VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

ÚSTAV SOUDNÍHO INŽENÝRSTVÍ
INSTITUTE OF FORENSIC ENGINEERING

ODBOR RIZIKOVÉHO INŽENÝRSTVÍ
DEPARTMENT OF RISK ENGINEERING

ŘÍZENÍ RIZIK SPOJENÝCH S IMPLEMENTACÍ CHYTRÝCH TECHNOLOGIÍ DO PODNIKOVÝCH PROCESŮ

RISK MANAGEMENT RELATED TO THE IMPLEMENTATION OF SMART TECHNOLOGIES IN BUSINESS PROCESSES

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. Zuzana Baďurová
AUTHOR

VEDOUCÍ PRÁCE — Ing. Barbora Schüllerová, Ph.D.
SUPERVISOR

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ ÚSTAV SOUDNÍHO INŽENÝRSTVÍ

Zadání diplomové práce

Studentka:	**Bc. Zuzana Baďurová**
Studijní program:	Rizikové inženýrství
Studijní obor:	Řízení rizik firem a institucí
Vedoucí práce:	**Ing. Barbora Schüllerová, Ph.D.**
Akademický rok:	2018/19
Ústav:	Odbor rizikového inženýrství

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách a se Studijním a zkušebním řádem VUT v Brně určuje následující téma diplomové práce:

Řízení rizik spojených s implementací chytrých technologií do podnikových procesů

Stručná charakteristika problematiky úkolu:

Diplomová práce bude zaměřena na analýzu současného stavu implementace chytrých tzv. smart technologií do vybraných podnikových procesů s ohledem na rizika a způsoby jejich minimalizace. Na vybraném procesu bude následně provedena analýza rizik vč. jejich vyhodnocení a stanovení preventivních opatření.

Cíle diplomové práce:

Cílem práce bude identifikovat, analyzovat a vyhodnotit rizika, spojená se zaváděním nových technologií do vybraných podnikových procesů, zhodnocení jejich bezpečnosti, efektivity a finanční náročnosti. Na základě zjištěných výsledků, navrhnout opatření ke snížení míry rizika.

Seznam doporučené literatury:

OSTROOM, L. T., Wilhelmsen, CH.A. Risk Assessment – Tools, Techniques and Their Applications. John Wiley & Sons, 2012. 1th edition. Chichester. p. 416. ISBN 978 – 0-470-89203-9.

AVEN, Terje et al. Uncertainty in Risk Assessment: The Representation and Treatment of Uncertainties by Probabilistic and Non-Probabilistic Methods. John Wiley & Sons, 2014. 1th edition.

HOLMES, Andrew. Smart Risk. John Wiley & Sons, 2004. p. 276. ISBN 978-1-84112-507-7.

WILSON, Charlie at al. Benefits and risks of smart home technologies. Energy Policy, 2017, 103, pp. 72 – 83. ISSN 0301-4215.

HUA, B. G. Smart Cities as a Solution for Reducing Urban Waste and Pollution. 1. vyd., Hershey: Information Science Reference, 2016. s. 362. ISBN 9781522503026

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2018/19

V Brně, dne

L. S.

doc. Ing. Vladimír Adamec, CSc. vedoucí odboru	doc. Ing. Aleš Vémola, Ph.D. ředitel

Abstrakt

Diplomová práce se zaměřuje na analýzu rizik spojených s implementací chytrých technologií do podniků nevýrobního charakteru. Součástí práce je analýza současného stavu implementace Průmyslu 4.0 v České republice i v zahraničí. Na základě získaných informací jsou identifikována a zhodnocena rizika spojená s implementací Průmyslu 4.0 do prostředí ČR a do podniků nevýrobního charakteru. Konkrétně je posuzována implementace chytrých technologií do modelového podniku. Výstupem práce je návrh vhodných opatření snižujících míru rizika a posouzení efektivity a bezpečnosti při implementaci chytrých technologií do podnikových procesů.

Abstract

The diploma thesis focuses on risk assessment related to the implementation of smart technologies to non-manufacturing companies. Part of the diploma thesis is analyze of the current state of implementation Industry 4.0 in the Czech Republic and abroad. Based on the obtained information are the risks related with implementation Industry 4.0. in Czech republic and into non-manufacturing companies identified and evaluated. In this case there are assessed implementation of smart technologies in model company. Output from this thesis is proposal of appropriate strategies to reduce the risk and assessing the effectiveness and safety of implementing smart technologies into business processes.

Klíčová slova

Průmysl 4.0, hodnocení rizika, analýza, chytré technologie, podnik

Keywords

Industry 4.0, risk assessment, analysis, smart technologies, company

Bibliografická citace

BAĎUROVÁ, Z. *Řízení rizik spojených s implementací chytrých technologií do podnikových procesů*. Brno: Vysoké učení technické v Brně. Ústav soudního inženýrství, 2019. 79 s. Vedoucí diplomové práce Ing. Barbora Schüllerová, Ph.D.

Prohlášení

Prohlašuji, že svou diplomovou práci na téma „Řízení rizik spojených s implementací chytrých technologií do podnikových procesů" jsem vypracovala samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autorka uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušila autorská práva třetích osob, zejména jsem nezasáhla nedovoleným způsobem do cizích autorských práv osobnostních a nebo majetkových a jsem si plně vědoma následků porušení ustanovení § 11 a následujících autorského 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, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně .....

.....

Podpis autora

Poděkování

Na tomto místě bych ráda poděkovala vedoucí práce Ing. Barboře Schüllerové Ph.D. za její odbornou pomoc a cenné rady, které jsem využila při zpracování diplomové práce.

OBSAH

1 ÚVOD

Tato diplomová práce se zabývá tématem implementace Průmyslu 4.0 a s ním spojených chytrých, také tzv. smart technologií do podniků nevýrobního charakteru. Cílem je zhodnocením rizik implementace těchto technologií a návrh opatření pro snížení míry rizika.

V řadě průmyslově a ekonomicky vyspělých států se v posledních letech setkáváme s nástupem čtvrté průmyslové revoluce, která výrazně mění mnoho oblastí jako je průmysl, energetika, obchod a má také značný vliv na změny napříč celou společností. Tato práce je zaměřena na analýzu rizik spojených s nástupem čtvrté průmyslové revoluce a implementací chytrých technologií do podnikových procesů. Pokud se vlády vyspělých zemí ve spolupráci s podniky nezaměří na rychlý nástup těchto změn bude velmi výrazně ovlivněna jejich konkurenceschopnost a udržitelnost na trhu. Pouze v případě včasného zapojení se podniků do konceptu Průmyslu 4.0, identifikaci hrozeb a dopadů se budeme moci připravit na možná rizika a plně tak využít příležitostí, které tento fenomén přináší.

Z pohledu aktuálnosti daného tématu můžeme usoudit, že řešení této problematiky je teprve v počátcích. Samotná implementace Průmyslu 4.0 má mnohá úskalí, které nejsou dosud zcela vyřešeny včetně povědomí podniků o rizicích implementace těchto technologií. Pokud by se vedení podniku rozhodlo implementovat chytré technologie bez přípravy, může dojít k naplnění negativního scénáře. Z těchto důvodů by se podniky měly na implementaci chytrých technologií připravit a nepodceňovat ji.

Tato diplomová práce se tedy zaměřuje jak na obecné hodnocení rizik Průmyslu 4.0, tak uvádí vzorový příklad implementace do konkrétního podniku s identifikací, zhodnocením rizik a konkrétním návrhem opatření.

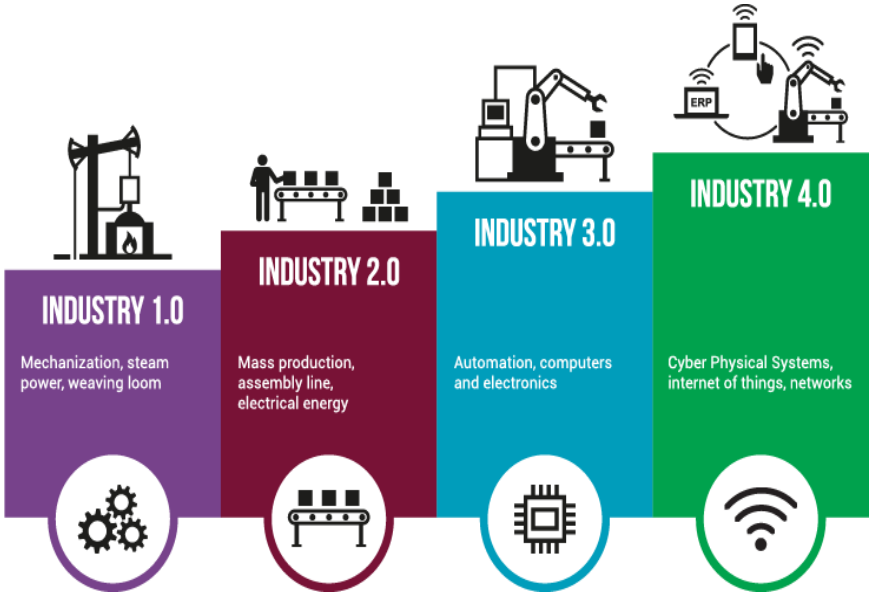
Cílem práce je na základě provedení analýzy současného stavu posoudit rizika implementace Průmyslu 4.0 do prostředí České republiky, dále budou obecně posouzena rizika spojená s implementací chytrých technologií do podniků nevýrobního charakteru a navržena vhodná opatření snižující míru těchto rizik. Na závěr bude provedena analýza rizik pro konkrétní modelový podnik implementující do svých prostor prvky chytrých technologií smart home. Pro rizika, která budou vyhodnocena jako nežádoucí nebo nepřijatelná budou navržena opatření snižující míru jejich závažnosti. Součástí práce bude také zhodnocení efektivity, bezpečnosti a finanční náročnosti implementace.

2 ANALÝZA SOUČASNÉHO STAVU

Tato část práce je zaměřena na analýzu současného stavu implementace Průmyslu 4.0. Součástí analýzy je porovnání jednotlivých přístupů k řešení jak v České republice, tak i v zahraničí, analyzování předpokladů a problémů spojených s implementací a popis konkrétních řešení pro implementaci Průmyslu 4.0 v České republice. Dále budou analyzovány možnosti využití chytrých technologií v podnicích nevýrobního charakteru. Získané poznatky budou využity v dalších částech práce.

2.1 HISTORICKÝ VÝVOJ PRŮMYSLOVÝCH REVOLUCÍ

První průmyslová revoluce započala v 18. století na základě využití páry a následné mechanizace výroby. Druhá revoluce přišla s masovou výrobou na montážních linkách na začátku 20. století. S příchodem počítačových technologií a elektronických systémů, díky nimž došlo k automatizaci výrobních linek můžeme hovořit o třetí průmyslové revoluci. Nyní stojíme na pokraji nástupu čtvrté průmyslové revoluce, se kterou přichází kyberneticko-fyzické systémy a zapojení umělé inteligence do výroby, služeb a dalších odvětví hospodářství [1].



Obr. č. 1 From industry 1.0 to industry 4.0 [1]

2.2 NÁSTUP PRŮMYSLU 4.0

V řadě průmyslově a ekonomicky vyspělých států se v posledních letech setkáváme s nástupem čtvrté průmyslové revoluce, která výrazně mění mnoho oblastí jako je průmysl, energetika a obchod ale má také značný vliv na změny napříč celou společností. Průmysl a ekonomika prochází zásadními

změnami v oblasti průmyslové výroby, implementace kyberneticko-fyzických systémů, umělé inteligence, internetu věcí do výroby, služeb a dalších odvětví. Za jádro této průmyslové revoluce je považováno propojení fyzické reality s virtuálním kybernetickým světem. V širším spektru pak můžeme tuto změnu považovat za revoluci kyberneticko-fyzicko-sociální.

Mezi významné technologie vytvářející podstatu Průmyslu 4.0 můžeme zařadit autonomní roboty, senzory, cloudové výpočty, datová úložiště, big data, aditivní výrobu, rozšířenou realitu a umělou inteligenci. V oblasti komunikace se očekává masové sdílení informací [2].

Prvotní změny konceptu výroby nastávají u velkých výrobních podniků, kde bude výrobní proces naprosto odlišný od toho stávajícího. *„Jedná se o koncept, podle kterého vzniknou „chytré továrny", které budou využívat kyberneticko-fyzikální systémy. Ty převezmou opakující se a jednoduché činnosti, které do té doby vykonávali lidé [3]."*

Stejně jako u předešlých průmyslových revolucí můžeme i u čtvrté průmyslové revoluce očekávat pozitivní dopad na životní úroveň obyvatelstva a rozvoj národních ekonomik, pokud na ně budeme dostatečně připraveni. Pokud se vlády vyspělých zemí ve spolupráci s podniky nezaměří na rychlý nástup těchto změn, nebudou v budoucnu schopny jak konkurence, tak ani udržitelnosti na trhu. V případě, že budou včas identifikovány možnosti podniků zapojit se do konceptu Průmyslu 4.0, hrozby s tím spojené a možné dopady, budeme moci se připravit na potenciální rizika a plně tak využít příležitostí, které Průmysl 4.0 přináší. Za tímto účelem jsou ve vyspělých státech formovány plány, které by měly nástup revoluce usnadnit.

2.3 IMPLEMENTACE PRŮMYSLU 4.0 V ZAHRANIČÍ

Řada vyspělých států v čele s Německem začala reagovat na nástup 4. průmyslové revoluce již před několika lety. Na Hannoverském veletrhu v roce 2011 byla představena prvotní vize německé vlády a o dva roky později pak byla představena oficiální německá platforma „Industrie 4.0". Hlavním členem této platformy je vláda zastoupena Ministerstvem hospodářství a ministerstvem pro výzkum, průmyslová oborová sdružení, výzkumné instituce a odbory. Celkově bylo na iniciativu vyčleněno 400 mil. EUR. Rozpracování iniciativy je soustředěno na oblasti výzkumu a inovace, právního rámce, bezpečnosti síťově propojených systémů, trhu práce a vzdělávání [2].

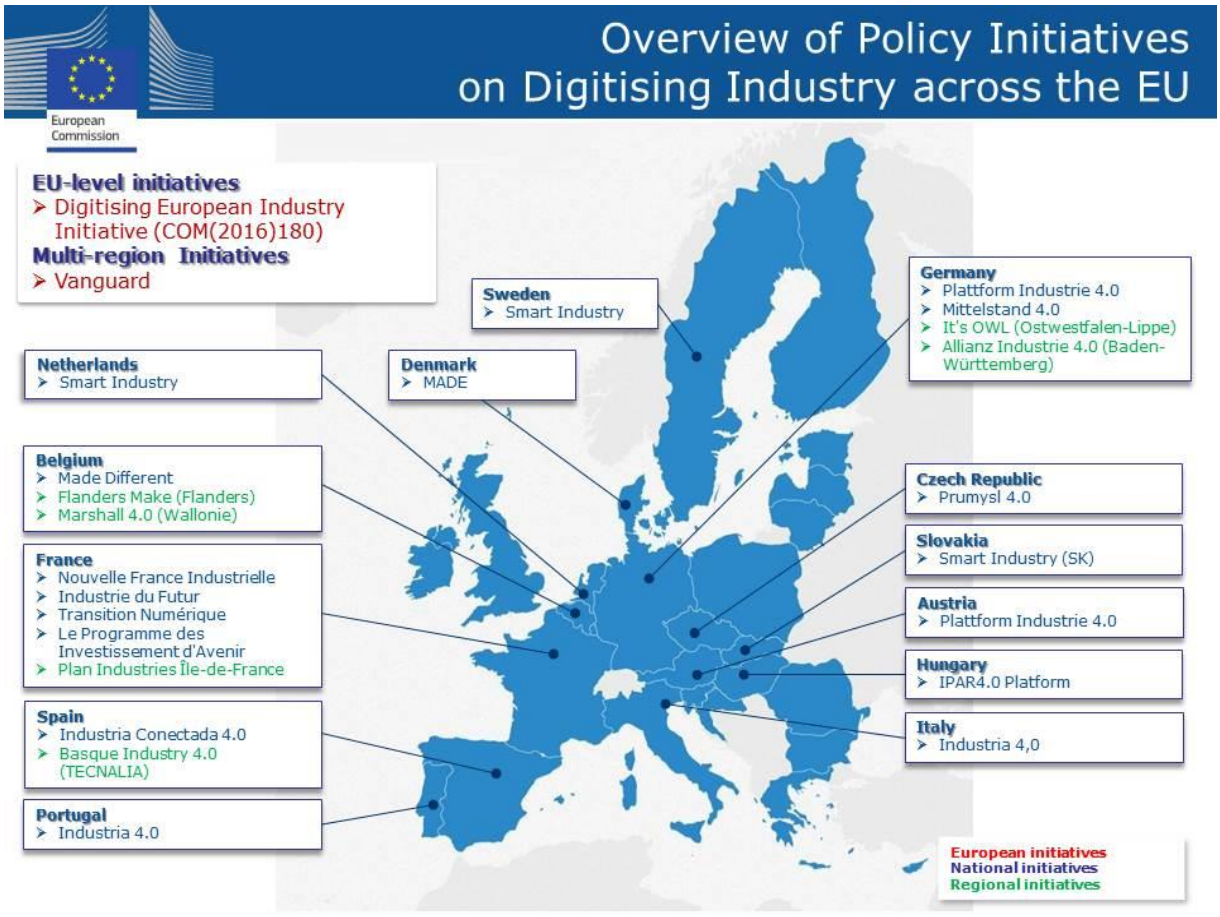
Ve Francii byla vládou spuštěna iniciativa „Industrie du Futur" s rozpočtem 730 mil. EUR. Součástí této iniciativy je jak finanční podpora malým a středním podnikům ve formě daňových úlev a zvýhodněných úvěrů, tak vzdělávání pracovníků a propagace formou uvádění příkladů využití nových technologií ve firmách do praxe. Program je primárně zaměřen na správu dat, inteligentní přístroje,

digitální bezpečnost, smart cities, nové zdroje energie a materiálu, eko-mobilitu nebo také dopravu a zdravotnictví budoucnosti [2].

Na podporu rozvoje Průmyslu 4.0 byla ve Spojených státech v toce 2012 založena platforma „Smart Manufacturing Leadership Coalition" (SMLC), jejímiž členy jsou soukromé společnosti, vláda a výzkumné a akademické instituty. Platforma se zaměřuje na transformování dosavadního průmyslu na Průmysl 4.0 ve smyslu vzájemného propojení na základě prostředí řízeného informacemi, optimalizací výrobního procesu a tím zvyšující se produktivitu a vysokou inovační aktivitu. Hlavním cílem SMLC je vytvoření kvalitní základny pro vývoj a výzkum, standardizování sdílené infrastruktury pro rozšíření inteligentní výroby s využitím pokročilé analýzy dat z inteligentních senzorů a simulaci v reálném čase. Specifikem v USA je zřízení tzv. poradního sboru „Advanced Manufacturing Partnership 2.0" , který navrhl 12 opatření převážně v oblasti vzdělání, inovací a zlepšení podmínek v oblasti podnikání [2].

V roce 2014 bylo poté v USA pěticí nadnárodních firem založena další platforma „Industrial Internet Consortium" s cílem urychlit rozvoj užívání technologií průmyslového internetu. Platforma se na prvním místě zaměřuje na zajištění vzájemné propojitelnosti a bezpečnosti systémů. Hlavními body, na které je upřena pozornost je formulování vizí, definování referenční architektury, podpora výzkumu, vytvoření bezpečnostního rámce a praktické využití průmyslového internetu [2].

Čínský program pro implementaci Průmyslu 4.0 s názvem „Made-in-China 2025" má za cíl zvyšovat podíl tamních vyráběných materiálů a komponentů ve vyráběných produktech na 70 %. Je z velké části inspirován německou platformou Industrie 4.0 [2].



Obr. č. 2 Přehled iniciativ v oblasti digitalizace průmyslu v zemích EU [4]

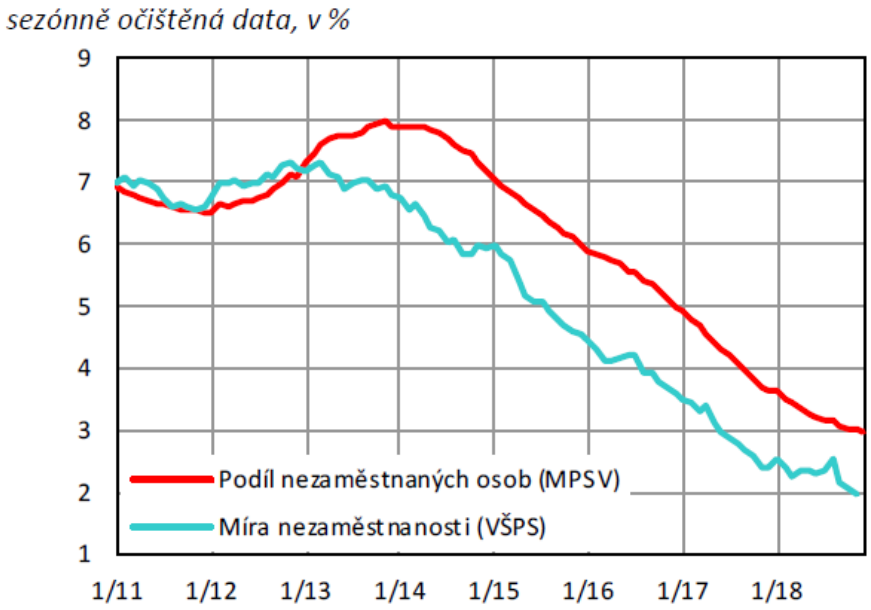
2.4 IMPLEMENTACE PRŮMYSLU 4.0 V ČESKÉ REPUBLICE

Na základě analýzy stávající situace v České republice můžeme definovat několik oblastí, které mají zásadní vliv na implementaci Průmyslu 4.0. Definování těchto klíčových oblastí je výchozím bodem pro analýzu rizik a návrh vhodných opatření.

Důležitým faktorem ovlivňujícím implementaci Průmyslu 4.0 je stav na trhu práce, jejímž ukazatelem je míra nezaměstnanosti. Nedostatek pracovní síly nebo také nutnost přijímat zaměstnance s nižší kvalifikací tlačí společnosti k rychlejšímu přechodu na automatizaci a digitalizaci firemních procesů. Vzhledem k extrémně nízké míře nezaměstnanosti je v mnoha případech omezena také samotná výroba či další expanze podniku. Proces implementace chytrých technologií by tak mohl vyřešit stávající situaci s nedostatkem pracovních sil.

Dle statistik Českého statistického úřadu (ČSÚ) a výpočtů Ministerstva financí České republiky (MF ČR) je predikce míry nezaměstnanosti pro celý rok 2018 na 2,3 %. Z důvodů dalšího poklesu v posledním čtvrtletí roku 2018 na ještě nižší hodnotu a s ohledem na pokračující růst ekonomiky pro

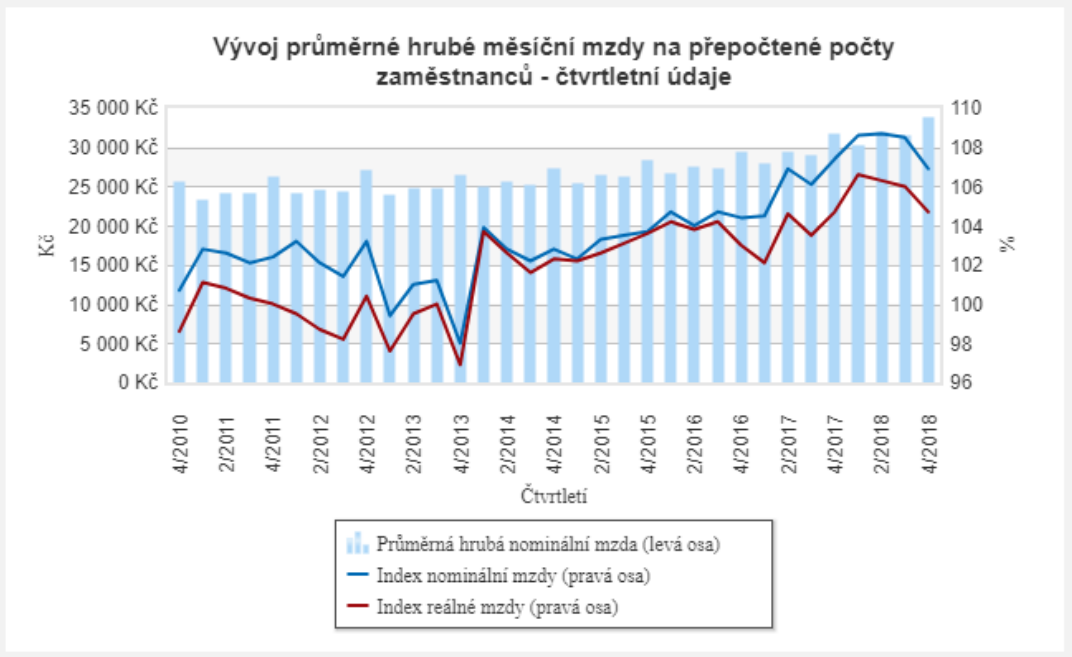
roky 2019 a 2020 je v těchto letech predikováno další snížení míry nezaměstnanosti na hodnotu 2,2 %. Celkový podíl nezaměstnaných osob za rok 2018 dosáhl 3,2 %. Pro nadcházející období je předpokládán další pokles podílu nezaměstnaných osob a to na 2,8 % v roce 2019 a na 2,6 % v roce 2020 [5]. Dle dlouhodobé prognózy je možné očekávat další pozvolné snižování nezaměstnanosti. Dlouhodobý vývoj míry nezaměstnanosti a podílu nezaměstnaných osob v ČR v jednotlivých letech je znázorněn na obrázku č.3.



Obr. č. 3 Vývoj míry nezaměstnanosti v ČR 2011-2019 [5]

Dalším faktorem pro urychlení implementace z pohledu firem je výrazný nárust mezd a zvyšování nákladů na zaměstnance. Tyto náklady mohou být optimalizovány se zavedením digitalizace a robotizace. Dle dlouhodobých prognóz ale bude mít tato změna za následek postupný úbytek pracovních míst a výrazné změny na trhu práce.

V posledních letech je celkový nárůst mezd považován za extrémní. V prvním čtvrtletí roku 2013 činila průměrná hrubá měsíční mzda na přepočtené počty zaměstnanců v národním hospodářství 23 985 Kč, v prvním čtvrtletí roku 2016 již 26 683Kč a na začátku roku 2018 vystoupala na 30 284 Kč. Ve druhém čtvrtletí 2018 činila celkem 31 851 Kč, což je o 2 515 Kč (8,6 %) více než ve stejném období roku 2017. V posledním čtvrtletí roku 2018 byl zaznamenán další výrazný nárůst a to až na 33 840 Kč [6, 7]. Přehled a srovnání vývoje průměrné hrubé měsíční mzdy je vyobrazeno na obrázku č. 4.



Obr. č. 4 Vývoj průměrné hrubé měsíční mzdy v letech 2010-2018 [6]

Česká republika patří mezi vysoce průmyslově vyspělé země. Podíl průmyslové výroby na hrubou přidanou hodnotu činí 25 %, což je téměř o 10 % více než průměr zemí EU [2]. V ekonomice ČR má průmysl velmi výrazný podíl. Tradice zpracovatelského průmyslu je zakotvena i v naší historii a podíl pracujících v tomto odvětví je výrazně vyšší než v ostatních členských zemích OECD. Dle zjištěných dat za rok 2018 je v ČR podíl zaměstnanců pracujících v průmyslu 37 % na rozdíl od členských zemí OECD, kde tento podíl činní pouhých 23 % [8].

Z pohledu implementace Průmyslu 4.0 může být vysoký podíl zaměstnanců v oblasti průmyslu výhodou z důvodu vysoké úrovně znalostí a know-how v tomto prostředí. Pokud by ovšem implementace neproběhla včas či úspěšně, mohl by tento sektor a tak i ekonomika ČR čelit existenčním problémům. Výzvou je rovněž možnost uplatnitelnosti těchto stávajících zaměstnanců v důsledku možných změn na trhu práce, které přicházejí s konceptem Průmyslu 4.0. Dle předpokladů by měla s nástupem Průmyslu 4.0 zanikat pracovní místa s nižší potřebnou kvalifikací a to především v oblasti výroby, což by mohlo způsobit dočasné zvýšení míry nezaměstnanosti. Tyto pracovní místa zaniknou z důvodu automatizace a digitalizace většiny firemních procesů.

Pro trh práce Průmyslu 4.0 je nezbytné zajistit dostatečný počet vysokoškolsky vzdělaných pracovníků a to především v technických, přírodovědných a ekonomických oborech. Dostatek specializované pracovní síly s vysokými technickými kompetencemi může ČR v budoucnu zajistit příliv nových investic zachovat stávající atraktivitu.

Pro implementaci a fungování konceptu Průmyslu 4.0 je důležité vytvářet také nová pracovní místa v souladu s nástupem digitalizace a automatizace procesů. Důležitým požadavkem v oblasti lidského kapitálu bude počítačová gramotnost a práce s informačními a novými technologiemi. V následující tabulce je vyobrazen přehled profesí s nejvyšším potenciálem pro trh práce Průmyslu 4.0.

ISCO – 3 Kód	Název profese	Index potenciálu digitalizace
252	Specialisté v oblasti databází a počítačových sítí	1,000
133	Řídící pracovníci v oblasti informačních a komunikačních technologií	0,937
251	Analytici a vývojáři softwaru a počítačových aplikací	0,845
215	Specialisté v oblasti elektrotechniky, elektroniky a elektronických komunikací	0,723
261	Specialisté v oblasti práva a příbuzných oblastech	0,675
132	Řídící pracovníci v průmyslové výrobě, těžbě, stavebnictví, dopravě a v příbuzných oborech	0,639
121	Řídící pracovníci v oblasti správy podniku, administrativních a podpůrných činností	0,631
351	Technici provozu a uživatelské podpory informačních a komunikačních technologií a příbuzní pracovníci	0,626
311	Technici ve fyzikálních a průmyslových oborech	0,626
122	Řídící pracovníci v oblasti obchodu, marketingu, výzkumu, vývoje, reklamy a styku s veřejností	0,622

Obr. č. 5 Profese s největším pozitivním potenciálem v rámci digitalizace a s nimi souvisejícími procesy [9]

2.4.1 Řešení implementace Průmyslu 4.0 v České republice

Pro udržení celkové konkurenceschopnosti České republiky a s ní spojený postupný přechod na Průmysl 4.0 je potřeba, aby vláda vytvořila a rozvíjela vhodné podnikatelské i společenské prostředí, které bude schopno využívat možností nového „digitálního světa" a bude v něm schopno obstát. Pokud by vláda včas neprováděla patřičné změny, budou výhody, které dnes Česká republika má v oblasti podnikaní považovány za nedostačující. Dále by tato situace mohla vést k výrazným makroekonomickým i sociálním problémům.

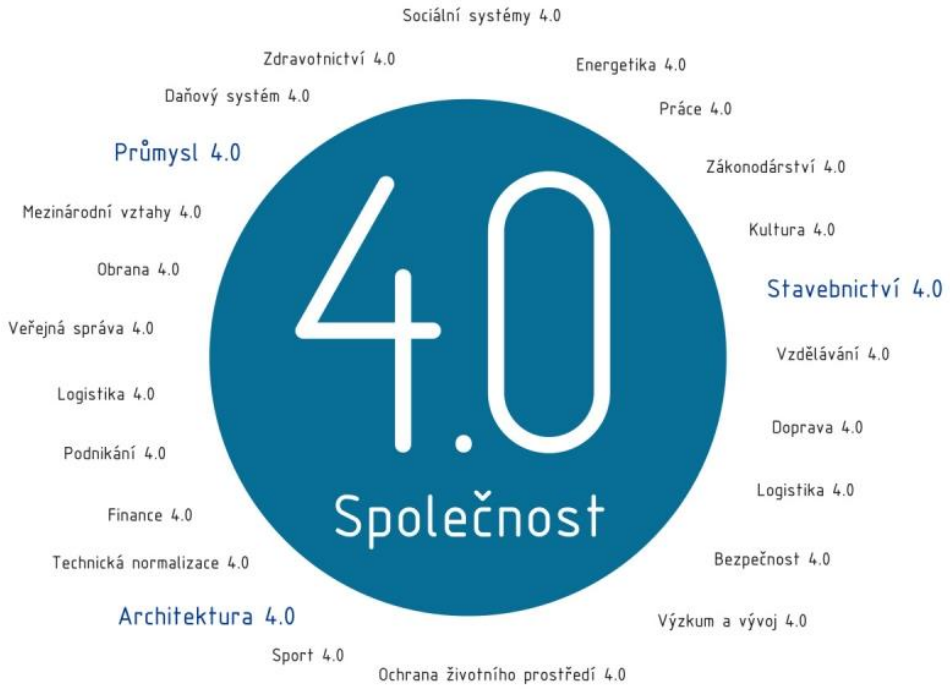
Vláda by při implementaci Průmyslu 4.0 měla pomoci hlavně v oblasti vybudování komunikační a datové infrastruktury, zavedení nových nástrojů trhu práce, změnou ve vzdělávacím systému, adaptací společenského prostředí a pomoci firmám s nutnými investicemi do know-how a nových technologií [2].

Pro implementaci čtvrté průmyslové revoluce v České republice byl vládou, konktrétně ministerstvem průmyslu a obchodu (MPO) vytvořen dokument Iniciativa Průmyslu 4.0. Tento podrobně vypracovaný dokument má podpořit procesy a reakce ČR v souvislosti s implementací Průmyslu 4.0 v České republice a zajistit tak konkurenceschopnost ČR v rámci evropských i celosvětových ekonomik. Iniciativa je rozdělena do kapitol, které popisují současný stav, směry dalšího vývoje a klíčové výzvy v jednotlivých oblastech. Z důvodu zvýšení připravenosti ČR na principy Průmyslu 4.0 je nutno tyto výzvy urgentně řešit [10]. Na Iniciativu Průmyslu 4.0 navazuje akční plán vlády ČR, který je návodem jak tuto společenskou a technologickou transformaci uskutečnit [2].

Akční plán pro Společnost 4.0 byl vytvořen v srpnu roku 2017 a je propojovacím článkem mezi iniciativami Práce 4.0, Průmysl 4.0 a Vzdělání 4.0. Tento plán představuje konkrétní opatření pro implementaci výše uvedených iniciativ. Pilíře agendy Společnosti 4.0 jsou konektivita a mobilita, vzdělávání a trh práce, elektronizace veřejné správy, bezpečnost a průmysl, podnikání a konkurenceschopnost [11].

Pro podniky jsou velmi důležitými iniciativami Firma 4.0 a Expedice 4.0. Iniciativa Firma 4.0 připravuje workshopy pro vedení podniků a představuje inovativní myšlenky expertů vztahující se k jednotlivým tématům Průmyslu 4.0. Uvádí příklady, jak v implementaci postupují jiné společnosti a uvádí doporučení pro jednotlivé kroky implementace. Expedice 4.0 je program, který zajišťuje exkurze do podniků, které již s prvky chytrých technologií pracují. Tyto podniky názorně představují, jak zavádějí prvky Průmyslu 4.0. [12].

S příchodem nových technologií zaznamenává naše společnost změny nejen v oblasti ekonomiky ale také v samotném způsobu našeho života. Na rozdíl od předcházejících průmyslových revolucí, které přinesly zásadní změny hlavně v oblasti průmyslové výroby můžeme čtvrtou průmyslovou revoluci považovat za celospolečenskou změnu zasahující do celé řady oblastí průmyslu, bezpečnosti, nových obchodních modelů a řízení, technické standardizace, systému vzdělávání, vědy a výzkumu, trhu práce, právního rámce až po sociální systém. Následkem změn v těchto oblastech můžeme hovořit transformaci na Společnost 4.0 [2].



Obr. č. 6 Společnost 4.0 [13]

2.5 VYUŽITÍ CHYTRÝCH TECHNOLOGIÍ V NEVÝROBNÍM ODVĚTVÍ

S příchodem Průmyslu 4.0 nastávají v sektoru služeb změny spojené zejména s využíváním internetu věcí, internetu služeb, zpracování velkých dat a nové formy obchodních modelů a komunikace se zákazníkem. Tyto technologie představují pro firmy nové příležitosti ve formě inovování starých, či vytváření nových forem v oblasti zacílení a péče o zákazníka. Největší rozvoj nových technologií je zaznamenán v zákaznickém servisu, elektronickém obchodování nebo v systémech, které spojují sociální sítě s analýzou velkých dat [10]. Tyto nové technologie poskytují firmám orientujícím se na služby správné zacílení na zákazníky vedoucí k následnému využívání služby, kvalitní zákaznický servis a péči.

Změny spojené s konceptem průmyslu 4.0 v oblasti poskytování služeb a péče o zákazníka díky vysokorychlostního připojení k internetu, připojení k sociálním sítím a nepřeberné množství informaci zapříčinily, že si zákazník zvyká na rychlý způsob komunikace s firmou a rychlé dodání výrobků a služeb. Pokud firmy na tyto nové možnosti komunikačních technologií se zákazníkem včas nereagují, vystavují se riziku ztráty zákazníků.

V posledních letech můžeme celosvětově zaznamenat obrovský nárůst tzv. P2P (peer-to-peer) projektů („rovný s rovným"), které nahrazují klasický vztah mezi firmou a zákazníkem, a naopak zprostředkovávají vztah dvou rovnocenných uživatelů v podmínkách tzv. sdílené ekonomiky. S využitím

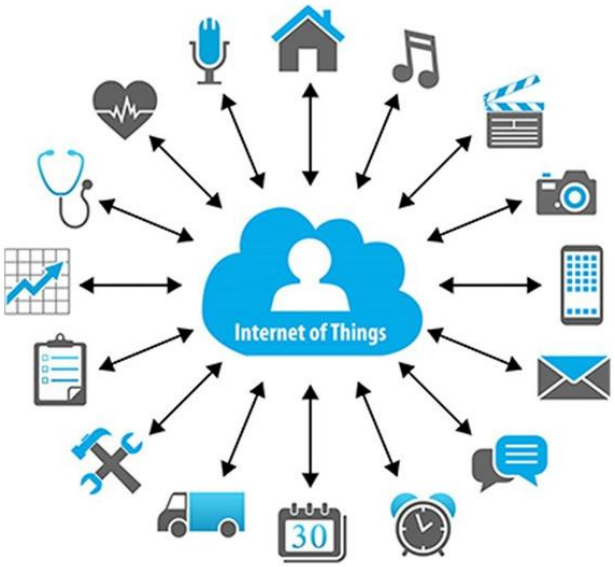
tzv. peer to peer transakcí je možné uspokojit rostoucí poptávku po službách bez nutnosti investování do nového vybavení. Výhodami pro uživatele i poskytovatele služeb ve sdílené ekonomice je dosažení lepších podmínek, než v rámci klasického vztahu poskytovatele a konzumenta služby [2]. Dle předpokladů by se měl objem prostředků tekoucí přes sdílenou ekonomiku do roku 2025 vyrovnat klasickým obchodním modelům. Z těchto předpokladů můžeme soudit, že význam těchto forem podnikání může v budoucnu výrazně převažovat [14].

Využívání nových technologií může pro tyto firmy do budoucna znamenat nejen konkurenční výhodu v oblasti zacílení, prodeje a péče o zákazníka, ale také možnost výrazného ušetření provozních nákladů. S rozvojem smart home (chytrá domácnost) smart grid (chytrá síť), využitím internetu věcí a senzorů mohou být výrazně regulovány náklady na energie, suroviny a pracovní sílu. Ušetření provozních nákladů může být velmi výrazné u podniků zabývajících se poskytováním služeb v oblasti ubytování či gastronomie. U těchto podniků mohou být využity technologie pro chytré domácnosti, zabezpečení objektů, čerpání energií přes chytré sítě, využití chytrých skladů, chytrých kanceláří, senzorů, internetu věcí a mobilních aplikací.

2.5.1 Využití internetu věcí

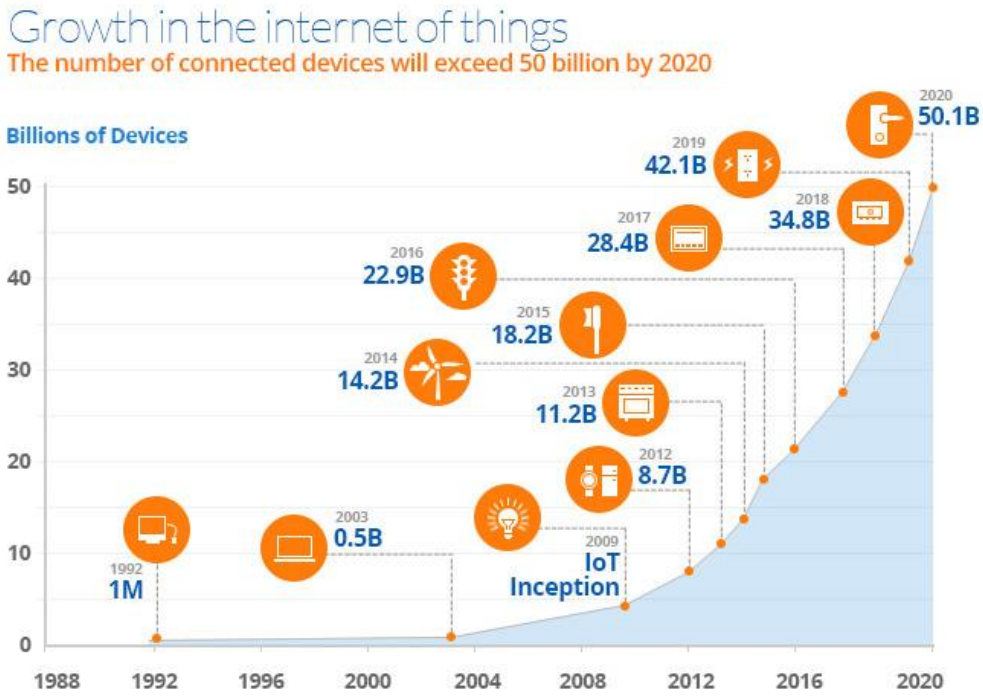
Internetem věcí (Internet of Things, IoT) je nazýván koncept, který zahrnuje velké množství objektů neboli „věcí", která pracují v rámci v vlastní sítě nebo internetové infrastruktury. Propojení mezi těmito objekty zajišťuje drátová nebo bezdrátová síť a rozlišení těchto objektů je zajištěno přiřazenou adresou dle příslušného schématu adresování. Vytvořená síť zajišťuje nejen vzájemnou komunikaci mezi objekty, ale také možnost reakce objektu na vykonávané úkony jiného objektu. Díky vzájemnému propojení jsou jednotlivé objekty schopny dosáhnout společných cílů. Díky internetu věcí můžeme hovořit o inteligentním prostředí, ve kterém je umožněno „věci" se spojit s ostatními objekty s využitím síťové cesty či služby [15].

Zařízení propojená tímto způsobem zajišťují sběr velkého objemu dat, která se po zpracování využívají v oblastech energetiky, zdravotnictví, logistiky a dopravy. Velký význam má tato technologie v oblasti chytrých elektroinstalací a jejich využití v konceptu smart home [16].



Obr. č. 7 Koncept internetu věcí [17]

Dle statistik je současný vývoj v těchto oblastech na výrazném vzestupu. V roce 2016 bylo zaznamenáno 1,6 bilionu zařízení připojených k internetu. Tento počet se však každým rokem výrazně zvyšuje. Počet zařízení připojených k internetu do roku 2020 se odhaduje až na 50 biliónů. Třetinu těchto zařízení by měly tvořit smartphony a televize, další dvě třetiny senzory a jiná chytrá zařízení. S počtem připojených zařízení bude také růst trh internetu věcí, do roku 2020 by měl vzrůst částku 1,7 bilionu dolarů [18].



Obr. č. 8 Nárůst zařízení připojených k IoT [19]

Využití internetu věcí se stává běžnou součástí dnešního světa a zasahuje do mnoha odvětví.

Chytrý průmysl a automatizace průmyslové výroby

- využití IoT při realizaci konceptu Průmysl 4.0
- budování chytrých továren
- autonomní roboti

Chytrá domácnost

- Vzdálené ovládání domácnosti přinášející komfort v ovládání osvětlení, zavlažování, topení, ovládání rolet a žaluzií a další
- Sledování spotřeby vody a energií sloužící k optimalizaci spotřeby a finančním úsporám
- Bezpečnostní systémy proti neoprávněnému vniknutí a protipožární ochrana
- Sledování skladovacích podmínek zejména v prostorách, kde se pracuje s potravinami.

Chytrá města

- Inteligentní dopravní komunikace, které budou řidiče informovat o plynulosti provozu, dopravních nehodách, potenciálním nebezpečí či překážkách a vlivech počasí.
- Chytrý systém parkovacích míst, který bude řidiče informovat a počtu volných parkovacích míst ve městech a jejich GPS poloze. Řidiči tak budou moci vyhledat parkovací místo rychleji a nezpomalovat tak provoz na komunikacích.
- Monitoring dopravy, který bude sledovat vytíženost jednotlivých komunikací a optimalizovat tak dopravu.
- Inteligentní systém osvětlení, který bude ve městech fungovat v závislosti na počasí, denní době, viditelnosti a pohybu chodců pod osvětlením.

Chytrý systém měření

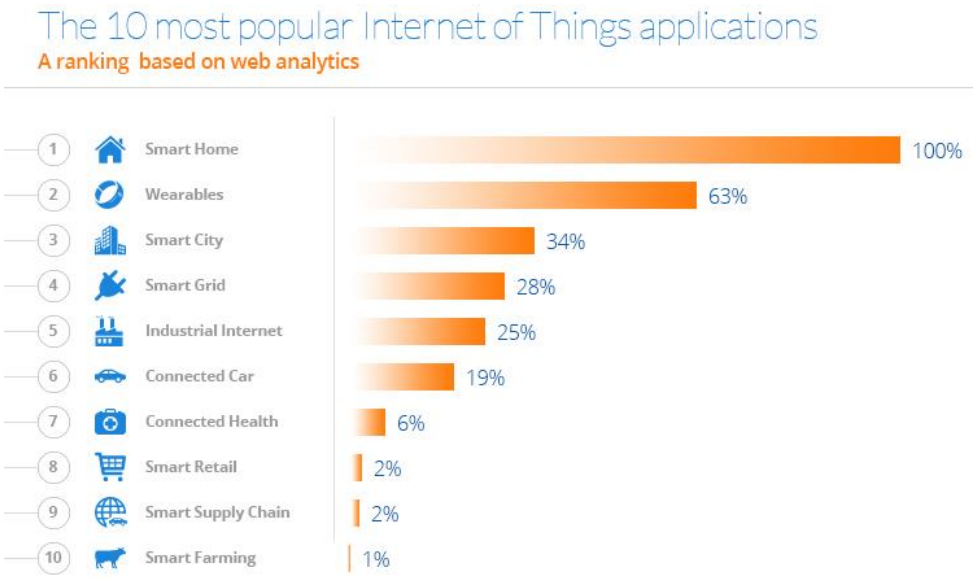
- Inteligentní rozvodná elektrická síť s výhodami měření a řízení spotřeby energie v reálném čase
- Inteligentní fotovoltaická síť s výhodou optimalizace výkonu solární energie.
- Chytré měření ve firmách zaměřené na optimalizaci ale také sledování úniku energií, monitorování stavu paliv, plynů a ostatních provozních energií.

– Měření tlaku ve vodovodní síti za účelem zjišťování úniku vody a haváriím ve vodovodní síti.

Chytrý způsob zabezpečení a ochrany objektů

– Kontrola přístupu a detekování osob povoluje přístup do objektů pouze určeným osobám a monitoruje pohyb osob v prostorách s omezeným přístupem.
– Monitorování výskytu nebezpečných látek upozorňuje na zvýšené koncentrace těchto látek obzvláště v průmyslových podnicích.
– Monitorování vlhkosti v objektu zabraňuje poškození např. uskladněného majetku podléhajícímu zkáze působením vody a vlhkosti [20].

Další možnosti uplatnění konceptu internetu věcí se využívají také v oblasti zdravotnictví, zemědělství, logistiky, obchodu a životního prostředí.



Obr. č. 9 Nejčastější využití IoT [19]

3 FORMULACE PROBLÉMŮ A STANOVENÍ CÍLŮ ŘEŠENÍ

Cílem práce je zhodnocení současného stavu při implementaci Průmyslu 4.0 a „smart" technologií do podnikových procesů. Na základě získaných informací o této problematice je provedena identifikace, analýza a vyhodnocení rizik, které jsou spojeny s implementací těchto technologií do firemního prostředí. Konktrétně je zhodnocena bezpečnost, efektivita a finanční náročnost implementace. Na základě zjištěných výsledků jsou navržena opatření ke snížení míry rizika a stanovena preventivní opatření. Daná problematika je řešena pomocí vybraných metod pro analýzu rizik a následně porovnána. Výstupem práce je návrh na ošetření rizik.

Z pohledu aktuálnosti daného tématu můžeme usoudit, že řešení této problematiky je teprve v počátcích. První dokumenty a platformy vytvořené na účelem implementace Průmyslu 4.0 vznikají teprve od roku 2013. Samotná implementace Průmyslu 4.0 má mnohá úskalí, které nejsou dosud zcela vyřešeny například otázky bezpečnosti práce, digitalizace, zabezpečení soukromí, právních norem a podobně.

Velkým problémem je také finanční náročnost spojena s přechodem na nové technologie především pro malé a střední firmy a také absence vzorových příkladů firem, které nové technologie využívají. Pokud takovéto firmy najdeme, tak převážně v oblasti průmyslové výroby, méně rozšířené jsou pak v oblasti služeb. Mnoho firem také nemá povědomí o možnostech, které implementace Průmyslu 4.0 přináší a nemají tak motivaci ke změně stávajícího systému. Do budoucna by tyto technologie pro firmu mohly být výraznou konkurenční výhodou.

V této práci bude uveden vzorový příklad firmy nevýrobního charakteru s návrhy implementace smart technologií a jejich posouzení. Výstupem tedy bude návrh pro implementaci chytrých technologií do firmy nevýrobního charakteru.

Nejvíce řešenými tématy ve spojitosti s implementací chytrých technologií ve firmách jsou počáteční investice, kyberbezpečnost, normy a standardizace, bezpečnost práce, překážky na trhu práce (nízká nezaměstnanost) a nekvalifikovaní pracovníci.

4 POUŽITÉ METODY A JEJICH ZDŮVODNĚNÍ

V této kapitole jsou popsány jednotlivé metody analýzy rizika, které budou v diplomové práci použity k řešení zadaného problému. K celkovému zhodnocení implementace Průmyslu 4.0 v prostředí České republiky a zhodnocení rizik při implementaci v podnicích nevýrobního charakteru je zvolena metoda rozšířené SWOT analýzy a metoda RIPRAN. Pro analýzu rizik implementace chytrých technologií ve vzorovém podniku je zvolena metoda WHAT IF a FMEA.

4.1 SWOT ANALÝZA

Hlavním principem SWOT analýzy je určení jak silných a slabých stránek, tak i příležitostí a hrozeb vztahujících se k dané společnosti. Informace, ze kterých SWOT analýza čerpá vycházejí z analýzy prostředí a větví se na interní a externí analýzu. Interní analýza definuje silné a slabé stránky, zatímco externí analýza má za cíl identifikovat příležitosti a hrozby. SWOT analýza bývá součástí komplexní analýzy, ale v některých případech může být také vytvořena jako samostatný krok [21].

Faktory patřící do externí analýzy jsou identifikovány při analýze makroprostředí, konkrétně v oblasti ekonomiky, technologie, legislativy, demografie, kultury, sociologie nebo ekologie. Zkoumány jsou faktory jak národního a zahraničního prostředí tak i globální situace, která je významná pro strategický záměr společnosti. Tyto faktory zařazujeme do příležitostí a hrozeb pro danou společnost. *„Cílem interní analýzy je nejen objektivně zhodnotit současné postavení firmy, ale posoudit i její potenciál realizovat uvažovaný strategický záměr* [22]."

Metoda SWOT byla zvolena pro analýzu rizik a určení vhodné strategie při implementaci Průmyslu 4.0 do prostředí ČR. Z důvodu velkého přesahu tohoto fenoménu do ekonomické a sociální roviny je třeba zhodnotit následky nástupu Průmyslu 4.0 i v národním a nadnárodním ohledu. Metoda bude posuzovat důležitosti jednotlivých faktorů související s nástupem Průmyslu 4.0. Cílem metody SWOT je určení vhodné strategie, kterou by se měla ČR při implementaci řídit.

4.2 METODA RIPRAN

Metoda RIPRAN (Risk Project Analysis) je jednoduchá empirická metoda, sloužící převážně k analýze středních a velkých projektů. Metoda vychází z procesního pojetí analýzy rizika. Zpracování analýzy rizik projektu se provádí před jeho vlastní implementací, ale může být použito i v jakékoli fázi projektu. Metoda neřeší proces monitorování rizik v projektu, ale posuzuje jejich důležitost.

Analýza rizik metodou RIPRAN se skládá z následujících fází:

- Identifikace rizika
- Kvantifikace rizika
- Reakce na riziko
- Celkové zhodnocení rizika [23]

Metoda RIPRAN je zvolena pro analýzu rizik při implementaci chytrých technologií do podniků nevýrobního charakteru. Implementaci chytrých technologií můžeme považovat za střední až velký projekt podniků, jehož rizika je nutné identifikovat, kvantifikovat a ošetřit před samotným zahájením implementace. V rámci této metody budou zvolena vhodná typová opatření ke snížení rizika.

4.3 METODA WHAT- IF

Analýza je zpracována formou brainstormingu na základě názorů, zkušeností a znalostí odborníků nebo zkušených pracovníků. Metoda funguje na základě pokládání otázek „Co se stane, když..?" a hledají se odpovědi na tyto otázky. V rámci porady a diskuze se hledají možné negativní dopady jednotlivých vzniklých situací včetně doporučení a návrhu opatření k jejich eliminaci.

Metoda WHAT IF bude v této práci využita pro hledání rizik při implementaci chytré technologie v konkrétní vzorové firmě. Rizika budou zpracována pro oblast implementace prvku smart home do restauračního zařízení. Brainstorming bude probíhat po konzultaci s pracovníkem firmy dodávající prvky smart home za účasti majitele a vedoucího provozu.

4.4 FMEA

FMEA (Failure Mode and Efekt Analysis) je analýza možných vad a jejich důsledků. Cílem je identifikovat možná rizika a vady související s novým výrobkem nebo procesem, jejich hodnocení a následná minimalizace rizik. Metoda může být zaměřena na analýzu výrobků nebo analýzu procesů.

Princip metody FMEA spočívá ve dvou částech. V první části probíhá identifikace rizika, během které se experti zaměřují na hledání potenciálních chyb, bez ohledu na jejich závažnost či pravděpodobnost vzniku a hledají možné příčiny a následky chyb. Druhá fáze je naopak soustředěna na výpočet míry rizika a je určeno tzv. prioritní rizikové číslo (PRČ), které je součinem bodového hodnocení výskytu, významnosti a odhalitelnosti [24].

Metoda FMEA bude využita pro analýzu rizik při implementaci prvků smart home v konkrétním restauračním zařízení. Zvolená metoda by měla identifikovat možné poruchy při procesu implementace smart technologií a jejich důsledky. Následně jsou navržena vhodná opatření ke snížení míry rizika.

5 DOSAŽENÉ VÝSLEDKY

V této kapitole jsou na základě vybraných materiálů a metod zpracovány analýzy rizik a zjištěny vlastní výsledky práce. Pro analýzu rizik implementace Průmyslu 4.0 byla použita SWOT analýza, metoda RIPRAN, metoda WHAT IF a FMEA.

5.1 SWOT ANALÝZA

Jednotlivé faktory interní i externí analýzy jsou uspořádány do matice.

Tab. č. 1 SWOT analýza implementace Průmyslu 4.0 [autor]

Silné stránky		**Slabé stránky**	
S1	ČR patří mezi vysoce průmyslově vyspělé země s vysokým podílem průmyslové výroby (zkušenosti a know-how na vysoké úrovni)	W1	Nedostatečná digitalizace a pokrytí ČR vysokorychlostním internetem
S2	Nízká míra nezaměstnanosti a zvyšující se náklady na zaměstnance	W2	Malé a střední podniky nedisponují dostatečnými prostředky do investic souvisejících s implementací Průmyslu 4.0
S3	Vysoká úroveň vzdělání na vysokých školách technického charakteru	W3	Nedostatečná představa o ekonomické efektivitě implementace Průmyslu 4.0
S4	Zájem státu podporovat inovace a investovat do výzkumu.	W4	Nedostatek kvalifikované pracovní síly (ubývá studentů technických oborů)

Příležitosti		Hrozby	
O1	Získání konkurenční výhody na trhu	T1	Nepříznivé změny na trhu práce.
O2	Zájem nových investorů	T2	Systém vzdělávání nebude schopen rychle reagovat na změny související s implementací Průmyslu 4.0.
O3	Vznik nových pracovních pozic	T3	Nevyřešena otázka kybernetické bezpečnosti
O4	Podílet se na tvorbě nových technologických řešení	T4	Vznik sociálních a ekonomických propastí ve společnosti

Dále je porovnána důležitost jednotlivých znaků na základě třístupňového hodnocení.

0	znak je méně důležitý než porovnávaný znak
0,5	váha znaků je rovna
1	znak je důležitější než porovnávaný znak

Tab. č. 2 Porovnání důležitosti silných stránek [autor]

	S1	S2	S3	S4	**Celkem**	**Váha**
S1	X	0	0,5	0	0,5	8 %
S2	1	X	1	0,5	2,5	42 %
S3	0,5	0	X	0,5	1	17 %
S4	1	0,5	0,5	X	2	33 %
Celkem	2,5	0,5	2	1	6	100 %

Tab. č. 3 Porovnání důležitosti slabých stránek [autor]

	W1	W2	W3	W4	**Celkem**	**Váha**
W1	X	1	1	0,5	2,5	42 %
W2	0	X	0,5	0,5	1	17 %
W3	0	0,5	X	0	0,5	8 %
W4	0,5	0,5	1	X	2	33 %
Celkem	0,5	2	2,5	1	6	100 %

Tab. č. 4 Porovnání důležitosti příležitostí [autor]

	O1	O2	O3	O4	**Celkem**	**Váha**
O1	X	0,5	1	1	2,5	42 %
O2	0,5	X	1	1	2,5	42 %
O3	0	0	X	0,5	0,5	8 %
O4	0	0	0,5	X	0,5	8 %
Celkem	0,5	0,5	2,5	2,5	6	100 %

Tab. č. 5 Porovnání důležitosti hrozeb [autor]

	T1	T2	T3	T4	**Celkem**	**Váha**
T1	X	0,5	0	0,5	1	16 %
T2	0,5	X	0,5	1	2	33 %
T3	1	0,5	X	1	2,5	41 %
T4	0,5	0	0	X	0,5	8 %
Celkem	2	1	0,5	2,5	6	100 %

Stanovení důležitosti jednotlivých znaků a následné přiřazení hodnoty bylo provedeno na základě brainstormingu, který byl zaměřen na posouzení důležitosti jednotlivých faktorů SWOT analýzy.

Na základě porovnání důležitosti jednotlivých znaků jsou zjištěny váhy jednotlivých silných stránek, slabých stránek, příležitostí a hrozeb. Nejsilnějšími stránkami jsou za základě zjištěných vah nízká míra nezaměstnanosti a zvyšující se náklady na zaměstnance (S2, 42 %) a zájem státu podporovat inovace a investovat do výzkumu (S4, 33 %). Tyto silné stránky mají vliv především na rychlost s jakou bude Průmysl 4.0 implementován. Nejvýznamnější slabou stránkou při zavádění Průmyslu 4.0 je nedostatečná digitalizace a pokrytí ČR vysokorychlostním internetem (W1, 42 %) a také nedostatek kvalifikované pracovní síly (W4, 33 %). Nejvýznamnějšími příležitostmi jsou možnosti získání konkurenční výhody na trhu (O1, 42 %) a zájem nových investorů (O2, 42 %). Z hlediska možných hrozeb byly identifikovány dvě nejzávažnější a to nevyřešená otázka kybernetické bezpečnosti (T3, 41 %) a možnost že systém vzdělávání nebude schopen rychle reagovat na změny související s implementací Průmyslu 4.0 (T2, 33 %).

Dále je posuzována a hodnocena intenzita vzájemných vztahů. Jednotlivé položky jsou zapsány do čtvercové matice a hodnotí se vztah mezi položkami vnitřních a vnějších faktorů. Škála pro hodnocení je v rozmezí 1 (není vztah mezi položkami) až 5 (silný vztah mezi položkami). U negativních vztahů je použito záporné znaménko.

Tab. č. 6 Posouzení vzájemných vztahů [autor]

Externí faktory	**Interní faktory**										
	Silné stránky						**Slabé stránky**				
		S1	S2	S3	S4	∑ O,T/S	W1	W2	W3	W4	∑ O,T/W
	O1	3	3	3	4	13	3	3	3	3	12
	O2	5	3	4	5	17	4	1	2	4	11
	O3	2	5	5	4	16	3	3	1	-4	3
	O4	4	2	4	5	15	2	3	2	3	10
	O/S, W	14	13	16	18	61	12	10	8	6	36
	T1	1	-4	0	0	-3	0	2	2	-4	0
	T2	1	0	3	1	5	1	0	0	-5	-4
	T3	0	0	1	4	5	4	2	0	1	7
	T4	2	1	1	0	4	2	1	0	2	5
	T/S, W	4	-3	5	5	11	7	5	2	-6	8

Tab. č. 7 Výsledky posouzení vzájemných vztahů [autor]

	Silné stránky	Slabé stránky
Příležitosti	**61**	36
Hrozby	11	10

Na základě zjištěných výsledků rozšířené SWOT analýzy je identifikována vhodná strategie.

Tab. č. 8 SWOT analýza - volba strategií [25]

		Analýza vnitřního prostředí	
		Silné stránky (S)	Slabé stránky (W)
Analýza vnějšího prostředí	Příležitosti (O)	**Max-Max strategie** (růstově orientovaná strategie)	Min-Max strategie (turnaround strategie)
	Hrozby (T)	Max-Min strategie (diverzifikační strategie)	Min- Min strategie (obranná strategie)

Z provedené SWOT analýzy bylo zjištěno, že nejvýraznější vztah je vytvořen mezi silnými stránkami a příležitostmi. Na základě těchto zjištění by měla být zvolena růstově orientovaná strategie Max-Max (SO). Při implementaci Průmyslu 4.0 by se mělo zaměřit na maximalizaci silných stránek a příležitostí.

5.2 METODA RIPRAN

V první fázi metody RIPRAN jsou identifikována rizika, které mohou nastat ve spojitosti s implementaci chytrých technologií do podnikových procesů. Tato analýza je konkrétně zaměřena na projekt implementace v podnicích nevýrobního charakteru. Identifikace rizik byla provedena v následujících oblastech:

Tab. č. 9 Kategorie členění rizik [autor]

I.	Pracovní síla
II.	Vzdělání
III.	Náklady
IV.	Kybernetická bezpečnost
V.	Technologické předpoklady
VI.	Provozní rizika

Součástí identifikace rizik je sestavení přehledu hrozeb a určení scénářů, které mohou nastat a ohrozit tak průběh projektu implementace. Tyto údaje se následně zapisují do tabulky [26].

Tab. č. 10 Metoda RIPRAN – Identifikace nebezpečí projektu [26]

Poř. číslo rizika	Hrozba	Scénář	Poznámka
1.	Výskyt chřipkové epidemie v jarním období březen-duben	Onemocnění skoro 30% zaměstnanců	Předpokládáme počasí podle předpovědi jako v předchozím roce

Hrozbou je zde konkrétní projev nebezpečí např. výskyt chřipkové epidemie. Scénářem se rozumí děj, který nastane v důsledku výskytu hrozby např. zaměstnanci onemocní.

Tab. č. 11 RIPRAN Identifikace rizik při implementaci chytrých technologií [autor]

ID	Kategorie	Hrozba	Scénář
I.1	**Pracovní síla I.**	Nedostatek kvalifikovaných pracovníků	Omezena implementace chytrých technologií, omezení chodu firmy, omezení expanze, finanční ztráty
I.2		Nízká kvalifikace zaměstnanců	Zaměstnanec nemá dostatečnou kvalifikaci pro práci s chytrými technologiemi, dopouští chyb v důsledku nízké kvalifikace a praxe
I.3		Nízké vzdělání zaměstnanců	Zaměstnanec není schopen naučit se pracovat s novými technologiemi

ID	Kategorie	Hrozba	Scénář
I.4		Neochota se učit novým postupům	Zaměstnanec používá staré postupy metody, neefektivita, vyšší náklady
I.5		Neochota zaškolování se pro práci s novými technologiemi	Zaměstnanec nemá motivaci a snahu změnit pracovní postupy.
II.1	**Vzdělání II.**	Malé povědomí o Průmyslu 4.0 mezi studenty	Pomalý rozvoj vzdělávání zaměřeného na dovednosti potřebné pro práci s chytrými technologiemi
II.2		Nedostatečné znalosti v IT technologiích	Zaměstnanci nejsou schopni plnit náročnější úkony, ovládají jen běžné uživatelské znalosti
II.3		Snižující se počet studentů technických a IT oborů	Nedostatek kvalifikovaných zaměstnanců pro potřeby Průmyslu 4.0
II.4		Systém vzdělávání zaostává za potřebami Průmyslu 4.0	Nedostatek kvalifikovaných zaměstnanců pro potřeby Průmyslu 4.0

ID	Kategorie	Hrozba	Scénář
II.5		Stávající zaměstnanci zaostávají za potřebami Průmyslu 4.0	Stávající zaměstnanci nejsou kompetentní k daným úkolům. Neabsolvovali potřebná zaškolení, kurzy a konference určené k práci s novými technologiemi.
II.6		Malé povědomí o možnostech Průmyslu 4.0 mezi manažery	Nedostatek informací potřebných k zahájení procesu implantace chytrých technologií do podniku
III.1	**Náklady III.**	Společnost nedisponuje dostatečnými prostředky do implementace chytrých technologií	Možná ztráta konkurenční výhody
III.2		Vysoké náklady spojené s nákupem, instalací a správou chytrých technologií	Finančně velmi náročné, zadlužení podniku, obavy spojené s návratností investice
III.3		Vysoké náklady spojené s digitalizací, pořízením a správou datových úložišť, cloudů a serverů	Finančně velmi náročné, zadlužení podniku, obavy spojené s návratností investice
III.4		Vysoké náklady spojené se zaškolením zaměstnanců	Časově a finančně nepříznivé pro chod společnosti, zanedbání práce, odkládaní pracovních úkolů, finanční ztráty

ID	Kategorie	Hrozba	Scénář
III.5		Prodlení a ztráty omezující běžný chod při implementaci nových technologií do podnikových procesů	Nutnost omezení provozu, prodlení služeb ve vztahu k zákazníkům z důvodu implementace nových technologií, finanční ztráta, postihy za nedodržení termínů, ztráta klienta
III.6		Nedostatečná představa o ekonomické efektivitě implementace	Neochota vedení podniku investovat do implementace z důvodu nedostatku informací o efektivitě a vzorových podniků
III.7		Vysoké náklady na zajištění kybernetické bezpečnosti	Nutnost zřízení úseku zabývající se kybernetickou bezpečností, náklady na školení zaměstnanců v této problematice
IV.1	**Kybernetická bezpečnost IV.**	Společnost je napadena formou Malware	Po napadení malwarem může dojít k vydírání, k těžbě kryptoměn, napadení routerů, napadení bankovnictví (finanční a reputační riziko, narušení soukromí)
IV.2		Slabě zabezpečená cloudová úložiště	Velké množství dat produkované podniky může být z cloudu jednoduše ukradeno a zneužito (důležitá firemní data, údaje o klientech)
IV.3		Používání jednofaktorových hesel (jednoduchá autentizace)	Zabezpečení jednofaktorovým heslem je lehce zneužitelné (např. krádež zaznamenaného hesla)

ID	Kategorie	Hrozba	Scénář
IV.4		Nasazení IoT do prostředí s minimálním zabezpečením	Zneužití v podobě získání přístupu do vnitřní sítě podniku za účelem krádeže dat nebo ovládnutí jednotlivých prvků připojených do sítě. Způsobuje ztráta kontroly nad technologiemi, zneužití dat a narušení soukromí (odposlechy, kamerové záznamy, vypnutí zabezpečení objektu, odemknutí objektu)
IV.5		Útok formou odepření služby Denial of service (DDoS)	Typ útoku na internetové služby nebo stránky, jehož cílem je cílovou službu znefunkčnit a znepřístupnit ostatním uživatelům (finanční ztráty)
IV.6		Porušení zásad pro kyberbezpečnost ze strany zaměstnanců (uživatele)	Firma se může stát terčem kybernetického útoku
IV.7		Nedořešena otázka kybernetické bezpečnosti na národní úrovni.	Společnosti nejsou dostatečně technologicky ani finančně připraveny bránit se velkým masivním útokům.
V.1	**Technologické předpoklady**	Nedostatečná digitalizace dat a firemních procesů	Může způsobit zdržení implementace chytrých technologií v podniku. Dokumenty a důležitá data nejsou zaznamenána v digitální podobě.
V.2		Nedostupnost vysokorychlostního internetového připojení	Pomalá rychlost procesů, nefunkčnost procesů.

ID	Kategorie	Hrozba	Scénář
VI.1	**Provozní rizika**	Výpadky elektrického proudu	Nefunkčnost systému, omezení služeb, finanční ztráta
VI.2		Výpadky internetového připojení	Nefunkčnost systému, omezení služeb, finanční ztráta
VI.3		Nefunkčnost softwaru	Nefunkčnost systému, omezení služeb, finanční ztráta
VI.4		Nefunkčnost hardwaru	Nefunkčnost systému, omezení služeb, finanční ztráta

Dalším krokem metody RIPRAN je kvantifikace rizik. Výchozí tabulka je rozšířena o pravděpodobnost výskytu scénáře, hodnotu dopadu scénáře na projekt a výslednou hodnotu rizika. Hodnota rizika je vypočtena jako pravděpodobnost scénáře x hodnota dopadu.

Tab. č. 12 Metoda RIPRAN – Hodnocení rizik projektu [26]

Poř. číslo rizika	Hrozba	Scénář	Pravděpodobnost	Dopad na projekt	Hodnota rizika
1.	Výskyt chřipkové epidemie v jarním období březen-duben	Onemocnění skoro 30 % zaměstnanců	50 %	Výpadek pracovní kapacity a zpoždění zakázky o 3 měsíce - penále 600 tis. Kč	300 tis. Kč

Metoda RIPRAN umožňuje číselnou i verbální kvantifikaci. Pro hodnocení rizik byla zvolena verbální kvantifikace stanovena na základě třídy pravděpodobnosti a kategorie dopadu.

Tab. č. 13 Třídy pravděpodobnosti [26]

Pravděpodobnost		
MP (malá)	pod 33 %	0,01 - 0,33
SP (střední)	33–66 %	0,34 – 0,66
VP (vysoká)	nad 66 %	0,67 – 0,99

Tab. č. 14 Kategorie dopadu [autor]

Kategorie dopadu		
MD (malý)	Škoda do 0,5 % z hodnoty projektu	Dopady vyžadují malé zásahy do projektu
SD (střední)	Škoda od 0,5 % do 20 % z hodnoty projektu	Dopady vyžadují mimořádné zásahy do projektu
VD (vysoký)	Škoda nad 20 % z hodnoty projektu	Ohrožení cíle a termínu projektu

Tab. č. 15 Verbální kvantifikace [26]

Verbální kvantifikace			
	MP	SP	VP
MD	MHR	MHR	SHR
SD	MHR	SHR	VHR
VD	SHR	VHR	VHR

Tab. č. 16 Hodnota rizik, reakce na riziko [autor]

Hodnota rizik	Reakce na riziko
VHR (vysoká hodnota rizika)	Vyhnutí se riziku
SHR (střední hodnota rizika)	Tvorba rizikového plánu
MHR (malá hodnota rizika)	Akceptace rizika

V následující tabulce je k jednotlivým hrozbám a scénářům přiřazena pravděpodobnost a dopad. Výsledkem je celková hodnota rizika.

Tab. č. 17 RIPRAN Kvantifikace rizik při implementaci chytrých technologií [autor]

ID	Kategorie	Hrozba	Scénář	P	D	HR	Reakce
I.1	**Lidé I.**	Nedostatek kvalifikovaných pracovníků	Omezena implementace chytrých technologií, omezení chodu firmy, omezení expanze, finanční ztráty	VP	VD	VHR	Vyhnutí se riziku
I.2		Nízká kvalifikace zaměstnanců	Zaměstnanec nemá dostatečnou kvalifikaci pro práci s chytrými technologiemi, dopouští chyb v důsledku nízké kvalifikace a praxe	SP	VD	VHR	Vyhnutí se riziku
I.3		Nízké vzdělání zaměstnanců	Zaměstnanec není schopen naučit se pracovat s novými technologiemi	SP	VD	VHR	Vyhnutí se riziku

ID	Kategorie	Hrozba	Scénář	P	D	HR	Reakce
I.4		Neochota se učit novým postupům	Zaměstnanec používá staré postupy metody, neefektivita	SP	SD	SHR	Tvorba rizikového plánu
I.5		Neochota zaškolování se pro práci s novými technologiemi	Zaměstnanec nemá motivaci a snahu změnit pracovní postupy.	SP	SD	SHR	Tvorba rizikového plánu
II.1	**Vzdělání II.**	Malé povědomí o Průmyslu 4.0 mezi studenty	Pomalý rozvoj vzdělávání zaměřeného na dovednosti potřebné pro práci s chytrými technologiemi	SP	VD	VHR	Vyhnutí se riziku
II.2		Nedostatečné znalosti v IT technologiích	Zaměstnanci nejsou schopni plnit náročnější úkony, ovládají jen běžné uživatelské znalosti	SP	VD	VHR	Vyhnutí se riziku
II.3		Snižující se počet studentů technických a IT oborů	Nedostatek kvalifikovaných zaměstnanců pro potřeby Průmyslu 4.0	VP	VD	VHR	Vyhnutí se riziku
II.4		Systém vzdělávání zaostává za potřebami Průmyslu 4.0	Nedostatek kvalifikovaných zaměstnanců pro potřeby Průmyslu 4.0	VP	VD	VHR	Vyhnutí se riziku

ID	Kategorie	Hrozba	Scénář	P	D	HR	Reakce
II.5		Stávající zaměstnanci zaostávají za potřebami Průmyslu 4.0	Stávající zaměstnanci nejsou kompetentní k daným úkolům. Neabsolvovali potřebná zaškolení a kurzy určené k práci s novými technologiemi.	SP	SD	SHR	Tvorba rizikového plánu
II.6		Malé povědomí o možnostech Průmyslu 4.0 mezi manažery	Nedostatek informací potřebných k zahájení procesu implementace chytrých technologií do podniku	SP	SD	SHR	Tvorba rizikového plánu
III.1	**Náklady III.**	Společnost nedisponuje dostatečnými prostředky do implementace chytrých technologií	Možná ztráta konkurenční výhody	VP	VD	VHR	Vyhnutí se riziku
III.2		Vysoké náklady spojené s nákupem, instalací a správou chytrých technologií	Finančně velmi náročné, zadlužení podniku, obavy spojené s návratností investice	VP	VD	VHR	Vyhnutí se riziku
III.3		Vysoké náklady spojené s digitalizací, pořízením a správou datových úložišť, cloudů a serverů	Finančně velmi náročné, zadlužení podniku, obavy spojené s návratností investice	VP	VD	VHR	Vyhnutí se riziku
III.4		Vysoké náklady spojené se zaškolením zaměstnanců	Časově a finančně nepříznivé pro chod společnosti, zanedbání práce, odkládaní pracovních úkolů, finanční ztráty	SP	SD	SHR	Tvorba rizikového plánu

ID	Kategorie	Hrozba	Scénář	P	D	HR	Reakce
III.5		Prodlení a ztráty omezující běžný chod při implementaci nových technologií do podnikových procesů	Nutnost omezení provozu a prodlení z důvodu implementace nových technologií, finanční ztráta, postihy za nedodržení termínů, ztráta klienta	SP	SD	SHR	Tvorba rizikového plánu
III.6		Nedostatečná představa o ekonomické efektivitě implementace	Neochota vedení podniku investovat do implementace z důvodu nedostatku informací o efektivitě a porovnání u vzorových podniků	VP	SD	VHR	Vyhnutí se riziku
III.7		Vysoké náklady na zajištění kybernetické bezpečnosti	Nutnost zřízení úseku zabývající se kybernetickou bezpečností, náklady na školení zaměstnanců k této problematice	SP	SD	SHR	Tvorba rizikového plánu
IV.1	**Kybernetická bezpečnost IV.**	Společnost je napadena formou Malware	Po napadení malwarem může dojít k vydírání, k těžbě kryptoměn, napadení routerů, napadení bankovnictví (finanční a reputační riziko, narušení soukromí)	SP	VD	VHR	Vyhnutí se Riziku
IV.2		Slabě zabezpečená cloudová úložiště	Velké množství dat produkované podniky může být z cloudu jednoduše ukradeno a zneužito.(důležité firemní data, údaje o klientech)	SP	VD	VHR	Vyhnutí se Riziku
IV.3		Používání jednofaktorových hesel (jednoduchá autentizace)	Zabezpečení jednofaktorovým heslem je lehce zneužitelné (např. krádež zaznamenaného hesla)	VP	VD	VHR	Vyhnutí se riziku

ID	Kategorie	Hrozba	Scénář	P	D	HR	Reakce
IV.4		Nasazení IoT do prostředí s minimálním zabezpečením	Zneužití v podobě získání přístupu do vnitřní sítě podniku za účelem krádeže dat nebo ovládnutí jednotlivých prvků připojených do sítě. Způsobuje ztráta kontroly nad technologiemi, zneužití dat a narušení soukromí (odposlechy, kamerové záznamy, vypnutí zabezpečení objektu, odemknutí objektu)	SP	VD	VHR	Vyhnutí se riziku
IV.5		Útok formou odepření služby Denial of service (DoS)	Útok na internetové služby nebo stránky, jehož cílem je službu znefunkčnit a znepřístupnit ostatním uživatelům (finanční ztráty)	SP	VD	VHR	Vyhnutí se riziku
IV.6		Porušení zásad pro kyberbezpečnost ze strany zaměstnanců (uživatele)	Firma se může snáze stát terčem kybernetického útoku	VP	VD	VHR	Vyhnutí se riziku
IV.7		Nedořešena otázka kybernetické bezpečnosti na národní úrovni.	Společnosti nejsou dostatečně technologicky ani finančně připraveny bránit se velkým masivním útokům.	VP	VD	VHR	Vyhnutí se riziku
V.1	**Technologické předpoklady**	Nedostatečná digitalizace dat a firemních procesů	Může způsobit zdržení implementace chytrých technologií v podniku. Dokumenty a důležitá data nejsou zaznamenána v digitální podobě.	SP	SD	SHR	Tvorba rizikového plánu

ID	Kategorie	Hrozba	Scénář	P	D	HR	Reakce
V.2		Nedostupnost vysokorychlostního internetového připojení	Pomalá rychlost procesů, nefunkčnost procesů.	VP	VD	VHR	Vyhnutí se riziku
VI.1	**Provozní rizika**	Výpadky elektrického proudu	Nefunkčnost systému, omezení služeb, finanční ztráta	SP	VD	VHR	Vyhnutí se riziku
VI.2		Výpadky internetového připojení	Nefunkčnost systému, omezení služeb, finanční ztráta	SP	VD	VHR	Vyhnutí se riziku
VI.3		Nefunkčnost softwaru	Nefunkčnost systému, omezení služeb, finanční ztráta	SP	VD	VHR	Vyhnutí se riziku
VI.4		Nefunkčnost hardwaru	Nefunkčnost systému, omezení služeb, finanční ztráta	SP	VD	VHR	Vyhnutí se riziku

5.2.1 Návrhy opatření k metodě RIPRAN

V poslední fázi metody RIPRAN k danému riziku navrženo vhodné opatření, jehož cílem je snížení pravděpodobnosti výskytu nebo míra dopadu. Dále jsou rizika projektu kvantifikována na základě přihlédnutí k nápravným opatřením a je stanovena nová hodnota rizika.

Tab. č. 18 RIPRAN Návrhy opatření ke snížení rizika [autor]

ID	K.	Hrozba	Scénář	Opatření	P	D	HR
I.1	**Lidé I.**	Nedostatek kvalifikovaných pracovníků	Omezena implementace chytrých technologií, omezení chodu firmy, omezení expanze, finanční ztráty	Spolupráce firmy s vysokými školami technických oborů při hledání potencionálních zaměstnanců, motivační programy pro studenty těchto oborů, benefity pro pracovní pozice tohoto typu	SP	SD	SHR
I.2		Nízká kvalifikace zaměstnanců	Zaměstnanec nemá dostatečnou kvalifikaci pro práci s chytrými technologiemi, dopouští chyb v důsledku nízké kvalifikace a praxe	Personální oddělení musí dbát na výběr vhodného kandidáta a ověření jeho kvalifikace	MP	SD	MHR
I.3		Nízké vzdělání zaměstnanců	Zaměstnanec není schopen naučit se pracovat s novými technologiemi	Tvorba vzdělávacích kurzů pro zaměstnance v oblasti IT a smart technologií	MP	SD	MHR
I.4		Neochota se učit novým postupům	Zaměstnanec používá staré postupy metody, neefektivita	Pravidelné meetingy a konference na téma Průmysl 4.0, kontrola dodržování postupů ze strany nadřízeného	MP	SD	MHR

ID	K.	Hrozba	Scénář	Opatření	P	D	HR
I.5		Neochota zaškolování se pro práci s novými technologiemi	Zaměstnanec nemá motivaci a snahu změnit pracovní postupy.	Kontroly pracovních postupů ze strany nadřízeného, pravidelný reporting, motivační bonusy	SP	MD	MHR
II.1	**Vzdělání II.**	Malé povědomí o Průmyslu 4.0 mezi studenty	Pomalý rozvoj vzdělávání zaměřeného na dovednosti potřebné pro práci s chytrými technologiemi	Rozvoj vědomostí o Průmyslu 4.0 formou přednášek a besed na úrovni základních až vysokých škol, přizpůsobení studijních plánů potřebám Průmyslu 4.0	MP	SD	MHR
II.2		Nedostatečné znalosti v IT technologiích	Zaměstnanci nejsou schopni plnit náročnější úkony, ovládají jen běžné uživatelské znalosti	Změny a přizpůsobení studijních plánů v oblasti výuky IT. Doplňování znalostí formou kurzů a školení.	MP	SD	MHR
II.3		Snižující se počet studentů technických a IT oborů	Nedostatek kvalifikovaných zaměstnanců pro potřeby Průmyslu 4.0	Motivační programy pro studenty těchto oborů, tvorba nových oborů zaměřených pro potřeby Průmyslu 4.0	SP	SD	SHR
II.4		Systém vzdělávání zaostává za potřebami Průmyslu 4.0	Nedostatek kvalifikovaných zaměstnanců pro potřeby Průmyslu 4.0	Přizpůsobení systému vzdělávání pro Průmysl 4.0, tvorba nových studijních plánů, vznik nových studijních oborů	SP	SD	SHR

ID	K.	Hrozba	Scénář	Opatření	P	D	HR
II.5		Stávající zaměstnanci zaostávají za potřebami Průmyslu 4.0	Stávající zaměstnanci nejsou kompetentní k daným úkolům. Neabsolvovali potřebná zaškolení a kurzy určené k práci s novými technologiemi.	Tvorba nových pracovních postupů, školení a kurzů pro zaměstnance.	MP	SD	MHR
II.6		Malé povědomí o možnostech Průmyslu 4.0 mezi manažery	Nedostatek informací potřebných k zahájení procesu implementace chytrých technologií do podniku	Propagace formou konferencí a veletrhů, pravidelné workshopy pořádané iniciativou Firma 4.0, návštěvy vzorových podniků v rámci programu Expedice 4.0	MP	SD	MHR
III.1	**Náklady III.**	Společnost nedisponuje dostatečnými prostředky do implementace chytrých technologií	Možná ztráta konkurenční výhody	Firemní půjčka s nízkým úrokem pro podnikatele, finanční dotace z EU, nový věřitel, průzkum trhu při nákupu nových technologií	MP	SD	MHR
III.2		Vysoké náklady spojené s nákupem, instalací a správou chytrých technologií	Finančně velmi náročné, zadlužení podniku, obavy spojené s návratností investice	Firemní půjčka s nízkým úrokem pro podnikatele, finanční dotace z EU, nový věřitel, průzkum trhu při nákupu nových technologií	MP	SD	MHR
III.3		Vysoké náklady spojené s digitalizací, pořízením a správou datových úložišť, cloudů a serverů	Finančně velmi náročné, zadlužení podniku, obavy spojené s návratností investice	Firemní půjčka s nízkým úrokem pro podnikatele, finanční dotace z EU, nový věřitel, průzkum trhu při nákupu nových technologií	MP	SD	MHR

ID	K.	Hrozba	Scénář	Opatření	P	D	HR
III.4		Vysoké náklady spojené se zaškolením zaměstnanců	Časově a finančně nepříznivé pro chod společnosti, zanedbání práce, odkládaní pracovních úkolů, finanční ztráty	Firemní půjčka s nízkým úrokem pro podnikatele, finanční dotace z EU, nový věřitel, průzkum trhu při nákupu nových technologií	MP	SD	MHR
III.5		Prodlení a ztráty omezující běžný chod při implementaci nových technologií do podnikových procesů	Nutnost omezení provozu a prodlení z důvodu implementace nových technologií, finanční ztráta, postihy za nedodržení termínů, ztráta klienta	Vytvoření časového plánu implementace, pravidelná kontrola plánu (Ganttův diagram)	MP	SD	MHR
III.6		Nedostatečná představa o ekonomické efektivitě implementace	Neochota vedení podniku investovat do implementace z důvodu nedostatku informací o efektivitě a porovnání u vzorových podniků	Zapojení se do iniciativy Firma 4.0, účast na workshopech a expedicích do vzorových firem.	MP	SD	MHR
III.7		Vysoké náklady na zajištění kybernetické bezpečnosti	Nutnost zřízení úseku zabývající se kybernetickou bezpečností, náklady na školení zaměstnanců k této problematice	Firemní půjčka s nízkým úrokem pro podnikatele, finanční dotace z EU, nový věřitel, průzkum trhu při nákupu nových technologií	SP	MD	MHR
IV.1	**Kybernetická bezpečnost IV.**	Společnost je napadena formou Malware	Po napadení malwarem může dojít k vydírání, k těžbě kryptoměn, napadení routerů, napadení bankovnictví (finanční a reputační riziko, narušení soukromí)	Nalezení chyb (děr) v systému, které mohou být využity malwarem a jejich odstranění. Nepřipojovat do firemní sítě neznámá zařízení.	MP	VD	SHR

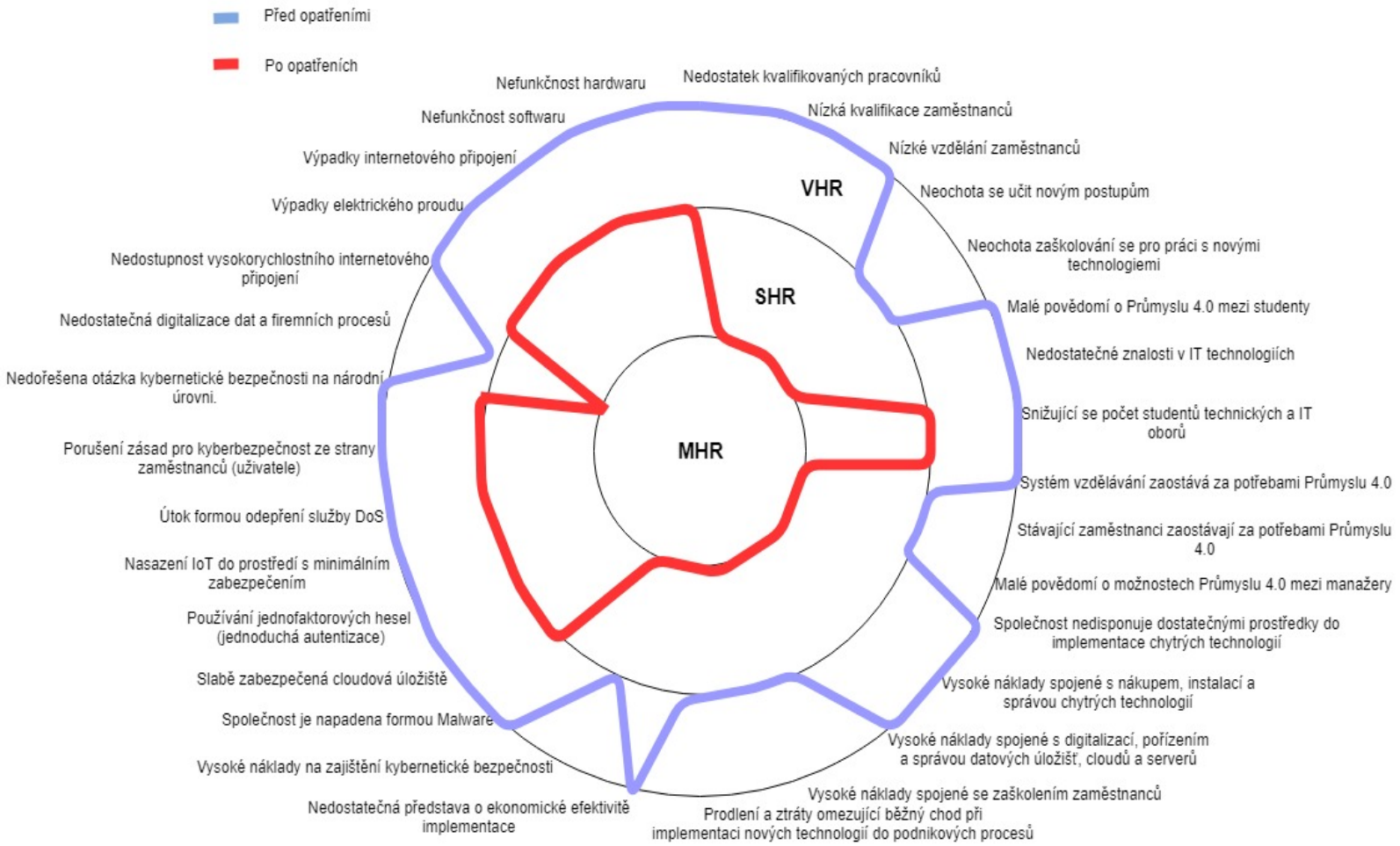
ID	K.	Hrozba	Scénář	Opatření	P	D	HR
IV.2		Slabě zabezpečená cloudová úložiště	Velké množství dat produkované podniky může být z cloudu jednoduše ukradeno a zneužito. (důležitá firemní data, údaje o klientech)	Prověření poskytovatele cloudu (úroveň poskytovaného zabezpečení)	MP	VD	SHR
IV.3		Používání jednofaktorových hesel (jednoduchá autentizace)	Zabezpečení jednofaktorovým heslem je lehce zneužitelné (např. krádež zaznamenaného hesla)	Zavedení dvou a vícefaktorové autentizace.	MP	VD	SHR
IV.4		Nasazení IoT do prostředí s minimálním zabezpečením	Zneužití v podobě získání přístupu do vnitřní sítě podniku za účelem krádeže dat nebo ovládnutí jednotlivých prvků připojených do sítě. Způsobuje ztrátu kontroly nad technologiemi, zneužití dat a narušení soukromí (odposlechy, kamerové záznamy, vypnutí zabezpečení objektu, odemknutí objektu)	Kontrola zabezpečení internetového připojení, routerů a jednotlivých zařízení připojených k podnikové síti. Používání technologií od prověřených výrobců. Školení zaměstnanců v oblasti kybernetické bezpečnosti	MP	VD	SHR

ID	K.	Hrozba	Scénář	Opatření	P	D	HR
IV.5		Útok formou odepření služby Distributed denial of service (DDoS)	Útok na internetové služby nebo stránky, jehož cílem je službu znefunkčnit a znepřístupnit ostatním uživatelům (finanční ztráty)	Řešení zabezpečení formou spolupráce s externími firmami specializujícími se na ochranu proti DDos. Ochrana již na úrovni poskytovatele internetového připojení např. O2 antiDDOS.	MP	VD	SHR
IV.6		Porušení zásad pro kyberbezpečnost ze strany zaměstnanců (uživatele)	Firma se může snáze stát terčem kybernetického útoku	Nepřipojování cizích zařízení do podnikových sítí, nesdělování citlivých údajů, dodržování základních principů pro zabezpečení	MP	VD	SHR
IV.7		Nedořešena otázka kybernetické bezpečnosti na národní úrovni.	Společnosti nejsou dostatečně technologicky ani finančně připraveny bránit se velkým masivním útokům.	Vývoj společné obrany, na kterém se podílí národní kybernetické centrály.	MP	VD	SHR
V.1	**Technologické předpoklady**	Nedostatečná digitalizace dat a firemních procesů	Může způsobit zdržení implementace chytrých technologií v podniku. Dokumenty a důležitá data nejsou zaznamenána v digitální podobě.	Vytvoření časového plánu digitalizace pravidelná kontrola plánu (Ganttův diagram)	MP	MD	MHR

ID	K.	Hrozba	Scénář	Opatření	P	D	HR
V.2		Nedostupnost vysokorychlostního internetového připojení	Pomalá rychlost procesů, nefunkčnost procesů.	Dokončení pokrytí území ČR vysokorychlostním internetem. Průzkum na trhu dodavatelů internetového připojení.	SP	VD	SHR
VI.1	**Provozní rizika**	Výpadky elektrického proudu	Nefunkčnost systému, omezení služeb, finanční ztráta	Koupě záložních energetických zdrojů UPS nebo možnost ovládat zařízení i manuálním způsobem	MP	VD	SHR
VI.2		Výpadky internetového připojení	Nefunkčnost systému, omezení služeb, finanční ztráta	Využití datové sítě různých poskytovatelů (Koupě routeru na sim kartu, koupě USB modemu s datovým připojením)	MP	VD	SHR
VI.3		Nefunkčnost softwaru	Nefunkčnost systému, omezení služeb, finanční ztráta	Pravidelná aktualizace, používání softwaru od prověřených dodavatelů, antivirová ochrana, stahování freeware programů z ověřených distribučních kanálů	MP	VD	SHR
VI.4		Nefunkčnost hardwaru	Nefunkčnost systému, omezení služeb, finanční ztráta	Pravidelná údržba a servisní prohlídky přístrojů a zařízení.	MP	VD	SHR

Pro snadnější přehlednost byl vytvořen následující pavučinový diagram, který vymezuje rozdíl mezi hodnotou jednotlivých rizik před zavedením opatření a po něm. Z grafu je patrné, že po zavedení opatření se vysoká rizika změnila v mírná a původní mírná rizika se stala malými.

5.2.2 Pavučinový diagram k metodě RIPRAN



Obr. č. 10 Pavučinový diagram [autor]

5.3 IMPLEMENTACE SMART TECHNOLOGIÍ DO PROSTŘEDÍ RESTAURACE

Pro implementaci smart technologií bylo zvoleno vybrané restaurační zařízení. Tento typ podnikání je velmi ovlivněn náklady, které vznikají v důsledku běžného provozu a jsou typově shodné s náklady na chod domácností např. náklady na energie. Tyto položky tvoří velkou část nákladů na provoz a je tudíž vhodné se zaměřit na jejich optimalizaci. Z těchto důvodů se vedení podniku rozhodlo pro investici do chytrých technologií, konkrétně pro implementaci prvků smart home. V minulém roce restaurace zaznamenala výrazné zvýšení odběru elektrické energie bez nalezení možných příčin, což také výrazně přispělo k rozhodnutí pro implementaci. Vedení restaurace od konceptu smart home očekává především snížení nákladů na energie, upozornění na vznik nenadálých událostí, ale také usnadnění práce zaměstnancům. Stávající finanční náklady na vytápění objektu činní 115 200 Kč ročně, náklady na elektrickou energie 180 000 Kč ročně. Předpokládaná úspora energií se dle dodavatelů prvků smart home pohybuje až okolo 30 %.

Pro implementaci prvků smart home byly na základě brainstormingu s vedením podniku zvoleny produkty značky Fibaro. Rozhodujícími kritérii pro výběr byly snadná instalace, bez nutnosti zásahů do elektroinstalace a finanční náročnost. Jedná se o bezdrátové řešení domácí automatizace s možností vzdáleného ovládání a sledování stavů. Výhodou tohoto systémů je, že nevyžaduje zásahy do stávající elektroinstalace. Jednotlivé komponenty jsou přenositelné a tak se dají jednoduše použít i v případě stěhování či rekonstrukce. Systém umožňuje ovládat spotřebiče jako topení, světla, ovládání žaluzií, kamerový systém a zajišťuje bezpečnou domácnost pomocí senzorů dveřního kontaktu, senzorů pohybu, světla, kouře či vody. Ovládání jednotlivých zařízení je možné z jednoho místa (počítač, smartphone či tablet), v případě vzdáleného ovládání je potřeba aby byla řídící jednotka (Home Center) připojena k internetu. Systém umožňuje:

- Sledování monitorovaných oblastí v reálném čase i historii
- Automatizaci jednotlivých úkonů (vytvoření scén), které šetří čas i náklady
- Upozornění na závažný problém ihned po jeho zaznamenání
- Vzdálené ovládání
- Monitorování spotřeby energií

Produkty zvoleného systému Fibaro využívají pro vzájemnou bezdrátovou komunikaci protokol Z-Wave, který se používá především pro systémy domácí automatizace a je mezinárodně standardizován. Jedná se o komunikaci od zařízení k zařízení přes síť s využitím rádiových vln, kde je přenášen pouze malý objem dat. Díky komunikaci v tomto pásmu není signál rušen na rozdíl od sítí wifi či Bluetooth. Výhodou komunikace přes systém Z-Wave je jeho mobilita, možnost připojení zařízení od různých výrobců (interoperabilita) a jednoduchost přidání nového modulu do systému. Dosah zařízení

je 100 metrů v otevřeném prostoru a 50 metrů uvnitř budovy. V uzavřeném prostoru musí prvky tvořit síť, tak aby mohly prvky umístěné blíže k řídící jednotce přijímat a vysílat příkazy vzdálenějších prvků do řídící jednotky. To znamená, že dosah Z-Wave sítě roste a rozšiřuje se s počtem Z-Wave zařízení v této síti [27].

5.3.1 Bezpečnost

Z-Wave využívá stejné zabezpečení šifrováním jako internetové bankovnictví. Od roku 2017 byly zavedeny silnější bezpečnostní standardy známé jako Security 2, které poskytují pokročilé zabezpečení pro inteligentní domácí zařízení. Nový typ zabezpečení Z-Wave S2 byl vyvinut ve spolupráci s odborníky na kybernetickou bezpečnost. Cílem je zajistit bezpečnou komunikaci mezi zařízeními a komunikaci mezi zařízeními a cloudem. Největší slabinou v zabezpečení je proces párování zařízení. Nová zařízení s označením S2 využívají fyzické prostředky k dalšímu zajištění před útoky hackerů. Jedná se o samolepky nebo výtisky na samotných zařízeních, která mají jedinečný QR nebo PIN kód, jehož použití je dalším krokem v procesu autentizace a párování. Dle prohlášní Z-Wave Alliance je bezpečnostní standard S2 pro inteligentní domácí zařízení nejvyspělejším zabezpečením na trhu. Z-Wave Aliance také dohlíží na dodržování norem S2 u výrobců zařízení. Ti musí splňovat bezpečnostní opatření, za které jim je udělena pečeť [28].

5.3.2 Finanční náročnost

Pro implementaci do prostředí restaurace byly zvoleny jednotlivé prvky v závislosti na optimalizaci nákladů za energie a předcházení možným škodám. Pro úsporu energie v oblasti vytápění byla zvolena implementace termohlavic na radiátory v celých prostorách restaurace. Ochranou před možným vznikem požáru jsou detektory kouře, které budou instalovány do kuchyně a u baru. Detektory zaplavení budou implementovány do prostor, kde jsou umístěny spotřebiče napojeny na přívod vody (myčky nádobí, ledovač a podobně) to znamená do kuchyně a přípravny. Bezdrátové zásuvky budou kontrolovat, kolik daný spotřebič odebírá elektrické energie ze sítě. Tyto zásuvky budou použity u spotřebičů s vysokým odběrem energie a starších spotřebičů, u kterých se odběry mohou zvyšovat.

Tab. č. 19 Finanční nákladnost implementace prvků smart home do restaurace [autor]

Produkt	Cena za kus	Počet kusů	Cena celkem
Řídící jednotka (FIBARO Home Center Lite)	7 490 Kč	1	7490 Kč
Termostatická hlavice	2 090 Kč	10	20 900 Kč
Detektor kouře	1 690 Kč	2	3 380 Kč
Detektor zaplavení	1 590 Kč	2	3180 Kč
Bezdrátová zásuvka	1 690 Kč	5	8 450 Kč
Náklady celkem			**43 400 Kč**

Náklady na implementaci zařízení do restaurace jsou vyčísleny bez nákladů za práci (instalaci zařízení), ta bude provedena provozním restaurace.

5.4 METODA WHAT-IF

Rizika jsou zpracována pro oblast implementace prvků smart home do prostor restauračního zařízení. Po konzultaci se zástupcem dodavatelské firmy pro smart home řešení byla v rámci brainstormingu za účasti majitele podniku a vedoucího provozu zjištěna rizika a odhadnuty možné následky zapsané do následující tabulky metody What-if.

Tab. č. 20 Výsledky metody What-If pro implementaci prvků smart home [autor]

Co se stane když?	Odhad možných následků	Zdroj rizika	Bezpečnostní opatření
Vypadne elektrický proudu	Nefunkčnost řídící jednotky (Home center) Nefunkčnost vzdáleného ovládání	Externí vlivy	Koupě a instalace záložního energetického zdroje UPS
Vypadne internetové připojení	Nefunkčnost vzdáleného ovládání řídící jednotky (Home center)	Výpadek poskytovatele (porucha síťových prvků poskytovatele nebo externími vlivy)	Záložní internetové připojení přes datovou síť
		Porucha vnitřních síťových prvků (např. routeru)	Restart zařízení, servisní zásah technika, koupě nového zařízení

Co se stane když?	Odhad možných následků	Zdroj rizika	Bezpečnostní opatření
Vybije se energetický zdroj v termohlavici či senzoru	Neodhalení nebezpečné situace. Senzor či termohlavice neodesílá řídící jednotce data potřebná k vyhodnocení situace- neodhalení nebezpečí. Prostory, které daný senzor monitoruje nemohou být ovládány dle předem stanovených scénářů.	Vybité baterie	Vizuální kontrola
Nefunguje bezdrátový modul termohlavice či senzoru	Neodhalení nebezpečné situace. Senzor či termohlavice neodesílá řídící jednotce data potřebná k vyhodnocení situace- neodhalení nebezpečí. Prostory, které daný senzor monitoruje nemohou být ovládány dle předem stanovených scénářů.	Výrobní vada/ vnější poškození	Vizuální kontrola poškození. Kontrola připojení v řídící jednotce. Servisní zásah nebo výměna
Nefunguje řídící jednotka	Nevyhodnocení získaných dat. Nefunkčnost celého systému	Výrobní vada/ vnější poškození	Vizuální kontrola poškození. Kontrola připojení v aplikaci. Servisní zásah nebo výměna.
Senzory nebudou přijímat a vysílat zadané příkazy	Nevyhodnocení získaných dat. Nefunkčnost systému v oblasti monitorované danými senzory	Špatné rozmístění senzorů, velká vzdálenost mezi senzory	Správné umístění senzorů, dle příručky. Kontrola konektivity.
Chyby v procesu párování zařízení	Využití vzniklých chyb v systému hackerem. Ovládnutí systému	Špatné spárování zařízení	Kontrola správného spárování. Využití prvků ochrany S2- využití QR nebo PIN kódu jako další krok v procesu autentizace a párování

Co se stane když?	Odhad možných následků	Zdroj rizika	Bezpečnostní opatření
Napadení cloudového úložiště poskytovatele	Krádež dat	Špatné zabezpečení cloudu poskytovatelem	Průzkum úrovně zabezpečení u zvoleného poskytovatele cloudu
Napadení řídící jednotky zvenčí (přes internet)	Ovládnutí systému	Nedostatečné zabezpečení internetového připojení uživatelem	Kontrola zabezpečení internetového připojení, routerů a jednotlivých zařízení připojených k podnikové síti.

Na základě výsledků metody What-if byly identifikovány možné situace a jejich důsledky. Tyto poznatky jsou dále využity a kvantifikovány v metodě FMEA.

5.5 ANALÝZA RIZIK METODOU FMEA

Metoda FMEA je využita k posouzení rizik spojených s implementací prvků smart home do prostor restauračního zařízení. Zvolená metoda identifikuje možné poruchy při procesu a jejich důsledky. Následně jsou navržena vhodná opatření ke snížení míry rizika.

Pro hodnocení rizik prostřednictvím modelu FMEA bude využito koeficientů pravděpodobnosti výskytu rizika P, následků dopadu N a možnosti odhalení O. Na základě stanovení těchto koeficientů se vypočítá prioritní rizikové číslo PRČ. Toto číslo se vypočítá součinem daných koeficientů. K hodnocení jednotlivých rizik bude přistoupeno pomocí slovního vyjádření, ke kterému je přiřazena odpovídající číselná hodnota. Výsledkem je stanovení závažnosti konkrétních rizik.

Na základě brainstormingu s vedoucími pracovníky a technikem byla vytvořena stupnice pro nežádoucí a nepřijatelná rizika s hodnotou PČR <50–125>. Vyhodnocená rizika s PČR spadající do tohoto rozmezí budou dále opatřena vhodným návrhem na snížení míry rizika.

Tab. č. 21 Klasifikační stupnice pro hodnocení rizik [autor]

Číselné hodnocení	**P**	**N**	**O**
1	Velmi málo pravděpodobná	Zanedbatelná	Velmi vysoká
2	Málo pravděpodobná	Nízká	Vysoká
3	Pravděpodobná	Střední	Střední
4	Velmi pravděpodobná	Vysoká	Nízká
5	Vysoce pravděpodobná	Velmi vysoká	Zanedbatelná

Tab. č. 22 FMEA Vyhodnocení rizik implementace prvků smart home [autor]

Prvek, funkce	Možná vada	Možné následky vady	Význam **N**	Možné příčiny	Výskyt **P**	Stávající opatření pro prevenci a odhalování	Odhalitelnost **O**	**Rizikové číslo**
Technologická	Výpadek elektrického proudu	Nefunkčnost řídící jednotky (Home center) Nefunkčnost vzdáleného ovládání.	5	Externí vlivy	4	X	4	80
	Výpadek internetového připojení	Nefunkčnost vzdáleného ovládání řídící jednotky (Home center)	5	Výpadek poskytovatele (porucha síťových prvků poskytovatele nebo externími vlivy)	3	X	4	60
			5	Porucha vnitřních síťových prvků (např. routeru)	3	X	3	45

Prvek, funkce	Možná vada	Možné následky vady	Význam **N**	Možné příčiny	Výskyt **P**	Stávající opatření pro prevenci a odhalování	Odhalitelnost **O**	**Rizikové číslo**
	Vybití energetického zdroje v termohlavici či senzoru	Neodhalení nebezpečné situace. Senzor či termohlavice neodesílá řídící jednotce data potřebná k vyhodnocení situace- neodhalení nebezpečí. Prostory, které daný senzor monitoruje nemohou být ovládány dle předem stanovených scénářů.	5	Vybité baterie	2	X	2	20
	Nefunkční bezdrátový modul termohlavice či senzoru	Neodhalení nebezpečné situace. Senzor či termohlavice neodesílá řídící jednotce data potřebná k vyhodnocení situace – neodhalení nebezpečí. Prostory, které daný senzor monitoruje nemohou být ovládány dle předem stanovených scénářů.	5	Výrobní vada/ vnější poškození	2	X	3	30
	Nefunkční řídící jednotka	Nevyhodnocení získaných dat. Nefunkčnost celého systému	5	Výrobní vada/ vnější poškození	3	X	2	30
	Senzory nebudou přijímat a vysílat zadané příkazy	Nevyhodnocení získaných dat. Nefunkčnost systému v oblasti monitorované danými senzory	5	Špatné rozmístění senzorů, velká vzdálenost mezi senzory	2	X	2	20

Prvek, funkce	Možná vada	Možné následky vady	Význam **N**	Možné příčiny	Výskyt **P**	Stávající opatření pro prevenci a odhalování	Odhalitelnost **O**	**Rizikové číslo**
Kybernetická bezpečnost	Chyby v procesu párování zařízení	Využití vzniklých chyb v systému hackerem. Ovládnutí systému	5	Špatné spárování zařízení	3	X	3	45
	Napadení cloudového úložiště poskytovatele	Krádež dat	5	Špatné zabezpečení cloudu poskytovatelem	2	X	4	40
	Napadení řídící jednotky zvenčí (přes internet)	Ovládnutí systému	5	Nedostatečné zabezpečení internetového připojení uživatelem	3	X	3	45

5.5.1 Návrhy opatření

Jako nejvýznamnější byla identifikována rizika spojená s výpadky elektrického proudu a výpadky připojení k internetové síti. V případě výpadku elektrické energie nebude řídící jednotka (Home center) v provozu a nebude tak schopna vyhodnocovat a zpracovávat data. Nefunkční bude v tomto případě i vzdálené ovládání. Jako vhodné opatření byla navržena koupě a instalace záložních energetických zdrojů , které by po dobu několika hodin napájela zařízení potřebná k fungování prvků smart home. V navrhovaném konceptu prvků smart home v restauraci je na napájení z elektrické sítě závislá pouze řídící jednotka. Ostatní prvky jako jsou senzory, termohlavice a ostatní používají jako zdroj baterie. Pro zachování funkce vzdáleného ovládání je důležité mít energetický zdroj také pro internetový přijímač a router. Návrhem pro zajištění chodu konceptu smart home v případě výpadku elektřiny je tedy koupě záložního energetického zdroje pro internetový přijímač, router a řídící jednotku (Home center).

Konektivita mezi jednotlivými zařízeními smart home je v restauraci řešena formou protokolu Z-Wave a není tudíž ovlivněna výpadkem internetového připojení. V souvislosti s výpadkem elektrické energie je ovlivněna pouze možnost vzdáleného ovládání těchto zařízení. Opatřením pro toto riziko je využití datového připojení ve formě koupě přenosného USB modemu, který se následně zapojí do routeru nebo koupě routeru s možností vložení SIM karty s daty.

Tab. č. 23 Ekonomické zhodnocení opatření [autor]

Výpadek elektrického proudu	Záložní zdroj pro internetový přijímač (anténu)	1100 Kč
	Záložní zdroj pro router umístěný v restauraci	1100 Kč
	Záložní zdroj pro řídící jednotku systému (Home center)	1100 Kč
Výpadek internetového připojení	Koupě routeru na sim kartu	2200 Kč
	Koupě USB modemu s datovým připojením (zapojení do routeru)	1150 Kč 300 Kč /měsíc
Celkem (bez nákladů na datové připojení)		**6650 Kč**

5.5.2 Vyhodnocení rizik po zavedení opatření

V následující tabulce jsou navržena opatření ke snížení míry rizika. Na základě těchto doporučení je vypočítána nová hodnota PRČ, která udává pravděpodobnou míru rizika po zavedení opatření.

Tab. č. 24 FMEA Vyhodnocení rizik po zavedení opatření [autor]

Prvek, funkce	Možná vada	Možné následky vady	**Původní RČ**	Doporučená opatření	Termín realizace / odpovědnost	Význam (N)	Výskyt (P)	Odhalitelnost (O)	**RČ po opatřeních**
Technologická	Výpadek elektrického proudu	Nefunkčnost řídící jednotky (Home center) Nefunkčnost vzdáleného ovládání	80	Koupě a instalace záložního energetického zdroje UPS	Před implementací /provozní	3	4	4	48
	Výpadek internetového připojení	Nefunkčnost vzdáleného ovládání řídící jednotky (Home center)	60	Záložní internetové připojení přes datovou síť	Před implementací / provozní	2	3	4	24
			45	Restart zařízení, servisní zásah technika, koupě nového zařízení	Při nefunkčnosti /provozní, technik	3	3	3	18

Prvek, funkce	Možná vada	Možné následky vady	**Původní RČ**	Doporučená opatření	Termín realizace / odpovědnost	Význam (N)	Výskyt (P)	Odhalitelnost (O)	**RČ po opatřeních**
	Vybití energetického zdroje v termohlavici či senzoru	Neodhalení nebezpečné situace. Senzor či termohlavice neodesílá řídící jednotce data potřebná k vyhodnocení situace- neodhalení nebezpečí. Prostory, které daný senzor monitoruje nemohou být ovládány dle předem stanovených scénářů.	20	Vizuální kontrola	V průběhu fungování/ 1x měsíčně/ provozní	5	1	1	5
	Nefunkční bezdrátový modul termohlavice či senzoru	Neodhalení nebezpečné situace. Senzor či termohlavice neodesílá řídící jednotce data potřebná k vyhodnocení situace- neodhalení nebezpečí. Prostory, které daný senzor monitoruje nemohou být ovládány dle předem stanovených scénářů.	30	Vizuální kontrola poškození. Kontrola připojení v řídící jednotce. Servisní zásah nebo výměna	Provozní /v případě nefunkčnosti Technik/v případě nefunkčnosti	5	2	1	10
	Nefunkční řídící jednotka	Nevyhodnocení získaných dat. Nefunkčnost celého systému	30	Vizuální kontrola poškození. Kontrola připojení v aplikaci. Servisní zásah nebo výměna.	Provozní /v případě nefunkčnosti Technik/v případě nefunkčnosti	5	3	1	15

Prvek, funkce	Možná vada	Možné následky vady	**Původní RČ**	Doporučená opatření	Termín realizace / odpovědnost	Význam (N)	Výskyt (P)	Odhalitelnost (O)	**RČ po opatřeních**
	Senzory nebudou přijímat a vysílat zadané příkazy	Nevyhodnocení získaných dat. Nefunkčnost systému v oblasti monitorované danými senzory	20	Správné umístění senzorů, dle příručky. Kontrola konektivity.	Během implementace /provozní	5	2	1	10
Kybernetická bezpečnost	Chyby v procesu párování zařízení	Využití vzniklých chyb v systému hackerem. Ovládnutí systému	45	Kontrola správného spárování. Využití prvků ochrany S2 - využití QR nebo PIN kódu jako další krok v procesu autentizace a párování	Před implementací/ provozní	5	2	2	20
	Napadení cloudového úložiště poskytovatele	Krádež dat	40	Průzkum úrovně zabezpečení u zvoleného poskytovatele cloudu	Před implementací /provozní	5	2	3	30
	Napadení řídící jednotky zvenčí (přes internet)	Ovládnutí systému	45	Kontrola zabezpečení internetového připojení, routerů a jednotlivých zařízení připojených k podnikové síti.	Před implementací /provozní	5	2	3	30

5.6 ZHODNOCENÍ EFEKTIVITY IMPLEMENTACE PRVKŮ SMART HOME

Pro zhodnocení efektivity implementace prvků smart home do restaurace byly zvoleny jednotlivé varianty roční úspory nákladů na energie. Optimistická varianta předpokládá ušetření nákladů ve výši až 30 %, jak deklarují dodavatelé smart home prvků. Střední varianta počítá s úsporou 20 % a pesimistická varianta počítá s ušetřením pouhých 10 % nákladů. V následující tabulce jsou porovnány jednotlivé scénáře úspory nákladů s náklady na implementaci technologií. Pokud bychom počítali s pesimistickou variantou, budou náklady na implementaci vyrovnány úsporou energie za 20 měsíců. Z hlediska efektivity v podobě ušetření nákladů za energie je implementace smart technologií do modelové restaurace vhodnou volbou.

Tab. č. 25 Zhodnocení efektivity implementace smart technologií do restaurace

Náklady na vytápění a elektřinu / ročně	295 200 Kč
Předpokládaná úspora dle poskytovatelů	až 30 %
Optimistická varianta (až 30 %)	**88 560 Kč**
Střední varianta (20 %)	**59 040 Kč**
Pesimistická varianta (10 %)	**29 520 Kč**
Náklady na implementaci prvků smart home do restaurace	43 400 Kč
Náklady na opatření ke snížení míry rizika	6 650 Kč
Náklady na implementaci celkem	**50 050 Kč**

6 ANALÝZA VÝSLEDKŮ ŘEŠENÍ

Z důvodu velkého přesahu Průmyslu 4.0 do ekonomické a sociální roviny byla zhodnocena rizika nástupu Průmyslu 4.0 i v národním měřítku. Pomocí metody SWOT byly identifikovány silné stránky, slabé stránky, příležitosti a hrozby pro implementaci Průmyslu 4.0 do prostředí České republiky. Na základě posouzení důležitosti jednotlivých faktorů souvisejících s nástupem Průmyslu 4.0 byl nejvýraznější vztah vytvořen mezi silnými stránkami a příležitostmi. Na základě těchto zjištění by měla být zvolena růstově orientovaná strategie Max-Max (SO). Při implementaci Průmyslu 4.0 by se tedy mělo zaměřit na maximalizaci příležitostí (získání konkurenční výhody na trhu, zájem nových investorů, vznik nových pracovních pozic, podílení se na tvorbě nových technologických řešení) a silných stránek (vysoce průmyslově vyspělá země, nízká míra nezaměstnanosti a zvyšující se náklady na zaměstnance, vysoká úroveň vzdělání na vysokých školách technického charakteru, zájem státu podporovat inovace a investovat do výzkumu).

Pomocí metody RIPRAN byla identifikována a ohodnocena rizika, která mohou nastat ve spojitosti s implementaci chytrých technologií do podniků nevýrobního charakteru. Identifikace rizik byla provedena v následujících oblastech: pracovní síla, vzdělání, náklady, kybernetická bezpečnost, technologické předpoklady a provozní rizika. Identifikováno bylo celkem 31 rizik v daných oblastech, která byla následně ohodnocena pomocí verbální kvantifikace na základě třídy pravděpodobnosti a kategorie dopadu. Byly vyhodnoceny následující rizika s vysokou hodnotou rizika (VHR): nedostatek kvalifikovaných pracovníků, nízká kvalifikace zaměstnanců, nízké vzdělání zaměstnanců, malé povědomí o Průmyslu 4.0 mezi studenty, nedostatečné znalosti v oblasti IT technologií, snižující se počet studentů technických a IT oborů, systém vzdělávání zaostává za potřebami Průmyslu 4.0, společnosti nedisponují dostatečnými prostředky pro implementaci chytrých technologií, vysoké náklady na nákup instalaci a správu chytrých technologií, vysoké náklady spojené s digitalizací a správou datových úložišť, nedostatečná představa o ekonomické efektivitě implementace, ohrožení formou kybernetických útoků: formou malware, cloudová úložiště, odepření služby DDoS, jednofaktorová hesla, IoT ve slabě zabezpečeném prostředí, porušování zásad pro kyberbezpečnost ze strany zaměstnanců, nedostupnost vysokorychlostního připojení, výpadky elektrického proudu, výpadky internetového připojení, nefunkčnost hardwaru a softwaru. Ke každému riziku bylo navrženo vhodné opatření ke snížení míry rizika. Výsledkem je snížení hodnoty rizik z (VHR) vysoké hodnoty rizika na střední hodnotu rizika (SHR), a původní střední hodnota rizika se stala malou (MHR).

Pro identifikaci rizik a návrh vhodných opatření v konkrétní firmě byla využita metoda What-If. Rizika byla identifikována konkrétně pro implementaci prvků smart home do restauračního zařízení na základě brainstormingu za účasti majitele a vedoucího provozu po konzultaci s pracovníkem dodavatelské firmy. Metodou What- If bylo položeno celkem 9 otázek „Co se stane když?“ a nalezeno

9 možných scénářů a jejich důsledků. Nalezenými vadami jsou: výpadek elektrického proudu, výpadek internetového připojení, vybití energetického zdroje v termohlavici či senzoru, nefungující bezdrátový modul termohlavice či senzoru, nefungující řídící jednotka, senzory nepřijímají a nevysílají zadané příkazy, chyby v procesu párování zařízení, napadení cloudového úložiště poskytovatele a napadení řídící jednotky. K nalezeným vadám jsou sepsány možné příčiny a důsledky a navrženo vhodné bezpečnostní opatření.

Metoda FMEA navazuje na výsledky metody What-If, kdy byly identifikovány možné poruchy při procesu implementace a jejich důsledky. Rizika byla následně ohodnocena pomocí koeficientů pravděpodobnosti výskytu rizika P, následků dopadu N a možnosti odhalení O. Na základě stanovení těchto koeficientů bylo vypočteno prioritní rizikové číslo a určena závažnost jednotlivých rizik. Následně byla u všech rizik navržena vhodná opatření ke snížení míry rizika. Nežádoucí a nepřijatelná rizika spadající do rozmezí s hodnotou PČR <50–125> byla dále opatřena vhodným detailnějším návrhem na snížení míry rizika. Konkrétně se jedná o rizika vznikající na základě výpadku elektrického proudu a výpadku internetového připojení. Ty mají vliv na celkové fungování systému a jeho vzdálené ovládání. Na základě bezpečnostních opatření u všech rizik byla stanovena nová hodnota prioritního rizikového čísla. Hodnota rizikového čísla u nežádoucích a nepřijatelných rizik se snížila a byla tak zařazena do kategorie přijatelná nebo mírná rizika.

Dále byla posouzena finanční náročnost samotné implementace společně s náklady na opatření ke snížení míry rizika. Pro posouzení byla použita data o nákladech za energie ve sledovaném podniku a vypočítána úspora za energie po implementaci v optimistické, střední a pesimistické variantě, dle předpokladu dodavatele. Z uvedených výsledků vyplývá, že investice nutné k implementaci zařízení smart home budou v případě pesimistické varianty navráceny v podobě snížení nákladů za energie do 20 měsíců. Z výše uvedeného tak vyplývá, že pokud se bude podnik řídit doporučeními a dodržovat navržená opatření ke snížení míry rizika při implementaci chytrých technologií ve všech specifikovaných oblastech, včetně návrhů pro oblast kybernetické bezpečnosti u nevýrobních podniků, bude implementace těchto technologií pro podniky představovat nesporný přínos.

7 ZÁVĚR

Tato diplomová práce se zabývala tématem implementace Průmyslu 4.0 a s ním spojených smart technologií do podniků nevýrobního charakteru s cílem zhodnotit rizika související s implementací těchto technologií a navrhnout vhodná opatření pro snížení míry rizika.

Cílem práce bylo zhodnocení současného stavu při implementaci Průmyslu 4.0 a „smart" technologií do podnikových procesů. Na základě získaných informací o této problematice byla provedena identifikace, analýza a vyhodnocení rizik, které jsou spojeny s implementací těchto technologií do firemního prostředí. Konktrétně byla zhodnocena bezpečnost, efektivita a finanční náročnost implementace. Na základě zjištěných výsledků byla navržena opatření ke snížení míry rizika a stanovena preventivní opatření. Výstupem práce je návrh na ošetření rizik.

Cíle práce byly splněny pomocí vybraných metod pro analýzu rizik. Konkrétně byla posouzena implementace Průmyslu 4.0 do prostředí České republiky a analyzována rizika spojená s implementací chytrých technologií do podniků nevýrobního charakteru metodou RIPRAN. Výsledkem jsou vhodná opatření snižující míru těchto rizik. Na závěr byla metodou FMEA provedena analýza rizik pro konkrétní podnik implementující prvky smart home. Pro nežádoucí nebo nepřijatelná rizika byla navržena konkrétní opatření snižující míru jejich závažnosti. Byla zhodnocena efektivita, bezpečnost a finanční náročnost implementace.

Pro zajištění konkurenceschopnosti podniků a jejich udržitelnost na trhu je pro implementaci Průmyslu 4.0 nezbytná podpora státu ve spolupráci s podniky. Pokud se podniky na implementaci chytrých technologií řádně připraví, budou se řídit doporučeními a dodržovat navržená opatření ke snížení míry rizika, bude implementace těchto technologií představovat nesporný přínos.

SEZNAM POUŽITÝCH ZDROJŮ

[1] *Industrie 4.0. The evolution*. In: https://medium.com [online]. 2019 [cit. 2019-03-10]. Dostupné z: https://medium.com/@jaydev_21091/industry-4-0-the-evolution-350996e50048

[2] MAŘÍK, Vladimír. *Průmysl 4.0: výzva pro Českou republiku*. Praha: Management Press, 2016, 262 stran. ISBN 978-80-7261-440-0.

[3] *Hospodářské noviny*. In: https://byznys.ihned.cz/ [online]. 2018 [cit. 2018-02-11]. Dostupné z: https://byznys.ihned.cz/c1-64009970-prumyslova-revoluce-4-0-za-10-let-se-tovarny-budou-ridit-samy-a-produktivita-vzroste-o-tretinu

[4] *European Commission, Digitising European Industry-catalogue of initiatives*. In: https://ec.europa.eu [online], 2019 [cit. 2019-04-19]. Dostupné z: https://ec.europa.eu/futurium/en/content/digitising-european-industry-catalogue-initiatives

[5] *Ministerstvo financí, Makroekonomická predikce leden 2019*. In: www.mfcr.cz [online]. 2019 [cit. 2019-04-23]. Dostupné z: https://www.mfcr.cz/cs/verejny-sektor/makroekonomika/makroekonomicka-predikce/2019/makroekonomicka-predikce-leden-2019-34169

[6] *Český statistický úřad, mzdy a náklady práce*. In: www.czso.cz [online]. 2019 [cit. 2019-04-23]. Dostupné z: https://www.czso.cz/csu/czso/prace_a_mzdy_prace

[7] *Kurzycz, Průměrná mzda v ČR*. In: www.kurzy.cz [online]. 2019 [cit. 2019-04-23]. Dostupné z: https://www.kurzy.cz/makroekonomika/mzdy/

[8] *The World Bank Group, Employment in industry*. In: https://data.worldbank.org [online]. 2019 [cit. 2019-04-24]. Dostupné z: https://data.worldbank.org/indicator/SL.IND.EMPL.ZS

[9] *Úřad vlády České republiky, OSTEU, Dopady digitalizace na trh práce v ČR a EU*. In: www.vlada.cz [online], 2019 [cit. 2019-04-20]. Dostupné z: https://www.vlada.cz/assets/evropske-zalezitosti/analyzy-EU/Dopady-digitalizace-na-trh-prace-CR-a-EU.pdf

[10] INICIATIVA PRŮMYSL 4.0. MPO [online]. 08.06.2016 [cit. 2019-03-15]. Dostupné z: https://www.mpo.cz/assets/dokumenty/53723/64358/658713/priloha001.pdf

[11] *Úřad vlády České republiky, Akční plán pro společnost 4.0*. In: www.databaze-strategie.cz [online], 2019 [cit. 2019-04-22]. Dostupné z: https://www.databaze-strategie.cz/cz/urad-vlady/strategie/akcni-plan-pro-spolecnost-4-0-2017

[12] *Firma 4.0*. In: www.firma40.cz [online], 2019 [cit. 2019-05-07]. Dostupné z: https://www.firma40.cz/workshopy

[13] *CZ BIM Stavebnictví 4.0 aneb na cestě za digitalizací stavebnictví*. In: http://www.konstrukce.cz [online], 2019 [cit. 2018-03-23]. Dostupné z: http://www.konstrukce.cz/clanek/cz-bim-stavebnictvi-4-0-aneb-na-ceste-za-digitalizaci-stavebnictvi/

[14] *Future of the Sharing Economy in Europe 2016*. In: www.pwc.co.uk [online]. 2018 [cit. 2018-02-10]. Dostupné z: https://www.pwc.co.uk/issues/megatrends/collisions/sharingeconomy/future-of-the-sharing-economy-in-europe-2016.html

[15] VERMESAN, O., FRIESS, P. *Internet of Thing - From Research and Innovation to Market Deployment*. Denmark: River Publishers Aalborg, 2014. ISBN 978-87-93102-94-1

[16] *IoT portál, Co je Iot*. In: www.iot-portal.cz [online], 2019 [cit. 2019-04-10]. Dostupné z: https://www.iot-portal.cz/co-je-iot/

[17] *Internet of things*. In: https://justcreative.com [online], 2019 [cit. 2019-04-12]. Dostupné z: https://justcreative.com/2018/11/19/internet-of-things-explained/

[18] *JIC magazin, Smart city/Home/Office*. In: www.jic.cz [online], 2019 [cit. 2018-04-05]. Dostupné z: https://www.jic.cz/magazin/smart-cityhomeoffice-chytre-technologie-se-objevuji-vsude-lide-je-muzou-najit-treba-i-v/

[19] *Iot online store, The Internet of Things*. In: www.iotonlinestore.com [online], 2019 [cit. 2019-04-02]. Dostupné z: http://www.iotonlinestore.com/

[20] MIKETA, Kamil. *Smart revoluce*. Praha: Mladá fronta, 2017,216 s. ISBN: 978-80-204-4611-4

[21] BLAŽKOVÁ, M. *Marketingové řízení a plánování pro malé a střední firmy*. 1. vyd. Praha : Grada, 2007. 278 s. ISBN 978-80-247-1535-3.

[22] FOTR, J., VACÍK, E., SOUČEK, I. ŠPAČEK, M., HÁJEK, S. *Tvorba strategie a strategické plánování: teorie a praxe. 1. vyd.* Praha: Grada, 2012, 381 s. ISBN 978-80-247-3985

[23] Management Mania, RIPRAN. In: managementmania.com [online], 2019 [cit. 2019-05-02]. Dostupné z: https://managementmania.com/cs/ripran-risk-project-analysis

[24] TICHÝ, Milík. *Ovládání rizika: analýza a management*. V Praze: C.H. Beck, 2006. Beckova edice ekonomie. ISBN 80-7179-415-5.

[25] SEDLÁČKOVÁ, H., BUCHTA, K. *Strategická analýza*. 2. přeprac. a rozš. vyd. Praha: C. H. Beck, 2006. 216 s. ISBN: 80-7179-367-1.

[26] DOLEŽAL, J., MÁCHAL, P., LACKO, B. a kolektiv. *Projektový management podle IPMA*. Praha: Grada, 2009. 507 s. ISBN 978-80-247-2848-3.

[27] *Fibaro*. In: www.mojefibaro.cz [online]. 2019 [cit. 2019-05-10]. Dostupné z: https://www.mojefibaro.cz/system/

[28] *Build your smart home, The security of Z-Wave*. In: https://buildyoursmarthome.co [online]. 2019 [cit. 2019-05-10]. Dostupné z: https://buildyoursmarthome.co/home-automation/protocols/security-of-z-wave-protocol/

SEZNAM TABULEK

SEZNAM OBRÁZKŮ

SEZNAM ZKRATEK

IoT.....Internet of Things

DDos.....Distributed denial of service

SMLC.....Smart Manufacturing Leadership Coalition

ČSÚ.....Český statistický úřad

MF.....Ministerstvo financí

OECD.....Organisation for Economic Co-operation and Development

MPO.....Ministerstvo průmyslu a obchodu

P2P.....Peer-to-peer

PČR.....Prioritní rizikové číslo

P.....Pravděpodobnost

N.....Následky dopadu

O.....Odhalení

D.....Dopad

UPS.....Uninterruptible Power Supply/Source

HR.....Hodnota rizika