

UNIVERZITA PARDUBICE
FAKULTA EKONOMICKO-SPRÁVNÍ

BAKALÁŘSKÁ PRÁCE

2024

Michal Vávrů

Univerzita Pardubice
Fakulta ekonomicko-správní

Návrh zabezpečení firmy
Bakalářská práce

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2023/2024

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: **Michal Vávrů**
Osobní číslo: **E21618**
Studijní program: **B0688A140004 Informatika a systémové inženýrství**
Specializace: **Informační a bezpečnostní systémy**
Téma práce: **Návrh zabezpečení firmy**
Zadávací katedra: **Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cílem práce je identifikovat slabá místa v zabezpečení firmy, identifikovat možnosti zabezpečení a pomocí metod vícekritériálního rozhodování navrhnout vhodné zabezpečení.

Osnova:

- Úvod do zabezpečení objektů, popis, druhy.
- Popis firmy a současného stavu zabezpečení.
- Definice rozhodovacího procesu, stanovení kritérií a variant.
- Řešení rozhodovacího problému pomocí metod vícekritériálního rozhodování.

Rozsah pracovní zprávy: **cca 35 stran**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

BURDA, Karel. *Základy elektronických zabezpečovacích systémů*. Brno: Akademické nakladatelství CERM, 2017. ISBN 978-80-7204-967-7.
KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.
KYNCL, Jaromír. *Bezpečnost objektu ve světle moderních technologií*. Praha: Komora podniků komerční bezpečnosti České republiky, 2014. ISBN 978-80-260-7115-0.
LOVEČEK, Tomáš, Ladislav MARIŠ a Anton ŠISER. *Plánovanie a projektovanie systémov ochrany objektov*. Žilina: Žilinská univerzita v Žiline, 2018. Vysokoškolské učebnice. ISBN 978-80-554-1482-9.
SMITH, Eric. *Workplace Security Essential: A Guide for Helping Organization Create Safe Work Environments*. Waltham: Elsevier, 2014. ISBN 978-0-12-416557-1.

Vedoucí bakalářské práce: **Ing. Renáta Máchová, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **1. září 2023**
Termín odevzdání bakalářské práce: **30. dubna 2024**

prof. Ing. Jan Stejskal, Ph.D. v.r.
děkan

L.S.

Ing. et Ing. Martin Lněnička, Ph.D. v.r.
garant studijního programu

V Pardubicích dne 1. září 2023

Prohlašuji:

Práci s názvem „*Návrh zabezpečení firmy*“ jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 30. 04. 2024

Michal Vávrů v. r.

PODĚKOVÁNÍ

Tímto bych rád poděkoval vedoucí mé bakalářské práce Ing. Renátě Máchové, Ph.D. za její odbornou pomoc, cenné rady a poskytnuté materiály a také za ochotu, trpělivost a vstřícnost, které mi pomohly při zpracování této práce. Také bych rád poděkoval své rodině a všem ostatním za podporu při tvorbě této práce.

ANOTACE

Bakalářská práce je zaměřena na návrh zabezpečení firmy. Obsahem je úvod do zabezpečení objektů, popis a druhy zabezpečení, popis firmy, její struktury, finanční situace, mise, vize a cílů, současného stavu a vyhodnocení rizik. Tyto informace jsou využity k identifikaci opatření pro zvýšení bezpečnosti, která budou podkladem pro definici rozhodovacího procesu a jeho řešení pomocí metod vícekriteriálního rozhodování.

KLÍČOVÁ SLOVA

zabezpečení firmy, fyzické zabezpečení, elektronické zabezpečovací systémy, vícekriteriální rozhodování

TITLE

Proposal for company security

ANNOTATION

The bachelor's thesis focuses on designing company security measures. It includes an introduction to object security, a description and types of security, a company profile, its structure, financial situation, mission, vision and goals, current status and risk assessment. These pieces of information are used to identify measures to increase security, which will be the basis for defining the decision-making process and its result using multi-criteria decision-making methods.

KEYWORDS

company security, physical security, electronic security systems, multi-criteria decision making

OBSAH

SEZNAM TABULEK	8
SEZNAM OBRÁZKŮ	9
SEZNAM ZKRATEK	10
ÚVOD.....	11
1. Úvod do zabezpečení objektů, popis, druhy	12
1.1. Problematika bezpečnosti objektu	13
1.2. Rozdělení objektů	15
1.3. Druhy zabezpečení objektů.....	16
2. Popis firmy a současného stavu	18
2.1. Popis současného zabezpečení	18
2.2. Organizační struktura.....	19
2.3. Finanční situace	20
2.4. Mise a vize.....	20
2.5. Cíle.....	20
2.6. SWOT analýza.....	22
2.6.1. Popis aspektů	22
2.6.2. Strategie	24
2.7. Analýza rizik a zranitelných míst	26
2.8. Opatření pro zvýšení bezpečnosti.....	27
3. Definice rozhodovacího procesu, stanovení kritérií a variant	30
3.1. Rozhodovací proces.....	30
3.2. Omezující podmínky	31
3.3. Hodnotící kritéria.....	32
3.4. Varianty	34
3.5. Rozhodovací tabulka	37
4. Řešení rozhodovacího problému pomocí metod vícekritériálního rozhodování	38
4.1. Stanovení vah kritérií.....	38
4.2. Ohodnocení variant.....	42
4.3. Porovnání výsledků	49
4.4. Doporučená varianta.....	51
Závěr	52
Použitá literatura	53
Seznam příloh	56

SEZNAM TABULEK

Tabulka 1 – SWOT analýza.....	22
Tabulka 2 – Rozhodovací tabulka	37
Tabulka 3 – Tabulka kritérií	38
Tabulka 4 – Tabulka variant	38
Tabulka 5 – Přímá metoda bodovací	39
Tabulka 6 – Váhy kritérií nepřímou metodou (Fullerovou)	39
Tabulka 7 – Intenzita relativních důležitostí.....	40
Tabulka 8 – Váhy kritérií nepřímou metodou (Saatyho).....	40
Tabulka 9 – hodnoty pro kritéria dle Saatyho metody.....	41
Tabulka 10 – Dílčí ohodnocení variant Fullerovou metodou pro K1	42
Tabulka 11 – Dílčí ohodnocení variant Fullerovou metodou pro K2	42
Tabulka 12 – Dílčí ohodnocení variant Fullerovou metodou pro K3	42
Tabulka 13 – Dílčí ohodnocení variant Fullerovou metodou pro K4.....	43
Tabulka 14 – Dílčí ohodnocení variant Fullerovou metodou pro K5.....	43
Tabulka 15 – Dílčí ohodnocení variant Fullerovou metodou pro K6.....	43
Tabulka 16 – Celkové ohodnocení variant Fullerovou metodou.....	44
Tabulka 17 – Dílčí ohodnocení variant Saatyho metodou pro K1	44
Tabulka 18 – Intenzita relativních důležitostí pro K1	45
Tabulka 19 – hodnoty pro kritéria dle Saatyho metody pro K1	45
Tabulka 20 – Dílčí ohodnocení variant Saatyho metodou pro K2	45
Tabulka 21 – Intenzita relativních důležitostí pro K2	45
Tabulka 22 – hodnoty pro kritéria dle Saatyho metody pro K2	46
Tabulka 23 – Dílčí ohodnocení variant Saatyho metodou pro K3	46
Tabulka 24 – Intenzita relativních důležitostí pro K3	46
Tabulka 25 – hodnoty pro kritéria dle Saatyho metody pro K3	46
Tabulka 26 – Dílčí ohodnocení variant Saatyho metodou pro K4	47
Tabulka 27 – Intenzita relativních důležitostí pro K4	47
Tabulka 28 – hodnoty pro kritéria dle Saatyho metody pro K4	47
Tabulka 29 – Dílčí ohodnocení variant Saatyho metodou pro K5	47
Tabulka 30 – Intenzita relativních důležitostí pro K5	48
Tabulka 31 – hodnoty pro kritéria dle Saatyho metody pro K5	48
Tabulka 32 – Dílčí ohodnocení variant Saatyho metodou pro K6	48
Tabulka 33 – Intenzita relativních důležitostí pro K6	48
Tabulka 34 – hodnoty pro kritéria dle Saatyho metody pro K6	49
Tabulka 35 – Celkové ohodnocení variant Saatyho metodou	49

SEZNAM OBRÁZKŮ

Obrázek 1 – Statistický přehled kriminality	12
Obrázek 2 – Organizační diagram	19
Obrázek 3 – Analýza rizik	26
Obrázek 4 – Výpočet λ_{\max}	41
Obrázek 5 – Graf porovnání vah kritérií jednotlivých metod.....	50
Obrázek 6 – Graf porovnání variant jednotlivých metod	50
Obrázek 7 – Hodnocení rizik	57
Obrázek 8 – Hodnoty RI	58

SEZNAM ZKRATEK

AI	Umělá inteligence
APS	Automatický parkovací systém
BOZP	Bezpečnost a ochrana zdraví při práci
CCTV	Uzavřený televizní okruh
CNC	Počítačové číslicové řízení
CR	Konzistenční poměr
EMS	Systém environmentálního managementu
EZS	Elektronický zabezpečovací systém
GDPR	Obecné nařízení o ochraně osobních údajů
HW	Hardware
ICT	Informační a komunikační technologie
ISO	Mezinárodní organizace pro normalizaci
IT	Informační technologie
OOPP	Osobní ochranné pracovní prostředky
OP PIK	Operační program Podnikání a inovace pro konkurenceschopnost
OP TAK	Operační program Technologie a aplikace pro konkurenceschopnost
OPPI	Operační program Podnikání a inovace
OSHA	Evropská agentura pro bezpečnost a ochranu zdraví při práci
PHM	Pohonné hmoty
PO	Požární ochrana
PZS	Poplachový zabezpečovací systém
QMS	Systém managementu kvality
RI	Náhodný konzistenční index
SPZ	Státní poznávací značka
SW	Software

ÚVOD

V dnešním dynamicky se vyvíjejícím světě je zabezpečení firmy klíčovým aspektem, který nemůže být přehlížen. S rostoucími hrozbami jak z fyzického, tak z kybernetického prostředí, je nezbytné, aby se organizace aktivně zaměřovaly na efektivní metody ochrany svého majetku, informací a lidí. Tato bakalářská práce se zaměřuje na návrh bezpečnostních řešení pro středně velkou strojírenskou společnost, která čelí specifickým bezpečnostním výzvám vyplývajícím z její velikosti, specifického charakteru činnosti a organizační struktury. V rámci této práce nejde pouze o návrh bezpečnostního systému založeného na dostupných technologiích, ale také o zahrnutí důkladné SWOT analýzy a analýzy rizik a zranitelných míst. Tyto analýzy jsou zásadní pro pochopení specifických hrozeb a slabých míst, kterým firma může čelit. Na základě těchto poznatků je možné navrhnout nejenom technicky adekvátní řešení, ale také vypracovat strategie pro efektivní řízení rizik. Tento komplexní přístup umožňuje nejen pasivně reagovat na současné bezpečnostní výzvy, ale i aktivně předcházet možným budoucím problémům. Analytický základ představuje cenný přínos v podobě strategických doporučení, která podporují dlouhodobou udržitelnost a zvyšují konkurenceschopnost firmy v dynamicky se vyvíjejícím prostředí.

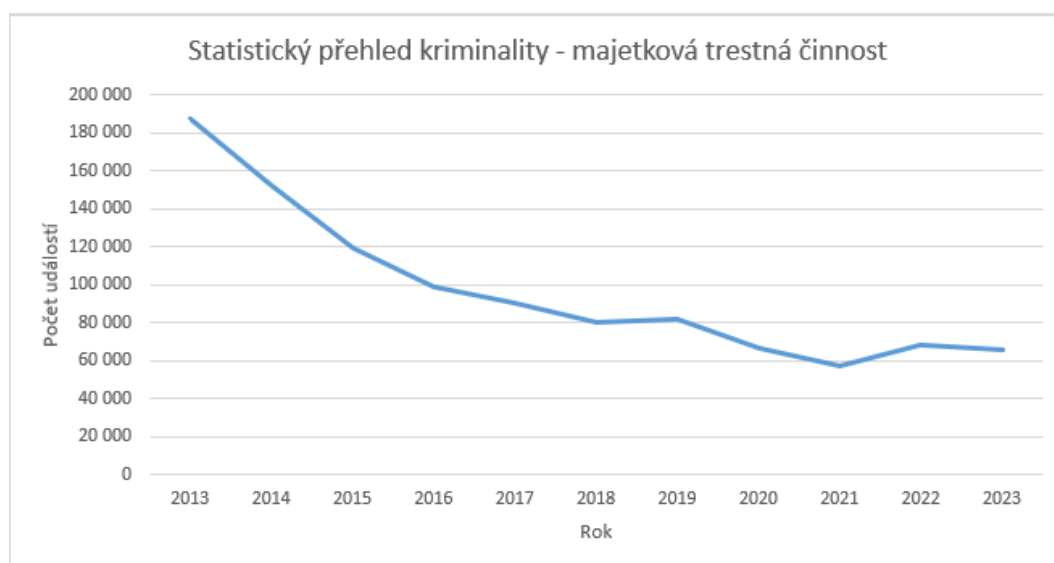
Cílem práce je definovat slabá místa v zabezpečení firmy, identifikovat možnosti zabezpečení a pomocí metod vícekritériálního rozhodování navrhnout vhodné zabezpečení. Dílčí kroky zahrnují vypracování SWOT analýzy a strategií, analýzu rizik a zranitelných míst, která vede k identifikaci specifických opatření pro zvýšení bezpečnosti. V rámci rozhodovacího procesu budou stanoveny omezující podmínky, kritéria a varianty pro návrh zabezpečení.

1. Úvod do zabezpečení objektů, popis, druhy

V současné době je riziko různých forem napadení, ať už kriminálních nebo teroristických, velmi vysoké, s motivacemi sahajícími od náboženských po ziskové. Z toho důvodu se efektivní zabezpečení objektů stává základní potřebou. Objektová bezpečnost zahrnuje technickou a personální ostrahu, která minimalizuje riziko napadení a zajišťuje ochranu citlivých informací. Při návrhu bezpečnostních systémů je klíčové počítat s motivací a metodami potenciálních pachatelů, aby bylo zajištěno, že překážky a čas potřebný k jejich překonání jsou nastaveny co nejlépe. [14]

Na pracovišti i v osobním životě je základem bezpečnosti povědomí o rizicích a hrozbách. Toto povědomí je nezbytné pro vývoj efektivních bezpečnostních programů. Každá organizace, ať už se jedná o podnik, školu, církev, nemocnici, či jiný typ organizace, která chce implementovat bezpečnostní plán, musí mít jasno o svém postavení v kontextu bezpečnosti. To zahrnuje pochopení rizik, kterým je vystavena, identifikaci možných problémů a vybudování základního zaměření na bezpečnost. Jedním z prvních kroků k zajištění bezpečnosti v organizaci je proto akceptování, že bezpečnost je základní součástí jejího fungování, identifikace toho, co je třeba chránit, a vytvoření přehledu o aktuálním stavu bezpečnosti nebo ochrany klíčových oblastí. [34]

Policejní statistiky sice ukazují mírně klesající trend majetkové trestné činnosti, jak ukazuje Obrázek 1, to ale neznamená, že můžeme bezpečnost svoji nebo podnikovou podceňovat nebo dokonce zcela ignorovat.



Obrázek 1 – Statistický přehled kriminality

Zdroj: [31]

1.1. Problematika bezpečnosti objektu

Předtím, než se zaměřím na bezpečnost objektu, je důležité pochopit několik širších pojmů. Podle Maslowovy pyramidy lidských potřeb [16] je bezpečnost druhou nejdůležitější potřebou člověka hned po základních fyziologických potřebách. Potřeby sdružení, uznání a seberealizace jsou až na dalších příčkách. Bezpečnost je základní hodnota lidské společnosti, která zajišťuje její přežití a rozvoj. Výklad termínu "bezpečnost" může být politický, vojenský, filozofický, či technický a nabývá konkrétního významu až ve spojení s určitým předmětem. V kontextu bezpečnosti objektu firmy je bezpečnost výsledkem analýzy rizik, zranitelných míst a opatření pro zvýšení bezpečnosti, která je plně v kompetenci pověřených osob. [14]

Primárním cílem zabezpečení objektů je minimalizace rizika škody na majetku a ochrana životů a zdraví osob. Tento cíl je dosahován prostřednictvím komplexního přístupu, který zahrnuje fyzické a technické bezpečnostní opatření, jako jsou systémy kontroly přístupu a video dohled. Pravidelné bezpečnostní audity jsou nezbytné pro identifikaci a řešení potenciálních zranitelností, to umožňuje neustálé zlepšování bezpečnostních strategií. Efektivní zabezpečení zahrnuje vícevrstevnou strategii a plánování odolnosti, které předchází nejen přímým hrozbám, ale také zvyšuje schopnost objektu rychle se zotavit po krizových událostech. [33]

Hodnota systému ochrany je definována jako soubor charakteristik, které systém činí efektivním ve splnění legitimních a očekávaných potřeb zainteresované strany, jako je například majitel objektu. Tyto atributy zajistí, že daný objekt bude v konkrétním prostředí, čase a za určitým účelem chráněný. Úspěšné nalezení optimální ochrany znamená identifikaci řešení, které je nejen spolehlivé, ale také ekonomicky výhodné a schopné uspokojit většinu funkčních požadavků na bezpečnostní systém daného objektu. [15]

Základy teorie bezpečnosti lze zkoumat z několika perspektiv, které zahrnují rozličné aspekty bezpečnostních studií. Teorie bezpečnosti je multidisciplinární oblast, která se vyvíjí na pomezí mezi různými vědeckými disciplínami, jako jsou policejní vědy a strategické studie. Tento obor se zabývá analýzou hrozeb a rizik, které mohou ohrozit bezpečnost konkrétních entit, ať už jsou to státy, organizace nebo jednotlivci. Rozlišuje se mezi statickou a dynamickou bezpečností, kde statická bezpečnost se zaměřuje na udržení současného stavu entity bez ohrožení její struktury a funkcí, zatímco dynamická bezpečnost se soustředí na ochranu rozvoje a evoluce entity. [32]

V rámci České republiky se základy teorie bezpečnosti odrážejí také ve strategických dokumentech, které adresují například kybernetickou bezpečnost, ochranu kritické

infrastruktury a vnitřní bezpečnost. Důležité je, že každá bezpečnostní strategie musí být průběžně přehodnocována a aktualizována, aby reflektovala neustále se měnící charakter hrozeb a rizik, kterým čelí. [21]

Bezpečnost je možno považovat za mnohostrannou vlastnost prostředí, která je vnímána jako výsledek hodnocení různých bezpečnostních faktorů, často označovaných jako dílčí bezpečnosti. Tyto faktory zahrnují personální, objektovou, organizační, transportní, režimovou, administrativní, technickou a infromatickou bezpečnost, každý s vlastními specifickými riziky a metodami hodnocení. Personální bezpečnost je považována za relativně nestabilní kvůli vysoké možnosti subjektivního ovlivnění člověka. Objektová a transportní bezpečnost se zaměřují na analýzu a snižování rizik spojených s fyzickými objekty nebo přepravními prostředky. Organizační bezpečnost zahrnuje pravidla a postupy upravující provozní činnosti. Režimová bezpečnost se vztahuje k pravidlům ovlivňujícím denní chod a bezpečnostní protokoly v organizaci. Administrativní bezpečnost je regulována zákony a vnitřními předpisy, zatímco technická bezpečnost se soustředí na ochranné zařízení a infrastrukturu. Infromatická bezpečnost je klíčová pro ochranu dat a informačních systémů a zahrnuje principy jako dostupnost, důvěrnost, integrita a odpovědnost. Každý typ bezpečnosti vyžaduje specifické přístupy k hodnocení a managementu rizik. [14]

Kybernetická bezpečnost je komplexní oblast, která zahrnuje ochranu systémů, sítí a programů před digitálními útoky, které mohou mít za cíl získání přístupu, modifikaci nebo zničení citlivých informací, vyžadování výkupného prostřednictvím ransomwaru, nebo narušení běžných obchodních procesů. Efektivní kybernetická bezpečnost zahrnuje různé technologie a nejlepší praktiky, které pomáhají organizacím snížit jejich zranitelnost vůči kybernetickým útokům a chránit jejich kritické informační systémy. Důležitost kybernetické bezpečnosti není omezena pouze na velké organizace nebo oddělení informačních technologií (IT). Každý jednotlivec, který využívá jakékoliv informační a komunikační technologie (ICT) a připojuje se k internetu, hraje klíčovou roli ve své vlastní kybernetické bezpečnosti. To zahrnuje běžné aktivity, jako je používání silných hesel, aktualizace softwaru a opatrné nakládání s osobními a citlivými údaji na internetu. Vzhledem k tomu, že kybernetické hrozby neustále vyvíjejí, je nutné neustále se vzdělávat o nových hrozbách a praktikách obrany. Celkově je kybernetická bezpečnost nezbytná pro ochranu soukromí, osobní a finanční bezpečnosti jednotlivců, jakož i pro ochranu operací, reputace a finančního zdraví organizací. Proto je důležité, aby všichni, od jednotlivců po velké korporace, přistupovali ke kybernetické

bezpečnosti proaktivně a s důrazem na neustálé zlepšování svých bezpečnostních opatření a protokolů. [11]

Bezpečnost a ochrana zdraví při práci (BOZP) a požární ochrana (PO) jsou v České republice příklady specificky regulovaných oblastí bezpečnosti, které vyžadují soulad s národními zákony a normami. V oblasti BOZP se rozlišují čtyři kategorie pracovních rizik od nejnižší, kde neexistují významnější rizika pro zaměstnance, po nejvyšší, kde jsou rizika tak významná, že i s použitím osobních ochranných prostředků (OOPP) může dojít ke zdravotnímu poškození v důsledku nadprahových zátěží. Na druhé straně, požární ochrana je závazně regulována a zahrnuje komplexní ustanovení na prevenci požárů, přičemž objekty jsou kategorizovány na základě úrovně požárního nebezpečí od těch bez zvýšeného požárního nebezpečí po objekty s vysokým požárním nebezpečím, to určuje míru potřebných preventivních opatření. Tyto systémy jsou nezbytné pro zajištění ochrany životů a zdraví na pracovišti a předcházení škodám na majetku. [1][2]

1.2. Rozdělení objektů

Pojem "objekt" může být chápán ve více rovinách – od celé budovy, přes jednotlivá patra, až po specifické místnosti. Bezpečnostní opatření navrhovaná pro tyto objekty by měla být efektivní v odrazení potencionálních narušitelů a v prevenci krádeže majetku. Při volbě těchto opatření je klíčové zvážit poměr mezi kvalitou, intenzitou zabezpečení a náklady na jejich implementaci. [14]

Objekty lze dále kategorizovat do několika základních skupin [14]:

- veřejný sektor: zahrnuje instituce státní správy a samosprávy,
- retail: od běžných prodejen, supermarketů, až po hypermarkety a obchodní domy,
- finanční instituce, banky: tyto objekty vyžadují speciální zabezpečení kvůli manipulaci s penězi a citlivými daty,
- průmysl a zemědělství: zde se často vyskytuje velký počet osob pohybujících se v areálu, to klade specifické požadavky na zabezpečení, zabezpečení musí být navrženo s ohledem na finanční možnosti a technické kapacity firmy, stejně jako na doporučení pojišťovny,
- bydlení, občanské stavby: tato kategorie zahrnuje rezidenční objekty a budovy občanské vybavenosti,
- „inteligentní“ budovy: tyto moderní budovy mají technologie pro zvýšení efektivity a bezpečnosti.

Všechny tyto kategorie mají různé požadavky a přístupy k zabezpečení, které se musí přizpůsobit charakteru objektu a jeho využití. Při plánování bezpečnostních opatření je důležité brát v úvahu nejen současnou funkci objektu, ale i potenciální rizika a hrozby, kterým může být vystaven.

1.3. Druhy zabezpečení objektů

Fyzické zabezpečení – plánování fyzické bezpečnosti může být zdánlivě náročný úkol, zejména když mnoho společností dnes klade důraz především na kybernetickou bezpečnost. Nicméně, plány fyzické bezpečnosti by měly být na stejné úrovni priority, protože jejich účelem je ochrana lidí, majetku a aktiv. Efektivní fyzická bezpečnost zahrnuje kombinaci různých opatření od jednoduchých zámků až po biometrické přístupové systémy, osvětlení, video kamery, a další. Fyzická bezpečnost není jen o „strážcích a branách“; moderní systémy fyzické bezpečnosti zahrnují více prvků a opatření, jako jsou [30]:

- konfigurace bezpečnosti lokality: identifikace slabých míst a nejvíce chráněných oblastí,
- viditelnost kritických oblastí: zajištění dostatečného osvětlení a video dohledu,
- kontrola přístupu: od jednoduchých zámků po klávesnice a biometrické systémy,
- ochrana obvodu: opatření pro zamezení neoprávněného vstupu,
- detekce průniku: včetně senzorů pohybu, kamer a alarmů,
- ochrana infrastruktury: zahrnuje elektrické, vodní a síťové systémy,
- školení zaměstnanců a reakce na incidenty: připravenost zaměstnanců na různé bezpečnostní incidenty.

Poplachový bezpečnostní systém (PZS) - elektronický systém navržený k detekci a signalizaci nežádoucích událostí v kontrolované oblasti, tedy místem pod kontrolou majitele, kde se nachází chráněný majetek. Nežádoucí události obvykle zahrnují vniknutí neoprávněných osob (například vloupání), pokusy o únik z oblasti (jako útěk z věznice), nebo neoprávněné manipulace se střeženými objekty (například sejmutí obrazu z galerie). Současné poplachové systémy mohou zahrnovat také detektory pro identifikaci požárů, úniků vody, nebezpečných plynů a dalších nevhodných či nebezpečných podmínek, které mohou v kontrolované oblasti vzniknout. Kromě těchto incidentů systém může detekovat i tzv. tísňové události, to jsou situace zdravotního ohrožení osob nebo násilí páchané na osobách v této oblasti. [3]

Elektronické zabezpečení – zahrnuje systémy jako je video dohled, systémy pro detekci pohybu a další technologie, které pomáhají identifikovat a reagovat na bezpečnostní incidenty. V současné době se stále více klade důraz na sjednocování fyzické a kybernetické bezpečnosti,

kde jsou ochranné systémy integrovány s infrastrukturou IT organizace pro lepší reakci na hrozby. V technologii kamer pro uzavřený televizní okruh (CCTV) jsou trendy pro rok 2024 zaměřeny na zlepšení bezpečnosti a efektivity prostřednictvím pokročilých technologií a integrovaných řešení, to umožňuje organizacím flexibilně a škálovatelně růst v oblasti bezpečnosti. Dalšími klíčovými trendy jsou cloudové řešení, video analýzy poháněné umělou inteligencí (AI) a přechod z analogových na 100% digitální video systémy. [29]

Organizační a právní ochrana – týká se implementace interních pravidel, politik, postupů a školení zaměstnanců, které jsou zaměřeny na ochranu majetku a dodržování právních a regulačních požadavků. To může zahrnovat dodržování standardů jako je obecné nařízení o ochraně osobních údajů (GDPR) pro ochranu dat nebo pro bezpečnost na pracovišti dle evropské agentury pro bezpečnost a ochranu zdraví při práci (OSHA) nebo pro systémy řízení informační bezpečnosti dle normy ČSN EN ISO/IEC 27001 [7] vydané mezinárodní organizací pro normalizaci (ISO). [20][26][27][28]

Každý z těchto druhů ochrany majetku a osob hraje důležitou roli v komplexním bezpečnostním plánu organizace a vyžaduje průběžnou revizi a aktualizaci, aby držel krok s neustále se vyvíjejícími hrozbami a technologiemi.

2. Popis firmy a současného stavu

Společnost MONTIFER s.r.o. je středně velká společnost zabývající se strojírenskou výrobou. Založena byla roku 1995. Výrobní a montážní prostory, které má firma k dispozici činí 40.0000 m². V současnosti zaměstnává 150 pracovníků. Firma má od roku 1999 zaveden systém managementu kvality ČSN EN ISO 9001 [4] a od roku 2013 také systém environmentálního managementu ČSN EN ISO 14001 [6]. [22]

Firma se díky čerpání dotačních výzev z Operačního programu Podnikání a inovace (OPPI) [19] a Operačního programu Podnikání a inovace pro konkurenceschopnost (OP PIK) [17] stala opět více soběstačnou, protože ke stávajícímu vybavení přidala CO₂ laser, horizontální a portálový počítačem řízený (CNC) obráběcí stroj, 3D měřicí rameno, pulsní svářečky a software (SW) s hardwarem (HW) pro vývoj a programování vlastního produktu – automatického parkovacího systému (APS) pod značkou MONTIPARK. [9]

2.1. Popis současného zabezpečení

Současný stav zabezpečení firmy je založen na několika klíčových systémech, které sice poskytují základní úroveň ochrany, ale s technologickým vývojem a rostoucími bezpečnostními požadavky mohou být nedostatečné. Aktuální bezpečnostní infrastruktura zahrnuje:

Analogové kamerové systémy

Analogové kamerové systémy sloužící jako dohled nad prostory. Tyto systémy mají nižší rozlišení obrazu, to je limitující při potřebě identifikace osob nebo detailů v záznamech, které jsou omezeny na 5 dní z důvodu velikosti úložného zařízení tohoto systému. Je vhodný pro základní monitorování oblastí, ale jeho efektivita v noci nebo za špatných světelných podmínek je omezená kvůli absenci pokročilých funkcí jako je noční vidění nebo dynamické rozsahy osvětlení.

Elektronický docházkový systém

Firma používá elektronický systém pro evidenci docházky zaměstnanců, to pomáhá udržovat přehled o pracovní době a přítomnosti na pracovišti a také jako dohled nad dodržování přestávek. Tento systém je základní a je určen primárně k administrativním účelům. Jeho integrace s bezpečnostními systémy není žádná, to znamená, že neposkytuje další bezpečnostní funkce, jako například kontrolu přístupu do citlivých oblastí.

Starý systém elektronického zabezpečení (EZS)

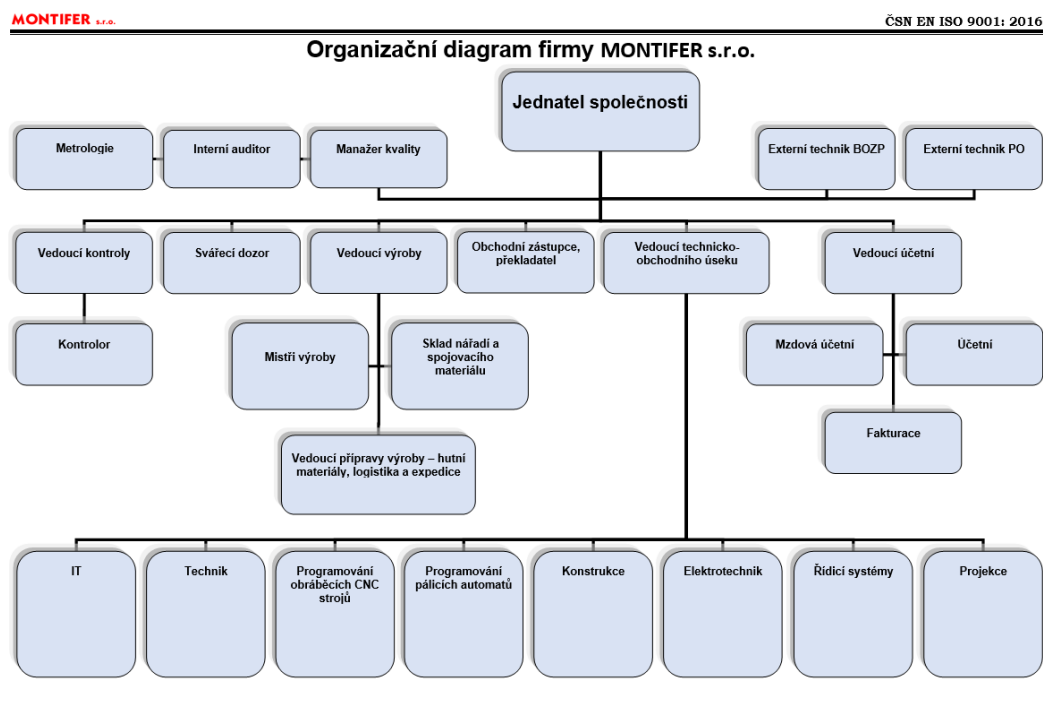
V současnosti je v provozu starší verze elektronického zabezpečovacího systému JABLOTRON, který je nastaven tak, že chrání celý vnitřní prostor pomocí pouze dvou pohybových čidel. Tento systém může být efektivní pro detekci neoprávněného vstupu v oblastech, kde jsou čidla instalována, ale neposkytuje komplexní pokrytí všech rizikových zón.

Celkové hodnocení

Ačkoliv současné zabezpečovací systémy poskytují základní úroveň ochrany, existuje několik oblastí, které by mohly být vylepšeny pro zvýšení celkové bezpečnosti. Modernizace analogových kamer na systémy digitální s vyšším rozlišením a nočním viděním, integrace docházkového systému s pokročilými systémy kontroly přístupu a aktualizace starého EZS na modernější a komplexnější řešení by mohla výrazně zlepšit schopnost firmy chránit své majetky, zaměstnance a operace.

2.2. Organizační struktura

Společnost MONTIFER s.r.o. má klasický model hierarchické struktury, kde jsou jasně definované úrovně od nejvyššího vedení až po řadové zaměstnance, jak zobrazuje Obrázek 2.



Obrázek 2 – Organizační diagram

Zdroj: [24]

2.3. Finanční situace

Společnost MONTIFER s.r.o. je vlastněná Milanem Kobrem (53,44 %) a firmou KASI spol. s r.o. (46,56 %). Jednateli jsou Milan Kobr, Ladislav Lhoták a Ing. Stanislav Ulm s právem jednat samostatně. [10]

Od svého působení si společnost vytvořila kvalitní obchodní vztahy s mnoha zákazníky a další nové vztahy usilovně a průběžně buduje. I přes obtíže s dodávkami materiálu, dodávkami subdodávek a pracovní silou v souvislosti s pandemií COVID 19 a válkou na Ukrajině je s obratem kolem 150 milionů Kč [10] finanční situace stabilní.

2.4. Mise a vize

Misí společnosti MONTIFER s.r.o. je poskytovat inovativní a kvalitní řešení v oblasti strojírenství, která plně vyhovují požadavkům a očekáváním zákazníků. Zavazuje se k dodávání výrobků a služeb, které nejenže splňují standardy kvality, ale také přispívají k efektivitě a produktivitě klientů. Firma je založena na hodnotách jako jsou inovace, spolehlivost a udržitelnost, díky kterým buduje pevné vztahy se zákazníky a partnery.

Vizí společnosti MONTIFER s.r.o. je být uznávaným lídrem v technologických inovacích a výrobních řešeních v oblasti strojírenství na domácím i mezinárodním trhu. Usiluje o stálé zlepšování svých technologických procesů a vývoj produktů, které jsou šetrné k životnímu prostředí a přinášejí maximalizaci hodnoty pro zákazníky. Cílí na rozšíření působnosti na nové trhy a rozšíření produktového portfolia, aby odpovídalo nejnovějším trendům a potřebám průmyslu.

2.5. Cíle

Politikou firmy MONTIFER s.r.o. je zpracovávání takových výrobků, které obstojí v konkurenci a svou kvalitou a cenou uspokojí potřeby zákazníků. Neustálé zlepšování kvality výroby je hlavním předpokladem pro vytváření dlouhodobých a trvalých vztahů se zákazníky. Pro zvyšování úrovně svého environmentálního chování s dopadem na životní prostředí se firma rozhodla zavést systém environmentálního managementu dle normy ČSN EN ISO 14001 [6].

Politika kvality (QMS) a environmentální politika (EMS) společnosti MONTIFER s.r.o. vytváří trvale potřebné a organizační, finanční a personální zdroje pro rozvíjení a zlepšování

systemu managementu kvality. Vytváří cíle společnosti a aktivní přístup k neustálému zlepšování v oblasti kvality a snižování zátěže na životní prostředí.

Pro rok 2024 jsou stanoveny tyto cíle v oblasti **QMS** [23]:

- rozšíření počtu svářečů s certifikátem svářeče dle ČSN EN ISO 9606-1 [5] z vlastních řad,
- aktualizace webových stránek,
- navýšení počtu zaměstnanců výroby,
- rozvoj lidských zdrojů – školení:
školení všech zaměstnanců ČSN EN ISO 9001 [4],
školení pro účetní,
školení pro personalisty,
školení pro konstruktéry,
- obnova infrastruktury:
nákup nového autogenního pálicího stroje kombinovaného s plazmovým hořákem,
modernizace HW,
modernizace SW,
- snížení reklamovosti o 15 %,
- rozšiřování zákaznického portfolia,
- inovace dílčích celků APS.

Pro rok 2024 jsou stanoveny tyto cíle v oblasti **EMS** [23]:

- rozvoj lidských zdrojů – školení:
školení všech zaměstnanců ČSN EN ISO 14001 [6],
- zvýšení havarijní připravenosti,
- snížení spotřeby elektrické energie,
- snížení spotřeby plynu.

Pro rok 2024 jsou stanoveny tyto cíle v oblasti **BOZP** [23]:

- snížení hlučnosti na hale výroby,
- zlepšení světelných podmínek na halách, v lakovně,
- snížení počtu pracovních úrazů o 10 %.

2.6. SWOT analýza

SWOT analýza je strategický plánovací nástroj používaný k identifikaci a analýze klíčových faktorů ovlivňujících organizaci. Tento nástroj pomáhá organizacím ve vývoji strategií tím, že poskytuje jasný přehled o jejich interních (silné a slabé stránky) a externích (příležitosti a hrozby) aspektech. [12]

Tabulka 1 ukazuje SWOT analýzu společnosti MONTIFER s.r.o.

Tabulka 1 – SWOT analýza

Silné stránky (S)	Slabé stránky (W)
zkušený tým široká škála služeb vysoké standardy kvality úspěšná historie projektů přizpůsobivost a inovativní přístup	závislost na dodavatelích potřeba aktualizace technologií nedostatečná online přítomnost a digitalizace vysoká fluktuace zaměstnanců slabé zabezpečení
Příležitosti (O)	Hrozby (T)
expanze na mezinárodní trhy dotační výzva Technologie 4.0 dotační výzva Inovace rostoucí poptávka po ekologicky šetrných řešeních	ekonomické poklesy růst cen materiálů zvýšená konkurence regulační změny

Zdroj: vlastní zpracování na základě konzultace s vedením firmy

2.6.1. Popis aspektů

Silné stránky (S):

- zkušený tým – jednou z největších výhod společnosti MONTIFER s.r.o. je tým odborníků s bohatými zkušenostmi v oboru strojírenství, tento tým je základem pro vysokou kvalitu a inovativnost produktů a služeb,
- široká škála služeb – společnost MONTIFER s.r.o. nabízí komplexní portfolio služeb, které pokrývají celý životní cyklus strojírenských projektů, od návrhu a vývoje po výrobu, montáž a servis, toto rozložení služeb umožňuje oslovit širší spektrum zákazníků,
- vysoké standardy kvality – společnost MONTIFER s.r.o. klade velký důraz na kvalitu, to se odráží na vysoké úrovni produktů a služeb, je to klíčový faktor pro zajištění zákaznické spokojenosti a budování dlouholetých vztahů,

- úspěšná historie projektů – tato historie slouží jako důkaz schopností společnosti MONTIFER s.r.o. plnit komplexní a technicky náročné požadavky zákazníků,
- přizpůsobivost a inovativní přístup k řešení problémů – v dynamickém prostředí strojírenského průmyslu je schopnost rychle reagovat na změny a vyvíjet kreativní řešení kritická. Společnost MONTIFER s.r.o. využívá týmový přístup k problematice a spolupráci na vývoji nových produktů a technologií, které nejenže splňují, ale často i překračují očekávání zákazníků. Tato schopnost neustálého inovování a přizpůsobování se změnám na trhu pomáhá firmě udržet si konkurenční výhodu a podporuje její dlouhodobý růst.

Slabé stránky (W):

- závislost na dodavatelích – závislost na dodavatelích hutního materiálu a subdodávek může vést k problémům s dodávkami nebo zvýšení nákladů v případě narušení dodavatelského řetězce,
- potřeba aktualizace technologií – aby zůstala konkurenceschopná, musí firma neustále investovat do nejnovějších technologií a inovací. Zpoždění v této oblasti by mohlo vést ke ztrátě konkurenční výhody,
- nedostatečná online přítomnost a digitalizace – nevyužívání nebo jen částečné využívání digitálního marketingu nebo sociálních médií, může ztrácet na důležitosti v očích digitálně zdatnějších zákazníků a zaostávat za konkurenty. Nedostatečná digitalizace procesů může také vést k nižší interní efektivitě a vyšším provozním nákladům,
- vysoká fluktuace zaměstnanců – vysoká míra fluktuace zaměstnanců může být značnou slabostí. Klíčovým faktorem pro řešení této slabosti je vytvoření atraktivního pracovního prostředí, kde se zaměstnanci cítí hodnotní a jsou odměňováni za svůj přínos k firmě,
- nedostatky v systémech fyzického i kybernetického zabezpečení, zvyšující riziko úniků dat, krádeží majetku a dalších bezpečnostních porušení. Nedostatečné zabezpečení může vést k finančním ztrátám, poškození pověsti a ztrátě důvěry zákazníků a obchodních partnerů.

Příležitosti (O):

- expanze na mezinárodní trhy – rozšíření působnosti na nové trhy by mohlo otevřít přístup k novým zákazníkům a zdrojům příjmů,
- dotační výzva Technologie 4.0 v rámci Operačního programu Technologie a aplikace pro konkurenceschopnost (OP TAK) [18] – příležitost investovat do nejnovějších

průmyslových technologií a automatizačních systémů souvisejících s konceptem Průmyslu 4.0. Využití dotace umožní firmě zmodernizovat své výrobní procesy, firemní sítě a bezpečnostní prvky, zvýšit efektivitu, snížit náklady, zlepšit kvalitu produktů a zlepšit zabezpečení,

- dotační výzva Inovace v rámci OP TAK [18] – finanční podpora pro projekty zaměřené na vývoj nových produktů nebo zlepšení existujících technologií. Je to významná příležitost k investici do výzkumu a vývoje, to může vést k vývoji technologií a produktů pod užitným vzorem, které by mohly otevřít nové segmenty trhu a posílit její tržní pozici. Využití této dotace by mohlo také znamenat zlepšení udržitelnosti a ekologické stopy společnosti skrze inovace zaměřené na zelené technologie,
- rostoucí poptávka po ekologicky šetrných řešeních – orientace na udržitelnost a ekologická řešení může získat nové zákazníky a otevřít nové trhy a zlepšit image.

Hrozby (T):

- ekonomické poklesy – hospodářské krize a recese mohou výrazně snížit poptávku po strojírenských produktech a službách,
- růst cen materiálů – zvýšení nákladů na suroviny a materiály může snížit marže a ziskovost,
- zvýšená konkurence – vstup nových hráčů na trh a technologický pokrok konkurentů mohou zvýšit konkurenční tlak,
- regulační změny – nové předpisy a normy mohou vyžadovat nákladné úpravy výrobních procesů nebo produktů, to může ovlivnit operace a finanční výkonnost firmy.

2.6.2. Strategie

Strategie SO:

- rozšíření na nové mezinárodní trhy – využití zkušeného týmu a úspěšné historie projektů k expanzi do nových zeměpisných oblastí,
- investice do technologií a vývoje – maximální využití dotační výzvy Technologie 4.0 a dotační výzvy Inovace, obě z OP TAK [18] k financování nákupu špičkových technologií a vývoje nových produktů. Tím se podpoří zlepšení interních procesů a zvýšení produktivity, ale také rozvoj nových, inovativních řešení, které mohou otevřít nové tržní segmenty a zvýšit konkurenceschopnost,

- rozvoj ekologicky šetrných produktů a služeb – využití inovativního přístupu k řešení problémů pro vývoj a nabídku produktů z oblasti elektromobility. Tímto způsobem lze reagovat na rostoucí poptávku po "zelených" řešeních a zlepšit svůj image na trhu.

Strategie ST:

- zvyšování odolnosti vůči ekonomickým poklesům – rozšíření trhů a služeb, využití široké škály služeb a úspěšnou historii projektů k expanzi na nové trhy a sektory, které mohou být méně citlivé na ekonomické kolísání. Rozvoj nových obchodních modelů, jako jsou konstrukční a projekční práce, služby po prodeji nebo údržba, může zvýšit stálé příjmy a snížit závislost na jednorázových velkých projektech,
- reakce na růst cen materiálů – strategické nákupy a dlouhodobé smlouvy, využití zkušeností a sítě dodavatelů k uzavření dlouhodobějších dodavatelských smluv za fixní ceny, aby se minimalizoval vliv zvyšujících se cen materiálů na zisk,
- obrana proti zvýšené konkurenci – inovace produktů, zaměření se na vysoké standardy kvality a inovace ve výrobě a službách. Vývoj unikátních řešení, která přesahují standardní nabídku konkurence, a využití odborných znalostí týmu k vytváření produktů a služeb s vysokou přidanou hodnotou, které jsou těžko napodobitelné,
- adaptace na regulační změny – pravidelné investice do odborného vzdělávání zaměstnanců, kteří pomohou předcházet potenciaálním dopadům nových zákonů, norem a vyhlášek na firmu a připravit strategie pro jejich zvládnání.

Strategie WO:

- zlepšení pracovního prostředí a snížení fluktuace zaměstnanců – prostřednictvím expanze na nové trhy a investic do inovací může firma získat nové zdroje příjmů, které umožní lepší odměňování a rozvoj zaměstnanců. Tím se může vytvořit atraktivnější pracovní prostředí, to pomůže snížit fluktuaci zaměstnanců a zvýšit celkovou spokojenost a produktivitu,
- posílení systémů fyzického a elektronického zabezpečení – implementace nejnovějších technologií získaných prostřednictvím dotačních výzev a inovačních projektů může zahrnovat i pokročilé bezpečnostní systémy, které by posílily fyzické i elektronické zabezpečení. Toto nejenže sníží riziko bezpečnostních incidentů, ale také zvýší důvěru zákazníků a obchodních partnerů v integritu firmy.

2.7. Analýza rizik a zranitelných míst

Analýza rizik a zranitelných míst je zásadním úkolem, který pomáhá identifikovat, hodnotit a řídit potencionální hrozby a slabá místa. Tento proces je nezbytný pro zajištění bezpečnosti, celkové odolnosti a schopnosti předcházet krizovým situacím. Obrázek 3 zobrazuje zpracovanou analýzu společnosti MONTIFER s.r.o. Rizika jsou rozdělena do 4 úrovní:

- bez rizika,
- mírné riziko,
- střední riziko,
- vysoké riziko.

Pro první dvě úrovně není požadovaná žádná akce, u úrovně střední riziko je akce doporučena a poslední úrovně vysoké riziko je akce nutná. Vysvětlivky k hodnocení a výpočtu rizik ukazuje Obrázek 7, který je v příloze A.

P.č.	Aspekt	Popis rizika	Míra rizika			
			P	Z	O	Mr
1.	Personální	podlehnouti praktikám sociálního inženýrství	2	3	4	24
		zneužití přístupových práv	1	4	2	8
		neoprávněné šíření důvěrných informací a dat	2	4	2	16
2.	Objektový	slabá místa v zabezpečení	4	5	3	60
		nedostatečně chráněné důležité přístupové body	4	5	3	60
		nedostatečné osvětlení a viditelnost	3	3	2	18
		kontrola pohybu osob	4	4	4	64
		kontrola pohybu vozidel	3	4	3	36
		kvalita stávajících bezpečnostních systémů	4	4	1	16
		základní fyzické bariéry	2	3	1	6
		reakce při incidentu	3	4	2	24
		antivirová bezpečnost	3	3	3	27
3.	Technicko - informační	SW bezpečnost	2	3	3	18
		fyzická ochrana HW	3	5	4	60
		zabezpečení dat	4	3	3	36
		síťová bezpečnost	3	3	3	27
		aktualizace a údržba	2	2	1	4
		zálohování a obnova	5	5	2	50
		zabezpečení koncových bodů	2	3	2	12
4.	BOZP	výdej OOPP	2	5	1	10
		dodržování pravidel BOZP	3	5	1	15
5.	PO	systémy detekce a alarmu	4	5	4	80
		přístupnost a únikové cesty	3	5	2	30

Vysoké riziko	>50
Střední riziko	30+50
Mírné riziko	10+29
Bez rizika	<10

Obrázek 3 – Analýza rizik

Zdroj: vlastní zpracování

2.8. Opatření pro zvýšení bezpečnosti

Na základě 2. bodu strategie WO ze SWOT analýzy a analýzy rizik bylo identifikováno několik bodů, které jsou potřeba vyřešit. V následujících kapitolách se budu věnovat řešení problému se systémem detekce a alarmu při požáru, s elektronickým zabezpečovacím a přístupovým systémem a kamerovým systémem. Zásadní je přijmout konkrétní opatření, aby se zvýšila bezpečnost objektu. Níže jsou popsána opatření pro každý z těchto systémů.

Systém detekce a alarmu při požáru

Instalace detektorů kouře a tepla, které rychle detekují potenciální požáry a jsou méně náchylné k falešným alarmům. Systém bude propojen s centrálním EZS, který umožňuje okamžité odeslání upozornění a spuštění alarmu pro zajištění rychlé evakuace zaměstnanců a návštěvníků. Tyto systémy budou umístěny na všech klíčových místech a v počtech kusů určených expertním posudkem, který vychází z dlouhodobé znalosti objektu a znalosti předchozích výskytů bezpečnostních incidentů:

- sklad barev a ředidel – 1 ks,
- sklad drobného nářadí, měřidel, úklidových prostředků – 1 ks,
- vybrané kanceláře – 9 ks,
- místnost archivu – 1 ks,
- místnost serverovny – 1 ks,
- místnost zálohovacího zařízení – 1 ks,
- racková místnost 1 – 1 ks,
- racková místnost 2 – 1 ks,
- kotelna velká – 1 ks,
- kotelna malá – 1 ks.

Elektronický zabezpečovací a přístupový systém

Instalace elektronického přístupového systému poskytuje vyšší úroveň zabezpečení a omezuje neautorizovaný přístup, zároveň ukládá záznamy o všech přístupových událostech, díky čemuž lze zjistit podrobnosti v případě bezpečnostních incidentů. Tento systém také umožňuje vzdálené upravování a přidávání přístupových oprávnění a monitorování v reálném čase, a tak lze rychle reagovat na jakékoli bezpečnostní hrozby. Elektronický přístupový systém by měl být plně integrován s celkovým systémem elektronického zabezpečení objektu pro dosažení komplexní ochrany. Integrace umožňuje, aby v případě detekce neoprávněného přístupu došlo k automatické aktivaci dalších bezpečnostních opatření, jako jsou alarmy,

odeslání upozornění kompetentním osobám nebo blokace dveří díky čemuž se zvýší celková účinnost systému ochrany. Tyto systémy budou umístěny na všech klíčových místech a v počtech kusů určených expertním posudkem, který vychází z dlouhodobé znalosti objektu a znalosti předchozích výskytů bezpečnostních incidentů:

- ústředna EZS – 1 ks,
- dveřní přístupové body – 7 ks (serverovna, archiv, zálohovací místnost, racková místnost 1, racková místnost 2, trezor, kancelář mzdové účetní),
- vnitřní pohybová čidla – 16 ks (sklad barev, sklad drobného nářadí, 9 kanceláří, archiv, serverovna, místnost zálohovacího zařízení, racková místnost 1, racková místnost 2),
- venkovní pohybová čidla – 2 ks (oblast hranice pozemku, kde je bariéra pouze plot),
- přístupové klávesnice – 6 ks:
 - (chodba pro server, trezor, rackovou místnost 1, 4 kanceláře) – 1 ks,
 - (chodba pro rackovou místnost 2, 4 kanceláře) – 1 ks,
 - (sklad drobného nářadí, 1 kancelář) – 1 ks,
 - (sklad barev a ředidel) – 1 ks,
 - (místnost archivu) – 1 ks,
 - (místnost zálohovacího zařízení) – 1 ks,
- alarmové sirény – 2 ks (vnitřní nádvoří, vrátnice – směrem do ulice).

Kamerový systém

Instalace bezpečnostních kamer s vysokým rozlišením a nočním viděním, které umožňují čisté a detailní záznamy i v nízkém osvětlení. Využití pokročilých funkcí analýzy videa, jako je rozpoznávání státních rozpoznávacích značek (SPZ), vznik požáru nebo narušení prostoru, to zvyšuje efektivitu monitorování a snižuje potřebu lidského zásahu. Propojení kamerového systému s firemním alarmovým systémem, to umožňuje automatické spouštění odeslání upozornění a spuštění alarmu při detekci neautorizovaného vstupu nebo jiných bezpečnostních incidentů. Na základě expertního posudku, který vychází z dlouhodobé znalosti objektu a znalosti předchozích výskytů bezpečnostních incidentů, bude rozmístění kamer s těmito funkcemi na všech klíčových místech:

- vjezdové prostory – funkce rozpoznávání SPZ – 2 ks (2 vjezdové brány),
- venkovní prostory – funkce detekce narušení prostoru + detekce vzniku požáru – 1 ks:
 - (sklad pohonných hmot (PHM)),
- venkovní prostory – funkce detekce narušení prostoru – 6 ks:

- (parkoviště hlavní),
- (parkoviště vnitřní),
- (sklad hutního materiálu),
- (průjezd u kolejí),
- (vrata lakovna),
- (pískovna),
- vnitřní prostory – funkce detekce narušení prostoru + detekce vzniku požáru – 6 ks:
 - (lakovna),
 - (tryskač),
 - (pálící automat autogen),
 - (pálící automat laser),
 - (chodba malé kotelny),
 - (chodba velké kotelny).
- vnitřní prostory – funkce detekce narušení prostoru – 10 ks (ostatní vnitřní prostory bez požárního nebezpečí).

3. Definice rozhodovacího procesu, stanovení kritérií a variant

Rozhodovací proces zaměřený na výběr systémů detekce a alarmu při požáru, elektronických zabezpečovacích a přístupových systémů a kamerových systémů vyžaduje komplexní pochopení specifických rizik, kterým je objekt vystaven, a stanovení úrovně ochrany, kterou je třeba dosáhnout. V dalším kroku se provádí rešerše dostupných technologií a řešení, které mohou tyto požadavky splnit. Rozhodovací proces zahrnuje porovnávání funkčnosti, účinnosti, nákladů na instalaci a údržbu různých systémů, stejně jako jejich schopnost integrace do stávající infrastruktury.

3.1. Rozhodovací proces

Při rešerši dostupných technologií a řešení v oblasti bezpečnostních systémů se ukázalo, že dodavatelé těchto systémů často nabízejí komplexní balíčky řešení, které zahrnují všechny potřebné komponenty jako jeden set.

Rozhodovací proces zaměřený na výběr a implementaci komplexního systému detekce a alarmu při požáru, elektronického zabezpečovacího a přístupového systému a kamerového systému od jednoho dodavatele je zásadní kvůli potřebě zajištění vysoce integrovaného a efektivního bezpečnostního řešení. Vzhledem k jeho významu a složitosti je rozhodovací proces výběru těchto systémů řízen metodami vícekritériálního rozhodování, které umožňují systematické a objektivní porovnání různých alternativ na základě stanovených kritérií. Tento přístup zaručuje, že vybrané řešení splní všechny technické, finanční a bezpečnostní požadavky a bude dosaženo optimální rovnováhy mezi náklady, účinností a spolehlivostí systémů s cílem zajištění maximální ochrany životů a majetku. Instalace systémů od jednoho dodavatele navíc zjednoduší logistiku a zprovoznění, zatímco komplexnost dodávaného řešení zajistí, že všechny komponenty spolehlivě spolupracují, to výrazně zvyšuje celkovou bezpečnost objektu.

Cíl rozhodovacího procesu

Cílem rozhodovacího procesu je vybrat optimální variantu zabezpečení složenou ze systému detekce a alarmu při požáru, elektronického zabezpečovacího a přístupového systému a kamerového systému, která vylepší stávající zabezpečení firmy a zároveň sníží rizika vyhodnocená jako vysoká. Nové vyhodnocení rizik proběhne po 6 měsících provozu.

3.2. Omezující podmínky

Při výběru optimální varianty zabezpečení je nezbytné brát v úvahu řadu omezujících podmínek, které mohou výrazně ovlivnit konečné rozhodnutí.

Maximální cena 650.000, - Kč bez DPH

Rozpočet schválený vedením společnosti omezuje celkové náklady projektu na 650.000, - Kč bez DPH. Toto finanční omezení vyžaduje pečlivé plánování a nákup, aby byly zahrnuty náklady na hardware, software, instalaci a zprovoznění systému. Je důležité vyjednat s dodavatelem nejlepší možné podmínky a eliminovat všechny skryté náklady, aby projekt nebyl finančně překročen.

Minimální záruka 12 měsíců

Všem systémům musí být poskytnuta minimální záruka 12 měsíců v režimu příjezdu servisního technika do 24 hodin v pracovních dnech. Toto omezení pomáhá minimalizovat riziko budoucích výdajů spojených s opravami nebo výměnou vadných dílů a zajišťuje jistotu dlouhodobé podpory.

Minimálně 6 provedených instalací bezpečnostních systémů v cenové relaci 500.000,- Kč až 1.000.000,- Kč za poslední 3 roky s uvedením referencí

Tato omezující podmínka slouží k ověření zkušeností a spolehlivosti dodavatele bezpečnostních systémů. Vyžaduje od dodavatelů, aby prokázali, že během posledních tří let úspěšně dokončili minimálně šest instalací bezpečnostních systémů, jejichž jednotlivé náklady se pohybovaly v rozmezí od 500.000,- Kč do 1.000.000,- Kč. Kritérium zahrnuje požadavek na předložení referencí od klientů, kteří tyto instalace objednali, to poskytuje konkrétní důkazy o odbornosti a úspěšném zvládnutí projektů v dané cenové kategorii. Tímto způsobem se zvyšuje jistota, že dodavatel má potřebné technické znalosti a zkušenosti pro realizaci komplexního zabezpečovacího systému, a zároveň umí efektivně pracovat s rozpočtem a dodržet kvalitativní standardy.

Kompatibilita s bezkontaktní kartou EMmarin

Systém musí být schopen integrace s již existujícími bezkontaktními kartami EMmarin, to je standard pro přístupové systémy v mnoha organizacích. Kompatibilita znamená, že nový systém může využívat stávající infrastrukturu bez potřeby drahých a časově náročných úprav.

Minimální počet uživatelů 30

System musí umožňovat správu minimálně 30 individuálních uživatelských profilů, to umožňuje flexibilní a bezpečné řízení přístupu. Tato funkce je klíčová pro zabezpečení prostředí, kde je přístup různých skupin uživatelů potřeba regulovat.

Podpora vzdáleného ovládání pomocí webové aplikace

Bezpečnostní systémy musí umožňovat vzdálenou administraci prostřednictvím webového rozhraní. Tato funkcionalita zajišťuje, že správci systému mohou efektivně monitorovat, nastavovat a reagovat na bezpečnostní události odkudkoliv, to je nezbytné pro rychlou a efektivní správu bezpečnostních hrozeb.

Minimální detekce pohybových čidel na 12 metrů

Pohybová čidla musí být schopna detekovat jakýkoliv pohyb v dosahu minimálně 12 metrů od místa jejich instalace. Tato specifikace zajišťuje dostatečné pokrytí velkých prostor, jako jsou sklady, velké kancelářské prostory nebo venkovní areály. Vhodná detekce na tuto vzdálenost umožňuje efektivní monitorování a reakci na potenciální bezpečnostní hrozby, to vede k rychlému zásahu a minimalizaci možného nebezpečí nebo škod.

Pohybová čidla s PET imunitou minimálně 10 kg

Pohybová čidla musí být vybavena technologií, která umožňuje ignorovat pohyb malých zvířat do hmotnosti 10 kg. Tato funkce zabraňuje falešným poplachům způsobeným malými zvířaty v prostoru, jako jsou drobní hlodavci nebo ptáci. Tato technologie umožňuje čidlům rozlišovat mezi pohyby způsobenými lidmi a zvířaty, čímž zvyšuje spolehlivost a efektivitu bezpečnostního systému.

3.3. Hodnotící kritéria

V této kapitole jsou uvedena hodnotící kritéria, která jsou seřazena dle jejich důležitosti od nejdůležitějšího k nejméně důležitému.

K1 – cena

Prvním hodnotícím kritériem je cena bez DPH. Jedná se o hodnotící kritérium kvantitativní minimalizační. Nejlepší hodnotou je nejnižší cena. Toto kritérium je také omezujícím kritériem a jeho maximální hodnota je 650.000, - Kč bez DPH. Do tohoto cenového stropu není problém pořídit kvalitní bezpečnostní systém s požadovanými vlastnostmi. Možnosti pro toto kritérium jsou číselné a mohou nabývat hodnot rovných nebo nižších než 650.000.

K2 – počet individuálních uživatelských profilů

Druhým hodnotícím kritériem je počet individuálních uživatelských profilů. Jedná se o hodnotící kritérium kvantitativní maximalizační. Nejlepší hodnotou je největší možný počet uživatelských profilů. Toto kritérium je také omezujícím kritériem, a to v tom smyslu, že musí umožňovat minimálně 30 individuálních uživatelských profilů. Toto kritérium je zásadní pro organizace všech velikostí, neboť určuje, jak dobře může systém zabezpečení pokrývat potřeby firmy v závislosti na počtu zaměstnanců nebo členů, kteří mají k systému přístup. Větší počet spravovaných uživatelů znamená vyšší flexibilitu a možnost škálování systému, to je klíčové pro růstové fáze firmy. Vyšší počet uživatelů zaručuje, že bezpečnostní systém bude efektivní i při rozšíření počtu uživatelů, aniž by bylo nutné provádět nákladné upgrady nebo přecházet na jiný systém. Možnosti pro toto kritérium jsou číselné a mohou nabývat hodnot rovných nebo vyšších než 30.

K3 – doplnění systému svépomocí

Třetím hodnotícím kritériem je možnost doplnění systému svépomocí. Jedná se o hodnotící kritérium kvalitativní nominální. Toto hodnotící kritérium se zaměřuje na flexibilitu a uživatelskou přívětivost bezpečnostního systému ve smyslu možností rozšíření nebo modifikace systému bez potřeby externích služeb. Hodnotí, zda mohou nebo nemohou uživatelé přidávat, odstraňovat nebo upravovat komponenty systému, jako jsou senzory, kamery, přístupové terminály a další integrované prvky. Toto kritérium není nezbytné, ale je zásadní s ohledem na budoucí nutné investice. Možnosti pro toto kritérium jsou ANO / NE.

K4 – časová náročnost instalace

Čtvrtým hodnotícím kritériem je garantovaná časová náročnost instalace systému zabezpečení v týdnech. Jedná se o hodnotící kritérium kvantitativní minimalizační. Nejlepší hodnotou je nejkratší časová náročnost. Toto hodnotící kritérium zkoumá rychlost, s jakou lze daný bezpečnostní systém nainstalovat a uvést do provozu. Klíčovým aspektem je zde doba, kterou dodavatel garantuje pro kompletní instalaci systému, včetně veškerého hardwaru a softwaru. Možnosti pro toto kritérium jsou číselné a mohou nabývat hodnot vyšších 0.

K5 – délka záruky

Pátým hodnotícím kritériem je délka záruky v měsících. Jedná se o hodnotící kritérium kvantitativní maximalizační. Nejlepší hodnotou je nejdelší záruka. Toto kritérium je také omezujícím kritériem, a to v tom smyslu, že musí být tato záruka poskytována a její minimální

doba je 12 měsíců. Někteří dodavatelé tuto záruku poskytují v základu a někteří jako příplatkovou. Možnosti pro toto kritérium jsou číselné a mohou nabývat hodnot rovných nebo vyšších 12.

K6 – počet realizovaných instalací

Šestým hodnotícím kritériem je počet úspěšně realizovaných instalací bezpečnostních systémů v cenovém rozmezí 500.000,- Kč až 1.000.000,- Kč během posledních tří let. Jedná se o hodnotící kritérium kvantitativní maximalizační. Nejlepší hodnotou je nejvíce doložených instalací za poslední 3 roky. Toto kritérium je také omezujícím kritériem a zaměřuje na ověření schopností dodavatelů bezpečnostních systémů na základě jejich historie a zkušeností s podobnými projekty. Dodavatel musí doložit minimálně šest takových instalací a poskytnout ověřitelné reference od klientů, to demonstruje jeho spolehlivost, odbornost a schopnost splnit specifické požadavky a očekávání klientů. Možnosti pro toto kritérium jsou číselné a mohou nabývat hodnot rovných nebo vyšších 6.

3.4. Varianty

Při výběru variant pro implementaci nového bezpečnostního systému bylo postupováno dle požadavků omezujících podmínek. Tento přístup zajistil, že každá vybraná firma disponuje potřebnými kvalifikacemi a zkušenostmi pro realizaci projektu. Díky těmto stanoveným kritériím bylo možné vybrat pět firem, seřazených abecedně:

ALARM KFS, BECO Link, Eurosat CS, JABLOTRON ALARMS a TOP security.

Výsledný výběr těchto pěti firem poskytuje kvalitní základ pro další rozhodovací proces, v němž bude na základě detailnějších hodnocení vybrána firma, která nejlépe odpovídá stanoveným potřebám.

V1

Firma **ALARM KFS** nabízí komplexní **bezpečnostní systém složený z výrobků značky JABLOTRON ALARMS** za cenu 600.000,- Kč bez DPH. Systém je navržen tak, aby poskytoval vysoce spolehlivou ochranu s rozšířenými funkcemi a moderními technologiemi. V cenové nabídce je zahrnuta záruka 24 měsíců s garantovaným dojezdem technika do 16 hodin během pracovních dní, to zajišťuje rychlou reakci na případné problémy nebo poruchy systému. Doložila sedm referencí, které dokládají úspěšnou realizaci projektů v požadovaném finančním rozmezí. Tato zkušenost a důvěra ve schopnosti firmy jsou klíčové pro zajištění kvality a spolehlivosti nabízeného systému. Systém je plně kompatibilní s bezkontaktními kartami

EMmarin a umožňuje správu až 50 uživatelů, to zvyšuje jeho flexibilitu a škálovatelnost. Další výhodou je podpora vzdáleného ovládání systému prostřednictvím webové aplikace, která umožňuje uživatelům snadnou kontrolu a správu zabezpečení i na dálku. Systém obsahuje pohybová čidla s dosahem detekce 12 metrů a PET imunitou do 25 kg, to minimalizuje falešné poplachy způsobené drobnými živočichy a ptáky. Systém ale neumožňuje doplnění svépomocí a je nutno do budoucna počítat s větší finanční náročností při potřebě systém rozšířit. Časová náročnost instalace systému je garantována na 8 týdnů. Nabídka firmy ALARM KFS tedy reprezentuje moderní a komplexní řešení bezpečnostních potřeb, které je podloženo pevnými zárukami a doloženou historií úspěšných instalací, avšak s určitými omezeními, které budou vzaty v úvahu při rozhodování.

V2

Firma **BECO Link** nabízí komplexní **bezpečnostní systém složený z výrobků značky HIKVISION** za 580.000,- Kč bez DPH. Značka HIKVISION je známá svou kvalitou a pokročilými technologickými řešeními. V cenové nabídce je zahrnuta záruka 24 měsíců s garantovaným dojezdem technika do 12 hodin v pracovní dny, to zajišťuje velice rychlou reakci na případné problémy nebo poruchy systému. Doložila sedm referencí, které dokládají úspěšnou realizaci projektů v požadovaném finančním rozmezí. Tato zkušenost a důvěra ve schopnosti firmy jsou klíčové pro zajištění kvality a spolehlivosti nabízeného systému. Systém je plně kompatibilní s bezkontaktními kartami EMmarin a umožňuje správu až 48 uživatelů, to zvyšuje jeho flexibilitu a škálovatelnost. Další výhodou je podpora vzdáleného ovládání systému prostřednictvím webové aplikace, která umožňuje uživatelům snadnou kontrolu a správu zabezpečení i na dálku. Systém obsahuje pohybová čidla s dosahem detekce 15 metrů s PET imunitou do 30 kg, to minimalizuje falešné poplachy způsobené drobnými živočichy a ptáky. Systém umožňuje doplnění systému svépomocí, to umožňuje flexibilní rozšíření nebo modifikaci systému podle vlastních potřeb. Časová náročnost instalace systému je garantována na 4 týdny. Celkově tedy BECO Link s výrobky HIKVISION nabízí robustní a flexibilní bezpečnostní řešení, které je podloženo solidními zárukami a doloženou historií úspěšných instalací.

V3

Firma **Eurosat CS** nabízí komplexní **bezpečnostní systém složený z výrobků značky Paradox** za 575.000,- Kč bez DPH. V cenové nabídce je zahrnuta záruka 12 měsíců s garantovaným dojezdem technika do 24 hodin během pracovních dnů, to zajišťuje rychlou

reakci na případné problémy nebo poruchy systému. Doložila šest referencí, které dokládají úspěšnou realizaci projektů v požadovaném finančním rozmezí. Tato zkušenost a důvěra ve schopnosti firmy svědčí o jejich spolehlivosti a kvalitě prováděných prací. Systém je plně kompatibilní s bezkontaktními kartami EMmarin a umožňuje správu až 32 uživatelů. Další výhodou je podpora vzdáleného ovládání systému prostřednictvím webové aplikace, která umožňuje uživatelům snadnou kontrolu a správu zabezpečení i na dálku. Systém obsahuje pohybová čidla s dosahem detekce 12 metrů s PET imunitou do 15 kg, to minimalizuje falešné poplachy způsobené drobnými živočichy a ptáky. Systém umožňuje doplnění systému svépomocí, to umožňuje flexibilní rozšíření nebo modifikaci systému podle vlastních potřeb. Časová náročnost instalace systému je garantována na 10 týdnů. To je relativně delší doba, ale Eurosat CS zaručuje důkladnou a precizní instalaci systému, aby byly splněny všechny bezpečnostní požadavky klienta. Tato nabídka od Eurosat CS poskytuje spolehlivé a ekonomicky efektivní řešení pro zabezpečení objektů, které představuje robustní základ pro zajištění bezpečnosti majetku a osob.

V4

Firma **JABLOTRON ALARMS** nabízí komplexní **bezpečnostní systém složený výhradně z vlastních výrobků** za cenu 630.000,- Kč bez DPH. Systém je navržen tak, aby poskytoval vysoce spolehlivou ochranu s rozšířenými funkcemi a moderními technologiemi. V cenové nabídce je zahrnuta záruka 24 měsíců s garantovaným dojezdem technika do 24 hodin během pracovních dní, to zajišťuje rychlou reakci na případné problémy nebo poruchy systému. Doložila osm referencí, které dokládají úspěšnou realizaci projektů v požadovaném finančním rozmezí. Tato zkušenost a důvěra ve schopnosti firmy jsou klíčové pro zajištění kvality a spolehlivosti nabízeného systému. Systém je plně kompatibilní s bezkontaktními kartami EMmarin a umožňuje správu až 50 uživatelů, to zvyšuje jeho flexibilitu a škálovatelnost. Další výhodou je podpora vzdáleného ovládání systému prostřednictvím webové aplikace, která umožňuje uživatelům snadnou kontrolu a správu zabezpečení i na dálku. Systém obsahuje pohybová čidla s dosahem detekce 12 metrů a PET imunitou do 25 kg, to minimalizuje falešné poplachy způsobené drobnými živočichy a ptáky. Systém ale neumožňuje doplnění svépomocí a je nutno do budoucna počítat s větší finanční náročností při potřebě systém rozšířit. Časová náročnost instalace systému je garantována na 5 týdnů. Nabídka firmy JABLOTRON ALARMS tedy reprezentuje moderní a komplexní řešení bezpečnostních potřeb, které je podloženo pevnými zárukami a doloženou historií úspěšných instalací, avšak s určitými omezeními, které budou vzaty v úvahu při rozhodování.

V5

Firma **TOP security** nabízí komplexní **bezpečnostní systém složený z výrobků značky Satel** za 590.000,- Kč bez DPH. V cenové nabídce je zahrnuta záruka 12 měsíců s garantovaným dojezdem technika do 24 hodin během pracovních dnů, to zajišťuje rychlou reakci na případné problémy nebo poruchy systému. Doložila sedm referencí, které dokládají úspěšnou realizaci projektů v požadovaném finančním rozmezí. Tato zkušenost a důvěra ve schopnosti firmy svědčí o jejich spolehlivosti a kvalitě prováděných prací. Systém je plně kompatibilní s bezkontaktními kartami EMmarin a umožňuje správu až 30 uživatelů. Další výhodou je podpora vzdáleného ovládání systému prostřednictvím webové aplikace, která umožňuje uživatelům snadnou kontrolu a správu zabezpečení i na dálku. Systém obsahuje pohybová čidla s dosahem detekce 12 metrů s PET imunitou do 20 kg, to minimalizuje falešné poplachy způsobené drobnými živočichy a ptáky. Systém umožňuje doplnění systému svépomocí, to umožňuje flexibilní rozšíření nebo modifikaci systému podle vlastních potřeb. Časová náročnost instalace systému je garantována na 12 týdnů. To je relativně delší doba, kterou je potřeba zvážit a pečlivě naplánovat.

3.5. Rozhodovací tabulka

Následující rozhodovací Tabulka 2 je nástroj používaný k systematickému porovnání různých variant na základě předem definovaných kritérií. V této tabulce jsou varianty umístěny v řádcích, zatímco hodnotící kritéria jsou rozvržena ve sloupcích. Každá buňka tabulky pak obsahuje hodnotu kritéria patřící k dané variantě.

Tabulka 2 – Rozhodovací tabulka

Kritéria Varianty	K1 cena Kč	K2 uživatelů ks	K3 svépomoc ANO/NE	K4 instalace týdny	K5 záruka měsíce	K6 reference ks
V1	600.000,-	50	NE	8	24	7
V2	580.000,-	48	ANO	4	24	7
V3	575.000,-	32	ANO	10	12	6
V4	630.000,-	50	NE	5	24	8
V5	590.000,-	30	ANO	12	12	7

Zdroj: vlastní zpracování

4. Řešení rozhodovacího problému pomocí metod vícekriteriálního rozhodování

Pro přehlednost je zde na začátku této kapitoly zobrazen přehled kritérií s označením a popis a přehled variant s označením a popisem.

Přehled kritérií seřazených dle jejich důležitosti zobrazuje Tabulka 3.

Tabulka 3 – Tabulka kritérií

K1	cena (v Kč bez DPH)
K2	počet individuálních uživatelských profilů (v ks)
K3	doplnění systému svépomocí (ANO/NE)
K4	časová náročnost instalace (v týdnech)
K5	délka záruky (v měsících)
K6	počet referencí v rozmezí 500.000,- ÷ 1.000.000,- Kč za 3 roky (v ks)

Zdroj: vlastní zpracování

Přehled variant zobrazuje Tabulka 4.

Tabulka 4 – Tabulka variant

V1	bezpečnostní systém dodaný firmou ALARM KFS
V2	bezpečnostní systém dodaný firmou BECO Link
V3	bezpečnostní systém dodaný firmou Eurosat CS
V4	bezpečnostní systém dodaný firmou JABLOTRON ALARMS
V5	bezpečnostní systém dodaný firmou TOP security

Zdroj: vlastní zpracování

4.1. Stanovení vah kritérií

Stanovení vah kritérií je klíčovou součástí rozhodovacích procesů, zejména při použití vícekriteriálního hodnocení. Různé metody stanovení vah kritérií mohou poskytnout různé perspektivy na důležitost jednotlivých kritérií vzhledem k celkovému rozhodnutí.

Přímá metoda bodovací (Metfesselova alokace)

Tato metoda je přímá a spočívá v přidělení bodů jednotlivým kritériím na základě jejich relativní důležitosti. Je použita stupnice 0 ÷ 100, nejdůležitějšímu případně nejvíce bodů, a nejméně důležitému případně nejméně bodů. Výsledné váhy jsou poté vypočítány jako

procentní podíl každého kritéria z celkového počtu bodů. Výsledné vyhodnocení této metody zobrazuje Tabulka 5. [8]

Tabulka 5 – Přímá metoda bodovací

Kritérium	K1	K2	K3	K4	K5	K6	Součet
Počet bodů	80	60	50	40	30	10	270
Nominální váha	0,30	0,22	0,19	0,15	0,11	0,03	1

Zdroj: vlastní zpracování

Nepřímá metoda párového srovnávání (Fullerova metoda)

Fullerova metoda je sofistikovanější a zahrnuje porovnávání kritérií v párech pro určení jejich relativní důležitosti. Každý pár kritérií je porovnán a musí se určit, který z nich je důležitější, a také stupně důležitosti. [8]

Výsledné vyhodnocení této metody zobrazuje Tabulka 6.

Tabulka 6 – Váhy kritérií nepřímou metodou (Fullerovou)

K _i	K1	K2	K3	K4	K5	K6	f _i	f _i + 1	v _i
K1		1	1	1	1	1	5	6	0,2857
K2			1	1	1	1	4	5	0,2381
K3				1	1	1	3	4	0,1905
K4					1	1	2	3	0,1429
K5						1	1	2	0,0952
K6							0	1	0,0476
								21	1

Zdroj: vlastní zpracování

Z této tabulky je zřejmá důležitost jednotlivých kritérií, kde K1 je nejdůležitější, následují kritéria K2, K3, K4, K5 a jako poslední je kritérium K6.

Nepřímá metoda párového porovnávání kritérií (Saatyho metoda)

Saatyho metoda, je jednou z nejrozšířenějších metod pro stanovení vah v rozhodovacím procesu. Tato metoda zahrnuje vytvoření matice párových porovnání, kde každé kritérium je porovnáno s každým jiným kritériem vzhledem k jejich relativní důležitosti. [8]

Tato důležitost se volí ze stupnice 1 ÷ 9 jak zobrazuje Tabulka 7. Výsledné vyhodnocení této metody zobrazuje .

Zdroj: vlastní zpracování

Tabulka 8. U této metody se dále musí vypočítat největší vlastní číslo matice λ_{\max} jak ukazuje Obrázek 4, podle počtu kritérií dosadit hodnotu náhodného konzistenčního indexu (RI) dle Whartona, tuto hodnotu zobrazuje Obrázek 8 v příloze B a vypočítat konzistenční poměr (CR), který musí být menší než 0,1 a ukazuje nám, jak je kvalitně sestavená Saatyho matice. Po provedení výpočtů je konzistenční poměr CR roven 0,0775 jak zobrazuje Tabulka 9. Saatyho matice je tedy sestavená správně.

Tabulka 7 – Intenzita relativních důležitostí

Intenzita relativních důležitostí	K_i
9	K1
7	K2
5	K3
3	K4
2	K5
1	K6

Zdroj: vlastní zpracování

Tabulka 8 – Váhy kritérií nepřímou metodou (Saatyho)

K_i	K1	K2	K3	K4	K5	K6	geometrický průměr	v_i
K1	1	3	5	7	8	9	4,43	0,4571
K2	1/3	1	3	5	7	8	2,56	0,2639
K3	1/5	1/3	1	3	5	7	1,38	0,1427
K4	1/7	1/5	1/3	1	3	5	0,72	0,0746
K5	1/8	1/7	1/5	1/3	1	3	0,39	0,0403
K6	1/9	1/8	1/7	1/5	1/3	1	0,21	0,0214
							9,69	1

Zdroj: vlastní zpracování

Input

eigenvectors

$$\begin{pmatrix} 1 & 3 & 5 & 7 & 8 & 9 \\ \frac{1}{3} & 1 & 3 & 5 & 7 & 8 \\ \frac{1}{5} & \frac{1}{3} & 1 & 3 & 5 & 7 \\ \frac{1}{7} & \frac{1}{5} & \frac{1}{3} & 1 & 3 & 5 \\ \frac{1}{8} & \frac{1}{7} & \frac{1}{5} & \frac{1}{3} & 1 & 3 \\ \frac{1}{9} & \frac{1}{8} & \frac{1}{7} & \frac{1}{5} & \frac{1}{3} & 1 \end{pmatrix}$$

Results

[Exact forms](#) [Step-by-step solution](#)

$v_1 \approx (19.2036, 10.7506, 5.83294, 3.07172, 1.66537, 1)$

$v_2 \approx (3.65486 + 16.9107i, -5.56064 + 6.12639i, -4.2992 - 0.765032i, -1.18819 - 2.13518i, 0.608216 - 1.14497i, 1)$

$v_3 \approx (3.65486 - 16.9107i, -5.56064 - 6.12639i, -4.2992 + 0.765032i, -1.18819 + 2.13518i, 0.608216 + 1.14497i, 1)$

$v_4 \approx (-6.97409 + 9.7196i, -4.36103 - 6.79549i, 5.79573 - 1.257i, -0.842899 + 3.31991i, -1.66066 - 1.29354i, 1)$

$v_5 \approx (-6.97409 - 9.7196i, -4.36103 + 6.79549i, 5.79573 + 1.257i, -0.842899 - 3.31991i, -1.66066 + 1.29354i, 1)$

$v_6 \approx (-12.3219, 7.1849, -3.76546, 3.07529, -2.34582, 1)$

Corresponding eigenvalues

[Exact forms](#) [Step-by-step solution](#)

$\lambda_1 \approx 6.4803$

$\lambda_2 \approx 0.0619451 + 1.72678i$

$\lambda_3 \approx 0.0619451 - 1.72678i$

$\lambda_4 \approx -0.214199 + 0.28375i$

$\lambda_5 \approx -0.214199 - 0.28375i$

$\lambda_6 \approx -0.175788$

Obrázek 4 – Výpočet λ_{\max}

Zdroj: [35]

Tabulka 9 – hodnoty pro kritéria dle Saatyho metody

λ_{\max}	6,4803
CI	0,0961
RI	1,2400
CR	0,0775

Zdroj: vlastní zpracování

4.2. Ohodnocení variant

Ohodnocení variant probíhá stejným způsobem jako ohodnocení vah kritérií, jen se u každého kritéria porovnává pár variant.

Nepřímá metoda párového srovnávání (Fullerova metoda)

Výpočet ohodnocení jednotlivých variant Fullerovy metody ukazuje Tabulka 10, Tabulka 11, Tabulka 12, Tabulka 13, Tabulka 14 a Tabulka 15.

Tabulka 10 – Dílčí ohodnocení variant Fullerovou metodou pro K1

K1	V1	V2	V3	V4	V5	f_i	$f_i + 1$	h_1^j
V1		0	0	1	0	1	2	0,1333
V2			0	1	1	3	4	0,2667
V3				1	1	4	5	0,3333
V4					0	0	1	0,0667
V5						2	3	0,2000
							15	1

Zdroj: vlastní zpracování

Tabulka 11 – Dílčí ohodnocení variant Fullerovou metodou pro K2

K2	V1	V2	V3	V4	V5	f_i	$f_i + 1$	h_2^j
V1		1	1	1/2	1	3	4	0,2857
V2			1	0	1	2	3	0,2143
V3				0	1	1	2	0,1429
V4					1	3	4	0,2857
V5						0	1	0,0714
							14	1

Zdroj: vlastní zpracování

Tabulka 12 – Dílčí ohodnocení variant Fullerovou metodou pro K3

K3	V1	V2	V3	V4	V5	f_i	$f_i + 1$	h_3^j
V1		0	0	1/2	0	0	1	0,09095
V2			1/2	1	1/2	2	3	0,2727
V3				1	1/2	2	3	0,2727
V4					0	0	1	0,09095
V5						2	3	0,2727
							11	1

Zdroj: vlastní zpracování

Tabulka 13 – Dílčí ohodnocení variant Fullеровou metodou pro K4

K4	V1	V2	V3	V4	V5	f_i	f_i + 1	h₄^j
V1		0	1	0	1	2	3	0,2000
V2			1	1	1	4	5	0,3333
V3				0	1	1	2	0,1333
V4					1	3	4	0,2667
V5						0	1	0,0667
							15	1

Zdroj: vlastní zpracování

Tabulka 14 – Dílčí ohodnocení variant Fullеровou metodou pro K5

K5	V1	V2	V3	V4	V5	f_i	f_i + 1	h₅^j
V1		1/2	1	1/2	1	2	3	0,2727
V2			1	1/2	1	2	3	0,2727
V3				0	1/2	0	1	0,09095
V4					1	2	3	0,2727
V5						0	1	0,09095
							11	1

Zdroj: vlastní zpracování

Tabulka 15 – Dílčí ohodnocení variant Fullеровou metodou pro K6

K6	V1	V2	V3	V4	V5	f_i	f_i + 1	h₆^j
V1		1/2	1	0	1/2	1	2	0,1667
V2			1	0	1/2	1	2	0,1667
V3				0	0	0	1	0,0832
V4					1	4	5	0,4167
V5						1	2	0,1667
							12	1

Zdroj: vlastní zpracování

Tabulka 16 – Celkové ohodnocení variant Fullerovou metodou

	K1	K2	K3	K4	K5	K6	H^j
V1	0,06093	0,07540	0,01298	0,01492	0,01100	0,00357	0,17879
V2	0,12190	0,05655	0,03891	0,02486	0,01100	0,00357	0,25680
V3	0,15235	0,03771	0,03891	0,00994	0,00367	0,00178	0,24436
V4	0,03049	0,07540	0,01298	0,01990	0,01100	0,00891	0,15867
V5	0,09142	0,01884	0,03891	0,00498	0,00367	0,00357	0,16138
							1

Zdroj: vlastní zpracování

Nejlepší varianta je V2 jak ukazuje Tabulka 16 – bezpečnostní systém složený z výrobků značky HIKVISION od firmy BECO Link.

Nepřímá metoda párového porovnávání kritérií (Saatyho metoda)

Výpočet ohodnocení jednotlivých variant Saatyho metody ukazuje Tabulka 17, Tabulka 20, Tabulka 23, Tabulka 26, Tabulka 29 a Tabulka 32.

Intenzitu relativních důležitostí zase ukazuje Tabulka 18, Tabulka 21, Tabulka 24, Tabulka 27, Tabulka 30 a Tabulka 33.

A hodnoty pro kritéria dle Saatyho metody ukazuje Tabulka 19, Tabulka 22, Tabulka 25, Tabulka 28, Tabulka 31 a Tabulka 34.

Tabulka 17 – Dílčí ohodnocení variant Saatyho metodou pro K1

K1	V1	V2	V3	V4	V5	geometrický průměr	h_{1^j}
V1	1	1/3	1/4	2	1/2	0,61	0,0975
V2	3	1	1/2	4	2	1,64	0,2634
V3	4	2	1	5	3	2,61	0,4174
V4	1/2	1/4	1/5	1	1/3	0,38	0,0615
V5	2	1/2	1/3	3	1	1	0,1602
						6,24	1

Zdroj: vlastní zpracování

Tabulka 18 – Intenzita relativních důležitostí pro K1

Intenzita relativních důležitostí	K1
9	V3
8	V2
7	V5
6	V1
5	V4

Zdroj: vlastní zpracování

Tabulka 19 – hodnoty pro kritéria dle Saatyho metody pro K1

λ_{\max}	5,0681
CI	0,0170
RI	1,1200
CR	0,0152

Zdroj: vlastní zpracování

Tabulka 20 – Dílčí ohodnocení variant Saatyho metodou pro K2

K2	V1	V2	V3	V4	V5	geometrický průměr	h_2^j
V1	1	2	7	1	8	2,57	0,3489
V2	1/2	1	6	1/2	7	1,60	0,2173
V3	1/7	1/6	1	1/7	2	0,37	0,0500
V4	1	2	7	1	8	2,57	0,3489
V5	1/8	1/7	1/2	1/8	1	0,26	0,0349
						7,36	1

Zdroj: vlastní zpracování

Tabulka 21 – Intenzita relativních důležitostí pro K2

Intenzita relativních důležitostí	K2
9	V1
9	V4
8	V2
3	V3
2	V5

Zdroj: vlastní zpracování

Tabulka 22 – hodnoty pro kritéria dle Saatyho metody pro K2

λ_{\max}	5,0857
CI	0,0214
RI	1,1200
CR	0,0191

Zdroj: vlastní zpracování

Tabulka 23 – Dílčí ohodnocení variant Saatyho metodou pro K3

K3	V1	V2	V3	V4	V5	geometrický průměr	h_3^j
V1	1	1/5	1/5	1	1/5	0,38	0,05885
V2	5	1	1	5	1	1,90	0,29410
V3	5	1	1	5	1	1,90	0,29410
V4	1	1/5	1/5	1	1/5	0,38	0,05885
V5	5	1	1	5	1	1,90	0,29410
						6,47	1

Zdroj: vlastní zpracování

Tabulka 24 – Intenzita relativních důležitostí pro K3

Intenzita relativních důležitostí	K3
7	V2
7	V3
7	V5
3	V1
3	V4

Zdroj: vlastní zpracování

Tabulka 25 – hodnoty pro kritéria dle Saatyho metody pro K3

λ_{\max}	5,0000
CI	0,0000
RI	1,1200
CR	0,0000

Zdroj: vlastní zpracování

Tabulka 26 – Dílčí ohodnocení variant Saatyho metodou pro K4

K4	V1	V2	V3	V4	V5	geometrický průměr	h_4^j
V1	1	1/5	3	1/4	4	0,90	0,1187
V2	5	1	7	2	8	3,55	0,4661
V3	1/3	1/7	1	1/6	2	0,44	0,0574
V4	4	1/2	6	1	7	2,43	0,3190
V5	1/4	1/8	1/2	1/7	1	0,29	0,0388
						7,61	1

Zdroj: vlastní zpracování

Tabulka 27 – Intenzita relativních důležitostí pro K4

Intenzita relativních důležitostí	K4
8	V2
7	V4
4	V1
2	V3
1	V5

Zdroj: vlastní zpracování

Tabulka 28 – hodnoty pro kritéria dle Saatyho metody pro K4

λ_{\max}	5,1689
CI	0,0422
RI	1,1200
CR	0,0377

Zdroj: vlastní zpracování

Tabulka 29 – Dílčí ohodnocení variant Saatyho metodou pro K5

K5	V1	V2	V3	V4	V5	geometrický průměr	h_5^j
V1	1	1	3	1	3	1,55	0,27270
V2	1	1	3	1	3	1,55	0,27270
V3	1/3	1/3	1	1/3	1	0,52	0,09095
V4	1	1	3	1	3	1,55	0,27270
V5	1/3	1/3	1	1/3	1	0,52	0,09095
						5,69	1

Zdroj: vlastní zpracování

Tabulka 30 – Intenzita relativních důležitostí pro K5

Intenzita relativních důležitostí	K5
5	V1
5	V2
5	V4
3	V3
3	V5

Zdroj: vlastní zpracování

Tabulka 31 – hodnoty pro kritéria dle Saatyho metody pro K5

λ_{\max}	5,0000
CI	0,0000
RI	1,1200
CR	0,0000

Zdroj: vlastní zpracování

Tabulka 32 – Dílčí ohodnocení variant Saatyho metodou pro K6

K6	V1	V2	V3	V4	V5	geometrický průměr	h_6^j
V1	1	1	3	1/3	1	1,00	0,1655
V2	1	1	3	1/3	1	1,00	0,1655
V3	1/3	1/3	1	1/5	1/3	0,37	0,0621
V4	3	3	5	1	3	2,67	0,4414
V5	1	1	3	1/3	1	1,00	0,1655
						6,04	1

Zdroj: vlastní zpracování

Tabulka 33 – Intenzita relativních důležitostí pro K6

Intenzita relativních důležitostí	K6
7	V4
5	V1
5	V2
5	V5
3	V3

Zdroj: vlastní zpracování

Tabulka 34 – hodnoty pro kritéria dle Saatyho metody pro K6

λ_{\max}	5,0420
CI	0,0105
RI	1,1200
CR	0,0094

Zdroj: vlastní zpracování

Tabulka 35 – Celkové ohodnocení variant Saatyho metodou

	K1	K2	K3	K4	K5	K6	H^j
V1	0,04457	0,09207	0,00840	0,00886	0,01099	0,00354	0,16843
V2	0,12040	0,05735	0,04197	0,03477	0,01099	0,00354	0,26902
V3	0,19079	0,01320	0,04197	0,00428	0,00367	0,00133	0,25523
V4	0,02811	0,09207	0,00840	0,02380	0,01099	0,00945	0,17282
V5	0,07323	0,00921	0,04197	0,00289	0,00367	0,00354	0,13451
							1

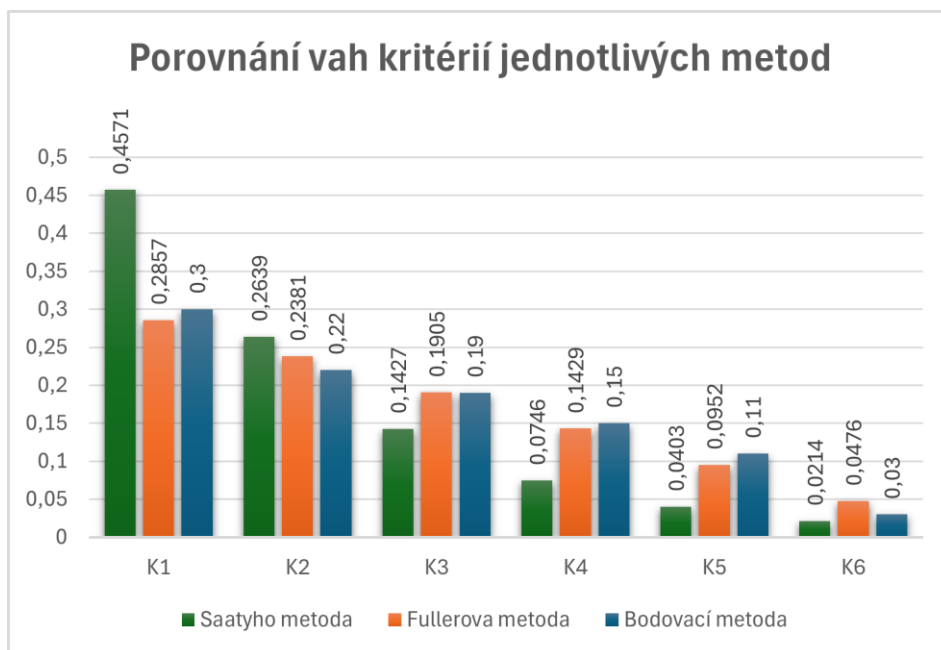
Zdroj: vlastní zpracování

Nejlepší varianta je V2 jak ukazuje Tabulka 35 – bezpečnostní systém složený z výrobků značky HIKVISION od firmy BECO Link.

4.3. Porovnání výsledků

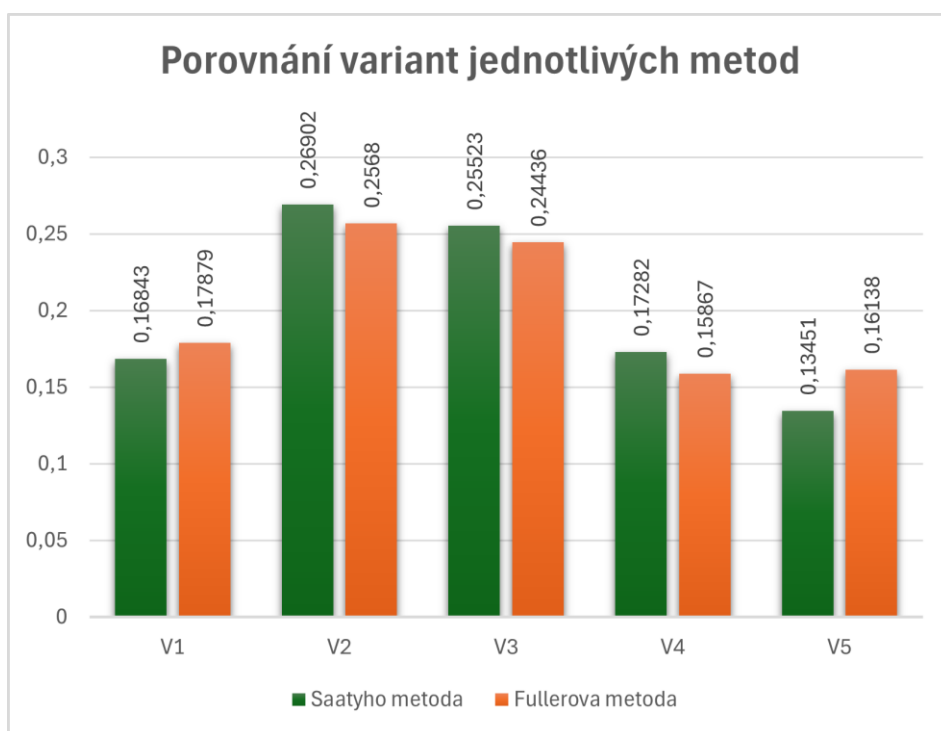
Porovnání výsledků vah kritérií a výsledků variant různých metod může odhalit rozdíly v přístupech a jejich efektivitě při řešení konkrétních problémů nebo výzev. Tento proces je zásadní pro vyhodnocení, která metoda nejlépe odpovídá specifickým potřebám projektu nebo organizace. Toto porovnání může pomoci objektivně vyhodnotit dostupné možnosti a zvolit optimální řešení, které nejlépe odpovídá konkrétním potřebám a cílům. Tento proces je nezbytný pro zajištění, že rozhodnutí jsou podložena, efektivní a vedou k dosažení požadovaných výsledků.

Jak ukazuje Obrázek 5, širší možnosti hodnocení důležitosti, které nabízí Saatyho metoda, jsou pro rozsáhlejší projekty velmi výhodné. Tato metoda umožňuje efektivně porovnat a vyhodnotit různé prvky projektu podle jejich relativní důležitosti. Použití váhového systému v této metodě také napomáhá lépe zachytit a zpracovat osobní preference a priority zúčastněných stran, což je klíčové pro úspěšnou implementaci rozsáhlých projektů.



Obrázek 5 – Graf porovnání vah kritérií jednotlivých metod

Zdroj: vlastní zpracování



Obrázek 6 – Graf porovnání variant jednotlivých metod

Zdroj: vlastní zpracování

Saatyho metoda, která je obzvláště užitečná v případech, kdy je potřeba vyhodnotit a porovnat více různých variant s podobnými vlastnostmi, může také odhalit určité rozdíly v porovnání variant s Fullerovou metodou. U Saatyho metody, která vyžaduje přidělení

relativní váhy kritériím na základě důležitosti, může dojít k posunům ve finálním pořadí variant, zejména pokud jsou si tyto varianty velmi blízké v hodnocení. [8]

To je také případ tohoto porovnání kde, jak ukazuje Obrázek 6 došlo ke změně pořadí, ke kterému došlo právě díky možnému většímu rozdílu mezi relativními váhami hlavně u kritérií K2 a K3.

Při aplikaci Saatyho metody se může stát, že i malé změny ve váhách kritérií mohou mít výrazný dopad na konečné pořadí variant, které mezi sebou měly původně jen nepatrné rozdíly. To je zvláště pravdivé v případech, kde jsou si varianty velmi podobné ve většině hodnotících kritérií, ale liší se v několika málo, které mohou být považovány za klíčové. Přehodnocení důležitosti těchto kritérií může vést k tomu, že varianta, která byla původně hodnocena jako méně příznivá, se posune výše v pořadí, zatímco jiné, dříve favorizované varianty, mohou klesnout. Tento jev zdůrazňuje význam pečlivého nastavení vah v procesu hodnocení. Je zásadní, aby každý, kdo Saatyho metodu používá, pochopil dynamiku a vliv, který váhy mají na výsledkové pořadí, a aby byl schopen kriticky posoudit a případně upravit váhy, pokud výsledky nepřinesou očekávanou soudržnost nebo pokud se objeví nové informace, které mění pohled na důležitost jednotlivých kritérií. Proto je doporučeno pravidelně revidovat a přizpůsobovat váhy, aby odrážely aktuální priority a realitu projektu. Důsledná validace a revize vah a kritérií jsou klíčové pro zajištění, že výsledky analýzy jsou relevantní a přesné, což je nezbytné pro úspěšné rozhodování v komplexních a dynamicky se vyvíjejících projektech.[8]

4.4. Doporučená varianta

Z obou použitých metod má nejvyšší hodnocení varianta V2 – tedy bezpečnostní systém složený z výrobků značky HIKVISION od firmy BECO Link. Tato nabídka je druhou nejlevnější (580.000,- Kč bez DPH), má také druhý nejvyšší počet individuálních uživatelských profilů (48) a také je možné si v budoucnu tento systém rozšířit svépomocí bez nutnosti objednání specializované firmy. Instalace zabere 4 týdny, záruka poskytnutá na tento systém je 24 měsíců. Společnost BECO Link doložila 7 referencí, které splňují požadovaná kritéria, a navíc jsou i z podobných provozů jako jsou tyto.

Výsledek této navržené varianty bude předán vedení společnosti s doporučením tuto variantu realizovat.

ZÁVĚR

Cílem této bakalářské práce bylo identifikovat slabá místa v zabezpečení firmy, identifikovat možnosti zabezpečení a pomocí metod vícekritériálního navrhnout vhodné zabezpečení. Práce je strukturována do několika kapitol, které postupně pokrývají úvod do zabezpečení objektů, popisu a druhů zabezpečení, dále popisují aktuální stav firmy, SWOT analýzu a analýzu rizik, až po definici rozhodovacího procesu se stanovením kritérií a variant, řešení rozhodovacího problému pomocí metod vícekritériálního rozhodování a představení navrhovaného řešení.

V první kapitole je uveden úvod do zabezpečení objektů a vysvětleny různé druhy zabezpečení.

Druhá kapitola se zaměřuje na detailní popis firmy, jejího současného stavu zabezpečení a finanční situaci. Také se věnuje důkladné SWOT analýze a rozboru rizik a zranitelných míst. To je klíčové pro identifikaci specifických opatření pro zvýšení bezpečnosti.

Ve třetí kapitole je popsán rozhodovací proces včetně stanovení omezujících podmínek, hodnotících kritérií a variant.

Čtvrtá kapitola popisuje samotné řešení rozhodovacího problému pomocí 2 metod vícekritériálního rozhodování, a to Fullerovou metodou a Saatyho metodou. Jsou zde tabulky s výpočty jednotlivých vah kritérií i s ohodnocením variant. Na konci této práce je grafické zobrazení a popis porovnání výsledků a je doporučena varianta.

Práce úspěšně splnila svůj cíl tím, že jasně identifikovala slabá místa v zabezpečení firmy a poskytla návrh zabezpečení, který zahrnul strategické a praktické aspekty a identifikovaná rizika potřebná pro zlepšení bezpečnostní situace firmy.

Přínos této práce je pro praktické využití v identifikaci a navrhování vhodných bezpečnostních řešení. Práce nabízí model, jak přistupovat k zabezpečení firmy, a zdůrazňuje význam hodnocení rizik a systematického plánování. Díky tomu může sloužit jako referenční materiál pro podobné projekty v budoucnosti a přispívat k lepšímu pochopení důležitosti integrovaného přístupu k bezpečnosti v podnikovém prostředí.

POUŽITÁ LITERATURA

- [1] BOZPinfo. *Kategorizace prací*. [Online] 2023. Dostupné z: <https://www.bozpinfo.cz/kategorizace-praci-1>.
- [2] BOZPinfo. *Míra požárního nebezpečí a povinnosti dle zákona o požární ochraně*. [Online] 2023. Dostupné z: <https://www.bozpinfo.cz/mira-pozarniho-nebezpeci-povinnosti-dle-zakona-o-pozarni-ochrane>.
- [3] BURDA, Karel. *Základy elektronických zabezpečovacích systémů*. Brno : Akademické nakladatelství CERM, 2017. ISBN 978-80-7204-967-7.
- [4] ČSN EN ISO 9001. *Systémy managementu kvality – Požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2016, 48 s. Třídící znak 010321
- [5] ČSN EN ISO 9606-1. *Zkoušky svářečů – Tavné svařování – Část 1: Oceli*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2018, 40 s. Třídící znak 050711
- [6] ČSN EN ISO 14001. *Systémy environmentálního managementu – Požadavky s návodem pro použití*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2016, 60 s. Třídící znak 010901
- [7] ČSN EN ISO/IEC 27001. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2023, 24 s. Třídící znak 369797
- [8] FOTR, Jiří a Lenka ŠVECOVÁ. *Manažerské rozhodování: postupy, metody a nástroje*. Praha : Ekopress, 2016. ISBN 978-80-87865-33-0
- [9] Generální finanční ředitelství. *Registr dotací* [Online] 2024. Dostupné z: <https://red.financnisprava.cz/registr-dotaci/prijemci/4d9aa756-68e5-4309-9b46-a4225704d4d7>.
- [10] Justice.cz. *Veřejný rejstřík a sbírka listin* [Online] 2024. Dostupné z: <https://or.justice.cz/ias/ui/rejstrik-firma.vysledky?subjektId=667389&typ=PLATNY>.
- [11] KOLOUCH, Jan a Pavel BAŠTA. *Cybersecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7
- [12] KOTLER, Philip a Kevin Lane KELLER. *Marketing management*. Praha : Grada, 2013. ISBN 978-80-247-4150-5

- [13] KŘUPKA, Jiří, Miloslava KAŠPAROVÁ a Renáta MÁCHOVÁ. *Rozhodovací procesy*. [Online] 2024. ISBN 978-80-7395-487-9. Dostupné z: <https://e-shop.upce.cz/epub/9003854/rozhodovaci-procesy>
- [14] KYNCL, Jaromír. *BEZPEČNOST OBJEKTU ve světle moderních technologií*. Praha : Komora podniků komerční bezpečnosti ČR, 2014. ISBN 978-80-260-7115-0.
- [15] LOVEČEK, Tomáš, Ladislav MARIŠ a Anton ŠISER. *Plánovanie a projektovanie systémov ochrany objektov*. Žilina : Žilinská univerzita v Žiline, 2018. Vysokoškolské učebnice. ISBN 978-80-554-1482-9.
- [16] MASLOW, Abraham Harold. *Motivace a osobnost*. Praha : Portál, 2021. ISBN 978-80-262-1728-2.
- [17] Ministerstvo průmyslu a obchodu České republiky. *OP PIK (2014 – 2020)*. [Online] 2024. Dostupné z: <https://www.mpo.gov.cz/cz/podnikani/dotace-a-podpora-podnikani/oppik-2014-2020/>.
- [18] Ministerstvo průmyslu a obchodu České republiky. *OP TAK (2021 – 2027)*. [Online] 2024. Dostupné z: <https://www.mpo.gov.cz/cz/podnikani/dotace-a-podpora-podnikani/optak-2021-2027/>.
- [19] Ministerstvo průmyslu a obchodu České republiky. *OPPI (2007 – 2013)*. [Online] 2024. Dostupné z: <https://www.mpo.gov.cz/cz/podnikani/dotace-a-podpora-podnikani/oppi-2007-2013/>.
- [20] Ministerstvo vnitra České republiky. *Orientace v GDPR*. [Online] 2024. Dostupné z: <https://www.mvcr.cz/gdpr/clanek/co-je-gdpr.aspx>.
- [21] Ministerstvo zahraničních věcí České republiky. *Bezpečnostní strategie České republiky 2023*. [Online] 2023. Dostupné z: https://mzv.gov.cz/file/5118610/Bezpecnostni_strategie_Ceske_republiky_2023.pdf.
- [22] MONTIFER. *O nás*. [Online] 2024. Dostupné z: <https://www.montifer.cz/o-nas>.
- [23] MONTIFER s.r.o., *Cíle*, interní dokument firmy MONTIFER s.r.o., 2023
- [24] MONTIFER s.r.o., *Organizační diagram všeobecný*, interní dokument firmy MONTIFER s.r.o., 2024
- [25] MONTIFER s.r.o., *Tabulka kritérií hodnocení rizik*, interní dokument firmy MONTIFER s.r.o., 2023

- [26] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Text s významem pro EHP). In: *EUR-Lex* [právní informační systém]. Úřad pro publikace Evropské unie. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32016R0679>
- [27] NQA. *ISO 27001*. [Online] 2024. Dostupné z: <https://www.nqa.com/cs-cz/certification/standards/iso-27001-2022>.
- [28] OSHA. *O agentuře EU-OSHA*. [Online] 2024. Dostupné z: <https://osha.europa.eu/cs/about-eu-osha>.
- [29] Pelco. *Commercial Security Camera Industry Trends*. [Online] 2024. Dostupné z: <https://www.pelco.com/blog/cctv-and-video-security-camera-trends>.
- [30] Pelco. *Guide To Physical Security: Controls and Policies*. [Online] 2024. Dostupné z: <https://www.pelco.com/blog/physical-security-guide>.
- [31] Policie České republiky. *Statistické přehledy kriminality*. [Online] 2024. Dostupné z: <https://www.policie.cz/clanek/statisticke-prehledy-kriminality-za-rok-2023.aspx>.
- [32] SAK, Petr. *Úvod do teorie bezpečnosti: nekonvenční pohledy na minulost, přítomnost a budoucnost lidstva*. Praha : Petrklíč, 2018. ISBN 978-80-7229-652-1.
- [33] SelectHub. *Facility Security: A Comprehensive Guide*. [Online] 2024. Dostupné z: <https://www.selecthub.com/cmms/facility-management-cmms/facility-security/>.
- [34] SMITH, Eric. *Workplace Security Essential: A Guide for Helping Organization Create Safe Work Environments*. Waltham : Elsevier, 2014. ISBN 978-0-12-416557-1.
- [35] WolframAlpha. *Kalkulačka vlastních vektorů*. [Online] 2024. Dostupné z: <https://www.wolframalpha.com/input?i=eigenvectros>

SEZNAM PŘÍLOH

Příloha AHodnocení rizik

Příloha BHodnoty RI

Příloha A

TABULKA KRITÉRIÍ HODNOCENÍ RIZIK					
Pravděpodobnost výskytu rizika (P)	1	2	3	4	5
	výskyt nepravděpodobný	nízká pravděpodobnost	střední pravděpodobnost	vysoká pravděpodobnost	jistý výskyt
	1	2	3	4	5
Závažnost rizika (Z)	1	2	3	4	5
	velmi nepatrná	mírná	střední	vysoká	velmi vysoká
Odhalení rizika (O)	1	2	3	4	5
	odhalení je jisté	odhalení je velmi pravděpodobné	odhalení je pravděpodobné	odhalení málo pravděpodobné	odhalení nepravděpodobné
R	Míra rizika $M_R = P \times Z \times O$				
I	Hodnocení Míry rizika M_R:				
Z	U pravděpodobnosti výskytu rizika hodnotíte, jaká je pravděpodobnost, že se riziko v současnosti nebo budoucnosti vyskytne. Zavřít				
I	U závažnosti rizika hodnotíte, jak závažné by bylo riziko pro Vaši společnost, kdyby nastalo. Při hodnocení nepřihlížíte na to, jaká je pravděpodobnost rizika, tak je hodnocena zvlášť kritériem "P".				
K	U odhalení rizika hodnotíte, jaké máte ve Vaší společnosti nastaveny kontrolní mechanismy tak, abyste odhalili riziko v předstihu, tj. dříve, než nastane.				
O	K rizikům, která jste identifikovali při analýze rizik a zranitelných míst, přiřadíte hodnocení kritérií P, Z, O a spočítáte Míru rizika $M_R = P \times Z \times O$. U všech rizik, kde M_R dosáhne nebo překročí stanovenou mez významnosti, musí být definována opatření ke snížení/ odstranění rizik, zodpovědnost za realizaci těchto opatření a termíny realizace. Mez pro přijímání opatření si stanovujete sami, např. rozhodnutím vedení a může se v průběhu let měnit.				
	Přehodnocení Míry rizika M_R:				
	Přehodnocení se provádí pouze u rizik, která byla identifikovaná jako závažná (M_R dosáhla nebo překročila stanovenou mez) - u těchto rizik byla definovaná opatření ke snížení/ odstranění rizik.				
	Přehodnocení se provádí až po úplné realizaci opatření a slouží jako kontrola toho, do jaké míry opatření snížilo míru rizika M_R . Způsob přehodnocení M_R je stejný, jako při prvotním hodnocení míry rizika (při změně hodnocení rizik se nové hodnoty uvádí do sloupců PŘEHODNOCENÍ). Pokud je M_R i po přehodnocení stále vysoká, je nutné nadefinovat další opatření ke snížení míry rizika. Pokud je míra rizika po přehodnocení vyhovující, je možné opatření uzavřít a ponechat ho v evidenci s přijatelnou mírou rizika bez uvedeného opatření. Jako důkaz o tom, jak se vaše rizika vyvíjí v čase.				
	Efektivnost opatření přijatých k řešení rizik, je daná poměrem původní M_R a M_R po přehodnocení (tj. nakolik se původní míra rizika snížila).				
Poznámky:					
1) Sloupec opatření může sloužit i jako komentář pro již přijatá opatření, v tomto případě se odpovědnost a termín neuvádí, protože se jedná o standardní zavedené postupy.					
2) Při pravidelném přezkoumání Analýzy rizik a zranitelných míst můžete dřívější hodnocení kritérií P, Z, O (u hodnocení rizik)/ P, R (u hodnocení příležitosti) měnit v souvislosti s tím, jak se vyvíjí kontext vaší společnosti (tj. dříve nevýznamná rizika/ příležitosti se mohou vývojem stát více významnými a bude pro ně nutné nastavit opatření).					

Obrázek 7 – Hodnocení rizik

Zdroj: [25]

Příloha B

Rozměr matice	Autor / Autoři								
	Oak Ridge	Wharton	Golden Wang	Lane, Verdini	Forman	Noble	Tumala, Wan	Aguaron wt al	Alonso, Lamata
	Počet simulací k získání RI								
	100	500	1000	2500	-	500	-	100000	100000
3	0,382	0,58	0,5799	0,52	0,5233	0,49	0,500	0,525	0,5245
4	0,946	0,90	0,8921	0,87	0,8860	0,82	0,834	0,882	0,8815
5	1,220	1,12	1,1159	1,10	1,1098	1,03	1,046	1,115	1,1086
6	1,032	1,24	1,2358	1,25	1,2539	1,16	1,178	1,252	1,2479
7	1,468	1,32	1,3322	1,34	1,3451	1,25	1,267	1,341	1,3417
8	1,402	1,41	1,3952	1,40		1,31	1,326	1,404	1,4056
9	1,350	1,45	1,4537	1,45		1,36	1,369	1,452	1,4499
10	1,464	1,49	1,4882	1,49		1,39	1,406	1,484	1,4854
11	1,576	1,51	1,5117			1,42	1,433	1,513	1,5141
12	1,476		1,5356	1,54		1,44	1,456	1,535	1,5365
13	1,564		1,5571			1,46	1,474	1,555	1,5551
14	1,568		1,5714	1,57		1,48	1,491	1,570	1,5713
15	1,586		1,5831			1,49	1,501	1,583	1,5838

Obrázek 8 – Hodnoty RI

Zdroj: [13]