Zabezpečení administrativních center z pohledu problematiky ochrany měkkých cílů

Securing Administrative Centres From the Soft Target Protection Perspective

Bc. Ondřej Moják

Diplomová práce
2021

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

Akademický rok: 2020/2021

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Ondřej Moják**
Osobní číslo:	**A20889**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Zabezpečení administrativních center z pohledu problematiky ochrany měkkých cílů**
Téma práce anglicky:	**Securing Administrative Centres From the Soft Target Protection Perspective**

Zásady pro vypracování

1. Zpracování literární rešerše na dané téma.
2. Seznamte se metodami pro minimalizaci rizik.
3. Pomocí analytických a praktických metod zhodnoťte problematiku měkkých cílů (v administrativních centrech).
4. Zhodnoťte stávající stav vybraného subjektu v rámci ochrany měkkých cílů.
5. Analyzujte slabá a potencionálně problémová místa v administrativních centrech.
6. Navrhněte opatření k minimalizaci rizik v administrativních centrech.

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

Seznam doporučené literatury:

1. ŠEFČÍK, Vladimír. Analýza rizik. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009. ISBN 9788073186968.
2. PALEČEK, Miloš. Prevence rizik. Praha: Oeconomica, 2006. ISBN 8024511177.
3. LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management. Zlín: Radim Bačuvčík – VeRBuM, 2015. ISBN 9788087500194.
4. KALVACH, Z. Základy ochrany měkkých cílů metodika. Vyd.1. Praha, 2016.
5. KYNCL, Jaromír. Bezpečnost objektu ve světle moderních technologií. Praha: Komora podniků komerční bezpečnosti České republiky, 2014. ISBN 978-80-260-7115-0.

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

Datum zadání diplomové práce: **15. ledna 2021**
Termín odevzdání diplomové práce: **17. května 2021**

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

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

Ing. Milan Navrátil, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 15. ledna 2021

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

Ve Zlíně, dne 7. 5. 2021

Bc. Ondřej Moják, v.r.
podpis diplomanta

ABSTRAKT

Cílem této práce je návrh zabezpečení administrativního centra z pohledu problematiky měkkých cílů. Teoretická část je zaměřená na seznámení s problematikou měkkých cílů, jejich popisem, možnostmi a metodami jejich zabezpečení a také současnými hrozbami. Dále práce přibližuje čtenáři relevantní zákony a normy. Součástí teoretické části je také stručný popis procesu a vybraných metod pro analýzy rizik. Praktická část je zaměřená na popis a bezpečnostní posouzení administrativního centra za využití SWOT analýzy a metody CARVER. Na výsledek analýz navazuje návrh bezpečnostních opatření. Dále praktická část popisuje dvě modelové situace ohrožení administrativního centra.

Klíčová slova: Měkký cíl, SWOT, CARVER, Analýza rizik, Administrativní centrum, TerEX

ABSTRACT

The aim of this thesis is to design the security of the administrative centre from the perspective of soft targets. The theoretical part is focused on getting acquainted with the issue of soft targets, their description, possibilities and methods of their security, as well as with the current threats. Furthermore, the work introduces the reader to the relevant laws and standards. A brief description of the process and selected methods for risk analysis are also included in the theoretical part. The practical part is focused on description and security evaluation of the administrative centre using SWOT analysis and CARVER methods. The result of analyses is followed by security measurements' proposal. Furthermore, the practical part describes two model situations of administrative centre being threaten.

Keywords: Soft Target, SWOT, CARVER, Risk Analysis, Administrative Center, TerEX

Tímto bych chtěl poděkovat svému vedoucímu panu doc. Ing. Martinovi Hromadovi, Ph.D. za čas a cenné rady, které mi věnoval při tvorbě diplomové práce.

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

OBSAH

ÚVOD

V dnešní době je svět zmítán nejrůznorodějšími bezpečnostními hrozbami, které jsou svými aktéry neustále zdokonalovány. Čím dál častěji jsou jejich útoky cílené především na objekty s velkou koncentrací lidí, které jsou svou charakteristikou složité zabezpečit. Je nutné si uvědomit, že i když se bezpečností technologie a bezpečnostní složky neustále rozvíjejí a adaptují na nejnovější formy útoků, tak velká část zodpovědnosti za vlastní bezpečí, ale také za bezpečí našeho nejbližšího okolí závisí právě na nás.

Hlavním cílem této diplomové práce je zhodnotit a následně navrhnout bezpečnostní opatření minimalizující potencionální hrozby objektu administrativního centra z pohledu měkkých cílů.

V teoretické části bude čtenář seznámen se zákony, vyhláškami a normami, které jsou relevantní pro problematiku bezpečnosti měkkých cílů. Především se bude jednat o trestní zákoník a jeho vybrané paragrafy přibližující pojmy jako je teror či teroristický útok. Další kapitola bude zaměřená na vysvětlení významu a možnosti rozdělení měkkých cílů a jejich odlišení od cílů tvrdých. Dále se kapitola bude věnovat principům a východiskům ochrany měkkých cílů a základním pilířům pro jejich ochranu z pohledu vlády České republiky vycházejícího z metodiky – Základy ochrany měkkých cílů. Následující kapitola bude přibližovat problematiku analýzy rizik, její rozdělení a popis vybraných metod. Dále kapitola nastiňuje aktuální hrozby pro měkké cíle v ČR, mezi které patří například teroristický útok nebo extrémismus. Čtenář následně bude v další kapitole seznámen s diagnostikou, prostředky a postupy pro zabezpečení měkkých cílů. Kapitola se také věnuje popisu bezpečnostních prvků při ochraně měkkých cílů, mezi které patří fyzická bezpečnost, režimová opatření a systémy technické ochrany, a jejich využití. Nakonec bude také vysvětlena role běžného občana při zabezpečení takto definovaných cílů. Poslední kapitola teoretické části popisuje softwarový nástroj TerEX sloužící pro odhad dopadů při výbuchu či úniku nebezpečné látky.

První kapitola praktické části bude zaměřena na přiblížení vybraného administrativního centra, popis jeho vnitřních prostorů a přilehlého okolí. Následně bude kapitola zhodnocovat bezpečnostní stav objektu a okolí, který bude vycházet z autorových poznatků při fyzické návštěvě objektu a dat z webového portálu www.mapakriminality.cz. Nakonec bude vytvořen katalog obsahující seznam potencionálních hrozeb. Další kapitola bude vyhodnocovat bezpečnostní stav objektu za využití dvou metod pro analýzu rizik. SWOT

analýza, která hodnotí vnitřní a vnější vlivy, které působí na budovu a metoda CARVER, která slouží k vyhodnocení hrozeb z pohledu útočníka. Následující kapitola bude zaměřena na vytvoření dvou scénářů popisujících bezpečnostní incidenty. Kapitola bude obohacena o strom událostí detailně popisující jeden z incidentů a také o výsledky softwarového nástroje TerEX, který popisuje dopady výbuchu bomby. Závěrečnou kapitolou praktické části budou návrhy bezpečnostních opatření vytvořených na základě dat získaných z jednotlivých analýz a také ze scénářů popisujících modelové situace.

I. TEORETICKÁ ČÁST

1 PRÁVNÍ RÁMEC

Kapitola věnována zákonům, které jsou spjaty s problematikou ochrany měkkých cílů. Především se jedná o zákon č. 40/2009 sb. nového trestního zákoníku, který vešel v platnost 1.1.2010. Jedná se o výpis relevantních částí a paragrafů jako jsou § 311 teroristický útok či § 272 obecné ohrožení a další. [1] [2]

V této kapitole budou také stručně zmíněny další zákony a relevantní normy jako je zákon o integrovaném záchranném systému (IZS), zákon o krizovém řízení, zákon o požární ochraně a příslušně normy průmyslu komerční bezpečnosti (PKB).

1.1 Zákon č. 40/2009 Sb. trestní zákoník

Trestní zákoník představuje důležitou část oblasti veřejného a hmotného práva. Nynější nová verze, která platí od roku 2010 nahrazuje československý trestní zákoník. Na jeho znění se podílelo několik expertů, ovšem primárním autorem finálního znění zákona je prof. Pavel Šámal. Zákoník je rozdělen do tří částí obecné, zvláštní a přechodná a závěrečná ustanovení. [1] [2]

§ 311 – Teroristický útok

Paragraf 311 se zabývá komplexním pohledem na problematiku teroristických útoků. Teroristický útok provádí jednotlivec nebo skupina, která si klade za úkol zaútočit na ústavní zřízení nebo schopnost obrany České republiky. Dále se může jednat o snahu napadnout hospodářskou, politickou nebo sociální strukturu republiky či mezinárodní organizace. Takovýto útočník vyvíjí tlak na společnost a představitele republiky za účelem plnění jeho požadavků. [1]

Za teroristický útok považujeme například manipulaci, narušení nebo přerušení dodávek energii (voda, elektřina atd.) za účelem vydírání nebo způsobením velkých hmotných škod. [1]

§ 312 – Teror

Z pohledu trestního zákoníku se teroru dopouští někdo, kdo si klade za cíl úmyslně poškodit ústavní zřízení České republiky, nebo usmrtit jiného jedince. Pokud bude útočník uznán vinným, tak mu může soud uvalit trest odnětí svobody ve výši patnáct až dvacet let. [1]

Dle trestního zákoníku i samotná příprava výše zmíněných trestných činů se považuje za trestný čin. [1]

§ 312f – Vyhrožování teroristickým trestním činem

Definuje trest pro osobu obviněnou z činnosti vyhrožování spáchání teroristického útoku v podobě, jakým je definován v § 311. Člověk, který je obviněn může být odsouzen k odnětí svobody na dobu tří až dvanácti let a také propadnutí majetku. [1]

Pokud se pachatel proviní tím, že byl členem teroristické organizace, propagací terorismu, spácháním útoku se zbraní či provedením teroristického útoku za stavu ohrožení státu nebo válečného stavu, bude odsouzen v rozmezí pěti až patnácti lety vězení. [1]

§ 107 – Pachatel trestného činu spáchaného ve prospěch organizované zločinecké skupiny

Paragraf zaměřený na definici pachatele, který překračuje meze zákona za účelem prospěchu takzvaného organizovaného zločinného uskupení. Jedná se o pachatele, který úmyslně spolupracoval a podporoval útvar organizovaného zločinu. [1]

Organizovanou zločineckou skupinou rozumíme uskupení minimálně tří osob, které mají vnitřní strukturu a organizaci funkcí, zaměřených na konstantní porušování zákona České republiky (§ 129 trestního zákoníku). [1]

§ 272 – Obecné ohrožení

Tato část trestního zákoníku se zaměřuje na definování trestného činu obecného ohrožování. Ten, kdo se dopouští obecného ohrožení je definován jako osoba, která úmyslně vystaví ostatní smrti či vážnému zranění či těžké újmy na zdraví. [1]

Dále tím myslíme osobu, která způsobí škodu na cizím majetku ve velkém rozsahu. Například se jedná žhářství, vytopení, poškození výbušninou, plynem, elektřinou nebo jiným způsobem. [1]

§ 274 – Ohrožení pod vlivem návykové látky

Jedná se o paragraf navazující na § 272. Zaměřuje se na osoby, které jsou pod vlivem alkoholu, nebo jiných omamných látek při zaměstnání či vykonávání jiných činností. Upravuje znění zákona v případě, že osoba pod vlivem alkoholu nebo jiné návykové látky způsobí rozsáhlé škody na cizím majetku či vystaví jiné osoby situací ohrožující jejich život. [1]

1.2 Zákon č. 239/2000 Sb. o integrovaném záchranném systému

Zákon pojednávající o vymezení působnosti jednotek spadající do IZS. Zákon uvádí, že: „*Integrovaným záchranným systémem je koordinovaný postup jeho složek při přípravě na mimořádné události a při provádění záchranných a likvidačních prací*“. [3]

Za základní složky IZS považujeme Hasičský záchranný sbor České republiky, jednotky požární ochrany, zdravotní záchranné služby a Policejní sbor České republiky. Zákon také udává ostatní složky jako jsou například ozbrojené síly. Tyto záchranné složky ovšem poskytují pomoc pouze na vyžádání. [3]

1.3 Zákon č. 240/2000 Sb. krizový zákon

Krizový zákon stanovuje pravomoc, pole a rozsah působnosti orgánů státu, územních samosprávných celků a zároveň upravuje práva a povinnosti fyzických a právnických osob v případě, že nastane krizová situace. [4]

Krizová situace je definována jako: *„krizovou situací mimořádná událost podle zákona o integrovaném záchranném systému, narušení kritické infrastruktury nebo jiné nebezpečí, při nichž je vyhlášen stav nebezpečí, nouzový stav nebo stav ohrožení státu (dále jen „krizový stav“)“*. [4]

Zákon definuje pojmy jako je krizové řízení či stav nebezpečí a zároveň tvoří hierarchii orgánů v případě krizového stavu. [4]

1.4 Zákon č. 133/1985 Sb. o požární ochraně

Zákon zaměřující se na vytvoření optimálních podmínek, které budou sloužit k zabezpečení zdraví a života obyvatel republiky v případě požárů. Zároveň je zaměřený na poskytování akutní pomoci při mimořádných událostech typu živelná pohroma (povodně, zemětřesení atd). [5]

Zákon dále poukazuje na povinnost každého jednotlivce nevytvářet situace, při kterých může dojít k požáru a na základě toho ohrožení života a zdraví osob, zvířat a majetku. V případě, že se vyskytneme v dění požáru nebo živelné pohromy nám zákon ukládá povinnost poskytnout odpovídající pomoc za podmínek, že se sami nevystavíme nebezpečí nebo neohrozíme jiné osoby. [5]

1.5 Příslušné normy průmyslu komerční bezpečnosti (PKB)

Normy popisující především technické požadavky na jednotlivé poplachové systémy. Předepsané normy také slouží jako konkrétní návody a postupy při implementaci poplachových systémů. Mezi takovéto normy řadíme například:

- **ČSN EN 50 130** – všeobecné požadavky poplachových systému,
- **ČSN EN 50 131** – poplachové zabezpečovací a tísňové systémy,
- **ČSN EN 50 132** – sledovací systémy (CCTV),
- **ČSN EN 50 134** - systém přivolání pomoci,
- **ČSN EN 50 135** – tísňové systémy,
- **ČSN EN 50 136** – poplachové přenosové systémy a zařízení,
- **ČSN EN 50 137** – kombinované či integrované systémy. [6]

1.6 Návrh zákona o soukromých bezpečnostních službách

Jedná se o návrh, který byl předložen Ministerstvem vnitra, jehož cílem má být podrobný dohled a správa činností v oblasti soukromých bezpečnostních služeb provozovaných jednotlivci či společnostmi. [7] [8]

V současném znění živnostenského zákona jsou bezpečnostní služby rozdělené do tří kategorií. Nová úprava rozděluje tyto služby do šesti kategorií dle specifických licencí:

- ochrana osob a majetku,
- ochrana majetku ve zvláštních případech,
- činnost soukromého detektiva,
- převoz peněz, hodnotných předmětů a cenin nad pět miliónů Kč,
- technická služba sloužící za účelem ochrany osob a majetku,
- konzultace v oblasti bezpečnostního poradenství. [7] [8]

Na základě těchto licencí získá kontrolní orgán přehled nad tím, kdo tyto činnosti smí a nesmí provádět. [7] [8]

Návrh dále upravuje a stanovuje bezpečnostní činnost za účelem vlastní potřeby na veřejně přístupných místech (sportovní haly, parky, obchodní centra, nemocnice a další.). Tato

úprava je nutná z důvodu častého narušování osobní svobody a porušováních základních lidských práv a svobod osob nacházející se v objektu ze strany přítomných zaměstnanců. Proto dle nových předpisů by tito zaměstnanci měli splňovat totožné podmínky, jako zaměstnanci soukromých bezpečnostních služeb. [7] [8]

Tyto změny přichází především z důvodů zvýšení úrovně kvality bezpečnostních služeb na veřejně přístupných místech. Na základě těchto změn by měli být jak zaměstnanci bezpečnostních agentur, tak osoby zajišťující vlastní ostrahu objektu stejnou odbornou tak fyzickou způsobilost k vykonávání jejich pracovních náplní. [7] [8]

Pomocí těchto změn chce Ministerstvo vnitra dosáhnout toho, aby občané pociťovali větší jistotu, že bezpečnostní činnost zajišťují opravdoví profesionálové. [7] [8]

V současné době neexistují žádné právní normy či předpisy, které by upravovaly problematiku ochrany měkkých cílů. Tudíž samotná ochrana připadá na majitele objektu definovaného jako měkký cíl, který může využít vlastnických či užívacích práv „pána domu“. [7] [8]

Prvním náznakem změny, bylo v roce 2011 podání návrhu zákona o bezpečnostní činnosti, kterou můžeme považovat za předchůdce výše zmíněného návrhu. [7] [8]

Prvním výrazným krokem ke změně přístupu bylo vydání metodiky Ministerstva vnitra pojednávající o základech ochrany měkkých cílů. Tato metodika komplexně popisuje právě nedostatky v oblasti ochrany veřejně dostupných míst. [7] [8]

Na základě schválení výše zmíněného návrhu, je možné říct, že vláda začala brát v potaz stoupající počet útoků na právě měkké cíle a je připravená podniknout potřebné kroky k zajištění bezpečnosti obyvatel České republiky. [7] [8]

Kapitola byla věnována zákonům a normám, které jsou spojeny s problematikou měkkých cílů. Především se věnovala trestnímu zákoníku a jeho relevantním částem a paragrafům jako jsou například § 311 teroristický útok. Následně zde byly popsány další související zákony a normy jako jsou například zákon o krizovém řízení nebo normy PKB.

Nakonec byl popsán návrh zákona o soukromých bezpečnostních složkách a v návaznosti na něj byla také přiblížena současná absence právního rámce, který řeší problematiku měkkých cílů.

2 MĚKKÉ CÍLE (SOFT TARGETS)

Za měkké cíle považujeme místa, která umožňují snadný přístup velkému množství lidí, a přitom disponují omezeným zabezpečením, jsou tedy snadnějším cílem pro potencionální útoky. Jako příklad můžeme uvést školy, obchodní domy, hotely či administrativní budovy a mnoho dalších. Ovšem nemusí se jednat pouze o budovy. Pod pojmem měkký cíl si také můžeme představit festivaly, sportovní události, průvody či demonstrace. [9] [10] [11] [12]

Termín „měkké cíle" jako takový nebyl zatím definován, ale dle Ministerstva vnitra se jedná o *„místa s vysokou koncentrací osob a nízkou úrovní zabezpečení proti násilným útokům"*. [12]

Tvrdé cíle (Hard Targets)

Abychom si lépe uvědomili, co přesně je měkký cíl je nutné si definovat také, co považujeme za cíle tvrdé. [10] [11] [12]

Tvrdé cíle jsou tedy místa, které mají zabezpečení na dostatečně vysoké úrovni, aby zamezili napadení či neoprávněnému vniknutí do objektu. Tedy se jedná o místa, které jsou velice dobře chráněny. Za takovéto objekty považujeme například vojenské objekty, důležité státní objekty a mezi tvrdé cíle můžeme zařadit také vybrané komerční objekty. [10] [11] [12]

2.1 Rozdělení měkkých cílů

Na základě výše nastíněnému rozdílu mezi tvrdými a měkkými cíli, můžou být nyní vybrány objekty, které mohou být definovány jako měkké cíle:

- školy a s nimi spojená místa jako jsou: menzy, koleje či knihovny,
- církevní místa (kostely, katedrály atd…),
- obchodní domy či tržiště (můžeme zde zařadit také celé nákupní zóny),
- kina, divadla, místa určena k pořádání koncertů či nejrůznější zábavní komplexy (IQ parky, únikové hry atd…),
- události spojené s velkou koncentrací osob v otevřených prostorech jako jsou demonstrace, průvody, poutě či nejrůznější shromáždění,
- hotelová či restaurační zařízení, bary, diskotéky, kluby,
- městské prostory jako jsou parky, náměstí, historické památky, muzea či galerie,

- velké dopravní uzly (nádraží, letištní terminály),
- zdravotnická zařízení (nemocnice, polikliniky či ordinace),
- objekty určené k pořádání sportovních akcí jako jsou například sportovní stadióny,
- komunitní centra. [12]

Dále můžeme rozdělit měkké cíle z pohledu zdroje, který může tyto cíle ohrozit:

- ohrožení nebezpečnou specifickou skupinou. Pod tímto pojmem rozumíme nebezpečné skupiny spadající pod organizovaný zločin,
- ohrožení teroristickou organizací (politicky či nábožensky motivovanou),
- ohrožení osamostatněným útočníkem (psychicky narušeného jedinec). [12]

Měkké cíle je také možné rozdělit na základě časové doby. Jestli se jedná o měkké cíle trvalé či dočasné. [12]

Trvalé

- venkovní (stadiony, sportoviště atd.),
- vnitřní (v této kategorii se nachází například administrativní centra, nemocnice, školy, nákupní centra a další). [12]

Dočasné

Pokud hovoříme o dočasných měkkých cílech máme na mysli většinou venkovní akce (za určitých okolností také ve vnitřních prostorech). Dočasné akce jsou rozdělené do dvou kategorií:

- první kategorií jsou například festivaly či koncerty, kde při vstupu musíte předložit zaplacený lístek,
- druhou kategorií jsou akce, které návštěvníkům umožňují volný vstup. Jedná se především o demonstrace nebo vybrané společenské akce, které nevyžadují poplatek za vstup. [12]

2.2 Principy a východiska ochrany měkkých cílů

Kapitola popisující základní principy a východiska při zajišťování ochrany měkkých cílů. Tyto principy jsou rozděleny do čtyř základních východisek: Bezpečnost měkkého cíle

je odpovědnost všech dotčených subjektů, proaktivní přístup, spolupráce a koordinace. [10] [11] [12]

Bezpečnost měkkého cíle jako odpovědnost všech dotčených subjektů

Z tohoto východiska vyplývá, že každá osoba si primárně za svou bezpečnost zodpovídá sama. Je nutné být ostražitý v každodenním životě, ne vždy je totiž možné se spolehnout na bezpečnostní složky, ozbrojené složky či stát. K napadení či jakékoliv činnosti ohrožující všeobecnou bezpečnost zpravidla dochází ve velmi malém časovém úseku a je prakticky nemožné, aby na každý útok došlo k náležité reakci. Obzvlášť při útocích na měkké cíle, které nejsou pod konstantním dohledem státu. [10] [11] [12]

Proaktivní přístup

Jedná se o vytváření dostatečných bezpečnostních opatření prevenčního charakteru, které jsou nezbytné k zabezpečení měkkého cíle. Je potřeba provádět analýzy na základě, kterých můžeme předvídat a předcházet násilným útokům směřovaným na bezpečnost měkkého cíle. Jak již bylo zmíněno k takovým to útokům dochází ve velmi krátkých časových intervalech (v rámci několika sekund) a je prakticky nemožné na ně reagovat okamžitě. Proto je proaktivní přístup naprosto nezbytný k minimalizaci bezpečnostních incidentů a následků, které tyto útoky mohou mít. [10] [11] [12]

Spolupráce

Spolupráce je nezbytná činnost při zajišťování bezpečnosti měkkých cílů. Na jejím zabezpečení by se měli podílet jednotliví majitelé, kteří využívají prostory definované jako měkké cíle, ale také především samotné obce, kraje a stát. [10] [11] [12]

Nastavení komunikačních procesů a organizaci a koordinaci činnosti osob v oblasti měkkých cílů

K tomu, aby bylo vytvořeno bezpečné prostředí v rámci měkkých cílů je nutné zvolení správných komunikačních procesů, spolupráce činností jednotlivých zaměstnanců, sdílení informací či zvolení správného školení. Tyto věci jsou často opomíjeny, jelikož z pohledu zaměstnavatelů využívajících například prostory obchodních center či administrativních budov se jedná o zbytečné náklady. [10] [11] [12]

2.3 Pilíře systému ochrany měkkých cílů České republiky

Následující kapitola je věnována čtyřem základním pilířům ochrany měkkých cílů v České republice, které byly definovány v roce 2017 Ministerstvem vnitra. Mezi tyto pilíře patří: [12]

Metodické vedení a vzdělávání

Na základě neustálého nárustu hrozeb teroristických útoků v Evropě se do značné míry projevuje nepřipravenost a podcenění hrozeb tohoto typu útoku. Proto si Ministerstvo vnitra klade za cíl, jak nejefektivněji zvýšit úroveň bezpečnosti měkkých cílů jako takových.

Jedna z odpovědí, která by mohla vyřešit problém bezpečnosti měkkých cílů je metodické vzdělávání personálu, ale i široké veřejnosti. Na základě tohoto zjištění si Ministerstvo vnitra dalo za cíl vytvořit dostatečné podpůrné školící materiály jak pro odborný personál, tak běžné občany. [11] [12]

Dotační podpora

Dalším pilířem je dle Ministerstva vnitra dostatečné financování ochrany měkkých cílů. Samotné zajištění bezpečnosti je poměrně nákladná záležitost, kterou si spousta subjektů nemůže dovolit. Na základě tohoto faktu jsou měkké cíle poměrně často nezabezpečené, nebo zabezpečené minimálně. Jako východisko vidí Ministerstvo vnitra dotační programy, které mohou vlastníci čerpat pro vytvoření dostatečných bezpečnostních podmínek. [11] [12]

Komunikace, spolupráce, výměna informací a sdílení dobré praxe

Cílem ministerstva vnitra, je vytvoření komunikačních kanálů subjektů dotýkajících se problematiky měkkých cílů. Na základě toho byl vytvořen poradní sbor, který se touto problematikou zabývá. Součástí sboru nejsou pouze jednotlivé subjekty měkkých cílů, ale také široká škála nezávislých odborníků v tomto směru. [11] [12]

Aktivní přístup Policie České republiky

Nezbytným faktorem zajištění bezpečnosti měkkých cílů je funkce Policie ČR. Její funkce v oblastech jako jsou příprava pro zajištění měkkého cíle, plánování bezpečnostních opatření a další je nenahraditelná. Například demonstrace či fotbalové utkání by se bez přítomnosti policejních složek těžko zabezpečovaly. [11] [12]

Kapitola zaměřená na přiblížení a vysvětlení pojmu měkký cíl a jeho rozdílu oproti cílům tvrdým. Následně byly popsány vybrané varianty, na základě kterých lze rozdělit jednotlivé měkké cíle. Nakonec kapitola pojednává o principech ochrany a základních pilířích pro zabezpečení měkkých cílů dle vlády České republiky.

3 ANALÝZA RIZIK

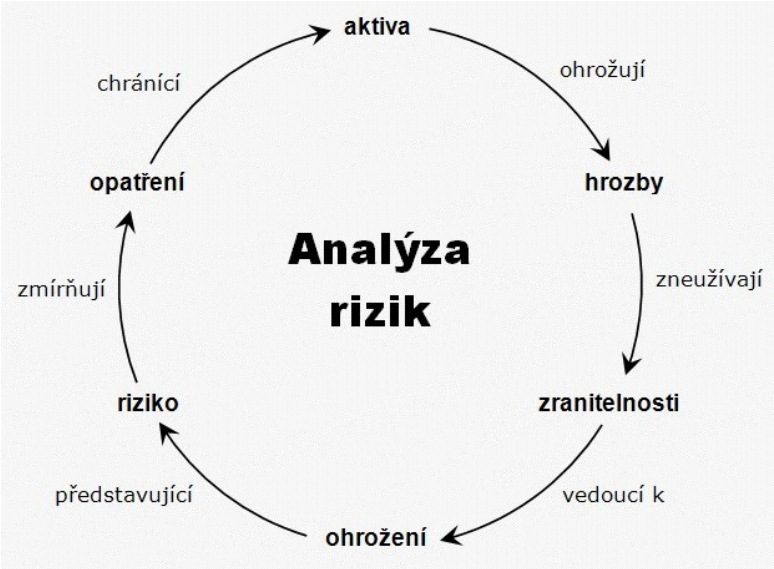
Analýza rizik je jedním ze šesti základních fází procesu řízení rizik neboli „Risk Managementu“ (proces, který je zaměřen na oblast analýzy a následné snížení rizik, na základě využití postupů a principů vedoucích k odhalení a minimalizování rizik, která se mohou vyskytnout v budoucnosti). [13] [14]

Při tvorbě analýzy rizik by měly být zodpovězeny otázky jako jsou například „Jaké hrozby působí na subjekt?“, „Jak moc je vůči těmto hrozbám subjekt zranitelný?“ či „Jaký dopad by to mělo na daný subjekt?“. [13] [14]

Samotný pojem je možné definovat jako proces, který si klade za cíl identifikovat jednotlivé bezpečnostní hrozby, včetně jejich dopadů za naplnění konkrétních podmínek. Na základě analýzy rizik je tedy možné definovat potencionální slabá místa v bezpečnosti subjektu, která by mohla vést k potencionální bezpečnostní hrozbě. Proces analýzy rizik je možné rozdělit na tři základní činnosti:

- identifikace rizikových faktorů,
- vytváření scénářů,
- ohodnocení rizik. [13] [14]

Pokud hovoříme o bezpečnosti administrativních center mohlo by se například jednat o vynesení citlivých dat společnosti, která konkrétní administrativní budovu využívá, či ohrožení na životě jednotlivých osob nacházejících se v administrativním centru. [13] [14]



Obrázek 1: Analýza rizik [15]

Primární faktory při posuzování rizika:

- **míra pravděpodobnosti rizika** (pravděpodobnost určující, že dojde k dané rizikové situaci),
- **úroveň rizika,**
- **dopady rizika** (důsledky, které vyvstanou za podmínek, že k dané rizikové situaci dojde),
- **předvídatelnost rizika** (zda je možné předem riziko odhalit, identifikovat a předvídat, jak se bude vyvíjet),
- **míra ovlivnitelnosti** (neovlivnitelné, ovlivnitelné nebo částečně ovlivnitelné),
- **vztah k organizaci** (interní a externí rizika),
- **úroveň rizika** (velké, střední a malé),
- **přijatelnost** (nutná, přijatelná nebo neúnosná),
- **pravděpodobnost vzniku a působení** (nepravděpodobná, málo pravděpodobná, pravděpodobná, velmi pravděpodobná a téměř jistá). [16]

Předmět a cíl analýzy

Za předmět analýzy rizik můžeme považovat jakoukoliv aktivitu, kterou provádíme a přináší potencionální rizika. Předmětem analýzy rizik tedy může být například:

- návrh a vývoj nového produktu,
- výstavba nového administrativního centra,
- půjčka,
- a další… [14] [15]

Cílem analýzy rizik je následné zpracování podkladů, které vypovídají o stávající situaci a nedostatcích, které by mohly vést k potencionálním rizikům spojeným s analyzovanou aktivitou. Výstup analýz může být například:

- podklady pro ovládání rizik,
- podklady pro rozhodování o riziku,

- a další… [14] [15]

Je nutné zmínit, že předmětem a cílem analýzy rizik není zkoumaní věnující konkrétním rizikům, ale rizikům, která by mohla v budoucnosti nastat. [14] [15]

3.1 Identifikace rizik

Prvním a nejdůležitějším krokem v procesu analýzy rizik je jejich identifikace. Je nutné identifikovat a popsat veškeré faktory, které působí na daný subjekt. Od zaměstnanců, výskytu externích osob až po identifikaci potencionálně nebezpečných situací, které se mohou vyskytnout. [14] [17] [18]

Při identifikaci dochází k nalezení a popsání všech nebezpečí, která by mohla mít v budoucnosti negativní dopad na subjekt jako jsou například úrazy zaměstnanců, ale také úrazy, které mohou nastat externím osobám nacházející se v objektu, krádeže či škody na majetku a další. [14] [17] [18]

K tomu, aby byla rizika správně identifikovaná je nutné si zodpovědět několik základních otázek, které se ptají, co konkrétně představuje nebezpečí a kdo představuje nebezpečí pro daný subjekt. [14] [17] [18]

Mezi metody sloužící k identifikaci rizik můžeme zařadit například:

- kontrolní listy (Check List),
- analýza bezpečnosti práce (BOZP) a další… [14] [17] [18]

Kromě rizik budoucích, které můžeme odhalit na základě výše zmíněných metod je vhodné využít retrospektivní pohled na rizika, které již vyvstaly v minulosti a mohly by se opakovat nebo jiným způsobem ovlivnit hrozby budoucí. [14] [17] [18]

3.2 Stanovení rizik

Jedná se o proces zahrnující subjektivní náhled a odhad autora na konkrétní negativní jevy, které mohou přinést bezpečnostní rizika. Na základě každého identifikovaného nebezpečí je nutné představit plánovaná nebo stávající bezpečnostní opatření, která těmto negativním jevům předchází. Při vytváření těchto opatření je také nutné brát v potaz možnost selhání a také následky, ke kterým dojde při selhání. [14] [19]

3.3 Metody stanovení rizik

Samotnou analýzu rizik je možné popsat jako multikriteriální hodnocení parametrů, které se nacházejí v našem okolí. Jedná se tedy o multikriteriální analýzy. Jednotlivé metody lze rozdělit na kvalitativní a kvantitativní, ovšem některé mohou spadat do kategorie takzvaných semikvantitativních metod. [14] [19]

Kvantitativní analýza rizik

Tato analytická metoda je založena na dvou krocích, a to jsou pravděpodobnost výskytu nechtěného jevu a pravděpodobnost ztráty hodnoty. Tyto dva faktory jsou důležité z důvodu nutnosti vyjádření hodnoty aktiva ve finančních jednotkách. Na základě toho je autorovi umožněno snadnější rozhodování ve zvládání rizik. [14] [19]

Kvalitativní analýza rizik

Metoda, která je využívána k vyjádření stupně důležitosti mezi jednotlivými riziky. Kvalitativní metoda pracuje na základě dat o následcích a ztrátách hodnoty. U kvalitativních metod je nutné stanovení zranitelnosti a míry ohrožení subjektu. [14] [19]

Kvantitativní x Kvalitativní analýza rizik

Tabulka 1: Kvantitativní x kvalitativní metody [19]

	Kvantitativní	**Kvalitativní**
Výpočtová náročnost	-	+
Transparentnost	+	-
Náklady	-	+
Náročnost na programové vybavení	-	+
Náročnost na lidské zdroje	-	+
Časová náročnost	-	+
Kontrola nákladů	+	-
Přesnost	+	-

Na výše uvedené tabulce jsou znázorněny výhody a nevýhody jednotlivých metod. Je nutné si ovšem uvědomit, že jednotlivé metody mezi sebou nesoupeří, naopak se navzájem doplňují ve svých nedostatcích. [19]

Semikvantitativní analýza rizik

Ke svému vyhodnocení využívají analýzy kvalitativně popsané stupnice s přidělenými číselnými hodnotami, na základě kterých je vyhodnocena míra rizika. Jako příklad užití analýz spadající do této kategorie může být bezpečnostní východisko v provozu subjektu. Spadá zde například analýza „Budová metoda“. [20]

3.4 Jednotlivé metody analýzy rizik

V následující části budou popsány vybrané metody využívané v analýze rizik. Jako příklad vybraných analýz můžeme uvést kontrolní seznamy, CARVER, bezpečnostní kontrola
a další.

3.4.1 Kontrolní seznamy (Check List)

Jedná se o velmi snadnou, rychlou a velice efektivní metodu, která je postavena na předem vytvořeném seznamu obsahující kontrolní otázky. K tomu, aby bylo možné vytvořit kontrolní seznam je nutné definovat související předpisy a normy pomocí kterých, je poté samotný seznam sestaven. Díky tomu je většina kontrolních seznamů velice podrobná a specifikovaná tak, aby bylo možné posoudit současný stav systému na základě předem vybraných norem a předpisů. [14] [21] [22]

Značnou nevýhodu kontrolních seznamů představuje především potencionální nízká úroveň zkušeností autora seznamu, proto je nutné, aby takovéto seznamy vytvářeli pouze pracovníci, kteří jsou dostatečně zdatní v daném oboru, pro který je seznam vytvořen. [14] [21] [22]

3.4.2 Bezpečnostní kontrola

Bezpečnostní kontrola neboli bezpečnostní audit je metoda zkoumající bezpečnostní situace na základě, kterých následně autor navrhuje zvýšení bezpečnosti ve vybraném sektoru. Tuto metodu je možné považovat za metodiku hledání potencionálně nechtěného jevu v provozu. [14] [23]

3.4.3 Analýza toho, co se stane když? (What-If Analysis)

Analýza nesoucí anglický název „What-if“ je poměrně jednoduchá analytická technika využívaná především v oblasti řízení rizik, která vyhledává potencionální dopady konkrétních situací. Následně po zjištění jednotlivých dopadů jsou určeny bezpečnostní opatření. [14] [24]

Tuto analýzu je také možné popsat jako „brainstormingový proces“ neboli diskusi expertů, kteří se snaží definovat možné nehody. Tito experti si pokládají otázku „Co se stane když…?“ a na základě odpovědí hledají optimální řešení. [14] [24]

Největší výhoda této metody spočívá v její flexibilitě a schopnosti se přizpůsobit jakékoliv situaci, ovšem na rozdíl od metod jako je například metoda Analýza příčin následku (FMEA), či Analýza ohrožení provozuschopnosti (HAZOP) není vnitřně strukturovaná. [14] [24]

3.4.4 Hazard Operation Process (HAZOP)

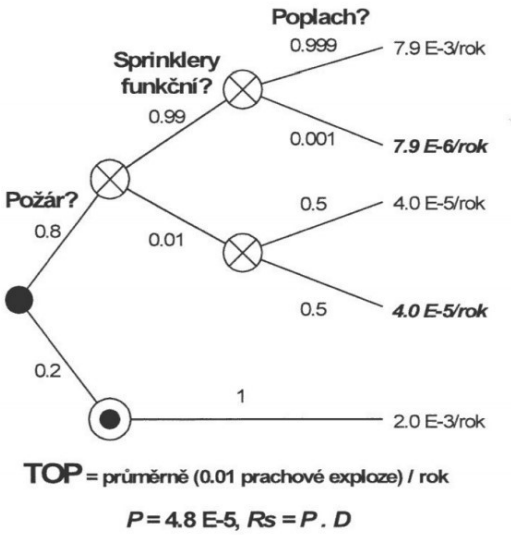
Metoda HAZOP, která v překladu znamená analýza ohrožení a provozuschopnosti se řadí mezi jednu z nejméně náročných a zároveň nejrozšířenějších možností identifikace potencionálních rizik. Analýza pracuje na principu hodnocení pravděpodobnosti ohrožení, z něhož plynou jednotlivá rizika. Výsledkem této metody jsou scénáře jednotlivých rizik, které mohou nastat. Pomocí těchto scénářů je autor schopen identifikovat potencionálně negativní jevy. Analýza se snaží o identifikaci takzvaných kritických míst při jejichž ohrožení by došlo k nežádoucímu bezpečnostnímu jevu celého objektu. [14] [25]

Stejně jako metoda „What If„ je postavená na diskuzi expertů z různých oborů, kteří vytváří scénáře negativních jevů a jejich dopady. Na základě těchto scénářů následně vytvoří seznam doporučení vedoucí ke zlepšení systému či procesu. [14] [25]

3.4.5 Strom poruch (FTA)

Jedná se o metodu vyhledávající konkrétní poruchy na základě, kterých poté definuje, jak k těmto poruchám došlo. FTA je analýza, která graficky znázorňuje lidské chyby v kombinaci s haváriemi či technickými problémy zařízení, na základě které vznikne porucha celého systému. Metoda FTA tuto událost popisuje jako „vrcholovou“. [14] [23] [26]

Metoda je také vhodná pro rozsáhle systémy, kde může konkretizovat jednotlivé poruchové události, které nastaly. [14] [23] [26].



Obrázek 2: Strom poruch [14]

3.4.6 Metoda CARVER

Analytická metoda vyvinutá během války ve Vietnamu (1955-1975). Tato metoda byla využívána elitní jednotkou americké armády s názvem SEALs. [27] [28]

Metodu řadíme do kategorie metod, které mají za cíl posoudit zranitelnost zabezpečení. Tím myslíme posouzení hrozeb, slabin a pravděpodobnost možného útoku, který by mohl mít dopad na daný subjekt. [27] [28]

Cíl metody CARVER je nalezení a popsání kritických faktorů pro danou vojenskou misi. V běžném životě lze metodu použití pro stanovení faktorů, které jsou pro nás samotné důležité a na základě toho nasměrovat naše síly k dosažení cílů. [27] [28]

Analýza pracuje s následujícími faktory:

- **Criticality (důležitost)** – to, co je pro nás důležité k dosažení našich cílů,
- **Accessibility (přístupnost) –** dosažitelnost cíle.
- **Recognizability (rozpoznatelnost) –** obtížnost rozpoznání faktorů,
- **Vulnerability (zranitelnost)** – jak velké úsilí musím vydat k dosažení cíle,
- **Effect on the overall mission (celkový efekt na misi) –** vliv na celkový životní vývoj,

- **Return on effort (návratnost) –** návratnost úsilí a kdy se to stane (výsledky). [27] [28]

3.5 Aktuální hrozby měkkých cílů pro Českou republiku

Na základě zhoršující se bezpečnostní situaci (terorismus, extremismus) v Evropě, ale celkově ve světě narůstá počet útoků podobných terorismu (tyto útoky nejsou podníceny žádnou ideologií). Ovšem stejně jako teroristické útoky jsou zacíleny na měkké cíle a kladou si za úkol zranit osoby nacházející se v dané lokalitě. [12]

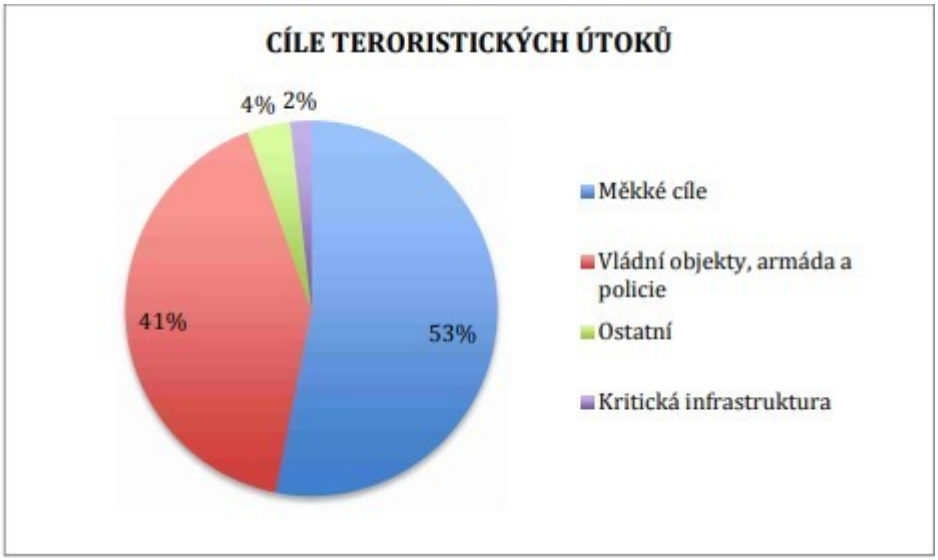
Teroristické útoky se na území České republiky ve smyslu práva jako takového nevyskytují. Jediný případ v novodobé historii České republiky, jenž byl spojen s teroristickým podnětem se týkal výhružného dopisu, který byl zaslán bývalému ministrovi financí. Odsouzena byla jedna osoba dle § 311 trestního zákoníku za teroristický útok. [12]

I když se teroristické útoky české republice v současné době vyhýbají, tak má již bohatou zkušenost s útoky s rasistickým či extrémistickým podnětem. Jako příklad je možné uvést útok, který proběhl v roce 2009 na dům obývaný romskou rodinou nebo útok na obchodní akademii (Žďár nad Sázavou), ve kterém žena pobodala studenty nacházející se v objektu (2014). Ovšem toto nejsou jediné příklady těchto útoku na našem území. Několik dalších útoků bylo uskutečněno a spoustu dalších útoků bylo překaženo nebo již zajištěno v přípravné fázi útoku. [12]

Díky tomu, jak jsou tyto útoky postaveny, tak převyšují možnosti potencionálně ohrožených subjektů se bránit (v rámci běžné kriminality). Jak můžeme vidět z výše zmíněných příkladů je nutné snažit se zamezit takovýmto útokům, jelikož jejich dopady mohou a mají ohromně škodlivé následky nejen na daný objekt, ale také na jeho široké okolí. [12]

V současnosti si útočníci vybírají právě cíle spadající do kategorie měkkých cílů. Z důvodu snadného přístupu k velkému počtu osob a nedostačující úrovně zabezpečení. Tato místa jsou vybírána náhodně, a to bez ohledu na to, jestli se jedná o místa nábožensky či politicky zaměřená. [12]

O tom, že se útočníci stále více zaměřují na cíle spadající do kategorie měkkých cílů poukazuje studie vytvořená Europolem, která vychází z počtu teroristických útoků, které proběhly v rozmezí let 1998-2014. Takovýchto útoků proběhlo 5 297. [12]



Obrázek 3: Cíle teroristických útoků [12]

Jak si můžeme povšimnou na Obrázku č.3 nejvíce napadané objekty jsou řazeny do kategorie měkkých cílů. [12]

3.5.1 Rozdělení aktuálních hrozeb

Kapitola pojednávající o současných hrozbách, které hrozí objektům definované jako měkké cíle. V současnosti můžeme říct, že mezi nejčastější hrozby můžeme považovat terorismus, organizovaný zločin, kybernetické útoky či extrémismus. V poslední době můžeme ovšem vnímat zvyšující se počet incidentů spojených s migraci národů či se současnou pandemií COVID-19.

Terorismus

Jedná se o formu útoku spojenou především s násilím při prosazování politických či náboženských ideologií určité skupiny lidí. V dnešní době se můžeme dočíst o spoustě možností, jak klasifikovat teroristické útoky, proto není jednoduché vybrat jedno rozdělení.

Pro naše účely můžeme využít rozdělené teroristických útoků dle police České republiky na několik kategorií:

- podle motivace: ultralevicový/pravicový, sociální, náboženský a další,
- podle metody útoku, která byla využita: kybernetický, chemický, jaderný a další. [12] [29] [30] [31]

Mezi typické příklady terorismu můžeme zařadit činy jako je únos letadla, atentát, sabotáž, ale také například dezinformační kampaně. [12] [29] [30] [31]

Po hrozivém teroristickém útoku ze dne 11. září 2001 se začal terorismus dostávat do podvědomí široké veřejnosti a jednotlivé státy a státní uskupení začali vytvářet bezpečnostní strategie a opatření vůči této „nové“ hrozbě. [12] [29] [30] [31]

Se současným vývojem technologií a bezpečnostních prostředků se musí aktéři terorismu neustále vyvíjet, hledají nové prostředky, způsoby a potencionální cíle na které, mohou zaměřit svůj útok. V současné době se teroristé zaměřují především na běžné obyvatelstvo, které se nachází ve volně dostupných prostorech tzv. měkkých cílech. [12] [29] [30] [31]

Organizovaný zločin

Za organizovaný zločin považujeme kriminální činnost, která je prováděna z pravidla organizovanými skupinami kriminálních živlů. Tyto skupiny jsou založeny na propracované organizační struktuře na základě, které mohou plánovat a provádět rozsáhlé a sofistikované kriminální činy. [32] [33]

V současné době považujeme organizovaný zločin za největší hrozbu (nevojenského charakteru) pro Českou republiku. Kriminální uskupení tohoto druhu se snaží svými činy narušovat strukturu společnosti, ekonomickou stabilitu státu, demokracii a v nejhorším možném případě může dojít až k samotnému zániku právního státu. Na základě těchto faktů je tato hrozba jednou z priorit bezpečnostních složek. [32] [33]

Česká republika v tomto ohledu každý den aktivně bojuje s organizovaným zločinem. V květnu 2018 vydala dokument s názvem „Koncepce boje proti organizovaného zločinu do roku 2023“. Dokument popisuje hrozby a také nástroje, které bezpečnostní složky využívají k boji proti organizovanému zločinu. [32] [33]

Součástí boje proti organizovanému zločinu je také působení republiky na mezinárodní půdě. Uskupení páchající zločiny, které můžeme klasifikovat jako organizovaný zločin většinou nejsou pouze na národní úrovni (takové případy jsou ojedinělé), ale jsou z velké části založeny na mezinárodních vztazích od přepravy zboží po samotnou distribuci. Česká republika je členem několika evropských a světových uskupení bojujících právě proti organizovanému zločinu. [32] [33]

Kybernetické útoky

V současné době, kdy jsou naše životy propojeny s informačními technologiemi si musíme uvědomit, že tyto technologie nám nepřináší pouze výhody, ale nesou s sebou také obří bezpečnostní hrozby. Tento typ útoku můžeme klasifikovat jako nejmladší, ale díky jeho

velkému rozmachu, právě díky digitálním technologiím, za jeden z největších současné doby. [33] [34]

V současnosti se kybernetický prostor stal lákavým místem pro zločin, a to především díky anonymitě, která se aktérům kriminality nabízí. Na základě toho se spoustu kriminální činnosti přesunuje do kybernetického prostoru. [33] [34]

Útoky, které můžeme klasifikovat jako informační (kybernetické) mají nejrůznější podoby od malých podvodů na uživatele přes šíření copyrightového obsahu, šíření pornografie, kybernetickou šikanu až po sofistikované e-špionáže, praní špinavých peněz či podporu terorismu nebo navádění k extrémistickým činům. [33] [34]

Mezi největší kybernetické hrozby můžeme zařadit útoky, které nesou název „Advanced Persistent Threat“ neboli zkráceně ATP. Mezi charakteristické znaky takovéhoto útoku patří například jeho sofistikovanost, perfektní zaměření na určitou věc, jeho schopnost napadat také „offline systémy“ a cena. Dalším charakteristickým znakem je, že proti nim nefungují běžné ochrany (antivirový program). [33] [34]

Mezi metody nejen právě ATP útoků, ale také běžných kybernetických útoků řadíme například metody sociálního inženýrství („phishingové kampaně“), zero-day exploits (sofistikované viry) či malware. [33] [34]

Mezi nejznámější a největší kybernetické útoky patří například Operace Aurora, ransomwarový útok WannaCry či e-špionážní kampaň nesoucí název Blue Termite.

V ochraně proti kybernetickým útokům hraje důležitou roli stát, který by měl chránit občany, proti tomuto novému typu hrozeb, ovšem měli bychom brát na vědomí, že každý z nás ručí za svou bezpečnost v kybernetickém prostoru sám. [33] [34]

Extrémismus

Jedná se o formu hrozby založené na idealistických postojích odporujících ústavním a právním nařízením. Jedním z předních charakteristických prvků je netolerance demokratických principů. [33] [35] [36]

Extrémismus není právně definován, ale je spojen s rasově zaměřenou kriminalitou. Můžeme ovšem narazit také na pojmy jako jsou extremistická činnost, zločiny s extrémistickým podtextem, rasová či národní nenávist a další. Ovšem patří zde také útoky proti náboženství, symbolům či systému. [33] [35] [36]

Ve skutečnosti se jedná především o trestné činy jako jsou například: vydírání, hanobení národa, vražda, obecné ohrožení, omezení osobní svobody a další. [33] [35] [36]

Dle Ministerstva vnitra České republiky spočívá skutečná hrozba extrémismu v následujících bodech (je nutné zmínit, že ne všechny body jsou spjaty se všemi typy extrémismu):

- oslabení demokracie, která může vést až k jejímu zániku,
- odpor vůči respektu základních lidských práv a svobod,
- rozpoutání teroru,
- narušení veřejného pořádku,
- vedou k násilným činům z nenávisti,
- cílené šíření strachu mezi zbytkem populace,
- urážení obětí totalitních režimů a extrémismu,
- své ideologie propagují populisticky a prognosticky,
- boj proti extrémistickým akcím je finančně náročný,
- kazí jméno České republiky. [37]

Tato kapitola popisuje proces analýzy rizik od samotné identifikace až po metody stanovení rizika. Následně byly popsány jednotlivé metody analýzy rizik jako jsou například metoda Carver, Strom poruch, Kontrolní listy, HAZOP a další.

V poslední části jsou popsány aktuální hrozby měkkých cílů pro českou republiku jako jsou například kybernetické útoky, terorismus, extremismus a další.

4 BEZPEČNOST MĚKKÝCH CÍLŮ

Měkké cíle jsou díky své definici velice rozsáhlou a různorodou kategorií. Na základě různých rozdělení uvedených v kapitole 2.1 Rozdělení měkkých cílů je možné specifikovat, které principy, opatření využít a kam přesně cílit ochranné prvky. [10] [11] [12] [38]

Dle bezpečnostní teorie na základě, které definujeme potřebná bezpečnostní opatření je nutné provést následující kroky nezbytné k vytvoření funkčního bezpečnostního systému:

- **Co je předmětem ochrany?** – Definování toho, co chceme chránit. Zájmem ochrany může být od věcného majetku přes lidské životy až po informace.
- **Kdo je hrozbou? Před kým se chráníme? –** Následně je nutné identifikovat a popsat možné zdroje hrozby jako jsou například skupiny potencionálně nechtěných a nebezpečných a další. K identifikaci takovýchto skupin je možné využít retrospektivní pohled na historické útoky.
- **Jaké metody využije útočník při napadení měkkého cíle?** – Identifikace metod napadení je možné popsat dle charakteristik jednotlivých měkkých cílů.
- **Analýza rizik.** – Analýza potencionálních budoucích rizik (této problematice se věnuje kapitola 3 Analýza rizik a její metody).
- **Metody a strategie zabezpečení.** – Definice postupů a strategií pro prevenci před útoky, co dělat, když dojde k útoku a jak minimalizovat jeho škody.
- **Vymezení bezpečnostních opatření. –** Popis toho jak a kde budou aplikované jednotlivé bezpečnostní prvky a pravidla.
- **Managment bezpečnostního týmu a samotného objektu.** [10] [11] [12] [38]

Zajištění bezpečnosti měkkého cíle je možné rozdělit do tří základních časových úseků, a to před útokem, během útoku a po útoku. [10] [11] [12] [38]

Obrázek 4: Časové úseky zabezpečení měkkého cíle [12]

- **Před útokem (incidentem) –** tato fáze je zaměřená především na preventivní opatření, která vedou k efektivnímu zakročení při možném incidentu. Využívají se zde takzvané „nástroje odstrašení“ (nástroje s odstrašujícím charakterem pro odrazení útočníka). [11] [12]
- **Během útoku (incidentu) –** fáze zaměřená na co nejrychlejší detekci a následnou reakci bezpečnostních pracovníku na narušení bezpečnosti. [11] [12]
- **Po útoku (incidentu) –** poslední fáze se zaměřuje na zmírnění dopadů za využití předpřipraveného koordinačního plánu. [11] [12]

4.1 Bezpečnostní diagnostika měkkých cílů

V předchozích kapitolách byly popsány vybrané metody klasifikace měkkých cílů. Ovšem k tomu, abychom byli schopni správně a efektivně vybrat vhodné bezpečnostní řešení je nutné zvolit individuální přístup ke každému měkkému cíli [12]

Je nutné se tedy podívat na dva určující faktory ovlivňující bezpečnost:

- atraktivita cíle z pohledu útočníky,
- možnosti zabezpečení cíle [12]

Atraktivita cíle z pohledu útočníka

- **Otevřenost pro veřejnost –** může se jednat jak o venkovní prostory, uzavřený objekt nebo objekt do kterého je umožněn volný přístup. Čím větší otevřenost daného prostoru, tím se zvyšuje atraktivita pro útočníky. [12]

- **Zaměstnanci zajišťující bezpečnost –** pokud se na místě vyskytuje soukromá společnost či zaměstnanci zajišťující bezpečnost, tak se atraktivita cíle pro útočníka výrazně snižuje. [12]
- **Množství a koncentrace osob –** jedná se o dva nejdůležitější faktory z pohledu útočníka. Čím větší množství a koncentrace osob na jednom místě, tím větší pravděpodobnost, že to přiláká potencionální útočníky. [12]
- **Přítomnost policie –** přítomnost policie výrazně snižuje atraktivitu cíle. Pokud se na místě trvale vyskytuje policie tak už objekt nepovažujeme za měkký cíl. Ve většině případů je výskyt policejních složek dočasný. [12]
- **Přítomnost médií –** na základě toho, že většina útočníků vyhledává pozornost je přítomnost jakýchkoliv médií v objektu měkkého cíle riskantní a musí se brát v potaz při jeho zabezpečení. [12]
- **Symboličnost –** jedná se o faktor, který je z pohledu jak teroristické skupiny, tak z pohledu jiné násilné skupiny velice důležitý. V české republice se můžeme převážně setkat s nenávistí například vůči romské menšině či určitému druhů náboženství. Většina takovýchto útočníku chce svým činem upozornit na problémy, které vnímají na základě svého přesvědčení jako klíčové pro fungování společnosti. [12]

Možnosti zabezpečení cíle

- **Organizační struktura –** k tomu, aby bezpečnost v objektu fungovala tak jak má, je důležité zvolit vhodnou organizační strukturu zajišťující bezpečnost měkkého cíle. Tato problematika se především týká objektů s více vlastnickou strukturou jako jsou například obchodní centra. Zde je důležitá koordinace jednotlivých vlastníků k zajištění bezpečnosti objektu. [12]
- **Zdroje a prostředky na bezpečnost –** důležitým faktorem zabezpečení měkkých cílů jsou zdroje, které jsou poskytnuty na vytvoření bezpečného prostoru v oblasti měkkých cílů. Za to, jakým způsobem bude nastavena ochrana objektu zodpovídá bezpečnostní manažer, nebo osoba pověřená k zajištění ochrany.
- **Schopnost identifikace vlastních rizikových situací –** na základě tohoto faktoru, můžeme zjistit, zda veškerá bezpečnostní rizika objektu a schopnost reagovat na hrozby, kterým můžeme čelit je optimální. [12]

K tomu, aby každý měkký cíl byl připraven na případné hrozby je silně doporučeno, aby byla vytvořena na základě výše zmíněných faktorů SWOT analýza k odhalení slabých a silných stránek, příležitostí a hrozeb. [12]

4.2 Bezpečnostní prvky a jejich využití při ochraně měkkých cílů

Pro optimální zabezpečení měkkých cílů je kritickým faktorem správné využití a zvolení bezpečnostních prvků. Tyto bezpečnostní prvky spadají do kategorie takzvané fyzické bezpečnosti, která se následně dělí na systémy technické ochrany (STO), fyzické ochrany a režimových opatření. STO následně můžeme rozdělit na elektronické prvky (systémy) a mechanické zábranné prvky (systémy). [10] [11] [12] [38]

Pro zabezpečení měkkých cílů je nutné kombinovat tyto kategorie. Například při využívání elektronických prvků jako jsou kamerové systémy je naprostá nutnost mít odborný personál, který ví, jak s nimi pracovat. [10] [11] [12] [38]

4.2.1 Fyzická ochrana

Jedná se o část fyzické bezpečnosti, která má své nenahraditelné místo v procesu zabezpečení měkkých cílů. Většinou se setkáme s fyzickou ochranou ve formě hlídací služby. Ovšem fyzickou ochranou nemusíme myslet pouze zaměstnance bezpečnostní služby, ale také běžný personál. [10] [11] [12] [38]

Bezpečnostní pracovníci

Pracovníci, kteří zajišťují kontroly při vstupu a výstupu do objektu, provádí kontrolní činnost na bázi pochůzek a obsluhují bezpečnostní technologie v takzvaných velínech. O bezpečnostních pracovnících je možné říct, že jsou jedním s nejefektivnějším způsobem ochrany. Správně vyškolený bezpečnostní pracovník nejenže funguje jako odstrašující prvek, ale také dokáže rozpoznat bezpečností riziko, vyhodnotit jej a efektivně zakročit. Proto, aby byli bezpečnostní pracovníci co nejefektivnější, měli by pracovat podle předepsaných řešení. Důležitou věcí je také pravidelné školení těchto pracovníků a to především v oblasti komunikace a asertivního přístupu. [10] [11] [12] [38]

Ostatní personál

Do této kategorie spadají běžní zaměstnanci pracující v objektu. Je nutné, aby i běžní zaměstnanci prošli školením nebo jinou edukací, jak se chovat při situaci ohrožující jejich bezpečnost nebo bezpečnost daného měkkého cíle. Ve spoustě případech se nenachází

na blízku žádný bezpečnostní pracovník a z toho důvodu je nutné, aby věděli jak se ve vybraných situacích chovat. [10] [11] [12] [38]

4.2.2 Režimová opatření

Režimová opatření představují souhrn postupu a pravidel pro vstup do dané chráněné oblasti. Tato opatření především slouží k zamezení vstupu nechtěných a potencionálně nebezpečných osob, ale také k tomu, aby do zabezpečené zóny nebyly proneseny věci jako jsou zbraně či jiný škodlivý materiál [10] [11] [12] [38]

Režimovou ochranu je možné rozdělit na dvě skupiny, a to využití technických prvků, které slouží k zabezpečení (turnikety, ploty atd..) a prvky ochrany netechnického charakteru, kterou splňují zaměstnanci, kteří mají na starost bezpečnost vybrané lokality. [10] [11] [12] [38]

4.2.3 Systémy technické ochrany

Jak již bylo zmíněno STO dělíme na dvě kategorie, a to elektronické prvky (systémy) a mechanické zábranné prvky (systémy). Tyto systémy mají zá úkol především detekovat a bránit ve vstupu do objektu měkkého cíle nechtěným a potencionálně problémovým jedincům. Tyto systémy je nutné vybírat na základě charakteristiky konkrétního měkkého cíle. Například jejich aplikace v otevřených prostorech je značně problematická a některé prvky těchto systémů jsou v takovýchto prostorech prakticky nevyužitelné. [10] [11] [12] [38]

Jak již z názvu vyplývá, mechanické zábranné systémy slouží k zamezení vstupu do objektu nepovoleným osobám. Mezi takovéto systémy můžeme zařadit bezpečnostní dveře a okna, ploty, turnikety, sloupky a betonové bloky. [10] [11] [12] [38]

Mezi elektronické systémy můžeme zařadit:

Kamerové systémy (CCTV)

systém prvků sloužící k monitorování prostorů měkkých cílů. Tyto systémy obsluhuje speciální proškolený personál. Vybrané kamerové systémy také obsahují nejrůznější analytické funkce na základě, kterých je možné například rozpoznání obličejů či podezřelé aktivity. [10] [11] [12] [38]

Dohledové zabezpečovací tísňové systémy (PZTS)

Systém prvků sloužící převážně k detekci nepovoleného či násilného vstupu do objektu. Tyto systémy je možné rozdělit na perimetrické, plášťové, prostorové a předmětové. Například se může jednat o detektory pohybu, otevření dveří a další. Tyto prvky vysílají signály, které jsou většinou svedeny do centrály, která má za úkol informovat pověřenou osobu. [10] [11] [12] [38]

Dohledové a poplachové přijímací centrum (PCO)

V praxi se jedná o středisko, ve kterém se nachází centrální dispečer, který disponuje možnostmi sběru informací z různých objektů a také dálkovým ovládáním jednotlivých prvků bezpečnosti. [10] [11] [12] [38]

Mezi další prvky elektronických systému řadíme například vnitřní rozhlas, rentgen, detektory kovů a výbušnin, přístupové docházkové systémy, čtečky dokladů, osvětlení a systémy šíření varování (mobilní aplikace, SMS brány aj.). [10] [11] [12] [38]

4.3 Role běžného občana při zabezpečení měkkých cílů

Problematika zabezpečení měkkých cílů je téma, které řeší nespočet uznávaných odborníků na celém světě. Na základě toho, jak široké spektrum subjektů je definováno jako měkký cíl není možné využít jednotný systém zabezpečení pro všechny. Odborníci proto spekulují nad tím, jaká je ta správná forma zabezpečení. [11]

Jednou z forem obrany měkkých cílů je jejich vlastní obranyschopnost. Jedním z hlavních faktorů měkkého cíle je velký počet civilních (nezúčastněných) osob. A právě tato skupina lidí se může stát efektivní formou obrany daného subjektu. [11]

Když hovoříme o zapojení běžného obyvatelstva do ochrany měkkých cílů, hovoříme o takzvané sdílené bezpečnosti. Tedy je to spolupráce běžného občana s bezpečnostními složkami, která je založená na aktivním přístupu, komunikaci, sdílení jednotlivých podnětů a všeobecném povědomí okolního dění. Na základě tohoto přístupu je možné zefektivnit stávající prvky zabezpečení a zajistit bezpečnost nejen pro sebe, ale také pro nejbližší okolí.

Tato kapitola byla věnována bezpečnosti měkkých cílů. V první části byly popsány kroky, které jsou nezbytné k vytvoření funkčního bezpečnostního systému mezi, které patří například analýza rizik či otázka „Co je předmětem hrozby?“.

Druhá část popisuje jednotlivé kategorie bezpečnostních prvků (fyzická ochrana, režimová opatření a STO). Dále jsou zde také popsány vybrané bezpečnostní prvky. Poslední část kapitoly popisuje podceňovaný faktor zabezpečení měkkých cílů, a to je zapojení běžného občana při zabezpečení měkkých cílů (sdílená bezpečnost).

5 INFORMAČNÍ A MODELOVÁ PODPORA OCHRANY MĚKKÝCH CÍLŮ

Jedná se o softwarový nástroj vyvinutý českou společnosti T-Soft a.s. a je určen pro pohotový odhad dopadů teroristických útoků, havárií, úniku nebezpečných látek či útoku jadernými, chemickými či biologickými zbraněmi. [39]

Své primární využití má v oblasti teroristických a vojenských útoků. Je využíván složkami IZS. Své uplatnění ovšem nachází také při analýzách územního plánování, pojišťovnictví, či navrhování zástavby. [39]

Velkou výhodou tohoto softwaru je, že dokáže poskytnout výsledky i při vložení neúplných či nepřesných informací. Výsledek vyhodnocování pomocí TerEXu odpovídá podmínkám, které počítají s nejhorší možnou variantou dopadu. [39]

Funkce softwaru je založená na několika základních modelech představujících nebezpečné událostí, od nejrůznějších variant průmyslových havárií až po teroristické útoky. Dále je možné si vybrat již z předem vytvořeného seznamu nejrůznějších nebezpečných látek (pokud se vámi požadovaná látka nenachází v databázi, je možné jí do programu vložit). [39]

Mezi tyto modely můžeme zařadit:

- **Modely nebezpečných chemických látek**
    - **TOXI** – znázorňuje dosah a tvar oblaku vycházející z koncentrace toxické látky.
    - **UVCE** – model založený na působení vzdušné rázové vlny (kontakt látky se vzduchem – detonace).
    - **PLUME** – jedná se o model pracující s déletrvajícím únikem plynu do oblak.
    - **PUFF** – podobný jako model PLUME pouze s tím rozdílem, že se jedná o jednorázový incident.
    - **FLASH FIRE** – velikost prostoru ohrožení osob plamennou zónou. [39]
- **Výbušné systémy**
    - **EXPLOSIVE** – dopady při výbuchu, zobrazuje také zónu, která je ohrožena možným výbuchem.

- **Otravné látky** [39]

Jak již bylo zmíněno TerEX vyniká právě v rychlosti a díky funkci „průvodce pro rychlý odhad“ také snadné využití pro kohokoliv i bez hlubší znalosti problematiky. Další výhodou je možnost porovnání naší události již se známými událostmi, které se odehrály v minulosti. [39]

Jako poslední funkcí tohoto teroristického Experta je geografický informační systém, který nám umožňuje zobrazit výsledky naší modelové situace přímo na mapách. Je možné připojit modul využívající lokální geografická data, mapový server, server Státního mapového centra, nebo možné využití Google map k určování rozsahu havárie či teroristického útoku. [39]

Kapitola je zaměřena na popis softwarového nástroje od společnosti T-Soft a.s., který slouží k simulaci teroristických útoků, havárií, úniku nebezpečných látek či útoku jadernými, chemickými či biologickými zbraněmi.

Následně se kapitola věnovala popisu jednotlivých modelů, které jsou obsaženy v tomto softwarovém nástroji.

ZÁVĚR TEORETICKÉ ČÁSTI

První kapitola teoretické části diplomové práce byla zaměřena na přiblížení relevantních zákonů a jejich paragrafy, které jsou spjaty s problematikou měkkých cílů v České republice. Jedná se například o trestní zákoník či zákon o krizovém řízení aj. Následně kapitola popisuje příslušné normy PKB a také návrh zákona o soukromých bezpečnostních službách. Nakonec se kapitola věnuje absenci legislativy v oblasti měkkých cílů.

Další kapitola pojednává o definici pojmu měkký cíl a jeho rozdíl oproti cílům tvrdým, také byly popsány jednotlivé klíče, podle kterých je možné měkké cíle rozdělit. V závěru kapitoly byl popsány základní pilíře zabezpečení měkkých cílů z pohledu vlády České republiky.

Následně byl čtenář seznámen s pojmem analýza rizik na základě, kterého je možné identifikovat, stanovit, ohodnotit, a nakonec vytvořit opatření pro jednotlivé hrozby. Velká část kapitoly je zaměřena na popis jednotlivých metod, které jsou využívány při samotné analýze rizik. Jedná se například o metodu Carver či kontrolní seznamy. Poslední část byla věnována aktuálním hrozbám měkkým cílům pro Českou republiku, a to zejména terorismus, extremismus, organizovaný zločin či kybernetické útoky.

V předposlední kapitole byl čtenář seznámen s bezpečností měkkých cílů, se základními principy a východisky při jejich diagnostice a zabezpečení. Poté byly zevrubně popsány bezpečnostní prvky sloužící k zajištění ochrany měkkých cílů a jejich základní dělení na fyzickou ochranu, režimová opatření a STO. Nakonec se kapitola věnovala krátkému popisu role běžného občana při zajišťování obrany měkkých cílů neboli principu sdílené bezpečnosti.

Poslední kapitola teoretické části kapitola představuje možnosti informační a modelové podpory ochrany měkkých cílů, a to konkrétně softwarový nástroj TerEX, které slouží k simulaci útoků na zájmový subjekt.

II. PRAKTICKÁ ČÁST

6 PROFIL MĚKKÉHO CÍLE (ADMINISTRATIVNÍ CENTRUM)

Prvním bodem praktické části je popis vybraného administrativního centra a jeho okolí. Pod pojmem administrativní centrum myslíme budovu nebo komplex budov, který primárně slouží k poskytování kancelářských prostor veřejným nebo státním subjektům. Centra je možné rozdělit do dvou kategorií, a to s jedním nájemcem (případ, kdy má celý administrativní komplex pronajatý jeden subjekt) a s několika nájemci (administrativní komplex je pronajat vícero nájemci). Majitel takového administrativního centra na základě smlouvy o pronájmu zajišťuje bezpečnost a chod celého komplexu (čím více nájemců, tím víc se zvyšují bezpečnostní nároky).

Pro účely této diplomové práce bylo vybráno administrativní centrum ABC Alfa, které je součástí komplexu tří administrativních budov (Alfa, Beta a Gama) ABC (Asental Business Center) od společnosti Asental Group. Komplex se nachází v Ostravě přesněji v městské části Přívoz na adrese Prokšovo náměstí 2020/6. [40] [41]

Historie budovy sahá až do roku 1938 kdy byla zahájena výstavba dle projektu architekta Karla Kotase, který měl za úkol postavit objekt pro generální ředitelství Severní dráhy a následně OKD a.s.. Celý projekt byl dokončen v roce 1940. Objekt obsahuje několik historicky významných děl jako jsou například vitráže Jana Baucha, fresky na fasádě nebo unikátní oběžný výtah páternoster. V roce 2016 prošla administrační budova komplexní rekonstrukcí díky které obsadila třetí místo v soutěži nejlepší realitní projekt za rok 2017. [40] [41]

6.1 Popis objektu a jeho okolí

Administrační budova je součástí velkého budovního celku, který tvoří takzvaný blok. Část, ve které je lokalizováno námi vybrané administrativní centrum se nachází na východní straně budovního celku a disponuje šesti nadzemními patry a suterénem. V prostorech před vchodem do budovy se nachází bezbariérový přístup v podobě výtahu a parkoviště určené pro zaměstnance firem, které využívají prostory administrativního centra ABC Alfa a Gama. Parkoviště obsahuje přibližně třicet parkovacích míst a je vybaveno závorami kontrolujícími vjezd a výjezd z parkoviště.

Obrázek 5: Administrativní centrum ABC Alfa [42]

6.1.1 Popis vnitřních prostor budovy

Jak již bylo zmíněno budova se skládá z šesti nadzemních pater a suterénu, který slouží jako technické zázemí a sklad budovy. Celková pronajímatelná plocha budovy je 6 000 m^2. [41]

První patro (přízemí)

V přízemí administračního centra se nachází veřejně dostupná vstupní hala, která je rozdělená na odpočinkovou zónu vybavenou několika křesly a gauči, recepci, kuchyňku se základním kuchyňským vybavením a schodištěm do suterénu.

Obrázek 6: Recepce administrativní budovy ABC Alfa [41]

Další část přízemí se nachází za turnikety. Tato část je přístupná pouze zaměstnancům či osobám, kterým je umožněn vstup (například klienti jednotlivých firem). V této části se nachází toalety dámské, pánské a pro hendikepované, schodiště do vyšších nadzemních pater, osobní a historický oběžný výtah páternoster.

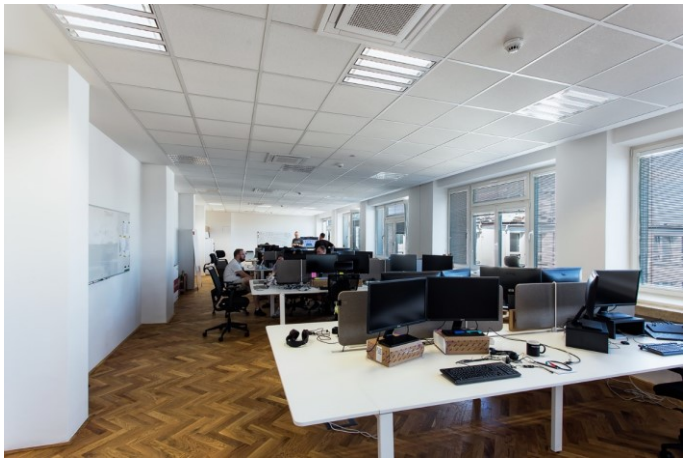
Obrázek 7: Vstupní hala administračního centra ABC Alfa [41]

Suterén

Před vstupem do suterénu se nachází mezipatro (mezi přízemním patrem a suterénem), na kterém je velký konferenční sál, který v současné době slouží jako skladiště. Samotný suterén je jediný prostor budovy, který nebyl zrekonstruován a nachází se zde technické zázemí budovy, sprchy a úschovna kol.

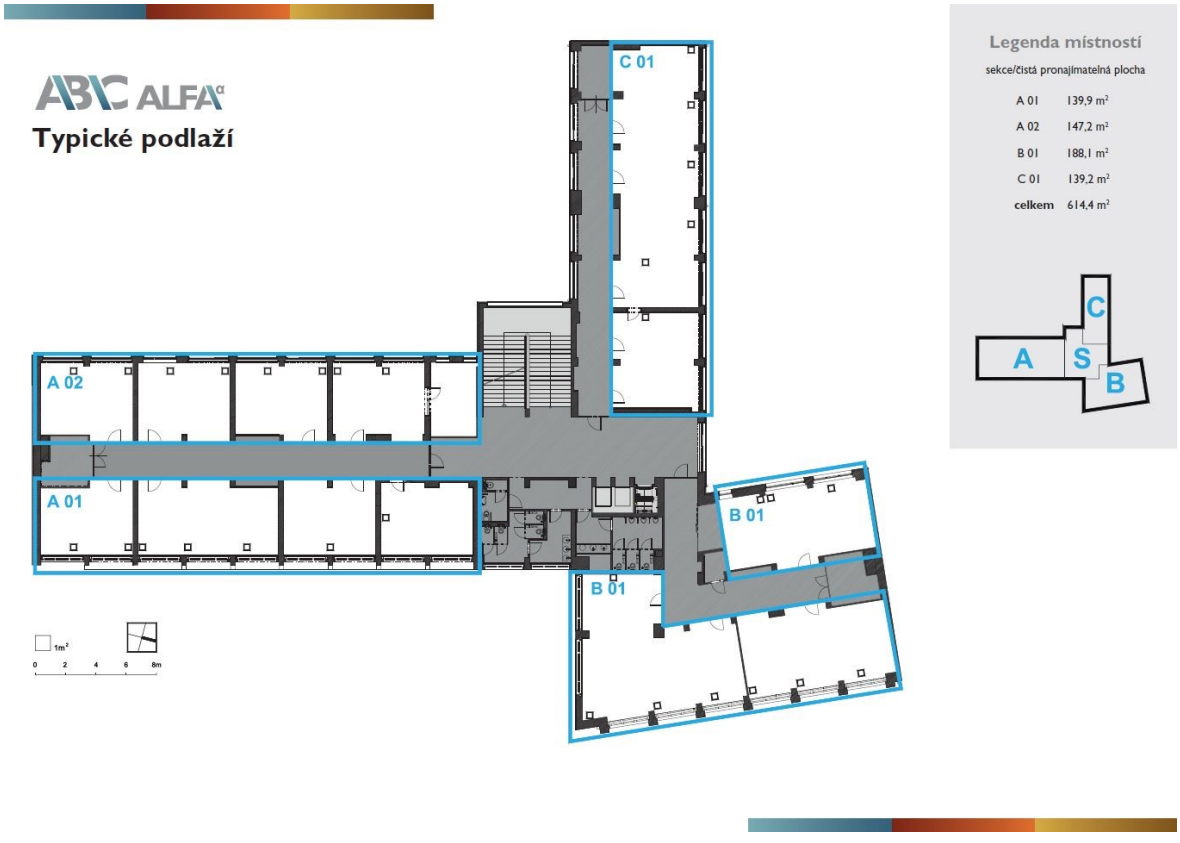
Druhé až šesté patro

Další nadzemní podlaží budovy jsou rozloženy totožně a skládají ze tří kancelářských komplexů, které jsou rozděleny na jednotlivé kancelářské bloky, chodbu a malou kuchyni obsahující základní kuchyňské vybavení.



Obrázek 8: Ukázková kancelář administračního centra ABC Alfa [41]

Dále se na každém patře nachází schodiště, osobní výtah a historický výtah, hala, místnost pro úklid a sociální zařízení pro dámy, pány a hendikepované, která jsou sdílena pro všechny nájemníky budovy.



Obrázek 9: Typické podlaží administrativního centra ABC Alfa [41]

6.1.2 Popis blízkého okolí administračního centra

Administrativní budova se nachází kousek od centra Ostravy v městské části Přívoz. Budova je napojena na dvě další budovy administrativního komplexu ABC. První touto

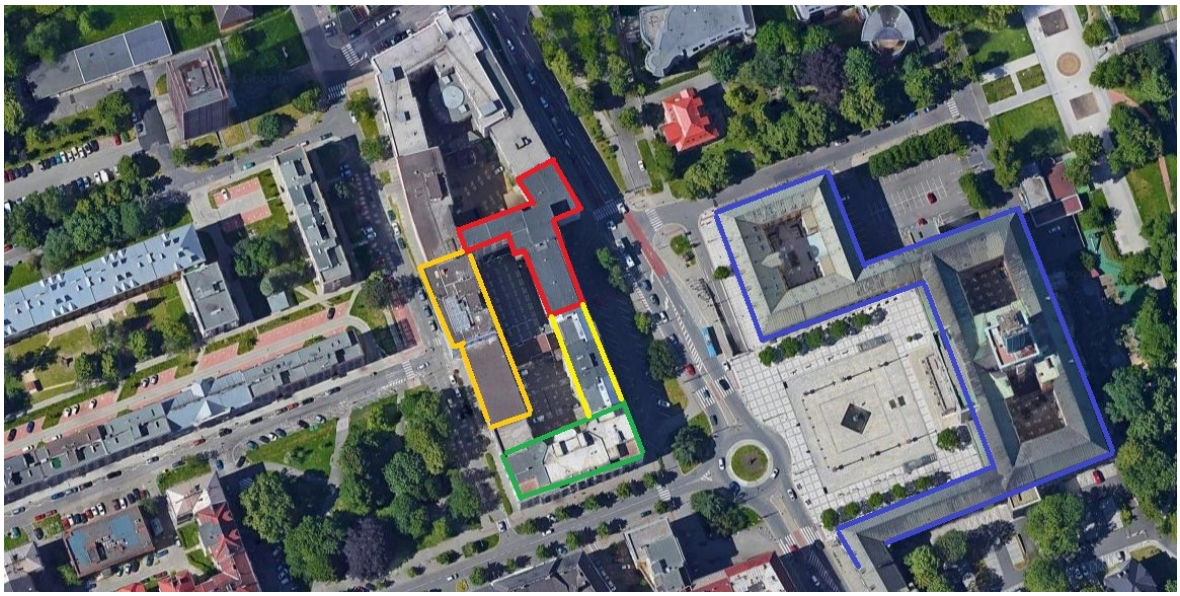
budovou je Gama, která je napojená v přízemním patře a nachází se v ní především zahraniční jazyková škola. Druhá budova s názvem Beta je propojená v posledním patře s budovou Alfa a nachází se v ní několik soukromých subjektů.

Dalším subjektem sídlícím v budovním celku je Magistrát města Ostravy a jeho odbor dopravně správních činností. Magistrát není součástí administrativního komplexu, ale je součástí budovního celku.

Kolem celého administrativního komplexu vede pozemní komunikace (cesta) na které, se nachází kruhový objezd, křižovatky a také zastávky hromadné městské dopravy (tramvaj, autobus, trolejbus).

Naproti administrativního komplexu ABC se nachází radniční budova města Ostravy, jehož součástí je také vyhlídková věž a Prokšovo náměstí. Jak již bylo zmíněno mezi těmito dvěma objekty stojí cesta a kruhový objezd.

Dále se v blízkosti objektu ABC nachází řeka Ostravice (za radniční budovou), malé kamenné prodejny, panelové domy, bytovky a park.



Obrázek 10: Mapa okolí administračního centra ABC Alfa [43] - upraveno

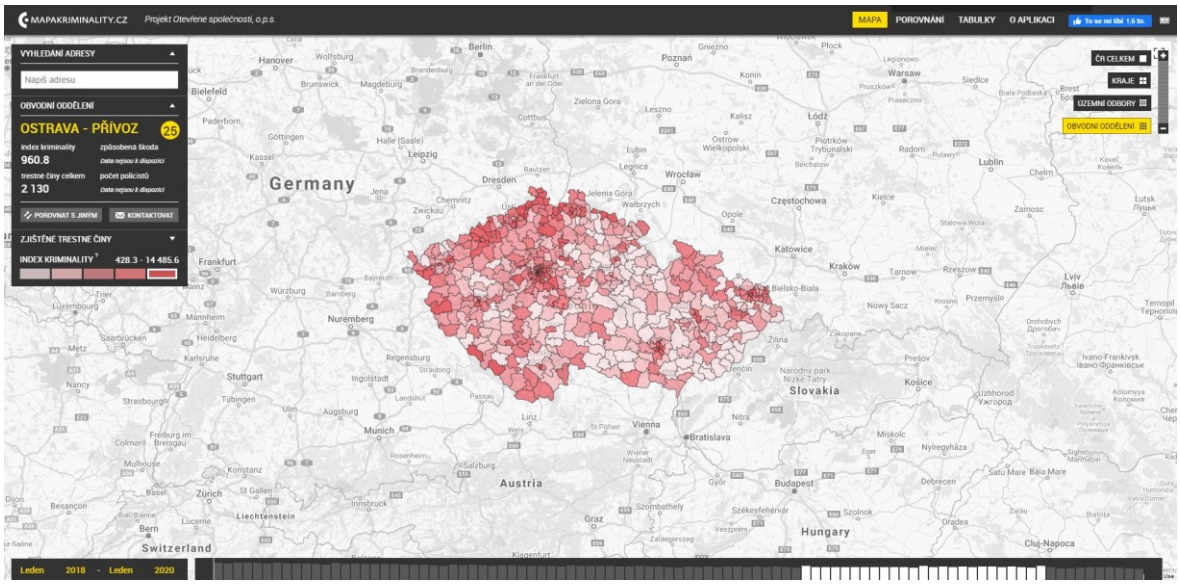
Tabulka 2: Legenda mapy okolí administračního centra ABC Alfa [Zdroj: Vlastní]

	Název
	Administrační centrum ABC Alfa
	Administrační centrum ABC Gama
	Administrační centrum ABC Beta
	Magistrát města Ostrava
	Radniční budova města Ostrava

6.2 Bezpečnost objektu a blízkého okolí

K tomu, abychom mohli dostatečně posoudit bezpečnost námi vybraného objektu je nutné analyzovat bezpečnostní situaci v přilehlém okolí. Toho bylo docíleno za využití webového portálů www.mapakriminality.cz, na kterém jsou zveřejněna data o trestných činech

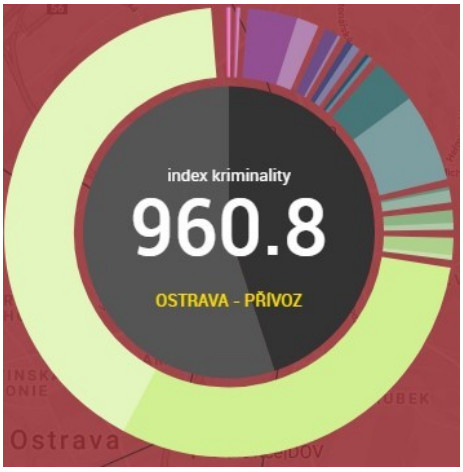
(data na stránce jsou pravidelně aktualizovány Policí ČR). Pro účely diplomové práce byla vyfiltrována data o trestných činech na území města Ostravy a její městské části Přívoz a to od 1. ledna 2018 do 1. ledna 2020 (období před pandemií COVID-19).



Obrázek 11: Webový portál www.mapakriminality.cz [44]

V námi zvoleném období se v městské části Ostrava Přívoz odehrálo 2 130 trestných činů. Na základě těchto údajů je index kriminality (dle webového portálu mapakriminality.cz)

městské části Přívoz 960,8 a je na 25 místě s největším výskytem kriminálních jevů v České republice. Index kriminality je stanoven na základě zjištěných skutků za určité období přepočteny na 10 000 obyvatel. [44]



Obrázek 12: Index kriminality
v městské části Ostrav Přívoz [44]

Mezi největší kategorie pro nás relevantních trestných činů můžeme zařadit prosté krádeže, kterých bylo zjištěno 871. Prostými krádežemi máme na mysli například kapesní krádeže či drobné krádeže v objektech. [44]

Další kategorií jsou krádeže vloupáním (245), tato kategorie je popsána jako krádeže, při kterých se pachatel musel vloupat do objektu. [44]

Poslední kategorií jsou činy násilné (148), do kterých například spadají fyzické útoky či krádeže věcí z automobilu. [44]

Dalším faktorem, který zvyšuje bezpečnostní hrozbu pro administrativní centra je přítomnost důležitých státních institucí jako jsou například magistráty, radnice atd. nebo symbolicky významných míst například kostely, památky atd..

V případě námi zvoleného objektu administračního centra ABC Alfa se v blízkém okolí nachází velké množství významných či symbolických míst. Mezi největší a nejdůležitější místa patří především Magistrát města Ostravy, který je lokalizovaný ve stejném budovním celku jako náš objekt, Radniční budova města Ostravy, která se nachází naproti naší budovy, školy, náměstí (součást radniční budovy) a také zastávky městské hromadné dopravy.

Na základě těchto faktů stoupá v očích potencionálního útočníka atraktivita námi zvoleného administrativního komplexu.

6.2.1 Bezpečnostní opatření administrativního centra ABC Alfa

Samotná budova ABC alfa je vybavená řadou bezpečnostních prvků a opatření. V objektu se CCTV, PZTS, kartový vstupní systém, požárně bezpečnostní systémy a fyzická ochrana. [41]

Parkoviště

Parkoviště, které je lokalizováno před vchodem do administračního centra ABC Alfa je vybaveno závorami, které lze otevřít pouze zaměstnaneckou kartou nebo po domluvě na recepci budovy. Prostor parkoviště je monitorován bezpečnostními kamerami, které jsou umístěny před vchodem a na fasádě administrativního centra.

První patro (přízemí)

Před tím, než je možné vstoupit do samotné budovy je nutné projít přes hlavní vchod kde jsou umístěny elektronické posuvné dveře, které jsou otevřené pouze v určité hodiny. K tomu, aby bylo možné vstoupit do budovy mimo tyto hodiny je nutné mít zaměstnaneckou kartu. V oblasti hlavního chodu se nacházejí prvky PZTS (detektory pohybu Passive Infrared Detctor (PIR)) a kamera monitorující situaci před vchodem.

Obrázek 13: Vstup do objektu [45]

Po vstupu do přízemní části budovy je možné si povšimnou recepce, ve které jsou vyvedeny všechny bezpečnostní prvky. Na recepci je přítomen zaměstnanec (recepční) společnosti Asental Group (recepční je přítomna v průběhu celého dne) a příslušník bezpečnostní agentury, který je přítomen vybranou část dne.

Další bezpečnostní prvek se nachází po pravé straně od recepce. Jedná se o zábradlí a turniket oddělující veřejně dostupnou část budovy a část určenou pouze pro zaměstnance či případné

návštěvníky s povolením. K tomu, aby bylo možné projít přes turniket je nutné vlastnit zaměstnaneckou kartu, nebo po sjednání schůzky.

Vstupní hala budovy je pod dohledem kamerového systému, dále se zde nachází prvky PZTS jako je například PIR senzor či ovladač PZTS ústředny. Na stropu jsou také umístěny kouřové detektory.

Obrázek 14: Turniket [46]

Suterén

Jak je možné vidět na Obrázku 14 tak schody vedoucí do suterénu se nacházejí mezi recepcí a turniketem. Zde se nacházejí místnosti, do kterých je přístup pouze na základě držení karet pro správce budovy.

Okna suterénu, která je možné vidět na Obrázku 13 jsou zabezpečeny mřížemi, které zabraňují vstupu neoprávněných osob při případném pokusu o vloupání.

Nadzemní patra (2-6 patro)

Po průchodu turniketem se dostáváme do části budovy, která je určena pouze zaměstnancům či případným hostům. Všechna nadzemní patra disponují totožným bezpečnostním vybavením. Především se jedná o dveře s bezpečnostním zámkem, které oddělují jednotlivé kancelářské prostory (každý kancelářský prostor je pronajat jiným soukromým subjektem). K tomu abychom se dostali do jednotlivých kancelářských komplexů je nutné vlastnit kartu která je nastavená pro odemknutí daného bezpečnostního zámku.

Společný prostor pater (chodba) je snímána bezpečnostními kamerami a je vybavena stejně jako vstupní hala prvky PZTS a prvky požární bezpečnosti. V samotných kancelářských prostorách se nevyskytují žádné kamerové systémy majitele budov (každý soukromý subjekt si může vybavit svou kancelář svým kamerovým systémem, pokud tak uzná za vhodné), pouze prvky požární bezpečnosti.

6.2.2 Katalog hrozeb

V následující podkapitole byl vytvořen a popsán katalog hrozeb pro měkké cíle, který byl konkretizovaný na administrativní centrum ABC Alfa. Jedná se tyto zdroje nebezpečí:

Tabulka 3: Katalog hrozeb [Zdroj: Vlastní]

Teroristický útok	Pád výtahu	Braní rukojmích
Napadení	Kolaps budovy	Verbální agrese s možnou eskalací k násilí
Epidemie	Vyhrožování	Falešné oznámení bomby
Úraz elektrickým proudem	Záplavy a povodně	Provozní havárie
Nehoda na parkovišti	Sebepoškozování	Hromadné násilí
Vražda	Vandalismus	Požár/žhářství
Absence bezpečnostní služby (hlídky)	Protesty a nepokoje v okolí objektu	

První kapitola praktické část je věnována obecnému popisu vybraného administrativního centra. Čtenář je na základě zevrubného popisu seznámen s charakteristikami administrativních center a s krátkou historií budovy vybranou pro tuto diplomovou práci.

Následně se práce věnuje popisu a bezpečnosti okolí budovy na základě dat získaných z webového portálu www.mapakriminality.cz a poznatků získaných z teoretické části práce, která se věnuje bezpečnosti měkkých cílů. V poslední části byla popsána bezpečnostní situace samotné budovy (parkoviště) a vytvořen katalog hrozeb, který byl konkretizován pro potřeby administrativní budovy ABC Alfa.

7 ANALÝZA RIZIK

K tomu, aby bylo možné zhodnotit bezpečnostní stav objektu je nutné provést některou z metod analýzy rizik. Jedná se o důležitou část procesu řízení rizik, která má za úkol odhalit potencionální slabiny zabezpečení vybraného subjektu.

Pro účely této diplomové práce byla zvolena SWOT analýza a metoda CARVER. Na základě vyhodnocení těchto dvou analýz je stanovená úroveň zabezpečení vybraného měkkého cíle v podobě administrativního centra ABC Alfa.

7.1 SWOT analýza

První metodou byla zvolena analýza SWOT. Jedná se o analýzu, která je zaměřená na porovnání a vyhodnocení vnitřních a vnějších faktorů, které působí na zkoumaný objekt. Vnitřními faktory myslíme věci, které je možné ovlivnit. Jedná se tedy o silné a slabé stránky v našem případě zabezpečení měkkého cíle. Mezi silné stránky je možné zařadit např. přítomnost bezpečnostní agentury, nebo výskyt prvků sloužící k zabezpečení objektu a mezi slabé stránky je možné zařadit například nedostatečný počet únikových východů. [47]

Druhou kategorií jsou vnější faktory, které působí na náš objekt z venku. Jedná se o faktory, které nemůžeme nijak nebo pouze částečně ovlivnit. Vnější vlivy dělíme na příležitosti a hrozby. Za příležitosti považuje stavy, které mohou nějak pozitivně ovlivnit úroveň zabezpečení jako jsou například státní dotace na zvýšení bezpečnosti měkkých cílů. Naopak hrozby jsou stavy, které vytváří nežádoucí situace ohrožující bezpečnost administrativního centra jako je např. požár, vandalismus a další. [47]

Po prozkoumání stávajícího zabezpečení vybraného administrativního centra a po prozkoumání bezpečnostní situace v okolí byly stanoveny tyto vnitřní a vnější vlivy, na základě kterých byla vyhodnocena stávající úroveň zabezpečení měkkého cíle ABC Alfa. Jednotlivé vnitřní a vnější vlivy jsou popsány v tabulce 4.

Tabulka 4: SWOT analýza [Zdroj: Vlastní]

	Silné stránky	Slabé stránky
Vnitřní vlivy	Systém IBS Přítomnost bezpečnostní agentury Přítomnost recepční	Vysoká kriminalita okolí Nedostatečný počet příslušníku SBS v objektu Atraktivní cíle v okolí objektu Jeden únikový východ Nepřítomnost příslušníku SBS 24/7
Vnější vlivy	Finanční zdroje Prevence Školení Dotace Přidání bezpečnostních opatření/prvků	Konkurenční boj Vandalismus Psychické zhroucení zaměstnanců Požár Teroristický útok Historická díla Fyzické napadení
	Příležitosti	**Hrozby**

K vyhodnocení budou sloužit následující tabulky 5,6,7 a 8, ve kterých jsou vypsány jednotlivé faktory rozdělené mezi silné a slabé stránky, příležitosti a hrozby. Každému faktoru je přiděleno hodnocení na stupnici od 1 až 5, které určuje míru důležitosti. Následně je autorem zvolená váha, kterou mají jednotlivé faktory na celkovou bezpečnost administrativního centra.

Jak již bylo zmíněno za silné stránky považujeme vlivy, které můžeme sami ovlivnit a v tomto případě se jedná o metody či prvky, které slouží k zabezpečení administrativního centra.

Největší váhu v kategorii silných stránek obdržel integrovaný bezpečnostní systém (IBS), který se nachází v objektu administrativního centra. Díky tomuto systému je objekt pod dohledem 24 hodin denně 7 dní v týdnu. IBS administrativního centra obsahuje následující prvky: CCTV, PZTS, kartový vstupní systém a požárně bezpečnostní systémy.

Kamerový systém, který se nachází v objektu zajišťuje neustálý dohled nad celou administrativní budovou ABC alfa a snímá především společné prostory budovy jako

je vstupní hala, recepce, vstupní dveře, parkoviště, společné prostory a obvod budovy. PZTS prvky jsou umístěny na strategických místech (slabých místech), kde my mohlo dojít k potencionální nežádoucí činnosti. Požární signalizace je napojená na hasičský záchranný sbor Moravskoslezského kraje a zajišťuje odhalení a následné vyhlášení poplachu požáru, havárie či jiného nouzového stavu. Posledním prvkem IBS je kartový vstupní systém, který se nachází při vstupu do budovy, turniketů, které oddělují část budovy pro veřejnost a část pro zaměstnance, a nakonec u jednotlivých kancelářských celků pro jednotlivé soukromé subjekty.

Druhým nejvíce hodnocený vlivem je přítomnost příslušníka bezpečnostní agentury, který se nachází v objektu budovy. Jedná se o zaměstnance soukromé společnosti zajišťující bezpečnost v budově. Pracovník agentury provádí pravidelné obchůzky během dne, na kterých se snaží odhalit potencionální hrozby.

Poslední zmíněnou silnou stránkou je přítomnost recepční, která se nachází v recepci ve vstupní hale budovy. Ta má za úkol pozorovat dění ve vstupní hale a zajišťovat přístup osobám, které nejsou zaměstnanci jednotlivých společností sídlících v budově.

Tabulka 5: Silné stránky [Zdroj: Vlastní]

Silné stránky	Váha	Hodnocení	Výsledek
Systém IBS	0,6	5	3
Přítomnost bezpečnostní agentury	0,3	4	1,2
Přítomnost recepční	0,1	1	0,1
Součet	**1**		**4,3**

Největší váhu v kategorii slabých stránek mají dva vlivy, které spolu úzce souvisí. Administrativní centrum sice disponuje fyzickou ostrahou, ale pouze vymezený časový úsek (nenachází se v objektu celých 24 hodin denně). Dále se v jeden okamžik nachází v budově pouze jeden zaměstnanec sboru bezpečnostní služby (SBS), který je primárně v prostorech recepce, ale v určitých časových intervalech se vydává na bezpečnostní pochůzku. V tento okamžik se při vstupu do budovy nachází pouze recepční. Na základě tohoto faktu je v moment nepřítomnosti fyzické ostrahy výrazně ovlivněna bezpečnost budovy.

Míra kriminality v blízkém okolí administrativního centra je dalším vysoce ohodnocenou slabou stránkou. Na základě dat z webového portálu www.mapakriminality.cz se nachází Ostrava na pátém místě s největším počtem trestných činů v České republice. V městské části Ostrava Přívoz, kde se administrativní centrům nachází se v období od 1. ledna 2018

do 1. ledna 2020 odehrálo 2 130 trestných činů. Samotné administrativní centrum se navíc nachází poměrně blízko centra města, kde je větší koncentrace potencionálního nebezpečí.

Další slabou stránkou administrativního centra je fakt, že v jeho okolí se vyskytuje velké množství budov, které je možné popsat jako cíle se zvýšenou atraktivitou pro potencionálního útočníka. Především tím myslíme Městský úřad, radnici a školu. Na základě toho, že jsou tyto budovy v bezprostřední blízkosti, tak případný útok na ně přímo ohrozí bezpečnostní stav administrativní budovy.

V samotné budově pracuje velké množství zaměstnanců z několika různých firem. Na základě toho, že se v objektu vyskytují nejen zaměstnanci společnosti vlastnící administrativní centrum, ale také zaměstnanci několika firem zde sídlících, je nutné dbát na to kdo kde přistupuje a kde se nachází. S tímto problémem se také váže poslední faktor slabých stránek, a to je nedostatečný počet únikových východů, které jsou v budově. Zde se nachází pouze jeden únikový východ, který je zároveň hlavním vchodem do budovy.

Tabulka 6: Slabé stránky [Zdroj: Vlastní]

Slabé stránky	Váha	Hodnocení	Výsledek
Vysoká kriminalita v okolí	0,2	-4	-0,8
Velké množství zaměstnanců	0,05	-2	-0,1
Atraktivní cíle v okolí objektu	0,2	-4	-0,8
Nedostatečný počet příslušníků SBS	0,25	-5	-1,25
Nepřítomnost příslušníka SBS 24/7	0,25	-5	-1,25
Jeden únikový východ	0,05	-2	-0,1
Součet	**1**		**-4,3**

Druhou částí jsou vnější vlivy. Jedná se o faktory, které je možné ovlivnit pouze částečně, nebo vůbec.

Nejdůležitějším faktorem příležitostí je prevence. Při zabezpečování měkkých cílů, je vytváření prevenčních opatření nejdůležitějším faktorem. Ve spoustě případech dochází k útoku během několika málo vteřin a je prakticky nemožné na ně zareagovat, proto je nutné vytvářet opatření, která těmto potencionálním nebezpečím předchází. S tímto faktorem souvisí také další vliv, a to je školení zaměstnanců, což je možné považovat za formu prevenčního opatření. Je nutné, aby každý zaměstnanec nacházející se v objektu věděl, jak zpozorovat hrozbu a jak se zachovat při krizové situaci.

I když se v administrativním centru nachází velké množství bezpečnostních opatření a prvků je nutné přidávat stále nové a modernější varianty. To především z toho důvodu, že techniky a technologie útočníků se každým dnem zlepšují a je nutné být na ně připraven.

Na základě toho, jak velké máme finanční prostředky se odvíjí míra bezpečnostních opatření, jaké si můžeme dovolit. Díky tomu, že budova je vlastněna bohatou společností je pravděpodobné, že bezpečnostní prvky a opatření budou na dostatečně vysoké úrovni.

Posledním faktorem jsou dotační programy, které jsou poskytnuty Ministerstvem vnitra České republiky, které mohou sloužit jako motivace pro snížení nákladů při zajišťování bezpečného prostředí měkkého cíle.

Tabulka 7: Příležitosti [Zdroj: Vlastní]

Příležitosti	Váha	Hodnocení	Výsledek
Finanční prostředky	0,2	3	0,6
Prevence	0,3	5	1,5
Školení	0,2	3	0,6
Dotace	0,05	2	0,1
Přidání bezp. Opatření/prvků	0,25	4	1
Součet	**1**		**3,8**

Největší váha je přidána hrozbě fyzického napadení, a to především z důvodů vysoké kriminality v okolí administrativní budovy, v možnosti volného přístupu do haly budovy a také díky současné pandemické situaci na území České republiky, která má jistý mentální vliv na chování jedinců.

Další hrozbou, která souvisí s vysokou kriminalitou v okolí je vandalismus, který je velmi častým jevem na území Ostravy. Stejně ohodnocenou hrozbou je také teroristický útok, který sice není na území České republiky tak běžný, ale na základě vysoké koncentrace atraktivních cílů v okolí je nutné tomuto problému věnovat zvýšenou pozornost.

Poslední výraznou hrozbou je možnost vzniku požáru. Na základě toho, že se jedná sice o zrekonstruovanou budovu, ale starou, je zde zvýšená možnost vzniku požáru. Dále je nutné brát v potaz například možnost úmyslného založení požáru například nespokojeným zaměstnancem. Ve SWOT analýze jsou také zmíněny dvě hrozby, které mohou mít minimální dopad, ale díky jejich charakteristice jsou pravděpodobné. Jedná se o možné zranění v prostorách historického výtahu a také hrozba konkurenčního boje soukromých subjektů nacházejících se v budově či celém komplexu.

Tabulka 8: Hrozby [Zdroj: Vlastní]

Hrozby	Váha	Hodnocení	Výsledek
Konkurenční boj	0,05	-2	-0,1
Vandalismus	0,2	-4	-0,8
Psychické zhroucení zaměstnanců	0,05	--2	-0,1
Požár	0,2	2	-0,4
Teroristický útok	0,2	-4	-0,8
Fyzické napadení	0,25	-4	-1
Historická výtah	0,05	-2	-0,1
Součet	**1**		**-3,3**

Na základě SWOT analýzy byly odhaleny faktory, které mají největší a nejmenší vliv na bezpečnost vybraného měkkého cíle. Tyto dílčí výsledky jsou zobrazeny v tabulkách 5,6,7 a 8.

Tabulka 9: Výsledky SWOT analýzy [Zdroj: Vlastní]

Silné stránky	4,3
Slabé stránky	-4,3
Příležitosti	3,8
Hrozby	-3,3
Silné – Slabé (vnitřní vlivy)	0
Příležitosti – Hrozby (vnější vlivy)	0,5
Součet	**0,5**

Pro přesnější znázornění byla autorem vytvořena stupnice rizika, která pracuje se součtem výsledků vnitřních a vnějších vlivů SWOT analýzy. Tyto stupně rizika znázorňují možnost výskytu nežádoucí situace v objektu:

- Malé riziko (hodnoty větší než jedna) – zabezpečení je na vysoké úrovni.
- Střední riziko (hodnoty od -1 do 1) – zabezpečení je na dostatečné úrovni (prostor pro zlepšení).
- Velké riziko (hodnoty menší než mínus jedna) – zabezpečení není na dostatečné úrovni.

Na základě výše zmíněné stupnice rizika můžeme určit, že objekt spadá do kategorie se středním rizikem.

Z dílčích vyhodnocení je očividné, že největší váha vnitřních vlivů je přikládána k výskytu prvku IBS v objektu. Ovšem pomocí SWOT analýzy byla odhalena poměrně velká bezpečnostní slabina, a to v podobě nedostatečného počtu pracovníku SBS a faktu, že se nevyskytují v administrativním centru po celý den.

Na základě této slabiny se zvyšuje riziko výskytu jednotlivých hrozeb jako je vandalismus, fyzické napadaní a další. Ovšem objekt disponuje příležitostmi, na základě kterých je možné odstranit odhalenou slabinu a to za využití dostatečných finančních zdrojů k rozšíření působení příslušníků SBS v objektu.

7.2 Metoda CARVER

Druhou metodou byla zvolena metoda CARVER, která má za úkol identifikovat a popsat největší hrozby pro zvolené administrativní centrum. Metoda je postavená na šesti faktorech, které jsou ohodnoceny na stupnici od 1 do 5, od minimálního rizika až po kritické riziko. Pro lepší pochopení jsou autorem přesněji popsané stupně rizika. Metoda se dívá na problematiku zabezpečení budovy pohledem samotného útočníka či událostmi vyvolanými přírodními jevy.

Hrozby byly vybrány z katalogu hrozeb (Tabulka 3), který byl vytvořen na základě charakteristiky objektu. Tyto hrozby přestavují jak mimořádné události, tak formy různých útoků.

Prvním kritériem je důležitost (Criticaly). Jedná se o faktor, který určuje, jakou důležitost má daný objekt v našem případě budova ABC Alfa. [28]

Tabulka 10: Stupnice důležitosti [Zdroj: Vlastní]

Criticaly (C)	Hodnota	Popis
Minimální	1	Neobývané objekty
Nízká	2	Objekty s občasným výskytem lidí
Střední	3	Obývané prostory (rodinné domy, panelové domy)
Vysoká	4	Úřady, administrativní centra, obchodní domy atd..
Kritická	5	Kritická infrastruktura

Faktor přístupnosti (Accessibility) popisuje, jak snadno útočník dokáže překonat překážky, které stojí mezi ním a jeho cílem. [28]

Tabulka 11: Stupnice přístupnosti [Zdroj: Vlastní]

Accessibility (A)	Hodnota	Popis
Minimální	1	Nepřístupné
Nízká	2	Omezený přístup
Střední	3	Přístupné
Vysoká	4	Snadno přístupné
Kritická	5	Volně dostupné prostory

Dalším faktorem je rozpoznatelnost (Recognizability). Jedná se o faktor, který určuje, jak snadno útočník rozpozná svůj cíl. [28]

Tabulka 12: Stupnice rozpoznatelnosti [Zdroj: Vlastní]

Recognizability (R)	Hodnota	Popis
Minimální	1	Cíl je velice obtížné rozpoznat
Nízká	2	Cíl je špatně rozpoznatelný
Střední	3	Cíl je rozpoznatelný
Vysoká	4	Cíl je snadně rozpoznatelný
Kritická	5	Cíl je velmi snadně rozpoznatelný

Následující faktor zranitelnost (Vulnerability) je zaměřený na zhodnocení bezpečnostních opatření a prvků, které slouží k zamezení nechtěné činnosti a také na znalosti, které musí útočník mít k tomu, aby útok provedl. [28]

Tabulka 13: Stupnice zranitelnosti [Zdroj: Vlastní]

Vulnerability (V)	Hodnota	Popis
Minimální	1	Minimální riziko zranitelnosti
Nízká	2	Nízké riziko zranitelnosti
Střední	3	Střední riziko zranitelnosti
Vysoká	4	Vysoké riziko zranitelnosti
Kritická	5	Riziko zranitelnosti je kritické

Dalším popsaným faktorem je efekt (Effect on), který je způsoben danou mimořádnou událostí a jeho vliv na ekonomiku, bezpečnost, psychiku a celkově na okolí.

Tabulka: 14 Stupnice dopadu [Zdroj: Vlastní]

Effect on (E)	Hodnota	Popis
Minimální	1	Minimální dopad na okolí
Nízká	2	Malý dopad na okolí
Střední	3	Středně velký dopad
Vysoká	4	Velký dopad na okolí
Kritická	5	Kritický dopad na okolí

Poslední faktorem metody CARVER je obnova (Recuperbility). Jedná se o časový úsek, který je nutný k obnově po vybraném incidentu. [28]

Tabulka 15: Stupnice obnovy [Zdroj: Vlastní]

Return on effort (R)	Hodnota	popis
Minimální	1	Do několika hodin
Nízká	2	V rámci dnů
Střední	3	V rámci týdnů
Vysoká	4	V rámci měsíců
Kritická	5	V rámci let

7.2.1 Vyhodnocení metody CARVER

Cílem metody je stanovení rizika pro administrativní centrum ABC Alfa na základě ohodnocení a sečtení hodnot všech kritérií, se kterými pracuje metoda CARVER. Výsledky jsou uvedeny v Tabulce 16.

Tabulka 16: Výsledky metody CARVER [Zdroj: Vlastní]

Hrozba	C	A	R	V	E	R	Celkem
Napadení	4	1	2	2	2	1	12
Nehoda na parkovišti	4	1	4	1	1	1	12
Úraz elektrickým proudem	4	1	3	2	1	3	14
Vyhrožování	4	1	2	4	3	1	15
Protesty a nepokoje v okolí objektu	4	1	4	4	1	1	15
Braní rukojmích	4	2	4	1	2	2	15
Vražda	4	2	2	3	3	2	16
Sebepoškozováni	4	1	4	4	2	1	16
Verbální agrese s možnou eskalací k násilí	4	1	3	5	2	1	16
Pád výtahu	4	1	5	2	1	4	17
Vandalismus	4	2	3	5	1	2	17
Provozní havárie	4	1	3	3	3	3	17
Hromadné násilí	4	3	3	2	3	2	17
Epidemie	4	2	3	1	3	4	17
Záplavy a povodně	4	2	3	1	4	4	18
Falešné oznámení bomby	4	1	3	4	4	2	18
Pandemie	4	1	3	1	4	5	18
Absence bezp. Hlídky	4	4	2	4	3	2	19
Kolaps budovy	4	4	2	1	4	5	20
požár/žhářství	4	4	3	1	4	4	20
Teroristický útok	4	2	5	5	5	5	26

Pro přesnější určení míry rizika byla vytvořena následující stupnice:

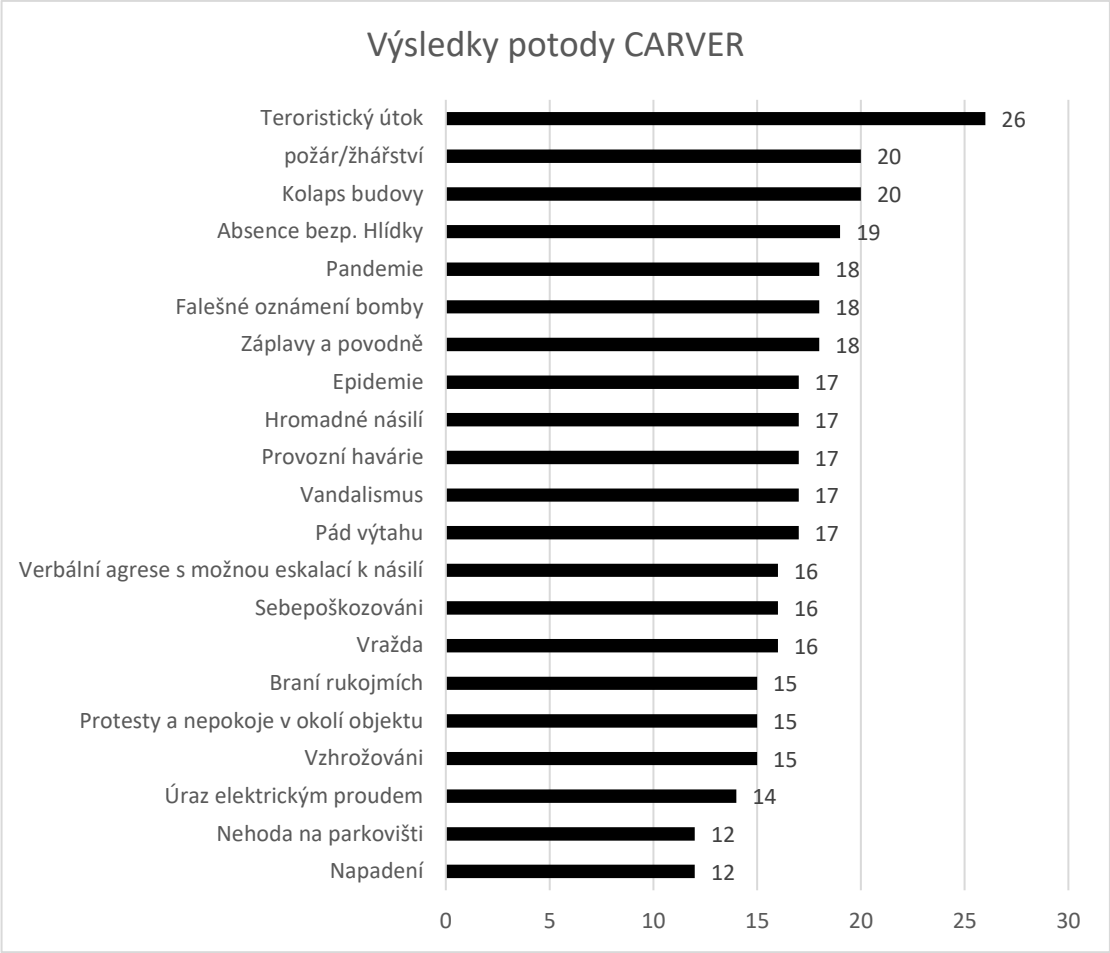
Tabulka 17: Stupnice míry rizika [Zdroj: Vlastní]

Hodnota	Stupeň ohrožení
0-9	Minimální riziko
10-14	Nízké riziko
15-19	Střední riziko
20-24	Vysoké riziko
25 a více	Kritické riziko

Na grafu 1 je možné přehledně vidět, která hrozba představuje pro zvolený objekt administrativního centra největší ohrožení. Jako první se umístil teroristický útok, který jako jediný spadá do kategorie hrozeb s kritickým stupněm ohrožení. Provedení takovéhoto útoku by bylo devastující nejen pro samotou budovu, ale také pro přilehlé okolí. U této hrozby také musíme brát v potaz, že v nejbližším okolí se nacházejí symbolicky významná místa, která se samy mohou stát objetí teroristického útoku. Další dvě hrozby, které představují vysoké riziko jsou kolaps budovy a požár/žhářství. Samotný kolaps budovy může být zapříčiněn zanedbáním rekonstrukce suterénních prostor či poddolováním objektu. Hrozba požáru je výrazně potlačena díky přítomnosti EPS v budově, ovšem není možné brát na lehkou váhu žhářský útok vandalů nebo nespokojeného zaměstnance.

Poslední vysoce hodnocenou hrozbou je absence bezpečnostní hlídky, které není v objektu zastoupena dostatečným počtem příslušníků SBS a také nehlídkuje v objektu v průběhu celého dne.

Zbylé hrozby byly rozděleny do kategorií se středním rizikem (např. falešné oznámení bomby, vandalismus a další), s nízkým rizikem (vyhrožování, napadení a další) a s minimálním rizikem kam nespadá žádná hrozba.



Graf 1: Výsledky metody CARVER [Zdroj: Vlastní]

Tato kapitola byla věnována analýze rizik administrativního centra ABC Alfa. K analýze byly využity dvě metody, a to SWOT analýza a metoda CARVER. Za pomocí SWOT analýzy byly odhaleny silné stránky, mezi které patří přítomnost systému IBS, slabé stránky, kam mezi nejvýznamnější vlivy řadíme malý počet příslušníků SBS a také jejich nepřítomnost v průběhu celého dne. U vnějších vlivů analýzy vyvstali hrozby typu teroristický útok, fyzické napadení či vandalismus a příležitosti kam mezi nejvýznamnější považujeme finanční zdroje majitele administrativního centra. Druhou analýzou byla metoda CARVER, která se zaměřila na zhodnocení jednotlivých hrozeb z katalogu hrozeb, kam mezi nejvýznamnější patří teroristický útok, kolaps budovy, požár/žhářství a absence bezpečnostní hlídky. Získané poznatky budou zohledněny v poslední kapitole diplomové práce pojednávající o možných zabezpečeních pro námi zvolený měkký cíl.

8 SCÉNÁŘE A POPIS VYBRANÝCH BEZPEČNOSTNÍCH INCIDENTŮ

Kapitola pojednávající o vzorových útocích, které mohou nastat a ohrozit administrativní centrum ABC Alfa. Konkrétně se bude jednat o konflikt začínající verbální agresí s eskalací k fyzickému násilí a bombový útok. K prvnímu příkladu bude vytvořen vzorový scénář útoku a také rozvětvený strom událostí, který je umístěn v přílohách. Strom událostí byl vytvořen za pomocí softwarového nástroje draw.io, který je volně dostupný na webovém portálu https://app.diagrams.net/ a také nabízí desktopovou aplikaci. U scénáře bombového útoku byl pro znázornění potencionálních škod využit softwarový nástroj teroristický expert TerEX.

8.1 Scénář 1.: Verbální agrese s eskalací k fyzickému nenásilí

První scénář je zaměřený na incident mezi útočníkem a obsluhou recepce administrativního centra, kde dochází k eskalaci z verbální agrese na fyzickou. Primárními aktéry (osoby zapojené do této potyčky) jsou útočník, obsluha recepce a příslušník SBS.

Neznámá osoba přichází v ranních hodinách před vchod do administrativního centra. Tato osoba je zachycena bezpečnostními kamerami a využívá faktu, že vchodové dveře jsou v ranních hodinách volně otevřené.

Vchází do vstupní haly a začne se nervózně rozhlížet kolem sebe. Díky tomu, že hala je rozdělená na veřejně dostupnou část a část pouze pro zaměstnance (je rozdělená turniketem) nemůže volně projít dále do objektu (je zřejmé, že v daný moment se v prostorech recepce nachází pouze obsluha recepce). Zaměstnanec/Zaměstnankyně recepce si všimne nervózně vyhlížejícího jedince a položí mu otázku: „Dobrý den, jak vám mohu pomoci. Hledáte někoho?“ neznámá osoba přistoupí k pultu recepce a odpoví „Hledám pána XXX ze společnosti XXX“. Obsluha recepce se zeptá na jméno a zavolá do kanceláře společnosti, kde jí administrativní pracovník odpoví: „Nikoho takového nečekáme, nemá domluvenou schůzku“. Zaměstnanec recepce telefon položí a objasní situaci pánovi XXX, že v dané společnosti nikoho dneska nečekají, proto ho nemůže vpustit do objektu. Pán XXX začíná být nervózní a jeho chování se razantně mění, začíná projevovat známky agrese verbálně. Na základě změny jeho chování jej začne obsluha recepce uklidňovat (snaží se mu asertivně vysvětlit situaci). Chování agresora se ovšem neklidní, proto ho obsluha recepce vyzve, aby opustil objekt nebo přivolá příslušníka SBS. Toto

vyzvání pana XXX ještě více rozčílí a všimne si, že přístup do recepce není nijak zajištěn a je schopen se k obsluze recepce bez problému dostat. Verbální agrese útočníka začíná přecházet k fyzickému násilí a přes pul začne fyzicky obtěžovat obsluhu recepce, která na základě tohoto agresivního jednání za využití poplašného zařízení požádá o pomoc příslušníka SBS. Útočník je rozčílen, rozhodne se překonat překážku pultu recepce a začne fyzicky napadat obsluhu. Příslušník SBS, který se nachází na obchůzce ve vyšších patrech administrativního centra zachytí signál a běží do oblasti vstupní haly. Zde si všimne útočníka, který fyzicky obtěžuje obsluhu recepce, která je v panickém záchvatu strachu. Zaměstnanec SBS na nic nečeká a přiběhne do prostorů recepce, za pomocí hmatů a chvatů zpacifikuje útočníka (útočník v záchvatu vzteku si příslušníka ani nevšimne). Příslušník SBS zajistí útočníka a požádá obsluhu recepce o přivolání Policie ČR. Při zajištění útočníka ochranka zjistí, že v kapse má chladnou zbraň, konkrétně kapesní nůž, který mu zajistí. Obsluha recepce je ovšem v šoku a nereaguje na výzvu příslušníka SBS, ten se jí snaží uklidnit, což se mu během několika minut podaří. Obsluha recepce zavolá Policii ČR, která dorazí na místo. Příslušníci policie si útočníka přeberou a vyslechnou zaměstnance bezpečnostní agentury a recepční, která je stále v šoku, proto je z preventivních důvodů přivolána záchranná služba.

Objekt administrativního centra ABC Alfa a jeho bezprostřední okolí je z tohoto důvodu na několik hodin uzavřen a jeho funkce je ochromena.

Podrobnější průběh incidentu je popsán pomocí stromu událostí, který je obsažený v příloze P3.

8.2 Scénář 2.: Bombový útok na administrativní centrum

Druhý scénář je zaměřený na útok bombou. Primárními aktéry jsou útočník, obsluha recepce a příslušník SBS, policejní složky a osoby nacházející se uvnitř objektu. Scénář je také obohacen o výstup ze softwarového nástroje teroristický expert TerEX, který znázorňuje potencionální škody vyvolané výbuchem bomby v prostorách administrativního centra.

Neznámá osoba přichází v ranních hodinách před vchod administrativního centra. Tato osoba je zachycena bezpečnostními kamerami a využívá faktu, že vchodové dveře jsou v ranních hodinách volně otevřené.

Vchází do vstupní haly a začne se nervózně rozhlížet kolem sebe. Díky tomu, že hala je rozdělená na veřejně dostupnou část a část pouze pro zaměstnance (je rozdělená turniketem) nemůže volně projít dále do objektu. Je zřejmé, že v okolí recepce se pohybuje několik osob. Tyto osoby je snadné rozklíčovat na obsluhu recepce, příslušníka bezpečnostní agentury a několik dalších návštěvníků/zaměstnanců administrativního centra. Osoba si bez povšimnutí kohokoliv z přítomných sedne do volně dostupných křesel, které jsou umístěny ve vstupní hale. Neznámá osoba chvíli sedí a po nějaké době se zvedne a odejde z budovy. Po několika minutách si zaměstnanec SBS všimne neznámého balíčku, který se nachází na křesle, ve kterém seděl pachatel. Přistoupí ke křeslu a zhodnotí pohledem neznámý předmět. Rozhodne se oznámit tento fakt příslušným orgánům, vyzve recepční ke spuštění poplachu a řízení evakuace osob, které se nacházejí v budově administrativního centra (dle interních předpisů provádí evakuaci osob zaměstnanec recepce či příslušník SBS). Samotný příslušník SBS zůstává v blízkosti neidentifikovatelného balíčku a popisuje situaci Policii ČR. Průběh evakuace budovy probíhá neorganizovaně, ale nakonec se podaří veškeré osoby dostat na místo shromáždění, které je před budovou (kontrolu, že budovu opustili všichni má opět na starost osoba provádějící evakuaci). Na místo činu přijíždí Policie ČR a její experti na výbušniny. Přebírají místo činu a kladou otázky tykající se proběhlé evakuace osob. Následně na to začíná probíhat evakuace nejbližších budov a zajištění okolí. Ve stejnou chvíli pyrotechnik přistupuje k neznámému balíčku a na základě předepsaných kroků začíná pracovat s potencionální výbušninou. Po prozkoumání balíčku je skutečně identifikovaná výbušnina. Pyrotechnik výbušninu zajistí a postará se o bezpečný převoz.

Objekt administrativního centra ABC Alfa a jeho bezprostřední okolí je z tohoto důvodu uzavřen až do chvíle kdy se incident vyjasní.

TerEX

Ne všechny případy mohou ovšem končit takto zdárně. Je nutné si uvědomit, že výbušnina mohla kdykoliv explodovat a proto, za využití teroristické experta můžeme identifikovat jaké škody by výbuch mohl způsobit nejen administrativnímu centru, ale i přilehlému okolí.

Pro potřeby práce byla zvolena výbušnina, která obsahuje 5 kg plastické trhaviny Semtex. Jedná se o víceúčelovou plastickou trhavinu vyrobenou v 50. letech minulého století na území bývalého Československa. Její nejčastější využití je pro demolici nebo vojenské účely. Ovšem tato trhavina je také velice populární při páchání teroristických zločinů. [48]

Pro vytvoření simulace byl využit havarijní model EXPLOSIVE simulující dopady výbuchu.

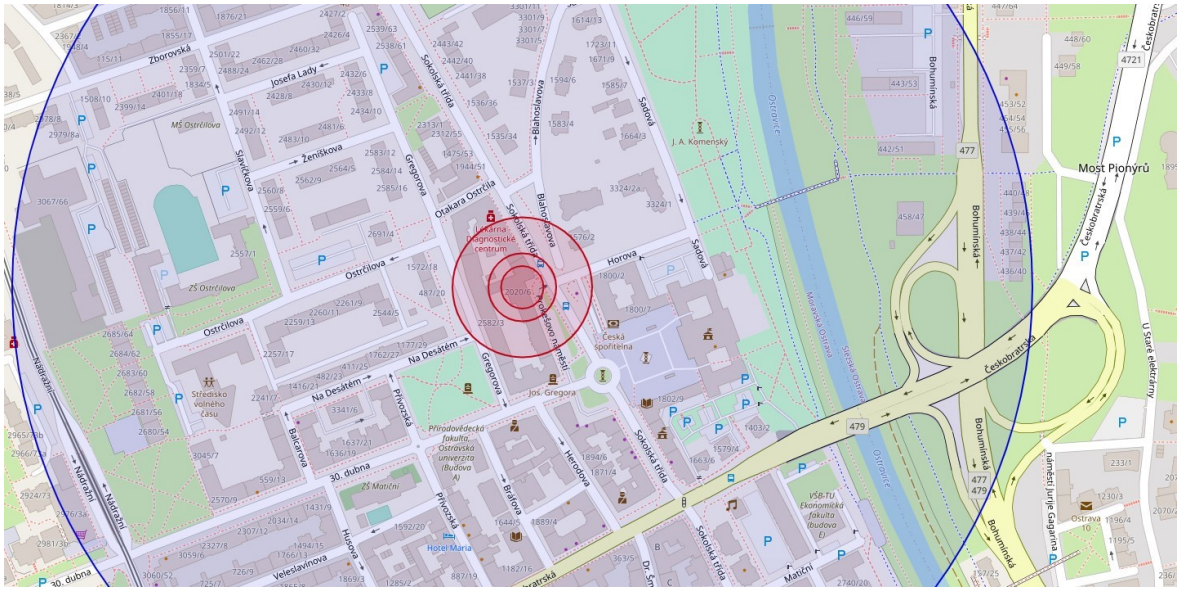
Obrázek 15: TerEX událost [Zdroj: Vlastní]

Dle výsledků simulace výbuchu je možné konstatovat, že samotná budova a také budovy v přilehlém okolí by byly zasaženy a poškozeny výbuchem trhaviny. Přesné výsledky jsou zaznamenány v následující tabulce.

Tabulka 18: výsledky simulace výbuchu [Zdroj: Vlastní]

	Vzdálenost
Závažné poškození budov	20 m
Ohrožení osob mimo budovy závažným poraněním	32 m
Ohrožení osob uvnitř budov okenním sklem	66 m
Bezpečnostní vzdálenost pro nekryté osoby	20 m

Pro přesné pochopení, jak moc velkou oblast by takováto výbušnina zasáhla, byla využita možnost TerEXu ukázky zasažené oblasti na mapě.



Obrázek 16: Zasažená oblast výbuchu [Zdroj: Vlastní]

Na obrázku mapy si je možné povšimnou, že výbuch zasáhl poměrně velkou část budovního bloku, ve které se administrativní centrum nachází. Potencionální výbuch by zasáhnul více než 1500 lidí. Navíc by byla ochromena doprava v okolí objektu.

Kapitola pojednává o bezpečnostních incidentech, které jsou potencionálním zdrojem rizika pro administrativní centrum. Kapitola je složena ze dvou scénářů. První scénář je zaměřen na hrozbu vzniku verbální agrese, která může eskalovat až k fyzickému napadení. Z popisu události jsou zjevně podstatné nedostatky, a to především malý počet příslušníků SBS v objektu a také nízké zabezpečení oblasti recepce. Následně byl vytvořen detailní strom událostí incidentu, který se nachází v přílohách diplomové práce.

Druhý scénář je popis bombového útoku na námi zvolený objekt. Scénář popisuje neznámého útočníka, který do objektu přinesl neidentifikovatelný balíček. Následně se scénář zabývá postupy při odhalování takového neidentifikovatelného balíčku. Další část je zaměřená na simulaci výsledků potencionálního výbuchu za využití softwarového nástroje TerEX. Díky dat získaných z tohoto nástroje je zjevné, jak velká oblast by byla výbuchem zasažena. Na základě této situace je možné konstatovat, že takovýmto útokům je velice těžké zabránit. Proto je nutné vytvářet preventivní opatření ve formách školení či vytváření krizových plánů, a to nejen v rámci objektu, ale i přilehlého okolí. Získané poznatky budou zohledněny v následující kapitole pojednávající o možnostech zabezpečení administrativního centra.

9 ZÁVĚREČNÉ ZHODNOCENÍ A NÁVRH BEZPEČNOSTNÍCH OPATŘENÍ

Poslední kapitola pojednává o závěrečném hodnocení bezpečnostních opatřeních vycházejících z provedených analýz, a to SWOT analýzy a metody CARVER. Následně jsou branné v potaz také jednotlivé scénáře, popisy, stromy událostí a modelování výbuchu nástrojem TERex, které odhalují potencionální nedostatky v současném zabezpečení budovy administrativního centra. Na základě těchto zjištění jsou následně vypracována bezpečnostní opatření, která mají za úkol minimalizovat rizika a vylepšit současný bezpečnostní stav budovy.

Z analýzy SWOT vyplývá, že objekt disponuje poměrně vysokou úrovní zabezpečení díky bezpečnostním prvkům systému IBS jako je například elektronický poplachový systém, kartový přístupový systém a elektronická požární signalizace. Na druhou stranu je zřejmé, že největší bezpečnostní nedostatky vyplývají z neuspokojivého zastoupení příslušníku SBS v budově. Tento fakt podporuje také výsledek metody CARVER, který hodnotí hrozbu nepřítomnosti příslušníka bezpečnostní agentury jako čtvrtou největší hrozbu z vytvořeného katalogu hrozeb.

Tato mezera v bezpečnosti objektu byla detailně popsaná v obou scénářích v kapitole 8. Z nich je zřejmé, že kdyby v krizový moment byl přítomný bezpečnostní zaměstnanec, tak by byla výrazně snížená hrozba, které musí čelit návštěvníci a zaměstnanci nacházející se v administrativním centru.

Z tohoto důvodu se budou navržená bezpečnostní opatření týkat především fyzické bezpečnosti objektu, režimových opatření a také nácvikům a školením připravenosti.

Ovšem i přesto, že administrativní centrum je po technické stránce zabezpečení na vysoké úrovni, tak na základě zjištěných faktů vyplívajících jak z analýz rizik, tak ze scénářů, bude zmíněno několik prvků, které by mohly zdokonalit již dobře navržený systém.

9.1 Návrhy bezpečnostních opatření budovy administrativního centra

Podkapitola popisující autorem navržené opatření k minimalizaci bezpečnostních hrozeb pro zvolenou budovu. Jedná se především o dvě varianty fyzického zabezpečení, režimová opatření a další.

Současné řešení zajištění fyzického zabezpečení objektu je přítomnost jednoho příslušníka SBS (pouze v určitých časových intervalech) a jednoho zaměstnancem recepce.

Jak vyplývá z předchozích kapitol práce jeden příslušník pro zajištění fyzické bezpečnosti objektu nestačí. Tento pracovník má několik povinností, které musí provádět po čas své služby. Mezi tyto povinnosti patří sledování kamerového systému, kontrolování dění ve veřejných prostorách, a to především vstupní haly budovy, která díky své volné přístupnosti představuje velké bezpečnostní riziko. S tím je spojená také kontrola návštěvníků, dále je jeho povinností provádět obchůzky v dalších patrech budovy, kontrola firemního parkoviště sloužícího pro parkování firemní automobilové flotily nájemníku administrativního centra, a nakonec figuruje jako pověřená osoba při evakuaci budovy.

V momentě, když je příslušník SBS nepřítomný, jak z důvodu provádění bezpečnostní obhlídky objektu nebo ukončení jeho směny připadají některé povinnosti na zaměstnance recepce, který je přítomný 24 hodin denně, ale nedisponuje takovou profesní znalostí jako právě proškolený zaměstnance bezpečnostní agentury. V době nepřítomnosti bezpečnostního pracovníka provádí kontrolu kamerového sytému zaměstnanec recepční služby a také je pověřen eventuální evakuací objektu.

Na základě těchto zjištění byly navrženy dvě varianty zajištění fyzické bezpečnosti objektu minimalizující hrozby, které mohou vyvstat za nepřítomnosti zaměstnance SBS.

Kalkulace nákladů pro jednotlivé varianty je problematická disciplína, jelikož takovéto zakázky jsou většinou dělány na míru. Ovšem pro přibližné vyčíslení nákladů na zajištění více příslušníku SBS můžeme využít informací poskytnutou Českým klubem bezpečnostních služeb z.s., který vyčíslil přibližnou hodinovou mzdu účtovanou bezpečnostními agenturami při zajišťování 24hodinové bezpečnosti.

Tabulka 19: Průměrná cenová kalkulace příslušníka SBS [49]

Průměrná cenová kalkulace na 1 hodinu	**Náklady na mzdu Kč/h**
Mzda ve druhé skupině práci při měsíční mzdě 16 100 Kč	98,40 Kč
Příplatek za noční směnu	3,30 Kč
Příplatek za sváteční směnu	3,50 Kč
Příplatek za sobotní směnu	3,00 Kč
Odvody na soc. a zdrav. Pojištění 34 %	36,80 Kč
Zákonné pojištění	0,60 Kč

Rezerva na dovolenou	12,10 Kč
Průměrné náklady	**157,70 Kč/h**

9.1.1 Varianta 1: posílení fyzické ochrany v administrativní budově ABC Alfa

První varianta je postavená na zvýšení počtu přítomnosti bezpečnostních pracovníku přímo v budově ABC Alfa z jednoho na tři. Příslušníci by byli přítomni v objektu po celý den. Na základě toho, že se zvýší počet příslušníků odpadají povinnosti méně proškolenému zaměstnanci recepce budovy, který se může věnovat jiným povinnostem jako je například přijímání zásilek či komunikace s jednotlivými firmami sídlícími v budově.

Dojde k minimalizaci vzniku situací, kdy se v prostorech vstupní haly nenachází žádný bezpečnostní pracovník. Dále budou posíleny bezpečnostní obchůzky, které nyní mohou provádět dva SBS příslušníci. Ve variantách obchůzky v páru, na základě které může dojít k zastrašení potencionálního útočníka, nebo varianty jednoho příslušníka provádějícího obchůzky ve vnitřních prostorách budovy a druhého provádějícího bezpečnostní obchůzku na parkovišti a kolem budovy administrativního centra.

Nakonec na základě zvýšení počtu bezpečnostních pracovníků v objektu vede k lepší organizaci případné evakuace osob, která díky velkému počtu zaměstnanců, kteří jsou navíc rozděleni mezi několik firem, je velice náročná na organizaci.

Na základě tabulky 19 je možné vyčíslit přibližnou cenu nákladů pro zajištění 24hodinové fyzické ochrany objektu třemi příslušníky SBS. Výsledná cena se bude pohybovat v měsíčních nákladech. Pro výpočet ceny nákladů na jednoho příslušníka SBS byla využita následující rovnice: 157,70 (průměrné náklady) * 24 (hodin) * 365 (dní) / 12

Tabulka 20: Kalkulace nákladů první varianty [Zdroj: Vlastní]

Cena za 24hodinnovou ochranu 1 příslušníkem SBS	115 121 Kč
Cena za 24hodinnovou ochranu 3 příslušníky SBS	**345 363 Kč**

9.1.2 Varianta 2: propojení fyzické ochrany ve všech budovách administrativního komplexu ABC

Druhá varianta zajištění fyzické bezpečnosti v objektu je formou sdílené bezpečnosti ve všech třech budovách administrativního komplexu ABC. Ta je postavená na nepřetržité přítomnosti jednoho zaměstnance bezpečnostní společnosti a vytvoření bezpečnostního

centra v jednom ze tří budov komplexu. Zde by se nacházelo dalších šest bezpečnostních pracovníků, kteří by prováděli bezpečnostní obhlídky vnitřních prostor a perimetru okolí budovy.

Při provádění bezpečnostních obchůzek by využívali chodeb, které propojují jednotlivá administrativní centra. V případě budovy Alfa se toto propojení nachází v posledním patře a přízemí. V současnosti jsou tyto průchody zamčeny a nevyužívají se. Díky využití těchto propojení by se také navýšil počet únikových východů. V současnosti je v budově Alfa pouze jeden.

Následně by tato varianta zabezpečení vedla k centralizaci fyzické bezpečnosti objektu, na základě které by byla značně zlepšena komunikace mezi budovami (o bezpečnostní hrozbě v jedné budově by byly informovány ostatní budovy prakticky okamžitě) a také by došlo k výraznému navýšení počtu přítomných bezpečnostních pracovníků při případném bezpečnostním incidentu.

Pro přibližnou kalkulaci nákladu spojených s touto variantou zabezpečení bude opět využita hodnota pro průměrné náklady z tabulky 19. Výsledná cena bude nakonec rozpočítána mezi všechny budovy stejně. Tato varianta počítá s faktem, že v celém komplexu se bude neustále vyskytovat 9 příslušníků SBS. Jeden pracovník v prostorách recepce a 8 provádějící obchůzky. Pro výpočet ceny nákladů na jednoho příslušníka SBS byla využita následující rovnice: 157,70 (průměrné náklady) * 24 (hodin) * 365 (dní) / 12

Tabulka 21: Kalkulace nákladů druhé varianty [Zdroj: Vlastní]

Cena za 24hodinnovou ochranu 1 příslušníkem SBS	115 121 Kč
Cena za 24hodinnovou ochranu 9 příslušníky SBS	1 036 089 Kč
Výsledná cena (rozdělení nákladů mezi jednotlivé budovy)	**345 363 Kč**

9.1.3 Režimová opatření

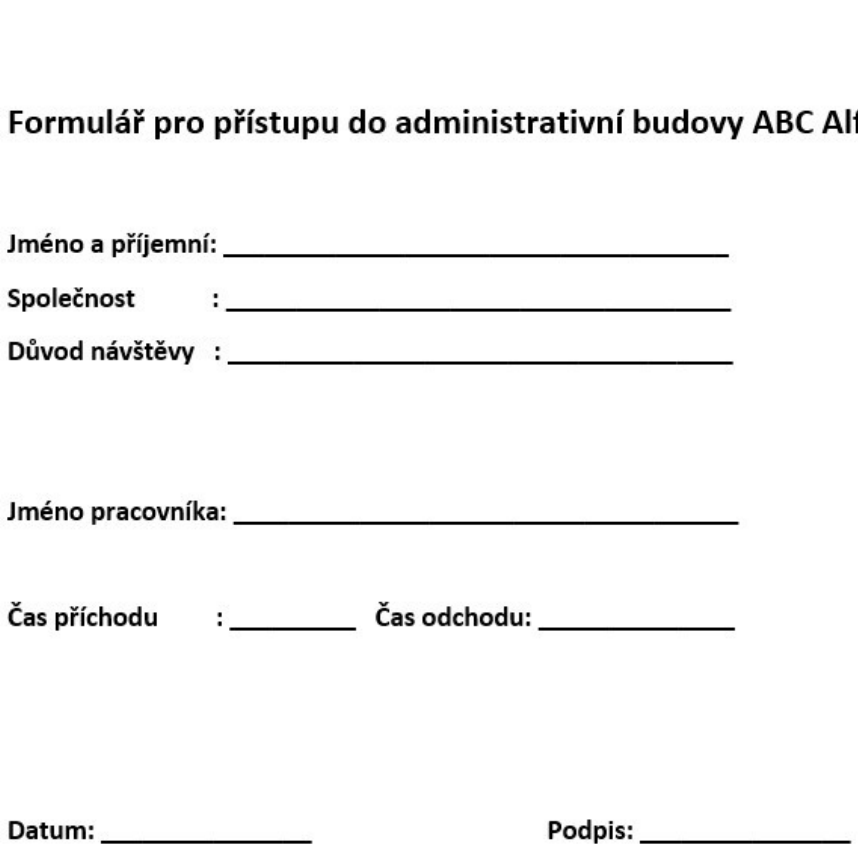
Režimová opatření slouží jako závazné pokyny, pravidla či nařízení zajišťující zamezení vzniku bezpečnostních hrozeb pro daný objekt. Může se jednat například o přístup jedince do prostoru, ve kterých by se neměl nacházet.

Prvním režimovým opatřením je vytvoření postupu, kterým by se obsluha recepce či přítomný bezpečností pracovník, ale také pověřená osoba (administrativní pracovníci jednotlivých firem nacházejících se v objektu) měla řídit při příchodu návštěvníka:

- Společnost informuje recepci o příchodu návštěvníka (přibližná hodina příchodu a jeho jméno).
- Zaměstnanec recepce vytvoří záznam.
- Návštěvníkovi je při příchodu předložen formulář, který obsahuje Jméno a Příjmení, firmu, kterou navštěvuje, účel návštěvy, čas odchodu a příchodu, jméno pracovníka, který jej přijímal a podpis návštěvníka.
- Zaměstnanec si vyžádá občanský průkaz či pas k potvrzení identity.
- Zaměstnanec recepce vytvoří záznam s časem příchodu návštěvníka do budovy.
- Návštěvníkovi je předána visačka, která jej identifikuje jako návštěvníka.
- Zaměstnanec recepce kontaktuje příslušnou firmu, ta má povinnost přijít do prostorů recepce a doprovodit návštěvníka do svých kancelářských prostor.
- Po ukončení schůzky pověřená osoba má povinnost odprovodit návštěvníka zpět do vstupní haly, kde odevzdá visačku a je zaznamenán jeho odchod.

Formulář by bylo možné vyplnit při příchodu do budovy, nebo před samotnou návštěvou a následně jej zaslat na k tomu vytvořenou e-mailovou adresu.

Formuláře budou po potřebnou dobu z bezpečnostních důvodů uchované v archivu administrativní budovy, pro případné dohledání návštěvníků, kteří mohli být zapojeni nebo mohli poskytnout informace k eventuálnímu bezpečnostnímu narušení.



Formulář pro přístupu do administrativní budovy ABC Alfa

Jméno a příjemní: _____

Společnost : _____

Důvod návštěvy : _____

Jméno pracovníka: _____

Čas příchodu : _____ **Čas odchodu:** _____

Datum: _____ **Podpis:** _____

Obrázek 17: Vzorový formulář pro přístup do administrativního centra [Zdroj: Vlastní]

Dalším opatřením je vytvoření rozvrhu nepravidelných bezpečnostních obchůzek příslušníků SBS v prostorách administrativní budovy/komplexu, který bude výrazně zmenšovat pravděpodobnost vytipování času obchůzek potencionálním útočníkem.

Následující opatření je založeno, na již fungujícím systému přístupových karet, který umožňuje vstup zaměstnancům do prostoru budovy. V současném řešení jsou rozděleny přístupové karty jednotlivým nájemcům, ale nejsou nijak identifikovatelné (v systému jsou pouze sériová čísla karet, které byly předány pověřeným osobám daných firem). Nový systém je založený na přiřazení karet konkrétním zaměstnancům. Následně by této kartě bylo přiděleno oprávnění přistupovat pouze do prostorů, do kterých má daný zaměstnanec přístup. Dále by na jednotlivé karty přibyly fotografie vlastníků, potvrzení, že se jedná o zaměstnance a firma ve které pracují.

Tato opatření budou vést k lepšímu monitoringu pohybu osob a jejich doby přítomnosti v budově, k lepší organizaci systému a výrazně také ulehčí práci zaměstnanci recepce či příslušníkovi SBS při kontrole jednotlivých osob. Například se může jednat

o zaměstnance společnosti XXX, kterému bude přidělen přístup pro průchod vstupními dveřmi budovy, průchod přes terminál oddělující část pro veřejnost a zaměstnance a přístup do kancelářských prostor firmy.

Na základě kartového přístupu je možné vytvořit další režimová opatření, které budou navyšovat úroveň zabezpečení. Propojení kartového systému se závorami na parkovišti před administrativní budovou, na kterém mohou parkovat pouze automobily firemních flotil nebo osobní auta vrcholných představitelů jednotlivých společností. Vjezd a výjezd bude povolen pouze vybraným přístupovým kartám.

Nedílnou součástí prevence před potencionálními bezpečnostními hrozbami je pravidelné školení a nácvik modelových situací, k zajištění maximální možné připravenosti personálu pracujícího v budově. Na základě pozorování jednotlivých nácviků je možné určit úroveň připravenosti pověřených pracovníků, ale také běžného personálu.

9.1.4 Technické a mechanické zabezpečení

Jak již bylo zmíněno v úvodu kapitoly administrativní centrum je z pohledu technického vybavení zabezpečeno na poměrně vysoké úrovni. Ovšem najdou se zde slabiny, které vyplynuli jak z jednotlivých analýz, tak také z vytvořeného stromu událostí (příloha P3) a popisu scénářů jednotlivých bezpečnostních situací.

Prvním potencionálně slabým místem zabezpečení je schodiště, které se nachází ve vstupní hale a vede do mezipatra a následně do suterénu budovy administrativního centra (Obrázek: 5). Na základě toho, že vstupní hala je volně dostupná veřejnosti je velmi pravděpodobné, že do této oblasti může vstoupit osoba, která by zde neměla přístup. Proto je nutné tento vchod zabezpečit turniketem (stejně jako je oddělený prostor pro veřejnost a zaměstnance), kterým budou moci projít pouze zaměstnanci.

Další opatření vyplývá z kapitoly 8.1. Scénář 1.: Verbální agrese s eskalací k fyzickému násilí, kde bylo popsáno, jak snadné je překonat překážku recepce a napadnout právě zaměstnance, který se zde nachází. Proto by vstup do recepce měl být zajištěn bezpečnostními dveřmi, které budou fungovat pomocí přístupového systému karet a přístup do něj budou mít pouze zaměstnanci recepce a příslušníci SBS. Dále by bylo vhodné zvednout přepážku recepce a přidat bezpečnostní sklo, které zamezí překonání překážky pultu recepce.

Jednou z nejlépe hodnocených příležitostí SWOT analýzy jsou finanční zdroje majitele objektu, na základě kterých by jednotlivá opatření nemělo být problém provést.

Tato kapitola byla věnována souhrnnému zhodnocení současného bezpečnostního stavu budovy, identifikování potencionálně slabých míst a jejich následnému návrhu zabezpečení. Součástí kapitoly je navržení dvou variant zajištění fyzické bezpečnosti objektu, a to přímé posílení administrativní budovy ABS Alfa nebo zajištění sdílené bezpečnosti v prostorách celého administrativního komplexu ABC.

Byla zde také znázorněna tabulka průměrného platu příslušníka SBS, která byla sdílena Českým klubem bezpečnostních služeb z.s., na základě které je možné si představit, jak velké finanční prostředky je nutné vynaložit na zajištění dostačující fyzické ochrany.

Následně byly autorem vytvořeny režimová opatření, jako je vytvoření metodiky a formuláře pro příchod návštěvy do prostor administrativního centra anebo podstatné zlepšení využití kartové přístupu do budovy. Poslední opatření jsou technického rázu, a to přidání vstupního turniketu na schodiště vedoucího do suterénu a zajištění větší bezpečnosti v prostoru recepce.

ZÁVĚR PRAKTICKÉ ČÁSTI

První kapitola praktické části je zaměřená na popis vybraného administrativního centra ABC alfa, které je součástí administrativního komplexu ABC nacházející se v Ostravě. Kapitola popisuje objekt definovaný jako administrativní centrum a zběžně nastiňuje historii objektu. Dále kapitola popisuje vnitřní prostory administrativního centra (vstupní halu, suterén a jednotlivá patra budovy) a přilehlé okolí. Následně se kapitola věnuje analýze bezpečnostní situace v přilehlém okolí objektu, který vychází z dat webového portálu www.mapakriminality.cz. a z popisu budov, které se v okolí nacházejí. Poté je provedeno posouzení zabezpečení objektu budovy a jeho vnitřních prostor. Nakonec je vytvořen katalog hrozeb, který je konkretizovaný na vybrané administrativní centrum.

Následující kapitola popisuje vybrané analytické metody SWOT a CARVER, které byly pro potřeby diplomové práce vybrány. První část je zaměřená na krátký popis SWOT analýzy a následné zvolení slabých a silných stránek objektu a také jeho příležitostí a hrozeb. Nakonec byla vytvořena stupnice, dle které je možné stanovit stupeň zabezpečení administrativního centra. Druhá část kapitoly popisuje metodu CARVER, která slouží k analýze objektu z pohledu útočníka.

Třetí kapitola praktické části obsahuje dva modelové scénáře, které popisují vybrané bezpečnostní incidenty. Prvním je verbální agrese s eskalací k fyzickému násilí, která nastiňuje situaci nespokojeného návštěvníka v administrativním centru. Scénář je obohacen o rozvětvený strom událostí znázorňující několik možných variant dopadu tohoto incidentu. Druhým scénářem je bombový útok. Scénář je zaměřen na neznámého pachatele, který v prostorách haly zanechá neznámý balíček obsahující výbušninu. Scénář je doplněn o výstup ze softwarového nástroje TerEX, které naznačuje škody, který by případný výbuch takovéto výbušniny mohl napáchat.

Poslední kapitola je zaměřená na závěrečné posouzení a návrh bezpečnostních opatření pro administrativní centrum. Autorem jsou navrženy dvě varianty zabezpečení založené na posílení fyzické ochrany a jejich následné kalkulace. První návrh je zaměřen na posílení fyzické ochrany přímo v objektu administrativní budovy Alfa a druhý na zajištění sdílené fyzické ochrany v celém administrativním komplexu (budovy Alfa, Beta a Gama). Dále jsou autorem vytvořena režimová opatření, mezi které patří například vytvoření formuláře a postupu pro přijímání návštěv v budově. Poslední část kapitoly je zaměřená na zlepšení

technického a mechanické zabezpečení jako je například přidání turniketu k zamezení vstupu do suterénu budovy.

ZÁVĚR

Hlavním cílem této diplomové práce bylo zhodnotit a následně navrhnout bezpečnostní opatření minimalizující potencionální hrozby vybraného administrativního centra z pohledu měkkých cílů.

První kapitola teoretické části pojednávala o právním rámci, který je relevantní pro problematiku bezpečnosti měkkých cílů. Především se jednalo o trestní zákoník a jeho paragrafy popisující pojmy jako jsou například teroristický útok či teror. Následující kapitola přibližovala čtenáři definici pojmu a možnosti rozdělení měkkých cílů a jejich odlišnosti od cílů tvrdých. Poté byly nastíněny principy, východiska a základní pilíře pro ochranu měkkých cílů z pohledu vlády České republiky vycházejícího z metodiky – Základy ochrany měkkých cílů. Další kapitola byla zaměřená na vysvětlení, rozdělení a popsání vybraných metod analýzy rizik. Následně kapitola pojednává o aktuálních hrozbách pro měkké cíle v České republice jako jsou například terorismus nebo organizovaný zločin. Čtvrtá kapitola přibližuje čtenáři bezpečnost měkkých cílů, a to v podobě jejich diagnostiky a popisu prostředků a postupů pro jejich zabezpečení. Kapitola následně pojednává o bezpečnostních prvcích, mezi které patří fyzická bezpečnost, režimová opatření a STO. Poté je představena role běžného občana jako prostředku pro zabezpečení měkkých cílů. Poslední kapitola teoretické části se věnuje softwarovému nástroji TerEX, který slouží k modelování nehod například výbuchu či úniku nebezpečné látky.

První kapitola praktické části je zaměřená na popis vybraného administrativního centra Alfa, které je součástí administrativního komplexu ABC nacházejícího se v Ostravě. Po zevrubném popisu rozložení vnitřních prostor budovy se kapitola zaměřuje na popis nejbližšího okolí, a to především budov, které se zde nacházejí. Následně se kapitola věnuje bezpečnostnímu posouzení blízkého okolí, a to především na základě dat z roků 2019 a 2020 získaných z webového portálu www.mapakriminality.cz. Od bezpečnostního posouzení okolí se kapitola následně přesunuje k bezpečnostnímu posouzení samotné budovy administrativního centra, které vychází z poznatků autora při návštěvě objektu. Nakonec byl vytvořen katalog hrozeb, který byl konkretizován pro potřeby vybraného objektu.

Druhá kapitola byla vytvořena za účelem provedení analýz rizik. První analýzou je analýza SWOT, pro kterou byly vybrány silné a slabé stránky a příležitosti a hrozby objektu. Mezi nejsilnější stránku patří IBS systém, na základě kterého je objekt zabezpečen na poměrně vysoké úrovni, ovšem objekt disponuje také poměrně velkou slabou stránkou

a to je nedostatečné zastoupení příslušníku SBS v objektu, na základě které vznikají mezery v bezpečnostním systému. Následně byly v analýze odhaleny slabiny jako je vandalismus (vysoká kriminalita v okolí a přítomnost historických fresek na fasádě budovy). Objekt také disponuje širokou řadou příležitostí jako jsou dostatečné finanční zdroje, které mohou být využity k posílení zabezpečení. Druhá část je zaměřená na metodu CARVER, která hodnotí hrozby z pohledu útočníka. Pro lepší orientaci byla popsána stupnice hodnocení jednotlivých kritérií metody CARVER. K vybrání hrozeb sloužil autorovi předem vytvořený katalog hrozeb. Z výsledků metody CARVER byly zjištěny největší hrozby, mezi které patří teroristický útok, kolaps budovy či požár, vysoce se také umístila hrozba absence bezpečnostní hlídky.

Následující kapitola popisuje vybrané bezpečnostní incidenty formou scénářů. První scénář popisuje příchod návštěvníka do budovy administrativního centra a jeho rostoucí agresivitu, která vede až k fyzickému napadení zaměstnance recepce. Scénář je obohacen o poměrně rozsáhlý strom událostí, který je zaměřený na popis možných konců, který tento incident může mít. Ze scénáře vyvstaly informace o nízkém zabezpečení recepce a také o důležitosti přítomnosti příslušníků SBS v budově. Druhý scénář popisuje bombový útok. Neznámý pachatel vchází do budovy a ve vstupní hale zanechává neznámý balíček. Celý scénář nastiňuje důležitost připravenosti zaměstnanců v takovýchto momentech a také zdůrazňuje, že veřejně dostupná hala bez přítomnosti příslušníků SBS je zdrojem nebezpeční. Scénář je doplněn o výsledky ze softwaru TerEX, pomocí kterého můžeme detailně znázornit zónu zasaženou výbuchem.

Na základě výsledku z přechozích kapitol byly vytvořeny dva návrhy zabezpečení. První je zaměřený na posílení fyzické ochrany přímo v objektu. Díky navýšení počtu přítomných příslušníků SBS dojde k výraznému snížení rizika výskytu bezpečnostních hrozeb v objektu. Druhou variantou je propojení fyzické bezpečnosti všech budov administrativního centra. Toto řešení přináší výhody v množství přítomných SBS pracovníků, možnosti rychlejší reakce na hrozby ve všech objektech a také využití propojení mezi budovami, které se v současnosti nevyužívá (přibydou únikové východy). Cena obou řešení je totožná, a tudíž druhé řešení je optimální variantou. Dále byla vytvořena režimová opatření, a to především využití kartového systému, který je v současnosti využíván pouze okrajově a vytvoření metodiky a formuláře pro návštěvníky budovy. Nakonec byly v na základě prvního scénáře navrženy opatření zabezpečující prostor recepce a vstupu do suterénu budovy.

10 SEZNAM POUŽITÉ LITERATURY

[1] 40/2009 Sb. Trestní zákoník. *Zákony pro lidi* [online]. Zlín: AION CS, s.r.o., 2010-2021 [cit. 2021-05-15]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40?text=40%2F2009

[2] Trestní zákoník - Aktuálně.cz. *Aktuálně.cz* [online]. Praha 8: Economia a.s., 2021 [cit. 2021-05-15]. Dostupné z: https://www.aktualne.cz/wiki/domaci/trestni-zakonik/r~i:wiki:3750/

[3] 239/2000 Sb. Zákon o integrovaném záchranném systému. *Zákony pro lidi* [online]. Zlín: AION CS, s.r.o., 2010-2021 [cit. 2021-05-15]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-239

[4] 240/2000 Sb. Krizový zákon. *Zákony pro lidi* [online]. Zlín: AION CS, s.r.o., 2010-2021 [cit. 2021-05-15]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-240

[5] 133/1985 Sb. Zákon o požární ochraně. *Zákony pro lidi* [online]. Zlín: AION CS, s.r.o., 2010-2021 [cit. 2021-05-15]. Dostupné z: https://www.zakonyprolidi.cz/cs/1985-133

[6] VALOUCH, Jan. *PROJEKTOVÁNÍ BEZPEČNOSTNÍCH SYSTÉMŮ* [online]. Druhé. Zlín: Univerzita Tomáše Bati ve Zlíně, 2019 [cit. 2021-05-15]. ISBN 978-80-7454-858-1. Dostupné z: https://digilib.k.utb.cz/handle/10563/45863

[7] Návrh zákona o soukromé bezpečnostní činnosti - Ministerstvo vnitra České republiky. *Ministerstvo vnitra České republiky* [online]. Praha 7: Ministerstvo vnitra České republiky, 2021 [cit. 2021-05-15]. Dostupné z: https://www.mvcr.cz/clanek/navrh-zakona-o-soukrome-bezpecnostni-cinnosti.aspx

[8] Vláda schválila návrh zákona o soukromých bezpečnostních službách - Ministerstvo vnitra České republiky. *Ministerstvo vnitra České republiky* [online]. Praha 7: Ministerstvo vnitra České republiky, 2021 [cit. 2021-05-15]. Dostupné z: https://www.mvcr.cz/clanek/vlada-schvalila-navrh-zakona-o-soukromych-bezpecnostnich-sluzbach.aspx

[9] Securing Soft Targets and Crowded Places Resources | CISA. *Cybersecurity & Infrastructure Secutrity Agency CISA* [online]. Rosslyn, Arlington, Virginia: Department of Homeland Security, 2018 [cit. 2021-05-15]. Dostupné z: https://www.cisa.gov/publication/securing-soft-targets-and-crowded-places-resources

[10] *Koncepce ochrany měkkých cílů pro 2017-2020* [online]. Praha 7: Ministerstvo vnitra, 2017 [cit. 2021-05-16]. Dostupné z: https://www.mvcr.cz/clanek/vlada-schvalila-koncepci-ochrany-mekkych-cilu-pro-roky-2017-2020.aspx#:~:text=Zpravodajstv%C3%AD-,Vl%C3%A1da%20schv%C3%A1lila%20Koncepci%20ochrany%20m%C4%9Bkk%C3%BDch%20c%C3%ADl%C5%AF%20pro%20roky%202017%E2%80%932020,pro%20roky%202017%20a%C5%BE%202020.&text=C%C3%ADlem%20koncepce%20je%20vytvo%C5%99it%20funguj%C3%ADc%C3%AD,pru%C5%BEn%C4%9B%20reagovat%20na%20vnikl%C3%A9%20hrozby.

[11] APELTAUER, Tomáš, Zdeněk DUFEK, Benedikt VANGELI et al. *Ochrana měkkých cílů*. Vydání první. Praha: Leges, 2019. ISBN isbn978-80-7502-427-5.

[12] KALVACH, Zdeněk.*Metodika - Základy ochrany měkkých cílů.pdf* [online]. Praha 7: Ministerstvo vnitra, 2016 [cit. 2021-05-16]. Dostupné z: https://www.mvcr.cz/clanek/ochrana-mekkych-cilu.aspx

[13] Řízení rizik (Risk Management) - ManagementMania.com. *Managementmania* [online]. Wilmington, New Castle County Delaware 19803: ManagementMania's Series of Management ISSN 2327-3658, 2011-2016 [cit. 2021-05-15]. Dostupné z: https://managementmania.com/cs/rizeni-rizik

[14] ŠEFČÍK, Vladimír. *Analýza rizik*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009. ISBN 9788073186968.

[15] Analýza rizik: Jemný úvod do analýzy rizik - CleverAndSmart Management Consulting. *Clever and Smart* [online]. Zálepy: Miroslav Čermák, 2021 [cit. 2021-05-15]. Dostupné z: https://www.cleverandsmart.cz/analyza-rizik-jemny-uvod-do-analyzy-rizik/

[16] Rizika (Risks) - ManagementMania.com. *Managementmania* [online]. Wilmington, New Castle County Delaware 19803: ManagementMania's Series of Management ISSN 2327-3658, 2011-2016 [cit. 2021-05-15]. Dostupné z: https://managementmania.com/cs/rizika

[17] Identifikace a hodnocení rizik - Znalostní systém prevence rizik v BOZP. *Zsbozp - Znalostní systém prevence rizik v BOZP* [online]. Praha 1: Výzkumný ústav bezpečnosti práce, v. v. i., 2021 [cit. 2021-05-15]. Dostupné z: https://zsbozp.vubp.cz/prevence-rizik/rizika-a-nebezpeci/130-identifikace-a-hodnoceni-rizik,

[18] Analýza a řízení rizik BOZP. Hodnocení a management | BOZP.cz. *BOZP.cz* [online]. Brno: CRDR spol. s r.o., 2021 [cit. 2021-05-15]. Dostupné z: https://www.dokumentacebozp.cz/aktuality/analyza-rizik-bozp-rizeni-hodnoceni-identifikace-management/

[19] Analýza rizik: kvantitativní vs. kvalitativní - CleverAndSmart Management Consulting. *Clever and Smart* [online]. Zálepy: Miroslav Čermák, 2021 [cit. 2021-05-15]. Dostupné z: https://www.cleverandsmart.cz/analyza-rizik-kvantitativni-vs-kvalitativni/

[20] Analýza rizik | GUARD7. *GUARD7* [online]. Pardubice: GUARD7, 2021 [cit. 2021-05-15]. Dostupné z: https://www.guard7.cz/lexikon/analyza-rizik

[21] Metody hodnocení rizik | GUARD7. *GUARD7* [online]. Pardubice: GUARD7, 2021 [cit. 2021-05-15]. Dostupné z: https://www.guard7.cz/po/metody-hodnoceni-rizik

[22] Využití kontrolních seznamů k interním kontrolám v organizacích | BOZPinfo.cz. *BOZPinfo.cz* [online]. Praha 1: Výzkumný ústav bezpečnosti práce, v. v. i., 2021 [cit. 2021-05-15]. Dostupné z: https://www.bozpinfo.cz/vyuziti-kontrolnich-seznamu-k-internim-kontrolam-v-organizacich

[23] Metody hodnocení rizik - Znalostní systém prevence rizik v BOZP. *Zsbozp - Znalostní systém prevence rizik v BOZP* [online]. Praha 1: Výzkumný ústav bezpečnosti práce, v. v. i., 2021 [cit. 2021-05-15]. Dostupné z: https://zsbozp.vubp.cz/prevence-rizik/rizika-a-nebezpeci/371-metody-hodnoceni-rizik#:~:text=Bezpe%C4%8Dnostn%C3%AD%20kontrola%20je%20postup%20hledaj%C3%ADc%C3%AD,a%20matice%20pro%20sk%C3%B3rov%C3%A1n%C3%AD%20rizik

[24] Co - když analýza (What-if Analysis) - ManagementMania.com. *Managementmania* [online]. Wilmington, New Castle County Delaware 19803: ManagementMania's

Series of Management ISSN 2327-3658, 2011-2016 [cit. 2021-05-15]. Dostupné z: https://managementmania.com/cs/co-kdyz-analyza-what-if-analysis

[25] HAZOP (Hazard and Operability Study) - ManagementMania.com. *Managementmania* [online]. Wilmington, New Castle County Delaware 19803: ManagementMania's Series of Management ISSN 2327-3658, 2011-2016 [cit. 2021-05-15]. Dostupné z: https://managementmania.com/cs/hazop-hazard-and-operability-study-analyza-ohrozeni-a-provozuschopnosti

[26] FTA (Fault Tree Analysis) - Analýza stromu poruchových stavů - ManagementMania.com. *Managementmania* [online]. Wilmington, New Castle County Delaware 19803: ManagementMania's Series of Management ISSN 2327-3658, 2011-2016 [cit. 2021-05-15]. Dostupné z: https://managementmania.com/cs/fault-tree-analysis#:~:text=Metoda%20FTA%20(Fault%20Tree%219550Analysis,pou%C5%BE%C3%ADv%C3%A1%20se%20obvykle%20zkratka%20FTA.&text=Jej%C3%ADm%20c%C3%ADlem%20je%20detailn%C3%AD%20anal%C3%BDza,pou%C5%BE%C3%ADt%20metody%20FMEA%20nebo%20HAZOP.

[27] Metoda CARVER | GrowJOB Institute. *GROWJOB* [online]. Brno: GrowJOB Institute, 2021 [cit. 2021-05-15]. Dostupné z: https://www.growjob.com/clanky-personal/metoda-carver/

[28] What is CARVER?. *SECURITY MANAGEMENT INTERNATIONAL, LLC - Intelligent Security Solution* [online]. Vienna, Virginia, USA: SMI, 2021 [cit. 2021-05-15]. Dostupné z: https://www.smiconsultancy.com/what-is-carver

[29] Národní kontaktní bod pro terorismus - Policie České republiky. *POLICIE ČESKÉ REPUBLIKY* [online]. Praha 7: Policie ČR, 2021 [cit. 2021-05-15]. Dostupné z: https://www.policie.cz/clanek/kopie-terorismus.aspx?q=Y2hudW09Mg%3d%3d

[30] Definice pojmu terorismus - Ministerstvo vnitra České republiky. *Ministerstvo vnitra České republiky* [online]. Praha 7: Ministerstvo vnitra České republiky, 2021 [cit. 2021-05-15]. Dostupné z: https://www.mvcr.cz/clanek/definice-pojmu-terorismus.aspx

[31] Terorismus | BIS. *BEZPEČNOSTNÍ INFORMAČNÍ SLUŽBA* [online]. Praha: Bezpečnostní informační služba, 2021 [cit. 2021-05-15]. Dostupné z: https://www.bis.cz/terorismus/

[32] Co je organizovaný zločin - Policie České republiky. *POLICIE ČESKÉ REPUBLIKY* [online]. Praha 7: Policie ČR, 2021 [cit. 2021-05-15]. Dostupné z: https://www.policie.cz/clanek/co-je-organizovany-zlocin.aspx

[33] Bezpečnostní hrozby - Ministerstvo vnitra České republiky. *Ministerstvo vnitra České republiky* [online]. Praha 7: Ministerstvo vnitra České republiky, 2021 [cit. 2021-05-15]. Dostupné z: https://www.mvcr.cz/clanek/bezpecnostni-hrozby-337414.aspx?q=Y2hudW09Mg%3d%3d

[34] Advanced Persistent Threat (APT). *AEC* [online]. Brno: AEC, 2021 [cit. 2021-05-15]. Dostupné z: https://www.aec.cz/cz/Documents/Files/AEC-Advanced-Persistent-Thread.pdf

[35] Co je extremismus - Ministerstvo vnitra České republiky. *Ministerstvo vnitra České republiky* [online]. Praha 7: Ministerstvo vnitra České republiky, 2021 [cit. 2021-05-15]. Dostupné z: https://www.mvcr.cz/clanek/co-je-extremismus.aspx

[36] Co je extremismus? - Policie České republiky. *POLICIE ČESKÉ REPUBLIKY* [online]. Praha 7: Policie ČR, 2021 [cit. 2021-05-15]. Dostupné z: https://www.policie.cz/clanek/ncoz-extremismus-co-je-extremismus.aspx

[37] V čem spočívá hrozba extremismu - Ministerstvo vnitra České republiky. *Ministerstvo vnitra České republiky* [online]. Praha 7: Ministerstvo vnitra České republiky, 2021 [cit. 2021-05-16]. Dostupné z: https://www.mvcr.cz/clanek/v-cem-spociva-hrozba-extremismu.aspx

[38] *Vyhodnocení ohroženosti měkkého cíle* [online]. Praha 7: Ministerstvo vnitra, 2016 [cit. 2021-05-16]. Dostupné z: https://www.mvcr.cz/cthh/clanek/vyhodnoceni-ohrozenosti-mekkeho-cile-metodika-ke-stazeni.aspx

[39] BARTA, Jiří a Tomáš LUDÍK. *TerEx – modelování a simulace (Studijní pomůcka pro předmět KRIZOVÉ SCÉNAŘE)* [online]. Brno: Univerzita obrany, 2012 [cit. 2021-05-16]. Dostupné z: https://moodle.unob.cz/pluginfile.php/26278/mod_resource/content/1/Studijni_pomucka_TerEx.pdf

[40] Ocenění pro kancelářský objekt ALFA v Ostravě. *Deník.cz* [online]. Ostrava: VLTAVA LABE MEDIA a.s., 2021 [cit. 2021-05-16]. Dostupné z: https://moravskoslezsky.denik.cz/podnikani/oceneni-pro-kancelarsky-objekt-alfa-20181124.html

[41] Naše portfolio | Asental. *Asental Group* [online]. Ostrava: Asental Group, 2021 [cit. 2021-05-16]. Dostupné z: https://www.asental.eu/cs/komercni-objekty/nase-portfolio/abc-alfa

[42] Pronájem kanceláří ABC Alfa, Ostrava | OfficeMap. In: *OfficeMAP* [online]. Praha 1: Colliers International, 2021 [cit. 2021-05-16]. Dostupné z: https://www.officemap.cz/office/abc-alfa-prokesovo-namesti-20206

[43] Google Maps. *Google* [online]. Mountain View, California, United States: Google, 2021 [cit. 2021-05-16]. Dostupné z: https://www.google.com/maps/place/ABC+ALFA/@49.8419972,18.2868177,724m/data=!3m2!1e3!4b1!4m5!3m4!1s0x4713e325cf4d1a81:0x791a5525019a4b1f!8m2!3d49.8420507!4d18.2892272

[44] MAPAKRIMINALITY.CZ. *MAPAKRIMINALITY.CZ* [online]. Praha 2: Otevřená společnost, o.p.s., 2020 [cit. 2021-05-16]. Dostupné z: https://www.mapakriminality.cz/#mapa

[45] ABC ALFA, 6, Prokešovo nám. 634/5, 702 00 Moravská Ostrava a Přívoz, Česko. In: *2POS* [online]. Praha: 2POS Česká republika, 2021 [cit. 2021-05-16]. Dostupné z: http://2pos.cz/177362/20068/abc-alfa

[46] Fotobanka ČTK - Titulní stránka : Kancelářský komplex ABC, interiér, Asental Business Center, vstupní, docházkový turniket, budova Alfa, foyer. In: *ČTK Fotobanka* [online]. Praha1: Česká tisková kancelář., 2021 [cit. 2021-05-16]. Dostupné z: http://multimedia.ctk.cz/foto/document/33313562/7

[47] SWOT analýza - ManagementMania.com. *Managementmania* [online]. Wilmington, New Castle County Delaware 19803: ManagementMania's Series of Management ISSN 2327-3658, 2011-2016 [cit. 2021-05-16]. Dostupné z: https://managementmania.com/cs/swot-analyza#:~:text=SWOT%20anal%C3%BDza%20je%20univerz%C3%A1ln%C3%AD%20analytick%C3%A1,r%C3%A1mci%20strategick%C3%A9ho%20%C5%99%C3%ADzen%C3%AD%20a%20marketingu.

[48] Semtex - legendární výbušnina, která proslavila Československo | ARMYWEB.cz. *Armyweb ARMY LIFESTYLE MAGAZINE* [online]. Plzeň: ArmyWeb.cz, 2013 [cit. 2021-05-16]. Dostupné z: https://www.armyweb.cz/clanek/semtex-vybusnina-ktera-proslavila-ceskoslovensko

[49] *CENY ZA FYZICKOU OSTRAHU V ROCE 2020* [online]. Praha 9: ckbs.cz, 2020 [cit. 2021-05-16]. Dostupné z: http://www.profesnikvalifikacestrazny.cz/wp-content/uploads/2016/01/Cena-ostrahy_2020.pdf

[50] KYNCL, Jaromír. *Bezpečnost objektu ve světle moderních technologií*. Vydání první. Praha: Komora podniků komerční bezpečnosti České republiky, 2014. ISBN 9788026071150.

[51] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management*. 1. vydání. Zlín: Radim Bačuvčík - VeRBuM, 2011-2015. ISBN 9788087500194.

[52] PALEČEK, Miloš. *Prevence rizik*. Vyd. 1. Praha: Oeconomica, 2006. ISBN 8024511177.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ABC	Administrativní komplex (Alfa, Beta, Gama)
ATP	Advanced Persistent Threat
BOZP	Bezpečnost a ochrana zdraví při práci
CCTV	Closed-Circuit Television
FTA	Fault Tree Analysis
HAZOP	Hazard and Operability Study
IBS	Integrovaný bezpečnostní systém
IZS	Integrovaný záchranný systém
PCO	Pult centralizované ostrahy
PIR	Passive Infrared Detector
PKB	Průmysl komerční bezpečnosti
SBS	Sbor soukromé bezpečnostní služby
SEALs	The United Sates Navy Sea, Air, and Land Teams
STO	Systém technické ochrany

SEZNAM OBRÁZKŮ A GRAFŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P 1: OBSAH DISKU CD

- \fulltext.pdf
- \prilohy
    - Data_SWOT&CARVER
    - Priloha_2_formular
    - Priloha_3_strom_udalosti

PŘÍLOHA P 2: FORMULÁŘ

ASENTAL

Formulář pro přístupu do administrativní budovy ABC Alfa

Jméno a příjemní: _____

Společnost : _____

Důvod návštěvy : _____

Jméno pracovníka: _____

Čas příchodu : _____ **Čas odchodu:** _____

Datum: _____ **Podpis:** _____

PŘÍLOHA P 3: STROM UDÁLOSTÍ