Ochrana utajovaných informací v objektu XY

Tereza Čížková, DiS.

Bakalářská práce
2021

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

*

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení

Akademický rok: 2020/2021

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Tereza Čížková, DiS.**
Osobní číslo:	**L18074**
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**Kombinovaná**
Téma práce:	**Ochrana utajovaných informací v objektu XY**

Zásady pro vypracování

1. Zpracujte teoretické a metodické poznatky týkající se ochrany utajovaných informací.
2. Analyzujte a zhodnoťte vybraný objekt z pohledu personální, administrativní a fyzické bezpečnosti.
3. Navrhněte a formulujte doporučení pro zlepšení zabezpečení ochrany utajovaných informací.

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

Seznam doporučené literatury:

1. BURDA, Karel. *Základy elektronických zabezpečovacích systémů.* CERM, 2018. ISBN 978-80-7204-967-7.
2. BRABEC, František. *Ochrana bezpečnosti podniku.* Praha: EUROUNION, 1996. ISBN 80-85858-29-0.
3. UHLÁŘ, Jan. *Technická ochrana objektů díl I.* Praha: Policejní akademie ČR, 2009. ISBN 9788072513123 8072513125.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Robert Pekaj**
Ústav krizového řízení

Datum zadání bakalářské práce: **1. prosince 2020**
Termín odevzdání bakalářské práce: **14. května 2021**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2020

PROHLÁŠENÍ AUTORA
BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji 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;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem 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 bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 14. 5. 2021

Jméno a příjmení studenta: Tereza Čížková, DiS.

.....
podpis studenta

ABSTRAKT

Hlavním tématem této bakalářské práce je ochrana utajovaných informací a problematika s ní spojen. V teoretické části práce jsou definovány základní pojmy, které úzce souvisí s daným tématem. Dále je zde přiblížena problematika personální, administrativní a fyzické bezpečnosti.

V praktické části je vybrán konkrétní objekt, který je popsán a následně zanalyzován z pohledu výše uvedených bezpečností. Pro sběr podkladů analýzy byla použita metoda brainstormingu. Samotná analýza byla provedena metodou FMEA (analýza možných vad a následků). V závěru je shrnuto zhodnocení bezpečnosti objektu a navrhnuta doporučení k většímu zabezpečení konkrétního objektu.

Klíčová slova: utajovaná informace, bezpečnost, personální bezpečnost, administrativní bezpečnost, fyzická bezpečnost

ABSTRACT

The main topic of this bachelor's thesis is the protection of classified information and issues related to it. The theoretical part of the thesis defines the basic concepts that are closely related to the topic. Furthermore, the issues of personnel, administrative and physical security are approached.

In the practical part, a specific object is selected, described and then analysed from the perspective of the above security. To collect the data for the analysis was used the method of brainstorming. The analysis itself was performed by the FMEA method (Failure Mode and Effect Analysis). In the end, I summarize the evaluation of the security of the object and I propose recommendations for greater security of a specific object.

Keywords: classified information, security, personnel security, administrative security, physical security

Ráda bych poděkovala svému vedoucímu bakalářské práce Ing. Robertu Pekajovi. Velice si vážím jeho vstřícnosti, ochoty a času, který si vyčlenil pro vedení této bakalářské práce i přesto, že ho měl velmi málo.

„Kde chybí informace, kvetou drby.“

- Stanislav Komenda

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

OBSAH

ÚVOD

Informace jako nejsilnější zbraň dnešní doby. Informaci, v jakékoli podobě, lze zneužít, přetvořit nebo také předat dále někomu, komu správná informace může i zachránit život. Předávání informací je každodenní chléb každého člověka. Ať už se jedná o obyčejný rozhovor mezi kamarády nebo sepisovaní knižního bestselleru. Při každé činnosti nepřetržitě každý den všichni lidé svým jednáním, mluvením nebo psaním předávají určité spektrum informací, které nemusí být důležité, nebo naopak, mohou tyto velice uškodit. Proto je potřeba určité informace chránit. Z tohoto důvodu došlo ke vzniku seznamu informací, které jsou veřejnosti nepřístupné a mají režim utajení (utajované informace), a zákona o jejich ochraně (zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti). Autorka této bakalářské práce se bude věnovat problematice utajovaných informací a jejich ochraně ve vybraném objektu, který těmito informacemi disponuje.

Cílem této bakalářské práce je přiblížit problematiku ochrany utajovaných informací a zanalyzovat, jak vybraný objekt tyto utajované informace chrání.

Bakalářská práce je členěna na teoretickou a praktickou část. Teoretická část obsahuje pět kapitol, které přibližují teoretické znalosti problematiky bakalářské práce. První kapitola vysvětluje základní pojmy: utajovaná informace, bezpečnost, poplachový zabezpečovací a tísňový systém a mechanické zábranné prostředky. Následně druhá, třetí a čtvrtá kapitola objasňují základní typy bezpečností, které musí být dodrženy při jakékoli manipulaci s utajovanými informacemi. Jedná se o personální bezpečnost, administrativní bezpečnost a fyzickou bezpečnost. V poslední kapitole teoretické části je pak přiblížena metoda analýzy, která je použita v praktické části práce.

Praktická část bakalářské práce se věnuje vybranému objektu nejmenované státní instituce, ve které je manipulováno s utajovanými informacemi a kde jsou tyto informace uloženy. Dále praktická část popisuje nastavení personální, administrativní a fyzické bezpečnosti v objektu a zobrazuje rozložení prvků fyzické bezpečnosti, tj. rozložení mechanických zábranných prostředků a prvků poplachové zabezpečovací signalizace. V závěru praktické části je provedena samotná analýza rizik metodou FMEA (analýza možných vad a jejich následků) a následné vymezení opatření a zhodnocení celé bezpečnosti vybraného objektu.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ POJMY

První kapitola pojednává o základních pojmech, které souvisejí s touto bakalářskou prací a jsou důležité k pochopení problematiky ochrany utajovaných informací. Jsou zde vysvětleny pojmy utajovaná informace, bezpečnost, poplachový zabezpečovací a tísňový systém a mechanické zábranné prostředky.

1.1 Utajovaná informace

Obecná definice pojmu informace má samozřejmě mnoho významů. Ten nejobecnější výklad je, že informace je určité sdělení, zpráva nebo souhrn údajů a poznatků, které se mohou určitým způsobem předávat. Informace jsou tedy určitá data, sdělení, vědomosti, znalosti, údaje, které dokážeme zachytit svými smysly a dokážeme jim rozumět, respektive pro nás mají smysl nebo určitý význam. Tato data mají určitý kontext, obsah, rozsah, kvalitu a mají pro příjemce klíčový význam. Informace jsou velmi cenným aktivem, který člověk může vlastnit. (Barták, Bečvář a Bechyně et al., 1999), (Informace a informační instituce, 2018)

Utajovaná informace je už pojem, který je přesně definovaný a vymezený zákonem číslo 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Tento zákon utajovanou informaci definuje v § 2 písm. a) *jako informaci v jakékoli podobě zaznamenanou na jakémkoliv nosiči označenou v souladu s tímto zákonem. Její vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro zájem nevýhodné. Tato informace je uvedena v seznamu utajovaných informací (§ 139)*. (Česko, 2005)

Utajované informace jsou pouze takové informace, které jsou zapsané v seznamu utajovaných informací. Návrh tohoto seznamu zpracovává Národní bezpečnostní úřad. Následně vláda svým nařízením tento seznam vydá. Dále to jsou takové informace, které současně musí splňovat všechny formální i materiální znaky. Formální znaky jsou dány nařízením vlády. Pokud některý povinný znak nebude utajovaná informace obsahovat, o utajovanou informaci se v tomto případě nejedná. (Dvořák, Chrobák, 2018)

1.1.1 Formální znaky

Jak už bylo řečeno, utajovaná informace musí obsahovat určité znaky, aby byla za utajovanou informaci považována.

Prvním formálním znakem je, že utajovaná informace musí být nějakým způsobem zaznamenána. V zákoně se dočteme, že by měla být zaznamenána v jakékoliv podobě a na jakémkoliv nosiči. To záleží na autorovi utajované informace. (Dvořák, Chrobák, 2018)

V pořadí druhým formálním znakem se myslí, že utajovaná informace musí být řádně označena v souladu se zákonem 412/2005 Sb., o ochraně utajovaných informací. Bohužel tento zákon neobsahuje řádný paragraf, který by tento formální znak dále vymezil a stanovil způsob, jak přesně utajovanou informaci označit. Zákon pouze obsahuje § 4, který vymezuje stupně utajení, a dále hlavu IV. Administrativní bezpečnost, která obsahuje § 21 a § 22. Tyto dva paragrafy upravují vyznačování údajů na utajované informaci, evidenci a vyznačení stupně utajení. (Dvořák, Chrobák, 2018), (Česko, 2005)

Dalším a zároveň posledním formálním znakem utajované informace je skutečnost, že tato informace musí být zapsána v seznamu utajovaných informací. Zákon 412/2005 Sb., o ochraně utajovaných informacích a bezpečnostní způsobilosti, odkazuje na § 139, ve kterém se píše, že Národní bezpečnostní úřad zpracovává návrh na seznam utajovaných informací, dále pak vláda vydá seznam utajovaných informací prostřednictvím svého nařízení. V současné době je účinné od 1. 1. 2006 nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. V tomto seznamu je každá utajovaná informace klasifikována do skupin jednotlivých úřadů, kterého se utajovaná informace týká, a do stupně utajení nebo do rozsahu stupňů utajení. (Dvořák, Chrobák, 2018), (Česko, 2005)

Návrh, co patří do seznamu utajovaných informací, podávají jednotlivé úřady, jako jsou například ministerstva, Bezpečnostní informační služba ČR, Vojenské zpravodajství ČR, Parlament ČR, Česká národní banka apod. (Dvořák, Chrobák, 2018), (Česko, 2005)

Stupně utajení

Jak již bylo zmíněno výše, jedním ze znaků utajovaných informací je vymezení jejich stupňů utajení. Stupně utajení vymezuje zákon č. 412/2005 Sb. v § 4. Pod tímto stupněm utajení je pak daná informace zapsána v seznamu utajovaných informací. Stupně utajení se přiřazují určité informaci na základě toho, jakou by vyzrazení této informace způsobilo újmu České republice.

Rozlišují se čtyři stupně utajení:

1) Vyhrazené
2) Důvěrné

3) Tajné
4) Přísně tajné

Stupeň utajení Vyhrazené je sice závažný, ale nese nejmenší riziko ze všech čtyř stupňů. Utajovaná informace je vyhrazená, jestliže její vyzrazení nebo zneužití neoprávněnou osobou může být nevýhodné pro zájmy České republiky.

Další stupeň utajení je Důvěrné. Stupeň Důvěrné je už více závažný. Vyzrazení nebo zneužití důvěrné informace neoprávněnou osobou by mohlo způsobit prostou újmu zájmům České republiky.

Druhým nejzávažnějším stupněm utajení je stupeň Tajné. Zde už vyzrazení nebo zneužití utajované informace může způsobit vážnou újmu České republice.

Nejzávažnějším stupněm utajení je klasifikace Přísně tajné. Tento stupeň je nejpřísněji trestán a může způsobit největší škodu. Znamená to, že když neoprávněná osoba vyzradí nebo zneužije utajovanou informaci, může způsobit mimořádně závažnou újmu zájmům České republiky. (Česko, 2005)

1.1.2 Materiální znaky

Mezi materiální znak se řadí skutečnost, že utajovaná informace může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodná, pokud bude tato informace vyzrazena nebo zneužita. (Dvořák, Chrobák, 2018), (Česko, 2005)

Újmy zájmu České republiky

Přesné pojmy újma zájmu České republiky nebo nevýhodnost pro tyto zájmy jsou vymezeny v § 3 zákona č. 412/2005 Sb. Tento paragraf definuje, že újmou zájmu ČR se rozumí poškození nebo ohrožení zájmu ČR. Dle závažnosti poškození nebo ohrožení zájmu se újma člení na mimořádně vážnou újmu, vážnou a prostou újmu. V návaznosti na toto rozčlenění je pak utajovaná informace klasifikována stupněm utajení. (Dvořák, Chrobák, 2018), (Česko, 2005)

Mimořádně vážná újma

Tato újma vznikne vyzrazením utajované informace neoprávněné osobě nebo zneužitím utajované informace, které může mít za následek:

a) bezprostřední ohrožení svrchovanosti, územní celistvosti nebo demokratických základů ČR,

b) rozsáhlé ztráty na lidských životech nebo rozsáhlé ohrožení zdraví obyvatel,
c) mimořádně vážné nebo dlouhodobé poškození ekonomiky ČR,
d) značné narušení vnitřního pořádku a bezpečnosti ČR,
e) mimořádně vážné ohrožení významných bezpečnostních operací nebo činnosti zpravodajských služeb,
f) mimořádně vážné ohrožení činnosti Organizace Severoatlantické smlouvy, EU nebo členského státu,
g) mimořádně vážné ohrožení bojeschopnosti ozbrojených sil ČR, Organizace Severoatlantické smlouvy nebo jejího členského státu nebo členského státu EU,
h) mimořádně vážné poškození diplomatických nebo jiných vtahů ČR k Organizaci Severoatlantické smlouvy, EU nebo členského státu. (Česko, 2005)

Vážná újma

Vážná újma vznikne opět z důvodu vyzrazení nebo zneužití utajované informace neoprávněnou osobou. Následky tohoto jsou vymezeny v zákoně jako:

a) ohrožení svrchovanosti, územní celistvosti a demokratických základů ČR,
b) značnou škodu ČR ve finanční, měnové nebo hospodářské oblasti,
c) ztráty na lidských životech nebo ohrožení zdraví obyvatel,
d) narušení vnitřního pořádku a bezpečnosti ČR,
e) vážné ohrožení bojeschopnosti ozbrojených sil ČR, Organizace Severoatlantické smlouvy nebo jejího členského státu nebo členského státu EU,
f) vážné ohrožení významných bezpečnostních operací nebo činnosti zpravodajských služeb,
g) vážné ohrožení činnosti Organizace Severoatlantické smlouvy, EU nebo členského státu,
h) vážné narušení diplomatických vtahů ČR k Organizaci Severoatlantické smlouvy, EU nebo členskému státu nebo jinému státu,
i) vážné zvýšení mezinárodního napětí. (Česko, 2005)

Prostá újma

Prostá újma je poslední v pořadí a je nejméně závažná. Tato újma opětovně vznikne, jako obě předchozí, tím způsobem, že se utajená informace dostane k neoprávněné osobě a tato osoba ji vyzradí nebo zneužije. Za následek se považuje:

a) zhoršení vztahů ČR s cizí mocí,

b) ohrožení bezpečnosti jednotlivce,
c) ohrožení bojeschopnosti ozbrojených si ČR, Organizace Severoatlantické smlouvy nebo jejího členského státu nebo členského státu EU,
d) ohrožení bezpečnostních operací nebo činnosti zpravodajských služeb,
e) ohrožení činnosti Organizace Severoatlantické smlouvy, EU nebo jejich členského státu,
f) zmaření, ztížení nebo ohrožení prověřování nebo vyšetřování zvlášť závažných zločinů nebo usnadnění jejich páchání,
g) vznik nezanedbatelné škody ČR,
h) závažné narušení ekonomických zájmů ČR. (Česko, 2005)

1.2 Bezpečnost

Pojem bezpečnost je v dnešní době velmi častý a čím dál více používaný. Existuje mnoho druhů bezpečností, jako je například vnitřní bezpečnost, vnější bezpečnost, požární, jaderná, zdravotní, bezpečnost práce a mnoho dalších. Všechny tyto bezpečnosti mají v názvu stejný pojem „bezpečnost“. Mají také velice podobnou definici, avšak v konečné fázi jsou jejich cíle velice rozdílné. Bezpečnost je také závislá na čase a vývoji společnosti. Je tedy velmi těžké tento pojem uchopit v nejobecnější možné míře.

Nejlépe tento pojem můžeme chápat tak, že bezpečnost představuje stav, kdy je určitý systém schopný odolávat vnitřním a vnějším hrozbám, které zná a které může předvídat. Systém je schopný odolávat tak, že se zachová jeho struktura, stabilita a spolehlivost. (Definice bezpečnosti)

Další definici vymezil Miroslav Mareš, který bezpečnost chápe jako určitý stav, při kterém jsou hrozby pro daný objekt a jeho zájmy eliminovány na co nejnižší možnou míru a daný objekt je k této eliminaci stávajících a potencionálních hrozeb efektivně vybaven a popřípadě ochoten při ní spolupracovat. (Sak, 2018)

Bezpečnost je také v komplexním pojetí chápána jako nějaký souhrn opatření, které slouží pro ochranu a zároveň pro rozvoj chráněného zájmu. Bezpečnost tedy vytváří základnu pro veškerý rozvoj. (Procházková, 2006)

Pro účely této práce je důležité vymezit pojem bezpečnost informací nebo také informační bezpečnost. Informační bezpečnost je v podstatě jakákoli ochrana určité fyzické nebo

elektronické informace před zničením, zneužitím, upravením, zveřejněním nebo neoprávněným přístupem k ní. (What is Inforamtion Security?, 2020)

Také tuto bezpečnost můžeme chápat jako sadu postupů určených k ochraně informací (dat) před neoprávněným přístupem nebo změnami, a to jak při ukládání, tak při přenosu z bodu A do bodu B, ať už oba body zobrazují stroj nebo prostor, kde bude informace uložena. (Fruhlinger, 2020)

Rizika, která by mohla ohrozit důležité informace dané instituce, mohou pocházet zevnitř i zvenčí. Dnes je mnohem více možností, jak informace získat. Je to především způsobeno rychlým vývojem IT technologií. Proto je silné zabezpečení velmi důležitým článkem každé instituce. Cílem a úkolem informační bezpečnosti je tedy především stanovit zásady bezpečné práce s informacemi, které jsou nějakým způsobem důležité pro subjekt, který je potřebuje chránit. Musí se stanovit zásady pro informace všech typů a druhů. Jde například o zásady skartace informací, jak fyzických, tak elektronických, dále o archiv informací, nakládání s informacemi při přemísťování nebo při transportu a také zásady zveřejňování informací. Ať už bude informace sebevíc chráněna technickými i fyzickými prostředky, bohužel za zneužití informace, ve většině případů, může převážně lidský faktor. Lidé jsou nejčastěji iniciátory úniku informací a dat. Jejich neznalost, nedbalost, neopatrnost a záměr ovlivňují spolehlivost počítačových systémů. (Brabec et al., 2001), (Doucek et al., 2011), (Information security, 2018)

1.3 Poplachový zabezpečovací a tísňový systém

Poplachové zabezpečovací a tísňové systémy se řídí základní normou ČSN EN 50 131-1. Jedná se o elektronické bezpečnostní systémy, které zajišťují ochranu v oblasti života, zdraví a hlavně majetku osob, společností a státních institucí. Hlavním úkolem těchto systémů je včasně detekovat a upozornit na hrozící nebo již vzniklou nežádoucí událost kontrolované oblasti. Kontrolovanou oblastí se rozumí převážně chráněný majetek, který má majitel pod svojí kontrolou. Nežádoucí událost je obvykle vniknutí do kontrolované oblasti neoprávněnou osobou, únik z kontrolované oblasti (např. útěk z věznice), neoprávněná manipulace s chráněným předmětem nebo detekce požáru, úniku vody či úniky nebezpečného plynu. (Pokorný, 2019), (Burda, 2017)

Výše uvedená norma stanoví čtyři stupně zabezpečení dle předpokládaného stupně rizika. Jedná se o nízké riziko, nízké až střední riziko, střední až vysoké riziko a vysoké riziko. Každý stupeň zabezpečení obsahuje minimální požadavky, které musí poplachový systém

splnit, aby mohl být zařazen do příslušného stupně zabezpečení. Jedná se především o technické komponenty, které zajišťují a předávají informace v daném objektu, kde jsou naistalovány. Monitorují a detekují incidenty nebo změny v chráněném prostředí. Celý tento systém je soubor zařízení, který je složený z mnoha částí. Tyto části pak tvoří komplexní zabezpečovací řetězec. Základním prvkem celého řetězce je ústředna, která vše řídí a vyhodnocuje. Na ústřednu jsou následně napojeny detektory, různé druhy čidel, tísňová tlačítka, napájecí zdroje, ovládací prvky a další druhy signalizace. (Zabezpečte svůj majetek opravdu pořádně - PZTS, © 2021), (Poplachový zabezpečovací a tísňový systém (PZTS), (Zabezpečovačka neboli PZTS: Co to je a k čemu slouží?), (Kameník, Brabec a kolektiv, 2019)

1.4 Mechanické zábranné prostředky

Mechanické zábranné prostředky jsou prostředky, které poskytují ochranu především pro prostory areálu, budovy nebo chráněného objektu. Jedná se o ploty, zdi, závory, branky, mříže, bezpečnostní fólie, bezpečnostní skla, bezpečnostní dveře, zámky různých druhů, trezory apod. Tyto prostředky chrání objekt svojí mechanickou pevností. Jejich hlavním úkolem je vytvořit pevnou hranici nebo překážku tak, aby potencionálnímu pachateli vznikla co nejdelší doba na jejich překonání. Chrání především před:

- násilným vniknutím osoby do chráněné zóny,
- znehodnocením, poškozením nebo odcizením techniky uvnitř chráněné zóny,
- krádeží předmětů z chráněné zóny,
- umístěním nebezpečného předmětu nebo materiálu v chráněné zóně.

Bohužel každý mechanický zábranný prostředek je nějakým způsobem překonatelný. Jejich odlišnost je pouze v tom, jakou potencionální pachatel vynaloží energii, čas a nástroje k jejich překonání. (Uhlář, 1995)

2 PERSONÁLNÍ BEZPEČNOST

Personální bezpečnost se řadí mezi základní druhy zajištění ochrany utajovaných informací. Je to v podstatě výběr nebo vymezení fyzických osob, které mají mít přístup k utajovaným informacím. Podmínkou pro tento přístup je, že každá takto oprávněná fyzická osoba musí splňovat zákonem stanovené podmínky. (Dvořák, Chrobák, 2018), (Obecně k personální bezpečnosti)

Cílem personální bezpečnosti je tedy zajistit, aby k utajovaným informacím měla přístup pouze ta fyzická osoba, která je nezbytně potřebuje ke své pracovní činnosti. Této osobě musí být vydáno potřebné oprávnění od Národního bezpečnostního úřadu s utajovanými informacemi pracovat. Každá osoba, která má přidělené oprávnění, je podřízena své odpovědné osobě. Odpovědná osoba ručí za každoroční proškolení své podřízené osoby a vede o tom záznamy. Pod tímto se skrývá celý systém opatření a eliminace hrozeb způsobených selháním lidského faktoru. Personální bezpečnost rovněž zajišťuje ochranu osob, které jsou seznamovány s citlivými informacemi (Rodryčová, Staša, 2000), (Dobda, 1998)

Každá fyzická osoba, která potřebuje mít přístup k utajovaným informacím, musí splnit zákonem stanovené podmínky a podstoupit prověrku osoby. S tímto úzce souvisí stupně utajení. Jiné podmínky jsou pro přístup k utajovaným informacím, které mají stupeň utajení Vyhrazené, a jiné podmínky jsou pro přístup k utajovaným informacím, které mají stupeň utajení Důvěrné, Tajné a Přísně tajné. Podle toho, k jakému stupni utajení utajované informace bude mít osoba přístup, se určí rozsah a způsob prověření, které musí fyzická osoba splnit, aby jí byl umožněn přístup k utajované informaci. Ke stupni Vyhrazené se vydává oznámení o splnění podmínek pro přístup k utajované informaci. K dalším stupňům utajení je vydáno osvědčení fyzické osoby. Veškeré podmínky jsou zobrazeny v následující tabulce (Tab. 1). (Obecně k personální bezpečnosti), (Česko, 2011)

Tabulka 1 Podmínky pro stupně utajení

Podmínky	Vyhrazené (oznámení)	Důvěrné, Tajné, Přísně tajné (osvědčení)
Svéprávnost	Ano	Ano

Podmínky	Vyhrazené (oznámení)	Důvěrné, Tajné, Přísně tajné (osvědčení)
Věk minimálně 18 let	Ano	Ano
Bezúhonnost	Ano	Ano
Státní občanství ČR, země EU, NATO	Ne	Ano
Osobní způsobilost	Ne	Ano
Bezpečnostní spolehlivost	Ne	Ano

(Obecně k personální bezpečnosti)

Toto jsou pouze základní parametry, které musí osoba splňovat. U stupně utajení Vyhrazené ověřuje podmínky odpovědná osoba, která byla fyzické osobě přidělena. Prověrka nebo také bezpečnostní řízení obsahuje daleko podrobnější zkoumání a prověřování a provádí se u stupně utajení Důvěrné, Tajné a Přísně tajné. Toto bezpečnostní řízení provádí Národní bezpečnostní úřad na základě odůvodněné žádosti, dále zpravodajské služby pro své příslušníky, zaměstnance nebo uchazeče a Ministerstvo vnitra pro vybrané příslušníky policie České republiky, kteří plní závažné úkoly. (Obecně k personální bezpečnosti)

3 ADMINISTRATIVNÍ BEZPEČNOST

Administrativní bezpečnost se také řadí mezi základní druhy bezpečností, které zajišťují ochranu utajovaných informací. Dle zákona 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, a dále dle Národního bezpečnostního úřadu se jedná o systém opatření, která se uplatňují při jakékoli manipulaci s utajovanými informacemi, tj. při tvorbě, příjmu, evidenci, zpracování odesílání, přepravě, přenášení, ukládání, archivaci, skartaci a jiném nakládání s utajovanými informacemi. Administrativní bezpečnost také dále podléhá vyhlášce číslo 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací. (Informace), (Česko, 2005)

Do administrativní bezpečnosti spadají tedy určitá pravidla, která se musí dodržovat při manipulaci s utajovanou informací. Tato pravidla se vztahují především na hmotný nosič, který utajovanou informaci obsahuje. Jde o pravidla řádného označení, evidence, přenášení, ukládání, předávání, zánik a zničení nosiče. Existují nosiče obrazové, zvukové, listinné nebo také elektronické. (Dvořák, Chrobák, 2018)

Každá utajovaná informace, respektive její nosič, musí být řádně označen stanovenými předepsanými náležitostmi. Mezi tyto náležitosti se řadí:

- název původce utajované informace,
- stupeň utajení (Vyhrazené, Důvěrné, Tajné, Přísně tajné),
- evidenční označení (číslo jednací),
- datum vzniku utajované informace. (Dvořák, Chrobák, 2018), (Česko, 2005)

Pro jakoukoli manipulaci s utajovanými informacemi se používají tzv. administrativní pomůcky, které stanoví vyhláška č. 529/2005 Sb., o administrativní bezpečnosti. Za administrativní pomůcky se považují například jednací protokoly, pomocné jednací protokoly, manipulační knihy, doručovací knihy, zápůjční knihy, kontrolní listy a sběrné archy apod. Všechny použité pomůcky musí evidovat pověřená osoba a nakládat s nimi způsobem, který zajišťuje jejich ochranu proti zneužití nebo ztrátě. (Česko, 2005)

Manipulace s utajovanými dokumenty se stupněm utajení Vyhrazené má jiné podmínky a pravidla při příjmu zásilky, evidenci, vyhotovení, přípravě zásilky k přepravě, přepravě zásilky a přenášení dokumentu než utajované dokumenty se stupněm utajení Důvěrné, Tajné a Přísně tajné.

STUPEŇ UTAJENÍ

UTAJOVAT DO:

Název orgánu státu,
právnické osoby nebo
jméno a příjmení podnikající fyzické osoby

Datum a místo vzniku

Výtisk č. (Výtisk jediný)
Počet listů:
Přílohy utajované: *)
Přílohy neutajované: *)

Č. j.:/ Jiné ev.ozn.:

……
.....obsah……
……

STUPEŇ UTAJENÍ

číslo listu nebo stránky**)

*) Uvádí se pouze, pokud utajovaný dokument přílohy obsahuje.
**) Umístění čísla listu nebo stránky nemusí být uprostřed.“.

Obrázek 1 Vzor přední strany utajovaného dokumentu (Česko, 2005)

Doručovací kniha

Datum	Č. j. nebo jiné ev. ozn.*)	Název orgánu státu, právnické osoby nebo jméno a příjmení podnikající fyzické osoby příjemce	Příjmení a podpis

*) Nehodící se škrtněte.
Na štítku doručovací knihy se uvede období, kdy byla používána, název orgánu státu, právnické osoby nebo jméno, příjmení a místo podnikání v případě podnikající fyzické osoby, evidenční označení doručovací knihy a případně záznam, ke kterému jednacímu protokolu je používána (jeho evidenční označení).“.

Obrázek 2 Vzor doručovací knihy (Česko, 2005)

4 FYZICKÁ BEZPEČNOST

Fyzická bezpečnost je další základní druh zajištění ochrany utajovaných informací. Tuto bezpečnost tvoří celý systém opatření, která mají zabránit, zamezit nebo co nejvíce ztížit přístup neoprávněné osobě k utajovaným informacím, popřípadě tento pokus neoprávněné osoby o přístup k utajované informaci zaznamenat, a v konečném důsledku tak zabránit poškození, zcizení nebo jinému ohrožení utajované informace. Dále fyzická bezpečnost zajišťuje ochranu proti náhodným a úmyslným hrozbám jakéhokoli druhu. (Informace k fyzické bezpečnosti), (Kloboučková, © 2017)

Problematiku fyzické bezpečnosti vymezuje zákon č. 412/2005 Sb., o utajovaných informacích a o bezpečnostním řízení, a dále je to vyhláška Národního bezpečnostního úřadu č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků. (Informace k fyzické bezpečnosti)

Ve fyzické bezpečnosti utajovaných informací se rozlišují objekty, zabezpečené oblasti a jednací oblasti. (Informace k fyzické bezpečnosti)

4.1 Objekt a jeho zabezpečení

Zákon č. 412/2005 Sb., o utajovaných informacích, objekt definuje jako budovu nebo případně jako jiný ohraničený prostor, ve kterém se nejčastěji nacházejí zabezpečené oblasti a jednací oblasti. Vyhláška NBÚ č. 528/2005 Sb., o fyzické bezpečnosti, tuto definici potvrzuje a opakuje s tím rozdílem, že následně vymezuje hranici objektu, pláště budov, vstup do objektu apod. Objekt je tedy obecně ohraničený prostor, který slouží k tomu, aby zde mohlo být bezpečně manipulováno s utajovanými informacemi. Hranici objektu vždy určuje k tomu odpovědná osoba nebo jí pověřená osoba. Zabezpečení objektu závisí na kategorii objektu, kde se zohledňuje charakter hranice daného objektu. Dále se vyhodnocují rizika, která by mohla nastat. Zohledňují se zde také stupně utajení utajovaných informací, se kterými bude v objektu manipulováno. Jednotlivé stupně utajení pak určují jednotlivé kategorie zabezpečení objektu. Objekt je následně přiřazen do kategorie dle nejvyššího stupně utajení utajované informace, se kterou bude v objektu manipulováno. Pro nejnižší kategorii Vyhrazené jsou určeny pouze mechanické zábranné prostředky. Pro stupeň utajení Důvěrné a Tajné určuje kategorii objektu Důvěrnou a Tajnou a zde musí být použito kromě mechanických zábranných prostředků dále i zařízení elektrické zabezpečovací signalizace. Poslední kategorii určuje stupeň utajení Přísně tajné a to na kategorii Přísně tajnou. Objekt v této nejvyšší kategorii musí pro své zabezpečení použít jak mechanické zábranné

prostředky a zařízení elektrické zabezpečovací signalizace, tak i speciální televizní systémy, které ovšem nesmí narušit ochranu utajovaných informací. Vše se řídí vyhláškou 528/2005 Sb., o fyzické bezpečnosti. (Česko, 2005), (Česko, 2005), (Informace k fyzické bezpečnosti), (Dvořák, Chrobák, 2018)

4.2 Zabezpečené oblasti a jejich zabezpečení

Zabezpečenou oblastí je pak dle zákona 412/2005 Sb., o ochraně utajovaných informací, chápán ohraničený prostor v objektu, který slouží především k ukládání utajovaných informací. V těchto oblastech se mohou vyskytovat úschovné objekty (trezory) nebo různé úložné a uzamykatelné schránky. Úroveň zabezpečení těchto oblastí závisí na kategorii oblasti, třídě oblasti a dále na vyhodnocení rizik, která by mohla nastat. Také se zohledňuje nejvyšší stupeň utajované informace, která bude v této zabezpečené oblasti uložena. Stejně jako u zabezpečení objektu, tak i zde jsou určeny tři kategorie, dle vyhlášky 528/2005 Sb., o fyzické bezpečnosti, zabezpečených oblastní dle stupně utajovaných informací. První a nejnižší kategorie je Vyhrazené. Zde opět musí být použito mechanických zábranných prostředků. Pro další kategorii Důvěrné a Tajné již k mechanickým zábranným prostředkům musí být přidáno zařízení s elektronickou zabezpečovací signalizací. U kategorie Přísně tajné je zabezpečení na nejvyšším stupni. Zde jsou použity mechanické zábranné prostředky, zařízení elektronické zabezpečovací signalizace, speciální televizní systémy, které by opět neměly narušit ochranu utajovaných informací. Dále by zde měl být uplatněn systém kontroly vstupů a zařízení elektronické požární signalizace. Třídy zabezpečených oblastí rozlišujeme pouze dvě, a to třídu I a II. U těchto tříd je rozhodující, zda se v zabečené oblasti seznamujeme, nebo neseznamujeme s utajovanou informací. U třídy I platí, že se vstupem do této zabezpečené oblasti se zároveň budeme seznamovat s utajovanou informací. Míra zabezpečení všech oblastí v objektu se určuje pomocí bodových hodnot v závislosti na vyhodnocení rizik. Bodové hodnocení je vymezeno v příloze č. 1 vyhlášky 528/2005 Sb. (Česko, 2005), (Kloboučková, © 2017), (Česko, 2005)

4.3 Jednací oblasti a jejich zabezpečení

Jednací oblastí je dle zákona 412/2005 Sb., o utajovaných informacích, chápán ohraničený prostor v objektu, který slouží k projednávání utajovaných informací. Utajované informace, které mají stupeň utajení Tajné a Přísně tajné, se musí vždy projednávat v těchto jednacích oblastech (místnostech). Úroveň zabezpečení jednacích oblastí závisí na stupni utajovaných informací, které jsou zde pravidelně projednávány, a dále na vyhodnocení rizik, která by

mohla nastat. Při projednávání utajovaných informací stupně Tajné nebo Přísně tajné musí být jednací oblast (místnost) zabezpečena mechanickými zábrannými prostředky, systémem pro kontrolu vstupů, zařízením elektronické zabezpečovací signalizace, speciálními televizními systémy, elektronickou požární signalizací a nakonec zařízením, které brání pasivnímu i aktivnímu odposlechu utajované informace. Zároveň musí být kontrolován jak vstup do této jednací oblasti, tak výstup. Toto se provádí opatřeními fyzické bezpečnosti. Žádná neoprávněná osoba by neměla do jednací oblasti vstoupit bez doprovodu osoby oprávněné ke vstupu. I zde se míra zabezpečení konkrétních jednacích oblastí určuje pomocí bodových hodnot dle přílohy č. 1 vyhlášky NBÚ 528/2005 Sb. (Dvořák, Chrobák, 2018), (Česko, 2005), (Česko, 2005)

4.4 Opatření fyzické bezpečnosti

Mezi výše zmíněná opatření fyzické bezpečnosti patří:

a) ostraha,

b) režimová opatření,

c) technické prostředky.

4.4.1 Ostraha

Na obecný pojem ostraha může být nahlíženo z různých úhlů. Ostraha může být chápána jako činnost, kterou vykonává fyzická osoba za účelem ochrany konkrétního objektu, majetku nebo osoby například před vandalismem, zneužitím, poškozením nebo ublížením na zdraví. (Ostraha, 2020)

Pro účely zákona č. 412/2005 Sb., o utajovaných informacích a o bezpečnostní způsobilosti, lze tento pojem chápat jako střežení objektu, zabezpečené oblasti nebo jednací oblasti. Toto střežení pak provádějí osobně fyzické osoby, které by měly zabránit nebo ztížit přístup neoprávněné osobě k utajovaným informacím nebo alespoň pokus o přístup neoprávněné osobě k utajovaným informacím nějakým způsobem zaznamenat. Aby ostraha byla platná dle zákona, musí ji provádět osobně fyzické osoby, které jsou zaměstnanci orgánu státu, podnikající fyzické osoby nebo právnické osoby. Dále ostrahu mohou provádět příslušníci ozbrojených bezpečnostních sborů, příslušníci ozbrojených sil cizí moci nebo zaměstnanci bezpečnostní ochranné služby. I zde se musí zajištění ostrahy u objektů, kde se nacházejí utajované informace, bodově ohodnotit a dle tohoto je pak rozhodnuto o konkrétním typu ostrahy u konkrétního objektu. Samozřejmě rozhodování závisí především na tom, jaký

nejvyšší stupeň utajované informace bude v objektu přítomen. Jiné podmínky pro ostrahu jsou u utajovaného dokumentu se stupněm utajení Přísně tajné a jiné u utajovaného dokumentu, který má stupeň utajení Vyhrazené. (Dvořák, Chrobák, 2018), (Česko, 2005), (Česko, 2005)

4.4.2 Režimová opatření

Definici režimových opatření zákon 412/2005 Sb., o utajovaných informacích a o bezpečnostní způsobilosti, neobsahuje, pouze určuje, co do režimových opatření zahrnout, regulovat a upravit. Režimová opatření můžeme tedy chápat jako soubor norem, které upravují a regulují určité režimy uvnitř daného objektu, kde se utajované informace nacházejí tak, aby se zabránilo přístupu neoprávněné osoby k utajovaným informacím nebo se její pokus o tento přístup ztížil nebo zaznamenal. Režimová opatření jsou vymezena v § 29 zákona o utajovaných informacích a dále ve vyhlášce NBÚ č. 528/2005 Sb. Mezi režimová opatření tedy patří:

a) oprávnění osob pro vstup a výstup do objektu,
b) oprávnění dopravních prostředků pro vjezd a výjezd do objektu,
c) oprávnění osob pro vstup do zabezpečených a jednacích oblastí,
d) oprávnění pohybu osob uvnitř objektu,
e) způsob manipulace s klíči,
f) způsob manipulace s identifikačními prostředky,
g) způsob manipulace s technickými prostředky a jejich používání,
h) způsob manipulace s utajovanými informacemi v objektu, zabezpečených oblastech a jednacích oblastech,
i) způsob vynášení utajovaných informací z objektu, zabezpečených oblastí a jednacích oblastí,
j) stanovení způsobu kontroly všech výše uvedených opatření.

Mezi režimovými opatřeními a technickými prostředky existuje velice úzká vazba. Režimová opatření řeší způsob manipulace s technickými prostředky. Dále režimová opatření vymezují způsob manipulace s klíči a identifikačními prostředky, které spadají pod technické prostředky. Tyto technické prostředky jsou pak používány pro režim vstupů do objektu s výstupů z něj. (Česko, 2005), (Česko, 2005), (Dvořák, Chrobák, 2018)

4.4.3 Technické prostředky

Technické zábranné prostředky jsou různá zařízení, systémy nebo jiné věci, které mají opět zabránit nebo ztížit neoprávněným osobám přístup k utajovaným informacím nebo tento přístup včasně odhalit nebo zaznamenat. Vyhláška NBÚ č. 528/2005 Sb. technický prostředek definuje jako bezpečnostní prvek, jehož použití zabraňuje, ztěžuje, identifikuje, nebo zaznamená narušení zabezpečení objektu, zabezpečené oblasti nebo jednací oblasti. Dále je to také prvek, který ničí utajované informace a jejich nosiče. Obecný výčet prostředků, které se mohou pro ochranu utajovaných informací použít, je uveden v § 30 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Jedná se o tyto technické prostředky:

a) mechanické zábranné prostředky,
b) elektronická zařízení a systémy pro kontrolu vstupů,
c) zařízení elektrické zabezpečovací signalizace,
d) speciální televizní systémy,
e) tísňové systémy,
f) zařízení elektrické požární signalizace,
g) zařízení sloužící k vyhledávání nebezpečných látek nebo předmětů,
h) zařízení fyzického ničení nosičů informací,
i) zařízení proti pasivnímu a aktivnímu odposlechu utajované informace.

Některé technické prostředky se samy o sobě běžně využívají (např. kamerový systém) při objektové ochraně soukromých či komerčních prostor. Technické prostředky, které se konkrétně využívají pro ochranu utajovaných informací, musí být certifikovány nebo musí být schváleny odpovědnou osobou nebo jí pověřenou osobou. Dále se opět použitým technickým prostředkům přiřazuje bodové hodnocení. Postupuje se dle přílohy č. 1 vyhlášky 528/2005 Sb. (Česko, 2005), (Česko, 2005)

5 ANALÝZA RIZIK

Analýza rizik je nedílnou součástí posuzování možného nebezpečí nebo odhalování chyb již zavedeného procesu nebo systému. Pro účely této bakalářské práce byly vybrány metody brainstorming a analýza FMEA. Principy využití těchto metod jsou v této kapitole vysvětleny.

5.1 Brainstorming

Brainstorming je jedna z tvůrčích intuitivních metod. Je to metoda pro tvorbu nápadů, která využívá potenciál skupiny osob. Jejím cílem je za co nejkratší časový úsek získat co nejvíce nápadů, myšlenek, námětů a názorů k danému problému od předem určené skupiny lidí. Tak jako ostatní metody, i brainstorming má své fáze provedení a určitá pravidla.

Metodu brainstorming můžeme rozdělit do tří fází:

1) Příprava sezení
    - Zde se stanoví téma sezení, velikost a složení skupiny brainstormingu. Také se určí moderátor a zapisovatel celého sezení. Moderátor po celou dobu sezení dohlíží na dodržování pravidel a toto sezení řídí. Zapisovatel zapisuje veškeré vyřčené nápady tak, aby na ně všichni účastníci viděli a mohli se dále inspirovat.
2) Realizace sezení
    - Jde už o samotné sdělování nápadů všech účastníků sezení. Na začátku sezení je dobré zopakovat pravidla brainstormingu a stanovené téma (sděluje moderátor). Účastníci sdělují své nápady postupně jeden po druhém nebo se může zvolit spontánní metoda, ve které účastníci sdělují nápady hned, jak je napadnou. Vše se zapisuje doslovně tak, jak je řečeno, na viditelné místo pro všechny účastníky sezení.
3) Hodnocení a využití výsledků sezení
    - Konečná fáze brainstormingu. Seskupení stejných nebo podobných nápadů do větších skupin a jejich následné hodnocení. Pro hodnocení se můžou použít různé způsoby.

První pravidlo brainstormingu je, že nikdo nesmí být po celý průběh sezení kritizován za to, co ho napadne a řekne. Všechny řečené nápady jsou vyhodnocovány až v poslední fázi

brainstormingu. Dalším pravidlem je, že každý účastník by měl říci každý nápad nebo myšlenku, která mu přijde na mysl. Čím více nápadů, tím je větší pravděpodobnost, že se najde ten pravý. Kombinace více nápadů jsou žádoucí. Všechna pravidla brainstormingu jsou po celou dobu sezení kontrolována moderátorem sezení. (Grasseová, Dubec a Řehák, 2012)

5.2 FMEA

Metoda Failure Mode and Effect Analysis neboli analýza možných vad a jejich následků je analytická technika, která má za cíl identifikovat možný vznik vady v nějakém systému. Hledá možné příčiny vzniku vady, a tím zamezuje vzniku budoucích ztrát. Tato metoda je velmi univerzální a může se použít v řadě oblastí, například v řízení bezpečnosti. (FMEA (Failure Mode and Effect Analysis), 2021), (Kocourek, 2012)

Princip této metody je založen na sestavení tabulky příčin poruch, jejich následků a doporučených opatření, aby se poruchy co nejvíce minimalizovaly nebo úplně odstranily. Výsledkem je rizikové číslo, které je pro nás přijatelné nebo ne.

Na začátku celé této metody je potřeba vymezit, co přesně se bude analyzovat. Poté by se měl svolat tým odborníků, kteří společně provedou soupis možných problémů a vad, které by mohly nastat. Pro zjištění možných problémů a vad se může použít například metoda brainstorming, která se uplatňuje i pro účely této práce. Všechny zjištěné problémy a vady vypíšeme do předem stanového formuláře FMEA. Následně se ke každému problému určí následky tohoto problému a možné příčiny vzniku. Dále se v předepsaném formuláři vyplní stávající opatření pro prevenci a stávající řízení procesu. Ke všemu výše vypsanému se přiřazují koeficienty na základě stanovených kritérií. (Kocourek, 2012)

První koeficient, který musíme vyplnit, je koeficient významu vady. Jde o číselnou hodnotu, která má vyjádřit závažnost důsledku chyby na celý systém. Vada je tedy bodově ohodnocena dle svého významu.

Druhý koeficient ukazuje výskyt vady. Opět jde o číselnou hodnotu, která stanovuje pravděpodobnost výskytu vady v celém systému. Vada je bodově ohodnocena dle svého výskytu.

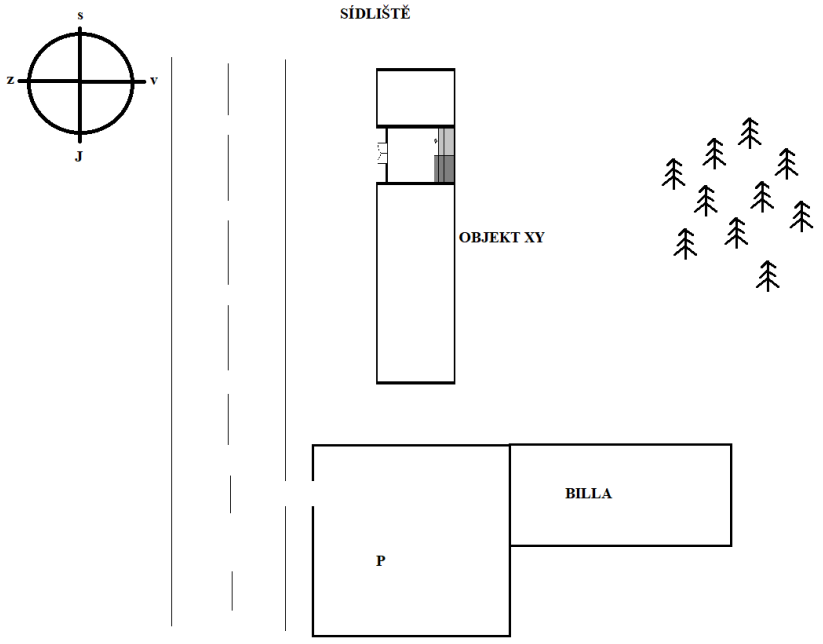
Třetí koeficient zobrazuje číselnou hodnotu pravděpodobnosti odhalení vady. Koeficient udává, jaká je pravděpodobnost odhalení či neodhalení vady.

Po přiřazení všech koeficientů tyto tři koeficienty mezi sebou v každém řádku vynásobíme. Výsledkem je rizikové číslo, které udává míru rizika daného problému nebo vady. I u rizikového čísla je potřeba stanovit kritéria hodnocení. Pro účely této práce byla kritéria stanovena následovně. Rozsah rizika byl rozdělen na nepatrné, malé, střední a vysoké riziko. Rozsah nepatrného rizika byl stanoven od 0 do 64. Je to součin hodnot významu vady, výskytu vady a pravděpodobnosti odhalení vady, tj. 4*4*4 = 64. Od této hodnoty se odvíjí malé riziko, které bylo stanoveno na číselný rozsah od 65 do 216. Horní hranice středního rizika je dána součinem čísel 6 významu vady, výskytu vady a pravděpodobnosti odhalení vady, tj. 6*6*6 = 216. Číselný rozsah středního rizika je pak dán součinem čísel 8 významu vady, výskytu vady a pravděpodobnosti odhalení vady, tj. 8*8*8 = 512, tudíž je stanoven od 217 do 512. Nejvyšší riziko je stanoveno od čísel 513 do 1000. Je to součin nejvyšších hodnot významu vady, výskytu vady a pravděpodobnosti odhalení vady, tj. 10*10*10=1000. (Kocourek, 2012)

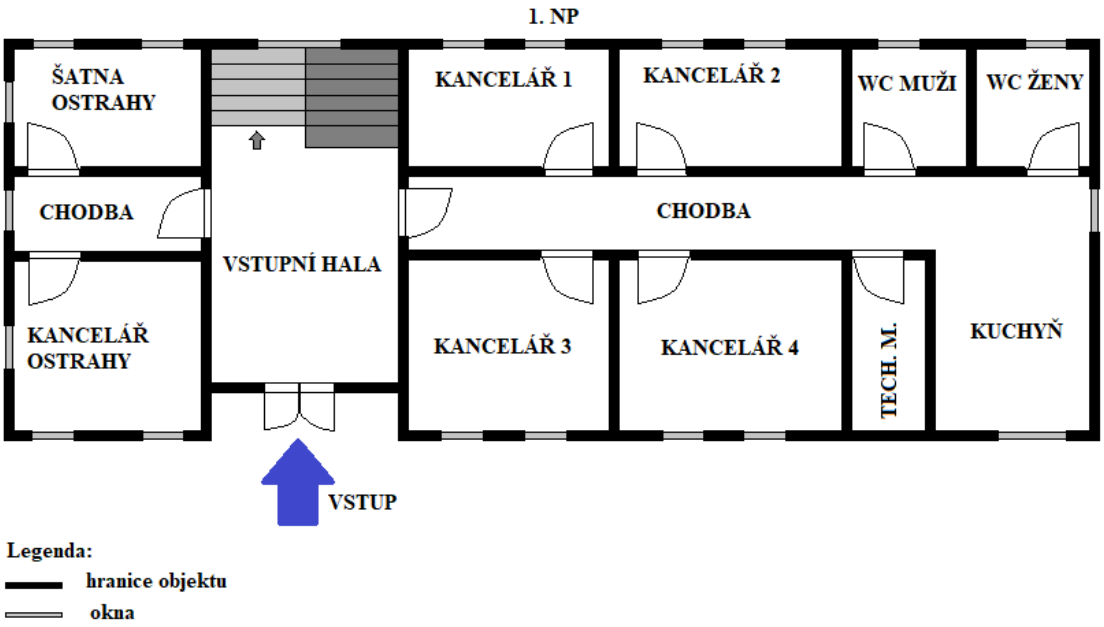
II. PRAKTICKÁ ČÁST

6 POPIS OBJEKTU XY

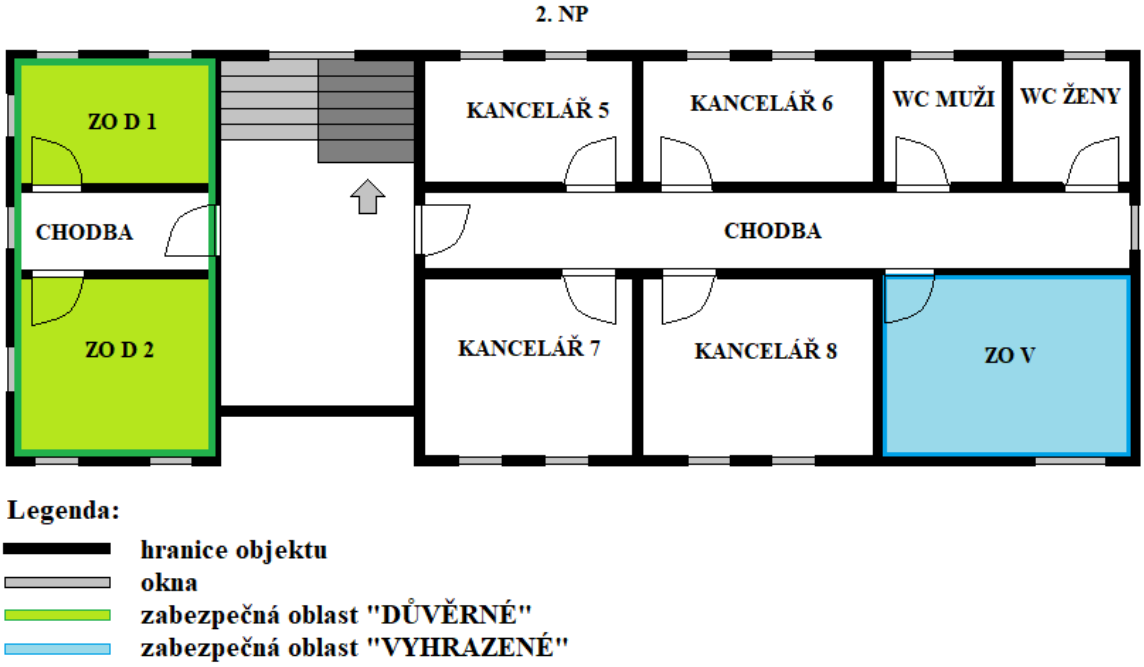
Pro potřeby této bakalářské práce byl vybrán objekt XY, který je ve vlastnictví nejmenované státní instituce. Tato státní instituce splňuje podmínky pro nakládání s utajovanými informacemi dle platných právních předpisů. Konkrétně jsou v objektu XY uloženy informace se stupněm utajení Vyhrazené a Důvěrné. Objekt se nachází ve Středočeském kraji na okraji nejmenovaného města. Jedná se o volně stojící budovu na rovinatém pozemku, která není součástí žádného komplexu. V nejbližším okolí se nachází v severní části městská zástavba bytových a rodinných domů. Dále v jižní části budovy je nákupní středisko BILLA, za kterým se dále nachází zahrádkářská kolonie. V západní části je budova lemována chodníkem pro chodce spolu s pozemní komunikací. Ve východní části budovy začíná po sto metrech lesní porost. Budova má tvar obdélníku s výklenkem na levé straně budovy. Do tohoto výklenku je zabudován jediný vchod do celého objektu. Uvnitř se naproti těmto vchodovým dveřím nachází vnitřní schodiště do patra. Objekt je tedy složen z prvního vyvýšeného a druhého nadzemního podlaží. Ve druhém nadzemním podlaží jsou tři zabezpečené oblasti. Dvě zabezpečené oblasti jsou v režimu „DŮVĚRNÉ“ a jedna zabezpečená oblast je v režimu „VYHRAZENÉ“. Budova se především využívá jako administrativní pracoviště a lokální zázemí pro pracovníky výše uvedené státní instituce. V objektu se bude tedy především nacházet kancelářský nábytek, několik kusů počítačových sestav a multifunkční tiskárny, trezory a další vybavení, které je potřeba k chodu celé budovy.



Obrázek 3 Umístění objektu v prostoru



Obrázek 4 Půdorys 1. nadzemního podlaží objektu XY



Obrázek 5 Půdorys 2. nadzemního podlaží objektu XY

6.1 Popis personální bezpečnosti

Všichni pracovníci musí splňovat podmínky pro vydání osvědčení na stupeň utajení Důvěrné. Návrh na požadavek na vyšší stupeň utajení je pouze u konkrétních pracovních míst. Tento návrh předkládá ředitel objektu řediteli státní instituce. Pokud pracovníkovi není vydáno osvědčení nebo platnost tohoto osvědčení skončila, ředitel objektu učiní nezbytná opatření taková, aby pracovník splňoval podmínky dle zákona č. 412/2005, o ochraně utajovaných informací a bezpečnostní způsobilosti, k tomu, aby se mohl seznamovat s utajovanými informacemi.

Předtím, než se pracovník začne seznamovat s utajovanými informacemi, musí absolvovat proškolení z právních předpisů v oblasti utajovaných informací, z přístupu k utajovaným informacím a v oblasti bezpečnosti informačních systémů. Všechna tato školení je pracovník povinen absolvovat každý rok. Ředitel objektu zajistí termíny těchto školení.

Ředitel objektu je povinen zajistit, aby se jeho podřízení pracovníci seznamovali pouze s těmi informacemi, které jsou nezbytné k výkonu jejich pracovní náplně. Přístup k utajovaným informacím se tedy řídí zásadou nezbytnosti. Seznam oprávněných osob, které mají přístup k utajovaným informacím, včetně stupně utajení, je veden na sekretariátu ředitele objektu.

6.2 Popis administrativní bezpečnosti

Na objektu XY probíhá manipulace s utajovanými informacemi pouze se stupněm utajení Vyhrazené a Důvěrné. Stupeň utajení se stanoví při vzniku utajované informace s ohledem na seznam utajovaných informací a na to, jakou může způsobit utajovaná informace újmu České republice. Vyznačení stupně utajení a další náležitosti, které musí dokument obsahovat, se řídí dle vyhlášky č. 529/2005 Sb., o administrativní bezpečnosti. Všechny utajované informace eviduje správce protokolu v příslušných jednacích protokolech.

V objektu jsou dvě počítačové sestavy v zabezpečených oblastech, kde se mohou zpracovávat utajované informace do stupně utajení Důvěrné. V těchto počítačových sestavách je nainstalován certifikovaný informační systém, který výše uvedené umožňuje. Do informačního systému se mohou přihlásit pouze vybraní pracovníci, kteří se k výkonu své pracovní činnosti mohou seznamovat s utajovanými informacemi. Pracovník je odpovědný za zpracovávání utajovaných informací v tomto informačním systému pouze do stupně utajení Důvěrné. Každý pracovník má svůj jedinečný uživatelský účet a v tomto také

pracuje. V jiném uživatelském účtu má pracovník zakázáno pracovat. Utajovanou informaci je možné vytisknout pouze na kopírovacích zařízeních, která jsou v zabezpečených oblastech.

Na nosné médium je možné nahrát utajovanou informaci v případě, že nosné médium je správně označené a zaevidované na konkrétního pracovníka, který s ním manipuluje. Toto nosné médium lze použít na počítačových sestavách, na kterých jsou nainstalovány pouze certifikované informační systémy. Opis, překlad nebo výpis z utajované informace je možný pouze po schválení ředitelem objektu a je dále ošetřen vnitřním předpisem státní instituce.

Utajované informace se ukládají do úschovných objektů (trezory) v zabezpečených oblastech příslušného stupně utajení. Jak zabezpečená oblast, tak úschovný objekt jsou v době nepřítomnosti oprávněných pracovníků uzamčeny a zabezpečeny poplachovým systémem. Klíče od zabezpečených oblastí nebo úschovných objektů jsou uloženy v kanceláři ostrahy objektu v zapečetěné schránce. Lze je vyzvednout proti podpisu u ostrahy objektu, která disponuje seznamem oprávněných osob, které mohou s klíči manipulovat. Duplikáty všech klíčů budovy jsou uloženy na centrále státní instituce. Ztráta či odcizení klíčů od zabezpečených oblastí či úschovných objektů se musí neprodleně nahlásit řediteli objektu a veškeré písemnosti se musí neprodleně přesunout do jiných zabezpečených oblastí nebo úschovných objektů.

Utajovanou informaci lze přepravovat pouze kurýrem, a to ve dvou obálkách – vnitřní, vnější. Vnitřní obálka se opatří razítkem odesílatele, adresou příjemce, způsobem doručení „KURÝREM“ a slovy „Otevře výhradně adresát“. Vnější obálkou je vždy přepravní nebo přenosná schránka (aktovka, kufřík, přenosná bezpečnostní schránka, kurýrní vaky), kterou je možno uzamknout. Dokument se předá k přepravě proti podpisu v doručovací knize. Kurýr musí mít platné osvědčení pro stupeň utajení Důvěrné a vždy dokumenty přepravuje ve vozidlech, které vlastní státní instituce.

6.3 Popis fyzické bezpečnosti

Z výše uvedených informací víme, že se objekt nachází ve Středočeském kraji na okraji blíže nespecifikovaného města. Za celý objekt a jeho provoz je odpovědný určený ředitel tohoto objektu a zároveň je také odpovědný za ochranu utajovaných informací. Celá budova je ohraničena okny a obvodovou zdí o síle zdi 30 centimetrů. Objekt se skládá ze dvou podlaží. Zabezpečení objektu je zajištěno kombinací opatření fyzické bezpečnosti, tj. ostrahy, technických prostředků a režimových opatření.

Ostraha

Objekt XY je nepřetržitě střezen jedním pracovníkem instituce. Pracovníci se střídají po 12 hodinách na denní a noční režim. Stanoviště ostrahy je umístěno v 1. nadzemním podlaží u hlavního vchodu budovy. Ostraha objektu neprovádí obchůzky a plní především úkoly ostrahy:

- dohlížení na oprávněný vstup do objektu,
- kontrola neporušenosti technických prostředků,
- zaznamenávat a nahlašovat závady technických prostředků řediteli objektu,
- vést přehled přidělených klíčů.

Režimová opatření

Ředitel objektu určuje oprávněné osoby, které mohou do objektu vstupovat. Těmto osobám je pak přiděleno oprávnění v systému elektronické kontroly vstupů (EKV). Přidělené oprávnění v systému se pak tedy projeví na přidělených čipových ID kartách, které umožní, po načtení na EKV čtečku, otevření dveří do objektu nebo oblasti. Každá osoba má na své ID kartě přidělena jen ta oprávnění, která v budově nezbytně potřebuje pro výkon svého zaměstnání, tj. ne všechny osoby v budově budou mít přístup např. do zabezpečených oblastí. Ostatní osoby, které nemají přidělena žádná oprávnění ke vstupu budovy, jsou chápány jako „návštěva“ a musí mít vždy přidělený doprovod s oprávněním. Před odchodem každý zaměstnanec uzavře okna, vypne elektrické zařízení a jiné spotřebiče a uzamkne svou kancelář. Přítomnost zaměstnance po pracovní době je možná pouze v případě, že se tato skutečnost nahlásí ostraze objektu. Mimopracovní dobou se rozumí čas od 22:00 do 06:00 hodin v pracovní dny a celé dny pracovního volna.

Ředitel objektu určuje oprávněné osoby, které mohou vstupovat do zabezpečených oblastí. Seznam oprávněných osob je uložen na sekretariátu ředitele objektu a v kanceláři ostrahy objektu. V zabezpečené oblasti se může samostatně pohybovat pouze oprávněná osoba. Oprávněná osoba odpovídá za řádné používání technických prostředků v zabezpečené oblasti a dodržuje pravidla této oblasti. Před vstupem do oblasti osoba zkontroluje uzamčení vstupních dveří a odblokuje danou oblast. Po vstupu osoba zkontroluje stav místnosti a stav oken. Před odchodem ze zabezpečené oblasti osoba ověří uzavření oken a vypnutí všech elektrických zařízení, které se v oblasti nachází. Poté uzamkne vstupní dveře do oblasti a oblast zakóduje. Vstup a pohyb neoprávněných osob v zabezpečené oblasti není možný za

žádných okolností. Vstup a pohyb v zabezpečené oblasti po pracovní době je možný pouze po nahlášení ostraze.

Technické prostředky

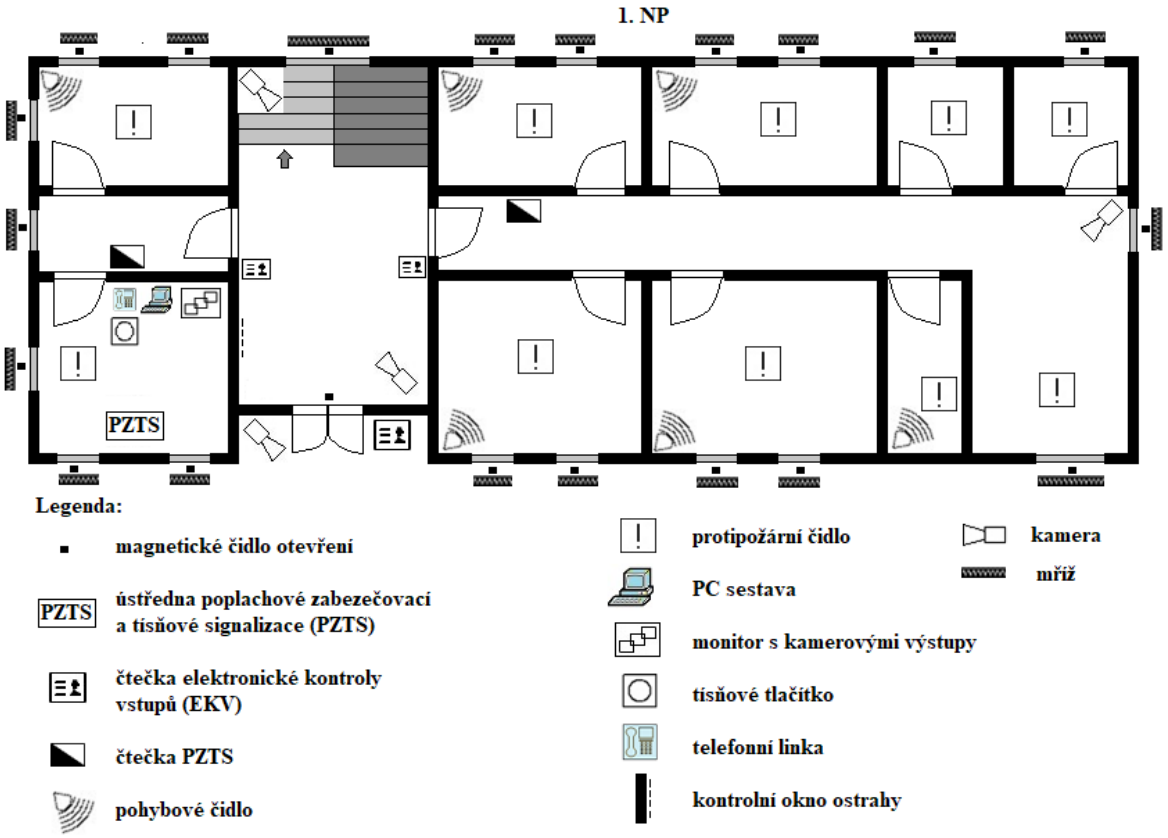
V 1. nadzemním podlaží jsou okna ve výšce 1,60 metrů nad úrovní terénu opatřená certifikovanými okenními mřížemi. Na všech oknech a vstupních dveřích budovy jsou nainstalována magnetická čidla otevření. Nachází se zde také jediný vstup do celého objektu. Tento vstup je určen jak pro zaměstnance instituce, tak pro návštěvy. Hlavní vstup je osazen dvoukřídlými dřevěnými dveřmi s certifikovaným uzamykacím systémem. Uzamykací systém je v provedení „knoflík/klika“ na levém křídle dveří.

Zaměstnanec instituce otevře vstupní dveře do budovy svou osobní přidělenou kartou, kterou přiloží na čtečku systému EKV. Návštěva pak tedy musí na svoji přítomnost upozornit ostrahu objektu zvonkem, který je umístěn vedle vstupních dveří. Ostraha prostřednictvím zvonku s kamerou návštěvu kontaktuje a případně pustí do objektu.

Vstupní hala disponuje kamerami a čtečkami elektronické kontroly vstupů v počtu dvou kusů od každého. Dále se ve vstupní hale nachází kontrolní okno ostrahy objektu a schodiště vedoucí do druhého nadzemního podlaží.

V levé části prvního podlaží sídlí ostraha objektu, která disponuje služebnou a šatnou. V šatně ostrahy je naistalováno pohybové čidlo a protipožární čidlo. Služebna ostrahy je zabezpečena čtečkou poplachových zabezpečovacích a tísňových systémů, protože v místnosti služebny se nachází ústředna poplachových zabezpečovacích a tísňových systémů, dále velký monitor zobrazující kamerové výstupy z budovy, tísňové tlačítko a počítačová sestava s interní zabezpečenou sítí bez přístupu k internetu.

V pravé části budovy jsou k dispozici čtyři kancelářské prostory, dvě místnosti toalet, technická místnost a kuchyňský kout. Kancelářské prostory a technická místnost jsou zabezpečeny poplachovým zabezpečovacím a tísňovým systémem. V každé místnosti najdeme opět protipožární čidla a pohybová čidla. Na chodbě pravé části objektu je umístěna kamera.

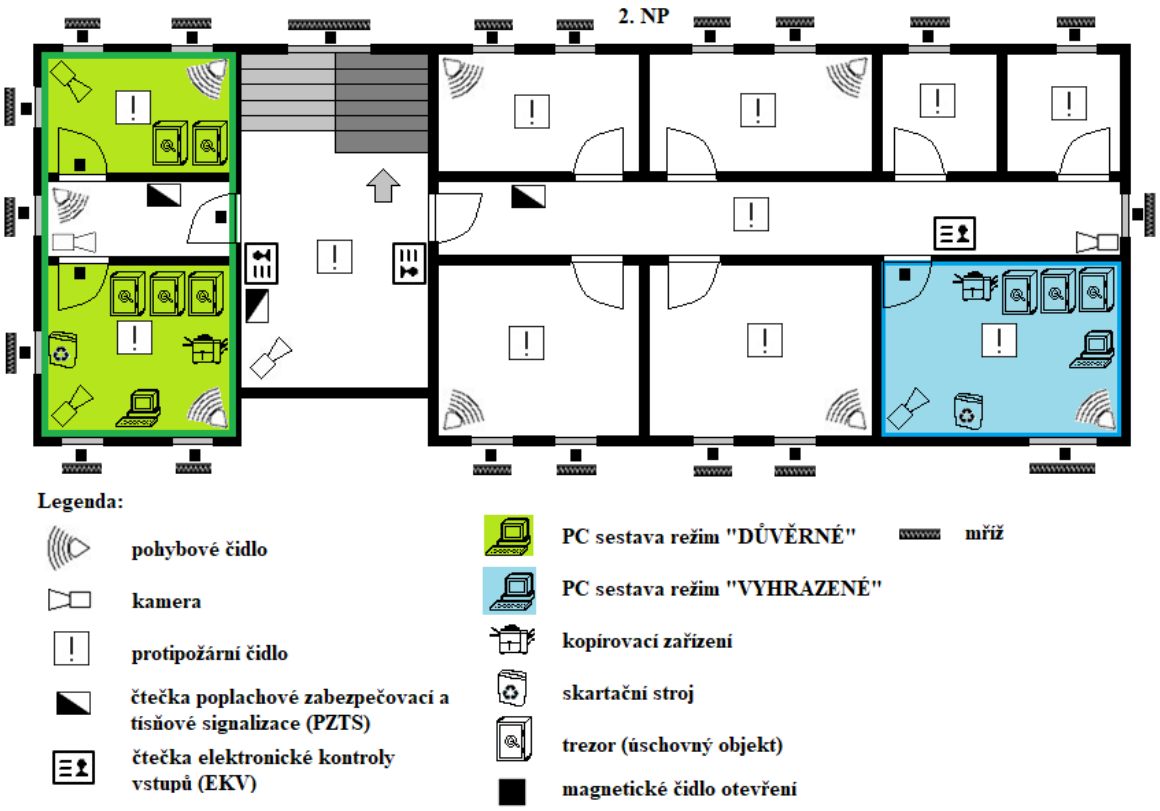


Obrázek 6 Vyznačení technických prostředků v 1. NP

Ve druhém nadzemním podlaží jsou opět okna s certifikovanými mřížemi a na všech jsou nainstalována magnetická čidla otevření. Hala nad schody disponuje protipožárním čidlem, kamerou zabírající celou halu, čtečkou poplachové zabezpečovací a tísňové signalizace, kterou si oprávněné osoby odblokují přístup do zabezpečené oblasti v režimu „DŮVĚRNÉ“, a nakonec jsou zde umístěny dvě čtečky elektronické kontroly vstupů u každých dveří.

V levé části druhého podlaží se nachází zabezpečená oblast, která se skládá z chodby a dvou kanceláří, které jsou využity jako úložné prostory pro utajované informace se stupněm DŮVĚRNÉ. Na vstupních dveřích do této oblasti je připevněno magnetické čidlo otevření. V chodbě této oblasti je nainstalována kamera, která zabírá celý prostor chodby, dále je zde nainstalováno pohybové čidlo a čtečka poplachové zabezpečovací a tísňové signalizace, sloužící pro odblokování jednotlivých kanceláří. Vstupní dveře do těchto kanceláří jsou osazeny magnetickými čidly otevření. Dále obě kanceláře disponují kamerami, pohybovými a protipožárními čidly. Úschovné objekty neboli trezory nalezneme v obou kancelářích. Západní kancelář navíc disponuje také skartačním a kopírovacím zařízením a počítačovou sestavou, kde se mohou utajované informace se stupněm utajení Důvěrné zpracovávat.

V pravé části druhého podlaží se nachází chodba, čtyři kancelářské prostory, dvě místnosti sociálního zařízení a zabezpečená oblast v režimu „VYHRAZENÉ“. Chodba disponuje čtečkou poplachové zabezpečovací a tísňové signalizace, kterou se odblokují jednotlivé kancelářské prostory a zabezpečená oblast. Každý ze čtyř kancelářských prostor je vybaven pohybovým a protipožárním čidlem. Protipožární čidla jsou dále nainstalována i v ostatních prostorech pravé části. Vstupní dveře do zabezpečené oblasti v režimu „VYHRAZENÉ“ jsou osazeny magnetickým čidlem otevření a dále čtečkou EKV. Zabezpečená oblast disponuje kamerou a pohybovým čidlem. I zde nalezneme trezory, kopírovací a skartační zařízení a počítačovou sestavu, která slouží ke zpracování utajovaných informací se stupněm utajení Vyhrazené.



Obrázek 7 Vyznačení technických prostředků v 2. NP

7 ANALÝZA RIZIK

Na základě provedeného brainstormingu byly poznatky z tohoto použity jako podklady pro analýzu FMEA. Analýza FMEA je zpracována z pohledu personální bezpečnosti, administrativní bezpečnosti a fyzické bezpečnosti.

Pro analýzu FMEA byla stanovena tato kritéria:

Tabulka 2 Kritéria významu vady

Číslo	Význam vady	Popis vady
1	Sotva postřehnutelný	Žádný důsledek
2-3	Nepatrný	Občasná, běžná, nezásadní porucha/vada
4-6	Středně závažný	Porucha vyvolá pozornost, ale není zas tak závažná
7-8	Velký	Výskyt závažné poruchy
9-10	Mimořádně závažný	Význam chyby mimořádně vysoký; ohrožena bezpečnost systému a legislativní předpisy

(Vargová, 2020), (Božek)

Tabulka 3 Kritéria výskytu vady

Číslo	Výskyt vady	Popis
1	Nepravděpodobná	Chyba je skoro vyloučená.
2-3	Nepatrná	Systém je pod kontrolou; ojedinělé vady.
4-6	Malá	Systém je pod kontrolou; vady v malém rozsahu.
7-8	Velká	Systém není pod kontrolou; vady se vyskytují často.
9-10	Velmi vysoká	Vadě nelze zabránit.

(Vargová, 2020)

Tabulka 4 Pravděpodobnost odhalení vady

Číslo	Pravděpodobnost odhalení vady	Popis
1	Vysoká	Vysoké zabezpečení, které odhalí možnou vadu.
2-5	Mírná	Metody zabezpečení můžou odhalit možnou vadu.
6-8	Malá	Metody zabezpečení pravděpodobně odhalí možnou vadu.
9	Velmi malá	Metody zabezpečení sotva odhalí možnou vadu.
10	Nepravděpodobná	Metody zabezpečení systému nezjistí, anebo nemůžou zjistit možnou vadu.

(Vargová, 2020)

Tabulka 5 Rozsah rizikového čísla

Rozsah rizikového čísla (RPN)	
0-64	Nepatrné riziko
65-216	Malé riziko
217-512	Střední riziko
513-1000	Vysoké riziko

(Zástřešek, 2018)

Tabulka 6 Analýza personální bezpečnosti

Objekt: Objekt XY										**Číslo FMEA: 1**					
Odpovědnost za proces: Tereza Čížková										**Rok výroby modelu / procesu: 2021**					
ANALÝZA SOUČASNÉHO STAVU PERSONÁLNÍ BEZPEČNOSTI										**NÁVRH OPATŘENÍ**		**ANALÝZA STAVU PO REALIZACI OPATŘENÍ**			
Prvek	**Možná chyba**	**Možné následky chyby**	**VÝZNAM**	**Možná příčina chyby**	**VÝSKYT**	**Stávající opatření**	**Stávající řízení procesu**	**ODHALENÍ**	**Rizikové číslo**	**Doporučená opatření**	**Odpovědnost**	**VÝZNAM**	**VÝSKYT**	**ODHALENÍ**	**Rizikové číslo**
Lidský faktor	Neudělení osvědčení	Zákaz přístupu k UI	**7**	Nesplnění podmínek k udělení osvědčení	**2**	NBÚ	NBÚ	**2**	**28**	Žádná	Nikdo	**7**	**2**	**2**	**28**
		Zákaz vykonávání pracovní činnosti	**7**		**2**			**2**	**28**			**7**	**2**	**2**	**28**
		Zákaz přístupu k UI	**7**	Skončení platnosti osvědčení	**2**	NBÚ	NBÚ	**2**	**28**	Zavedení evidence platností osvědčení	Sekretářka ředitele objektu	**7**	**1**	**1**	**7**
		Zákaz vykonávání pracovní činnosti	**7**		**2**			**2**	**28**			**7**	**1**	**1**	**7**

Objekt: Objekt XY										Číslo FMEA: 1				
Odpovědnost za proces: Tereza Čížková										Rok výroby modelu / procesu: 2021				
ANALÝZA SOUČASNÉHO STAVU PERSONÁLNÍ BEZPEČNOSTI										NÁVRH OPATŘENÍ		ANALÝZA STAVU PO REALIZACI OPATŘENÍ		
Prvek	Možná chyba	Možné následky chyby	VÝZNAM	Možná příčina chyby	VÝSKYT	Stávající opatření	Stávající řízení procesu	ODHALENÍ	Rizikové číslo	Doporučená opatření	Odpovědnost	VÝZNAM	VÝSKYT	ODHALENÍ	Rizikové číslo
Lidský faktor	Neabsolvování školení k seznamování s UI	Zákaz přístupu k UI	8	Nepřihlášení na termín školení	2	Osobní odpovědnost	Sekretariát	2	32	Zavedení evidence platností školení	Zaměstnanci, sekretariát	8	2	1	16
	Seznámení s UI, kterou osoba nepotřebuje ke své pracovní činnosti	Zneužití UI	10	Zaměstnanec	2	Osobní odpovědnost	Vnitřní předpis	4	80	Beze změn	Zaměstnanci	10	2	4	80

Tabulka 7 Analýza administrativní bezpečnosti

Objekt: Objekt XY										**Číslo FMEA: 2**					
Odpovědnost za proces: Tereza Čížková										**Rok výroby modelu / procesu: 2021**					
ANALÝZA SOUČASNÉHO STAVU ADMINISTRATIVNÍ BEZPEČNOSTI										**NÁVRH OPATŘENÍ**		**ANALÝZA STAVU PO REALIZACI OPATŘENÍ**			
Prvek	**Možná chyba**	**Možné následky chyby**	**VÝZNAM**	**Možná příčina chyby**	**VÝSKYT**	**Stávající opatření**	**Stávající řízení procesu**	**ODHALENÍ**	**Rizikové číslo**	**Doporučená opatření**	**Odpovědnost**	**VÝZNAM**	**VÝSKYT**	**ODHALENÍ**	**Rizikové číslo**
Technické hrozby	Nefunkční PC určené ke zpracování UI	Ztráta dat	**10**	Technická závada	**2**	Záloha dat na utajovaný disk	Vnitřní předpis	**2**	**40**	Beze změny	Zaměstnanci	**10**	**2**	**2**	**40**
			10	Životnost komponentů	**3**			**2**	**60**			**10**	**3**	**2**	**60**
	Neoprávněný vstup do zabezpečené oblasti	Odcizení, zneužití UI	**10**	Poškozena čtečka EKV, PZTS	**4**	Klíče od oblastní uložené u ostrahy objektu	Vnitřní předpis	**2**	**80**	Beze změny	Ostraha	**10**	**4**	**2**	**80**
	Nefunkční kopírovací zařízení	Nemožnost tisku, scanu a kopírování	**9**	Technická závada	**4**	Žádné	Žádné	**1**	**36**	Záložní kopírovací zařízení	IT oddělení	**3**	**2**	**1**	**6**
	Nefunkční úschovný objekt	Nemožnost uložení UI	**10**	Technická závada	**4**	Žádné	Žádné	**1**	**40**	Záložní úschovný objekt	Ředitel objektu	**3**	**2**	**1**	**6**

Objekt: Objekt XY										Číslo FMEA: 2					
Odpovědnost za proces: Tereza Čížková										Rok výroby modelu / procesu: 2021					
ANALÝZA SOUČASNÉHO STAVU ADMINISTRATIVNÍ BEZPEČNOSTI										NÁVRH OPATŘENÍ		ANALÝZA STAVU PO REALIZACI OPATŘENÍ			
Prvek	Možná chyba	Možné následky chyby	VÝZNAM	Možná příčina chyby	VÝSKYT	Stávající opatření	Stávající řízení procesu	ODHALENÍ	Rizikové číslo	Doporučená opatření	Odpovědnost	VÝZNAM	VÝSKYT	ODHALENÍ	Rizikové číslo
Lidský faktor	Únik UI z informačního systému	Zneužití UI	10	Zaměstnanec	5	Vnitřní předpis	Vnitřní předpis	4	200	Beze změn	Zaměstnanci	10	5	4	200
	Neoprávněné vynesení UI ze zabezpečené oblasti	Zneužití UI	10	Zaměstnanec	5	Vnitřní předpis	Vnitřní předpis	4	200	Beze změn	Zaměstnanci	10	5	4	200
	Neoprávněný vstup do zabezpečené oblasti	Zneužití UI	10	Zaměstnanec	3	Vnitřní předpis	Vnitřní předpis	2	60	Beze změn	Zaměstnanci	10	3	2	60

Objekt: Objekt XY										Číslo FMEA: 2					
Odpovědnost za proces: Tereza Čížková										Rok výroby modelu / procesu: 2021					
ANALÝZA SOUČASNÉHO STAVU ADMINISTRATIVNÍ BEZPEČNOSTI										NÁVRH OPATŘENÍ		ANALÝZA STAVU PO REALIZACI OPATŘENÍ			
Prvek	Možná chyba	Možné následky chyby	VÝZNAM	Možná příčina chyby	VÝSKYT	Stávající opatření	Stávající řízení procesu	ODHALENÍ	Rizikové číslo	Doporučená opatření	Odpovědnost	VÝZNAM	VÝSKYT	ODHALENÍ	Rizikové číslo
Lidský faktor	Přihlášení se do jiného uživatelského účtu	Zneužití účtu	10	Vyzrazení přihlašovacích údajů zaměstnancem	3	Vnitřní předpis	Vnitřní předpis	5	150	Změna hesla po třech měsících	Zaměstnanci	8	2	3	48
	Ztráta/odcizení nosného média	Zneužití dat	10	Zaměstnanec	3	Vnitřní předpis	Vnitřní předpis	2	60	Beze změn	Zaměstnanci	10	3	2	60
	Neschválený opis, překlad, výpis UI	Zneužití UI	10	Zaměstnanec	3	Vnitřní předpis	Vnitřní předpis	5	150	Beze změn	Zaměstnanci	10	3	5	150
	Ztráta klíče od zabezpečené oblasti	Nemožnost uzamčení/ odemčení zabezpečené oblasti	10	Zaměstnanec	2	Vnitřní předpis	Vnitřní předpis	2	40	Beze změn	Zaměstnanci/ ostraha	10	2	2	40

Objekt: Objekt XY										Číslo FMEA: 2				
Odpovědnost za proces: Tereza Čížková										Rok výroby modelu / procesu: 2021				
ANALÝZA SOUČASNÉHO STAVU ADMINISTRATIVNÍ BEZPEČNOSTI										NÁVRH OPATŘENÍ		ANALÝZA STAVU PO REALIZACI OPATŘENÍ		
Prvek	Možná chyba	Možné následky chyby	VÝZNAM	Možná příčina chyby	VÝSKYT	Stávající opatření	Stávající řízení procesu	ODHALENÍ	Rizikové číslo	Doporučená opatření	Odpovědnost	VÝZNAM	VÝSKYT	ODHALENÍ	Rizikové číslo
Lidský faktor	Neoznačení vnitřní obálky při přepravě UI	Doručení UI nesprávné osobě	10	Zaměstnanec	2	Vnitřní předpis	Vnitřní předpis	2	40	Beze změn	Zaměstnanci	10	2	2	40
	UI nevložena do dvou obálek při přepravě	Odtajnění UI	10	Zaměstnanec, kurýr	2	Vnitřní předpis	Vnitřní předpis	2	40	Beze změn	Kurýr	10	2	2	40
	Nepodepsání doručovací knihy při předání UI	Nepotvrzené předání UI	10	Kurýr	4	Vnitřní předpis	Vnitřní předpis	2	80	Beze změn	Kurýr	10	4	2	80
	Odcizení UI při přepravě	Zneužití UI	10	Nedodržení vnitřních předpisů	2	Vnitřní předpis	Vnitřní předpis	2	40	Přepravu zajistí dva kurýři	Kurýr	8	1	1	8

Tabulka 8 Analýza fyzické bezpečnosti

Objekt: Objekt XY										**Číslo FMEA: 3**					
Odpovědnost za proces: Tereza Čížková										**Rok výroby modelu / procesu: 2021**					
ANALÝZA SOUČASNÉHO STAVU FYZICKÉ BEZPEČNOSTI										**NÁVRH OPATŘENÍ**		**ANALÝZA STAVU PO REALIZACI OPATŘENÍ**			
Prvek	**Možná chyba**	**Možné následky chyby**	**VÝZNAM**	**Možná příčina chyby**	**VÝSKYT**	**Stávající opatření**	**Stávající řízení procesu**	**ODHALENÍ**	**Rizikové číslo**	**Doporučená opatření**	**Odpovědnost**	**VÝZNAM**	**VÝSKYT**	**ODHALENÍ**	**Rizikové číslo**
Přírodní hrozby	Nefunkční kameru u hlavního vchodu	Ztráta vizuálního přehledu vstupu osob do budovy	**10**	Meteorologické podmínky (vítr, déšť)	**5**	Vnitřní předpis	Vnitřní předpis	**2**	**100**	Nainstalování více kamer na plášť budovy	IT oddělení	**5**	**3**	**2**	**30**
	Snížená viditelnost kamer u hl. vchodu	Ztráta vizuálního přehledu vstupu osob do budovy	**8**	Hmyz	**7**	Vnitřní předpis	Vnitřní předpis	**2**	**112**	Použití chemických prostředků	Ostraha	**5**	**3**	**1**	**15**
	Poškození okenní tabule	Neoprávněný vstup do budovy	**10**	Meteorologické podmínky (vítr, déšť)	**3**	Vnitřní předpis	Vnitřní předpis	**2**	**60**	Nalepení bezpečnostní fólie do oken	Údržba objektu	**7**	**1**	**1**	**7**

Objekt: Objekt XY										Číslo FMEA: 3				
Odpovědnost za proces: Tereza Čížková										Rok výroby modelu / procesu: 2021				
ANALÝZA SOUČASNÉHO STAVU FYZICKÉ BEZPEČNOSTI										NÁVRH OPATŘENÍ		ANALÝZA STAVU PO REALIZACI OPATŘENÍ		
Prvek	Možná chyba	Možné následky chyby	VÝZNAM	Možná příčina chyby	VÝSKYT	Stávající opatření	Stávající řízení procesu	ODHALENÍ	Rizikové číslo	Doporučená opatření	Odpovědnost	VÝZNAM	VÝSKYT	ODHALENÍ	Rizikové číslo
Přírodní hrozby	Nefunkční čtečka EKV hlavního vchodu	Nemožnost přístupu do budovy	10	Meteorologické podmínky (vítr, déšť)	3	Vnitřní předpis	Vnitřní předpis	3	90	Nainstalování ochranného krytu na čtečku	Údržba objektu	10	2	2	40
	Výpadek elektřiny	Nemožnost přístupu do budovy	10	Meteorologické podmínky (vítr, déšť)	3	Záložní zdroj	Vnitřní předpis	2	60	Beze změn	Ostraha	10	3	2	60

Objekt: Objekt XY										Číslo FMEA: 3					
Odpovědnost za proces: Tereza Čížková										Rok výroby modelu / procesu: 2021					
ANALÝZA SOUČASNÉHO STAVU FYZICKÉ BEZPEČNOSTI										NÁVRH OPATŘENÍ		ANALÝZA STAVU PO REALIZACI OPATŘENÍ			
Prvek	Možná chyba	Možné následky chyby	VÝZNAM	Možná příčina chyby	VÝSKYT	Stávající opatření	Stávající řízení procesu	ODHALENÍ	Rizikové číslo	Doporučená opatření	Odpovědnost	VÝZNAM	VÝSKYT	ODHALENÍ	Rizikové číslo
Technické hrozby	Výpadek elektřiny	Nefunkčnost PZTS	10	Technická závada	3	Záložní zdroj	Vnitřní předpis	2	60	Beze změn	Ostraha	10	3	2	60
	Nefunkční čidlo pohybu	Nedetekování pohybu v místnosti	10	Technická závada	4	Vnitřní předpis	Vnitřní předpis	2	80	Záložní čidla pohybu na skladě	IT oddělení	10	2	1	20
				Špatné umístění v místnosti	3			4	120	Přeinstalování čidla a správné místo		10	2	1	20
	Nefunkční magnetické čidlo otevření	Neschopnost kontroly uzavření oken, dveří	10	Technická závada	4	Vnitřní předpis	Vnitřní předpis	5	200	Pravidelná měsíční kontrola čidel	IT oddělení	10	2	2	40

Objekt: Objekt XY									Číslo FMEA: 3					
Odpovědnost za proces: Tereza Čížková									Rok výroby modelu / procesu: 2021					
ANALÝZA SOUČASNÉHO STAVU FYZICKÉ BEZPEČNOSTI									NÁVRH OPATŘENÍ		ANALÝZA STAVU PO REALIZACI OPATŘENÍ			
Prvek	Možná chyba	Možné následky chyby	VÝZNAM	Možná příčina chyby	VÝSKYT	Stávající opatření	Stávající řízení procesu	ODHALENÍ	Rizikové číslo	Doporučená opatření	Odpovědnost	VÝZNAM	VÝSKYT	ODHALENÍ	Rizikové číslo
Technické hrozby	Nefunkční protipožární čidlo	Nezjištění požáru v daném místě	10	Technická závada	4	Vnitřní předpis	Vnitřní předpis	6	240	Pravidelná měsíční kontrola čidel	IT oddělení	10	2	2	40
	Nefunkční kamera	Ztráta vizuálního přehledu pohybu v budově	10	Technická závada	3	Vnitřní předpis	Vnitřní předpis	2	60	Pravidelná měsíční kontrola kamer	IT oddělení	10	2	2	40
	Nefunkční tísňové tlačítko	Nemožnost ohlášení napadení objektu	10	Technická závada	3	Zkouška tlačítka 1x za 6 měsíců	Vnitřní předpis	6	180	Zkouška tlačítka 1x za měsíc	IT oddělení	10	2	2	40

Objekt: Objekt XY									Číslo FMEA: 3					
Odpovědnost za proces: Tereza Čížková									Rok výroby modelu / procesu: 2021					
ANALÝZA SOUČASNÉHO STAVU FYZICKÉ BEZPEČNOSTI									NÁVRH OPATŘENÍ		ANALÝZA STAVU PO REALIZACI OPATŘENÍ			
Prvek	Možná chyba	Možné následky chyby	VÝZNAM	Možná příčina chyby	VÝSKYT	Stávající opatření	Stávající řízení procesu	ODHALENÍ	Rizikové číslo	Doporučená opatření	Odpovědnost	VÝZNAM	VÝSKYT	ODHALENÍ	Rizikové číslo
Technické hrozby	Nefunkční čtečka EKV	Nemožnost přístupu do oblasti	10	Technická závada	3	Vnitřní předpis	Vnitřní předpis	2	60	Beze změn	IT oddělení	10	3	2	60
	Nefunkční tečka PZTS	Nemožnost odblokování oblasti	10	Technická závada	3	Vnitřní předpis	Vnitřní předpis	2	60	Beze změn	IT oddělení	10	3	2	60
	Nefunkční pevná linka	Nemožnost telefonování	9	Výpadek elektřiny	3	Záložní zdroj	Vnitřní předpis	2	54	Pořízení mobilního telefonu	IT oddělení	3	2	2	12
				Technická závada	4	Žádné	žádné	2	72						

Objekt: Objekt XY										Číslo FMEA: 3					
Odpovědnost za proces: Tereza Čížková										Rok výroby modelu / procesu: 2021					
ANALÝZA SOUČASNÉHO STAVU FYZICKÉ BEZPEČNOSTI										NÁVRH OPATŘENÍ		ANALÝZA STAVU PO REALIZACI OPATŘENÍ			
Prvek	Možná chyba	Možné následky chyby	VÝZNAM	Možná příčina chyby	VÝSKYT	Stávající opatření	Stávající řízení procesu	ODHALENÍ	Rizikové číslo	Doporučená opatření	Odpovědnost	VÝZNAM	VÝSKYT	ODHALENÍ	Rizikové číslo
Lidský faktor	Poškozená okenní mříž	Neoprávněné vniknutí do budovy	10	Úmysl potencionálního pachatele	3	Žádná	Vnitřní předpis	5	150	Obchůzky ostrahy	Ostraha	9	2	2	36
	Poškozená okenní tabule	Neoprávněné vniknutí do budovy	10	Úmysl potencionálního pachatele	3	Mříž	Vnitřní předpis	4	120	Nainstalování čidel tříštění skel	IT oddělení	10	3	2	60
	Nežádoucí předmět v budově	Poškození objektu nebo zaměstnanců	10	Nedbalost ostrahy	3	Ostraha	Vnitřní předpis	6	180	Koupě rentgenového rámu	IT oddělení	10	3	3	90

Objekt: Objekt XY										Číslo FMEA: 3					
Odpovědnost za proces: Tereza Čížková										Rok výroby modelu / procesu: 2021					
ANALÝZA SOUČASNÉHO STAVU FYZICKÉ BEZPEČNOSTI										NÁVRH OPATŘENÍ		ANALÝZA STAVU PO REALIZACI OPATŘENÍ			
Prvek	Možná chyba	Možné následky chyby	VÝZNAM	Možná příčina chyby	VÝSKYT	Stávající opatření	Stávající řízení procesu	ODHALENÍ	Rizikové číslo	Doporučená opatření	Odpovědnost	VÝZNAM	VÝSKYT	ODHALENÍ	Rizikové číslo
Lidský faktor	Nezakódovaná zabezpečená oblast	Neoprávněný přístup do oblasti	10	Zaměstnanec	3	Vnitřní předpis	Vnitřní předpis	4	120	Kontrola ostrahy prostřednictvím ústředny PZTS	Ostraha	10	3	2	60
	Nezakódovaná kancelář po odchodu zaměstnance	Neoprávněný přístup do kanceláře	10	Zaměstnanec	3	Vnitřní předpis	Vnitřní předpis	4	120	Kontrola ostrahy prostřednictvím ústředny PZTS	Ostraha	10	3	2	60

8 SHRNUTÍ, DOPORUČENÁ OPATŘENÍ

Po provedení analýzy byly zjištěny jen nepatrné a malé chyby systému. Ochrana utajovaných informací má jasně dané podmínky dle zákona 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, a souvisejících vyhlášek.

Z pohledu personální bezpečnosti byly zjištěny tři možné chyby, které mohou v systému nastat a jsou způsobeny lidským faktorem: neudělení osvědčení, neabsolvování školení a seznámení s UI, kterou osoba nepotřebuje ke své pracovní činnosti. První dvě chyby byly vyhodnoceny jako nepatrné. Proces udělení osvědčení si řídí Národní bezpečnostní úřad. U neabsolvování školení se navrhla zavést evidence platnosti školení zaměstnanců objektu, kterou povede sekretariát ředitele objektu. Třetí chyba byla vyhodnocena jako malá. Zde nebylo navrhnuto žádné opatření, protože stávající opatření jsou dostatečná a nelze je více ošetřit. Vnitřní předpis objektu jasně stanovuje, kdo a s jakou informací se může a nemůže seznamovat. Tato chyba zůstává na lidské zodpovědnosti, kterou nelze ošetřit.

Z pohledu administrativní bezpečnosti byly možné chyby rozděleny na technické hrozby a hrozby způsobené lidským faktorem. U technických hrozeb vše vyšlo jako nepatrné riziko až na neoprávněný vstup do zabezpečené oblasti z důvodu poškozené čtečky EKV nebo PZTS, který byl vyhodnocen jako riziko malé. Přístup do zabezpečených oblastí je ošetřen vnitřním předpisem, který uvádí, že klíče od zabezpečených oblastí vydává ostraha proti podpisu pouze oprávněným osobám, které mají přístup do těchto oblastí. Pokud bude rozbitá jedna z výše uvedených čteček, nelze se přesto do oblasti dostat bez klíče. Pokud osoba nemá oprávnění ke vstupu, klíč jí ostraha nevydá. Hrozby způsobené lidským faktorem jsou převážně hodnoceny jako nepatrná rizika. Jako malá rizika vyšly hrozby: únik UI z informačního systému, neoprávněné vynesení UI ze zabezpečené oblasti, přihlášení se do jiného uživatelského účtu, neschválený opis, překlad, výpis UI a nepodepsaní doručovací knihy při předání UI. Veškerá manipulace a nakládání s utajovanými informacemi jsou ošetřeny v zákoně 412/2005 Sb. a také ve vnitřním předpisu objektu. Selhání lidského faktoru nelze eliminovat.

Fyzická bezpečnost byla analyzována z pohledu přírodních hrozeb, technických hrozeb a hrozeb způsobených lidským faktorem. V objektu byly vyhodnoceny tyto malé vady v důsledku meteorologických podmínek: nefunkční kamera u hlavního vchodu, snížená viditelnost kamery u hlavního vchodu a nefunkční čtečka EKV hlavního vchodu. Bylo navrhnuto řešení nainstalováním více kamer na plášť budovy, aby byl zachován vizuální

přehled o dění kolem budovy, a ochranný kryt na čtečku. Technické vady byly zhodnoceny jako malá a nepatrná rizika, kdy se u těchto navrhly pravidelné měsíční kontroly a záložní materiál na objektu, aby byl ihned k dispozici na výměnu. Jako střední riziko byla vyhodnocena nefunkčnost protipožárního čidla. Opět je zde jako návrh opatření uvedeno zavedení pravidelných měsíčních kontrol funkčnosti čidla. Analýza hrozeb, z hlediska lidského faktoru, nynějšího stavu byla vyhodnocena jako malá rizika. Tato rizika se snížila na nepatrná návrhem zavedení obchůzek ostrahy po objektu a kolem něj, nainstalováním čidel tříštění skla, koupí rentgenového rámu a rozšířením práv ostrahy kontrolovat po pracovní době, zda jsou veškeré oblasti a kanceláře zakódovány.

Samotná analýza vyhodnocení rizik, po aplikaci opatření, je součástí výše provedených analýz (str. 40 až 52).

ZÁVĚR

Cílem práce bylo přiblížit problematiku ochrany utajovaných informací a zanalyzovat vybraný objekt, ve kterém se tyto informace nacházejí.

V teoretické části byly vysvětleny základní pojmy, které úzce souvisí s problematikou ochrany utajovaných informací. Dále jsou zde přiblíženy tři základní druhy bezpečností, které musí dodržovat a splňovat každá osoba nebo instituce, která nějakým způsobem nakládá nebo manipuluje s utajovanými informacemi. Jedná se o personální bezpečnost, administrativní bezpečnost a fyzickou bezpečnost. Personální bezpečnost vymezuje podmínky pro fyzické osoby v případě, že mají mít přístup k utajovaným informacím. Tyto zákonem dané podmínky musí splňovat každá fyzická osoba. Administrativní bezpečnost je pak systém opatření, která se musí využívat při jakékoli manipulaci s utajovanými informacemi, tj. od vzniku informace až po její zánik. Nakonec fyzická bezpečnost představuje souhrn opatření, která mají znemožnit nebo co nejvíce ztížit přístup k utajované informaci neoprávněné osobě. Do fyzické bezpečnosti se řadí ostraha, režimová opatření a technické prostředky.

Praktická část obsahuje popis vybrané budovy nejmenované státní instituce, včetně vyobrazených modelů, umístění objektu v prostoru a rozložení jednotlivých nadzemních podlaží, místností a zabezpečených oblastí uvnitř budovy, popis objektu a instituce z hlediska personální, administrativní a fyzické bezpečnosti.

Na základě provedeného brainstormingu byly výsledky tohoto použity jako podklad pro analýzu rizik metodou FMEA. Zjištěné výsledky byly rozčleněny do tří oblastí dle personální, administrativní nebo fyzické bezpečnosti a následně zanalyzovány.

V oblasti personální bezpečnosti byly zjištěny jen nepatrné a malé chyby, které může způsobit lidský faktor. K těmto chybám bylo navrhnuto opatření v podobě zavedení evidencí pro zpětnou kontrolu.

V oblasti administrativní bezpečnosti opět vyšla nepatrná a malá rizika. Pravidla administrativní bezpečnosti v budově jsou nastavena tak, že z technického hlediska v celku nehrozí žádné větší nebezpečí. I zde je větší riziko selhání lidského faktoru, v důsledku porušení pravidel nakládání s UI nebo špatnou manipulací. Nakládání a manipulace s utajovanými informacemi jsou ošetřeny vnitřním předpisem objektu a převážně zákonem 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti. Zde jsou návrhy

jakýkoli dalších opatření bezpředmětná, jelikož je vše stanoveno zákonem a porušení zákona je trestné.

Analýza fyzické bezpečnosti odhalila nepatrné, malé a střední vady. Jako faktory rizika zde byly zvoleny meteorologické podmínky, technické vady a selhání lidského faktoru. Za střední a zároveň nejvíce závažné riziko celé analýzy je považováno nefunkční protipožární čidlo. Zde bylo navrhnuto opatření v podobě pravidelných měsíčních kontrol funkčnosti těchto čidel. Dále bylo navrhnuto nainstalování více kamer na celý plášť budovy pro lepší vizuální kontrolu okolí objektu, pořízení rentgenového rámu z důvodu zamezení pronesení nebezpečného předmětu do budovy, zavedení pravidelných obchůzek ostrahy a nainstalování čidel tříštění skel.

SEZNAM POUŽITÉ LITERATURY

Knižní zdroje:

1. DVOŘÁK, Jan, Jiří CHROBÁK, 2018. *Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti*. Praha 3: Wolters Kluwer. ISBN 978-80-7598-016-8.
2. RODRYČOVÁ, Danuše, Pavel STAŠA, 2000. *Bezpečnost informací jako podmínka prosperity firmy*. Praha 7: Grada Publishing. ISBN 80-7169-144-5.
3. DOBDA, Luboš 1998. *Ochrana dat v informačních systémech*. Praha: Grada. ISBN 80-7169-479-7.
4. BARTÁK, Jan, Jindřich BEČVÁŘ a Miroslav BECHYNĚ et al., 1999. *Malá ilustrovaná encyklopedie: A-Ž*. Praha: Encyklopedický dům. ISBN 80-860-4412-2.
5. UHLÁŘ, Jan, 1995. *Technická ochrana objektů*. Praha: Policejní akademie České republiky.
6. KAMENÍK, Jiří, František BRABEC a kolektiv, 2019. *Komerční bezpečnost*. Praha 3: Wolters Kluwer. ISBN 978-80-7598-303-9.
7. GRASSEOVÁ, Monika, Radek DUBEC a David ŘEHÁK, 2012. *Analýza podniku v rukou manažera*. Druhé vydání. Brno: BizBooks. ISBN 978-80-265-0032-2.
8. BRABEC, František et al., 2001. *Bezpečnost pro firmu, úřad, občana*. Praha: Public History. ISBN 80-86445-04-06.
9. PROCHÁZKOVÁ, Dana, 2006. *Bezpečnost a krizové řízení*. Praha: POLICE HISTORY. ISBN 80-86477-35-5.
10. DOUCEK, Petr et al., 2011. *Řízení bezpečnosti informací*. Praha: Professional Publishing. ISBN 978-80-7431-050-8.
11. SAK, Petr, 2018. *Úvod do teorie bezpečnosti*. Havlíčkův Brod: Petrklíč. ISBN 978-80-7229-652-1.
12. BURDA, Karel, 2017. *Základy elektronických zabezpečovacích systémů*. Brno: Akademické nakladatelství CERM. ISBN 978-80-7204-967-7.

Internet:

13. Obecně k personální bezpečnosti. *Národní bezpečnostní úřad* [online]. [cit. 2021-01-27]. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/personalni-bezpecnost-oznameni-pro-v-osvedceni-d-t-pt-certifikaty/1043-obecne-k-personalni-bezpecnosti/
14. Informace. *Národní bezpečnostní úřad* [online]. [cit. 2021-01-27]. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/administrativni-bezpecnost-tvori-system-opatreni-pri-tvorbe-prijmu-evidenci-zpracovani-odesilani-preprave-prenaseni-ukladani-skartacnim-rizeni-archivaci-pripadne-jinem-nakladani-s-utajovanymi-informacemi/987-informace/
15. Informace k fyzické bezpečnosti. *Národní bezpečnostní úřad* [online]. [cit. 2021-01-27]. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/fyzicka-bezpecnost-technicke-prostredky-a-dalsi-prvky-fyzicke-bezpecnosti-a-jejich-certifikace/1014-informace/
16. Bezpečnostní řízení. In: *Národní bezpečnostní úřad* [online]. [cit. 2021-01-27]. Dostupné z: https://www.nbu.cz/cs/bezpecnostni-zpusobilost/881-bezpecnostni-rizeni/
17. KLOBOUČKOVÁ, Sylvie, © 2017. Utajované informace. In: *Digitální repozitář Univerzity Karlovy* [online]. Univerzita Karlova [cit. 2021-01-27]. Dostupné z: https://dspace.cuni.cz/bitstream/handle/20.500.11956/1120/150030355.pdf?sequence=1&isAllowed=y
18. POKORNÝ, Michal, 2019. Návrh zabezpečovacích a datových systémů v budově. In: *ČVUT DSpace* [online]. Praha: České vysoké učení technické [cit. 2021-03-26]. Dostupné z: https://dspace.cvut.cz/handle/10467/82478
19. ČESKO, 2005. Zákon č. 412/2005 Sb. Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-412
20. ČESKO, 2005. Vyhláška č. 528/2005 Sb. Vyhláška o fyzické bezpečnosti a certifikaci technických prostředků. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-528

21. Informace a informační instituce, 2018. *WikiSkripta* [online]. [cit. 2021-01-27]. Dostupné z: https://www.wikiskripta.eu/w/Informace_a_informa%C4%8Dn%C3%AD_instituce
22. Ostraha, 2020. *Wikipedie, otevřená encyklopedie* [online]. [cit. 2020-12-27]. Dostupné z: https://cs.wikipedia.org/wiki/Ostraha
23. What is Information Security?, 2020. *Geeks for Geeks* [online]. [cit. 2021-03-26]. Dostupné z: https://www.geeksforgeeks.org/what-is-information-security/
24. Definice bezpečnosti. *Google* [online]. [cit. 2021-04-26]. Dostupné z: https://www.google.com/search?q=definice+bezpe%C4%8Dnosti&oq=definice+bezpe%C4%8D&aqs=chrome.0.0l2j69i57j0j0i22i30l6.2806j0j15&sourceid=chrome&ie=UTF-8
25. ZABEZPEČTE SVŮJ MAJETEK OPRAVDU POŘÁDNĚ - PZTS, © 2021. *PZTS.cz* [online]. [cit. 2021-03-26]. Dostupné z: http://www.pzts.cz/
26. Poplachový zabezpečovací a tísňový systém (PZTS). *Security Technologies* [online]. [cit. 2021-03-28]. Dostupné z: https://www.security.cz/elektricka-zabezpecovaci-signalizace-pzts--2419.html
27. Zabezpečovačka neboli PZTS: Co to je a k čemu slouží? *Securitas* [online]. [cit. 2021-03-26]. Dostupné z: https://www.securitas.cz/novinky--blog/blog/zabezpecovacka-neboli-pzts-co-to-je-a-k-cemu-slouzi/
28. ČESKO, 2005. Vyhláška č. 529/2005 Sb. o administrativní bezpečnosti a o registrech utajovaných informací. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.aspi.cz/products/lawText/1/60727/0/2/vyhlaska-c-529-2005-sb-o-administrativni-bezpecnosti-a-o-registrech-utajovanych-informaci/vyhlaska-c-529-2005-sb-o-administrativni-bezpecnosti-a-o-registrech-utajovanych-informaci
29. ČESKO, 2011. Vyhláška č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2011-363

30. FMEA (Failure Mode and Effect Analysis), 2021. *Management Mania* [online]. [cit. 2021-03-27]. Dostupné z: https://managementmania.com/cs/failure-mode-and-effect-analysis

31. FRUHLINGER, Josh, 2020. What is information security? Definition, principles, and jobs. *CSO* [online]. [cit. 2021-03-26]. Dostupné z: https://www.csoonline.com/article/3513899/what-is-information-security-definition-principles-and-jobs.html

32. KOCOUREK, Jaromír, 2012. Kvalita/Procesní řízení. *Vlastní cesta* [online]. [cit. 2021-03-27]. Dostupné z: https://www.vlastnicesta.cz/metody/fmea/

33. ČESKO, 2005. Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-522

34. Information security. *Protective Security Requirements* [online]. [cit. 2021-5-4]. Dostupné z: https://www.protectivesecurity.govt.nz/information-security/why-information-security-matters/

35. VARGOVÁ, Slavomíra, 2020. LUKR/LBRAR Analýza rizik: FMEA [online přednáška].

36. BOŽEK, František. Failure Mode and Effect Analysis. In: *Moodle UTB* [online]. [cit. 2021-5-9]. Dostupné také z: https://moodle.utb.cz/course/view.php?id=23168

37. ZÁSTŘEŠEK, David. *Analýza bezpečnostních rizik IT infrastruktury vybrané organizace*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2017 [online]. [cit. 2021-5-9]. Dostupné také z: http://hdl.handle.net/10563/42948.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

EKV Elektronická kontrola vstupu

FMEA Failure Mode and Effect Analysis neboli aAnalýza možných vad a jejich následků

ID Identifikační (karta)

NBÚ Národní bezpečnostní úřad

PZTS Poplachový zabezpečovací a tísňový systém

UI Utajovaná informace

SEZNAM OBRÁZKŮ

SEZNAM TABULEK