POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Katedra kriminalistiky

Technické zabezpečení fyzického objektu určeného k ochraně utajovaných informací

Diplomová práce

Technical safety and security of a physical object intended for the protection of classified information

Master thesis

VEDOUCÍ PRÁCE

doc. Ing. Jiří Jonák, Ph.D.

AUTOR PRÁCE

Bc. Michal Přenosil

PRAHA

2023

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu přiložené literatury.

V Praze dne 29. 2. 2023

Bc. Michal PŘENOSIL

Poděkování

Děkuji panu doc. Ing. Jiřímu Jonákovi, Ph.D. za odborné vedení, konzultace a připomínky při tvorbě této práce. Dále děkuji panu mjr. Ing. Ivu Hrubému za jeho konzultace a diskuse na témata z oblasti ochrany utajovaných informací. Na závěr děkuji panu Bc. Janu Židlickému za věcné připomínky při tvorbě této práce.

ANOTACE

Tato diplomová práce se zaměřuje na technické zabezpečení fyzického objektu určeného k ochraně utajovaných informací. Pojednává o právním rámci ochrany utajovaných informací, orgánech vykonávajících státní správu v oblasti ochrany utajovaných informací a v oblasti normalizace, metrologie a státního zkušebnictví. Práce rovněž představuje vybrané druhy technických prostředků určených k ochraně utajovaných informací a vybrané administrativní náležitosti dané problematiky. Je zde představen postup k definování vhodnosti objektu určeného pro zpracovávání a uchovávání utajovaných informací. Výsledkem této práce je stanovení dostačující ochrany určeného objektu vycházejících z analýzy požadavků na jeho ochranu.

KLÍČOVÁ SLOVA

Technické prostředky ochrany utajovaných informací * legislativa ochrany utajovaných informací * management rizik * analýza rizik FMEA * Ishikawův diagram.

ANNOTATION

This thesis focuses on the technical security of a physical object designed to protect classified information. It discusses the legal framework for the protection of classified information, the bodies performing state administration in the field of the protection of classified information and in the field of standardization, metrology, and state testing. The work also presents selected types of technical devices intended to protect classified information and selected administrative requirements of the given issue. A procedure for determining the suitability of an object for processing and storing classified information is presented here. The result of this work is the determination of sufficient protection of the designated object based on the analysis of the requirements for its protection.

KEYWORDS

Protection of a classified information * legislative framework of a protection of a classified information * risk management * FMEA risk analysis * Ishikawa diagram.

OBSAH

ÚVOD 10

CÍLE A METODIKA 11

1 PRÁVNÍ RÁMEC OCHRANY UTAJOVANÝCH INFORMACÍ A DEFINICE ZÁKLADNÍCH POJMŮ 12

1.1 PRÁVNÍ PŘEDPISY SOUVISEJÍCÍ S OCHRANOU UTAJOVANÝCH INFORMACÍ V ČR 12

1.1.1 DEFINICE VYBRANÝCH POJMŮ PODLE ZÁKONA Č. 412/2005 SB. A ROZKAZU MINISTRA OBRANY Č. 14/2013 12

1.1.2 STUPNĚ UTAJENÍ PODLE ZÁKONA Č. 412/2005 SB. 13

1.2 ORGÁNY VYKONÁVAJÍCÍ STÁTNÍ SPRÁVU V OBLASTI OCHRANY UTAJOVANÝCH INFORMACÍ 14

1.2.1 NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD (NBÚ) 14

1.2.2 NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST (NÚKIB) 14

1.3 ORGÁN VYKONÁVAJÍCÍ STÁTNÍ SPRÁVU V OBLASTI NORMALIZACE, METROLOGIE A STÁTNÍHO ZKUŠEBNICTVÍ 15

2 VYBRANÉ TECHNICKÉ PROSTŘEDKY URČENÉ K OCHRANĚ UTAJOVANÝCH INFORMACÍ 16

2.1 DEFINICE POJMŮ KAPITOLY 16

2.2 ÚSCHOVNÉ OBJEKTY 17

2.3 ZABEZPEČENÉ OBLASTI A JEJICH UZAMYKACÍ SYSTÉMY 20

2.4 SYSTÉM KONTROLY VSTUPU DO ZABEZPEČENÉ OBLASTI NEBO OBJEKTU A REŽIM NÁVŠTĚV 22

2.5 ZAŘÍZENÍ ELEKTRONICKÉ ZABEZPEČOVACÍ SIGNALIZACE 23

2.6 INSTALACE ZAŘÍZENÍ ELEKTRONICKÉ ZABEZPEČOVACÍ SIGNALIZACE 25

2.7 SPECIÁLNÍ TELEVIZNÍ SYSTÉMY 25

2.8 FYZICKÉ BARIÉRY 26

2.9 ZAŘÍZENÍ ELEKTRICKÉ POŽÁRNÍ SIGNALIZACE 27

2.10 ZAŘÍZENÍ SLOUŽÍCÍ K VYHLEDÁVÁNÍ NEBEZPEČNÝCH LÁTEK NEBO PŘEDMĚTŮ 27

2.11 ZAŘÍZENÍ FYZICKÉHO NIČENÍ NOSIČŮ INFORMACÍ NEBO DAT 28

2.12 ZAŘÍZENÍ PROTI PASIVNÍMU A AKTIVNÍMU ODPOSLECHU UTAJOVANÝCH INFORMACÍ 29

2.13 FYZICKÁ BEZPEČNOST INFORMAČNÍHO SYSTÉMU 30

2.13.1 OPATŘENÍ PROTI KRÁDEŽI POČÍTAČOVÝCH SYSTÉMŮ 30

2.13.2 OPATŘENÍ PŘED ROZEBRÁNÍM A ÚPRAVOU POČÍTAČOVÝCH SYSTÉMŮ 31

2.13.3 OCHRANA PŘED PŘIPOJENÍM CIZÍCH PERIFERIÍ K POČÍTAČOVÝM SYSTÉMŮM 31

2.14 CERTIFIKACE POČÍTAČOVÉHO SYSTÉMU A NÁLEŽITOSTI ZAJIŠTĚNÍ OCHRANY PROTI KOMPROMITUJÍCÍMU VYZAŘOVÁNÍ 32

3 URČENÍ OBJEKTU, ZABEZPEČENÝCH A JEDNACÍCH OBLASTÍ 33

3.1 VSTUPNÍ INFORMACE ZÁJMOVÉHO OBJEKTU 33

3.2 POŽADAVKY NA ZABEZPEČENÉ A JEDNACÍ OBLASTI 36

3.2.1 ZABEZPEČENÁ OBLAST Č. 1 36

3.2.2 JEDNACÍ OBLAST Č. 2 36

3.2.3 ZABEZPEČENÁ OBLAST Č. 3 36

3.2.4 ZABEZPEČENÁ OBLAST Č. 4 36

3.3 ÚPRAVY STÁVAJÍCÍ OCHRANY OBJEKTU 37
3.3.1 NUTNÉ STAVEBNÍ A JINÉ ÚPRAVY OBJEKTU 37
3.3.2 ÚSCHOVNÉ OBJEKTY A JEJICH ZÁMKY 37
3.3.3 UZAMYKACÍ SYSTÉMY URČENÉ K UZAMYKÁNÍ ZABEZPEČENÝCH OBLASTÍ 37
3.3.4 SYSTÉM KONTROLY VSTUPU DO ZABEZPEČENÉHO OBJEKTU 37
3.3.5 OSTRAHA, NAMÁTKOVÉ PROHLÍDKY A REŽIM NÁVŠTĚV 38
3.3.6 OSTRAHA A ZAŘÍZENÍ ELEKTRICKÉ ZABEZPEČOVACÍ SIGNALIZACE (EZS) 38
3.3.7 INSTALACE EZS 38
3.3.8 SPECIÁLNÍ TELEVIZNÍ SYSTÉMY 39
3.3.9 ZAŘÍZENÍ FYZICKÉHO NIČENÍ NOSIČŮ INFORMACÍ NEBO DAT. 39
3.3.10 ZAŘÍZENÍ PROTI PASIVNÍMU A AKTIVNÍMU ODPOSLECHU UTAJOVANÝCH INFORMACÍ 39
3.3.11 FYZICKÁ BEZPEČNOST INFORMAČNÍHO SYSTÉMU 39

3.4 NÁKRES ZÁJMOVÉHO OBJEKTU PO ÚPRAVÁCH 40

4 MANAGEMENT RIZIK 42

4.1 DEFINICE POJMŮ KAPITOLY 42

4.2 PŘEHLED IDENTIFIKOVANÝCH HROZEB 43

4.3 ANALÝZA FMEA 45

4.4 DEFINICE IDENTIFIKOVANÝCH HROZEB 47
4.4.1 LIDSKÝ FAKTOR VNITŘNÍ 47
4.4.2 LIDSKÝ FAKTOR VNĚJŠÍ 48
4.4.3 PROSTŘEDKY FYZICKÉ BEZPEČNOSTI 49
4.4.4 NATUROGENNÍ MIMOŘÁDNÁ UDÁLOST BIOTICKÁ 49
4.4.5 NATUROGENNÍ MIMOŘÁDNÁ UDÁLOST ABIOTICKÁ 50
4.4.6 FYZICKÁ BEZPEČNOST INFORMAČNÍHO SYSTÉMU 51

5 STANOVENÍ MÍRY RIZIKA A BODOVÉ OHODNOCENÍ PRO JEDNOTLIVÉ ZABEZPEČENÉ A JEDNACÍ OBLASTI 52

5.1 STANOVENÍ MÍRY RIZIKA A BODOVÉ OHODNOCENÍ PRO ZABEZPEČENOU OBLAST Č. 1 52
5.1.1 SPECIFIKACE AKTIV PRO ZABEZPEČENOU OBLAST Č. 1 52
5.1.2 TABULKA BODOVÉHO OHODNOCENÍ OPATŘENÍ FYZICKÉ BEZPEČNOSTI V ZABEZPEČENÉ OBLASTI Č. 1 53

5.2 STANOVENÍ MÍRY RIZIKA A BODOVÉ OHODNOCENÍ PRO JEDNACÍ OBLAST Č. 2 56
5.2.1 SPECIFIKACE AKTIV PRO JEDNACÍ OBLAST Č. 2 56
5.2.2 TABULKA BODOVÉHO OHODNOCENÍ OPATŘENÍ FYZICKÉ BEZPEČNOSTI V JEDNACÍ OBLASTI Č. 2 57

5.3 STANOVENÍ MÍRY RIZIKA A BODOVÉ OHODNOCENÍ PRO ZABEZPEČENOU OBLAST Č. 3 60
5.3.1 SPECIFIKACE AKTIV PRO ZABEZPEČENOU OBLAST Č. 3 60
5.3.2 TABULKA BODOVÉHO OHODNOCENÍ OPATŘENÍ FYZICKÉ BEZPEČNOSTI V ZABEZPEČENÉ OBLASTI Č. 3 61

5.4 STANOVENÍ MÍRY RIZIKA A BODOVÉ OHODNOCENÍ PRO ZABEZPEČENOU OBLAST Č. 4 64
5.4.1 SPECIFIKACE AKTIV PRO ZABEZPEČENOUÍ OBLAST Č. 4 65
5.4.2 TABULKA BODOVÉHO OHODNOCENÍ OPATŘENÍ FYZICKÉ BEZPEČNOSTI V ZABEZPEČENÉ OBLASTI Č. 4 65

ZÁVĚR 68

SEZNAM POUŽITÝCH ZDROJŮ 69

SEZNAM OBRÁZKŮ 71

SEZNAM TABULEK 71

SEZNAM ZKRATEK 73

SEZNAM PŘÍLOH 73

ÚVOD

Motivace chránit svůj život, zdraví a majetek se řadí neodmyslitelně k základním potřebám člověka od počátků lidské civilizace až po současnost. Dynamický rozvoj lidské společnosti napříč dějinami se promítá do všech oblastí lidského života, tedy i do zmíněné roviny ochrany života, zdraví a majetku. Zatímco ve starověku dřevěná palisáda obklopující osadu představovala dostatečnou ochranu proti nepřátelům, s rozvojem doby představovala pro nepřítele stále menší překážku. Vývojem prochází i metody, nástroje a technika nepřátel. Pro udržení přijatelné úrovně bezpečnosti osady bylo tedy nezbytné neustále udržovat i adekvátní úroveň obranného systému, neboť dříve či později nepřítel našel způsob, kterým je tento systém překonatelný. Tento trend trvá do dnešní doby a trvat bude i v dobách budoucích. Chráněným zájmem pro potřeby této práce je utajovaná informace (dále jen UI). V České republice je ochrana utajovaných informací řešena na úrovni zákona, kde zákon definuje UI a její úrovně, prováděcí právní předpis potom možný způsob provedení ochrany UI, provedení a posouzení kvality jednotlivých prvků systému ochrany UI a v neposlední řadě kvality vazeb prvků systému ochrany UI. Mezi základní prvky systému ochrany UI řadíme technické prostředky zajišťující ochranu UI, a právě tyto technické prostředky, kvalita jejich provedení, způsob využití a hodnocení jejich úrovně na základě právních předpisů jsou tématem této práce. Autor má ke zvolenému tématu blízký vztah, neboť s jeho zaměstnáním téma ochrany UI úzce souvisí. Při tvorbě této práce tak může zúročit zkušenosti z praxe ve služebním poměru vojáka z povolání, znalosti získané studiem na Policejní akademii v Praze a technické znalosti získané studiem Vojenské střední školy v Brně v oboru radiotechnického zabezpečení. Jako základní monografii při tvorbě této práce pro dokreslení souvislostí autor použil komentář J. Dvořáka k zákonu č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti.[1]

[1] DVOŘÁK, Jan. *Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti: komentář*. Praha: Wolters Kluwer, 2018. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7598-016-8.

CÍLE A METODIKA

Cílem této diplomové práce je představit formou případové studie možnosti využití technických prostředků k ochraně utajovaných informací v souladu s uvedenými právními předpisy. Tato práce není plnohodnotným projektem fyzické bezpečnosti ve smyslu zákona č. 412/2005 Sb., může však být průvodním manuálem pro vytvoření technické části projektu fyzické bezpečnosti. Pomáhá lépe se orientovat ve značení jednotlivých druhů technických prostředků a značení kvality úrovně jejich zpracování. Zároveň ukazuje vzájemné souvislosti a návaznosti jednotlivých druhů ochrany a odkazuje na předepsané administrativní úkony související s problematikou ochrany utajovaných informací.

V teoretické části této práce autor představí vybrané druhy technických prostředků na základě rozdělení podle vyhlášky č. 528/2005 Sb., s nimi související režimová opatření a předepsané administrativní úkony. V praktické části pak představí smyšlený zájmový objekt určený k ochraně utajovaných informací dislokovaný do fiktivního vojenského zařízení na území České republiky, pomocí Ishikawova diagramu definuje jednotlivé množiny hrozeb pro zájmový objekt směřující k riziku úniku nebo zneužití utajované informace a následně metodou FMEA stanoví míru rizika pro jednotlivé množiny hrozeb. Výsledná míra rizika je jedním z podkladů pro určení použití vhodných druhů a kvality technických prostředků tak, aby míra zabezpečení jednotlivých oblastí objektu vyhovovala souvisejícím právním předpisům.

1 PRÁVNÍ RÁMEC OCHRANY UTAJOVANÝCH INFORMACÍ A DEFINICE ZÁKLADNÍCH POJMŮ

V jednotlivých podkapitolách autor představí právní předpisy související s ochranou utajovaných informací v České republice (dále jen ČR), definici vybraných pojmů podle souvisejících právních předpisů, stupně utajení podle zákona č. 412/2005 Sb., orgány vykonávající státní správu v oblasti ochrany utajovaných informací a orgán vykonávající státní správu v oblasti normalizace, metrologie a státního zkušebnictví. Výčet jednotlivých právních předpisů a pojmů zde není vyčerpávající, jsou zde uvedeny pouze právní předpisy a pojmy související s potřebami této práce.

1.1 PRÁVNÍ PŘEDPISY SOUVISEJÍCÍ S OCHRANOU UTAJOVANÝCH INFORMACÍ V ČR

Právní předpisy související s ochranou utajovaných informací jsou zejména klíčový zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, dále vyhláška č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací, vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, vyhláška č. 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací a vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor.

1.1.1 DEFINICE VYBRANÝCH POJMŮ PODLE ZÁKONA Č. 412/2005 SB. A ROZKAZU MINISTRA OBRANY Č. 14/2013

V této podkapitole autor uvede definice jednotlivých pojmů týkajících se problematiky ochrany utajovaných informací, citovaných ze zákona č. 412/2005 Sb., a dále jednotlivé stupně utajení definované zákonem č. 412/2005 Sb.

Utajovaná informace – Zákon č. 412/2005 Sb., definuje utajovanou informaci jako cit.: "*informace v jakékoliv podobě zaznamenaná na jakémkoliv nosiči označená v souladu s tímto zákonem, jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné, a která*

je uvedena v seznamu utajovaných informací (§ 139)“, jednací oblast je cit.: „*ohraničený prostor v objektu. Utajovanou informaci stupně utajení přísně tajné nebo tajné lze pravidelně projednávat pouze v jednací oblasti“,* zabezpečenou oblastí se rozumí cit.: „*ohraničený prostor v objektu“ a* objektem cit.: „*budova nebo jiný ohraničený prostor, ve kterém se zpravidla nachází zabezpečená oblast nebo jednací oblast.*“[2] Zabezpečené oblasti zákon rozděluje ještě na oblasti třídy I a oblasti třídy II. Vstupem do oblasti třídy II nedochází přímo k seznámení s utajovanou informací, zatímco v oblasti třidy I k tomuto seznámení dochází. Rozkaz ministra obrany (dále jen RMO) č. 14/2013 definuje technické zařízení jako cit.: „*vojenský materiál, který je definován v § 2 písm. k) vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 454/2011 Sb., a § 30 odst. 1 vyhlášky č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací*“, **informačním systémem** v rezortu MO se rozumí cit.: „*jeden nebo více počítačů, jejich programové vybavení, periferní zařízení, správa systému, personální obsluha, procesy nebo prostředky, které tvoří celek schopný sbírat, tvořit, zpracovávat, ukládat, zobrazovat nebo přenášet utajované informace včetně kryptografických prostředků používaných pro daný informační systém*“ a **komunikačním systémem** v rezortu MO potom cit.: „*systém, který zajišťuje přenos utajovaných informací mezi koncovými uživateli. Zahrnuje koncové komunikační zařízení, přenosové prostředí, prostředky kryptografické ochrany, správu systému, personální obsluhu a provozní podmínky a postupy.*“[3]

1.1.2 STUPNĚ UTAJENÍ PODLE ZÁKONA Č. 412/2005 SB.

Autor zde cituje jednotlivé stupně utajení utajovaných informací sestupně, jak je klasifikuje zákon č. 412/2005 Sb.: **přísně tajné** – cit.: „*vyzrazení informace neoprávněné osobě nebo zneužití může způsobit mimořádně vážnou újmu zájmům České republiky“,* **tajné** – cit.: „*vyzrazení informace neoprávněné osobě nebo zneužití může způsobit vážnou újmu zájmům České republiky“,* **důvěrné** – cit.: „*vyzrazení informace neoprávněné osobě nebo zneužití může způsobit*

[2] ČESKO, Zákon č. 412 ze dne 21. září 2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: *Sbírka zákonů České republiky*. 2005, částka143/2005.
[3] ČESKO. Rozkaz Ministra obrany: Ochrana utajovaných informací v resortu Ministerstva obrany. In: Praha, 2013, ročník 2013, číslo 14.

prostou újmu zájmům České republiky“ a **vyhrazené** – cit.: „*vyzrazení informace neoprávněné osobě nebo zneužití může být nevýhodné pro zájmy České republiky.“*[4]

1.2 ORGÁNY VYKONÁVAJÍCÍ STÁTNÍ SPRÁVU V OBLASTI OCHRANY UTAJOVANÝCH INFORMACÍ

Orgány vykonávající státní správu v oblasti ochrany utajovaných informací v České republice jsou Národní bezpečnostní úřad a Národní úřad pro kybernetickou a informační bezpečnost.

1.2.1 NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD (NBÚ)

Zákonem č. 148/1998 Sb. o ochraně utajovaných skutečností zahájil NBÚ svoji činnost dne 1. srpna 1998. Dle vlastních webových stránek je NBÚ cit.: “*ústředním správním úřadem pro oblasti ochrany utajovaných informací, bezpečnostní způsobilosti a ve své činnosti se NBÚ řídí zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.*“[5]

1.2.2 NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST (NÚKIB)

NÚKIB vznikl ke dni 1. srpna 2017 zákonem č. 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) vyčleněním z NBÚ. Dle vlastních webových stránek je NÚKIB cit.: „*ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů kryptografické ochrany. Je správním orgánem a zajišťuje problematiku v oblasti kybernetické bezpečnosti, ochrany utajovaných*

[4] ČESKO, Zákon č. 412 ze dne 21. září 2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: *Sbírka zákonů České republiky*. 2005, částka143/2005.
[5] WEB Národní bezpečnostní úřad *nbu.cz* [online]. [cit. 2023-01-20]. Dostupné z: https://www.nbu.cz.

informací, kryptografickou ochranu a oblast komunikačních a informačních systémů.“[6]

1.3 ORGÁN VYKONÁVAJÍCÍ STÁTNÍ SPRÁVU V OBLASTI NORMALIZACE, METROLOGIE A STÁTNÍHO ZKUŠEBNICTVÍ

Zákonem České národní rady č. 20/1993 Sb. o zabezpečení výkonu státní správy v oblasti technické normalizace, metrologie a státního zkušebnictví byl zřízen Úřad pro technickou normalizaci, metrologii a státní zkušebnictví jako správní úřad se sídlem v Praze, který je podřízen Ministerstvu průmyslu a obchodu. Jeho hlavním posláním je cit.: „*zabezpečovat úkoly vyplývající ze zákonů České republiky upravujících technickou normalizaci, metrologii a státní zkušebnictví a úkoly v oblasti technických předpisů a norem uplatňovaných v rámci členství ČR v Evropské unii.“*[7]

[6] WEB, Národní úřad pro kybernetickou a informační bezpečnost *nukib.cz* [online]. [cit. 2023-01-20]. Dostupné z: https://www.nbu.cz.cz

[7] WEB, Úřad pro technickou normalizaci, metrologii a státní zkušebnictví unmz.cz [online]. [cit. 2023-01-20]. Dostupné z: https://www.unmz.cz/obecne/o-uradu/.

2 VYBRANÉ TECHNICKÉ PROSTŘEDKY URČENÉ K OCHRANĚ UTAJOVANÝCH INFORMACÍ

V této kapitole autor prezentuje vybrané technické prostředky určené k ochraně utajovaných informací podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti a k němu se vztahující prováděcí vyhlášky NBÚ č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků a vyhlášky č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor. V úvodu podkapitoly budou prezentovány pojmy týkající se řešené problematiky.

2.1 DEFINICE POJMŮ KAPITOLY

Autor zde uvádí několik základních pojmů týkajících se řešené problematiky v této kapitole. Prvním užívaným pojmem je pojem **integrovaný bezpečnostní systém**. Je tvořen třemi základními prvky, a sice **mechanické zábranné systémy**, **signalizační zařízení a monitorovací prostředky** a **systém organizačních opatření a ostraha.** [8] Vyhláška č. 528/2005 Sb. mechanické zábranné prostředky definuje jako cit.: „*zejména zámky, dveře, mříže, folie, skla a další* bezpečnostní *konstrukční a stavební prvky“*[9]*.* Dle Jana Uhláře je jejich charakteristickým znakem cit.: “*bezpečnostní úroveň reprezentovaná pasivní bezpečností, resp. průlomovou odolností.“*[10] Smysl jejich využití spočívá ve vytvoření překážky proti průniku neoprávněné osoby do zájmového (chráněného prostoru/objektu). Signalizační zařízení a monitorovací prostředky detekují, vyhodnocují a předávají informace, zda došlo k napadení zájmového prostoru/objektu. Ostraha v rámci systému organizačních opatření vyhodnotí vzniklý abnormální stav a přijme odpovídající opatření vedoucí k odstranění abnormálního stavu. Dalším užívaným pojmem je **doba průlomové odolnosti**. Podle ČSN EN 1627 se jedná o cit.: “*pracovní doba zkušebního technika, který provádí zkoušku odolnosti proti manuálním pokusům*

[8] UHLÁŘ, Jan. *Technická ochrana objektů II. díl*., 2. vyd. Praha: Policejní akademie České republiky v Praze, 2009. ISBN 978-80-7251-313-0., str. 9.
[9] ČESKO, Vyhláška č. 528/2005 Sb. ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků. In *Sbírka zákonů České republiky.* 2005, částka 179/2005.
[10] UHLÁŘ, Jan. *Technická ochrana objektů I. díl*., 2. vyd. Praha: Policejní akademie České republiky v Praze, 2009. ISBN 978-80-7251-312-3, str. 13.

o vloupání.“[11] Jednotkou **RU** je potom cit.: „*průlomová jednotka proti vloupání a manipulaci. Ukazuje vypočtený výsledek určité hodnoty v průběhu časového období za použití nástroje.“*[12]

2.2 ÚSCHOVNÉ OBJEKTY

Účel úschovného objektu (dále jen ÚO), jakož i způsob a možnosti jeho využití nám vyplívají z jeho názvu, i když na první pohled může být pro laiky jeho název lehce zavádějící. Hlavním účelem ÚO není chráněný předmět (v našem případě je tímto předmětem utajované informace) schovat před nepovolanou osobou, ale znemožnit této osobě se k chráněnému předmětu dostat, respektive ho získat. Pakliže UO není schopen zcela zabránit nepovolané osobě dostat se ke chráněnému předmětu, úkolem ÚO, spolu v kombinaci s jeho zámkem, je dobu nezbytnou k získání chráněného subjektu prodloužit na maximum. Jan Uhlář ve skriptech s názvem *Technická ochrana objektů, I. díl* řadí ÚO do kategorie **mechanických zábranných systémů předmětové ochrany** a rozděluje je do dvou základních kategorií: **komorové trezory** a **komerční úschovné objekty.**[13] Druhou zmíněnou kategorii dále dělí na skříňové trezory, ohnivzdorné skříně, účelové trezory, ocelové a kartotéční skříně a příruční pokladničky. Právě podkategorie **skříňové trezory** bude předmětem dalšího zájmu této práce. Uhlář dále rozděluje do kategorií č. I *až č.* III podle stupně technického vývoje, podle tloušťky jejich stěn a použitého materiálu na plášť trezoru a materiál výplně mezery mezi stěnami.[14] Pro potřeby této práce autor použije dělení úschovných objektů do skupin podle první kapitoly přílohy č. 1, vyhlášky č. 528/2005 Sb.[15] Podle této vyhlášky jsou úschovné objekty rozdělené podle typu do devíti skupin představených v tabulce č. 1 v prvním sloupci.

[11] ČESKO, ČSN EN 1627, Praha: Český normalizační institut, březen 2022.
[12] ČESKO, ČSN EN 1300, Praha: Český normalizační institut, březen 2020.
[13] UHLÁŘ, Jan. *Technická ochrana objektů I. díl*., 2. vyd. Praha: Policejní akademie České republiky v Praze, 2009. ISBN 978-80-7251-312-3, str. 149.
[14] UHLÁŘ, Jan. *Technická ochrana objektů I. díl*., 2. vyd. Praha: Policejní akademie České republiky v Praze, 2009. ISBN 978-80-7251-312-3, str. 154.
[15] ČESKO, Vyhláška č. 528/2005 Sb. ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků. In *Sbírka zákonů České republiky.* 2005, částka 179/2005.

V tabulce č. 1 je možno vyčíst rovněž různé druhy tzv. bezpečnostních tříd. Bezpečnostní třída je hlavním měřítkem kvality provedení ÚO. Třídy jsou určovány státem akreditovanou zkušebnou podle ČSN 1143–1.

Tabulka č. 1 – Typy úschovných objektů podle vyhlášky č. 528/2005 Sb.

Úschovný objekt (ÚO) podle vyhl. č. 528/2005 Sb.	Požadavek na certifikaci NBÚ	Odkazovaná norma ČSN	Bezpečnostní třída podle ČSN 1143–1	Bodová hodnota SS1
ÚO Typ 4	ano	ČSN EN 1143-1+A1	II. nebo vyšší*	4
ÚO Typ 3	ano	ČSN EN 1143-1+A1	I. *	3
ÚO Typ 2	ano	ČSN EN 1143-1+A1	0*	2
ÚO Typ 1	ne	-	-	1
ÚO Typ 1 A	ano	ČSN 91 6012	Z1	1
ÚO Typ 1 B	ano	ČSN 91 6012	Z2	2
ÚO Typ 1 C	ano	ČSN 91 6012	Z3	3
ÚO Typ 0	ne	-		N**

* Úschovný objekt tohoto typu musí být osazen zámkem typu 2.

** Nehodnoceno.

ÚO jsou podrobeny několika druhům zkoušek v závislosti na požadavku zařazení do bezpečnostní třídy. Tyto požadavky zasílá výrobce ÚO akreditované zkušebně spolu s ÚO ještě před uvedením na trh. Koncový zákazník má poté díky bezpečnostní třídě vyznačené na výrobním štítku ÚO spolu s certifikátem o zařazení do bezpečnostní třídy jasnou představu nejenom o technickém provedení ÚO, ale i o době, po kterou je ÚO schopen odolávat pachateli, a za jakých podmínek. Klíčovým parametrem rozdělení do bezpečnostních tříd je tzv. Doba průlomové odolnosti.

Ruku v ruce s kvalitou technického provedení ÚO jde i kvalita provedení **zámků** ÚO. Podstatnou částí bezpečnostního zámku je zámková vložka. J. Ivanka dělí zámkové vložky na cylindrickou, dozickou nebo motýlkovou.[16] Na trhu dnes převažují vložky cylindrické, byť např. dozické se i nadále vyrábějí. Staly se však díky své konstrukci snadno překonatelné. Cylindrické vložky lze rozdělit podle mnoha hledisek. JUDr. Jan Uhlář je dělí podle tvaru tělesa, délky tělesa, profilu pro klíč, počtu stavítek, počtu řad stavítek, principu ovládání stavítek a

[16] IVANKA, Ján, 2014. *Mechanické zábranné systémy*. Zlín [cit. 2023-1-3]. ISBN 978-80-7454-427-9., s. 49.

podle pasivní bezpečnosti.[17] Podle posledního jmenovaného hlediska je možné další rozdělení na standardní cylindrické vložky a bezpečnostní cylindrické vložky. Certifikaci jednotlivých druhů zámku a jejich následné rozdělení do příslušných skupin provádí akreditovaná zkušební laboratoř a certifikační orgán podle ČSN EN 1627 a ČSN EN 1630. Pro potřeby této práce je důležité rozdělení zámků do bezpečnostních tříd podle ČSN 1300+A1 a jejich následné rozřazení podle typu podle vyhlášky č. 528/2005 Sb. ČSN 1300+A1 stanovuje požadavky na spolehlivost a odolnost proti napadení a neoprávněnému otevření zámků s vysokou bezpečností (dále jen ZVB) spolu se způsoby zkoušek. Hodnotícím kritériem je zde mechanická a průlomová odolnost vyjádřená dobou průlomové odolnosti a jednotkami RU. Vyhláška č. 528/2005 Sb. rozděluje zámky do tří typů, a sice typ 2, typ 3 a typ 4. Zámek typu 2 splňuje bezpečnostní požadavky třídy A, zámek typu 3 musí splňovat bezpečnostní požadavky třídy B a zámek typu 4 požadavky třídy C, vše podle ČSN 1300+A1.[18] Tabulka č. 2 uvádí typ zámku podle vyhl. č. 528/2005 Sb., jemu odpovídající bezpečnostní třídu podle ČSN 1300+A1, nutnost požadavku na certifikaci NBÚ a bodovou hodnotu SS2.

Tabulka č. 2 – Typy zámků podle vyhlášky č. 528/2005 Sb.

Typ zámku podle vyhl. č. 528/2005 Sb.	Požadavek na certifikaci NBÚ	Odkazovaná norma ČSN	Bezpečnostní třída podle ČSN 1300+A1	Bodová hodnota SS2
Typ 2	ano	ČSN 1300+A1	A	2
Typ 3	ano	ČSN 1300+A1	B	3
Typ 4	ano	ČSN 1300+A1	C	4

[17] UHLÁŘ, Jan. *Technická ochrana objektů I. díl*. 2. vyd. Praha: Policejní akademie České republiky v Praze, 2009. ISBN 978-80-7251-312-3, str. 93.
[18] ČESKO, Vyhláška č. 528/2005 Sb. ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků. In *Sbírka zákonů České republiky*. 2005, částka 179/2005.

2.3 ZABEZPEČENÉ OBLASTI A JEJICH UZAMYKACÍ SYSTÉMY

Vyhláška č. 528/2005 Sb. vyžaduje nutnost zabezpečení průlezných otvorů mechanickými zábrannými prostředky, které dovolí průchod šablony o rozměrech uvedených v tabulce č. 3. Průlezným otvorem rozumíme okna, dveře, nouzové východy z objektu apod.

Tabulka č. 3 – Šablony a jejich rozměry podle vyhlášky č. 528/2005 Sb.

Šablona	Rozměr [mm]
Obdélník	400 x 250
Elipsa	400 x 300
Kruh	Průměr 350

Vyhláška č. 528/2005 Sb. ještě stanovuje nemožnost průchodu šablony ve tvaru elipsy o rozměrech 250 mm × 150 mm a tloušťky 20 mm, použitým mechanickým zábranným prostředkem s jedním a více otvory. Vyhláška č. 528/2005 Sb. udává požadavky na zabezpečení plášťové ochrany zabezpečených a jednacích oblastí. Rozděluje tuto ochranu do celkem pěti typů, a to podle způsobu provedení, použitých stavebních materiálů, a použitých zábranných mechanických prostředků k zabezpečení průlezných otvorů. Požadavky podle jednotlivých typů zabezpečených oblastí nám udává tabulka č. 4.

Tabulka č. 4 – Požadavky jednotlivých typů zabezpečených oblastí podle vyhlášky č. 528/2005 Sb.

Typ oblasti podle vyhl. č. 528/2005 Sb.	Požadavek na konkrétní stavební konstrukci	Požadavek na zabezpečení průlezných otvorů podle ČSN	Odkazovaná norma ČSN	Bezpečnostní třída podle ČSN EN 1627	Bodová hodnota SS3
Typ 4	ano	ano	ČSN EN 1627	RC 4, RC 5	4
Typ 3	ano	ano	ČSN EN 1627	RC 3	3
Typ 2	ano	ano	ČSN EN 1627	RC 2	2
Typ 1	ano	ne	-	-	1
Typ 0	ne	ne	-	-	0

Informace uvedené v tabulce č. 4 nejsou vyčerpávající, v mnoha případech klade vyhláška č. 528/2005 Sb. ještě další podmínky. Příkladem může být např. absentující nutnost použití zábranných mechanických prostředků k zabezpečení průlezných otvorů u oblasti typu 2, pokud se tento otvor cit.: „*a) nachází se alespoň*

5,5 m nad terénem, b) nelze k němu jednoduše proniknout ze střechy nebo za pomoci hromosvodů, okapů, parapetů, jiných stavebních prvků, terénních nerovností, stromů či jiných staveb.“[19] K porovnání rozdílu ve kvalitě mechanických zábranných prostředků autor použije údaje z tabulky č. 14, ČSN EN 1627, která např. udává maximální dobu průlomové odolnosti 3 minuty u bezpečnostní třídy RC 2 za použití sady nářadí A2 a maximální dobu průlomové odolnosti 15 minut u bezpečnostní třídy RC 5 za použití sady nářadí A5. Pro porovnání – sada nářadí A2 podle ČSN EN 1630 obsahuje např. šroubovák, hasák, plastový klín nebo rámovou pilu, tedy pouze ruční nástroje, naproti tomu sada A5 již zahrnuje např. elektrickou vrtačku se sadou vrtáků, přímočarou pilu nebo úhlovou brusku.[20] ČSN EN 1627 při testování výrobků posuzuje výrobek jako celek, tedy v případě okna je posuzován např. okenní rám, sklo, uzavírací mechanismus, ukotvení okenního křídla i způsob ukotvení do zdiva.[21] Bezpečnostní třída tedy udává komplexní údaj o kvalitě výrobku. Vyhláška č. 528/2005 Sb. posuzuje komplexně zabezpečení pláště objektu a při projektování je nutné uvést takový typ oblasti, kterému odpovídá nejslabší prvek systému zabezpečení. Uzamykací systémy zabezpečených oblastí rozděluje vyhláška č. 528/2005. Sb. do čtyř kategorií, analogicky ke kategoriím mechanických zábranných prostředků, a sice typ 0 až typ 4. Tabulka č. 5 přiřazuje k jednotlivým typům uzamykacích systémů příslušnou bezpečnostní třídu podle ČSN EN 1627 a bodovou hodnotu SS4 podle vyhl. č. 528/2005 Sb.

Tabulka č. 5 – Typy uzamykacích systémů zabezpečené oblasti dle vyhlášky č. 528/2005 Sb.

Typ uzamykacího systému zabezpečené oblasti dle vyhl. č. 528/2005 Sb.	Požadavek na certifikaci NBÚ	Odkazovaná norma ČSN	Bezpečnostní třída podle ČSN EN 1627	Bodová hodnota SS4
Typ 4	ano	ČSN EN 1627	RC 5	4
Typ 3	ano	ČSN EN 1627	RC 4	3
Typ 2	ano	ČSN EN 1627	RC 3	2
Typ 1	ano	-	RC 2	1
Typ 0	ne	-	-	nehodnoceno

[19] ČESKO, Vyhláška č. 528/2005 Sb. ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků. In *Sbírka zákonů České republiky.* 2005, částka 179/2005.
[20] ČESKO, ČSN EN 1630, Praha: Český normalizační institut, březen 2022.
[21] ČESKO, ČSN EN 1627, Praha: Český normalizační institut, březen 2022.

Maximální doby průlomové odolnosti jsou u jednotlivých bezpečnostních tříd shodné, jako v případě zabezpečených oblastí.

2.4 SYSTÉM KONTROLY VSTUPU DO ZABEZPEČENÉ OBLASTI NEBO OBJEKTU A REŽIM NÁVŠTĚV

Systém kontroly vstupu (dále jen SKV) definuje L. Lukáš jako cit.: "*soubor opatření k zajištění řízení a evidence přístupu do zabezpečeného objektu nebo prostor na základě jednoznačně přidělených přístupových práv.*"[22] Podle vyhlášky č. 528/2005 Sb. je SKV v oblasti OUI řešen pouze v případě, že je realizován na všech vstupech do objektu nebo zabezpečené oblasti. Vyhl. č. 528/2005 Sb. dělí SKV do čtyř skupin, a sice typ 1 až typ 4, přičemž typ 2, 3 a 4 vyžadují provedení podle stupně 3 podle ČSN EN 60839-11-1. Požadavky na jednotlivé typy SKV a jejich dílčí SS6 hodnoty autor uvádí v tabulce č. 6.

Tabulka č. 6 – Typ systému kontroly vstupu podle vyhlášky č. 528/2005 Sb.

Typ SKV dle vyhl. č. 528/2005 Sb.	Požadavek na certifikaci NBÚ	Odkazovaná norma ČSN	Stupeň podle ČSN EN 60839-11-1	Bodová hodnota SS6
Typ 4	ano	ČSN EN 60839-11-1	3	4
Typ 3	ano	ČSN EN 60839-11-1	3	3
Typ 2	ano	ČSN EN 60839-11-1	3	2
Typ 1	ne	-	-	1

Typ 4 a typ 3 podle vyhl. č. 528/2005 Sb. vyžaduje k přístupu kombinaci identifikačního prvku (např. čipová karta) a PINu, nebo biometrie a PINu, nebo identifikačního prvku a biometrie, přičemž typ 4 zároveň vyžaduje doplnění přístupovou bariérou znemožňující režim opakovaného přístupu. Při praktickém použití SKV typu 4 je tedy nutné identifikace při vstupu, aby byl následně možný výstup ze zabezpečené oblasti/objektu. Nelze tedy realizovat vstup „na jednu kartu" s kolegou a následně oblast/objekt opustit s vlastní identifikací. U typu 2 je k realizaci vstupu používán identifikační prvek, PIN, nebo biometrie. Typ 1 potom tvoří pouze mechanická zábrana vstupu.

[22] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík – VeRBuM, 2015. ISBN 978-80-87500-05-7, str. 123.

Identifikace pomocí biometrie vychází z faktu, že určité fyziologické, případně behaviorální vlastnosti jedince jsou jedinečné. Mezi typické fyziologické vlastnosti řadíme např. otisk prstu, oční sítnice, oční duhovka, obličej, tvar ruky nebo obraz krevního řečiště. Mezi znaky behaviorální lze zařadit např. podpis nebo chůzi. Identifikace proběhne na základě vyhodnocení snímačem zjištěných dat řídící jednotkou, která porovná zjištěná data s předem definovanou databází a následně povolí nebo zamítne vstup /výstup.[23]

Režim návštěv rozděluje vyhláška č. 528/2005 Sb. do tří kategorií, a sice návštěvy s doprovodem, návštěvy bez doprovodu a návštěvy bez kontroly. Návštěva s doprovodem je realizována doprovázením návštěvy po celou dobu trvání návštěvy, nemusí být nutně realizována pracovníkem fyzické ostrahy, postačí doprovod zaměstnance/oprávněné osoby. Vyžaduje zároveň vedení evidence návštěv (jméno, identifikační číslo (např. občanský průkaz) a čas příchodu a odchodu). Zároveň je požadováno viditelné označení návštěvy. Tato kategorie je hodnocena podle vyhlášky č. 528/2005 Sb. hodnotou SS7=3 body. Režim návštěv bez doprovodu vyžaduje rovněž evidenci a viditelné označení návštěvy jako v předchozím případě, je zde však nutná i viditelné označení oprávněných osob/zaměstnanců. Tato kategorie je hodnocena hodnotou SS7=1 bod. V případě návštěv bez kontroly, kdy návštěvy vstupují bez kontroly a doprovodu, se tento režim podle vyhlášky č. 528/2005Sb. nehodnotí.[24]

2.5 ZAŘÍZENÍ ELEKTRONICKÉ ZABEZPEČOVACÍ SIGNALIZACE

Primárním úkolem elektronických zabezpečovacích a tísňových systémů (dále jen EZTS, případně EZS) je detekování, vyhodnocení a následná signalizace změn v chráněném prostoru vyvolaných neoprávněnou osobou. V kombinaci s mechanickými zábrannými systémy představují jedno z nejspolehlivějších řešení ochran prostoru nebo objektu. Při vyhodnocení změny v zájmovém prostoru signalizují tuto změnu pracovníkům ostrahy, kteří následně přijímají další opatření v režimu své působnosti. Mezi prvky systému EZTS řadíme **pohybová**

[23] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík-VeRBuM, 2015. ISBN 978-80-87500-05-7, str. 129.
[24] ČESKO, Vyhláška č. 528/2005 Sb. ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků. In *Sbírka zákonů České republiky*. 2005, částka 179/2005.

čidla (detektory pohybu), která na základě fyzikálně či chemicky vyvolaných změn reagují a vysílají signál **ústředně. Ústředna** přijaté informace vyhodnotí a na základě předem nastaveného programu odešle signál přes **přenosové prostředky signalizačnímu zařízení**, které informuje (akusticky či světelně) ostrahu o zjištěné změně v zájmovém prostoru/objektu. Doplňujícím prvkem systému EZTS je **ovládací zařízení**.[25]

Vyhláška č. 528/2005 Sb. dělí EZTS do 4 skupin označených jako typ 1 až typ 4. Požadavky na jednotlivé typy podle ČSN, Certifikaci NBÚ a bodové hodnocení SS91 jednotlivých typů autor uvádí v tabulce č. 7.

Tabulka č. 7 – Typy EZTS podle vyhlášky č. 528/2005 Sb.

Typ EZTS dle vyhl. č. 528/2005 Sb.	Požadavek na certifikaci NBÚ	Stupeň zabezpečení podle ČSN EN 50131-1 ed. 2	Stupeň rizika podle ČSN EN 50131-1 ed. 2	Bodová hodnota SS91
Typ 4	ano	4	vysoké	4
Typ 3	ano	3	střední až vysoké	3
Typ 2	ano	2	nízké až střední	2
Typ 1	ne	-	-	1

Vyhláška č. 528/2005 Sb. přiřazuje k jednotlivým typům EZTS i stupeň utajení, pro které je nutné tento typ použít. Jednotlivá stupně utajení přiřazené k typů EZTS uvádí tabulka č. 8.

Tabulka č. 8 – Způsobilost EZTS pro stupně utajení podle vyhlášky č. 528/2005 Sb.

Typ EZTS dle vyhl. č. 528/2005 Sb.	Stupeň utajení, pro který byla schválena způsobilost
Typ 4	Přísně tajné
Typ 3	Tajné
Typ 2	Důvěrné

[25] ŠČUREK, Radomír a Daniel MARŠÁLEK. *Technologie fyzické ochrany civilního letiště*. Brno: Akademické nakladatelství CERM, 2014. ISBN 978-80-7204-862-5., str. 23.

2.6 INSTALACE ZAŘÍZENÍ ELEKTRONICKÉ ZABEZPEČOVACÍ SIGNALIZACE

Hodnocen je i rozsah a způsob instalace EZTS. Instalace typu 4 je realizována v rozsahu – prostorová ochrana, plášťová ochrana, tísňový systém a detektory rozbitého skla nebo speciální televizní systém snímající nepřetržitě průlezné otvory zabezpečené oblasti (dále jen STS), typ 3 – prostorová ochrana, plášťová ochrana a tísňový systém nebo STS, typ 2 – prostorová a plášťová ochrana a typ 1 pouze v rozsahu prostorové ochrany. Bodové ohodnocení SS92 jednotlivých typů autor uvádí v tabulce č. 9.[26]

Tabulka č. 9 – Bodové ohodnocení pro jednotlivé typy EZTS podle vyhlášky č. 528/2005 Sb.

Typ EZTS dle vyhl. č. 528/2005 Sb.	Bodové ohodnocení instalace zařízení elektrické zabezpečovací signalizace SS92
Typ 4	4
Typ 3	3
Typ 2	2

2.7 SPECIÁLNÍ TELEVIZNÍ SYSTÉMY

Speciální televizní systémy, často označované zkratkou CCTV (closed circuit television), představují uzavřený televizní okruh sloužící k zajištění bezpečnosti snímáním zájmového prostoru/předmětu pomocí systematicky rozmístěných televizních kamer. Snímaný obraz je následně pomocí přenosových soustav (drátových či bezdrátových) přenášen do místa pracoviště ostrahy, případně na jiná určená místa. Ostraha tak může zájmový prostor/předmět monitorovat v reálném čase. Automatizace systému ve spolupráci s EZTS umožňuje zobrazení prostoru přímo v místě ETZS detekované změny. Usnadňuje tak vyhodnocovací proces obsluhy v reálném čase a zároveň tento systém zpravidla umožňuje záznam přenášeného obrazu k pozdějšímu zpětnému vyhodnocení. Velmi vhodným doplňkem je zařízení umožňující snímání zájmového prostoru/předmětu i za ztížených světelných podmínek. Na základě principu

[26] ČESKO, Vyhláška č. 528/2005 Sb. ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků. In *Sbírka zákonů České republiky*. 2005, částka 179/2005.

činnosti je možno tato zařízení rozdělit na noktovizory a termovize.[27] Speciální televizní systémy musí podle vyhlášky č. 528/2005Sb. splňovat požadavky normy ČSN EN 62676-1-1 a nevyžadují certifikaci NBÚ.

2.8 FYZICKÉ BARIÉRY

Primárním určením fyzických bariér je znemožnění, či maximální možné zpoždění neoprávněného vstupu do zájmového/chráněného prostoru. Do této množiny můžeme zařadit např. mříže, zámky, závory, ploty, retardéry, výškové a podhrabové překážky, bezpečnostní dveře, bezpečnostní skla apod. Každá fyzická bariéra je překonatelná v určitém čase. Tento časový interval je nazýván odporovým časem a je vyjádřen rozdílem času zahájení práce na překonání bezpečnostního prvku a času ukončení práce na překonání bezpečnostního prvku. Vyhláška č. 528/2005 Sb. rozděluje fyzické bariéry zajišťující ochranu perimetru do čtyř kategorií, a sice typ 1 až typ 4. Požadavky vyhlášky č. 528/2005 Sb. na jednotlivé typy a jejich bodové ohodnocení autor uvádí v tabulce č. 10.

Tabulka č. 10 – Požadavky na jednotlivé typy fyzických bariér podle vyhl. č. 528/2005 Sb.

Typ fyzické bariéry podle vyhl. č. 528/2005 Sb.	Minimální výška [m]	Možnost pozorování okolního terénu	Ochrana proti přelezení	Perimetrický detekční systém	Bodová hodnota SS10
Typ 4	2,15	ano	Ano – oboustranné šikmé vzpěry vyčnívající ven i dovnitř pod úhlem 45° o minimální délce 40 cm + ostnatý drát	ano	4
Typ 3	2,15	ano	Ano – jednostranné šikmé vzpěry vyčnívající ven pod úhlem 45° o minimální délce 40 cm, na nichž je po celé délce připevněn ostnatý drát	ne	3
Typ 2	2,15		ano		2
Typ 1	-	ne	ne	ne	1

Doplnění fyzické bariery sloužící jako ochrana perimetru lze podle vyhlášky č. 528/2005 Sb. provést ještě certifikovaným perimetrickým detekčním systémem, jemuž odpovídá bodová hodnota SS13 = 2 body, necertifikovaným perimetrickým

[27] ŠČUREK, Radomír a Daniel MARŠÁLEK. *Technologie fyzické ochrany civilního letiště*. Brno: Akademické nakladatelství CERM, 2014. ISBN 978-80-7204-862-5., str. 29.

detekčním systémem, jemuž odpovídá bodová hodnota SS13 = 1 bod, bezpečnostním osvětlením na perimetru, jemuž odpovídá hodnota SS14 = 2 body a speciálním televizním systémem umístěným na perimetru s hodnotou SS15 = 2 body.

2.9 ZAŘÍZENÍ ELEKTRICKÉ POŽÁRNÍ SIGNALIZACE

Zařízení elektrické požární signalizace (dále jen EPS) je soubor technických prostředků, jehož úkolem je včasná detekce a následná signalizace vznikajícího požáru. Prvky systému EPS tvoří hlásiče požáru, ústředny a doplňující zařízení EPS. Informace o vznikajícím požáru je detekována hlásičem požáru. Pomocí přenosové soustavy (kabelové či bezdrátové) je tato informace formou signálu předána ústředně a tato ústředna zabezpečuje přenos signálu určeným osobám, případně systémům kompetentním k adekvátnímu represivnímu zásahu.[28] Technické požadavky na EPS jsou normovány v ČSN 34 2710 a ČSN EN 54. Vyhláška č. 528/2005 Sb. nepožaduje certifikaci NBÚ, stanovuje však podmínku o nutnosti vyvedení signálu poplachu na stanoviště určené pro stálý výkon ostrahy. EPS dále cit.: "*musí splňovat požadavky jiných právních předpisů, například § 8 vyhlášky č. 246/2001 Sb., o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci), ve znění pozdějších předpisů.*"[29]

2.10 ZAŘÍZENÍ SLOUŽÍCÍ K VYHLEDÁVÁNÍ NEBEZPEČNÝCH LÁTEK NEBO PŘEDMĚTŮ

Vyhláška č. 528/2005 Sb. pouze stanovuje nutnost použití těchto zařízení na vstupu do objektu, případně do zabezpečené/jednací oblasti stupně utajení přísně tajné, bez požadavku na certifikaci NBÚ v předepsané podobě: cit.: „*1. Průchozí detektor kovových předmětů, případně doplněný ručním detektorem kovových předmětů. 2. Rentgenový přístroj pro kontrolu zavazadel, doložený kladným Rozhodnutím Státního úřadu pro jadernou bezpečnost o typovém schválení zdroje ionizujícího záření podle zákona č. 18/1997 Sb., o mírovém využívání jaderné*

[28] UHLÁŘ, Jan. *Technická ochrana objektů III. díl*., Praha: Vydavatelství PA ČR, 2006. ISBN 80-7251-235-8.
[29] ČESKO, Vyhláška č. 528/2005 Sb. ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků. In *Sbírka zákonů České republiky*. 2005, částka 179/2005.

energie a ionizujícího záření a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.“[30]

2.11 ZAŘÍZENÍ FYZICKÉHO NIČENÍ NOSIČŮ INFORMACÍ NEBO DAT

Zařízení fyzického ničení nosičů informací (dále jen NNI) rozděluje vyhláška č. 528/2005 Sb. do pěti kategorií, bez nutnosti certifikace a bez bodového ohodnocení. Vyhláška udává pouze maximální přípustnou velikost odpadních částic, kterým odpovídá maximální možný stupeň utajení, případně jejich úplné zničení. Údaj o přípustné velikosti částic k jednotlivým stupňům utajení uvádí tabulka č. 11.[31]

Tabulka č. 11 – Požadavky na jednotlivé typy NNI podle vyhlášky č. 528/2005 Sb.

Nosič informací nebo dat podle vyhl. č. 528/2005 Sb.	Velikost odpadních částic	Max. stupeň utajení
Typ NNI 4	plocha částic ≤ 5 mm^2	přísně tajné
Typ NNI 3	plocha částic ≤ 10 mm^2	tajné
Typ NNI 2	plocha částic ≤ 30 mm^2 a šířka částic ≤ 2 mm	důvěrné
Typ NNI 1	plocha částic ≤ 160 mm^2 a šířka částic ≤ 6 mm	vyhrazené
Typ 0	Zařízení fyzického ničení nosičů informací nebo dat typu 0 jsou určena pro ničení utajovaných informací stupně utajení přísně tajné nebo nižší. K ničení se používá spálení, roztavení, drcení nebo rozvláknění	

[30] ČESKO, Vyhláška č. 528/2005 Sb. ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků. In *Sbírka zákonů České republiky.* 2005, částka 179/2005.
[31] ČESKO, Vyhláška č. 528/2005 Sb. ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků. In *Sbírka zákonů České republiky.* 2005, částka 179/2005.

2.12 ZAŘÍZENÍ PROTI PASIVNÍMU A AKTIVNÍMU ODPOSLECHU UTAJOVANÝCH INFORMACÍ

Elementární úkolem těchto zařízení je zabránit možnosti úniku utajované informace z jednací oblasti. Pasivní ochranu proti odposlechu je nutno dle vyhlášky č. 528/2005 Sb. zajistit cit.: „*dostatečně zvukotěsnými stěnami, dveřmi, podlahou a stropem,*“[32] a dále nařizuje chránit jednací oblasti proti vizuálnímu odezírání z prostorů nacházejících se mimo oblast. Vizuální odezírání je typicky řešeno roletami, žaluziemi, případně neprůhlednými okenními foliemi. Aktivní ochranu nařizuje vyhláška řešit jednak režimovými opatřeními, v podobě např. odpojování koncového zařízení neutajovaného komunikačního systému (telefonu) při projednávání utajované informace v jednací oblasti, zákazu vnášení mobilních telefonů do jednacích a utajovaných oblastí, provádění tzv. obranných prohlídek ve lhůtách stanovených zákonem č. 412/2005 Sb. apod. Během obranných prohlídek se mimo jiné provádí detekce odposlechových zařízení. K té je možné podle R. Ščurka použít indikátory pole odposlechových prostředků, nebo analyzátory odposlechových prostředků připojených k linkovému vedení komunikačního systému. Odposlechové prostředky připojené k linkovému vedení jsou však funkční pouze na analogových telefonních linkách, které se již v současné době používají jen velmi zřídka. Jako relevantní možnost řešení ochrany proti aktivnímu odposlechu např. pro rozvody klimatizací R. Ščurek uvádí použití generátoru šumu.[33] Generovaný šum obsahuje všechny frekvence hovorového spektra a aktivně tak zabraňuje možnosti odposlechnutí (i nechtěnému) mluveného slova např. přes rozvody klimatizace. Generátory šumu nepodléhají nutnosti certifikace ze strany NBÚ.

[32] ČESKO, Vyhláška č. 528/2005 Sb. ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků. In *Sbírka zákonů České republiky.* 2005, částka 179/2005

[33] ŠČUREK, Radomír a Daniel MARŠÁLEK. *Technologie fyzické ochrany civilního letiště*. Brno: Akademické nakladatelství CERM, 2014. ISBN 978-80-7204-862-5., str. 30.

2.13 FYZICKÁ BEZPEČNOST INFORMAČNÍHO SYSTÉMU

J. Kolouch dělí fyzickou bezpečnost počítačových systémů obecně na **ochranu před krádeží**, **ochranu před rozebráním a úpravou** a **ochranu před připojením periférií**.[34] Ochrany popsané v této kapitole je třeba vnímat pouze jako jednu z vrstev ochrany. Dále zmíněné ochrany tedy nemohou působit samostatně, ale pouze ve spojení s ochranou objektu jako celku. Následující poznatky, informace a doporučení v této kapitole vychází z informací a poznatků čerpaných z odkazované monografie.[35] Autor zde uvede pouze vybrané druhy ochran s ohledem na potřeby této práce.

2.13.1 OPATŘENÍ PROTI KRÁDEŽI POČÍTAČOVÝCH SYSTÉMŮ

J. Kolouch rozděluje toto opatření na dvě kategorie: **ochrana serverů a klíčových prvků informačních a komunikačních technologií** (dále jen ICT) a **ochrana ostatních počítačových systémů**. Ochrana serverů a klíčových prvků ICT na této vrstvě ochrany je založena na umístění serverů klíčových prvků ICT do standardizovaných skříní, tzv. racků. Tyto skříně umožňují, podobně jako úschovné objekty, řízený přístup v podobě mechanických, biometrických, či elektronických zámků. Tento způsob ochrany je možný s ohledem na absenci nutnosti častého fyzického přístupu k technologiím a sním spojenou, v praxi hojně využívanou, možností vzdáleného datového přístupu k těmto technologiím z tzv. pracovních stanic. Pod pojmem pracovní stanice si lze představit běžný osobní počítač, případně notebook. Právě ochranu proti krádeži osobních počítačů a notebooků J. Kolouch řadí do kategorie **ochrana ostatních počítačových systémů.** K ochraně těchto zařízení doporučuje využití technologie Kensington security slot.

[34] KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7, str. 416.
[35] KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.

2.13.1.1 Kensington security slot

Jedná se o malý slot umístěný zpravidla na boční straně notebooků, monitorů či osobních počítačů. Tento slot umožňuje uzamykatelné připojení ocelového lanka zabraňující krádeži, případně neoprávněné manipulaci s chráněným zařízením. Kvalita této ochrany závisí na kvalitě materiálů použitých při výrobě této ochrany a způsobu její výroby.

2.13.2 OPATŘENÍ PŘED ROZEBRÁNÍM A ÚPRAVOU POČÍTAČOVÝCH SYSTÉMŮ

V případě **ochrany serverů** je základní ochrana řešena většinou již při výrobě skříně serveru v podobě možnosti mechanického uzamčení této skříně. Složitější je provedení tohoto druhu **ochrany ostatních počítačových systémů**, zejména pokud nejsou permanentně umístěna v prostoru s řízeným přístupem. J. Kolouch se zde doporučuje soustředit na ochranu dat uložených na pevném disku v podobě softwarového uzamčení dat v BIOSu počítače, případně šifrování dat pomocí externího softwarového nástroje. Jako příklad zde lze uvést šifrovací nástroje VeraCrypt nebo BitLocker. Specifikou skupinu představují tiskárny, jakožto výstupní zařízení informačního systému. I tiskárny obsahují svá vlastní úložiště dat. V případě použití tiskárny k výstupu utajovaných informací je tedy nezbytné zajistit nemožnost zneužití těchto dat.

2.13.3 OCHRANA PŘED PŘIPOJENÍM CIZÍCH PERIFERIÍ K POČÍTAČOVÝM SYSTÉMŮM

J. Kolouch v odkazované monografii uvádí příklady periferií v podobě USB zařízení, určených přímo ke skrytému čtení zpracovávaných dat v počítačovém systému. Tato zařízení jsou volně prodejná a jejich použití tak zvládne i běžný uživatel. Jedním z nich je USB zařízení *USB Rubber Ducky,* které umožňuje skryté ukládání zpracovávaných dat, případně jejich přímé předávání pomocí bezdrátové technologie třetím zařízením.[36] J. Kolouch zde doporučuje použít ochranu USB

[36] WEB, Mall.cz. *Mall.cz* [online]. [cit. 2022-10-20]. Dostupné z: < https://www.mall.cz/brasny-kufry-motorka/keelog-airdrive-usb-keylogger-100093873900?gclid=Cj0KCQjw48OaBhDWARIsAMd966AxkoAHesBVW7ktSLTmA3H6riLfgYAppmcWlE7JA9XP0WPrfVsSB04aAiXiEALw_wcB>.

portů, jako je například technologie *USB Lock Cable Guard*, umožňující mechanické uzamčení volných portů a připojených periferií.

2.14 CERTIFIKACE POČÍTAČOVÉHO SYSTÉMU A NÁLEŽITOSTI ZAJIŠTĚNÍ OCHRANY PROTI KOMPROMITUJÍCÍMU VYZAŘOVÁNÍ

Podle zákona č. 412/2005 Sb. a vyhlášky č. 523/2005 Sb. s sebou nese zavedení nového informačního systému nutnost certifikace tohoto informačního systému. Certifikační autoritou je Odbor bezpečnosti informačních a komunikačních technologií Národního úřadu pro kybernetickou a informační bezpečnost. Vyhláška č. 523/2005 Sb. dále stanovuje nutnost zabezpečení proti kompromitujícímu vyzařování jednotlivých částí informačního systému (dále jen IS) podle tzv. standardů[37]. Podle těchto standardů probíhá hodnocení IS, hodnocení prostorů a hodnocení instalace IS. Hodnocení IS se provádí podle standardu NATO SDIP-27/2 nebo standardu EU IASG7-03 a částečně podle ČSN EN 55022, k hodnocení prostorů, nebo též určení zóny prostorů je standardem standard NATO SDIP -28/2 nebo EU IASG 7-02 a hodnocení instalace IS v zabezpečené oblasti podle NATO SDIP-29/2 nebo standardu EUIASG 7-01.

[37] ČESKO, Vyhláška č. 523/2005 Sb. ze dne 25. prosince 2005, o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor. In *Sbírka zákonů České republiky*. 2005, částka 179/2005.

3 URČENÍ OBJEKTU, ZABEZPEČENÝCH A JEDNACÍCH OBLASTÍ

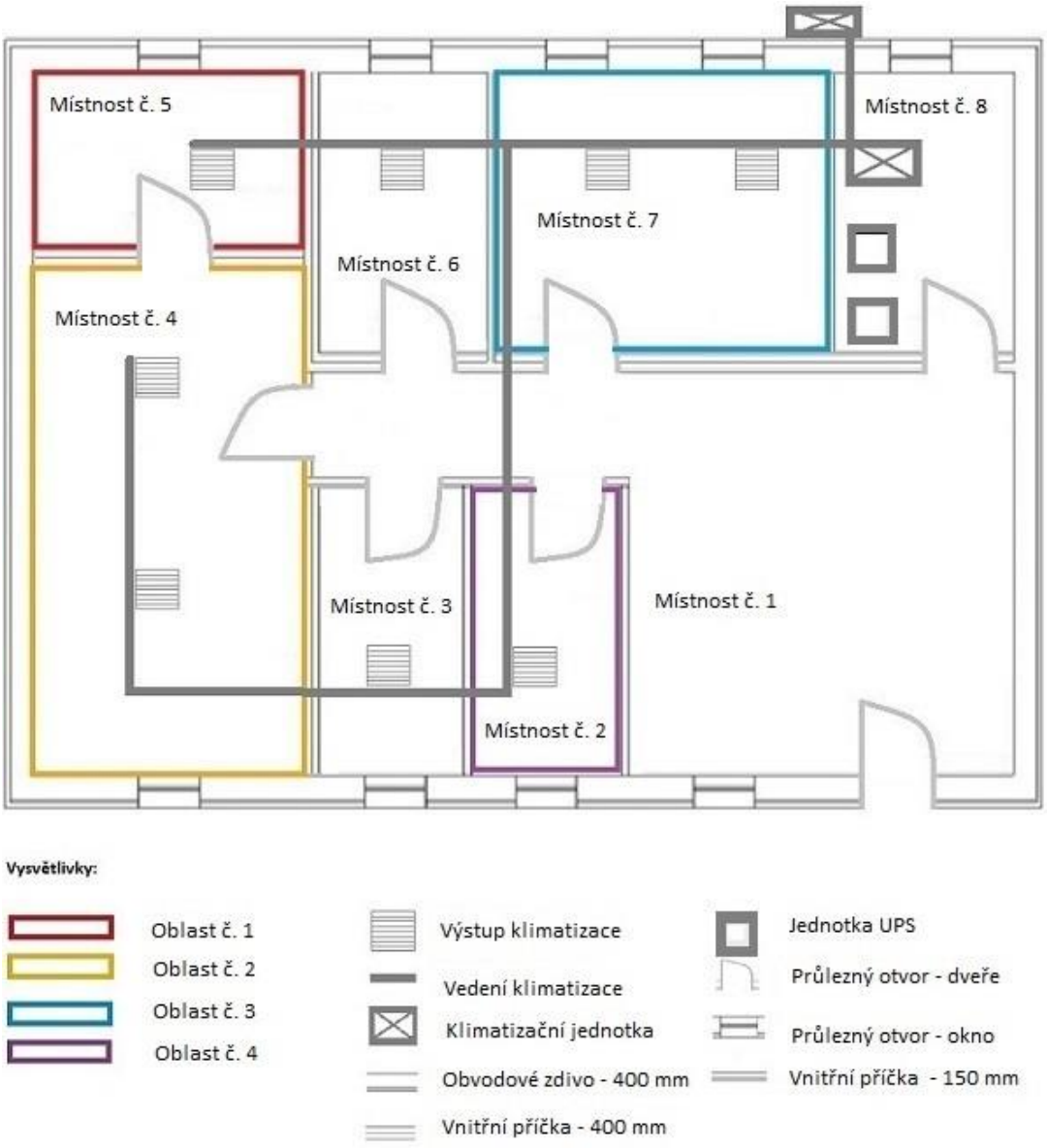
V úvodní části této kapitoly je představen stávající stav zájmového objektu a definovány požadavky na stav cílový. V následujících podkapitolách pak autor definuje jednotlivé nutné stavební a jiné úpravy zájmového objektu, a to v takovém rozsahu, aby objekt splňoval požadavky uvedených právních předpisů vztahujících se na ochranu utajovaných informací.

3.1 VSTUPNÍ INFORMACE ZÁJMOVÉHO OBJEKTU

Zájmový objekt představuje fiktivní budova dislokovaná ve vojenském zařízení na území České republiky. V tomto vojenském zařízení je zřízen pult centrální ochrany (dále jen PCO) s možností vyslání ozbrojené ostrahy tvořené příslušníky ozbrojených sil AČR. Doba příjezdu ozbrojené ostrahy je 5 minut. Zájmový objekt je po obvodu perimetru ohraničen dřevěným oplocením o výšce 2,2m s jedním přístupovým bodem pro pěší i pro vozidla. Jedná se o administrativní budovu s jedním nadzemním patrem projektovanou a postavenou v 80. letech minulého století. Nákres budovy je znázorněn na obrázku č. 1.

Budova byla částečně rekonstruována v roce 2010. Tato rekonstrukce zahrnovala kompletní výměnu elektrických rozvodů včetně umístění záložních bateriových zdrojů energie a montáž klimatizační jednotky zajišťující vytápění a cirkulaci vzduchu v budově. Budova má obdélníkový půdorys. Plášť budovy představuje zděná cihlová konstrukce o síle 400 mm. Plášť budovy je osazen deseti vstupy, z nichž 9 jsou plastová okna o rozměrech 600 x 1000 mm a jedny vstupní plastové dveře o rozměru 800 x 1970 mm. Okna jsou umístěna v plášti budovy ve výšce 1500 mm nad úrovní terénu. Vnitřek budovy představuje chodba s předsálím a 8 místností, z nichž 7 je přístupných z chodby s předsálím a místnost číslo 5 je přístupna z místnosti č. 4. Předsálí s chodbou je označeno jako místnost č. 1. Místnosti č. 2, 4, 5 a 7 jsou místnosti určené k administrativní činnosti, v místnosti č. 6 je umístěna kuchyňka a v místnosti č. 3 jsou umístěna sociální zařízení. Místnost č. 8 je technickou místností budovy. Je zde umístěna vnitřní jednotka klimatizace a záložní bateriové zdroje el. energie UPS (dále je UPS). V této místnosti je zároveň přípojný bod objektu na veřejnou síť el. energie. Venkovní jednotka klimatizace je umístěna na vnějším plášti budovy. Vnitřní příčky budovy tvoří cihlové zdi o síle 400 mm nebo o síle 150 mm. Obvodové zdivo a příčky

o síle 400 mm jsou na výkresu budovy vyznačeny trojitou čarou, příčky o síle 150 mm čarou dvojitou. Podlahu celé budovy tvoří betonová základová deska o síle 600 mm a pod budovou se nenachází žádné podzemní patro ani jiné objekty. Budova je napojena na inženýrské sítě v podobě silových kabelů a vodovodní řadu. Dále je v místnosti č. 5 ukončen optický kabel připojený na telekomunikační infrastrukturu vojenského zařízení. Stropy ve všech místnostech jsou konstruovány z vápenocementových bloků o síle 160 mm. Střecha budovy je původní rovné konstrukce s plechovou krytinou. Vnější prostor budovy představuje volné prostranství bez vzrostlých stromů. Nejbližší sousední objekt se nachází ve vzdálenosti 105 m. V budově je nainstalováno zařízení EZPS splňující požadavky § 8 vyhlášky č. 246/2001Sb., o požární prevenci. V odstínech šedi je na obrázku č. 1 vyznačen aktuální stav budovy, plášť budovy, průlezné otvory (okna a dveře) spolu se zdroji UPS a vnitřní jednotkou klimatizace v místnosti č. 8. a rozvody klimatizace včetně jejích výstupů v jednotlivých místnostech. Barevně jsou zde znázorněny požadované zabezpečené a jednací oblasti v určených stupních utajení.



Obrázek č. 1 – Nákres zájmového objektu

3.2 POŽADAVKY NA ZABEZPEČENÉ A JEDNACÍ OBLASTI

V zájmovém objektu je požadováno zřízení čtyř oblastí podle zákona č. 412/2005 Sb. specifikovaných v následujících podkapitolách.

3.2.1 ZABEZPEČENÁ OBLAST Č. 1

Zamýšlená zabezpečená oblast ve smyslu znění § 24 odst. 3 zákona č. 412/2005 Sb. bude primárně určena ke zpracovávání utajovaných informací ve stupni utajení přísně tajné třídy 1. Informace budou zpracovávány informačním systémem spolu s kryptografickým prostředkem ke zpracovávání informací do stupně utajení přísně tajné.

3.2.2 JEDNACÍ OBLAST Č. 2

Zamýšlená jednací oblast ve smyslu znění § 24 odst. 4 zákona č. 412/2005 Sb. bude primárně určena k projednávání, zpracovávání a zobrazování utajovaných informací do stupně utajení tajné. Je zde požadavek na zřízení informačního systému určeného k zobrazování utajovaných informací do stupně utajení tajné.

3.2.3 ZABEZPEČENÁ OBLAST Č. 3

Tato zabezpečená oblast ve smyslu znění § 24 odst. 3 zákona č. 412/2005 Sb. bude primárně určena ke zpracovávání utajovaných informací ve stupni utajení důvěrné třídy 1. V oblasti je také požadováno použití úschovného objektu k ukládání informací do stupně utajení důvěrné a zařízení fyzického ničení informací nebo dat do stupně utajení důvěrné.

3.2.4 ZABEZPEČENÁ OBLAST Č. 4

Zabezpečená oblast č. 4 ve smyslu znění § 24 odst. 3 zákona č. 412/2005 Sb. je předurčena ke zpracovávání utajovaných informací ve stupni utajení vyhrazené třídy 1. V oblasti je rovněž zamýšleno použití úschovného objektu k ukládání informací do stupně utajení vyhrazené a zařízení fyzického ničení informací nebo dat do stupně utajení vyhrazené.

3.3 ÚPRAVY STÁVAJÍCÍ OCHRANY OBJEKTU

Vzhledem ke specifickým požadavkům na jednotlivé oblasti je nutné provést na zájmovém objetu úpravy uvedené v následujících podkapitolách.

3.3.1 NUTNÉ STAVEBNÍ A JINÉ ÚPRAVY OBJEKTU

Vybudovaní ochrany perimetru zájmového objektu v podobě fyzické bariéry typu 4 včetně vstupní brány umožňujících kontrolovaný pohyb osob a vozidel. Ochranu perimetru v podobě fyzické bariéry je nutné doplnit perimetrickým detekčním systémem, bezpečnostním osvětlením perimetru (příp. noktovizorem) a speciálním televizním systémem umístěným na perimetru. Dále výměnu oken a dveří zájmového objektu za okna a dveře splňující požadavky bezpečnostní třídy RC 4 podle ČSN EN 1627, opařená magnetickými čidly detekující otevření dveří /oken, okna vybavená žaluziemi znemožňujícími odezírání z vnějších prostor a čidly detekujícími rozbití skla. Dále je nutné vybudovat opatření omezující působení blesků. Autor považuje za nutné zajistit instalaci bleskosvodu, a dále ochranu proti přepětí umístěnou nejlépe v místě připojení zájmového objektu na elektrickou síť, v případě našeho zájmového objektu tedy v místnosti č. 8.

3.3.2 ÚSCHOVNÉ OBJEKTY A JEJICH ZÁMKY

Pořízení úschovného objektu typu 2 opatřeného zámkem typu 2 do zabezpečené oblasti č. 3 a rovněž do zabezpečené oblasti č. 4.

3.3.3 UZAMYKACÍ SYSTÉMY URČENÉ K UZAMYKÁNÍ ZABEZPEČENÝCH OBLASTÍ

Pořízení uzamykacího systému typu 3, splňujícího požadavky bezpečnostní třídy RC 4 podle ČSN EN 1627 k uzamykání oblastí č. 1, 2, 3 a 4.

3.3.4 SYSTÉM KONTROLY VSTUPU DO ZABEZPEČENÉHO OBJEKTU

Pořízení a instalace systému kontroly vstupu pro kontrolu stupu do perimetru objektu, vstupu do objektu a vstupů do všech zabezpečených a jednacích oblastí typu 3. Ovládací panely systému kontroly vstupu umístit u hrany vstupního otvoru po vnitřní i vnější straně. Realizaci zabezpečené oblasti stupně utajení přísně tajné podmiňuje instalace zařízení k vyhledávání nebezpečných předmětů, a to na

základě znění vyhl. č. 528/2005 Sb., v podobě průchozího bezpečnostního rámu – detektoru kovů. Vzhledem ke stavebnímu řešení zájmového objektu se autor přiklání k umístění tohoto zařízení u vstupu do objektu.

3.3.5 OSTRAHA, NAMÁTKOVÉ PROHLÍDKY A REŽIM NÁVŠTĚV

Ostraha objektu může být prováděna příslušníky ozbrojených sil Armády České republiky formou útvarových směn. Ekonomické náklady na zřízení této ostrahy by byly zcela minimální. Z tohoto důvodu je možné navrhnout zřízení ostrahy typu 4. Zároveň je možné v průběhu provádění ostrahy provádět namátkové kontroly vstupujících a vystupujících osob jak do prostoru perimetru objektu, tak do budovy samotné, doprovod návštěv dle názoru autora není nutný. Zřízení stanoviště ostrahy bude provedeno v místnosti č. 1 v zájmovém objektu.

3.3.6 OSTRAHA A ZAŘÍZENÍ ELEKTRICKÉ ZABEZPEČOVACÍ SIGNALIZACE (EZS)

Zajištění ostrahy objektu typu 4 podle vyhlášky č. 528/2005 Sb. a dále instalace zařízení EZS typu 4, zároveň tísňového systému splňujícího požadavky ČSN EN 50134-1. Ochrana průlezných otvorů – oken pomocí detektoru rozbití skla s mikrofonem, tísňový systém pomocí bezpečnostních tlačítek. Rozmístění čidel pohybu do všech místností objektu. Typ 4 je nutný na základě hodnot tabulky přiřazení kategorií k typům technických prostředku EZS uvedenou v příloze č. 1 vyhlášky č. 528/2005 Sb.[38]

3.3.7 INSTALACE EZS

Instalace EZS typu 4 do všech místností objektu. Detekce pohybu bude prováděna v podobě rozmístění pohybových PIR čidel. Výstupní hlášení EZS a ovládání EZS bude vyvedeno na stanoviště ostrahy zájmového objektu a zároveň na stanoviště obsluhy PCO vojenského zařízení.

[38] ČESKO, Vyhláška č. 528/2005 Sb. ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků. In *Sbírka zákonů České republiky.* 2005, částka 179/2005.

3.3.8 SPECIÁLNÍ TELEVIZNÍ SYSTÉMY

Instalace speciálního televizního systému nepřetržitě snímající ochranu perimetru a dále nepřetržitě snímající průlezné otvory do zabezpečených a jednacích oblastí. Obrazový výstup speciálního televizního systému bude vyveden na stanoviště ostrahy zájmového objektu a zároveň na PCO vojenského zařízení.

3.3.9 ZAŘÍZENÍ FYZICKÉHO NIČENÍ NOSIČŮ INFORMACÍ NEBO DAT

Pořízení a instalace zařízení fyzického ničení nosičů informací nebo dat typu 2 do zabezpečené oblasti č. 3 a typu 1 do zabezpečené oblasti č. 4.

3.3.10 ZAŘÍZENÍ PROTI PASIVNÍMU A AKTIVNÍMU ODPOSLECHU UTAJOVANÝCH INFORMACÍ

Požadavky na zajištění jednací oblasti proti pasivnímu a aktivnímu odposlechu definuje příloha č. 1 vyhlášky č. 528/2005Sb.[39] a je nutné zabezpečit splnění těchto podmínek v jednací oblasti č. 2.

3.3.11 FYZICKÁ BEZPEČNOST INFORMAČNÍHO SYSTÉMU

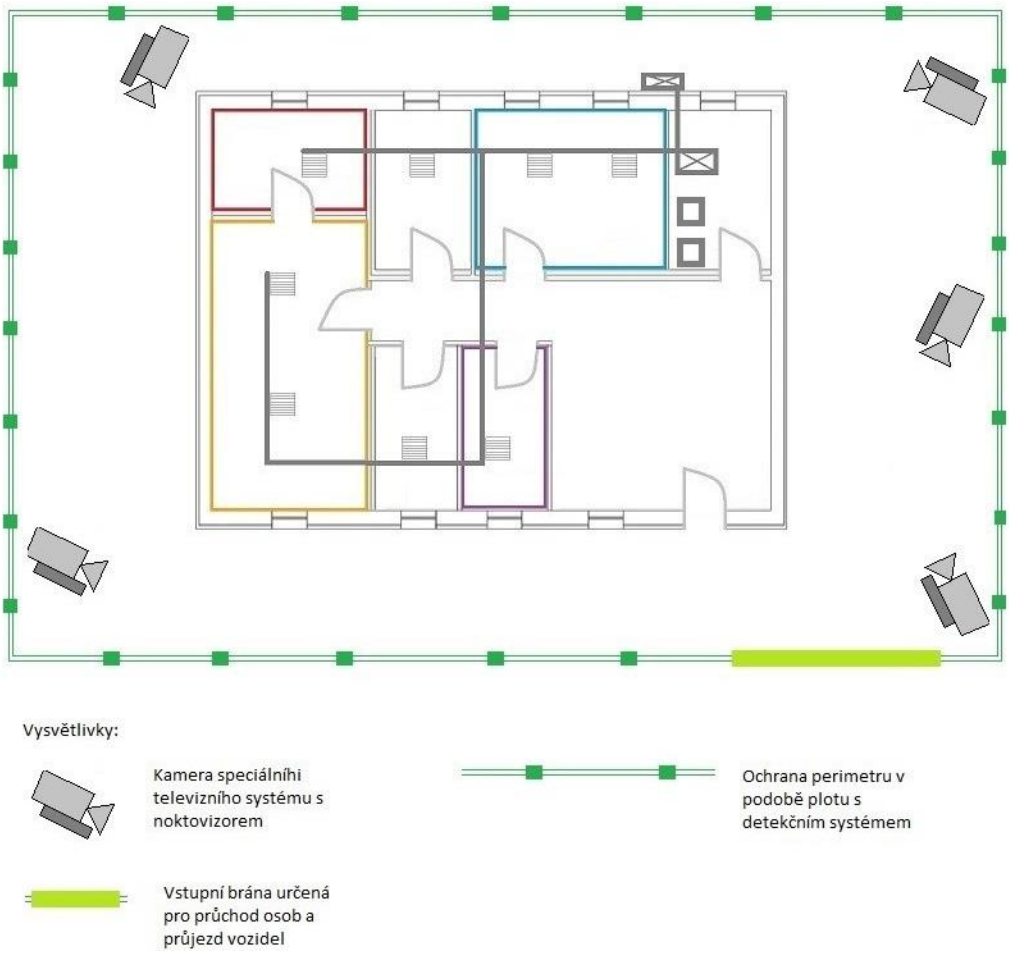
Při zřizování informačního systému je nutné dodržet podmínky stanovené § 20 vyhlášky č. 523/2005 Sb. Zobrazovací zařízení informačního systému bude tedy místěno na zdi oddělují místnost č. 4 a místnost č. 3 tak, aby nevznikla možnost zpozorování zobrazované utajované informace z prostoru vstupních dveří do jednací oblasti č. 2. Autor dále navrhuje systém rozdělit na dvě části, a sice část šifrovanou a nešifrovanou. Hranici rozdělení by tvořil kryptografický prostředek umístěný v zabezpečené oblasti č. 1, z důvodu ukončení komunikační infrastruktury (optického kabelu) v této oblasti. Přenos nešifrované utajované informace bude zajištěn pomocí strukturované kabeláže pouze v rámci oblastí č. 1 a č. 2. Jako fyzickou ochranu ICT autor doporučuje umístit serverovou část ICT technologie do uzamykatelného racku. Stejně tak umístění kryptografického prostředku do samostatného uzamykatelného racku s řízeným přístupem. Identifikace uživatele pro přístup k utajovaným informacím se provádí jménem a autentizace uživatele heslem. Certifikace počítačového systému a zajištění

[39] ČESKO, Příloha č. 1, Vyhláška č. 528/2005 Sb. ze dne 14. prosince 2005, o fyzické bezpečnosti a certifikaci technických prostředků. In *Sbírka zákonů České republiky.* 2005, částka 179/2005.

ochrany proti kompromitujícímu vyzařování musí odpovídat podmínkám stanoveným vyhláškou č. 523/2005 Sb., uvedeným v kapitole č. 2.13.4. Dále je zde nezbytná certifikace kryptografického prostředku odpovídající podmínkám vyhl. č. 525/2005 Sb., a další náležitosti uvedené ve vyhlášce č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací.

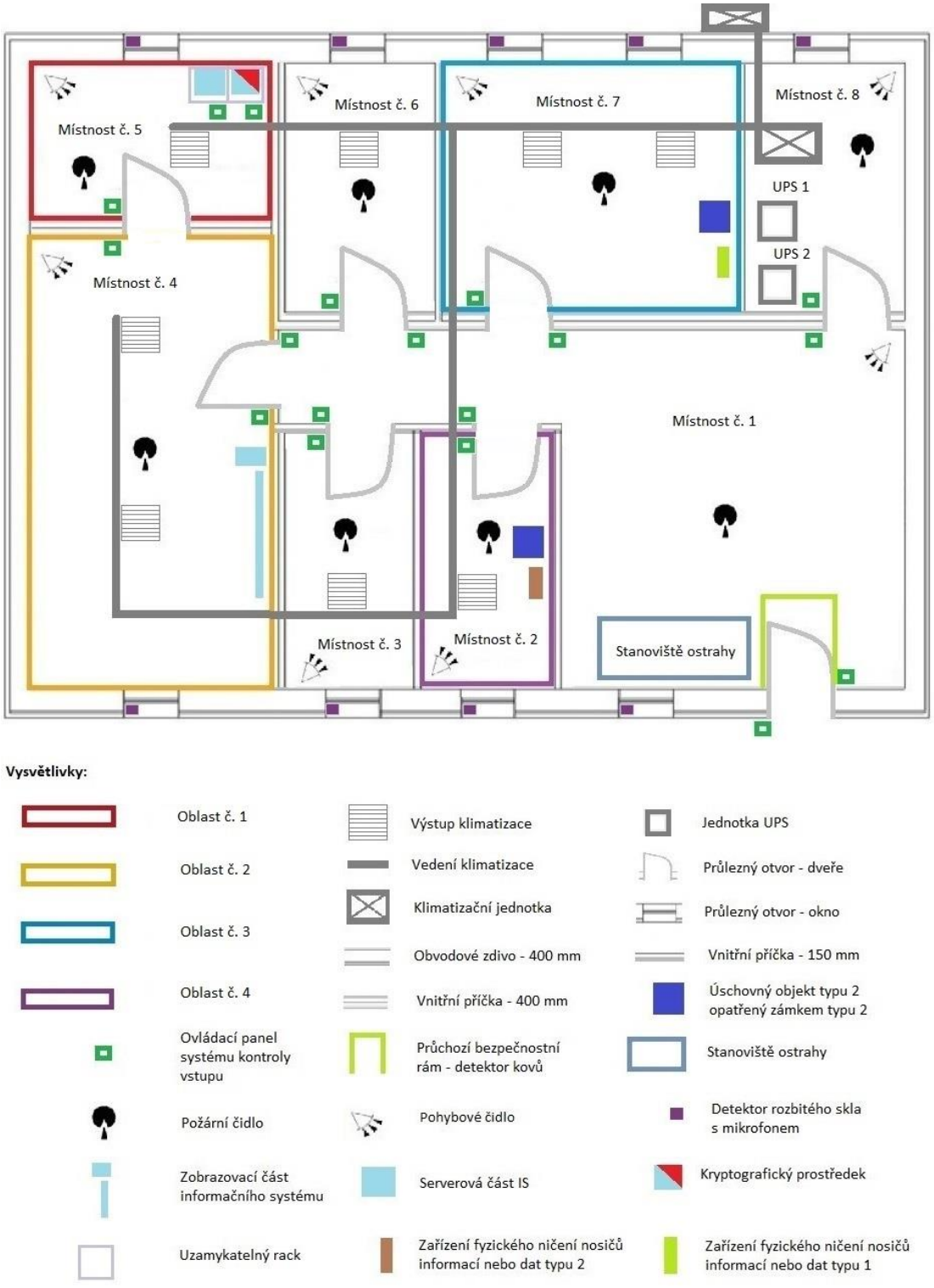
3.4 NÁKRES ZÁJMOVÉHO OBJEKTU PO ÚPRAVÁCH

Obrázek č. 2 zobrazuje nákres ochrany perimetru zájmového objektu v podobě bezpečnostního oplocení doplněné o prvky kamerového systému se zařízením umožňující snímání zájmového prostoru za ztížených podmínek.



Obrázek č. 2 – Nákres ochrany perimetru zájmového objektu po úpravách

Na obrázku č. 3 je představen výkres zájmového objektu po nutných úpravách uvedených v kapitole č. 3 s vybranými prvky jednotlivých systémů zabezpečení objektu.



Obrázek č. 3 – Nákres zájmového objektu po úpravách

4 MANAGEMENT RIZIK

Využití jednotlivých druhů ochran závisí na způsobu využití objektů určených k ochraně utajovaných informací. Zejména na druhu skladovaného materiálu, povaze utajovaných informací, a zároveň na příslušném stupni utajení daného objektu, nebo prostoru. Analyzovány zde budou množiny hrozeb znázorněné pomocí Ishikawova diagramu. Na základě výsledků analýzy budou pro jednotlivé množiny hrozeb určeny výsledné míry rizika pro každou zabezpečenou nebo jednací oblast zvlášť. Z těchto výsledků následně vychází hodnocení provedení ochrany utajovaných informací 2.13 tabulky bodového ohodnocení opatření fyzické bezpečnosti v zabezpečené a jednací oblasti uvedené v kapitole č. 14.3.1 přílohy č. 1. vyhlášky č. 528/2005 Sb. Tabulka bodového ohodnocení opatření fyzické bezpečnosti v zabezpečené a jednací oblasti podle kapitoly č. 14.3.1 přílohy č. 1. vyhlášky č. 528/2005 Sb. je současně přílohou č. 1 této práce. Vypočtené hodnoty zároveň musí dosahovat bodových hodnot nejnižší míry zabezpečení zabezpečené oblasti, případně jednací oblasti, určené kategorie, uvedené v kapitolách č. 12.1 a 12.2 přílohy č. 1. vyhlášky č. 528/2005 Sb. při vypočtené míře rizika, a zároveň splňovat další podmínky bodových hodnot současně uvedených v těchto kapitolách.

4.1 DEFINICE POJMŮ KAPITOLY

V této podkapitole autor uvede klíčové pojmy týkající se řešené problematiky. Autor zde použil definice uvedené v Terminologickém slovníku ministerstva vnitra ČR. Prvním pojmem je pojem **ohrožení**. Jedná se o *cit.: „potenciálně nebezpečné fyzické události, jevy nebo lidská činnost, které mohou způsobit ztrátu života nebo zranění, škodu na majetku, sociální a ekonomické narušení nebo zhoršováním životního prostředí. Ohrožení mohou obsahovat skryté podmínky, které mohou představovat budoucí hrozby a mohou mít různý původ: přírodní (geologické, hydrometeorologické a biologické), nebo vyvolané lidskými procesy (zhoršování životního prostředí a technologických rizik).“* Dalším souvisejícím pojmem je pojem **hrozba**, která představuje cit*.: „přírodní nebo člověkem podmíněný proces představující potenciál, tj. schopnost zdroje hrozby být aktivován a způsobit škodu. Tento potenciál může být spuštěn záměrně nebo náhodně využit pro atakování*

specifických zranitelností aktiva. Hrozba bývá zdrojem rizika.“ a pojem **riziko**, který je definován jako cit.: *„možnost, že s určitou pravděpodobností vznikne událost, kterou považujeme z bezpečnostního hlediska za nežádoucí. Riziko je vždy odvoditelné a odvozené z konkrétní hrozby.“* [40] **Mimořádná událost** je definována dle zákona č. 239/200Sb. jako cit.: “*škodlivé působení sil a jevů vyvolaných činností člověka, přírodními vlivy, a také havárie, které ohrožují život, zdraví, majetek nebo životní prostředí a vyžadují provedení záchranných a likvidačních prací.“*[41] Posledním zde uváděným pojmem je pojem **Ishikawův diagram**, též diagram příčin a následků, případně označovaný jako diagram „rybí kosti“. Jedná se o metodu, která cit.: „*identifikuje a nalézá pravděpodobné příčiny posuzovaného jevu.“*[42] Pro potřeby této práce je posuzovaným jevem únik nebo zneužití utajované informace.

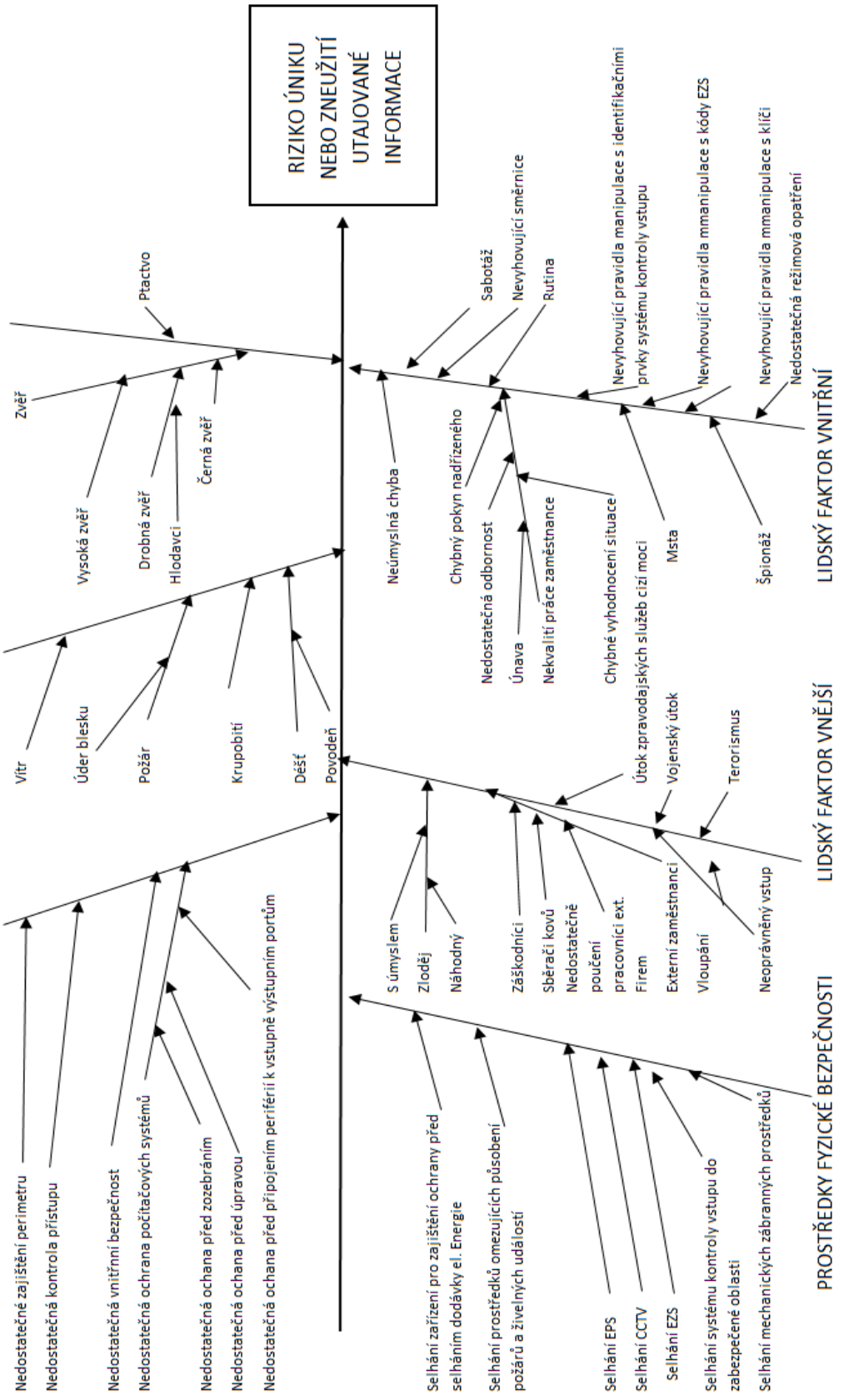
4.2 PŘEHLED IDENTIFIKOVANÝCH HROZEB

V této podkapitole autor představí identifikované hrozby potenciálně způsobilé vzniku rizika úniku nebo zneužití utajované informace. Autor tyto hrozby rozdělil do šesti množin:

- Lidský faktor vnitřní
- Lidský faktor vnější
- Prostředky fyzické bezpečnosti
- Naturogenní mimořádná událost biotická
- Naturogenní mimořádná událost abiotická
- Fyzická bezpečnost IS.

Množiny identifikovaných hrozeb jsou znázorněny pomocí Ishikawova diagramu na obrázku č. 4. Jednotlivé hrozby byly identifikovány na základě zkušeností autora získaných praxí v AČR.

[40] ČESKO. Terminologický slovník ministerstva vnitra. PRAHA 2016, dostupné z: https://www.mvcr.cz/soubor/terminologicky-slovnik-mv-verze-ke-stazeni.aspx.
[41] ČESKO, Zákon č. 239 ze dne 9. srpna 2005 o integrovaném záchranném systému a o změně některých zákonů. In: *Sbírka zákonů České republiky*. 2005, částka 73/2000.
[42] *Ishikawa Diagram: Anticipate and solve problems within your business (Management & Marketing)* [online]. 50Minutes.com, 2015 [cit. 2023-02-10]. ISBN 978-2806270658., str. 5



Obrázek č. 4 – Ishikawův diagram – Přehled identifikovaných hrozeb

4.3 ANALÝZA FMEA

Výraz FMEA je zkratkou slov Failure Mode and Effects Analysis. Odborný časopis Journal of Advanced Research in Aeronautics and Space Science definuje metodu FMEA jako cit.: "*systematickou metodu předběžné identifikace a prevence systémových, produktových a procesních rizik.*"[43] Míra posuzovaného rizika R je určena vzorcem:

$R = P \times N \times H,$

přičemž písmeno P znamená velikost pravděpodobnosti vzniku hrozby, písmeno N závažnost následků hrozby a písmeno H odhalitelnost hrozby. Citace, stejně jako názvy jednotlivých veličin uvedených ve vzorci jsou přeloženy autorem z původního anglického textu. Autor zvolil právě metodu FMEA pro určení míry rizika pro potřeby této práce. Vyhláška č. 528/2005 Sb. stanoví cit.: „*bodové ohodnocení jednotlivých opatření fyzické bezpečnosti, nejnižší míru zabezpečení zabezpečené oblasti a jednací oblasti, základní metodu hodnocení rizik, další požadavky na opatření fyzické bezpečnosti a náležitosti certifikace technického prostředku.*"[44] Tabulka č. 12 znázorňuje bodové hodnocení pravděpodobnosti vzniku množiny hrozeb ve spektru 1 až 5, přičemž vyšší hodnota čísla znamená vyšší pravděpodobnost vzniku. Bodové škály v tabulkách č. 12, č. 13, č. 14 a č. 15, stejně jako názvosloví úrovní pravděpodobnosti vzniku, závažnost následků, odhalitelnost hrozby a výsledné míry rizika jsou zvoleny autorem.

Tabulka č. 12 – Bodové hodnocení pravděpodobnosti vzniku množiny hrozeb

Bodové hodnocení	Pravděpodobnost vzniku P
1	Velmi málo pravděpodobná
2	Málo pravděpodobná
3	Pravděpodobná
4	Velmi pravděpodobná
5	Vysoce pravděpodobná

[43] SHARMA, Kapil Dev; SRIVASTAVA, Shobhit. Failure mode and effect analysis (FMEA) implementation: a literature review. *J Adv Res Aeronaut Space Sci*, 2018, 5.1-2: 1-17.
[44] ČESKO, Vyhláška č. 528/2005 Sb. ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků. In *Sbírka zákonů České republiky.* 2005, částka 179/2005

V tabulce č. 13 lze vyčíst bodové hodnocení závažnosti následků určité hrozby opět v bodovém hodnocení 1 až 5, přičemž vyšší hodnota číslice znamená vyšší míru závažnosti následků dané hrozby.

Tabulka č. 13 – bodové hodnocení závažnosti následků hrozby

Bodové hodnocení	Závažnost následků N
1	Velmi malá
2	Malá
3	Střední
4	Velká
5	Kritická

Tabulka č. 14 ve stejném bodovém rozmezí zobrazuje stupeň odhalitelnosti hrozby.

Tabulka č. 14 – Bodové hodnocení stupně odhalitelnosti hrozby

Bodové hodnocení	Odhalitelnost hrozby H
1	Velmi snadná
2	Snadná
3	Střední
4	Velmi nesnadná
5	Neodhalitelná

Tabulka č. 15 určuje na základě zobrazeného bodového spektra vypočteného podle výše uvedeného vzorce míru výhledného rizika vycházející z dílčích veličin.

Tabulka č. 15 – Bodové spektrum výsledné míry rizika

Bodové hodnocení	Výsledná míra rizika R
1 až 40	Malé
41 až 79	Střední
80 až 125	Velké

4.4 DEFINICE IDENTIFIKOVANÝCH HROZEB

V následující kapitole autor definuje identifikované hrozby pro jednotlivé zabezpečené a jednací oblasti zájmového objektu. Podle kapitoly č. 14. 1. přílohy č. 1 vyhlášky č. 528/2005 Sb. toto vyhodnocení rizik musí obsahovat specifikaci aktiv, stanovení jednotlivých hrozeb a zranitelností, jejich vyhodnocení a stanovení celkové míry rizika. Stanovení výsledné míry rizika bude provedeno pro každou množinu hrozeb uvedenou v kapitole č. 4.2 zvlášť, podle postupu uvedeného v kapitole č. 5.

4.4.1 LIDSKÝ FAKTOR VNITŘNÍ

U této množiny hrozeb je hlavním zdrojem hrozby člověk zaměstnaný v organizaci. Hrozbu s nízkým potenciálem představuje podmnožina nazvaná „nekvalitní práce zaměstnance“. Zaměstnanci již obdrželi bezpečnostní prověrku a prochází pravidelným každoročním školením ze zákona č. 412/2005 Sb. Toto školení je vždy zakončeno písemným testem. Nízký potenciál rovněž představují podmnožiny „nevyhovující pravidla manipulace s identifikačními prvky systému kontroly vstupu“, „Nevyhovující pravidla manipulace s kódy EZS“, „Nevyhovující pravidla manipulace s klíči“ a „Nedostatečná režimová opatření“. Tato pravidla a opatření jsou zajištěna formou bezpečnostních směrnic a podléhají několikastupňové kontrole před jejich vydáním, a to nejen v rámci organizačního celku. Proto autor považuje rovněž i hrozbu „Nevyhovující směrnice“ za hrozbu s nízkým potenciálem. Do kategorie hrozeb s nízkým potenciálem autor řadí i hrozby označenou jako „Msta“ a „Sabotáž". Autor nevylučuje možnost vzniku pohnutky pomstít se kolegovi formou např. odcizení jeho identifikačního prvku, avšak i přesto přiřazuje těmto hrozbám nízký potenciál. Mezi hrozby se středně velkým potenciálem však řadí „rutinu“ a „neúmyslnou chybu“. Rutinní činností ztrácí i kvalitní zaměstnanec pozornost. Příkladem může být rutinní činnost ukládání dokumentů. Např. při výstupu (tisku) z informačního systému zaměstnanec tento dokument správně zaznamená, avšak uloží do úschovného objektu určeného pro nižší stupeň utajení. Neúmyslnou chybou může být například také připojení záznamového zařízení (flashdisku) do zařízení s nižším stupněm utajení. Tyto události mají sice vysokou pravděpodobnost vzniku hrozby, ovšem zároveň velmi snadnou odhalitelnost. Špionáž prováděná interním

zaměstnancem je sice velmi nesnadno odhalitelná, avšak její pravděpodobnost vzniku je autorem považována za velmi málo pravděpodobnou s ohledem na pravidla personální bezpečnosti podle zákona č. 412/2005 Sb. Závažnost následků jednotlivých hrozeb je potom přímo úměrná stupni utajení zpracovávaných informací.

4.4.2 LIDSKÝ FAKTOR VNĚJŠÍ

Jako hrozbu s nejnižším potenciálem spadající do této množiny autor označuje „Neoprávněný vstup“. Vzhledem k provedeným opatřením fyzické bezpečnosti na perimetru a na vstupu do budovy popsaným v kapitole č. 3.3.1 by k neoprávněnému či náhodnému vstupu do zabezpečených nebo jednacích oblastí v zájmovém objektu nemělo dojít vůbec. Nízký potenciál autor přiřazuje i hrozbě „Záškodníci“ a „Sběrači kovů". Sice mohou způsobit majetkovou škodu například při pokusu poničit, v případě sběračů kovů odcizit např. část ochrany perimetru s úmyslem ji následně prodat do sběrných surovin, nicméně odhalitelnost u této hrozby je velmi snadná a závažnost následků velmi malá. Středním potenciálem disponují hrozby „Zloděj“ a „Nedostatečně poučení pracovníci externích firem“. U externích zaměstnanců by dle názoru autora byla hlavním motivem ke spáchání krádeže utajované informace pouhá zvědavost, co taková tajná informace obsahuje, čeho se může týkat. Potom například volně položený flashdisk může být pro externího pracovníka úklidové firmy jistým lákadlem, byť se jedná o pracovníka prověřeného a v zájmovém objektu vykonává úklidovou službu třeba již několik let. Pravděpodobnost vzniku těchto hrozeb autor označuje jako „pravděpodobnou" s velkými následky a velmi nesnadnou odhalitelností. Jako hrozby s velmi vysokým potenciálem potom autor označuje „Útok zpravodajských služeb cizí moci“ a „Terorismus“. Autor tak usuzuje na základě jedné z vyšetřovacích verzí událostí ve skladu ve Vrběticích v roce 2014, podle které stojí za útokem na tamní muniční sklad agenti ruské zpravodajské služby. Do této kategorie autor řadí i „Vojenský útok“ cizí mocnosti vzhledem k aktuální situaci na Ukrajině. Závažnost následků jednotlivých hrozeb je potom přímo úměrná stupni utajení zpracovávaných a projednávaných informací v jednotlivých utajovaných a jednacích oblastech.

4.4.3 PROSTŘEDKY FYZICKÉ BEZPEČNOSTI

Potenciál jednotlivých prvků této množiny hrozeb závisí především na poruchovosti jednotlivých komponentů fyzické ochrany. Zajištění proti této poruchovosti je podmíněno kvalitním zpracováním režimových opatření v podobě např. směrnic výkonu ostrahy objektu. Za klíčový prvek této množiny hrozeb autor považuje „Selhání zařízení pro zajištění ochrany před selháním dodávky el. energie“. Selhání dodávky el. energie z veřejné sítě bývá poměrně častým jevem. Náhradní zdroje energie by tedy měli být řešeny, stejně jako v případě našeho zájmového objektu, minimálně dvěma redundantními systémy náhradního napájení. Každý tento systém by měl být schopen dodat v případě výpadku veřejné sítě potřebné množství el. energie po dobu min. 24 hodin. V našem zájmovém objektu je tato problematika řešena dvěma bateriovými UPS. Riziko vycházející z hrozeb označených jako „Selhání EZS“ a „Selhání EPS“ autor označuje za velmi nesnadno odhalitelné. Na těchto zařízeních by tedy měly být prováděny pravidelné kontroly funkčnosti prostřednictvím např. dodavatelské firmy. Hrozby „Selhání systému kontroly vstupu do zabezpečených (jednacích) oblastí“ a „Selhání CCTV“ je naopak velmi snadno odhalitelné a dá se řešit v rámci režimových opatření v podobě např. dočasného posílení ostrahy objektu. Hrozbu „Selhání mechanických zábranných prostředků autor označuje za velmi málo pravděpodobnou, avšak velmi nesnadně odhalitelnou. Uvolněné mříže v okně si například někdo všimne, až při odpadnutí mříže na zem. Měly by zde tedy probíhat alespoň namátkové kontroly pevnosti a uchycení mechanických zábranných prostředku např. v rámci obchůzek ostrahy objektu.

4.4.4 NATUROGENNÍ MIMOŘÁDNÁ UDÁLOST BIOTICKÁ

K definici této množiny hrozeb použije část definice mimořádné události podle § 2 zákona č. 239/2000 Sb. Jedná se tedy o cit.: „*škodlivé působení sil a jevů vyvolaných přírodními vlivy“,*[45] v tomto případě biotickými. Ishikawův diagram dělí tuto množinu na dvě hlavní podmnožiny, a sice „zvěř“ a „ptactvo“. Ptactvo představuje dle autora minimální hrozební potenciál. V působení zvěře vidí autor

[45] ČESKO, Zákon č. 239 ze dne 9. srpna 2005 o integrovaném záchranném systému a o změně některých zákonů. In: *Sbírka zákonů České republiky*. 2005, částka 73/2000.

rovněž nízký potenciál hrozby. Může zde však nastat situace v podobě narážení zvěře do plotu s detekcí pohybu. Drobná ani vysoká zvěř při snížené viditelnosti, případně v noci, objekt plotu nevidí a slepě naráží neustále do jednoho místa. Způsobuje tím falešné poplachy, neboť otřesová čidla umístěná na těle plotu tyto nárazy zaznamenávají. Může potom dojít k situaci, kdy ostraha objektu dočasně tato čidla vypne. Dojde zde tedy k dočasnému snížení kvality ochrany perimetru a zároveň zde vniká hrozba, že dojde k opomenutí ostrahy tato čidla opět aktivovat. Potenciál této hrozby autor doporučuje snížit v podobě úpravy směrnic pro výkon ostrahy objektu. Střední potenciál hrozby však představuje působení hlodavců, zejména v kabelových šachtách. Pokud dojde například k přehryzání kabelu, který zajišťuje přenos signálu z ochrany perimetru ke stanovišti ostrahy, systém sice tento incident zaznamená, ovšem ve valné většině případů není ve vlastních silách ostrahy tuto závadu odstranit na místě. Je tedy nutné tuto závadu předat externí firmě, a i v tomto případě není lokalizace této závady snadná a je tedy časově náročná. Dojde zde tedy rovněž ke snížení kvality ochrany perimetru třeba i na několik dní.

4.4.5 NATUROGENNÍ MIMOŘÁDNÁ UDÁLOST ABIOTICKÁ

I abiotické přírodní faktory představují určitý potenciál hrozby. Úder blesku je schopen způsobit nejen výpadek dodávky elektrické energie, ale i případný požár. Výpadek elektrické energie spolu s možností vzniku přepětí autor považuje, vzhledem k opatřením uvedeným v kapitole č. 3.3.1 za hrozby s nízkým potenciálem. V případě vzniklého požáru, ať již způsobeného úderem blesku, či např. nedbalostí, je nezbytně nutné zajistit ochranu utajovaných informací, např. v listinné podobě, nebo uložené na datovém mediu, pomocí režimových opatření, či vnitřních směrnic, stejně tak i v případě hrozící povodně nebo záplavy. Působení silného větru nebo krupobití je schopno zapříčinit „falešné“ poplachy zejména aktivací otřesových čidel na ochraně perimetru zájmového objektu, v případě krup poté aktivaci mikrofonních čidel na oknech objektu. Zde je nutné tedy opět potenciál této hrozby snížit na minimum pomocí režimových opatření. Pro potřeby této práce považujme tedy působení větru a krupobití za hrozbu s nízkým potenciálem.

4.4.6 FYZICKÁ BEZPEČNOST INFORMAČNÍHO SYSTÉMU

V této množině hrozeb autor využil dělení fyzické bezpečnosti IS podle J. Koloucha, uvedené v kapitole č. 2.13. Podmnožině označené jako „ochrana proti krádeži IS“ autor uvažuje nízký potenciál, vzhledem k výše uvedeným opatřením fyzické bezpečnosti zájmového objektu. Přiklání se však k využití Kensington security slotu u ostatních počítačových systémů, byť není žádným právním předpisem explicitně vyžadován. Ochrana před rozebráním a úpravou počítačových systémů je dle názoru autora dostačující, vzhledem k ostatním vrstvám ochrany zájmového objektu. I přes nastaveném režimu výkonu ostrahy objektu v podobě návštěv bez doprovodu považuje autor potenciál této hrozby za zcela minimální. Střední až vysoký potenciál hrozby doporučuje autor snížit v podmnožině nazvané „ochrana před připojením cizích periférií“ pomocí následujících opatření. I v případě absentující nutnosti připojovat jakékoli USB/PS2 zařízení, například z důvodu přenosu, nebo zpracovávání dat, autor doporučuje užití hardwarové ochrany USB Lock Cable Guard doplněné softwarovou ochranou Lumendion, která softwarově zabrání rozpoznání a následnému připojení neznámého hardwarovému zařízení. Toto opatření autor doporučuje zejména z důvodu možnosti neúmyslné záměny USB zařízení a připojení k „nesprávnému“ počítačovém systému.

5 STANOVENÍ MÍRY RIZIKA A BODOVÉ OHODNOCENÍ PRO JEDNOTLIVÉ ZABEZPEČENÉ A JEDNACÍ OBLASTI

V této kapitole autor provede stanovení míry rizika množin hrozeb identifikovaných v kapitole č. 4, specifikuje aktiva, a na základě zpracované tabulky bodového ohodnocení opatření fyzické bezpečnosti podle vyhlášky č. 528/2005 Sb. a znění vyhlášky č. 523/2005 Sb. stanoví, zda autorem navrhované opatření fyzické bezpečnosti vyhovuje podmínkám výše uvedených právních předpisů.

5.1 STANOVENÍ MÍRY RIZIKA A BODOVÉ OHODNOCENÍ PRO ZABEZPEČENOU OBLAST Č. 1

Tabulka č. 16 stanovuje míry rizika množin hrozeb identifikovaných v kapitole č. 4.4 metodou FMEA.

Tabulka č. 16 – Míra rizika identifikovaných množin hrozeb pro zabezpečenou oblast č. 1

Identifikované množiny hrozeb	P	N	H	Míra rizika
Lidský faktor vnitřní	2	4	4	malá
Lidský faktor vnější	3	4	4	střední
Prostředky fyzické bezpečnosti	4	4	5	velká
Naturogenní mimořádná událost biotická	4	4	1	malá
Naturogenní mimořádná událost abiotická	3	4	1	malá
Fyzická bezpečnost IS	4	4	3	střední

Na základě vypočtených hodnot uvedených v tabulce č. 16 autor stanovil celkovou míru rizika množin identifikovaných hrozeb na úroveň střední.

5.1.1 SPECIFIKACE AKTIV PRO ZABEZPEČENOU OBLAST Č. 1

Aktivem pro oblast č. 1 jsou utajované informace zpracovávané určeným informačním systémem. Identifikace k informačnímu systému bude prováděna uživatelským jménem a autentizace uživatele heslem. Informace budou informačním systémem zpracovávány. Zpracovávaná data nebudou šifrována. Zpracovávané informace budou označeny do stupně utajení přísně tajné. Bude se jednat o informace poskytnuté spolupracujícími subjekty v rámci resortu

ministerstva obrany. Počet zpracovávaných informací za jeden kalendářní rok ve stupni utajení přísně tajné je 80, do stupně utajení tajné 120.

5.1.2 TABULKA BODOVÉHO OHODNOCENÍ OPATŘENÍ FYZICKÉ BEZPEČNOSTI V ZABEZPEČENÉ OBLASTI Č. 1

V tabulce č. 17, která je tvořena předlohou pro výpočet bodových hodnot podle přílohy č. 1 vyhlášky č. 528/2005 Sb. autor uvádí bodové hodnoty přiřazené dle jednotlivých typů a použitých opatření podle výše uvedené vyhlášky[46]. Na základě tabulky výpočtů bodového ohodnocení opatření fyzické bezpečnosti v zabezpečené oblasti č. 1 podle kapitoly č. 14 přílohy č. 1 vyhlášky č. 528/2005 Sb.[47] autor provede výpočet dílčích a celkových výsledků jednotlivých *S* hodnot, ze kterých stanoví vhodnost použitých prostředků fyzické ochrany pro oblast č. 1 s hodnoceným stupněm rizika. Hodnoty SS1 a SS2 jsou ekvivalentem k informačnímu systému podle vyhlášky č. 523/2005 Sb.

[46] ČESKO, Vyhláška č. 528/2005 Sb. ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků. In *Sbírka zákonů České republiky.* 2005, částka 179/2005.
[47] ČESKO, Vyhláška č. 528/2005 Sb. ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků. In *Sbírka zákonů České republiky.* 2005, částka 179/2005.

Tabulka č. 17 – Bodové ohodnocení zabezpečené oblasti č. 1 podle vyhlášky č. 528/2005 Sb.

Zabezpečená oblast č. 1	Typ	Bodové hodnocení [b]
Úschovný objekt (informační systém IS)	Typ 1	SS1 = 1
Zámek úschovného objektu (autentizace k IS)	Typ 1	SS2 = 1
Zabezpečená oblast	Typ 4	SS3 = 4
Uzamykací systém zabezpečené oblasti	Typ 3	SS4 = 3
Hranice objektu	Typ 3	S3 = 3
Systém kontroly vstupu	Typ 3	SS6 = 3
Prohlídky u vstupu		SS12= 1
Návštěvy bez doprovodu		SS7 = 1
Ostraha	Typ 4	SS8 = 4
Zařízení EZS	Typ 4	SS91 = 4
Instalace zařízení EZS	Typ 4	SS92 = 4
		SS9 = 4*
Fyzická bariéra	Typ4	SS10 = 4
Kontrola vstupu ve všech příst. bodech perimetru		SS11 = 1
Perimetrický detekční systém necertifikovaný		SS13 = 1
Bezpečnostní osvětlení perimetru		SS14 = 2
Speciální televizní systém na perimetru		SS15 = 2
S1 = SS1 x SS2 =		S1 = 1
S2 = SS3 x SS4 =		S2 = 12
S3 =		S3 = 3
S4 = SS6 +SS7 =		S4 = 4
S5 = SS8 + SS9 =		S5 = 8
S6 = (SS10 x SS11) + SS12 + SS13+SS14+SS15		S6 = 10

*pro výpočet hodnoty SS9 je dán vzorec:

SS9 = (SS91 + SS92) /2 x SS92/OBL

Hodnota SS9 se matematicky zaokrouhluje na celé číslo. Maximální hodnota SS9 může být 4body.

OBL je bodová hodnota určená kategorií zabezpečené oblasti, hodnoty OBL pro jednotlivé stupně utajení udává tabulka č. 18.[48]

Tabulka č. 18 – OBL – bodová hodnota určená kategorií zabezpečené oblasti

Kategorie zabezpečené oblasti	Hodnota OBL
Přísně tajné	4 body
Tajné	3 body
Důvěrné	2 body
Vyhrazené	1 bod

Tabulka č. 19 představuje bodové hodnoty nejnižší míry zabezpečení zabezpečené oblasti podle přílohy č. 1 vyhlášky č. 528/2005 Sb. pro zabezpečenou oblast stupně utajení přísně tajné.

Tabulka č. 19 – Tabulka bodových hodnot nejnižší míry zabezpečení zabezpečené oblasti podle přílohy č. 1 vyhlášky č. 528/2005 Sb.

Zabezpečená oblast kategorie přísně tajné	Míra rizika[b]		
	malá	střední	Velká
Povinné: (S1) + (S2) + (S3)	10	11	13
Povinné: (S4) + (S5)	6	7	7
Nepovinné: (S6)	4	5	5
Celkový výsledek	20	23 (38)	25

S1 + S2 + S3 = 16 bodů, S4 + S5 = 12 bodů, S6 = 10 bodů

Celkový výsledek je 38 bodů.

Při porovnání hodnot uvedených v tabulce č. 19 s celkovým výsledkem můžeme konstatovat, že navrhované prostředky pro zabezpečenou oblast č. 1 vyhovují požadavkům podle vyhlášky č. 528/2005 Sb. pro nakládání s utajovanými informacemi do stupně utajení přísně tajné se střední mírou rizika.

[48] ČESKO, Vyhláška č. 528/2005 Sb. ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků. In *Sbírka zákonů České republiky*. 2005, částka 179/2005.

5.2 STANOVENÍ MÍRY RIZIKA A BODOVÉ OHODNOCENÍ PRO JEDNACÍ OBLAST Č. 2

Tabulka č. 20 stanovuje míry rizika množin hrozeb identifikovaných v kapitole č. 4.4 metodou FMEA.

Tabulka č. 20 – Míra rizika identifikovaných množin hrozeb pro jednací oblast č. 2

Identifikované množiny hrozeb	P	N	H	Míra rizika
Lidský faktor vnitřní	2	4	4	malá
Lidský faktor vnější	2	4	4	malá
Prostředky fyzické bezpečnosti	3	4	5	střední
Naturogenní mimořádná událost biotická	4	4	1	malá
Naturogenní mimořádná událost abiotická	3	4	1	malá
Fyzická bezpečnost IS	4	4	3	střední

Na základě vypočtených hodnot uvedených v tabulce č. 20 autor stanovil celkovou míru rizika množin identifikovaných hrozeb na úroveň malá.

5.2.1 SPECIFIKACE AKTIV PRO JEDNACÍ OBLAST Č. 2

Aktivem pro jednací oblast č. 2 jsou utajované informace v listinné podobě a informace zpracovávané určeným informačním systémem. Informace budou informačním systémem zpracovávány, ukládány a zobrazovány. Identifikace k informačnímu systému bude prováděna uživatelským jménem a autentizace uživatele heslem. Zpracovávaná data nebudou šifrována. Manipulace s utajovanými informacemi probíhá nepravidelně. Zpracovávané informace budou označeny maximálním stupněm utajení tajné. Bude se jednat o informace poskytnuté spolupracujícími subjekty v rámci resortu ministerstva obrany. Počet zpracovávaných informací za jeden kalendářní rok ve stupni utajení tajné je 120.

5.2.2 TABULKA BODOVÉHO OHODNOCENÍ OPATŘENÍ FYZICKÉ BEZPEČNOSTI V JEDNACÍ OBLASTI Č. 2

V této podkapitole autor provede na základě tabulky výpočtů bodového ohodnocení opatření fyzické bezpečnosti v jednací oblasti č. 2 podle kapitoly č. 14 přílohy č. 1 vyhlášky č. 528/2005 Sb.[49] výpočet dílčích a celkových výsledků jednotlivých *S* hodnot, podle kterých stanoví vhodnost použitých prostředků fyzické ochrany pro oblast č. 2 s hodnoceným stupněm rizika. Hodnoty SS1 a SS2 jsou ekvivalentem k informačnímu systému podle vyhlášky č. 523/2005 Sb. Tabulka č. 21 uvádí bodové hodnoty přiřazené podle jednotlivých typů a použitých opatření podle výše uvedené vyhlášky.[50]

[49] ČESKO, Vyhláška č. 528/2005 Sb. ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků. In *Sbírka zákonů České republiky.* 2005, částka 179/2005.
[50] ČESKO, Vyhláška č. 528/2005 Sb. ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků. In *Sbírka zákonů České republiky.* 2005, částka 179/2005.

Tabulka č. 21 – Bodové ohodnocení jednací oblasti č. 2 podle vyhlášky č. 528/2005 Sb.

Jednací oblast č. 2	Typ	Bodové hodnocení [b]
Úschovný objekt (informační systém IS)	Typ 1	SS1 = 1
Zámek úschovného objektu (autentizace k IS)	Typ 1	SS2 = 1
Zabezpečená oblast	Typ 4	SS3 = 4
Uzamykací systém zabezpečené oblasti	Typ 3	SS4 = 3
Hranice objektu	Typ 3	S3 = 3
Systém kontroly vstupu	Typ 3	SS6 = 3
Prohlídky u vstupu		SS12= 1
Návštěvy bez doprovodu		SS7 = 1
Ostraha	Typ 4	SS8 = 4
Zařízení EZS	Typ 4	SS91 = 4
Instalace zařízení EZS	Typ 4	SS92 = 4
		SS9 = 4*
Fyzická bariéra	Typ4	SS10 = 4
Kontrola vstupu ve všech příst. bodech perimetru		SS11 = 1
Perimetrický detekční systém necertifikovaný		SS13 = 1
Bezpečnostní osvětlení perimetru		SS14 = 2
Speciální televizní systém na perimetru		SS15 = 2
S1 = SS1 x SS2 =		S1 = 1
S2 = SS3 x SS4 =		S2 = 12
S3 =		S3 = 3
S4 = SS6 +SS7 =		S4 = 4
S5 = SS8 + SS9 =		S5 = 8
S6 = (SS10 x SS11) + SS12 + SS13+SS14+SS15		S6 = 10

*pro výpočet hodnoty SS9 je dán vzorec:

SS9 = (SS91 + SS92) /2 x SS92/OBL

Hodnota SS9 se matematicky zaokrouhluje na celé číslo. Maximální hodnota SS9 může být 4body.

Bodové hodnoty jednotlivých kategorií jednacích oblastí podle stupně utajení podle vyhl. č. 528/2005 Sb. autor uvádí v tabulce č. 22. OBL je bodová hodnota určená kategorií zabezpečené oblasti.

Tabulka č. 22 – OBL – bodová hodnota určená kategorií zabezpečené oblasti

Kategorie jednací oblasti	Hodnota OBL
Přísně tajné	4 body
Tajné	3 body
Důvěrné	2 body
Vyhrazené	1 bod

Tabulka č. 23 představuje bodové hodnoty nejnižší míry zabezpečení jednací oblasti podle přílohy č. 1 vyhlášky č. 528/2005 Sb. pro jednací oblast stupně utajení tajné.

Tabulka č. 23 – Tabulka bodových hodnot nejnižší míry zabezpečení jednací oblasti podle přílohy č. 1 vyhlášky č. 528/2005 Sb.

Jednací oblast kategorie tajné	Míra rizika[b]		
	malá	střední	velká
Povinné (S1) + (S2) + (S3)	5	5	6
Povinné: (S4) + (S5)	4	5	5
Nepovinné: (S6)	4	5	5
Celkový výsledek	13 (38)	15	16

S1 + S2 + S3 = 16 bodů, S4 + S5 = 12 bodů, S6 = 10 bodů

Celkový výsledek je 38 bodů.

Při porovnání hodnot uvedených v tabulce č. 23 s celkovým výsledkem můžeme konstatovat, že navrhované prostředky pro jednací oblast č. 2 vyhovují požadavkům podle vyhlášky č. 528/2005 Sb. pro nakládání s utajovanými informacemi do stupně utajení tajné s malou mírou rizika.

5.3 STANOVENÍ MÍRY RIZIKA A BODOVÉ OHODNOCENÍ PRO ZABEZPEČENOU OBLAST Č. 3

Tabulka č. 24 stanovuje míry rizika množin hrozeb identifikovaných v kapitole č. 4.4 metodou FMEA.

Tabulka č. 24 – Míra rizika identifikovaných množin hrozeb pro zabezpečenou oblast č. 3

Identifikované množiny hrozeb	P	N	H	Míra rizika
Lidský faktor vnitřní	2	3	4	malá
Lidský faktor vnější	2	3	4	malá
Prostředky fyzické bezpečnosti	4	3	5	střední
Naturogenní mimořádná událost biotická	4	3	1	malá
Naturogenní mimořádná událost abiotická	3	3	1	malá
Fyzická bezpečnost IS	4	3	3	střední

Na základě vypočtených hodnot uvedených v tabulce č. 24 autor stanovil celkovou míru rizika množin identifikovaných hrozeb na úroveň označenou jako malá.

5.3.1 SPECIFIKACE AKTIV PRO ZABEZPEČENOU OBLAST Č. 3

Aktivem pro zabezpečenou oblast č. 3 jsou utajované informace v listinné podobě. Manipulace s utajovanými informacemi bude probíhat nepravidelně. Zpracovávané informace budou označeny maximálním stupněm utajení důvěrné. Bude se jednat o informace poskytnuté spolupracujícími subjekty v rámci resortu ministerstva obrany. Počet zpracovávaných informací za jeden kalendářní rok ve stupni utajení tajné je 100.

5.3.2 TABULKA BODOVÉHO OHODNOCENÍ OPATŘENÍ FYZICKÉ BEZPEČNOSTI V ZABEZPEČENÉ OBLASTI Č. 3

V této kapitole autor provede na základě tabulky výpočtů bodového ohodnocení opatření fyzické bezpečnosti (tabulka č. 25) v zabezpečené oblasti č. 3 podle kapitoly č. 14 přílohy č. 1 vyhlášky č. 528/2005 Sb.[51] výpočet dílčích a celkových výsledků jednotlivých *S* hodnot na základě kterých stanoví vhodnost použitých prostředků ochrany pro oblast č. 3 s hodnoceným stupněm rizika.

[51] ČESKO, Vyhláška č. 528/2005 Sb. ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků. In *Sbírka zákonů České republiky.* 2005, částka 179/2005.

Tabulka č. 25 – Bodové ohodnocení zabezpečené oblasti č. 3 podle vyhlášky č. 528/2005 Sb.

Zabezpečená oblast č. 3	Typ	Bodové hodnocení [b]
Úschovný objekt	Typ 2	SS1 = 2
Zámek úschovného objektu	Typ 2	SS2 = 2
Zabezpečená oblast	Typ 2	SS3 = 2
Uzamykací systém zabezpečené oblasti	Typ 3	SS4 = 3
Hranice objektu	Typ 3	S3 = 3
Systém kontroly vstupu	Typ 3	SS6 = 3
Prohlídky u vstupu		SS12= 1
Návštěvy bez doprovodu		SS7 = 1
Ostraha	Typ 4	SS8 = 4
Zařízení EZS	Typ 4	SS91 = 4
Instalace zařízení EZS	Typ 4	SS92 = 4
		SS9 = 8*
Fyzická bariéra	Typ4	SS10 = 4
Kontrola vstupu ve všech příst. bodech perimetru		SS11 = 1
Perimetrický detekční systém necertifikovaný		SS13 = 1
Bezpečnostní osvětlení perimetru		SS14 = 2
Speciální televizní systém na perimetru		SS15 = 2
S1 = SS1 x SS2 =		S1 = 4
S2 = SS3 x SS4 =		S2 = 6
S3 =		S3 = 3
S4 = SS6 +SS7 =		S4 = 4
S5 = SS8 + SS9 =		S5 = 12
S6 = (SS10 x SS11) + SS12 + SS13+SS14+SS15		S6 = 10

*Pro výpočet hodnoty SS9 je dán vzorec:

SS9 = (SS91 + SS92) /2 x SS92/OBL

Hodnota SS9 se matematicky zaokrouhluje na celé číslo. Maximální hodnota SS9 může být 4body.

OBL je bodová hodnota určená kategorií zabezpečené oblasti uvedená v tabulce č. 26.

Tabulka č. 26 – OBL – bodová hodnota určená kategorií zabezpečené oblasti

Kategorie zabezpečené oblasti	Hodnota OBL
Přísně tajné	4 body
Tajné	3 body
Důvěrné	2 body
Vyhrazené	1 bod

Tabulka č. 27 představuje bodové hodnoty nejnižší míry zabezpečení zabezpečené oblasti podle přílohy č. 1 vyhlášky č. 528/2005 Sb. pro zabezpečenou oblast stupně utajení důvěrné.

Tabulka č. 27 – Tabulka bodových hodnot nejnižší míry zabezpečení zabezpečené oblasti podle přílohy č. 1 vyhlášky č. 528/2005 Sb.

Zabezpečená oblast kategorie důvěrné	Míra rizika [b]		
	malá	střední	velká
Povinné: (S1) + (S2) + (S3)	5	5	6
Povinné: (S4) + (S5)	4	5	5
Nepovinné: (S6)	4	5	5
Celkový výsledek	13 (39)	15	16

S1 + S2 + S3 = 13 bodů, S4 + S5 = 16 bodů, S6 = 10 bodů

Celkový výsledek je 39 bodů.

Při porovnání hodnot uvedených v tabulce č. 27 s celkovým výsledkem můžeme konstatovat, že navrhované prostředky pro zabezpečenou oblast č. 3 vyhovují požadavkům podle vyhlášky č. 528/2005 Sb. pro nakládání s utajovanými informacemi do stupně utajení důvěrné s malou mírou rizika.

5.4 STANOVENÍ MÍRY RIZIKA A BODOVÉ OHODNOCENÍ PRO ZABEZPEČENOU OBLAST Č. 4

Stanovení míry rizika definovaných hrozeb pro posouzení vhodnosti prostředků fyzické ochrany vyhláška č. 528/2005 Sb. pro oblast dané kategorie nevyžaduje. Stejně tak není nutné uvádět specifikaci aktiv a zpracovávat tabulku bodového ohodnocení zabezpečené oblasti kategorie vyhrazené, pokud se nejedná o oblast cit: *„sloužící k ukládání utajované informace v komponentách informačního systému nebo krypto grafickému prostředku nebo která vyžaduje zvláštní režim nakládání.“*[52] Pro porovnání však autor stanovil míry rizika množin hrozeb identifikovaných v kapitole č. 4.4 metodou FMEA v tabulce č. 28 i pro oblast č.4.

Tabulka č. 28 – Míra rizika identifikovaných množin hrozeb pro zabezpečenou oblast č. 4

Identifikované množiny hrozeb	P	N	H	Míra rizika
Lidský faktor vnitřní	2	1	4	malá
Lidský faktor vnější	2	1	4	malá
Prostředky fyzické bezpečnosti	4	1	5	malá
Naturogenní mimořádná událost biotická	4	1	1	malá
Naturogenní mimořádná událost abiotická	3	1	1	malá
Fyzická bezpečnost IS	4	1	3	malá

Na základě vypočtených hodnot uvedených v tabulce č. 28 autor stanovil míru rizika množin identifikovaných hrozeb na úroveň označenou jako malá.

[52] ČESKO, Vyhláška č. 528/2005 Sb. ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků. In *Sbírka zákonů České republiky.* 2005, částka 179/2005.

5.4.1 SPECIFIKACE AKTIV PRO ZABEZPEČENOUÍ OBLAST Č. 4

Aktivem pro zabezpečenou oblast č. 4 jsou utajované informace v listinné podobě. Manipulace s utajovanými informacemi bude probíhat nepravidelně. Zpracovávané informace budou označeny maximálním stupněm utajení vyhrazené. Bude se jednat o informace poskytnuté spolupracujícími subjekty v rámci resortu ministerstva obrany. Počet zpracovávaných informací za jeden kalendářní rok ve stupni utajení vyhrazené bude 100.

5.4.2 TABULKA BODOVÉHO OHODNOCENÍ OPATŘENÍ FYZICKÉ BEZPEČNOSTI V ZABEZPEČENÉ OBLASTI Č. 4

V této kapitole autor provede na základě tabulky výpočtů bodového ohodnocení opatření fyzické bezpečnosti v zabezpečené oblasti č. 4 podle kapitoly č. 14 přílohy č. 1 vyhlášky č. 528/2005 Sb.[53] výpočet dílčích a celkových výsledků jednotlivých *S* hodnot, ze kterých stanoví vhodnost použitých prostředků ochrany pro oblast č. 4. Bodové ohodnocení zabezpečené oblasti č. 4 podle vyhlášky č. 528/2005 Sb. uvádí tabulka č. 29.

[53] ČESKO, Vyhláška č. 528/2005 Sb. ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků. In *Sbírka zákonů České republiky.* 2005, částka 179/2005.

Tabulka č. 29 – Bodové ohodnocení zabezpečené oblasti č. 4 podle vyhlášky č. 528/2005 Sb.

Zabezpečená oblast č. 4	Typ	Bodové hodnocení [b]
Úschovný objekt	Typ 2	SS1 = 2
Zámek úschovného objektu	Typ 2	SS2 = 2
Zabezpečená oblast	Typ 2	SS3 = 2
Uzamykací systém zabezpečené oblasti	Typ 3	SS4 = 3
Hranice objektu	Typ 3	S3 = 3
Systém kontroly vstupu	Typ 3	SS6 = 3
Prohlídky u vstupu		SS12= 1
Návštěvy bez doprovodu		SS7 = 1
Ostraha	Typ 4	SS8 = 4
Zařízení EZS	Typ 4	SS91 = 4
Instalace zařízení EZS	Typ 4	SS92 = 4
		SS9 = 16*
Fyzická bariéra	Typ4	SS10 = 4
Kontrola vstupu ve všech příst. bodech perimetru		SS11 = 1
Perimetrický detekční systém necertifikovaný		SS13 = 1
Bezpečnostní osvětlení perimetru		SS14 = 2
Speciální televizní systém na perimetru		SS15 = 2
S1 = SS1 x SS2 =		S1 = 4
S2 = SS3 x SS4 =		S2 = 6
S3 =		S3 = 3
S4 = SS6 +SS7 =		S4 = 4
S5 = SS8 + SS9 =		S5 = 16
S6 = (SS10 x SS11) + SS12 + SS13+SS14+SS15		S6 = 10

*Pro výpočet hodnoty SS9 je dán vzorec:

SS9 = (SS91 + SS92) /2 x SS92/OBL

Hodnota SS9 se matematicky zaokrouhluje na celé číslo. Maximální hodnota SS9 může být 4body. OBL je bodová hodnota určená kategorií zabezpečené oblasti, uvedená v tabulce č. 30.

Tabulka č. 30 OBL – bodová hodnota určená kategorií zabezpečené oblasti

Kategorie zabezpečené oblasti	Hodnota OBL
Přísně tajné	4 body
Tajné	3 body
Důvěrné	2 body
Vyhrazené	1 bod

Tabulka č. 31 představuje bodové hodnoty nejnižší míry zabezpečení zabezpečené oblasti podle přílohy č. 1 vyhlášky č. 528/2005 Sb. pro zabezpečenou oblast stupně utajení vyhrazené.

Tabulka č. 31 Tabulka bodových hodnot nejnižší míry zabezpečení zabezpečené oblasti podle přílohy č. 1 vyhlášky č. 528/2005 Sb.

Zabezpečená oblast kategorie **vyhrazené** sloužící k ukládání utajované informace v komponentách informačního systému nebo krypto grafickému prostředku nebo která vyžaduje zvláštní režim nakládání	
Povinné: (S1) + (S2) + (S3)	2 body
Nepovinné: (S4) + (S5) + (S6)	1 bod
Celkový výsledek	3 body

S1 + S2 + S3 = 13 bodů, S4 + S5 + S6 = 30 bodů

Celkový výsledek je 43 bodů.

Při porovnání hodnot uvedených v tabulce č. 31 s celkovým výsledkem lze konstatovat, že navrhované prostředky pro zabezpečenou oblast č. 4 vyhovují požadavkům podle vyhlášky č. 528/2005 Sb. pro nakládání s utajovanými informacemi do stupně utajení vyhrazené.

ZÁVĚR

Vytyčeným cílem této diplomové práce bylo představit možnosti využití technických prostředků k ochraně UI v souladu s uvedenými právními předpisy. V teoretické části v kapitole č. 2 autor pomocí tabulek uvedl souvislosti v rozdílném značení jednotlivých druhů technických prostředků. Například poněkud nešťastně značený úschovný objekt třídy 0 (nula) podle ČSN EN 1143-1+A1 odpovídá úschovnému objektu typu 2 podle vyhlášky č. 528/2005 Sb., (viz. kapitola č. 2.2). Vyhláška č. 528/2005 Sb. odkazuje podle vlastního značení u jednotlivých druhů technických prostředků na odpovídající značení podle ČSN pouze v textu a stává se tak v mnoha případech poněkud nepřehlednou. V praktické části v kapitole č. 3. autor formou případové studie pro názornost představil smyšlený objekt dislokovaný do vojenského zařízení a představil požadavky na úpravy tohoto objektu nutné ke zpracovávání a uchovávání utajovaných informací v různých stupních utajení podle platných právních předpisů. V této kapitole je následně také představena jedna z možných variant realizace těchto úprav. V kapitole č. 4. autor provedl posouzení definovaných množin hrozeb a určil míru rizika úniku nebo zneužití utajované informace. Vyhodnocení rizik je podle zákona č. 412/2005 Sb. nezbytné pro sestavení projektu fyzické bezpečnosti. Tato práce není přímo projektem fyzické bezpečnosti, není ani podkladem pro jeho vytvoření, jejím primárním cílem při její tvorbě bylo ukázat možnosti kombinace využití jednotlivých druhů technické ochrany a režimových opatření tak, aby tyto kombinace vyhovovaly souvisejícím právním předpisům. Varianty možných kombinací autor uvádí v kapitole č. 5 pomocí tabulky bodového ohodnocení a dílčích výpočtů podle vyhlášky č. 528/2005 Sb. Provedená bezpečnostní opatření odpovídající právním předpisům však nikdy nezaručí snížení možného rizika úniku nebo zneužití UI na nulovou hodnotu. Pouze kontinuální proaktivní přístup v oblasti bezpečnostních opatření a kvalitní hodnocení rizik na základě dobré znalosti daného prostředí muže snížit riziko úniku nebo zneužití UI na přijatelné minimum.

SEZNAM POUŽITÝCH ZDROJŮ

[1.] DVOŘÁK, Jan. *Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti: komentář*. Praha: Wolters Kluwer, 2018. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7598-016-8.

[2.] IVANKA, Ján, 2014. *Mechanické zábranné systémy*. Zlín [cit. 2023-1-3]. ISBN 978-8-7454-427-9.

[3.] KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ. NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.

[4.] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík – VeRBuM, 2015. ISBN 978-80-87500-05-7.

[5.] ŠČUREK, Radomír a Daniel MARŠÁLEK. *Technologie fyzické ochrany civilního letiště*. Brno: Akademické nakladatelství CERM, 2014. ISBN 978-80-7204-862-5.

[6.] UHLÁŘ, Jan. *Technická ochrana objektů I. díl*. 2. vyd. Praha: Policejní akademie České republiky v Praze, 2009. ISBN 978-80-7251-312-3.

[7.] UHLÁŘ, Jan. *Technická ochrana objektů II. díl*. 2. vyd. Praha: Policejní akademie České republiky v Praze, 2009. ISBN 978-80-7251-313-0.

[8.] UHLÁŘ, Jan. *Technická ochrana objektů III. díl*., Praha: Vydavatelství PA ČR, 2006. ISBN 80-7251-235-8.

[9.] SHARMA, Kapil Dev; SRIVASTAVA, Shobhit. Failure mode and effect analysis (FMEA) implementation: a literature review. *J Adv Res Aeronaut Space Sci*, 2018, 5.1-2: 1-17.

[10.] *Ishikawa Diagram: Anticipate and solve problems within your business (Management & Marketing)* [online]. 50Minutes.com, 2015 [cit. 2023-02-10]. ISBN 978-2806270658.

[11.] ČESKO, Zákon č. 239 ze dne 9. srpna 2005 o integrovaném záchranném systému a o změně některých zákonů. In: *Sbírka zákonů České republiky*. 2005, částka 73/2000.

[12.] ČESKO, Zákon č. 412 ze dne 21. září 2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: *Sbírka zákonů České republiky*. 2005, částka143/2005.

[13.] ČESKO, Vyhláška č. 528/2005 Sb. ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků. In *Sbírka zákonů České republiky.* 2005, částka 179/2005.
[14.] ČESKO, Vyhláška č. 523/2005 Sb. ze dne 25. prosince 2005, o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor. In *Sbírka zákonů České republiky.* 2005, částka 179/2005.
[15.] ČESKO. Rozkaz Ministra obrany: Ochrana utajovaných informací v rezortu Ministerstva obrany. In: Praha, 2013, ročník 2013, číslo 14.
[16.] ČESKO, ČSN EN 1627, Praha: Český normalizační institut, březen 2022
[17.] ČESKO, ČSN EN 1300, Praha: Český normalizační institut, březen 2020
[18.] ČESKO, ČSN EN 1630, Praha: Český normalizační institut, březen 2022
[19.] ČESKO. Terminologický slovník ministerstva vnitra. PRAHA 2016, dostupné z: https://www.mvcr.cz/soubor/terminologicky-slovnik-mv-verze-ke-stazeni.aspx
[20.] WEB Národní bezpečnostní úřad *nbu.cz* [online]. [cit. 2023-01-20]. Dostupné z: https://www.nbu.cz
[21.] WEB, Národní úřad pro kybernetickou a informační bezpečnost *nukib.cz* [online]. [cit. 2023-01-20]. Dostupné z: https://www.nukib.cz/cs/o-nukib/
[22.] WEB, Úřad pro technickou normalizaci, metrologii a státní zkušebnictví unmz.cz [online]. [cit. 2023-01-20]. Dostupné z: https://www.unmz.cz/obecne/o-uradu/
[23.] WEB, Mall.cz. *Mall.cz* [online]. [cit. 2022-10-20]. Dostupné z: https://www.mall.cz/

SEZNAM OBRÁZKŮ

Obrázek č. 1 – Nákres zájmového objektu 35
Obrázek č. 2 – Nákres ochrany perimetru zájmového objektu po úpravách 40
Obrázek č. 3 – Nákres zájmového objektu po úpravách 41
Obrázek č. 4 – Ishikawův diagram – Přehled identifikovaných hrozeb 44

SEZNAM TABULEK

Tabulka č. 1 – Typy úschovných objektů podle vyhlášky č. 528/2005 Sb. 18
Tabulka č. 2 – Typy zámků podle vyhlášky č. 528/2005 Sb. 19
Tabulka č. 3 – Šablony a jejich rozměry podle vyhlášky č. 528/2005 Sb. 20
Tabulka č. 4 – Požadavky jednotlivých typů zabezpečených oblastí podle vyhlášky č. 528/2005 Sb. 20
Tabulka č. 5 – Typy uzamykacích systémů zabezpečené oblasti dle vyhlášky č. 528/2005 Sb. 21
Tabulka č. 6 – Typ systému kontroly vstupu podle vyhlášky č. 528/2005 Sb. 22
Tabulka č. 7 – Typy EZTS podle vyhlášky č. 528/2005 Sb. 24
Tabulka č. 8 – Způsobilost EZTS pro stupně utajení podle vyhlášky č. 528/2005 Sb. 24
Tabulka č. 9 – Bodové ohodnocení pro jednotlivé typy EZTS podle vyhlášky č. 528/2005 Sb. 25
Tabulka č. 10 – Požadavky na jednotlivé typy fyzických bariér podle vyhl. č. 528/2005 Sb. 26
Tabulka č. 11 – Požadavky na jednotlivé typy NNI podle vyhlášky č. 528/2005 Sb. 28
Tabulka č. 12 – Bodové hodnocení pravděpodobnosti vzniku množiny hrozeb . 45
Tabulka č. 13 – bodové hodnocení závažnosti následků hrozby 46
Tabulka č. 14 – Bodové hodnocení stupně odhalitelnosti hrozby 46
Tabulka č. 15 – Bodové spektrum výsledné míry rizika 46
Tabulka č. 16 – Míra rizika identifikovaných množin hrozeb pro zabezpečenou oblast č. 1 52
Tabulka č. 17 – Bodové ohodnocení zabezpečené oblasti č. 1 podle vyhlášky č. 528/2005 Sb. 54
Tabulka č. 18 – OBL – bodová hodnota určená kategorií zabezpečené oblasti. 55

Tabulka č. 19 – Tabulka bodových hodnot nejnižší míry zabezpečení zabezpečené oblasti podle přílohy č. 1 vyhlášky č. 528/2005 Sb. 55
Tabulka č. 20 – Míra rizika identifikovaných množin hrozeb pro jednací oblast č. 2 56
Tabulka č. 21 – Bodové ohodnocení jednací oblasti č. 2 podle vyhlášky č. 528/2005 Sb. 58
Tabulka č. 22 – OBL – bodová hodnota určená kategorií zabezpečené oblasti. 59
Tabulka č. 23 – Tabulka bodových hodnot nejnižší míry zabezpečení jednací oblasti podle přílohy č. 1 vyhlášky č. 528/2005 Sb. 59
Tabulka č. 24 – Míra rizika identifikovaných množin hrozeb pro zabezpečenou oblast č. 3 60
Tabulka č. 25 – Bodové ohodnocení zabezpečené oblasti č. 3 podle vyhlášky č. 528/2005 Sb. 62
Tabulka č. 26 – OBL – bodová hodnota určená kategorií zabezpečené oblasti. 63
Tabulka č. 27 – Tabulka bodových hodnot nejnižší míry zabezpečení zabezpečené oblasti podle přílohy č. 1 vyhlášky č. 528/2005 Sb. 63
Tabulka č. 28 – Míra rizika identifikovaných množin hrozeb pro zabezpečenou oblast č. 4 64
Tabulka č. 29 – Bodové ohodnocení zabezpečené oblasti č. 4 podle vyhlášky č. 528/2005 Sb. 66
Tabulka č. 30 OBL – bodová hodnota určená kategorií zabezpečené oblasti.... 67
Tabulka č. 31 Tabulka bodových hodnot nejnižší míry zabezpečení zabezpečené oblasti podle přílohy č. 1 vyhlášky č. 528/2005 Sb. 67

SEZNAM ZKRATEK

ICT – Informační a komunikační technologie

PS/2 – Typ konektoru používaný pro počítačové myši a klávesnice

BIOS – Basic imput output systém

UPS – Záložní zdroj elektrické energie

PCO – Pult centralizované ochrany

AČR – Armáda České republiky

OUI – Ochrana utajovaných informací

EZS – Elektronický zabezpečovací systém

EZTS – Elektronický zabezpečovací a tísňový systém

STS – Speciální televizní systém

IS – Informační systém

MÚ – Mimořádná událost

SKV – Systém kontroly vstupu

SEZNAM PŘÍLOH

[1.] ČESKO, Vyhláška č. 528/2005 Sb., ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků. In *Sbírka zákonů České republiky.* 2005, částka 179/2005, příloha č. 1, kapitola č. 14.3.1.

PŘÍLOHA Č. 1

ČESKO, Vyhláška č. 528/2005 Sb. ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků. In *Sbírka zákonů České republiky.* 2005, částka 179/2005, příloha č. 1, kapitola č. 14.3.1.

14.3.1. TABULKA BODOVÉHO OHODNOCENÍ OPATŘENÍ FYZICKÉ BEZPEČNOSTI V ZABEZPEČENÉ A JEDNACÍ OBLASTI

Záhlaví tabulky obsahuje tyto údaje:

a) název zabezpečené (jednací) oblasti,

b) kategorii a třídu zabezpečené oblasti,

c) druh jednací oblasti v závislosti na utajovaných informacích, které jsou v ní pravidelně projednávány,

d) účel, k němuž má zabezpečená oblast sloužit.

BEZPEČNOSTNÍ OPATŘENÍ	TYP	BODOVÉ OHODNOCENÍ
Úschovné objekty	❑ T. 4 – 4 body ❑ T. 3 – 3 body ❑ T. 2 – 2 body	SS1 =
Zámky úschovných objektů	❑ T. 4 – 4 body ❑ T. 3 – 3 body ❑ T. 2 – 2 body	SS2 =
Úschovný objekt včetně uzamykacího systému	❑ T. 1 – 1 bod ❑ T. 1A – 1 bod ❑ T. 1B – 2 body ❑ T. 1C – 3 body	**S1 =**
Celkové hodnocení úschovného objektu a jeho zámku	S1 = SS1 x SS2	**S1 =**
Zabezpečené oblasti	❑ T. 4 – 4 body ❑ T. 3 – 3 body ❑ T. 2 – 2 body ❑ T. 1 – 1 bod	SS3 =

Uzamykací systém zabezpečené oblasti	❑ T. 4 – 4 body ❑ T. 3 – 3 body ❑ T. 2 – 2 body ❑ T. 1 – 1 bod	SS4 =
Celkové ohodnocení zabezpečené oblasti a jejího uzamykacího systému	S2 = SS3 x SS4	**S2 =**
Objekt	❑ T. 4 – 4 body ❑ T. 3 – 3 body ❑ T. 2 – 2 body ❑ T. 1 – 1 bod	**S3 =**
Systém kontroly vstupu	❑ T. 4 – 4 body ❑ T. 3 – 3 body ❑ T. 2 – 2 body ❑ T. 1 – 1 bod	SS6 =
Režim návštěv v objektu a) Návštěvy s doprovodem b) Návštěvy bez doprovodu c) Návštěvy bez kontroly	❑ ad a) – 3 bod ❑ ad b) – 1 bod ❑ ad c) – nehodnoceno	SS7 =
Celkové hodnocení kontroly vstupu	S4 = SS6 + SS7	**S4 =**
Ostraha	❑ T. 5 – 5bodů ❑ T. 4 – 4 body ❑ T. 3 – 3 body ❑ T. 2 – 2 body ❑ T. 1 – 1 bod	SS8 =
Zařízení elektrické zabezpečovací signalizace	❑ T. 4 – 4 body ❑ T. 3 – 3 body ❑ T. 2 – 2 body	

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

Celkové hodnocení ochrany perimetru	S6 = (SS10 x SS11) + SS12 + SS13 + SS14 + SS15	**S6 =**

Hodnoty proměnných S1 až S6 získané vyplněním tabulky bodového ohodnocení opatření fyzické bezpečnosti v zabezpečené oblasti je nutné porovnat s tabulkou bodových hodnot nejnižší míry zabezpečení zabezpečené a jednací oblasti podle bodu 12. přílohy.

Na základě tohoto porovnání je nutné stanovit, zda přijatá opatření fyzické bezpečnosti jsou pro danou míru rizika a kategorii zabezpečené oblasti dostatečná.

Na základě tohoto porovnání je nutné stanovit, zda přijatá opatření fyzické bezpečnosti jsou pro danou míru rizika a dále na stupni utajovaných informací pravidelně projednávaných v jednací oblasti dostatečná.

Ověření, zda jednotlivá použitá opatření fyzické bezpečnosti a vyhodnocení rizik odpovídají projektu fyzické bezpečnosti a právním předpisům v oblasti ochrany utajovaných informací, provádí odpovědná osoba nebo jí pověřená osoba.

Funkční zkoušky pro elektrické zabezpečovací systémy se provádí podle TNI 3345 91-3. Rozsah a časový interval funkčních zkoušek je stanoven v tabulce A1 (stupeň 1). Podmínky funkčních zkoušek u ostatních technických zařízení stanoví odpovědná osoba nebo jí pověřená osoba.

Zápis o provedení funkční zkoušky u technických prostředků uvedených v § 30 odst. 1 zákona se ukládají u odpovědné osoby nebo jí pověřené osoby.