Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra práva

Bakalářská práce

Právní úprava ochrany utajovaných informací v rezortu Ministerstva obrany

Jakub Machynek

© 2022 ČZU v Praze

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jakub Machynek

Veřejná správa a regionální rozvoj – k.s. Hradec Králové

Název práce

Právní úprava ochrany utajovaných informací v rezortu Ministerstva obrany

Název anglicky

Legislation of the protection of classified information in the Ministry of Defense

---

Cíle práce

Na základě rozboru platné právní úpravy provést vyhodnocení stavu z právního pohledu týkající se ochrany utajovaných informací v České republice se zaměřením na rezort Ministerstva obrany. Na základě zjištění vytvořit ideální bezpečnostní prostředí pro práci s utajovanými informacemi a jejich ukládání.

Metodika

Teoretická část se bude zabývat vysvětlením základních pojmů a souvislostí řešené problematiky. Praktická část se bude týkat stanovení míry rizika a vyhodnocení možných hrozeb úniku, nebo zneužití utajovaných informací. Na základě toho, bude vytvořen model zabezpečeného pracoviště pro uchovávání a zpracování utajovaných informací.

Doporučený rozsah práce

30 – 40 stran

Klíčová slova

Utajovaná informace, zabezpečená oblast, pracoviště, Ministerstvo obrany, bezpečnostní prověrka, Národní bezpečnostní úřad, zákon, stupeň utajení, žadatel, ochrana

---

Doporučené zdroje informací

Ing. Oldřich Luňáček, Ph.D. Druhy zajištění ochrany utajovaných informací OUI. UNOB reg. č.: CZ.1.01/2.2.00/15.0070

Jan Dvořák, Jiří Chrobák Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti Wolters Kluwer 2018 ISBN : 978-80-7598-016-8

Jan Kolouch CyberSecurity, CZ:NIC 2019 ISBN : 978-80-88168-31-7

JUDr. Ing. Ivan Pavelka PhD. Základní institut ochrany utajovaných informací v ČR – Správní právo Ročník L, ISSN 0139-6005.

POŽÁR, J. *Informační bezpečnost.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

Štěpán Kalamár, Markéta Brunová a kol. Vnitřní bezpečnost (vybraná témata ochrany utajovaných informací. Praha: Vysoká škola finanční a správní a.s. 2020 ISBN : 978-80-7408-202-3

Vyhláška č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti, ve znění pozdějších předpisů,

Vyhláška č. 405/2011 Sb., o průmyslové bezpečnosti ve znění vyhlášky č. 416/2013 Sb.

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

Zákon č. 413/2005 Sb., o změně zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

Předběžný termín obhajoby

2021/22 ZS – PEF

Vedoucí práce

Mgr. Michal Reichert, DiS.

Garantující pracoviště

Katedra práva

Elektronicky schváleno dne 5. 10. 2021

JUDr. Jana Borská, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 19. 10. 2021

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 05. 03. 2022

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci „Právní ochrana utajovaných informací v rezortu Ministerstva obrany“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15. 3. 2022 _____

Jakub Machynek

Poděkování

Rád bych touto cestou poděkoval Mgr. Michalu Reichertovi, DiS., za vedení práce a pomoc při jejím zpracování.

Právní úprava ochrany utajovaných informací v rezortu Ministerstva obrany

Abstrakt

Předkládaná práce se zabývá zhodnocením stavu české legislativy, která je implementována v oboru ochrany utajovaných informací v České republice se zaměřením na rezort Ministerstva obrany, tedy na zákony, nařízení vlády, vyhlášky, rozkazy ministra obrany anebo normativní výnosy ministerstva obrany. Kromě toho práce vyhodnocuje všechny výše uvedené právní normy, kterými se musí řídit osoby, které se seznamují s utajovanými informacemi a dokumenty. V praktické části se pak tato práce zabývá fyzickou bezpečností, respektive navržením vzorového fiktivního pracoviště pro zpracování utajovaných informací až do stupně „Přísně tajné“. Toto pracoviště má sloužit jak pro práci s utajovanými informacemi, tak i k jejich ukládání. Práce s takto citlivými informacemi je pro Ministerstvo obrany, a tedy obecně i pro celou armádu České republiky velmi důležitá, kdy dbá se na striktní dodržování pravidel pro zacházení s těmito informacemi.

Klíčová slova: Utajovaná informace, zabezpečená oblast, pracoviště, Ministerstvo obrany, bezpečnostní prověrka, Národní bezpečnostní úřad, zákon, stupeň utajení, žadatel, ochrana

Legislation on Classified Information at the Czech Ministry of Defence

Abstract

The presented thesis deals with evaluation of the Czech legislation being implemented in the field of protection of classified information in the Czech Republic, focusing on the Ministry of Defence itself, on the laws, government regulations, decrees and orders issued by the Minister of Defence, and on normative regulations issued by the Ministry of Defence. In addition, the thesis evaluates all the above-mentioned legal regulations and norms that are to be observed by the people getting acquainted with such classified information and/or classified documents. In its practical part, the thesis deals with a notion of specific security or, as the case may be, with a model fictitious workplace suggested for the classified information to be processed up to the "Top Secret" level. This workplace shall be used both for work with classified information and for storing it. The work with such sensitive information is crucially important not only for the Ministry of Defence, but also for the Czech armed forces in general, and it pays attention to strict adherence to the rules concerning the way of how to handle classified information.

Keywords: Classified information; secured area; workplace; Ministry of Defence; security clearance; National Security Authority; law; classification level; applicant; protection

Obsah

1 Úvod

Každá společnost v kterékoli době si uvědomovala a třídila informace na ty, které byly nedůležité, a na ty, které bylo potřeba chránit před únikem. Důvod byl jasný, a to náskok před konkurencí, ať to byly tajné receptury, zdroje obživy či rozmístění vojsk nebo taktiky při válečných konfliktech. Relevantní a včasně podaná informace totiž může znamenat přežití, vítězství nebo zisk. Tato výhoda mohla být využita pouze za předpokladu, že klíčová informace byla určena výlučně jedné osobě nebo úzkému okruhu osob a konkurenci byl ztížen přístup k této informaci. Vůle utajovat informace vznikla už v dávných dobách a držitel utajované informace se pokoušel vytvořit taková opatření, kterými by k nim ztížil přístup. Díky těmto opatřením mohl protivníka poškodit nebo připravit o výhodu. Vyzrazení znamenalo nebezpečí a přímou hrozbu, že bude těchto informací použito proti osobě, jejímž zájmem bylo tuto informaci chránit.

Stát je povinen chránit zájmy tak, aby nedošlo k ohrožení svrchovanosti ČR, k újmě na demokratických základech, poškození ekonomiky, dobrých diplomatických vztahů či ztrátám na životech a dalším závažným situacím. Právní řád ČR řeší oblast ochrany utajovaných informací, a to konkrétně zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti (dále jen „zákon o ochraně utajovaných informací“ nebo jen „ZUS“). Dále byly k tomuto zákonu vydány prováděcí právní předpisy upravující jednotlivé druhy zajištění ochrany utajovaných informací.

V rámci předkládané práce je ústřední pozornost věnována ochraně informací, které byly označeny z důvodu ohrožení bezpečnosti státu určitým stupněm utajení, a způsobu jejich ochrany, což představuje udržení jejich integrity a důvěrnosti. Na základě vlastních zkušeností ze služby u Vojenské policie a Vězeňské služby je vytvořeno modelové pracoviště určené ke zpracovávání a ukládání utajovaných informací i jednací oblasti. Tento projekt byl vybrán především z důvodů, že s utajovanými informacemi se seznamuji a osobně mne zajímají faktory, které tyto informace ochraňují, nebo přinejmenším minimalizují vznik situací, které vedou k ohrožení či ztrátě utajovaných informací.

2 Cíl práce a metodika

2.1 Cíle bakalářské práce

Cílem bakalářské práce je zhodnotit současný stav v legislativě týkající se ochrany utajovaných informací v ČR se zaměřením na rezort Ministerstva obrany (dále jen „MO“).

V praktické části je vytvořeno modelové pracoviště a navržen projekt fyzické bezpečnosti. Pracoviště v tomto projektu bude zpracovávat a ukládat utajované informace do stupně utajení „Přísně tajné“. Vytvořeno bude dle právních norem nastudovaných v průběhu služby u bezpečnostních složek a v průběhu vytváření této bakalářské práce. Bude zhodnoceno, zda jsou opatření fyzické bezpečnosti dostačující pro ochranu utajovaných informací a zda neobsahují zásadní nedostatky.

2.2 Metodika bakalářské práce

Z metodického hlediska se práce člení do tří hlavních částí.

1. Úvod, cíl a metodika práce
2. Teoretická část
3. Praktická část

Kapitola následující po cíli a použité metodice představuje teoretickou část, ve které je hlavní pozornost zaměřena na vysvětlení základních pojmů a souvislostí řešené problematiky. Dále rozpracovává právní normy pro problematiku ochrany utajovaných informací a interní předpisy rezortu MO. Obsahuje také popis orgánů zastřešujících tuto problematiku pro ČR a následně i pro MO.

Třetí částí je část praktická a ta se bude týkat stanovení míry rizika a vyhodnocení možných hrozeb úniku nebo zneužití utajovaných informací. Na základě toho bude vytvořen model zabezpečeného pracoviště pro uchovávání a zpracování utajovaných informací.

Hlavními datovými zdroji jsou dostupné zákony, navazující právní předpisy a doplňkově jsou využity odborné knihy, monografie, články a další relevantní internetové zdroje.

3 Právní úprava ochrany utajovaných informací v ČR

Problematika ochrany utajovaných informací je upravena v právním řádu ČR dvěma zásadními zákony. Ty jsou dále upřesňovány nařízeními vlády, vyhláškami a prováděcími předpisy Národního bezpečnostního úřadu (dále jen „NBÚ“). V rezortu MO jsou dále definovány vnitřní předpisy, které aplikují problematiku ochrany utajovaných informací do podmínek MO. Závazné jsou pro ČR také právní předpisy EU a NATO.

Obrázek 1: Posloupnost právních předpisů[1]

3.1 Historie informace a její předávání

Pojem informace vznikl z latinského *informare*, což znamená utváření, vrytí nebo ztvárnění. V dnešní době můžeme informaci vykládat mnoha způsoby dle vztahu k danému oboru. V nejobecnějším smyslu chápeme informaci jako údaj o prostředí, jeho stavu a procesech v něm probíhajícím.[2]

Předávání informací bylo pro přežití člověka klíčové již od pravěku, kdy se předávaly informace o rozdělávání ohně, výrobě nástrojů, ošacení, způsobu lovu, sběru jídla a vytváření přístřešků. Tyto informace se předávaly po generace. Některé se dochovaly až dodnes, jako malby na stěnách jeskyní, které zobrazovaly nejčastěji zvířata nebo činnosti, a můžeme si jen domýšlet, co jimi chtěl autor říci. Ve starověku se již běžně zaznamenávaly

[1] Vlastní zpracování na základě Evropská justice. *Vnitrostátní právní předpisy* [online]. 2020 [cit. 2022-01-26]. Dostupné z: https://e-justice.europa.eu/content_member_state_law-6-cz-maximizeMS-cs.do?member=1

[2] JONÁK, Z. Informace. *KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV)* [online]. Praha: Národní knihovna ČR, 2003 [cit. 2022-02-05]. Dostupné z: https://aleph.nkp.cz/F/?func=direct&doc_number=000000456&local_base=KTD

informace z nejdůležitějších oborů, jako bylo zemědělství, řemeslo a astronomie. Vznikaly i první kalendáře. To vše nejen za pomoci maleb, ale také písma. Avšak šíření informací se uskutečňovalo nejčastěji ústně, protože většina lidí tehdy neuměla číst ani psát. Ve středověku přišel obrat v šíření informací, a to díky vynálezu knihtisku, kdy se zkrátil čas strávený přepisováním knih, a tak se informace daly šířit rychleji. V novověku se již šíření informací skokově zrychlovalo. Pomocí telegrafu, tedy Morseovy abecedy, se dokázala informace dostat během pár minut na místo určení. Zpočátku se používal elektrický telegraf, který pomocí drátů přenášel zprávy mezi odesílatelem a příjemcem. Ten byl později nahrazen bezdrátovým telegrafem neboli radiotelegrafem, kdy příjemce nemusel být propojen drátem, ale musel být v dosahu antény. I bezdrátový telegraf byl nakonec vytlačen modernějšími technologiemi a byl nahrazen radiofonickými a telefonickými zvukovými zprávami, které měly vyšší přenosovou rychlost a byly srozumitelnější.[3] Telegrafie skončila s příchodem a rozvojem datových (digitálních) druhů přenosu dálnopisu a později faxu. Vývoj se dále ubíral přes telefonní modemy, satelitní transpondéry až k internetu, jak ho známe dnes.

3.2 Historie zákona o ochraně utajovaných informací

Ochrana utajovaných informací je jeden z nejzásadnějších úkolů národní a evropské bezpečnosti. Rozhoduje o tom, zda budeme úspěšní v boji proti vnitřním či vnějším hrozbám, ať už se jedná o terorismus, nebo o válečný konflikt, který se odehrává nejen na bojištích, ale rovněž v kyberprostoru. Cílem každé země je mít převahu nad nepřítelem, který představuje potencionální nebo reálnou bezpečnostní hrozbu. Zda bude tato převaha dostatečná, záleží na důsledné ochraně utajovaných informací, a tedy na její právní úpravě, které se bude tato práce věnovat.[4]

V novodobé české historii se setkáváme spíše s termínem „státní tajemství“, který byl poprvé upraven v roce 1923 v zákoně č. 50/1923 Sb. z. a n., na ochranu republiky, kde bylo velmi obecně popsáno jako: *„… skutečnost, opatření nebo předmět, jež vláda tají v důležitém zájmu republiky nebo jež v takovém zájmu mají zůstati utajeny před cizí*

[3] NĚMEČEK, K., VOPÁLENSKÝ, V. *Spojovací technika: telefonie. Učebnice pro 3. a 4. ročník SPŠST obor 37-46-6 spojová technika – oddělení telekomunikační technika po vedeních*. Praha: Nakladatelství dopravy a spojů, 1982, s. 13.

[4] PAVELKA, I. Institucionální zajištění ochrany utajovaných informací v ČR. *Správní právo* [online]. 2017, roč. L, č. 5, s. 258–268 [cit. 2022-02-02]. ISSN 0139-6005. Dostupné z: https://www.mvcr.cz/clanek/spravni-pravo-cislo-5-2017.aspx, s. 258.

mocí…"[5], pod čímž si můžeme představit prakticky cokoli, protože vláda nestanovila žádným předpisem výčet nebo klasifikaci těchto skutečností, opatření nebo předmětů. Toto vymezení pojmů převzal v roce 1948 tehdejší režim v zákoně č. 231/1948 Sb., na ochranu lidově demokratické republiky, který trestní sazby za vyzvědačství zvýšil na tresty doživotí nebo trest smrti, což bylo využíváno režimem v politických procesech v 50. letech. Definice státního tajemství se změnila pouze nepatrně: *„Státním tajemstvím se rozumí 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]

Až díky zákonu č. 102/1971 Sb., o ochraně státního tajemství, a na něj navazujícímu nařízení vlády č. 149/1971 Sb., o zvláštních skutečnostech tvořících státní tajemství, se podařilo vytvořit zákonnou formu vymezení státního tajemství. O vhodnosti jasně definovat státní tajemství svědčí i to, že tento zákon a nařízení vlády obstálo, pouze s dvěma novelizacemi, i v demokratickém režimu po roce 1989, dokud nebylo potřeba přijmout zákon, který by byl kompatibilní s režimem utajení ve státech Severoatlantické aliance. Tímto byl zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a změně některých zákonů, který zřizuje NBÚ, vymezuje jeho kompetence a kompetence dalších orgánů na tomto úseku, procesní a sankční pravidla v této oblasti nebo režim nakládání s utajovanými informacemi.[7] V roce 2005 byl vydán zatím poslední zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti (ZUS), který prozatím nejlépe reflektuje potřeby státu v oblasti utajovaných informací.

V reakci na stále větší digitalizaci a zvyšování hrozeb z kyberprostoru byl v roce 2014 vydán zákon č. 181/2014 Sb., o kybernetické bezpečnosti, a k 1. 8. 2017 byl podle § 21a odst. 1 zákona č. 205/2017 Sb. zřízen Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB").

---

[5] § 5 odst. 1 a § 6 odst. 2 zákona č. 50/1923 Sb. z. a n., na ochranu republiky.
[6] § 5 odst. 3 zákona č. 231/1948 Sb., na ochranu lidově demokratické republiky.
[7] SVATOŠOVÁ, H. *Návrh zákona o ochraně utajovaných informací – studie a připomínky: Studie k úpravě utajovaných skutečností v historii, v zahraničí a rozbor návrhu nového zákona o utajovaných informacích ve verzi z prosince 2003* [online]. Praha: Iuridicum Remedium, 2004 [cit. 2022-01-26]. Dostupné z: https://www.iure.org/sites/default/files/article/downloads/07_navrh_zakona_o_ochrane_utajovanych_informaci.pdf, s. 3.

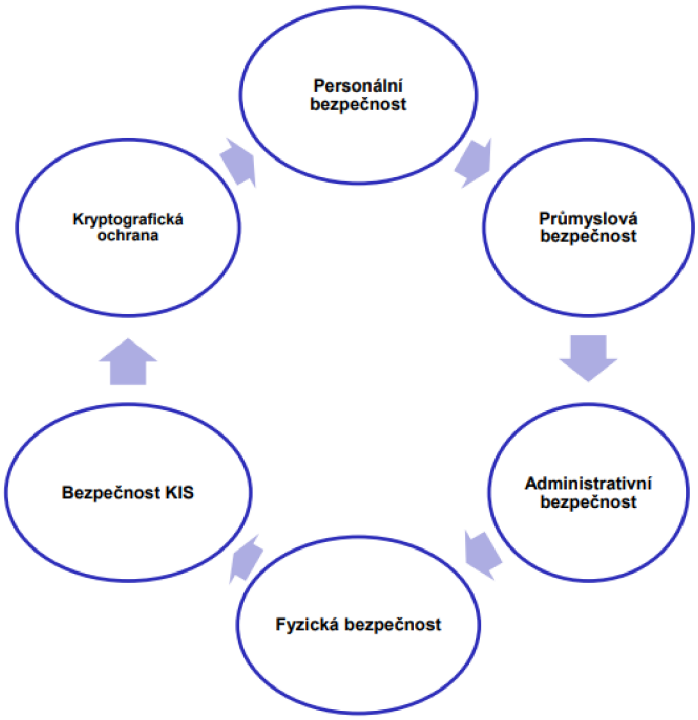
3.3 Zákony upravující ochranu utajovaných informací

3.3.1 Zákon č. 412/2005 Sb., zákon o ochraně utajovaných informací

Utajovaná informace se klasifikuje v ZUS těmito stupni utajení.

- Přísně tajné – za přísně tajnou označujeme informaci, jejíž vyzrazení neoprávněné osobě nebo její zneužití může způsobit mimořádně vážnou újmu zájmům ČR,
- Tajné – za tajnou označujeme informaci, jejíž vyzrazení neoprávněné osobě nebo zneužití může způsobit vážnou újmu zájmům ČR,
- Důvěrné – za důvěrnou označujeme informaci, jejíž vyzrazení neoprávněné osobě nebo zneužití může způsobit prostou újmu zájmům ČR,
- Vyhrazené – za vyhrazenou označujeme informaci, jejíž vyzrazení neoprávněné osobě nebo zneužití může být nevýhodné pro zájmy ČR.[8]

Obrázek 2: Druhy zajištění OUI[9]



[8] § 4 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.
[9] LUŇÁČEK, O. *Fyzická bezpečnost: Druhy zajištění ochrany utajovaných informací (OUI)* [online]. Brno: Univerzita obrany, 2004 [cit. 2022-01-26]. Dostupné z: https://moodle.unob.cz/pluginfile.php/18153/mod_resource/content/9/Druhy%20zaji%C5%A1t%C4%9Bn%C3%AD.pdf

Tento stěžejní zákon řešící tuto problematiku legislativně zajišťuje ochranu utajovaných informací v ČR, a to zejména v těchto oblastech:

- personální bezpečnost,
- průmyslová bezpečnost,
- administrativní bezpečnost,
- fyzická bezpečnost,
- bezpečnost informačních a komunikačních systémů,
- kryptografická ochrana.

Personální bezpečnost

Personální bezpečnost se především zaměřuje na výběr, výchovu a obranu zaměstnanců, kteří se setkávají s utajovanými informacemi. Tyto osoby musí splňovat podmínky NBÚ pro získání osvědčení fyzické osoby na stupně „Důvěrné", „Tajné" a „Přísně tajné". Na stupeň „Vyhrazené" po splnění podmínek níže uvedených vydává osvědčení velitel organizačního celku. Jednou za rok je odpovědná osoba povinna zajistit proškolení osob, které mají přístup k utajovaným informacím, a o proškolení vést dokumentaci. Toto proškolení se týká právních předpisů v oblasti ochrany utajovaných informací. Ministerstva a další správní orgány mají povinnost do 31. 6. vypracovat a odeslat personální projekt NBÚ, kde se hodnotí stav personální bezpečnosti za uplynulý rok, dále tento projekt obsahuje počet utajovaných informací, počet přístupů k těmto informacím, počet držitelů osvědčení a předpokládaný počet osob, u kterých bude nutné v následujícím roce provést bezpečnostní řízení, včetně stupně utajení.[10]

Podmínky fyzických osob pro seznamování se s utajovanými informacemi

Jestliže je fyzická osoba držitelem osvědčení fyzické osoby[11] nebo dokladu o bezpečnostní způsobilosti[12], je poučena a seznámení se s utajovanými informacemi je nezbytné pro výkon její funkce, pracovní či jiné činnosti, lze umožnit fyzické osobě přístup k utajované informaci do výše daného stupně utajení.

---

[10] NBÚ. *Obecně k personální bezpečnosti* [online]. Praha: Národní bezpečnostní úřad [cit. 2022-01-26]. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/personalni-bezpecnost-oznameni-pro-v-osvedceni-d-t-pt-certifikaty/1043-obecne-k-personalni-bezpecnosti/

[11] § 54 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

[12] § 80 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

Seznamování se s utajovanými informace ve stupni utajení „Vyhrazené“ (V)

Osvědčení fyzické osoby pro stupeň „Vyhrazené“ vydává velitel organizačního celku na základě prohlášení fyzické osoby o svéprávnosti, dovršení 18 let věku a výpisu z evidence Rejstříku trestů, který nesmí být starší 3 měsíců a kterým se dokládá bezúhonnost. Toto Oznámení o splnění podmínek pro přístup k utajované informaci stupně utajení „Vyhrazené“ velitel vlastnoručně podepíše, předá fyzické osobě a kopii založí do personálního spisu spolu s dokumenty výše uvedenými.

Zákon dále ukládá v § 10 další povinnosti.[13]

Seznamování se s utajovanými informacemi ve stupni utajení „Důvěrné“ (D), „Tajné“ (T) a „Přísně tajné“ (PT)

Odpovědná osoba provede nebo zajistí poučení před prvním přístupem k utajované informaci stupně „Přísně tajné“, „Tajné“ nebo „Důvěrné“. Poučení fyzická osoba podepíše společně s odpovědnou osobou ve třech výtiscích, jeden si ponechá fyzická osoba, jeden se uloží do spisu a jeden se odešle NBÚ.[14] NBÚ vydá osvědčení fyzické osoby tomu, kdo je občanem ČR, je svéprávný, bezúhonný a dovršil věk 18 let, je osobnostně způsobilý a bezpečnostně spolehlivý. Tyto podmínky musí splňovat po celou dobu držení osvědčení. Osobnostní způsobilost znamená, že fyzická osoba netrpí poruchou nebo obtížemi, které mají vliv na spolehlivost nebo schopnost utajovat informace.[15] Bezpečnostní spolehlivost je specifikována v § 14 ZUS.

Platnost osvědčení fyzické osoby dle § 55 ZUS:[16]

- ve stupni „Přísně tajné“ 5 let,
- ve stupni „Tajné“ 7 let,
- ve stupni „Důvěrné“ 9 let.

Zákon o ochraně utajovaných informací pamatuje v § 58 na osoby se zvláštním přístupem ke všem stupňům utajovaných informací bez potřeby platného osvědčení fyzické osoby a poučení. Jsou to prezident republiky, poslanci, senátoři, členové vlády, veřejný

[13] DVOŘÁK, J., CHROBÁK, J. *Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti: komentář*. Praha: Wolters Kluwer, 2018. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7598-016-8, s. 51.
[14] § 17 odst. 2 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.
[15] § 12 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.
[16] DVOŘÁK, J., CHROBÁK, J. *Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti: komentář*. Praha: Wolters Kluwer, 2018. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7598-016-8, s. 191.

ochránce práv a zástupce veřejného ochránce práv, soudci, prezident, viceprezident a členové Nejvyššího kontrolního úřadu. Dále jsou v § 60 odst. 1 a § 58 odst. 3 a 4 téhož zákona popsané osoby, které mají zvláštní přístup k utajovaným informacím.

Průmyslová bezpečnost

K zajišťování a ověřování podmínek pro přístup podnikatelů k utajovaným informacím a k zajištění správné manipulace s utajovanými informacemi slouží systém opatření, který tvoří průmyslovou bezpečnost. Jestliže podnikatel ke své činnosti potřebuje přístup k UI, umožní se mu přístup k informaci do stupně „Vyhrazené" za předpokladu doložení písemného prohlášení, že je schopen zabezpečit ochranu utajovaných informací nebo, že je držitelem platného osvědčení podnikatele. Toto osvědčení vydá NBÚ podnikateli, který je ekonomicky stabilní, bezpečnostně způsobilý, je schopen zabezpečit ochranu těchto informací, jestliže odpovědná osoba je držitelem platného osvědčení fyzické osoby nejméně pro takový stupeň utajení, pro který žádá podnikatel o vydání osvědčení podnikatele, který při podání žádosti uhradil správní poplatek. Podnikatel musí splňovat podmínky, které jsou upraveny v § 17 až § 19 ZUS a to po celou dobu platnosti osvědčení podnikatele.[17] Osvědčení se vydává pro stupně „Důvěrné", „Tajné", „Přísně tajné".

Administrativní bezpečnost

Cílem systémových opatření, která tvoří administrativní bezpečnost, je ochrana utajovaných informací při jejich tvorbě, evidenci, zpracování, ukládání, příjmu, archivaci, vyřazování a skartaci nebo jiné manipulaci. O všech utajovaných informacích musí být přehled, tedy kde je místo jejich uložení, stav a pohyb. O všech těchto skutečnostech se musí vést evidence, a to i o osobách, které s nimi přišly do kontaktu. Pravidla administrativní bezpečnosti jsou uvedena v § 21 až 23 ZUS. Velmi důležitá je správná specifikace a označení utajované informace v souladu s požadavky zákona, protože při nesplnění nebo nesprávném označení utajované informace se jedná o jeden z případů neoprávněného nakládání s utajovanou informací.

[17] DVOŘÁK, J., CHROBÁK, J. *Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti: komentář*. Praha: Wolters Kluwer, 2018. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7598-016-8, s. 96–101.

Fyzická bezpečnost

Účelem systémových opatření fyzické bezpečnosti je zabránit nebo ztížit přístup k utajovaným informacím neoprávněné osobě nebo pokus tento přístup zaznamenat. Na rozdíl od administrativní bezpečnosti formuluje fyzická bezpečnost zásady, pravidla a opatření režimová a technická, která jsou spjatá bezprostředně s fyzickým objektem, kde se utajované informace nacházejí. Fyzická bezpečnost je souhrn opatření, tedy ostraha, nasazení technických prostředků a režimová opatření. Opatření se stanovují na základě nejvyššího stupně utajované informace, která má být v objektu uložena nebo zpracovávána, a dále na základě vyhodnocení rizik. Každý objekt má stanovena rizika dle specifických podmínek objektu a tato rizika se vyhodnocují dle bodového ohodnocení jednotlivých opatření fyzické bezpečnosti. Toto hodnocení má zásadní význam pro určení rozsahu a způsobu použití příslušných bezpečnostních opatření. Použité technické prostředky musí být certifikovány NBÚ. Technické prostředky, které nemají certifikaci, se mohou jen doplňkově a v případě, že tím nedojde ke snížení požadované ochrany pro daný stupeň utajení. Certifikací technických prostředků se rozumí schválení technických prostředků NBÚ.

Bezpečnost informačních a komunikačních systémů

V oblasti bezpečnosti informačních a komunikačních systémů vykonává státní správu NÚKIB. Tato oblast je tvořena systémem opatření, která zajišťují integritu, důvěrnost a dostupnost utajovaných informací, se kterými tyto systémy pracují.

Informačním systémem nakládajícím s utajovanými informacemi se pro účely tohoto zákona rozumí jeden nebo více počítačů, jejich programové vybavení a k tomu patřící periferní zařízení, správa tohoto informačního systému a k tomuto systému se vztahující procesy nebo prostředky schopné provádět sběr, tvorbu, zpracování, ukládání, zobrazení nebo přenos utajovaných informací.[18]

Takovýto informační systém musí být certifikován NÚKIB dle § 46 odst. 1 písm. b) ZUS a písemně schválen do provozu odpovědnou osobou nebo osobou pověřenou. Schválení informačního systému do provozu je odpovědná osoba nebo osoba pověřená povinná písemně oznámit NÚKIB do 30 dnů od tohoto schválení.

Požadavky na informační systém a podmínky jeho bezpečného provozování v závislosti na stupni utajení utajovaných informací dále řeší vyhláška č. 523/2005 Sb.,

[18] § 34 odst. 1 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor. Tato vyhláška také stanovuje požadavky na informační a komunikační systémy nakládající s utajovanými informacemi a požadavky na provádění certifikace informačních systémů a stínicích komor a požadavky na schvalování projektů bezpečnosti komunikačních systémů. Komunikační systém zajišťuje přenos utajovaných informací mezi koncovými uživateli, který zahrnuje koncové komunikační zařízení, kryptografické prostředky, přenosové prostředí, obsluhu a provozní podmínky a postupy. Komunikační systém musí být v souladu s projektem bezpečnosti komunikačního systému, který je schválen NÚKIB nebo NBÚ, a jeho uvedení do provozu je schváleno písemně odpovědnou osobou nebo osobou pověřenou.[19]

Kryptografická ochrana

Kryptografii je možné definovat jako vědu, která konstruuje a aplikuje matematické metody, a tím zajišťuje důvěrnost a autentičnost zpráv. Zprávou se rozumí posloupnost symbolů, kde je zakódována informace veřejným kódem. Symboly mají podobu buď obrazů, pohyblivých obrazů, anebo podobu písmen neboli textu. Ve všech případech je možno jednotlivé symboly nahradit čísly, tedy vyjádřit zprávu jako posloupnost čísel. Tato podoba nám dovoluje matematickými operacemi tuto zprávu zabezpečit.[20]

Kryptografickou ochranu utajovaných informací má ve své působnosti NÚKIB, který zde vykonává legislativní působnost, metodickou činnost a kontrolu. NÚKIB provádí v rámci zajištění informačních a komunikačních systémů certifikace kryptografických prostředků, pracovišť a stínicích komor, které zamezují úniku utajovaných informací kompromitujícím vyzařováním.[21] V oblasti kryptografické ochrany utajovaných informací vykonává NÚKIB zkoušky zvláštní odborné způsobilosti. Úřad po splnění těchto zkoušek vydá osvědčení o zvláštní odborné způsobilosti pracovníka kryptografické ochrany. Výkon kryptografické ochrany smí provádět pouze pracovník, který je držitelem osvědčení

[19] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.
[20] BURDA, K. *Úvod do kryptografie*. Brno: Akademické nakladatelství CERM®, 2015. 110 s. ISBN 978-80-7204-925-7, s. 7–8.
[21] PAVELKA, I. Institucionální zajištění ochrany utajovaných informací v ČR *Správní právo* [online]. 2018, roč. LI, č. 3, s. 202–216 [cit. 2022-02-02]. ISSN 0139-6005. Dostupné z: https://www.mvcr.cz/webpm/clanek/spravni-pravo-cislo-3-2018.aspx

o zvláštní odborné způsobilosti pracovníka kryptografické ochrany, je držitelem platného osvědčení fyzické osoby a je pověřen odpovědnou osobou nebo osobou pověřenou.[22]

3.3.2 Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

V tomto zákoně je upravena působnost a pravomoci orgánu veřejné moci v oblasti kybernetické bezpečnosti, kterým je NÚKIB, a dále práva a pravomoci osob v této oblasti. Je zde také část zákona, která zapracovává předpisy EU v oblasti kybernetické bezpečnosti a upravuje zajišťování sítí elektronických komunikací a informačních systémů.

Citovaným zákonem, resp. jeho § 21a, se zřizuje NÚKIB, který má sídlo v Brně a § 22 stanovuje úkoly tohoto úřadu. Dále zákon řeší kontrolní činnost a přestupky, kterých se může dopustit právnická nebo fyzická osoba.[23]

3.4 Nařízení vlády

Nařízení vlády č. 522/2005 Sb. stanoví seznam utajovaných informací. Toto nařízení zakotvuje seznam utajovaných informací jednotlivých orgánů státní moci a také rozmezí klasifikace těchto informací. Ty jsou uvedeny v přílohách nařízení.

3.5 Vyhlášky NBÚ upravující ochranu utajovaných informací

Vyhlášky NBÚ dále rozvíjejí ZUS a doplňují jednotlivé části zákona. Z pohledu této práce bude stěžejní vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů (dále také jen „vyhláška o fyzické bezpečnosti a certifikaci technických prostředků“) podle které se bude sestavovat projekt fyzické bezpečnosti a fiktivní model pracoviště ochrany informací.

- Vyhláška č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti, ve znění pozdějších předpisů,
- Vyhláška č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací, ve znění vyhlášky č. 417/2013 Sb.,

[22] § 38 odst. 2 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.
[23] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti.

- Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, ve znění vyhlášky č. 453/2011 Sb.,
- Vyhláška č. 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací, ve znění vyhlášky č. 434/2011 Sb.,
- Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů,
- Vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů.

3.6 Orgány zastřešující ochranu utajovaných informací v ČR

Zásadními orgány, prostřednictvím nichž je řešena otázka ochrany utajovaných informací v ČR, jsou NBÚ a NÚKIB. Od těchto orgánů se odvíjí veškeré upřesňující legislativní dokumenty týkající se této problematiky.

3.6.1 NBÚ

Od vydání zákona č. 148/1998 Sb., zákona o ochraně utajovaných skutečností, se postavení NBÚ nezměnilo. *„Je orgánem výkonné moci, je ústředním správním úřadem pro oblast ochrany utajovaných informací a bezpečnostní způsobilosti.“*[24]

Náleží tedy do soustavy správních i ústředních úřadů. Práce NBÚ spočívá v analytické a vyhodnocovací činnosti. Informace získává od samotného prověřovaného, fyzických a právnických osob, příslušných orgánů státu, z evidencí, registrů vedených příslušnými orgány státu a organizacemi a z veřejných zdrojů. Poté co NBÚ zjistí, že neexistují překážky, které by bránily v přístupu k utajovaným informacím nebo vykonávání citlivých činností, vydá osvědčení fyzické nebo právnické osoby. Chrání tím důležité zájmy ČR pro obranu, ekonomiku, bezpečnost, a tím přispívá k ochraně zdraví, života a majetku občanů.

[24] NBÚ. *O nás* [online]. Praha: Národní bezpečnostní úřad [cit. 2022-01-26]. Dostupné z: https://www.nbu.cz/cs/o-nas/955-o-nas/

Hlavní úkoly NBÚ:

- Rozhoduje o vydání osvědčení fyzické osoby, osvědčení podnikatele a o vydání dokladu o bezpečnostní způsobilosti fyzické osoby. Dále rozhoduje o zrušení platnosti osvědčení fyzické osoby, osvědčení podnikatele a dokladu o bezpečnostní způsobilosti.
- Plní úkoly v oblasti ochrany utajovaných informací v souladu se závazky vyplývajícími z členství ČR v EU. ČR je také vázána na organizaci Severoatlantické aliance a na další mezinárodní smlouvy.
- V určených případech dává souhlas k poskytování utajovaných informací v mezinárodním styku, vede ústřední registr a schvaluje zřízení registrů.
- Ukládá sankce za nedodržení povinností stanovených zákonem a vykonává kontroly.

NBÚ není pověřen vyšetřovacími pravomocemi ani oprávněním orgánů činných v trestním řízení, není zpravodajskou službou a tyto instituce nevyužívá, a ze zákona ani nemůže.[25]

3.6.2 NÚKIB

Byl zřízen na základě zákona č. 205/2017 Sb., o kybernetické bezpečnosti, kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti. NÚKIB je orgánem veřejné moci v oblasti kybernetické bezpečnosti. Stará se o ochranu utajovaných informací v oblasti informačních a komunikačních systémů a o kryptografickou ochranu. Dále řeší problematiku veřejně regulované služby navigačního systému Galileo (PRS).[26] Mimo jiné jím byla implementována směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společenské úrovně bezpečnosti sítí a informačních systémů v Unii. NÚKIB převzal po NBÚ práva a povinnosti v oblasti kybernetické bezpečnosti včetně ochrany utajovaných informací v oblasti informačních a telekomunikačních systémů a kryptografické ochrany.[27] Oblasti působnosti a oprávnění jsou dále popsány v § 137a a § 138 ZUS.

---

[25] NBÚ. *O nás* [online]. Praha: Národní bezpečnostní úřad [cit. 2022-01-26]. Dostupné z: https://www.nbu.cz/cs/o-nas/955-o-nas/

[26] NÚKIB. *O úřadu* [online]. Praha: Národní úřad pro kybernetickou a informační bezpečnost [cit. 2022-01-26]. Dostupné z: https://www.nukib.cz/cs/o-nukib/o-uradu/

[27] KOLOUCH, J., BAŠTA, P. *CyberSecurity*. Praha: CZ.NIC, 2019. ISBN 978-80-88168-31-7, s. 93.

4 Legislativní úprava ochrany utajovaných informací v rezortu MO

Legislativní dokumenty pro potřeby MO jsou vydávány tak, aby aplikovaly zákony a navazující právní předpisy pro interní účely. V rezortu MO se dále tvoří a zpracovávají utajované informace používané na mezinárodní úrovni, zejména NATO a EU.

4.1 Ministerstvo obrany (MO)

Bylo zřízeno zákonem č. 548/1992 Sb., kterým byl změněn zákon č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy ČR, a byla jím stanovena jeho působnost. MO je ústředním orgánem státní správy zejména pro zabezpečování obrany ČR, řízení AČR a správu vojenských újezdů.[28]

V čele rezortu MO stojí v současné době ministryně obrany.

4.2 Utajované informace NATO

Předpisy NATO nejsou volně k dispozici a nesou označení jako utajovaná informace. V případě NATO UNCLASSIFIED, neboli neutajovaných informací, může žadatel u odboru administrativní a fyzické bezpečnosti NBÚ zažádat o poskytnutí takového dokumentu. V žádosti zdůvodní, jak požadované informace souvisí s jeho činností. Uvede platný poštovní kontakt a po zvážení žádosti ze strany NBÚ může být požadovaný předpis poskytnut. V případě utajovaných předpisů žadatel kromě zdůvodnění také doloží, zda je oprávněn k přístupu k utajovaným informacím a do jakého stupně.[29]

Utajované informace NATO se dělí do čtyř skupin, a to následovně:

- COSMIC TOP SECRET (CTS) – neoprávněné vyzrazení této informace nebo materiálu by způsobilo Severoatlantické alianci mimořádně vážnou škodu
- NATO SECRET (NS) – neoprávněné vyzrazení této informace nebo materiálu by způsobilo Severoatlantické alianci vážnou škodu.

[28] § 16 zákona č 2/1969 Sb., České národní rady o zřízení ministerstev a jiných ústředních orgánů státní správy České socialistické republiky.
[29] NBÚ. *Předpisy NATO vztahující se k ochraně utajovaných informací* [online]. Praha: Národní bezpečnostní úřad [cit. 2022-02-02]. Dostupné z: https://www.nbu.cz/cs/pravni-predpisy/1078-predpisy-nato-vztahujici-se-k-ochrane-utajovanych-informaci/

- NATO CONFIDENTIAL (NC) – neoprávněné vyzrazení této informace nebo materiálu by poškodilo zájmy Severoatlantické aliance.
- NATO RESTRICTED (NR) – neoprávněné vyzrazení této informace nebo materiálu by bylo pro zájmy nebo působnost Severoatlantické aliance nevýhodné.

Dokumenty, které nejsou utajovány, jsou označovány NATO UNCLASSIFIED.

V případě dokumentů týkajících se oblasti zbraní hromadného ničení, je tato informace označována ATOMAL.[30]

4.3 Utajované informace Evropské Unie

Rozhodnutím Rady 2013/488/EU o bezpečnostních pravidlech na ochranu utajovaných informací EU stanovila Rada EU základní zásady a standardy pro ochranu EUCI. Tyto zásady a standardy se vztahují na Radu EU a její generální sekretariát a musí je dodržovat i členské státy, pokud s EUCI pracují. Rozhodnutí Rady stanovuje několik způsobů ochrany včetně personální, fyzické a průmyslové bezpečnosti, a také způsoby sdílení EUCI v rámci orgánů EU s mezinárodními organizacemi a třetími zeměmi.

Dle závažnosti dopadu při vyzrazení jsou UECI rozděleny do čtyř úrovní:

- TRÈS SECRET UE / EU TOP SECRET: vyzrazením by mohlo dojít k závažnému ohrožení zásadních zájmů jednoho nebo více států nebo EU.
- SECRET UE / EU SECRET: vyzrazením by mohlo dojít k vážnému poškození zásadních zájmů jednoho nebo více států nebo EU.
- CONFIDENTIEL UE / EU CONFIDENTIAL: vyzrazením by mohlo dojít k poškození zásadních zájmů jednoho nebo více států nebo EU.
- RESTREINT UE / EU RESTRICTED: vyzrazením by mohlo dojít ke znevýhodnění jednoho nebo více států nebo EU.[31]

[30] NATO. *Security brief* [online]. North Atlantic Treaty Organization [cit. 2022-02-02]. Dostupné z: https://www.act.nato.int/images/stories/structure/reserve/hqrescomp/nato-security-brief.pdf

[31] Evropská rada, Rada Evropské unie. *Ochrana utajovaných informací Evropské unie (EUCI)* [online]. 2020 [cit. 2022-02-14]. Dostupné z: https://www.consilium.europa.eu/cs/general-secretariat/corporate-policies/classified-information/

4.4 Rozkazy ministra obrany

Rozkazy ministra obrany (dále jen „RMO“) slouží k aplikaci zákonů a dalších právních norem do prostředí MO a jako takové mají působnost pouze v rezortu MO:

- RMO č. 33/2012, ve znění RMO č. 98/2014 Věstníku, o personální bezpečnosti v rezortu MO.
- RMO č. 14/2013, ve znění RMO č.3/2019 Věstníku, o ochraně utajovaných informací v rezortu MO.

4.5 Normativní výnosy MO

Normativní výnosy MO (dále jen „NV MO“) plní stejnou funkci jako RMO, avšak mají nižší právní sílu.

- NV MO č. 77/2013 Věstníku, o fyzické bezpečnosti v rezortu MO.
- NV MO č. 111/2013 Věstníku, o kryptografické ochraně utajovaných informací v rezortu MO.
- NV MO č. 85/2013 Věstníku, o bezpečnosti informačních a komunikačních systémů a elektronických zařízení nakládajících s utajovanými informacemi.

4.6 Sekce zastřešující ochranu utajovaných informací v rezortu MO

MO je velký celek čítající desetitisíce zaměstnanců, kteří slouží či pracují na celém území České republiky. Tito pracovníci zpracovávají tisíce utajovaných informací a informací pro služební potřebu. Z důvodu zajištění ochrany utajovaných informací jsou v rezortu MO zřízena specializovaná pracoviště popsaná dále.

4.6.1 Odbor bezpečnosti MO

Ustanovení § 69 ZUS ukládá orgánům státu povinnost garantovat dodržování právních předpisů, a proto byl zřízen Odbor bezpečnosti MO (dále jen „OB MO“), který tuto funkci vykonává. NBÚ totiž není schopen sám kontrolovat dodržování těchto zásad. OB MO tedy zajišťuje ochranu utajovaných informací dle zákona a mezinárodních smluv, provádí kontrolní činnost nad dodržováním zákona a další podmínky dané zákonem. Dále aplikuje zákony a právní předpisy spojené s ochranou utajovaných informací a řídí se jimi, konkrétně zákony, vyhláškami, prováděcími předpisy a vnitřními předpisy. V čele OB MO je

ustanoven bezpečnostní ředitel, který je odpovědnou osobou a zabezpečuje součinnost mezi rezortem MO a správními úřady v oblasti utajovaných informací.

4.6.2 Rada pro kybernetickou bezpečnost a CIRC (Computer Incident Response Capability)

V rezortu MO zajišťují kybernetickou a komunikační bezpečnost dva subjekty.

1) Rada pro kybernetickou bezpečnost MO, jedná se o vrcholný orgán kybernetické obrany. Rada je taktéž kontaktním orgánem pro NÚKIB, resp. NBÚ, a je hlavním koordinačním a poradním orgánem ministryně obrany.
2) CIRC, které je zařazeno pod Velitelství kybernetických sil a informačních operací (dále jen „VeKySIO“). Z pohledu kybernetické bezpečnosti pokrývá celý rezort MO. Hlavním cílem CIRC je detekce kybernetických bezpečnostních hrozeb a incidentů, což vykonává díky nepřetržitému monitoringu různých částí datových sítí rezortu MO. Následně tyto informace vyhodnocuje, analyzuje a podává o nich zprávu relevantním partnerům. Dále chrání informační systémy a data v nich uložená, technické prostředky a na svém informačním portálu poskytuje rady, návody a postupy pro bezpečnou práci v informačních systémech, aby se uživatele připravili na potenciální počítačové útoky a hrozby.

5 Projekt fyzické bezpečnosti

V této části práce je pracováno se zákonem o ochraně utajovaných informací, a zejména s vyhláškou o fyzické bezpečnosti a certifikaci technických prostředků. Projekt fyzické bezpečnosti obsahuje prioritně umístění zabezpečených oblastí v objektu včetně jejich tříd, kategorií a způsobu použití vnitřních opatření při vnější a vnitřní ochraně objektu. Běžně se v rezortu MO označují zabezpečené oblasti, které zpracovávají a ukládají utajované informace, zkratkou POI. Tato zkratka znamená pracoviště ochrany informací.

Vnější ochrana objektu – jedná se nejen o hranice objektu, ale i vstupy do objektu, ochranu nouzových cest a jiných průlezných otvorů do objektu. Je zabezpečována fyzickou ostrahou objektu, technickými prostředky i režimovými opatřeními.

Vnitřní ochrana objektu – jedná se o soubor bezpečnostních opatření, mezi které patří fyzická ostraha objektu, technické prostředky a režimová opatření. Její rozsah a podmínky nesmí být v rozporu s projektem fyzické bezpečnosti. V zabezpečené oblasti musí být obsaženy certifikované prostředky příslušných kategorií.

Certifikace – rozumí se jí proces ověřování a schvalování způsobilosti technických prostředků, informačních systémů a kryptografických prostředků používaných při ochraně utajovaných informací. Též shoda technických prostředků, informačních systémů a kryptografických prostředků s bezpečnostními standardy. Certifikaci provádí NBÚ, NÚKIB nebo jimi pověřená organizace, která stanoví právním předpisem postupy, způsoby certifikačního procesu a náležitosti certifikátu.[32]

Dále je pracováno s pojmy, které jsou vymezeny níže:

- Objekt – je ohraničený prostor nebo budova, kde se obvykle nacházejí zabezpečené nebo jednací oblasti.
- Hranice objektu – je fyzická bariéra (oplocení) či jinak viditelně vymezený pozemek nebo plášť budovy
- Hranice zabezpečené oblasti nebo jednací oblasti – stavebně nebo jinak viditelně ohraničený prostor.

[32] § 46 zákona č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, ve znění pozdějších předpisů.

- Vstup do objektu nebo jednací oblasti, zabezpečené oblasti – místo, které je určené pro vstup a výstup osob, ale jedná se i o místo, které je stanovené pro vjezd a výjezd dopravních prostředků.
- Hrozba – riziko vyzrazení nebo zneužití utajované informace, které může vzniknout při narušení fyzické bezpečnosti.
- Riziko – jedná se o pravděpodobnost uskutečnění určité hrozby
- Mimořádná situace – stav, kdy bezprostředně hrozí, že dojde ke zneužití nebo vyzrazení utajované informace.
- Technické prostředky – bezpečnostní prvek, zabraňující, stěžující nebo omezující narušení ochrany objektu nebo zaznamenávající tento pokus.[33]
- Fyzická ostraha – je zabezpečena vyškolenými zaměstnanci provozovatele objektu, příslušníky ozbrojených sil nebo zaměstnanci pověřené bezpečnostní služby.

Mezi technické prostředky patří:

- Mechanické zábranné prostředky, kterými jsou úschovné objekty, zámky, dveře, mříže, folie, rámy a skla.
- Elektronická zámková zařízení a systémy pro zabezpečení vstupů do objektů a zabezpečených oblastí, zařízení a systémy sloužící k elektronickému prokazování oprávněnosti a totožnosti osob.
- Zařízení elektrické zabezpečovací signalizace sloužící ke zjišťování a vyhodnocování neoprávněného vstupu.
- Speciální televizní systémy pro snímání, přenos a zobrazování pohybu osob a dopravních prostředků v objektech.
- Tísňové systémy, zejména tísňové hlásiče, které fungují jako součást elektrické zabezpečovací signalizace.
- Zařízení elektrické požární signalizace.
- Detektory látek nebo zařízení sloužící zejména k detekci kovů.
- Zařízení proti pasivnímu a aktivnímu odposlechu utajovaných informací z míst vně objektu.[34]

[33] § 2 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.
[34] § 3 odst. 4 písm. c) vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.

Režimová opatření – určují režim vstupu a výstupu osob a vjezdu a výjezdu dopravních prostředků do objektu. Tato opatření stanovují:

- Oprávnění osob a dopravních prostředků pro vstup a vjezd do objektu, výstup a výjezd z objektu a způsob kontroly.
- Podmínky a způsob kontroly vynášení a vyvážení utajovaných informací z objektu.
- Režim pohybu osob, dopravních prostředků a utajovaných informací v objektu a jeho jednotlivých částech v pracovní i mimopracovní dobu.
- Režim manipulace s klíči, identifikačními prostředky a médii, která se používají pro systémy zabezpečení vstupů. Důležitou činností u vstupů je zejména systém a způsob označování, přidělování a odevzdávání klíčů, jejich úschovny, evidence, uložení duplikátů a způsob jejich použití.
- Režim manipulace s technickými prostředky a jejich používání.[35]

5.1 Vyhodnocení rizik

Dle normativního výnosu Ministerstva obrany č. 77/2013 Věstníku, o fyzické bezpečnosti v rezortu MO vyhodnocuje rizika a definuje požadavky na opatření fyzické bezpečnosti bezpečnostní manažer daného objektu.[36] Každý objekt má specifické požadavky, na základě kterých nejde sjednotit ani postup ani jednotlivé body. Proto nikde není specifikována jednotná forma vyhodnocení rizik. V praxi probíhá vyhodnocování rizik tak, že se ustanoví komise, skládající se z bezpečnostního manažera, odborníka z oddělení řízení a správy bezpečnostních systémů, velitele Vojenské policie pro daný objekt a pracovníka oddělení bezpečnosti. Toho vyhodnocení se poté předkládá veliteli organizačního celku, tedy odpovědné osobě.

V rezortu MO vznikají utajované informace stupně „Vyhrazené“, „Důvěrné“, „Tajné“ a „Přísně tajné“. Tyto informace zde nejen vznikají, ale jsou i poskytovány rezortu MO od jiných subjektů. Utajované informace se v rezortu MO nacházejí v listinné i elektronické podobě. Práce s elektronickými dokumenty v rezortu MO je zajištěna informačním systémem certifikovaným NBÚ, který do užívání schválila odpovědná osoba. Aktivy v rezortu MO jsou utajované informace, nosiče těchto informací v listinné i elektronické formě, vojáci z povolání a občanští zaměstnanci.

---

[35] § 6 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.
[36] Čl. 3 č. 9) písm. a) normativního výnosu MO č. 77/2013 Věstníku, o fyzické bezpečnosti v rezortu MO.

Rizika se vyhodnocují identifikací jednotlivých stupňů UI, a to dle jejich množství vyskytujících se v objektu. V potaz jsou brány také případné následky jejich vyzrazení nebo zneužití. Vyhodnocují se hrozby, kterým jsou utajované informace vystaveny a jejich zranitelnost vůči těmto hrozbám. Míry rizika se následně stanovují jako malá, střední nebo velká.[37] Odhadované množství utajovaných informací, které budou ukládány a zpracovávány v rezortu MO, viz tabulka 1.

Tabulka 1: Množství a druh utajovaných informací

Stupeň utajení	Počet utajovaných informací
„V“	4 500
„D“	4 000
„T“	580
„PT“	120

Zdroj: vlastní zpracování

Při sestavování projektu fyzické bezpečnosti a následně modelového pracoviště je klíčové stanovení a vyhodnocení rizik i hrozeb, které mohou nastat při práci s utajovanými informacemi, a snaha jim předcházet. Do vyhodnocení se musí také promítnout újma, která by mohla nastat při úniku nebo zničení utajované informace. Tento projekt, jakož i vyhodnocení rizik je vytvořen ve spolupráci s odborníky z řad Vojenské policie. Po konzultaci s kolegy z oddělení bezpečnosti a oddělení řízení a správy bezpečnostních systémů velitelství ochranné služby Vojenské policie jsou vyhodnocena rizika pro daný objekt MO.

5.1.1 Hrozba neoprávněného nakládání s utajovanými informacemi týkající se poučených osob

Může se jednat o úmyslné i neúmyslné jednání zaměstnance, který je držitelem platného osvědčení fyzické osoby a je poučen odpovědnou osobou. Neúmyslné jednání může spočívat ve vyzrazení neoprávněné osobě z nedbalosti, nedbalost při práci se systémem, kde se zpracovávají utajované informace, neoprávněné skartaci, ztrátě utajované informace nebo nevrácením utajované informace do úschovného objektu po skončení manipulace a dalšími nepředvídatelnými skutečnostmi. V případě úmyslného vyzrazení utajované informace to dělá pachatel pro finanční nebo osobní prospěch.

[37] § 10 odst. 3 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.

Nejčastěji tak učiní předáním kopie utajované informace nebo ústním sdělení osobě neoprávněné. Pravděpodobnost úmyslného vyzrazení se nejeví jako velká z důvodu důkladného výběru zaměstnanců, školení a poučení i následné kontroly ze strany NBÚ nebo VZ. Ačkoli nelze vyloučit úmyslné vyzrazení, jeho míra byla vyhodnocena jako nízká. V případě nedbalostního vyzrazení se jedná o nepředvídatelnou skutečnost, kterou lze také minimalizovat pomocí školení, výběru zaměstnanců a následných kontrol ze strany odpovědných osob. Nelze ji však vyloučit, a tak bude míra neúmyslného vyzrazení nebo manipulace s utajovanými informacemi stanovena na míru nízká až střední. Újma, která může nastat při takovém útoku, je závažná, a tak je míra rizika stanovena na ***velká***.

5.1.2 Hrozba manipulace s utajovanou informací osobou neoprávněnou

V rezortu MO se pracuje s velkým množstvím utajovaných informací všech stupňů utajení a také s utajovanými informacemi NATO a EU. Zájem o tyto informace z pohledu různých teroristických skupin, cizích mocností nebo jiných subjektů nebude zanedbatelný. Hrozí tedy, že může z pohledu fyzické bezpečnosti dojít k pokusu o vloupání do zabezpečené oblasti, přepadení při transportu utajovaných informací nebo k napadení zabezpečené oblasti. Hrozí zde také ztráta utajované informace, ale při nalezení této informace je malé nebezpečí zneužití. Vzhledem k umístění zabezpečené oblasti v objektu, který střeží vysoký počet příslušníků Vojenské policie, je dojezdová rychlost hlídky PČR a hlídek Vojenské policie v řádech minut. V tomto případě je vyhodnocena míra rizika přepadení zabezpečené oblasti jako nízká. Vzhledem k technickému zabezpečení perimetru i budovy, ve které se nachází zabezpečená oblast, a samotnému zabezpečení této oblasti je míra rizika vloupání nebo vniknutí neoprávněné osoby vyhodnocena jako nízká. Ztráta utajované informace je aspekt, který je nahodilý a dá se mu jen těžko předejít, jelikož se jedná o selhání jedince. Újma, která může nastat při takovém útoku, je závažná, a tak je míra rizika stanovena jako ***velká***.

5.1.3 Hrozba zničení či poškození utajovaných informací při technických závadách a živelních katastrofách

Při živelních katastrofách a technických závadách, jako jsou třeba zatopení v důsledku závady na vodovodním potrubí vedeném v budově nebo požár způsobený závadou na elektroinstalaci nebo při manipulací s otevřeným ohněm či kouřením na místech k tomu neurčených, může dojít k nenávratnému poškození nebo zničení utajované informace.

Technickým závadám lze předcházet pravidelnou kontrolou elektrických rozvodů a spotřebičů, školením zaměstnancům a také včasnou detekcí požáru a jeho likvidací. Totéž platí při závadách na vodovodním potrubí. Díky místní znalosti a zastavení přívodu vody do určité části budovy lze zabránit poškození nebo zničení utajované informace. Živelní katastrofy se nedají předpovídat, ale dá se zmírnit jejich dopad vhodným umístěním budovy a dále nezanedbáváním jejího technického stavu. Ačkoli jsou budova i zabezpečená oblast zcela nové, nelze vyloučit poškození živelní katastrofou ani technickou závadu. Újma, která může nastat při takové situaci, je závažná, a tak je míra rizika stanovena na ***velká.***

5.1.4 Hrozba zničení či poškození utajované informace způsobena teroristickým útokem

Poškození může nastat kvůli výbušnině umístěné v budově, kde se nachází utajované informace, zasláním výbušniny formou poštovní zásilky nebo útokem skupiny nebo jednotlivce. Provozní řád v objektu MO stanovuje, že příslušníci vojenské policie kontrolují soukromé a nevyžádané poštovní zásilky za pomoci rentgenu. Tito příslušníci jsou vyškoleni k vyhledávání zbraní a nástražných výbušných zařízení. Proto riziko, že zásilka obsahující výbušniny se dostane do objektu MO, je nízké. Díky technickému zabezpečení perimetru, budovy a zabezpečené oblasti je riziko umístění výbušniny taktéž nízké. Policejní ochranu objektu vykonávají nepřetržitě příslušníci vojenské policie a v pracovní době je tento počet navýšen o příslušníky štábu. Fiktivní objekt MO se nachází na okraji Prahy a dojezdová rychlost hlídky Vojenské policie a PČR je v řádu minut. Tím lze prakticky vyloučit útok jednotlivce nebo skupiny na objekt MO nebo zabezpečenou oblast. Je zde taktéž historická absence takového útoku, který však nelze vyloučit, a v případě zvýšení stupně zajištění bezpečnosti by se mohla míra rizika zvýšit. Armáda ČR zná čtyři stupně bezpečnostních a pohotovostních stavů, které vychází z bezpečnostní politiky NATO. Tyto stupně stanoví míru rizik a sílu hrozeb. Újma, která může nastat při takovém útoku, je závažná, a tak je míra rizika stanovena na ***velká.***

- Alpha – tento stupeň je preventivní a znamená normální stav zabezpečení.
- Bravo – tento stupeň je preventivní, ale znamená zvýšení kontrol při vstupech a vjezdech do objektů.
- Charlie – tento stupeň znamená možnost přímého ohrožení.
- Delta – tento stupeň přichází jako reakce na útok proti České republice.

5.1.5 Hrozba zneužití UI nasazením operativní techniky nebo pasivním odposlechem

Hrozba náhodného nebo cíleného odposlechu a pozorování je vzhledem k umístění budovy malá. Ta je ze všech stran kryta oplocením a do budovy ani zabezpečené oblasti není možné vidět. Okna jsou vybavena žaluziemi, které mohou zabránit pozorování. Cílenému odposlechu lze zamezit důkladným dodržováním režimových opatření, školením zaměstnanců a v případě jednání instalací rušiček signálu. Újma, která může nastat při takovém útoku, je závažná, a tak je míra rizika stanovena na ***velká***.

5.1.6 Hrozba ztráty nebo vyzrazení utajované informace únikem z informačního systému

Pro informační systémy řeší analýzu rizik vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor.[38]

Aktiva informačního systému jsou utajované informace a jejich nosiče. Vzhledem k používání certifikovaných informačních systémů, školení zaměstnanců, neustálému vývoji informačního systému, aktualizacím systému a také práci centra CIRC je míra rizika vyhodnocena jako střední. Cílem centra CIRC je detekce kybernetických bezpečnostních hrozeb a incidentů, což centrum vykonává díky nepřetržitému monitoringu různých částí datových sítí rezortu. Nelze však vyloučit selhání jednotlivce, který úmyslně či neúmyslně umožní útočníkovi přístup do informačního systému. Útoky můžou mít formu zakódování důležitých dat a následného vydírání, kdy jde útočníkovi o finanční obnos, nebo útoky zpravodajských skupin cizích mocností nebo teroristických skupin za účelem získání utajovaných informací. Újma, která může nastat při takovém útoku, je závažná, a tak je míra rizika stanovena na ***velká***.

[38] § 11 vyhlášky č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor.

5.1.7 Stanovení celkové míry rizika

Tabulka 2: Stanovení míry rizika

Druh hrozby	Vyhodnocení
Hrozba neoprávněného nakládání s utajovanými informacemi osobami týkající se poučených osob	velká
Hrozba manipulace s utajovanou informací osobou neoprávněnou	střední
Hrozba zničení či poškození utajovaných informací při živelních katastrofách a technických závadách	velká
Hrozba zničení či poškození utajované informace způsobena teroristickým útokem	střední
Hrozba zneužití utajované informace nasazením operativní techniky nebo pasivním odposlechem	střední
Hrozba ztráty nebo vyzrazení utajované informace únikem z informačního systému	velká
Celková míra rizika	**velká**

Zdroj: vlastní zpracování

Celkové stanovení rizika bylo určeno dle možnosti výskytu a potencionálních škod. V tomto případě byla stanovena celková míra rizika jako ***velká***. K minimalizaci těchto rizik byla připravena bezpečnostní opatření administrativní a fyzické povahy.

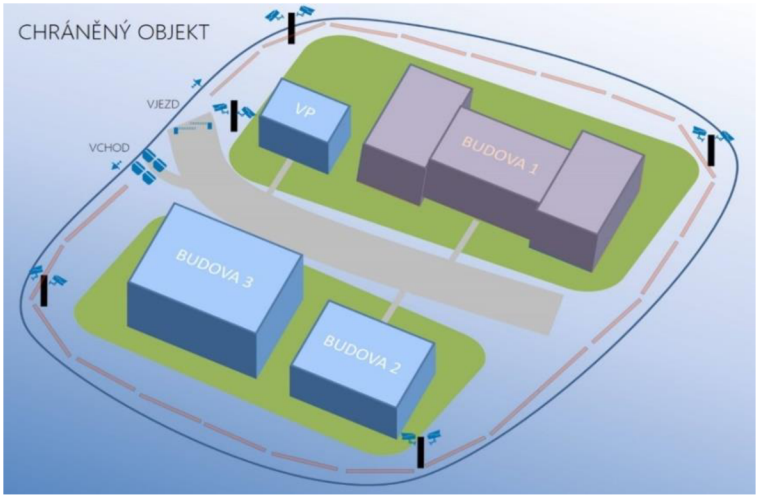
Po určení míry rizika je potřeba připojit popis objektu MO, budovy, zabezpečené oblasti a jednotlivá opatření fyzické bezpečnosti. V této části bude pracováno s fiktivním objektem MO. Modelové pracoviště bude vytvořeno na základě podmínek ZUS a vyhlášky o fyzické bezpečnosti a certifikaci technických prostředků.

5.2 Určení objektu a zabezpečených oblastí, včetně jejich hranic, určení tříd a kategorií zabezpečených oblastí

Objekt MO se nachází na okraji města Prahy v jeho těsné blízkosti. V tomto areálu se nachází několik budov viditelných na obrázku č. 3, kterými se z bezpečnostních důvodů nebudeme zabývat. Důležitá pro nás ovšem bude budova 1, ve která bude situována zabezpečená oblast a jednací oblast. Celý areál je zabezpečen plotem kombinujícím zděné sloupy a železný kovaný plot o výšce nejméně 3,5 metrů. Vstup do areálu je možný přes turniket u pěší brány. Tento vstup je nepřetržitě střežen příslušníky Vojenské policie a slouží jako vstup nejen pro zaměstnance, ale také pro návštěvy a firmy, které v objektu provádí servis a jiné práce. Vjezd je vybaven prostředky na detekci nebezpečných látek a předmětů a provádí se zde bezpečnostní prohlídky osob, zavazadel a poštovních

zásilek. Vjezd do objektu přímo sousedí se vstupem. Nachází se zde také stanoviště směny policejní ochrany Vojenské policie. Tento vjezd je vybaven technickými prostředky pro zabránění násilného vjezdu vozidel a kontrolu osob a vozidel při vjezdu a výjezdu z objektu. Celý areál MO je sledován kamerovým systémem se záznamovým zařízením.

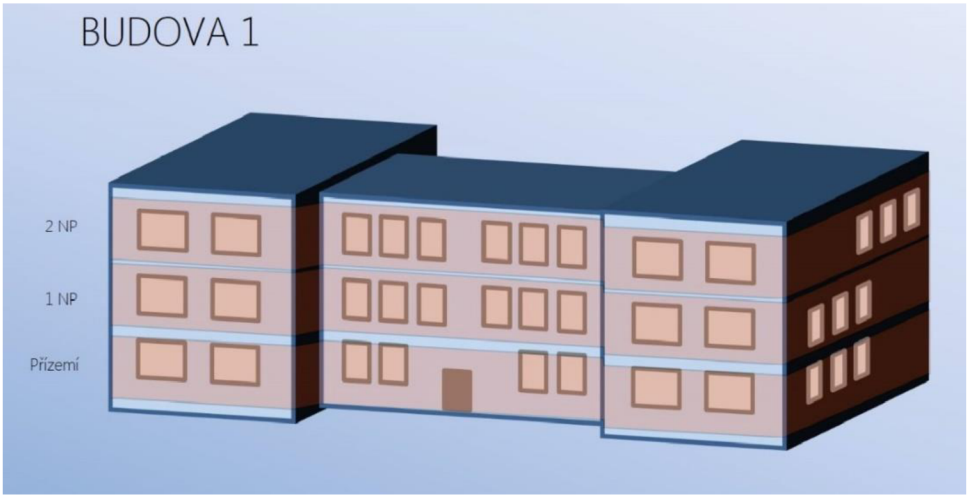
Obrázek 3: Areál MO



Zdroj: vlastní zpracování v programu C4

Objekt označený na obrázku jako budova 1 (viz obrázek 3) má dvě nadzemní podlaží. Jedná se o betonovou stavbu s ocelovými výztužemi. Tato budova sousedí se služebnou VP, kde se nachází pult centrální ochrany obsluhovaný příslušníky vojenské policie. Do budovy je možné se dostat dvěma vstupy, z přední a zadní části budovy. Oba tyto vstupy jsou monitorovány kamerovým systémem (dále jen „CCTV“) a zabezpečeny systémem kontroly vstupů, kdy je pro vstup do budovy potřeba čipová karta.

Obrázek 4: Budova 1



Zdroj: vlastní zpracování v programu C4

5.2.1 Popis zabezpečeného objektu, stanovení hranice

Zabezpečená oblast se nachází v druhém nadzemním podlaží v pravém křídle budovy, jak je vidět na obrázku 4. Tato oblast je tvořena kancelářemi 1, 2 a 3, chodbou, jednací místností a pracovištěm ochrany informací, které je vyobrazeno jako místnost č. 6. Zde se zpracovávají a ukládají utajované informace do stupně utajení „Přísně tajné“. Vstupem do této oblasti se osoby neseznamují s utajovanou informací, a proto je pracoviště ochrany informací ve třídě I.

5.3 Způsob použití opatření fyzické bezpečnosti

V této části práce jsou popsány jednotlivé prvky. Jejich druh, třída, zda jsou certifikovány a jak jsou v daném objektu použity.

5.3.1 Úschovné objekty

V zabezpečené oblasti jsou umístěny tři trezory NS 8 třídy 11 bezpečnostní třídy II, které odpovídají ČSN EN 1143.1. Jsou to trezory na dokumenty typu 4 – Přísně tajné a certifikované NBÚ.

SS1 = 4 body[39]

Úschovné objekty jsou osazeny časovými zámky typu EK 1500 COMPAKT, které odpovídají ČSN EN 1300 a dle NBÚ spadají do třídy bezpečnosti B.

SS2 = 3 body[40]

5.3.2 Zabezpečená oblast

Stěny podlahy a stropy v zabezpečených a jednacích oblastech mají stavební konstrukci z vyztuženého betonu o tloušťce 180 mm. Beton je vyztužen ocelovými vlákny a odpovídá ČSN EN 14889-1. Okna v zabezpečené oblasti jsou hliníková ve třídě RC 4 doplněná o prvky a příslušenství, které zajišťují nejvyšší odolnost proti vloupání. Jedná se o okna MB70RC4, která splňují požadavky dle ČSN EN 1628, 1629, 1630, od firmy Aluprof SA. Dveře jsou taktéž ve třídě RC 4 a jsou to kování dveří a bezpečnostní ocelové

[39] Bod 1.1.1. přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.
[40] Bod 1.2.2. přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.

dveře Hörmann typ D65-RC4, které odpovídají ČSN EN 1627. Okna jsou dále vybavena mřížemi, které splňují požadavky NBÚ. To znamená, že tyto otvory nedovolují průchod šablony elipsy o rozměrech 250 mm x 150 mm a tloušťky 20 mm. Jedná se o mříže MPK 4 PT od zámečnické firmy František Kopeček – zámečnictví.

Zabezpečená oblast typ 4, SS3 = 4 body[41]

Systém určený k uzamykání zabezpečené oblasti tvoří skládaná ocelová zárubeň značky Hörmann určená pro typ bezpečnostních dveří D65-RC4 s bezpečnostní cylindrickou vložkou typu 333 SIGMA PLUS. Oba tyto prostředky splňují požadavky na uzamykací systém typu 3 dle NBÚ.

SS4 = 3 body[42]

Mechanické zábranné prostředky nevykazují znaky poškození nebo takového opotřebení, které znemožňuje identifikaci pokusů o neoprávněný vstup.

Hranice objektu

Podlahy, stropy a stěny mají stavební konstrukci z vyztuženého betonu, která odpovídá ČSN EN 14889-1, a uzamykací systém odpovídá bezpečnostnímu typu 3. Okna a dveře jsou zabezpečena nejméně ve stupni bezpečnostního typu 3 dle NBÚ.

Objekt typ 3, SS3 = 3 body[43]

5.3.3 Systém kontroly vstupu do zabezpečeného objektu a zabezpečené oblasti

Vstup do objektu je kontrolován certifikovaným SKV v programu C4, který odpovídá ČSN EN 50133. Ten je takzvanou nástavbou neboli integrovaným řídicím bezpečnostním systémem, který sdružuje jednotlivé systémy, jako jsou SKV, CCTV odpovídající normě ČSN EN 50132, elektronický požární systém (dále jen „EPS“), poplachové zabezpečovací a tísňové systémy odpovídající normě ČSN EN 50131 (dále jen „PZTS“). Ve vyhlášce o fyzické bezpečnosti a certifikaci technických prostředků se vyskytuje pojem elektrické zabezpečovací systémy (dále jen „EZS“), který nezahrnuje tísňové systémy, a tak je v

[41] Bod 2.1.1. přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.
[42] Bod 2.2.2. přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.
[43] Bod 3.2. přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.

normách ČSN toto nahrazeno pojmem poplachové zabezpečovací a tísňové systémy. Tento pojem lépe vystihuje daný typ zabezpečení a je běžně používán jako synonymum EZS. Ke vstupu do zabezpečené oblasti je potřeba identifikační prvek, v tomto případě čipová karta a PIN kód.

Systém kontroly vstupu typ 3, SS6 = 3 body[44]

Ze směrnic pro výkon služby Vojenské policie vyplývá povinnost provádět namátkové kontroly u osob, které vycházejí ze zabezpečené oblasti. Tyto prohlídky slouží jako odstrašující prvek.

SS12 = 1 bod[45]

5.3.4 Režim návštěv v objektu MO

Dle provozního řádu se evidují a kontrolují všechny návštěvy a je povinnost tyto osoby po celou dobu návštěvy doprovázet. Je jim zapůjčena čipová karta a to znamená, že je přehled o pohybu těchto osob v objektu. Návštěvy musí být viditelně označeny. Dle § 34 zákona 300/2013 Sb., o Vojenské policii a změně některých zákonů, je před vstupem do objektu provedena u těchto osob bezpečnostní prohlídka. Při odchodu jsou prováděny namátkové prohlídky dle směrnic objektu MO.

SS7 = 3 body[46]

5.3.5 Ostraha

Ostrahu zabezpečují příslušníci Vojenské policie dle § 4 odst. 1 písm. f) zákona č. 300/2013 Sb., o Vojenské policii a změně některých zákonů. Ti jsou vyškoleni a poučeni pro zásahy proti narušení pořádku a bezpečnosti v objektu MO a proti dalším mimořádným situacím. Vojenská policie provádí obchůzky po náhodně vybraných trasách a v náhodných intervalech ne větších než 2 hodiny. V průběhu obchůzek jsou stanoviště obsazena nejméně jedním příslušníkem Vojenské policie. Ostraha je zajištěna nepřetržitě, a to nejméně v počtu 12 příslušníků Vojenské policie.

---

[44] Bod 4.1.2. přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.
[45] Bod 4.2.1. přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.
[46] Bod 4.3.1. přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.

Ostraha typu 5, SS8 = 5 bodů[47]

5.3.6 Zařízení EZS (PZTS)

V objektu je tento systém zaručen díky programu C4. Zabezpečená oblast je vybavena prvky PZTS. Tyto splňují normu ČSN EN 50131-1 ed. 2 Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – pro stupeň zabezpečení 4 – vysoké riziko a tísňový systém splňuje ČSN EN 50134-1 Poplachové systémy – Systémy přivolání pomoci.

Prvky, které jsou použity v zabezpečené oblasti:

- Ústředna PZTS GALAXY G3-520PT od firmy Honeywell UK.
- Tísňový hlásič HB304/1 UTC Fire and Security (držitel certifikace společnost Honeywell, spol. s r.o.).
- Detektor otevření dveří a oken DC111 od firmy UTC Fire and Security (držitel certifikace společnost Honeywell, spol. s r.o.).
- Detektor pohybu SCM 3000 BUS-2 od firmy Honeywell UK.
- Detektor otřesu VVS302PLUS od firmy Cosmotron AB (držitel certifikace společnost Honeywell, spol. s r.o.).
- Detektor rozbití skla S5812A-W/SR od firmy GE Security (držitel certifikace společnost Honeywell, spol. s r.o.).

Zařízení elektrické zabezpečovací signalizace typ 4, SS91 = 4 body[48]

Tabulka 3: Tabulka přiřazení kategorií k typům prostředků EZP

Typ technického prostředku PTZS	Stupeň utajení, pro který byla schválena způsobilost, je vypsán zkratkou nebo slovy	Bodová hodnota
Typ 4	„PT – Přísně tajné“	4 b.
Typ 3	„T – Tajné“	3 b.
Typ 2	„D – Důvěrné“	2 b.

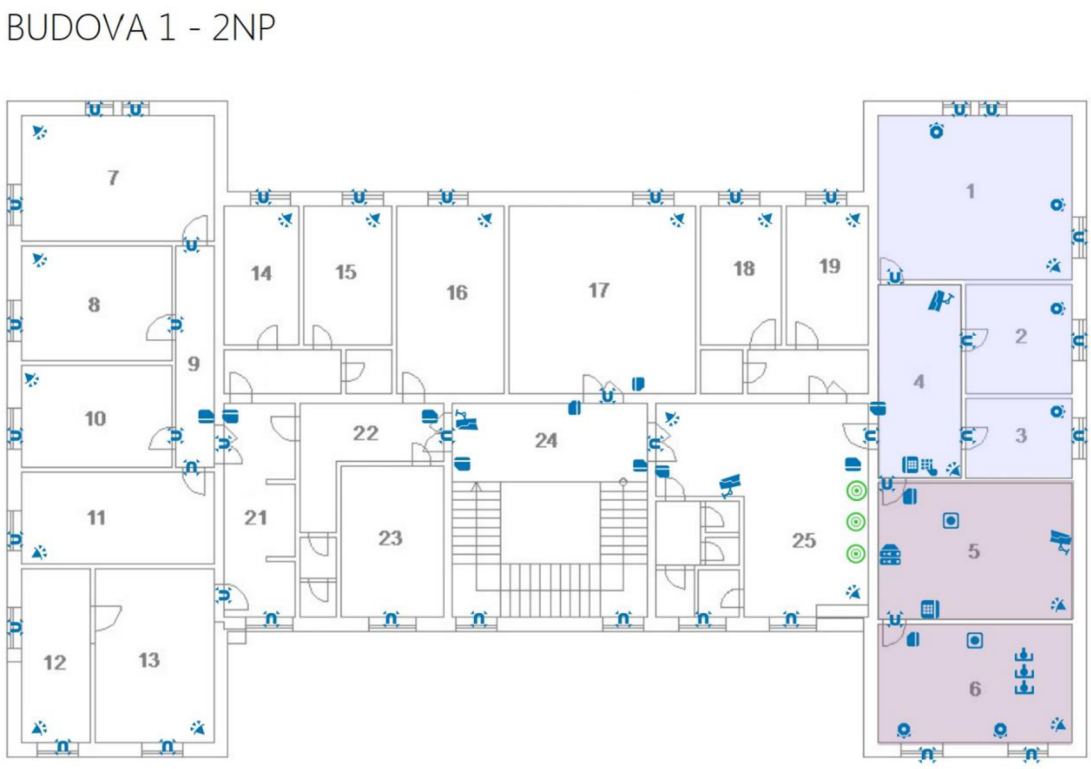
Zdroj: Bod 5.2.4. přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů

[47] Bod 5.1.1. přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.
[48] Bod 5.2.1. přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.

5.3.7 Instalace PZTS

U vchodu do zabezpečené oblasti je z vnější i vnitřní strany instalována klávesnice s číselníkem a čtečka karet. Na dveřích jsou instalovány detektory otevření na principu magnetu. Zámky dveří jsou elektronicky zabezpečeny. V případě, že dojde k jejich otevření, aniž by byl zadán správný PIN kód a použita určená čipová karta, zahlásí systém ostraze, že došlo k násilnému otevření dveří. Dále jsou instalovány detektory rozbití skla, což jsou prvky plášťové ochrany. Prostorová čidla PIR jsou instalována nejen v zabezpečené oblasti, ale i v celé budově. Kamerový systém snímá nepřetržitě průlezné prostory do zabezpečené oblasti, ale nijak nenarušuje ochranu utajovaných informací. Na trezorech jsou instalovány detektory otřesu a v jednací i zabezpečené oblasti se nachází tísňové tlačítko.

Obrázek 5: Instalace prvků PTZS



Zdroj: vlastní zpracování v programu C4

Instalace zařízení PZTS typ 4, SS92 = 4 body[49]

Výpočet SS9 podle bodového hodnocení SS91 a SS92 je dle vyhlášky o fyzické bezpečnosti a certifikaci technických prostředků následující:

- SS9 = (SS91 + SS 92)/2 × SS92/OBL

OBL je bodová hodnota určená kategorií zabezpečené oblasti, viz tabula 4.

Tabulka 4: Tabulka hodnot OBL v závislosti na stupni utajení

Kategorie zabezpečené oblasti	Bodová hodnota OBL
„PT“	4 b.
„T“	3 b.
„D“	2 b.
„V“	1 b.

Zdroj: Bod 5.2.9. přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů

SS9 = (4 + 4) /2 × 4/4 = 4

SS9 = 4[50]

5.3.8 CCTV

Slouží ke snímání celého objektu, a nejen zabezpečené oblasti. Snímá, přenáší a zobrazuje pohyb osob a dopravních prostředků v objektu. Tyto systémy nejsou certifikovány. Záznam z těchto zařízení sledují příslušníci Vojenské policie z důvodu bezpečnosti. Tento kamerový systém nijak nenarušuje ochranu utajovaných informací. Garance uchování záznamu je 21 dní.

5.3.9 Ochrana perimetru

Hranice perimetru je po celém obvodu tvořena fyzickou bariérou, vstup je na totožné úrovni bezpečnosti jako konstrukce fyzické bariéry. Fyzická bariéra je tvořena kombinací zděných sloupů a železného plotu s ostny vysokého 3,5 metru.

[49] Bod 5.2.5. přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.
[50] Bod 5.2.9. přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.

SS10 = 2 body[51]

Ve všech přístupových bodech se vykonává kontrola ze strany příslušníků Vojenské policie. Její rozsah je uveden v zákoně č. 300/2013 Sb., o Vojenské policii a změně některých zákonů, a také v provozním řádu Objektu MO.

SS11 = 1 bod[52]

Je nainstalován perimetrický detekční systém, který je napojen na program C4. Tento systém funguje jako „laserové brány". Jsou to 2D LiDAR senzory (Light Detection And Ranging), které pracují na principu Dopplerova jevu. Jsou to zařízení měřící vzdálenost objektů, které se objeví v zorném poli. Software poté vyhodnocuje velikost objektu a rychlost pohybu. Proto jsou schopny „vidět" narušitele. Laserový paprsek rotuje a při každé rotaci provádí měření. Softwarově lze pak určit, v jaké výseči a na jakou vzdálenost bude sledována detekční zóna. Detekční perimetrický systém je certifikovaný.

SS13 = 2 body[53]

Celý perimetr je osvětlen bezpečnostním osvětlením po celém perimetru. Osvětlení zajišťují 6metrové stožáry K 6-133/89/60 od firmy BB Elektro. Toto osvětlení nemusí být certifikováno.

SS14 = 2 body[54]

CCTV na perimetru je zajištěno za pomocí DOME kamer, které snímají 360° a mají také přepínáni do nočního režimu. Garance ukládání záznamů je po dobu minimálně 21 dnů. CCTV není certifikováno Úřadem. Příslušníci z důvodu bezpečnosti nepřetržitě monitorují dění v objektu MO. Garance uchování záznamu je po dobu 21 dnů.

[51] Bod 6.1.3. přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.
[52] Bod 6.2. přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.
[53] Bod 6.3.1. přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.
[54] Bod 6.4. přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.

SS15 = 2 body[55]

5.3.10 Zařízení EPS

Zařízení požární signalizace je instalováno ve všech budovách objektu. Všechny komponenty splňují normu ČSN 34 2710. Požární signalizace je připojena do programu C4. Jedná se o systém EPS FS720 CERBERUS PRO od firmy Siemens s.r.o.

5.3.11 Zařízení sloužící k vyhledávání nebezpečných nebo látek

U vstupu do objektu je realizována bezpečnostní kontrola za pomoci rentgenového přístroje na kontrolu zavazadel Rapiscan 638DV, který odpovídá všem předpisům. Dále zde probíhá kontrola osob za pomocí rámového detektoru kovů Garrett PD6500i a za pomocí ručního detektoru kovů Garrett Super Scanner V.

5.3.12 Zařízení fyzického ničení nosičů informací nebo dat

Skartovací stroj KOBRA 310 TS HD (řez 0,8 x 9,5 mm), který dle NBÚ splňuje podmínky pro zařízení fyzického ničení nosičů informací nebo dat typu 4. Toto zařízení tedy splňuje podmínky pro ničení nosičů obsahující utajené informace stupně „Přísně tajné“.

5.3.13 Bodové hodnocení opatření fyzické bezpečnosti

Název zabezpečené oblasti: místnost č. 6 ve 2. nadzemním patře budovy 1 v areálu objektu MO

Kategorie zabezpečené oblasti: „Přísně tajné“

Třída zabezpečené oblasti: třída II

Typ zabezpečené oblasti: typ 4

Účel zabezpečené oblasti: V této oblasti vznikají, ukládají se a zpracovávají utajované informace až do stupně „Přísně tajné“. Toto není pracoviště se stálou přítomností zaměstnanců.

[55] Bod 6.5. přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.

Tabulka 5: Přehled bodového hodnocení jednotlivých prvků

Bezpečnostní opatření	Typ	Bodové ohodnocení
Úschovné objekty	● □ **T. 4 – 4 body**	SS1 = 4 b.
	~~□ T. 3 – 3 body~~	
	~~□ T. 2 – 2 body~~	
Zámky úschovných objektů	~~□ T. 4 – 4 body~~	SS2 = 3 b.
	● □ **T. 3 – 3 body**	
	~~□ T. 2 – 2 body~~	
Úschovný objekt včetně uzamykacího systému	~~□ T. 1 – 1 bod~~	S1 =
	~~□ T. 1A – 1 bod~~	
	~~□ T. 1B – 2 body~~	
	~~□ T. 1C – 3 body~~	
Celkové hodnocení úschovného objektu a jeho zámku	S1 = SS1 × SS2	S1 = 12 b.
Zabezpečené oblasti	● □ **T. 4 – 4 body**	SS3 = 4 b.
	~~□ T. 3 – 3 body~~	
	~~□ T. 2 – 2 body~~	
	~~□ T. 1 – 1 bod~~	
Uzamykací systém zabezpečené oblasti	~~□ T. 4 – 4 body~~	SS4 = 3 b.
	● □ **T. 3 – 3 body**	
	~~□ T. 2 – 2 body~~	
	~~□ T. 1 – 1 bod~~	
Celkové ohodnocení zabezpečené oblasti a jejího uzamykacího systému	~~S2 = SS3 × SS4~~	S2 = 12 b.
Objekt	~~□ T. 4 – 4 body~~	S3 = 3 b.
	● □ **T. 3 – 3 body**	
	~~□ T. 2 – 2 body~~	
	~~□ T. 1 – 1 bod~~	
Systém kontroly vstupu	~~□ T. 4 – 4 body~~	SS6 = 3 b.
	● □ **T. 3 – 3 body**	
	~~□ T. 2 – 2 body~~	
	~~□ T. 1 – 1 bod~~	
Režim návštěv v objektu		SS7 = 3 b.
a) Návštěvy s doprovodem	● □ **ad a) – 3 bod**	
b) Návštěvy bez doprovodu	~~□ ad b) 1 bod~~	
c) Návštěvy bez kontroly	~~□ ad c) nehodnoceno~~	
Celkové hodnocení kontroly vstupu	S4 = SS6 + SS7	S4 = 6 b.

Bezpečnostní opatření	Typ	Bodové ohodnocení
Ostraha	● □ **T. 5 – 5 bodů**	SS8 = 5 b.
	~~□ T. 4 – 4 b.~~	
	~~□ T. 3 – 3 b.~~	
	~~□ T. 2 – 2 b.~~	
	~~□ T. 1 – 1 b.~~	
Zařízení elektrické zabezpečovací signalizace	● □ **T. 4 – 4 b.**	SS91 = 4 b.
	~~□ T. 3 – 3 b.~~	
	~~□ T. 2 – 2 b.~~	
	~~□ T. 1 – 1 b.~~	
Instalace zařízení elektrické zabezpečovací signalizace	● □ **T. 4 – 4 b.**	SS92 = 4 b.
	~~□ T. 3 – 3 b.~~	
	~~□ T. 2 – 2 b.~~	
	~~□ T. 1 – 1 b.~~	
Mezivýsledek (SS 9)		SS9 = 4 b.
Celkové hodnocení ostrahy a systému EZS	S5 = SS8 + SS9	S5 = 9 b.
Fyzické bariéry	~~□ T. 4 – 4 b.~~	SS10 = 2 b.
	~~□ T. 3 – 3 b.~~	
	● □ **T. 2 – 2 b.**	
	~~□ T. 1 – 1 b.~~	
Kontrola vstupu v přístupových bodech perimetru		SS11 = 1 b.
a) Kontrola je realizována	□ **ad a) – 1 b.**	
b) Kontrola není realizována	~~□ ad b) – 0 b.~~	
Namátkové vstupní a výstupní prohlídky		SS12 = 1 b.
a) Prohlídky jsou prováděny		
b) Prohlídky nejsou prováděny	● □ **ad a) – 1 b.**	
	~~□ ad b) – 0 b.~~	
Perimetrický detekční systém (PDS)		SS13 = 2 b.
- certifikovaný Úřadem	**2 b.**	
- necertifikovaný Úřadem	~~1 b.~~	
Bezpečnostní osvětlení perimetru	**2 b.**	SS14 = 2 b.
Speciální televizní systém na perimetru	**2 b.**	SS15 = 2 b.
Celkové hodnocení ochrany perimetru	S6 = (SS10 × SS11) + SS12 + SS13 + SS14 + SS15	S6 = 9 b.

Zdroj: Bod 14.3.1. přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů, upraveno autorem

Poté, co je vyhodnocena míra rizika, a v tomto případě je vyhodnocena jako ***velká,*** je potřeba, aby byly splněny podmínky fyzické bezpečnosti ve stupni „Přísně tajné“. Tabulka v bodě 12.1. přílohy č. 1 vyhlášky o fyzické bezpečnosti a certifikaci technických prostředků určuje nejnižší bodové hodnoty míry zabezpečení zabezpečené oblasti s danou mírou rizika.

Tabulka 6: Tabulka bodových hodnot nejnižší míry zabezpečení zabezpečené oblasti

Zabezpečená oblast kategorie „PT“	**Míra rizika**		
	malá	**střední**	**velká**
Povinné: (S1) + (S2) + (S3)	10 b.	11 b.	13 b.
Povinné: (S4) + (S5) *	6 b.	7 b.	7 b.
Nepovinné: (S6)	4 b.	5 b.	5 b.
Celkový výsledek	**20 b.**	**23 b.**	**25 b.**

*Poznámka: * Hodnota (S5) musí dosáhnout alespoň 5 bodů.*

Zdroj: Bod 12.1. přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů

Tabulka 7: Tabulka bodových hodnot zabezpečeného objektu

Zabezpečená oblast kategorie „PT“	**Míra rizika**
	velká
Povinné: (S1) + (S2) + (S3)	27 b.
Povinné: (S4) + (S5) *	15 b.
Nepovinné: (S6)	9 b.
Celkový výsledek	**51 b.**

Zdroj: Bod 12.1. přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů, upraveno autorem

Při porovnání tabulek je patrné, že prostředky fyzické bezpečnosti, které se použily v modelovém objektu, zcela vyhovují podmínkám zabezpečení objektu kategorie „Přísně tajné“ při velké míře rizika.

5.3.14 Technická dokumentace projektu fyzické bezpečnosti

Technická dokumentace je upravena a popsána v příloze č. 1 vyhlášky o fyzické bezpečnosti a certifikaci technických prostředků.

Dále se tato dokumentace dělí na dvě části:

1) Výkresová dokumentace

Vyznačení hranice objektu, hranice zabezpečené oblasti, rozmístění jednotlivých technických prostředků určených k ochraně utajovaných informací v objektu jsou obsahem výkresové dokumentace.

2) Dokumentace technických prostředků

Výčet jednotlivých technických prostředků, jejich počty, názvy, druhy a umístění, dále kopie certifikátů a příloh platných při instalaci a případně zápisy o posouzení shody platné při instalaci jsou součástí dokumentace technických prostředků.[56]

5.4 Provozní řád

Náležitosti provozního řádu jsou stanoveny v příloze č. 1 vyhlášky o fyzické bezpečnosti a certifikaci technických prostředků a jsou součástí projektu fyzické bezpečnosti. Provozní řád je rozdělen do několika bodů obsahujících pravidla:

- režimu pohybu dopravních prostředků a osob (včetně návštěv) v areálu/budově,
- režimu pohybu dopravních prostředků a osob (včetně návštěv) v zabezpečených objektech a oblastech,
- režimu pohybu utajovaných informací v objektu,
- manipulace s provozní dokumentací k technickým prostředkům,
- zacházení s klíči a identifikačními prostředky od vstupů do objektu a zabezpečených oblastí a s klíči od úschovných objektů,
- popis režimových opatření pro ochranu jednacích oblastí.[57]

[56] Bod 15.2.1. přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.
[57] Bod 14.4. přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.

6 Závěr

Cílem bakalářské práce bylo zhodnocení stavu současné legislativy, která je implementována na obor ochrany utajovaných informací v České republice se zaměřením na rezort MO. V této souvislosti byly popsány stěžejní právní normy a navazující legislativní předpisy. Na základě shromážděných poznatků byl následně vytvořen model fiktivního pracoviště, které se zabývá ukládáním a zpracováváním utajovaných informací až do stupně „Přísně tajné“.

Za tímto účelem byla bakalářská práce strukturována do několika kapitol. Těmi nejdůležitějšími jsou zejména kapitola třetí, v rámci, které je popsán stěžejní zákon o ochraně utajovaných informací v ČR, a kapitola pátá, která aplikuje poznatky z praktické části, zejména z vyhlášky o fyzické bezpečnosti a certifikaci technických prostředků.

Toto téma, ačkoli si to lidé neuvědomují, je stěžejní pro fungování a obranu státu. Stát je povinen chránit své zájmy, přičemž jeho největším zájmem je život a zdraví občanů. I proto musí některé informace tajit před cizími mocnostmi, firmami, a dokonce před svými občany. Tyto informace mohou v rukou nepřítele znamenat ztráty na lidských životech, finanční ztráty nebo poškození diplomatických vztahů. Nepřítele lze totiž chápat i jako někoho, kdo chce stát napadnout vojenskými silami, ale i někoho, kdo chce ČR poškodit například ekonomicky, technologicky nebo psychologicky. Důkazem takových postupů je i současnu taktika hybridní války.

MO pracuje dlouhodobě jako jeden z hlavních nosných pilířů bezpečnosti státu s informacemi důležitými pro obranu státu, a to od informací o umístění důležitých objektů přes mobilizační plány až po alianční projekty a mise. Každý držitel osvědčení fyzické osoby může říct, že NBÚ je opravdu důsledný. Není se čemu divit. Svěřit informace nejvyšší důležitosti není možné člověku, u kterého NBÚ zjistil jakoukoli překážku, která zavdává příčinu k nedůvěře. Vážnost újmy, která by hrozila při ztrátě či zničení utajované informace, odráží i stupeň utajení („V“, „D“, „T“ a „PT“) a dle těchto stupňů se odvíjí také rozsah prověřování. Po získání tohoto osvědčení ale práce NBÚ nekončí, kontroluje držitele osvědčení po celou dobu jeho platnosti.

V praktické části byla popsána tvorba projektu fyzické bezpečnosti. Z výčtu použitých opatření fyzické bezpečnosti je znát, jak moc důležitá je pro stát ochrana utajovaných informací. Takové zabezpečení a proces, který se musí dodržet během práce s těmito informacemi, se může zdát přehnaný, ale odráží, s jak důležitým obsahem se zachází.

Právní úprava ochrany utajovaných informací je zpracována velmi komplexně a přesto, že už byla mnohokrát novelizována, je na dnešní pokročilou dobu v některých ohledech zastaralá, zejména co se týče popisu utajovaných informací, které se označují pouze datem vzniku. V dnešní době, kdy války probíhají i v kyberprostoru a kdy je čas rozhodujícím faktorem, by bylo potřeba změnit v tomto směru zákon a při vzniku utajované informace neudávat pouze datum, ale také čas. Informace nesoucí určité datum nemusí být ještě tentýž den relevantní a může ztratit svou hodnotu. Avšak co se týče fyzické bezpečnosti, je tato právní úprava dostačující.

Z teoretické i praktické části je evidentní, že bezpečnost není brána na lehkou váhu a jediný slabý článek tohoto řetězce je pouze lidský faktor. Ten ohrožuje utajované informace nejvíce, ať už je jednání úmyslné, nebo neúmyslné. Proto je potřeba dbát na správný výběr zaměstnanců, školení zaměstnanců v dané problematice a samozřejmě dostatečné prověřování.

Cíle práce stanovené na začátku byly splněny jak v praktické, tak v teoretické části. Tedy ve třetí části jsou shrnuty nejdůležitější právní normy týkající se řešené problematiky. Čtvrtá část se zaměřuje přímo na rezort MO, kde jsou zmíněny vnitřní právní normy a sekce MO řešící ochranu utajovaných informací. V páté části je vytvořen projekt fyzické bezpečnosti dle právních norem tak, aby prvky byly certifikovány NBÚ a proběhla bezproblémová atestace osobou pověřenou v rezortu MO.

7 Seznam použitých zdrojů

Monografie

BURDA, K. *Úvod do kryptografie*. Brno: Akademické nakladatelství CERM®, 2015. 110 s. ISBN 978-80-7204-925-7.

DVOŘÁK, J., CHROBÁK, J. *Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti: komentář*. Praha: Wolters Kluwer, 2018. 480 s. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7598-016-8.

KOLOUCH, J., BAŠTA, P. *CyberSecurity*. Praha: CZ.NIC, 2019. 560 s. ISBN 978-80-88168-31-7.

NĚMEČEK, K., VOPÁLENSKÝ, V. *Spojovací technika: telefonie. Učebnice pro 3. a 4. ročník SPŠST obor 37-46-6 spojová technika – oddělení telekomunikační technika po vedeních*. Praha: Nakladatelství dopravy a spojů, 1982. 621 s.

Odborné články

PAVELKA, I. Institucionální zajištění ochrany utajovaných informací v ČR. *Správní právo* [online]. 2017, roč. L, č. 5, s. 258–268 [cit. 2022-02-02]. ISSN 0139-6005. Dostupné z: https://www.mvcr.cz/clanek/spravni-pravo-cislo-5-2017.aspx

PAVELKA, I. Institucionální zajištění ochrany utajovaných informací v ČR. *Správní právo* [online]. 2018, roč. LI, č. 3, s. 202–216 [cit. 2022-02-02]. ISSN 0139-6005. Dostupné z: https://www.mvcr.cz/webpm/clanek/spravni-pravo-cislo-3-2018.aspx

Internetové zdroje

2/1969 Sb., Zákon České národní rady o zřízení ministerstev a jiných ústředních orgánů státní správy České socialistické republiky. *Zákony pro lidi – Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online] AION CS, s.r.o. 2010 [cit. 15.3.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/1969-2

181/2014 Sb., Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů. *Zákony pro lidi – Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online] AION CS, s.r.o. 2010 [cit. 15.3.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

231/1948 Sb., Zákon na ochranu lidově demokratické republiky. *Zákony pro lidi – Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online] AION CS, s.r.o. 2010 [cit. 15.3.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/1948-231

412/2005 Sb., Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti. *Zákony pro lidi – Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online] AION CS, s.r.o. 2010 [cit. 15.3.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-412

523/2005 Sb., Vyhláška o bezpečnosti informačních a telekomunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor. *Zákony pro lidi – Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online] AION CS, s.r.o. 2010 [cit. 15.3.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-523

528/2005 Sb., Vyhláška o fyzické bezpečnosti a certifikaci technických prostředků. *Zákony pro lidi – Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online] AION CS, s.r.o. 2010 [cit. 15.3.2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-528

Evropská justice. *Vnitrostátní právní předpisy* [online]. 2020 [cit. 2022-01-26]. Dostupné z: https://e-justice.europa.eu/content_member_state_law-6-cz-maximizeMS-cs.do?member=1

Evropská rada, Rada Evropské unie. *Ochrana utajovaných informací Evropské unie (EUCI)* [online]. 2020 [cit. 2022-02-14]. Dostupné z: https://www.consilium.europa.eu/cs/general-secretariat/corporate-policies/classified-information/

JONÁK, Z. Informace. *KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV)* [online]. Praha: Národní knihovna ČR, 2003 [cit. 2022-02-05]. Dostupné z: https://aleph.nkp.cz/F/?func=direct&doc_number=000000456&local_base=KTD

LUŇÁČEK, O. *Fyzická bezpečnost: Druhy zajištění ochrany utajovaných informací (OUI)* [online]. Brno: Univerzita obrany, 2004 [cit. 2022-01-26]. Dostupné z: https://moodle.unob.cz/pluginfile.php/18153/mod_resource/content/9/Druhy%20zaji%C5%A1t%C4%9Bn%C3%AD.pdf

MO ČR. *Působnost a činnosti* [online]. Praha: Ministerstvo obrany ČR [cit. 2022-01-26]. Dostupné z: https://mocr.army.cz/ministr-a-ministerstvo/pusobnost/pusobnost-a-cinnosti-5131/

NATO. *Security brief* [online]. North Atlantic Treaty Organization [cit. 2022-02-02]. Dostupné z: https://www.act.nato.int/images/stories/structure/reserve/hqrescomp/nato-security-brief.pdf

NBÚ. *O nás* [online]. Praha: Národní bezpečnostní úřad [cit. 2022-01-26]. Dostupné z: https://www.nbu.cz/cs/o-nas/955-o-nas/

NBÚ. *Obecně k personální bezpečnosti* [online]. Praha: Národní bezpečnostní úřad [cit. 2022-01-26]. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/personalni-bezpecnost-oznameni-pro-v-osvedceni-d-t-pt-certifikaty/1043-obecne-k-personalni-bezpecnosti/

NBÚ. *Předpisy NATO vztahující se k ochraně utajovaných informací* [online]. Praha: Národní bezpečnostní úřad [cit. 2022-02-02]. Dostupné z: https://www.nbu.cz/cs/pravni-predpisy/1078-predpisy-nato-vztahujici-se-k-ochrane-utajovanych-informaci/

NÚKIB. *O úřadu* [online]. Praha: Národní úřad pro kybernetickou a informační bezpečnost [cit. 2022-01-26]. Dostupné z: https://www.nukib.cz/cs/o-nukib/o-uradu/

SVATOŠOVÁ, H. *Návrh zákona o ochraně utajovaných informací – studie a připomínky: Studie k úpravě utajovaných skutečností v historii, v zahraničí a rozbor návrhu nového zákona o utajovaných informacích ve verzi z prosince 2003* [online]. Praha: Iuridicum Remedium, 2004 [cit. 2022-01-26]. Dostupné z: https://www.iure.org/sites/default/files/article/downloads/07_navrh_zakona_o_ochrane_utajovanych_informaci.pdf

Vnitřní předpisy

NV MO 77/2013. Fyzická bezpečnost v rezortu Ministerstva obrany ze dne 9.července 2013, Čj. 49-17/2013-OB MO

NV MO 111/2013. Kryptografická ochrana utajovaných informací v rezortu Ministerstva obrany ze dne 25. listopadu 2013, č. j. 278-10/2013-OB MO.

RMO 14/2013. Ochrana utajovaných informací v rezortu Ministerstva obrany ze dne 25. února 2013, č. j. 42-7/2013-OB MO.

RMO 33/2012. O personální bezpečnosti v rezortu Ministerstva obrany ze dne 26. června 2012, č. j. 220/2012-OB MO.

Legislativní zdroje

Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor

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

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

Zákon č. 2/1969 Sb., České národní rady o zřízení ministerstev a jiných ústředních orgánů státní správy České socialistické republiky

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

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

Zákon č. 50/1923 Sb. z. a n., na ochranu republiky

8 Seznam obrázků a tabulek

Seznam obrázků

Seznam tabulek

9 Seznam použitých zkratek

CCTV	kamerový systém
CD	compact disc (kompaktní disk)
ČR	Česká republika
EPS	elektronická požární signalizace
EU	Evropská unie
EUCI	European Union classified information
MO	Ministerstvo obrany
NATO	North Atlantic Treaty Organization (Severoatlantická aliance)
NBÚ	Národní bezpečnostní úřad
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
NV MO	normativní výnos Ministerstva obrany
OB MO	oddělení bezpečnosti Ministerstva obrany
PTZS	poplachové zabezpečovací a tísňové systémy
RMO	rozkaz ministra obrany
SKV	systém kontroly vstupů
USB	Universal Serial Bus (univerzální sériová sběrnice)
ZUS	zákon o ochraně utajovaných skutečností

10 Přílohy

Ikona	Popis
	Řídící jednotka PZTS, SKV
	Tísňové tlačítko
	Magnetický detektor
	Detektor pohybu
	Detektor pohybu 360°
	Infrazávora
	Detektor rozbití skla
	Otřesový detektor
	Signalizace zastřežení oblasti
	Klávesnice PZTS
	Oblast
	Dveře
	Čtečka karet
	Klávesnice SKV
	Kamera
	PTZ kamera