Ochrana utajovaných informací v podmínkách Policie ČR

Bc. Martin HROMEK

Diplomová práce
2018/2019

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2018/2019

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Martin Hromek**
Osobní číslo:	**A17675**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Ochrana utajovaných informací v podmínkách Policie ČR**
Téma anglicky:	**Protection of Classified Information under the Czech Republic Police Conditions**

Zásady pro vypracování:

1. **Nastudujte právní prameny v oblasti ochrany utajovaných informací.**
2. **Popište teoretická východiska pro zpracování práce.**
3. **Charakterizujte proces zabezpečení objektu pro zpracování utajovaných informací ve stupni VYHRAZENÉ a DŮVĚRNÉ.**
4. **Proveďte analýzu rizik ve vztahu k ohrožení utajované informace.**
5. **Výsledky analýzy aplikujte do návrhu zabezpečení objektu.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **Zákon č. 412/2005 Sb. ze dne 21. září 2005 o ochraně utajovaných informací a bezpečnostní způsobilosti.**
2. **Vyhláška č. 523 ze dne 5. prosince 2005 o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a certifikaci stínících komor.**
3. **Vyhláška č. 528 ze dne 5. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků.**
4. **www.nbu.cz.**

Vedoucí diplomové práce: **doc. Ing. Martin Hromada, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **30. listopadu 2018**

Termín odevzdání diplomové práce: **17. května 2019**

Ve Zlíně dne 14. prosince 2018

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 14. května 2019

Bc. Martin HROMEK v. r.
podpis diplomanta

ABSTRAKT

Cílem této diplomové práce je popsat proces ochrany utajovaných informací v podmínkách Policie ČR. Práce je rozdělena na část teoretickou a praktickou. V teoretické části jsou charakterizovány právní prameny v oblasti utajovaných informací, jsou popsány jednotlivé druhy bezpečnosti z pohledu zákona č. 412/2005 Sb. a také instituce, které se ochranou utajovaných informací zabývají. V posledních kapitolách teoretické části, je popsán proces řízení rizik a současné trendy v oblasti fyzické bezpečnosti objektů.

Praktická část se věnuje samotné analýze rizik a návrhu zabezpečení objektu Policie ČR, ve kterém se zpracovávají utajované informace ve stupni utajení Vyhrazené a Důvěrné.

Klíčová slova: ochrana utajovaných informací, fyzická bezpečnost, policie, zákon o ochraně utajovaných informací, řízení rizik, KARS

ABSTRACT

The aim of this thesis is to describe the process of classified information protection in the Czech Police. The thesis is divided into theoretical and practical part. In the theoretical part there are characterized the legal sources in the area of classified information, individual types of security are described from the perspective of Act No. 412/2005 Coll. as well as institutions that deal with the protection of classified information. The last chapters of the theoretical part describe the risk management process and current trends in the area of physical security.

The practical part deals with the risk analysis itself and the security measures design of the Police of the Czech Republic object, where classified information is processed at the restricted and confidential level.

Keywords: Protection of Classified Information, Physical Security, Police, Act on the Protection of Classified Information, Risk Management, KARS

Děkuji vedoucímu mé práce doc. Ing. Martinu Hromadovi, Ph.D., za cenné rady, ochotu a trpělivosti při zpracování této diplomové práce. Také bych chtěl poděkovat své rodině a přítelkyni za podporu a vytvoření podmínek při studiu.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Téměř v každém oboru lidské činnosti se můžeme setkat se situací, kdy je nutné chránit informace před nepovolanými osobami. Takovou informaci někdy můžeme obecně nazývat jako tajemství, čímž zdůrazňujeme vážnost informací a snahu takové informace neprozrazovat. Může se jednat o citlivé osobní údaje, obchodní tajemství, know-how ve výrobě, nebo lékařské, bankovní nebo tajemství v oblasti poskytování právní pomoci apod. Prozrazení takových informací, může způsobit materiální škody nebo jiné újmy fyzickým i právnickým osobám a v některých případech i státním institucím nebo státu samotnému.

V oblasti bezpečnosti se může jednat o informace, které jsou běžným osobám nedostupné a jsou chráněny zvláštním souborem opatření, které takové informace chrání již při vzniku, přenosu, uchování, až do samotného zániku informace, a to před únikem, zneužitím nebo vyzrazením informace. Takové informace jsou dostupné jen osobám, mající povolení a jsou oprávněny se s takovou informací seznamovat, nebo mají zvláštní postavení. Většinou v takových případech hovoříme o utajovaných informacích.

Garantem za ochranu utajovaných informací v České republice je Národní bezpečnostní úřad, který je orgánem výkonné moci v oblasti ochrany utajovaných informací a bezpečnostní způsobilosti a Národní úřad pro kybernetickou a informační bezpečnost, který je orgánem pro kybernetickou bezpečnost o ochranu utajovaných informací v oblasti informačních a komunikačních systémů.

Cílem diplomové práce je popsat proces ochrany utajovaných informací v podmínkách Policie České republiky, v nejčastěji se vyskytujících stupních utajení Vyhrazené a Důvěrné a na základě vyhodnocené analýzy rizik, provést návrh zabezpečení objektu s opatřeními vedoucími k minimalizaci ohrožení utajované informace.

V teoretické části diplomové práce jsou v jednotlivých kapitolách popsány základní legislativní prameny, které se ochranou utajovaných informací v České republice zabývají a další prováděcí předpisy a vyhlášky. Podrobněji je rozebrán zákon o ochraně utajovaných informací a bezpečnostní způsobilosti č. 412/2005 Sb. v platném znění, druhy jednotlivých bezpečností z pohledu tohoto zákona a jsou zde také popsány právní postihy za vyzrazení utajované informace, nebo nedodržení zákonných zásad a pravidel při zpracování a manipulaci s utajovanou informací. Stručně jsou také popsány instituce, které se ochranou utajovaných informací zabývají, včetně institucí Ministerstva vnitra a útvarů Policie České

republiky. Poslední kapitola teoretické části se věnuje trendům v oblasti zabezpečení objektů z pohledu fyzické bezpečnosti.

Praktická část diplomové práce se věnuje samotné analýze rizik, vyhodnocením analýzy, a tvorbě návrhu zabezpečení objektu pro kategorii Vyhrazené a Důvěrné s důrazem na aplikaci výsledků analýzy rizik, vedoucích ke snížení rizika ohrožení utajované informace.

V poslední řadě bych chtěl uvést, že vzhledem k povaze tématu diplomové práce, je posuzovaný objekt a jeho popis pouze ilustrativní.

I. TEORETICKÁ ČÁST

1 PRÁVNÍ PRAMENY V OBLASTI UTAJOVANÝCH INFORMACÍ

V oblasti ochrany utajovaných informací se nelze řídit jinak, než zákony a nařízeními. V následující kapitole jsou popsány zákony a vyhlášky, které provází ochranu utajovaných informací v České republice a kterými se musí každý subjekt při zpracování utajovaných informací řídit.

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

Věcná působnost tohoto zákona, jak již jeho název napovídá, je v oblasti ochrany utajovaných informací a v oblasti bezpečnostní způsobilosti. Zákon upravuje zásady a podmínky pro stanovení informací jako informace utajované, podmínky pro jejich přístup a požadavky na jejich ochranu. Dále upravuje zásady pro stanovení citlivých činností a výkon státní správy. [1]

V ustanovení § 2 tohoto zákona jsou vymezeny základní pojmy. Základní pojem, který se v zákoně vyskytuje mnohokrát i v jeho samotném názvu, je pojem utajovaná informace.

„*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)*“ [1]

Čtenář by si mohl myslet, že utajovaná informace je každá informace zaznamenaná na jakémkoliv nosiči, v jakékoliv podobě. Dále, že stačí aby byla označena v souladu se zákonem a její vyzrazení nebo zneužití může způsobit újmu nebo může být nevýhodné pro zájmy ČR a v neposlední řadě musí být uvedena v seznamu utajovaných informací. Tato definice je výčtem znaků, které musí informace mít, aby mohla být považována za informací utajovanou. Jedná se o znaky:

a) **Materiální** – za materiální znak, v tomto případě považujeme tu část definice, ve které se hovoří o možnosti způsobení újmy nebo nevýhodnosti pro ČR.
b) **Formální** – v tomto případě se jedná o tři znaky.

[1] § 2 písm. a) zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti

- **je zaznamenána,**
- **je označena v souladu se zákonem,**
- **je uvedena v seznamu utajovaných informací.**

Aby mohla být informace označena jako utajovaná, musí splňovat všechny tři formální znaky a znak materiální současně. Při neexistenci jakéhokoliv z uvedených znaků, nelze informaci považovat za informaci utajovanou.

Utajovanou informaci zařazujeme do stupňů utajení, a to na základě výčtu v § 3 zákona. V tomto ustanovení jsou vymezeny újmy zájmům České republiky, které mohou být způsobeny vyzrazením nebo zneužitím utajované informace.

Mimořádně vážná újma může způsobit například bezprostřední ohrožení svrchovanosti ČR, demokracie a územní celistvosti. Může způsobit rozsáhlé ztráty na lidských životech nebo rozsáhlé ohrožení zdraví obyvatelstva.[2]

Vážná újma může způsobit značnou škodu finanční, měnové nebo v hospodářské oblasti ČR. Vážné ohrožení významných bezpečnostních operací nebo činností zpravodajských služeb.[3]

Prostá újma může způsobit zhoršení diplomatických vztahů, ohrožení bezpečnosti jednotlivce, zmaření, ztížení nebo ohrožení prověřovaní nebo vyšetřovaní zvlášť závažných zločinů.[4]

Nevýhodné pro zájmy ČR může mít za následek poškození významných ekonomických zájmů ČR, EU nebo jejího členského státu, narušení bezpečnosti operací nebo činnosti zpravodajských služeb, zmaření, ztížení nebo ohrožení prověřovaných, vyšetřovaných ostatních trestných činů než uvedených v odstavci 4 písm. f).[5]

Stupně utajení jsou uvedeny v § 4 zákona. Český právní systém uznává čtyři klasifikace utajované informace. Následující výčet odkazuje na stupně utajení od nejnižšího po nejvyšší.

- **Vyhrazené –** jde o takovou klasifikaci utajované informace, jejíž vyzrazení nebo zneužití může být nevýhodné pro zájmy ČR.

[2] § 3 odst. 2 zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti
[3] § 3 odst. 3 zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti
[4] § 3 odst. 4 zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti
[5] § 3 odst. 5 zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti

- **Důvěrné** – vyzrazení nebo zneužití takové informace, může způsobit prostou újmu zájmům ČR.
- **Tajné –** vyzrazení nebo zneužití takové informace, může způsobit vážnou újmu zájmům ČR.
- **Přísně tajné –** vyzrazení nebo zneužití takové informace, může způsobit mimořádně vážnou újmu zájmům ČR. [3]

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

Tato vyhláška je prováděcím předpisem, ve kterém jsou stanoveny podmínky a požadavky na informační systémy určené pro nakládání s utajovanými informacemi. Vyhláška je rozdělena do sedmi částí.

V první části je popsán předmět úpravy vyhlášky a jsou vymezeny základní pojmy v souvislosti s touto vyhláškou, jako je aktivum, objekt a subjekt informačního systému, analýza rizik, auditní záznam, autentizace a autorizace subjektu, kdo je bezpečnostní správce informačního systému a dalšími pojmy.[6] [4]

Ve druhé části jsou popsány požadavky na bezpečnost informačních systémů a požadavky na certifikaci informačních systémů.[7] [4]

Třetí část se věnuje komunikačním systémům. Je zde uvedeno, co musí obsahovat projekt bezpečnosti komunikačního systému, žádost o schválení projektu bezpečnosti komunikačního systému a jeho způsob a schvalování.[8] [4]

Čtvrtá část se věnuje specifické oblastí, a to kompromitujícím vyzařováním eklektických a elektronických zařízení, které by mohlo způsobit únik utajovaných informací ve stupni utajení Důvěrné, Tajné nebo Přísně tajné. Jedná se o vyzařování elektromagnetického pole. Tato část se také věnuje stínícím komorám, jejich certifikaci, podmínkami a způsoby

[6] § 1-2 vyhlášky č. 523/2005 Sb. v platném znění
[7] § 3 – 26 vyhlášky č. 523/2005 Sb. v platném znění
[8] § 27 – 29 vyhlášky č. 523/2005 Sb. v platném znění

provádění certifikace stínící komory, ve kterých je prováděno měření vyzářeného elektromagnetického pole výše uvedených zařízení.[9] [4]

V páté části jsou uvedeny náležitosti žádosti o uzavření smlouvy o zajištění činnosti orgánem státu nebo podnikatele.[10] [4]

Šestá část se věnuje podmínkám bezpečného provozování zařízení pro zpracování utajovaných informací v elektronické podobě, které není součástí informačního nebo komunikačního systému. Jedná se zejména o psací stroje s pamětí nebo kopírky.[11] [4]

Poslední část vyhlášky stanovuje účinnost vyhlášky. [12] [4]

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

Tato vyhláška stanoví 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. [5]

Součástí této vyhlášky jsou dvě přílohy. V první příloze nalezneme 15 částí, ve kterých jsou bodově ohodnoceny požadavky a vlastnosti např. u úschovných objektů a jejich zámků, zabezpečovacích zařízení, jsou zde stanoveny požadavky na ochranu perimetru, hranice objektu, ostrahu, systémy kontroly vstupu apod.

Druhou přílohou je vzor certifikátu technické prostředku, který vydává Národní bezpečnostní úřad.

1.4 Vyhláška č. 529/2005 Sb. o administrativní bezpečnosti a o registrech utajovaných informací

Tato vyhláška jsou popsány všechny administrativní požadavky při manipulaci s utajovanou informací. Od toho, jakým způsobem je utajovaná informace označena, a to jak v listinné,

[9] § 29a – 36 vyhlášky č. 523/2005 Sb. v platném znění
[10] § 37 vyhlášky č. 523/2005 Sb. v platném znění
[11] § 38 vyhlášky č. 523/2005 Sb. v platném znění
[12] § 39 vyhlášky č. 523/2005 Sb. v platném znění

tak i v nelistinné podobě, až po podrobnosti k přepravě, přenášení, převzetí utajované informace apod. [6]

Součástí vyhlášky je třináct příloh, které obsahují vzory administrativní pomůcek např. jednací protokol, manipulační kniha, zápůjční kniha, sběrný arch apod.

1.5 Nařízení vlády č. 522/2005 Sb. kterým se stanový seznam utajovaných informací

V tomto nařízení vlády je stanoven seznam utajovaných informací, které jsou přílohou tohoto nařízení. Příloha č. 1 je určena pro obecnou oblast působnosti, 9 příloh je určeno pro vyjmenovaná ministerstva České republiky a zbylých 10 příloh je určeno pro další orgány státu, jako je například Česká národní banka, zpravodajské služby České republiky, Národní úřad pro kybernetickou a informační bezpečnost, Generální inspekce bezpečnostních sborů, Národní bezpečnostní úřad apod. V jednotlivých přílohách je vždy popsána oblast působnosti a charakteristika informací, které mohou být utajovanými informacemi. Dále je zde uveden i stupeň, případně rozsah stupňů utajení těchto informací. [7]

1.6 Postihy za ohrožení, vyzrazení utajované informace de lege lata

V moderní společnosti jsou zákony a vyhláškami stanoveny jakési pravidla, kterými by se měl řídit každý. Vynucení povinností vyplývajících z podstaty zákona o ochraně utajovaných informací, je již v zákoně řešeno sankcemi. V zákoně č. 412/2005 Sb. jsou popsány přestupky. Trestné činy spojené s nedodržením povinností při nakládání s utajovanými informacemi jsou popsány v Trestním zákoníku v zákoně č. 40/2009 Sb. v platném znění.

1.6.1 Přestupky dle zákona č. 412/2005 Sb. § 148 - § 155a zákona.

V části osmé tohoto zákona jsou uvedeny skutkové podstaty jednotlivých přestupků, kterých se může dopustit subjekt, při neplnění povinností, vyplívajících z jednotlivých ustanovení tohoto zákona. V jednotlivých paragrafech jsou uvedeny i sankce za porušení povinností. Za přestupky, dle tohoto zákona, může být uložena peněžitá sankce, pokuta od 30 000,- Kč až do výše 5 000 000,- Kč. [1]

1.6.2 Trestné činy zákona dle č. 40/2009 Sb.

Nový trestní zákoník obecně definuje trestný čin v § 13. Dle tohoto ustanovení je trestný čin, takový protiprávní čin, který trestný zákoník označuje za trestný a který vykazuje znaky uvedené v tomto zákoně. K trestní odpovědnosti je třeba úmyslu, nestanoví-li trestní zákoník výslovně, že postačí zavinění z nedbalosti. [9]

V § 14 jsou trestné činy rozděleny na přečiny a zločiny. Přečiny jsou všechny nedbalostní trestné činy a úmyslné trestné činy, u kterých je horní hranice trestu odnětí svobody do 5 let. Zločiny jsou trestné činy, které nejsou podle trestního zákoníku přečiny. S dalším pojmem u trestného činu, se kterým se můžeme setkat je zvlášť závažný zločin, kterým je úmyslný trestný činy, u kterých je dle trestního zákona horní hranice trestní sazby nejméně 10 let. [9]

Trestné činy, jejichž skutková podstata souvisí s ochranou utajovaných informací jsou v trestním zákoníku trestné činy uvedené v deváté hlavě, dílu druhém, ve které jsou popsány trestné činy proti bezpečnosti České republiky, cizího státu a mezinárodní organizace. [9]

§ 316 – Vyzvědačství

Tento trestný čin sankcionuje odnětím svobody na dvě až osm let každého, kdo utajovanou informaci vyzvídá, sbírá údaje obsahující utajované informace s cílem tyto informace a údaje vyzradit cizí moci, nebo kdo takovou informaci cizí moci vyzradí. Stejná sankce hrozí i tomu, kdo umožní nebo usnadní takovou činnost pachateli nebo organizaci.

Odnětím svobody na osm až patnáct let je potrestán každý, kdo takové informace vyzvídá jako člen organizace, jejímž cílem je vyzvídat utajované informace, dále ten, komu byla ochrana utajovaných informací zvlášť uložena. Trestného činu se dopustí i ten, kdo takovým činem získá pro sebe, nebo jiného značný prospěch, nebo spáchá-li čin ve značném rozsahu. V neposlední řadě takový čin spáchá i ten, kdo vyzvídá utajované informace klasifikované ve stupni utajení Přísně tajné.

V případě vyhlášeného válečného stavu nebo stavu ohrožení státu, je trest odnětí svobody v délce trvání dvanáct až dvacet let, nebo výjimečný trest.

Je nutné také podotknout, že i příprava k těmto činům je trestná. [9]

§ 317 – Ohrožení utajované informace

Trestný čin *„Ohrožení utajované informace“* spáchá osoba, která utajované informace vyzvídá s cílem vyzradit ji nepovolané osobě, nebo ten kdo sbírá údaje obsahující utajované informace nebo i ten kdo takovou informaci nepovolané osobě úmyslně vyzradí. Za takové

jednání bude pachatel potrestán trestem odnětí svobody až na tři léta nebo zákazem činnosti. Na pět až dvanáct let bude potrestán ten za výše uvedenou činnost, bude-li se jednat o utajované informace z oblasti zabezpečení obranyschopnosti ČR, které jsou klasifikovány stupněm utajení Přísně tajné, případně bude-li vyhlášen válečný stav nebo stav ohrožení státu.

Trestem odnětí svobody na dvě až osm let, je potrestán pachatel, který úmyslně vyzradí nepovolané osobě utajovanou informaci klasifikovanou stupněm utajení Tajné nebo Přísně tajné, dále spáchá-li takový čin jako osoba, jemuž byla ochrana utajovaných informací zvlášť uložena nebo získá-li pachatel takovým jednáním značný prospěch, způsobí-li značnou škodu, nebo jiný zvlášť závažný následek.

I u tohoto trestného činu je příprava stejně trestná jako čin samotný. [9]

§ 318 – Ohrožení utajované informace z nedbalosti

Jak již název tohoto trestného činu napovídá, jedná se o nedbalostní trestný čin. Takového činu se pachatel dopustí, pokud z nedbalosti způsobí vyzrazení utajované informace klasifikované stupněm utajení Tajné a Přísně tajné. Za takové hrozí trest odnětí svobody až do výše tří let, nebo zákaz činnosti. [9]

Cílem této kapitoly bylo charakterizovat základní právní prameny, se kterými se v oblasti ochrany utajovaných informací můžeme setkat. Nalezneme zde definici, která vysvětluje pojem ***utajovaná informace***, a jaké znaky, z pohledu práva, musí taková informace nést, aby mohla být označena jako utajovaná informace. Dále byly vyjmenovány jednotlivé stupně utajení, které charakterizuje zákon č. 412/2005 Sb. v platném znění. Stručně jsou popsány jednotlivé vyhlášky, které provází zákon č. 412/2005 Sb. v platném znění, v jednotlivých oblastech. V neposlední řadě zde nalezneme také podkapitolu, která seznamuje s možnými postihy, za nedodržení povinností při nakládání s utajovanou informací. Ať už se jedná o přestupky dle zákona č. 412/2005 Sb. v platném znění, nebo trestné činy dle zákona č. 40/2009 Sb. v platném znění.

2 DRUHY BEZPEČNOSTÍ Z POHLEDU ZÁKONA Č. 412/2005 SB. O OCHRANĚ UTAJOVANÝCH INFORMACÍ A BEZPEČNOSTNÍ ZPŮSOBILOSTI

Jednotlivé druhy bezpečností tvoří ucelený soubor opatření, které slouží k ochraně utajovaných informací. V zákoně č. 412/2005 Sb. je definováno šest oblastí, které jednotlivě i jako celek slouží k ochraně utajovaný informací.

2.1 Personální bezpečnost

Personální bezpečnost je založena na vhodném výběru osob, které se smí seznamovat s utajovanými informacemi.

Personální bezpečnost je zakotvena v zákoně č. 412/2005 Sb. v hlavě II. Zde jsou stanoveny podmínky, pro vydání oznámení v případě stupně utajení Vyhrazené a poučení pro stupně utajení Důvěrné, Tajné a Přísně tajné.

Základními podmínkami pro získaní oznámení pro stupeň Vyhrazené jsou:

- Stanovená hranice 18 let věku,
- Bezúhonnost,
- Svéprávnost.

Podmínky pro získání osvědčení pro stupně Důvěrné, Tajné a Přísně tajné jsou:

- Osobnostní způsobilost,
- Bezpečnostní spolehlivost,
- Občan ČR, EU nebo Organizace severoatlantické smlouvy – NATO,
- Dále musí splnit podmínky pro získání oznámení pro stupeň Vyhrazené.

Platnost oznámení a osvědčení pro fyzické osoby je zobrazena v následující tabulce. Součástí tabulky je uveden také anglický ekvivalent pro české stupně utajení.

Tab. 1 Přehled platnosti osvědčení a oznámení [zdroj: 1, upraveno autorem]

Stupeň utajení	Doba platnosti	Anglický název
Vyhrazené (oznámení)	5 let	RESTRICTED
Důvěrné (osvědčení)	9 let	CONFIDENTIAL
Tajné (osvědčení)	7 let	SECRET
Přísně tajné (osvědčení)	5 let	TOP SECRET

2.2 Průmyslová bezpečnost

Průmyslovou bezpečností se rozumí systém opatření k zjišťování a ověřování podmínek pro přístup podnikatele k utajovaným informacím a k zajištění nakládání s utajovanou informací u podnikatele v souladu s tímto zákonem. [13]

Podnikatel může mít přístup k utajovaným informacím, pokud je potřebuje nezbytně pro výkon své činnosti, musí ale zároveň doložit schopnost zabezpečit utajované informace. Podnikatel, který potřebuje pro výkon své činnosti informace stupně utajení Vyhrazené, nepotřebuje osvědčení. Národnímu bezpečnostnímu úřadu, předkládá podnikatel pouze písemné prohlášení, že je schopen zajistit ochranu utajovaných informací. U vyšších stupňů utajení, Důvěrné, Tajné a Přísně tajné musí proběhnout bezpečnostní řízení a podnikateli je vydáno osvědčení. [2]

2.3 Administrativní bezpečnost

Administrativní bezpečnost v sobě zahrnuje systém opatření při tvorbě, příjmu, evidenci, zpracování, odesílání, přepravě, přenášení, ukládání, skartační řízení, archivaci, případně jiné nakládání s utajovanými informacemi. [14]

[13] § 5 písm. b) zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti
[14] § 5 písm. c) zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti

2.4 Fyzická bezpečnost

Fyzickou bezpečností tvoří systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím, popřípadě přístup nebo pokus o něj zaznamenat.[15]

Předmětem fyzické bezpečnosti jsou všechna místa a prostory, v nichž jsou zpracovávány nebo ukládány utajované informace. Podle stupně a četnosti výskytu utajovaných informací pak jsou definována opatření k jejich ochraně. Všechny budovy, komplexy budov nebo prostory ohraničené oplocením, místnosti a stavebně či jinak ohraničené prostory určené k ochraně utajovaných informací, musí být chráněny pomocí odpovídajících bezpečnostních opatření. Při rozhodování o tom, jaký stupeň ochrany bude použit, je brán na zřetel zejména stanovený stupeň utajení, množství utajovaných informací, forma zpracování a uchovávání, stupeň bezpečnostní prověrky zaměstnanců a dalších osob, které budou vstupovat do těchto prostor, místní vyhodnocení možných hrozeb napadení nebo narušení objektu. [10]

2.5 Bezpečnost informačních a komunikačních systému

Bezpečností informačních a komunikačních systémů tvoří systém opatření, jejichž cílem je zajistit důvěrnost, integritu a dostupnost utajovaných informací, s nimiž tyto systémy nakládají, a odpovědnost správy a uživatele za jejich činnost v informačním nebo komunikačním systému. [16]

Znaky důvěrnost, integrita a dostupnost tvoří základní pravidla bezpečnosti informací.

- Důvěrnost – Confidentality – informace jsou dostupné jen těm, kdo k nim má přístup,
- Integrita – Integrity – je zajištěna úplnost informací,
- Dostupnost – Availability – informace jsou dostupné právě v okamžiku, kdy jsou potřeba.

Odpovědnost za tuto problematiku převzal Národní úřad pro kybernetickou a informační bezpečnost. [11]

[15] §5 písm. d) zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti
[16] §5 písm. e) zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti

2.6 Kryptografická ochrana

Kryptografickou ochranou tvoří systém opatření na ochranu utajovaných informací použitím kryptografických metod a kryptografických materiálů při zpracování, přenosu nebo ukládání utajovaných informací. [17]

Kryptografická ochrana zajišťuje ochranu důvěrnosti informace při jejím přenosu komunikačním kanálem. Kryptografický prostředek, který zajišťuje kryptografickou ochranu utajované informace musí být certifikován Národním bezpečnostním úřadem pro stupeň utajení shodným se stupněm utajení utajované informace nebo pro stupeň utajení vyšší.

Zajištění kryptografické ochrany je vymezeno ve vyhlášce č. 432/2011 Sb. o zajištění kryptografické ochrany utajovaných informací a ve vyhlášce č. 525/2005 Sb. o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací.

V této kapitole jsou stručně charakterizovány jednotlivé druhy bezpečností ve smyslu zákona č. 412/2005 Sb. o ochraně utajovaných informací a bezpečnostní způsobilosti v platném znění. Některé druhy bezpečnosti jsou provázeny v samostatných vyhláškách. Ochrana utajovaných informací je účinná tehdy, jsou-li zajištěny veškeré povinnosti vyplívající ze zákona a vyhlášek, včetně podmínek z jednotlivých druhů bezpečností.

[17] § 5 písm. f) zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti

3 INSTITUCE V OBLASTI OCHRANY UTAJOVANÝCH INFORMACÍ V ČR

Garantem za oblast utajovaných informací je v ČR Národní bezpečnostní úřad, od kterého se v roce 2017 oddělil Národní úřad pro kybernetickou a informační bezpečnost. Ředitelem Národního bezpečnostního úřadu je genmjr. Bc. Jiří Lang, který v minulosti zastával funkci ředitele Bezpečnostní informační služby a ředitele Úřadu pro zahraniční styky a informace.

Ředitelem Národního úřadu pro kybernetickou a informační bezpečnost je Ing. Dušan Navrátil, který také v minulosti zastával funkci asistenta ředitele u BIS a později byl také ředitelem NBÚ.

3.1 Národní bezpečnostní úřad

Národní bezpečnostní úřad, byl zřízen zákonem č. 148/1998 Sb. o ochraně utajovaných skutečností k 1. 8. 1998 a v současné době se řídí zákonem č. 412/2005 Sb. Je ústředním správním úřadem pro oblast ochrany utajovaných informací a bezpečnostní způsobilosti. Hlavní úkoly Národního bezpečnostní úřadu jsou ukotveny v § 137 zákona č. 412/2005 Sb. v platném znění, kterými jsou:

- *rozhoduje o žádosti fyzické osoby, žádosti podnikatele a žádosti o doklad a o zrušení platnosti osvědčení fyzické osoby, osvědčení podnikatele a dokladu, s výjimkou případů stanovených tímto zákonem[18], a vydává osvědčení fyzické osoby podle § 56a,*
- *vykonává kontrolu v oblasti ochrany utajovaných informací a bezpečnostní způsobilosti (§ 143) a metodickou činnost, s výjimkou případů stanovených tímto zákonem (§ 143 odst. 5),*
- *plní úkoly v oblasti ochrany utajovaných informací v souladu se závazky vyplývajícími z členství České republiky v Evropské unii, Organizaci Severoatlantické smlouvy a z mezinárodních smluv, jimiž je Česká republika vázána,*
- *vede ústřední registr a schvaluje zřízení registrů v orgánech státu a u podnikatelů,*
- *ve stanovených případech povoluje poskytování utajovaných informací v mezinárodním styku,*

[18] § 140 odst. 1 písm. a) a § 141 odst. 1 zákona č. 412/2005 Sb.

- *ke kurýrní přepravě utajovaných informací stupně utajení Přísně tajné, Tajné nebo Důvěrné poskytovaných v rámci mezinárodního styku, s výjimkou utajované informace poskytované podle § 78 odst. 1, vydává na základě písemné žádosti odpovědné osoby nebo bezpečnostního ředitele kurýrní listy a v odůvodněných případech zajišťuje jejich přepravu,*
- *provádí certifikaci technického prostředku,*
- *vydává bezpečnostní standardy,*
- *ukládá správní tresty za nedodržení povinností stanovených tímto zákonem,*
- *rozhoduje v dalších věcech a plní další úkoly na úseku ochrany utajovaných informací a bezpečnostní způsobilosti stanovené tímto zákonem a*
- *vydává Věstník Úřadu, který zveřejňuje na svých internetových stránkách.* [13]

3.2 Národní úřad pro kybernetickou a informační bezpečnost

Národní úřad pro kybernetickou a informační bezpečnost vznikl 1. srpna 2017 na základě zákona č. 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

Působnost Národního úřadu pro kybernetickou a informační bezpečnost:

- *zajišťuje zkoušky zvláštní odborné způsobilosti a vydává osvědčení o zvláštní odborné způsobilosti,*
- *plní úkoly v souladu se závazky vyplývajícími z členství České republiky v Evropské unii, Organizaci Severoatlantické smlouvy a z mezinárodních smluv, jimiž je Česká republika vázána, ve vybraných oblastech ochrany utajovaných informací,*
- *vykonává metodickou činnost,*
- *zajišťuje činnost Národního střediska komunikační bezpečnosti, Národního střediska pro distribuci kryptografického materiálu, Národního střediska pro měření kompromitujícího vyzařování a Národního střediska pro bezpečnost informačních systémů, které jsou jeho součástí,*
- *provádí certifikaci informačního systému, kryptografického prostředku, kryptografického pracoviště a stínící komory a schvaluje projekt bezpečnosti komunikačního systému,*
- *zajišťuje výzkum, vývoj a výrobu národních kryptografických prostředků,*

- *vyvíjí a schvaluje národní šifrové algoritmy a vytváří národní politiku kryptografické ochrany,*
- *zjišťuje kompromitující vyzařování tam, kde se vyskytují nebo budou vyskytovat utajované informace,*
- *zjišťuje v součinnosti se zpravodajskými službami a policií, zda v jednací oblasti nedochází nedovoleným použitím technických prostředků určených k získávání informací k ohrožení nebo únikům utajovaných informací,*
- *vydává bezpečnostní standardy,*
- *ukládá správní tresty za nedodržení povinností stanovených tímto zákonem,*
- *rozhoduje v dalších věcech a plní další úkoly na úseku ochrany utajovaných informací stanovené tímto zákonem.* [14]

3.3 Zajištění ochrany utajovaných informací u Ministerstva vnitra a Policie České republiky

Úlohu ochrany utajovaných informací v rezortu Ministerstva vnitra spravuje bezpečnostní odbor ministerstva vnitra.

„*Bezpečnostní odbor řídí a koordinuje ochranu utajovaných informací v ministerstvu, v organizačních složkách státu, státních příspěvkových organizacích, zřízených k plnění úkolů v oboru působnosti ministerstva, ke kterým ministerstvo vykonává zřizovatelské funkce a v policii, včetně personální, administrativní a fyzické bezpečnosti. Ředitel bezpečnostního odboru z pověření ministra vnitra vykonává funkci bezpečnostního ředitele a plní povinnosti odpovědné osoby v oblasti ochrany utajovaných informací a bezpečnostní způsobilosti, dále odbor přijímá, eviduje a vyřizuje žádosti o vydání tzv. lustračního osvědčení.“* [12]

V rámci jednotlivých krajských ředitelství policie České republiky jsou začleněny odbory ochrany utajovaných informací (OOUI).

Na krajském ředitelství policie Jihomoravského kraje, stejně jako u většiny ostatních krajských ředitelství spadá OOUI pod kancelář ředitele krajského ředitelství. Mezi základní náplň práce zaměstnanců odboru je zajištění agendy fyzické a personální bezpečnosti KŘ, tvorba projektů fyzické bezpečnosti ve spolupráci s lokálními správci IS, správa IS a krypto prostředků a v neposlední řadě školení držitelů osvědčení a pověření.

Tato kapitola stručně charakterizuje instituce, které mají v České republice ochranu utajovaných informací na starost. Národní bezpečnostní úřad je hlavním garantem za tuto problematiku. V oblasti ochrany utajovaných informací v prostředí kyberprostoru, má tuto problematiku na starost Národní úřad pro kybernetickou a informační bezpečnost. Vzhledem k tématu této diplomové práce, je zde také zmíněn Bezpečnostní odbor Ministerstva vnitra a Odbor ochrany utajovaných informací na úrovni Krajského ředitelství policie ČR a jejich působnost.

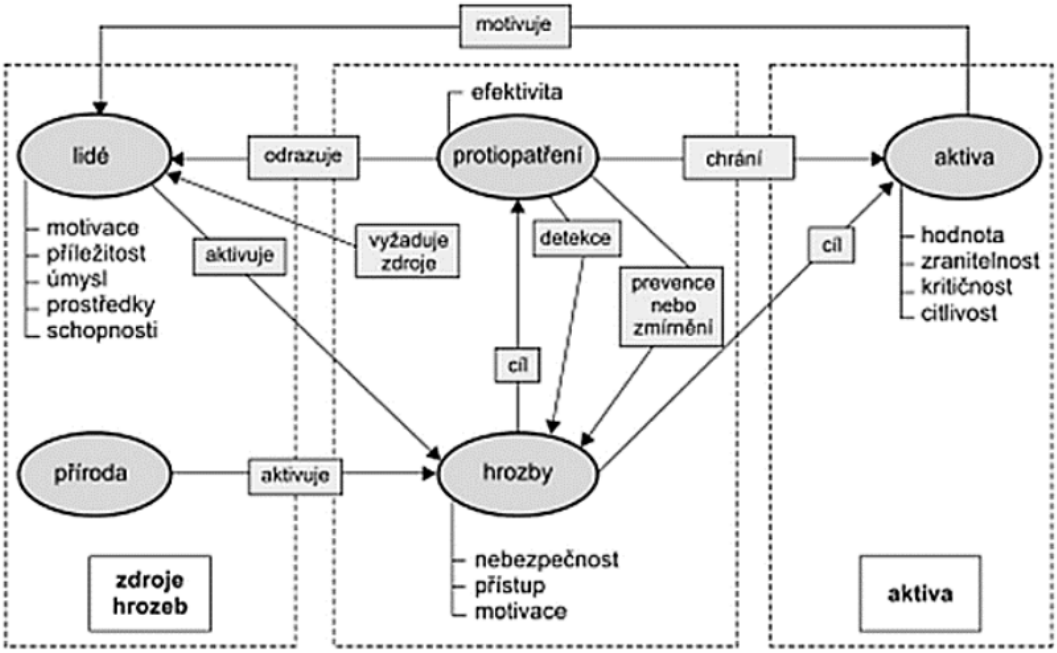
4 ŘÍZENÍ RIZIK

Řízení rizik je proces, který se zaměřuje na identifikaci, analýzu a vyhodnocení rizik s cílem jejich snížení na přijatelnou mez. Součástí tohoto procesu, je rozhodovací proces, kterému předchází analýza rizik. [15]

4.1 Základní pojmy v oblasti řízení rizik

- **Riziko** – pojem riziko má v dnešní době mnoho významů, mnoho definic.
  - Pravděpodobnost nebo možnost vzniku ztráty.
  - Nebezpečí chybného rozhodnutí.
  - Neurčitost spojená s vývojem hodnoty aktiva.
  - Pravděpodobnost jakéhokoliv výsledku, odlišného od výsledku očekávaného. [15]
- **Aktivum** – aktivem můžeme označit vše, co má pro subjekt určitou hodnotu, kterou ohrožuje hrozba. Aktiva můžeme rozdělit na hmotné a nehmotné. Mezi hmotné aktiva subjektu můžeme zařadit např. cenné papíry, peníze, nemovitosti a za nehmotná aktiva můžeme označit např. informace, know-how, personálu apod. [15]
- **Hrozba** – jedná se o událost, aktivitu, osobu, která má nežádoucí vliv na aktiva nebo může způsobit škodu. Některé hrozby mají potenciál zasáhnout více aktiv. [15]
- **Zranitelnost** – jedná se o slabinu, nedostatek aktiva, na kterou míří hrozba, k uplatnění svého negativního vlivu. [15]
- **Protiopatření** – můžeme chápat cokoliv (proces, postup, prostředek), čím je zmírněno působení hrozby, snížení zranitelnosti nebo dopadu hrozby. [15]

Následující obrázek zobrazuje vztahy mezi jednotlivými pojmy jako entitami při řízení rizik.



Obr. 1 Vztahy v analýze rizik [zdroj: 15]

4.2 Metody analýzy rizik a jejich stručný popis

Metody pro analýzu rizik můžeme rozdělit na metody kvalitativní a kvantitativní, případně kombinované metody.

- **Kvalitativní metody** řízení rizik popisujeme závažností dopadu a pravděpodobností, že událost nastane. Míra rizika je vyjádřena čísly v určitém rozsahu nebo slovním vyjádřením. Číselné vyjádření může být např. od 1 až 5 nebo logickou formulací 0/1. Slovní vyjádření přestavuje pojmy malé, střední, vysoké apod. [15]
- **Kvantitativní metody** řízení rizik jsou založeny na matematickém výpočtu, vycházejícího ze dvou proměnných. První proměnou je frekvence výskytu a druhou proměnou je dopad rizika. Výsledek je často vyjádřen číselnou formou. Pokud působí riziko na hmotné aktivum, výsledek často vyjadřuje finanční dopad. Nevýhodou těchto metod je jejich náročnost na provedení a zpracování výsledků a často vysoce formalizovaný postup. [15]
- **Kombinované metody** řízení rizik se vyznačují kombinací číselných údajů a verbálním hodnocením. [15]

Následující výčet stručně popisuje vybrané metody, se kterými se můžeme setkat při řízení rizik.

- **Checklist (kontrolní seznam)** – jedná se o jednoduchou metodu, při které je využit seznam položek, u kterých se ověřuje, zda jsou splněny, případně v jaké míře. Zjednodušeně můžeme říct, že se jedná o klasický zaškrtávací seznam úkolů, položek ke splnění. [17]
- **Metoda Delphi** – jedná se o kvalitativní metodu, jejímž základem je řízená diskuze mezi experty a zadavateli analýzy. Obvykle se této metody účastní 8 až 12 nezávislých expertů. Experti své myšlenky vyjadřují anonymně, tak aby nemohlo docházet k ovlivňování, avšak mohou se navzájem se svými názory seznamovat. [15, 18]
- **Analýza What – If (co se stane když?) -** tato metoda je založena na metodě brainstorming. Základní otázkou při debatě je otázka: „Co se stane když…?“. Tým se snaží formulovat všechny možné otázky a odpovědi na ně k vybranému problému. [17]
- **Event Tree Analysis – ETA (analýza stromu událostí) –** metoda, která graficky znázorňuje možné výsledky, které můžou způsobit události. Výsledkem je posloupnost událostí, které mohou vést k havarijnímu stavu. [17]
- **Hazard Operation Process – HAZOP (analýza ohrožení a provozuschopnosti) –** tato metoda slouží k identifikaci a hodnocení nebezpečí. Principem a postupy se zabývá norma ČSN IEC 61882. Základem metody využito tzv. klíčových slov. [17]

4.3 Popis metody KARS

Metoda KARS neboli kvalitativní analýza rizik a jejich souvztažností, vypracoval a prezentoval Ing. Štefan Pacinda, Ph.D. ve své disertační práci, kterou v roce 2007 obhájil na Universitě Obrany v Brně. Disertační práce má názvem *„Analýza rizik, jeden ze základních nástrojů krizového managementu při řešení nevojenských krizových situací“*. Ing. Pacinda tuto metodu vytvořil z důvodu, že žádná jiná metoda, neřešila prioritu řešení rizik, tedy která rizika řešit prvotně a která následně.

Vzhledem k tomu, že žádný systém neovlivňuje pouze jedno riziko, může docházet k eskalaci rizik. To můžeme chápat tak, že jedno riziko přímo působí na druhé. Z tohoto důvodu o této metodě hovoříme jako o metodě souvztažnosti rizik. [16] Detailněji se s metodou KARS seznámíme v praktické části této diplomové práce.

V této kapitole je stručně popsán význam řízení rizik a jsou charakterizovány některé základní pojmy, se kterými se při procesu řízení rizik můžeme setkat. Dále některé metody, které lze využít v procesu řízení rizik. Zvláštní podkapitola je věnována metodě KARS, která je aplikována v praktické části této diplomové práce.

5 SOUČASNÉ TRENDY A PŘÍSTUPY K FYZICKÉ BEZPEČNOSTI OBJEKTU

Současná doba nabízí nepřeberné možnosti v oblasti technických prostředků určených k fyzické bezpečnosti objektu. Objekty lze střežit již daleko před přiblížením potencionálního narušitele. V takovém případě hovoříme o perimetrické ochraně objektu. Plášťová ochrana zajišťuje ochranu samotného objektu v půdorysném prostoru. To lze učinit kamerovými systémy, systémy kontroly vstupu nebo detektory pohybu a jinými detektory. Uvnitř střeženého objektu, lze také kontrolovat a detekovat narušení. Opět zde můžeme nalézt kamerový systém, detektory pohybu, systémy kontroly vstupu apod. Uvnitř se také můžeme setkat s personálem, který má úkoly podobné povahy, jako výše uvedené technické prostředky, případně tyto technické prostředky ke své činnosti využívají. V následujících podkapitolách jsou popsány některé technické prostředky určené k podpoře fyzické bezpečnosti a jsou popsány pojmy jako fyzická ochrana a ostraha. V dalších podkapitolách jsou stručně charakterizovány jednotlivé prostředky využívané při fyzické ochraně objektu.

5.1 Poplachové zabezpečovací a tísňové systémy – PZTS

Tyto systémy jsou primárně určeny k detekci a hlášení o nežádoucím vniknutí do střeženého objektu. Současné moderní systémy dokáží také informovat i o jiných zdrojích nebezpečí, jako jsou například úniky plynu, vody nebo mohou vysílat tísňová hlášení, např. při přepadení. [3]

Normy v souvislosti PZTS:

- **ČSN EN 50131-1 ed. 2** - Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 1: Systémové požadavky,
- **ČSN CLC/TS 50131-7** - Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 7: Pokyny pro aplikace,
- **TNI 33 4591-1**: část 1 návrh systému PZTS – návrh systému, bezpečnostní posouzení, obsah projektové dokumentace, značky a zkratky pro projektování, vzorové zabezpečení objektu,
- **TNI 33 4591-2**: část 2 montáž PZTS – montáž systému – ústředny, napájecí zdroj, ovládací zařízení, detektory, signalizační zařízení, kabeláž,

- **TNI 33 4591-3**: část 3 uvedení PZTS do provozu a jeho následný provoz, údržba a servis prohlídka systému, funkční zkouška, revize elektrického zařízení, proškolení obsluhy, zkušební provoz, pravidelná kontrola a údržba,
- **ČSN EN 50131-6 ed. 2** - Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 6: Napájecí zdroje,
- **ČSN EN 50131-3** - Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 3: Ústředny. [19]

Základní prvky systému PZTS:

- **Ústředna** – vyhodnocuje stavy a signály z připojených detektorů v reálném čase a na základě těchto signálů a stavů provádí předem nastavené scénáře (vyhlášení poplachu, odeslání zpráv apod.).
- **Přenosové prostředky –** mezi přenosové prostředky můžeme zařadit GSM komunikátory, komunikátory se sítí LAN, s telefonní sítí apod. Slouží k propojení mezi ústřednou a dohledovým příjímacím a poplachovým centrem.
- **Detektory** – detektory jsou zařízení, které na základě vyhodnocení fyzikálních změn ve střeženém prostoru odesílají signály do ústředny, ve které jsou signály zpracovány a vyhodnocovány.
- **Hlásiče** – mají za úkol informovat o narušení střeženého prostoru. Hlásiče můžou být akustické (sirény) nebo optické (majáky) nebo kombinované.
- **Ovládací zařízení** – jsou zejména klávesnice a klíčenky, které slouží k ovládání systému. Můžou sloužit k zastřežení nebo odstřežení objektu, nastavení předání informací o stavu systému. [20]

5.2 Mechanické zábranné systémy – MZS

Mechanické zábranné systémy jsou základním prvkem ochrany objektů. Mechanické zábranné systémy jsou takové systémy, které svou konstrukcí stěžují vniknutí nepovolané osoby do chráněného prostoru. Především se jedná o oplocení, okenní a dveřní výplně objektu, čímž poskytují ochranu tím, že tvoří překážku nebo kladou narušiteli odpor.

V oblasti MZS rozlišujeme:

- **Obvodová ochrana** zajišťuje ochranu kolem střeženého objektu. Ve většině případů se jedná o pevnou mechanickou zábranu, která je vyrobena pro tento účel.
- **Plášťová ochrana** svým účelem znesnadňuje případnému narušiteli vniknutí do střeženého objektu prostřednictvím vstupních otvorů, a to jak cestou vstupních dveří, oken, balkónových dveří, ale i střešních oken a dalších staveních otvorů, kterými je možné do střeženého objektu proniknout.
- **Předmětová ochrana** chrání zejména cennosti, dokumenty mající zvláštní význam, utajované informace, a to zejména před neoprávněným nakládáním případně odcizením. Mezi technické prostředky předmětové ochrany řadíme zejména trezory. [21]

Některé mechanické zábranné prvky:

- Zámky,
- Mříže,
- Bezpečnostní dveře a kování,
- Rolety,
- Bezpečnostní folie na okenních tabulích,
- Trezory a bezpečnostní skříně.

Každý zábranný systém je překonatelný. Je to vždy jen otázka času, prostředků a energie, kterou potřebuje případný narušitel k překonání takových mechanických zábranných systémů. Tím je dána úroveň bezpečnosti objektu. V této souvislosti se s odolností mechanického zábranného systému užívá pojem ***průlomová odolnost.*** [21]

Průlomová odolnost[19] – „*Doba, kterou musí pachatel vynaložit na překonání mechanické pevnosti MZS“.*

[19] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management. Zlín: Radim Bačuvčík - VeRBuM, 2015, s. 254, ISBN 978-80-87500-57-6.

Některé normy v oblasti MZS:

- **ČSN 91 6010** - Úschovné objekty. Zkušební metody a klasifikace odolnosti proti vloupání. Skříňové a komorové trezory,
- **ČSN EN 1627** - Dveře, okna, lehké obvodové pláště, mříže a okenice – odolnost proti vloupání – Požadavky a klasifikace,
- **ČSN EN ISO 12543-2** - Sklo ve stavebnictví – Vrstvené sklo a vrstvené bezpečnostní sklo – Část 2: Vrstvené bezpečnostní sklo,
- **ČSN EN ISO/IEC 17067** - Posuzování shody – Základní principy certifikace produktu a směrnice pro certifikační schémata,
- **ČSN EN 1143-1** - Bezpečnostní úschovné objekty – Požadavky, klasifikace a metody zkoušení odolnosti proti vloupání – Část 1: Skříňové trezory, ATM trezory, trezorové dveře a komorové trezory,
- **ČSN EN 1143-2** - Bezpečnostní úschovné objekty – Požadavky, klasifikace a metody zkoušení odolnosti proti vloupání – Část 2: Depozitní systémy,
- **ČSN 91 6012** - Bezpečnostní úschovné objekty – Požadavky, klasifikace a metody zkoušení odolnosti proti vloupání – Trezory se základní bezpečností.

5.3 Kamerové systémy – CCTV/VSS[20]

Kamerové systémy, jsou dnes již dostupným technickým řešením vzdáleného pozorování střeženého objektu. Kamerové systémy jsou také určitým druhem prevence před případným neoprávněným vniknutím do střeženého objektu. Kamerové systémy můžeme rozdělit dle principu snímaní záznamu, a to na analogové a digitální kamerové systémy. V dnešní době jsou hodně rozšířené IP kamerové systémy. Což jsou digitální kamerové systémy, které pro přenos videosignálu využívají síť Ethernet. Toto umožňuje budování rozsáhlých kamerových systému. Výhodou může být i jednoduchá prostupnost do sítě internet a možnost napájení kamerových jednotek prostřednictvím sítě Ethernet tzv. PoE[21] injektorem.

[20] CCTV/VVS – Closed-circuit television / Video Surveillance Systems
[21] PoE – Power over Ethernet – napajení po síti ethernet

Základní prvky kamerových systémů:

- **Kamera (snímací prvek) –** jedná se o základní prvek všech kamerových systémů. Úlohou kamer v kamerovém systému je přímé pozorování a zpracování signálu na videosignál, který je dále přenášen prostřednictvím přenosových prostředků a dále zpracováván, ukládán nebo zobrazován.

  Při výběru kamer můžeme volit mezi kamerami vnitřními a vnějšími, podle zvoleného umístnění. Dále si můžeme vybrat na základě mnoha dalších parametrů kamer. Ať už podle způsobu zpracování signálu (analogové, digitální, IP, HD-SDI), rozlišení v pixelech, světelná citlivost, velikost a druhu snímacího prvku nebo dle provozního napětí. Vše záleží na výběru vhodného typu kamery dle jejího použití.
- **Objektiv –** jedná se o soustavu čoček, která pomáhá vytvořit obraz snímané scény, který je dále zpracováván snímacím zařízením. Objektivy v oblasti CCTV volíme dle principu činnosti jeho uzávěrky. Buď to na mechanicky ovládanou záběrku nebo elektronickou závěrku. Dále můžeme objektivy rozdělit podle šířky úhlu záběru na širokoúhlé nebo zoom objektivy, které umožňují snímat obraz na větší vzdálenost, avšak za cenu užšího úhlu záběru. Dalším základním měřítkem ve volbě objektivu je jeho světelnost. Světelnost objektivu představuje schopnost propustit světlo skrze soustavu čoček na snímací prvek. U zoom objektivů se s narůstajícím přiblížením zhoršuje schopnost objektivu propouštět světlo.
- **Záznamové zařízení –** záznamové zařízení slouží k ukládání videozáznamu k pozdějšímu využití. V případě větších kamerových záznamů jsou často zaznamenávány jen zájmové videosekvence, které byly vybrány na základě nějakého podnětu např. změna ve snímaném obraze, alarm, detekce narušení.
- **Přenosové prostředky** – přenos mezi kamerou a záznamovým př. zobrazovacím zařízením lze realizovat jak drátově, tak i bezdrátově. U starších analogových kamer je přenos realizován pomocí koaxiálního kabelu. U novějších digitálních kamer může být přenos realizován přes datovou síť ethernet nebo speciální koaxiální kabely v případě HD-SDI rozhraní.
- **Zobrazovací jednotky –** jsou převážně monitory a u větších kamerových systémů potom televizní stěny a projektory.

Normy upravující provoz a instalaci kamerových systému:

- **ČSN EN 50130-4 ED.2** - Poplachové systémy – Část 4: Elektromagnetická kompatibilita – Norma skupiny výrobků: Požadavky na odolnost komponentů požárních systémů, poplachových zabezpečovacích a tísňových systémů a systémů CCTV, kontroly vstupu a přivolání pomoci,
- **ČSN EN 62676-1-1** - Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 1-1: Systémové požadavky – Obecně,
- **ČSN EN 62676-1-2** - Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 1-2: Systémové požadavky – Výkonové požadavky na video přenos,
- **ČSN EN 62676-2-1 -** Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 2-1: Video přenosové protokoly – Obecné požadavky,
- **ČSN EN 62676-2-2** - Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 2-2: Video přenosové protokoly – Implementace vzájemné spolupráce IP systémů založených na využití HTTP a REST,
- **ČSN EN 62676-2-3** - Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 2-3: Video přenosové protokoly – Implementace vzájemné spolupráce IP systémů založené na síťových (web) službách,
- **ČSN EN 62676-3** - Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 3: Analogové a digitální video rozhraní,
- **ČSN EN 62676-4** - Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 4: Pokyny pro aplikace,
- **ČSN EN IEC 62676-5** - Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 5: Specifikace dat a kvalita obrazu pro kamerová zařízení (s účinností od 04/2019).

5.4 Systémy kontroly vstupu – ACCESS

Systém kontroly vstupu je dalším druhem způsobu zajištění ochrany střeženého objektu nebo prostoru. Systém kontroly vstupu umožňuje oprávněným osobám vstup a opuštění chráněného prostoru. Dále může být tento systém integrován do dalších systému organizace, jako je např. evidence docházky, kamerový systém, systém PZTS, případně další aplikace. [21]

Základní prvky systému kontroly vstupu:

- **Řídící jednotka** – jedná se o elektronické zařízení, které vyhodnocuje informace ze snímačů (čteček karet) a na základě přidělených oprávnění umožní, držiteli karty vstup do chráněného prostoru prostřednictvím ovládaného zařízení.
- **Snímače** – snímače systémů kontroly vstupu jsou zpravidla čtečky karet, čtečky biometrických údajů nebo klávesnice. Tyto snímače čtou informace z identifikačních karet, načítají biometrické údaje nebo snímají číselné kombinace a pomocí přenosových prostředků (sběrnic, kabeláže) odesílají tyto informace do řídících jednotek.
- **Ovládané zařízení** – jedná se o zařízení jako jsou elektromagnetické zámky, turnikety, závory apod.
- **Server se softwarem** – v případě rozsáhlých objektů u kterých je systém kontroly vstupu instalován, jsou jednotlivé přístupové údaje nahrány v databázi softwaru, který umožňuje správu, monitoring přístupového systému. [21]

Normy u systému kontroly vstupu:

- **ČSN EN 60839-11-1** - Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty,
- **ČSN EN 60839-11-2** - Poplachové a elektronické bezpečnostní systémy – Část 11-2: Elektronické systémy kontroly vstupu – Pokyny pro aplikace,
- **ČSN EN 60839-11-31** - Poplachové a elektronické bezpečnostní systémy – Část 11-31: Elektronické systémy kontroly vstupu – Implementace IP interoperability na základě webových služeb – Základní specifikace,
- **ČSN EN 60839-11-32** - Poplachové a elektronické bezpečnostní systémy – Část 11-32: Elektronické systémy kontroly vstupu – Implementace IP interoperability na základě webových služeb – Specifikace systému kontroly vstupu.

Toto byl stručný přehled základních technických prostředků, které lze využít pro střežení chráněného objektu. Tím, že jsou tyto systémy do jisté míry autonomní, tudíž nepotřebují, 24hodinový dohled personálu, jsou výrazně levnější na provoz než systémy s nutnou fyzickou přítomností obsluhujícího personálu. Na druhou stranu je nutné také brát v úvahu, že se ve většině případu jedná, jen o elektrická zařízení, která mají své limity a k bezchybnému provozu, potřebují obslužný personál. Kamerový systém dokáže odhalit

případného narušitele, ale bez údržby, dohledového aparátu a zásahové jednotky pak takový kamerový systém jen dohlíží na narušení a pokud se jedná o technicky zastaralé typy kamer, s nízkým rozlišením, je v případě usvědčení pachatele k ničemu. Také systémy PZTS, které varují o narušení, prostřednictvím signálů a zpráv budou bez zajištění včasného zásahu jen preventivním opatřením.

5.5 Fyzická ostraha objektu

Fyzická ostraha objektu, je dalším druhem ochrany, kde svou nezastupitelnou roli hraje lidská síla. Jedná se tedy o přímou fyzickou ostrahu, kterou provádí vyškolená a vycvičená osoba. Touto činností se v dnešní době zabývá mnoho soukromých bezpečnostních složek. Způsobů provádění fyzické ostrahy objektu je několik.

Nejčastěji je fyzická ostraha prováděna formou:

- Strážní služby – kdy může být formou pevných stanovišť, případně pochůzková strážní služba. Cílem je zabránit případnému narušení nebo neoprávněné činnosti.
- Propustkové služby – tato forma ochrany, zabraňuje vstupu, vjezdu nebo naopak odjezdu a odchodu bez příslušných oprávnění. Dále tento druh ochrany, zabraňuje vnášení nebo vynášení materiálu např. z výrobních prostor.
- Bezpečnostní dohled – je zajišťován personálem fyzické ostrahy přímo v objektu nebo prostoru okolo objektu, který dohlíží na dodržování vnitřních pravidel v objektu, dále výkon doprovodu osob a dozor nad vykonávanými pracemi.
- Bezpečnostní průzkum – jedná se o přímou nebo vzdálenou kontrolu prostor, prostřednictvím elektronických systémů.
- Bezpečností výjezd – zde se jedná o reakci na signály elektronických zabezpečovacích systému a informace z DPPC[22] o narušení střeženého objektu. [22]

[22] DPPC – Dohledové a poplachové přijímací centrum (dříve PCO – pult centrální ochrany)

Dále můžeme fyzickou ostrahu členit z hlediska času:

- Ostraha vázaná na pracovní dobu (taková ostraha je prováděna pouze v pracovní době),
- nepřetržitá ostraha (je prováděna celých 24 hodin),
- nárazová ostraha (ostraha je využívaná dle potřeb organizace).

Další způsoby rozdělení fyzické ostrahy můžou být z pohledu toho, zda je fyzická ostraha prováděna otevřeně nebo skrytě, se zbraní nebo bez zbraně, nebo zda pracovníci ostrahy při své práci využívají vycvičených psů. Otevřená, nebo také veřejná fyzická ostraha, je taková ostraha, kdy jsou pracovníci viditelně označeni jako ostraha např. stejnokrojem. [23]

Při své činnosti, zejména při zákrocích proti případným narušitelům střeženého objektu, vychází pracovník ostrahy z obecně platných zákonů. V současné době neexistuje žádná komplexní norma, které by práva a povinnosti pracovníka fyzické ostrahy upřesňovala.

Obecné zákony a ustanovení, kterými se musí pracovník fyzické ostrahy řídit jsou např.:

- Zákon č. 89/2012 Sb. Občanský zákoník,
- Zákon č. 40/2009 Sb. Trestní zákoník,
- Zákon č. 141/1969 Sb. Trestní řád,
- Zákon č. 119/2002 Sb. O zbraních a střelivu.

Tato kapitola nastínila možnosti zabezpečení bezpečnosti objektů, a to jak z pohledu technických prostředků, tak i z pohledu využití fyzické ostrahy. V jednotlivých kapitolách jsou také vyjmenovány právní prameny a normy, které se danou oblastí zabývají.

5.6 Shrnutí teoretické části

Cílem teoretické části této diplomové práce, bylo shrnout právní prameny, které se zabývají ochranou utajovaných informací v České republice. Z pohledu zákona č. 412/2005 Sb. o ochraně utajovaných informací a bezpečnostní způsobilosti, byly shrnuty jednotlivé druhy bezpečností, se kterými při ochraně utajovaných informací pracuje. V dalších kapitolách jsou popsány instituce v České republice, které se ochranou utajovaných informací zabývají. Poslední kapitoly v teoretické části, se věnují řízení rizik a charakteristikou jednotlivých přístupů k technickému a fyzickému přístupu při zajištění fyzické ostrahy a bezpečnosti objektu.

II. PRAKTICKÁ ČÁST

6 ANALÝZA RIZIK VE VZTAHU K OCHRANĚ UTAJOVANÝCH INFORMACÍ

Analýza rizik je hojně využívanou manažerskou metodou, která slouží k identifikaci rizik, dopadů a určením způsobů, jak zmírnit působení rizik nebo jejich eliminaci. V případě této diplomové práce, se analýza rizik vztahuje na oblast ochrany utajovaných informací.

6.1 Analýza rizik z hlediska zákona 412/2005 Sb. a vyhlášky č. 528/2005 Sb.

Z pohledu zákona č. 412/2005 Sb. a provázejících vyhlášek, zejména vyhlášky č. 528/2005 Sb., se vyskytuje pojem **„riziko“,** v souvislosti ověřování opatření fyzické bezpečnosti a pojem „**vyhodnocení rizik“** v § 10 této vyhlášky. Zde je stanoveno, že vyhodnocení rizik se provádí:

„*identifikací stupňů utajovaných informací a zjištěním množství utajovaných informací, které se v objektu vyskytují nebo budou vyskytovat, zejména z hlediska následku jejich vyzrazení nebo zneužití, popisem a vyhodnocením hrozeb, kterým jsou tyto utajované informace vystaveny, popisem a vyhodnocením zranitelnosti utajovaných informací vůči těmto hrozbám, stanovením míry rizika, jako "malé", "střední" nebo "velké", na základě vyhodnocení hrozeb a zranitelnosti utajovaných informací*.“ [23]

Z textu tohoto ustanovení je patrné, že analýza rizik může probíhat jednoduchou bodovou analýzou. Metodou bodového hodnocení následku, hrozby a zranitelnosti. Tím získáme pro jednotlivá rizika, míru jejich rizika.

$$\boldsymbol{mR = NxHxZ} \qquad \textbf{(1)}$$

kde:

mR … míra rizika {malé, střední, velké}

N… následek (dopad) v rozsahu {1–V, 2–D, 3–T, PT}

[23] § 10 - Ověřování opatření fyzické bezpečnosti a vyhodnocení rizik, vyhlášky č. 528/2005 Sb. v platném znění

H… hrozba v rozsahu {1, 2, 3}

Z … zranitelnost v rozsahu {1, 2, 3}

Z teoretické části diplomové práce, víme, jaké náležitosti musí mít informace, aby se dala klasifikovat jako utajovaná. Víme že, její vyzrazení, nebo zneužití může být pro zájmy ČR nevýhodné, nebo může způsobit újmu. Výše újmy nebo nevýhodnosti můžeme kategorizovat příslušnými stupni utajení. Nejnižší škodu při vyzrazení nebo zneužití způsobí utajovaná informace stupně Vyhrazené, naopak nejvyšší škodu způsobí vyzrazení utajované informace stupně Přísně tajné. Následek tedy můžeme určit podle toho na jakou kategorii utajované informace působí hrozba. V tomto případě, kdy je prováděno vyhodnocení rizik pouze pro stupeň utajení Důvěrné, nemá hodnota ve sloupci „**Následek“**, zásadní vliv na výsledek stanové míry rizika, proto ani nebude uveden.

Požadavek na provedení analýzy rizik je vyhláškou[24] stanoven pouze u kategorie stupně utajení Důvěrné a vyšší a pokud provádíme vyhodnocení rizik pro objekt, ve kterém se nachází zabezpečené oblasti kategorie Vyhrazené a Důvěrné, musí být splněny požadavky pro kategorii s vyšším stupněm. Není tedy relevantní provádět vyhodnocení zvlášť pro kategorii Důvěrné a zvlášť pro kategorii Vyhrazené, i když v tomto případě to zákon ani vyhláška nevyžaduje.

Tab. 2 Rozšířený katalog rizik – vyhodnocení rizik [zdroj: vlastní]

	Riziko	**Z**	**H**	**mR**
40	Zpracování UI mimo zabezpečenou oblast	3	2	6
41	Zpracování UI na nezabezpečeném PC	3	2	6
1	Přístup k UI neoprávněnou osobou	3	2	6
2	Nedodržení stanovených postupů	3	2	6
8	Chybné stanovení stupně utajení	3	2	6
9	Chybné uložení utajované informace	2	3	6
12	Neúmyslné vyzrazení UI	3	2	6
13	Úmyslné vyzrazení UI	2	3	6
14	Ztráta, zničení přidělené UI	3	2	6

[24] Vyhláška č. 528/2005 Sb. fyzické bezpečnosti a certifikaci technických prostředků

	Riziko	Z	H	mR
20	Nesprávné nebo neoprávněné pořízení kopii, opisů	3	2	6
22	Ukládání UI mimo zabezpečené oblasti	3	2	6
23	Použití necertifikovaných prostředků	3	2	6
25	Vniknutí zloděje	3	2	6
27	Umožnění vstupu neoprávněné FO, PO	2	3	6
35	Odeslání UI nezabezpečeným kanálem	3	2	6
3	Nedostatečné proškolení	2	2	4
4	Neověření oprávnění přístupu k UI	2	2	4
7	Neoznámení změn uvedených v žádosti	2	2	4
21	Nedostatky v realizaci opatření projektu FB	2	2	4
36	Užití cizí identity v IS	2	2	4
37	Výpadek HW	2	2	4
38	Výpadek SW	2	2	4
42	Zpracování UI na sestavě pro nižší stupeň utajení	2	2	4
6	Nepředložení dokladů ke znovu ověření přístupu k UI	1	3	3
15	Neoprávněné zrušení stupně utajení	1	3	3
16	Nesprávné uvedení nebo opomenutí náležitostí UI	1	2	2
17	Nesprávné přenášení – přeprava UI	1	2	2
18	Nedodržení postupu při skartačním řízení	1	2	2
19	Chybný postup při zapůjčování UI	1	2	2
24	Použití nesprávných MZS	2	1	2
28	Nesprávné používání technických prostředků	2	1	2
30	Nesprávná manipulace s klíči od vstupu do ZO (ztráta)	2	1	2
31	Nízká úroveň zabezpečení IS	2	1	2
39	Vyzrazení uživatelského hesla	2	1	2
10	Nezaevidování UI v administrativní pomůcce	2	1	2
11	Používání nezaevidovaných pomůcek	2	1	2
26	Přírodní havárie a katastrofy	2	1	2
29	Nedodržení pravidel pro pohyb osob a vozidel v objektu a ZO	1	2	2
32	Kompromitace IS	1	2	2
5	Neúčast nebo formální proškolení 1x ročně	1	1	1
33	Nesprávná politika hesel	1	1	1
34	Nezajištění HDD při servisu	1	1	1

Z uvedeného katalogu, bylo vybráno 23 nejvýznamnějších rizik, pro provedení následné analýzy metodou KARS.

6.2 Analýza rizik metodou KARS

Jak již bylo napsáno v teoretické části této diplomové práce, metodu KARS, prezentoval ve své disertační práci, Ing. Štefan Pacinda, Ph.D. na univerzitě obrany v Brně. Principem této analýzy spočívá v posouzení vzájemného působení rizik mezi sebou, tzv. souvztažnosti rizik.

6.2.1 Postup řešení metodou KARS

Samotný postup při analýze rizik metodou KARS zahrnuje následující kroky:

1. Identifikace rizik
2. Sestavení tabulky souvztažností
3. Vyplnění tabulky souvztažností
4. Výpočet koeficientů aktivity a pasivity
5. Sestavení grafu a určení kvadrantů významnosti

Ad 1) Identifikace rizik – identifikace a popis jednotlivých rizik představuje nejdůležitější, a nejnáročnější část celé analýzy. Přesnost a správnost identifikace a popis záleží na zkušenostech řešitele, případně na konkrétnosti zadání. Po identifikaci a popisu rizik je sestaven katalog rizik.

Katalog rizik představuje výčet možných ohrožení, z hlediska konkrétních oblastí bezpečnosti. Pro potřeby analýzy rizik metodou KARS bylo vybráno 23 nejvýznamnějších rizik.

Z těchto rizik, byla sestavena tabulka, dle oblastí bezpečnosti. Vzhledem k tomu, že ochrana utajovaných informací, je souborem jednotlivých druhů bezpečnosti, byla analýza prováděna komplexně, napříč všemi oblastmi bezpečnosti.

Tab. 3 Tabulka rizik pro analýzu KARS [zdroj: vlastní]

Personální bezpečnost	Přístup k UI neoprávněnou osobou
	Nedodržení stanovených postupů
	Nedostatečné proškolení
	Neověření oprávnění přístupu k UI
	Neoznámení změn uvedených v žádosti
Administrativní bezpečnost	Chybné stanovení stupně utajení
	Chybné uložení utajované informace
	Neúmyslné vyzrazení UI
	Úmyslné vyzrazení UI
	Ztráta, zničení přidělené UI
	Nesprávné nebo neoprávněné pořízení kopii, opisů
Fyzická bezpečnost	Nedostatky v realizaci opatření projektu FB
	Ukládání UI mimo zabezpečené oblasti
	Použití necertifikovaných prostředků
	Vniknutí zloděje
	Umožnění vstupu neoprávněné FO, PO
Bezpečnost informačních a komunikačních systémů	Odeslání UI nezabezpečeným způsobem
	Užití cizí identity v IS
	Výpadek HW
	Výpadek SW
	Zpracování UI mimo zabezpečenou oblast
	Zpracování UI na nezabezpečeném PC
	Zpracování UI na sestavě pro nižší stupeň utajení

Ad 2) Sestavení tabulky souvztažností – sestavená tabulka přestavuje výčet jednotlivých rizik, se kterými můžeme dále pracovat. První sloupec určuje pořadové číslo rizika. Druhý sloupec její popis. Do prvního řádku transformujeme počet rizik z vertikálního směru na horizontální a získáme kompletní tabulku. V tomto případě je zde 23 rizik, což představují řádky **i** a ten stejný počet sloupců **j**. Pozice sloupec **i** a řádku **j** je označena $\mathbf{r_{ij}}$. Posledním krokem k sestavení tabulky, je vyřadit hrozby, které nemůžou způsobit samy sebe, tzn. riziko v řádku **i,** nemůže způsobit to stejné riziko, které je uvedeno ve sloupci **j** ($\mathbf{r_{ij} = x}$)**.**

	Riziko	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	Přístup k UI neoprávněnou osobou	X	1	0	0	0	0	0	1	1	1	1	0	0	0	0	0	1	0	0	0	0	0	0
2	Nedodržení stanovených postupů	1	X	1	0	1	1	1	1	1	1	1	1	1	1	0	1	1	1	0	0	1	1	1
3	Nedostatečné proškolení	1	1	X	1	0	1	1	1	0	0	1	1	1	1	0	1	1	0	0	0	1	1	1
4	Neověření oprávnění přístupu k UI	1	1	0	X	1	0	0	1	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0
5	Neoznámení změn uvedených v žádosti	0	1	1	0	X	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
6	Chybné stanovení stupně utajení	0	0	1	0	0	X	1	1	0	0	1	0	1	0	0	0	1	0	0	0	0	0	1
7	Chybné uložení utajované informace	1	1	1	0	0	0	X	0	0	1	0	0	1	0	0	0	1	0	0	0	0	0	0
8	Neúmyslné vyzrazení UI	1	0	1	0	0	0	0	X	0	0	1	0	0	0	0	0	1	1	0	0	0	1	0
9	Úmyslné vyzrazení UI	1	0	0	0	0	0	0	0	X	0	1	0	0	0	0	0	1	1	0	0	0	1	0
10	Ztráta, zničení přidělené UI	1	0	0	0	0	0	0	1	1	X	0	0	0	0	0	0	1	1	0	0	0	0	0
11	Nesprávné nebo neoprávněné pořízení kopii, opisů	1	1	1	1	0	1	1	1	1	1	X	0	1	0	0	0	1	0	0	0	1	1	1
12	Nedostatky v realizaci opatření projektu FB	1	1	0	0	0	0	1	0	0	0	0	X	1	1	1	1	0	0	1	0	1	0	0
13	Ukládání UI mimo zabezpečené oblasti	1	1	1	0	0	0	1	1	1	1	0	0	X	0	0	0	0	0	0	0	0	0	0
14	Použití necertifikovaných prostředků	1	1	1	0	0	0	1	0	0	0	0	1	0	X	1	0	0	0	1	0	0	0	0
15	Vniknutí zloděje	1	0	0	0	0	0	0	0	1	1	1	0	0	0	X	1	0	1	1	1	0	0	0
16	Umožnění vstupu neoprávněné FO, PO	1	0	1	0	0	0	0	1	1	1	1	0	0	0	1	X	0	0	1	0	0	0	0
17	Odeslání UI nezabezpečeným způsobem	1	1	1	0	0	1	1	1	1	1	1	0	1	0	0	0	X	0	0	0	1	1	1
18	Užití cizí identity v IS	1	1	0	0	0	1	1	1	1	1	1	0	0	0	0	0	1	X	0	0	1	1	1
19	Výpadek HW	0	1	0	0	0	0	0	0	0	1	1	0	0	0	0	0	1	1	X	1	1	1	1
20	Výpadek SW	0	1	0	0	0	0	0	1	1	1	1	0	0	0	0	0	1	1	0	X	1	1	1
21	Zpracování UI mimo zabezpečenou oblast	1	1	0	0	0	0	0	1	1	1	1	0	1	0	0	0	1	1	0	0	X	1	1
22	Zpracování UI na nezabezpečeném PC	1	1	1	0	0	0	0	1	1	1	1	0	1	0	0	0	1	0	0	0	1	X	1
23	Zpracování UI na sestavě pro nižší stupeň utajení	1	1	0	0	0	1	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	X

Obr. 2 Sestavená tabulky pro metodu KARS [zdroj: vlastní]

Ad 3) Vyplnění tabulky souvztažností – tento krok spočívá ve vzájemném posouzen rizik. Při vyplňovaní tabulky, se můžeme ptát, zda může riziko v řádku **i,** vyvolat riziko ve sloupci **j.** Pokud existuje reálná možnost, že riziko v řádku **i,** může vyvolat riziko ve sloupci **j,** vyplníme do příslušného pole $\mathbf{r_{ij}}$ číslo **1.** Pokud tato možnost neexistuje, vyplníme číslo **0.** Postupujeme vždy po řádcích zleva doprava. Tímto způsobem vyplníme celou tabulku. Dalším krokem k sestavení kompletní tabulky souvztažností rizik, je provést sečtení výskytů čísel 1 v řádcích a sloupcích. Do tabulky vložíme další sloupec a řádek a popíšeme si jej jako ***součet***. Tím získáme hotovou tabulku souvztažností rizik.

	Riziko	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	Součet
1	Přístup k UI neoprávněnou osobou	X	1	0	0	0	0	0	1	1	1	1	0	0	0	0	0	1	0	0	0	0	0	0	6
2	Nedodržení stanovených postupů	1	X	1	0	1	1	1	1	1	1	1	1	1	1	0	1	1	1	0	0	1	1	1	18
3	Nedostatečné proškolení	1	1	X	1	0	1	1	1	0	0	1	1	1	1	0	1	1	0	0	0	1	1	1	15
4	Neověření oprávnění přístupu k UI	1	1	0	X	1	0	0	1	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	6
5	Neoznámení změn uvedených v žádosti	0	1	1	0	X	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	3
6	Chybné stanovení stupně utajení	0	0	1	0	0	X	1	1	0	0	1	0	1	0	0	0	1	0	0	0	0	0	1	7
7	Chybné uložení utajované informace	1	1	1	0	0	0	X	0	0	1	0	0	1	0	0	0	1	0	0	0	0	0	0	6
8	Neúmyslné vyzrazení UI	1	0	1	0	0	0	0	X	0	0	1	0	0	0	0	0	1	1	0	0	0	1	0	6
9	Úmyslné vyzrazení UI	1	0	0	0	0	0	0	0	X	0	1	0	0	0	0	0	1	1	0	0	0	1	0	5
10	Ztráta, zničení přidělené UI	1	0	0	0	0	0	0	1	1	X	0	0	0	0	0	0	1	1	0	0	0	0	0	5
11	Nesprávné nebo neoprávněné pořízení kopii, opisů	1	1	1	1	0	1	1	1	1	1	X	0	1	0	0	0	1	0	0	0	1	1	1	14
12	Nedostatky v realizaci opatření projektu FB	1	1	0	0	0	0	1	0	0	0	0	X	1	1	1	1	0	0	1	0	1	0	0	9
13	Ukládání UI mimo zabezpečené oblasti	1	1	1	0	0	0	1	1	1	1	0	0	X	0	0	0	0	0	0	0	0	0	0	7
14	Použití necertifikovaných prostředků	1	1	1	0	0	0	1	0	0	0	0	1	0	X	1	0	0	0	1	0	0	0	0	7
15	Vniknutí zloděje	1	0	0	0	0	0	0	0	1	1	1	0	0	0	X	1	0	1	1	1	0	0	0	8
16	Umožnění vstupu neoprávněné FO, PO	1	0	1	0	0	0	0	1	1	1	1	0	0	0	1	X	0	0	1	0	0	0	0	8
17	Odeslání UI nezabezpečeným způsobem	1	1	1	0	0	1	1	1	1	1	1	0	1	0	0	0	X	0	0	0	1	1	1	13
18	Užití cizí identity v IS	1	1	0	0	0	1	1	1	1	1	1	0	0	0	0	0	1	X	0	0	1	1	1	12
19	Výpadek HW	0	1	0	0	0	0	0	0	0	1	1	0	0	0	0	0	1	1	X	1	1	1	1	9
20	Výpadek SW	0	1	0	0	0	0	0	1	1	1	1	0	0	0	0	0	1	1	0	X	1	1	1	10
21	Zpracování UI mimo zabezpečenou oblast	1	1	0	0	0	0	0	1	1	1	1	0	1	0	0	0	1	1	0	0	X	1	1	11
22	Zpracování UI na nezabezpečeném PC	1	1	1	0	0	0	0	1	1	1	1	0	1	0	0	0	1	0	0	0	1	X	1	11
23	Zpracování UI na sestavě pro nižší stupeň utajení	1	1	0	0	0	1	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	X	7
	Součet	18	16	11	2	2	6	9	15	13	14	16	3	9	3	3	6	14	8	4	2	9	10	10	

Obr. 3 Vyplněná tabulka souvztažností [zdroj: vlastní]

Ad 4) Výpočet koeficientů aktivity a pasivity – koeficienty aktivity a pasivity představují procentuální vyjádření počtu návazných rizik, která mohou být nebo mohou vyvolat následné riziko. Zde hraje roli počet kombinací **x**, kde může jedno riziko vyvolat riziko další, ale ne samo sebe. Z toho vyplívá že počet kombinací **x** je dán vztahem: [16]

$$\boldsymbol{x - 1}$$

Koeficient aktivity – procentuální vyjádření počtu návazných rizik, která mohou být vyvolána v případě, že nastane riziko v řádku **i.** To vypočítáme následujícím vzorcem: [16]

$$\boldsymbol{K_{ARi} = \frac{\sum 1\, Ri}{x - 1} \times 100}\ [\%] \qquad \textbf{(2)}$$

kde:

$\boldsymbol{K_{ARi}}$ **…** koeficient aktivity rizika

$\boldsymbol{\sum 1\, Ri}$ **…** součet jedniček v řádku rizika **i**

Koeficient pasivity – procentuální vyjádření počtu rizik pro riziko **i**, která mohou následně vyvolat riziko **i**. [16]

$$\boldsymbol{K_{PRi} = \frac{\sum \mathbf{1}\, Rj}{x - 1} \times 100}\ [\%] \qquad \textbf{(3)}$$

kde:

$\boldsymbol{K_{PRi}}$ **…** koeficient pasivity rizika

$\boldsymbol{\sum 1\, Ri}$ **…** součet jedniček ve sloupci rizika **j**

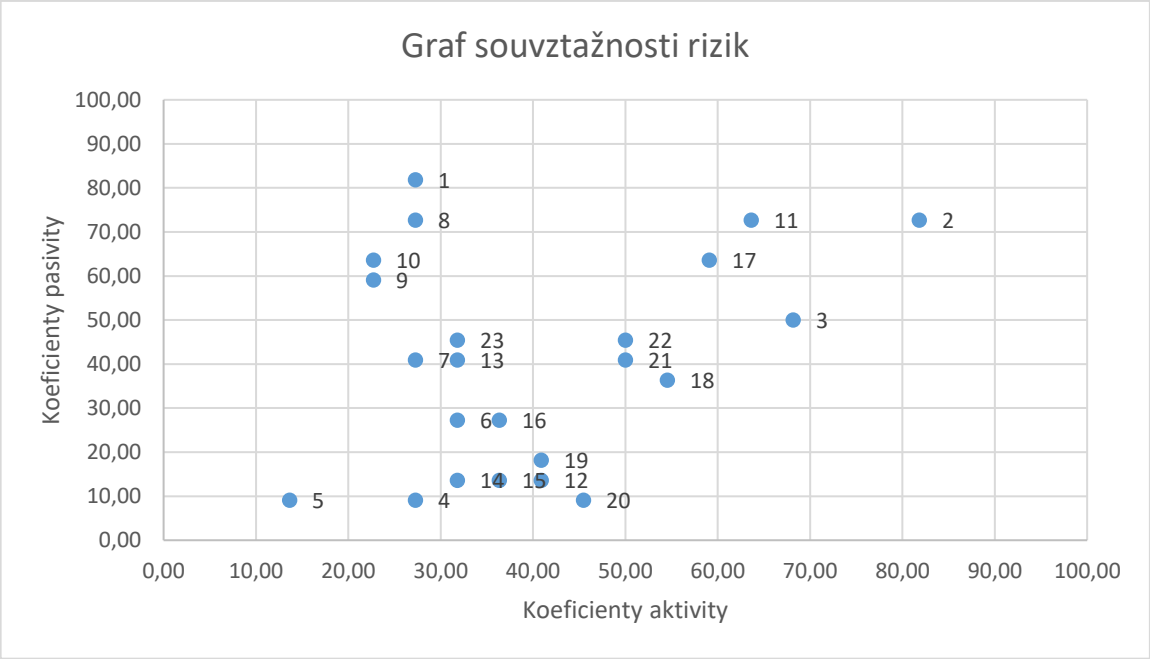
Pro výpočet koeficientů aktivity a pasivity vytvoříme další, pomocnou tabulku a vypočítáme koeficienty pro jednotlivá rizika. Tyto poté představují souřadnice bodů rizik v grafu.

Tab. 4 Tabulka s koeficienty aktivity a pasivity [zdroj: vlastní]

Riziko	KA	KP
Přístup k UI neoprávněnou osobou	27,27	81,82
Nedodržení stanovených postupů	81,82	72,73
Nedostatečné proškolení	68,18	50,00
Neověření oprávnění přístupu k UI	27,27	9,09
Neoznámení změn uvedených v žádosti	13,64	9,09
Chybné stanovení stupně utajení	31,82	27,27
Chybné uložení utajované informace	27,27	40,91
Neúmyslné vyzrazení UI	27,27	72,73
Úmyslné vyzrazení UI	22,73	59,09
Ztráta, zničení přidělené UI	22,73	63,64
Nesprávné nebo neoprávněné pořízení kopii, opisů	63,64	72,73
Nedostatky v realizaci opatření projektu FB	40,91	13,64
Ukládání UI mimo zabezpečené oblasti	31,82	40,91
Použití necertifikovaných prostředků	31,82	13,64
Vniknutí zloděje	40,91	13,64
Umožnění vstupu neoprávněné FO, PO	36,36	27,27
Odeslání UI nezabezpečeným způsobem	59,09	63,64
Užití cizí identity v IS	54,55	36,36
Výpadek HW	40,91	18,18
Výpadek SW	45,45	9,09
Zpracování UI mimo zabezpečenou oblast	50,00	40,91
Zpracování UI na nezabezpečeném PC	50,00	45,45
Zpracování UI na sestavě pro nižší stupeň utajení	31,82	45,45

S vyplněnou tabulkou koeficientů aktivity a pasivity můžeme sestrojit výsledný graf.

Ad 5) Sestavení grafu a určení oblastí významnosti – sestavení grafu souvztažností rizik, docílíme vynesením jednotlivých hodnot koeficientů aktivity a pasivity na osy **x** a **y** v kartézském souřadnicovém systému. Osa **x** představuje hodnoty koeficientů aktivity a osa **y** hodnoty koeficientů pasivity.



Obr. 4 Graf souvztažnosti rizik [zdroj: vlastní]

Pro lepší orientaci v grafu a následnou analýzu rizik, graf rozdělíme pomocí osy O_1 a O_2 na čtyři oblasti.

I. Oblast – **primárně** i **sekundárně** nebezpečná rizika
II. Oblast – **sekundárně** nebezpečná rizika
III. Oblast – **primárně** nebezpečná rizika
IV. Oblast – **relativně** bezpečná rizika

Dále je nutné stanovit významnost zobrazených rizik. Rizika s nejvyšší hodnotou koeficientů aktivity a pasivity, jsou rizika, která bychom měli řešit primárně. Řekněme, že chceme v I. oblasti grafu zobrazit 80 % rizik.

Pro osu O_1, která je rovnoběžnou s osou **y** grafu, musíme znát maximální a minimální hodnotu ze všech hodnot koeficientů aktivity.

Abychom pokryli 80 % z uvedených rizik, musíme získat hodnotu bodu pro osu **O1** z následujícího vztahu:

$$\boldsymbol{O_1 = \max(K_A) - \frac{\left(\max(K_A) - \min(K_A)\right)}{100} \times 80} \quad \textbf{(4)}$$

kde:

O_1 … osa O_1

$\max(K_A)$… maximální hodnota z koeficientů aktivity

$\min(K_A)$ … minimální hodnota z koeficientů aktivity

Analogicky získáme hodnotu bodu pro osu **O2** ze vztahu:

$$\boldsymbol{O_2 = \max(K_P) - \frac{\left(\max(K_P) - \min(K_P)\right)}{100} \times 80} \quad \textbf{(5)}$$

kde:

O_2 … osa O_2

$\max(K_P)$… maximální hodnota z koeficientů pasivity

$\min(K_P)$ … minimální hodnota z koeficientů pasivity

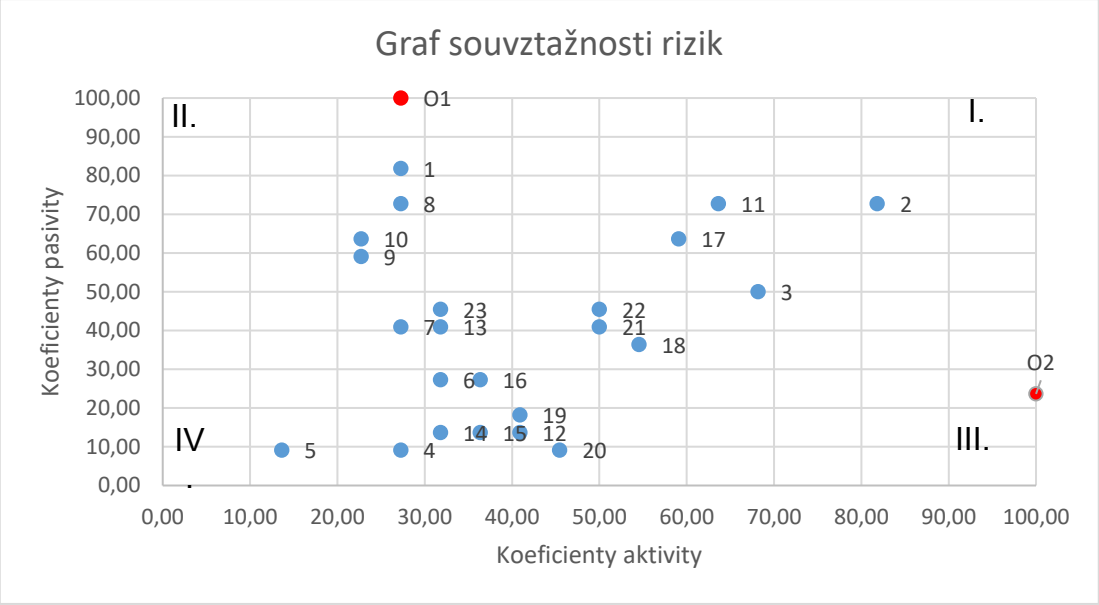
Do těchto vzorců dosadíme maximální a minimální hodnoty koeficientů aktivity a pasivity a získáme hodnoty bodů osy **O1** a **O2**.

$$\boldsymbol{O_1 = \max(K_A) - \frac{(\max(K_A) - \mathrm{min}(K_A))}{100} \times 80 = 81,82 - \frac{(81,82 - 13,64)}{100} \times 80 = 22,27}$$

$$\boldsymbol{O_2 = \max(K_P) - \frac{(\max(K_P) - \mathrm{min}(K_P))}{100} \times 80 = 81,82 - \frac{(81,82 - 9,09)}{100} \times 80 = 23,63}$$

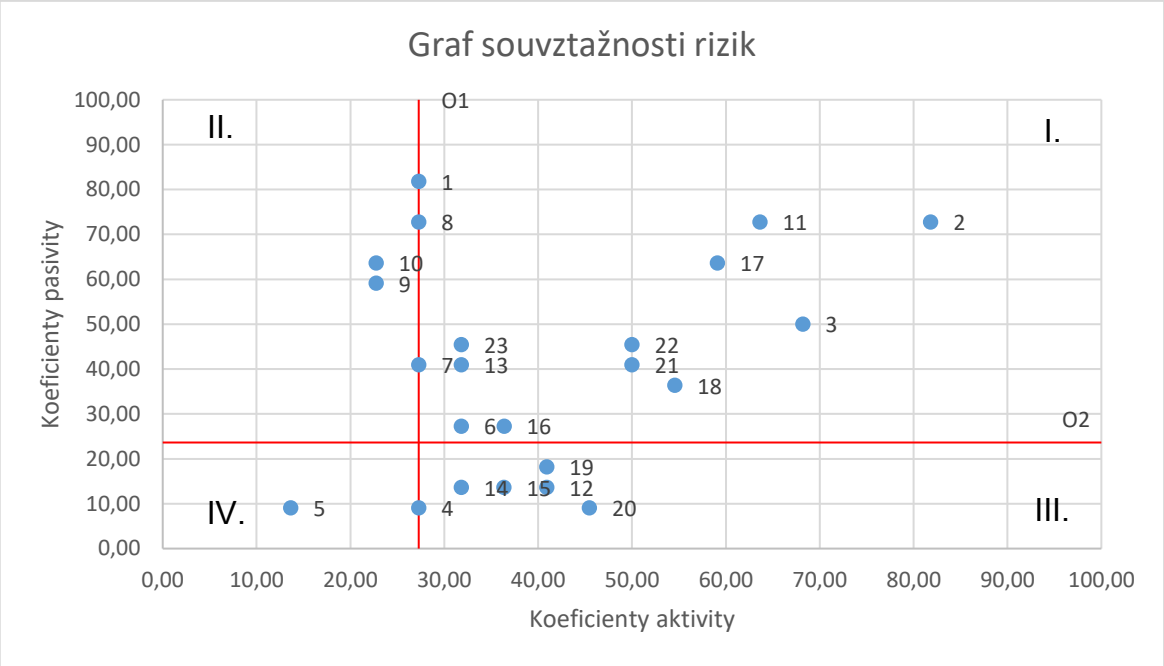
Hodnota bodu osy **O1**, představuje hodnotu bodu na ose **x,** na ose **y** je vždy hodnota 100. Naopak hodnota bodu osy **O2**, představuje hodnotu bodu na ose **y**, hodnota na ose **x** je 100. Výsledná hodnota bodu osy **O1** je rovna 22,27 a osy **O2** 23,63.

Tyto body vyneseme do grafu souvztažnosti rizik a protažením těchto bodů na osu **x** a **y** grafu, získáme osy, které nám graf rozdělí do požadovaných oblastí.



Obr. 5 Graf souvztažnosti rizik s vynesenými body osy O_1 a osy O_2 [zdroj: vlastní]

Po vynesení osy **O1** a **O2** do grafu souvztažnosti rizik, získáme výsledný graf, který můžeme číst a analyzovat rizika v jednotlivých oblastech. Vynesením osy **O1** a **O2** do grafu rozdělíme graf do požadovaných oblastí, což nám umožní určit rizika, která řešit primárně a které se můžou řešit následně.



Obr. 6 Výsledný graf souvztažnosti rizik [zdroj: vlastní]

6.3 Vyhodnocení analýzy rizik metodou KARS

Po úspěšném sestavení grafu souvztažnosti rizik, můžeme určit rizika v jednotlivých oblastech.

I. Oblast – rizika č. 2, 3, 6, 11, 13, 16, 17, 18, 21, 22, 23.

II. Oblast – rizika č. 1, 7, 8, 9, 10.

III. Oblast – rizika č. 12, 14, 15, 19, 20.

IV. Oblast – riziko č. 4 a 5.

Pro lepší orientaci ve výsledcích jsou výsledky prezentovány formou tabulky, ve které jsou jednotlivá rizika rozčleněna do oblastí s grafickým zvýrazněním.

Tab. 5 Tabulka s grafickým zvýrazněním rizik dle oblastí grafu z analýzy rizik metodou KARS [zdroj: vlastní]

č.	Riziko	Oblast grafu	Oblast rizika
2.	Nedodržení stanovených postupů	1	PB
3.	Nedostatečné proškolení	1	PB
6.	Chybné stanovení stupně utajení	1	AB
11.	Nesprávné nebo neoprávněné pořízení kopii, opisů	1	AB
13.	Ukládání UI mimo zabezpečené oblasti	1	FB
16.	Umožnění vstupu neoprávněné FO, PO	1	FB
17.	Odeslání UI nezabezpečeným způsobem	1	IB
18.	Užití cizí identity v IS	1	IB
21.	Zpracování UI mimo zabezpečenou oblast	1	IB
22.	Zpracování UI na nezabezpečeném PC	1	IB
23.	Zpracování UI na sestavě pro nižší stupeň utajení	1	IB
1.	Přístup k UI neoprávněnou osobou	2	PB
7.	Chybné uložení utajované informace	2	AB
8.	Neúmyslné vyzrazení UI	2	AB
9.	Úmyslné vyzrazení UI	2	AB
10.	Ztráta, zničení přidělené UI	2	AB
12.	Nedostatky v realizaci opatření projektu FB	3	FB
14.	Použití necertifikovaných prostředků	3	FB
15.	Vniknutí zloděje	3	FB
19.	Výpadek HW	3	IB
20.	Výpadek SW	3	IB
4.	Neověření oprávnění přístupu k UI	4	AB
5.	Neoznámení změn uvedených v žádosti	4	AB

PB … personální bezpečnost

AB… administrativní bezpečnost

FB … fyzická bezpečnost

IB … bezpečnost informačních a komunikačních systémů

- **Riziko č. 2 – Nedodržení stanovených postupů**

Nedodržení stanovených postupu je rizikem z oblasti personální bezpečnosti. Jedná se zejména o nedodržování postupů při nakládání s utajovanou informací. Každá činnost, při manipulaci s utajovanou informací, má své pravidla a postupy. Toto riziko je obecným rizikem. Každá činnost má své stanovené postupy, proto toto riziko skončilo ve významnosti na prvním místě.

Opatření ke zmírnění toho rizika, spočívá v důsledném dodržování stanovených postupů a předpisů, kontrole a v pravidelném proškolování.

- **Riziko č. 3 – Nedostatečné proškolení**

Zákon ukládá provádět školení prokazatelným způsobem každý rok, nejpozději před prvním seznámením s utajovanou informací. V případě pouze formálního, nebo nedostatečného proškolení, zejména z povinností vyplívajících ze zákona, případně novinek v této oblasti, se muže nedostatečně proškolená osoba dopustit chyb, čímž může být utajovaná informace ohrožena.

Opatření ke zmírnění rizika spočívá v provádění pravidelných, kvalitních proškolení pracovníky odborných útvarů.

- **Riziko č. 6 – Chybné stanovení stupně utajení**

Chybné stanovení stupně utajení, vychází částečně z neznalosti nebo nezkušenosti zpracovatele. Zákon ukládá, jaké náležitosti musí informace splňovat, aby se mohla informace klasifikovat jako utajovaná, a podle toho je také stanoven příslušný stupeň utajení. Chybně stanovený stupeň utajení, může způsobit další rizika, např. chybné uložení rizika, skartaci, přenos apod. V neposlední řadě, se může s takovou utajovanou informací seznámit osoba, nedisponující osvědčení pro styk s utajovanou informací. Např. osoba nedisponující osvědčením pro stupeň Důvěrné, se s takovou informací může seznámit, je-li taková informace chybně klasifikována stupněm utajení Vyhrazené.

Opatření ke zmírnění tohoto rizika spočívá v pravidelných školeních, kontrolách a důsledných dodržování postupů.

- **Riziko č. 11 - Nesprávné nebo neoprávněné pořízení kopii, opisů**

Další riziko spadá do oblasti administrativní bezpečnosti. Pořizování kopií a opisů utajované informace podléhá přísným pravidlům, spočívající zejména v administrativní činnosti, evidenci a kontrole. Provádění kopií se může provádět pouze na certifikovaných kopírovacích strojích oprávněnou osobou.

Opatření ke zmírnění rizika spočívá zejména v dodržování postupů a důsledné evidenci při pořizování kopií a opisů utajované informace.

- **Riziko č. 13 – Ukládání utajované informace mimo zabezpečené oblasti**

Zákon stanoví, že utajovaná informace se smí ukládat v zabezpečených oblastech příslušené kategorie nebo vyšší. Uvnitř zabezpečených oblastí se utajované informace smí ukládat v trezoru, uzamykatelné skříni nebo jiné schránce, a to pouze za podmínek stanovených prováděcím předpisem. Zabezpečená oblast je ve smyslu zákona ohraničený prostor, ve kterém lze utajovanou informaci pořizovat, zpracovávat nebo ukládat. Jedná se o oblast, který je v závislosti na její kategorii a třídě, zabezpečen technickými prostředky. V případě zabezpečené oblasti kategorie Vyhrazené, je stanoven požadavek, na minimální úroveň zabezpečení pomocí mechanických zábranných prostředků. Zabezpečená oblast kategorie Důvěrné se zabezpečuje také mechanickými zábrannými prostředky a zařízením elektronické zabezpečovací signalizace.

Opatření ke zmírnění rizika – pravidelná proškolení, dodržování zásad, pravidel a kontrola, užití certifikovaných MZS a systémů PZTS.

- **Riziko č. 17 - Odeslání UI nezabezpečeným způsobem**

Riziko s odesláním utajované informace prostřednickým nezabezpečeného komunikačního kanálu, spadá do kategorie rizik z oblasti bezpečnosti informačních a komunikačních systémů. Způsob odesílání utajovaných informací elektronickou poštou, je možný pouze za použití certifikovaných softwarových a hardwarových produktů, které umožní bezpečné zašifrování předávané zprávy. Informaci o zaslání UI prostřednictvím elektronické pošty, je odesilatel povinen zaznamenat na listinný dokument.

Opatření ke zmírnění rizika – pravidelná proškolení, dodržení zásad, pravidel a kontrola, mít přístup k certifikovanému PC s kryptoprostředkem.

❖ **Riziko č. 18 – Užití cizí identity v informačním systému**

Současná politika hesel v IS pro zpracování utajovaných informací pro stupeň utajení Vyhrazené a Důvěrné, stanoví požadavky na tvorbu hesel k přístupu do IS. Požadavky jsou:

- minimální délka hesla 8 znaků,
- musí obsahovat velká a malá písmena a číslice,
- platnost hesla je nastavena na 180 dnů,
- IS si „pamatuje“ 5 předchozích hesel,
- počet neúspěšných pokusů o přihlášení je nastaven na 3 pokusy, poté je účet uzamčen a jeho odemčení musí provést bezpečnostní správce IS,

Vezmeme-li v potaz, že uživatel takového systému si musí pamatovat dalších několik takových hesel do různých IS, policejních databází a soukromých emailových účtů, nutí to některé uživatele si heslo poznamenat, a ne vždy to dělají tak bezpečně, aby se k poznamenanému heslu nedostal někdo jiný. Nehledě na to, že využívá jedno heslo do více takových systémů, včetně soukromých.

Opatření ke zmírnění rizika – používání různých hesel do IS, zaznamenávat pouze část hesla, nikdy ne celé, možnost nasazení jiných způsobů autentifikace a autentizace, např.: USB tokeny, čtečky otisků prstů, čtečky karet apod.

❖ **Riziko č. 21 – Zpracování utajované informace mimo zabezpečenou oblast**

Zákon č. 412/2005 Sb. stanoví v §24, že utajovanou informaci lze zpracovávat pouze v zabezpečeném objektu a v zabezpečené oblasti příslušné kategorie nebo vyšší. Utajovanou informaci lze zpracovávat také v kategorii pro nižší stupeň utajení nebo mimo zabezpečenou oblast, ale to pouze v odůvodněných případech a s písemných souhlasem oprávněné osoby nebo bezpečnostního ředitele. V takovém případě je nutné zabezpečit, aby k utajované informaci neměla přístup nepovolaná osoba.

V operativní činnosti policistů se lze setkat s činnostmi, kdy i obyčejná žádost o úkon dle trestního řádu, musí být zpracován jako utajovaný dokument, tudíž v certifikovaném IS a v zabezpečené oblasti.

Opatření ke zmírnění rizika je mít přístup k dostatku ZO, vyžadování souhlasu ke zpracování UI mimo ZO, pravidelná proškolení, kontrola dodržování nařízení a zákona.

- **Riziko č. 22 – Zpracování utajované informace na nezabezpečeném PC**

Stupeň utajení utajované informace stanovuje původce informace při jejím vzniku. Je-li utajovaná informace zpracovávána elektronicky, je nutné takovou informaci zpracovávat na zabezpečeném PC s certifikovaným IS. Tudíž nelze zpracovávat informaci, o které víme že je utajovaná na nezabezpečeném PC bez certifikovaného IS s tím, že náležitosti jako označení stupně utajení a evidenčním označení doplníme po zpracování utajované informace.

NBÚ při svých kontrolách takové pochybení ze strany původce utajované informace již několikrát zjistil. Vezmeme-li v úvahu, že každý, kdo zpracovává utajovanou informaci v certifikovaném IS, zanechává za sebou v IS stopu, v podobě logu – auditního záznamu, který, na základě směrnice k IS, bezpečnostní správce každý měsíc min. 1x zálohuje. Neexistuje-li v certifikovaném IS auditní záznam k tomu kdo utajovanou informaci zpracovával, lze se domnívat, že taková informace vznikla jiným způsobem než v certifikovaném IS.

Opatření ke zmírnění rizika – dostupnost zabezpečeného PC s certifikovaným IS, školení, kontrola.

- **Riziko č. 23 – Zpracování UI na sestavě pro nižší stupeň utajení**

Utajovanou informaci lze zpracovávat pouze na PC sestavě pro příslušný stupeň utajení nebo vyšší. Zpracování utajované informace na soupravě pro nižší stupeň utajení, není vystavena utajovaná informace tak vysokému ohrožení, jako v případě zpracování na nezabezpečeném PC bez certifikovaného IS. Může se ale stát dostupnou osobám nedisponující oprávněním ke styku pro danou kategorii stupně utajení.

Opatření ke zmírnění rizika – dostupnost zabezpečené soupravy pro příslušné stupně utajení, kontroly a pravidelná školení.

- **Riziko č. 1 – Přístup k utajované informaci neoprávněnou osobou**

Riziko z oblasti personální bezpečnosti, kdy se osoba nedisponující oznámením nebo osvědčením, může dostat k utajované informaci. Zde se jedná zejména o osoby např. provádějící údržbu a servis v objektech, ve kterých se utajované informace nachází.

Opatření ke zmírnění rizika spočívá v dodržování zásad fyzické, personální a administrativní bezpečnosti, také bezpečnosti informačních a komunikačních systémů, proškolování a kontrola.

- **Riziko č. 7 – Chybné uložení utajované informace**

Ve výročních zprávách Bezpečnostního odboru MV anebo výroční zprávě NBÚ se toto riziko již několikrát objevilo, jako zjištěný nedostatek při plánovaných i neplánovaných kontrolách. Jedná se např. o uložení dokumentu ve stupni utajení stupni utajení mimo zabezpečenou oblast, nebo mimo určené trezory, uložení utajované informace v zabezpečené oblasti nižší kategorie.

Opatření ke snížení rizika – dostatečné prostory v pro ukládání utajovaných informací v příslušných kategoriích, školení, kontrola.

- **Riziko č. 8 – Neúmyslné vyzrazení utajované informace**

K neúmyslnému vyzrazení utajované informace může dojít např. při rozhovoru, nebo zapomenutím dokumentů na místech veřejných. V dnešní době se nabízí i neúmyslný unik utajovaných informací např. zapomenutí digitálního nosiče (USB Flashdisku, CD, HDD). V případě informací, klasifikovaných stupněm utajení Tajné a Přísně tajné, můžou být naplněny znaky skutkové podstaty trestného činu Ohrožení utajované informace z nedbalosti.

Opatření ke zmírnění rizika – dodržování všech zásad jednotlivých bezpečností z pohledu zákona, kontrola a pravidelná školení, motivace k dobře odvedené práci.

- **Riziko č. 9 – Úmyslné vyzrazení utajované informace**

Toto riziko, spočívá ve vědomém předávání informací s klasifikací stupně utajení nepovolané osobě, ať už s cílem obohacení nebo způsobení např. konkurenčních výhod, ekonomického prospěchu apod. Úmyslné vyzrazení utajované informace klasifikované stupněm utajení Tajné a Přísně tajné je dle § 317 Trestního zákona, trestným činem.

Opatření ke zmírnění rizika – dodržování zásad personální, fyzické, administrativní bezpečnosti a bezpečnosti informačních a komunikačních systémů, pravidelná školení,

kontrola, motivace zaměstnanců k dodržování zásad při nakládávání s utajovanými informacemi.

- **Riziko č. 10 – Ztráta, zničení přidělené utajované informace**

Ke ztrátě utajované informace může dojít např. při špatně vedené evidenci utajovaných informací, každý pohyb utajované informace, musí být zapsán v manipulačních knihách a jiných administrativních pomůckách. Při špatné evidenci a s odstupem času, může dojít ke zapomenutí, jak bylo s utajovanou informací naloženo a tím dojít k její ztrátě. Zničením se rozumí, zejména fyzické poškození, zničení nosiče utajované informace, zničení listinných dokumentů apod.

Opatření ke zmírnění rizika – kontrola v oblasti administrativní bezpečnosti, fyzické bezpečnosti, dodržování zásad a postupů, pravidelná proškolování.

- **Riziko č. 12 – Nedostatky v realizace opatření projektu FB**

Projekt fyzické bezpečnosti je dokumentem, který obsahuje informace o prostředcích a opatřeních použitých pro zajištění fyzické ochrany utajované informace, dále informace o objektu a zabezpečených oblastech. Pokud by mezi opatřeními pro fyzickou ochranu a skutečným stavem v objektu existovali rozdíly, např. výměnou zámků, dveří, oken, které již nesplňují předepsané požadavky pro zajištění ochrany utajované informace, musí být tyto nedostatky odstraněny nebo doplněny na požadovanou úroveň bezpečnosti. Totéž platí v případě stěhování vybavení kanceláří v zabezpečené oblasti. Projekt fyzické bezpečnosti obsahuje i grafickou část, ve které jsou zakresleny umístění trezorů, certifikovaných IS, detektorů PZTS apod.

Opatření ke zmírnění rizika – kontroly v dodržování opatření v projektu FB, opakovaná proškolení odborným útvarem, vytváření podmínek pro realizaci opatření z projektu FB.

- **Riziko č. 14 – Použití necertifikovaných prostředků**

Certifikovanými prostředky rozumíme takové mechanické, elektronické, softwarové a jiné prostředky, které jsou certifikovány Národním bezpečnostním úřadem a schváleny pro užití při vzniku, ukládání, přenášení, archivaci, skartaci utajované informace. Jsou to

např. mechanické zábranné prostředky, zámky, dveře, trezory, dále elektronické zabezpečovací systémy, systémy kontroly vstupu, software a hardware apod. Z pohledu fyzické bezpečnosti, lze pro zabezpečené oblasti a objekty pro kategorii Vyhrazené využít i necertifikované technické prostředky. Tyto lze však použít pouze v případě, že nedojde ke snížení úrovně ochrany požadovaný pro daný stupeň utajení. Pro kategorie vyšší musí být použity výhradně certifikované prostředky.

Opatření ke zmírnění rizika – používání certifikovaných prostředků, kontrola těchto prostředků, dodržování předpisů.

- **Riziko č. 15 – Vniknutí zloděje**

Vniknutí zloděje do označeného objektu Policie ČR je málo pravděpodobné, ale i taková situace může nastat. Jsou ale i objekty, které označení Policie nemají, přičemž se uvnitř nacházejí zabezpečené oblasti s utajovanými informacemi.

Opatření ke zmírnění toho rizika spočívají v důkladném zabezpečení objektu, a to jak na jeho obvodu, tak i uvnitř objektu. Obvod – plášť a perimetr lze zabezpečit za použití kamerových systémů, systémů elektronického zabezpečení nebo ostrahou objektu. Dalšími způsoby zmírnění rizika je použití bezpečnostních mechanických zábranných systémů.

- **Riziko č. 19 – Výpadek HW**

Riziko výpadku, selhání hardwaru se může vyskytnou z příčin např. kolísání napětí v elektrické síti, úderu blesku, zkratu, či „dosloužení“ životnosti některého z hardwarových komponent uvnitř počítače. Dnešní požadavky na počítačové soupravy pro kategorii Vyhrazené, již nevyžadují přítomnost UPS zdrojů nebo filtrů napětí, tudíž u této kategorie může k těmto selháním docházet.

Opatření ke zmírnění rizika – přítomnost druhého PC s certifikovaným IS, školení, dodržování zásad a postupu při zpracování utajované informace, umístnění filtru, UPS k soupravě, použití kvalitních hardwarových komponent.

- **Riziko č. 20 – Výpadek SW**

Zpracování utajovaných informací v elektronické podobě je možné pouze v PC s certifikovaným informačním systémem pro příslušný stupeň utajení. Dojde-li vlivem působení vyšší moci, lidského faktoru nebo faktoru technického selhání, hrozí situace, že utajovanou informaci nebude možné ihned zpracovat na PC s certifikovaným systémem. V takovém případě, může dojít k situaci, že bude utajovaná informace zpracována na nezabezpečeném PC bez informačního systému a tím k úniku utajované informace.

Opatření ke zmírnění rizika – přítomnost druhého PC s certifikovaným IS, školení, dodržování zásad a postupu při zpracování utajované informace.

- **Riziko č. 4 – Neověření oprávnění přístupu k UI**

Každý, kdo má přístup k utajovaným informacím, má povinnost na vyžádání předložit potvrzení o tom, že je držitelem oznámení nebo osvědčení, které opravňuje k seznamování s utajovanými informacemi. Může se tak stát, že osoba, které nebylo vydáno, nebo nebylo prodlouženo oznámení nebo osvědčení, bude seznámena s utajovanými informacemi.

Opatření ke zmírnění rizika spočívá v důkladné kontrole, dodržování administrativní a personální bezpečnosti.

- **Riziko č. 5 – Neoznámení změn uvedených v žádosti**

Každý držitel oznámení, nebo osvědčení je povinen hlásit tomu, kdo oznámení nebo osvědčení vydal, změny, které nastanou v průběhu trvání držení osvědčení nebo oznámení. Jedná se o změny vůči údajům uvedeným v žádosti. Např. změna adresy pro účely doručování, změna zaměstnavatele, nabytí nemovitého majetku mimo území ČR, údaje k osobě manžela/manželky, nebo osoby starší 18 let žijící ve společné domácnosti, vznik finančních závazků nad 100 tis. Kč nebo pětinásobek průměrného měsíčního příjmu po odečtení zákonných odvodů. Toto nastává, pokud závazek vznikne pouze mezi fyzickými osobami. Držitel je také povinen hlásit zahájení trestního stíhání vůči své osobě.

Opatření ke zmírnění rizika opět spočívá v důkladném proškolování držitelů oznámení nebo osvědčení ze zákona, správně nastavená organizační opatření.

Z výčtu všech možných rizik a možností ke zmírnění působení rizika, je dodržování zásad všech bezpečností tzn. zásad administrativní, fyzické, personální a bezpečnosti informačních a komunikačních systémů. Pravidelná školení ze zákona č. 412/2005 Sb. a souvisejících vyhláškách prohlubují u policistů povědomí, jak s utajovanými informacemi nakládat. Zákon přímo tyto školení ukládá absolvovat minimálně 1x ročně.

7 POŽADAVKY TVORBU PROJEKTU FYZICKÉ BEZPEČNOSTI OBJEKTU

Vycházíme-li z východisek zákona č. 412/2005 Sb. a vyhlášky č. 528/2005 Sb. stanovíme obsah projektu následovně.

V případě, že se v objektu nachází pouze zabezpečené oblasti pro stupeň utajení **Vyhrazené**, musí projekt obsahovat:

- určení objektu a zabezpečených oblastí, včetně jejich hranic a určení kategorií a tříd zabezpečených oblastí,
- způsob použití opatření fyzické bezpečnosti,
- technickou dokumentaci,
- tabulka bodového hodnocení se zpracovává v případě ukládání utajované informace v informačním systému nebo kryptografickém prostředku.

V případě vyšších stupňů **Důvěrné, Tajné a Přísně tajné** musí projekt obsahovat:

- určení objektu a zabezpečených oblastí, včetně jejich hranic a určení kategorií a tříd zabezpečených oblastí,
- vyhodnocení rizik,
- způsob použití opatření fyzické bezpečnosti,
- provozní řád objektu,
- plán zabezpečení objektu a zabezpečení oblastí v krizových situacích.

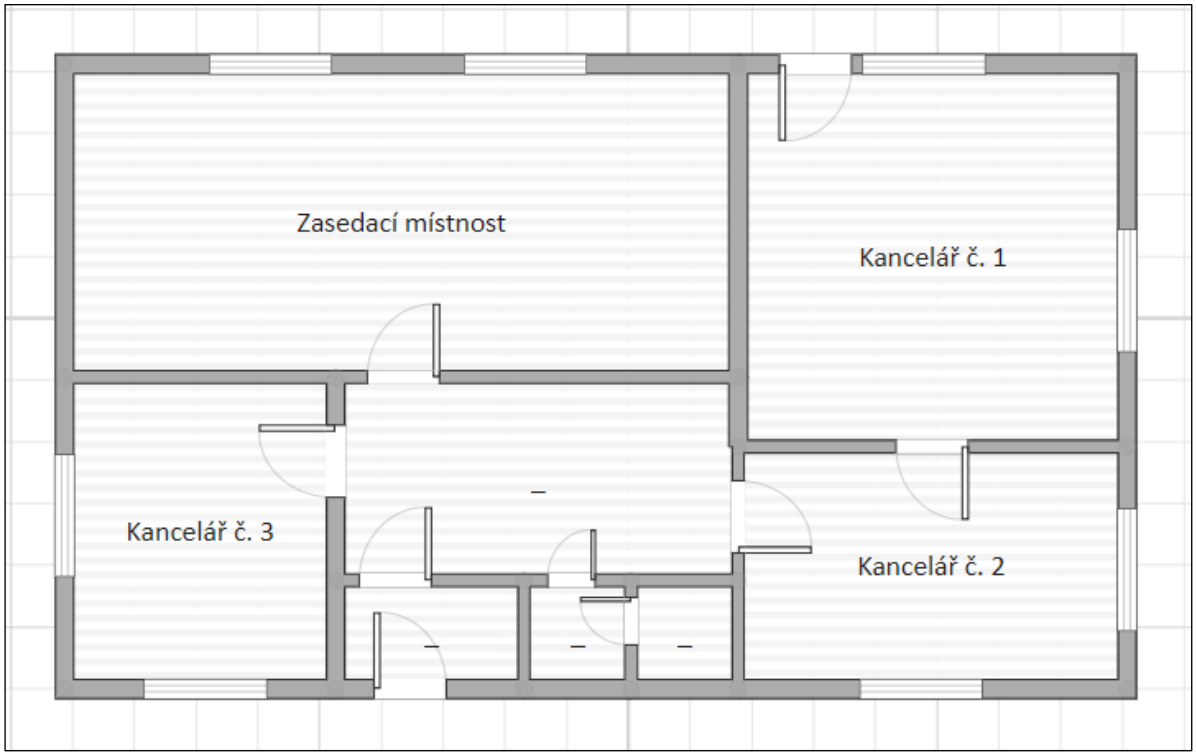
V případě, že se v objektu nachází zabezpečené oblasti kategorie Vyhrazené a oblasti kategorie vyšší, zpracovává se jeden projekt fyzické bezpečnosti ve výše uvedeném rozsahu, přičemž na oblasti kategorie Vyhrazené se aplikují pravidla stanovená pro tuto kategorii.

7.1 Určení objektu a zabezpečených oblastí

Pro potřeby této diplomové práce, byl vytvořen fiktivní půdorys objektu, ve kterém se mají zpracovávat utajované informace ve stupni utajení Vyhrazené a Důvěrné.

V areálu objektu budovy policie České republiky, který je zde popisován, sídlí vedení detašovaného pracoviště odboru služby kriminální policie a vyšetřování (dále jen SKPV). Jedná se o jednopodlažní budovu, ve které se nachází 3 kanceláře a jedna zasedací místnost a zázemí. Obvodové zdivo budovy je tvořeno 45 cm silnou cihlovou zdí. Vnitřní nosné příčky tvoří 35 cm cihlové zdi a ostatní příčky jsou tvořeny 15 cm silnou cihlovou zdí. Okna

jsou plastová a umístěna ve výšce menší než 5,5 m a jsou opatřeny kovovými mřížemi. Ve dvoře areálu se nachází místa určená pro parkování. Hranice areálu tvoří drátěné oplocení ve výšce 1,8m. Vstup do areálu je tvořen vstupní brankou osazenou zámkovým systémem knoflík – knoflík. Další možný vstup – vjezd do areálu je opatřen elektronicky ovládanou vjezdovou branou, kterou lze otevírat pomocí dálkového řízení. V okolí objektu se nachází zástavba rodinných domů. Příjezd k objektu je po veřejné komunikaci.



Obr. 7 Půdorys objektu [zdroj: vlastní]

Zabezpečená oblast kategorie Vyhrazené se nachází v kanceláři č. 3 a v zasedací místnosti. Hranice zabezpečené oblasti kanceláře č. 3, je tvořena obvodovými stěnami budovy a vnitřními stěnami místnostmi. Okna jsou zabezpečena pevnými kovovými mřížemi se zápisem o posouzení shody. Utajované informace jsou ukládány v úschovném objektu, který je pevné konstrukce, je uzamykatelný a pečetěn.

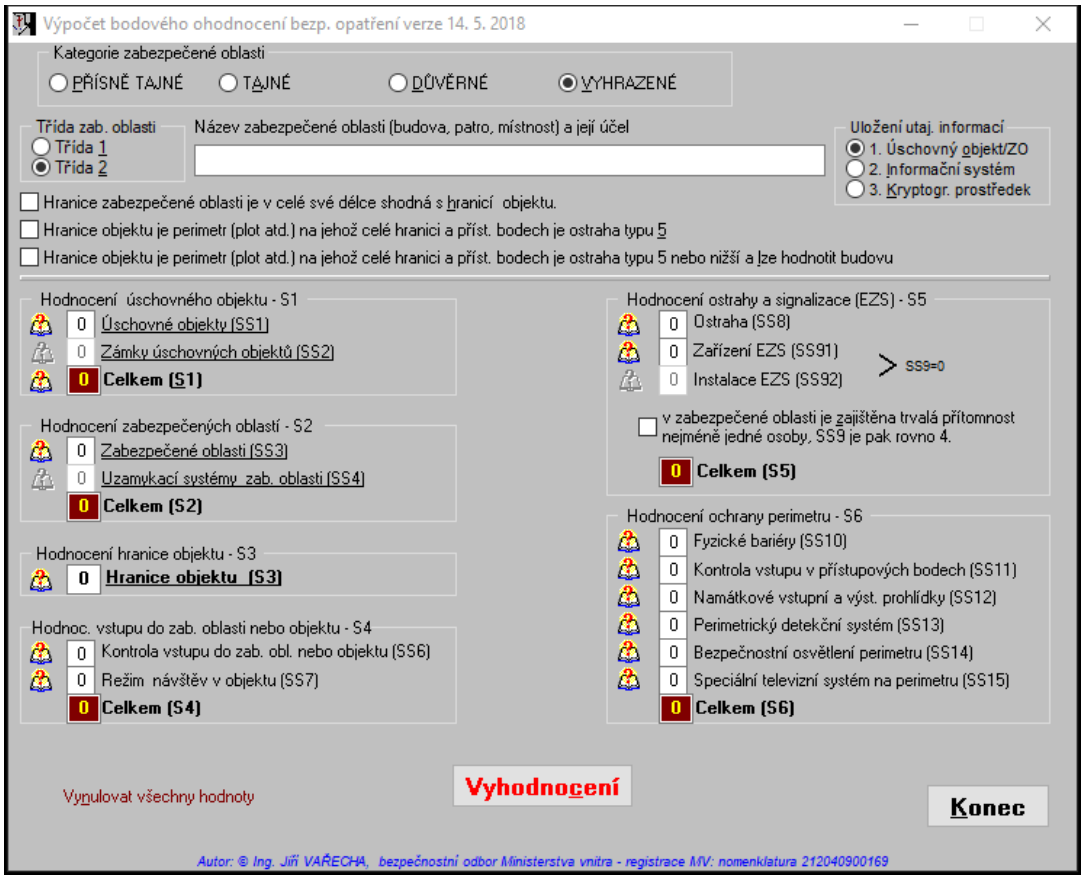
Zabezpečená oblast v zasedací místnosti je také kategorie Vyhrazené. Uvnitř zabezpečené oblasti se nachází certifikovaný informační systém, určený pro zpracování informací ve stupni utajení Vyhrazené.

Zabezpečená oblast kategorie Důvěrně se nachází v kanceláři č. 1 a 2. Utajované informace ve stupni utajení Důvěrně se ukládají v úschovném objektu uvnitř kanceláře č. 2 a 3. Uvnitř zabezpečené oblasti se nachází certifikovaný informační systém určený pro zpracování utajovaných informací ve stupni utajení Důvěrné.

7.2 Požadavky na použitá opatření fyzické bezpečnosti

Tak aby použitá opatření fyzické bezpečnosti byla akceptovatelná NBÚ, bylo stanoveno bodové ohodnocení jednotlivých opatření fyzické bezpečnosti pro jednotlivé kategorie, nejnižší míru zabezpečení zabezpečených oblastí nebo jednacích oblastí. Bodové ohodnocení pro jednotlivá opatření jsou uvedeny v příloze č. 1 vyhlášky č. 528/2005 Sb. o fyzické bezpečnosti a certifikaci technických prostředků.

Na bezpečnostním odboru Ministerstva vnitra, vyvinul Ing. Jiří Vařecha, softwarový produkt k výpočtu bodového ohodnocení bezpečnostních opatření.



Obr. 8 Screen SW pro výpočet bodového ohodnocení [zdroj: intranetové stránky BO MV]

Pomocí tohoto softwaru určíme, jaká opatření a v jakém rozsahu musíme použít, pro zabezpečení objektu a zabezpečených oblastí pro kategorii Vyhrazené a Důvěrné.

Posuzované oblasti pro výpočet nejnižší míry zabezpečení jsou:

- S1 – Hodnocení úschovného objektu nebo informačního systému,
- S2 – Hodnocení zabezpečených oblastí,
- S3 – Hodnocení hranice objektu,
- S4 – Hodnocení vstupu do zabezpečené oblasti nebo objektu,
- S5 – Hodnocení ostrahy a signalizace (EZS/PZTS),
- S6 – Hodnocení ochrany perimetru.

S1 – Hodnocení úschovného objektu nebo informačního systému

Podle toho, kde se utajovaná informace ukládá, zda v certifikovaném informačním systému nebo v úschovném objektu, je výsledná hodnota S1 jako součet hodnot SS1 a SS2.

Tab. 6 Tabulka bodového hodnocení pro úschovné objekty [zdroj: 24, upraveno autorem]

Body	**SS1 – Úschovný objekt – typ objektu odpovídá počtu bodů**
0	Úschovný objekt typu 0 je pevné konstrukce (např. schránka, kancelářský nábytek) a je opatřen zámkem, který je uzamykán. Nesmí vykazovat takové znaky poškození nebo opotřebení, které by znemožnily identifikovat pokusy o neoprávněný vstup. Úschovný objekt typu 0 není certifikovaný Úřadem. Shodu vlastností těchto úschovných objektů s výše uvedenými požadavky odpovědná osoba nebo jí pověřená osoba v projektu fyzické bezpečnosti
1	**Typ 1A –** Úschovný objekt typu 1B je certifikovaný Úřadem a splňuje, včetně uzamykacího systému, požadavky bezpečnostní třídy Z2 podle ČSN 91 6012.
2	**Typ 1B –** Úschovný objekt typu 1B je certifikovaný Úřadem a splňuje, včetně uzamykacího systému, požadavky bezpečnostní třídy Z2 podle ČSN 91 6012.
3	**Typ 1C –** Úschovný objekt typu 0 je pevné konstrukce (např. schránka, kancelářský nábytek) a je opatřen zámkem, který je uzamykán. Nesmí vykazovat takové znaky poškození nebo opotřebení, které by znemožnily identifikovat pokusy o neoprávněný vstup. Úschovný objekt typu 0 není certifikovaný Úřadem. Shodu vlastností těchto úschovných objektů s výše uvedenými požadavky odpovědná osoba nebo jí pověřená osoba v projektu fyzické bezpečnosti
2	Úschovný objekt typu 2 je certifikovaný Úřadem a splňuje požadavky **bezpečnostní třídy 0** podle ČSN EN 1143-1+A1.
3	Úschovný objekt typu 3 je certifikovaný Úřadem a splňuje požadavky **bezpečnostní třídy I** podle ČSN EN 1143-1+A1.
4	Úschovný objekt typu 4 je certifikovaný Úřadem a splňuje požadavky **bezpečnostní třídy II** nebo vyšší podle ČSN EN 1143-1+A1

Tab. 7 Tabulka bodového hodnocení zámků pro úschovné objekty [zdroj: 24, upraveno autorem]

Body	**SS2 – Zámek úschovného objektu**
2	Zámek typu 2 je certifikovaný Úřadem v rámci certifikace úschovného objektu a splňuje požadavky **bezpečnostní třídy A** podle ČSN EN 1300+A1.
3	Zámek typu 3 je certifikovaný Úřadem v rámci certifikace úschovného objektu a splňuje požadavky **bezpečnostní třídy B** podle ČSN EN 1300+A1.
4	Zámek typu 4 je certifikovaný Úřadem v rámci certifikace úschovného objektu a splňuje požadavky **bezpečnostní třídy C** podle ČSN EN 1300+A1.

V případě, že je v úschovném objektu typu 3 nebo 4 uložen kryptografický materiál, musí být tento úschovný objekt vybaven mechanickým, minimálně třípolohovým kombinačním zámkem.

V souladu s ČSN EN 1143-1+A1 musí být úschovný objekt typu 2, 3 a 4 osazen zámkem minimálně třídy A podle ČSN EN 1300+A1.

Hodnocení informačního systému je ekvivalentem k hodnocení úschovných systémů a zámkům k úschovným objektům.

Tab. 8 Tabulka bodového hodnocení ukládání dat v informačním systému [zdroj: 24, upraveno autorem]

Body	**SS1 – Zpracování a ukládání dat na mediích**
1	Uložená data nejsou šifrována Tento způsob uložení dat tvoří bezpečnostní ekvivalent úschovného objektu typu 1.
4	Uložená data jsou šifrována certifikovaným kryptografickým prostředkem.

Tab. 9 Tabulka bodového hodnocení pro identifikaci a autentizaci uživatele IS [zdroj: 24, upraveno autorem]

Body	**SS2 – Identifikace a autentizace uživatele**
1	Identifikace jménem a autentizace heslem. Minimální délka a způsob vytváření hesla musí být schválen Úřadem v rámci certifikace informačního systému. Tento způsob autentizace tvoří bezpečnostní ekvivalent zámku úschovného objektu typu 1.
2	Identifikace jménem a autentizace předmětem. Předmět používaný pro autentizaci musí být schválen Úřadem v rámci certifikace informačního systému. Tento způsob autentizace tvoří bezpečnostní ekvivalent zámku úschovného objektu typu 2.

Body	SS2 – Identifikace a autentizace uživatele
3	Identifikace jménem a autentizace předmětem s šifrovaným obsahem. Kryptografické mechanismy předmětu používaného pro autentizaci musí být certifikované Úřadem. Tento způsob autentizace tvoří bezpečnostní ekvivalent zámku úschovného objektu typu 3.
4	Identifikace jménem a autentizace předmětem s šifrovaným obsahem a přenosem. Kryptografické mechanismy předmětu používaného pro autentizaci musí být certifikované Úřadem. Tento způsob autentizace tvoří bezpečnostní ekvivalent zámku úschovného objektu typu 4.

S2 – Hodnocení zabezpečených oblastí

Mechanickými zábrannými prostředky se zabezpečují průlezné otvory, které dovolí průchod šablony o níže uvedených rozměrech obdélníku o délce stran 400 mm x 250 mm nebo elipsy o rozměrech 400 mm x 300 mm, případně kruhu o průměru 350 mm. Pokud je průlezný otvor zabezpečen mechanickým zábranným prostředkem s jedním nebo více otvory (např. mříž), nesmí tyto otvory dovolit průchod šablony ve tvaru elipsy o rozměrech 250 mm x 150 mm a tloušťky 20 mm. Určení typu zabezpečené oblasti je dáno nejméně odolným prvkem její hranice.

Tab. 10 Tabulka bodového hodnocení zabezpečených oblastí [zdroj: 24, upraveno autorem]

Body	SS3 – Zabezpečené oblasti – typ oblasti odpovídá počtu bodů
0	Zabezpečení průlezných otvorů musí umožňovat kontrolu pohybu osob a vozidel. Mechanické zábranné prostředky nesmí vykazovat takové znaky poškození nebo opotřebení, které by znemožnily identifikovat pokusy o neoprávněný vstup. Shodu s výše uvedenými požadavky potvrzuje odpovědná osoba nebo jí pověřená osoba v projektu fyzické bezpečnosti.
1	Stěny, podlahy a stropy jsou lehké stavební konstrukce z materiálů jako například: sádrokartónu, lehké zděné stavební konstrukce, dřeva, dřevotřískových desek, plastických tvrzených hmot, profilovaného nebo vlnitého plechu, skla. Průlezné otvory musí být zabezpečeny mechanickými zábrannými prostředky, které poskytují stejný stupeň odolnosti jako zbývající části hranice zabezpečené oblasti typu 1, nebo jsou chráněny certifikovanými zařízeními elektrické zabezpečovací signalizace (EZS/PZST), jejichž instalace odpovídá minimálně hodnotě SS92 = 3. Průlezné otvory nemusí být zabezpečeny těmito mechanickými zábrannými prostředky, pokud spodní okraj průlezného otvoru splňuje následující požadavky: 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. Mechanické zábranné prostředky musí být pevné konstrukce a nesmí vykazovat takové znaky poškození nebo opotřebení, které by znemožnily identifikovat pokusy o neoprávněný vstup a shodu s těmito požadavky posuzuje odpovědná osoba nebo jí pověřená osoba. Zápis o posouzení shody se stává součástí projektu fyzické bezpečnosti.

Body	**SS3 – Zabezpečené oblasti – typ oblasti odpovídá počtu bodů**
2	Stěny, podlahy a stropy musí mít následující stavební konstrukci: a) zděnou (cihelné nebo vápenocementové bloky, pórobetonové tvárnice) tloušťky 100 až 150 mm, nebo b) z vyztuženého betonu tloušťky do 100 mm. Podlahy a stropy mohou být i z jiného materiálu tloušťky větší než 150 mm (např. dřevěná sendvičová trámová konstrukce). Bodové hodnocení ostatních mechanických zábranných prostředků musí splňovat minimálně hodnotu SS3 = 2.
	Okna, dveře a uzávěry musí splňovat požadavky bezpečnostní třídy RC 2 podle ČSN EN 1627. Průlezné otvory nemusí být zabezpečeny certifikovanými mechanickými zábrannými prostředky, pokud spodní okraj průlezného otvoru splňuje následující požadavky: 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. Mechanické zábranné prostředky nesmí vykazovat takové znaky poškození nebo opotřebení, které by znemožnily identifikovat pokusy o neoprávněný vstup.
3	Stěny, podlahy a stropy musí mít následující stavební konstrukci: a) zděnou (cihelné nebo vápenocementové bloky, pórobetonové tvárnice) tloušťky větší než 150 mm, nebo b) z vyztuženého betonu tloušťky větší než 100 mm. Bodové hodnocení ostatních mechanických zábranných prostředků musí splňovat minimálně hodnotu SS3 = 3. Mechanické zábranné prostředky nesmí vykazovat takové znaky poškození nebo opotřebení, které by znemožnily identifikovat pokusy o neoprávněný vstup. Okna, dveře a uzávěry musí splňovat požadavky bezpečnostní třídy RC 3 podle ČSN EN 1627.
4	Stěny, podlahy a stropy musí mít následující stavební konstrukci: a) zděnou (cihelné nebo vápenocementové bloky, pórobetonové tvárnice) tloušťky větší než 300 mm, nebo b) z vyztuženého betonu tloušťky větší než 150 mm. Bodové hodnocení ostatních mechanických zábranných prostředků musí splňovat hodnotu SS3 = 4. Mechanické zábranné prostředky nesmí vykazovat takové znaky poškození nebo opotřebení, které by znemožnily identifikovat pokusy o neoprávněný vstup. Okna, dveře a další uzávěry musí splňovat požadavky bezpečnostní třídy RC 4 nebo třídy RC 5 podle ČSN EN 1627 Okna, dveře, uzávěry – Odolnost proti násilnému vniknutí – Požadavky a klasifikace.

Tab. 11 Tabulka bodového hodnocení uzamykacích systému pro zabezpečené oblasti [zdroj: 24, upraveno autorem]

Body	**SS4 – Uzamykací systémy**
0	Uzamykací systém typu 0 není certifikovaný Úřadem.
1	Uzamykací systém typu 1 je certifikovaný Úřadem. Uzamykací systém a jeho komponenty musí splňovat požadavky bezpečnostní třídy RC 2 podle ČSN EN 1627.
2	Uzamykací systém typu 2 je certifikovaný Úřadem. Uzamykací systém a jeho komponenty musí splňovat požadavky bezpečnostní třídy RC 3 podle ČSN EN 1627.

Body	SS4 – Uzamykací systémy
3	Uzamykací systém typu 3 je certifikovaný Úřadem. Uzamykací systém a jeho komponenty musí splňovat požadavky bezpečnostní třídy RC 4 podle ČSN EN 1627.
4	Uzamykací systém typu 4 je certifikovaný Úřadem. Uzamykací systém a jeho komponenty musí splňovat požadavky bezpečnostní třídy RC 5 podle ČSN EN 1627.

S3 – Hodnocení hranice objektu

Při určení typu objektu je rozhodující ta část hranice objektu, která má nejnižší odolnost. V případě, že hranice objektu je v celé své délce shodná s hranicí zabezpečené oblasti, hodnotí se pouze zabezpečená oblast a bodové hodnocení objektu (S3 = 0). Režim návštěv v objektu se v tomto případě nehodnotí. Zvláštním případem hranice objektu je perimetr (plot atd.) na jehož celé hranici a přístupových bodech je realizována ostrahou typu 5.

Tab. 12 Tabulka bodového hodnocení hranice objektu [zdroj: 24, upraveno autorem]

Body	SS3 – Hranice objektu – typ odpovídá počtu bodů
0	Objekt má viditelně vymezenou hranici, v jejímž rámci existuje možnost kontroly jednotlivých osob a vozidel. Hranici objektu stanoví odpovědná osoba nebo jí pověřená osoba v projektu fyzické bezpečnosti
1	Objekt je vylehčená prefabrikovaná konstrukce, která chrání osoby, materiál a zařízení před povětrnostními vlivy.
2	Objekt je lehké stavební konstrukce. Průlezné otvory musí být zabezpečeny mechanickými zábrannými prostředky nebo technickými prostředky EZS/PZTS minimálně s instalací SS92=1. Tato podmínka neplatí, pokud spodní okraj průlezného otvoru splňuje následující požadavky: 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.
3	Stěny, podlahy a stropy musí mít pevnou stavební konstrukci z cihel nebo tvárnic, případně je použita stavební technologie využívající prefabrikovaných a montovaných panelů apod. Průlezné otvory musí být zabezpečeny mechanickými zábrannými prostředky, které poskytují stejný stupeň odolnosti proti narušiteli jako ostatní části hranice objektu typu 3. Průlezné otvory nemusí být zabezpečeny těmito mechanickými zábrannými prostředky, pokud spodní okraj průlezného otvoru splňuje následující požadavky: 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.
4	Stěny, podlahy a stropy musí mít zvýšenou nebo zvlášť pevnou stavební konstrukci (např. železobetonová konstrukce). Objekt typu 4 má minimální počet dveří, oken a ostatních průlezných otvorů, které musí být zabezpečeny mechanickými zábrannými prostředky a poskytují stejný stupeň odolnosti proti narušiteli jako ostatní části hranice objektu typu 4.

S4 – Hodnocení vstupu do zabezpečené oblasti nebo objektu

Systém kontroly vstupu je hodnocen za předpokladu, že je realizován všech vstupech do objektu nebo zabezpečené oblasti.

Tab. 13 Tabulka bodového hodnocení vstupu do zabezpečené oblasti nebo objektu [zdroj: 24, upraveno autorem]

Body	**SS6 – Kontrola vstupu do zabezpečené oblasti nebo objektu – typ odpovídá počtu bodů**
1	Systém kontroly vstupu typu 1 tvoří uzamykatelná mechanická zábrana na vstupu.
2	Systém kontroly vstupu typu 2 musí být certifikovaný Úřadem, splňovat minimálně stupeň 3 podle ČSN EN 60839-11-1 Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty, a k přístupu je používán: a) identifikační prvek, b) PIN, nebo c) biometrie. Systém kontroly vstupu typu 2, lze nahradit kontrolou vstupu, kterou nepřetržitě provádí ostraha příslušníků ozbrojených sil nebo ozbrojených sborů, a to na všech vstupech do objektu nebo zabezpečené oblasti.
3	Systém kontroly vstupu typu 3 musí být certifikovaný Úřadem, splňovat minimálně stupeň 3 podle ČSN EN 60839-11-1 Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty, a k přístupu je používán: a) identifikační prvek a PIN, b) biometrie a PIN, nebo c) identifikační prvek a biometrie.
4	Systém kontroly vstupu typu 4 musí být certifikovaný Úřadem, splňovat minimálně stupeň 3 podle ČSN EN 60839-11-1 Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty, a k přístupu je používán: a) identifikační prvek a PIN, b) biometrie a PIN, nebo c) identifikační prvek a biometrie. Systém kontroly vstupu typu 4 musí být doplněn přístupovou bariérou znemožňující opakovaný přístup a zabezpečující režim "jedna transakce – jeden průchod".

Tab. 14 Tabulka bodového hodnocení režimu návštěv objektu [zdroj: 24, upraveno autorem]

Body	**SS7 – Režim návštěv objektu**
0	Návštěvy vstupují bez kontroly a doprovodu.
1	Návštěvy, které mají povolen vstup bez doprovodu, musí být viditelně označeny. V tomto případě musí být viditelně označeni i všichni vlastní zaměstnanci. Musí být vedena evidence údajů o návštěvách, která obsahuje osobní identifikační údaje návštěv a časové údaje o tom, kdy byla návštěva vykonána.
3	Návštěvy musí být doprovázeny po celou dobu pobytu v objektu. Musí být vedena evidence údajů o návštěvách, která obsahuje osobní identifikační údaje návštěv, doprovázejících osob a časové údaje o tom, kdy byla návštěva vykonána.

S5 – Hodnocení ostrahy a signalizace (EZS/PZTS)

Stanovená pravidla pro výkon ostrahy jsou nutná v případě objektu, ve kterém se nachází zabezpečená oblast kategorie Důvěrné, Tajné anebo Přísně tajné nebo jednací oblast. Tyto pravidla musí být stanovena v písemné formě.

Ostraha zabezpečených oblastí, ve kterých se ukládají utajované informace Evropské unie stupně utajení Důvěrné a vyšší, se zabezpečuje ostrahou typu 2 a vyšší, s tím že frekvence obchůzek musí být stanovena v intervalech ne větších než 2 hodiny. První obchůzka ostrahy se provede ihned po skončení pracovní doby. Stanoviště stálé ostrahy je umístěno od zabezpečené oblasti kategorie Přísně tajné a Tajné nejdále 500 m nebo pokud je vzdálenost stanoviště stálé ostrahy větší než 500 m musí být zásah ostrahy proveden do 5 minut od přijetí poplašného nebo nouzového signálu z objektu, zabezpečené oblasti nebo jednací oblasti.

Ostrahu typu 1 lze použít jen pro objekty kategorie Důvěrné nebo Vyhrazené. Ostraha musí být vybavena při obchůzce prostředky umožňujícími spojení se stanovištěm pro stálý výkon ostrahy. Doba reakce ostrahy na poplašný nebo nouzový signál musí být ověřována odpovědnou osobou nebo jí pověřenou osobou.

Tab. 15 Tabulka bodového hodnocení ostrahy [zdroj: 24, upraveno autorem]

Body	**SS8 – Ostraha – typ odpovídá počtu bodů**
1	Ostraha typu 1 odpovídá střežení objektu napojením na dohledové a poplachové přijímací centrum umožňující rychlý zásah.
2	Ostrahu typu 2 zabezpečují zaměstnanci orgánu státu, právnické osoby nebo podnikající fyzické osoby, o jejichž objekt jde, příslušníci ozbrojených sil nebo ozbrojených sborů anebo zaměstnanci bezpečnostní ochranné služby. U ostrahy typu 2 nejsou vyžadovány obchůzky.
3	Ostrahu typu 3 zabezpečují zaměstnanci orgánu státu, právnické osoby nebo podnikající fyzické osoby, o jejichž objekt jde, příslušníci ozbrojených sil nebo ozbrojených sborů anebo zaměstnanci bezpečnostní ochranné služby. Intervaly obchůzek jsou závislé na vnitřním provozu a míře předpokládaného rizika. V průběhu výkonu ostrahy, včetně doby obchůzky, musí být na stanovišti stálé ostrahy neustále přítomna nejméně jedna osoba určená pro výkon ostrahy.
4	Ostrahu typu 4 zabezpečují pouze příslušníci ozbrojených sil nebo ozbrojených sborů a je vykonávaná způsobem nepravidelných obchůzek. Ostraha provádí obchůzky v intervalu ne větším než 6 hodin. V noci a v mimopracovní době se četnost obchůzek zvyšuje. V průběhu výkonu ostrahy, včetně doby obchůzky, musí být na stanovišti stálé ostrahy neustále přítomna nejméně jedna osoba určená pro výkon ostrahy.
5	Ostrahu typu 5 zabezpečují pouze příslušníci ozbrojených sil nebo ozbrojených sborů a je vykonávaná způsobem nepravidelných obchůzek. Ostraha provádí obchůzky po náhodně vybraných trasách v náhodných intervalech ne větších než 2 hodiny. V průběhu výkonu ostrahy, včetně doby obchůzky, musí být na stanovišti stálé ostrahy neustále přítomna nejméně jedna osoba určená pro výkon ostrahy.

Tab. 16 Tabulka bodového hodnocení zařízení EZS/PZTS [zdroj: 24, upraveno autorem]

Body	**SS91 – Zařízení EZS/PZTS**
1	Zařízení elektrické zabezpečovací signalizace typu 1 nejsou certifikovaná Úřadem.
2	Zařízení elektrické zabezpečovací signalizace typu 2 musí být certifikováno Úřadem a splňuje požadavky podle ČSN EN 50131-1 ed. 2 pro stupeň zabezpečení 2 - nízké až střední riziko. Tísňový systém splňuje dále požadavky ČSN EN 50134-1.
3	Zařízení elektrické zabezpečovací signalizace typu 3 musí být certifikováno Úřadem a splňuje požadavky podle ČSN EN 50131-1 ed. 2 pro stupeň zabezpečení 3 - střední až vysoké riziko. Tísňový systém splňuje dále požadavky ČSN EN 50134–1.
4	Zařízení elektrické zabezpečovací signalizace typu 4 musí být certifikováno Úřadem a splňuje požadavky podle ČSN EN 50131-1 ed. 2 Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – pro stupeň zabezpečení 4 - vysoké riziko. Tísňový systém splňuje dále požadavky ČSN EN 50134–1 Poplachové systémy – Systémy přivolání pomoci.

Tab. 17 Tabulka bodového hodnocení instalace zařízení EZS/PZTS [zdroj: 24, upraveno autorem]

Body	**SS92 – Instalace EZS/PZTS**
1	Instalace typu 1 je realizovaná v rozsahu prostorové ochrany zabezpečené oblasti.
2	Instalace typu 2 je realizovaná v zabezpečené oblasti v rozsahu: a) prostorová ochrana, b) plášťová ochrana. Průlezné otvory v hranici zabezpečené oblasti v případě instalace zařízení elektrické zabezpečovací signalizace typu 2 nemusí být chráněny prvky plášťové ochrany, pokud jejich spodní okraj splňuje následující podmínky: 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.
3	Instalace typu 2 je realizovaná v zabezpečené oblasti v rozsahu: a) prostorová ochrana, b) plášťová ochrana. Průlezné otvory v hranici zabezpečené oblasti v případě instalace zařízení elektrické zabezpečovací signalizace typu 2 nemusí být chráněny prvky plášťové ochrany, pokud jejich spodní okraj splňuje následující podmínky: 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.
4	Instalace typu 4 je realizovaná v zabezpečené oblasti v rozsahu: a) prostorová ochrana, b) plášťová ochrana, c) tísňový systém, d) otřesové detektory nebo speciální televizní systém snímající nepřetržitě průlezné otvory zabezpečené oblasti.

S6 – Hodnocení ochrany perimetru a jeho podsystémů

Tab. 18 Tabulka bodového hodnocení ochrany perimetru [zdroj: 24, upraveno autorem]

Body	**SS10 – Fyzické bariéry**
1	Fyzické bariéře typu 1 odpovídá oplocení bez speciálních bezpečnostních požadavků. Účelem tohoto oplocení je vyznačit hranice a zajistit minimální úroveň odrazení nebo odolnosti. Fyzická bariéra typu 1 může být tvořena jakýmkoliv typem materiálu.
2	Fyzická bariéra typu 2 musí poskytovat překážku proti pokusu o překonání lezením a proti průniku průlomem. Minimální výška vertikální části bariéry je 2,15 metru.
3	Fyzická bariéra typu 3 umožňuje pozorování přilehlého terénu. Je-li to možné, musí být ponechán kolem chráněného objektu 25metrový volný prostor. Minimální výška vertikální části bariéry je 2,15 metru. Musí být navržena a zkonstruována tak, aby poskytovala co největší překážku proti průniku průlomem. Horní část bariéry musí zajišťovat ochranu proti překonání lezením – jednostranné šikmé vzpěry vyčnívající ven pod úhlem 45° o minimální délce 40 cm, na nichž je po celé délce připevněn ostnatý drát.
4	Fyzická bariéra typu 4 umožňuje pozorování přilehlého terénu. Je-li to možné, musí být ponechán kolem chráněného objektu 25metrový volný prostor. Minimální výška vertikální části bariéry je 2,15 metru. Musí být navržena a zkonstruována tak, aby poskytovala co největší překážku proti průniku průlomem. Horní část bariéry musí zajišťovat ochranu proti překonání lezením – oboustranné šikmé vzpěry vyčnívající ven i dovnitř pod úhlem 45° o minimální délce 40 cm, na nichž je po celé délce připevněn ostnatý drát. Fyzická bariéra typu 4 musí být doplněna perimetrickým detekčním systémem.

Tab. 19 Tabulka bodového hodnocení kontroly vstupu v přístupových bodech [zdroj: 24, upraveno autorem]

Body	**SS11 – Kontrola vstupu v přístupových bodech**
0	Kontrola vstupu není realizována ve všech přístupových bodech perimetru
1	Kontrola vstupu ve všech přístupových bodech perimetru

Tab. 20 Tabulka bodového hodnocení namátkových kontrol a výstupních prohlídek [zdroj: 24, upraveno autorem]

Body	**SS12 – Namátkové vstupní a výstupní prohlídky**
0	Nejsou prováděny
1	Namátkové prohlídky zabezpečuje orgán státu, právnická nebo podnikající fyzická osoba a jsou prováděny náhodně při vstupu, vjezdu, výstupu a výjezdu z objektu. Namátkové prohlídky jsou určeny jako odstrašující prvek proti porušení ochrany utajovaných informací.

Tab. 21 Tabulka bodového hodnocení perimetrického detekčního systému [zdroj: 24, upraveno autorem]

Body	**SS13 – Perimetrický detekční systém**
0	Není realizován
1	Perimetrický detekční systém není certifikovaný Úřadem a vztahují se na něj požadavky uvedené v bodě 5.2. přílohy (EZS/PZTS)
2	Perimetrický detekční systém je certifikovaný Úřadem a vztahují se na něj požadavky uvedené v bodě 5.2. přílohy. (EZS/PZTS)

Tab. 22 Tabulka bodového hodnocení bezpečnostního osvětlení perimetru [zdroj: 24, upraveno autorem]

Body	**SS14 – Bezpečnostní osvětlení perimetru**
0	Není realizováno
2	Požadavky na instalaci bezpečnostního osvětlení vyplývají například z požadavků speciálního televizního systému na perimetru.

Tab. 23 Tabulka bodového hodnocení instalace systému CCTV [zdroj: 24, upraveno autorem]

Body	**SS15 – Speciální televizní systém na perimetru**
0	Není realizováno
2	Speciální televizní systém není certifikovaný Úřadem. Instalace speciálního televizního systému musí splňovat požadavky norem řady ČSN EN 50132 - Poplachové přenosové systémy a zařízení – CCTV sledovací systémy pro použití v bezpečnostních aplikacích.

Z výše uvedených tabulek, které stanovují požadavky na jednotlivé oblasti, lze spočítat hodnoty a výsledek porovnat s uvedenými tabulkami pro stanovení nejnižší míry bodového hodnocení oblastí bezpečnosti, tak aby bylo umožněno v příslušném objektu pořizovat, zpracovávat nebo ukládat utajované informace.

Dalšími prostředky bez bodového hodnocení, se kterými je možné se setkat při zabezpečení objektu a oblastí určených pro nakládání s utajovanými informacemi jsou zejména zařízení elektrické požární signalizace, zařízení pro vyhledávání nebezpečných látek a předmětů, které můžou být používány na vstupech do objektů nebo oblastí, případně do jednací oblasti kategorie Přísně tajné. Zde se jedná zejména o detektory kovových předmětů a rentgenové přístroje pro kontrolu zavazadel. Specifickým prostředkem je zařízení proti pasivnímu

a aktivnímu odposlechu utajovaných informací. Tyto prostředky jsou použity v jednacích oblastech kategorie Přísně tajné a Tajné, ve které se pravidelné projednávají utajované informace. Požadavky na zajištění takových oblastí jsou uvedeny v příloze č. 1 vyhlášky[25].

Posledním technický prostředkem, se kterým se lze setkat jsou přístroje pro fyzické ničení nosičů informací nebo dat. Zařízení jsou NBÚ rozděleny do typu (0–4), podle toho, jaký je nosič utajované informace, jakým způsobem je ničen, jak velký odpad vzniká a pro jakou kategorii stupně utajení lze zařízení použít. Přesné údaje k těmto zařízením jsou opět uvedeny v příloze č. 1 vyhlášky[25].

Tab. 24 Nejnižší hodnoty oblastí pro kategorii Vyhrazené [zdroj: 24, upraveno autorem]

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

U kategorie stupně utajení Důvěrné a vyšší, musíme ještě stanovit míru rizika, a to podle předpokládaného množství výskytu utajované informace.

Tab. 25 Nejnižší hodnoty pro kategorii Důvěrné [zdroj: 24, upraveno autorem]

Zabezpečená oblast kategorie Důvěrné	**Míra rizika**		
	malá	**střední**	**velká**
Povinné: **(S1) + (S2) + (S3)**	6	8	9
Povinné: **(S4) + (S5)**	2	3	3
Nepovinné: **(S6)**	3	3	4
Celkový výsledek:	**11**	**14**	**16**

[25] Příloha č. 1 vyhlášky č. 528/2005 Sb. o fyzické bezpečnosti a certifikaci technických prostředků

8 NÁVRH ZABEZPEČENÍ OBJEKTU S APLIKACÍ VÝSLEDKŮ ANALÝZY RIZIK

Cílem této kapitoly je provést zabezpečení objektu a jednotlivých oblastí, tak aby působení vytipovaných rizik, bylo co nejmenší. Zabezpečení bude provedeno pomocí technických prostředku, návrhů organizačních opatření apod. V úvodu bych ještě rád upozornit, že se nejedná o vytvoření projektu fyzické bezpečnosti z pohledu zákona.

Návrh zabezpečení objektu, bude vycházet z jednotlivých druhů bezpečnosti, stanovených zákonem o ochraně utajovaných informací, tzn. z pohledu personální bezpečnosti, fyzické bezpečnosti, administrativní bezpečnost a bezpečnost informačních a komunikačních systémů. Zároveň bude návrh proveden, také s ohledem na výsledky analýzy rizik, provedené v šesté kapitole, kdy výsledky analýzy, zejména možnosti a opatření vedoucí ke snížení dopadů působení rizika, budou aplikovány do samotného návrhu zabezpečení. Návrhy zabezpečení jsou doplněny nákresy s grafickým určením zabezpečených oblastí, rozmístění prvků PZTS, MZS a dalších prostředků k zabezpečení utajovaných informací, jako jsou prvky certifikovaných informačních systémů a úschovných objektů. V každé části návrhu zabezpečení se také nachází bodové hodnocení jednotlivých prvků, tak aby odpovídaly požadavkům NBÚ.

8.1 Provozní řád a základní organizační opatření

Provozní řád a základní organizační opatření pro stanovený objekt vymezuje zejména režim pohybu osob v objektu a v zabezpečených oblastech, a to včetně návštěv, režim při manipulaci s klíči a řešení mimořádných událostí. Některé z těchto režimových opatření jsou uvedeny v bezpečnostní dokumentaci areálu a také v projektu fyzické bezpečnosti.

Pohyb osob v objektu a zabezpečených oblastech

Oprávněné osoby k samostatnému vstupu do objektu schvaluje vedoucí odboru SKPV. Oprávněné osoby jsou povinny příchod a odchod z objektu provádět hlavním vchodem. Osoby oprávněné k samostatnému vstupu jsou policisté kmenově zařazeni na příslušném detašovaném pracovišti. Seznam oprávněných policistů je uložen u vedoucího detašovaného pracoviště.

Do zabezpečené oblasti může samostatně vstupovat pouze osoba, která je ke vstupu do příslušné zabezpečené oblasti oprávněna. Uživatele zabezpečených oblastí stanovuje vedoucí odboru SKPV, který je za zabezpečenou oblast odpovědný. Seznam oprávněných

osob je uložen u vedoucího detašovaného pracoviště. Oprávněný uživatel zabezpečené oblasti odpovídá za pohyb osob uvnitř zabezpečené oblasti. Před vstupem do zabezpečené oblasti musí uživatel zkontrolovat uzamčení a stav vstupních dveří, technických prostředků a poté i stav dalších MZS např. mříží a oken.

Neoprávněná osoba zabezpečené oblasti má vstup do takové oblasti umožněn pouze za splnění podmínek že:

- **a)** Utajované informace jsou zabezpečeny před unikem a vyzrazením (uloženy v úschovném objektu a zamčeny).
- **b)** Je ukončeno nebo přerušeno jednání, jehož předmětem jsou utajované informace.
- **c)** Osoba je v doprovodu uživatele zabezpečené oblasti.

Při opuštění zabezpečené oblasti musí uživatel ověřit stav uzamčení oken a dveří, vypnutí elektrických a jiných spotřebičů, které by mohly způsobit požár. Uzamkne a zapečetí příslušný úschovný objekt a vstupní dveře. Klíče od úschovného objektu jsou uloženy v krabičce a zapečetěny. Přítomnost uživatele v zabezpečené oblasti mimo pracovní dobu je možné, pouze se souhlasem vedoucího detašovaného pracoviště.

Režim manipulace s klíči

Mimo pracovní dobu musí být kanceláře uzamčeny. Klíče od jednotlivých kanceláří – zabezpečených oblastí se ukládají po skončení pracovní doby do krabiček a následně jsou zapečetěny a uloženy v kanceláři č. 2. Náhradní klíče od zabezpečených oblastí
a úschovných objektů jsou uloženy v zapečetěných obálkách v kanceláři č. 2. Jakákoliv manipulace s náhradními klíči musí být zaznamenána.

Řešení mimořádných událostí

Mezi mimořádné události můžeme zařadit, požár v objektu, napadení objektu cizí osobou, úraz a smrt při výkonu zaměstnání apod. Každý vznik mimořádné události musí hlášen vedoucímu detašovaného pracoviště a vedoucímu odboru a v případě nutnosti zásahu jiných složek také cestou operačního střediska dotčeným složkám. Vedoucí detašovaného pracoviště, případně odboru stanovuje další postup při řešení mimořádné události.

Součástí bezpečnostní dokumentace areálu je dokumentace požární ochrany, plán evakuace a ukrytí, požární a poplachové směrnice a důležitá čísla vyrozumění.

8.2 Návrh zabezpečení v rámci personální bezpečnosti

Z pohledu zákona č. 412/2005 Sb. o ochraně utajovaných informací a bezpečnostní způsobilosti, personální bezpečnost zahrnuje ověřování podmínek, které musí fyzická osoba splnit, aby se s utajovanými informacemi mohla seznamovat, ale zahrnuje také výchovu těchto osob, formou proškolování z právních předpisů. Tato proškolování musí osoba absolvovat minimálně 1x ročně.

Z pohledu bezpečnosti je právě proškolování ze znalosti právních předpisů z oblasti ochrany utajovaných informací tím správným opatřením, které může snížit riziko.

8.2.1 Návrh obsahu proškolení

Možností, jak proškolení může probíhat je několik. V našem objektu se nachází jedna zasedací místnost s dostatečnou kapacitou a technickým vybavením v podobě počítače a dataprojektoru. Další možností, jak může proškolení probíhat, je formou e-learningu. Konkrétně tato forma je předmětem každoročního ověřování způsobilosti bezpečnostních správců IS. V našem případě bude probíhat proškolování formou prezentace a přednášky zaměstnancem Krajského ředitelství, odboru ochrany utajovaných informací.

Obsah proškolení:

- Zákon č. 412/2005 Sb. a příslušné vyhlášky provádějící zákon
  - Personální bezpečnost.
  - Administrativní bezpečnost.
  - Fyzická bezpečnost.
  - Bezpečnost informačních a komunikačních systémů.
- Problematika hlášení změn držitelů oznámení nebo osvědčení.
- Zjištěné nedostatky a forma jejich nápravy.
- Sankce za nedodržení povinností.

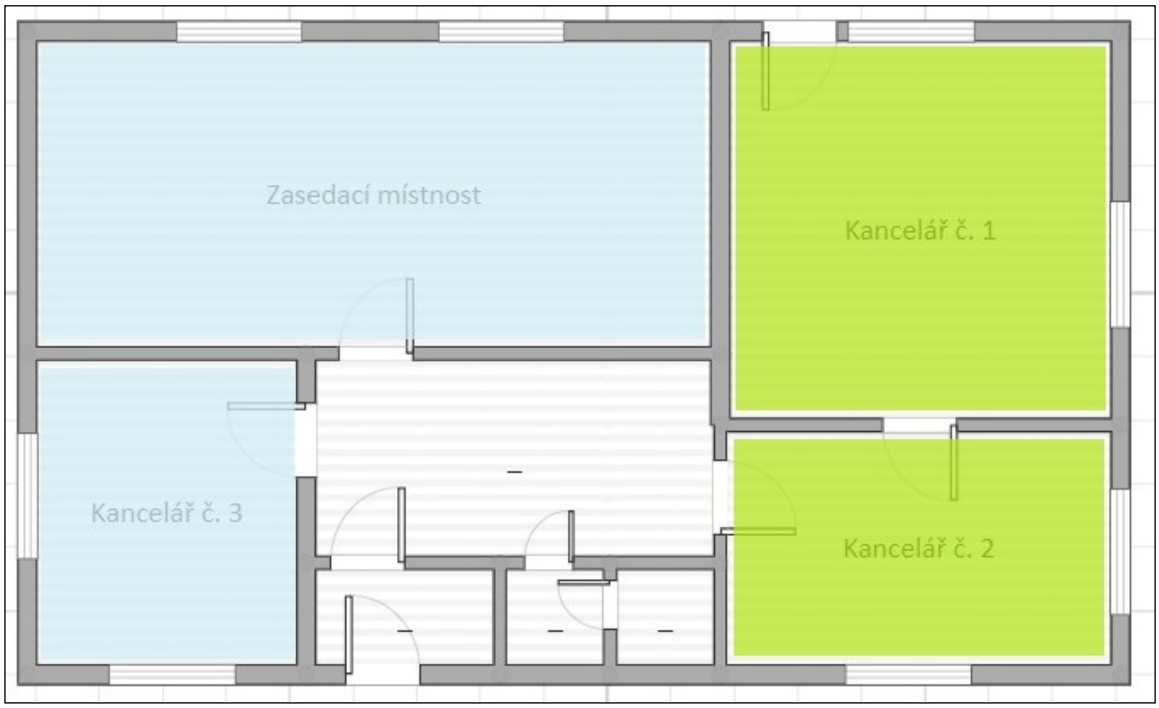
Cílem každoročního proškolení je prohlubování znalostí z problematiky ochrany utajovaných informací, prevence v podobě prezentace zjištěných nedostatků a sankcí hrozících za nedodržení povinností.

8.3 Návrh zabezpečení v rámci fyzické bezpečnosti

Zákon stanovuje objekt z pohledu fyzické bezpečnosti jako budovu nebo prostor, ve kterém se nachází zabezpečená oblast nebo jednací oblast. V našem objektu se nachází zabezpečené

oblasti kategorie Vyhrazené a kategorie Důvěrné, ve kterých se nachází příslušné IS a úschovné objekty.

Zabezpečené oblasti jsou graficky znázorněny na následujícím obrázku.



Obr. 9 Určení zabezpečených oblastí [zdroj: vlastní]

Zabezpečená oblast kategorie Důvěrné

Zabezpečená oblast kategorie Vyhrazené

Systém kontroly vstupu do objektu a zabezpečených oblastí je typu 1 a tvoří jej uzamykatelné fyzické zábrany. Návštěvy smí do objektu pouze v doprovodu po celou dobu návštěvy. Je vedena evidence návštěv, která obsahuje osobní identifikační údaje návštěv, doprovázejících osob a časové údaje o tom, kdy byla návštěva vykonána, což odpovídá typu 3.

Tab. 26 Bodové hodnocení vstupu do objektu a ZO S4 [zdroj: vlastní]

Název	**Typ**	**Body**
Kontrola vstupu	Typ 1	SS6 = 1
Režim návštěv	Typ 3	SS7 = 3
Celkem	**SS6+SS7**	**S4 = 4**

8.3.1 Návrh zabezpečení mechanickými zábrannými prostředky

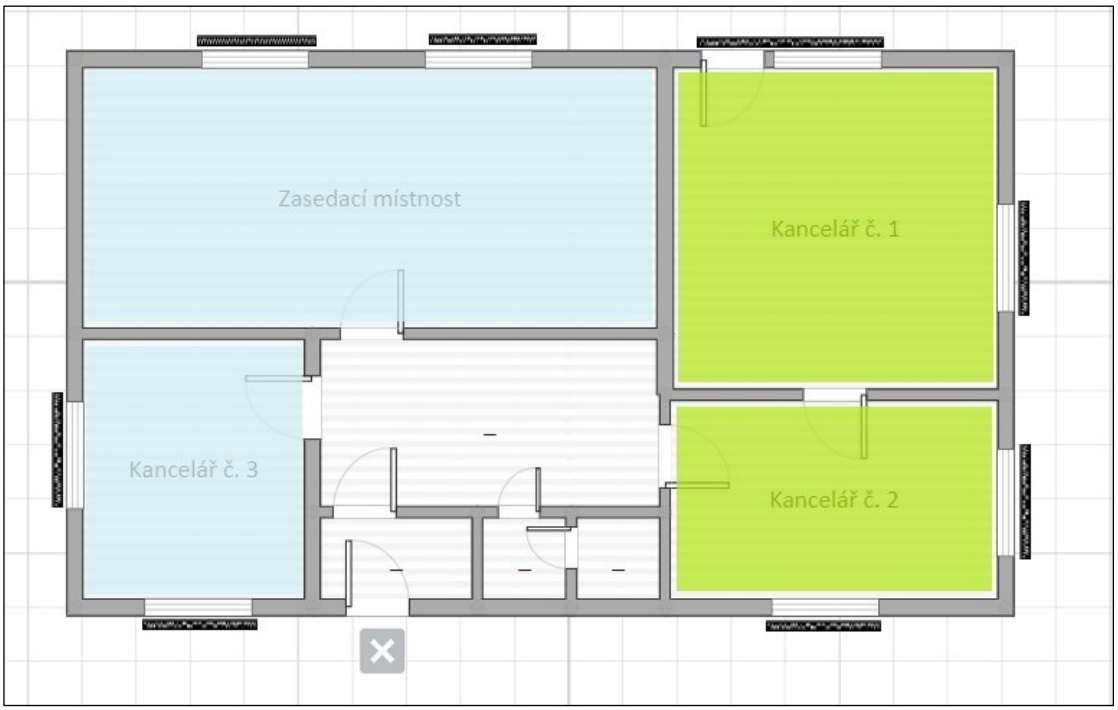
Mechanické zábranné prostředky použité v objektu, jsou vstupní dveře do objektu a do zabezpečených oblastí a jejich uzamykací systémy, okenní mříže.

Stanovení hranic objektu – vyhláška[26] stanovuje, že při určování typu objektu při stanovení jeho hranic a jeho bodovém hodnocení je nutno vycházet z nejméně odolné části. Náš objekt je vystavěn z pálených cihel po celém svém obvodu v šířce 45 cm. Veškeré další vstupní otvory jsou zabezpečeny mřížemi. V našem případě se jedná o typ objektu 3. Mříže jsou namontovány na oknech u zabezpečených oblastí a u dveří do kanceláře č. 1.

Zabezpečené oblasti – v objektu jsou zřízeny 4 zabezpečené oblasti. Hranice zabezpečených oblastí tvoří z části obvodové zdivo a z části příčky budovy. Vstupy do zabezpečených oblastí kategorie Důvěrné je tvořen dveřmi splňující požadavky bezpečnostní třídy RC2 podle normy[27] a jsou vybaveny uzamykacím systémem typu 2.

[26] Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů

[27] Norma č. ČSN EN 1627 - Dveře, okna, lehké obvodové pláště, mříže a okenice – Odolnost proti vloupání



Obr. 10 Návrh zabezpečení MZS [zdroj: vlastní]

Bezpečnostní dveře

Okenní mříže

Tab. 27 Bodové hodnocení zabezpečených oblastí S2 [zdroj: vlastní]

Název	**Typ**	**Bodové hodnocení**
Zabezpečené oblasti	Typ 2	SS3 = 2
Uzamykací systémy do ZO	Typ 2	SS4 = 2
Cekem	**SS3 x SS4**	**SS2 = 4**

8.3.2 Návrh zabezpečení PZTS

Pro příslušnou kategorii utajení je nutné použití také odpovídající systém elektronického zabezpečení, tak aby splňoval požadavky NBÚ. U objektu kategorie Důvěrné je povinným prvkem fyzické bezpečnosti instalace systém PZTS. Objekt je v době mimo pracovní dobu zastřežen systémem PZTS s připojením na DPPC na operačním středisku Krajského

ředitelství Policie ČR. V objektu je řešena prostorová ochrana s detekcí otevření vstupních dveří.

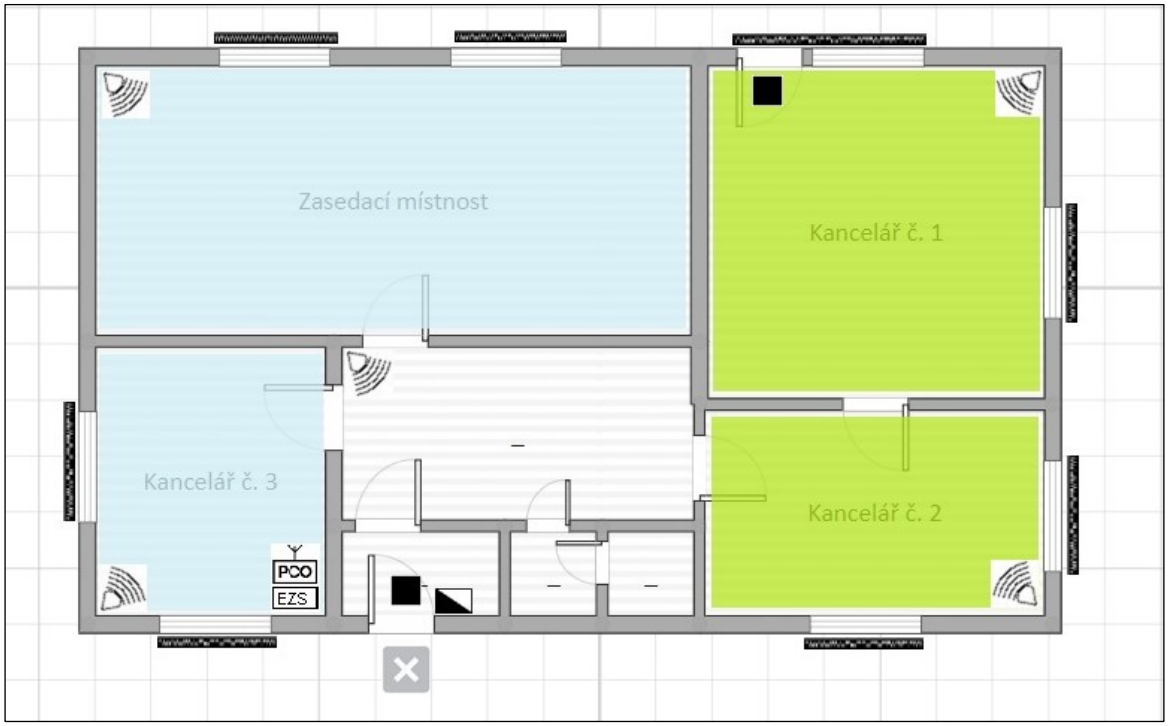
Instalované zařízení systému PZTS odpovídá typu 2 a je certifikováno NBÚ a splňuje požadavky podle normy[28]. Instalace je realizována v rozsahu prostorové ochrany a odpovídá typu 1. Fyzická ostraha v objektu je realizována napojením objektu na DPPC a odpovídá typu 1, pouze v pracovní době je fyzická ostraha prováděna zde pracujícími policisty.

Tab. 28 Bodové hodnocení ostrahy a signalizace PZTS [zdroj: vlastní]

Název	**Typ**	**Bodové hodnocení**
Ostraha	1	SS8 = 1
Zařízení PTZS	2	SS91 = 2
Instalace PZTS	1	SS92 = 1
Celkem	**SS8 + min(SS91;SS92)**	**S5 = 2**

[28] Norma č. ČSN EN 50131-1 ed. 2 - Poplachové systémy – Poplachové zabezpečovací a tísňové systémy

Grafické znázornění umístnění detektorů pohybu a prvků PZTS v objektu a zabezpečených oblastech.



Obr. 11 Návrh zabezpečení PZTS [zdroj: vlastní]


Detektor pohybu

Ústředna PZTS (dříve EZS) s napojením na DPPC (dříve PCO)


Detektor otevření dveří


Klávesnice PZTS

8.4 Návrh zabezpečení v rámci administrativní bezpečnosti

Administrativní bezpečnost chrání utajované informace v jednotlivých stádiích jejího životního cyklu tzn. od vzniku, zpracování, odesílání, přepravě nebo přenášení, ukládání archivaci, až po skartaci, případně při jiném nakládání s takovou informací.

Pro ukládání utajovaných informací, slouží úschovné objekty pro příslušnou kategorii. V případě kategorie Důvěrné a nižší se jedná o úschovný objekt typu 2, který je certifikován

NBÚ a musí splňovat požadavky na třídu bezpečnosti 0 dle příslušené normy[29] a musí být osazen zámkem typu 2 a minimálně třídy A podle normy[30]. V objektu se nachází 4 ks úschovných objektů pro ukládání utajovaných informací. Jedná se skříňový trezor typu ASJ3E od společnosti T-Safe s. r. o.

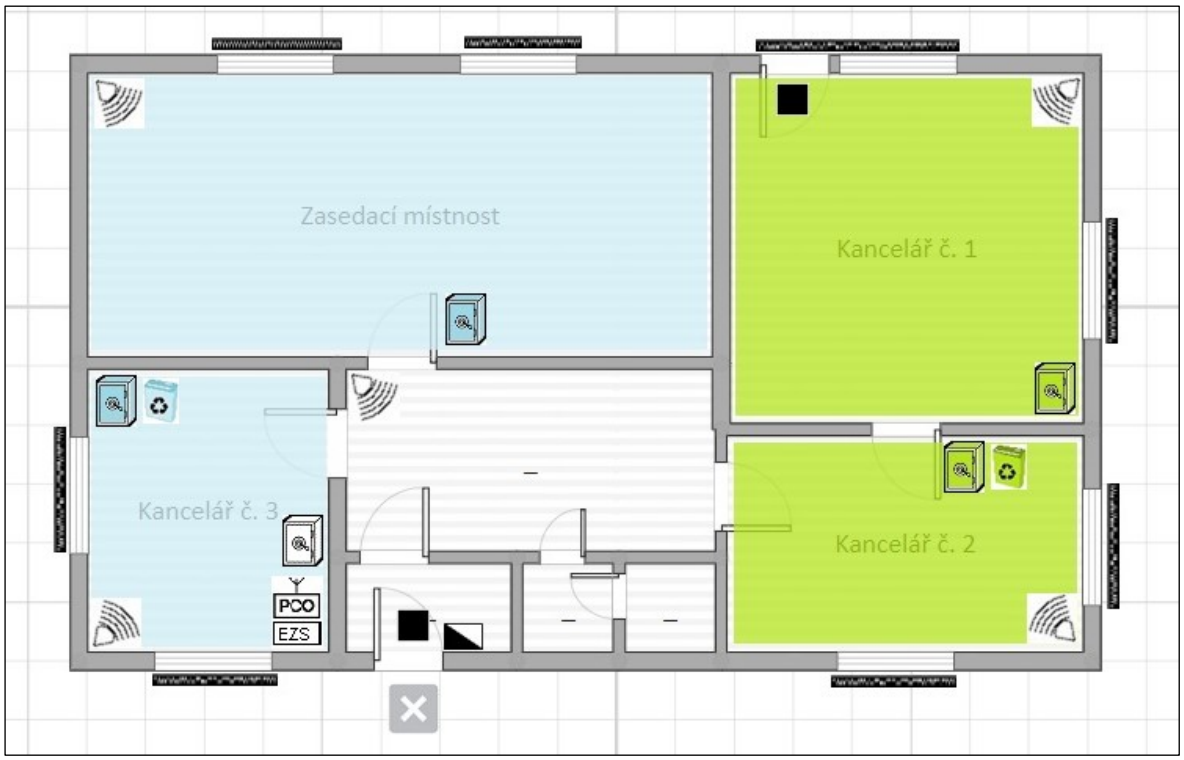
Tab. 29 Bodové hodnocení úschovného objektu S1 [zdroj: vlastní]

Název	**Typ**	**Bodové hodnocení**
Úschovné objekty	Typ 2	SS1 = 2 body
Zámky úschovných objektů	Typ 2	SS2 = 2 body
Celkové hodnocení	**S1 = SS1 x SS2**	**S1 = 4 body**

Ochrana utajované informace při jejím vzniku, potažmo při zpracování, je dána charakterem jejího vzniku. V případě zpracování utajované informace v certifikovaném IS, chrání takovou informaci původce utajované informace právě tím, že ji zpracovává v certifikovaném IS na zabezpečeném PC, na kterém je aplikována bezpečnostní politika pro danou kategorii utajované informace a prošel testem bezpečnosti a je schválen k provozu. Zákon pamatuje i na způsob zpracování utajované informace mimo certifikovaný IS, zejména na elektronických psacích strojích s pamětí, kopírkách apod. Pro tyto zařízení musí být zpracována bezpečnostní provozní směrnice, která musí obsahovat, jak takové zařízení bezpečně používat. Taková zařízení musí být umístněná tak, aby bylo zařízení chráněno před případnou neoprávněnou manipulací, poškození či ovlivnění činnosti. Dále je nutné zabezpečit, aby z daného zařízení nebylo možné utajovanou informaci odezírat.

V případě, že se takové zařízení používá pro zpracování utajovaných informací pro stupně utajení Důvěrné a vyšší, je nutné zabezpečit unik zpracovávaných informací kompromitujícím vyzařováním. Každé elektronické zařízení vysílá do svého okolí, při svém provozu, elektromagnetické vlny, které se dají zachytit, analyzovat a také zrekonstruovat do původní podoby. [4, 8] Opatření před unikem kompromitujícím vyzařováním, výrazně zasahuje také do oblasti bezpečnosti informačních a komunikačních systémů.

[29] Norma č. ČSN EN 1143-1+A1
[30] Norma č. ČSN EN 1300+A1



Obr. 12 Návrh zabezpečení v rámci administrativní bezpečnosti [zdroj: vlastní]


Úschovný objekt kategorie Vyhrazené


Úschovný objekt kategorie Důvěrné


Běžný úschovný objekt


Skartovací stroj – Vyhrazené


Skartovací stroj – Důvěrné

Dále jsou v objektu umístěny zařízení pro fyzické ničení nosičů utajovaných informací – skartovací stroje, které odpovídají typu 2 bez bodové hodnocení. Jedná se o skartovací stroje certifikované NBÚ pro ničení nosičů informací stupně utajení Důvěrné. Velikost odpadní částice v křížovém řezu ≤ 4,0 x 80,0 mm a v přímém řezu ≤ 2,0 x 297x0 mm s plochou částice do 320 mm^2. Tyto zařízení lze použít i pro ničení nosičů informace pro nižší stupeň utajení.

8.5 Návrh zabezpečení v rámci bezpečnosti informačních a komunikačních systémů

Zabezpečení informačních a komunikačních systému v podmínkách Policie ČR spravuje Bezpečnostní odbor ministerstva vnitra, který je garantem za ochranu utajovaných informací u Policie ČR. Bezpečnostní odbor žádá o certifikaci informačních systému, provádí testy bezpečnosti a povoluje provoz IS. Bezpečnostní politika informačních systémů, dokumentace a jejich nastavení je také předmětem utajení.

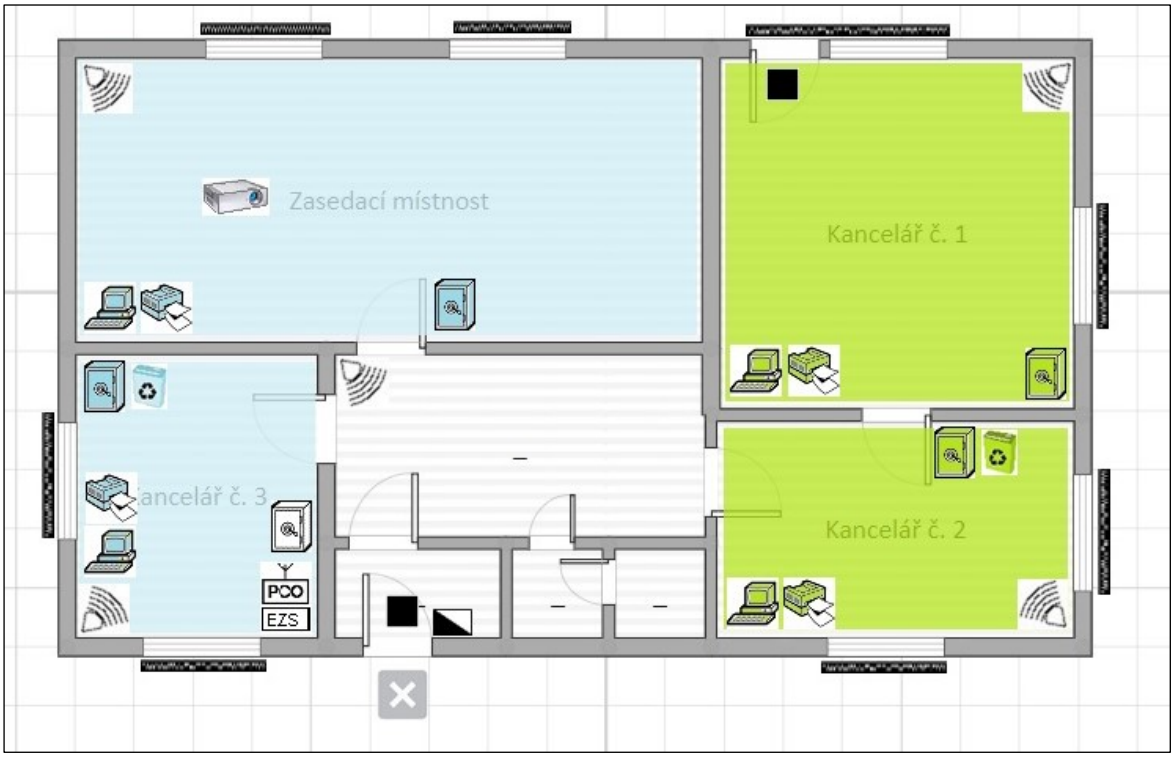
Uvnitř našeho objektu se nachází dva certifikované informační systémy, a to jak pro stupeň utajení Vyhrazené, tak i Důvěrné. Bezpečnosti je dosaženo jak správnou aplikaci bezpečnostních politik, tak i formou personální bezpečnosti a fyzické bezpečnosti. Počítače s informačními systémy jsou v zabezpečených oblastech příslušné kategorie. Pro přístup k jednotlivým PC jsou policisté určeni vedoucím odboru. Policisté musí být před prvním přihlášením a prací v IS seznámeni se směrnicí, která stanovuje určení IS, popisuje umístnění bezpečnostních prvků v podobě hologramů, které přelepují jednotlivé části PC soupravy tak, aby bylo patrné neoprávněné vniknutí do jednotlivých komponent PC soupravy. Směrnice také popisuje práva a povinnosti uživatelů IS. Každé přihlášení do IS musí uživatel zaznamenat do provozního deníku IS.

Přítomnost obou certifikovaných IS v zabezpečených oblastech, snižuje riziko zpracování utajované informace v soupravě pro nižší stupeň utajení, nebo na nezabezpečeném PC, případě mimo zabezpečenou oblast.

Riziko výpadku HW a SW lze minimalizovat přítomností více souprav pro příslušnou kategorii stupně utajení.

Riziko užití cizí identity v IS do jisté míry snižuje povinnost uživatele IS zaznamenat svou činnost v IS do provozního deníku soupravy. V případě podezření ze zneužití identity, může bezpečnostní správce pomocí vyhodnocení auditních záznamů a porovnání s informacemi v provozním deníku určit, zda činnost v IS (např. vznik, zpracování UI) provedla oprávněná osoba, či nikoliv. Zde přichází ještě v úvahu riziko selhání lidského faktoru, kdy policista nedodrží povinnost provést zápis v provozním deníku. Toto riziko ovšem nelze nikdy vyloučit, a jen opakovaná proškolení a kontrola pomůže policistům tuto povinnost zařadit do rutinní práce při zpracování utajovaných informací v certifikovaném IS.

Další míra snížení rizika zneužití identity, spočívá ve správně nastavených organizačních opatřeních a taky v tom, že se IS nachází v zabezpečených oblastech, jejichž vstupní dveře musí být vybaveny zámkovým systémem typu knoflík – klika a klíče musí být uloženy v zapečetěné krabičce a vydávány proti podpisu.



Obr. 13 Rozmístění IS v objektu [zdroj: vlastní]

 Dataprojektor

 IS – Vyhrazené

 IS – Důvěrné

 Tiskárna pro IS – Vyhrazené

 Tiskárna pro IS – Důvěrné

8.6 Závěrečné shrnutí

Cílem této kapitoly, bylo provést návrh zabezpečení fiktivního objektu z pohledu zákona o ochraně utajovaných informací a bezpečnostní způsobilosti. Vzhledem k tomu, že ochranu utajovaných informací tvoří souhrn jednotlivých druhů bezpečnosti dle zákona, nelze provádět zabezpečení objektu, pouze z jednoho pohledu. Cílem nebylo vytvořit projekt fyzické bezpečnosti, jak se dokument, který určuje objekt, zabezpečené oblasti a její hranice, kategorie a třídy zabezpečení, dle zákona nazývá. Mým cílem bylo provést zabezpečení objektu tak, aby splňoval požadavky NBÚ pro zpracování utajovaných informací ve stupni utajení Vyhrazené a Důvěrné a aby se v něm nacházeli veškeré dostupné prostředky, které zpracování utajovaných informací provází.

Samotnému návrhu zabezpečení předcházela analýza rizik, které se při nakládání s utajovanými informacemi můžou vyskytnou. Samotná analýza rizik byla provedena metodou KARS a její výsledky prezentovány formou grafů a tabulek.

ZÁVĚR

Cílem diplomové práce bylo popsat oblast ochrany utajovaných informací v podmínkách Policie České republiky a dále provést analýzu rizik ve vztahu k možnostem ohrožení nebo vyzrazení utajovaných informací. Motivací pro tuto práci bylo hlouběji prostudovat oblast ochrany utajovaných informací, zákony a vyhlášky, které tuto problematiku provází, dále stanovit stručný katalog rizik, se kterými lze nejčastěji setkat, provést analýzu a vyhodnocení a výsledky aplikovat do návrhu zabezpečení objektu, ve kterém se utajované informace zpracovávají. Cílem diplomové práce nebylo sestavit projekt fyzické bezpečnosti, tak jak se to běžně při posouzení bezpečnosti objektu a zabezpečených oblastí dělá, ale spíše prostudovat jednotlivé oblasti bezpečnosti z pohledu zákona o ochraně utajovaných informací.

Druhá část diplomové práce se věnuje praktické analýze rizik metodou stanovení míry rizika pomocí následku a hrozby. Ze základního katalogu hrozeb byly vytipovány nejvýznamnější rizika. Tyto rizika byla analyzována metodou kvalitativní analýzy rizik s využitím jejich souvztažností. Tuto metodu prezentoval Ing. Štefan Pacinda, Ph.D. ve své disertační práci, kterou zpracoval na Univerzitě obrany v Brně. Výsledky jsou prezentovány pomocí grafu s vyznačenými riziky. Dále jsou rizika sepsány do tabulky podle jejich významnosti. Rizika jsou vypsána, stručně charakterizovány a jsou navržena opatření ke zmírnění působení rizika.

Poslední část diplomové práce se věnuje návrhu zabezpečení z pohledu jednotlivých oblastí bezpečnosti tak, aby použité opatření a prostředky odpovídaly požadavkům NBÚ pro zpracování utajovaných informací v objektu a zabezpečených oblastech.

Během psaní této práce jsem si prohloubil znalost v oblasti řízení rizik, v oblasti ochrany utajovaných informací, v bodovém hodnocení jednotlivých požadavků na fyzickou bezpečnost a v neposlední řadě také ve zpracování návrhu zabezpečení zabezpečených oblastí, i když se tato problematika řeší jiným způsobem, a to vytvořením projektu fyzické bezpečnosti.

SEZNAM POUŽITÉ LITERATURY

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

[2] ČESKO. Zákon č. 412/2005 Sb. In: Zákony pro lidi.cz [online]. © AION CS 2010-2019 [cit. 18. 2. 2019]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-412

[3] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management I.* 1. vyd. Zlín*: VeRBuM,* 2011, 316 s. ISBN 978-80-87500-05-7.

[4] ČESKO. Vyhláška č. 523/2005 Sb. In: Zákony pro lidi.cz [online]. © AION CS 2010-2019 [cit. 19. 2. 2019]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-523.

[5] ČESKO. Vyhláška č. 528/2005 Sb. In: Zákony pro lidi.cz [online]. © AION CS 2010-2019 [cit. 25. 2. 2019]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-528

[6] ČESKO. Vyhláška č. 529/2005 Sb. In: Zákony pro lidi.cz [online]. © AION CS 2010-2019 [cit. 25. 2. 2019]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-529

[7] ČESKO. Nařízení vlády č. 522/2005 Sb. In: Zákony pro lidi.cz [online]. © AION CS 2010-2019 [cit. 19. 2. 2019]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-522

[8] BALOGH, Petr. *Ochrana informací před jejich únikem vlivem kompromitujícího vyzařování* [online]. Ostrava, 2018 [cit. 2019-02-21]. Dostupné z: http://hdl.handle.net/10084/128294. Diplomová práce. Vysoká škola báňská – Technická univerzita Ostrava.

[9] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. Praha: C.H. Beck, 2010. Velké komentáře. ISBN 978-80-7400-109-3.

[10] ČESKO. Vyhláška č. 528/2005 Sb. In: Zákony pro lidi.cz [online]. © AION CS 2010-2019 [cit. 24. 2. 2019]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-528

[11] *Ochrana utajovaných informací v ICT* [online]. [cit. 2019-02-24]. Dostupné z: https://nukib.cz/cs/ochrana-utajovanych-informaci-v-ict/

[12] Bezpečnostní odbor – Ministerstvo vnitra České republiky [online]. [cit. 2019-02-24]. Dostupné z: https://www.mvcr.cz/clanek/bezpecnostni-odbor.aspx

[13] ČESKO. § 137 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: Zákony pro lidi.cz [online]. © AION CS 2010-2019 [cit. 24. 2. 2019]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-412#p137

[14] ČESKO. § 137a zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: Zákony pro lidi.cz [online]. © AION CS 2010-2019 [cit. 24. 2. 2019]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-412#p137a

[15] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013. Expert (Grada), s. 10,1 ISBN 978-80-247-4644-9.

[16] PACINDA, Štefan. Analýza rizik, jeden ze základních nástrojů krizového managmentu při řešení nevojenských krizových situací. Brno, 2007. Disertační práce. Univerzita obrany.

[17] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík – VeRBuM, 2015. ISBN 978-80-87500-19-4.

[18] Metoda Delphi. In: ManagementMania.com [online]. Wilmington (DE) 2011-2019, 12.11.2018 [cit. 07.03.2019]. Dostupné z: https://managementmania.com/cs/metoda-delphi

[19] Variant Plus: Technické normy [online]. [cit. 2019-03-17]. Dostupné z: https://www.variant.cz/dokumenty/podpora/technicke-normy/

[20] Bezpečnostní poradce: Základní pojmy [online]. [cit. 2019-03-17]. Dostupné z: http://www.bepo.eu/component/k2/item/13-pzts-zakladni-pojmy

[21] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management. Zlín: Radim Bačuvčík – VeRBuM, 2015. ISBN 978-80-87500-57-6.

[22] Organizační a režimové opatření [online]. [cit. 2019-03-19]. Dostupné z: https://www.slu.cz/math/cz/knihovna/ucebni-texty/Ochrana-osob-a-majetku/Organizacni-a-rezimove-opatreni-a-fyzicka-ochrana.pdf/

[23] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management. Zlín: Radim Bačuvčík – VeRBuM, 2015. ISBN 978-80-87500-67-5.

[24] Příloha č. 1 k vyhlášce č. 528/2005 Sb., ve znění vyhlášky č. 204/2016 Sb. Www.nbu.cz [online]. [cit. 2019-05-06]. Dostupné z: https://www.nbu.cz/download/pravni-predpisy/container-nodeid-596/528novela2042016pr1.pdf

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BO	Bezpečnostní odbor
CCTV	Systém průmyslové televize
ČR	Česká republika
ČSN	Chráněné označení českých technických norem
DPPC	Dohledové a přijímací poplachové centrum
EN	Evropská norma
FO	Fyzická osoba
HW	Hardware – veškeré fyzické vybavení počítače
IS	Informační systém
KARS	Kvalitativní analýza rizik s využitím jejich souvztažností
MV	Ministerstvo vnitra
MZS	Mechanické zábranné systémy
NATO	Severoatlantická aliance
NBÚ	Národní bezpečnostní úřad
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PČR	Policie České republiky
PO	Právnická osoba
PZTS	Poplachový, zabezpečovací a tísňový systém
Sb.	Sbírka zákonů
SKPV	Služba kriminální policie a vyšetřování
SW	Software – programové vybavení počítače
TNI	Technické normalizační informace
UI	Utajovaná informace
UTB	Univerzita Tomáše Bati

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: TABULKA BODOVÉHO OHODNOCENÍ

Tabulka bodového ohodnocení opatření fyzické bezpečnosti v zabezpečené oblasti

Název zabezpečené oblasti: **Fiktivní objekt - Diplomová práce**

Kategorie: **Důvěrné** Míra rizika: malá Třída: **II.**

Utajovaná informace je ukládána v úschovném objektu v zabezpečené oblasti.

Bezpečnostní opatření		Typ	Bodové ohodnocení
Úschovné objekty		☐ T.4 - 4 body ☐ T.3 - 3 body ☒ T.2 - 2 body	SS1 = 2
Zámky úschovných objektů		☐ T.4 - 4 body ☐ T.3 - 3 body ☒ T.2 - 2 body	SS2 = 2
_____		☐ T.1 - T1.A - 1 bod ☐ T.1B - 2 body ☐ T.1C - 3 body	_____
Celkové hodnocení uschovného objektu a jeho zámku		*S1 = SS1 x SS2*	**S1 = 4**
Zabezpečené oblasti		☐ T.4 - 4 body ☐ T.3 - 3 body ☒ T.2 - 2 body ☐ T.1 - 1 bod	SS3 = 2
Uzamykací systémy zabezpečené oblasti		☐ T.4 - 4 body ☐ T.3 - 3 body ☒ T.2 - 2 body ☐ T.1 - 1 bod	SS4 = 2
Celkové hodnocení zabezpečené oblasti a jejího uzamykacího systému		*S2 = SS3 x SS4*	**S2 = 4**
Objekt		☐ T.4 - 4 body ☐ T.3 - 3 body ☐ T.2 - 2 body ☐ T.1 - 1 bod	**S3 = 0**
Kontrola vstupu		☐ T.4 - 4 body ☐ T.3 - 3 body ☐ T.2 - 2 body ☒ T.1 - 1 bod	SS6 = 1
Režim návštěv v objektu	*a) Návštěvy s doprovodem* *b) Návštěvy bez doprovodu* *c) Návštěvy bez kontroly*	☐ add a) - 3 body ☐ add b) - 1 bod ☒ add c) - 0 bodů	SS7 = 0
Celkové hodnocení kontroly vstupu		*S4 = SS6 + SS7*	**S4 = 1**
Ostraha		☐ T.5 - 5 bodů ☐ T.4 - 4 body ☐ T.3 - 3 body ☐ T.2 - 2 body ☒ T.1 - 1 bod	SS8 = 1
Zařízení elektrické zabezpečovací signalizace		☐ T.4 - 4 body ☐ T.3 - 3 body ☒ T.2 - 2 body ☐ T.1 - 1 bod	SS91 = 2
Instalace zařízení elektrické zabezpečovací signalizace		☐ T.4 - 4 body ☐ T.3 - 3 body ☐ T.2 - 2 body ☒ T.1 - 1 bod	SS91 = 1
Mezivýsledek (SS9)		*SS9=(SS91+SS92)/2xSS92/OBL*	SS9 = 1
Celkové ohodnocení ostrahy a systému EZS		*S5=SS8+SS9*	**S5 = 2**
Fyzické bariéry		☐ T.4 - 4 body ☐ T.3 - 3 body ☐ T.2 - 2 body ☐ T.1 - 1 bod	SS10 = 0
Kontrola vstupu v přístupových bodech fyzické bariéry	*a) kontrola je realizována* *b) kontrola není realizována*	☐ add a) - 1 bod ☒ add b) - 0 bodů	SS11 = 0
Namátkové vstupní a výstupní prohlídky	*a) prohlídky jsou prováděny* *b) prohlídky nejsou prováděny*	☐ add a) - 1 bod ☒ add b) - 0 bodů	SS12 = 0
Perimetrický detekční systém (PDS)	*- certifikovaný Úřadem* *- necertifikovaný Úřadem*	2 body 1 bod	SS13 = 0
Bezpečnostní osvětlení perimetru		2 body	SS14 = 0
Speciální televizní systém na perimetru		2 body	SS15 = 0
Celkové ohodnocení ochrany perimetru		*S6=(SS10xSS11)+SS12+SS13+ SS14+SS15*	**S6 = 0**

Výsledné hodnocení úrovně fyzické bezpečnosti

	Požadované hodnoty Míra rizika: malá	Vypočtené hodnoty
Povinné : (S1) + (S2) + (S3)	6	**8**
Povinné : (S4) + (S5)	2	**3**
Nepovinné : (S6)	3	**0**
Celkový výsledek	11	**11**

Splňuje na stupeň utajení: 'Důvěrné' - malé riziko