

Analýza bezpečnosti rodinného zábavního parku ve Zlíně

Tomáš Nevřala



Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav bezpečnostního inženýrství

Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: Tomáš Nevřala
Osobní číslo: A22443
Studijní program: B1032A020001 Bezpečnostní technologie, systémy a management
Forma studia: Prezenční
Téma práce: Analýza bezpečnosti rodinného zábavního parku ve Zlíně
Téma práce anglicky: Safety analysis of a family amusement park in Zlín

Zásady pro vypracování

- Pojednejte o legislativě a právních předpisech ochrany měkkých cílů.
- Definujte jednotlivá ohrožení v souvislosti s provozem zábavního parku.
- Popište současné prvky ochrany parku.
- Provedte analýzu bezpečnostních rizik a prvků ochrany.
- Na základě výsledků analýzy navrhněte opatření k bezpečnému provozu zábavního parku.

Forma zpracování bakalářské práce: tištěná/elektronická

Seznam doporučené literatury:

1. VALOUCH, Jan. Projektování bezpečnostních systémů. Online. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2019. ISBN 978-80-7454-858-1.
2. LAUCKÝ, Vladimír. Technologie komerční bezpečnosti I. Zlín. Univerzita Tomáše Bati ve Zlíně. Vyd. 3. 2010. ISBN 978-80-7318-889-4.
3. LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management V. Zlín: VerBuM, 2015. ISBN 978-80-87500-67-5.
4. UHLÁŘ, Jan. Technická ochrana objektů. I. díl. Policejní akademie České republiky. Vyd 2. 2009. ISBN 978-80-7251-312-3.
5. KALVACH, Z., VANGELI, B. Vyhodnocení ohroženosti měkkého cíle: aneb co, kdy, kde a od koho vám hrozí. Ministerstvo vnitra ČR, Vyd. 1. Praha, 2018.

Vedoucí bakalářské práce: **Ing. Gabriela Králíčková**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **11. prosince 2024**
Termín odevzdání bakalářské práce: **2. června 2025**

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan



Ing. Jan Valouch, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 11. prosince 2024

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že

- odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení bakalářské práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – bakalářskou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na bakalářské práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne

.....
podpis autora

ABSTRAKT

Bakalářská práce se zabývá identifikací fyzických a technických hrozeb ve vazbě na možnost vzniku mimořádných událostí a efektivitu současných bezpečnostních opatření rodinného zábavního parku. Práce je rozdělena na teoretickou a praktickou část. Teoretická část pojednává o problematice měkkých cílů, legislativním rámci, analýze rizik a současných trendech v oblasti systémů technické ochrany. V praktické části je analyzována bezpečnost parku Galaxie ve Zlíně pomocí kontrolního seznamu, PNH metody a dalších analytických nástrojů. Na základě výsledků jsou navržena opatření ke zlepšení zabezpečení a zajištění bezchybného provozu.

Klíčová slova: bezpečnost, analýza rizik, hrozba, riziko, bezpečnostní opatření

ABSTRACT

The bachelor's thesis focuses on the identification of physical and technical threats in relation to the possibility of emergency events and the effectiveness of current safety measures in a family amusement park. The thesis is divided into theoretical and practical parts. The theoretical part deals with the issue of soft targets, the legislative framework, risk analysis, and current trends in technical security systems. The practical part analyzes the safety of the Galaxie amusement park in Zlín using a checklist, the PNH method, and other analytical tools. Based on the results, security improvements and measures to ensure error-free operation are proposed.

Keywords: Safety, Risk Analysis, Threat, Risk, Safety Measures

Rád bych poděkoval vedoucí mé bakalářské práce Ing. Gabriele Králíčkové a prof. Ing. Martinu Hromadovi, Ph.D. za jejich odborné vedení, cenné rady a připomínky. Mé poděkování rovněž patří vedení zábavního parku Galaxie zejména Kateřině Danielové a Ing. Janě Valáškové za podklady a informace pro zpracování.

OBSAH

ÚVOD	11
I TEORETICKÁ ČÁST	12
1 TEORETICKÝ RÁMEC BEZPEČNOSTI MĚKKÝCH CÍLŮ.....	13
1.1 ANALÝZA TERORISTICKÝCH ÚTOKŮ NA MĚKKÉ CÍLE.....	14
1.2 OBECNÁ VÝCHODISKA OCHRANY MĚKKÝCH CÍLŮ	16
1.3 LEGISLATIVA A PRÁVNÍ PŘEDPISY	18
1.3.1 Právní rámec problematiky	18
2 VYBRANÉ ASPEKTY MANAGEMENTU RIZIK	20
2.1 BEZPEČNOSTNÍ HROZBY, ANALÝZA A ŘÍZENÍ RIZIK	20
2.1.1 Hrozba.....	20
2.1.2 Nebezpečí.....	20
2.1.3 Riziko.....	21
2.1.4 Zranitelnost	21
2.2 METODY ANALÝZY RIZIK.....	21
3 SOUČASNÉ TRENDY SYSTÉMŮ TECHNICKÉ OCHRANY.....	24
3.1 MECHANICKÉ ZÁBRANNÉ SYSTÉMY	24
3.2 PLÁŠŤOVÁ OCHRANA.....	26
3.3 PROSTOROVÁ OCHRANA	26
3.4 INTEGROVANÝ BEZPEČNOSTNÍ SYSTÉM	26
3.5 POPLACHOVÝ ZABEZPEČOVACÍ A TÍŠŇOVÝ SYSTÉM (PZTS).....	27
3.5.1 Čidla kontaktní	29
3.5.2 Čidla pohybu	29
3.5.3 Antimasking	29
3.5.4 Detektory pohybu	30
3.6 PASIVNÍ DETEKTORY	31
3.6.1 Pasivní infračervené světla.....	31
3.6.2 Magnetické kontakty	32
3.6.3 Detektory tříštění skla.....	32
3.7 AKTIVNÍ DETEKTORY	32
3.7.1 Ultrazvukové detektory.....	32
3.7.2 Mikrovlnné detektory	33
3.8 ELEKTRICKÁ KONTROLA VSTUPU	33
3.8.1 Komponenty ESKV.....	34
3.9 BEZPEČNOSTNÍ KAMERY.....	34
II PRAKTICKÁ ČÁST.....	36
4 RODINNÝ ZÁBAVNÍ PARK GALAXIE.....	37

4.1	BEZPEČNOST RODINNÉHO ZÁBAVNÍHO PARKU	37
4.2	VÝSKYT BEZPEČNOSTNÍCH UDÁLOSTÍ	38
4.3	KONTROLNÍ SEZNAM AKTUÁLNÍHO STAVU (CHECK LIST)	38
5	ANALÝZA A HODNOCENÍ RIZIK	45
5.1	IDENTIFIKACE AKTIV	46
5.2	VYHODNOCENÍ PNH METODY	52
6	SOUČASNÝ STAV ZABEZPEČENÍ	54
6.1	AKTUÁLNÍ STAV PŘÍSTUPOVÝCH CEST A JEJICH ŘEŠENÍ	54
6.2	POPLACHOVÝ ZABEZPEČOVACÍ A TÍŠŇOVÝ SYSTÉM	55
6.2.1	Denní kontrola atrakcí	57
6.3	DVS A MONITOROVACÍ SYSTÉM	58
6.4	EVAKUAČNÍ SYSTÉMY	60
6.4.1	Požární hlídka	60
6.5	INCIDENT MANAGEMENT	61
6.5.1	Školení personálu	62
7	NÁVRH OPATŘENÍ	63
7.1	PERIMETRICKÁ OCHRANA A OKOLÍ BUDOVY	63
7.2	PLÁŠŤOVÁ OCHRANA BUDOVY	64
7.3	PROSTOROVÁ A PŘEDMĚTOVÁ OCHRANA	64
7.3.1	Kontrola vstupů	65
7.4	SCÉNÁŘ VYBRANÝCH BEZPEČNOSTNÍCH INCIDENTŮ	66
	ZÁVĚR	70
	SEZNAM POUŽITÉ LITERATURY	71
	SEZNAM OBRÁZKŮ	75
	SEZNAM TABULEK	76
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	77

ÚVOD

Rodinné zábavní parky jsou oblíbenými místy pro odpočinek a zábavu, kde lidé tráví čas s rodinou či přáteli. Jejich veřejná dostupnost a velké množství návštěvníků z nich však činí tzv. měkké cíle, které jsou náchylné k různým bezpečnostním rizikům. Mezi tyto hrozby patří například teroristické útoky, technické poruchy, krádeže nebo požáry. Aby byla zajištěna bezpečnost návštěvníků i zaměstnanců, je nutné přistupovat k ochraně těchto míst komplexně.

Cílem této bakalářské práce je analyzovat současný stav bezpečnosti rodinného zábavního parku Galaxie ve Zlíně, odhalit potenciální slabiny a navrhnout opatření, která posílí ochranu na fyzické, technologické i organizační úrovni. Práce vychází z teoretických základů, jako je definice měkkých cílů, analýza bezpečnostních hrozeb, přehled legislativy a moderních technologií, a aplikuje je na konkrétní případ.

Výsledky mají přispět k vyšší bezpečnosti parku Galaxie a vytvoření prostředí, kde se návštěvníci budou cítit bezpečně. V dnešní době, kdy ve veřejných prostorech narůstá počet bezpečnostních incidentů, je prevence a rychlá reakce na hrozby klíčová. Tato práce tak zdůrazňuje důležitost systematického přístupu k ochraně rodinných zábavních parků a nabízí praktická doporučení pro jejich zlepšení.

I. TEORETICKÁ ČÁST

1 TEORETICKÝ RÁMEC BEZPEČNOSTI MĚKKÝCH CÍLŮ

Měkké cíle jsou veřejná místa, ve kterých se může vyskytovat velký počet osob. Tato místa jsou spojena s žádnou nebo malou mírou ochrany a snadnou dostupností. Jejich ochrana a celkové zabezpečení je klíčové, protože hrozby, které mohou ohrožovat měkké cíle mají často široký dopad na společnost. Mezi nejrizikovější místa spadají veřejná prostranství, nákupní centra, koncertní sály, zábavní parky a další veřejné prostory, jenž bývají málokdy stejnou váhou zabezpečené jako kritická infrastruktura, u které je nutné se na celkovou bezpečnost zaměřovat. U teroristů, či aktivních střelců jsou tato místa vnímána jako snadný potenciální cíl útoku z důvodu vysoké četnosti pohybujících osob. [1]

V souvislosti s útoky na měkké cíle můžeme mluvit o hromadném strachu a nejistotě. Když je útok ze strany teroristů úspěšný, spustí řetězovou reakci. Média začínají informovat o události, široká veřejnost se bojí o svoji bezpečnost a státní orgány opět se scházejí a debatují o bezpečnosti své země. Všechny tyto procesy a úvahy vedou k tomu, že se o útočnících píše a vše medializuje, což jsou hlavní důvody činů. Teroristické organizace stojí o světovou pozornost a snaží se vyčnívat mezi dalšími organizacemi. [1]

Atraktivitu měkkého cíle pro útočníky mohou zvyšovat tato kritéria:

- otevřenost pro veřejnost
- přítomnost a kvalita bezpečnostního personálu
- množství a koncentrace osob
- přítomnost Policie České republiky nebo obecní (městské) policie
- přítomnost médií
- symboličnost cíle

Z pohledu zdroje ohrožení lze měkké cíle rozdělit následovně:

- cíle ohrožené jednotlivým aktivním útočníkem, a to bez ohledu na jeho motivaci
- cíle, které mohou být napadeny teroristickou organizací
- cíle v ohrožení ze strany jiné specifické skupiny, například organizovaného zločinu

Měkké cíle můžeme rozdělit na trvalé a dočasné.

Trvalé cíle se pak dělí na:

- a) venkovní prostory (například stadiony, sportovní areály, tržnice)
- b) vnitřní prostory (například rodinné zábavní parky, obchodní centra, divadla, zdravotnická zařízení)

Dočasné měkké cíle představují určitá shromáždění, obvykle venkovní akce, které mohou probíhat na veřejných i soukromých pozemcích. Tyto cíle lze dále rozdělit na:

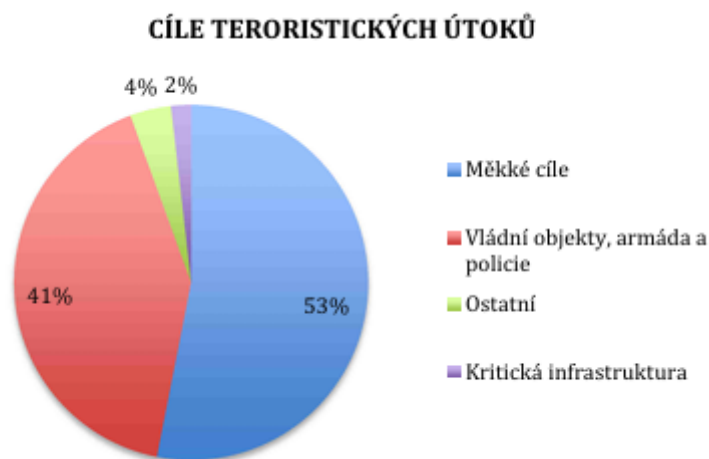
- a) dočasné akce se vstupným (například festivaly, koncerty)
- b) dočasné akce s volným přístupem (například demonstrace, vánoční či velikonoční trhy, další podobná setkání nebo sportovní setkání)

Další kategorií měkkých cílů může být sledování počtu osob v určitém intervalu. Tento interval se např. v rodinném zábavním parku může měnit v závislosti na tom, jaké je právě roční období. Poté bude jiná četnost osob o víkendech v odpoledních hodinách než v jiných všedních dnech. Takovou dobu nazýváme „peak time“, tedy doba, kdy je v určitém objektu nebo veřejném prostranství nejvyšší počet lidí. [1]

1.1 Analýza teroristických útoků na měkké cíle

Analýza je zaměřena na rozbor dostupných statistik vytvořených Ministerstvem vnitra České republiky, které umožňují přehledně porozumět typům útoků na jejich vybrané cíle. Takové analýzy jsou následně schopné v určitém směru ukázat chování teroristů a slouží nám k více efektivnímu zabezpečení objektů, kde se pohybuje veřejnost. [2]

Uvedené výšečové grafy ilustrují cíle a typy teroristických útoků v Evropě mezi lety 1998 a 2014. Oba grafy jsou rozděleny do několika kategorií a ukazují, jaké objekty či metody byly nejčastěji voleny teroristy v rámci evropského prostředí. [2]

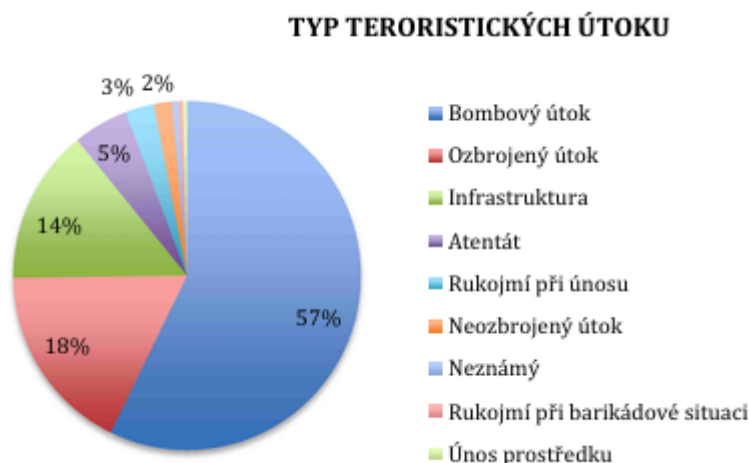


Obrázek 1 Analýza násilných útoků na vybrané cíle

(zdroj: [2])

První graf se zaměřuje na to, na jaké cíle byly útoky zaměřeny. Většina útoků (53 %) směřovala na tzv. měkké cíle. Další velká část (41 %) cílila na vládní objekty, armádu a policejní složky. To odráží skutečnost, že tyto instituce představují symboly moci a autority, což je pro teroristy atraktivní. [2]

Kritická infrastruktura, která zahrnuje důležité sítě jako energetické zdroje či dopravní infrastrukturu, představuje 4 % cílů. Kategorii „Ostatní“ tvoří zbývající 2 %, což mohou být specifické cíle nebo méně časté druhy útoků, které nespádají do výše zmíněných kategorií. [2]



Obrázek 2 Typ teroristických útoku

(zdroj: [2])

Druhý graf se zaměřuje na metody, jakými byly útoky provedeny. Největší podíl (57 %) představují bombové útoky, což odráží snadnou dostupnost výbušnin a jejich silný dopad na cíle i okolní veřejnost.

Ozbrojené útoky tvoří 18 % všech útoků. Jedná se o častou formu útoku, kdy jsou zbraně snadno přenosné a útočník má nad cílem přímou kontrolu.

Třetí nejčastější kategorií (14 %) je útok na infrastrukturu, což může zahrnovat sabotáž kritických systémů a narušení veřejných služeb.

Ostatní kategorie (každá méně než 10 %) zahrnují například atentáty (5 %), rukojmí při únosu, neozbrojené útoky a další. Každý typ útoku má svá specifika a různé dopady na bezpečnostní opatření a krizovou připravenost. [2]

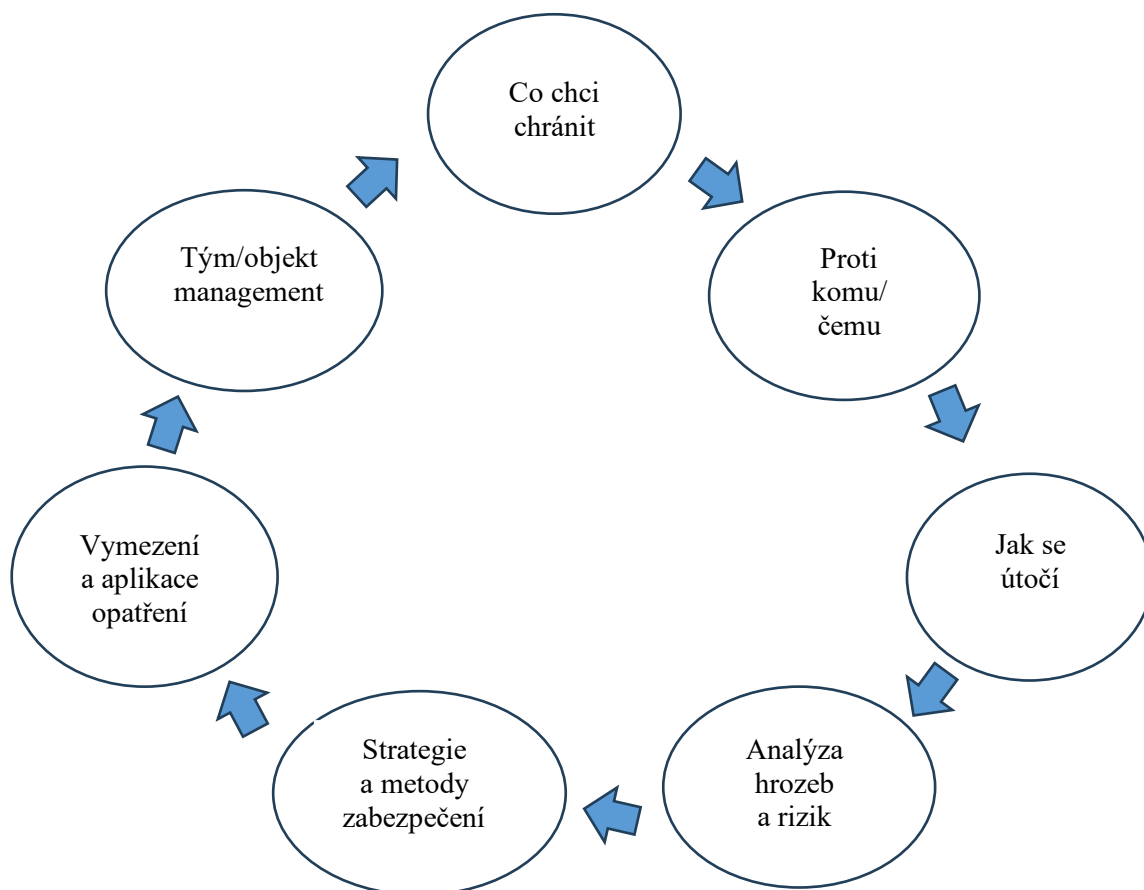
1.2 Obecná východiska ochrany měkkých cílů

Bezpečnostní opatření u míst výše zmiňovaných nelze zcela zaručit dokonale s porovnáním u objektů s vysokým stupněm ochrany, a proto jsou zranitelnější vůči ozbrojeným nebo násilným útokům. Mezi jedny z hlavních cílů u objektů, které jsou více zranitelné, je snaha minimalizovat možnost vzniku útoku a zajistit bezpečnost všech návštěvníků a také personálu.

Do dnešní doby bylo provedeno nespočet analýz provedení různých útoků na měkké cíle, zvláště pak jakým způsobem byly prováděny a součástí těchto šetření je i dopad

na veřejnost. Kromě toho je třeba zohlednit i psychologický efekt bezpečnostních opatření, který může přispět ke snížení pocitu ohrožení mezi návštěvníky.

Efektivní ochrana měkkých cílů vyžaduje pravidelnou aktualizaci bezpečnostních opatření a přizpůsobení se novým typům hrozeb. Z těchto analýz plyne, jaké kroky jsou potřeba provést pro nastavení funkčního systému pro bezpečnost.



Obrázek 3 Principy zabezpečení měkkých cílů

(zdroj: [3])

Základem je snaha vytvořit koncepční systém, jenž bude na začátku tvořen jasnou strukturou chráněných zájmů. Na úvod je potřeba si definovat to, čeho si vážíme a nechtěli bychom o to přijít. Ve valné většině jde hlavně o naše zdraví a životy ostatních osob, majetek nebo data. Soustředěnost je věnována především na ochranu života a zdraví před násilnými útoky, ale navržená opatření mohou zároveň pomoci předcházet narušení veřejného pořádku

a poškození majetku. Může také sloužit jako prevence proti nebezpečným situacím způsobeným technickými haváriemi. [2]

Další část se zabývá hrozbami a možnými zdroji nebezpečí s ohledem na objekt který zabezpečujeme. Poté je třeba identifikovat možné nepřátelské skupiny nebo osoby s potenciální motivací zaútočit. K tomu jsou používána data získaná z útoků z minulých let. K další specifikaci je nutno zohlednit i různé zvláštnosti daného místa např. návštěva vysokých představitelů států nebo riziko v datu konání akce. [2]

Bezpečnostní systém musí zaručovat důkladnou analýzu konkrétních hrozeb a způsobu útoku, aby byl co nejvíce efektivní a úsporný. Analyzované hrozby jsou zkoumány pomocí různých metod, aby se identifikovaly ty nejzávažnější. Dále je třeba odborně posoudit pravděpodobnost skutečné realizace hrozby a v závěru vyhodnotit výsledky. [2]

Po identifikaci možných hrozeb a k nim udělení patřičných bezpečnostních opatření jsou tato opatření aplikována na daný objekt. Podle toho jsou v objektu rozmísťovány technické prvky na ochranu a vytvořeny únikové a další bezpečnostní plány, které jsou v případě nenadálých situací připraveny minimalizovat vzniklé škody. [2]

1.3 Legislativa a právní předpisy

Evropští i čeští zástupci spravují legislativu podle aktuálních hrozeb na veřejně přístupné objekty, jako jsou školy nebo zdravotnická zařízení. Ochrana měkkých cílů patří na celém světě mezi hlavní bezpečnostní témata posledních dvou dekad. Právní předpisy jsou zaměřené na snížení rizik spojených s násilnými útoky. [3]

1.3.1 Právní rámec problematiky

Po tragické události v prosinci roku 2023 v Praze na Univerzitě Karlově, kdy mladý střelec zabil několik lidí a další dvě desítky byly zraněny, vycházely na povrch otázky, zda je legislativa a právní normy v České republice správně nastavena. Po této smutné až bolestivé události bylo řečeno, že legislativa je dostatečná, ale ochrana měkkých cílů je v dnešní době nevyhovující.

Jeden z představitelů české politické strany zdůraznil, že je potřeba zvýšit tlak na jednotlivé instituce. Další člen jiné politické strany podotkl, že na prvním místě jsou občané ČR a poté je možno analyzovat případy a vyhodnocovat, zda je v legislativě něco špatně. [4]

Společně s dalšími členy, kteří se zaměřují na oblast bezpečnosti, se shodli na tom, že je nejdůležitější začít diskutovat o bezpečnosti s jednotlivými subjekty, ve kterých se shromažďuje nejvíce osob. To by podle jejich slov znamenalo, že tyto instituce budou schopny reagovat na hrozby, či jakákoliv rizika a zároveň je nutné, aby osoby v objektu věděly, jak jednat v krizových situacích. Během těchto úvah a analýz byl odhalen problém ČR v nedokonalosti v civilní ochrany a informovanosti obyvatel. Zaškolení občanů a důsledná prevence na nenadále hrozby jsou podle všech bezpečnostních expertů nutné. [4]

Na tento výsledek někteří reagovali s nesouhlasem s tím, aby na základě jedné události vznikala pravidla a určité postupy pro všechny. Hlavní podstatou řešení problémů je nastavení legislativy a mechanismů, které by nezahrnovaly jen pár oblastí, ale pokrývaly by celou problematiku. [4], [5]

Kapitola se věnuje definici a charakteristice měkkých cílů jako objektů s vysokou koncentrací lidí, nízkou úrovní ochrany a vysokou zranitelností. Popisuje vývoj hrozeb, které měkké cíle ohrožují, zejména terorismus, násilné útoky a jiné formy násilí. Upozorňuje na nutnost identifikace zranitelných míst a komplexního přístupu k jejich ochraně.

2 VYBRANÉ ASPEKTY MANAGEMENTU RIZIK

Provoz zábavního parku přináší specifická rizika, která mohou ohrozit bezpečnost návštěvníků, zaměstnanců i majetku. Identifikace, analýza a následná prevence těchto rizik jsou klíčové pro zajištění bezpečného prostředí a plynulého chodu parku. Kapitola je zaměřena na různé aspekty řízení rizik, včetně principů bezpečnosti, analýzy hrozeb, zranitelnosti a také na metody analýzy rizik, které jsou nezbytné pro efektivní management rizik v zábavních parcích.

2.1 Bezpečnostní hrozby, analýza a řízení rizik

Rizika a hrozby jsou všude kolem nás a ovlivňují každodenní život jednotlivců, různých institucí i veřejných míst. Abychom se s nimi dokázali vypořádat, je potřeba pochopit, co je riziko, jak ho rozpoznat a co dělat, když se objeví. Klíčem k úspěchu je přemýšlet dopředu, hledat slabá místa a snažit se snížit jejich dopad. K tomu slouží různé metody a postupy, které pomáhají situace zvládat. Důležité je také nezapomínat na krizové řízení, které hraje zásadní roli v okamžicích, kdy se rizika stanou realitou. Správný přístup k rizikům tak může rozhodnout o tom, jak úspěšně zvládneme výzvy, kterým čelíme.

2.1.1 Hrozba

Událost, která může způsobit ztrátu, poškození nebo narušení aktiva či procesu, a organizace by měla chránit svá aktiva a procesy před těmito riziky. Může jít o útok, krádež nebo přírodní katastrofu. Hrozby vznikají úmyslně, neúmyslně nebo náhodně a mohou být vnější, vnitřní, například způsobené lidskou chybou či nedodržením pracovních postupů. Jedná se o faktory, které nelze vždy přímo ovlivnit, ale které mohou mít vážné dopady na firmu. Analýza hrozeb je klíčovou součástí řízení rizik a zabezpečení. [6], [10]

2.1.2 Nebezpečí

Nebezpečí je v rizikovém inženýrství chápáno jako hrozba, která může ohrozit zdraví člověka nebo poškození majetku. Může jít například o nebezpečné materiály, stroje nebo situace, které mají potenciál způsobit škody. Nebezpečí může být viditelné a zřejmé, ale někdy je skryté a projeví se až v určitých podmínkách. [6]

Nebezpečí dělíme na známé a neznámé. Známá nebezpečí se dají lépe předvídat a počítat s nimi, zatímco neznámá nebezpečí vedou ke zbytkovým rizikům – těm, která zůstávají

i přes všechna opatření. Tato zbytková rizika se nedají přesně spočítat, ale pracuje se s nimi pomocí zkušeností, intuice nebo rozpočtových rezerv. [6]

Kromě toho se rozlišuje absolutní nebezpečí, které je nevyhnutelné (např. přírodní katastrofy), a relativní nebezpečí, které může být pro někoho dokonce příznivé (např. zvýšení zájmu o pojištění po povodni). Takové události mohou mít z dlouhodobého pohledu i pozitivní efekt, protože ovlivní například hodnotu služby. [4], [6]

2.1.3 Riziko

Riziko se dá popsat jako pravděpodobnost, že dojde k nechtěné události, která způsobí škodu nebo negativní dopady. Souvisí s očekáváním toho, co se může stát, a jaké následky to může způsobit, například poškození zdraví nebo majetku. Riziko je vlastně kombinací dvou faktorů:

- pravděpodobnosti, že něco špatného nastane,
- závažnosti možných následků.

Riziko se často vyjadřuje číslem, které ukazuje, jak často se nějaký problém může vyskytnout, a jaké škody by způsobil. Může to být také kvalitativní popis, který určuje, jak vážné důsledky může konkrétní negativní událost přinést. Jinými slovy, riziko znamená šanci, že něco špatného nastane, a zároveň závažnost toho, jak moc to ovlivní osoby, prostředí nebo majetek. [7]

2.1.4 Zranitelnost

Zranitelnost budovy nebo zábavního parku je stav, kdy určité aspekty, jako konstrukce, bezpečnostní systémy nebo evakuační cesty, nejsou dostatečně chráněny před riziky. Může se jednat o slabé místo, které usnadní přístup neautorizovaných osob, nebo zvýší riziko při požáru, přírodní katastrofě či technologickém selhání. Zranitelnosti mohou zahrnovat i nedostatečné školení personálu nebo špatně navržené evakuační cesty. [7]

2.2 Metody analýzy rizik

Analýza rizik představuje klíčovou součást procesu řízení rizik, jejímž cílem je identifikace, hodnocení a posouzení rizik, která mohou ohrozit bezpečnost, majetek, zdraví osob nebo kontinuitu činností organizace. Správně provedená analýza rizik umožňuje stanovit priority a navrhnout účinná opatření k jejich eliminaci nebo minimalizaci. [7]

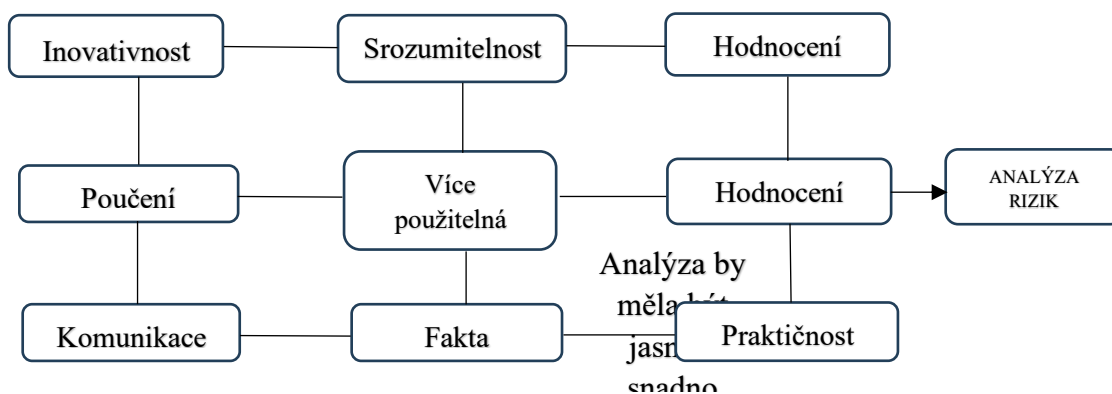
Existuje řada metod, které lze pro analýzu rizik využít, přičemž jejich výběr závisí na konkrétním prostředí, typu analyzovaných hrozeb, dostupnosti informací i časových a finančních možnostech. Mezi nejběžněji používané metody patří například:

- Check-list (kontrolní seznam) – jednoduchá a rychlá metoda využívající předem definovaný seznam otázek nebo položek, které slouží ke kontrole přítomnosti nebo nepřítomnosti rizikových faktorů.
- PNH metoda (pravděpodobnost – následky – hrozba) – metoda založená na posouzení tří základních charakteristik rizika, které se bodově hodnotí a následně se vypočítává celkové riziko.
- What-if analýza – metoda zkoumající možné scénáře „co když“, která pomáhá identifikovat rizika vyplývající z odchylek od běžného provozu.
- SWOT analýza je jednoduchý analytický nástroj, který slouží k posouzení vnitřních a vnějších faktorů ovlivňujících daný objekt nebo prostředí. Název je tvořen z počátečních písmen čtyř anglických slov:
 - Strengths (silné stránky) – vnitřní přednosti, které přispívají k vyšší bezpečnosti (např. přítomnost ostrahy, kamerový systém),
 - Weaknesses (slabé stránky) – vnitřní nedostatky nebo zranitelná místa (např. nedostatek školení personálu, absence evakuačního plánu),
 - Opportunities (příležitosti) – vnější faktory, které lze využít ve prospěch zvýšení bezpečnosti (např. dotační programy, spolupráce s IZS),
 - Threats (hrozby) – vnější rizika, která mohou ohrozit bezpečnost (např. nárůst kriminality v okolí, teroristické hrozby). [7]

Samotný proces analýzy se skládá ze tří hlavních kroků:

1. Identifikace rizikových faktorů – hledání toho, co může představovat hrozbu.
2. Vytváření scénářů – předpovědi, co se může stát za různých okolností.
3. Ohodnocení rizika – určení závažnosti a pravděpodobnosti jednotlivých scénářů.

[10]



Obrázek 4 Parametry analýzy rizik

(upraveno z:[9])

Tato kapitola se zaměřuje na základní pojmy, jako jsou riziko, hrozba, zranitelnost a dopad, a ukazuje jejich vzájemnou provázanost. Kapitola také popisuje jednotlivé fáze procesu řízení rizik. Od identifikace hrozeb a zranitelností přes jejich analýzu, hodnocení až po navržení opatření ke zmírnění rizik. To bylo navrženo v rámci technických prostředků např. detekčních systémů, tak i organizačních opatření, jako je školení zaměstnanců, evakuační plány či krizová komunikace.

Založená na faktech

Logické uspořádání

Inovativní přístup

Analýza by měla být jasná a snadná
Musí mít strukturu a postupovat systematicky
(Hollá, 2005).

Analýza musí mít strukturu a postupovat systematicky
(Hollá, 2005).

Měla by zahrnovat nové metody a přístupy, pokud je to možné
(Hollá, 2005).

Musí být přizpůsobená

3 SOUČASNÉ TRENDY SYSTÉMŮ TECHNICKÉ OCHRANY

Moderní technologie a systémy jsou v komerční bezpečnosti hojně využívány. Měkké cíle zahrnující koncerty, instituce, nemocnice nebo rodinné zábavní parky musí být zabezpečeny různými technologiemi, které pomáhají chránit aktiva včetně osob. Dnešní technologie přispívají ke snížení hrozeb a ochraně osob i majetku.

Mezi nejčastěji využívané technologie patří elektronické systémy, jako jsou PZTS (poplachové zabezpečovací a tísňové systémy), které slouží k detekci neoprávněných vniknutí nebo tísňových situací. Mnohdy se s nimi můžeme setkat v kombinaci s DVS (uzavřeným televizním okruhem), jehož činnost se zakládá na monitorování dění v reálném čase. Dalším zásadní technologií je EPS (elektrická požární signalizace), která se zaměřuje na včasnou detekci požárů, což je klíčové zejména v prostorách s vysokým počtem osob. Na regulaci osob do vyhrazeného prostoru nám pomáhá elektronický systém (ESKV). Vzhledem k důležitosti a vysoké spolehlivosti jsou tyto systémy pomocnou silou perimetrické, předmětové, prostorové a předmětové ochrany, čímž přispívají k celkové bezpečnosti chráněných objektů. [8]

3.1 Mechanické zábranné systémy

V rámci mechanických zábranných systémů (MZS) zahrnujeme všechny mechanické součásti, které představují překážku pro vniknutí do hlídaného prostoru. To představuje například oplocení nebo všechny okenní a vstupní otvory do chráněného objektu. MZS jsou využívány díky své mechanické odolnosti vůči destrukčnímu narušení. MZS zabraňuje:

- riziku nelegálního vstupu do chráněné zóny,
- ztrátě nebo poškození zařízení v rámci chráněného prostoru,
- ztrátě hodnotných předmětů z chráněné oblasti,
- možnost umístění nebezpečných objektů uvnitř chráněné zóny. [11]

Mechanické zábranné systémy představují jeden z hlavních bodů ochrany objektů a osob v komerční bezpečnosti. Do těchto systémů zapadají všechny mechanické prvky a prostředky, které slouží především ke ztížení násilného vniknutí do budovy, či chráněného území přes perimetrické prvky např. oplocení, dveře, okenice nebo okna [11] To lze vyjádřit prodloužením počáteční doby Δt (potřebná doba k překonání překážky neoprávněnou osobou) mezi časem t_1 (doba napadení objektu) a dobou t_2 (doba dokončení napadení objektu), a pak: $\Delta t = t_2 - t_1$. [13]



Obrázek 5 Grafické znázornění pyramidy postoupnosti procesů bezpečnosti v MZS

(zdroj:[11])

Pyramida znázorňuje opatření, která jsou používána pro ochranu objektů, přičemž MZS tvoří základní úroveň. V praxi jsou to fyzické prvky jako zámky, dveře nebo různé bariéry.

Na základní úrovni pyramidy jsou to například zámky, bezpečnostní kování nebo další kovové a nekovové prvky, které chrání vstupní místa proti nepovolenému vstupu. Vyšší úroveň pyramidy zahrnuje technologie jako jsou kamerové sledování (DVS), poplachové systémy nebo kontroly přístupu, které poskytují dodatečné vrstvy ochrany. Pravidla a postupy, které by měl personál používat pro zajištění bezpečnosti, jako je např. školení a evakuační koordinace souvisí s organizačním opatřením. Nejvyšší vrstva pyramidy se zaměřuje na pojištění jako druh určitého vyrovnání způsobených škod vzniklých při porušení bezpečnosti. [11]

3.2 Plášťová ochrana

Jedná se o detekci obvodu střeženého objektu nebo hlídaného předmětu. Na rozdíl od perimetrické ochrany, která se zaměřuje na hranice pozemku, je plášťová ochrana specializována na hranice budovy a její vstupní prvky. V dalším srovnání dochází ke zkrácení doby, kdy můžeme identifikovat neoprávněný vstup, ale detekování probíhá ještě před vniknutím například pachatele do chráněného objektu. [14] K ochraně objektu pomáhá celá řada různých nástrojů. Nemělo by se opomenout na základní ochranu, která se týká dveří, oken, střech, jež bývají v komerční bezpečnosti doplněné kontaktními, destrukčními nebo bariérovými čidly. [11], [13]

3.3 Prostorová ochrana

Poskytuje bezpečnostní opatření, jehož cílem je monitorovat vnitřní prostory objektu a detekovat neoprávněný vstup nebo činnost. Hlavními body prostorové ochrany jsou vstupy, chodby spojující více cest nebo schodišťové přístupy. Používají se zejména pohybová čidla nebo mikrovlnné detektory. Výhodou u tohoto typu ochrany jsou nižší náklady na instalování a montáž prvků ochrany než např. u magnetických kontaktů u plášťové ochrany. [15]

3.4 Integrovaný bezpečnostní systém

Integrovaný bezpečnostní systém, zahrnující PZTS (Poplachový zabezpečovací tísňový systém), ESKV (Elektronická kontrola vstupu), DVS (Uzavřený televizní okruh) a EPS (Elektrická požární signalizace), je navržen tak, aby poskytoval komplexní ochranu a zajišťoval bezpečnost na všech úrovních. Plášťová a prostorová ochrana tvoří nezbytnou součást tohoto systému, protože zajišťují detekci neoprávněného přístupu a přispívají k prevenci potenciálního ohrožení osob nebo majetku. [16]

Plášťová ochrana je zpravidla tvořena detektory pohybu, okenními kontakty nebo vibračními senzory, které jsou napojeny na PZTS a zajišťují ochranu obvodu objektu. Tyto prvky se přímo propojují s kamerovými systémy DVS, které poskytují vizuální dohled, a s EPS, která upozorňuje na případné požáry. ESKV doplňuje tento systém kontrolou vstupů, ať už prostřednictvím čipových karet, biometrických čteček nebo jiných technologií. [14], **Chyba! Nenalezen zdroj odkazů.**

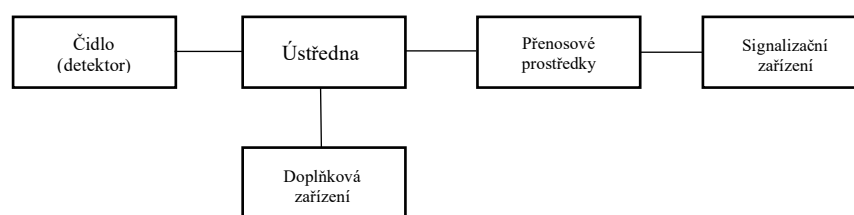
Propojením všech těchto složek do jednoho systému lze vytvořit efektivní bezpečnostní systém, který umožňuje okamžitou reakci na hrozby, minimalizuje lidské chyby a zvyšuje

celkovou bezpečnost. Každý prvek tohoto systému má zaměření na jednu speciální funkci. Společně tvoří jednotný celek, který zajišťuje maximální ochranu objektu nebo osob.

3.5 Poplachový zabezpečovací a tísňový systém (PZTS)

Patří mezi základní součást systémů ochrany objektu. Je systém tvořený různými čidly nebo hlásiči, které komunikují s ústřednou. Na základě signálů z těchto zařízení ústředna vyhodnocuje situaci a v případě potřeby spouští poplach, ať už akustický, optický, nebo jiný. Hlavní funkcí tohoto systému je včasná identifikace neoprávněného vstupu do chráněného prostoru nebo pokusu o něj a následná signalizace, která upozorní na narušení. [8]

Podle ČSN 50131-1 musí disponovat PZTS minimálně ústřednou, jedním nebo více detektory, či signalizačních zařízení nebo poplachových přenosných systémů a napájecích zařízení. [11], [12]



Obrázek 6 Blokové schéma PZTS

(upraveno:[13])

- Čidlo (detektor) je komponent, jehož úkolem je reagovat na fyzikální změny, které se vztahují na střežený objekt, či prostor a jeho narušení. V případě zaznamenání narušení reaguje čidlo vysláním poplachového signálu nebo zprávy.
- Ústředna shromažďuje a analyzuje data z čidel dle předem stanovených instrukcí a následně je vykonává. Kromě toho umožňuje ovládání nebo systému zajišťuje napájení.
- Přenosové prostředky zajišťují tok informací od ústředny k signalizačním místům, a naopak zajišťují zpětný přenos povelů.
- Signalizační zařízení převádí získané informace na vhodný signál (vyhlášení poplachu nebo výstrahy)

- e) Doplnková zařízení zjednodušují správu systému a umožňují provádění specifických funkcí. [13]

Jednotlivé požadavky na PZTS přesně definuje evropská technická norma ČSN EN 50131-1 ED.2 Poplachové zabezpečovací a tísňové systémy – Část 1: Systémové požadavky. Nejdůležitějším požadavkem je určení tzv. stupně zabezpečení systému. [12] Stupeň zabezpečení určuje komponent s nejnižší váhou zabezpečení. To znamená, že pokud PTZS má komponent, kterému je přiřazen stupeň dva, tak celkový systém je zařazen do stupně zabezpečení téhož čísla. Máme následující stupeň zabezpečení:

Tabulka 1 Stupeň zabezpečení

(zdroj:[13], [19])

Rizika	Znalosti a vybavení narušitelů	Stupně zabezpečení
Nízké	Narušitel má malou znalost PZTS a jen snadno dostupné nástroje. Jde např. o rodinné byty nebo domy.	1
Nízké až střední	Narušitel má už určité znalosti o PZTS, a kromě nástrojů mají k dispozici i přenosné přístroje např. multimetr. Jsou to převážně komerční objekty nebo i některé rodinné domy	2
Střední až vysoké	Narušitelé jsou obeznámeni s PZTS a mají úplný sortiment nástrojů a přenosných přístrojů. Do této skupiny patří peněžní ústavy, směnárny, památky nebo sklad zbraní.	3
Vysoké	Zde má zabezpečení prioritu před všemi ostatními hledisky. Předpokládá se, že narušitelé disponují detailními plány a kompletním vybavením pro obcházení prvků PZTS. V této skupině se nachází objekty nejvyššího významu – státní instituce nebo jaderné elektrárny.	4

Podle stupňů zabezpečení se dají odvozovat parametry různých komponentů a požadavky, které jsou na ně kladené. Jednotlivé komponenty PZTS se dále kategorizují do tříd prostředí:

- I. Třída: vnitřní prostředí ve vytápěných místech.
- II. Třída: vnitřní prostředí, kde není udržovaná teplota.
- III. Třída: venkovní prostředí chráněné, kde komponenty EZS nejsou vystaveny plně vlivům počasí.
- IV. Třída: venkovní prostředí se všemi vlivy počasí [8]

3.5.1 Čidla kontaktní

Z názvu vyplývá, že v konstrukci těchto čidel je kontakt. Ten je založen na fungování při přerušení nebo uzavření proudového okruhu zabezpečovací smyčky, kde je zaimplementován. V zabezpečovací smyčce protéká tzv. klidový proud, který je pod dohledem ústředny. Pokud dojde ke změně na smyčce, tak ústředna vyhlásí poplach. Z pohledu použití se kontaktní čidla instalují tak, aby bylo rozpoznáno otevření, či oddálení oken a dveří do 30 mm. [20]

3.5.2 Čidla pohybu

Jsou určena k detekci pohybu lidí či předmětů a využívají různé technologie, které zpracovávají signály a reagují na změny v prostředí např. světlo nebo různé vibrace. Moderní čidla jsou navržena tak, aby byla spolehlivá a odolná proti nežádoucím poplachům. Kromě hlavní funkce detekce pohybu nabízejí doplňkové funkce, jako je dálkové ovládní, indikace stavu pomocí LED, nebo testování a kontroly. Čidla lze snadno montovat a jejich správná instalace a údržba zajišťuje dlouhou životnost a nízké provozní náklady. [13]

3.5.3 Antimasking

Tato funkce se používá u čidel, které jsou instalované v objektech s vyšším rizikem narušení. Antimasking chrání čidlo manipulací jako je zakrytí nebo přestříkání, což by mohlo zabránit jeho správné funkci. Čidlo neustále kontroluje hlídáný prostor pomocí různých technologií, například infračerveného nebo mikrovlnného záření. Jestliže čidlo vyhodnotí, že je výhled na zabezpečovaný prostor zakrytý (např. plechem nebo kartonem), spustí sabotážní poplach. Existují různé metody, jak tato technologie funguje, včetně odrazu záření nebo detekce překážek. Základním typem je vysílání infračerveného záření. [13]

Dioda vysílá do chráněného prostoru infračervené záření a posléze ho přijímá zpět. Jestliže je vyhlášen detektorem poplach, tak infračervené záření bylo přijato infradiodou. Antimasking zvyšuje bezpečnost tím, že i při pokusu o manipulaci zůstává čidlo funkční. [19]

V prostorách se můžeme setkávat s dalšími typy pohybových čidel, nicméně jejich fungování je odlišné. Některé využívají ke své činnosti jinou část kmitočtového spektra elektromagnetického vlnění. Další čidla mohou být:

1. VKV čidla
2. Mikrovlnná čidla
3. Ultrazvuková čidla [13]

3.5.4 Detektory pohybu

Důvody instalace detektorů pohybu se mění v závislosti na tom, co chceme zabezpečovat. Eliminace odcizení předmětů, vandalismu nebo ztráta dat je hlavním důvodem zejména u komerčních objektů. U soukromých domů převažuje především vlastní ochrana před potenciálním útočníkem nebo odcizení důležitých předmětů. U prostorové ochrany se používá několik senzorů, které mohou reagovat na různé stavy dle jejich účelu. Všechny tyto detektory se začleňují do poplachových a zabezpečovacích tísňových systémů (PZTS), kde slouží jako klíčová součást ochrany před neoprávněným vniknutím. Detektory pohybu dělíme jednotlivé skupiny:

- Drátové detektory pohybu
- Bezdrátové detektory pohybu

Drátové pohybové detektory vyžadují ke svému napájení kabelové připojení. Díky tomu se vyznačují vysokou stabilitou, spolehlivým provozem a nízkými provozními náklady. Na druhou stranu možnou nevýhodou je menší variabilita, protože kabelové svazky neumožňují snadné přemístění. [20]

Bezdrátové detektory se vyznačují svou zjednodušenou instalací. Nevyžadují žádnou kabeláž, a tudíž umožňují snadné přemístění. Ovšem jejich provoz závisí na bateriovém napájení, které vyžaduje průběžnou kontrolu, aby se předešlo vybití. [20]

Dále je můžeme kategorizovat, podle toho, jak reagují na jednotlivé podněty. Lze je rozdělit na:

- Detektory pohybu s pasivními čidly
- Detektory pohybu s aktivními čidly [20]

3.6 Pasivní detektory

Pasivní detektory zahrnují magnetické kontakty, které jsou určeny k detekci nechtěného otevření dveří, oken nebo jiných vstupních otvorů. Tyto kontakty pro běžné využití mohou být konstrukčně jednoduché pro běžné využití. Existují také skryté kontakty, které jsou instalovány tak, aby je případný pachatel nemohl snadno najít. Další typy, jako jsou například zámkové kontakty, reagují přímo na pohyby uvnitř zámků. Pro ochranu skleněných ploch se používají detektory rozbití skla, které reagují na zvuky, jako je třesk skla, nebo na charakteristické tlakové vlny. [19]

3.6.1 Pasivní infračervené světla

Pasivní infračervená čidla (PIR) fungují na principu detekce změn infračerveného záření, které vyzařují objekty s teplotou vyšší než absolutní nula ($-273,15\text{ °C}$). Tato čidla nevyzařují žádnou energii, ale pouze snímají infračervené záření v okolním prostředí. Infračervené spektrum zahrnuje tzv. teplotní záření, které lidské oko nedokáže vnímat jako světlo, ale PIR čidla jej zaznamenávají. [20]

PIR čidla využívají pyroelektrický senzor, který detekuje změny v teplotě, když se předmět pohybuje v detekční zóně. Jsou obzvláště citlivá na rychlé změny, například pohyb osob nebo zvířat, a pracují spolehlivě v širokém rozsahu teplot. Typická konstrukce zahrnuje Fresnelovu čočku, která směřuje infračervené záření na senzor a zlepšuje jeho účinnost. [20]

Čidla se často instalují tak, aby pokrývala určité oblasti, například vstupy do místností nebo venkovní prostory, přičemž jsou chráněna před přímým světlem nebo proudy vzduchu, které by mohly způsobit falešné poplachy. Díky tomu se PIR detektory staly oblíbeným prvkem bezpečnostních systémů, protože jsou spolehlivé, nenáročné na údržbu a mají nízkou spotřebu energie. [20]

3.6.2 Magnetické kontakty

Mezi nejpoužívanější kontaktní čidla se řadí magnetické kontakty, jejichž činnost se využívá v mnoha aplikacích, neboť mezi jejich hlavní výhody spadá např. vysoká životnost, odolnost proti rušení anebo nenáročná instalace. Magnetické kontakty musí být umístěny tak, aby při obyčejném otvírání dveří nedocházelo k planým poplachům. K častým poplachům může docházet v případě, že máme běžný kontakt, který není odolný proti překonání. K těmto běžným kontaktům lze přiložit dostatečně silný magnet a poté okno, či dveře bez jakékoliv větší snahy jednoduše otevřít. [20]

3.6.3 Detektory tříštění skla

Jedná se o zařízení, které se používají k detekci rozbití oken v chráněném prostoru. Jejich princip fungování je založen na analýze akustického spektra a jejich reakce spojené s frekvencí praskání skla. Umísťovány bývají zpravidla na skleněném okně nebo dveři a v případě rozbití, tak detektor identifikuje zvukový signál a posléze vyvolá alarm. Pro celkové pokrytí celého chráněného objektu jsou instalovány společně s prvky, jako jsou magnetické kontakty nebo pohybové detektory. [21]

3.7 Aktivní detektory

Aktivní detektory, založené na Dopplerově jevu, pracují na principu vysílání a přijímání elektromagnetického vlnění. Tyto detektory měří změny kmitočtu vlnění, které vznikají při pohybu předmětu nebo osoby. Typickým příkladem jsou mikrovlnné detektory s frekvenčním rozsahem 3 až 12 GHz. Změna kmitočtu, způsobená pohybujícím se objektem, je detekována a analyzována. Tyto detektory jsou obzvláště citlivé na přímý pohyb směrem k detektoru. [20]

3.7.1 Ultrazvukové detektory

Tyto detektory pracují na principu vysílání ultrazvukových vln o frekvenci 25–45 kHz. Vlny odráží překážky v prostoru a zpětně se zachycují přijímačem. Slouží především k zabezpečení vnitřních prostor, často v kombinaci s PIR detektory. Jejich výhodou je schopnost detekovat pohyb v hlídaném prostoru, ale jejich účinnost může být snížena vlivem nízké teploty nebo vysoké vlhkosti vzduchu. Uplatňují se zejména tam, kde je kladen důraz na přesnou montáž a nastavení. [8]

3.7.2 Mikrovlnné detektory

Další často používanou detekcí je radarová mikrovlnná technologie. Součástí je anténa, která vysílá do chráněného prostoru elektromagnetické vlny, jejichž frekvence se pohybuje v řádech GHz. Tyto vlny se v prostoru odrazí od předmětu a vrací se zpět na anténu detektoru. Ta vzápětí obdržený signál vyhodnocuje, zda jsou v signálu posuny frekvence, které by byly důsledkem pohybu těles v objektu. Stejně jako u ultrazvukového detektoru se zde využívá Dopplerův efekt, což je změna frekvence a vlnové délky oproti vysílanému signálu, způsobenou vzájemnou nenulovou rychlostí zdroje. Občas se mikrovlnné detektory nazývají Dopplerovy detektory. [8]

U mikrovlnných detektorů je největší citlivost v ose detektoru, což znamená směrem k detektoru nebo od něj. Výhodou může být fakt, že citlivost není ovlivněna teplotním rozdílem mezi prostorem a detekovaným prostorem. Tudiž detektor dokáže odhalit narušitele, i když se pokusí zakrýt použitím předmětů z domu (stejná teplota), oblékne si neopren, nebo zakryje detektor sklem, což může být snadné, pokud je detektor umístěn nevhodně, například u okna, které narušitel může otevřít. [8], [23]

Instalace musí být provedena tak aby se zabránilo vlivům, které by mohly narušovat bezproblémovou detekci chráněného prostoru. Mikrovlnný signál může procházet sklem nebo tenkými dřevěnými stěnami. V blízkosti těchto čidel by se neměly nacházet pokovené objekty (zrcadla nebo ochranné fólie) nebo z kovu jako jsou např. mříže či oplechované dveře). Dále by se tyto senzory neměly vyskytovat v prostoru, kde jsou psi nebo kočky a také, kde může docházet k elektromagnetickým rušivým vlivům (zářivkové světlo). [8]

3.8 Elektrická kontrola vstupu

Svým účelem umožňuje na základě přesně definovaných oprávnění, přístup do vymezených prostor pouze autorizovaným osobám (např. budovy, místnosti, trezoru...). Toto vymezení se děje na základě oprávnění, řešeného nejčastěji identifikací osoby prostřednictvím identifikační (ID) karty, čipu nebo biometrické identifikace např. otisku prstu, ID duhovky oka. [24]

Při vstupu do chráněného objektu uživatel přiloží kartu ke čtečce, která přečte uložené údaje a odešle je k vyhodnocení do řídicí jednotky. Na základě předem nastavených pravidel rozhodne řídicí jednotka, zda daná osoba splňuje podmínky pro přístup. V případě kladného

rozhodnutí je mechanická bariéra, například elektromagnetický zámek, turniket, branka nebo závora, uvolněna pro průchod. [24]

Moderní technologie přinášejí do oblasti identifikace stále pokročilejší řešení. V systémech s nejvyšší úrovní zabezpečení se dnes často využívají biometrické čtečky, které ověřují totožnost osob na základě otisku prstu, skenu oční duhovky nebo jiných unikátních biologických znaků. [24]

3.8.1 Komponenty ESKV

Autonomní čtečka je zařízení, které umožňuje ověřeným osobám vstup do konkrétní části objektu. Obsahuje integrované vyhodnocovací a řídicí komponenty a moderní modely mohou navíc měřit tělesnou teplotu nebo detekovat absenci roušky. [24]

Turnikety představují mechanické bariéry, které brání neoprávněnému vstupu do chráněných prostor. Mohou být navrženy pro jednosměrný i obousměrný průchod a vyrábí se v různých provedeních. Jejich ovládání lze zajistit dálkově, přístupovým systémem nebo přes EPS. [24]

3.9 Bezpečnostní kamery

Účelem DVS je vizuální kontrola nad zájmovým prostorem, často i záznam událostí ze snímané scény a eventuálně také vyhodnocení změn (pohybová detekce) sloužící k vyhlášení poplachu. Ve většině případech jsou bezpečnostní kamery instalovány jako doplňující prvek PZTS a pomáhá zefektivňovat zabezpečení hlídaného prostoru. [25]

IP kamery, často označované jako webové kamery, se díky technologickému pokroku v přenosových sítích a digitalizaci videosignálu staly významným prvkem moderního monitorování. Tato zařízení kombinují funkce analogové videokamery s integrovaným videoserverem, který zajišťuje digitalizaci a kompresi videosignálu. Připojení kamery k počítačové síti umožňuje sledování obrazu prostřednictvím webového prohlížeče z libovolného místa v síti, a to jak v lokální síti (LAN), tak i přes internet. [25], [26]

Tato kapitola poskytuje přehled o současných technických a organizačních opatřeních používaných k ochraně měkkých cílů, konkrétně zábavních parků. Představuje klíčové prvky bezpečnostního systému, mezi které patří mechanické zábranné systémy (oplocení, dveře, okna), plášťová a prostorová ochrana (např. čidla pohybu, magnetické kontakty), a elektronické systémy – zejména poplachové zabezpečovací a tísňové systémy (PZTS),

kamerové systémy (DVS), elektrická kontrola vstupu (ESKV) a elektrická požární signalizace (EPS).

Jednotlivé technologie jsou podrobně popsány včetně způsobu fungování pasivních a aktivních detektorů, ultrazvukových a mikrovlnných čidel či detektorů tříštění skla. Kapitola zdůrazňuje význam integrovaného přístupu, kdy jednotlivé bezpečnostní komponenty spolupracují v rámci celkového systému.

Teoretická část práce poskytuje komplexní přehled o problematice bezpečnosti měkkých cílů, vymezuje základní pojmy, popisuje relevantní hrozby a zdůrazňuje nutnost systematického řízení rizik. Představuje dostupné technologie a nástroje ochrany a poukazuje na význam vzájemného propojení organizačních, technických i personálních opatření. Teorie tvoří základ pro následné hodnocení současného stavu zabezpečení.

II. PRAKTICKÁ ČÁST

4 RODINNÝ ZÁBAVNÍ PARK GALAXIE

Rodinný zábavní park Galaxie se nachází na okraji města Zlín v části Vršava. Tato oblast je známá především sportovním zázemím. Nachází se zde infrastruktura pro mládežnické kategorie fotbalového klubu FC Zlín a totéž platí i pro zlínský tenisový klub. Galaxie je snadno dostupná městskou hromadnou dopravou. Pro návštěvníky přijíždějící autem je k dispozici parkoviště přímo před budovou. Ti, kteří upřednostní jiný způsob dopravy, mohou využít přilehlou cyklostezku, která spojuje centrum města s částí Kostelec.

Park byl otevřen pro veřejnost v roce 2009. Za vznikem parku stojí manželé Tomáš a Jana Valáškoví, kteří provozují síť zábavních parků v ČR pod názvem TOBOGA. Hala parku má rozlohu více než 2 000 m² s kapacitou do tisíce návštěvníků a skládá se ze přízemí a prvního poschodí. V posledních letech během víkendů a školních prázdnin v podzimních a zimních měsících dosahuje návštěvnost 70-80% využití celkové kapacity. Velkou část haly obohacuje hrací plocha v přízemí s několika atrakcemi, trampolínami, skluzavkami a zóny připomínající vesmírnou galaxii.

Kromě zábavních aktivit pro děti nabízí park i ubytování pro rodiny s dětmi nebo dětské tábory díky hotelu, jenž je součástí Galaxie v prvním poschodí. Hotel disponuje kapacitou více než třiceti lůžek od jednolůžkových až po čtyřlůžkové pokoje. Párkrát během roku je k dispozici možnost pro velké skupiny dětí přespat přímo u atrakcí na hrací ploše. Hoteloví hosté mohou využít restauraci nacházející se po levé straně hlavního vchodu do budovy, kde jsou denně podávány snídaně a obědové menu.

4.1 Bezpečnost rodinného zábavního parku

Je klíčovým faktorem ovlivňujícím návštěvnost i celkový komfort návštěvníků. Z poskytnuté mapy kriminality Policie ČR, která pokrývá období od 6. 5. 2024 do 6. 5. 2025, vyplývá, že lokalita Vršava, kde se nachází rodinný zábavní park Galaxie Zlín, ukazuje široké spektrum trestných činů, které mohou potenciálně ovlivnit provoz takového parku. Mezi nejvýznamnější zaznamenané delikty patří krádeže, podvody a jiné majetkové trestné činy. Dopravní nehody v okolí mohou znamenat bezpečnostní riziko při příjezdu návštěvníků. Přítomnost drogové závislosti či případných incidentů spojených se zbraněmi může být rovněž důležitým faktorem při posuzování bezpečnostních opatření a nutnosti policejní přítomnosti v blízkosti parku. [27]

4.2 Výskyt bezpečnostních událostí

V minulosti došlo ke dvěma výpadkům elektrického proudu (blackoutům), které nastaly vždy v době konání Film Festivalu Zlín (FF Zlín). Tyto výpadky způsobily paniku mezi návštěvníky, zejména kvůli velkému počtu dětí ubytovaných v hotelu v rámci festivalu. Po zjištění výpadku personál okamžitě reagoval a přistoupil k zásahům. Prvním krokem bylo vyslání obsluhy do rozvodné místnosti, kde bylo zjištěno, že jistič není možné znovu aktivovat. V takovém případě personál kontaktoval společnost EPOS Kroměříž, který poskytl pokyny, jak postupovat v dané situaci. Pokud systém funguje správně a doporučení proběhly správně, není nutné volat společnost EON pro okamžitou opravu.

V těchto případech byla situace vyřešena v řádu minut, ale kvůli výpadku elektrického proudu, zejména v oblasti únikových cest, vznikla situace, která vyvolala paniku, protože vchodové dveře začaly vydávat tísňové signály. Tento problém byl způsoben nedostatkem elektrické energie, což ovlivnilo funkčnost systému vchodových dveří. Záložní zdroj energie, který je součástí bezpečnostního systému, má kapacitu na 20 minut nepřetržitého provozu, ale během výpadku pracoval kontinuálně po dobu 3–4 hodin. Po opětovném obnovení napájení došlo k otevření dveří, což umožnilo normální fungování zařízení.

Kromě problémů s elektrickým napájením došlo k několika zdravotním událostem. Mezi incidenty, které vyžadovaly okamžitou pozornost, patřily spáleniny, přejeté nohy, naraženiny, krvácení z nosu, nevolnosti a potřeba podání léků. Lékárničky jsou umístěny na recepci v případě potřeby.

Nevolnosti a krvácení z nosu u některých návštěvníků byly pravděpodobně způsobeny vysokými teplotami v Galaxii, zejména během letních měsíců. V přízemí na hrací ploše jsou okna na obvodových stěnách pouze částečně otevíratelná. Otevřít se můžou jen čtyři horní obvodová okna. Klimatizace je v některých oblastech budovy velmi omezená, a navíc není možné regulovat teplotu v jednotlivých zónách. Například na hrací ploše by vzduch měl cirkulovat rychleji než v restauraci nebo hotelových pokojích, ale klimatizace zde není nainstalována. Tato kombinace problémů může vést k přehřátí vzduchu v určitých částech budovy, což může způsobit zdravotní potíže u návštěvníků.

4.3 Kontrolní seznam aktuálního stavu (Check List)

V kontextu rodinného zábavního parku Galaxie ve Zlíně je kontrolní seznam klíčovým nástrojem pro zajištění bezpečnosti návštěvníků a personálu. Pomáhá identifikovat

a hodnotit potenciální rizika, jako jsou technické závady, nedostatky v personálním zabezpečení nebo neadekvátní reakce na krizové situace.

Tabulka 2 CHECK List perimetrická ochrana budovy

(zdroj: [vlastní])

Otázka	ANO	NE
1. Perimetrická ochrana budovy		
Je příjezdová cesta do areálu volně a snadno průjezdná pro jednotky IZS?		X

Tabulka 3 CHECK List obvodová ochrana budovy

(zdroj: [vlastní])

2. Obvodová ochrana budovy		
Je zajištěn trvalý monitoring vstupů do areálu?	X	
Je prováděn monitoring příchozích a odchozích osob?		X
Je areál vybaven kamerovým systémem pro detekci neoprávněného vstupu?	X	

Tabulka 4 CHECK List plášťová a prostorová ochrana

(zdroj: [vlastní])

3. Plášťová a prostorová ochrana		
Jsou všechny vstupy zabezpečeny proti neoprávněnému vniknutí?	X	
Je zajištěn režim pro kontrolu vstupu osob mimo pracovní dobu?	X	
Jsou v areálu umístěny zámky na dveře a okna pro zajištění proti vloupání?		X
Je klávesnice ústředny PZTS umístěna na místě, které není snadno přístupné veřejnosti a neoprávněným osobám?		X
Jsou dodržovány standardy pro bezpečnostní skla a dveře?	X	

Tabulka 5 CHECK List zabezpečení vstupů

(zdroj: [vlastní])

4. Zabezpečení vstupů		
Je přístup na klíčové vstupy do zábavního parku řízen systémem identifikace (např. vstupní čipové karty, turnikety)?		X
Jsou všechny únikové východy monitorovány kamerovým systémem bez slepých míst?		X
Jsou všechny vstupy označeny viditelně pro návštěvníky?	X	

Tabulka 6 CHECK List požární systémy

(zdroj: [vlastní])

5. Požární systémy		
Je park vybaven požárními hlásiči, hasicími přístroji a zásahovými systémy (např. požárními hydranty, hasicími zařízeními)?	X	
Jsou vyznačeny evakuační cesty, včetně značek pro evakuaci návštěvníků a personálu?	X	
Jsou vyznačeny evakuační cesty, včetně značek pro evakuaci návštěvníků a personálu?	X	

Tabulka 7 CHECK List bezpečnostní incidenty

(zdroj: [vlastní])

6. Bezpečnostní incidenty		
Je zaveden krizový plán pro evakuaci návštěvníků a personálu v případě požáru nebo jiné mimořádné události?	X	
Nachází se v areálu budovy defibrilátor pro případ náhlé zástavy srdce?		X
Jsou všechny krizové situace (požár, zranění) monitorovány a má park připravený zásahový tým?	X	
Existují systémové hlášení v případě poruchy nebo nebezpečí pro personál a návštěvníky?	X	

Tabulka 8 CHECK List personální zabezpečení a BOZP

(zdroj: [vlastní])

7. Personální zabezpečení a BOZP		
Jsou zaměstnanci pravidelně školeni v oblasti bezpečnosti práce (BOZP) a krizového řízení?	X	
Je zajištěno dostatečné množství zaměstnanců pro obsluhu a zajištění bezpečnosti během prevencí nebo krizových situací?	X	
Má park vypracovaný interní směrnice pro ohlášení úrazů a jiných nehod v areálu?		X

Tabulka 9 CHECK List zabezpečení technologických prvků

(zdroj: [vlastní])

8. Zabezpečení technologických prvků		
Jsou zabezpečeny technologické a zábavní zařízení proti neoprávněné manipulaci a poškození?	X	
Jsou počítače v parku důkladně zabezpečeny proti všem kybernetickým hrozbám, včetně pravidelných aktualizací a antivirové ochrany?		X
Jsou všechny elektrické a technické systémy pravidelně kontrolovány a udržovány v souladu s normami bezpečnosti?	X	

Byla vyhodnocena bezpečnostní opatření v rodinném zábavním parku Galaxie na základě nedostatků, kde byly v kontrolním seznamu uvedeny odpovědi "NE". U každého z těchto bodů byla níže popsána potenciální rizika a možné důsledky, které by mohly vzniknout v případě, že by nedostatky nebyly včas vyřešeny.

1. Příjezdová cesta do areálu volně a snadno průjezdná pro jednotky IZS?

Příjezdová cesta je často ucpaná, což může zpozdit příjezd záchranných složek. To by mohlo ohrozit bezpečnost návštěvníků a personálu v případě požáru nebo jiné nouze.

2. Monitoring přicházejících a odcházejících osob?

Po opuštění parku a zpětném příchodu návštěvníkům dávají razítko na ruku, což je neefektivní a může vést k záměně nebo opomenutí. Tento postup není dostatečně bezpečný a umožňuje snadný přístup neoprávněným osobám

3. Zámky na dveřích a oknech pro zajištění proti vloupání?

Nezabezpečené vstupy znamenají, že objekt Galaxie je náchylný k vloupání a poškození majetku. Tento nedostatek může vést k finančním ztrátám, ale i ohrožení bezpečnosti zaměstnanců a návštěvníků

4. Klávesnice ústředny PZTS umístěná na místě, které není snadno přístupné veřejnosti?

Umístění klávesnice ústředny PZTS je na snadno přístupném místě u hlavního vchodu směřující do restaurace, čímž se zvyšuje riziko jejího zneužití neoprávněnými osobami. Tento problém může vést k deaktivaci alarmů nebo zneplatnění bezpečnostního systému možnými pachateli.

5. Přístup na klíčové vstupy řízen systémem identifikace?

Pokud klíčové vstupy nejsou řízeny systémem identifikace, může to vést ke vstupu neoprávněných osob do jednotlivých zón v Galaxii. Zvyšuje se riziko, že osoby s nepovoleným přístupem získají citlivé údaje.

6. Únikové východy monitorovány kamerovým systémem bez slepých míst?

Je nezbytné zajistit, aby všechny východy byly pod dohledem pro bezpečnost v parku anebo pro rychlé řízení evakuace.

7. Defibrilátor pro případ náhlé zástavy srdce v areálu?
Rychlá akce může být rozhodující pro záchranu života a bez defibrilátoru je šance na přežití výrazně nižší. Tento nedostatek ztěžuje poskytování pomoci při situacích, které ohrožují život.
8. Interní směrnice pro ohlášení úrazů a nehod v areálu?
Bez interního protokolu pro ohlášení úrazů a nehod je obtížné koordinovat pomoc v případě nehody. Protokol je nezbytný pro zajištění rychlé a efektivní reakce na nehodu.
9. Počítače zabezpečeny proti kybernetickým hrozbám?
Nedostatečné zabezpečení počítačů proti kybernetickým hrozbám zvyšuje riziko napadení systému. Bez spolehlivé antivirové ochrany mohou být data parku snadno zneužita.

Kapitola analyzuje aktuální úroveň zabezpečení zábavního parku Galaxie na základě interní dokumentace, pozorování a rozhovorů. Hodnotí fyzickou bezpečnost, technické prostředky i organizační opatření. Zjištění ukazují na silné i slabé stránky systému a identifikují oblasti pro zlepšení. Důraz je kladen na potřebu modernizace technologií a pravidelného školení personálu.

Lze doporučit základní preventivní opatření, která pomáhají udržet aktiva Galaxie, návštěvníky a služby v bezpečí. Patří mezi ně zejména technické zabezpečení vstupních a parkovacích prostor prostřednictvím kamerového systému, pravidelný dohled městské nebo státní policie, případně i informační cedule upozorňující návštěvníky, aby nenechávali cenné předměty bez dozoru.

5 ANALÝZA A HODNOCENÍ RIZIK

Analýza rizik je klíčovým procesem pro identifikaci, hodnocení a řízení potenciálních hrozeb, které mohou ovlivnit bezpečnost a plynulý provoz rodinného zábavního parku Galaxie ve Zlíně. Cílem této analýzy je zajistit ochranu návštěvníků, zaměstnanců a majetku parku před možnými nebezpečími.

Hodnocení rizik je proces, při kterém se odhaduje možný výskyt nebezpečí spojených s konkrétními situacemi nebo pracovními podmínkami. Cílem tohoto odhadu je navrhnout vhodná bezpečnostní opatření, která by minimalizovala riziko škod na zdraví, majetku nebo životním prostředí. Každé riziko se vyhodnocuje z hlediska: [7], [9]

1. Závažnosti následků (N): Závažnost může zahrnovat například vážné zranění, smrtelné úrazy nebo škody na majetku. Hodnota se vyjadřuje číslem od 1 (mírné následky) do 5 (katastrofální následky). [7]
2. Pravděpodobnosti (P): Pravděpodobnost, že dojde k rizikové události se také hodnotí na škále od 1 (velmi nízká pravděpodobnost) do 5 (vysoká pravděpodobnost). [7]

Celkové riziko (R) se vypočítá jako součin těchto dvou veličin: $R = P \times N$

Kromě závažnosti a pravděpodobnosti se k přesnějšímu odhadu rizika přidává třetí faktor:

3. Názor hodnotitelů (H): Zohledňuje další specifické okolnosti, jako jsou počet ohrožených osob, technická opatření, dynamika rizika (jak rychle se může situace zhoršit), možnosti ochrany apod. Tato složka odráží názory a zkušenosti odborníků. [7]

Součinem všech tří složek se určí celková hodnota rizika (R): $R = P \times N \times H$

Rizika jsou na základě své hodnoty rozdělována do čtyř hlavních kategorií, které odpovídají míře závažnosti a potřebě zásahu:

1. Nepříjemné riziko:

Tato kategorie zahrnuje situace, které představují závažné a bezprostřední ohrožení života, zdraví, majetku nebo prostředí. V tomto případě je nutné okamžitě přerušit všechny činnosti spojené s tímto rizikem a přijmout opatření, která toto riziko odstraní nebo alespoň sníží na bezpečnou úroveň.

Bez odstranění těchto rizik není možné pokračovat v dané činnosti, protože by mohly mít katastrofální následky. [7]

2. Nežádoucí riziko:

Sem spadají situace, které neohrožují lidský život v daný moment, ale přesto vyžadují přijetí odpovídajících opatření ke snížení rizika na přijatelnou úroveň. Tato opatření by měla být realizována co nejdříve, protože ponechání rizika bez zásahu by mohlo v budoucnu vést k závažnějším problémům nebo ohrožení. [7]

3. Mírné riziko:

V této kategorii se nacházejí rizika, která sice nepředstavují zásadní nebezpečí, ale měli bychom je řešit, pokud je to možné. Bezpečnostní opatření se v těchto případech obvykle plánují jako součást běžné údržby nebo dlouhodobého plánování. Cílem je preventivní snižování rizik, aby nedošlo k jejich zhoršení. [7]

4. Akceptovatelné riziko:

Tato kategorie zahrnuje situace, kdy je riziko tak nízké, že není potřeba provádět žádná další opatření. Přestože není nutný aktivní zásah, je vhodné pravidelně monitorovat stav rizika, aby bylo zajištěno, že se nezvyšuje. [7]

5.1 Identifikace aktiv

Prvním krokem v analýze rizik je identifikace aktiv, která zahrnuje určení všech hodnotných prvků, jež je třeba chránit. Mezi tato aktiva patří:

- Zaměstnanci parku: jejich bezpečnost je priorita
- Návštěvníci: rodiny s dětmi, které navštěvují park za účelem zábavy
- Atrakce a zařízení: autíčka, trampolíny a další zábavní zařízení
- Elektronická data a systémy: rezervační a platební systémy, databáze návštěvníků
- Prostor: samotná budova

Tabulka 10 Klasifikace úrovně rizika

(zdroj: [7])

Rizikový stupeň	R	Míra rizika
I.	> 100	Nepřijatelné riziko
II.	51–100	Nežádoucí riziko
III.	11–50	Mírné riziko
IV.	3–10	Akceptovatelné riziko
V.	< 3	Bezvýznamné riziko

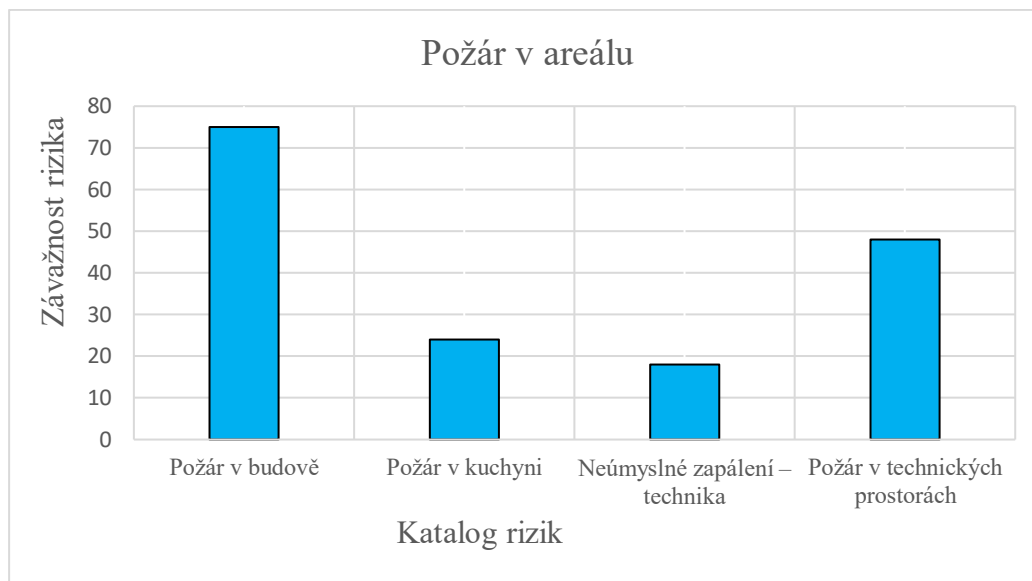
Tabulka 11 Přehled rizik požáru v areálu a navrhovaná opatření

(zdroj: [vlastní])

Zdroj rizika	Identifikace rizika	Závažnost rizika				Bezpečnostní opatření
		P	N	H	R	
Požár v areálu	Požár v budově	3	5	5	75	Pro minimalizaci rizik je nezbytné mít efektivní hasicí systémy, nouzové osvětlení a evakuační plány pro návštěvníky i personál
	Požár v kuchyni	2	4	3	24	
	Neúmyslné zapálení – technika	2	3	3	18	
	Požár v technických prostorách	3	4	4	48	

Tabulka 12 Závažnost rizik požáru v areálu dle metody

(zdroj: [vlastní])



Tabulka 13 Přehled závažnosti rizik požáru v areálu dle metody

(zdroj: [vlastní])

Zdroj rizika	Identifikace rizika	Závažnost rizika				Bezpečnostní opatření
		P	N	H	R	
Útočník a bezpečnostní incidenty	Vyhrůžky střelnou zbraní	3	5	5	75	V případě krizových situací je nutné zajistit přítomnost bezpečnostního personálu, zabezpečené východy a spolehlivý komunikační systém
	Útočník s rukojmími	1	5	5	50	
	Teroristický útok – výbuch	1	5	5	25	
	Bezpečnostní událost – střelba	2	5	5	50	
	Útok chladnou zbraní nebo jiným nebezpečným předmětem	2	4	4	32	
	Únos dítěte z areálu	2	5	5	50	
	Útočník se zbraní vnikající do budovy přes střechu	2	4	3	24	

Tabulka 14 Závažnosti rizik útoků a bezpečnostních incidentů

(zdroj: [vlastní])



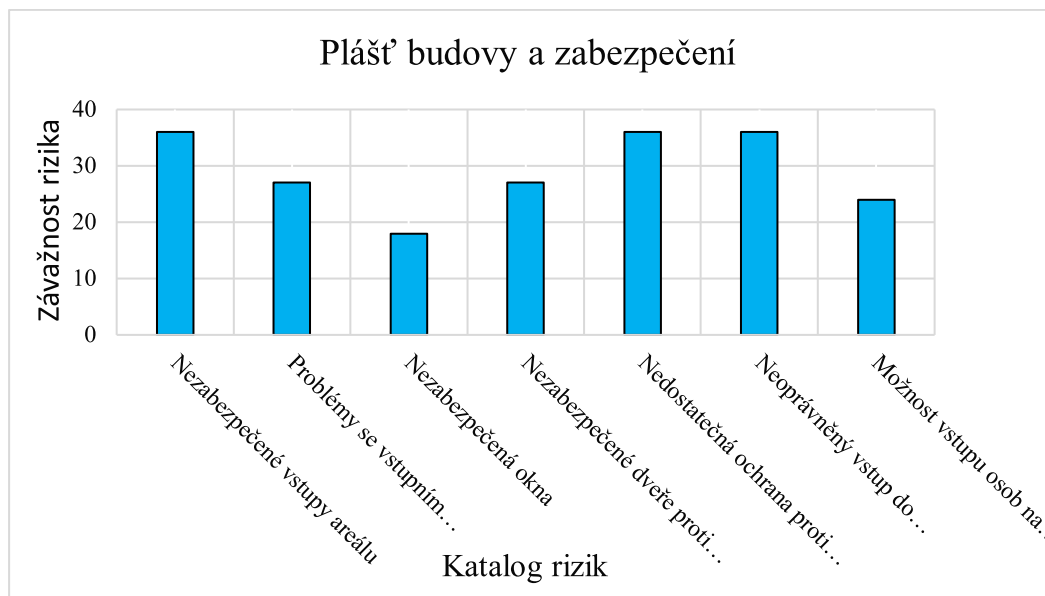
Tabulka 15 Přehled závažnosti rizik útoků a bezpečnostních incidentů

(zdroj: [vlastní])

Zdroj rizika	Identifikace rizika	Závažnost rizika				Bezpečnostní opatření
		P	N	H	R	
Plášť budovy a zabezpečení	Nezabezpečené vstupy areálu	3	4	3	36	Je nutné zajistit uzamykatelné dveře a okna, nainstalovat bezpečnostní zámky a systémy pro kontrolu vstupu, aby se zabránilo nelegálnímu vniknutí
	Problémy se vstupním systémem (turnikety)	3	3	3	27	
	Nezabezpečená okna	2	3	3	18	
	Nezabezpečené dveře proti vloupání	3	3	3	27	
	Nedostatečná ochrana proti nelegálnímu vstupu	3	4	3	36	
	Neoprávněný vstup do administrativních a technických prostor	3	4	3	36	
	Možnost vstupu osob na střechu nebo do uzavřených částí parku	2	4	3	24	

Tabulka 16 Závažnost rizik zabezpečení pláště budovy

(zdroj: [vlastní])



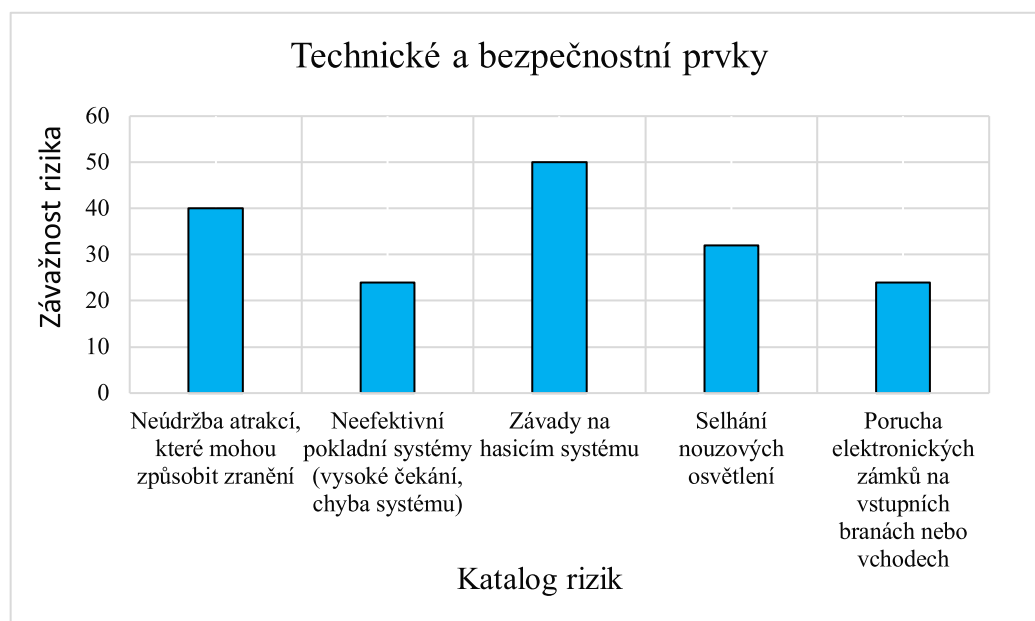
Tabulka 17 Přehled závažnosti rizik zabezpečení pláště budovy

(zdroj: [vlastní])

Zdroj rizika	Identifikace rizika	Závažnost rizika				Bezpečnostní opatření
		P	N	H	R	
Technické a bezpečnostní prvky	Neúdržba atrakcí, které mohou způsobit zranění	2	5	4	40	Pravidelná údržba atrakcí, pokladních systémů a hasicího zařízení je nezbytná pro bezpečnost návštěvníků a personálu
	Neefektivní pokladní systémy (vysoké čekání, chyba systému)	4	3	2	24	
	Závady na hasicím systému	2	5	5	50	
	Selhání nouzových osvětlení	2	4	4	32	
	Porucha elektronických zámků na vstupních branách nebo vchodech	2	4	3	24	

Tabulka 18 Rizika související s technickými a bezpečnostními prvky

(zdroj: [vlastní])



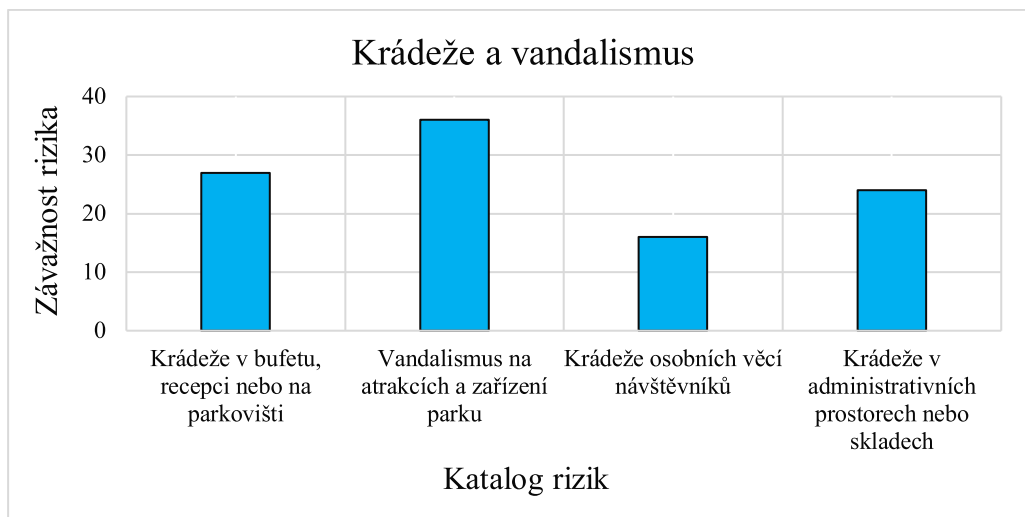
Tabulka 19 Přehled rizik související s technickými a bezpečnostními prvky

(zdroj: [vlastní])

Zdroj rizika	Identifikace rizika	Závažnost rizika				Bezpečnostní opatření
		P	N	H	R	
Krádeže a vandalismus	Krádeže v bufetu, recepci nebo na parkovišti	3	3	3	27	Instalace kamerového systému, zvýšená přítomnost bezpečnostního personálu a ochrana hodnotných předmětů pomohou minimalizovat krádeže a vandalismus
	Vandalismus na atrakcích a zařízení parku	3	4	3	36	
	Krádeže osobních věcí návštěvníků	4	2	2	16	
	Krádeže v administrativních prostorech nebo skladech	2	4	3	24	

Tabulka 20 Závažnost rizik krádeží a vandalismu

(zdroj: [vlastní])



Tabulka 21 Přehled závažnosti rizik krádeží a vandalismu

(zdroj: [vlastní])

5.2 Vyhodnocení PNH metody

Metoda PNH byla aplikována na vybrané oblasti zábavního parku Galaxie s cílem identifikovat nejzávažnější bezpečnostní rizika. Výsledky slouží jako základ pro návrh účinných opatření ke zvýšení bezpečnosti. Následující tabulka shrnuje pět nejvýznamnějších rizik podle vypočtené hodnoty rizika R.

Tabulka 22 Vyhodnocení nejzávažnějších rizik

(zdroj: [vlastní])

Tabulka	Nejvyšší R	Kategorie (stupeň)	Zdroj rizika	Identifikace rizika
Požár v areálu	75	II – Nežádoucí	Požár v areálu	Požár v budově
Útočník a krizové situace	75	II – Nežádoucí	Útočník a krizové situace	Útočník se střelnou zbraní
Plášť budovy a zabezpečení	50	III – Mírné	Plášť budovy a zabezpečení	Nezabezpečené vstupy / Nedostatečná ochrana / Neoprávněný vstup
Technické a bezpečnostní prvky	50	III – Mírné	Technické a bezpečnostní prvky	Závady na hasicím systému
Krádeže a vandalismus	36	III – Mírné	Krádeže a vandalismus	Vandalismus na atrakcích a zařízení parku

Z pěti sledovaných oblastí zábavního parku vyplývá, že největší hrozbu představují scénáře násilného útoku a požáru. V obou případech byla zjištěna nejvyšší hodnota rizika $R = 75$, která PNH metodě spadá do stupeň II – nežádoucí riziko. To znamená, že současná opatření nejsou dostačující a je nutné zavést dodatečné technické i organizační kroky. Zefektivnit hasicí a evakuační systémy, zvýšit připravenost personálu na bezpečnostní incidenty a zajištění areálu proti ozbrojenému útočníkovi.

Třetí nejvýznamnější problém se týká technických a bezpečnostních prvků. Závady na hasicím systému dosahují hodnoty $R = 50$. To potvrzuje, že požární ochrana je slabinou parku. Pravděpodobnost vzniku požáru, ale i selhání klíčového prvku pro jeho zvládnutí zvyšuje celkové riziko.

Na úrovni stupeň III – mírné riziko se v parku objevují tři okruhy. Plášť budovy a zabezpečení s hodnotou $R = 50$, kde se řeší nezabezpečené vstupy, nedostatečná ochrana perimetru a možnost neoprávněného vstupu. Technické a bezpečnostní prvky rovněž s $R = 50$ kvůli závadám na hasicích zařízeních a krádeže a vandalismus s $R = 36$. Přestože tato rizika přímo neohrožují životy, dlouhodobě narušují pocit bezpečí návštěvníků, přinášejí finanční ztráty a zvyšují pravděpodobnost závažnějších incidentů.

Rizika, jako je požár v areálu a útočník s rukojmími, spadají do kategorie středního rizika (III.), což znamená, že i když pravděpodobnost jejich výskytu není extrémně vysoká, jejich následky mohou mít vážný dopad na bezpečnost zaměstnanců i návštěvníků. Proto je nezbytné zajistit důkladnou prevenci a připravenost bezpečnostních opatření, jako jsou evakuační plány nebo pravidelná školení zaměstnanců.

Elektrická rizika a krádeže jsou hodnocena jako mírná rizika (III. a IV.), což znamená, že i když jejich pravděpodobnost je nižší, mohou mít negativní dopad na provoz a majetek zábavního parku Galaxie. Některá rizika, jako například možnost vstupu na střechu, spadají do kategorie akceptovatelného rizika (IV.), což znamená, že jejich kontrola není nezbytná, ale stále je potřeba přijmout preventivní opatření k jejich eliminaci, což je např. uzamčení přístupových bodů nebo instalace fyzických bariér.

Celá kapitola vyzdvihuje důležitost komplexního posouzení nejen aktuálního stavu, ale i kontextu rizik, přičemž metodika napomáhá navrhnout specifická a cílená preventivní opatření. Tato struktura umožňuje bezpečnější řízení rizik a dává jasné směřování, kdy a jaké zásahy jsou třeba provést, aby se minimalizovaly možné škody.

6 SOUČASNÝ STAV ZABEZPEČENÍ

Bezpečnost v Galaxii je zajištěna systémem ochranných prvků, alarmů, kamerového monitorování a evakuačních opatření. Objekt je rozdělen do jednotlivých bezpečnostních zón a pravidelně kontrolován s cílem minimalizovat možné hrozby a rizika. Zaměstnanci absolvují školení na krizové události a požární ochranu, přičemž je kladen důraz na rychlou reakci na mimořádné situace.

6.1 Aktuální stav přístupových cest a jejich řešení

Most vedoucí k zábavnímu parku Galaxie a přilehlým sportovištím představuje stěžejní bod perimetrické ochrany a bezpečnosti. Konstrukce mostu by měla odpovídat aktuálním technickým standardům, poněvadž zde není zajištěn plynulý provoz vozidel a bezpečný přístup, což je umocněno tím, že je to jediná přístupová cesta. Most je příliš úzký. Může na něj vjet pouze jedno vozidlo, zatímco ostatní musí čekat a tato situace vede k následnému zablokování hlavní přístupové cesty ze Zlína, Fryštáku a směru z Galaxie a zdejších sportovišť.



Obrázek 7 Most ke Galaxii

(zdroj: [vlastní])

To nejen zpomaluje dopravu, ale v případě krizové situace, například požáru nebo jiné mimořádné události v Galaxii, znemožňuje rychlý příjezd složek integrovaného záchranného systému (IZS). Pokud je situace na mostě bezproblémová, tak hasičský záchranný sbor (HZS) je v případě krizové situace v Galaxii do 15 minut. Doba příjezdu zdravotnického záchranného sboru (ZZS) a policejní hlídky se pohybuje od 3–10 minut. Příjezdová doba záchranných složek v případě zablokování mostu neukázněnými řidiči a následně zablokovanou cestou auty přijíždějící na most, by se mohla vyšplhat na dvojnásobek uvedeného času. Komplikace spojené s mostem představuje riziko pro rodiny

s dětmi, které využívají cestu ze zastávky městské hromadné dopravy k navštívení Galaxie. Úzký průjezd a omezený výhled na mostě zvyšuje pravděpodobnost nehody mezi vozidly, chodci a lidmi využívající cyklostezku křižující tento problematický úsek.

Rekonstrukce mostu by měla být prioritou, aby byla zajištěna plynulá doprava. Nový most s bezpečnostními prvky, odděleným chodníkem a dostatečným prostorem pro průjezd vozidel záchranných složek. Celkově by byla zvýšena bezpečnost a minimalizovalo by se riziko fatálních následků během mimořádné události v Galaxii.

Most je pravděpodobně ve vlastnictví města Zlína, a jeho údržba i případná rekonstrukce je tedy záležitostí městské správy. Jelikož most slouží nejen návštěvníkům Galaxie, ale i sportovišť a celé přilehlé lokality, měl by být jeho technický stav prioritně řešen jako veřejný zájem. Zábavní park Galaxie sám o sobě nemá pravomoc ani prostředky k jeho zásadní rekonstrukci bez účasti města.

6.2 Poplachový zabezpečovací a tísňový systém

Zabezpečení objektu Galaxie je zajištěno kombinací různých ochranných prvků, které zahrnují kouřové detektory, senzory pohybu a magnetické kontakty na dveřích. Na vchodové dveře a skleněné plochy jsou instalovány detektory tříštění skla. V hotelové části jsou protipožární dveře, které musejí být neustále uzavřeny. Tyto dveře jsou pravidelně kontrolovány a v případě jakýchkoli nedostatků opraveny nebo vyměněny. V celém objektu jsou rozmístěny požární hlásiče, přičemž výjimku tvoří prostory s minimálním rizikem vzniku požáru, jako jsou WC.



Obrázek 8 Únikové východy

(zdroj: [vlastní])

Objekt je rozdělen do několika zón, mezi něž patří obvodový plášť, restaurace, obchod, hotel, kancelář, hrací plocha, recepce a vstupní prostor. Kódování zón probíhá tak, že poslední osoba odcházející z haly provádí aktivaci zabezpečení, přičemž většina prostor, kromě vstupního prostoru a hotelu, je kódována.



Obrázek 9 Klávesnice PZTS

(zdroj: [vlastní])

U atrakcí jsou umístěny informační cedule s přísnými pravidly a instrukcemi, jak se chovat a maximální počet osob přítomných na atrakci. Na tato opatření pravidelně dohlíží personál a je školen, aby mohl rychle reagovat na jakékoli situace. Správu kapacit na atrakcích zajišťuje společnost Babykoutek s.r.o., která provádí pravidelné inspekce, aby zajistila maximální bezpečnost návštěvníků.

6.2.1 Denní kontrola atrakcí

Denní vizuální kontrola všech atrakcí musí být provedena každý den před uvedením hracího zařízení do provozu. Kontrolu provádí pověřená osoba, většinou to je brigádník, který zaznamenává stav zařízení do kontrolního listu a po ukončení jej stvrzuje svým podpisem.

Tabulka 23 Denní kontrola

(zdroj:[vlastní])

Kalendářní týden	Po	Út	St	Čt	Pá	So	Ne	Poznámky
ČALOUNĚNÍ NA STĚNÁCH								
1) bezpečné upevnění na stěně								
2) spojovací místa zarovnána								
3) spojovací místa bez špičatých předmětů								
4) potažení bezvadné (trhliny , opotřebení atd.)								
ROHOŽE NA OCHRANU PROTI PÁDU								
1) leží ve správné pozici, šrouby podlah dotažené								
2) spojovací místa zarovnána								
3) spojovací místa bez špičatých předmětů								
4) potažení bezvadné (trhliny , opotřebení atd.)								
SÍŤOVÉ STĚNY / SÍŤOVÉ STŘECHY								
1) šňůry pevné a napjaté								
2) sítě jsou nepoškozené								
3) sítě jsou svázány pevně a napjatě								
ZIPY								
1) oka v pořádku, nevytržená								
2) zipy a suché zipy zavřeny / zamknuty a v pořádku								
SKLUZY								
1) mezery bez předmětů								
2) plochy skluzů čisté								
3) plochy skluzů nepoškozené								
NARÁŽECÍ PYTLE/DORAZY/ZAVĚŠENÉ PRVKY/ATD.								
1) bezvadné zavěšení								
2) materiál plachty bezvadný (žádné trhliny atd.)								
ELEKTRO (děla, kompresory, dmýchadla atd.)								
1) všechny kabely neporušené a „neviditelné“								
2) žádné problémy , všechno jde bezvadně								
PROSTORY PRO MÍČKY								
1) bez předmětů a odpadů								
ČALOUNĚNÍ								
1) nepoškozené a zarovnané								
PODPIS								

6.3 DVS a monitorovací systém

Systém kamerového dohledu zahrnuje 30 kamer, z nichž 16 je sledováno v reálném čase na recepci a 5 je vybaveno nočním viděním. Záznamy se uchovávají po dobu 30 dní a jsou přístupné pouze oprávněným osobám, tj. majitelům a provozní manažerce. Restaurace

není pokryta kamerami a je to z toho důvodu, že jsou na stěnách instalované LED osvětlení a během dne je zde stále personál. Kamery jsou rozmístěny tak, aby pokrývaly všechny klíčové oblasti, včetně atrakcí, recepcce, jídelní zóny se stoly a rohů objektu. Ve druhém patře, kde se nachází multifunkční hřiště, jsou také nainstalovány kamery, aby zajistily maximální dohled. Některé únikové východy nejsou z vnější strany dostatečně viditelné, a proto je jejich stav monitorován buď kódovacím systémem, nebo vnitřní kamerou. Pravidelně každé čtyři roky probíhá výměna kamer, přičemž ke správě se využívá software SmartPss, který umožňuje efektivní dohled a správu záznamů.

Interní přístup ke kamerám mají majitelé a provozní manažerka. Ti mohou systém spravovat i na mobilních zařízeních, například při rušení poplachů.



Obrázek 10 Vstupní bariéra

(zdroj: [vlastní])

6.4 Evakuační systémy

V případě nouzové situace jsou návštěvníci informováni prostřednictvím evakuačního rozhlasu, který umožňuje rychlé předání pokynů pro bezpečný a organizovaný odchod z budovy. Hlášení je možné provádět jak automatizovaně, tak i manuálně prostřednictvím mikrofonu obsluhovaného personálem na recepci. Tento systém zajišťuje okamžitou komunikaci v krizových situacích, například při požáru nebo jiné mimořádné události.

Evakuační trasy jsou v souladu s bezpečnostními normami jasně označeny na stěnách pomocí směrových značek, které jsou viditelné i při výpadku elektrického proudu. Součástí bezpečnostních prvků jsou také nouzová světla, která se aktivují při poruše hlavního napájení a zajišťují minimální úroveň osvětlení potřebnou k bezpečné evakuaci.

Evakuační plány jsou pravidelně testovány každých šest měsíců, aby byla ověřena jejich funkčnost a připravenost personálu na krizové situace. Součástí těchto kontrol je i důsledné prověřování průchodnosti únikových cest, které nesmí být žádným způsobem blokovány, například uskladněným materiálem nebo nábytkem. Hlavní revize požární bezpečnosti objektu je prováděna hasičským záchranným sborem v tříletých intervalech, během nichž se ověřuje funkčnost evakuačních systémů, stav únikových tras a celková úroveň požární prevence.

Pro rychlé odpojení elektrického napájení v případě požáru nebo jiného technického incidentu je v objektu instalováno nouzové tlačítko Total Stop, které okamžitě přeruší napájení vybraných zařízení či celého objektu.

Budova je navíc chráněna proudovými chrániči, které monitorují elektrický obvod a v případě detekce nežádoucího rozdílu proudů okamžitě odpojí napájení, čímž minimalizují riziko úrazu elektrickým proudem nebo vzniku požáru. Tyto prvky jsou umístěny v rozvaděči nacházející se v mezipatře, kde jsou snadno dostupné pro obsluhu i záchranné složky v případě nutnosti zásahu.

6.4.1 Požární hlídka

Pokyny pro činnost preventivních požárních hlídek jsou složeny ze dvou fází. Prvních z nich je požární prevence a druhá fáze se aplikuje v případě vzniku požáru. V hlídce je zařazeno hned několik členů. Majitel Galaxie Tomáš Valášek zastává funkci vedoucího hlídky.

V případě požární prevence je jeho povinností spolupracovat s vedoucím zaměstnancem v otázkách dodržování požární ochrany na pracovišti a dbát na dodržování

požárního řádu. Valášek Tomáš v případě vzniku požáru oznamuje vznik požáru na ohlašovnu požáru HZS Zlínského kraje. Do příjezdu jednotky požární ochrany odpovědný za činnost členů požární prevence a kontrolu přípravy hasících prostředků.

Členové požární hlídky, kde je např. majitelka Galaxie Jana Valášková nebo provozní manažerka a další dvě osoby mají několik rozdělených specifických úkolů v prevenci proti požáru. Jeden člen kontroluje, zda je volný přístup k prostředkům PO, volně průchodné únikové cesty a zda je pracoviště v řádném stavu z hlediska PO. Další člen požární hlídky dohlíží na to, aby návštěvníci nevnašeli do ubytovacích prostor hořlavé či jiné pyrotechnické látky. Poslední člen kontroluje pořádek na pokojích. Všichni tito členové požární hlídky v případě vzniku požáru okamžitě organizují bezpečnou evakuaci všech prostor a provádí koordinovaný hasební zásah přenosnými hasicími přístroji nebo pomocí hydrantů do doby, než se dostaví jednotka HZS.

Povinnosti ostatních zaměstnanců v prevenci jsou takové, že každý je povinen si na pracovišti počínat tak, aby nezpůsobil vznik požáru, zejména při používání tepelných, elektrických, plynových a jiných spotřebičů. Při vzniku požáru se řídí pokyny poplachových požárních směrnic do příjezdu jednotky požární ochrany plní rozkazy vedoucího požární hlídky, dále velitele zásahu.

6.5 Incident management

V rámci krizového řízení jsou pravidelně organizována cvičení, která simulují různé krizové situace, a to pod dohledem společnosti EPOS Kroměříž. Během těchto cvičení je personál vystaven reálným scénářům, které se mohou vyskytnout v Galaxii a je potřeba na ně reagovat.

Mezi klíčové úkoly patří odpovědi na otázky týkající se správného postupu, například jak reagovat na aktivaci tísňového hlásiče, jak provádět prohlídku objektu v případě hrozby, a co dělat v situacích, kdy se objeví potřeba evakuace. Komunikace mezi integrovaným záchranným systémem (IZS) a personálem probíhá telefonicky. Krizová strategie, která je součástí firemního plánu, je pravidelně aktualizována, přičemž poslední revize proběhla na podzim roku 2023.

6.5.1 Školení personálu

Školení personálu je zaměřeno na identifikaci a reakci na různé hrozby, kterým mohou zaměstnanci čelit. V rámci školení jsou proškoleni nejen majitelé a zaměstnanci, ale i dlouhodobí brigádníci a členové požární čety, kterou vede pan Valášek. Tato četa se skládá z 5 kvalifikovaných členů, kteří jsou připraveni na krizové situace. Školení zahrnuje i postupy v případě úrazu, kde se personál učí, jak správně reagovat a jak poskytovat první pomoc. Během školení se probírá zhruba 10 klíčových zásad, které personál musí ovládat. V současnosti není k dispozici defibrilátor, což je oblast, která by mohla být v budoucnu zvážena pro zajištění vyšší úrovně bezpečnosti.

Každý rok probíhá školení o bezpečnosti a ochraně zdraví při práci (BOZP), kde jsou zaměstnanci seznámeni s aktuálními předpisy a postupy pro prevenci úrazů a ochranu zdraví v pracovním prostředí. Toto školení je nedílnou součástí pravidelných bezpečnostních opatření.

Zmíněná kapitola shrnuje bezpečnostní opatření v zábavním parku Galaxie ve Zlíně, která zahrnují kamerový systém, požární signalizaci, poplachový systém a evakuační plán. Objekt je rozdělen do zón, které jsou monitorovány kamerami a pravidelně kontrolovány. Důraz je kladen na bezpečnost atrakcí, přehledné značení únikových cest a funkčnost evakuačních prostředků. Kapitola rovněž upozorňuje na možné komplikace při příjezdu do areálu a na důležitost správné správy záznamů.

7 NÁVRH OPATŘENÍ

Cílem je vytvořit bezpečnostní systém pro rodinný zábavní park Galaxie Zlín. Návrh zahrnuje kombinaci perimetrické ochrany, která se vztahuje na parkoviště a okolí budovy, plášťové ochrany všech vstupů a obvodu objektu, a také prostorové a předmětové ochrany vnitřních prostor a cenného vybavení. Využity budou moderní technologie, mezi něž patří inteligentní kamery s AI analýzou, elektronické zabezpečovací a tísňové systémy (PZTS), kontrola vstupu a záložní napájecí systémy. Součástí návrhu je i rozpracování rizikových scénářů, jako jsou vloupání, požár, ozbrojený útok nebo výpadek proudu, včetně doporučených postupů a vhodných technologií pro jejich zvládnutí.

7.1 Perimetrická ochrana a okolí budovy

Perimetr areálu ohraničíme plotem a zajistíme jeho důležitá místa. V noci bude areál dobře osvětlen pomocí LED reflektorů s čidly, aby se snížila temná místa a zlepšily podmínky pro kamery. Osvětlení nejen odrazuje narušitele, ale také zvyšuje kvalitu záznamu kamer při slabém světle.

Okolí parkoviště a budovy pokryje soustava IP bezpečnostních kamer ve vysokém rozlišení (min. 4–8 Mpx). Kamery budou instalovány tak, aby měly překrývající se zorná pole a nevznikala hluchá místa. Na rozích budovy a stožárech okolo parkoviště budou umístěny fixní bullet nebo dome kamery se širokým úhlem záběru pro střežení celého obvodu. Oba typy kamer (bullet i dome) mohou mít objektivy, které pokrývají široký úhel záběru.

To znamená, že jsou schopny sledovat větší plochu než běžné kamery za nižší cenu. [28], [29]

Všechny kamery perimetru budou vybaveny pokročilou AI analýzou chování. Systém umí automaticky detekovat podezřelé aktivity v obraze v reálném čase. Patří sem detekce pohybu v zakázané zóně, překročení definované čáry, např. překonání plotu nebo loitering, což je podezřelé postávání osob na místě po abnormálně dlouhou dobu či tvoření davu. AI algoritmy dnes umí také rozlišovat osoby a vozidla od zvířat a jiných pohybů, čímž snižují počet planých poplachů např. ignorují pohybující se větve či toulavou kočku. [29]

Záznam a monitoring všech kamer bude napojen na centrální NVR server (Network Video Recorder) s dostatečnou kapacitou úložiště pro uchování záznamů min. 30 dní záznamu ze všech kamer v plné kvalitě. Dohledové centrum v rámci objektu např. v kanceláři majitele parku bude vybaveno více monitorovou stěnou, kde lze sledovat obrazy

z kamer v reálném čase. Alternativně lze využít i vzdálený dohled (připojení DPPC nebo mobilní aplikace pro majitele parku). [29]

7.2 Plášťová ochrana budovy

Všechny vchodové dveře, brány a snadno přístupná okna budou osazeny magnetickými kontakty. Tyto senzory detekují otevření dveří či oken – při nežádoucím otevření v zajištěném stavu spustí poplach. Lze využít například robustní kovové kontakty s pracovní mezerou cca 5–7 cm pro vrata a standardní skryté kontakty pro okna. Moderní kombinované senzory umí spojit funkci detekce otevření a vibrací. Existují kombinované detektory integrující otřesový senzor a magnet pro okna, které zaznamenají, jak pokus o vypáčení, tak samotné otevření. [30]

V místnostech s většími prosklenými plochami jako jsou okna, skleněné vstupní dveře budou nainstalovány detektory tříštění skla. Interiér podél obvodových stěn pokryjeme PIR čidla pro detekci pohybu narušitele. Kombinované čidlo v rohu místnosti tak chrání prostor pohybu a současně slyší tříštění skla. [31]

V technických místnostech můžeme nasadit detektory úniku vody. To je u toalet a kuchyněk hlídají vytápění. Pro střešní světlíky nebo ventilační otvory lze použít buď magnetické kontakty, otřesová čidla nebo naklonění, která detekují otevření nebo demontáž. Na objektu bude minimálně jedna vnitřní siréna s houkačku s intenzivním zvukem a jedna venkovní siréna s vlastním záložním napájením a stroboskopem. [30]

Kromě elektronických prvků je vhodné nepodcenit mechanické zabezpečení. Všechny vstupní dveře by měly mít kvalitní vícebodové zámky a bezpečnostní kování. Okna v přízemí by měla mít bezpečnostní fólii proti snadnému rozbití, aby útočníkovi se znesnadnilo roztržít sklo nebo použít skla např. vrstvená, která při rozbití drží. [32]

7.3 Prostorová a předmětová ochrana

Tato část ochrany je zaměřena na vnitřní prostory parku, ochranu návštěvníků, zaměstnanců a cenného vybavení uvnitř zábavního parku.

Uvnitř haly budou rozmístěny bezpečnostní kamery tak, aby bylo dodrženo soukromí návštěvníků. Kamery by měly být zejména u hlavních vstupních dveří a recepce kdy, monitorujeme tok návštěvníků a dohled nad pokladnou, herní plochy pro dohled nad bezpečností dětí, např. možné úrazy či ztracení, chodby a schodiště kvůli vandalismu či

požáru, vstupy do zaměstnaneckých částí, sklady a pokladny. Použity budou stropní kamery s 360° záběrem nebo širokoúhlé kamery, aby jedna kamera pokryla co největší plochu.

V místech, kde je třeba detail například u pokladny na recepci, lze dát kameru s vyšším rozlišením a užším úhlem. Všechny kamery budou opět napojeny na centrální NVR. Záznam z vnitřních kamer pomůže řešit případné incidenty např. krádeže, vandalismus a zároveň může sloužit při hledání ztraceného dítěte apod.

Trezor by měl být vybaven otřesovým (seizmickým) detektorem, který zaznamená pokus o násilné otevření trezoru jako je vrtání, páčení, náraz nebo prudké změny teploty např. řezání plamenem. Tyto trezorové detektory naslouchají vibracím a úderům na konstrukci trezoru a při detekci atypických vibrací spustí okamžitě alarm. [33]

Pro herní automaty a simulátory lze využít alarm při naklonění či pohybu. Na vhodných místech u recepcce, pokladny a kanceláře budou instalována tlačítka tísňového poplachu. Tato nenápadná tlačítka umožní personálu v případě ohrožení, což může být loupežné přepadení pokladny či útok, potichu spustit alarm napojený přímo na DPPC nebo policii.

7.3.1 Kontrola vstupů

Pro návrh kontrolovaného vstupu do zábavního parku Galaxie, kde bude jeden turniket pro běžný vstup, větší turniket pro kočárky a turniket pro výstup.

Pro běžný vstup návštěvníků lze použít tříramenný turniket pro jednotlivé osoby. Daný turniket bude umístěn u hlavního vstupu do parku. Ten může být vybaven RFID čtečkou pro čipové karty nebo QR čtečkou pro lístky. Po načtení vstupenky nebo čipu se turniket otočí a umožní vstup. Turniket bude zajišťovat jednosměrný přístup, a to pouze do parku.

Další turniket bude uzpůsoben pro návštěvníky s kočárky a na invalidním vozíčku. Zmíněný turniket bude mít širší průchod než standardní turniket, aby umožnil bezproblémový průchod rodičů s kočárky. Ideálně to bude otáčivý turniket nebo automatické dveře, které se otevrou pro kočárky a osoby na vozíku. Turniket by měl mít obousměrnou funkčnost, což znamená, že se bude moci otevírat nejen pro vstup, ale i pro výstup. Daný turniket by mohl být vybaven bezkontaktními čtečkami QR nebo RFID, stejně jako automatickými dveřmi pro pohodlí návštěvníků.

Posledním turniketem bude pro výstup návštěvníků z parku. Tento turniket by sloužit k regulaci odchodu návštěvníků. Lze použít standardní turniket, který bude zajišťovat jednosměrný průchod ven z parku.

System řízení přístupu by měl být integrovaný pro všechny tři turnikety. Každý turniket bude propojen s centrální správní jednotkou např. pomocí RFID čtečky nebo QR systémů pro ověření lístků, která bude zajišťovat bezpečnostní a kontrolní mechanismy. Pohybové senzory nebo obousměrné RFID čtečky mohou detekovat, zda někdo prochází ve správném směru tzn. vstup nebo výstup, čímž se zamezí neoprávněnému průchodu. Pokud je detekován nesprávný směr, turniket automaticky zablokuje cestu. Během krizové situace, kdy je potřeba nouzový východ návštěvníků, budou všechny turnikety automaticky otevřeny pro rychlý a bezpečný únik z budovy.

Vedle turniketů pro veřejnost bude u personálního vchodu instalován přístupový systém pro zaměstnance. Každý zaměstnanec dostane RFID čipovou kartu nebo přívěsek, případně využije otisk prstu k odemčení zaměstnaneckého vchodu. Čtečka u dveří ovládá elektrický zámek a vpustí dovnitř jen oprávněné osoby. V systému jsou definovány přístupové úrovně např. manažeři mají karty do všech prostor, údržba jen do strojovny. Elektrické zámky, tzn. např. elektromagnetické zámky nebo elektrické otvírače, fungují v propojení s přístupovou jednotkou. Ta po přiložení platné karty pošle impulz do zámku k otevření dveří.

U všech průchodů bychom měli zjistit, kdo kdy vstoupil. Dveře s elektronickými zámky budou samozřejmě rovněž chráněny magnetickými kontakty pro případ násilného otevření. V citlivých vnitřních prostorách v kanceláři vedení, sklady nebo serverovna, by mohly být elektronické kódové zámky nebo čtečky. Pouze pověřeni pracovníci s kódem či kartou se dostanou dovnitř. Serverovna by měla být zabezpečena kombinací karty, kódu a biometrie. Tím vzniká vícefaktorová ochrana, která výrazně zvyšuje úroveň zabezpečení.

7.4 Scénář vybraných bezpečnostních incidentů

Zde analyzujeme několik modelových bezpečnostních incidentů s popisem, jak navržené technologie pomohou v detekci a řešení těchto scénářů.

Scénář incidentu: Vloupání v noci (narušitel se pokouší dostat dovnitř mimo otevírací dobu)

- Detekce a poplach: Kamery v rámci perimetru zaznamenají pohyb osoby v areálu (AI detekce narušení zóny) a spustí upozornění. Senzory na plášti (magnety, detektor skla) ihned detekují pokus o vstup (otevření dveří, rozbití okna) a vyhlásí poplach. PIR čidla uvnitř zachytí pohyb narušitele, pokud pronikne dovnitř.

- Opatření a reakce: PZTS ústředna spustí alarm. Vnitřní i venkovní sirény začnou houkat a stroboskop začne blikat, což může působit stresově na pachatele. Ústředna okamžitě přenáší poplach na DPPC bezpečnostní agentury. Do několika minut vyjíždí zásahová jednotka či je informována PČR. Odpovědná osoba může přes mobil obdržet zprávu o poplachu. Kamerový systém v reálném čase předává obraz dálkově či pověřené osobě, čímž umožní ověřit situaci a informovat zasahující složky o pohybu pachatele.
- Technologie: Ústředna se všemi čidly, sirény, GSM komunikátor na DPPC, noční vidění kamerového systému, AI analýza pohybu. Mechanické zábrany zámky, fólie pro zdržení pachatele.

Scénář incidentu: Ozbrojený útočník (aktivní střelec nebo nebezpečná osoba v areálu)

- Detekce a poplach: Detekce takovéto hrozby je obtížná preventivně. Může pomoci AI kamerová analýza rozpoznání náhlého zběsilého pohybu, paniky davu či pádů osob, což by automaticky vyhlásilo stav nouze. Všimne si někdo podezřelé osoby se zbraní, může potají spustit tichý poplach stiskem tlačítka na recepci. Ostraha na kamerách zaznamenaná neobvyklé chování jako je běžící dav či křik.
- Opatření a reakce: Okamžitá reakce personálu. Pokud je to možné, personál varuje ostatní např. kódovým hlášením v rozhlase: „návštěva červená“ apod., aby zahájili úkryt nebo útěk dle plánu pro aktivního střelce.

Tichá signalizace policii přes personál na recepci, který stisknutím tísňová tlačítka vyšle alarm na DPPC nebo policii, že probíhá útok. Policie vyráží do Galaxie.

V případě potřeby mohou být některé vstupy do budovy uzamčeny na dálku prostřednictvím elektronických zámků, pokud to situace umožní. Tím se útočnickovi ztíží přístup do citlivých prostor, jako je například řídicí místnost nebo sklady.

Prostřednictvím ozvučení v parku lze dát návštěvníkům pokyn k ukrytí: „prosím, ukryjte se a zůstaňte v klidu“, případně specifické instrukce. Hlášení může spustit manuálně vedení nebo automaticky jako přednastavenou zprávu při stisku tichého poplachu.

Na místě zásahu kamerový systém poskytuje policii online přenos. Pokud je integrace, lze sdílet přístup ke kamerám, aby měli přehled o pohybu útočníka.

Po zneškodnění útočníka se zajistí první pomoc zraněným. V areálu je lékárnička a defibrilátor.

- Technologie: tísňová tlačítka propojená na DPPC nebo policii. Rozhlasová jednotka pro krizová hlášení. Vstupní systém umožňující dálkové zamčení a odemčení dveří. Kamerový systém s možnou analýzou davu a paniky a vzdáleným přístupem pro složky IZS. Krizový plán a nácvik takové situace.

Scénář incidentu: Výpadek elektrického proudu (blackout v okolí, porucha trafostanice)

- Detekce a poplach: Při ztrátě napájení přechází systémy na záložní zdroj, což je indikováno technickým poplachem. UPS jednotky začnou napájet kritické systémy bez přerušení. [34]
- Opatření a reakce: Nepřerušovaný provoz zabezpečení zásluhou UPS zůstává alarm, kamery i přístupový systém v chodu po dobu desítek minut. Kamery i záznam fungují dál, případně se sníží kvalita záznamu pro úsporu energie. Nouzové osvětlení okamžitě rozsvítí nouzová LED světla na únikových cestách, mají vlastní baterie, aby byla zajištěna orientace osob ve tmě. Venkovní osvětlení může vypadnout, proto areál zůstane monitorován kamerami s nočním viděním.

Režim dveří a turniketů bude takový, že elektronické zámky přejdou do bezpečného stavu. Většina se bez proudu odemkne, aby neuvěznily osoby. Turnikety díky padacímu rameni uvolní průchod, takže lidé mohou kdykoli volně vyjít ven nebo vpustit dovnitř záchranné složky.

Pokud by výpadek trval déle než výdrž nepřerušitelného napájecího zdroje, což je kolem 30 minut, je vhodné mít připraven benzínový nebo diesel generátor, který automaticky nastartuje a zajistí elektřinu pro klíčové systémy zahrnující světla, alarmy, mrazáky v kuchyni atd. Po návratu proudu se systémy postupně přepnou zpět na síť.

Technologie: UPS 1–2 kVA pro kamerový server a ústředny. [34]

Každý scénář ukazuje, že navržené technologie spolupracují. Detekční prvky jako kamery a senzory aktivují odpovídající poplachové a reakční systémy, například sirény nebo varovné zprávy. Tím dochází k efektivnímu zmírnění dopadů incidentu. V případě vloupání sehrává klíčovou roli kombinace mechanických zábran, jako jsou dveře a zámky, spolu s elektronickými čidly, které pachatelům výrazně ztěžují průnik a zároveň zvyšují

pravděpodobnost jejich zadržení. Při požáru pak včasná detekce spolu s automatickým spuštěním evakuačních mechanismů přispívá k ochraně životů a majetku.

Daná kapitola shrnuje komplexní bezpečnostní systém pro rodinný zábavní park Galaxie Zlín. Cílem je ochránit areál, budovu i osoby před různými hrozbami, jako jsou vloupání, nebo útok. Kapitola popisuje návrh tří typů ochrany.

Perimetrická ochrana zahrnuje oplocení, osvětlení a venkovní kamerový systém vybavený umělou inteligencí, který slouží k detekci podezřelého chování v okolí parku.

Plášťová ochrana budovy se zaměřuje na zabezpečení vstupů, oken a technických otvorů prostřednictvím senzorů, detektorů pohybu, detektorů tříštění skla a požárních hlásičů, přičemž důraz je kladen i na mechanické zabezpečení dveří a oken.

Prostorová a předmětová ochrana se orientuje na vnitřní prostory objektu, kde je instalován kamerový systém na klíčových místech a zajištěna ochrana pokladen, trezoru a cenného vybavení. Součástí této ochrany je také návrh systému kontroly vstupů pro návštěvníky i zaměstnance, který využívá turnikety, čtečky a přístupové karty. V celé kapitole je kladen důraz na využití moderních technologií a propojení jednotlivých systémů s centrálním dohledovým centrem. Celý návrh má za cíl zvýšit bezpečnost, efektivitu reakce na incidenty a přehled o dění v objektu.

Praktická část bakalářské práce se zaměřuje na analýzu bezpečnostních rizik v konkrétním prostředí rodinného zábavního parku Galaxie Zlín. K tomuto účelu byla využita CHECK list a PNH metoda, která umožnila systematicky identifikovat možná nebezpečí, ohodnotit pravděpodobnost jejich výskytu a závažnost jejich dopadu. Analýza zahrnovala několik oblastí, mimo jiné rizika zabezpečovacího charakteru, rizika spojená s elektrickým zařízením, možnosti útoku ze strany jednotlivce a další hrozby, které mohou ohrozit návštěvníky i zaměstnance. Výsledkem je návrh konkrétních opatření pro snížení těchto rizik, včetně doporučení pro posílení bezpečnostních prvků a zavedení preventivních kroků.

ZÁVĚR

Bakalářská práce Analýza bezpečnosti rodinného zábavního parku ve Zlíně poskytla komplexní pohled na současný stav zabezpečení rodinného zábavního parku Galaxie ve Zlíně a identifikovala klíčová rizika spojená s jeho provozem. Na základě teoretických poznatků o měkkých cílech a bezpečnostních technologiích byla navržena řada opatření, která mají za cíl zvýšit úroveň bezpečnosti jak pro návštěvníky, tak pro zaměstnance parku. Práce zdůraznila důležitou kombinaci fyzických, technologických a organizačních prvků ochrany a ukázala, jak mohou moderní technologie, jako jsou inteligentní kamerové systémy či integrované bezpečnostní systémy, přispět k prevenci a rychlé reakci na potenciální hrozby.

Z výsledků této práce vyplývá, že efektivní bezpečnost měkkých cílů, jako jsou rodinné zábavní parky, vyžaduje komplexní přístup, který zahrnuje nejen kvalitní mechanické a elektronické prvky, ale také pravidelná školení personálu a dobře připravené krizové plány na negativní události. Tento komplexní přístup umožňuje minimalizovat rizika a efektivně reagovat na bezpečnostní incidenty.

Navržená opatření a závěry práce mohou sloužit jako doporučení nejen pro konkrétní analyzovaný objekt, ale i pro další obdobné objekty, které hledají možnosti zlepšení svého zabezpečení.

SEZNAM POUŽITÉ LITERATURY

- [1] CHOVANEC, Milan, 2017. *Koncepce ochrany měkkých cílů pro roky 2017-2020*. Online. 3. Praha: PostSignum Qualified. Dostupné z: *Koncepce_ochrany_měkkých_cílů_pro_2017-2020.pdf*. [cit. 2024-11-04].
- [2] *Základy ochrany měkkých cílů – metodika*, 2016. Online. Praha: Soft Targets Protection Institute. Dostupné z: *ZÁKLADY OCHRANY MĚKKÝCH CÍLŮ METODIKA.pdf*. [cit. 2024-11-04].
- [3] KOTEK, Lukáš, *Základy ochrany měkkých cílů* [prezentace]. Bezpečnostní inženýrství. [s.l.], [rok prezentace neuveden].
- [4] ČESKÁ JUSTICE, 2023. *Legislativa je dostatečná, musí se řešit ochrana měkkých cílů, soudí poslanci*. Online. 2023-12-21. Dostupné z: <https://www.ceska-justice.cz/2023/12/legislativa-je-dostatecna-musi-se-resit-ochrana-mekkych-cilu-soudi-poslanci/>. [cit. 2024-11-13].
- [5] KALVACH, Zdeněk a VANGELI, Benedikt, 2018. *VYHODNOCENÍ OHROŽENOSTI MĚKKÉHO CÍLE aneb co, kdy, kde a od koho vám hrozí*. Online. Praha: Ministerstvo vnitra ČR. [cit. 2025-05-15].
- [6] LUKÁŠ, Luděk, 2014. *Bezpečnostní technologie, systémy a management*. IV. Zlín: VeRBuM. ISBN 978-80-87500-57-6.
- [7] ŠEFČÍK, Vladimír, 2009. *Analýza rizik*. Zlín: Univerzita Tomáše Bati Academia Centrum. ISBN 978-80-7318-696-8.
- [8] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management V*. Zlín: VeRBuM, 2015. ISBN 978-80-87500-67-5.
- [9] LOVÁS, Juraj, 2010. *Eliminácia rizík bezpečnosti práce vo vybranom podniku*. Online, Bakalářská práce, vedoucí Viera Šukalová. Banská Bystrica: Zahraničná vysoká škola Banská Bystrica. Dostupné z: https://is.ambis.cz/th/u84mk/BP_Juraj_Lovas_-_Eliminacia_rizik_bezpecnosti_prace_vo_vybranom_podniku.pdf. [cit. 2024-12-27].
- [10] APTIEN. *Co je to hrozba*. Online. Dostupné z: <https://aptien.com/cs/kb/articles/what-is-threat>. [cit. 2024-12-27].
- [11] IVANKA, Ján, 2014. *Mechanické zábranné systémy*. Online. [cit. 2024-12-06].

- [12] VALOUCH, Jan, 2019. Projektování bezpečnostních systémů. Online. Zlín: Univerzita Tomáše Bati. ISBN 978-80-7454-858-1. [cit. 2025-05-15].
- [13] UHLÁŘ, Jan. *Technická ochrana objektů. I. díl*. Policejní akademie České republiky. Vyd 2. 2009. ISBN 978-80-7251-312-3.
- [14] PERIMETRIE.CZ. *Plášťová ochrana*. Online. Dostupné z: <https://www.perimetrie.cz/perimetrie/plastova-ochrana/>. [cit. 2024-12-06].
- [15] ELEKTROMIKA. *Kamerové systémy*. Online. Dostupné z: <https://www.elektromika.cz/nabizime/kamerove-systemy/>. [cit. 2024-12-06].
- [16] EBIS. *EISS Integrovaný zabezpečovací systém*. Online. Dostupné z: <https://www.ebis.cz/cs/clanky/clanky-eiss/eiss-integrovaný-zabezpečovací-systém>. [cit. 2024-12-06].
- [17] SOLID SECURITY. *DVS kamery a EZS*. Online. Dostupné z: <https://solidsecurity.cz/DVS-kamery-a-ezs/>. [cit. 2024-12-06].
- [18] KŮTKA, MICHAL, 2016. https://www.vut.cz/www_base/zav_prace_soubor_verejne.php?file_id=124910. Online, BAKALÁŘSKÁ PRÁCE, vedoucí Ing. MIROSLAV JIRGL. BRNO: VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ. Dostupné z: https://www.vut.cz/www_base/zav_prace_soubor_verejne.php?file_id=124910.. [cit. 2025-05-25].
- [19] ALARMYZABEZPEČENÍ.CZ. *Stupeň zabezpečení*. Online. Dostupné z: <https://www.alarmyzabezpeceni.cz/stupen-zabezpeceni.html>. [cit. 2024-12-06].
- [20] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti I*. Zlín. Univerzita Tomáše Bati ve Zlíně. Vyd. 3. 2010. ISBN 978-80-7318-889-4.
- [21] ABBAS SHOP. *Detektory tříštění skla*. Online. Dostupné z: <https://eshop.abbas.cz/detektory-tristeni-skla#:~:text=Detektory%20t%C5%99%C3%AD%C5%A1t%C4%9Bn%C3%AD%20skla%20jsou%20za%C5%99%C3%ADzen%C3%AD%20pou%C5%BE%C3%ADvan%C3%A1%20v%20zabezpe%C4%8Dovac%C3%ADch,zvukov%C3%BDch%20sign%C3%A1l%C5%AF%2C%20kter%C3%A9%20jsou%20vyd%C3%A1v%C3%A1ny%20p%C5%99i%20t%C5%99%C3%AD%C5%A1t%C4%9Bn%C3%AD%20skla..> [cit. 2024-12-19].

- [22] TOP SECURITY. *Detektory pohybu v praxi*. Online. Dostupné z: <https://www.topsecurity.cz/blog/clanek/detektory-pohybu-v-praxi>. [cit. 2024-12-19].
- [23] ATKM JSME ZABEZPEČENÍ, 2024. *Poradna: PIR, MW, Antimasking – Jak fungují a jaká jsou rizika?* Online. Dostupné z: <https://www.atkm.cz/poradna-pir-mw-antimasking-jak-funguji-a-jaka-jsou-rizika>. [cit. 2024-12-27].
- [24] VA ELEKTRONIK. *Elektronická kontrola vstupu*. Online. Dostupné z: <https://www.va-elektronik.cz/elektronicka-kontrola-vstupu-ESKV>. [cit. 2024-12-27].
- [25] NĚMEČEK, Milan, 2008. *DVS kamery a jejich využití v zabezpečení objektů*. Online, Diplomová práce, vedoucí Milan Adámek. Zlín: Univerzita Tomáše Bati. Dostupné https://digilib.k.utb.cz/bitstream/handle/10563/5906/n%20me%20ek_2008_dp.pdf?sequence=1&isAllowed=n. [cit. 2024-12-27].
- [26] KELCOM INTERNATIONAL. *Analogové vs. digitální kamery*. Online. Dostupné z: <https://kelcom-sc.cz/novinky/analogove-vs-digitalni-kamery/>. [cit. 2024-12-27].
- [27] *Kriminalita Policie.cz*. Online. Dostupné z: <https://kriminalita.policie.gov.cz/>. [cit. 2025-05-13].
- [28] AVIGILON. *Complete guide to using parking lot security cameras*. Online. Dostupné z: <https://www.avigilon.com/blog/parking-lot-cameras#:~:text=The%20camera%E2%80%99s%20high,at%20any%20angle%2C%20in%20any%C2%A0light>. [cit. 2025-03-26].
- [29] HIKCENTRALLICENSE. *How Hikvision AI Cameras are Transforming Security Surveillance*. Online. Dostupné z: [AVIGILON. Complete guide to using parking lot security cameras](https://www.avigilon.com/blog/parking-lot-cameras#:~:text=The%20camera%E2%80%99s%20high,at%20any%20angle%2C%20in%20any%C2%A0light). Online. Dostupné z: <https://www.avigilon.com/blog/parking-lot-cameras#:~:text=The%20camera%E2%80%99s%20high,at%20any%20angle%2C%20in%20any%C2%A0light>. [cit. 2025-03-26]. [cit. 2025-03-26].
- [30] ATOM-SAFE. *Detektory tříštění skla s MG kontaktem*. Online. Dostupné z: <https://www.atom-safe.cz/c/ezs-eps/detekcni-technologie-vnitri/audio-detektory/gb-mg>. [cit. 2025-03-26].
- [31] ESHOP.EUROSAT. *JA-122PB Sběrníkový kombinovaný PIR detektor pohybu s detektorem tříštěním skla*. Online. Dostupné z: <https://eshop.eurosat.cz/product/122165/10373/ja-122pb-sbernicovy-kombinovany-pir-detektor-pohybu-s-detektorem-tristenim-skla>. [cit. 2025-03-26].

- [32] TSHPLAS. *Bezpečnosti sklo*. Online. Dostupné z: <https://www.tshplast.cz/bezpecnostni-skla/#:~:text=Bezpe%C4%8Dnostn%C3%AD%20sklo%20je%20tvo%C5%99eno%20slepen%C3%ADm%20dvou%20sklen%C4%9Bn%C3%BDch%20tabul%C3%AD%2C,bezpe%C4%8Dnostn%C3%AD%20f%C3%B3lie%20Connex%20ur%C4%8Dje%20jej%C3%AD%20pevnost%20a%20odolnost..> [cit. 2025-03-26].
- [33] ATOM-SAFE. *Trezorové detektory*. Online. Dostupné z: <https://www.atom-safe.cz/c/ezs-eps/detekcni-technologie-vnitri/detektory-otresu/trezorove-detektory>. [cit. 2025-03-26].
- [34] VOLTY.CZ. *UPS prevence výpadků elektrického proudu*. Online. Dostupné z: <https://www.volty.cz/2019/11/13/ups-prevence-vypadku-elektrickeho-proudu/#:~:text=UPS%20prevence%20v%C3%BDpadk%C5%AF%20elektrick%C3%A9ho%20proudu, dobu%2010%20%E2%80%93%2060%20minut.> [cit. 2025-03-26].

SEZNAM OBRÁZKŮ

Obrázek 1 Analýza násilných útoků na vybrané cíle	15
Obrázek 2 Typ teroristických útoku.....	16
Obrázek 3 Principy zabezpečení měkkých cílů	17
Obrázek 4 Parametry analýzy rizik	23
Obrázek 5 Grafické znázornění pyramidy postoupnosti procesů bezpečnosti v MZS	25
Obrázek 6 Blokové schéma PZTS	27
Obrázek 7 Most ke Galaxii	54
Obrázek 8 Únikové východy	56
Obrázek 9 Klávesnice PZTS.....	57
Obrázek 10 Vstupní bariéra	59

SEZNAM TABULEK

Tabulka 1 Stupeň zabezpečení.....	28
Tabulka 2 CHECK List perimetrická ochrana budovy	39
Tabulka 3 CHECK List obvodová ochrana budovy	39
Tabulka 4 CHECK List plášťová a prostorová ochrana	40
Tabulka 5 CHECK List zabezpečení vstupů	40
Tabulka 6 CHECK List požární systémy	41
Tabulka 7 CHECK List bezpečnostní incidenty.....	41
Tabulka 8 CHECK List personální zabezpečení a BOZP.....	42
Tabulka 9 CHECK List zabezpečení technologických prvků.....	42
Tabulka 10 Klasifikace úrovně rizika	47
Tabulka 11 Přehled rizik požáru v areálu a navrhovaná opatření	47
Tabulka 12 Závažnost rizik požáru v areálu dle metody	47
Tabulka 13 Přehled závažnosti rizik požáru v areálu dle metody	48
Tabulka 14 Závažnosti rizik útoků a bezpečnostních incidentů.....	48
Tabulka 15 Přehled závažnosti rizik útoků a bezpečnostních incidentů.....	49
Tabulka 16 Závažnost rizik zabezpečení pláště budovy	49
Tabulka 17 Přehled závažnosti rizik zabezpečení pláště budovy	50
Tabulka 18 Rizika související s technickými a bezpečnostními prvky	50
Tabulka 19 Přehled rizik související s technickými a bezpečnostními prvky.....	51
Tabulka 20 Závažnost rizik krádeží a vandalismu.....	51
Tabulka 21 Přehled závažnosti rizik krádeží a vandalismu	52
Tabulka 22 Vyhodnocení nejzávažnějších rizik.....	52
Tabulka 23 Denní kontrola.....	58

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AI – Umělá inteligence

BOZP – Bezpečnost a ochrana zdraví při práci

CBRN – Chemické, biologické, radiologické a jaderné hrozby

DVS – Digital Video Surveillance

CO₂ – Oxid uhličitý

ČR – Česká republika

DPPC – Dohledové poplachové a přijímací centrum

ESKV – Elektronický systém kontroly vstupu

EN – Evropská norma

PZTS – Poplachová zabezpečovací a tísňová signalizace

GSM – Global System for Mobile Communications

HZS – Hasičský záchranný sbor

IZS – Integrovaný záchranný systém

LED – Light Emitting Diode (Světlo emitující dioda)

MZS – Mechanické zábranné systémy

NVR – Network Video Recorder (Síťový videorekordér)

PČR – Policie České republiky

PIR – Passive Infrared (Pasivní infračervený senzor)

PO – Požární ochrana

QR – Quick Response (kód)

RFID – Radio Frequency Identification

FF – Filmový festival

UPS – Nepřerušitelný zdroj napájení