Bezpečnostní audit vybraného objektu státní správy

Bc. Dagmar Zerzanová

Diplomová práce
2020

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektroniky a měření

Akademický rok: 2019/2020

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

Jméno a příjmení:	**Bc. Dagmar Zerzanová**
Osobní číslo:	**A18584**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Bezpečnostní audit vybraného objektu státní správy**
Téma práce anglicky:	**A Security Audit of a Selected State Administration Building**

Zásady pro vypracování

1. Uveďte základní terminologii související s tématem práce.
2. Popište v obecné rovině bezpečnostní audit.
3. Charakterizujte vybraný objekt státní správy.
4. Proveďte bezpečnostní audit, který se bude skládat z popisu současného stavu, analýzy rizik a vyhodnocení auditu.
5. Navrhněte konkrétní bezpečnostní opatření

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

Seznam doporučené literatury:

1. LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management II*. Zlín: Radim Bačuvčík – VeRBuM, 2012. ISBN 978-80-87500-19-4.
2. LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management V*. Zlín: Radim Bačuvčík – VeRBuM, 2015. ISBN 978-80-87500-67-5.
3. ŠEFČÍK, Vladimír. *Analýza rizik*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009. ISBN 978-80-7318-696-8.
4. SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013. Expert (Grada). ISBN 978-80-247-4644-9.
5. KAMENÍK, Jiří a František BRABEC. *Komerční bezpečnost: soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur*. Praha: ASPI, 2007. ISBN 978-80-7357-309-6.

Vedoucí diplomové práce: **Ing. Dora Lapková, PhD.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **9. prosince 2019**
Termín odevzdání diplomové práce: **29. května 2020**

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Milan Navrátil, Ph.D.
ředitel ústavu

Ve Zlíně dne 9. prosince 2019

Jméno, příjmení: Dagmar Zerzanová

Název diplomové práce: Bezpečnostní audit vybraného objektu státní správy

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové 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 práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byla jsem seznámena s tím, že na moji diplomovou 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 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 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 práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové 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 práci pracovala samostatně a použitou literaturu jsem citovala. 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 3. 8. 2020

Dagmar Zerzanová v. r.
podpis diplomanta

ABSTRAKT

Cílem diplomové práce je provedení bezpečnostního auditu vybraného objektu státní správy. V teoretické části jsou pojmenovány základní pojmy související s problematikou bezpečnosti, řízení rizik a je popsán bezpečnostní auditu v obecné rovině. V praktické části je popsán skutečný stav stanovených oblastí auditu a jsou na základě vstupních informací identifikovány hrozby pomocí metody „Kontrolní seznam“. Pro posouzení a ohodnocení rizik byla použita polokvantitativní metoda označována zkratkou „PNH“. Organizaci byla na základě výsledků doporučena bezpečnostní opatření.

Klíčová slova: bezpečnostní audit, hrozba, bezpečnost, riziko.

ABSTRACT

The aim of the diploma thesis is to perform a security audit of a selected state administration building. The theoretical part names the basic concepts related to security, risk management and describes the security audit in general. The practical part describes the actual state of the identified audit areas and, based on the input information, threats are identified using the "Checklist" method. A semi-quantitative method called "PNH" was used to assess and evaluate the risks. Based on the results, safety measures were recommended to the organization.

Keywords: security audit, threat, security, risk.

Tímto bych ráda poděkovala vedoucí mé diplomové práce paní Ing. Doře Lapkové, Ph.D. za odborné vedení, cenné rady a trpělivost při psaní práce. Dále mé poděkování patří celé mé rodině a zejména mé mamince a kamarádce Jarmilce, kteří mě po celou dobu studia podporovali.

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

OBSAH

ÚVOD

Téma bezpečnost se v současné době dostává stále více do popředí. V současnosti se každá organizace zaobírá bezpečností ve všech oborech svého působení, neboť stále se zvyšující kriminalita, ať už majetková, násilná či informační, mohou pro organizaci znamenat nové potencionální hrozby. Z tohoto důvodu je nutné bezpečnost organizace vnímat v širším kontextu. Je nezbytné ošetřit všechny oblasti bezpečnosti dotýkající se celé činnosti organizace.

V současnosti je samozřejmostí, že součástí firemní strategie je nastavení řady bezpečnostních opatření. Na základě pokynů, nařízení a pravidel se snaží maximálně zabezpečit a ochránit celou organizaci. Tyto pokyny a předpisy vznikají na základě vyhodnocení slabých stránek, které je v předstihu možné zabezpečit na úroveň, jenž bude splňovat požadovaný bezpečnostní stupeň.

Bezpečnostní audit je vhodným nástrojem, jak porovnat skutečný stav bezpečnosti s požadovaným. Nutností je opakování auditů v pravidelných intervalech a tím předcházet rizikům.

Cílem diplomové práce je zpracovat bezpečnostní audit vybraného objektu státní správy.

Diplomová práce je rozdělena do dvou částí, a to na teoretickou, a praktickou část. V teoretické části je popsána základní terminologie související s problematikou a popis bezpečnostního auditu v obecné rovině. Dále jsou popsány druhy, cíle a vymezeny oblasti, kterých se bude audit týkat.

V praktické části je popsána činnost a organizační struktura organizace. Auditované oblasti jsou podrobněji popsány a u každé oblasti jsou vytyčeny silné a slabé stránky. Je popsán současný stav obvodové bezpečnosti areálu, režimová opatření, fyzická ostraha areálu, technická ochrana areálu, objektová bezpečnost, požární ochrana, bezpečnost a ochrana zdraví při práci a informační bezpečnost. Pomocí metody Kontrolní seznam a metod PNH byly identifikovány hrozby a následně ohodnocena rizika. V závěrečné kapitole byla navržena konkrétní opatření vedoucí k minimalizaci rizik.

Organizace, které se týká zpracování diplomové práce, se mé osoby velmi blízce dotýká, neboť jsem jejím zaměstnancem. Z tohoto důvodu bylo vypracování práce pro mne samotnou nejen velmi zajímavé, ale i přínosné.

Vypracováním této práce bych ráda přispěla ke zlepšení bezpečnostní situace v organizaci.

I. TEORETICKÁ ČÁST

1 ÚVOD DO PROBLEMATIKY

Abychom správně pochopili význam definice bezpečnostní audit, je potřeba si alespoň okrajově vysvětlit a definovat základní terminologii. V této kapitole budou vysvětleny pojmy, které jsou důležité pro komplexní pochopení tématu diplomové práce. Mělo by být samozřejmostí, že v každé firmě či organizaci si otázka bezpečnosti žádá systémový a komplexní přístup. Povinností každého vrcholového vedení firmy nebo organizace je nést za bezpečnost plnou odpovědnost.

1.1 Základní terminologie

1.1.1 Bezpečnost

Bezpečnost charakterizujeme jako stav bez péče, bezstarostnost, stav, kdy člověk cítí, že se nemůže nic špatného přihodit. Samozřejmě, že toto tvrzení neplatí absolutně, neboť neexistuje situace, kdy se nemůže nic stát. [1]

„Bezpečnost můžeme definovat jako stav, když jsou zůstatková rizika přijatelná.“ [1]

1.1.2 Aktivum

Vše, co má pro určitý subjekt nějakou hodnotu, se nazývá aktivum. Může být zmenšeno působením hrozby. Dělí se na hmotná a nehmotná. Mezi aktiva hmotná patří např. budovy, pozemky, zařízení, cenné papíry. Mezi aktiva nehmotná je možno zahrnout například licence, know-how, informace a kvalitu zaměstnanců. [2]

Při posuzování aktiv se berou v úvahu zejména tyto hlediska:

- kupní náklady či hodnota aktiva,
- významnost aktiva pro samotné fungování daného subjektu,
- náklady potřebné na překonání potencionální škody na aktivu,
- rychlost schopnosti subjektu reagovat na možné škody na aktivu. [2]

1.1.2.1 Identifikace aktiv

Aktivum je prvek nebo část celku systému. Organizace mu přiděluje určitou hodnotu, pro kterou tudíž požaduje přiměřenou ochranu. Vytváří se soupis aktiv, kterých se analýza bude týkat, uvádí se jejich název a umístění. [2]

1.1.2.2 Ohodnocení aktiv

Po identifikaci aktiv je nutné k nim přiřadit hodnoty, které představují, jak velký význam mají aktiva pro činnost organizace. Mělo by se rozlišit, zda se jedná o jedinečná aktiva, na jejichž existenci je objekt závislý, nebo aktiva lehce nahraditelná. Vstupní údaje zajišťuje vlastník či uživatel aktiv. Není nutné, aby hodnota byla oceněna finančně, ale např. z pohledu nežádoucích dopadů na činnost organizace plynoucí ze ztráty důvěrnosti, dostupnosti, integrity, individuální odpovědnosti a spolehlivosti. K hodnocení se používá např. hodnotová stupnice 1–5, kdy 1 představuje nízkou hodnotu a 5 velmi vysokou hodnotu. [2][3]

1.1.3 Hrozba

Hrozbou se označuje zdroj určité negativní události, aktivity, síly či osoby, která může poškodit určité aktivum. Hrozba má negativní vliv na bezpečnost a vyznačuje se způsobenou škodou, nežádoucí změnou, ztrátou či jinými nežádoucími jevy. [4]

Podle působení hrozeb na subjekt rozdělujeme hrozby do dvou kategorií, a to na vnější a vnitřní.

Vnější hrozby jsou hrozby neovlivnitelné, pouze lze mírnit jejich působení. Naopak vnitřní hrozby lze minimalizovat, či dokonce úplně vyloučit jejich působení.

Vnější hrozby dělíme dle oblastí na:

- ekonomické – finanční krize, bankovní kolapsy,
- politické – válečné konflikty, terorismus, šíření zbraní hromadného ničení,
- technologické – dopravní nehody, výbuchy, kontaminace vody,
- legislativní – soudní hrozby a hrozby související s vyhláškami, smlouvami a zákony,
- sociální – migrace, náboženská nesnášenlivost, epidemie, organizovaný zločin,
- ekologické – živelné pohromy, hrozby globálního oteplování. [5]

Vnitřní hrozby dělíme dle oblastí na:

- personální,
- finanční,
- informační,

- provozní,
- procesní,
- projektové. [4]

Každý subjekt by měl vědět, čím a jak může ohrozit své okolí, nebo i sám sebe. Proto se provádí analýza hrozeb, aby bylo možno provést účinná protiopatření na jejich snížení či eliminaci.

„*Hrozba využívá zranitelnosti a způsobuje rizika (škody). Ty se nazývají dopad hrozby a lze je vyčíslit jako ztrátu (náklad na znovuobnovení aktiv nebo náklad na odstranění následků škod). Základní charakteristikou hrozby je úroveň hrozby, tedy nebezpečnost hrozby, schopnost hrozby způsobit škodu*.“ [4]

1.1.3.1 Identifikace a hodnocení hrozeb

Hrozba představuje možnost poškodit organizaci a jeho aktiva. Identifikují se takové hrozby, které by mohly ohrozit alespoň jedno aktivum. Seznam hrozeb sestavíme podle literatury, dříve provedených průzkumů analýz či vlastních zkušeností. Hrozby mohou být lidského či přírodního původu a mohou být náhodné nebo úmyslné. Také je rozdílné, zda se jedná o hrozby, které se vztahují k podnikatelskému subjektu, neziskovým organizacím či orgánům státu. Hodnocení hrozeb souvisí s identifikovanými aktivy společnosti. [2][3]

1.1.3.2 Analýza hrozeb

Jednotlivé hrozby se hodnotí ke každému aktivu zvlášť. Úroveň hrozby vychází z faktorů, jako je nebezpečnost, přístup a motivace. Tam, kde se hrozba na aktivu uplatňuje, je výsledkem soupis dvojic hrozba a aktivum s vymezenou úrovní hrozby a zranitelnosti. [2]

1.1.3.3 Pravděpodobnost jevu zdroje hrozby

O jevech, které se zkoumají, se neví, zda nastanou, proto se ke každému jevu doplňuje údaj, který dává přehled o tom, s jakou pravděpodobností může tento jev nastat. Aby se mohla pravděpodobnost určit, musí se stanovit, zda jev je náhodný či nikoliv. Při určování pravděpodobnosti se berou v úvahu zkušenosti a údaje ze statistik. U zdrojů úmyslných hrozeb se bere v úvahu motivace a schopnosti útočníků, které se mohou v čase měnit, a zdroje, které mohou být případným útočníkům přístupné. U zdrojů náhodných hrozeb se berou v úvahu geografické faktory, dále možnosti extrémních atmosférických podmínek a faktory ovlivňující lidská selhání. [2]

1.1.4 Zranitelnost

Zranitelnost je komplexní vlastnost, která odráží slabá místa systému, jeho sníženou odolnost vůči možnému narušení jeho funkce, poškození nebo zničení. Vyjadřuje míru poškození systému v případě vzniku nebezpečného jevu. [6]

Zranitelnost vzniká především tam, kde dochází k vzájemnému působení mezi aktivem a hrozbou. Základním činitelem zranitelnosti je její úroveň, která se klasifikuje dle těchto faktorů:

- citlivost – značí, zda dané aktivum má tendenci být danou hrozbou poškozeno,
- kritičnost – významnost aktiva pro analyzovaný objekt. [5]

1.1.4.1 Odhad zranitelností

Odhad zranitelnosti odhaluje nedostatečně zabezpečená místa ve fyzickém prostředí, organizaci, personálu, managementu, komunikačních zařízeních, postupech. Tyto mohou být využity jako zdroje hrozeb a působit škody na aktivech. [3]

1.1.5 Riziko

Riziko je pravděpodobný vznik negativního specifického účinku, ke kterému dojde v průběhu určité doby nebo za určité situace. [7]

Rizikem se dá označit nejistý výsledek, který může být ovlivněn nežádoucím stavem. Riziko vyjadřuje hrozbu, problém nebo vznik škody, který může nastat, možnost neúspěchu, poškození či destrukce. Riziko tedy vyjadřuje jistou míru nejistoty, řečeno jinak, vyjadřuje pravděpodobnost dosažení výsledku, který je jiný od očekávaného. [8]

S pojmem riziko souvisí také pojem nejistota. Pojem nejistota značí možnost nestejných výsledků, jejichž pravděpodobnost není kvantifikována. [7]

Tab. 1. Srovnání pojmů riziko × nejistota (dle Tony Merna a Faisal F. Al-Thani). [7]

	Nejistota	Riziko
Data	Kvalitativní	Kvantitativní
Měřitelnost	Neměřitelná	Měřitelné
Metody	Subjektivní	Statistika a pravděpodobnost

Rizika v organizaci souvisí zejména s jejím okolím, zdroji i změnami a inovacemi uvnitř společnosti. Rizikům se lze vyhýbat vhodným řízením, případné finanční dopady rizik je možné zmenšit pomocí pojištění. [7]

Mezi nejdůležitější charakteristiky rizika patří:

- míra pravděpodobnosti rizika,
- úroveň rizika,
- předvídatelnost rizika,
- dopady,
- míra ovlivnitelnosti,
- vztah k organizaci – interní a externí rizika,
- pořadí působení při vzniku a odstranitelnosti,
- míra únosnosti a přijatelnosti,
- velikost rizika,
- pravděpodobnost vzniku a působení,
- rozsah působení. [7]

Členění rizik v organizaci:

- finanční a ekonomická rizika,
- kybernetická,
- informační,
- provozní,
- sociální,
- ekologická,
- bezpečnostní,
- živelná a přírodní,
- projektová,
- politická. [7]

1.1.5.1 Měření rizika

Výše rizika se mění dle určitých situací a vyplývá z hodnoty aktiva, zranitelnosti aktiva a úrovně hrozby. Při analýze rizik se převážně pracuje s kvalifikovaným odhadem odborníka, protože veličiny při analýze rizik se nedají ve většině případů přesně změřit. Odborníci obvykle používají stupnice 1 až 10 a termíny malý, střední a velký. [2]

1.1.6 Opatření

Opatření lze charakterizovat jako snižování zranitelnosti a ochrana aktiva před určitou hrozbou. Může se jednat o opatření na úrovni administrativní, fyzické nebo logické bezpečnosti. [9]

1.1.6.1 Výběr ochranných opatření

Mezi hlavní zásadu ochranných opatření patří minimalizace eventuálních rizik na minimum. Pro usnadnění popisů rozdílných typů ochranných opatření bývají v rámci norem vytvořeny skupiny ochranných opatření, které tvoří základ pro zdárné řízení bezpečnosti. Na výběr ochranných opatření je třeba nahlížet jak z pohledu velikosti organizace, tak její ochrany. V organizaci by měla být určena osoba s odpovídajícími pravomocemi, která bude odpovědná za řízení bezpečnosti. [10]

1.1.7 Bezpečnostní posouzení

Bezpečnostní posouzení je proces, který na základě zkoumání stanoví stav ochrany na posuzovaném objektu.

Cílem je vytvořit či optimalizovat ochranné opatření po zhodnocení bezpečnostních rizik daného systému ochrany objektu a jeho aktiv.

Bezpečnostní posouzení zahrnuje:

- příprava – sběr informací, zjišťování problému,
- fyzická prohlídka objektu – zaměřena na celý objekt, případně na problematickou část objektu,
- analýza bezpečnostního prostředí objektu – vymezení lokality, označení rizikových zdrojů, přístupnost,
- charakteristika posuzovaného objektu – činnost a bezpečnostní politika firmy,
- posouzení současného stavu referenčního objektu. [11]

1.1.8 Bezpečnostní politika firmy

Bezpečnostní politika firmy ovlivňuje, na jaké úrovni jsou ve firmě zpracovány bezpečnostní analýzy, prognózy ale především bezpečnostní projekty. Řídí se platnými právními normami, vychází ze specifických požadavků vedení organizace na zajištění bezpečnosti a vyžadovaných způsobech ochrany. Velmi důležité je také na kolik je firma schopna a ochotna bezpečnost podniku financovat. [12]

Bezpečnostní politika je charakterizována:

- metodami a postupy, jak řešit ochranu bezpečnosti organizace,
- finančními a časovými předpoklady řešení,
- pravidly pro havarijní plánování,
- druhy zabezpečení firmy. [12]

1.1.9 Bezpečnostní audit

Mezi základní terminologii patří samozřejmě i pojem „bezpečnostní audit“, který se ovšem nedá vysvětlit v několika odstavcích a je mu v této diplomové práci věnována samostatná kapitola č. 2.

1.2 Analýza rizik

1.2.1 Obecný postup analýzy rizik

Analýza rizik přináší odpovědi na otázky, jakým působícím hrozbám je například společnost nebo objekt vystaven, a jak moc jsou jejich aktiva proti těmto hrozbám zranitelná. Dále řeší, jak velká je pravděpodobnost, že bude zneužita určitá zranitelnost konkrétní hrozbou, a jak velký dopad by to na společnost či objekt mohlo mít. [9]

Obr. 1. Analýza rizik. [9]

Analýza rizik se provádí za účelem zachycení hrozeb a zároveň vymezuje rizika ke každému zranitelnému místu a hrozbě. Účelem je pokles rizik na akceptovatelnou úroveň, lépe řečeno, přistoupit na zbytková rizika tam, kde by byla jejich minimalizace neúčinná. [13]

1.2.2 Identifikace plánovaných a existujících ochranných opatření

Součástí analýzy rizik je tzv. identifikace plánovaných nebo již existujících bezpečnostních opatření, což znamená, aby již existující bezpečnostní opatření či plánovaná byla identifikována či popsána. Tím se organizace vyhne práci navíc či zvýšeným nákladům, které mohou být způsobeny zdvojeným ochranným opatřením. Často se stává, že dané ochranné opatření je přezkoumáváno a na základě tohoto přezkoumání je nahrazeno vhodnějším či lépe vyhovujícím ochranným opatřením. Dalším zásadním důvodem, proč se provádí revize bezpečnostních opatření, je kontrola sladění individuálních řešení. Při uplatnění systému řízení bezpečnostních opatření často dochází k souběžné práci jednotlivých pracovních skupin. Může se stát, že již existující a navržená opatření si mohou navzájem překážet. Výsledkem je pak bezpečnostní díra, ze které se stává bezpečnostní incident. Při provádění identifikace již existujících ochranných opatření je účelné udělat kontrolu, zda tato opatření fungují tak, jak se předpokládá, a zda nejsou v rozporu s novými navrhovanými opatřeními. Výsledkem, mimo výše popsané, by měl být seznam všech do této doby platných a všech plánovaných bezpečnostních opatření. Pokud by se tento krok podcenil, mohlo by to vést k podstatným bezpečnostním zranitelnostem. [10]

1.2.3 Stanovení hranic analýzy rizik (revize)

Stanovení hranice analýzy rizik se provádí před hodnocením a identifikací aktiv. Je nutné pečlivě identifikovat hranice a tím se vyvarovat zbytečných činností. Určením hranic se definuje, jakých prvků se analýza rizik bude týkat. [11]

1.3 Proces řízení rizik

Řízení rizik je proces, kdy se subjekt snaží zamezit působení existujících nebo předpokládaných hrozeb a navrhuje řešení, která prostřednictvím vhodných bezpečnostních opatření mohou minimalizovat závažnost dopadu anebo pravděpodobnost výskytu mimořádných událostí. Je nedílnou součástí řízení organizace, skládá se z těchto pěti základních subprocesů, v pořadí:

1. Komunikace a konzultace.
2. Vymezení souvislostí.
3. Posuzování rizik.
4. Zvládání rizik.
5. Monitorování a přezkoumání procesu. [5]

1.3.1 Komunikace a konzultace

Komunikace a konzultace se všemi zainteresovanými stranami subjektu je neopomenutelnou podmínkou každého řízení rizik. Z tohoto důvodu je třeba v prvé řadě vypracovat plán komunikace a konzultací se všemi stranami s vazbou na daný posuzovaný subjekt. Tyto strany si vytváří své vlastní úsudky o rizicích podle toho, jak tato rizika vnímají, což je samozřejmě z pohledu každé zainteresované strany jiné. [5]

1.3.2 Vymezení souvislostí

V této fázi definujeme interní a externí faktory, které je nutno mít na zřeteli při procesu řízení rizik. Nejdříve je nutno provést vymezení externích souvislostí, které můžeme také definovat jako prostředí, které je vně organizace, a ve kterém se subjekt snaží o dosažení svých cílů. Toto vnější okolí organizace je prostředím externích zainteresovaných stran a jejich očekávání z výsledků subjektu, které vyplývají např. ze sociálního, politického, ekologického, ekonomického prostředí. Po zmapování externích souvislostí přistupujeme k vymezení interních souvislostí. Interními souvislostmi rozumíme vnitřní prostředí, ve

kterém se subjekt snaží o dosažení svých cílů. Vymezení interních souvislostí je významnou fází řízení rizik, jelikož zásadním rizikem organizace bývá selhání při dosahování např. projektových cílů, což má za následek stav, který ohrozí splnění smluvního závazku, a potažmo důvěryhodnost organizace. Dalším krokem je vymezení hranice řízení rizik a to tak, že přesně specifikujeme cíle a rozsah činností organizace. Posledním krokem je stanovení kritérií pro hodnocení rizik, které poslouží k hodnocení významnosti rizik. Tato riziková kritéria musí být zpracována hned na startu řízení rizik a neustále přezkoumávána. Při jejich definování je nutné přihlížet k významným činitelům, jako jsou např.:

- úroveň, na které se riziko stává přijatelné a tolerované,
- způsob stanovení pravděpodobnosti rizika,
- způsob určení úrovně rizika a úrovně, která vyžaduje jeho zvládání,
- vzít v úvahu kombinaci více rizik. [5]

1.3.3 Posuzování rizik

Fáze posuzování rizik obsahuje tyto tři zásadní aktivity:

- identifikace rizik,
- analýza rizik,
- hodnocení rizika.

Identifikace rizik zahrnuje identifikaci aktiv, stanovení jejich hodnot a jejich seskupování, a dále pak identifikaci konkrétních hrozeb a jejich zdrojů. Výsledkem je komplexní seznam rizik, který vychází z událostí, jež by mohly zamezit či ohrozit dosažení cílů organizace.

Podstata analýzy rizik spočívá ve zdokonalování porozumění rizik. Zohledňuje příčiny a zdroje hrozeb, následky hrozeb a pravděpodobnost, že hrozba zneužije určitou zranitelnost. Jejím výsledkem je odhad úrovní jednotlivých rizik. V rámci analýzy rizik provádíme tyto úkony:

- analýza hrozeb a zranitelností,
- analýza rizika stanovením závažnosti dopadů nežádoucí události a stanovením pravděpodobnosti vzniku nežádoucí události. [5]

Analýza rizik má několik způsobů provedení:

- kvalitativní (slovní vyjádření různého stupně pravděpodobnosti a důsledků),

- semikvantitativní (kombinace metody kvalitativní a kvantitativní),
- kvantitativní (pracuje již s číselnými hodnotami).

V poslední fázi posuzování rizika, kterou je hodnocení rizik, se rozhoduje na základě výsledků analýzy rizik o tom, která rizika je potřeba zvládat přednostně. [5]

1.3.4 Zvládání rizik

Úkolem této fáze řízení rizik je vybrat jednu nebo více eventualit minimalizace rizik a jejich začlenění do řídicích systémů organizace. Dochází k rozhodování, zda zůstatková úroveň rizika je akceptovatelná nebo ne. Pokud riziko je neakceptovatelné, provede se nové zvládání rizik, a opět se posuzuje jeho efektivita. To vše cyklicky do doby, dokud se zbytkové riziko nestane přijatelným.

Metodami zvládání rizik jsou např.:

- retence rizika (vědomá i nevědomá),
- redukce rizika (optimálně snížením pravděpodobnosti výskytu nežádoucí události),
- transfer rizika (přesun rizika na ekonomicky silnější subjekt),
- vyhnutí se riziku (vyhnutí se dané aktivitě). [5]

V druhé fázi zvládání rizik provádíme implementaci plánů zvládání rizik. Tyto plány se diskutují mezi zainteresovanými stranami a poté jsou zaváděny do řídících procesů organizace. Důležitým výstupem této části zvládání rizik je stanovení přijatelnosti zbytkového rizika a zajištění realizovatelnosti vybraných bezpečnostních opatření. [5]

1.3.5 Monitorování a přezkoumání procesu

Tento proces může zabezpečovat např. stálý dozor v rámci pravidelných kontrol, ale také nahodilých, nečekaných. Nevyhnutelnou součástí tohoto procesu je jeho nepřetržité zaznamenávání. Všechny doklady musí být v každém okamžiku náležitě dohledatelné. [5]

1.4 Řízení rizik v oblasti fyzické ochrany

Člověk a jeho počínání je ovlivňováno v prvé řadě obavou o život svůj, svých blízkých a dojmem ohrožení majetku. Maslowova pyramida potřeb řadí potřebu bezpečí po fyziologických potřebách na 2. základní stupeň potřeb nižšího řádu motivujících lidské chování. Proto musíme brát v úvahu, že vytváření stálého bezpečného prostředí má podstatný význam na lidské chování v čase a místě. Ačkoli procesy spojené s lidskými

pohnutkami není možné dokonale zachytit, hledají se metody nebo aplikace vyzkoušených nástrojů z jiných odvětví. Jejich cílem je přinejmenším zčásti vymezit a charakterizovat procesy spojené s lidským faktorem. [5]

Vodítkem pro posouzení fyzické ochrany je identifikace řetězce v pořadí: nebezpečí – ohrožení – poškození – škoda. Poté se vybere metoda analýzy a výpočet rizika, včetně ověřování výsledků. Na základě posouzení rizika dle stupnice se zvolí nejideálnější řešení vedoucí k minimalizaci rizika a implementují se nová technická nebo organizační opatření, provádí se školení personálu. Po těchto krocích následuje proces řízení rizik, který vyžaduje rozdělení odpovědností. [5]

1.4.1 Postup analýzy rizik uplatněný na fyzickou ochranu

V oblasti fyzické ochrany je účinný postup, který spočívá v definování problému, následné analýze současného stavu, poté předložení návrhu na jeho optimalizaci. V prvé řadě je zapotřebí určit, před čím se chráníme a jak tuto ochranu zrealizujeme. Dále se posoudí, jaká je pravděpodobnost vzniku následků na daném místě a jakého dosáhnou objemu. U každého aktiva posuzujeme riziko samostatně. Provede se posouzení klíčovosti aktiv pro činnost objektu jako celku. Pro každé aktivum se provede podrobná analýza rizik, rizika se ohodnotí a určí jejich pořadí dle závažnosti. [5]

V analýze rizik, konkrétně pro identifikaci rizika, je možno použít metody grafického analytického modelování rizik, např. metodu FTA nebo Ishikawův diagram příčin a následků. Pro výpočet a hodnocení identifikovaných rizik se užívá např. metoda FMEA. Minimalizace rizika na akceptovatelnou úroveň, s ohledem na finanční náročnost této optimalizace, se řídí dle principu ALARA, v němž se hovoří, že riziko je třeba snižovat na takovou hladinu, kdy budou výdaje na jeho snížení neúměrné ve srovnání s příslušným omezením rizika. [5]

1.4.2 Rozbory definování lidské chyby u fyzické ochrany objektu

Definování lidské chyby je další etapou posuzování fyzické ochrany objektu v souvislosti s fyzickou ostrahou, technickou ostrahou a režimovými opatřeními. Často se jedná o chyby v důsledku nepozornosti, špatného vedení, nedostatečným proškolením, nedostatečnou fyzickou dispozicí a nemalou roli hraje i motivace a nerozhodnost v daném okamžiku. [5]

Ke kvantifikaci lidské chyby můžeme použít řadu metod, např. TESEO, THERP, HEART, IDA, HCR, SLIM. Prvně jmenovaná, metoda TESEO, vyniká svou jednoduchostí

a spolehlivost lidského faktoru se pomocí ní určuje na základě pěti faktorů, vzájemně propojených. Jsou to tyto faktory:

- typ činnosti,
- podmínky a čas,
- osobní kvality,
- úzkost, únava a stres,
- ergonomický faktor. [5]

Z pohledu lidského selhání může hrát velkou roli i vliv prostředí a vzájemné působení ostatních předmětů, používaných pro výkon fyzické ostrahy, na člověka. Zde se doporučuje užití metody SHELL, kdy sama zkratka napovídá výběr prvků pro použití metody:

S – software (postupy).

H – hardware (např. DPPC).

E – enviroment (prostředí).

L – liveware (člověk, jedinec v centru zájmu).

L – liveware (další osoby, se kterými se v práci strážný setká). [5]

1.4.3 Techniky minimalizace rizika objektu

Mezi techniky minimalizace rizika v objektu se řadí metody stanovení vah při návrhu na minimalizaci rizika objektu. Dělí se podle informace, kterou nesou. Čím významnější je kritérium, tím větší váha je mu přidělena. Vždy však celkový součet vah všech kritérií musí být roven jedné. V případě výše uvedeném se hovoří o stanovení vah kritérií bez informace o preferenci kritérií. [5]

Další možností je Fullerova metoda, kdy je známo pořadí důležitosti kritérií a je možno uplatnit metodu pořadí. [5]

Poslední typem stanovení vah je situace, kdy je známo pořadí důležitosti kritérií i poměr důležitosti mezi jednotlivými kritérii. V tomto případě se nabízí použití například Saatyho metody. [5]

1.5 Vybrané techniky posuzování rizik

1.5.1 Metoda FTA – analýza stromem poruchových stavů

Analytická technika použitelná pro vyhodnocení pravděpodobnosti selhání, popřípadě spolehlivosti složitých systémů, zejména v oblasti řízení rizik, kvality či bezpečnosti. Tuto metodu analýzy používáme obvykle po aplikaci analýzy FMEA. [14]

Metoda FTA je založená na rozboru obecně negativního jevu a přispívá k systematické identifikaci faktorů, které jev způsobují. Cílem je detailní analýza pro nalezení příčin negativního jevu. [14]

1.5.2 Metoda ETA – analýza stromem událostí

Příčinná analytická technika pro vyhodnocování průběhu procesu a jeho dějů směřujících k možné nehodě. Princip této metody je obdobný jako u metody FTA, ovšem s tím rozdílem, že se pozorují děje vedoucí k závadě, a ne jenom k selhání, jak je tomu u metody FTA. Využitelná především v oblasti řízení rizik a řízení kvality, také v řízení bezpečnosti. [15]

Rozbor sledu činností a událostí v procesu vedoucí k havárii je zobrazován pomocí grafického logického modelu. Tato metoda bere v úvahu také případné reakce bezpečnostního systému a operátorů a jejím výsledkem jsou různé scénáře nehody. [15]

Používá se pro analýzu procesních slabých míst a výsledkem je seznam návrhů pro snížení pravděpodobnosti nehody a snížení jejich následků. [15]

1.5.3 Metoda FMEA – analýza možných vad a přínosů

Analytická technika, jejímž úkolem je označit místa eventuálního vzniku vad nebo poruch v systémech. Základem metody FMEA je uspořádaná identifikace všech možných chyb a jejich důsledků, identifikace kroků zamezení, zmenšení nebo omezení příčin těchto chyb a zaznamenání celého procesu. Jedná se o preventivní metodu nejčastěji používanou ve výrobě. Metoda umožňuje včasně identifikovat případné poruchy, které mohou ovlivnit funkce systému, konečnou kvalitu či bezpečnost. Tím také snižuje míru rizika. Použití metody předpokládá velkou zkušenost kolektivu s analyzovaným systémem složeným z více lidí tak, aby se jejich vědomosti vzájemně vykrývaly. Metoda FMEA je základem normy IEC 60812 - Failure Mode and Effect Analysis. [16]

1.5.4 Metoda HAZOP – analýza ohrožení a provozuschopnosti

Nejjednodušší a nejrozšířenější přístup k identifikaci rizik. Založena na hodnocení pravděpodobnosti ohrožení a z nich plynoucích rizik. Pomocí této metody jsou vyhledávána tzv. kritická místa a následně vyhodnocena potenciální rizika a nebezpečné stavy. Při aplikaci této týmové expertní multioborové metody členové týmu hledají scénáře např. s využitím metody brainstormingu, výsledkem jsou pak závěrečná doporučení směřující ke zlepšení procesu nebo systému. [17]

Postup metody HAZOP:

1. krok – identifikace příčin,
2. krok – odhad možných následků a rizik,
3. krok – návrhy opatření eliminace rizik,
4. krok – ocenění. [17]

Metoda byla vyvinuta společností ICI (divizí ICI Petrochemical) k systematické podrobné analýze bezpečnosti složitého technologického zařízení. Je to metoda vhodná pro velké i malé organizace. [17]

1.6 Dílčí závěr

V této kapitole byla popsána a vysvětlena základní terminologie vztahující se k tématu diplomové práce. Dále je popsána analýza rizik, proces řízení rizik a vybrané techniky posuzování rizik.

2 BEZPEČNOSTNÍ AUDIT

Pojem audit se stal synonymem pro hloubkovou kontrolu, kde přídavné jméno (např. provozní, jakostní, finanční, interní atd.) určuje zaměření auditu. Typickým znakem všech auditů je jejich interní charakter. Jsou převážně určeny pouze pro vedení organizace a mají poskytnout objektivní odpověď na jasně stanovené otázky. Objednatel auditu jako jediný obdrží prezentaci výsledných zjištění, protokol a sumarizující výrok auditora a sám rozhodne o jeho případném zveřejnění. [18]

Bezpečnostní audit by měl odhalit, jak fungují a jak jsou účinná bezpečnostní opatření v dané organizaci. Představuje písemnou bezpečnostní zprávu, kde je posouzen stav bezpečnosti organizace, tzn. porovnání např. bezpečnostní politiky firmy s její realitou. [18]

Bez ohledu na to, pro jak velkou oblast je bezpečností audit zpracováván, např. komplexní audit nebo audit jen vymezené části, výsledkem by měla být jasná a konkrétní odpověď na otázku, zda zkoumaný bezpečnostní systém je funkční a vyhovující. Pokud by tomu tak nebylo, je nutno zdokumentovat a popsat nalezené nedostatky a rozdíly, upozornit na možná rizika a navrhnout taková doporučení, aby byl systém funkční. [18]

Bezpečnostní audit zkoumá a identifikuje skutečný aktuální stav procesů a opatření v určených oblastech bezpečnosti, organizační, administrativní, personální, fyzické, počítačové a komunikační, a porovnává ho s požadovanými kritérii auditu. Provádí se zejména v souladu s mezinárodními standardy, interní dokumentací organizace a se standardy, které jsou prověřeny praxí. [19]

Obr. 2. Šest kroků auditu. [19]

2.1 Hlavní cíle auditu

Hlavním smyslem a cílem auditu je poskytnutí objektivního obrazu o stavu bezpečnosti organizace, aby se mohla přijmout taková opatření, která by vyloučila, či alespoň eliminovala zjištěná bezpečnostní rizika, díky nimž by mohly vzniknout újmy pro

organizaci. Porovnává se a posuzuje míra dosažené shody aktuálního stavu procesů a opatření vůči požadovaným kritériím, konkretizují se místa, kde je nutné investovat a kde lze naopak ušetřit, dokumentují se nalezené rozdíly a nedostatky, navrhuje se profesionální řešení a upozorňuje se na potenciální rizika. Důležité je znát účel auditu, a komu je audit určen. [18]

Další cíle auditu spočívají ve zjištění, jestli:

- v organizaci existuje bezpečnostní politika,
- má organizace zpracovány bezpečnostní plány ochrany,
- jsou nastavena a dodržována režimová opatření,
- existují a jsou dodržovány havarijní plány,
- je v objektu protipožární technika,
- jsou respektována nařízení, normy a směrnice,
- jsou prověřeny slučitelnosti reálných procesů s vedenou dokumentací,
- jsou přesně popsány odhalené neshody včetně doložení objektivních důkazů,
- jsou navržena nápravná opatření, určen termín jejich odstranění a jmenovány konkrétní osoby odpovědné za splnění nápravy. [20]

2.2 Specifikace jednotlivých druhů auditu

Bezpečnostní audity lze rozlišovat podle řady hledisek. K rozdělení lze přistupovat z různých úhlů pohledu, např. z hlediska časového nebo věcného kritéria, z hlediska smyslu auditu či komplexnosti. [21]

2.2.1 Dělení z hlediska smyslu auditu

Lidé se často domnívají, že hlavní odlišnost mezi interním a externím auditem spočívá v tom, kdo ho realizuje. Potom logicky vzniká dojem, že interní provádí interní pracovník. Rozdíl je ovšem ve smyslu auditu. [22]

Interní audit

Cílem interního auditu je napomáhat pracovníkům v organizaci, aby plnili cíle co nejefektivněji a vyvarovali se rizikům a ztrátám. Interní audit pracuje s aktuálními procesy činností, které posuzuje a zdokonaluje. Je nutné, aby audit prováděl pracovník s potřebnými

zkušenostmi, ale proto není třeba mít v organizaci zvláštní skupinu odborníků na kvalitu, či auditory. Praxe ukázala, že to není efektivní, neboť auditoři začlenění do vyčleněného týmu směřují k formalismu, protože nejsou experty na oblast, kde audit provádějí. Ideální je zajistit interní audit na úrovni vyššího středního managementu a za pomoci střídání pozic. Tento způsob obvykle komplikuje nedostatek času kompetentních manažerů, v případě výkonných pracovníků pro změnu neznalost procesů organizace. Další účinnou možností je objednat si interní audit externě jako službu (outsourcing). Výrazně tím snížíme náklady na realizaci auditu, ale především, což je důležité, vztahy externího auditora jsou jednodušší než u interních auditorů. Organizace ví, že jeho stanovisko je nepředpojaté, externí auditor se nebojí negativně hodnotit, prvořadá je pro něho, před vztahy s manažery, kvalitně odvedená práce. Interní audit v organizaci je vyžadován závazným standardem (v České republice to jsou nejčastěji normy z řady ISO). Kvalitně provedený interní audit dává užitečné výsledky pro řízení firmy, slouží jako nástroj k nepřetržitému zlepšování kvality nebo efektivity a zprostředkovává podněty, kde organizaci zlepšovat. [22]

Externí audit

Externí audit, na rozdíl oproti internímu auditu, se zaměřuje na ověření plnění externích, případně i interních standardů. Ověřuje, jestli organizace dodržuje pravidla, ke kterým se zavázala anebo, které ji nařizuje legislativa. Podklady pro externí audit jsou historické záznamy, popřípadě znalosti pracovníků. Vykonání externího auditu se vyžaduje od autorizované organizace, která má oprávnění tento audit vykonávat. Je nutné si ověřit, že pro příslušnou normu má tato firma oprávnění a že rozumí oboru organizace, ve které má být audit proveden. [22]

Rozdíl mezi interním a externím auditem je v jejich účelu, v jejich vstupech i výstupech. Naopak rozdíl nespočívá v tom, kdo jej realizuje. Klidně může být externí audit prováděn interním pracovníkem, ale je složité přesvědčit externí subjekty o jeho objektivitě. Interní audit je více komplexní a nepodléhá ve větší míře standardům a normám. Externí audit je vždy omezen konkrétním účelem, proto hovoříme o auditu konkrétní oblasti, např. audit plnění konkrétního standardu (požárními předpisy, CMMI, ČSN EN ISO 9001:2009), audit finanční, audit personální. [22]

2.2.2 Dělení z hlediska komplexnosti auditu

Komplexní bezpečnostní audit

Komplexní bezpečnostní audit se vypracovává při posuzování bezpečnosti firmy jako celku. Jestliže je ve firmě nastavena bezpečnostní politika, je nutné kontrolovat již nastavená opatření a tím zjišťovat, zda jsou skutečně efektivní, zda bezpečnostní opatření jsou dostatečná a pokrývají všechny oblasti firmy, nebo naopak jsou zbytečně nadsazená. [23][24]

Dílčí bezpečnostní audit

Jedná se o audit, který řeší jen jednu z činností ve firmě. Přistupuje se k němu v případě, že pouze v určité sféře firmy se projevují slabiny v bezpečnostní oblasti, přičemž ostatní systémy bezpečnosti fungují bezproblémově. [21]

2.2.3 Dělení z časového hlediska auditu

Plánovaný audit

Plánované audity by měly být naplánované zodpovědnou osobou organizace na dlouhou dobu dopředu v předem nastavených periodických cyklech. Díky tomu mají auditoři vždy dostatek času se seznámit s potřebnými doklady. [25]

Mimořádný audit

Mimořádný audit se realizuje v případě významných změn v organizaci, nebo podmínek, ve kterých působí, nebo pokud se vyskytnou závažné problémy. Zde lze zahrnout např. pojistnou událost, změnu vlastníka firmy, spáchání trestného činu v objektu, nebo že došlo k mimořádné události. Výskyt mimořádných událostí (havárie, výpadky v provozu, krizové stavy) jsou jedněmi z velmi objektivních indikátorů účinnosti bezpečnostního systému v organizaci. [25]

Následný audit

Následný audit se provádí na doporučení auditora, pokud byly při plánovaném nebo mimořádném auditu zjištěny zásadní změny bezpečnostního systému organizace. Cílem je prošetřit dodržení zavedených nápravných protiopatření. [25]

2.2.4 Dělení dle objektu prověřovaného auditem

Bezpečnostní audit dle objektu prověřování lze provádět několika způsoby. Patří zde audit objektové bezpečnosti, audit jakosti výrobků (služeb), audit systémů (jakosti procesů) a audit lidských zdrojů. [26]

Audit objektové bezpečnosti

Audit objektové bezpečnosti hodnotí zejména technické a fyzické zabezpečení určeného objektu. Vychází z bezpečnostní prověrky firem a její uplatnění do dalších řídících dokumentů.

Audit systémů

U tohoto auditu jde především o posouzení zavedení bezpečnostní ochrany systému jakosti a vyhodnocení její účinnosti. Cílem je důkladně posoudit efektivnost, stupeň a výhodnost pracovních procesů a postupů, jejichž výsledkem jsou výrobky a bezpečnostní služby. Tento typ auditu vyžaduje přítomnost specialisty na prověřovaný proces. [26]

Audit jakosti výrobků a služeb

Audit jakosti výrobků a služeb je zaměřen na prověrku schopnosti určitého výrobku plnit požadavky zákazníka. Sleduje se úroveň plnění parametrů spolehlivosti, funkčnosti, technické úrovně a bezpečnosti. Provádí se řada funkčních zkoušek, testy, měření, zátěžové testy, zkoušky spolehlivosti a funkčnosti apod. U služeb se posuzuje efektivnost a funkčnost dle požadavků zákazníků, případně doklad o certifikaci apod. [26]

Audit lidských zdrojů

U tohoto auditu se jedná o ucelený proces hodnocení fyzických a psychických požadavků na pracovníky pro výkon daného povolání.
Audit se zaměřuje zejména na odhalení neshod:

- v dodržování popisu práce,
- v zjišťování pracovních podmínek,
- v plnění požadavků na tělesné a duševní vlastnosti zaměstnanců,
- v celkové úrovni osobní odpovědnosti a úrovni profesních znalostí,
- v úrovni dalšího vzdělávání zaměstnanců,
- v úrovni personální práce,
- v úrovni hygieny a bezpečnosti práce v podniku. [26]

2.3 Jednotlivé etapy auditu

Lze říci, že auditní etapy jsou stejné, ať se audit vypracovává pro kohokoliv a cokoliv, a jde o plánovací, přípravnou, realizační, následně kontrolní a zakončovací fázi. Níže popisované fáze auditu jsou fázemi auditu na systém jakosti.

2.3.1 Plánovací fáze

Fáze plánování vyžaduje důkladnou přípravu a provedení. Vypracování ročních plánů auditů má za úkol rozdělit lidské a materiální zdroje v čase, a tím mít doklady o tom, že audity jsou plánovány, realizovány a dokumentovány. Plán auditů může zahrnovat všechny typy auditů, včetně interních. Měly by vždy pokrýt během roku celý dotyčný podnik. Plány auditů je nutno kontrolovat, doplňovat a aktualizovat podle momentálního operativního vývoje bezpečnostní, ekonomické či technické situace. Aktualizace se provádí zpravidla 1x měsíčně a po revizi se plán stává závazným. [26]

2.3.2 Přípravná fáze

Přípravná fáze má za úkol vytvořit podmínky pro hladký a efektivní průběh auditu. Přípravu auditu realizujeme v tzv. krocích.

Krok 1.

Zde se získávají a shrnují bezpečnostní informace, které tvoří podklady pro cíle auditu, typ a délku auditu, termín auditu a vytvoří se auditorský tým. [26]

Krok 2.

Oznámení auditní návštěvy je nutné dané organizaci včas oznámit. Oznamuje se cíl auditu, datum, prověřovaná oblast, požadované základní dokumenty, jména členů týmu a hrubý časový rozvrh. Termín návštěvy se oznamuje nejméně 3 měsíce dopředu, a to z důvodu, aby se prověřovaná organizace mohla řádně připravit. Sdělení se předává elektronicky, e-mailem, telefonicky, ovšem po ústním sdělení musí následovat i sdělení písemné. Součástí oznámení auditu je i potvrzení termínů, které jsou navrhovány. Pokud auditovanému nevyhovují, musí být oznámeny nové, s uvedením důvodu změny. Tento proces vždy předchází před konečným vytvořením programu auditu. [26]

Krok 3.

Úkolem v tomto kroku je získání předběžných údajů o kontrolované oblasti. Jedná se např. o kopie příručky jakosti, systém jakosti pracovních instrukcí, dokumenty k řízení procesů, organizační směrnice, dispoziční plány řízení a provozních prostor, kopie výroční zprávy, vyhodnocení informace o výrobních a ekonomických ukazatelích, zpráva o posledním bezpečnostním auditu, zprávu o realizaci bezpečnostní politiky firmy a její model, jméno bezpečnostního manažera a kontaktních osob, spojení s nimi, pracovní doba aj. [26]

Krok 4.

Prostudování a přezkoumání všech dostupných informací a zpráv z předchozích auditů, studium záznamů o nesrovnalostech včetně přijatých nápravných opatření, zápisy o bezpečnostních problémech včetně problémů bezpečnosti a hygieny práce, požární ochrany, security managementu, informační bezpečnosti, krizového řízení systému, technického zabezpečení aj. Auditor má v tomto kroku možnost provést informační návštěvu podniku. [26]

Krok 5.

Stanovení členů týmu. Auditu se kromě vlastních auditorů mohou zúčastnit i techničtí experti a pozorovatelé z řad vedoucích pracovníků auditovaného podniku. [26]

Krok 6.

Zpracování vývojových diagramů, technických expertíz, matic prvků činností a kontrolních seznamů. [26]

Krok 7.

Vypracování a distribuce programu auditu. V tomto kroku musí každý člen týmu auditorů a prověřovaného útvaru v organizaci obdržet oficiální čistou kopii programu auditu nejméně 14 dní předem. [26]

Krok 8.

Pokud je to možné, pak ještě před vlastním auditem by se všichni členové týmu měli sejít ke krátké instruktáži. [26]

Krok 9.

Aktualizace programu. Pokud dojde na jedné či druhé straně k závažným změnám, měly by se promítnout i v programu auditu ještě před jeho vlastním uskutečněním. [26]

2.3.3 Realizační fáze

Krok 1. - Vstupní jednání

Vede jej vedoucí auditor. Tento krok je orientován na vzájemné seznámení auditorů se zástupci prověřovaného útvaru nebo organizace. Ve vstupním jednání se diskutuje o detailním harmonogramu auditu, připomínkách, upozornění na každodenní přehled zjištění

z auditu, na prezentaci a způsobu hlášení zjištěných neshod. Auditoři se zde seznámí s průvodcem auditu a informují ho o svých představách o průběhu auditu.

Krok 2. - Sběr informací a objektivních důkazů

Postup záleží na řadě faktorů, a to především na zvoleném postupu při plánování pořadí pracovních operací v dané oblasti, řídících zásadách a návycích managementu prověřované organizace či útvaru. Pro méně zkušené či začínající auditory se doporučuje následující scénář:

- jako první dojde k představení auditora a snahy vytvořit neformální atmosféru,
- ověření relevantnosti základních informací o daném útvaru získaných v přípravné fázi jako např. organizační schéma, popisy práce, odpovědnost a pravomoci, technologické reglementy, dokumentace sytému jakosti a jak je vedena a udržována,
- auditor porovná dokumentaci s příručkou jakosti, předpisy, vyhláškami, normami, pracovními postupy a jinými legislativními doklady,
- požádá pracovníky na prověřovaném místě, aby mu popsali pracovní metody, výrobní technologie, kontrolní činnost a kontrolní místa,
- auditor zjišťuje důkazy pro potvrzení informací, které získal od pracovníků např. formou zkoumání záznamů o jakosti a pozorováním provádění práce, pomocí dotazů kladených pracovníkům apod., podle toho vyhodnocuje efektivnost procesu,
- auditor upozorňuje na zlepšení práce a zároveň předává návrhy na zlepšení, když zjistí, že formální požadavky jsou sice splněny, ale činnost by bylo možné provést efektivněji či rychleji, nebo s nižší spotřebou zdrojů,
- po získání a zaznamenání všech potřebných údajů a záznamů zjištěných nedostatků i kladů poděkuje za spolupráci,
- auditor shrne zjištěná fakta poznatků za účasti zástupců prověřované organizace.

Auditor si sám určuje, která místa a technologické procesy chce vidět. Vždy by měl dokázat poradit, jak by se mohly řešit odchylky, neshody, problémy či jiné nedostatky. Špatně je, pokud to neumí a poukazuje jen na nedostatky.

Krok 3. - Závěrečné jednání a protokol o auditu.

Realizační fáze bezpečnostního auditu je zakončena oficiálním závěrečným jednáním za účasti auditorů a vedoucího managementu organizace. Je nutné ho připravit tak, aby

nedocházelo k nedorozuměním. Je nezbytné řádně popsat neshody, pečlivě presentovat výsledky a závěry auditu v průběhu závěrečného jednání. Toto jednání se koná po ukončení zjišťovacích a analytických činností. Cílem je stanovit nápravná opatření a předat ucelenou informaci o bezpečnostní situaci v organizaci. Je vypracován a předán protokol o auditu. [26]

2.3.4 Fáze následné kontroly

Každá auditorská činnost musí mít i kontrolní fázi. Všechna nápravná opatření k odstranění neshod je nutné správně implementovat. Není nutné, aby následná kontrola nápravných opatření byla prováděna dalším auditem v oblastech, kde byly zjištěny neshody. Existují i jiné varianty prověření, které jsou výrazně levnější a časově méně náročné, a to např.

a) pokud původní opatření nevyžaduje okamžitou akci, ověření se provede až při následném auditu,

b) prověření se provede vstupní přejímkou,

c) prověření kontrolovaných článků nových dokumentů, např. u systémů jakosti, které jsou spjaty s prověřovanou oblastí,

d) uskutečnění ověření specialitou (elektro, bezpečnosti a ochrany zdraví při práci, bezpečnostním, požárním apod.) při obvyklé návštěvě prověřované organizace,

e) při externích auditech, kdy je vhodný poradce v rámci interních auditů.

Následná kontrola má za úkol ověřit úroveň využití a účinnost nápravných opatření. Lze konstatovat, že bezpečnostní audit je vlastně diagnostický subsystém řízení a všechny auditní činnosti jsou hlavním zjišťujícím nástrojem vedení organizace a fungují jako zpětná vazba sdělující údaje o stavu bezpečnostních systémů v organizaci a bezpečnostních procesů v něm probíhajících. [26]

2.3.5 Zakončení auditu

Audit je zakončen zhotovením závěrečné zprávy a vypracováním hodnocení činnosti skupiny auditorů. Vedoucí auditor zodpovídá za správný průběh a řádné ukončení auditu. Závěrečná zpráva podává kompletní, přesný a jasný záznam o auditu. Zpráva by měla obsahovat:

- předmět a cíl auditu, především označení organizačních a funkčních jednotek nebo procesů kontrolovaných v určitém čase,
- identifikační údaje auditora a jeho týmu,
- seznam představitelů organizace, která byla auditována,
- data a místa konání auditu,
- kritéria, zjištění a závěr auditu,
- překážky, které při auditu nastaly a které mohou snížit spolehlivost závěru z auditu,
- rozsah splnění cíle auditu a nepokryté oblasti, i když byly v předmětu auditu,
- nedořešené rozdílné názory mezi auditory a organizací,
- návrhy ke zlepšování, pokud jsou popsány v cílech auditu,
- rozdělovník zprávy. [27]

V praxi je běžné prezentování bezpečnostní zprávy před vedením společnosti a její závěry si obhájit. [18]

Závěrečnou zprávu obdrží zadavatel auditu a organizace, která audit provádí. Záznamy, které jsou podstatné pro prokázání auditu, např. plán auditu, použité podklady a jednotlivá zjištění, se vyhodnotí dle vhodnosti a použitelnosti pro další audit a jsou archivovány. [27]

2.4 Vymezení oblastí auditu

Základním pravidlem u kvalitně provedeného bezpečnostního auditu je nutnost daný problém řešit a posuzovat komplexně. V každé organizaci je nutné chránit:

- fyzické osoby,
- hmotný majetek,
- nehmotný majetek,
- informace.

Pro získání co nejvyššího stupně zabezpečení se využívají bezpečnostních opatření a prostředky:

- fyzická ostraha,
- administrativně organizační a režimová opatření,

- technická ochrana,
- kombinace předchozích prostředků a opatření. [20]

Audit se dá rozdělit do následujících oblastí:

- audit objektové bezpečnosti,
- audit fyzické ostrahy,
- audit technické ochrany,
- audit režimových opatření,
- audit personální bezpečnosti,
- audit bezpečnosti a ochrany zdraví při práci,
- audit požární ochrany,
- audit informační bezpečnosti.

2.4.1 Audit objektové bezpečnosti

Při auditu objektové bezpečnosti dochází ke kontrole technického a fyzického zabezpečení objektu organizace. Kontroluje se, zda vůbec toto zabezpečení existuje, a pokud ano, tak do jaké míry je efektivní. [20]

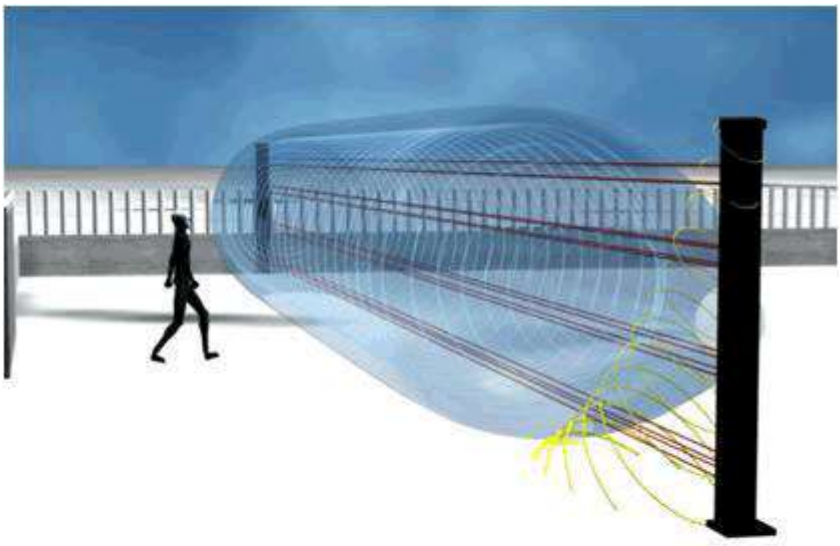
Z prostorového hlediska lze vnější ochranu objektů rozdělit na:

a) perimetrickou (0. linie = venkovní ochrana) – perimetrickou ochranou se rozumí ochrana okolí domu či pozemku před nepovolaným vstupem osob. Protože téměř nikdy není možné střežit celou plochu pozemku, střeží se pouze určitá pásma na obvodu daného pozemku. Mezi nejvíce používané systémy patří mikrofonické kabely vpletené do drátěných plotů, infračervené závory, mikrovlnné bariéry nebo zemní detekční kabely, [28][29]

b) plášťovou (1. linie ochrany) – slouží k odhalování pokusu o vniknutí přes vnější plášť střeženého prostoru. Je to ochrana prostupů do objektu (dveře, okna, světlíky). Výhodou plášťové ochrany je, že k detekci narušení nastává již v prvním okamžiku vniknutí. Plášťovou ochranu lze využít pro střežení i v době, kdy je zaměstnanec přítomen v objektu, a to např. v noci. U této ochrany se používají magnetické kontakty, detektory tříštění skleněných ploch, poplachové fólie, polepy, [30]

c) prostorovou (2. linie ochrany) – využívá se v případech plošného zabezpečení celého zájmového prostoru. V době střežení se v prostorách nesmějí pohybovat žádné osoby a ani v něm nelze volně skladovat materiál bez předem určených podmínek. Prostorovou ochranu je možné zajišťovat fyzickou ostrahou nebo technickými prostředky, např. pasivními infračervenými detektory, mikrovlnnými detektory nebo laserovými systémy, [29][31]

d) předmětovou (3. linie ochrany) – předmětovou ochranou rozumíme samostatné zabezpečení vybraných předmětů v objektu. Detektory bývají připojeny do samostatně ovládané skupiny z důvodu střežení i v době zvýšeného provozu. [32]



Obr. 3. Příklad perimetrické ochrany – infračervené závory. [28]

2.4.2 Audit fyzické ostrahy

Fyzická ostraha (dále jen FO) je nejstarší, a i v dnešní době nejčastější, formou zajišťování ochrany objektu. Významná je skutečnost, že v případě nutnosti je schopná zasáhnout k odvrácení nebezpečí. Aktivně se podílí na překažení incidentu narušitele a na pomoci k jeho dopadení. FO může být realizována buď vlastními zaměstnanci nebo soukromou bezpečnostní službou. [21]

FO lze dělit z hlediska:

a) časového – vázaná na pracovní dobu, nepřetržitá, kombinovaná,

b) dle způsobu zajištění – z řad vlastních pracovníků firmy, najímaná, kombinovaná,

c) dle rozsahu výkonu – propustková, obvodová, dohledová, přehledová dozorová a výjezdové skupiny,

d) podle výzbroje a výstroje – ozbrojená, neozbrojená,

e) podle vystupování vůči veřejnosti – veřejná, skrytá,

f) podle složení – se pracovním psem, bez psa. [23]

Z dosavadních zkušeností lze možno odvodit následující metody FO:

- fyzické pozorování,
- kontroly osob,
- přesvědčování,
- osobní prohlídky a kontroly zavazadel,
- evakuační a ochranná opatření,
- kontroly dokladů,
- kontroly vozidel a nákladů,
- fyzické zábrany a bariéry,
- zajištění místa činu,
- obranné a ochranné zákroky. [21]

2.4.3 Audit technické ochrany

Technická ochrana používá systémy a technické prostředky – tedy bezpečnostní prvky, pomocí nichž se má zabránit, ztížit nebo oznámit narušení chráněného objektu, ale také systémy, které signalizují vznik požáru či změny stavů vedoucí k různým haváriím. Jedná se o detekční systém, který zajišťuje a předává údaje o stavu ve střeženém prostoru. [21][33]

Technickou ochranu členíme podle základních technických principů do tří skupin:

a) mechanické zábranné systémy (dále jen MZS) – zde je důležitá mechanická odolnost, která má zabránit neoprávněnému vniknutí do objektu. Mezi MZS patří:

- kovové mříže – pevné, pohyblivé,
- bezpečnostní dveře – plechové, pancéřované, požární, trezorové apod.,

- bezpečnostní skla – tvrzená, neprůstřelná, kalená apod.,
- úschovná místa – trezory, plechové skříně,
- bezpečnostní uzamykatelné systémy – dozické, cylindrické, dveřní závory, elektrické zámky, s magnetickou kartou apod. [21]

b) elektronické systémy – poplachové zabezpečovací a tísňové systémy, kamerové systémy, dohledové a přijímací poplachové centrum, elektrická požární signalizace, systém kontroly vstupu, tísňová tlačítka pro přivolání pomoci při zdravotních potížích a nouzi, prostředky pro detekci látek, komunikační systémy. [23]

c) mechatronické systémy – představují kombinaci mechanických zábranných systémů se systémy elektronickými, např. přístupový systém s jednoznačně nastavenými přístupovými právy uživatelů. [23]

2.4.4 Audit režimových opatření

Režimovou ochranu tvoří souhrn administrativních a organizačních opatření vedoucích k zajištění chráněných zájmů a hodnot. Jednotlivé pokyny, zajišťující režimovou ochranu, mohou být jak psané, tak slovní, následně tedy trvalé či dočasné a mohou být závazné pro určitou skupinu osob nebo pro všechny. Režimová opatření by měla zajistit požadovaný stupeň bezpečnosti, ale neměla by příliš omezovat pohyb zaměstnanců v objektu. [34]

Za důležité se považuje hlavně:

- vstupní a výstupní režim osob a dopravních prostředků – kontrola vstupu a odchodu zaměstnanců a návštěv do objektu, kontrola příjezdu a odjezdu vozidel do areálu, oprávněnost vnášení, vynášení a vyvážení předmětů a materiálu,
- režim pohybu zaměstnanců v objektu – určuje části objektu s omezenou přístupností, a označení příslušnosti pracovníků k určitým provozům či pracovištím,
- materiálový a expediční režim – stanovuje postup při příjmu, skladování, výdeji a pohybu materiálu,
- provozní režim – zajišťuje plynulost a bezpečnost provozu a činnosti při mimořádných událostech,
- klíčový režim provozu – stanoví označování, přidělování a předávání klíčů, výrobu náhradních klíčů, výměnu zámků v důležitých částech objektu apod.,
- provozní režim spojený s fungováním systémů zabezpečovací techniky. [35]

2.4.5 Audit personální bezpečnosti

Personální bezpečnost je nejméně spolehlivý faktor bezpečnostního prostředí, neboť člověk je silně ovlivnitelný, a tedy je nestabilním elementem v organizaci. Personální bezpečnost je základním druhem zajištění ochrany utajovaných informací, a kromě ověřování podmínek, které musí fyzická osoba splňovat, aby jí byl umožněn přístup k utajované informaci, zahrnuje personální bezpečnost i výchovu těchto osob. [25][36]

Základem je výběr vhodného budoucího zaměstnance na základě nároků na konkrétní pozici. Rozhodující vliv na přijetí by měla být úroveň profesních znalostí, vzdělání a celková schopnost vykonávat požadovanou práci. [25]

Oblast personální práce zahrnuje především vstupní školení, následné další prohlubování profesních znalostí a taktéž průběžné hodnocení a kontrola zaměstnanců. [25]

V personální bezpečnosti může být audit zaměřený na:

- úroveň odborné přípravy zaměstnanců,
- duplicitu pracovních pozic,
- spolehlivost zaměstnanců,
- jazykovou bariéru na pozicích, kde je to potřeba. [25]

2.4.6 Audit bezpečnosti a ochrany zdraví při práci

Bezpečnost a ochranu zdraví při práci (dále jen BOZP) lze definovat jako legislativou vymezená opatření či pravidla, jimiž zaměstnavatel eliminuje vznik potenciálních rizik na pracovišti a to jak pro zaměstnance, tak i pro ostatní fyzické osoby (zákazníky, klienty apod.), které se mohou pohybovat v blízkosti pracoviště. Nejdůležitějším zákonem z pohledu BOZP je zákon č. 262/2006 Sb. Zákoník práce, kde jsou zakotveny základní požadavky na vztah mezi zaměstnancem a zaměstnavatelem. Mezi další zásadní předpisy patří zákon č. 309/2006 Sb. O zajištění dalších podmínek BOZP. [37][38]

BOZP zahrnuje kontrolu sytému řízení, kontrolu plnění v jednotlivých úsecích BOZP a přímou kontrolu pracovišť. [25]

Předmětem auditu je:

- prevence rizik,
- školení zaměstnanců na všech stupních pracovní činnosti,

- kontrola všech pracovišť,
- bezpečnost a hygiena práce,
- kontrola bezpečnosti technických zařízení,
- kontrola a ověření správnosti dokumentů,
- pracovně lékařská péče,
- osobní ochranné pracovní pomůcky,
- nebezpečné látky nacházející se na pracovišti,
- roční prověrka BOZP. [25]

2.4.7 Audit požární bezpečnosti

Dle vyhlášky č. 246/2001 Sb., o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci) ve znění Vyhlášky č. 221/2014 Sb. lze požární bezpečnost definovat následně:

„Souhrn organizačních, územně technických, stavebních a technických opatření k zabránění vzniku požáru nebo výbuchu s následným požárem, k ochraně osob, zvířat a majetku v případě vzniku požáru a k zamezení jeho šíření.“ [39]

Dle výše uvedené vyhlášky se do věcných prostředků požární ochrany řadí např.:

- pojízdné hasicí přístroje,
- přenosné a přívěsné hasicí přístroje,
- hasiva a příměsi do hasiv,
- osobní ochranné prostředky,
- prostředky pro evakuaci a záchranu osob (např. žebříky, seskokové matrace),
- přenosné zásahové prostředky (např. požární stříkačky),
- prostředky pro dekontaminaci a pro práci s nebezpečnými látkami,
- požární výzbroj a výstrojní součástky,
- spojovací a komunikační prostředky operačních středisek. [39]

Mezi požárně bezpečnostní zařízení řadíme:

- zařízení pro požární signalizaci (např. zařízení dálkového přenosu, elektrická požární signalizace),
- náhradní zdroje a předměty pro zabezpečení provozuschopnosti požárně bezpečnostních zařízení,
- zařízení pro únik osob při požáru (např. nouzové osvětlení, výtahy evakuační či požární),
- zařízení pro utlumení požáru (např. samočinné hasicí systémy),
- zařízení pro usměrňování pohybu kouře v důsledku požáru (např. kouřová klapka včetně ovládacího mechanismu),
- zařízení pro omezení šíření požáru (např. požární klapky, požární dveře),
- zařízení pro zásobování požární vodou (např. vnitřní i vnější požární vodovod včetně nástěnných či nadzemních a podzemních hydrantů),
- zařízení zamezující vznik požáru nebo výbuchu. [39]

Do požárního auditu můžeme zařadit kontrolu:

- systému požární ochrany,
- bezpečnostních značek a značení,
- prostředků požární ochrany a volného přístupu k nim,
- označení únikových cest a východů při krizových a mimořádných událostech,
- zpracování dokumentace.

2.4.8 Audit informační bezpečnosti

Informační bezpečnost můžeme definovat jako ochranu důvěrnosti, integrity a dostupnosti informací. Důvěrností se rozumí zajištění, že informace jsou přístupné pouze těm, kdo jsou k přístupu oprávněni, integrita znamená zajištění správnosti a úplnosti informací a metod jejich zpracování a konečně dostupnost informace je totéž, co její použitelnost pro oprávněné uživatele v okamžiku potřeby. [40]

Při ochraně informací jsou zásadním faktorem lidé, jejich možnost selhání a nespolehlivost. Primárním předmětem ochrany jsou informace. Čím větší hodnotu pro organizaci informace mají, tím větší pozornost se musí věnovat bezpečnosti jejich nosičů. Každá organizace by si proto měla vypracovávat alespoň základní hodnocení a kategorizaci svých informací a tomu

přizpůsobit i způsob jejich ochrany. Velikost investic do bezpečnosti musí odpovídat důležitosti aktiv a míře možných rizik. Změny v procesech organizace při zavádění systému řízení bezpečnosti informací, a při aplikaci opatření v ICT systémech, musí dostatečně redukovat dopady možných rizik za akceptovatelných nákladů. [37][41]

Obr. 4. Schéma základních procesů řízení bezpečnosti informací dle ITIL (Information Technology Infrastructure Library). [41]

Při auditu je nutné se soustředit na možnosti napadnutelnosti sítě jak zvenku, tak i zevnitř organizace.

Úkolem každé organizace by mělo být:

- bezpečná manipulace se všemi informacemi, týká se to hlavně ochrany osobních údajů a informací typu státního, obchodního, bankovního a služebního tajemství,
- upozornění všech zaměstnanců na zachování mlčenlivosti o skutečnostech, které by mohly poškodit jméno organizace. [25]

Součástí informační bezpečnosti je zabezpečení technických prostředků sloužících ke zpracování a přenosu informací. Je zapotřebí, aby způsob ochrany byl vymezen

v jedinečném dokumentu, který bude neoddělitelnou a nezbytnou dokumentací při vytváření auditu v této oblasti.

I v této oblasti je třeba stanovit určitá pravidla, opatření (zálohy, archivace, šifrování), přiřazení odpovědnosti jednotlivým pracovníkům, jejich přístupy např. na určité servery, sdílené disky, helpdesky. Hlavní úloha IT je zabezpečení sítě proti škodlivým vlivům. V rámci bezpečnostní politiky je třeba klást velký důraz při bezpečnostním auditu na stáří jednotlivých technických počítačových komponentů, jako např. servery, počítačové pracovní stanice. [25]

V oblasti IT bezpečnostních auditů se klade důraz na tyto oblasti:

a) síťová bezpečnost – definuje pravidla v síťovém prostředí,

b) bezpečnost dat – definuje pravidla nakládání s daty:

- klasifikace dat – řízení bezpečnosti dat,
- ochrana osobních dat,
- pravidla pro zálohování dat, archivaci a šifrování.

c) dokumentace – dokumentuje aktuální stav informační bezpečnosti v organizaci:

- definování rozsahu ISMS (systém stanovující základní požadavky na bezpečnost všech forem reprezentace informací podle normy ISO27001),
- dokumentování aktuálního stavu informační bezpečnosti v organizaci,
- aktuální stav bezpečnostních opatření.

d) směrnice platné pro oblast informační bezpečnosti,

e) budování bezpečnostního povědomí:

- členění uživatelů,
- definování stupně bezpečnostního školení. [42]

Nejdůležitější částí informačního auditu je zjištění nedostatků při napadnutí IT systému. K ověření a posouzení úrovně zabezpečení se používá tzv. penetrační test. Jeho snahou je vniknutí do informačního systému, zjištění co možná nejvíce možných děr a cest, kterými může být napaden. Tento test má svoje náležitosti a pravidla, a musí být v souladu s normami. Pokud je zadáván externí firmou, je třeba zaručit ochranu dat, a to za účasti někoho z IT, a společně zabezpečit bezpečný průběh testu, tzv. nepoškození dat. [43]

2.5 Dílčí závěr

V této kapitole byl podrobně popsán bezpečnostní audit, konkrétně jeho cíle, druhy, etapy a oblasti.

II. PRAKTICKÁ ČÁST

3 OBECNÉ INFORMACE O PŘEDMĚTU AUDITU

Pro svou diplomovou práci jsem si vybrala objekt státní správy, konkrétně Krajskou hygienickou stanici Zlínského kraje (dále jen KHS ZK). Budova, ve které KHS ZK sídlí, byla schválena a zkolaudována pro administrativní a zdravotnický provoz v roce 1976.

Objekt byl původně realizován jako objekt Okresní hygienické stanice, byly zde kancelářské prostory a laboratoře. Během doby užívání došlo k úpravám a změnám účelů prostor, a to zejména o změnu užívání laboratoří na kancelářské prostory, spisovny, ordinace lékařů s čekárnami a podobně. Charakter objektu je daný dobou výstavby a po dobu užívání nebyl měněn.

3.1 Charakteristika činnosti objektu státní správy

Krajská hygienická stanice Zlínského kraje, se sídlem ve Zlíně, plní úkoly v oblasti ochrany veřejného zdraví v rozsahu stanoveném zákonem č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, ve znění pozdějších předpisů a dalšími právními předpisy a dokumenty.

Plní úkoly stanovené příslušným orgánem krizového řízení kraje a Ministerstvem zdravotnictví České republiky (dále jen MZ ČR) v oblasti ochrany veřejného zdraví ve svém správním obvodu, v rozsahu stanoveném zákonem č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, ve znění pozdějších předpisů a dalšími právními předpisy.

Dále plní úkoly MZ ČR, které jí byly uloženy vládou České republiky v době vyhlášení krizového stavu a souvisí s ochranou veřejného zdraví a úkoly související s činností krajské epidemiologické komise, spolupracuje s Ústřední epidemiologickou komisí.

Informuje bez prodlení MZ ČR o připravovaných i přijatých opatřeních v oblasti ochrany veřejného zdraví, realizovaných v souvislosti s řešením krizové situace na území kraje, nebo v souvislosti s přípravou na řešení, hrozí-li vznik krizové situace.

3.1.1 Organizační struktura objektu státní správy

Hlavní činnost KHS ZK je rozdělena do 5 odborů, které spadají do sekce ochrany a podpory veřejného zdraví. Jsou to tyto:

1. **Odbor protiepidemický** – zde patří protiepidemické oddělení, oddělení hygieny zdravotnických zařízení a oddělení desinfekce, desinsekce a deratizace.

Epidemiologie je lékařské odvětví, které se zabývá zkoumáním faktorů ovlivňujících zdraví a nemocnost obyvatelstva, jde především o přenosné choroby. Odbor protiepidemický vykonává mimo jiné státní dohled nad infekčními chorobami, provádí opatření v centru nákazy, vydává karanténní opatření, sleduje drogovou problematiku v kraji, sleduje proočkovanost dětí.

Oddělení hygieny zdravotnických zařízení se zabývá problematikou hygieny ve zdravotnických zařízení s cílem předcházet vzniku a šíření nemocničních nákaz.

Oddělení desinfekce, desinsekce a deratizace zahrnuje činnosti vedoucí k ochraně zdraví osob, životních a pracovních podmínek, před živočichy přenášející infekční onemocnění.

2. **Odbor hygieny obecné a komunální** – je vykonavatelem státního zdravotního dozoru péče o životní podmínky v oblastech např. ubytovacích služeb, vnitřního prostředí staveb, koupališť, pohřebnictví, ochrany před hlukem a vibracemi v mimopracovním prostředí, hygienických požadavků na vodu a povinnosti osob při kontrole pitné vody, dále v oblasti odpadů a výkon činností epidemiologicky závažných (kadeřnictví, manikúra, solária, kosmetika, masáže a činnosti, při kterých je porušována integrita kůže – tetováže, piercing, permanentní make-up apod.).
3. **Odbor hygieny výživy a předmětů běžného užívání** – vykonává dozor v rámci provozování hostinské živnosti v restauračních zařízeních všech typů, stravování zaměstnanců a žáků, v zdravotních a sociálních službách včetně lázeňské péče, a také odběry vzorků potravin k laboratornímu vyšetření. Dále provádí kontrolu bezpečnosti výrobků určených pro styk s potravinami, kosmetické přípravky, hračky. Tento odbor se také podílí na zajišťování úkolů plynoucích ze systémů rychlého varování členských zemí EU (Rapid Alert System), které varují před riziky v oblasti zdraví a bezpečnosti spotřebitele (varovný systém pro potraviny a krmiva a varovný systém pro nepotravinářské výrobky).
4. **Odbor hygieny práce** – provádí dozor nad zajištěním pracovně-lékařských služeb, řeší problematiku kategorizace prací a stanovují rizikové práce, řeší podněty občanů na nevyhovující pracovní podmínky, zajišťují dozor v oblasti ochrany zdraví při nakládání s nebezpečnými chemickými látkami a ověřují pracovní podmínky na pracovišti jako podklad pro případné hlášení nemoci z povolání.

5. **Odbor hygieny dětí a mladistvých** – kontroluje, zda jsou plněny povinnosti stanovené k ochraně veřejného zdraví: ve školách mimo vysokých škol, v zařízeních sociálně právní ochrany dětí, v dětských zdravotnických zařízeních (jesle, kojenecké ústavy, dětské domovy, stacionáře), při provozování venkovní hrací plochy s pískovištěm, při provozu živnosti péče o dítě do 3 let věku v denním režimu a živnosti mimoškolní výchova a vzdělávání.

3.2 Charakteristika budovy KHS ZK

Objekt je v současné době rozdělen provozně a prostorově následovně:

- na část sloužící ředitelství Krajské nemocnice T. Bati, a. s. (dále jen KNTB) - 5. NP, 6. NP a 7. NP. V 1. NP má KNTB lékárnu, bufet, pokladnu, WC pro veřejnost a poštovní oddělení.
- na část sloužící Krajské hygienické stanici Zlínského kraje se sídlem ve Zlíně - 2. NP (pouze ½), 3. NP a 4. NP. V 1. NP KHS ZK buduje novou podatelnu, archiv a technické místnosti.
- a na část užívanou oběma subjekty v 1. NP – tj. vstupní prostory, komunikační koridor, technický suterén, rozvodna, prostor schodiště, výtahy, strojovna výtahů a rovněž střechy nad 7. NP a 8. NP.

3.3 Dílčí závěr

V rámci této kapitoly bylo seznámení s objektem státní správy, kterým je KHS ZK. Je popsána charakteristika vykonávaných činností KHS ZK, dále objekt, ve kterém sídlí a který bude předmětem bezpečnostního auditu.

4 POPIS OKOLÍ BUDOVY KHS ZK

V této kapitole je popsán pozemek, na kterém se nachází budova a který tvoří okolí objektu, neboť i on je důležitý pro provedení bezpečnostního auditu. Bezpečnost uvnitř objektu výrazným způsobem ovlivňuje i zabezpečení perimetru objektu.

4.1 Výchozí informace o areálu

Budova KHS ZK je součástí areálu KNTB, který se nachází na okraji města. Celková rozloha areálu je zhruba 16,5 ha. V těsné blízkosti budovy, na její východní straně, se nachází dvoupodlažní parkovací dům pro zaměstnance a návštěvníky objektu, viz Příloha P III: Plán areálu nemocnice Tomáše Bati ve Zlíně.

Důležitým aspektem, který ovlivňuje celkovou bezpečnost, i když netvoří součást pozemku objektu, je řeka. Její koryto je vzdáleno od hlavního vstupu cca 30 metrů. V minulosti již totiž několikrát došlo k vylití vody z koryta řeky.

4.2 Obvodová bezpečnost areálu

Areál je volně přístupný všemi jeho třemi vstupy, hlavní vstup do areálu se nachází cca 20 m od silnice. Celkově je areál zabezpečen pouze ze severní strany, a to kovovým plotem vysokým 1,80 m, kde hlavním důvodem oplocení bylo zamezení vniknutí zvěře z blízkého lesa. Z jižní strany je přístupový chodník od silnice k budově lemován kovovým plotem vysokým 1,20 m, v němž je průchod bez branky.

Dvoupatrový parkovací dům je z východní strany od budovy vzdálen cca 3 m. Mezi parkovacím domem a budovou je z jižní strany kovová branka, která se nezamyká. Vjezd a výjezd ze spodního patra parkoviště, které je převážně určeno pro návštěvy, je přímo ze silnice a je zabezpečen závorami.

Vjezd a výjezd automobilů do celého areálu, také přímo k objektu a rovněž do druhého patra parkoviště, které je vyhrazeno pouze pro zaměstnance, je směřován přes vjezdové brány, které jsou zabezpečeny závorami. Zaměstnanci mají vjezd i výjezd umožněn na základě čipových karet, ostatní si odebírají z automatu parkovací lístky. Vstup do celého parkoviště je volně přístupný cizím osobám.

4.3 Režimová opatření areálu

Vjezd a výjezd z areálu je zcela nekontrolován, mohou vjíždět i vyjíždět jakákoliv osobní nebo nákladní auta, nebo také vstupovat a odcházet jakékoliv osoby.

Do areálu vjíždějí nejčastěji osobními automobily zaměstnanci, kteří parkují na vyhrazených parkovištích, dále automobily externích firem, které dovážejí zboží do skladů, a auta od dopravních společností.

4.4 Fyzická ostraha areálu

Fyzická ostraha celého areálu je zabezpečována soukromou bezpečnostní agenturou. Tato služba je zajišťována na základě smlouvy o poskytování soukromých bezpečnostních služeb, objednatelem je KNTB.

Zaměstnanci soukromé bezpečnostní agentury vykonávají v rámci areálu následující činnosti:

- klíčový režim celého objektu,
- kontrolní pochůzkovou činnost po 18. hodině v celém objektu,
- požární hlídku a asistenci v případě potřeby,
- v případě mimořádných událostí realizaci zásahu,
- při zjištění narušení objektu cizí osobou vyrozumí Policii ČR.

Fyzická ostraha probíhá nepřetržitě po celý rok.

4.5 Technická ochrana areálu

Technickou ochranu areálu představují automatické mechanické závory, kterými jsou zabezpečeny vjezdové brány do areálu. Tyto závory jsou ovládány vjíždějícími řidiči, zaměstnanci, pomocí čipových karet, ostatní řidiči, návštěvníci areálu skrze zakoupení parkovacích lístků z parkovacího automatu.

4.6 Dílčí závěr

V této kapitole je popsána obvodová bezpečnost areálu, nastavená režimová opatření a fyzická ostraha areálu a technická ochrana.

5 CHARAKTERISTIKA OBJEKTU KHS ZK

Tato kapitola se zaměřuje na popis vybraného objektu. V budově se nachází hlavně kanceláře, ordinace, serverovna a sklady.

5.1 Základní informace o objektu

Jednotlivá podlaží jsou přístupná z vnitřního schodiště vedoucího z úrovně technického suterénu až do úrovně 8. NP. Dále jsou zde dva výtahy se stanicemi v 1. NP až 7. NP. Od úrovně 2. NP probíhá středem objektu vnitřní atrium. Jednotlivé místnosti jsou přístupné z vnitřních chodeb. Obvod 7. NP je ustoupený a je zde terasa ze čtyř stran, která je přístupná z chodby. Na úrovni 8. NP je strojovna výtahu a místnost vysílače. Z prostoru podesty schodiště je přístupná terasa střechy, kde jsou umístěny jednotky vzduchotechniky. Od prostoru střechy je terasa oddělena zdivem různé výšky.

Objekt je čtvercového půdorysu s technickým (nízkým) suterénem, se sedmi nadzemními podlažími (z toho sedmé podlaží je ustupující) a s technickým 8. podlažím na části střechy. Objekt je založen na pilotách a má nosnou konstrukci tvořenou technologií Lift-Slab, tj. zvedanými stropními deskami na ocelových sloupech, s jejich obepnutím betonovými tvarovkami a stažením ovinutým přepjatým drátem. Obvodové konstrukce jsou tvořeny vyzdívanými parapetními řemeny a vyzdívkou meziokenních pilířů. Zastavěná plocha objektu je 1070,60 m^2, obestavený prostor činí 23 500 $m^{3.}$ Výška objektu je cca 28 m. [44]

Dále má objekt technické podlaží, které je celé pod úrovní terénu. Zde jsou umístěny rozvody splaškové a dešťové kanalizace, vodovodu a silnoproudých instalací. Konstruktivní výška podlaží je 3,3 m, instalačního suterénu 2,10 m. [44]

V současné době na objekt navazuje ze severní strany spojovací krček, který spojuje objekt s další budovou KNTB. V současné době je velmi zřídka využívaný a taktéž není v dobrém technickém stavu, proto se KNTB rozhodla většinu nadzemní části objektu zbourat a ponechat pouze podzemní část – energo kanál.

Objekt se nenachází v ochranném pásmu památkové rezervace, památkové zóny, ani zvláště chráněného území.

5.2 Objektová bezpečnost

Hlavní vstup do objektu je situován z jižní strany. Ze západní strany je rovněž umožněn vstup do budovy z prostoru areálu nemocnice a z východní strany vstup ze dvora. V objektu, který je zde popisován, není zřízena žádná vrátnice. Ve vstupním prostoru je umístěn elektronický systém docházky – čtečka otisků prstů. Osoby mohou do budovy v pracovní dny vstupovat volně od 6:00 do 18:00 hodin třemi vchody. Hlavní vchod, který tvoří skleněné dveře s mříží, je z jižní strany budovy a dva jsou na opačné straně budovy. Ty vedou na dvůr a do areálu nemocnice. Jedny zadní dveře jsou dřevěné a druhé skleněné. V 1. NP budovy jsou umístěny skleněné dveře opatřené mříží, které toto patro rozdělují na dvě části, a to na vstupní halu s hlavním vchodem a na chodbu, kde se nachází bufet a dvoje zadní dveře. V 18.00 hodin se hlavní vstup a vnitřní skleněné dveře automaticky uzavírají, ráno v 6:00 hodin se automaticky odemykají. Mimo otevírací dobu mohou vstupovat do budovy pouze určení zaměstnanci, kteří tomuto účelu vlastní čipovou kartu. V posledním roce byla na hlavní dveře z vnitřní strany namontována klika, aby se zaměstnanci v době uzamknutí dveří mohli dostat z budovy ven, aniž by museli použít čip. Po 18:00 hodině přichází na kontrolu již uzamčených prostor fyzická ostraha, která fyzicky prochází všechna patra v budově a kontroluje, zda jsou uzamčené vstupy od schodiště ke kancelářím. Po takto vykonané kontrole uzamyká i vstupy do budovy ze zadní strany objektu.
Osoby pobývající v objektu můžeme rozdělit do těchto kategorií:

- zaměstnanci,
- osoby, které vstupují do budovy za účelem návštěvy,
- osoby z dopravních společností,
- osoby, jejich zájem je spojen s oborem státní správy (podatelna a odbory KHS ZK),
- náhodné osoby, které budovou jen procházejí nebo ji v 1. NP použijí jako odpočinkovou zónu.

Pohyb osob po budově není nikterak omezován, lidé se na jakékoliv patro dostanou po schodišti nebo výtahem. Chodby na patrech, kterými se vchází do kanceláří, jsou taktéž volně přístupné skleněnými dveřmi, které i přesto, že ze strany od výtahu a schodiště mají kouli, jsou neustále otevřené, aby se zaměstnanci mohli volně pohybovat v celém objektu. Vstupy do objektu, a tudíž i 1. NP, jsou přístupné přímo z úrovně terénu. Proto jsou ve všech oknech v 1. NP umístěny kovové mříže, které se dají otevřít pouze z vnitřní strany místností.

Součástí stavebních konstrukcí jsou původní dřevěná výklopná okna. Technický stav oken však neumožňuje jejich otevírání z důvodu možného vypadnutí z kování na pracovníka, nebo do venkovního prostoru na komunikaci, kde mohou být ohroženi návštěvníci a zaměstnanci.

Nemožnost otevírání oken zamezuje v možnosti základní údržby, tedy mytí oken. Podstatnější problém je, že neumožňuje větrání na pracovišti, které není vybaveno jinou možností (vzduchotechnika, klimatizace). Zároveň nelze zasahovat do větších oprav žaluzií, čímž dochází v letních měsících k značnému přehřívání pracovních prostorů.

Technický stav oken způsobuje rovněž zatékání okny, zejména do elektrických rozvodů. Tím se zvyšuje pravděpodobnost vzniku požáru a úrazu elektrickým proudem. Špatný technický stav oken zároveň způsobuje velké energetické ztráty.

5.3 Požární ochrana

Objekt tvoří samostatný požární úsek vyjma prostoru lékárny v 1. NP. V budově se nachází pouze nechráněné únikové cesty. Hlavní únikovou cestu tvoří jediné středové schodiště v budově, spojující jednotlivá podlaží, a ústící na volné prostranství v 1. NP. Objekt byl dán do užívání před účinností „kodexu požárních norem“, proto se při hodnocení tohoto objektu vychází hlavně z kritérií uvedených v ČSN 73 0834 (Požární bezpečnost staveb – Změny staveb).

Činnost v budově je klasifikována jako činnost se zvýšeným požárním nebezpečím, s odkazem na § 4 odst. (2) písm. g) zákona č.133/1985 Sb., o požární ochraně, ve znění pozdějších předpisů. Za provozované činnosti se zvýšeným požárním nebezpečím se považují činnosti v budovách administrativních a zdravotnických provozů budovách o sedmi a více nadzemních podlaží, nebo o výšce větší než 22,5 m. Dále se jedná o činnost, která je charakterizována v § 4 odst. (2) písm. j) zákona č.133/1985 Sb., o požární ochraně, ve znění pozdějších předpisů. Za provozované činnosti se zvýšeným požárním nebezpečím se považují činnosti, u kterých nejsou běžné podmínky pro zásah. Za složité podmínky pro zásah se považují činnosti provozované v objektech zdravotnických provozů o 4 a více nadzemních podlažích (§ 18 písm. e) vyhlášky č. 246/01 Sb. o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci), pokud tyto objekty nemají zřízeny chráněné únikové cesty. [39]

Únikové cesty

Z jednotlivých podlaží v budově je pro únik použitelné pouze jediné únikové schodiště, a to středem budovy, viz Příloha P II: Únikový plán – 3. NP.

Toto schodiště je únikovou cestou pro více než 250 osob a zároveň jedinou zásahovou cestou pro hasiče v případě požáru. V objektu se jedná pouze o nechráněné únikové cesty, neboť objekt tvoří jeden požární úsek bez požárních předělů. Únikové cesty nejsou vybaveny nouzovým osvětlením. Povrch schodiště je z lepeného PVC, které se na některých místech odlepuje.

Během provozu objektu, při změnách majitelů a provozovatelů docházelo v budově i ke stavebním úpravám, při kterých došlo k přepažení únikových chodeb v některých podlažích, čímž došlo k prodloužení únikových cest, případně snížení počtu směru úniku ze dvou na jeden. Dále byly na některých chodbách instalovány dveře, které zužují únikovou cestu, nebo zamezují trvalý průchod. Hlavní východ z objektu je po pracovní době elektronicky blokován a dveře bez použití čipu dříve nešly otevřít. V posledním roce byla z vnitřní strany hlavního vchodu namontována klika, aby osoby mohly z budovy odejít i po pracovní době, aniž by musely použít čip.

V budově se nenachází požární evakuační výtah. Výtahy a osvětlení v budově jsou napojeny na náhradní zdroj elektrické energie (dieselagregát je umístěný mimo budovu v energetickém centru KNTB).

Dělení do požárních úseků

S ohledem na stáří objektu není objekt členěný do požárních úseků, což má vliv na skutečnost, že v případě požáru nebude zabráněno v šíření požáru, zejména toxických zplodin, které obsahují dým (možnost vzniku komínového efektu apod.). Dělení do požárních úseků minimalizuje i rozsah škod. Mezi jednotlivými podlažími je spousta prostupů (stupačky apod.). Rizikem pro rychlé šíření požáru je i vnitřní atrium budovy, kde může při požáru docházet k přenosu požáru otevřenými požárními plochami (okna) v obvodových stěnách.

Vnitřní stavební konstrukce

Vnitřní omítky jsou původní a v posledních letech dochází k uvolňování betonového podkladu a následnému odpadávání. V minulosti byl již řešen úraz zaměstnankyň po pádu stavebních částí v prostoru jídelny. Těchto incidentů bylo již několik a jen se štěstím se to obešlo bez poškození zdraví.

Komunikace v areálu objektu jsou rovněž v původním stavu a nesplňují již požadavky, které jsou v dnešní době kladeny na bezpečnost.

Elektrické rozvody

Budova a jednotlivá patra trpí neustálými výpadky elektřiny vlivem přetížení, a co hůř, na mnoha místech jsou hodnoty jističů posunuty o třídu výš, což představuje u dožitého hliníku velmi vysoké riziko požáru, případně úrazu elektrickým proudem. Jde o starou původní instalaci, také částečně řešenou předpisy platnými v době realizace, které se od té doby zásadně změnily. Nároky na spotřebu byly tenkrát mnohonásobně nižší. O jeden elektrický obvod v budově se dělí i tři kanceláře, navíc hodnoty jističe jsou posunuty, což nese riziko, že díky smyčkování v AYKY (kabely pro pevné uložení v zemi nebo na vzduchu s hliníkovým jádrem) může zahořet kterákoli zásuvka bez ohledu na to, zda v ní spotřebič je či ne. Z provozních důvodů jsou využívány prodlužovací přívody, které dané riziko jen umocňují. Bylo zde řešeno i několik situací, např. spečené zásuvky apod. V budově dochází navíc v chladném počasí také k pouštění elektrických přímotopů v kancelářích, které ještě víc zatěžují elektrickou síť.

Budova může mít v součtu až 250 shromažďujících se osob a tomu jsou přizpůsobeny normy 33 2000-6 ed.2 a 331500 Z4, kdy musí být i četnější prohlídky a revize.

Prostory v KNTB nemají žádné revize a v tomto stavu jsou dokonce nerevidovatelné. V prostorách KHS ZK jsou sice revize prováděny, ale je otázkou, do jaké míry jsou při tomto stavu objektivní. [45]

5.3.1 Požární řád

V rámci požární ochrany organizace na základě smlouvy spolupracuje s externí odborně způsobilou osobou v požární ochraně (dále jen PO), která provádí nejméně 1x za měsíc preventivní požární prohlídku.

Požární řád má organizace vypracovaný dle § 31 vyhlášky č. 246/2001 Sb., o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci).

Obsahuje charakteristiku požárního nebezpečí, což jsou zdroje možného zapálení, které se v objektu přímo nevyskytují (porušení zákazů, nedbalost) a zdroje zapálení v objektu vyskytující se:

- otevřený oheň (kouření v blízkosti hořlavých látek),

- elektrický zkrat (možnost hoření izolace),
- osvětlovací tělesa (zářivky při nedostatečné údržbě, odstraňování krytů),
- tepelné zařízení (vadná varná konvice, správné používání spotřebičů),
- atmosférická elektřina (uvolněný spoj zemního vedení),
- sálavé teplo (hořlavý materiál v blízkosti nebo kontaktu s vyhřívanou částí technologického zařízení).

Dále jsou v požárním řádu stanoveny podmínky požární bezpečnosti. Zaměstnanci a osoby zdržující se v objektu musí dodržovat tyto podmínky:

- kouření v objektu je zakázáno,
- dodržování výstražně bezpečnostního značení,
- přístupy k hasicím přístrojům, elektrickým rozvaděčům, vypínačům elektrického proudu a uzávěrům vody musí být vždy volné,
- nepoužívat poškozené elektrické zařízení,
- nikde neskladovat materiál, který nesouvisí s provozem,
- neprovádět práce, které mohou vést ke vzniku požáru (oprava elektrického zařízení). [46]

Další bodem v požárním řádu je vymezení oprávnění a povinností osob a stanovení podmínek pro bezpečný pobyt a pohyb osob:

- únikové cesty musí být volné, nezaskládány zařízením či materiálem, označené výstražnými bezpečnostními značkami,
- udržovat volné příjezdové komunikace k budově o minimální šířce 3 m a udržovat volné nástupní plochy pro požární techniku u objektu,
- východy z jednotlivých podlaží a východy z budovy musí být zajištěny tak, aby byly použitelné pro evakuaci (např. náhradní klíče u zamykaných dveří),
- v objektu by se měly zdržovat cizí osoby pouze v určených prostorech, s povolením organizace a za doprovodu některého ze zaměstnanců. [46]

Dalším bodem v požárním řádu je přehled rozmístění výstražných a bezpečnostních značek, viz tabulka *Tab. 2*.

Tab. 2. Přehled výstražných a bezpečnostních tabulek včetně jejich rozmístění. [Zdroj: vlastní]

Název tabulky	Umístění	Počet kusů
Zákaz kouření.	Hlavní vchod a po stranách budovy	4
Zákaz vstupu se psem (netýká se vodících a asistenčních psů).	Průchod mezi budovou a parkovištěm.	1
Úniková cesta.	1. NP	0
	Schodiště	4
	Chodby na patrech	21
Drž se zábradlí.	Schodiště	3
Výstraha – životu nebezpečno dotýkat se elektrických zařízení.	Hlavní vypínače elektrické energie - na každém patře	4
Nehas vodou ani pěnovými přístroji	Hlavní vypínače elektrické energie – na každém patře	6
Hydrant	Na chodbě každého patra	7
Hasicí přístroje	Na chodbě každého patra	10
Výměníková stanice	Uzávěr vody	1

5.3.2 Požární poplachová směrnice

Požární poplachová směrnice vymezuje činnosti zaměstnanců, popřípadě dalších osob, při vzniku požáru, viz Příloha P I: Požární poplachová směrnice.

Účinnost opatření uvedených v poplachových směrnicích se neprověřuje formou cvičného požárního poplachu, ale pouze se prověřuje správnost údajů uvedených ve směrnici např. prověření telefonních čísel a pokynů.

5.3.3 Požární evakuační řád

Požární evakuační řád upravuje postup při evakuaci osob a majetku z objektu zasaženým nebo ohroženým požárem. Zpracovává se pro objekty, ve kterých jsou složité podmínky pro zásah (§ 18 vyhlášky o požární prevenci), a takovým objektem budova KHS ZK je. Úplnost

a správnost evakuačního plánu se neprověřuje formou cvičného požárního poplachu, pouze se prověřuje správnost údajů uvedených v evakuačních plánech např. únikové cesty, shromaždiště, telefonní čísla.

5.3.4 Dokumentace zdolávání požáru

Tvoří ji operativní karty zdolávání požárů (§ 34 vyhlášky o požární prevenci) pro jednotlivá podlaží. Karty jsou uloženy u příslušné jednotky Hasičského záchranného sboru Zlínského kraje a v dokumentaci požární ochrany. Tato dokumentace se zpracovává pro objekty, ve kterých jsou složité podmínky pro zásah.

5.3.5 Požární kniha

Požární kniha je určena k záznamu preventivních požárních prohlídek, kontrol a všech důležitých skutečností, týkající se požární ochrany. V požární knize se zaznamenává, kdy a jak byly zjištěné závady odstraněny, ale i prohlídky, při nich nebyly zjištěny žádné závady. Každý záznam se opatřuje datem a podpisem kontrolujícího pracovníka požární ochrany. Kniha je uložena u pověřeného pracovníka organizace.

5.3.6 Školení zaměstnanců

Školení požární ochrany se provádí při nástupu zaměstnance do zaměstnání a při každé změně pracovního zařazení zaměstnance. Školení se opakuje 1x za 2 roky. O školení je vedena dokumentace. Znalosti získané při školení se ověřují namátkovými ústními dotazy.

5.3.7 Věcné prostředky požární ochrany

Prostory budovy jsou pro zásah při mimořádných událostí vybaveny přenosnými hasicími přístroji. Podle charakteru hořlavých látek (administrativní provoz) se mohou použít buď přístroje práškové s náplní hasební látky 6 kg hasícího prášku, nebo přístroje s náplní oxidu uhličitého pro hašení plynového zařízení.

Přenosné hasicí přístroje jsou umístěné tak, aby byly snadno viditelné a volně přístupné. Rukojeti zavěšených přístrojů jsou ve vzdálenosti maximálně 150 cm nad podlahou. Hasicí přístroje se umisťují do blízkosti míst pravděpodobného požáru, a to ke vchodům do místností nebo na únikové cesty. V objektu jsou z většiny umístěny na chodbách, ale také v některých kancelářích.

Obr. 5. Pěnový hasicí přístroj. [Zdroj: vlastní]

Tab. 3. Tabulka počtů a umístění přenosných hasicích přístrojů. [Zdroj: vlastní]

Umístění	Druh přenosného hasicího přístroje	Počet
parkoviště	Práškový - 6 kg	1
1. NP		0
2. NP	Práškový - 6 kg	2
3. NP	Práškový - 6 kg	5
	CO_2 - 5 kg	4
4. NP	Práškový - 6 kg	3
	CO_2 - 5 kg	1

5.3.8 Požárně bezpečnostní zařízení

V případě požáru je v budově zajištěna i vnější požární voda ze dvou podzemních hydrantů, které jsou ve vzdálenosti do 15 m od objektu západním směrem.

Na úrovni každého podlaží jsou v současné době vybaveny dvě hydrantové skříně. Požární úseky jsou vybaveny vnitřními hadicovými systémy staršího typu.

Na každém patře u výtahu je umístěn tlačítkový hlásič.

5.3.9 Prevence v oblasti požární ochrany

Organizace má zpracovanou požární poplachovou směrnici, ta je umístěna pouze u schodiště v 2. NP. Revize hasicích přístrojů je provádí 1x za rok. Cvičný požární poplach se neprovádí. V rámci prevence je zvolena preventivní požární hlídka, kde má každý člen hlídky stanovený úkol v rámci prevence, a také při vzniku požáru. Tyto úkoly jsou zaznamenány v tabulce *Tab. 4*.

Tab. 4. Úkoly členů preventivní požární hlídky. [Zdroj: vlastní]

Členové hlídky	Úkoly na úseku prevence	Úkoly při vzniku požáru
Velitel hlídky	Dbá, aby byl dodržován požární řád, a dohlíží, aby byly volné únikové cesty a východy.	Oznamuje vznik požáru na ohlašovnu HZS stlačením tlačítka EPS a do příjezdu jednotky řídí a organizuje evakuaci osob a majetku.
Člen hlídky č. 1	Dohlíží na volné přístupy k elektrickým rozvaděčům.	Provádí hasební zásah od hydrantu.
Člen hlídky č. 2	Dohlíží na volné přístupy k hasicím přístrojům a hydrantům.	Provádí hasební zásah s hasicími přístroji.

5.4 Bezpečnost a ochrana zdraví při práci

Pro oblast BOZP pracuje pro organizace bezpečnostní technik na dohodu konanou mimo pracovní poměr. Bezpečnostní technik 1x ročně prověřuje bezpečnost a ochranu zdraví při práci zaměstnanců v souladu s platnou legislativou a vnitřními předpisy organizace. Zaměřuje s především na:

- kontrolu aktuálnosti rizik a opatření k jejich eliminaci,
- používání osobních ochranných pracovních prostředků (dále jen OOPP),
- provádění pracovně lékařských prohlídek ve stanovených termínech – tyto prohlídky probíhají u smluvního lékaře pro pracovně-lékařskou službu,

- platnost školení BOZP a PO,
- kontrolu evidence pracovních úrazů,
- kontrolu únikových cest,
- kontrolu bezpečnostního a informačního značení,
- dodržování zákazu kouření v objektech,
- dodržování pravidel pro dodržování bezpečnostního úklidu – používání bezpečnostních kuželů při mytí chodeb a schodiště,
- kontrolu technického stavu drobných spotřebičů a osvětlovacích těles (celistvost) a vhodnost osvětlení,
- kontrolu způsobu skladování v reálech – přístupnost, nepřetěžování, stabilita a neporušenost konstrukcí,
- kontrolu stavu technicko-požárních zařízení, zejména požárních dveří, nouzového osvětlení, přenosných hasicích přístrojů a vnitřních požárních hydrantů,
- kontrolu požární dokumentace – požární poplachová směrnice, požární řády a únikové plány,
- kontrolu požadavků na technický stav pracovišť, pracovního prostředí a dopravní prostředky.

5.4.1 Školení BOZP

V rámci školení zajišťuje bezpečnostní technik následující úkony:

- vstupní školení a instruktáž – provádí se před nástupem do služebního úřadu,
- periodické školení BOZP – u zaměstnanců se provádí 1x za 2 roky, u vedoucích pracovníků 1x za 3 roky,
- mimořádné školení – provádí se po pracovním úrazu, hrubém porušení pracovní kázně, technické havárii a pro osoby, které provádí v organizaci smluvní činnosti,
- speciálně odborná školení – provádí se dle požadavků zvláštních předpisů, školení první pomoci 1x za 3 roky, školení řidičů referentů 1x za 2 roky,
- kontroluje vybavení lékárniček,

- v rámci případných změn bezpečnostních podmínek v organizaci vytvoří bezpečnostní opatření.

V organizaci je vydán služební předpis organizování a provádění školení bezpečnosti a ochrany zdraví při výkonu služby. Zde jsou podrobně popsány povinnosti osob pověřených organizovat a provádět školení, instruktáže bezpečnosti a ochrany zdraví při výkonu služby a zácvik u nového nástupu do zaměstnání. O školení je povinnost vést písemné záznamy a také je povinné ověřování znalostí po ukončení školení a to:

- vstupní školení – formou písemného přezkoušení,
- periodické zkoušení zaměstnanců a představených – forma ústního přezkoušení,
- mimořádné školení – ústní přezkoušení,
- speciální školení – dle zvláštních předpisů.

Osnova k periodickému školení pro představené státní zaměstnance je zpracována vždy aktuálně před provedením školení. Osnova ke vstupnímu školení je vždy shodná s posledním provedeným periodickým školením pro státní zaměstnance.

5.4.2 Osobní ochranné pracovní prostředky

Na základě vyhodnocení rizik spojených s výkonem určitých činností organizace přiděluje vhodné OOPP, a to při nástupu do zaměstnání nebo změně pracovní činnosti. Každý zaměstnanec, který má přiděleny OOPP, má osobní kartu, kde písemně potvrdí jejich převzetí a seznámení se způsobem používání. Při snížení ochranné funkce OOPP organizace zajistí výměnu.

V případě řidičů referentů nemá každý řidič přidělenu vlastní výstražnou vestu. Vedoucí pracovník pravidelně kontroluje a zajišťuje umístění výstražných vest s vysokou viditelností v každém osobním automobilu.

Praní OOPP (např. bílé pláště, kalhoty bílé, košile bílé) zajišťuje pro organizaci smluvní firma, jejíž služby má možnost využít každý zaměstnanec.

Druhy poskytovaných OOPP:

- plášť bílý,
- ochranná obuv do terénu,
- ochranná obuv nepromokavá – holínka gumové,

- termoponožky,
- záchranná vesta plovací,
- kalhoty bílé,
- košile bílá,
- ochranná obuv lehká zdravotní s protiskluzovou podešví,
- rouška zdravotní obličejová,
- rukavice zdravotní jednorázové,
- obličejový štít.

5.5 Informační bezpečnost

Kybernetická bezpečnost a bezpečnost informací patří mezi nejrizikovějších oblasti ochrany organizace. Hlavním úkolem je ochránit data a informace ať už před úmyslným poškozením či zneužitím, tak i před neúmyslnou ztrátou.

5.5.1 Informační systém

V informačním systému této organizace je v převážné většině využíváno notebooků, stolní počítače používá jen několik málo zaměstnanců. Přes počítačovou síť jsou všichni připojeni na internet. Je zde zřízeno IT oddělení, kde pracují dva zaměstnanci. Ti se v případě problémů prostřednictvím vzdáleného přístupu pomocí TeamVieweru připojí ze své kanceláře na kterýkoliv počítač a problém odstraní.

Hlavní úkoly pracovníků IT oddělení:

- zřizování práv a přístupů do jednotlivých počítačů i IS,
- monitorovat dění ve vlastní síti a informačních systémech, umět vyhodnotit bezpečnostní útoky,
- pomoc při nakupování IT techniky,
- kontrola obměn hesel,
- provádění zálohování dat,
- zajišťování potřebných aktualizací,
- úprava IS dle potřeb organizace.

Hlavní servery se nachází v samostatné kanceláři, kde je vstup povolen pouze pracovníkům IT. Místnost je vybavena klimatizací, kde je teplota nastavena na 18 °C. Místnost není vybavena požárními hlásiči ani hlásiči reagující na změnu teploty v případě poruchy klimatizace. Servery jsou kvůli nenadálému výpadku elektrické energie napojeny na záložní UPS. V loňském roce organizace nakoupila multifunkční tiskárny, které jsou umístěny na chodbách. Každý rok se také nakupuje několik počítačů, jimiž se nahrazuje již zastaralá IT technika.

SW výbava počítačů:

- Windows 7 a 10,
- Microsoft Office 2010, 2013, 2016, Office 365,
- Internet Explorer,
- Pošta MS Outlook 2010, 2013, 2016,
- Adobe Reader,
- TeamViewer,
- CTI klient,
- ESET antivir,
- Codexis,
- IS spisové služby,
- agendové IS,
- ekonomický IS.

Také všichni zaměstnanci by měli v rámci kybernetické bezpečnosti dodržovat pravidla pro užívání výpočetní techniky. Zde např. patří:

- u firemních e-mailů – používat pouze pro firemní účely a nepřihlašovat se na e-mail z nechráněných zařízení,
- zákaz přístupu na stránky se škodlivým obsahem,
- mobilní zařízení – vstup chráněn heslem, nastavení automatického zamykání po stanovené době nečinnosti,

- chránit data uložená v paměťových médiích koncových stanic před neoprávněným přístupem,
- zamezit fyzickému přístupu ke koncové stanici neoprávněným osobám,
- při krátkodobém opuštění pracoviště uzamknout koncovou stanici,
- při dlouhodobém opuštění pracoviště ukončit veškerý spuštěný software, uložit rozpracované dokumenty a koncovou stanici vypnout,
- zákaz aktivně vytvářet nebo šířit škodlivý software,
- v případě poruchy, nefunkčnosti softwarového a hardwarového vybavení, podezření na nakažení svého počítače virem apod. neprodleně informovat odpovědné pracovníky.

5.5.2 Ochrana osobních údajů

Organizace vykonává činnosti, při nichž dochází ke zpracování osobních údajů, nejen v přímé souvislosti s výkonem své odborné působnosti, ale rovněž např. z pozice zaměstnavatele nebo účastníka smlouvy.

V organizaci jsou identifikována společná aktiva, která zpracovávají osobní údaje. K jednotlivým aktivům bylo přiřazeno označení, zda se jedná o listinné nebo elektronické úložiště osobních údajů (Elektronické úložiště - "E", Listinné úložiště - "L"). Tímto vznikl následující seznam identifikovaných aktiv:

- listinné úložiště v rámci výkonu agend úřadu (L) – veškeré listiny, které jsou uloženy na úřadě a souvisí s výkonem agend úřadu,
- listinné úložiště v rámci vnitřního chodu úřadu (L) – veškeré listiny, které jsou uloženy na úřadě a souvisejí s vnitřním chodem úřadu (zaměstnanci, účetnictví atd.),
- informační systém spisové služby (E),
- agendové informační systémy – samostatná působnost (E),
- agendové informační systémy – přenesená působnost (E),
- ekonomický informační systém (E),
- portály – veřejné i neveřejné webové portály (E),
- ostatní elektronická úložiště (E) – e-mail, sdílené disky, lokální disky na počítačových sestavách.

Ke každému aktivu má organizace vytvořenou tabulku hodnocení pravděpodobnosti uplatnění hrozeb na jednotlivá aktiva.
Jedná se o následující hrozby:

- vnější útoky,
- technické chyby,
- lidský faktor,
- narušení integrity osobních údajů,
- neoprávněné přístupy,
- narušení dostupnosti,
- ztráta osobních údajů,
- narušení práv a svobod subjektu údajů.

Organizace nedisponuje pokročilou technologií na zabezpečení listinných úložišť, jakými jsou bezpečnostní dveře, bezpečnostní zámky, kamerové systémy, docházkové systémy pro sledování přístupů do budov a místností s listinnými úložišti. Listinná úložiště jsou umístěna v uzamykatelných místnostech, kdy zámky a dřevěné dveře nepředstavují zásadní překážku pro násilné vniknutí. Dokumenty jsou uloženy ve skříních, které buď nejsou uzamykatelné, nebo zámky na skříních jsou lehce překonatelné.

Dále organizace disponuje elektronickými úložišti, která jsou umístěna na počítačových sestavách zaměstnanců úřadu a zejména ve sdílených adresářích s nastavenými právy pro jednotlivé pracovní pozice v datovém centru. Počítače disponují základní ochranou před vnějšími útoky. Zálohy jsou prováděny na diskové pole, které je uloženo v uzamykatelné místnosti v budově úřadu. Organizace disponuje datovými úložišti pro sdílení dat a tento systém je umístěn v budově úřadu a napojen na interní síť, která je propojena od veřejné sítě. Ethernetové vstupy, které jsou umístěny u tiskáren stojících na chodbách, nejsou nijak chráněny.

Povinností organizace je zabezpečit zpracování osobních údajů vhodným technickým a organizačním opatřením k zajištění zabezpečení příslušnému danému riziku.

Při zajišťování bezpečnosti osobních údajů by se měla každá organizace zaměřit na několik základních oblastí bezpečnosti a to:

- v oblasti fyzické bezpečnosti – zabezpečení přístupu do prostor, kde je možnost dostat se k datům, resp. k osobním údajům,

- v oblasti autorizace a autentizace – každý uživatel má mít přístup pouze k těm datům, které potřebuje pro výkon své profese, co se týká autentizace, zde je podstatná strategie v užívání hesel,
- v oblasti ochrany proti kybernetickým útokům a jejich detekce – zajištění ochrany pomocí kvalitních a stále aktualizovaných bezpečnostních nástrojů,
- v oblasti systému řízení informační bezpečnosti – jedná se o organizační opatření, které tvoří systém politik (např. politika ochrany bezpečnostního perimetru, politika hesel). [47]

5.6 Dílčí závěr

V této kapitole jsou popsány základní informace o objektu, objektová bezpečnost, požární ochrana, bezpečnost a ochrana zdraví při práci a informační bezpečnost.

6 BEZPEČNOSNÍ AUDIT

Při provádění auditu je třeba se držet několika kroků. V první řadě je nutné vymezit oblasti auditu, ve kterých se prověřuje požadovaný i reálný stav. Dalším krokem je analýza rizik a následně vyhodnocení rizik. Pro tento bezpečnostní audit je použita metoda kontrolního seznamu k identifikaci hrozeb a metoda PNH k celkovému vyhodnocení rizik. Posledním krokem jsou návrhy opatření vedoucí k minimalizaci či úplnému odstranění rizik.

Cílem je provedení bezpečnostního auditu objektu státní správy.

Byl zvolen následující postup:

- fyzická prohlídka objektu a popis objektu,
- analýza současného stavu,
- analýza dokumentace a interních dokumentů,
- analýza rizik,
- stanovení závěru auditu,
- na základě zjištěných výsledků navrhnout opatření, která budou bezpečnostní rizika minimalizovat.

6.1 Vymezení oblastí auditu

Bezpečnostní audit je orientován na posouzení celkové bezpečnosti objektu. Aby byl výsledek auditu objektivní, je nezbytné se zaměřit i na zabezpečení areálu, ve kterém se objekt nachází.

Bezpečnostní audit byl proveden v následujících oblastech:

Obvodová bezpečnost – popsáno zabezpečení perimetru a možnosti vstupů osob z areálu do objektu.

Režimová opatření – vjezdy a výjezdy automobilů do areálu, ve kterém se objekt nachází.

Fyzická ostraha areálu – činnosti vykonávané fyzickou ostrahou.

Technická ochrana areálu – vjezdy a výjezdy zabezpečené pomocí mechanických závor.

Objektová bezpečnost – popsán současný stav zabezpečení samotného objektu – dveře, okna.

Požární ochrana – únikové cesty, dělení do požárních úseků, popsána stavební konstrukce, stav elektrických rozvodů, dostupné dokumenty k této problematice, věcné prostředky požární ochrany, požárně bezpečnostní zřízení, prevence.

Bezpečnost a ochrana zdraví při práci – zaměření, školení pracovníků, poskytování OOPP.

Informační bezpečnost – informační systém, ochrana osobních údajů.

Popis současného stavu jednotlivých auditovaných oblastí byl proveden v předešlých kapitolách diplomové práce a to následovně – viz tabulka *Tab. 5*.

Tab. 5. Přehled kapitol o provedení analýz auditovaných oblastí. Zdroj: vlastní]

Auditovaná oblast	Číslo kapitoly
Obvodová bezpečnost areálu	4
Režimová opatření	4
Fyzická ostraha	4
Technická ochrana areálu	4
Objektová bezpečnost	5
Požární ochrana	5
BOZP	5
Informační bezpečnost	5

Během auditu byly prověřeny dokumenty a interní směrnice uvedené v tabulce *Tab. 6*.

Tab. 6. Seznam prověřených dokumentů a interních směrnic. [Zdroj: vlastní]

Auditovaná oblast bezpečnosti	Název dokumentu nebo interní směrnice
Požární ochrana	Směrnice pro stanovení organizace zabezpečení PO
Požární ochrana	Požární řád
Požární ochrana	Požární evakuační řád

Požární ochrana	Požární kniha
Požární ochrana	Dokumentace zdolávání požárů
Požární ochrana	Zápis o kontrole hasicích přístrojů
Požární ochrana	Záznam o školení zaměstnanců v PO
Požární ochrana	Požární poplachová směrnice
Požární ochrana	Protokol o provedení prověrek PO
Požární ochrana	Stanovení podmínek k zabezpečení PO a podmínek pro hašení požárů a pro záchranné akce v objektu
BOZP	Služební předpis organizování a provádění školení bezpečnosti a ochrany zdraví při výkonu služby
BOZP	Služební předpis poskytování pracovně-lékařské služby
BOZP	Přidělování OOPP
BOZP	Protokol o provedení prověrek BOZP
BOZP	Zpráva o revizi elektrických zařízení
BOZP	Záznam o školení zaměstnanců BOZP
BOZP	Záznam o školení řidičů referentů
Informační bezpečnost	Bezpečnostní směrnice pro uživatele informačních systémů

6.2 Vyhodnocení analyzovaných oblastí

V jednotlivých posuzovaných oblastech byly vyhodnoceny silné a slabé stránky. Tyto informace vycházejí z fyzické prohlídky objektu a areálu.

6.2.1 Obvodová bezpečnost areálu

Silné stránky: U obvodové bezpečnosti areálu nebyly zjištěny žádné silné stránky zabezpečení.

Slabé stránky: Objekt není po celém svém obvodu oplocen a ani do budoucna, díky jeho poloze, toto nebude možné.

6.2.2 Režimové opatření

Silné stránky: Kontrola automobilů do areálu probíhá pouze u hlavní brány, kde je umístěna vrátnice.

Slabé stránky: U ostatních vjezdů do areálu kontroly neprobíhají.

6.2.3 Fyzická ostraha

Silné stránky: Po uzavření objektu probíhá pochůzková kontrola celé budovy. V případě výtržnictví či napadení je možné fyzickou ostrahu zavolat.

Slabé stránky: Během pracovní doby kontrolní pochůzky neprobíhají, fyzická ostraha nemá v objektu své zázemí.

6.2.4 Technická ochrana areálu

Silné stránky: Všechny vjezdy do areálu disponují automatickými závorami.

Slabé stránky: Zaměstnanci nemocnice otevírají závory na dálku na zazvonění bez jakékoliv kontroly.

6.2.5 Objektová bezpečnost

Silné stránky: V 1. NP jsou okna zabezpečena mřížemi, rovněž hlavní vchodové dveře. Během dvou let je plánovaná výměna oken a dveří.

Slabé stránky: Dvoje zadní dveře jsou bez mříží, také okna v 2. NP, která směřují na parkoviště, nedisponují mřížemi, je tu možnost snadného vniknutí z druhého patra parkoviště.

6.2.6 Požární ochrana

Silné stránky: V této oblasti je velmi dobře zpracována dokumentace. Zaměstnanci jsou pravidelně školeni. Počet přenosných hasicích přístrojů je v části objektu patřící státní správě dodržen.

Slabé stránky: V objektu je pouze jedno únikové schodiště, ani jeden z výtahů není evakuační. Elektrické rozvody jsou v původním stavu, což při přetížení může mít vliv na vznik požáru. Požární poplachová směrnice není vyvěšena na chodbách u kanceláří a v 3.

a 4. NP u únikového schodiště. Značení únikových cest tabulkami je nedostatečné, tabulky jsou umístěny pouze na bočních stěnách chodeb. Vstupy v patrech od schodiště nejsou opatřeny požárními dveřmi. Chodba u bufetu je osazena stoly a tím je zúžená úniková cesta. V 3. NP je na chodbě multifunkční tiskárna, která taktéž velmi zužuje únikovou cestu.

6.2.7 BOZP

Silné stránky: Všechny druhy školení pracovníků probíhají v pravidelných, předem stanovených termínech. OOPP jsou přidělovány v pravidelných intervalech. Systém BOZP je velmi dobře zpracovaný. Značení a tabulky vztahující se k BOZP jsou dostačující.

Slabé stránky: Nášlapné plochy u schodů jsou v PVC, které se na některých místech odlepují. Tím vzniká riziko zakopnutí a následného úrazu. Při mytí chodeb a schodů se velmi málo využívají výstražné kužely a přenosné značky upozorňující na riziko uklouznutí.

6.2.8 Informační bezpečnost

Silné stránky: Dodržování hesel se silnou ochranou, tak jak stanoví kybernetická bezpečnost. Počítačová síť je vedena přes jednotlivé kanceláře, ne přes veřejné chodby, takže není možnost přístupu k počítačové síti zvenčí. Ověřování tisku se provádí ID kartou.

Slabé stránky: V serverovně chybí požární hlásiče a hlásiče změny teploty. Někteří zaměstnanci nezamykají během pracovní doby při odchodu své kanceláře dveře, vzniká tak možnost krádeže dokumentů v listinné podobě, které mohou obsahovat osobní údaje, a také krádeže osobních věcí.

6.3 Analýza rizik

Po analýze současného stavu je důležité provést analýzu rizik, a to vyhodnocením aktiv. V organizaci je nutné ochraňovat následující klíčová aktiva:

- fyzické osoby,
- hmotný majetek – IT technika, vybavení kanceláří, osobní věci zaměstnanců,
- nehmotný majetek – data a informace o objektu uložené na nosičích dat, software, výstupy ze software, data osobní povahy např. lékařské zprávy.

6.3.1 Kontrolní seznam

Metoda Kontrolní seznam umožňuje identifikovat bezpečnostní hrozby pomocí vytvořených otázek – viz tabulka *Tab. 7*.

Tab. 7. Kontrolní seznam. [Zdroj: vlastní]

	ANO	NE
1. Obvodová ochrana areálu		
Je zajištěno oplocení okolí budovy?		X
Je zajištěn trvalý monitoring vstupu do areálu?		X
Je zřízen režim pro kontrolu vstupu osob, vozidel do areálu?		X
Funguje bezpečnostní služba v rámci areálu nepřetržitě?	X	
Je areál, parkoviště a samotný objekt snímám kamerami?		X
2. Objektová ochrana objektu		
Jsou všechny vchodové dveře do objektu v dobrém technickém stavu?		X
Jsou okna, kterými by se dalo vniknout do objektu zamřížována?		X
Je objekt zabezpečen proti vstupu nepovolených osob mimo pracovní dobu?	X	
Je objekt zabezpečen proti vstupu nepovolených osob v pracovní dobu?		X
Je prostor budovy monitorován?		X
3. Režimová opatření		
Jsou všechny automobily vjíždějící do areálu monitorována?		X
Jsou vydávána povolení ke vstupu/vjezdu do areálu?		X
4. Fyzická ostraha		
Probíhají kontroly fyzické ostrahy během pracovní doby?		X
Probíhá kontrola fyzické ostrahy po uzavření objetu?	X	
5. Technická ochrana areálu		

Při otevírání závor na dálku probíhá kontrola např. pomocí nahlášení hesla?		X
Je areál monitorován kamerami?		X
6. Požární ochrana		
Jsou zpracovány požadované dokumenty k této oblasti?	X	
Jsou pravidelně prováděny revizní zkoušky u elektrotechnických zařízení?	X	
Provádějí se pravidelné školení k požární ochraně?	X	
Dochází k pravidelné revizi hasicích přístrojů?	X	
Je objekt napojen na agregát pro případ nefunkčnost elektrické sítě?	X	
Jsou všechny cesty a prostory únikových cest trvale průchodné?		X
Je značení únikových cest tabulkami dostatečné?		X
7. BOZP		
Jsou zpracovány požadované dokumenty k této oblasti?	X	
Provádějí se pravidelné školení k BOZP?	X	
Používají určení zaměstnanci při práci vhodné OOPP?	X	
Je vedena evidence OOPP?	X	
Stal se za posledních 5 let pracovní úraz na pracovišti?	X	
Jsou nášlapné plochy schodů zajištěny proti uklouznutí či zakopnutí?		X
Absolvují noví zaměstnanci vstupní prohlídku u smluvního lékaře?	X	
8. Informační bezpečnost		
Je zpracována interní směrnice pro oblast informační bezpečnosti?	X	
Jsou všechny informační systémy chráněny proti virům?	X	
Jsou všechny počítače chráněny heslem proti zneužití?	X	
Používají zaměstnanci notebook při práci mimo objekt?	X	

Jsou dokumenty v listinné podobě, obsahující osobní údaje, řádně zabezpečeny?		X
Jsou všichni zaměstnanci školeni v oblasti informační bezpečnosti?		X
Zamykají všichni zaměstnanci v pracovní době při odchodu kanceláře dveře?		X
Udála se za poslední 3 roky v organizaci krádež?	X	

Pomocí metody Kontrolní seznam byly identifikovány následující hrozby:

- volný přístup do areálu i objektu nežádoucí osobou,
- nepřehlednost o pohybu vozidel v areálu,
- překonání vstupu do budovy,
- možnost vniknutí do objektu okny,
- krádež osobních věcí i majetku organizace,
- nedodržení volného průchodu únikových cest,
- zranění při opouštění objektu v případě požáru,
- možnost chaotického chování cizích osob při opuštění objektu při vyhlášení požáru díky nedostačujícímu značení,
- vandalismus,
- možnost fyzického napadení zaměstnanců osobami zvenčí,
- možnost pracovního úrazu,
- možnost ztráty nebo krádeže notebooků,
- nedostatečná informovanost zaměstnanců v oblasti informační bezpečnosti,
- možnost nekontrolovaného vstupu cizích osob do kanceláří během pracovní doby,
- únik informací a dat.

Pomocí metody Kontrolní seznam bylo identifikováno 15 možných hrozeb.

6.3.2 Polokvantitativní metoda PNH

Pro posouzení a ohodnocen rizik byla vybrána metoda PNH. Pomocí této metody se vyhodnocuje příslušné riziko ve třech jeho složkách, a to s ohledem na:

- pravděpodobnost vzniku hrozby – P
- závažnost následků – N
- názor hodnotitelů – H

U všech kritérií bylo zvoleno vzestupné číselné hodnocení 1–5, jak je vidět v následujících tabulkách *Tab. 8 Tab. 9 Tab. 10*.

Tab. 8. Stupnice pravděpodobnosti vzniku hrozby. [Zdroj: vlastní]

Pravděpodobnost vzniku hrozby	Číselné hodnocení
Opomenutelné	1
Nepravděpodobná	2
Pravděpodobná	3
Velmi pravděpodobná	4
Téměř jistá	5

Tab. 9. Stupnice závažnosti následků. [Zdroj: vlastní]

Závažnost následků	Číselné hodnocení
Bez následků	1
Mírný dopad	2
Významný dopad	3
Velmi významný dopad	4
Katastrofický dopad	5

Tab. 10. Názor hodnotitelů. [Zdroj: vlastní]

Názor hodnotitelů	Číselné hodnocení
Zanedbatelný vliv	1
Mírný vliv	2
Větší, nezanedbatelný vliv	3
Velký a významný vliv	4
Kritický vliv	5

Součinem jednotlivých činitelů se získá celkové hodnocení rizika. Míra rizika se určuje podle následujícího vzorce:

R = P x N x H

„R“ určuje míru rizika, podle které se určí, zda je nutné navrhnout protiopatření, viz tabulka *Tab. 11*.

Tab. 11. Míra rizika. [Zdroj: vlastní]

Rizikový stupeň	Míra rizika ohodnocená slovně	R
I.	Nepřijatelné	≥ 50
II.	Nežádoucí	31-50
III.	Mírné	21-30
IV.	Akceptovatelné	11-20
V.	Bezvýznamné	≤ 10

Po stanovení číselného hodnocení u popsaných kritérií byly hrozby, které byly identifikovány dle metody Kontrolní seznam, zpracovány do tabulky a následně bylo provedeno hodnocení. Ke každé hrozbě byl připsán rizikový stupeň, viz tabulka *Tab. 12*.

Tab. 12. Metoda PNH. [Zdroj: vlastní]

Hrozba	P	N	H	R	Rizikový stupeň
Volný přístup nežádoucích osob do areálu i do objektu	2	3	3	18	IV.
Nepřehlednost o pohybu vozidel v areálu	2	3	3	18	IV.
Překonání vstupu do budovy	3	2	2	12	IV.
Možnost vniknutí osob do objektu okny	3	4	4	48	II.
Krádež osobních věcí i majetku organizace	3	4	4	48	II.
Nedodržení volného průchodu únikových cest	3	3	3	27	III.
Zranění osob při opouštění objektu v případě požáru	3	3	3	27	III.
Možnost chaotického chování cizích osob při opouštění objektu po vyhlášení požáru díky nedostačujícímu značení	3	4	4	48	II.
Vandalismus	2	2	2	8	IV.
Možnost fyzického napadení zaměstnanců osobami zvenčí	3	3	3	27	III.
Možnost pracovního úrazu	1	4	4	16	IV.
Možnost ztráty nebo krádeže notebooků	2	4	5	40	II.
Nedostatečná informovanost zaměstnanců v oblasti informační bezpečnosti	2	4	4	32	II.
Možnost nekontrolovaného vstupu cizích osob do kanceláří během pracovní doby	2	4	3	24	III.
Únik informací a dat	2	4	5	40	II.

Po provedení hodnocení pomocí metody PNH vzešly z tabulky *Tab. 12* následující výsledky:

Rizikový stupeň I. – 0 hrozeb

Rizikový stupeň II. – 6 hrozeb

- krádež osobních věcí i majetku organizace,
- možnost chaotického chování cizích osob při opouštění objektu po vyhlášení požáru díky nedostačujícímu značení,
- možnost vniknutí osob do objektu okny,
- možnost ztráty nebo krádeže notebooků,
- nedostatečná informovanost zaměstnanců v oblasti informační bezpečnosti,
- únik informací a dat.

Rizikový stupeň III. – 4 hrozby

- nedodržení volného průchodu únikových cest,
- možnost vzniku zranění osob při opouštění objektu v případě požáru,
- možnost fyzického napadení zaměstnanců osobami zvenčí,
- možnost nekontrolovaného vstupu cizích osob do kanceláří během pracovní doby.

Rizikový stupeň IV. – 5 hrozeb

- volný přístup nežádoucích osob do areálu i do objektu,
- nepřehlednost o pohybu vozidel v areálu,
- vandalismus,
- možnost vzniku pracovního úrazu,
- překonání vstupu do budovy.

Rizikový stupeň V. – 0 hrozeb

6.4 Dílčí závěr

V této kapitole byl zvolen postup bezpečnostního auditu. Byly vymezeny oblasti, kterých se bude audit týkat a v každé oblasti vyhodnoceny silné a slabé stránky. V další části kapitoly je popsána analýza rizik. Pomocí metody Kontrolní seznam byly vyhodnoceny hrozby. Pro posouzení a ohodnocení rizik byla vybrána metoda PNH, díky níž byl u každé hrozby určen rizikový stupeň.

7 ZÁVĚR AUDITU

V rámci prováděného auditu byl hodnocen systém bezpečnosti, který je v organizaci nastaven v současné době. Organizaci byla poskytnuta dostupná dokumentace k prostudování. K možnosti jmenování názvu organizace v diplomové práci byl udělen ústní souhlas.

Bezpečnostní audit se týkal následujících oblastí:

- obvodová bezpečnost areálu,
- objektová ochrana objektu,
- režimová opatření,
- fyzická ostraha,
- technická ochrana areálu,
- požární ochrana,
- BOZP,
- informační bezpečnost.

V každé oblasti prováděného auditu byly zjištěny větší či menší nedostatky.

Celkové vyhodnocení auditu nastaveného bezpečnostního systému: **vyhovuje s výhradou**.

Pro hodnocení rizik bezpečnostního auditu byla zvolena metoda analýzy Kontrolního seznamu a metoda PNH. Výsledkem je vyhodnocení rizik a jejich zařazení do kategorií. Byla zjištěna rizika v rizikových stupních II., III. a IV. Do kategorie I. a V. nespadá žádné z rizik. Hodnocení míry rizika (R) je popsáno v tabulce *Tab. 13*.

Tab. 13. Hodnocení míry rizika (R). [48]

Kategorie rizika	Doporučení
II.	Nežádoucí riziko, vyžaduje urychlené provedení bezpečnostních opatření snižující riziko na přijatelnou úroveň
III.	Mírné riziko, bezpečnostní opatření provedeno ve stanoveném časovém období

IV.	Akceptovatelné riziko, přijatelné se souhlasem vedení organizace, ke snížení těchto rizik převážně stačí zavedení vhodných organizačních opatření

7.1 Shrnutí a doporučení pro odbor státní správy

Na základě provedené analýzy byly navrženy konkrétní bezpečnostní opaření, Po jejich přijetí organizací by se rizika měla minimalizovat na přijatelnou úroveň. Navržená opatření jsou popsána v tabulce *Tab. 14*.

Tab. 14. Navržená opatření. [Zdroj: vlastní]

Číslo	Kategorie rizika	Hrozba
1	IV. stupeň	Volný přístup nežádoucích osob do areálu i objektu
2	IV. stupeň	Nepřehlednost o pohybu vozidel v areálu
3	IV. stupeň	Překonání vstupu do budovy
4	II. stupeň	Možnost vniknutí do objektu okny
5	II. stupeň	Krádež osobních věcí i majetku organizace
6	III. stupeň	Nedodržení volného průchodu únikových cest
7	III. stupeň	Zranění osob při opouštění objektu v případě požáru
8	II. stupeň	Možnost chaotického chování cizích osob při opouštění objektu po vyhlášení požáru díky nedostačujícímu značení
9	IV. stupeň	Vandalismus
10	III. stupeň	Možnost fyzického napadení zaměstnanců osobami zvenčí
11	IV. stupeň	Možnost pracovního úrazu
12	II. stupeň	Možnost ztráty nebo krádeže notebooků
13	II. stupeň	Nedostatečná informovanost zaměstnanců v oblasti informační bezpečnosti

14	III. stupeň	Možnost nekontrolovaného vstupu cizích osob do kanceláří během pracovní doby
15	II. stupeň	Únik informací a dat

Organizaci doporučuji povést následující opatření, aby se zjištěné nedostatky, které byly zjištěny během auditu, co nejvíce minimalizovaly. Podrobnější popis opatření je číslován dle číslování v tabulce *Tab. 14*.

1. Bohužel areál nejde zabezpečit proti volnému vstupu nežádoucími osobami z důvodu velkého pohybu osob – pacientů. V objektu je možno provést některé z následujících opatření. Jako první je možnost do vstupní haly umístit recepci, kde by se každá návštěva nahlásila, a recepční by upozornil dotyčného zaměstnance na návštěvu nebo by si pro ni přišel do recepce. Další možností je umístění kamerového systému, čímž by byl monitorován pohyb osob v budově a zároveň navrhuji uzamknutí vstupů do budovy po pracovní době.
2. Navrhuji okamžitý zákaz vjezdu cizích vozidel do areálu, které probíhá otevřením závor na dálku osobou pověřenou, a současně příkaz vjezdu pouze okolo vrátnice, kde má své stanoviště fyzická ostraha. Každý vjezd i výjezd zapsat a provést kontrolu.
3. Výměna dvou nevyhovujících vstupních dveří, kdy jedny jsou se skleněnou výplní a druhé celodřevěné. Navrhuji bezpečnostní dveře, které by znemožnily násilný vstup nežádoucím osobám vstup do objektu.
4. U oken v 2. NP na východní straně budovy, jež jsou v úrovni 2. patra dvoupodlažního parkoviště ve vzdálenosti cca 2 metry, navrhuji instalaci bezpečnostních mříží. V horizontu cca 3 let je plánována výměna všech oken v budově. Pokud se výměna uskuteční, navrhuji tato okna vyměnit za bezpečnostní okna 4. třídy – nejvyšší odolnost. Tyto jsou vyrobeny z odolné konstrukce, jsou opatřeny vhodným uzamykáním a jsou osazeny bezpečnostními skly.
5. Přístupy na každé patro jsou umožněny dvěmi vstupními dveřmi. Nikde není určeno v kolik hodin a kdo dveře pravidelně uzamkne. Protože již několikrát došlo ke krádeži jak osobních věcí zaměstnanců, tak i majetku organizace, navrhuji celodenního uzamknutí vstupních dveří na patra. Dále instalaci telefonu, který by byl

napojen např. na podatelnu. Návštěva by uvedla jméno zaměstnance, kterého by pracovnice podatelny informovaly, a ten by si dotyčného přišel vyzvednout. Další opatřením proti krádeži je při každém odchodu z kanceláře zamykat dveře a nenechávat je bez dozoru odemknuté.

6. Na chodbě u bufetu, která vede ke dvěma zadním vstupům do objektu, je několik stolků se židličkami pro zákazníky bufetu, čímž je úniková cesta velmi zúžená. Tento nábytek nejde vidět, neboť chodba směřuje do pravého úhlu a při případném úniku osob je 100 % pravděpodobnost nárazu do tohoto nábytku. Užívání tohoto prostoru je za účelem chodby, ne za účelem posezení. Navrhuji okamžité odstranění tohoto nábytku. Ve 3. NP je na chodbě umístěna multifunkční tiskárna, čímž je opět zúžená úniková cesta. Navrhuji umístění do samostatné místnosti, tak jako jsou umístěny další tiskárny na patrech. Dále bych k problematice únikových cest navrhla umístění tabulek o volném průchodu a pravidelnou kontrolu těchto cest.
7. Jelikož schodiště slouží jako jediná úniková cesta, doporučuji výměnu povrchu schodiště. V současné době je povrch z PVC, hrany schodů se odlepují a tím vzniká možnost zakopnutí a úrazu. Dále navrhuji jeden z výtahů vyčlenit jako evakuační. Bude nutné ho napojit na náhradní zdroj energie a zajistit větrání šachty. Oba výtahy opatřit dveřmi s požární odolností. Další nutností je výměna všech dveří vedoucí na patra za dveře požární.
8. Doporučuji novou instalaci bezpečnostních značek „únikový východ“. V současné době jsou značky umístěny pouze na bočních stranách chodeb, což je nedostačující. Navrhuji značky umístit na stropy chodeb pro lepší orientaci při úniku. V současné době se běžně stává, že jsou zaměstnanci pohybující se po chodbě dotazování osobami zvenčí na východ z patra.
9. Navrhuji instalaci kamerového systému, jehož záznamy by bylo možné prohlížet i zpětně. Kamery by měly být umístěné u všech vchodů do budovy a ve vstupní hale, kde je umístěn automat na kávu a docházkový systém. Je předpoklad, že by kamery mohly mít i psychologický efekt, a to na odrazení potencionálních vandalů.
10. Navrhuji snímání prostoru na každém patře u vchodů do pater. Opět je tu eventualita psychologického efektu. Další možností opatření je uzamykání vchodů na patra, jak již bylo popsáno v bodě 5.

11. Při mytí chodeb a schodiště doporučuji ve větší míře používat přenosné značky „možnost uklouznutí“ a bezpečností kužely. Na schody nalepit protiskluzné pásky, jelikož se již v minulosti úraz na schodech stal. Dále doporučení přidržovat se při chůzi na schodech zábradlí. Další možností vzniku pracovního úrazu je při provádění kontrol odborných pracovníků v terénu. Nutností je používání OOPP.
12. Neodmyslitelnou součástí při provádění kontrol odborných pracovníků je používání notebooků a přenosných tiskáren mimo pracoviště. Doporučuji tato IT zařízení nenechávat v žádném případě bez dozoru, a to jak z důvodu krádeže, tak i z důvodu úniku dat z počítače. Při každém výjezdu je povinnost vozidlo dotankovat palivem. Navrhuji doporučit těmto zaměstnancům při tankování a placení paliva mít vozidlo vždy uzamčené.
13. Navrhuji pravidelné školení všech zaměstnanců v oblasti informační bezpečnosti. Každý zaměstnanec by měl mít přinejmenším základní znalosti v oblasti kyberbezpečnosti. E-mail je nejčastějším nástrojem využívaný hackery pro napadení firem. Navrhuji při školení fyzicky ukázat, jak takový falešný e-mail obsahující útok vypadá a jak se správně zachovat při jeho obdržení. Dále zákaz používání soukromých e-mailů, případně centrálně zablokovat.
14. Jelikož se v celém objektu pohybuje větší počet lidí, kteří přicházejí jak do KHS, tak i KNTB, vzniká možnost jejich nekontrolovaného vstupu do kanceláří. Často se stává, že po chodbách chodí lidé zvenčí, kteří někoho hledají. Doporučuji při každém odchodu z kanceláří zamykat dveře, a dále ve vstupní hale umístit podrobnou informační tabuli s popisy kdo se kde na každém patře nachází.
15. Navrhuji vytvoření směrnice, která by informovala zaměstnance, jak se chovat, aby nedocházelo k úniku informací a citlivých dat. Je nutné, aby zaměstnanci pravidelně měnili hesla v počítačích, při posílání dokumentů, které obsahují citlivé informace, používali šifrování či autentizací kódy. Dokumenty v listinné podobě nenechávat v pracovní době volně přístupné, mimo pracovní dobu by měly být vždy uzamčeny ve skříních k tomu určených.

7.2 Dílčí závěr

V kapitole je popsáno, do jakých rizikových stupňů spadají rizika, která byla zjištěna při provedeném auditu. Dále byla navržena konkrétní bezpečností opatření, která byla v závěru kapitoly podrobněji popsána.

ZÁVĚR

Bezpečnostní audit je vhodným nástrojem ke zjištění, na jakém stupni se bezpečnost v dané organizaci ve skutečnosti nachází. Určuje se skutečný stav bezpečnosti a porovnává se s požadovaným. Velmi důležité je věnovat se navrhnutým opatřením a ty pak realizovat do praxe. Podstatným krokem by měla být také následná kontrola.

Cílem diplomové práce bylo provedení bezpečnostního auditu vybraného objektu státní správy. Na základě vstupních informací byly analyzovány hrozby a po analýze rizik ke každé hrozbě navrženy konkrétní bezpečnostní opatření.

V teoretické části byly popsány základní pojmy z oblasti bezpečnosti a řízení rizik, jako je bezpečnost, hrozba, riziko, opatření nebo bezpečnostní posouzení. Dále bylo popsáno několik technik pro posuzování rizik. V druhé kapitole byly popsány hlavní cíle auditu, druhy a etapy auditu a vymezení oblastí auditu.

V třetí kapitole, kterou začíná praktická část diplomové práce, byla charakterizována činnost objektu státní správy, organizační struktura a charakteristika budovy.

V rámci čtvrté kapitoly byla popsána obvodová bezpečnost areálu, režimová opatření, fyzická ostraha areálu a technická ochrana areálu.

V páté kapitole byl podrobněji popsán samotný objekt státní správy, objektová bezpečnost, požární ochrana, bezpečnost a ochrana zdraví při práci a informační bezpečnost.

Šestá kapitola se zabývá zpracováním samotného bezpečnostního auditu. Byl vytyčen cíl auditu a vymezení oblastí, kterých se bude bezpečnostní audit týkat. U každé oblasti byly popsány silné a slabé stránky. Pomocí zjištěných vstupních informací byla provedena analýza rizik. Pomocí metody Kontrolní seznam byly identifikovány hrozby. Pro posouzení a ohodnocení rizik byla vybrána metoda PNH. Ke každé hrozbě tak byl přiřazen rizikový stupeň. Rizika byla zjištěna v rizikových stupních II., III. a IV.

V sedmé kapitole byly na základě provedené analýzy navrženy konkrétní bezpečnostní opaření. Po jejich přijetí organizací by se rizika měla snížit na přijatelnou úroveň.

Dle mého názoru vedení organizace téma bezpečnosti považuje za velmi důležité. S nadšením uvítali téma mé diplomové práce s tím, že navržená opatření budou implementovat do praxe.

SEZNAM POUŽITÉ LITERATURY

[1] KOČÍ, Miroslav, Miroslava KOPECKÁ a Jindřich STIEBITZ. *Průvodce odborně způsobilých osob problematikou bezpečnosti a ochrany zdraví při práci, hornické činnosti a požární ochrany*. Olomouc: ANAG, 2013. Práce, mzdy, pojištění. ISBN 978-807-2638-345.

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

[3] BEZPEČNOST ICT. *ČESKÝ INSTITUT MANAŽERŮ INFORMAČNÍ BEZPEČNOSTI* [online]. Praha: ČIMIB, o.s., 2016 [cit. 2020-03-14]. Dostupné z: http://webcache.googleusercontent.com/search?q=cache:uzcmoF6GINoJ:www.cimib.cz/ors/fileadmin/user_upload/dokumenty/CIMIB_Bezpecnost_ICT.pdf+&cd=1&hl=cs&ct=clnk&gl=cz

[4] Hrozba (Threat). *Management Mania* [online]. Creative Commons BY-NC: ManagementMania.com, 2011 [cit. 2020-03-02]. Dostupné z: https://managementmania.com/cs/hrozba-threat

[5] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management II*. Zlín: Radim Bačuvčík - VeRBuM, 2012. ISBN 978-80-87500-19-4.

[6] *TERMINOLOGICKÝ SLOVNÍK KRÍZOVÉHO RIADENIA* [online]. Aktualizované vydanie v roku 2006. Žilina: FAKULTA ŠPECIÁLNEHO INŽINIERSTVA ŽILINSKEJ UNIVERZITY V ŽILINE, 2005 [cit. 2020-03-19]. ISBN 80-88829-75-5. Dostupné z: http://fsi.uniza.sk/kkm/files/publikacie/tskr.pdf

[7] ČESKO. Zákon č. 224/2015 Sb.: o prevenci závažných havárií způsobených vybranými nebezpečnými chemickými látkami nebo chemickými směsmi. In: *Sbírka zákonů ČR*. Ročník 2015, částka 93, s. 2762-2801. ISSN 1211-1244.

[8] Rizika (Risks*). Management Mania* [online]. 2011: ManagementMania.com, 2011 [cit. 2020-03-08]. Dostupné z: https://managementmania.com/cs/rizika

[9] Analýza rizik: Jemný úvod do analýzy rizik. *Clever and Smart* [online]. WordPress: Miroslav Čermák., 2020 [cit. 2020-03-11]. Dostupné z: https://www.cleverandsmart.cz/analyza-rizik-jemny-uvod-do-analyzy-rizik/

[10] Analýza rizik (2. část). *Bezpečnost v kostce* [online]. Brno: GITY, 2020 [cit. 2020-03-12]. Dostupné z: http://www.chrantesidata.cz/cs/art/1152-dil-5/

[11] BEZPEČNOSTNÍ POSOUZENÍ SYSTÉMU OCHRANY OBJEKTU. *G4S* [online]. London: G4S, 2020 [cit. 2020-03-11]. Dostupné z: https://www.g4s.com/cs-cz/-/media/g4s/czechrepublic/files/radek/1g4s_list_a4_posouzen_cz.ashx?la=cs-cz&hash=A2281BBEA0E741ECB2DC7D0AEAC39D0A

[12] BRABEC, František. *Hlídací služby*. Praha: Eurounion, 1995. ISBN 80-85858-12-6.

[13] Analýza rizik (1. část). *Bezpečnost v kostce* [online]. Brno: GITY, 2020 [cit. 2020-03-12]. Dostupné z: http://www.chrantesidata.cz/cs/art/1150-dil-4/

[14] FTA (Fault Tree Analysis) - Analýza stromu poruchových stavů. *Management Mania* [online]. Creative Commons BY-NC: ManagementMania.com, 2011 [cit. 2020-03-19]. Dostupné z: https://managementmania.com/cs/eta-event-tree-analysis-analyza-stromu-udalosti

[15] ETA (Event tree analysis) - analýza stromu událostí. *Management Mania* [online]. Creative Commons BY-NC: ManagementMania.com, 2011 [cit. 2020-03-19]. Dostupné z: https://managementmania.com/cs/eta-event-tree-analysis-analyza-stromu-udalosti

[16] FMEA (Failure Mode and Effect Analysis). *Management Mania* [online]. Creative Commons BY-NC: ManagementMania.com, 2011 [cit. 2020-03-19]. Dostupné z: https://managementmania.com/cs/failure-mode-and-effect-analysis

[17] HAZOP (Hazard and Operability Study). *Management Mania* [online]. Creative Commons BY-NC: ManagementMania.com, 2011 [cit. 2020-03-19]. Dostupné z: https://managementmania.com/cs/hazop-hazard-and-operability-study-analyza-ohrozeni-a-provozuschopnosti

[18] KAMENÍK, Jiří a František BRABEC. *Komerční bezpečnost: soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur*. Praha: ASPI, 2007. ISBN 978-80-7357-309-6.

[19] *BEZPEČNOSTNÍ AUDIT* [online]. Praha: Risk Analysis Consultants, 2020 [cit. 2020-04-05]. Dostupné z: https://www.rac.cz/rac/homepage.nsf/CZ/SS/$FILE/RAC%20Bezpecnostni%20audit_Datasheet_CZ_151210.pdf

[20] HROMADA, Martin. *Speciální technologie komerční bezpečnosti.* Prezentace. Zlín, 2018.

[21] BRABEC, František. *Ochrana bezpečnosti podniku*. Praha: Eurounion, 1996. ISBN 80-858-5829-0.

[22] Interní nebo externí audit. *S PDQM standardy skutečně pomáhají* [online]. Praha: PDQM, 2016 [cit. 2020-04-05]. Dostupné z: http://ww.pdqm.cz/Standards/Business-Excellence/interni-nebo-externi-audit.html

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

[24] ŠEFČÍK, Vladimír. *Analýza rizik*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009. ISBN 978-807-3186-968.

[25] SEILER, Milan. *Bezpečnostní audit v organizaci*. Praha: Soukromá vysoká škola ekonomických studií, 2014. ISBN 80-86744-20-5.

[26] LAUCKÝ, Vladimír a Rudolf DRGA. *Speciální technologie komerční bezpečnosti* [online]. Zlín, 2012 [cit. 2020-05-19]. ISBN 978-80-7454-146-9 (elektronická verze). Dostupné z: https://digilib.k.utb.cz/ldap-login

[27] Ukončení auditu. *Tretiruka.cz* [online]. Praha: České ekologické manažerské centrum, 2011 [cit. 2020-05-26]. Dostupné z: https://www.tretiruka.cz/news/ukonceni-auditu/

[28] Perimetrická ochrana objektů. *Alcam Profi s.r.o.* [online]. Frýdek-Místek: ALCAM PROFI, 2011 [cit. 2020-06-15]. Dostupné z: http://www.alcamprofi.cz/perimetricka-ochrana-objektu.html

[29] *Perimetrická, plášťová, prostorová a předmětová ochrana SPŠSE a VOŠ Liberec* [online]. Liberec: Střední průmyslová škola strojní a elektrotechnická a

Vyšší odborná škola, Liberec 1, Masarykova 3, příspěvková organizace, 2020 [cit. 2020-06-15]. Dostupné z: https://www.pslib.cz/jiri.kubin/ELZ/03_20Perimetricka_20plastova_20prostorova_20predmetova_20ochrana.pdf

[30] Elektrická zabezpečovací signalizace – EZS. *Alcam Profi s.r.o.* [online]. Frýdek-Místek: ALCAM PROFI, 2011 [cit. 2020-06-15]. Dostupné z: http://www.alcamprofi.cz/elektricka-zabezpecovaci-signalizace-ezs.html

[31] PROSTOROVÁ OCHRANA. *ABBAS Perimetrie* [online]. Brno: ABBAS, 2020 [cit. 2020-06-15]. Dostupné z: http://www.perimetrie.cz/perimetrie/prostorova-ochrana/

[32] PŘEDMĚTOVÁ OCHRANA. *Trade FIDES, a.s.* [online]. 2020: Trade FIDES, Brno [cit. 2020-06-15]. Dostupné z: https://www.fides.cz/technologicke-prostredky/pred-ochrana.html

[33] UHLÁŘ, Jan. *Technická ochrana objektů*. Praha: Vydavatelství PA ČR, 2005. ISBN 80-725-1189-0.

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

[35] Čo je to režimová ochrana? *DAST Holding a.s.* [online]. Bratislava: DAST Security, 2020 [cit. 2020-06-15]. Dostupné z: http://www.dastholding.sk/security/faq/rezimova-ochrana

[36] BRABEC, František a kol.. *Bezpečnost pro firmu, úřad, občana*. Praha: Public History, 2001. ISBN 80-86445-04-06.

[37] Co je BOZP? Definice, cíle, legislativa a principy. *BOZP a PO - bezpečnost práce moderně a efektivně* [online]. Praha: CRDR spol. s r.o., 2015 [cit. 2020-06-16]. Dostupné z: https://www.bozp.cz/aktuality/co-je-bozp/

[38] KAMENÍK, Jiří a František BRABEC. *Komerční bezpečnost: soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur*. Praha: ASPI, 2007. ISBN 978-80-7357-309-6.

[39] ČESKO. Vyhláška č. 246/2001 Sb.: o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci). In: *Sbírka zákonů ČR*. Ročník 2001, částka 95, s. 5446-5489. ISSN 8591449095013-01.

[40] Bezpečnost informací. *Kvalita a informační bezpečnost* [online]. 10. Praha: Ikaros, 2006 [cit. 2020-020-06]. ISSN 1212-5075. Dostupné z: https://ikaros.cz/bezpecnost-informaci

[41] *Standardy a definice pojmů bezpečnosti informací* [online]. Praha: CyberSecurity.CZ, 2019 [cit. 2020-06-21]. Dostupné z: https://www.cybersecurity.cz/data/Gogela.pdf

[42] Kritická komunikační infrastruktura – Centrum technické pomoci. *Informační bezpečnost* [online]. Kroměříž: KKI-CTP, 2019 [cit. 2020-07-01]. Dostupné z: http://www.kki-ctp.cz/11000-informacni-bezpecnost/

[43] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press, 2004. ISBN 80-251-0106-1.

[44] *Souhrná technická zpráva o budově č. 26 KHS Zlín.* KHS Zlín, 2019.

[45] *Vyjádření k požární bezpečnosti a bezpečnosti provozu (práce) budovy č. 26 v areálu Krajské nemocnice T. Bati, a. s. ve Zlíně.* KHS Zlín, 2018.

[46] *Požární řád.* KHS Zlín, 2018.

[47] GDPR-Modelove situace - Kyberbezpečnost. *Ministerstvo vnitra České republiky* [online]. Praha: Ministerstvo vnitra České republiky, 2019 [cit. 2020-07-21]. Dostupné z: https://www.mvcr.cz/gdpr/soubor/gdpr-modelove-situace-kyberbezpecnost.aspx

[48] RIZIKA A JEJICH ANALÝZA. *VŠB - Technická univerzita Ostrava* [online]. Ostrava: VŠB, 2006 [cit. 2020-07-31]. Dostupné z: https://fei1.vsb.cz/kat420/vyuka/Magisterske%20nav/prednasky/web/RIZIKA.pdf

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AYKY Instalační kabely s hliníkovým jádrem.

BOZP Bezpečnost a ochrana zdraví při práci.

CO2 Oxid uhličitý.

CMMI Capability Maturity Model Integration.

ČR Česká republika.

ČSN Česká státní norma.

DPPC Dohledové a poplachové přijímací centrum.

EN Evropská norma.

EPS Elektrická požární signalizace.

EU Evropská unie.

FO Fyzická ostraha.

HZS Hasičský záchranný sbor.

ICT Information and Communication Technologies.

IEC Intemational Electrotechnical Commission.

ISMS Information Security Management Systém.

ISO International Organization for Standardization.

IT Information technology.

ITIL Information Technology Infrastructure Library.

KHS Krajská hygienická stanice.

KNTB Krajská nemocnice Tomáše Bati.

MZ Ministerstvo zdravotnictví.

MZS Mechanické zábranné systémy.

NP Nadpodlaží.

OOPP Osobní ochranné pracovní prostředky.

PO Požární ochrana.

PVC Polyvinylchlorid.

Sb. Sbírka zákonů.

SW Software.

UPS Uninterruptible Power Supply.

WC Water closet.

ZK Zlínský kraj.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: POŽÁRNÍ POPLACHOVÁ SMĚRNICE

POŽÁRNÍ POPLACHOVÉ SMĚRNICE

Požární poplachové směrnice vymezující činnost osob v případě vzniku požáru.

Krajská hygienická stanice Zlínského kraje se sídlem ve Zlíně

1. **Postup osob při zpozorování požáru**
   - uhasit požár hasebními prostředky, které má v nejbližším dosahu (hasicí přístroj, nástěnný hydrant)
   - **ohlásit požár na ohlašovnu požáru, kterou je ohlašovnu požáru Hasičského záchranného sboru Zlínského kraje, tísňové volání na č. 150 nebo 112 (HASIČI), s uvedením místa kde hoří, co hoří a kdo požár hlásí.**
   - **nebo přivolat pomoc stlačením tlačítka požárního hlásiče elektrické požární signalizace v budově**
   - i v případě uhašení požáru je osoba (zaměstnanec) povinna neprodleně případ ohlásit vedoucímu zaměstnanci pracoviště nebo přímo na operační středisko HZS Zlínského kraje

2. **Vyhlášení poplachu v budově**
   - hlasitým voláním „ H O Ř Í “

3. **Postup osob při vyhlášení poplachu**
   - osoby v objektu zahájí hasební práce, nehasit elektrické zařízení pod napětím vodou (hlavní vypínač el. proudu pro budovu je v el. rozvodně v přízemí)
   - po příjezdu požární jednotky se řídí pokyny velitele hasebního zásahu
   - na pokyn velitele zásahu je osoba povinna poskytnout pomoc při zdolávání požáru
   - nesmí svévolně zasahovat do hasebních prací,
   - po vyhlášení evakuace se osoby shromáždí v bezpečné vzdálenosti mimo objekt dle únikového plánu

4. **Důležitá čísla veřejné telefonní sítě (při volání z pobočkového telefonu zvolte nejdříve č. 0)**

Hasičský záchranný sbor Zlínského kraje (tísňové volání)	**150**
Zdravotnická záchranná služba Zlín (tísňové volání)	**155**
Městská policie Zlín (tísňové volání)	**156**
Policie ČR Zlín (tísňové volání)	**158**
Integrovaný záchranný systém Zlín (tísňové volání)	**112**

5. **Důležitá telefonní čísla poruchových služeb:**

Poruchová služba - voda	**840 668 668**
Poruchová služba - plyn	**1239**
Poruchová služba - el. energie	**800 225 577**

6. **Zpracoval:** Ing. Eduard Petr, odborně způsobilá osoba, č. osvědčení Z-632/97

7. **Schválil:** MUDr. Eva Sedláčková, Ph.D., ředitel – vedoucí služebního úřadu

Krajská hygienická st nice
Zlínského k
se sídlem ve Z
Havlíčkovo nábřeží 600 Zlín

Zlín, dne 22.7.2019

PŘÍLOHA P II: ÚNIKOVÝ PLÁN – 3. NP

PŘÍLOHA P III: PLÁN AREÁLU NEMOCNICE TOMÁŠE BATI VE ZLÍNĚ