

Analýza rizik v procesu zajištění fyzické bezpečnosti objektu

Erik Vyoral



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:	Erik Vyoral
Osobní číslo:	A22261
Studijní program:	B1032A020001 Bezpečnostní technologie, systémy a management
Forma studia:	Prezenční
Téma práce:	Analýza rizik v procesu zajišťování fyzické bezpečnosti objektu
Téma práce anglicky:	Risk analysis in the process of ensuring the physical security of an object

Zásady pro vypracování

1. Zpracujte literární rešerši vztahující se k současnému stavu předmětné oblasti.
2. Identifikujte analytické metody v souvislosti s požadavky na zajištění fyzické bezpečnosti objektu.
3. Vyhodnoťte analytické metody k praktickému použití při zajištění fyzické ochrany objektu.
4. Navrhněte metodu vhodnou pro objektivní posuzování fyzické ochrany objektu.
5. Vytvořte návrh plánu fyzické ochrany objektu.

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

Seznam doporučené literatury:

1. ČESKÁ AGENTURA PRO STANDARDIZACI. ČSN ISO 31000:2018 Management rizik – Směrnice. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2018. 28 s. ISO 31000:2018.
2. ČESKÁ REPUBLIKA. Vyhláška č. 225/2015 Sb., o stanovení rozsahu bezpečnostních opatření fyzické ochrany objektu zařazeného do skupiny A nebo skupiny B. In: Sbírka zákonů České republiky. 2015, částka 93, s. 2674-2700.
3. PROCHÁZKOVÁ, Dana a PROCHÁZKA, Jan. Analýza rizik I. Praha: Vysoká škola regionálního rozvoje Praha, 2014. ISBN 978-80-87174-26-5.
4. PROCHÁZKOVÁ, Dana a PROCHÁZKA, Jan. Analýza rizik II. Praha: Vysoká škola regionálního rozvoje Praha, 2014. ISBN 978-80-87174-27-2.
5. KORECKÝ, Michal a TRKOVSKÝ, Václav. Management rizik projektů: se zaměřením na projekty v průmyslových podnicích. Expert. Praha: Grada, 2011. ISBN 978-80-247-3221-3.

Vedoucí bakalářské práce: **Ing. Mgr. Kamila Čížová**
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

Tato bakalářská práce se zaměřuje na zajištění fyzické ochrany objektu s důrazem na komplexní soubor technických, režimových a organizačních opatření. Analýza rizik je využívána jako podpůrný nástroj pro identifikaci potenciálních hrozeb a návrh vhodných bezpečnostních opatření. Teoretická část práce poskytuje přehled principů fyzické ochrany, včetně mechanických zábran, systémů MZS a PZTS, kamerových systémů a režimových opatření. Praktická část se zaměřuje na konkrétní objekt, pro který jsou aplikovány vybrané metody analýzy rizik, jež slouží k návrhu a ověření vhodnosti zvolených opatření. Výstupy práce mohou být využity jako podklad pro efektivní řízení bezpečnostních procesů a snížení rizik ohrožujících majetek a osoby.

Klíčová slova: fyzická bezpečnost, bezpečnostní opatření, mechanické zábrany, PZTS, MZS, kamerové systémy, režimová opatření

ABSTRACT

This bachelor's thesis focuses on ensuring the physical security of a facility through a comprehensive set of technical, procedural, and organizational measures. Risk analysis is used as a supporting tool to identify potential threats and to propose appropriate security measures. The theoretical part provides an overview of the principles of physical protection, including mechanical barriers, intrusion detection systems (IDS), access control systems, DVS systems, and procedural measures. The practical part applies selected risk analysis methods to a specific facility in order to design and verify the suitability of the proposed measures. The findings of this thesis may serve as a basis for effective security management and risk reduction related to the protection of assets and people.

Keywords: physical security, security measures, mechanical barriers, IDS, access control systems, DVS, procedural measures

Rád bych touto cestou poděkoval vedoucí své bakalářské práce Ing. Mgr. Kamile Čížové za odborné vedení, cenné rady, podněty a vstřícný přístup při řešení jednotlivých částí práce. Dále děkuji všem vyučujícím Fakulty aplikované informatiky za získané znalosti a podporu v průběhu studia. Velké díky patří také mé rodině a blízkým za trpělivost, motivaci a podporu během celého studia a zpracování této práce.

OBSAH

ÚVOD.....	11
I TEORETICKÁ ČÁST	13
1 FYZICKÁ BEZPEČNOST.....	14
1.1 MECHANICKÉ ZÁBRANNÉ SYSTÉMY	14
1.1.1 Obvodová ochrana	15
1.1.2 Plášťová ochrana	15
1.2 POPLACHOVÉ ZABEZPEČOVACÍ A TÍŠŇOVÉ SYSTÉMY	16
1.2.1 Dohledové videosystémy (DVS).....	16
1.2.2 Detektory pohybu.....	19
1.2.3 Přístupové systémy.....	21
1.3 REŽIMOVÁ OPATŘENÍ	22
1.3.1 Areálové omezení přístupu	22
1.3.2 Kontrola vstupu a výstupu	23
1.3.3 Časové omezení přístupu	24
2 CHARAKTERISTIKA RIZIKA	27
2.1 DEFINICE RIZIKA	27
3 ANALÝZA RIZIK	29
3.1 ZÁKLADNÍ POJMY	29
3.2 PŘÍKLADY ANALÝZ RIZIK	30
3.2.1 SWOT analýza	30
3.2.2 Jednoduchá bodová analýza	30
3.2.3 Multikriteriální analýza rizik.....	31
3.2.4 ETA – Stromová analýza událostí.....	31
4 ANALÝZA MOŽNOSTI NEOPRÁVNĚNÉHO VNIKNUTÍ.....	32
4.1 PŘEDMĚT ČINNOSTI PROVOZOVATELE	32
4.2 INTERNÍ PŘEDPISY A LEGISLATIVA.....	32
4.3 ORGANIZAČNÍ A PERSONÁLNÍ STRUKTURY	33
4.4 HROZBY PLYNOUCÍ Z CELOSPOLEČENSKÉ SITUACE A JEJÍHO VÝVOJE MIMOŘÁDNÝCH UDÁLOSTÍ.....	34
5 DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI	36
II PRAKTICKÁ ČÁST	37
6 ÚVOD DO PRAKTICKÉ ČÁSTI.....	38
6.1 POPIS MODELOVÉHO OBJEKTU SPOLEČNOSTI BLASTEX S.R.O.	38
6.2 PŘEDMĚT ČINNOSTI PROVOZOVATELE	39
6.3 INTERNÍ PŘEDPISY A LEGISLATIVA.....	40
6.4 TECHNICKÉ A TECHNOLOGICKÉ ZABEZPEČENÍ.....	40

6.5	ORGANIZAČNÍ A PERSONÁLNÍ STRUKTURA	42
7	SWOT ANALÝZA	44
7.1	POSTUP PRÁCE SE SWOT ANALÝZOU	44
7.2	KONKRÉTNÍ SWOT ANALÝZA SPOLEČNOSTI BLASTEX S.R.O.	45
7.3	VYHODNOCENÍ SWOT ANALÝZY	47
8	ETA ANALÝZY SPOLEČNOSTI BLASTEX S.R.O.	48
8.1	ETA – NEOPRÁVNĚNÉ VNIKNUTÍ	49
8.2	ETA – VZNIK POŽÁRU	50
8.3	POROVNÁNÍ VÝSLEDKŮ OBOU ETA ANALÝZ	51
9	NÁVRH ZLEPŠENÍ BEZPEČNOSTNÍHO SYSTÉMU OBJLEKU BLASTEX S.R.O.	52
	ZÁVĚR.....	53
	SEZNAM POUŽITÉ LITERATURY	55
	SEZNAM OBRÁZKŮ	59
	SEZNAM TABULEK.....	60
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	61

ÚVOD

Zvyšující se potřeba efektivní ochrany podniků a jejich majetku před různými hrozbami, jako jsou krádeže, vandalismus, poškození nebo terorismus, je v současnosti stále více pocíťována. Ochrana objektů je proto pojímána jako komplexní proces, v jehož rámci jsou uplatňována technická opatření (např. PZTS, MZS, DVS), ale také opatření organizační a fyzická. Tento požadavek je vyvoláván rostoucí kriminalitou a omezenými kapacitami policie při řešení těchto událostí. Klíčovou rolí před zavedením ochranných opatření sehraje důkladná analýza rizik, na jejímž základě je vytvářena efektivní bezpečnostní strategie.

Analýza rizik je chápána jako systematický proces, v němž jsou potenciální hrozby identifikovány, hodnoceny a řízeny. Jejím cílem je minimalizovat pravděpodobnost vzniku rizik a omezit jejich dopad na činnost organizace. V rámci tohoto procesu je často využíváno softwarových nástrojů, které napomáhají zpřesnění a zefektivnění analýzy. Jeden z těchto nástrojů je představován v teoretické části práce.

V podnicích je bezpečnost řízena ředitelem společnosti ve spolupráci s klíčovými vedoucími pracovníky. Rizikové faktory jsou jimi identifikovány a vyhodnocovány a následně jsou navrhována odpovídající opatření. Tato opatření jsou rozdělována do několika hlavních kategorií:

- **Technická opatření:** jsou uplatňovány systémy elektronického zabezpečení (např. pohybové a požární detektory), mechanické zábrany (např. ploty, závory, dveře) a kamerové systémy.
- **Režimová opatření:** jsou nastavovány v podobě pravidel a postupů, jejichž cílem je minimalizace rizik, např. omezením přístupu do citlivých prostor, kontrolou vjezdu vozidel nebo evidencí návštěvníků.
- **Fyzická ochrana:** je zajišťována formou stálé nebo doplňkové ostrahy, přičemž jsou monitorovány pohyby osob, kontrolován přístup a chráněna bezpečnost zaměstnanců i majetku.

Fyzická ochrana je považována za nedílnou součást bezpečnostního systému, avšak její rozsah je omezován legislativou. Pracovníkům bezpečnostních agentur nejsou přiznávány rozšířené pravomoci jako policii; jejich kompetence jsou určovány vnitřními předpisy podniku. Například vyžádání dokladu totožnosti je umožněno pouze v rámci interních

pravidel, zatímco policie tak může činit na základě zákona. Při výběru bezpečnostní agentury je přihlíženo ke kvalitě poskytovaných služeb, která je posuzována dle referencí a pověsti na trhu. Nedostatečná regulace v tomto odvětví vede k výrazným rozdílům v úrovni služeb. Od roku 1989 je bezpečnostní průmysl dynamicky rozvíjen, zejména s příchodem moderních technologií. Pokročilé kamerové systémy umožňují identifikaci osob i na velké vzdálenosti a za zhoršených světelných podmínek. Tyto a další trendy jsou v práci analyzovány za účelem poskytnutí přehledu o aktuálních možnostech v oblasti ochrany podniků a jejich majetku.

I. TEORETICKÁ ČÁST

1 FYZICKÁ BEZPEČNOST

Fyzická bezpečnost zahrnuje opatření zaměřená na ochranu budov, místností, zařízení, vybavení a další infrastruktury před neoprávněným přístupem, krádeží, vandalismem, zničením nebo jiným poškozením. Bezpečnostní opatření zabraňují neoprávněnému vniknutí a chrání majetek i osoby před možnými hrozbami.

Fyzická bezpečnost hraje klíčovou roli při zajištění kontrolovaného přístupu do prostor organizace. Zabraňuje tomu, aby se neoprávněné osoby dostaly na místa, kam nemají přístupová práva. Zahrnuje implementaci různých ochranných prvků, jakými jsou vstupní systémy, závory, elektronická zabezpečení, dveře, zámky nebo klíče, které přispívají k ochraně majetku a zajištění bezpečnosti provozu. [1][2]

1.1 Mechanické zábranné systémy

Mechanické zábranné systémy (MZS) jsou souborem mechanických prvků navržených k zamezení neoprávněného přístupu do chráněných prostor nebo objektů. Jejich hlavním úkolem je vytvořit fyzickou překážku, která odradí nebo zpomalí potenciálního pachatele při pokusu o násilné vniknutí. Mezi tyto prostředky patří například zdi, ploty, bezpečnostní dveře, mříže, turnikety či bezpečnostní skla. Jejich účinnost spočívá v mechanické odolnosti, která zvyšuje čas potřebný k jejich překonání, čímž se zvyšuje pravděpodobnost odhalení pachatele nebo jeho odrazení od činu.

Kvalitu mechanického zábranného systému určuje zejména doba, kterou zloděj nebo jiný narušitel potřebuje k překonání ochrany objektu. Tento časový interval lze vyjádřit vztahem:

$$\Delta t = t_1 - t_2$$

Kde: Δt

t_1 je čas zahájení útoku na objekt,

t_2 je čas dokončení útoku.

Vyšší hodnota Δt indikuje účinnější a kvalitnější zabezpečení.

Druhy mechanických zábranných systémů lze rozdělit podle jejich umístění a funkce. Mezi vnější mechanické systémy patří zejména oplocení, bariéry, zdi, brány a závory, které slouží k fyzickému vymezení chráněného prostoru a zamezení neoprávněnému přístupu. Z hlediska stavebních prvků je důležité zabezpečení konstrukcí, jako jsou hradby, stropy,

podlahy a střešní systémy, jejichž odolnost přispívá k celkové stabilitě objektu. Ochrana otvorových výplní zahrnuje především dveře, okna a v některých případech také balkony, které musí být opatřeny vhodným zajištěním proti násilnému vniknutí. Samostatnou skupinu tvoří zabezpečení úschovných objektů, kam řadíme trezory, úschovné skříně a specializované sejfy určené například pro uložení zbraní nebo citlivých materiálů. [3][4]

1.1.1 Obvodová ochrana

Obvodová ochrana definuje hranici pozemku náležejícího k budově, čímž vytváří právně vymezený prostor. K tomuto účelu se používají oplocení, brány, branky nebo závory.

Typy obvodové ochrany:

Klasické drátěné oplocení – Výška cca 1,5 m, vyrobeno z železného drátu o průměru 2,5 mm. Používá se u méně významných objektů.

Bezpečnostní oplocení – Výška 1–2,5 m, pevnější materiály (ocel, beton), vhodné pro školy, sklady či průmyslové objekty.

Vysokobezpečnostní oplocení – Výška až 5 m, kombinace s bariérami (např. ostnatý drát). Používá se pro vojenské a průmyslové objekty či elektrárny.

Vrcholové zábrany – Ostnaté dráty, žiletkové bariéry nebo otočné hroty, zvyšují ochranu oplocení.

Podhrabové překážky – Ocelové rošty, betonové desky nebo pevné zdi zabráňující podkopání oplocení.

Vstupy a vjezdy: Brány, branky, závory tvoří přechod mezi volně přístupným a chráněným prostorem.

Obvodová ochrana pro průmyslové podniky, vyjma provozů s výbušninami, nemá legislativně definované požadavky týkající se parametrů, jakými je typ, výška, použitý materiál. [3]

1.1.2 Plášťová ochrana

Plášťová ochrana slouží k zabránění neoprávněného vstupu do objektu. Jejím cílem je nejen narušitele fyzicky zastavit, ale také ho odradit a usměrnit jeho pohyb tak, aby bylo možné včas reagovat.

Mezi základní prvky plášťové ochrany patří stavební konstrukce, jako jsou zdi, stropy, podlahy a střešní systémy, a dále výplňové prvky otvorů – především dveře, okna, průmyslová vrata, rolety, mříže a bezpečnostní fólie. Tyto prvky by měly být navrženy s ohledem na odolnost vůči násilnému vniknutí, případně doplněny o mechanické nebo elektronické zabezpečení.

Z hlediska bezpečnostní praxe bývají nejrizikovějšími místy vstupní a servisní otvory, které jsou často zneužívány pro neoprávněné vniknutí. Dveře jsou zmiňovány ve více než 90 % případů vloupání, přičemž pachatelé často překonávají běžné uzamykací systémy. Významnou zranitelností bývají také okna a technické vstupy, které mohou být snadno dosažitelné. Pro zvýšení bezpečnosti se doporučuje doplnit tyto prvky o certifikované bezpečnostní zámky, mříže, vrstvené zasklení či externí stínící prvky.

Celková úroveň plášťové ochrany výrazně ovlivňuje odolnost objektu vůči vnějšímu napadení a její správné navržení tvoří základní vrstvu ochranného systému fyzické bezpečnosti. [5]

1.2 Poplachové zabezpečovací a tísňové systémy

Poplachové zabezpečovací a tísňové systémy (PZTS) představují komplexní soustavu technologií, která zahrnuje čidla, kamery, detektory pohybu, ústředny, ovládací zařízení, hlásiče a poplachovou signalizaci. Tyto systémy slouží k detekci narušení střeženého prostoru či objektu a upozorňují na něj prostřednictvím optických nebo akustických signálů podle požadavků stanovených normou ČSN EN 50131.

PZTS jsou v současnosti široce využívány díky své schopnosti aktivní ochrany, která přesahuje možnosti mechanického zabezpečení (např. zámky nebo závory). Zatímco mechanické zábrany pouze znesnadňují přístup narušitelům, PZTS po detekci vniknutí okamžitě spustí poplach a odesílají upozornění na předem nastavené telefonní číslo nebo na DPPC – dohledové a poplachové přijímací centrum. [6]

1.2.1 Dohledové videosystémy (DVS)

Dohledové videosystémy (DVS), dříve označované jako kamerové systémy, patří mezi nejčastěji používané prostředky pro monitorování a kontrolu zabezpečených prostor. Slouží k nepřetržitému sledování pohybu osob, vozidel nebo událostí v místech, kde je potřeba zajistit vizuální dohled, a zároveň k uchování záznamu pro případné zpětné vyhodnocení. Využívají se v průmyslových areálech, obchodních centrech, kancelářských budovách,

školách, garážích i v soukromých objektech, a představují důležitý nástroj prevence i důkazní podpory v případě incidentu.

Systémy DVS lze nasadit jak ve vnitřních, tak venkovních prostorách. Podle prostředí a účelu se volí vhodné technické provedení – kamery mohou být pevné i otočné, s různým rozlišením obrazu, nočním režimem a možností zvětšení. Jejich funkce a cena se liší v závislosti na požadovaném rozsahu sledování, kvalitě obrazu nebo doplňkových funkcích. Některé systémy umožňují rozpoznání pohybu nebo automatické upozornění při narušení vymezené zóny.

DVS jsou důležitou součástí celkového systému fyzické ochrany, protože nejen odrazují pachatele od úmyslného jednání, ale také usnadňují zpětné dohledání skutečností po události. Jejich výhodou je možnost propojení s dalšími systémy – například s přístupovým nebo zabezpečovacím zařízením, čímž lze zvýšit efektivitu a rychlost reakce na bezpečnostní hrozbu. Kamery lze ovládat ručně nebo nastavit do automatického režimu, přičemž v moderních instalacích je běžné i vzdálené ovládání prostřednictvím telefonu nebo počítače.

Jejich charakteristika a požadavky jsou definovány v normě **ČSN EN 62 676**, která upravuje základní technické požadavky na dohledové videosystémy z hlediska provozních, kvalitativních i bezpečnostních parametrů. [7]

Rozdělení podle technologie (dle ČSN EN 62 676)

Digitální dohledové videosystémy (IP kamery) jsou moderní technologie s vysokým rozlišením (v řádu megapixelů), možností síťové komunikace, inteligentní analýzy obrazu a snadného přístupu k záznamu. Využívají se zejména v moderních bezpečnostních aplikacích a vyžadují vyšší investice.

Analogové dohledové videosystémy jsou starší technologie s nižším rozlišením (obvykle 600–1000 TV řádků), vhodné pro méně náročný monitoring. Nižší pořizovací náklady, ale omezené možnosti integrace s digitálními prvky.

Hybridní videosystémy kombinují prvky analogových a digitálních videosystémů (např. HD-SDI, HD-CVI), často využívané při rekonstrukci starších systémů, kde je zachováno původní kabelové vedení.

Autonomní videosystémy jsou jednoduchá zařízení vhodná pro malé prostory, umožňují snadnou instalaci, často s možností online přístupu k záznamům. Využívají se například v domácnostech. [8]

Instalace a použití

DVS jsou využívány ve veřejných i neveřejných prostorech – např. v obchodech, kancelářích, výrobních halách, domech i bytových jednotkách. Instalace kamerového systému vyžaduje odborné znalosti, a pro zajištění jeho správné funkce a spolehlivosti je vhodné svěřit montáž a servis certifikovaným odborníkům.

PZTS jsou zařízení, které slouží k identifikaci a upozornění na narušení chráněného prostoru nebo přítomnost rizika, jako je neoprávněný vstup, požár nebo únik plynu. Prostřednictvím akustických, vizuálních či elektronických signálů varuje uživatele nebo příslušné bezpečnostní složky. PZTS jsou využívány k ochraně osob, majetku a budov v rezidenčních, komerčních a průmyslových prostorách. [7]

Funkce PZTS

Funkce elektronických zabezpečovacích systémů lze rozdělit do několika logických kroků, které společně tvoří ucelený bezpečnostní řetězec. Prvním z nich je detekce, při které senzory a detektory zjišťují výskyt určitého jevu – nejčastěji pohybu, otevření dveří, rozbití skla, zvýšení teploty, přítomnosti kouře nebo úniku plynu. V závislosti na konkrétním prostředí a typu chráněného prostoru se používají různé typy čidel, jako jsou pasivní infračervené detektory, mikrovlnné senzory nebo kombinované jednotky s více typy detekce.

Následuje fáze signalizace, kdy systém po vyhodnocení poplachu spustí varovný signál. Ten může mít různou podobu – od klasické akustické sirény přes blikající světla až po automatické odeslání upozornění na mobilní zařízení správce objektu. V moderních systémech je možné navázat signalizaci i na chytré aplikace, které umožní uživateli vzdáleně ověřit situaci prostřednictvím kamery nebo okamžitě kontaktovat zásahovou jednotku.

Tato výstražná signalizace často plní zároveň funkci psychologického odstrašení. Zjevné a hlasité varování narušitele často demotivuje od dalšího postupu a zvyšuje šanci, že pachatel opustí prostor dříve, než dojde k větší škodě. Právě tento moment je z hlediska fyzické bezpečnosti klíčový, protože přerušení činnosti pachatele v rané fázi může zabránit samotnému dokonání činu.

Poslední a neméně důležitou fází je reakce na incident. Cílem této fáze je zajistit rychlý a cílený zásah, a to buď prostřednictvím bezpečnostní agentury, přímo majitelem objektu, nebo ve spolupráci s integrovaným záchranným systémem v případě potvrzeného incidentu. V dobře nastaveném systému probíhá reakce automaticky, bez nutnosti manuálního potvrzení – např. přivoláním zásahové jednotky, uzamčením přístupových bodů nebo aktivací dalších bezpečnostních prvků. Rychlost reakce přitom přímo ovlivňuje míru škod a pravděpodobnost zadržení pachatele.[7]

Typy alarmů

Zabezpečovací systémy lze rozdělit podle několika kritérií v závislosti na jejich účelu, umístění, způsobu aktivace a typu přenosu signálu. Podle účelu se rozlišují zabezpečovací alarmy, které slouží k ochraně před neoprávněným vstupem do objektu, požární detektory, které upozorňují na přítomnost kouře nebo zvýšenou teplotu, plynové detektory určené k včasnému zjištění nebezpečných plynů (například oxidu uhelnatého) a tísňové systémy, jež umožňují přivolat pomoc v krizových situacích. Z hlediska umístění se systémy dělí na interiérové, které chrání vnitřní prostory budov, a exteriérové, zaměřené na zabezpečení vnějších částí objektu, jako jsou zahrady nebo oplocení. Dle způsobu aktivace rozlišujeme manuální systémy, které spouští uživatel pomocí tlačítka nebo klíče, a automatické systémy, jež reagují na podnět z detektorů, například při zaznamenání pohybu. Posledním kritériem je způsob přenosu signálu – drátové systémy mají jednotlivé komponenty propojené kabely, zatímco bezdrátové využívají rádiové přenosy, Wi-Fi nebo technologii Bluetooth. [9]

1.2.2 Detektory pohybu

Snímač pohybu je zařízení, které detekuje pohyb objektů, nejčastěji osob. Bývá součástí větších systémů, jako jsou bezpečnostní systémy, řízení domácností, automatizace osvětlení nebo úspora energie. Jeho hlavním úkolem je zaznamenat narušení chráněného prostoru a odeslat upozornění ústředně nebo monitorovacímu centru. Čidla pohybu se využívají například v kancelářích, bankách, nákupních centrech nebo domácnostech.

Detektory pohybu nacházejí využití nejen v oblasti zabezpečení, ale také při zvyšování komfortu a efektivity provozu. Mohou například sloužit k automatické aktivaci zvonku při přiblížení osoby ke vchodovým dveřím, čímž zajišťují bezdotykové oznámení návštěvy. Dále mohou upozornit uživatele v případě, že děti vstoupí do zakázaných nebo rizikových prostor, jako je například lékárnička, technická místnost nebo sklep. Významným přínosem

je také úspora energie díky funkci automatického vypínání osvětlení v místnostech, kde není detekován pohyb, což přispívá ke snížení provozních nákladů.

Typy snímačů pohybu:

Pasivní infračervený detektor (PIR) detekuje infračervené záření vyzařované teplokrevnými organismy. Pyroelement (polovodičový senzor - z lithia, tantalu) měří tepelné změny. Jakmile člověk projde střeženým prostorem, změní se množství IR záření, které dopadá na pyroelement. Dojde k polarizaci náboje a vznikne napěťový signál, který je elektronicky zesílen a vyhodnocen. PIR detektory jsou energeticky úsporné a využívají se především v interiérových alarmech nebo k ovládání osvětlení.

Ultrazvukový detektor může být aktivní (vysílají a přijímají ultrazvukové vlny) nebo pasivní (sledují specifické zvuky, jako je tříštění skla). Aktivní detektory měří odraz zvukových vln od pohybujících se objektů. Jsou velmi citlivé, ale dražší a náchylné k falešným poplachům. Zvířata, jako psi nebo kočky, mohou tyto vlny slyšet, což je může vyrušovat.

Mikrovlnný detektor generuje mikrovlnné impulzy a sleduje jejich odraz, aby zjistil pohyb. Tyto detektory jsou citlivé, ale mohou zachytit pohyb i mimo cílený rozsah. Spotřebovávají více energie, a proto bývají navrženy tak, aby pracovaly v cyklech zapnutí a vypnutí.

Tomografický detektor používá rádiové vlny, které detekují narušení při průchodu objektem. Tento typ je schopen „vidět“ skrze zdi a často pokrývá velké plochy. Kvůli vysoké ceně se využívá zejména v komerčních bezpečnostních systémech.

Kombinované detektory kombinují více technologií, například PIR a mikrovlnné detektory, což snižuje falešné poplachy. Tyto detektory se aktivují pouze tehdy, když obě technologie detekují pohyb, což zvyšuje přesnost.[9][10]

Principy fungování a využití

Většina čidel pohybu pracuje na základě detekce změn frekvencí, infračerveného záření nebo narušení rádiových vln. Hlavní funkcí je zaznamenat pohyb, upozornit na něj a v případě potřeby spustit poplach. Používají se pro bezpečnostní účely v domácnostech, komerčních prostorách nebo veřejných místech a mohou zabránit vážným nehodám nebo narušení bezpečnosti.

Díky kombinaci různých technologií jsou moderní snímače pohybu efektivnější, spolehlivější a nacházejí široké uplatnění v různých typech prostředí. [9]

1.2.3 Přístupové systémy

Přístupové systémy (ESKV) jsou důležitou součástí technického zabezpečení objektů. Často doplňují další bezpečnostní prvky, jako jsou kamerové systémy (DVS), elektronické zabezpečovací systémy (PZTS) nebo elektronická požární signalizace (EPS). Používají se v průmyslových objektech, administrativních budovách, zdravotnických zařízeních, na úřadech, v ubytovacích či bytových prostorách a všude tam, kde je kladen důraz na vysokou míru zabezpečení. Přístupové systémy fungují na principu přidělování přístupových práv, která lze přizpůsobit konkrétním požadavkům:

- Prostorová oprávnění: určují přístup do konkrétních míst.
- Časová oprávnění: omezují přístup na určitá časová období.
- Personální oprávnění: umožňují nastavit specifická pravidla pro jednotlivé osoby.

Systémy mohou být jednoduché, zaměřené pouze na snímání vstupů bez archivace dat, nebo komplexní on-line systémy s centrální evidencí záznamů, analýzou pohybu osob, sledováním zón či propojením s dalšími bezpečnostními systémy.

Aby přístupové systémy splnily svůj účel, musí být zajištěna identifikace osob prostřednictvím identifikátorů, které lze rozdělit do tří skupin:

- Informace, kterou osoba zná: hesla nebo PIN kódy.
- Identifikační předmět: přístupové karty, čipové karty, čárové kódy.
- Biometrické charakteristiky: otisk prstu, rozpoznání obličeje, geometrie ruky, sken oční duhovky apod.

Proces identifikace zahrnuje čtení dat ze zvoleného média, jejich zpracování v řídicí jednotce a následnou aktivaci ovládacího zařízení, například turniketů, dveřních zámků nebo závor.

Identifikační systémy lze rozdělit do dvou hlavních kategorií – na systémy využívající identifikační média a na systémy biometrické. První skupina zahrnuje optické systémy, které pracují s čárovými kódy snímanými čtečkou, magnetické systémy s kartami vybavenými magnetickým proužkem, dále kontaktní systémy, kde je karta nebo předmět mechanicky připojen ke čtečce, a bezkontaktní systémy, které využívají přenos dat prostřednictvím

radiofrekvenční technologie (např. RFID). Druhou skupinu tvoří biometrické identifikační systémy, které se zaměřují na jedinečné charakteristiky jednotlivce a patří mezi nejspolehlivější metody ověření identity. Mezi běžné typy patří otisk prstu, využívající unikátní papilární linie, a geometrie ruky, analyzující tvar dlaně. Dále lze využít rozpoznání obličeje, které hodnotí pozici očí, nosu a úst, nebo hlasovou identifikaci, která kontroluje identitu na základě zvukové analýzy hlasu. Některé systémy zohledňují také dynamiku podpisu, tedy tlak, směr a rychlost pohybu při psaní, nebo strukturu žil na ruce, kde jedinečná síť krevního řečiště zajišťuje vysokou úroveň ochrany. Mezi méně běžné metody pak patří pachová identifikace, která využívá specifický tělesný pach například při kombinaci se speciálním oděvem, a papilární linie na dlani, které stejně jako otisky prstů slouží k přesnému ověření totožnosti. Přístupové systémy je tak možné přizpůsobit konkrétním podmínkám prostředí, přičemž biometrické varianty vykazují vysokou spolehlivost a odolnost vůči zneužití. [11][12]

1.3 Režimová opatření

Režimová opatření představují soubor pravidel a vnitřních předpisů, jejichž cílem je omezit pohyb osob v chráněných částech objektu a zajistit kontrolu nad tím, kdo, kdy a kam vstupuje. Tato opatření jsou důležitým prvkem fyzické bezpečnosti a tvoří doplňkovou vrstvu k technickému a organizačnímu zabezpečení. V praxi jsou režimová opatření realizována zejména prostřednictvím systému oprávnění k přístupu, evidence vstupů a výstupů, nastavení časových omezení a povinností identifikace. Správně nastavený režim umožňuje minimalizovat rizika neoprávněného pohybu osob, interních hrozeb a neopatrné manipulace v rizikových zónách objektu.

V následující podkapitole jsou popsána konkrétní opatření v oblasti školení, řízení přístupu a vnitřní bezpečnostní kázně, která přispívají k celkovému zvýšení bezpečnostní úrovně střeženého prostoru.

1.3.1 Areálové omezení přístupu

Součástí režimových opatření je školení zaměstnanců fyzické ostrahy a dalších pracovníků, kteří se pohybují v chráněném prostoru. Zaměstnanci fyzické ostrahy musí projít odborným školením, které je zaměřeno na jejich specifické úkoly. Školení zahrnuje seznámení s charakteristikami střeženého objektu, s technologií zabezpečení (např. EPS), bezpečnostními směrnici a pravidly vstupu. Dále jsou proškoleni v oblasti požární

ochrany (PO), bezpečnosti práce (BOZP), poskytování první pomoci, zvládání krizových situací a orientace v prostoru objektu. Tato školení je nutné pravidelně opakovat, aby si zaměstnanci udržovali potřebnou odbornou úroveň. Nedílnou součástí režimu je také pravidelná kontrola výkonu, kterou provádí zaměstnavatel s cílem zhodnotit činnost ostrahy. Pro výkon činnosti je navíc nezbytné příslušné profesní osvědčení, například kvalifikace „Strážný“.

Bezpečnostní školení se však netýká pouze pracovníků ostrahy, ale všech zaměstnanců, kteří se pohybují v chráněném prostoru. Všichni musí být pravidelně školeni v oblasti BOZP a PO. Školení se dělí na vstupní, které je zaměřeno na seznámení se s pracovním prostředím, bezpečnostními pravidly a možnými riziky, na pravidelná školení, která slouží k aktualizaci znalostí a opakování stanovených bezpečnostních postupů, a na školení specifická, přizpůsobená konkrétním rizikům a pracovním činnostem, jako je např. manipulace s nebezpečnými látkami, práce ve výškách nebo obsluha technologií. Zajištění bezpečnostního školení všech zaměstnanců je důležitým nástrojem prevence pracovních úrazů, zvyšování bezpečnosti a ochrany zdraví osob pohybujících se v areálu.

1.3.2 Kontrola vstupu a výstupu

Přístupový systém představuje soubor opatření, která slouží k řízení a evidenci přístupu do vymezených prostor na základě přesné identifikace osob. Tyto systémy, dnes převážně elektronické, mají za úkol kontrolovat vstupy, zabránit neoprávněným osobám v přístupu do chráněných prostor a sledovat pohyb oprávněných osob v definovaných zónách. Princip fungování přístupových systémů spočívá ve čtení zakódovaných údajů pomocí čteček, jejich vyhodnocení a následném rozhodnutí o povolení či zamítnutí přístupu.

Přístupové systémy slouží k řízení a kontrole vstupu osob do vymezených prostorů a tvoří důležitou součást technicko-organizačního zabezpečení objektu. Podle normy ČSN EN 50133-1 (čl. 3.2) se za přístupový systém (ESKV) považuje systém zahrnující technická a organizační opatření určená pro řízení vstupů. Pokud je tento systém rozšířen o elektronické prostředky, hovoříme o elektronickém přístupovém systému (EACS – Electronic Access Control System), který umožňuje automatizované řízení vstupu oprávněným osobám a zároveň zamezuje přístup osobám neoprávněným. Specifikace těchto systémů je dále uvedena v technické normě ČSN CLC/TS 50398.

Přístupové systémy se přizpůsobují úrovni rizika a jsou navrženy na základě požadavků konkrétního prostoru. Klíčovým faktorem je přidělení přístupových práv, která se nastavují na základě:

- Prostorových dispozic: přístup do konkrétních míst.
- Časových omezení: vstup pouze v určených časových intervalech.
- Personálních oprávnění: rozlišení přístupových práv podle uživatele.

Identifikace osob probíhá pomocí různých technologií, od klávesnicového vstupu a karet až po biometrické systémy, které využívají hlas, otisky prstů, dlaně, obraz oční duhovky nebo obličeje. [13]

Propojení přístupových a poplachových systémů

Přístupový systém tvoří často jádro zabezpečení objektu a je úzce propojen s mechanickými zábranami, jako jsou dveře nebo závory. Tyto systémy lze považovat za inteligentnější elektronickou alternativu klasických klíčů. Na rozdíl od ostatních poplachových systémů, které slouží primárně k signalizaci a vyžadují lidskou reakci, přístupový systém zajišťuje přímou fyzickou ochranu přístupu k chráněným aktivům.

V moderním pojetí je přístupový systém považován za nezbytný technický prostředek fyzické ochrany, který kombinuje bezpečnost, efektivitu a snadnou správu přístupových práv. [13]

1.3.3 Časové omezení přístupu

Časové omezení přístupu představuje jednu z klíčových funkcí moderních přístupových systémů (ESKV), která umožňuje přesně definovat, v jakých časových intervalech mohou jednotliví uživatelé vstupovat do konkrétních prostor. Tato funkce umožňuje rozlišit přístupová práva nejen podle osoby, ale i podle času – například lze nastavit, že zaměstnanci mohou vstupovat pouze během své pracovní směny, zatímco dodavatelé či návštěvy pouze v přesně stanovených časových oknech.

Díky časovému omezení lze efektivně zamezit neoprávněným vstupům mimo provozní dobu, omezit pohyb osob v rizikových částech objektu v noci nebo o víkendech a snížit tak riziko zneužití přístupových práv. V praxi se tato funkce často využívá také v kombinaci s kalendáři svátků, střídavými směnami nebo pro přístup v mimořádných situacích (např. servisní zásahy). Správně nastavené časové profily tak významně přispívají k optimalizaci bezpečnostních procesů a minimalizaci lidských chyb.

Nastavení a implementace časového omezení

Moderní přístupové systémy umožňují velmi přesné přiřazení časových omezení jak jednotlivcům, tak celým skupinám uživatelů. Každému držiteli přístupového oprávnění lze definovat konkrétní časové zóny, v nichž je vstup povolen. Například běžní zaměstnanci mohou mít vstup umožněn pouze během standardní pracovní doby, zatímco úklidový nebo technický personál má přístup ve večerních hodinách, mimo hlavní provoz. Pro externí firmy či návštěvy lze nastavit pouze krátkodobá časová okna s omezenou platností.

Pokročilejší systémy navíc umožňují propojení časových oprávnění s organizačním kalendářem – tím je možné přístupová práva automaticky upravit v závislosti na svátcích, dovolených, víkendech nebo jiných mimořádných režimech. Systém tak dynamicky reaguje na provozní plánování, čímž se minimalizuje riziko lidské chyby a zneužití přístupových práv.

Součástí správného nastavení časových omezení by měla být i aktivace bezpečnostních logik, jako je například funkce Anti-Passback. Ta brání opakovanému použití stejné přístupové identifikace ve stejném směru (např. opakovaný vstup bez předchozího výstupu) v krátkém časovém intervalu. Tím se snižuje riziko neoprávněného sdílení přístupových karet nebo kódů mezi osobami. V praxi tak tato funkce zvyšuje dohled nad skutečným pohybem osob v objektu a zajišťuje konzistentní evidenci průchodů v čase i prostoru.

[13]

Výhody časového omezení přístupu

Zavedení časového omezení přístupu přináší celou řadu výhod, které výrazně zvyšují úroveň zabezpečení objektu. Především umožňuje omezit vstup do vyhrazených prostor pouze na přesně stanovené časové úseky, čímž se minimalizuje riziko neoprávněného pohybu mimo pracovní dobu nebo mimo režimově povolené intervaly. Tím lze účinně zabránit situacím, kdy by například zaměstnanec zneužil přístupové oprávnění v době, kdy se v objektu nikdo nenachází, nebo kdy by externí osoba měla volný přístup v nevhodnou dobu.

Časové zóny lze velmi flexibilně přizpůsobit konkrétním potřebám různých skupin uživatelů – zaměstnancům lze přiřadit přístup v rámci jejich směny, úklidovým nebo technickým službám pouze v mimoprovozních časech a návštěvám pouze po dobu předem definované návštěvy. To vede k lepší organizaci provozu a přehlednějšímu řízení přístupových práv. Výhodou je také snadná aktualizace těchto nastavení, a to buď ručně, nebo automaticky v návaznosti na kalendář, plán směn či typ uživatele.

Další zásadní výhodou je možnost detailního monitorování vstupů a výstupů – systém zaznamenává přesné časy a místa průchodů jednotlivých osob. Tyto údaje lze následně využít při interních auditech, vyšetřování incidentů nebo zpětné analýze narušení bezpečnosti. Přístupový systém s časovými omezeními tak neslouží jen jako prostředek kontroly, ale také jako důležitý nástroj pro vyhodnocování bezpečnostních událostí a optimalizaci provozního režimu.

V neposlední řadě představuje časové omezení významný nástroj pro eliminaci lidské chyby. Předdefinovaná oprávnění brání například tomu, aby pracovník omylem vstoupil do prostoru, kde v daný čas nemá být, nebo aby se přístupová práva zapomněla zneplatnit při změně režimu. Při správném nastavení tak časové omezení zvyšuje bezpečnost, snižuje administrativní zátěž a přispívá ke spolehlivému fungování přístupového systému jako celku.[13]

2 CHARAKTERISTIKA RIZIKA

Riziko je základním pojmem v oblasti bezpečnosti a krizového řízení a jeho správné pochopení je klíčové pro tvorbu účinných preventivních a ochranných opatření. V kontextu fyzické bezpečnosti se riziko vztahuje zejména na hrozby, které mohou narušit integritu, funkčnost nebo bezpečný provoz objektu. Charakteristika rizika tedy slouží k systematickému určení toho, co konkrétně může nastat, jak často, s jakým dopadem a jak lze dané situaci předejít nebo na ni reagovat.

Riziko je vždy spojeno s určitou mírou nejistoty a variabilitou – ať už jde o působení lidského faktoru, selhání technických prostředků, nepříznivé vnější vlivy nebo kombinaci více faktorů. Jeho hodnocení představuje proces, při kterém se zvažuje jak pravděpodobnost výskytu události, tak závažnost jejích dopadů. Tyto dvě složky jsou často doplněny i dalšími parametry, například mírou expozice, citlivostí chráněného objektu nebo schopností detekce a reakce.

Charakteristika rizika dále vyžaduje přesné určení, jaké následky mohou z události vyplynout – například ohrožení života, ztráty na majetku, narušení provozu, ekologické nebo společenské dopady. V tomto kontextu se riziko stává hodnotitelnou veličinou, která umožňuje nastavit priority a určit vhodná opatření na jeho eliminaci či zmírnění. Znalost povahy rizik je tak nezbytným předpokladem pro plánování, rozhodování i správu fyzické bezpečnosti.

2.1 Definice rizika

V širším smyslu lze riziko chápat jako vztah mezi očekávanou ztrátou (např. újmou na zdraví, ohrožením života nebo poškozením majetku) a nejistotou, která se této ztráty týká. Riziko se obvykle vyjadřuje pravděpodobností nebo četností výskytu, přičemž jeho posouzení závisí také na míře expozice – tedy na tom, do jaké míry může být sledovaný objekt nebo osoba danému vlivu vystavena.

Důležité je zdůraznit, že riziko nelze nikdy zcela eliminovat. I při maximální snaze o jeho minimalizaci nelze vyloučit všechny možnosti selhání nebo nepředvídatelných vlivů. Jediná situace, kdy je riziko skutečně nulové, nastává tehdy, pokud je expozice zcela vyloučena – např. když k danému jevu objektivně nemůže dojít.

V rámci prevence a hodnocení rizik je dále důležité chápat některé specifické pojmy, které se vztahují k rozsáhlým nebo řetězovým mimořádným událostem. Mezi ně patří

například scénář havárie, což je předpokládaný nebo modelovaný průběh havarijní události, který zahrnuje posloupnost jednotlivých kroků, systémových selhání nebo lidských chyb vedoucích k jejímu vzniku a rozvoji. Využívá se především při plánování reakce na mimořádné situace nebo při tvorbě havarijních plánů.

Dalším důležitým pojmem je tzv. domino efekt, který označuje situaci, kdy jedna havárie vyvolá sekundární havárie v sousedních nebo navazujících částech systému. Typicky jde o exploze, požáry nebo úniky nebezpečných látek, jejichž účinky způsobí poškození dalších technologií nebo zásah dalších provozních celků. Tento jev je obzvlášť významný v areálech s koncentrací nebezpečných látek a je přímo řešen v evropské i národní legislativě.

[14][15]

3 ANALÝZA RIZIK

Analýza rizik je základním nástrojem pro systematické posouzení bezpečnostní situace, a to jak ve fázi návrhu, tak při provozním řízení fyzické ochrany. Jejím hlavním cílem je identifikovat možné hrozby, stanovit jejich závažnost a pravděpodobnost výskytu a následně na jejich základě navrhnout účinná a přiměřená ochranná opatření. Tato metoda není omezena pouze na reakci na již známá rizika, ale umožňuje aktivně vyhledávat slabá místa v systému a předcházet vzniku krizových situací ještě před jejich realizací.

Proces analýzy rizik přináší logickou strukturu pro rozhodování o prioritách v oblasti zabezpečení. Umožňuje porovnávat různé typy rizik mezi sebou a efektivně alokovat zdroje tam, kde je to nejvíce potřeba. V oblasti fyzické bezpečnosti tak představuje nedílnou součást návrhu i optimalizace bezpečnostních opatření – od technických systémů až po organizační a režimová pravidla.

Důležitým výstupem analýzy rizik je také schopnost zdokumentovat proces rozhodování o bezpečnostních investicích. V praxi je často vyžadována transparentní a opakovatelná metodika, kterou lze obhájit před vedením organizace, auditorem nebo kontrolním orgánem. Právě z tohoto důvodu jsou metody analýzy rizik nedílnou součástí nejen bezpečnostních studií, ale také požadavků v oblasti legislativy, certifikace nebo provozního plánování.

Analýza rizik se navíc stále častěji propojuje s dalšími nástroji hodnocení, jako je plánování kontinuity provozu, krizové řízení nebo řízení informační bezpečnosti. Díky tomu se stává univerzálním nástrojem, který nachází uplatnění nejen při ochraně fyzických aktiv, ale i při širším posuzování odolnosti organizace vůči různým typům narušení. Ve fyzické bezpečnosti pak umožňuje přesně zacílit ochranná opatření, vyhodnotit jejich přiměřenost a navrhnout efektivní zlepšení v návaznosti na aktuální hrozby i provozní podmínky.

3.1 Základní pojmy

V rámci této analýzy se pracuje s několika základními pojmy. Aktivum představuje jakoukoli hodnotu, kterou je třeba chránit – může jít například o informace, zařízení, osoby nebo provozní procesy. Hrozba je vnější nebo vnitřní faktor, který má potenciál ohrozit funkčnost, bezpečnost nebo stabilitu chráněného aktiva. Zranitelnost označuje slabé místo v systému, které může být hrozbou zneužito, a opatření představují konkrétní technické, organizační nebo personální kroky, jejichž cílem je tuto zranitelnost snížit nebo odstranit.

Analýza rizik tedy nevnímá hrozbu izolovaně, ale hodnotí její vztah ke zranitelnosti aktiva a výslednému dopadu. Riziko vzniká tehdy, když existuje hrozba, která může využít konkrétní slabinu systému. Účinným řízením rizik lze tuto pravděpodobnost a dopad významně omezit. [14][15]

3.2 Příklady analýz rizik

Pro správné řízení bezpečnosti je nezbytné znát nejen existující rizika, ale také způsob, jak je efektivně identifikovat, hodnotit a snižovat. K tomuto účelu se používají různé metody analýzy rizik, které se liší složitostí, účelem i oblastí použití. V oblasti fyzické bezpečnosti se uplatňuje několik základních analytických nástrojů, které pomáhají správně nastavit systém ochrany a reagovat na potenciální hrozby.

3.2.1 SWOT analýza

Metoda SWOT slouží k rychlé a přehledné orientaci v aktuální bezpečnostní situaci objektu. V rámci této metody jsou posuzovány **vnitřní faktory** – silné stránky (*Strengths*) a slabé stránky (*Weaknesses*) organizace, a zároveň **vnější faktory** – příležitosti (*Opportunities*) a hrozby (*Threats*). Výstupem je čtyřpólová matice, která umožňuje stanovit, na jaké oblasti se organizace může soustředit v rámci zlepšení ochranných opatření. [16]

Například silnou stránkou může být kvalitní kamerový systém, slabinou nedostatečně proškolený personál, hrozbou rostoucí kriminalita v okolí a příležitostí dotační program na bezpečnostní technologie. SWOT analýza se využívá zejména v úvodní fázi analýzy rizik, kdy je třeba získat celkový přehled o stavu zabezpečení a směřování dalšího rozvoje. [15]

3.2.2 Jednoduchá bodová analýza

Jednoduchá bodová metoda představuje nástroj pro kvantitativní hodnocení rizik. V této metodě se riziko počítá jako součin tří faktorů, a to pravděpodobnosti výskytu hrozby (P), závažnosti jejího dopadu (D) a schopnosti její detekce (Z). Výsledkem je celková míra rizika R.

$$R = P \times D \times Z$$

Každý faktor je ohodnocen na škále, například od 1 do 5, a výsledné číslo určuje vážnost rizika. Pokud je výsledek vyšší než stanovený práh, je nutné přijmout opatření. Metoda je vhodná pro rychlé srovnání více rizik a jejich seřazení podle priority. Je jednoduchá, srozumitelná a lze ji snadno přizpůsobit konkrétním potřebám podniku. [14]

3.2.3 Multikriteriální analýza rizik

Tato metoda umožňuje porovnat více variant řešení daného rizika na základě několika různých kritérií, jako jsou například náklady, technická náročnost, čas realizace nebo účinnost řešení. Každému kritériu je přiřazena váha dle jeho důležitosti a varianty jsou obodovány. Na základě součtu bodů je následně určena nejvhodnější varianta. Multikriteriální analýza se hodí v situacích, kdy má organizace k dispozici více možností řešení rizika a potřebuje se rozhodnout, která z nich bude optimální. Pomáhá také při tvorbě investičního plánu bezpečnostních opatření. [15]

3.2.4 ETA – Stromová analýza událostí

ETA (Event Tree Analysis) je grafická metoda, která zobrazuje možné scénáře vývoje událostí po určité iniciační události. Každá větev stromu představuje konkrétní rozhodnutí nebo výsledek – například zda určitý bezpečnostní systém zafungoval či selhal. Tato metoda pomáhá zjistit, jak velké riziko představuje určitý výchozí incident, a zároveň simuluje následky jeho různých průběhů. ETA se často používá v krizovém plánování, při analýze reakčních scénářů nebo při tvorbě plánů obnovy. V oblasti fyzické bezpečnosti může posloužit například při hodnocení účinnosti evakuačních cest nebo přístupových systémů v případě narušení objektu. [17]

4 ANALÝZA MOŽNOSTI NEOPRÁVNĚNÉHO VNIKUTÍ

Tato kapitola se zabývá souhrnným posouzením rizik spojených s neoprávněným vstupem do střeženého objektu. Sledují se faktory, které mohou ovlivnit pravděpodobnost vniknutí i možné následky takové události. Cílem je identifikovat slabá místa a navrhnout vhodná preventivní i reaktivní bezpečnostní opatření.

4.1 Předmět činnosti provozovatele

Charakter a předmět činnosti organizace patří mezi klíčové faktory, které ovlivňují míru bezpečnostních rizik a následně i nároky na úroveň fyzické ochrany objektu. Zatímco administrativní budovy bez přístupu k citlivým datům mohou vyžadovat spíše základní úroveň zabezpečení, provozy, které manipulují s vysoce rizikovými materiály, technologiemi nebo informacemi strategického významu, vyžadují komplexní ochranu s víceúrovňovým přístupem.

Obzvláště vysoké nároky na bezpečnost se kladou na provozy, které slouží ke skladování cenného majetku, výbušnin, chemických látek nebo citlivých dokumentů. Tyto objekty se stávají potenciálním cílem cílených krádeží, sabotáží nebo neoprávněného vniknutí s úmyslem získat, poškodit nebo zneužít uložené prostředky. Rizika jsou zvýšena i v případě, že se jedná o infrastrukturu zvláštního významu pro obranu státu, zásobování obyvatelstva nebo výrobní podniky v režimu kritické infrastruktury.

Z toho důvodu je nezbytné přizpůsobit úroveň fyzického zabezpečení nejen obecným normám, ale i specifickým požadavkům vyplývajícím z povahy činnosti. Při nastavování bezpečnostního režimu je důležité zohlednit typ skladovaných nebo zpracovávaných položek, hodnotu chráněného majetku, provozní režim (nepřetržitý, vícesměnný, omezený) i návaznost na externí subjekty nebo návštěvníky. Důsledná analýza předmětu činnosti umožňuje navrhnout efektivní kombinaci technických, režimových a organizačních opatření, která odpovídají reálným hrozbám spojeným s provozem daného objektu. [18]

4.2 Interní předpisy a legislativa

Základem efektivního bezpečnostního řízení je dodržování právních a interních předpisů, které upravují pravidla pro ochranu osob, majetku a provozovaných technologií. Legislativa určuje povinnosti provozovatele a nastavuje rámec činností v oblasti fyzické ochrany, které je nezbytné respektovat.

V kontextu fyzické bezpečnosti objektu je klíčové dodržování požadavků stanovených technickými normami, zejména ČSN EN 50131, která se vztahuje k navrhování, instalaci a údržbě elektronických zabezpečovacích systémů. Tato norma stanovuje minimální úroveň technického zabezpečení v závislosti na rizikovosti objektu a přispívá tak k systematickému přístupu k ochraně majetku a osob.

Interní část řízení bezpečnosti je postavena na vnitropodnikových směrnících, provozních řádech a pracovních postupech, které určují pravidla pro pohyb osob v objektu, vymezují zóny se zvýšeným režimem a nastavují reakční schémata v případě incidentů nebo mimořádných situací. Tyto dokumenty specifikují organizační odpovědnosti, určují způsob implementace bezpečnostních opatření a zajišťují jednotný přístup ke správě fyzické bezpečnosti v rámci celé organizace. [18]

4.3 Organizační a personální struktury

Organizace může zajišťovat fyzickou ochranu buď prostřednictvím vlastních zaměstnanců, nebo formou externí spolupráce s bezpečnostní agenturou. V obou případech je nutné splnit zákonné podmínky stanovené pro výkon této činnosti. Pokud je fyzická ostraha zajišťována prostřednictvím soukromé bezpečnostní služby, jedná se o koncesovanou živnost „Ostraha majetku a osob“ dle **zákona č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon)**. Tuto živnost může provozovat pouze subjekt, který splní odborné a bezúhonnostní požadavky uvedené v příslušných přílohách zákona. Samotní pracovníci, kteří vykonávají činnost strážného, pak musí doložit svou odbornou způsobilost prostřednictvím profesní kvalifikace „Strážný“ (kód: 68-008-E), definované v rámci Národní soustavy kvalifikací. Tato zkouška ověřuje jak teoretické znalosti v oblasti bezpečnosti, právního základu a komunikace, tak praktické dovednosti nezbytné pro výkon služby. Pravidelná kontrola odbornosti a aktuálnosti školení je zásadní pro udržení standardu kvality poskytované ostrahy, ať už ze strany interního personálu, nebo externí agentury. [18]

Technické a technologické vybavení

Technické prostředky představují nezbytný prvek fyzického zabezpečení objektu. Jejich hlavní funkcí je detekce a signalizace nežádoucích událostí, jako je neoprávněný vstup, pohyb osob v nepovolených zónách nebo pokus o násilné vniknutí. Mezi nejčastěji využívané technologie patří elektronické zabezpečovací systémy (PZTS), kamerové systémy (DVS), přístupové systémy (ESKV) a detektory pohybu. Tyto prvky bývají často

vzájemně propojené, čímž vytvářejí integrovaný bezpečnostní systém, schopný okamžitě reagovat na vzniklé hrozby.

Kvalitní technické řešení vyžaduje správný návrh systému s ohledem na konkrétní podmínky objektu. Nedílnou součástí efektivity je také odborná instalace, pravidelná údržba a testování funkčnosti. Včasné odhalení bezpečnostního incidentu umožňuje organizaci okamžitě reagovat a předejít větším škodám. [18]

Stavební a konstrukční řešení objektu

Z hlediska fyzické bezpečnosti hraje významnou roli také samotné stavební provedení objektu. Již při jeho návrhu je třeba zohlednit bezpečnostní aspekty, tedy způsob, jak účinně zabránit neoprávněnému vniknutí, ale také minimalizovat dopady technických selhání nebo mimořádných událostí, jako jsou požáry či výbuchy.

Zásadní význam mají použité konstrukční materiály, které by měly být pevné, odolné vůči mechanickému poškození, ideálně nehořlavé nebo s vysokou požární odolností, a v některých případech i zdravotně nezávadné. V objektech s vyšší mírou rizika (např. sklad výbušnin nebo chemikálií) se běžně používají výbušninovzdorné stěny, výměnné nebo lehké střešní panely, které v případě exploze uvolní přetlak mimo chráněný prostor, případně speciální fasádní systémy s cíleně řízeným směrem destrukce.

Mezi běžně posuzované prvky patří oplocení, obvodové zdi, bezpečnostní dveře, brány, mříže, speciální zasklení nebo podhrabové překážky. Posuzuje se také počet a rozmístění vstupních bodů, jejich ochrana a odolnost výplní (např. vrstvená nebo polykarbonátová skla), a použití certifikovaných materiálů s odpovídajícími bezpečnostními vlastnostmi.

Konstrukční řešení objektu tvoří základní linii obrany, na kterou navazují další vrstvy ochrany, a je proto nezbytné, aby bylo v souladu s celkovou bezpečnostní koncepcí objektu a umožňovalo efektivní fungování všech navazujících elektronických a organizačních opatření. [18]

4.4 Hrozby plynoucí z celospolečenské situace a jejího vývoje mimořádných událostí

Bezpečnostní rizika objektu nejsou ovlivňována pouze interními faktory, ale také celospolečenským děním. Organizace musí zohlednit aktuální stav kriminality v dané lokalitě, ekonomickou a politickou stabilitu, případně zvýšenou hrozbu teroristických útoků nebo projevů sociálního napětí. Dále je nutné být připraven na možné mimořádné události,

jako jsou přírodní katastrofy (povodně, vichřice), pandemie, výpadky infrastruktury nebo blackouty.

Zvýšené riziko může vzniknout i dočasně, např. při pořádání veřejných akcí, demonstracích nebo změnách v bezpečnostní politice státu. Organizace by proto měla mít připravený havarijní plán, který stanoví způsob reakce na tyto typy událostí. Součástí takového přístupu je i pravidelná aktualizace analýzy rizik, sledování bezpečnostního vývoje a přizpůsobování ochranných opatření reálným podmínkám. [18]

5 DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI

Teoretická část této práce se zaměřila na klíčové principy a nástroje, které tvoří základ fyzického zabezpečení objektů, a to jak z hlediska obecného přístupu, tak konkrétních metod a systémových prvků. Byly popsány základní pojmy v oblasti bezpečnosti, struktura rizika a jeho klasifikace, dále pak přístupy k analýze rizik, především SWOT a ETA. Důraz byl kladen také na organizační a režimová opatření, legislativní rámec včetně požadavků na práci s výbušninami, a možnosti technického a technologického vybavení. Podrobněji byly rozebrány mechanické a elektronické prostředky ochrany, přístupové a identifikační systémy i pravidla pro jejich nasazení a správu. Získané poznatky budou v praktické části aplikovány na konkrétní modelový objekt, kde dojde k jejich využití v rámci bezpečnostního posouzení a návrhu konkrétních opatření. Cílem je propojit teoretické principy s praktickými výstupy a ověřit, jak lze pomocí systematického přístupu efektivně vyhodnotit úroveň ochrany a navrhnout její zlepšení.

II. PRAKTICKÁ ČÁST

6 ÚVOD DO PRAKTICKÉ ČÁSTI

Cílem této praktické části je poskytnout názorný, podrobný a přenositelný návod, jak systematicky přistoupit k analýze bezpečnostních rizik v rámci konkrétního objektu. Jednotlivé analýzy jsou sestaveny tak, aby je bylo možné aplikovat na libovolný průmyslový či technologický areál, zejména však na objekty se zvýšeným rizikem, jako jsou výrobní nebo sklady výbušnin. V rámci této části je modelově zpracován fiktivní objekt společnosti **BLASTEX s.r.o.**, jehož prostřednictvím jsou demonstrovány jednotlivé postupy a metody.

Praktická část je koncipována tak, aby čtenář – ať už bezpečnostní technik, manažer provozu nebo student – získal konkrétní představu, jak dané metody využít v praxi. Jednotlivé kapitoly postupně popisují způsoby identifikace hrozeb, bodové hodnocení pravděpodobnosti a následků, analýzu slabých míst objektu a návrhy na zlepšení zabezpečení. Součástí výstupů jsou i grafické prvky, rozhodovací stromy (ETA) a vícekritériální hodnocení rizik.

Důraz je kladen nejen na výsledky, ale i na srozumitelnost postupů – tak, aby bylo možné tuto část bakalářské práce využít jako praktický manuál pro vlastní posouzení bezpečnostního stavu v jiných objektech. Každý krok je vysvětlen a podložen reálně použitelnými nástroji, které lze snadno upravit podle konkrétní situace.

6.1 Popis modelového objektu společnosti **BLASTEX s.r.o.**

Modelovým objektem pro účely této praktické části je výrobní a skladovací areál fiktivní společnosti **BLASTEX s.r.o.**, jejíž činnost je zaměřena na vývoj, výrobu, skladování a distribuci průmyslových výbušnin a související pyrotechniky. Z hlediska požární bezpečnosti se jedná o objekt zařazený do skupiny B, který podléhá zvláštnímu režimu dohledu ze strany státní báňské správy a dalších kontrolních orgánů. Areál se nachází v okrajové části průmyslové zóny, je provozován samostatně a přístup do něj je možný pouze přes kontrolovaný vstupní bod.

Celý objekt tvoří několik oddělených budov propojených vnitřní dopravní infrastrukturou. Hlavní částí je výrobní hala určená pro zpracování a kompletaci výbušnin. Na ni navazují dva samostatné sklady – jeden pro skladování surovin a druhý pro hotové výrobky připravené k expedici. Administrativní část se nachází ve zvláštní budově s kanceláři vedení, technologického oddělení a bezpečnostního managementu. Vstup do areálu zajišťuje vrátnice s kontrolním stanovištěm a elektronickým přístupovým systémem.

Součástí areálu je také parkoviště pro zaměstnance a návštěvníky a vlečka, která umožňuje přímou nakládku zboží na železniční dopravu.

Areál je chráněn oplocením s vrcholovou zábranou a je monitorován kamerovým systémem. Bezpečnostní režim zajišťuje kombinace elektronických technologií, mezi které patří elektronická zabezpečovací signalizace (PZTS), přístupový systém, elektronická požární signalizace (EPS) a automatické hasicí systémy v klíčových prostorách. Objekt je strážěn vlastní fyzickou ostrahou, která zajišťuje nepřetržitý dohled, kontrolu vstupních bodů, obchůzkovou činnost i reakce na vzniklé incidenty. Celý systém je navržen tak, aby dokázal reagovat na neoprávněné vniknutí, pokus o krádež, technické selhání i případný požár.

Bezpečnostní politika společnosti zahrnuje krizový plán, interní režimová opatření, pravidelné revize a školení zaměstnanců. Veškerá činnost se řídí platnou legislativou a technickými normami. Objekt **BLASTEX s.r.o.** tak slouží jako vhodný modelový příklad pro aplikaci bezpečnostních analýz, jejichž výstupy mohou být využity i v praxi jiných podniků s obdobným rizikovým profilem.

6.2 Předmět činnosti provozovatele

Společnost **BLASTEX s.r.o.** je výrobním a skladovacím podnikem zaměřeným na produkci průmyslových tržavin určených pro důlní a stavební činnost. Firma zajišťuje kompletní proces od vývoje přes výrobu až po distribuci a prodej emulzních, patronových a plastických výbušnin, přičemž se řadí mezi subjekty skupiny B z hlediska požární bezpečnosti dle platné legislativy.

Výrobní areál je umístěn v odlehlejší části průmyslové zóny s přímou návazností na železnici a přístupovou komunikací. Objekt je rozdělen na několik oddělených zón – administrativní, výrobní, skladovací a nakládací. S ohledem na charakter činnosti je kladen důraz na přísná bezpečnostní opatření včetně režimových, technických a organizačních pravidel.

Kromě vlastní výroby firma poskytuje i poradenské a školicí služby v oblasti manipulace s výbušninami. Zákazníky tvoří stavební společnosti, těžební firmy, armáda a subjekty působící v oblasti demolic. [17]

6.3 Interní předpisy a legislativa

Bezpečnostní politika společnosti **BLASTEX s.r.o.** vychází z platné legislativy v oblasti ochrany zdraví, života, majetku a prevence závažných havárií. Právními rámci jsou:

- **Zákon č. 224/2015 Sb.**, *o prevenci závažných havárií způsobených vybranými nebezpečnými chemickými látkami nebo chemickými směsmi a o změně zákona č. 634/2004 Sb., o správních poplatcích, ve znění pozdějších předpisů, (zákon o prevenci závažných havárií)*
- **Zákon č. 133/1985 Sb.**, *České národní rady o požární ochraně*
- **Zákon č. 61/1988 Sb.**, *České národní rady o hornické činnosti, výbušninách a o státní báňské správě*
- **Zákon č. 262/2006 Sb.**, *zákoník práce*
- **Vyhláška č. 538/2002**, *kteou se mění vyhláška č. 66/1988 Sb., kteou se provádí zákon České národní rady č. 20/1987 Sb., o státní památkové péči, ve znění vyhlášky č. 139/1999 Sb.*

Interně je bezpečnost řízena souborem závazných dokumentů, mezi které patří bezpečnostní politika objektu, provozní řády jednotlivých budov, krizový plán pro mimořádné události, plán fyzické ochrany objektu, požární řád a evakuační plán. Zaměstnanci procházejí pravidelnými školeními v oblasti BOZP a požární ochrany, včetně speciální přípravy na manipulaci s výbušninami.

Veškeré technické zabezpečení, jako jsou elektronické zabezpečovací systémy, kamerové systémy, elektronická požární signalizace a přístupové systémy, podléhá pravidelným servisním kontrolám a revizím. Funkčnost těchto zařízení je ověřována odborně způsobilými osobami minimálně jednou ročně. Mechanické zábrany a plášťová ochrana objektu procházejí kontrolami v tříletých intervalech. Elektroinstalace v prostorách s nebezpečím výbuchu se reviduje podle harmonogramu stanoveného platnými technickými normami. [20][21][22][23]

6.4 Technické a technologické zabezpečení

Součástí celkového bezpečnostního posouzení objektu je také přehled technického a technologického vybavení, které se v provozu nachází. Toto vybavení je důležité nejen z hlediska provozní funkčnosti, ale také z pohledu možného vzniku

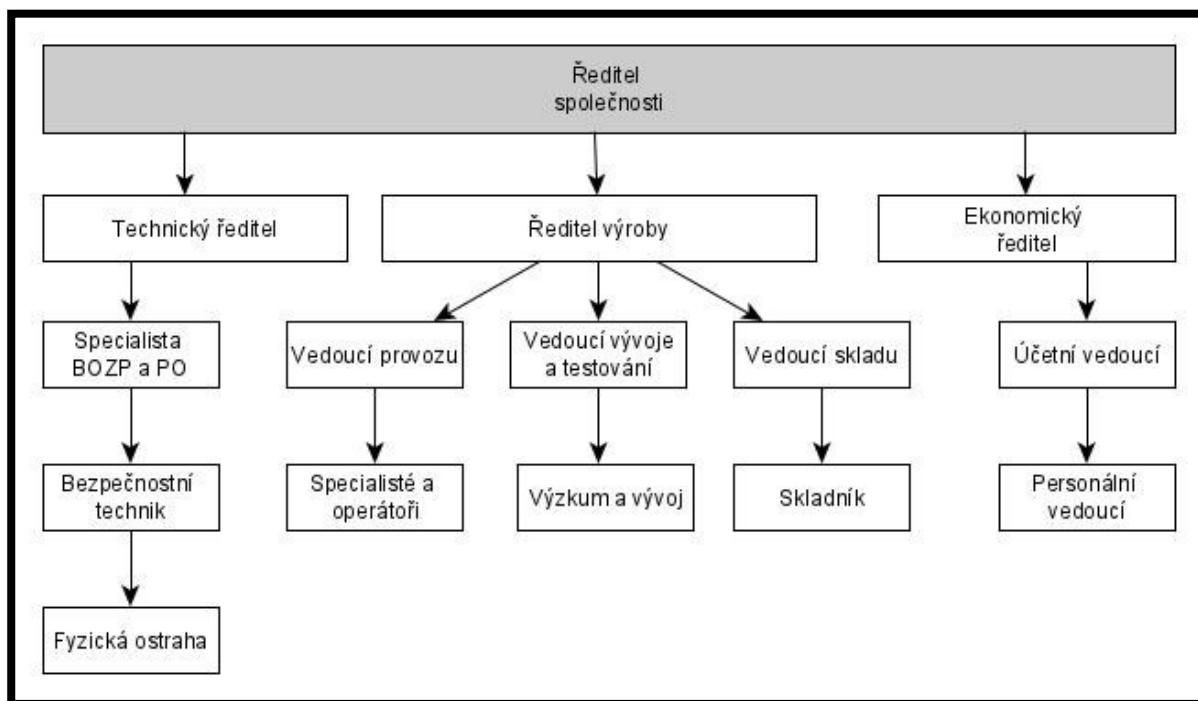
rizik a potřeby specifických ochranných opatření. Ve výrobních prostorách se nacházejí technologická zařízení pro míchání, tvarování a balení pyrotechnických směsí, která pracují s materiály podléhajícími přísné kontrole. Součástí provozu jsou míchací zařízení s řízeným dávkováním, poloautomatické lisy, dávkovací a balicí systémy. Ve skladovacích částech objektu jsou vyhrazené prostory pro příjem a výdej surovin, regálové systémy, zabezpečené úložné jednotky a manipulační technika (paletové a vysokozdvizné vozíky).

Celé technologické vybavení je napojeno na bezpečnostní systémy – především elektronickou požární signalizaci (EPS), havarijní detekci plynů a uzávěrové systémy. V místech s vyšší mírou rizika bývá instalován i kamerový dohled pro kontrolu technologických procesů. Všechna zařízení podléhají pravidelné revizi a evidenci. Zásahy do technologie jsou dokumentovány, a jejich údržba se řídí nejen pokyny výrobce, ale i požadavky právních předpisů.

Z hlediska legislativy je provoz s výbušninami regulován především **zákonem č. 61/1988 Sb.**, který upravuje podmínky výroby, skladování, nakládání a likvidace výbušnin. Prováděcí předpisy, např. *vyhláška č. 74/1988 Sb., federálního ministerstva paliv a energetiky, kterou se mění a doplňuje vyhláška federálního ministerstva paliv a energetiky č. 172/1982 Sb., o základních podmínkách dodávky topných plynů, ropy a gazolinu*. Pokud objekt spadá do kategorie zvlášť rizikových provozů, uplatní se požadavky **zákona č. 224/2015 Sb.**, o prevenci závažných havárií, včetně zpracování bezpečnostní zprávy a havarijního plánu. U technologických zařízení se dále uplatňují požadavky vyplývající z požární ochrany (**zákon č. 133/1985 Sb.**, a související vyhlášky MV ČR), a také **zákona č. 258/2000 Sb.**, o ochraně veřejného zdraví a o změně některých souvisejících zákonů v souvislosti s hygienickými limity pro práci s nebezpečnými látkami, nebo **zákona č. 206/2015 Sb.**, o pyrotechnických výrobcích a zacházení s nimi a o změně některých zákonů (*zákon o pyrotechnice*)

Technologické celky musí být rovněž provozovány kvalifikovanými osobami s odbornou způsobilostí podle § 22 **zákona č. 61/1988 Sb.** a vedeny v souladu s požadavky na systém řízení kvality dle ČSN EN ISO 9001, případně i s normami ADR v oblasti přepravy nebezpečných věcí. Společnost je dále povinna vést evidence, pravidelně hlásit stavy orgánům státní správy, provádět revize a zajišťovat školení včetně havarijní připravenosti. [20][21][22][23][24][25]

6.5 Organizační a personální struktura



Obrázek 1 Organizační a personální struktura

(zdroj: vlastní)

Organizační schéma společnosti **BLASTEX s.r.o.** přehledně znázorňuje strukturu řízení a vazby mezi jednotlivými odbornými útvary, které se podílejí na chodu provozu a zabezpečení objektu. V čele organizace stojí ředitel společnosti, který odpovídá za celkové strategické vedení a zastřešuje tři hlavní oblasti: technické řízení, výrobní řízení a ekonomické řízení. Každý z těchto úseků plní specifickou roli v rámci zajištění jak výrobních cílů, tak bezpečnostních standardů.

Pod technického ředitele spadá oblast prevence a řízení rizik, kterou zajišťuje specialista BOZP a PO. Ten úzce spolupracuje s bezpečnostním technikem, který zodpovídá za správu technických prostředků ochrany, tvorbu bezpečnostní dokumentace, školení zaměstnanců a interní kontrolní činnost. Součástí této linie je také fyzická ostraha, která může být tvořena interními zaměstnanci nebo externí bezpečnostní agenturou. Ostraha vykonává kontrolu vstupů, obchůzkovou činnost, reakce na poplachové stavy a zajišťuje pohyb v režimových zónách objektu.

Ředitel výroby řídí provozní část areálu a dohlíží na vedoucí jednotlivých oblastí. Vedoucí provozu je zodpovědný za organizaci výrobních směn a přímé řízení specialistů a operátorů pracujících na výrobních linkách. Vedoucí vývoje a testování má na starosti technologický rozvoj, zkušební činnosti a dokumentaci vývoje nových směsí a produktů. Vedoucí skladu odpovídá za evidenci, skladování a výdej surovin i hotových výrobků, přičemž úzce spolupracuje se skladníky a logistikou, například při expedici výbušnin.

Ekonomický ředitel zajišťuje administrativní a personální agendu. Pod něj spadají účetní vedoucí, který má na starosti vedení účetnictví, fakturaci a finanční toky, a personální vedoucí odpovědný za nábor, evidenci zaměstnanců, organizaci školení, zajištění lékařských prohlídek a další personální procesy.

Tato víceúrovňová organizační struktura je v podmínkách **BLASTEX s.r.o.** nezbytná pro zajištění plynulého provozu v rizikovém prostředí a pro efektivní řízení bezpečnostních opatření. Jasné rozdělení kompetencí a přehledné vazby mezi jednotlivými úseky přispívají k lepší orientaci v krizových situacích, zajišťují odpovědnost za specifické oblasti ochrany a umožňují rychlou reakci v případě incidentu nebo selhání.

7 SWOT ANALÝZA

SWOT analýza je nástroj, který umožňuje systematicky vyhodnotit silné a slabé stránky objektu a zároveň identifikovat vnější faktory v podobě příležitostí a hrozeb. V kontextu bezpečnostního posouzení výrobního a skladovacího areálu, jako je objekt společnosti **BLASTEX s.r.o.**, slouží SWOT analýza jako úvodní krok pro celkové zmapování bezpečnostní situace a odhalení prioritních oblastí pro zlepšení.

7.1 Postup práce se SWOT analýzou

SWOT analýza je metodou, která v úvodní fázi rozděluje klíčové faktory do čtyř základních kategorií – silné stránky, slabé stránky, příležitosti a hrozby. Silné stránky představují interní prvky, které zvyšují úroveň zabezpečení, jako jsou například moderní technické systémy, kvalifikovaný personál nebo dobře nastavený krizový plán. Oproti tomu slabé stránky označují vnitřní nedostatky, které mohou bezpečnostní úroveň snižovat, například vysoké provozní náklady, omezenou provozní flexibilitu nebo závislost na externích službách.

Příležitosti jsou vnější faktory, které lze ve prospěch bezpečnosti využít – typicky se jedná o možnost čerpání dotací, legislativní podporu nebo spolupráci se složkami IZS. Hrozby pak označují negativní vnější vlivy, jako je například zprísňení právních předpisů, kybernetické útoky nebo veřejný tlak. Po této kategorizaci následuje formulace konkrétních bodů na základě analýzy provozu, technologií, procesů a okolního prostředí, přičemž každý bod by měl být formulován věcně, s ohledem na jeho skutečný dopad. V rámci pokročilejšího zpracování lze jednotlivým položkám přiřadit váhy a hodnoty významu, což umožní vytvořit bodovou SWOT analýzu a kvantitativně porovnat jednotlivé oblasti. Takové zpracování přináší jasnější obrázek o tom, zda systém čerpá ze svých silných stránek, nebo naopak převažují slabiny, a jak výrazný vliv mají externí příležitosti a hrozby. SWOT analýza tak tvoří důležitý podklad pro navazující hodnotící metody, jako je analýza stromu událostí (ETA) nebo vícekritériální hodnocení bezpečnostních rizik.

7.2 Konkrétní SWOT analýza společnosti Blastex s.r.o.

Silné stránky	Váha	Význam	Bilance
Vlastní výrobní a skladovací areál s perimetrovým zabezpečením	0,2	5	1
Moderní kamerový a přístupový systém napojený na DPPC	0,13	4	0,52
Vysoce kvalifikovaný personál s certifikacemi pro manipulaci s výbušninami	0,05	4	0,2
Samostatná vlečka – efektivní logistika a přeprava	0,1	3	0,3
Provozní režim 24/7 – rychlá reakce na incidenty	0,1	3	0,3
Dobrá znalost rizik a zpracovaný krizový plán	0,2	5	1
Jasně definovaná interní pravidla a bezpečnostní směrnice	0,08	4	0,32
Dlouhodobá spolupráce s odbornými dodavateli bezpečnostních systémů a servisních firem	0,03	3	0,09
Jasně stanovené role a odpovědnosti zaměstnanců při řešení bezpečnostních událostí	0,11	4	0,44
Celkem	1		4,17
Slabé stránky			
Vysoké provozní náklady na údržbu bezpečnostních technologií	0,12	-4	-0,48
Náročné požadavky na kvalifikaci personálu pro práci s výbušninami	0,08	-3	-0,24
Složitý schvalovací proces při zavádění nových bezpečnostních opatření	0,06	-3	-0,18
Omezená flexibilita provozu kvůli přísným režimovým pravidlům	0,13	-5	-0,65
Závislost na dodavatelských službách pro revize a údržbu systémů	0,06	-2	-0,12
Větší tlak na povinnosti odpovědných zaměstnanců	0,18	-3	-0,54
Malý počet vyškolených pracovníků v oblasti krizového řízení	0,12	-3	-0,36
Časově náročné vstupní školení a zácvik nových zaměstnanců	0,15	-2	-0,3
Nedostatek zkušenosti	0,1	-4	-0,4
Celkem	1		-3,27
Příležitosti	Váha	Význam	Bilance
Rostoucí poptávka po službách v oblasti těžby, demolice a speciálních staveb	0,05	2	0,1
Možnost získání dotací na modernizaci bezpečnostních systémů	0,2	4	0,8
Spolupráce s armádními nebo státními složkami (např. při likvidaci munice)	0,06	3	0,18
Rozšíření služeb o poradenství v oblasti pyrotechnické bezpečnosti	0,3	5	1,5
Zavedení automatizace ve výrobě pro zvýšení efektivity	0,18	2	0,36
Export výbušnin do zahraničí v rámci certifikovaných programů	0,05	2	0,1
Využití vývojových partnerství pro inovace (např. nové typy rozbušek)	0,06	3	0,18
Sladění zdrojů a cílů	0,08	2	0,16
Zlepšení pracovního prostředí	0,02	1	0,02
Celkem	1		3,4
Hrozby			
Zpřísnění legislativy v oblasti nakládání s výbušninami	0,03	-3	-0,09
Zpoždění nebo neobnovení povolení k provozu ze strany státní správy	0,04	-3	-0,12
Cílené útoky, krádeže nebo sabotáže kvůli povaze materiálů	0,05	-3	-0,15
Ztráta klíčového odběratele nebo pokles zakázek	0,08	-2	-0,16
Kritika veřejnosti nebo tlak ekologických organizací	0,18	-4	-0,72
Výpadek dodávek surovin kvůli mezinárodním omezením	0,12	-4	-0,48
Riziko havárie a následné právní nebo reputační důsledky	0,28	-5	-1,4
Vzrůstající kybernetická rizika spojená s napojením bezpečnostních systémů na síť	0,06	-3	-0,18
Nárůst kriminality v regionu nebo blízkosti kritické infrastruktury	0,16	-3	-0,48
Celkem		1	-3,78

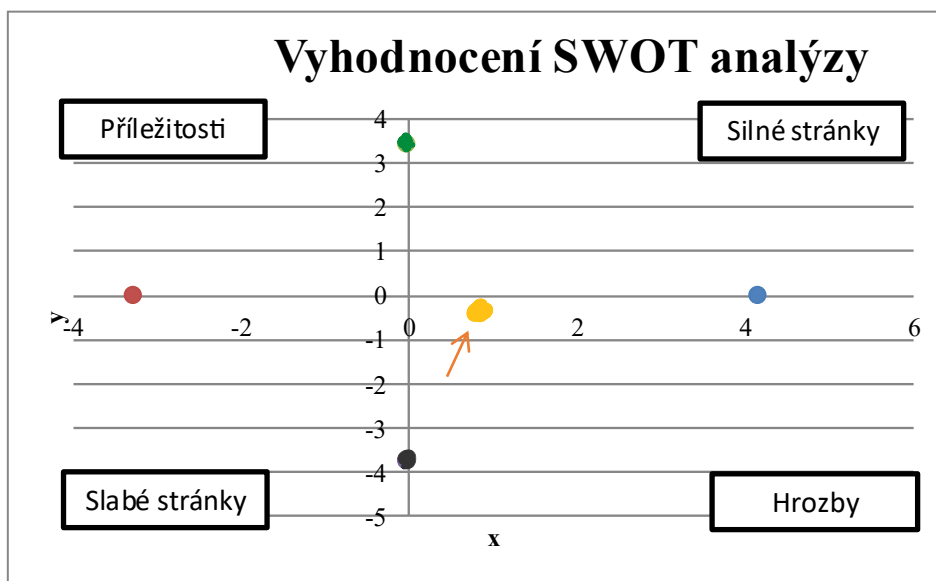
Obrázek 2 SWOT analýza společnosti BLASTEX s.r.o.

(zdroj: vlastní)

Matice		x	y
Silné stránky	S	4,17	0
Slabé stránky	W	-3,27	0
Příležitosti	O	0	3,4
Hrozby	T	0	-3,78
Celkem		0,9	-0,38

Obrázek 3 Matice SWOT analýzy

(zdroj: vlastní)



Obrázek 4 Vyhodnocení SWOT analýzy

(zdroj: vlastní)

Tabulka 1 Vysvětlení grafu SWOT analýzy

Barva bodu	SWOT oblast	Popis umístění	Doporučení
	Příležitosti	Levá horní část – vysoký potenciál, nízké využití	Zaměřit se na realizaci a přenos do praxe
	Slabé stránky	Levá dolní část – negativní dopad, vyšší váha	Prioritně řešit a omezit jejich vliv
	Silné stránky	Pravá horní část – pozitivní vliv, významný přínos	Udržovat a dále rozvíjet
	Hrozby	Pravá dolní část – negativní externí vlivy, vysoké riziko	Monitorovat a připravit opatření
	Souhrnný bod	Střed grafu – vyvážený stav, prostor ke zlepšení	Směřovat strategii k posílení pozitivních oblastí

(Data čerpána z: [15])

7.3 Vyhodnocení SWOT analýzy

SWOT analýza představuje ucelený pohled na vnitřní i vnější faktory ovlivňující bezpečnostní strategii společnosti BLASTEX s.r.o. Výsledky kvantitativního hodnocení ukazují na silnou pozici podniku v provozním a bezpečnostním prostředí, zároveň však poukazují na několik oblastí vyžadujících zvýšenou pozornost.

Mezi hlavní silné stránky patří vlastnictví moderně vybaveného výrobního a skladovacího areálu s kamerovým, přístupovým a perimetrickým zabezpečením. Významným přínosem je také kvalifikovaný personál s odbornou certifikací a propracovaný krizový plán s jasně vymezenými kompetencemi. Tato opatření přispívají k vysoké připravenosti na incidenty a zvyšují odolnost areálu vůči rizikům.

Slabé stránky se týkají především vysokých nákladů na údržbu technologií a organizační náročnosti spojené s přísnými režimovými opatřeními a požadavky na kvalifikaci. Jako problém se jeví i složitý proces zaškolování nových pracovníků a nedostatek zkušeností v krizovém řízení, což může snižovat pružnost reakce na mimořádné události.

Mezi příležitosti lze zařadit rostoucí poptávku po specializovaných službách v oblasti těžby a demolic, možnost získat dotace na modernizaci zabezpečení, rozšíření služeb o pyrotechnické poradenství nebo spolupráci se státními institucemi a zapojení do vývojových projektů v oblasti trhavin. Naopak hrozby souvisejí se zpříšňováním legislativy, kybernetickými útoky na technické systémy, cílenými útoky či krádežemi kvůli povaze skladovaného materiálu a výpadky v dodavatelském řetězci.

Celkově SWOT analýza ukazuje, že **BLASTEX s.r.o.** má silný základ pro rozvoj bezpečnostní strategie. Pokud dokáže zmírnit interní slabiny a připravit se na hrozby, může nejen stabilně fungovat, ale také efektivně využít externí příležitosti pro další růst.

8 ETA ANALÝZY SPOLEČNOSTI BLASTEX S.R.O

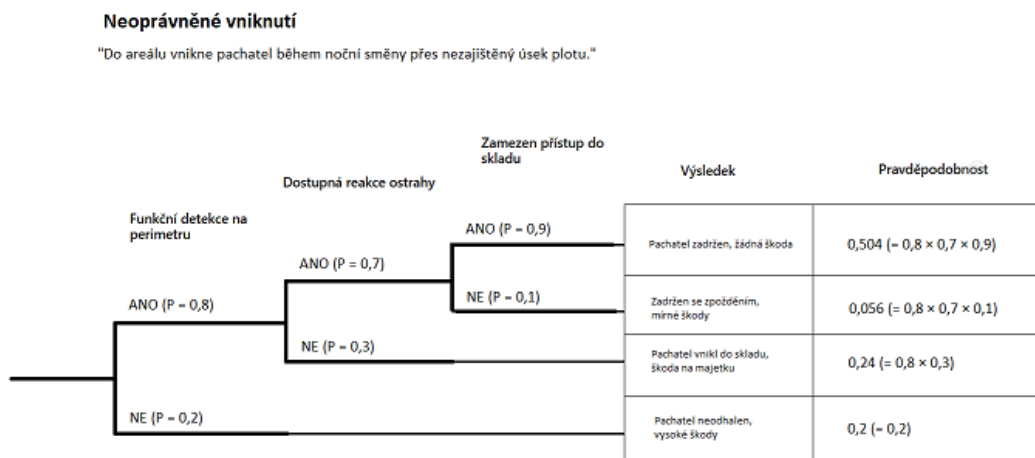
Analýza stromu událostí (ETA – Event Tree Analysis) představuje metodu určenou k modelování možného vývoje situace po vzniku bezpečnostního incidentu. Na rozdíl od analýzy stromu poruch (FTA), která se zabývá hledáním příčin selhání, se ETA zaměřuje na sledování následků již nastalé události a na to, jak jednotlivé bezpečnostní prvky ovlivňují její průběh. Cílem je znázornit a vyhodnotit, jak různé kombinace fungujících nebo selhávajících opatření vedou k rozdílným scénářům s různou závažností dopadu.

V této práci je metoda ETA aplikována na dva reálně hrozící scénáře, které jsou typické pro prostředí objektu **BLASTEX s.r.o.** Prvním je neoprávněné vniknutí do areálu mimo provozní dobu a druhým vznik požáru ve výrobní hale. Každá analýza začíná přesně definovanou počáteční událostí, která se považuje za jistou. Následuje rozvětvení podle toho, zda jednotlivá opatření – například perimetrická detekce, reakce ostrahy, aktivace EPS, zásah hasicí techniky nebo složek IZS – fungují, nebo selžou. Každému rozhodovacímu bodu je přiřazena pravděpodobnost, která vychází z předpokládané účinnosti opatření.

Výsledkem je přehledný strom událostí zakončený čtyřmi až šesti možnými scénáři, přičemž ke každému je přiřazena výsledná pravděpodobnost, která je součinem jednotlivých větví. Scénáře jsou popsány jak věcně (např. „pachatel zadržen bez škody“ nebo „požár zcela nekontrolovaně rozšířen“), tak číselně. Právě díky této kombinaci umožňuje ETA rychle identifikovat slabá místa systému a vyhodnotit, která opatření mají největší vliv na zvládnutí celé události.

ETA analýza je mimořádně užitečná při tvorbě krizových plánů, testování funkčnosti navržených systémů a rozhodování o posílení konkrétních složek zabezpečení. Vzhledem ke své jednoduché logice, přehledným výstupům a možnosti kvantifikace je vhodná nejen pro odborníky, ale i pro praktické využití v rámci interní bezpečnostní politiky každého podniku.

8.1 ETA – neoprávněné vniknutí



Obrázek 5 ETA analýza neoprávněného vniknutí

(zdroj: vlastní)

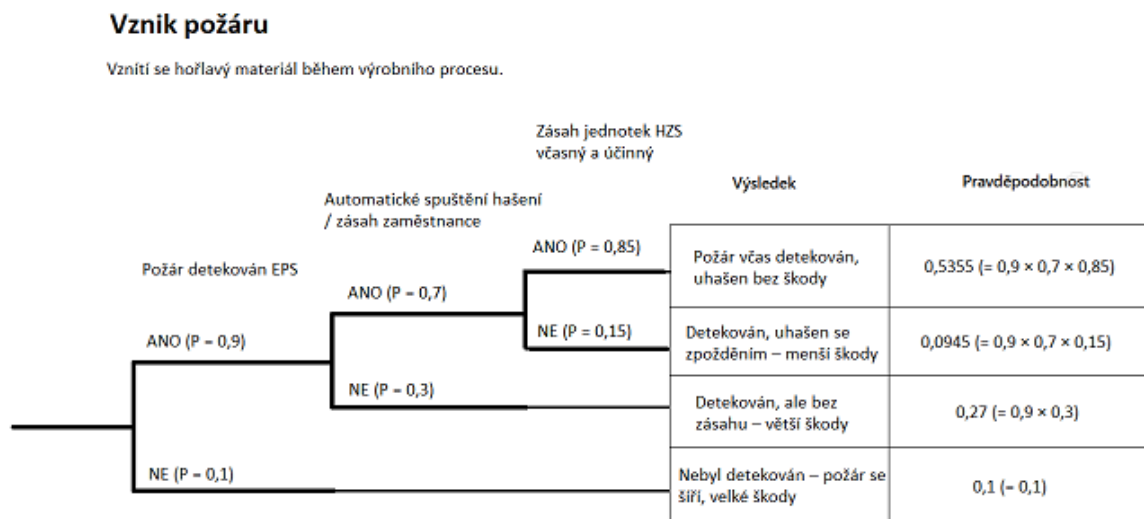
Shrnutí výsledků ETA analýzy – vniknutí pachatele

Analýza stromu událostí (ETA) názorně ukazuje možné scénáře vývoje situace v případě neoprávněného vniknutí do areálu společnosti **BLASTEX s.r.o.**, a to v závislosti na funkčnosti jednotlivých bezpečnostních opatření. Nejpravděpodobnější výsledek, s pravděpodobností 50,4 %, nastává tehdy, pokud jsou všechny bezpečnostní prvky plně funkční – detekce na perimetru zachytí pohyb, ostraha na incident včas zareaguje a pachatel je zastaven ještě před vstupem do skladových prostor. V tomto případě nedochází ke vzniku žádné škody.

Za nejzávažnější scénář je považována situace, kdy detekce selže a pachatel zůstane zcela neodhalen. Tento výsledek má pravděpodobnost 20 % a představuje vysoké riziko vzniku závažných škod. Mezi těmito krajními variantami se nacházejí meziscénáře – například zadržení pachatele se zpožděním (5,6 %) nebo jeho průnik do skladu s následnou materiální škodou (24 %).

Z provedené analýzy vyplývá, že nejdůležitějšími faktory pro zvládnutí incidentu jsou spolehlivá detekce pohybu na perimetru a rychlá reakce fyzické ostrahy. Selhání v kterékoli z těchto oblastí významně zvyšuje riziko materiálních i reputačních ztrát.

8.2 ETA – Vznik požáru



Obrázek 6 ETA analýza vznik požáru

(zdroj: vlastní)

Shrnutí výsledků ETA analýzy – požár

Analýza stromu událostí (ETA) simuluje vývoj situace v případě vzniku požáru ve výrobní hale společnosti **BLASTEX s.r.o.** Nejpravděpodobnější pozitivní scénář, s pravděpodobností 53,6 %, nastává tehdy, pokud je požár včas detekován systémem elektronické požární signalizace (EPS), bezodkladně je zahájen zásah – ať už automatickým hasicím systémem, nebo zaměstnanci – a následně proběhne účinný zásah jednotek HZS. Tento vývoj zajišťuje zvládnutí události bez vzniku škody.

S rostoucí pravděpodobností selhání jednotlivých kroků však úměrně roste i riziko škod. V případě, že EPS požár sice detekuje, ale zásah je zpožděn nebo zcela selže, stoupá pravděpodobnost vzniku materiálních škod na 27 %. Nejzávažnějším scénářem je selhání detekce, kdy požár zůstane bez povšimnutí a rozšíří se – tento případ má pravděpodobnost 10 % a vede k rozsáhlým škodám na majetku.

Analýza potvrzuje, že rozhodujícím prvkem pro zvládnutí požáru je včasná funkce detekčního systému EPS a okamžité spuštění zásahových opatření. Důležitou roli zde hraje i provázanost technických a lidských reakcí, jejichž správná koordinace určuje, jak výrazné budou dopady mimořádné události.

8.3 Porovnání výsledků obou ETA analýz

Obě zpracované analýzy stromu událostí, a to scénář neoprávněného vniknutí do areálu a vznik požáru ve výrobním prostoru, ukazují důležitost správné funkce jednotlivých bezpečnostních prvků a schopnosti systému efektivně reagovat. V obou případech se ukazuje, že při ideálním průběhu, kdy veškerá technická i personální opatření fungují správně, lze mimořádnou událost zvládnout bez vzniku škody. Tyto pozitivní scénáře mají nejvyšší pravděpodobnost – 50,4 % u vniknutí a 53,6 % u požáru.

Naopak v případě selhání klíčových opatření prudce narůstá riziko škod. Nejzávažnější negativní scénář u vniknutí, kdy pachatel není vůbec detekován, vykazuje pravděpodobnost 20 %, zatímco u požáru je tato hodnota 10 %. I přes nižší pravděpodobnost má požár potenciálně závažnější dopad na majetek i bezpečnost osob.

Obě analýzy tedy potvrzují, že největší vliv na vývoj krizové situace mají včasná detekce, bezprostřední aktivace zásahových opatření a připravenost fyzické ostrahy či personálu. ETA tak umožňuje nejen odhad pravděpodobného vývoje událostí, ale zároveň pomáhá jednoznačně určit slabá místa systému, která je nutné posílit pro minimalizaci následků.

9 NÁVRH ZLEPŠENÍ BEZPEČNOSTNÍHO SYSTÉMU OBJLEKU BLASTEX S.R.O.

Na základě provedených bezpečnostních analýz lze identifikovat několik oblastí, ve kterých je vhodné posílit stávající bezpečnostní systém společnosti **BLASTEX s.r.o.** Návrhy vycházejí ze zjištěných slabých míst, pravděpodobných a závažných scénářů mimořádných událostí a celkového hodnocení ohrožení klíčových částí objektu. Za prioritní lze označit posílení detekčních a signalizačních systémů – ETA analýzy prokázaly, že včasná detekce (např. vniknutí, požár) výrazně zvyšuje šanci na zvládnutí události bez škod. Doporučuje se rozšířit perimetrickou ochranu o další typy čidel (např. mikrovlnné, infračervené, detektory pohybu) a zavést redundanci pro případ výpadku. U požární bezpečnosti je vhodné doplnit systém EPS o adresné hlášení a automatické ovládání hasicích systémů, zejména ve skladech a výrobních prostorách.

Reakční schopnost fyzické ostrahy je dalším klíčovým prvkem. Doporučuje se přezkoumat její vnitřní nastavení, posílit školení zaměstnanců a zavést pravidelná taktická cvičení zaměřená na zvládnutí typových scénářů, zejména v nočních hodinách. Lze uvažovat i o zřízení samostatného dispečinku pro centralizovaný dohled nad bezpečnostními událostmi v reálném čase. Z hlediska provozní organizace se doporučuje zpřesnit režimová opatření vůči externím dodavatelům a návštěvám – zavést povinnou registraci vstupů, krátké instruktáže a fyzický doprovod po areálu. V oblasti IT bezpečnosti byla identifikována střední až vysoká míra rizika kybernetického útoku. Doporučuje se provést audit zranitelností, zavést více faktorové ověřování, pravidelně aktualizovat software a omezit přístup externích zařízení k síti.

Zároveň je vhodné revidovat krizové a evakuační plány z hlediska jejich aktuálnosti, reálnosti postupů a souladu s fyzickým uspořádáním objektu. Zapojením zaměstnanců do nácviku modelových situací (např. evakuace, zvládnutí útoku) lze zvýšit jejich připravenost. Zavedením výše uvedených opatření se významně zvýší odolnost objektu **BLASTEX s.r.o.** vůči bezpečnostním hrozbám a bude zajištěno, že klíčové procesy výroby a skladování probíhají bezpečně, spolehlivě a v souladu se zákonnými požadavky.

ZÁVĚR

Cílem této bakalářské práce bylo analyzovat možnosti fyzické ochrany objektu z pohledu aktuálních požadavků na bezpečnost, legislativních předpisů a dostupných technických prostředků. Na základě výsledků provedených analýz byl dále zpracován návrh konkrétních bezpečnostních opatření s ohledem na charakter provozu, identifikovaná rizika a reálné potřeby zabezpečení. Práce byla strukturována tak, aby naplnila všech pět zásad stanovených pro její vypracování a přinesla ucelený, metodicky správný a prakticky využitelný výstup.

První zásadou bylo zpracování literární rešerše vztahující se k současnému stavu problematiky fyzické bezpečnosti. Tato část byla naplněna prostřednictvím teoretického přehledu, který zahrnoval klasifikaci rizik, obecné principy fyzické ochrany, přehled metod jejich hodnocení a podrobné rozdělení technických, mechanických, režimových a organizačních prostředků zabezpečení. Dále byl zohledněn legislativní rámec, který se vztahuje zejména k provozům s výskytem výbušnin, ochraně zdraví a požární bezpečnosti.

Druhá zásada spočívala v identifikaci analytických metod, které lze uplatnit při návrhu a hodnocení fyzické ochrany. V práci byly vybrány a využity především SWOT analýza a analýza stromu událostí (ETA), přičemž obě tyto metody byly podrobně popsány a přizpůsobeny charakteru modelového objektu. SWOT analýza umožnila strukturované zhodnocení silných a slabých stránek bezpečnostního systému, stejně jako identifikaci relevantních příležitostí a hrozeb. ETA pak sloužila pro rozbor konkrétních scénářů ohrožení objektu, a to jak z hlediska jejich průběhu, tak pravděpodobnosti jednotlivých větvení.

Třetí zásadou bylo posoudit vybrané analytické metody z hlediska jejich praktického využití. Tento požadavek byl naplněn aplikací obou metod na modelový výrobní a skladovací areál společnosti BLASTEX s.r.o., přičemž výsledky analýz posloužily jako vstupní podklad pro návrh konkrétních opatření. Analýzy umožnily nejen systematické vyhodnocení aktuální úrovně ochrany, ale také určení priorit, na které se při zlepšení bezpečnostního systému zaměřit.

Čtvrtá zásada požadovala navrhnout metodu pro objektivní posouzení fyzické ochrany. Tato část byla naplněna zpracováním vícekritériální analýzy hrozeb, ve které byly jednotlivé scénáře ohrožení hodnoceny podle sedmi parametrů: dostupnost, komplexita, atraktivita cíle, míra poškození objektu, ohrožení života, společenský a ekonomický dopad. Díky bodovému ohodnocení a stanovení váženého skóre bylo možné určit pořadí závažnosti hrozeb a stanovit priority pro navržená opatření.

Pátá a závěrečná zásada se týkala návrhu konkrétního plánu fyzické ochrany objektu. Tento požadavek byl naplněn sestavením uceleného návrhu zabezpečení modelového objektu, který zahrnuje přehled organizační struktury, popis režimových opatření, rozdělení odpovědnosti, použití technických a mechanických prostředků ochrany, návrh kamerového systému, přístupových bodů i opatření pro zvládání specifických scénářů ohrožení.

Na základě výše uvedeného lze konstatovat, že všechny stanovené zásady pro vypracování práce byly beze zbytku splněny. Práce tak představuje kompletní bezpečnostní koncepci aplikovanou na modelový objekt s rizikovým provozem a prokazuje možnosti využití teoretických znalostí v praxi. Výstupy jsou přehledné, prakticky využitelné a mohou sloužit jako metodický podklad pro návrh fyzické ochrany obdobných typů objektů v reálném prostředí. Zároveň práce přináší i doporučení k rozvoji bezpečnostního systému a ukazuje, jak lze analytické, technické a organizační přístupy efektivně kombinovat k dosažení vyšší úrovně ochrany.

SEZNAM POUŽITÉ LITERATURY

- [1] WEB - APTIEN. *Co je fyzická bezpečnost*. Online. ©2025. Dostupné z: <https://aptien.com/cs/kb/articles/what-is-physical-security>. [cit. 2025-01-03].
- [2] ČESKO. Vyhláška č. 205 ze dne 17. června 2008, o listinách, které je české zúčastněné družstvo povinno předložit notáři k vydání osvědčení o zákonnosti dokončení založení evropské družstevní společnosti fúzí. Online. In: *Zákony pro lidi*. 2010–2025. Dostupné z: <https://www.zakonyprolidi.cz/cs/2008-205>. [cit. 2025-01-03].
- [3] Ivanka, Ján. *Mechanické zábranné systémy*. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2014. ISBN 978-80-7454-427-9.
- [4] ZEDEK, Karel. *Aplikace systémového přístupu v oblasti objektové bezpečnosti*. Online. Diplomová práce. Praha: Česká zemědělská univerzita v Praze, Provozně ekonomická fakulta, Katedra systémového inženýrství, 2015. Dostupné z: https://theses.cz/id/cpr21h/zaverecna_prace.pdf. [cit. 2025-01-03].
- [5] WEB - ABBAS. *Plášťová ochrana*. Online. ©2025. Dostupné z: <https://www.perimetrie.cz/perimetrie/plastova-ochrana/>. [cit. 2025-01-03].
- [6] TECHNICKÉ NORMY ČSN – ČESKO. ČSN EN 50131-1 ed. 2 (334591): *Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 1: Systémové požadavky*. Online. In: Technické normy ČSN. 2007–2025. Dostupné z: <https://www.technicke-normy-csn.cz/csn-en-50131-1-ed-2-334591-181882.html>. [cit. 2025-01-03].
- [7] WEB - SECURIA PRO. *Jak probíhá montáž kamerového systému*. Online. ©2024. Dostupné z: <https://www.securiapro.cz/clanek/jak-probiha-montaz-kameroveho-systemu/>. [cit. 2025-01-03].
- [8] TECHNICKÉ NORMY ČSN – ČESKO. ČSN EN 62676-1-2 (334592): *Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 1-2: Systémové požadavky – Výkonové požadavky na video přenos*. Online. In: Technické normy ČSN. 2014–2025. Dostupné z: <https://www.technicke-normy-csn.cz/csn-en-62676-1-2-334592-181979.html>. [cit. 2025-02-12].
- [9] WEB - ELEKTROPRŮMYSL.CZ. *Co jsou snímáče pohybu a jak fungují*. Online. ©2021. Dostupné z: <https://www.elektroprumysl.cz/elektroinstalace/co-jsou-snimace-pohybu-a-jak-funguji>. [cit. 2025-02-12].

- [10] WEB - ALARMSECURITY.CZ. *Typy pohybových senzorů*. Online. ©2025. Dostupné z: <https://www.alarmsecurity.cz/www-alarmsecurity-cz/5-TECHNICKA-PODPORA/38-Typy-pohybovych-senzoru>. [cit. 2025-02-12].
- [11] WEB - ACS-LINE. *Přístupový systém*. Online. ©2025. Dostupné z: <https://www.acsline.cz/cs/pristupovy-system>. [cit. 2025-02-12].
- [12] WEB - SECURITAS ČR. *Přístupové systémy: Klíče nebo oční duhovka?* Online. ©2020. Dostupné z: <https://www.securitas.cz/novinky--blog/blog/pristupove-systemy--kllice-nebo-ocni-duhovka/>. [cit. 2025-02-12].
- [13] ATP JOURNAL. *Docházkové a přístupové systémy*. In: IDB Journal, 2012, č. 2, s. 24–26. Online. Dostupné z: <https://www.atpjournals.sk/buxus/docs/idb%20journal%202%202012%20str%2024-26.pdf>. [cit. 2025-04-25].
- [14] PROCHÁZKOVÁ, Dana a PROCHÁZKA, Jan. *Analýza rizik I*. Praha: Vysoká škola regionálního rozvoje Praha, 2014. ISBN 978-80-87174-26-5.
- [15] PROCHÁZKOVÁ, Dana a PROCHÁZKA, Jan. *Analýza rizik II*. Praha: Vysoká škola regionálního rozvoje Praha, 2014. ISBN 978-80-87174-27-2.
- [16] WEB - COMMUNITY TOOL BOX. *SWOT Analysis: Strengths, Weaknesses, Opportunities, and Threats*. Online. ©2025. Dostupné z: <https://ctb.ku.edu/en/table-of-contents/assessment/assessing-community-needs-and-resources/swot-analysis/main>. [cit. 2025-04-25].
- [17] RAUSAND, Marvin. *Chapter 3: Event Tree Analysis*. Online. ©2012. Dostupné z: <https://www.ntnu.edu/documents/624876/1277590549/chapt03-eta.pdf/6f3e1b19-4824-4812-adc8-9762d2201c22>. [cit. 2025-04-25].
- [18] KORECKÝ, Michal a TRKOVSKÝ, Václav. *Management rizik projektů: se zaměřením na projekty v průmyslových podnicích*. Expert. Praha: Grada, 2011. ISBN 978-80-247-3221-3.
- [19] ČESKO. Vyhláška č. 225 ze dne 11. září 2015, o stanovení rozsahu bezpečnostních opatření fyzické ochrany objektu zařazeného do skupiny A nebo skupiny B. Online. In: *Zákony pro lidi*. 2010–2025. Dostupné z: <https://www.zakonyprolidi.cz/cs/2015-225>. [cit. 2025-05-23].

- [20] ČESKO. Zákon č. 224 ze dne 11. srpna 2015, o prevenci závažných havárií způsobených vybranými nebezpečnými chemickými látkami nebo chemickými směsmi a o změně zákona č. 634/2004 Sb., o správních poplatcích, ve znění pozdějších předpisů, (zákon o prevenci závažných havárií) Online. In: *Zákony pro lidi*. 2010–2025. Dostupné z: <https://www.zakonyprolidi.cz/cs/2015-224>. [cit. 2025-05-23].
- [21] ČESKO. Zákon č. 133 ze dne 17. prosince 1985, Zákon České národní rady o požární ochraně. Online. In: *Zákony pro lidi*. 2010–2025. Dostupné z: <https://www.zakonyprolidi.cz/cs/1985-133>. [cit. 2025-05-23].
- [22] ČESKO. Zákon č. 61 ze dne 21. dubna 1988, Zákon České národní rady o hornické činnosti, výbušninách a o státní báňské správě. Online. In: *Zákony pro lidi*. 2010–2025. Dostupné z: <https://www.zakonyprolidi.cz/cs/1988-61>. [cit. 2025-05-23].
- [23] ČESKO. Vyhláška č. 538 ze dne 31. prosince 2002, kterou se mění vyhláška č. 66/1988 Sb., kterou se provádí zákon České národní rady č. 20/1987 Sb., o státní památkové péči, ve znění vyhlášky č. 139/1999 Sb. Online. In: *Zákony pro lidi*. 2010–2025. Dostupné z: <https://www.zakonyprolidi.cz/cs/2002-538>. [cit. 2025-05-23].
- [24] ČESKO. Zákon č. 206 ze dne 20. srpna 2015, o pyrotechnických výrobcích a zacházení s nimi a o změně některých zákonů (zákon o pyrotechnice). Online. In: *Zákony pro lidi*. 2010–2025. Dostupné z: <https://www.zakonyprolidi.cz/cs/2015-206>. [cit. 2025-05-23].
- [25] ČESKO. Vyhláška č. 74 ze dne 24. května 1988, kterou se mění a doplňuje vyhláška federálního ministerstva paliv a energetiky č. 172/1982 Sb., o základních podmínkách dodávky topných plynů, ropy a gazolinu. Online. In: *Zákony pro lidi*. 2010–2025. Dostupné z: <https://www.zakonyprolidi.cz/cs/1988-74>. [cit. 2025-05-23].

SEZNAM OBRÁZKŮ

Obrázek 1 Organizační a personální struktura.....	42
Obrázek 2 SWOT analýza společnosti BLASTEX s.r.o.	45
Obrázek 3 Matice SWOT analýzy	46
Obrázek 4 Vyhodnocení SWOT analýzy.....	46
Obrázek 5 ETA analýza neoprávněného vniknutí	49
Obrázek 6 ETA analýza vznik požáru	50

SEZNAM TABULEK

Tabulka 1 Vysvětlení grafu SWOT analýzy	46
---	----

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BOZP Bezpečnost a ochrana zdraví při práci

ČSN Česká technická norma

DVS Dohledový videosystém

ETA Event Tree Analysis

EPS Elektronická požární signalizace

ESKV Elektronický systém kontroly vstupu

FTA Fault Tree Analysis

HZS Hasičský záchranný sbor

IS Informační systém

IZS Integrovaný záchranný systém

MZS Mechanický zábranný systém

Např. Například

PIR Passive InfraRed

PZTS Poplachový zabezpečovací a tísňový systém

SWOT Strengths, Weaknesses, Opportunities, Threats