

**VYSOKÁ ŠKOLA EKONOMIE A MANAGEMENTU**

Nárožní 2600/9a, 158 00 Praha 5

# **DIPLOMOVÁ PRÁCE**



# VYSOKÁ ŠKOLA EKONOMIE A MANAGEMENTU

Nárožní 2600/9a, 158 00 Praha 5

## NÁZEV DIPLOMOVÉ PRÁCE/TITLE OF THESIS

Identifikování rizik a zpracování krizových scénářů a plánů v podniku/Identifying risks and designing crisis scenarios and plans in the company

## TERMÍN UKONČENÍ STUDIA A OBHAJOBA (MĚSÍC/ROK)

10/2023

## JMÉNO A PŘÍJMENÍ STUDENTA / STUDIJNÍ SKUPINA

Daniela Mertlová/ KEMMA05

## JMÉNO VEDOUCÍHO DIPLOMOVÉ PRÁCE

Doc. Ing. Roman Zuzák, Ph.D.

## PROHLÁŠENÍ STUDENTA

Odevzdáním této práce prohlašuji, že jsem zadanou diplomovou práci na uvedené téma vypracovala samostatně a že jsem ke zpracování této diplomové práce použila pouze literární prameny v práci uvedené.

Jsem si vědoma skutečnosti, že tato práce bude v souladu s § 47b zák. o vysokých školách zveřejněna, a souhlasím s tím, aby k takovému zveřejnění bez ohledu na výsledek obhajoby práce došlo.

Prohlašuji, že informace, které jsem v práci užila, pocházejí z legálních zdrojů, tj. že zejména nejde o předmět státního, služebního či obchodního tajemství či o jiné důvěrné informace, k jejichž použití v práci, popř., k jejichž následné publikaci v souvislosti s předpokládanou veřejnou prezentací práce, nemám potřebné oprávnění.

Datum a místo: Datum a místo: 4. 4. 2023, Lety u Dobřichovic.

## PODĚKOVÁNÍ

Ráda bych tímto poděkovala vedoucímu diplomové práce za metodické vedení a odborné konzultace, které mi poskytl při zpracování mé diplomové práce a mé rodině za podporu.



# VYSOKÁ ŠKOLA EKONOMIE A MANAGEMENTU

Národní 2600/9a, 158 00 Praha 5

## SOUHRN

### 1. Cíl práce:

Hlavním cílem diplomové práce je identifikování kritických rizik ve vybrané společnosti a posouzení jejího stavu připravenosti na tato rizika. K dosažení hlavního cíle je nutné splnit dílčí cíle:

1. Shromáždění teoretických poznatků v oblasti řízení rizik a krizového řízení, díky čemuž vznikne základ pro další analýzu.
2. Správná volba vlastního výzkumu a efektivní využití primárních zdrojů pro získání potřebných dat.
3. Tvorba krizových scénářů a plánů na základě nejkritičtějších rizik.
4. Analýza výsledků výzkumu, na jejíž základě budou formulována doporučení.

### 2. Výzkumné metody:

Práce byla vytvořena na základě analýzy sekundárních zdrojů v teoretické části a primárních zdrojů v praktické části. Další data byla získána pomocí polostrukturovaných rozhovorů a brainstormingu s manažery zkoumané organizace. V rámci polostrukturovaných rozhovorů byly identifikovány příležitosti a hrozby. Výstupy z tohoto výzkumu byly dále analyzovány a komparovány pomocí STEP analýzy. Takto identifikovaná rizika byla dále hodnocena a kategorizována. Pro tento účel byla zvolena metoda matice rizik. Pro hodnocení rizik byla zvolena metoda brainstormingu s manažery banky, konkrétně s ředitelem řízení rizik, vedoucím operačních rizik a vedoucím tržních rizik. Pomocí What-if analýzy byly představeny potenciální scénáře, které by mohly nastat v případě výskytu těchto rizik.

### 3. Výsledky výzkumu/práce:

Na základě výzkumu byly identifikovány příležitosti a hrozby. V rámci výzkumu bylo zaměřeno na sociální, ekonomické a technicko-technologické faktory. Z výzkumu vyplynulo, že nejkritičtější rizika se týkají kybernetických incidentů, snížení solvence kvůli ekonomické nestabilitě, ztráty tržního podílu kvůli konkurenci a finanční ztrátě kvůli ekonomické nejistotě. Pro nejkritičtější rizika byla vypracována konkrétní opatření, jejichž cílem bylo snížit pravděpodobnost jejich výskytu či jejich dopad. Na závěr byly pro tyto scénáře vypracovány krizové plány, což je krok vedoucí k zajištění, že organizace má připraveny strategie a postupy pro řešení potenciálních krizových situací.

### 4. Závěry a doporučení:

Příprava scénářů vyžaduje pečlivé prozkoumání, schválení managementem před vlastní realizací. Scénáře musí reflektovat skutečné hrozby a rizika. Je zapotřebí jak teoretické (table-top cvičení), tak praktické (simulace krizových situací). Je nutná analýza po testu (hodnocení efektivnosti, reakční doby, kvality reakce), revize postupů a aktualizace a připravenost. V rámci zhodnocení stavu připravenosti lze vyhodnotit kladné stránky, tedy banka má komplexní plán kontinuity podnikání, probíhá pravidelná aktualizace plánů obnovy po havárii (DRP), investice do školení a simulací, funguje kooperace mezi odděleními. Jako prostor ke zlepšení je doporučováno detailněji vypracovat krizové scénáře a plány, zejména pro kybernetickou bezpečnost a pravidelně je testovat.

## KLÍČOVÁ SLOVA

Řízení rizik, krizový management, analýza rizik, krizový plán, krizový scénář

# VYSOKÁ ŠKOLA EKONOMIE A MANAGEMENTU

Nárožní 2600/9a, 158 00 Praha 5

## SUMMARY

### 1. Main objective:

The main objective of this thesis is to identify critical risks in the chosen organization and to assess its state of readiness towards these risks. To achieve the main objective, it is necessary to meet the subsequent goals:

1. Gathering theoretical knowledge in the area of risk management and crisis management, which will form the fundament for further analysis.
2. The right selection of research and effective use of primary sources to obtain the necessary data.
3. Creating crisis scenarios and plans based on the most critical risks.
4. Analysis of the research results, based upon which recommendations will be formulated.

### 2. Research methods:

The thesis was written based on the analysis of secondary sources in the theoretical part and primary sources in the practical part. Additional data was gathered through semi-structured interviews and brainstorming with managers of the analysed organisation. The outputs from this research were further analysed and compared by applying STEP analysis. The risks thus identified were further assessed and categorized. The risk matrix method was chosen for this purpose. For the risk assessment, the brainstorming method was chosen with the bank's managers, namely the Director of Risk Management, the Head of Operational Risk and the Head of Market Risk. Potential scenarios that could occur if these risks were to occur were presented using what-if analysis.

### 3. Result of research:

The research identified opportunities and threats. The research focused on social, economic and technical and technological factors. The research found that the most critical risks relate to cyber incidents, reduced solvency due to economic instability, loss of market share due to competition and financial loss due to economic uncertainty. Specific measures were developed for the most critical risks to reduce their likelihood or impact. Finally, crisis plans were developed for these scenarios as a step towards ensuring that the organisation has strategies and procedures in place to deal with potential crisis situations.

### 4. Conclusions and recommendation:

Preparation of scenarios requires careful review, management approval prior to actual implementation. Scenarios must reflect the actual threats and risks. Both theoretical (table-top exercises) and practical (crisis simulations) are necessary. Post-test analysis (evaluation of effectiveness, response time, quality of response), revision of procedures and updating and preparedness is required. As part of the evaluation of the level of readiness, the positive aspects can be assessed, i.e. the bank has a comprehensive business continuity plan, regular updates of disaster recovery plans (DRPs) are in place, investments in training and simulations, and cross departmental cooperation is in place. It is recommended that crisis scenarios and plans, especially for cyber security, should be developed in more detail and tested regularly as room for improvement.

## KEYWORDS

Risk management, crisis management, risk analysis, crisis plan, crisis scenario

## JEL CLASSIFICATION

G32 Financial Risk and Risk Management  
H12 Crisis Management  
D81 Criteria for Decision-Making under Risk and Uncertainty

**Vysoká škola ekonomie a managementu**  
**Nárožní 2600/9a, 158 00 Praha 5**

## ZADÁNÍ DIPLOMOVÉ PRÁCE

Jméno a příjmení:	Bc. Daniela Mertlová
Studijní program:	Ekonomika a management (Ing.)
Studijní skupina:	KEMMA05
Název DP:	Identifikování rizik a zpracování krizových scénářů a plánů v podniku
Zásady pro vypracování (stručná osnova práce):	<ol style="list-style-type: none"><li>1. Úvod</li><li>2. Teoreticko-metodologická část<ol style="list-style-type: none"><li>2.1. Řízení rizik</li><li>2.2. Krizové řízení</li><li>2.3. Krizové scénáře a plány</li><li>2.4. Metodika práce</li></ol></li><li>3. Praktická část<ol style="list-style-type: none"><li>3.1. Představení společnosti</li><li>3.2. Identifikování a rozbor rizik společnosti</li><li>3.3. Identifikování krizových scénářů a plánů</li><li>3.4. Doporučení</li></ol></li><li>4. Závěr</li></ol>
Seznam literatury: (alespoň 4 zdroje)	<ul style="list-style-type: none"><li>• MYŠKOVÁ, R. <i>Analytické přístupy pro podporu řízení podniku</i>. Brno: Akademické nakladatelství CERM, 2022. ISBN 978-80-7623-093-4.</li><li>• ROBERTSON, J. <i>Executing crisis: a C-suite crisis leadership survival guide</i>. Brookfield: Rothstein Publishing, 2020. ISBN 978-1-944480-64-6.</li><li>• RUBENS, D. <i>Strategic Risk and Crisis Management: A Handbook for Modelling and Managing Complex Risks</i>. London: Kogan Page, 2023. ISBN 978-1398609754.</li><li>• SHAYB, H. A. <i>Enterprise Crisis Management</i>. Independently Published. Israel: Independently Published, 2021. ISBN 978-9655998139.</li><li>• THANI, F. B. H. A., OBEIDAT, A. M. The Impact of Strategic Leadership on Crisis Management, <i>International Journal of Asian Social Science</i>, 2020, vol. 10, no. 6, pp. 307–326.</li></ul>
Harmonogram:	<ul style="list-style-type: none"><li>• Zpracování cílů a metodiky do 30. 04. 2023</li><li>• Zpracování teoretické části do 30. 06. 2023</li><li>• Zpracování výsledků do 31. 07. 2023</li><li>• Finální verze do 31. 08. 2023</li></ul>
Vedoucí práce:	doc. Ing. Roman Zuzák, Ph.D.

V Praze dne 20. 02. 2023

prof. Ing. Milan Žák, CSc.  
rektor

**Prof. Ing.  
Milan  
Žák CSc.**

Digitálně podepsal Prof. Ing. Milan Žák CSc.  
DN: cn=Prof. Ing. Milan Žák CSc., c=CZ, o=Vysoká škola ekonomie a managementu, a.s., givenName=Milan, sn=Žák, serialNumber=ICA-10393535  
Datum: 2023.02.20 12:00:56 +01'00'

# Obsah

1	Úvod .....	1
2	Teoreticko-metodologická část práce .....	3
2.1	Řízení rizik .....	3
2.1.1	Definice řízení rizik .....	3
2.1.2	Základní pojmy .....	4
2.1.3	Enterprise Risk Management .....	5
2.1.4	Business Continuity Management .....	6
2.1.5	Proces řízení rizik .....	7
2.2	Krizové řízení .....	14
2.2.1	Definice krize a její typy .....	14
2.2.2	Fáze krizového řízení .....	16
2.2.3	Strategie v oblasti krizového řízení .....	18
2.2.4	Krizová komunikace .....	19
2.2.5	Role centrální banky v krizovém řízení .....	19
2.3	Krizové scénáře a plány .....	20
2.3.1	Definice a význam krizových scénářů a plánů .....	20
2.3.2	Tvorba krizových scénářů .....	21
2.3.3	Plánování a struktura krizových plánů .....	21
2.4	Metodika práce .....	23
3	Praktická část .....	26
3.1	Představení společnosti .....	26
3.1.1	Současný stav .....	27
3.1.2	Rizika a řízení rizik a organizační struktura .....	27
3.2	Identifikování a rozbor rizik společnosti .....	29
3.2.1	Analýza rizik .....	47
3.2.2	What-if analýza .....	52
3.3	Identifikování krizových scénářů a plánů .....	53
3.3.1	Tvorba krizových scénářů .....	53
3.3.2	Krizový scénář č. 1 Nedostupnost – ztráta systému .....	54
3.3.3	Krizový scénář č. 2 Ztráta dat v interním systému banky .....	55
3.3.4	Krizový scénář č. 3 Únik citlivých informací o zákaznících .....	57
3.4	Doporučení .....	58
3.5	Zhodnocení stavu připravenosti .....	59
4	Závěr .....	60

Literatura .....	61
Přílohy .....	I

## Seznam zkratk

BCM – Business Continuity Management  
COSO – Standard pro nastavení systému vnitřního řízení a kontrol  
ČNB – Česká národní banka  
ERM – Integrované řízení podnikových rizik  
EU – Evropská unie  
ETOP – Profil environmentálních hrozeb a příležitostí  
FAÚ – Finanční analytický úřad  
FMEA – Analýza možného výskytu vlivu vad  
FTA – Analýza stromu poruch  
HDP – Hrubý domácí produkt  
HICP – Harmonizovaný index spotřebitelských cen  
IRM – Integrované řízení rizik  
ISO – Mezinárodní organizace pro standardizaci  
IZS – Integrovaný záchranný systém  
MAP – Monitoruj/Analyzuj/Predikuj  
MFČR – Ministerstvo financí České republiky  
MVČR – Ministerstvo vnitra České republiky  
NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost  
PRIBOR – Stanovení pražské mezibankovní nabídky úrokových sazeb  
RPN – Rizikový index  
WFA – What-if analýza

## Seznam tabulek

Tabulka 1 Hodnocení vlivu inflace metodou STEP, ETOP a MAP .....	11
Tabulka 2 Matice rizik .....	11
Tabulka 3 Krizový audit .....	16
Tabulka 4 Počet cizinců v ČR – předběžné čtvrtletní údaje 2020–2023.....	34
Tabulka 5 Klasifikační stupnice .....	50
Tabulka 6 Stupnice pro hodnocení rizik.....	50

## Seznam obrázků

Obrázek 1 Proces řízení rizik .....	7
Obrázek 2 Monitoring rizik .....	13
Obrázek 3 Systém firemního krizového plánování .....	23
Obrázek 4 Organizační struktura „Banky X“ .....	28

## Seznam grafů

Graf 1 Přírůstky/úbytky obyvatel ČR, 2001–2020.....	31
Graf 2 Zahraníční stěhování, 2001–2020 .....	33
Graf 3 Vývoj HDP v letech 2012–2022 v ČR.....	37
Graf 4 Vývoj HDP na 1 obyvatele v letech 2012–2022 v ČR .....	38
Graf 5 Míra inflace v ČR v letech 2012–2022 .....	39
Graf 6 Výpočty a predikce MF ČR .....	40
Graf 7 Prognóza úrokové sazby .....	41
Graf 8 Klientské úrokové sazby .....	42

# 1 Úvod

V dnešní dynamickém a neustále se proměňujícím podnikatelském prostředí je řízení rizik a rizikového řízení významnější než kdy dříve. Globalizace, technologické pokroky, politické změny, ekonomická nestabilita, válka, geopolitické napětí, pandemie, klimatické změny či dokonce přírodní katastrofy – to vše jsou aspekty, které připravují organizacím nové a neznámé výzvy. Ty musí čelit různým druhům rizik, které mohou zapříčinit krizové situace, a tak negativně ovlivnit jejich činnost, reputaci, či dokonce samotnou existenci. V této turbulentní době je jednou z klíčových schopností organizací schopnost se v těchto rizicích orientovat, identifikovat a řídit, aby zabránily situacím, kdy se rizika mohou stát nekontrolovatelnými, či dokonce destruktivními.

Neřízená rizika mohou vést ke ztrátám na trhu, k finančním obtížím, narušení provozu, újmě na pověsti, nebo dokonce ohrožit bezpečnost zaměstnanců a zákazníků. Proto je nezbytné, aby organizace měly strukturovaný a systematický přístup k řízení rizik a připravenosti na krizové situace. Zvýšená složitost a nejistota podnikatelského prostředí vyžaduje, aby organizace proaktivně identifikovaly a hodnotily rizika na všech úrovních a v různých oblastech své činnosti. Nejde jen o fyzická rizika, jako jsou přírodní katastrofy nebo technologické havárie, ale také o rizika spojená s finančními, právními, etickými, reputačními a dalšími oblastmi. Identifikace rizik je prvním krokem k prevenci a minimalizaci negativních dopadů, zároveň pak umožňuje organizacím připravit se na krizové situace.

Podle Ozaka (2016, str. 30) je budoucnost krizového managementu výrazně ovlivněna novými technologiemi a sociálními médii. Rychlé šíření informací a schopnost oslovit široké publikum v reálném čase změnily způsob, jakým jsou krize identifikovány, řízeny a komunikovány. Využití umělé inteligence a strojového učení může zlepšit posouzení rizik a reakci na krizi. Virtuální a rozšířená realita poskytují možnosti simulace a testování plánů reakce na krizi. Sociální média jsou důležitým kanálem komunikace se zúčastněnými stranami a veřejností během krizových situací. Organizace musí být schopny přizpůsobit své strategie a využívat nové technologie, aby efektivně reagovaly na měnící se potřeby v oblasti krizového managementu.

Hlavním cílem diplomové práce je identifikování kritických rizik ve vybrané společnosti a posouzení jejího stavu připravenosti na tato rizika. Jednou z klíčových oblastí, kterými se tato diplomová práce zabývá, je potřeba identifikovat a vyhodnotit specifická rizika, kterým vybraná organizace čelí. Každá organizace je jedinečná a může čelit odlišným výzvám v závislosti na svém odvětví, velikosti, geografické lokalitě a dalších vnitřních či vnějších faktorech. Tato práce se zaměří na konkrétní organizaci, aby byly pochopeny její specifické potřeby a předpoklady pro úspěšné řízení rizik a krizové řízení.

Práce bude zahrnovat literární rešerše primárních a sekundárních zdrojů, polostrukturované rozhovory s odborníky, brainstorming, nástroje pro identifikaci a analýzu rizik a tvorbu krizových scénářů a plánů. Struktura práce je navržena tak, aby poskytla logický a souvislý pohled na problematiku řízení rizik a krizového řízení. Po úvodní kapitole následuje teoreticko-metodologická část, kde budou vymezeny klíčové pojmy v oblasti řízení rizik a krizového řízení. Budou zkoumány různé přístupy k řízení rizik, proces identifikace rizik a jejich řízení. Dále budou zkoumány fáze krizového řízení, strategie a krizová komunikace.

V analytické části bude provedena důkladná analýza vybrané organizace. Následovat bude analýza makroprostředí pomocí metodiky STEP a identifikace rizik. Rovněž bude provedena analýza a hodnocení rizik a zpracování konkrétních krizových scénářů a plánů, které mohou sloužit jako modelový příklad pro reálnou situaci.



Závěrečná doporučení práce shrnou získané poznatky a budou prezentována doporučení pro vybranou organizaci z hlediska identifikace rizik a zpracování krizových scénářů a plánů.

## 2 Teoreticko-metodologická část práce

V této části diplomové práce bude vymezena základní terminologie, která se týká problematiky řízení rizik a krizového řízení. V rámci řízení rizik budou podrobněji zkoumány principy a postupy řízení rizik v podnikovém prostředí. Blíže bude rozebrána identifikace, analýza a hodnocení rizik. V rámci krizového řízení budou rozebrány principy a procesy krizového řízení v organizaci. Podrobněji bude popsána příprava na krizové situace, řízení během krize a obnově po krizi. Budou prezentovány osvědčené postupy a strategie v oblasti krizového řízení. V oblasti krizových scénářů a plánů bude podrobněji vysvětleno vytváření krizových scénářů a plánů. Budou diskutovány metody identifikace a rozboru potenciálních krizových situací, jejich připravenost a návrh plánů pro řešení těchto situací. V metodologické části bude popsána metodika použitá při výzkumu a aplikace rizikového a krizového řízení v praktické části diplomové práce. Budou diskutovány postupy pro sběr dat, rozbor a vyhodnocení výsledků.

### 2.1 Řízení rizik

Dle Fotra et al. (2020, str. 283) je řízení rizik v současnosti důležitou problematikou, která se týká teorie i praxe myšlení a rozhodování vedoucích pracovníků v organizaci. Autoři dále uvádí, že pomocí metod řízení rizik se identifikují a ovlivňují klíčové faktory pro přežití a konkurenceschopnost organizace v současném turbulentním podnikatelském prostředí. Balog a Iakovets (2020, str. 74) definují řízení rizik jako složitý a komplexní proces, který probíhá ve více stupních na různých hierarchických úrovních činností organizace. Autoři dále dodávají, že jednotlivé fáze a aktivity v tomto procesu jsou uspořádány tak, aby zajistily kvalitní řízení rizik a že přesné pořadí fází může být flexibilní, klade však důraz na identifikaci specifických aktivit a popis postupu.

Risk management neboli řízení rizik, je velmi komplexní disciplína. Řízení rizik může být aplikováno napříč různými odvětvími. Smith a M. Merrit (2020, str. 5), uvádí, že řízení rizik je činnost, která spočívá v aktivním identifikování a řízení nežádoucích výsledků v organizaci. Dodávají, že současně je třeba maximalizovat příležitosti spojené s těmito riziky. Tyto aktivity jsou spojeny s plánováním, které má za účel minimalizovat pravděpodobnost a celkové dopady neúspěchu. Mazareanu (2020, str. 7) např. pohlíží na řízení rizik z pohledu IT, pro které je řízení rizik důležitou součástí integrovaného řízení, které má za cíl poskytnout nástroje potřebné pro analýzu a implementaci řešení, která snižují negativní dopady poškození bezpečnosti informací.

#### 2.1.1 Definice řízení rizik

Dle Markse (2020, str. 9) existuje mnoho definic týkajících se rizika a řízení rizik. Obecně lze však říct, že se zaměřují na zvládnutí a zmírňování potenciálních škod a selhání. Autor dále pokračuje ve výčtu definic řízení rizik, např. „*řízení rizik je celkový proces identifikace rizik, hodnocení rizik, rozhodování, ošetření rizik a jejich kontroly*“. Z jeho pohledu je řízení rizik nedílnou součástí vedení organizace k úspěchu. Vilášek a Antušák (2016, str. 22) definují řízení rizik jako „*specifickou aktivitu, jejímž cílem je minimalizovat společenské ztráty plynoucí z existující nebo potenciální (latentní) hrozby*“. Vochozka a Váchal (2013, str. 533) dodávají, že organizace může být ohrožena také v důsledku změn, které se dějí v makroekonomickém prostředí (kromě již výše zmíněných politicko-právních a ekonomických faktorů se může jednat o faktory sociální či technicko-technologické).

Lima, Crema a Verbano (2018, str. 3) tvrdí, že vzhledem k nepředvídatelnosti podnikání způsobené externími vlivy, jako jsou politické či ekonomické problémy, přírodní vlivy a technologický pokrok, je řízení rizik jedním z hlavních přístupů, které firmám umožňuje zajistit přežití a překonat nejistoty, aby dosáhly svých cílů. Antušák (2013, str. 70) definuje řízení rizik jako „*systematickou aplikaci cíleně plánovaných aktivit, procedur a praktik zaměřených na identifikaci a analýzu hrozeb, hodnocení a kvantifikaci rizik, rozhodování o způsobu řízení rizik, monitorování a vnitřní a vnější reporting o firemních rizicích*“.

Copello (2019, str. 17) dále konstatuje, že hlavním cílem řízení rizik je ochrana a tvorba hodnot. To přináší zlepšení výkonu organizace, podporuje inovace a pomáhá dosáhnout stanovených cílů. V posledních letech se stále zvětšuje zájem o řízení rizik a roste potřeba pro silný rámec na identifikaci, hodnocení a řízení rizik.

### **2.1.2 Základní pojmy**

Bašta et al. (2019, str. 71) upozorňují na fakt, že analýza rizik je velmi komplexní a náročný proces, který vyžaduje znalosti o aktivech, potenciálních hrozbách a také praxi v této oblasti. Na základě správně provedené analýzy rizik lze stanovit opatření, která minimalizují nebo úplně odstraňují identifikovaná rizika. Proto níže budou vysvětleny základní pojmy, které se oblasti řízení rizik týkají, tedy aktivum, nejistota, hrozba, riziko. Tyto termíny budou dále používány jak v teoretické, tak v praktické části.

#### **Aktivum**

Dle Smejkal a Reise (2013, str. 97) označují aktivum jak vše, co má pro daný subjekt hodnotu. Aktiva se mohou členit na hmotná (nemovitosti, cenné papíry atd. či nehmotná (informace, pověst firmy, kvalita personálu atd). Autoři dále specifikují, že podstatnou pro aktiva je „*hodnota aktiva, která je založena na objektivním vyjádření obecně vnímané ceny nebo na subjektivním ocenění důležitosti (kritičnosti pro daný subjekt, popřípadě kombinaci obou přístupů*“ . Bašta et al. (2019, str. 72) dodává, že aktiva se mohou dělit na podpůrná a primární, kdy podpůrným aktivem může být např. technické aktivum, zaměstnanci a dodavatelé a primárním je např. informace či služba.

#### **Nejistota**

Balog a Iakovets (2020, str. 14) se zamýšlí nad samotným konceptem rizika a nejistoty, dle nich se jedná o úzce propojené pojmy. V odborné literatuře se dokonce může jednat o synonyma a tyto pojmy mohou být často zaměňovány. Autoři dále uvádí, že nejistota souvisí s nedostatečným množstvím informací nebo s nejasností ohledně výsledků dané aktivity. Kromě toho, nejasnost může zahrnovat neschopnost pojmout všechny informace pro plné a přesné zhodnocení ekonomického procesu. Akinfenwa (2023, str. 10) souhlasí a dodává, že nejistota lze rozdělit na dva hlavní typy: aleatorní a epistemická. Aleatorní nejistota představuje přirozenou proměnlivost událostí, např. nepředvídatelnost přírodních katastrof nebo výkyvů na trhu. Epistemická nejistota se vztahuje k nejistotě ohledně znalostí systému nebo události (např. omezené údaje nebo nedostatečné pochopení procesu).

#### **Hrozba**

Smejkal a Rais (2013, str. 97) definují hrozbu jako „*sílu, událost, aktivitu nebo osobu, která má nežádoucí vliv na aktiva nebo může způsobit škodu, respektive poškodit organizaci jako celek*“ . Dále autoři člení hrozby dle přírodního (např. přírodní katastrofa) či lidského charakteru (požár, krádež zařízení atd). a doplňují, že mohou být náhodné či úmyslné, vnější či vnitřní. Dle definice MVČR (2023) je hrozba jev, který může potenciálně ohrozit hodnoty a zájmy chráněné

státem a míra této hrozby je určena rozsahem možných škod a časovou pravděpodobností jejího nastoupení.

## Riziko

Copello (2019, str. 13) specifikuje samotné riziko jako jakoukoliv událost, která by mohla organizaci bránit v dosažení jejich strategických, provozních, finančních cílů, popřípadě cílů v oblasti dodržování předpisů. Dle autorů Smithe a M. Merrita (2020, str. 5) riziko představuje možnost, že nežádoucí výsledek nebo absence žádoucího výsledku může narušit chod organizace. Oba výše zmínění autoři definují riziko spíše jako negativní jev. Řízení rizik se může také pojit s pozitivním přínosem, jak zmiňuje Paula (2023, str. 11). S tím souhlasí také Smejkal a Rais (2013, str. 93), kteří přidávají, že je třeba hodnotit riziko také z pozitivní strany. Pomocí správných rozhodnutí v procesu řízení rizik může organizace aplikací vhodných opatření např. navýšit zisk či být úspěšnější.

### 2.1.3 Enterprise Risk Management

Zhu, Li a Mishra (2023, str. 1) poukazují na to, že v literatuře se můžou vyskytnout různé přístupy k řízení rizik, jeden z nich je např. Enterprise Risk Management (ERM, integrované řízení podnikových rizik). Autoři konstatují, že pro efektivní řízení rizik je zapotřebí neustálé sladění mezi podnikem a oddělením řízení rizik, čehož lze dosáhnout začleněním ERM do rozhodovacích procesů podniků. Výše uvedení autoři dále dodávají, že společnosti v současné době využívají různé rámce ERM. Běžné rámce pro řízení rizik jsou např. Mezinárodní organizace pro standardizaci (International Organization for Standardisation – ISO) či COSO (Comittee of Sponsoring Organizations of the Treadway Commission – Standard pro nastavení systému vnitřního řízení a kontroly). Např. norma ČSN ISO 31000 (2018) poskytuje obecné principy a pokyny pro řízení rizik na jakékoliv úrovni organizace. Alexander (2018, str. 130) vnímá ERM také jako nástroj ke zvážení dopadu makroekonomických vlivů na celý podnik, například změn úrokových sazeb, cen komodit a míry inflace na podnik a dodává, že cílem řízení podnikových rizik je minimalizovat neočekávané odchylky ve výkonnosti a maximalizovat vnitřní hodnotu firmy. Vávrová (2014, str. 81) dodává, že ERM „*přístupuje k systému risk managementu v podobě strukturovaného přístupu spojující strategii, procesy, lidi, technologie a znalosti*“.

Fraser, Quail a Simkins (2021, str. 5) hovoří o benefitech, které pro organizace plynou z implementace ERM. Může to být zajištění, že obchodní cíle jsou jasně definovány. Může dojít ke snížení nákladů na kapitál či být dosaženo zlepšení úvěrového ratingu. Implementace ERM také předchází překvapením a nepředvídatelným událostem. Autoři dále dodávají, že implementace dále pomáhá zajistit, že zdroje jsou přiděleny do nejdůležitějších oblastí rizik. Yun (2023, str. 1–2) doplňuje, že ERM pomáhá organizacím překonávat úskalí tradičního „silového“ přístupu řízení podnikových rizik, kde často dochází k situaci, kde každé riziko je řízeno izolovaně. Autor dále dodává, že ERM zahrnuje širší kategorie rizik, jako je strategické riziko, riziko ztráty dobré pověsti, riziko nedodržování předpisů či operační riziko. S narůstající různorodostí rizik ve firemním portfoliu se společnosti mohou zaměřit na efektivnější řízení těchto různých rizik.

Smejkal a Rais (2013, str. 152) souhlasí s názorem Yuna (2023, str. 1–2), že ERM na rozdíl od tradičního vnímání definice rizika považován za nový směr manažerského rozhodování, který se stává nedílnou součástí strategie organizace. Zároveň ale autoři podotýkají, že pro organizace může být svazující vyrovnávat se s regulátory a plnění norem v určitých odvětvích. Ibnalkadi a Ibnalkadi (2021, str. 20–21) také hovoří o tom, že ERM představuje nový pohled na řízení rizik. Souhlasí s Yunem (2023, str. 1–2), že mnoho organizací stále

přístupuje k riziku z oddělených perspektiv. Autoři dále dodávají, že v rámci ERM by všechny oblasti rizika fungovaly jako součást integrovaného celopodnikového systému. Zaměstnanci napříč organizací by také měly být motivováni, aby riziko vnímali jako nedílnou a kontinuální součást svých pracovních pozic. Dle autorů by měl rámec pro řízení rizik vypadat následovně:

1. Vymezení celkové firemní filozofie a cílů.
2. Rozpoznání ohrožení nebo vystavení rizikům.
3. Měření vystavení rizikům.
4. Vymezení směrnic a postupů řízení rizik.
5. Identifikace strategií pro řízení rizik.
6. Provedení strategií.
7. Monitorování vystavení rizikům a zajištění opatření.
8. Hodnocení a měření výkonnosti.

Gartner (2023) dodává, že oproti tradičnímu přístupu k řízení rizik, které je zpravidla v organizaci možné realizovat i bez specializovaných softwarových nástrojů, je pro zavedení a provoz ERM nutné implementovat softwarový nástroj zaměřený na centralizovanou správu identifikovaných podnikových rizik. Tento typ softwarových nástrojů spadá do kategorie Integrated Risk Management (IRM) a jedná se o kombinaci technologií, procesů a dat, které slouží k naplnění cíle umožnit zjednodušení, automatizaci a integraci strategického, provozního a IT řízení rizik v rámci organizace.

#### **2.1.4 Business Continuity Management**

Další významný podnikový rámec zaměřený na odolnost organizace je Business Continuity Management (BCM). Calder (2021, str. 7) uvádí, že řízení kontinuity podnikání, což zahrnuje plánování, ochranu a zajištění obnovy po nepředvídatelných událostech, je nyní důležitější než kdykoliv dříve. V důsledku toho se stále více organizací obrací k normě ISO 22301, což je mezinárodní standard, který stanovuje požadavky na systém kontinuity podnikání (BCMS), aby zajistily svou budoucnost. Smejkal a Rais (2013, str. 441) definují BCM jako „*program řízení kontinuity činností organizace definuje strategický a provozní rámec k aktivnímu zvyšování odolnosti organizace proti narušení, přerušení výroby a/nebo ztrátě služeb*“. Alexander (2018, str. 10) dodává, že BCM je řídicí proces, který identifikuje rizika, hrozby a zranitelnosti, které by mohly ovlivnit nepřetržité fungování organizace. Souhlasí s Calderem (2021, str. 7), že tento proces zahrnuje plánování a doplňuje, že dále zahrnuje také vytváření strategií kontinuity či údržbu systému kontinuity podnikání (BCMS).

Geary (2022, str. 77) pohlíží na změnu trendu BCM v návaznosti na události v posledních letech, kdy se BCM zaměřuje na provozní odolnost. Důvodem je několik faktorů; pandemie covid-19 ukázala, že existují nové úrovně přerušení kontinuity podnikání, které lze obtížně předvídat a řídit. Kromě toho, nástup cloud computingu způsobil, že některé prvky tradičního BCM (záloha systému, zálohovací centra, alternativní kancelářské prostory) mohou být méně relevantní než dříve. Wong (2019, str. 1) souhlasí s Geary (2022, str. 77) a dodává, že obor se v současnosti nachází ve stavu změny, kdy se stále více manažerů snaží překračovat hranice při implementaci BCM na korporátní úrovni. Je však nezbytné, aby dokázali dosáhnout měřitelných a přínosných výsledků v oblasti BCM, které skutečně ovlivní schopnosti poskytovaných služeb a podnikání. Autor dále uvádí, že BCM je jedním z mnoha klíčových faktorů úspěchu, které lze sledovat a které mohou pro firmu představovat zdroj konkurenční výhody. Na rozdíl od jiných faktorů, jako jsou výnosy, produktivita, doba životního cyklu a kvalita produktu či služby se při obhajování BCM mohou manažeři setkat s podobnými scénáři, například že implementace BCM přináší pomalé a postupné výsledky, které se mohou projevit až po delší době. V dnešním proměnlivém podnikatelském prostředí, kde se vedení

často zaměřuje na krátkodobé výsledky a očekávají se rychlé zisky pro akcionáře, musí obhajoba BCM čelit odporu ze strany vedoucích manažerů.

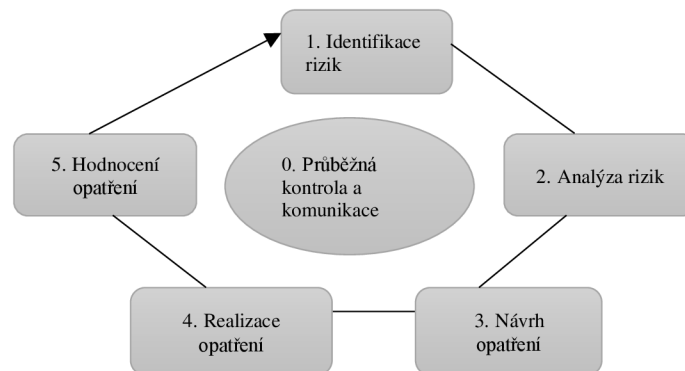
### 2.1.5 Proces řízení rizik

Organizace, které se zabývají řízením podnikových rizik, implementují soubor procesů, které mají být dodržovány jednotlivými funkčními oblastmi v rámci organizace, tvrdí Alexander (2018, str. 133). Akinfenwa (2023, str. 4) rozděluje řízení rizik do čtyř klíčových činností, a to následovně:

- identifikace rizik (vztahující se k možným rizikům),
- analýza (posouzení) rizik (určení pravděpodobnosti a důsledků výskytu identifikovaných rizik),
- ošetření rizik (jak snížit výskyt nebo důsledky přijatelných rizik, jak snížit dopady nepřijatelných rizik a zvolit na ně správné reakce),
- monitorování rizik.

Dle normy ISO 31000 (2018, str. 9) by proces řízení rizik měl být zcela začleněn do všech aspektů řízení a rozhodovacích procesů organizace, a to na všech úrovních – od strategické až po provozní a projektovou. Proces by měl být přizpůsoben potřebám a kontextu každé organizace, a to s ohledem na proměnlivou povahu lidského chování a kultury. Ačkoli je proces řízení rizik často prezentován jako postupný, ve skutečnosti je iterativní. Oškrdal a Doucek (2014, str. 195) jednotlivé aktivity dělí do šesti činností, a sice identifikace rizik, kvalitativní riziková analýza, kvantitativní analýza rizik, návrh opatření, realizace opatření, hodnocení opatření a průběžná kontrola a komunikace. Následující obrázek popisuje tento základní proces.

Obrázek 1 Proces řízení rizik



Zdroj: Oškrdal a Doucek (2014, str. 196)

Procesu řízení rizik se také věnují ve své knize Fotr et al. (2020, str. 283), kteří narozdíl od Akinfenwy (2023, str. 4) vnímají jako počáteční fázi vymezení kontextu řízení rizika a jeho cílů. Z jejich hlediska je tato fáze důležitá, jelikož vyjadřuje jak vnitřní, tak vnější prostředí a určení cílů v souvislosti se strategickými cíli organizace. Lima, Crema a Verbano (2018, str. 3) souhlasí s Fotrem et al. (2020, str. 283), že důležitá je předběžná či počáteční fáze, kde jsou nejprve definovány cíle procesu řízení rizik v souladu se strategickými cíli společnosti a následně jsou specifikovány zdroje a samotný proces potřebný k aplikaci řízení rizik. Jednotlivé fáze se také shodují s Akinfenwou (2023, str. 4).

## Identifikace rizik

Podle Paula (2023, str. 33) identifikace a hodnocení rizik zahrnuje hledání možných rizik, kterým může organizace čelit, a posouzení jejich pravděpodobnosti a potenciálního dopadu. Hnilica a Fotr (2014, str. 26) uvádí, že cílem identifikace rizik je nalézt komplexní soubor faktorů, které mohou mít vliv (ať už pozitivní nebo negativní) na hospodářské či jiné výsledky organizace, hodnotu určitých aktiv nebo úspěšnost plánovaných nebo probíhajících projektů. Oškrdal a Doucek (2014, str. 196) konstatují, že cílem identifikace rizik je identifikovat, pojmenovat a zdokumentovat potenciální hrozby a příležitosti, které mohou ovlivnit průběh projektu. Dle autorů mohou rizika vznikat z různých faktorů, je proto velmi důležité předem určit jejich klasifikaci pro efektivní řízení.

Rizika se mohou kategorizovat na základě mnoha parametrů. Dle Paula (2023, str. 33) mohou být rozdělena následně:

- strategická (mohou mít vliv na schopnost organizace dosáhnout svých cílů),
- finanční (mohou mít dopad na finanční výkonnost organizace, např. riziko úvěrových sazeb či riziko likvidity),
- provozní (mohou ovlivnit provoz organizace, např. přerušení dodavatelského řetězce, selhání it či přírodní katastrofy),
- rizika spojená s dodržováním předpisů (právní předpisy, regulace, průmyslové standardy), riziko ztráty dobré pověsti (negativní publicity, krize na sociálních médiích),
- riziko třetích stran (vztahy s dodavateli, zákazníky a dalšími třetími stranami).

Myšková (2022, str. 110) dále rozvádí členění z pohledu finančního rizika a uvádí, že souvisí s tržním rizikem, zadlužeností, a operačního rizika. Oškrdal a Doucek (2014, str. 196) člení rizika na externí či interní. Externí rizika autoři dělí do tří kategorií. První kategorie zahrnuje rizika, která jsou nepředvídatelná a nekontrolovatelná, jako jsou státní regulace, přírodní katastrofy, kriminální aktivity či legislativní změny. Druhá kategorie se týká předvídatelných, avšak špatně ovladatelných rizik, např. tržních rizik, operačních rizik, daňové úpravy či inflace. Třetí kategorie se týká situací, kdy dochází k selhání předpokladů realizace, např. změny ve financování projektu či změny ve vlastnické struktuře. Interní rizika dále autoři člení na netechnické či technické. Smejkal a Rais (2013, str. 92) dodávají, že existují i další druhy rizik, např. politické a teritoriální, bezpečnostní, právní, specifická (např. pojišťovací, manažerská apod.).

Akinfewna (2023, str. 4) specifikuje, že v rámci procesu identifikace rizik se rizika mohou rozpoznávat podle různých metod, jako jsou např. brainstorming, SWOT analýza či scénářovou analýzu. Paula (2023, str. 33) dodává, že k dalším účinným technikám identifikování a hodnocení rizik patří také workshopy, dotazníky, registr rizik či analýza hlavních příčin tzv. „*root cause analysis*“.

## Hodnocení rizik

Akinfenwa (2023, str. 4) zdůrazňuje, že hodnocení rizik, jakožto součást procesu řízení rizik, je klíčovým prvkem pro organizace všech velikostí a odvětví, jelikož umožňuje efektivní alokaci zdrojů a minimalizaci negativních dopadů. Autor dále konstatuje, že prostřednictvím identifikace a hodnocení rizik mohou organizace provádět informovaná rozhodnutí, lépe alokovat své zdroje a být lépe připraveny na nečekané události. Tímto procesem organizace získávají důležité informace, které jim umožňují efektivně reagovat na rizika a zajistit jejich řízení a kontrolu.

Smejkal a Rais (2013, str. 132) dodávají, že cíle řízení rizik by měly být v souladu s podnikovými strategickými cíli. Pokud je cílem firmy přežití, měla by se soustředit na snížení nákladů, diverzifikaci odbytu a ověření solventnosti nových partnerů. Je-li cílem firmy růst, je důležité spravovat rizika ve financích. Jestliže firma chápe krizi jako příležitost, měla by investovat do inovací a marketingu. Autoři dále upozorňují, že významným krokem v procesu řízení rizik je výpočet a hodnocení rizik. Elliota (2020, str. 14–15) poukazuje na hodnocení rizik z pohledu kontinuity podnikání, jehož hlavním cílem je vypracování plánu pro řešení mimořádných událostí neboli plán kontinuity podnikání. Plán by měl zahrnovat hodnocení rizik, identifikaci událostí, které mohou narušit provoz a odpovídající strategie pro minimalizaci rizik. Dle autora by plán měl také zahrnovat záložní plán pro poskytování služeb, včetně alternativních dodavatelů a ochranu počítačových systémů a dat.

### **Metody analýzy rizik**

Eriksson (2023, str. 1) popisuje analýzu rizik jako klíčovou součást preventivního přístupu k řízení krizí. Autor konstatuje, že analýza rizik pomáhá organizaci předcházet a připravit se na rizika, místo reaktivního jednání a řešení problémů až v případě vzniku krizí. Sobia Publication (2022, str. 35) vnímá analýzu rizik jako důležitou fázi v procesu řízení rizik, jelikož poskytuje různé pohledy na identifikovaná rizika, což je důležité, protože komplexní a opakující se analýza vytváří solidní základ pro monitorování a řízení rizik. Alexander (2018, str. 33) zmiňuje, že jakmile jsou rizika identifikována, je zapotřebí provést analýzu rizik. Hlavním cílem je odhadnout rizika, která ovlivňují klíčové aktivity organizace. Autor dále uvádí, že po provedení analýzy rizika následuje proces hodnocení rizika.

Dumitrascu (2018, str. 38) rozděluje rizika na negativní rizika, a pozitivní rizika. Autor dále uvádí, že je důležité, aby organizace byla schopná určit pravděpodobnost výskytu rizika a také jeho dopad, tedy pravděpodobný důsledek. Dle autora existuje mnoho různých metod pro identifikaci příležitostí, jako je průzkum trhu, výzkum a vývoj, testovací marketing. Marks (2020, str. 107) dodává, že mezi běžné metody hodnocení rizik patří také analýza trendů a modelování, sofistikované nástroje, jako je strojové učení (machine learning), workshopy či rozhovory s manažerem rizik.

Balog a Iakovets (2020, str. 74) konstatují, že existují dva typy metod pro analýzu rizik: induktivní a deduktivní. Induktivní metody mají výhodu v tom, že umožňují předpovídat možné selhání celých zařízení. Tyto metody se zaměřují na identifikaci konkrétních okolností, které mohou vést ke vzniku rizikových situací. Mohou také poskytnout možnost vyhodnotit počet a důsledky rizikových situací a přijmout vhodná preventivní opatření. Naopak deduktivní metody se zaměřují na analýzu již nastalých rizikových situací v rámci organizací a hledají souvislosti, které k nim vedly. Machado, Ribieiro a Nascimento (2023, str. 1) dodávají, že metody analýzy rizik se mohou používat v různých kontextech a pomáhají snižovat poruchy, nehody, ekonomické nevýhody atd. Často jsou zakotveny v rozhodovacím procesu zainteresovaných stran.

Autoři Balog a Iakovets (2020, str. 74) dále pokračují ve členění nejběžnějších metod analýz rizik:

- Tradiční metody (kontrolní seznam či registr rizik, rutinní testy, audit bezpečnosti, Co se stane, když analýza (what-if Analysis).
- Metody evaluace (relativní klasifikace, rychlá klasifikace, Paretův princip, systémová analýza).
- Kvantitativní metody (analýza ohrožení a provozuschopnosti, analýza selhání a jejich dopadů),
- Grafické metody (analýza stromu poruch, analýza stromu událostí, analýza nebezpečí, analýza příčin a dopadů, metoda rozhodovací matice).



## **What-if analýza (WFA)**

Managementmania.com (2015) popisuje tuto metodu jako analytický nástroj určený k identifikaci pravděpodobného dopadu různých scénářů. Tento přístup je v podstatě strukturovaný brainstorming, ve kterém skupina odborníků používá otázky „co kdyby“ k prozkoumání potenciálních důsledků a vhodných opatření. Autoři dále uvádí, že proces zahrnuje definování oblastí a cílů, formulování otázek a odpovědí a vývoj opatření. V praxi se WFA používá k identifikaci a řešení potenciálních problémů a rizik. Guard7.cz (2022) doplňuje, že přestože je tato metoda méně časově náročná, může být méně systematická, než jsou jiné metody, jako je např. HAZOP (Hazard and Operability Study). Smejkal a Rais (2013, str. 120) souhlasí s výše uvedeným a doplňují, že What-if analýza definuje nebezpečná místa systému a dále identifikuje vstupy pro metody FMEA (Failure Modes and Effects Analysis) a FTA (Fault Tree Analysis).

## **Brainstorming**

Managementmania.com (2016) popisuje brainstorming jako kreativní techniku skupinového řešení problémů, jejímž cílem je získání co největšího množství nápadů. Klíčovými principy této techniky jsou vytváření příjemné atmosféry, omezení kritiky, přijímání všech nápadů bez ohledu na jejich praktičnost či logiku. V brainstormingu jsou všechny nápady cenné a všichni účastníci mají rovné postavení. Snyder (2016, str. 16) dodává, že často nejde jen o to, který nápad funguje, ale spíše o to, jakou kombinaci nápadů lze použít k řešení konkrétního problému. Tato metoda je založena na kvantitě místo kvality, přičemž každý nápad je zaznamenán v nějaké formě. Po shromáždění co nejvíce nápadů účastníci hodnotí, kombinují a vylepšují je. Mitre.org (2023) dodává, že nápady je vhodné zaznamenat, např. na flipchart nebo tabuli, a to s minimálním upravováním a také číslováním nápadů pro budoucí použití. Může být využita technika strukturovaného (každý účastník postupně přednáší svůj nápad), volného (účastníci spontánně přispívají nápady) nebo tichého brainstormingu (účastníci sdílí své nápady anonymně pomocí lístků papírů).

## **STEP analýza**

Hnilica a Fotr (2014, str. 27) uvádí, že v rámci strategické analýzy podnikatelského prostředí může být aplikována SWOT analýza, STEP analýza či Porterův model pěti sil. STEP analýza je anglickou zkratkou počátečních písmen oblastí (Social, Technical, Economical, Political) pomocí této analýzy mohou být definovány sociální, ekonomické, politické a technologické faktory, které mají dle Fotra et al. (2020, str. 58) významný vliv na strategické záměry organizace. Popřípadě může být analýza rozšířena o ekologické a legislativní oblasti (SLEPT, PESTEL). Pokud organizace působí v globálním prostředí a její strategické plány se s ním přímo spojují, je důležité sledovat vývoj na relevantních teritoriích. Tyto metody pomáhají identifikovat především externí rizika. Myšková (2022, str. 26) specifikuje, že v rámci STEP analýzy je vhodné uplatnit metodu ETOP, jež je anglickou zkratkou pro Environment Threat and Opportunity Profile, jež upřesňuje, zda se vlivy, které na organizaci působí, identifikují jako příležitost (označení znaménkem +) či hrozba (označení znaménkem -). Pokud nastane situace, kdy identifikovaný vliv se jeví jako významný, jeho dopad však v době hodnocení nelze stanovit, označí se jako 0. Autorka dále uvádí, že analýzu je dále možné rozšířit o metodu MAP (Monitoruj – Analyzuj – Predikuj), která právě v uvedené situaci dokáže výsledky analýzy lépe specifikovat. V následující tabulce bude zobrazen příklad hodnocení ekonomického faktoru inflace pomocí metody STEP, ETOP a MAP.

Tabulka 1 Hodnocení vlivu inflace metodou STEP, ETOP a MAP

STEP	ETOP	MAP			Výsledné posouzení
Faktor	Vliv +/- /0	Monitoruj (Současný stav)	Analyzuj (Analýza dosavadního vývoje)	Predikuj (Předpoklad vývoje)	Hrozba, příležitost
Inflace	-	3,8 %	Od roku 2018 (2,1 %), postupný růst	Růst inflace v důsledku růstu cen energií, pohonných hmot a potravin	Hrozba

Zdroj: Český statistický úřad (2022) in Myšková (2022, str. 26)

### Matice rizik

Akinfewna (2023, str. 4) dodává, že při analýze se rizika také vyhodnocují pomocí matice rizik na základě pravděpodobnosti jejich výskytu a potenciálního dopadu. Vochozka a Váchal (2013, str. 536) s názorem Akinfewny (2023, str. 4) souhlasí a dodávají, že i přes prokazatelný benefit v podobě jednoduchosti a rychlosti této metody je nevýhoda v nižší míře spolehlivosti, která je způsobena subjektivitou této metody. Názorný příklad matice rizik bude uveden v následující tabulce.

Tabulka 2 Matice rizik

Pravděpodobnost výskytu	Závažnost důsledků				
	Zanedbatelná (1)	Malá (2)	Střední (3)	Významná (4)	Katastrofální (5)
Jistá (5)	5	10	15	20	25
Pravděpodobná (4)	4	8	12	16	20
Možná (3)	3	6	9	12	15
Nepřavděpodobná (2)	2	4	6	8	10
Vzácná (1)	1	2	3	4	5

Zdroj: Vochozka a Váchal (2013, str. 536)

Autoři Vochozka a Váchal k této matici uvádí, že riziko je vypočítáno pomocí následující rovnice, dle které je možno vyjádřit riziko jako „logický součin“:

$$\text{Riziko} = \text{pravděpodobnost výskytu} * \text{závažnost důsledků}$$

V matici rizik je použito barevné rozlišení pro různé stupně rizik. Nejnižší riziko má bílou barvu, střední riziko žlutou barvu, vysoké riziko oranžovou a extrémní riziko barvu červenou.

### **Opatření rizik**

V literatuře se objevuje různé členění přístupů ošetření rizik, nejčastější to jsou však strategie, které popisuje např. autor. Akinfenwa (2023, str. 4). Jedná se o akceptaci rizika, zmírnění rizika, vyhnutí se riziku a přenos rizika. Zeeshan a Javedrozprac (2021, str. 40) ve své publikaci hovoří také o dalších přístupech (využití rizika, sdílení rizika či zvýšení rizika). Detailněji však autoři rozebírají uvedené čtyři základní strategie ošetření rizik.

#### Zmírnění rizika

Smyslem snižování rizik je omezit negativní dopady rizik prostřednictvím preventivních opatření. Často používané strategie snižování rizik zahrnují provádění opatření ke snížení pravděpodobnosti nebo dopadu rizika. Zavedení těchto opatření může být nákladné a časově náročné, proto je důležité pečlivě vyvážit náklady a přínosy. Tento kompromis je kritický, protože rozhodnutí v procesu řízení rizik ovlivňují obchodní výsledky.

#### Přenos rizika

Výše uvedení autoři konstatují, že rizika mohou být převedena nebo sdílena s cílem přenést vlastnictví a odpovědnost na třetí stranu. Může se jednat o rizika, které nelze zvládnout samostatně a vyžadují pomoc externího subjektu. V případě přesunu nebo sdílení je nezbytné, aby smlouva nebo dohoda jasně stanovila, jak budou rizika rozdělena např. mezi zákazníka a dodavatele. Pro zajištění a ospravedlnění nákladové efektivity přenosu rizik lze provést analýzu nákladů a přínosů (tzv. „Cost-benefit analysis“). Rizika lze přesunout na třetí stranu prostřednictvím smlouvy, pojištění nebo subdodávky, často s sebou nese placení pojistného.

#### Vyhnutí se riziku

Na základě informací od výše uvedených autorů je nejlepší strategií na nejrizikovější činnost pokusit se ji eliminovat. Nejradikálnější strategií vyhnutí se je zrušení nebo kompletní ukončení projektu. Vyhnout se riziku znamená odstranění hrozby tím, že bude odstraněna její příčina a projekt bude veden jiným způsobem.

#### Akceptace

Tato strategie může být reakcí na rizika, která již nelze řešit jinými strategiemi. Zahrnuje neprovádění změn v plánu a souhlas s tolerováním rizika, která se řeší pouze v případě jeho výskytu. Může být dělena na aktivní akceptaci, které zahrnuje přijetí rizika a přidělení dodatečných zdrojů, jako jsou finance, čas a plány zálohy nebo pasivní akceptace, která znamená přijetí rizika bez konkrétního plánu nebo monitorování. Na rozdíl od ostatních strategií, která jsou vnímány jako preventivní a uplatňují se před výskytem rizika se akceptace realizuje pouze při skutečném výskytu během provádění projektu.

Hnilica a Fotr (2014, str. 18) souhlasí s výše zmíněnými strategiemi na ošetření rizik s Zeeshanem a Javedem (2021, str. 40) a k problematice vyhýbání se riziku dodávají, že vyhnutí se riziku může také znamenat, že se organizace rozhodne neúčastnit se určité aktivity nebo projektu s vysokým rizikem, které by bylo nepřijatelné. Například by se mohlo jednat o zavedení nového produktu nebo technologie, realizace akvizice, vstup na nové trhy apod.

Výše uvedení autoři však zdůrazňují, že příliš časté vyhýbání se riziku může mít negativní dopad na konkurenční postavení organizace, protože při tomto přístupu mohou být přehlídny příležitosti. Některá rizika jsou nevyhnutelná a jejich úplné vyhnutí se nemusí vždy ukázat jako výhodné. Sobia Publication (2022, str. 53) dodává, že snižování rizik znamená také plánování

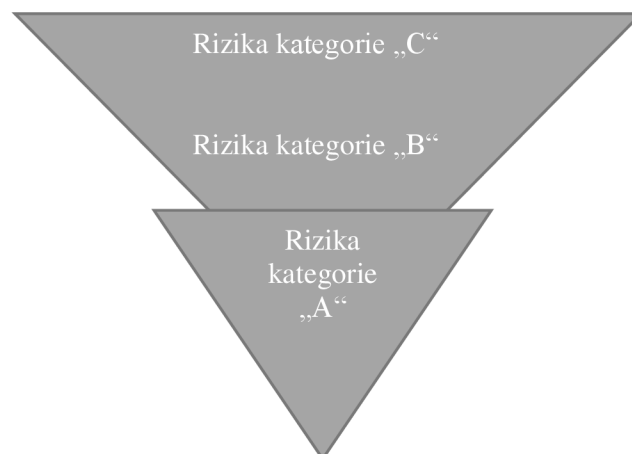
aktivit, které sníží nebo eliminují dopad rizik na projekt či vývoj produktu. Dumitrascu (2018, str. 106) dodává, že kontingenční reakční strategie představují důležitou možnost, kterou je třeba zvážit při rozhodování, jak reagovat na rizika. Jedná se o aktivní formu přijetí rizika, která zahrnuje plánování reakcí v případě, že se rizikové události skutečně vyskytnou. Tyto strategie také zahrnují přidělení rezerv, aby mohly být reakce realizovány, když je to nezbytné. Rezervy mohou zahrnovat finanční prostředky, čas, materiál i personál.

### **Plánování a monitorování řízení rizik**

Geary (2022, str. 65–66) pohlíží na plánování jako součást aktivit vedoucího pracovníka pro řízení rizik. Dle Geary plánování zahrnuje vytváření směrnic týkajících se řízení rizik, stanovení mandátu správní rady a závazku k řízení rizik, definování rolí auditního a rizikového týmu. Autorka dále uvádí, že v rámci monitorování je potřeba zahrnout zaznamenávání a vyhodnocování rizik, hodnocení opatření, která by je měla snížit, agregaci dopadů incidentů spojených s riziky a porozumění důvodům jejich výskytu, s cílem jim v budoucnu předejít.

Dumitrascu (2018, str. 117) popisuje možný proces monitorování řízení rizik. Autor uvádí, že jej lze provést například vyhodnocením účinnosti jednotlivých fází procesu. První fáze spočívá v identifikaci rizik, se kterými se organizace potýká. Druhá fáze je posouzení identifikovaných rizik. Ve třetí fázi je doporučováno zabývat se řešením rizik. Autor dále uvádí, že pro posouzení každé fáze je možné si položit několik otázek, aby bylo zjištěno, zda byla daná fáze zvládnuta. Např. pro první fázi, zda byla všechna rizika identifikována. Pro druhou fázi, zda bylo posouzení rizik účinné. Pro třetí fázi, zda byly reakce účinné. Pokud jsou odpovědi negativní, je důležité analyzovat důvody a zdokumentovat jakékoliv získané poznatky. Antušák (2013, str. 86) hodnotí správnou evidenci (registraci) rizik jako klíčovým prvkem systému monitorování. Autor dále konstatuje, že každé riziko, které je považováno za nebezpečné nebo důležité na základě stanovených kritérií (kategorie A, B, C), musí být pečlivě zaznamenáno a informace o jeho vývoji průběžně předávány odpovědným pracovníkům ve firmě, kteří následně rozhodují o dalším postupu s těmito riziky. Jednotlivé kategorie rizik jsou popsány v následujícím obrázku.

Obrázek 2 Monitoring rizik



Zdroj: Antušák (2012, str. 86), vlastní zpracování

Dle výše uvedených autorů je v rámci kategorie „C“ uskutečňován průběžný monitoring a nadále sledují vývoj rizik. Kontinuálně informují řídicí pracovníky o situaci, popřípadě zahájí přípravu intervenčních opatření (kategorie „B“). V případě extrémní eskalace (kategorie „A“) jsou řídicí pracovníci informováni okamžitě za pomoci systému včasné výstrahy.

## 2.2 Krizové řízení

Vilášek a Antušák (2016, str. 20) vnímají současnou dobu jako velmi turbulentní a neustále se měnící prostředí. Manažeři čelí výzvám, které vyžadují rychlé přizpůsobení se novým požadavkům, popř. zbavení se zastaralých postupů. Autoři dále rozvíjejí tuto myšlenku a jako důvod tohoto „chaosu“ v manažerském uvažování vnímají přítomnost nových směrů (globalizace, nové technologie), které vyžadují zavedení nových technik a přístupů v řízení organizace – tzv. „*managementu v podmínkách kritických změn*“. Willie (2023, str. 4) dodává, že krize mohou přicházet v různých podobách a mají potenciál narušit běžný život. Přináší ale také možnosti růstu a odolnosti. Efektivní řízení krizí je nezbytné pro minimalizaci negativních dopadů a maximalizaci přínosů. Shuaib (2019, str. 21) doplňuje, že klíčové pojmy v oblasti krizového řízení jsou „hrozba“, „organizace“ a „neočekávaná událost“. Elliot (2020, str. 20–21) doplňuje, že organizace mohou čelit pracovním krizím, které ovlivňují pracovní prostředí. Připravenost na tyto krize je klíčová a musí být součástí plánu kontinuity podnikání. Mezilidské dovednosti, jako je proaktivita, klidné chování a empatie jsou nezbytné pro řízení krizových situací. Al-Da'abseh, Aljawarneh & Shwiyat (2018) in Thani (2020, str. 308) uvádí, že krizový management je jedinečný administrativní proces, který čelí nečekaným událostem. Krize dle autorů vyžaduje rozhodné kroky a rychlá rozhodnutí, která se odvíjí od toho, jak vážná je situace a jakou rychlostí se vyvíjí.

Dle Ozaka (2016, str. 3) se krizové řízení zaměřuje na identifikaci, hodnocení a kontrolu potenciálního dopadu neočekávané a závažné události, která může negativně ovlivnit organizaci nebo komunitu. Jeho hlavním cílem je minimalizovat dopady krize, chránit lidi a majetek a co nejrychleji a nejefektivněji obnovit postiženou organizaci nebo komunitu do normálního stavu. Gozora (2017, str. 82) hovoří o tom, že v minulosti v rámci podnikového managementu byla prováděna preventivní opatření s cílem předejít přírodním katastrofám, minimalizovat dopady ekonomických krizí na podnikovou ekonomiku a předcházet vzniku krizových jevů. I přes tyto vyvíjené aktivity však nebylo možné zcela eliminovat vznik krizí a následné ekonomické či lidské ztráty. Proto vznikla potřeba efektivního mechanismu, který by minimalizoval negativní dopady krizových situací. V této souvislosti se v 60. letech 20. století prosadil koncept krizového managementu.

### 2.2.1 Definice krize a její typy

Dle zákona č. 240/2000 Sb., zákon o krizovém řízení a o změně některých zákonů, je krizová situace „*mimořádná událost podle zákona o integrovaném záchranném systému, narušení kritické infrastruktury nebo jiné nebezpečí, při nichž je vyhlášen stav nebezpečí, nouzový stav nebo stav ohrožení státu*“. Gozora (2017, str. 67) definuje, že krize je kritický okamžik, při němž dochází k negativnímu obratu ve vývoji a aktuální stav se zhoršuje. Představuje složitý a těžko překonatelný stav v mnoha aspektech, především ve společenském, ekonomickém či organizačním systému. Bednář (2022, str. 30) podotýká, že bez ohledu na příčinu nebo charakter krize je potřeba ji brát jako dočasný stav, který musí být překonán, odstraněn a nahrazen normálním stavem. Autor dále uvádí, že akceptování krize jako nového normálu může vést k neustálému stresu, přetížení a obavám z negativního vnímání budoucnosti a je důležité brát krizi pouze jako časově omezenou situaci, kterou je potřeba vnímat jako příležitost ke změně, zlepšení na lidské úrovni či na úrovni organizace, popřípadě implementace nových procesů.

Vilášek a Antušák (2016, str. 41) upozorňují na to, že definice nejen krize, ale i dalších pojmů v oblasti krizového managementu nejsou v literatuře jednotné, vzhledem k širokému pojetí této

problematiky. Souhlasí s výše uvedenými autory, že krize je „*složitá, kombinovaná krizová situace*“, Dle autorů znamená krize nestabilní dobu či stav, kdy se blíží rozhodující změna, která může přinést buď pozitivní, nebo negativní výsledky. Gozora (2017, str. 67) ve své definici vnímá krizi spíše jako negativní jev. Vilášek a Antušák dále uvádí, že krize může ohrozit bezproblémový provoz organizace a narušit základní struktury a hodnoty společenského systému. Krize může také poukazovat na neschopnost vedení adekvátně na situaci reagovat či vůbec reagovat.

Fotr et al. (2020, str. 307) vnímají podobně jako Gozora (2017, str. 67) krizi jako situaci, která může mít významné negativní dopady na výkon organizace. Zásadním způsobem může ovlivnit činnost, integritu, pověst, a dokonce i životaschopnost podniku. Z pohledů autorů je tedy důležité být připraven na krizové situace a mít vytvořené plány na jejich řešení. To zahrnuje identifikaci možných rizik, vytvoření krizového plánu a pravidelné testování jeho účinnosti. Willie (2023, str. 8) vnímá krizový management pro organizace jako klíčový z několika aspektů:

- Chrání reputaci a udržuje důvěru stakeholderů.
- Předchází podobným krizím v budoucnu pomocí identifikace hlavních příčin a implementací opatření, které jim zabrání.
- Pomáhá zachovat kontinuitu provozu a minimalizuje narušení činnosti organizace.
- Implementuje účinná a efektivní opatření k vyřešení krize a co nejrychlejšímu návratu k normálnímu provozu.
- Zajišťuje bezpečnost a pohodu zaměstnanců, zákazníků a dalších zúčastněných stran, kterých se krize týká.

V literatuře se krize mohou skloňovat v mnoha podobách, její kategorizace se mohou lišit. Rolínek et al. (2017, str. 30) in Smejkal a Rais (2013, str. 26) rozděluje podnikové krize na vnitřní či vnější. Mezi vnitřní patří především materiálové a surovinové krize, finanční či personální. Krize spojené s vnějším okolím souvisí například s odbytovou krizí, signifikantních změn v cenové politice dodavatelů, legislativa apod. Smejkal a Rais (2013, str. 26) dále rozlišují krizi na závažnou či méně závažnou. Krize může také dělit podle toho, zda se jedná o pomalý vývin krize (např. zánik trhů) nebo rychlý vývin krize (živelní katastrofa, epidemie).

Shayb (2021, str. 18 in Shrivastava a Mitroff) souhlasí s Rolínkem et al. (2017, str. 30 in Smejkal a Rais, 2013, str. 26) a doplňuje, že dělení krizí na vnitřní a vnější je klíčové, jelikož varovné signály se liší pro každý typ krize a mohou naznačovat odlišné charakteristiky a projevy. Dle něj je také velmi důležité odlišovat, zda byla krize způsobená technickými nebo ekonomickými selháními, od těch způsobenými lidským či organizačním faktorem. Ozak (2016, str. 6) také vnímá důležitost rozlišování různých typů krizí a jejich charakteristik. Jen díky tomu lze krizi efektivně zvládnout. Z jeho pohledu mezi nejběžnější typy krizí patří např. přírodní katastrofy, technologické krize, finanční krize, zdravotní krize, politické krize a enviromentální krize. Přikrylová et al. (2019, str. 133) zmiňuje, že před krizí je potřeba vykonat krizový audit, který je graficky znázorněn v následující tabulce:

Tabulka 3 Krizový audit

<b>Technické a ekonomické příčiny krize</b>	
<b>Vnitřní:</b> vady výrobků/služeb, průmyslové havárie, selhání výpočetní techniky, nesprávné nebo utajené informace, bankrot	<b>Vnější:</b> poškození životního stylu, rozsáhlé selhání systémů, přírodní katastrofy, nepřátelské převzetí firmy, vládní a mezinárodní krize
<b>Lidské, sociální a organizační příčiny</b>	
<b>Vnitřní:</b> neschopnost přizpůsobení či změny, organizační selhání, komunikační nedorozumění, sabotáž a poškození výrobku v podniku, fámy, hloupé žerty, pomluvy, protiprávní aktivity, nemoci z povolání	<b>Vnější:</b> sabotáže a poškození výrobků vně, bojkoty, teroristické činy, únosy vrcholových manažerů, opozice, stávky

Zdroj: Přikrylová et al. (2019, str. 143)

Přikrylová et al. (2019, str. 143) souhlasí s rozdělením krizí na vnitřní a vnější se Smejkalem a Raisem (2013, str. 26) in Rolínek et al. (2017, str. 30). Rozdělení dále specifikuje na technické a ekonomické nebo příčiny způsobeny lidským faktorem, s čímž souhlasí Shayb (2021, str. 18 in Shrivastava a Mitroff). Dle výše uvedené autorky je možné na základě tohoto rozdělení vytipovat možná rizika a pravděpodobnosti výskytu.

### 2.2.2 Fáze krizového řízení

Fáze krizového řízení zahrnují několik klíčových činností, které se provádějí při přípravě na krizi, během samotné krize a po jejím skončení. Shuaib (2019, str. 22) kategorizuje fáze krizí jako předkrizovou fázi, která představuje varovnou fázi, akutní krizovou fázi, která nastává v okamžiku krizové situace a post krizová fáze, která přichází po přijetí vhodných opatření a zahrnuje vyhodnocení a zhodnocení incidentu. Tyto fáze reflektují časový průběh krize a umožňují lépe porozumět procesu krizového řízení a komunikace. Crandall, Parnell a Spillan (2013, str. 5) rozdělují krizi na čtyři fáze, a sice jako předpoklady vedoucí ke krizi, spouštěcí událost, samotnou krizi a post krizovou fázi. Shodují se se Shuaibem (2019, str. 22) že rozdělení na tři fáze patří mezi nejběžnější. Coombs (2023, str. 55–56) souhlasí se Shuaibem (2019, str. 22) s rozdělením procesu řízení krizí do tří fází a specifikuje jednotlivé fáze následovně:

#### Předkrizová fáze

Tokakis, Polychroniou a Boustras (2018, str. 2) tvrdí, že předkrizová fáze zahrnuje detekci signálů předcházejících krizí, přípravu na krizi a její prevenci. Autoři dále uvádí, že další faktory, jako je organizační kultura a struktura mohou ovlivňovat pravděpodobnost vzniku krize. Murray (2022, str. 4–5) souhlasí s výše zmíněnými autory Tokakis, Polychroniou a Boustras (2018, str. 2), že předkrizová fáze se zaměřuje na prevenci a připravenost. S tímto tvrzením souhlasí také autoři Coombs a Laufer (2018, str. 2) a jako důvod dodávají, že je potřeba, aby se minimalizovala škoda pro organizaci. Murray (2022, str. 4–5) dále uvádí, že účinné řízení krizí je klíčové pro ochranu organizace a jejích zainteresovaných stran před škodami a snižováním dopadů krizových situací.

Shearsett a Bevoc (2016, str. 121–125) definují následujících sedm kroků, které by měly být učiněny v rámci předkrizové fáze:

- První krok je dle autorů vytvoření krizového týmu, kdy je potřeba vytvořit tým z kvalifikovaných jedinců, kteří budou mít na starost všechny aspekty programu a řešení krizových situací při jejich výskytu. Organizace nemusí být omezena ve výběru pouze na interní zaměstnance, může zahrnovat i externí odborníky.
- Druhý krok výše zmínění autoři uvádí jako definování nejhoršího možného scénáře. Ten by nikdy by neměl být podceňován potenciál vzniku krize a na základě toho je třeba přizpůsobit plánování a řízení krizí. Tento přístup vyžaduje aktivní a proaktivní postup namísto pouhé reaktivity. Jedna z možností tohoto procesu je brainstorming, který umožňuje týmu pro krizový management identifikovat potenciální krizové situace, které by mohly v organizaci nastat. Na základě těchto identifikovaných rizik je pak možné formulovat příslušné reakce a plány, které by měly být implementovány v případě krizové situace.
- Jako třetí krok uvádí autoři ustanovení mluvčího. V případě krizové situace by měla být ve vedení týmu pro krizový management určena osoba, která bude zodpovědná za komunikaci s vnějším světem. Tato osoba by měla být schopna odpovídat na otázky dodavatelů, zákazníků, vlády, veřejnosti a médií. Není doporučováno určit více lidí pro tuto roli, jelikož by mohli podávat rozlišné informace a krizovou situaci tak ještě zhoršit.
- Jako čtvrtý krok následuje dle autorů určení příslušných odborníků. Jedná se o autority, které budou kontaktovány v případě krize. Jsou to také zkušení odborníci, kteří jsou schopni poskytnout pomoc a poradit v krizových situacích, např. Policie ČR, Hasičský záchranný sbor atd.).
- Pátý krok výše zmínění autoři uvedli jako seznam potenciálních krizí. Tento seznam má cíl identifikovat možné krizové situace, které by mohly vzniknout.
- Šestý krok je dle autorů tvorba seznamu opatření. Konkrétní krize je identifikována spolu s opatřeními, která budou přijata.
- Posledním, sedmým krokem je dle autorů trénink zasaženého personálu. Jedná se o školení se zaměřením na členy krizového řízení. Je možné že všichni zaměstnanci budou potřebovat nějakou formu školení, aby byli seznámeni s možností vzniku krize, s kroky při krizi a s dopady krize.

### **Akutní fáze krize**

Vilášek a Antušák (2016, str. 26) konstatují, že akutní krize vzniká v okamžiku, kdy se rozdíl mezi zájmy subjektu a jeho vnějším prostředím prohlubuje natolik, že už je krize evidentní, což vede ke zjevnému ohrožení zájmu subjektu a jeho další existence. Autoři dále uvádí, že tato fáze vyžaduje okamžitou protikrizovou intervenci a nasazení veškerých dostupných prostředků za účelem získání kontroly nad krizí. Shayb (2021, str. 35) souhlasí s tvrzením Viláška a Antušáka (2016, str. 26) a dodávají, že krize přechází z předkrizové do akutní fáze v momentě, kdy se stává viditelnou vně organizace. V této fázi nemají manažeři jinou možnost než ji aktivně řešit. V této fázi je již pozdě na preventivní opatření, protože jakákoli akce podniknutá v tomto bodě je spíše spojena s omezením škod a kontrolou situace.



## Post krizová fáze

Tato fáze slouží na vyhodnocení a zdokonalení plánu pro budoucí krize. Bevoic a Shearsett (2016, str. 126) dodávají, že po ukončení krize je nezbytné, aby zodpovědní pracovníci provedli rozbor situace. Tento rozbor slouží k lepšímu pochopení příčin krizové situace a potenciálně umožňuje přijmout opatření k jejímu předejití v budoucnosti. Agnes (2018, str. 204–205) dodává, že cílem post krizového hodnocení by mělo být vypracování akčního plánu nebo seznamu úvah, který pomůže efektivně zhodnotit a analyzovat krizi a její řízení, stejně jako vypracovat strategii po krizi a identifikovat další kroky. Autorka dále uvádí, že v rámci hodnocení by měl být diskutován skutečný incident (co se stalo, proč se tak stalo a jak se situaci vyvarovat do budoucna), strategické další kroky, krátkodobé a dlouhodobé dopady krize na organizaci, jaké akce je třeba podniknout k obnovení případně způsobených škod a ke snížení dalšího poškození nebo narušení.

### 2.2.3 Strategie v oblasti krizového řízení

Rubens (2023, str. 14) tvrdí, že v literatuře o rozhodování v prostředích řízení krizí v prostředích řízení krizí je možné identifikovat dvě oblasti. První zahrnuje teoretická studia o různých aspektech rozhodování v širším organizačním kontextu (leadership, autorita, skupinové myšlení, sdílení informací atd.), která jsou relevantní i pro řízení krizí. Druhá oblast se dle autora zaměřuje na výzkum operativních selhání v reakcích na krizové a mimořádné situace s cílem identifikovat jejich příčiny. Murray (2022, str. 26–27) detailněji identifikuje klíčové strategie v oblasti krizového řízení:

- 1. Předvídání:** Je důležité být proaktivní a připravit se na potenciální krizové situace. Intenzivní brainstorming by měl být uskutečněn s cílem projít všechny možné krizové scénáře a vytvořit plán reakce na krizi.
- 2. Vytvoření a otestování plánu:** Plán reakce na krizi by měl být přizpůsoben organizaci a zahrnovat jak operační, tak komunikační aspekty. Je nezbytné, aby tyto zprávy byly doručeny efektivně a s důvěryhodností, proto je nutné je otestovat. V této fázi se také konají krizové školení a simulace, stejně jako mediální školení těm, kteří budou veřejně vystupovat. Provedením těchto kroků bude zajištěno, že organizace bude schopná provést plán reakce v reálné situaci, nejen v teorii.
- 3. Identifikace týmu pro komunikaci v krizi:** Je důležité vybrat malý tým vysoce postavených manažerů, kteří budou zodpovědní za komunikaci v krizových situacích. Tento tým by měl stanovit proces komunikace pro organizaci a zajistit, že zaměstnanci budou informováni o postupu v případě krize.
- 4. Zřízení systémů pro notifikaci a monitoring:** Je důležité sledovat, co je řečeno o organizaci v tradičních i sociálních médiích a komunikovat s interními a externími zainteresovanými stranami. Monitoring zpětné vazby během krizové situace umožňuje přesné přizpůsobení strategie a taktik.
- 5. Komunikace:** Nejvýznamnějším pravidlem krizového řízení je krizová komunikace. Rané fáze krize jsou klíčové a určují tón pro celou krizi. Otevřenost a informování veřejnosti o situaci, oprava dezinformací a aktivní zapojení jsou nezbytné. Mlčení nebo zdání ignorování problémů může vyvolat nevoli veřejnosti.
- 6. Analýza po krizi:** Po krizi je důležité provést analýzu toho, co bylo provedeno dobře, co by se mohlo zlepšit a jak lze zvýšit efektivitu krizového plánu. Tato analýza posiluje plán a přispívá ke zlepšení reakce na krizové situace.

#### 2.2.4 Krizová komunikace

Pohled autorů na problematiku krizové komunikace je vesměs jednotný. Robertson (2019, str. 14) uvádí, že krize se často vyznačují zmatkem. Informace mohou být protichůdné a je značný zájem o to, co se děje. Bez adekvátní komunikace se příběh snadno zakotví v dezinformacích či kolují různé spekulace. Oproti tomu efektivní krizová komunikace může navzdory výzvám povýšit reakci organizace nad úroveň vytváření omluv a poskytnout důležité informace zainteresovaným stranám. Tomandl (2020, str. 47) definuje krizovou komunikaci jako „*součást reakce organizací (nebo i jednotlivců) na ohrožení reputace a na mimořádné události*“. Autor dále vnímá jako podstatný fakt, že v případě krize je organizace automaticky vystavena pozornosti veřejnosti a médií. Je tedy klíčové, aby problém či události, které nastaly, byly řešeny věcně a v rámci krizového managementu. Ten je zpravidla v kompetenci nejvyššího vedení organizace. Karlíček (2016, str. 141) definuje krizovou komunikaci z marketingového pohledu. Zdůrazňuje, že percepce veřejnosti je často mnohem důležitější než realita. Jako zásadní tedy vnímá nutnost komunikace a přístupnosti k médiím a také rychlé jednání.

Tomandl (2020, str. 49–73) zmiňuje jako hlavní zásady správné krizové komunikace transparentnost, pravdivost, akceschopnost, zodpovědnost, srozumitelnost, konzistentnost, rychlost, aktivitu, budování důvěry. Wheeler (2019, str. 20) souhlasí s Tomandlem (2020, str. 49–73) a k zásadám krizové komunikace dodává, že důležitá je také příprava. Mlčení a nečinnost nejsou přijatelné možnosti v krizové situaci. Je nezbytné být připraven k aktivnímu postupu a vyjádření se. Média i veřejnost mohou považovat mlčení a zmatek za projev viny. Proto je nezbytné provést alespoň základní přípravu na krizovou komunikaci, bez ohledu na velikost, strukturu či typ podnikání. K dalším zásadám dle autora patří, že komunikace samotná je důležitější než detaily krize. V tomto aspektu tedy souhlasí s Karlíčkem (2016, str. 141). Wheeler (2019, str. 20) dále uvádí, že silné vedení je klíčové. Pokud vedoucí pracovník přijme zodpovědnost a vystoupí před médii, vypadá to mnohem důvěryhodněji, než když stejný krok podnikne mluvčí organizace.

Hemus (2020, str. 111–116) zdůrazňuje důležitost plánu krizové komunikace (krizový manuál). Dle autora představuje základní nástroj pro ochranu reputace. Jeho hlavním cíle je umožnit rychlou a vhodnou komunikaci se zúčastněnými stranami za účelem udržení důvěry. Plán by měl obsahovat směrnice, role a odpovědnosti týmu, kontrolní seznamy prvních kroků, klíčové komunikační principy a také šablony komunikačních materiálů a průvodce postupy. Autor dále uvádí, že je důležité, aby plán byl flexibilní a přizpůsobitelný situaci, a aby bylo plánování komunikace spojeno s krizovým řízením a lidským úsudkem. Karlíček (2016, str. 143) souhlasí se souhrnem Hemuse (2020, str. 111–116) a dodává, že krizový manuál by také měl obsahovat nejvýznamnější a nejpravděpodobnější rizika, kterým může organizace čelit. Manuál by také měl obsahovat různé typy podkladových materiálů, např. různé certifikáty, statistiky, schémata.

Přikrylová (2019, str. 135) zmiňuje tři strategie, které lze uplatnit v rámci krizové komunikace, a sice defenzivní strategie (organizace se rozhodne nepodávat vyjádření, než budou známy bližší informace), ofenzivní strategii (proaktivní přístup a transparentnost), či strategii „mrtvého brouka“ (běžná reakce nepřipravené organizace na krizi, která většinou má negativní ohlas veřejnosti).

#### 2.2.5 Role centrální banky v krizovém řízení

Dle serveru podnikatel.cz (2023) se ČNB aktivně připravuje na krizové situace, což zahrnuje zřizování krizového štábu, identifikaci a analýzu potenciálních rizik a provádění preventivních kroků k odstranění nedostatků. V rámci této přípravy ČNB také vytváří podmínky pro nouzovou komunikaci s dalšími správními úřady a subjekty a konzultuje s vládou o krizových opatřeních.

ČNB je také pověřena projednáváním přestupků spojených s porušením krizových opatření a vydáváním speciálních povolení. Kromě toho ČNB připravuje krizový plán, který je schválen guvernérem a koordinuje s ostatními ministerstvy a správními úřady. V kontextu ochrany kritické infrastruktury, ČNB navrhuje odvětvová kritéria, získává nezbytné informace pro identifikaci klíčových prvků infrastruktury a určuje opatření k její ochraně.

ČNB (2023) uvádí, že je v rámci zákona č. 240/2000 Sb. povinna připravovat se na krizové situace prostřednictvím vytváření krizových a havarijních plánů, zejména v oblasti měnové politiky a bankovníctví. Tyto plány se zaměřují na řešení mimořádných událostí, které by mohly destabilizovat finanční trh České republiky. Důraz je kladen na zajištění kontinuity služeb, zejména díky záložním informačním systémům a pravidelnému testování v reálném prostředí. V rámci své role v evropském systému národních bank ČNB aktivně spolupracuje s dalšími centrálními bankami a dodržuje mezinárodní standardy a doporučení, což potvrzuje její závazek k dosažení vysoké úrovně krizového řízení.

ČNB (2023) dále dodává, že v případě blížícího se selhání finanční instituce upřednostňuje likvidaci nebo insolvenční řízení. Pokud je však ve veřejném zájmu, může ČNB využít speciální nástroje pro řešení krize, např. „bail-in“, což zahrnuje přerozdělení ztrát. Pro zajištění transparentního a efektivního krizového řešení stanovuje ČNB minimální kapitálové požadavky (MREL) pro finanční instituce.

## **2.3 Krizové scénáře a plány**

Harazín et al. (2018, str. 18) vnímají plánování a tvorbu scénářů budoucích událostí jako neustále probíhající proces, který bere v úvahu nepředvídatelné události a proměnlivost prostředí. Autoři dále rozvíjí myšlenku a tvrdí, že klasické postupy strategického plánování často selhávají v dnešním rychle se vyvíjejícím světě, což může vést ke frustraci a nedůvěře v tuto metodu. Proto se metoda strategického plánování pomocí scénářů stala rozhodujícím faktorem úspěchu firem, které se dokážou rychle přizpůsobit změnám a získat tak konkurenční výhodu na globálním trhu. Cane (2019, str. 35) tvrdí, že pečlivá příprava a plánování jsou klíčovými kroky při jakémkoli podnikání. Plány a postupy jsou zásadní součástí každé organizace a poskytují mapu pro provoz společnosti, zajišťují dodržování zákonů a předpisů, poskytují směrnice pro rozhodování a zefektivňují interní procesy. Autor dále uvádí, že plány krizového řízení se používají k přípravě správných kroků pro řešení krizových situací a minimalizaci negativních dopadů na podnikání. Olafsson (2014, str. 54–55) tvrdí, že v oblasti řízení krizí existuje dlouhá tradice tvorby plánů, které identifikují spouštěče, stanoví organizační strukturu a poskytují soubor procesů pro hodnocení, reakci a obnovu. Autor dále dodává, že přítomnost dobře napsaného a pružného plánu poskytuje všem ve společnosti jasnou strukturu, v rámci, ve kterém mohou jednat a vědět, jak se vypořádat s různými situacemi.

### **2.3.1 Definice a význam krizových scénářů a plánů**

Hemus (2020, str. 89) poukazuje na to, že příprava scénářů umožňuje připravit se na budoucí situace před jejich skutečným výskytem. Tato metoda umožňuje zkoumat různé krizové situace a následně vyhodnotit alternativní strategie pro jejich řešení. Deuschel (2021, str. 68) s Hemusem (2020, str. 89) souhlasí a doplňuje, že pomocí plánování krizových scénářů je možné analyzovat různé krizové situace a posoudit různé možnosti reakce, získat strukturovaný přístup k identifikaci nezbytných zdrojů a schopností pro řešení každé situace. Autor dále doplňuje, že adekvátní rozhodnutí a důkladná příprava jsou zásadní pro ochranu podnikání. Plánování scénářů umožňuje systematický trénink rozhodování a myšlení před vypuknutím krizové situace, čímž se šetří čas a zajistí se efektivní reakce v kritických okamžicích.

Prozkoumáním procesů, kontrolních mechanismů a komunikačních kanálů lze zhodnotit jejich správnost a dostupnost.

Harazín et al. (2018, str. 17) definují krizové scénáře z perspektivy bezpečnosti a obrany státu, definici však lze aplikovat napříč odvětvími. Dle autorů strategické plánování prostřednictvím použití scénářů reaguje na významnou nejistotu v dnešním světě. Hlavním cílem scénářů je konfrontovat existující myšlenkové rámce a předpoklady o budoucnosti, aby je zpochybnil a odhalil klíčové trendy nebo signály, které by mohly mít budoucí význam. Autoři dále rozvíjí myšlenku a tvrdí, že scénáře také poskytují rámec, na kterém lze postavit strategie, plány a projekty a umožňují měřit dopady různých rozhodnutí. Maldonado a Vera (2014, str. 3) však upozorňují, že v literatuře existuje mnoho doporučení pro přípravu na krizi, přesto ne všechny organizace mají krizové plány pro přípravu na krizi nebo reakci na ně. Coombs a Laufer (2018, str. 199–203) posuzují problematiku krizových plánů z globálního hlediska a dle jejich názoru jsou krizové plány obecně flexibilní, s výjimkou situací, kdy existují standardní postupy pro specifický typ krize. Je možné zkoumat rozdíly v plánech krizového řízení mezi různými zeměmi, odchylky týmů krizového řízení od plánů a úroveň detailnosti plánů pro podobné krize. Koncept mocenské vzdálenosti může hrát důležitou roli při dodržování směrnic a postupů.

Vochozka a Váchal (2013, str. 540) definují krizový plán jako „*souhrn opatření a postupů k řešení vzniklé podnikové krizové situace*“. Dle autorů je krizový plán klíčovým nástrojem pro rychlé a efektivní řešení krizových situací. Plán by měl obsahovat relevantní kroky a postupy pro zvládnutí krize, avšak neměl by být příliš podrobný, aby umožnil flexibilitu a rychlost při reakci. Prevence a schopnost pracovat s riziky jsou klíčové pro úspěšné zvládnutí krizových situací, a v některých případech je možné je využít ve svůj prospěch. Antušák (2013, str. 44) souhlasí s Vochozkou a Váchalem (2013, str. 540) v tom, že cílem krizového plánování je vytvořit efektivní systém pro prevenci krizových situací. Autor dále dodává, že účelem plánování je také zvládnutí vybraných krizových situací prostřednictvím proaktivního přístupu zaměstnanců, spolupráce se státními orgány a vnitropodnikových sil a prostředků.

### **2.3.2 Tvorba krizových scénářů**

Deuschel (2021, str. 71–75) uvádí, že klíčové scénáře se odvozují od identifikovaných kritických rizik. Každý scénář vyžaduje účast odpovědných osob, které mají pravomoc rozhodovat v souvislosti s daným rizikem. Autor dále zmiňuje, že pro každý klíčový scénář je důležité stanovit strategický záměr. Tento záměr určuje cíle a směřuje veškeré následné činnosti v oblasti řízení krize. Strategický záměr by se měl měnit během krize jen minimálně. Je důležité mít jasný záměr pro každé riziko a nejprve ho pečlivě promyslet a schválit. Dare (2022, str. 8) doporučuje jako proaktivní krok zajištění stability podnikání ve formě sepsání seznamu možných krizových situací a následně vypracování systému reakce pro každý typ situace, aby bylo zřejmé, jak postupovat. Autorka dále uvádí, že s připraveným procesem se organizace vyvaruje překvapení a bude schopna účinně se vypořádat s jakýmkoli typem krize.

### **2.3.3 Plánování a struktura krizových plánů**

Dle Murray (2022, str. 15–16) je plán řízení krizí klíčovým nástrojem, který poskytuje strukturu a směr pro reakci na krizové situace. Měl by obsahovat klíčové kontakty, postupy a formuláře, které usnadňují organizaci správnou a koordinovanou odezvu na krizi. Je navržen tak, aby minimalizoval chaos, umožňoval rychlé rozhodování a chránil pověst organizace. Efektivní krizový plán představuje zásadní konkurenční výhodu a je nedílnou součástí celkového řízení rizik a kontinuity podnikání. Cane (2019, str. 35) souhlasí s Murray (2022, str. 15–16) s tím, že krizový plán by měl obsahovat seznam klíčových kontaktů, které rozděluje na kontakty týmu

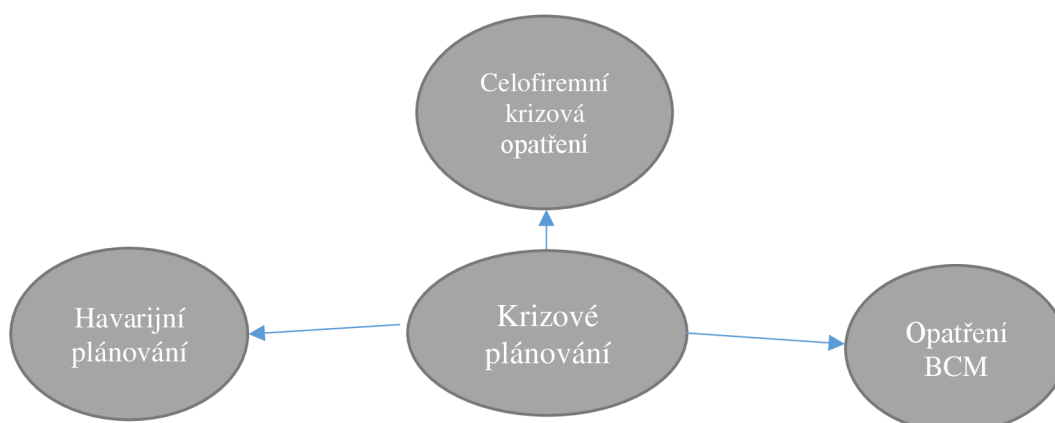
pro řízení krizí a seznam kontaktů zainteresovaných stran a dodává, že krizový plán dále obvykle obsahuje tyto základní prvky: matici hodnocení rizik, formulář pro hlášení incidentů, pracovní list se strategií, monitorování médií, vyhodnocení po krizi a opatření pro obnovu.

Maldonado a Vera (2014, str. 4) specifikují, že v kumulativních krizích mají vedoucí pracovníci více času k detekci krize před tím, než se stane veřejnou událostí. Organizace vyvíjejí plány a směrnice pro řešení situací, jako jsou bezpečnost pracoviště, korupce a pracovní spory, které jsou zakotveny v právním systému země. Hemus (2020, str. 99–101) upozorňuje na to, že krizový plán není přesným průvodcem pro každou situaci. I když je neocenitelným nástrojem, nemůže garantovat stoprocentní úspěch v řízení krize. Místo toho však poskytuje rámcové směrnice a oporu pro efektivní reakci na krizi. Autor dále podotýká, že je důležité si uvědomit, že každá krizová situace je jedinečná a vyžaduje individuální přístup a rozhodnutí. Dle Willieho (2023, str. 16–17) je vytvoření plánu krizového řízení důležitým krokem při přípravě a reakci na krizovou situaci. Plán krizového řízení by měl zahrnovat následující prvky:

1. Role a odpovědnost – Defínování rolí a odpovědností členů týmu krizového řízení a dalších zainteresovaných stran, jako jsou zaměstnanci, externí partneři a vládní agentury. Deuschel (2021, str. 80) tento bod také považuje za důležitý a doplňuje, že zajištění jasnosti ohledně rolí a odpovědností jednotlivých členů organizace je klíčovým prvním krokem pro úspěšné krizové řízení. Deuschel (2021, str. 80) dále uvádí, že nedostatek této jasnosti patří mezi nejčastější chyby v krizovém řízení.
2. Plán komunikace – Vytvoření plánu pro komunikaci se zúčastněnými stranami během krize, včetně využití sociálních médií, tiskových zpráv a jiných kanálů.
3. Postup reakce – Vymezení kroků, které budou přijaty k reakci na krizi, včetně nouzových postupů, evakuací a dalších opatření.
4. Plán obnovy – Identifikace kroků, které budou přijaty k obnovení po krizi a návratu k normálním provozům, včetně oprav, úklidu a dalších akcí.
5. Hodnocení rizik a jejich mitigace – Identifikace rizik spojených s krizí a vypracování strategií k jejich omezení.
6. Vyhodnocení a revize – Zavedení procesu pro vyhodnocování účinnosti plánu krizového řízení a provedení případných změn nebo aktualizací. Je důležité, aby organizace pravidelně přezkoumávaly a testovaly své plány krizového řízení, aby zajistily jejich účinnost, aktuálnost. Tímto způsobem se zaměstnanci také trénují a zdokonalují.

Dare (2022, str. 12) specifikuje klíčové prvky plánování obnovy po havárii, tzv. „disaster recovery plan“, tedy klíčovým nástrojem pro řízení rizik a ochranu organizace před ztrátou dat, finančními ztrátami a reputačními škodami v případě vzniku katastrofické události následovně: je zapotřebí mít dokumentovaný plán reakce, seznam veškerého vybavení (eventuelně lze pořídit fotografie a účtenky a doporučuje se zajistit si vhodné doporučení pro rychlou náhradu v případě škody), podrobný inventář majetku, zajištění integrity dat, kontrola backup systémů, informace o dodavatelích a poskytovatelích služeb, přístup k finančním prostředkům. Antušák (2013, str.44) souhlasí s Dare (2022, str.12) že plánování obnovy po havárii spadá do krizového plánování a dále definuje další pilíře krizových opatření v následujícím obrázku.

Obrázek 3 Systém firemního krizového plánování



Zdroj: Antušák (2013, str. 44)

Antušák (2013, str. 44) uvádí, že do pilíře celofiremních krizových opatření by měly být zahrnuty cíle krizového plánování, opatření plynoucí ze strategie řízení rizik a ze systému řízení rizik, opatření krizové komunikace a etiky řízení krizí a také metodické a organizační opatření, která zajišťují funkčnost systému krizového řízení. Opatření pro řízení kontinuity podnikání (BCM) zahrnují činnosti zaměřené na snížení dopadů krizových událostí na klíčové podnikové procesy. Tato opatření zahrnují plánování kontinuity podnikání, které se zaměřuje na návrh opatření a procedur umožňujících organizaci reagovat tak, aby klíčové části firmy mohly pokračovat v činnosti podle strategie kontinuity. Součástí BCM by podle autora mělo být také plánování obnovy po havárii, které zahrnuje předběžná opatření nezbytná pro minimalizaci ztrát a zajištění kontinuity klíčových částí organizací v případě havárie nebo katastrofy. Mimo jiné se do opatření BCM řadí plánování zdrojů pro obnovu podnikání. Autor dále specifikuje havarijní plánování, do kterého spadá spolupráce se složkami integrovaného záchranného systému (IZS), „opatření vyplývající ze zákona č. 59/2006 Sb., o prevenci závažných havárií“ a dále příspěvek do vnějšího havarijního plánu, pakliže je to vyžadováno zákonem.

## 2.4 Metodika práce

Tato diplomová práce je rozdělena na teoretickou a praktickou část a vznikla na základě analýzy primárních (v praktické části) a sekundárních (v teoretické části) zdrojů. Metodika je součástí teoretické části a je detailně popsána v této kapitole. Teoretická část je zpracována formou literární rešerše. Cílem teoretické části bylo získat teoretické poznatky a pochopit komplexní problematiku oblasti řízení rizik, krizového řízení a krizových scénářů a plánů. Literární rešerše se opírá o sekundární zdroje v podobě odborných knih, článků, časopisů a online databází. Jelikož k dané problematice nebylo k dispozici dostatečné množství odborné literatury v českém jazyce, byly tyto sekundární zdroje následně zpracovány primárně z anglického jazyka. Sekundární zdroje byly čerpány z online knihoven, jako je Amazon.com, Google scholar a Google books. Tyto zdroje obsahují mnoho odborných knih na téma řízení rizik a krizového řízení. Odborné články byly čerpány ze serverů ScienceDirect, Web of Science a dalších. Jako další sekundární zdroje byly využity relevantní monografie českých autorů. Ty byly získány buďto fyzicky v Městské knihovně v Praze, nebo prostřednictvím online databáze bookport.cz. Díky kombinaci těchto zdrojů bylo možné získat všechny potřebné poznatky týkající se teorie řízení rizik, krizového řízení a krizových scénářů a plánů. Je důležité

podotknout, že vzhledem k tomu, že většina sekundárních zdrojů byla zpracována z anglického jazyka, může mít překlad vliv na interpretaci informací. Nicméně byl v rámci příprav diplomové práce kladen velký důraz na to, aby byla terminologie správně uchopena a byly zachovány pojmy, které se běžně používají v českém jazyce.

V první kapitole řízení rizik byly popsány definice rizika a řízení rizik, byly vymezeny základní pojmy, přístupy k řízení rizik (Enterprise Risk Management a Business Continuity Management) a v neposlední řadě byl detailně zkoumán proces řízení rizik, konkrétně identifikace rizik, hodnocení rizik, metody analýzy rizik, opatření rizik a plánování a monitorování rizik. Ve druhé kapitole je podrobně zkoumána problematika krizového řízení. Jednotlivé podkapitoly se věnují obecným definicím krize a jejím typům, fázím krizového řízení, strategii v oblasti krizového řízení. Pozornost je také věnována neméně důležité oblasti krizové komunikace a roli centrální banky v krizovém řízení ve finančním sektoru. Poslední část teoretické části se zabývá krizovými scénáři a plány. V této podkapitole jsou vymezeny definice a význam krizových scénářů a plánů, prostor je věnován také tvorbě krizových scénářů a plánování a strukturu krizových plánů. Napříč teoretickou částí jsou komparovány názory různých autorů a odborných článků. Záměr byl získat na danou problematiku co nejkomplexnější pohled. Získané poznatky jsou dále aplikovány v praktické části.

Hlavním cílem diplomové práce je identifikování kritických rizik ve vybrané společnosti a posouzení jejího stavu připravenosti na tato rizika. S ohledem na citlivost uvedených informací bude v rámci této diplomové práce vybraná organizace anonymizována, dále bude použit obecný název „Banka X“. Pomocí naplnění dílčích cílů směřuje práce k naplnění hlavního cíle. Dílčí cíle na sebe logicky navazují a tvoří postupný proces, jehož výsledkem je dosažení hlavního cíle práce.

Dílčí cíle:

1. Shromáždění teoretických poznatků v oblasti řízení rizik a krizového řízení, díky čemuž vznikne základ pro další analýzu.
2. Správná volba vlastního výzkumu a efektivní využití primárních zdrojů pro získání potřebných dat.
3. Analýza výsledků výzkumu, na jejíž základě budou formulována doporučení.

Praktická část logicky navazuje na část teoretickou. První kapitola je věnována představení vybrané organizace, její historii, strategii, nabídce produktů a současného stavu. Pozornost je také věnována přístupu k internímu řízení rizik a organizační strukturu. Data v této kapitole byla získána z veřejně dostupných zdrojů, konkrétně z výroční zprávy banky a z relevantních internetových zdrojů. Za účelem dosažení hlavního cíle diplomové práce byly ve druhé kapitole praktické části identifikovány faktory hrozeb a příležitostí, které z vnějšího prostředí ovlivňují činnost „Banky X“. Tyto faktory byly identifikovány na základě kvalitativního výzkumu v rámci polostrukturovaného rozhovoru s ředitelem řízení rizik a vedoucím operačních rizik „Banky X“.

Cílem rozhovoru bylo získat důležité poznatky pro vypracování identifikace rizik. Dle Fotra a Součka (2019, str. 103) je při přípravě polostrukturovaných rozhovorů důležité dodržet výběr účastníků, náplň a způsob vedení rozhovorů, ale také zpracování informací, aby byla zajištěna úspěšnost rozhovorů. Jak již bylo zmíněno, na polostrukturovaný rozhovor byl osloven ředitel divize řízení rizik a vedoucí oddělení řízení operačních rizik. Tito manažeři byli ujištěni, že vzhledem k citlivosti dat bude rozhovor i následné zpracování dat anonymizováno. V rámci přípravy byl vytvořen seznam otevřených otázek, které byly logicky rozčleněny dle klíčových oblastí – analýza vnějších vlivů, identifikace jednotlivých příležitostí a hrozeb. Manažeři souhlasili s nahráním rozhovorů, které byly následně přepsány do finální formy.



Pro identifikaci rizik byla použita STEP analýza, která se soustředila na sociální, ekonomický a technicko-technologické faktory. Analýza se opírala jak o expertní názory zaměstnanců banky, tak byly také analyzovány relevantní statistické údaje Českého statistického úřadu, České národní banky, Ministerstva financí ČR. Dále byly využity veřejně dostupné informace z výroční zprávy banky. Na základě STEP analýzy bylo identifikováno 28 hrozeb a z toho plynoucích rizik pro „Banku X“.

Dalším dílčím cílem práce bylo hodnocení rizik. Pro získání těchto vstupů byla zvolena metoda brainstormingu. Toho se zúčastnili manažeři banky, konkrétně ředitel řízení rizik, manažer operačních rizik a manažer tržních rizik. Ti byli seznámeni s klasifikační stupnicí a stupnicí pro hodnocení rizik, aby následně jednotlivá identifikovaná rizika ohodnotili. Samotný proces trval přibližně hodinu, kdy se podařilo ohodnotit všechna rizika, která byla v rámci polostrukturovaného rozhovoru identifikována. Na základě ohodnocených rizik byla vypracována opatření pro jejich minimalizaci.

Vyhodnocená rizika byla zanesena do matice rizik, ze které lze identifikovat rizika s nejvyšší mírou rizika. Pro nejkritičtější rizika byla vypracována opatření vedoucí ke snížení rizik. Pomocí metody What-if jsou následně vytvořeny další scénáře, které by mohly nastat v oblasti kybernetických incidentů, tedy nejvýše ohodnoceného rizika.

Další kapitola je věnována tvorbě krizových scénářů a plánů. Krizové scénáře jsou vypracovány na základě vybraného rizika s nejvyšší mírou dopadu a pravděpodobnosti. Navazuje vyhotovení krizového plánu, který poskytuje postupné instrukce a doporučené kroky k řešení krizové situace. Následují závěrečná doporučení a zhodnocení stavu připravenosti organizace.



### 3 Praktická část

V praktické části diplomové práce jsou využity poznatky z teoretické části. V první části bude představena organizace „Banka X“. Bude popsána oblast její činnosti, organizační struktura a specifika prostředí, ve kterém působí. Následně budou identifikovány příležitosti a hrozby pomocí STEP analýzy, bude zhodnocena pravděpodobnost výskytu jednotlivých rizik a jejich potenciální dopad na činnost organizace. Dále bude proveden rozbor příčin a faktorů, které tato rizika generují a budou navrženy opatření na jejich minimalizaci. Následně budou vypracovány krizové scénáře a krizové plány na rizika, která budou vyhodnocena jako nejkritičtější. Cílem je připravit se na možné krizové situace a navrhnout preventivní opatření a plány pro jejich řešení.

#### 3.1 Představení společnosti

V této kapitole bude představena vybraná organizace „Banka X“. Právní forma organizace je akciová společnost. Dle Janouše (2014) byla tato organizace založena v roce 2011 skupinou „Y“ jako reakce na potřeby moderního bankovníctví v České republice. Jejím zakladatelem a prvním ředitelem byl člověk, který předtím úspěšně řídil českou pobočku jedné z předních finančních institucí. „Banka X“ se rozhodla přinést inovativní přístup k bankovníctví a poskytovat klientům jednoduché a efektivní bankovní služby.

Autor dále uvádí, že v přípravné fázi před zahájením činnosti „Banky X“ byly provedeny důkladné analýzy trhu s cílem identifikovat klíčové segmenty a potřeby zákazníků. „Banka X“ se zaměřila především na střední masovou část populace, která byla identifikována jako skupina s vysokým potenciálem a ochotou ke změnám. Rozhodla se nabízet moderní bankovní produkty a služby, které byly přizpůsobeny potřebám této specifické cílové skupiny.

Autor dále podotýká, že díky svému inovativnímu přístupu a využívání moderních technologií se „Banka X“ rychle etablovala na trhu a získala si pozornost a důvěru zákazníků. Jednou z klíčových priorit banky bylo poskytovat jednoduché a přehledné rozhraní pro své klienty, které umožňuje snadné a rychlé provádění bankovních transakcí. „Banka X“ se také zaměřila na poskytování kvalitního zákaznického servisu a aktivní komunikaci s klienty.

Výše zmíněný autor dodává, že v rámci svého rozvoje a růstu si „Banka X“ uvědomila potenciál expanze na zahraniční trhy. Vzhledem k úspěchu a uznání na domácím trhu se rozhodla pro vstup na trhy Číny a Indonésie. Tato strategie byla podpořena přítomností mateřské „Skupiny Y“ na těchto trzích, což představovalo výhodu při budování nových vztahů a navazování partnerství.

Banky.cz (2023) níže popisuje nabídku finančních služeb „Banky X“:

- účet (běžný, dětský, účet pro mladé, spořicí účet),
- půjčka (spotřební úvěr, konsolidace a refinancování, kontokorent, rozložení platby v souvislosti s nákupy),
- hypotéka (nová i převedení hypotéky),
- investice a spoření,
- pojištění (cestovní, osobní, pojištění schopnosti splácet půjčku, pojištění schopnosti splácet hypotéku).

Dle výše uvedeného zdroje jsou výhody banky přehlednost v nabídce a služeb, absence poplatků při online manipulaci s penězi nebo výběru z domácího bankomatu, propracovaná

mobilní aplikace a internetové bankovníctví, dostupnost většiny produktů online včetně převedení hypotéky, flexibilní úvěry.

Jako nevýhody uvádí stejný zdroj Banky.cz (2023) omezenou nabídku pro náročnější klienty, banka se zaměřuje pouze na základní bankovní produkty. Další nevýhody jsou očekávání internetové a počítačové zdatnosti u klientů, nižší úroky na spoření než u konkurence a vyšší poplatky za výběr z cizích bankomatů.

Na základě informací na webu „Banky X“ (2023) zatím není v nabídce možnost založení účtu pro právnickou osobu, kreditní karta, dobití kreditu, proplácení šeků, platební terminály, hotovostní přepážky a kryptoměnové účty.

### **3.1.1 Současný stav**

Výroční zpráva „Banky X“ (2020) poukazuje na fakt, že i přes silnou orientaci na digitalizaci služeb si banka vybuďovala strategickou síť poboček, která se dostala na současné číslo 34. Dle tiskové zprávy banky (2023, str. 4) je současný počet klientů 1 100 000. Banka poskytuje 370 moderních bankomatů, které umožňují i bezkontaktní výběry. Podle průzkumů zůstávali klienti banky i na konci roku 2020 mezi nejspokojenějšími klienty bank v Česku. Celkový objem úvěrů v portfoliu banky se v roce 2020 zvýšil o 3,3 miliardy korun na 58,6 miliardy korun. K růstu přispěl zejména pokračující zájem klientů o spotřebitelské úvěry, hypotéky a kontokorent. V roce 2020 dosáhla banka kladného výsledku hospodaření s čistým ziskem 1,4 miliardy korun. Zisk byl o 12 % nižší než v předchozím roce, což bylo způsobeno zhoršenou ekonomickou situací v ČR kvůli boji proti epidemii koronaviru. Banka disponovala na konci roku 2020 vlastním kapitálem ve výši 11,1 miliardy korun a základním kapitálem ve výši 500 milionů korun. Celkový kapitálový poměr banky byl 15,8 %. K 31. prosinci 2020 dosáhla bilanční suma výše 136,7 miliardy korun. Nejvýznamnějším závazkem banky byly k 31. prosinci 2020 vklady na běžných a spořicích účtech klientů v celkové výši 123,6 miliardy korun. V roce 2020 došlo ke zvýšení kapitálu, s Tier 1 (T1) kapitálem narůstajícím z 8,318 miliardy korun na 9,186 miliardy korun a Tier 2 (T2) kapitálem narůstajícím z 200 milionů korun na 254,1 milionů korun. Celkové kapitálové požadavky vzrostly meziročně z 4,426 miliardy korun na 4,787 miliardy korun.

### **3.1.2 Rizika a řízení rizik a organizační struktura**

Dle výroční zprávy (2020) „Banka X“ přistupuje k řízení rizik pomocí základních principů a východisek. Mezi ty patří:

1. Komplexní pokrytí rizik – „Banka X“ se zaměřuje na identifikaci, hodnocení a řízení tržních rizik, likviditních rizik, kreditních rizik, rizik koncentrace a operačních rizik. Cílem je minimalizovat negativní dopady těchto rizik na banku.
2. Dodržování legislativních pravidel – „Banka X“ striktně dodržuje předpisy a legislativu, které upravují bezpečné podnikání v bankovním sektoru. Zvláštní důraz je kladen na kapitálovou přiměřenost, což zajišťuje dostatečný kapitál pro pokrytí rizik.
3. Ochrana klientů – „Banka X“ se zavazuje chránit své klienty i v nepříznivém finančním prostředí. To znamená mít opatření, která minimalizují riziko ztráty klientů a zabezpečují jejich finanční prostředky.
4. Nezávislost řídicích útvarů – Útvary odpovědné za řízení rizik v bance jsou nezávislé na obchodních útvarech. Tím se zajišťuje objektivita a integrita procesu řízení rizik a minimalizují se konflikty zájmů.

5. Reporting rizik – „Banka X“ pravidelně a dle potřeby poskytuje vedení banky reporty o rizicích. Tyto poskytují informace o aktuálním stavu rizik, jejich hodnocení a případných opatření k jejich ovládnutí.
6. Použití vhodných metod – „Banka X“ využívá metody odpovídající složitosti bankovních produktů a investičních nástrojů, které banka nabízí. Tyto metody slouží k poskytování přesných a relevantních informací pro řízení rizik.

Cílem těchto východisek je zajistit, že „Banka X“ má efektivní systém řízení rizik, který jí umožňuje identifikovat, hodnotit a řídit rizika, se kterými se v jejím podnikání setkává. Tím se chrání banka, její klienti a dodržují se požadavky regulačního prostředí.

Následující obrázek zobrazuje organizační strukturu „Banky X“, aby bylo patrné, jaké zastoupení má řízení rizik v rámci organizace.

Obrázek 4 Organizační struktura „Banky X“



Zdroj: Výroční zpráva „Banky X“, vlastní zpracování

Pro účely této diplomové práce bude níže popsáno oddělení řízení rizik a provozu. Z organizační struktury je patrné, že řízení rizik je věnována dostatečná pozornost. Dle rozhovoru s ředitelem divize řízení rizik, viz příloha č. 2, jsou aktivity jednotlivých oddělení dále objasněny. V rámci řízení a provozu je zahrnuto vyšší vedení, která má na starosti strategické rozhodování, formulaci směrnic a plánování bankovních operací. Řízení retailových rizik se specializuje na řízení a řešení rizik spojených s retailovými produkty a službami banky. Řízení rizik – nové produkty a komerční se zaměřuje na řízení rizik spojenými s novými produkty a komerčními aktivitami banky. Řízení operačních rizik se specializuje na identifikaci, hodnocení a řízení operačních rizik v bance. Řízení tržních rizik a stres testů se zaměřuje na monitorování a řízení tržních rizik, jako je riziko spojené s fluktuacemi cen finančních instrumentů, úrokovými sazbami a devizovými kurzy. Provádí stres testy, které hodnotí schopnost banky odolávat

extrémním ekonomickým podmínkám. Mezi pravomoci tohoto týmu patří také identifikace a analýza možných krizových scénářů, které by mohly ovlivnit činnost společnosti. Podpora klientských procesů se zabývá zlepšením kvality služeb, optimalizací procesů souvisejících s poskytováním služeb klientů. Manuální schvalování zajišťuje proces manuálního schvalování specifických transakcí nebo žádostí, které vyžadují dostatečnou kontrolu a schválení ze strany vyššího managementu nebo specializovaného týmu. Treasury back office se zaměřuje na operace týkající se treasury managementu, což zahrnuje řízení finančních toků, likvidity a investic banky. Dále se zabývá správou transakcí vyrovnáváním plateb, řízením pozic a komunikací s externími finančními institucemi. Provoz se stará o každodenní operace banky, jako je zpracování transakcí, správa účtů, vedení platebního styku a další provozní činnosti.

### 3.2 Identifikování a rozbor rizik společnosti

Tato kapitola se bude věnovat identifikování a rozboru rizik organizace. V první části budou na základě provedeného výzkumu zpracovány faktory vnějších vlivů prostřednictvím STEP analýzy. Oblasti, které přímo ovlivňují činnost banky, jsou sociální, ekonomická a technicko-technologická. Na základě polostrukturovaného rozhovoru s ředitelem řízení rizik a manažerem operačních rizik „Banky X“ byly identifikovány příležitosti a hrozby. Jak podotýká Oškrdal a Doucek (2014, str. 195), často se opomíjí fakt, že rizika mohou mít i pozitivní efekt, a proto budou identifikovány jak příležitosti, tak i hrozby. Dle autorů by se k oběma rizikům mělo přistupovat stejně. Je to však vesměs novodobá záležitost. V praxi se tedy často riziko rovná hrozbě, tedy je vnímáno negativně. Identifikované příležitosti a hrozby budou dále komparovány se statistickými údaji. Hrozby budou v další části kapitoly posouzeny pomocí kvantitativní analýzy rizik a na základě nejvyšší míry rizik budou vybrána ta rizika, která mohou nejvíce ovlivnit činnost organizace a její strategické cíle. Pro přehlednost jsou veškeré identifikované příležitosti a hrozby shrnuty do tabulky v příloze č. 3.

Vzhledem k probíhající válce na Ukrajině a faktu, že tato situace má významný ekonomický i geopolitický dopad na celý svět a zasahuje do všech oblastí v rámci STEP analýzy, bude toto téma rozebráno samostatně v následujícím textu.

#### **Válka na Ukrajině**

Dle Spišáka (2022) je válka na Ukrajině považována za největší mezinárodní ozbrojený konflikt v Evropě od druhé světové války. Konflikt, který vyvolala rusko-ukrajinská krize, vyvrcholil v roce 2014 anexí Krymu. Lze jej považovat za vrchol rusko-ukrajinské krize. Zahrnuje nejen Rusko a Ukrajinu, ale i řadu dalších států a organizací a je bedlivě sledován a analyzován celým světem. Dle ECB.europa.eu (2023) válka Ruska proti Ukrajině má negativní dopad na důvěru, zvyšovala ceny energií a potravin, a společně s hospodářskými potížemi v Číně kvůli pandemii zhoršovala stávající tlaky v dodavatelském řetězci. Tyto faktory představují značný negativní vliv na hospodářské oživení eurozóny. S tím souhlasí také ředitel řízení rizik a dodává viz příloha č. 2, že „Zdražení energií zvýšilo rapidně náklady na provoz IT systémů a pobočkové sítě, vysoká inflace tlačí na navýšení cen všech komodit a služeb. Zaměstnanci požadují vyšší platy a zvyšují tím náklady.“

#### **Růst inflace v eurozóně**

Dle ECB.europa.eu (2023) po výrazném nárůstu inflace na začátku roku 2022 se očekává vyšší a trvalejší inflace. Celková inflace měřená HICP (Harmonizovaný index spotřebitelských cen) by měla v průměru dosáhnout 6,8 % v roce 2022 a postupně se snížit k inflačnímu cíli ECB

ve druhé polovině roku 2024. Cenové tlaky zůstanou vysoké kvůli vyšším cenám ropy a plynu a růstu cen potravin, ovlivněným válkou na Ukrajině, a dopady znovuotevření ekonomiky a mezer v globálních dodávkách. Očekávaný pokles inflace pro eurozónu na 3,5 % v roce 2023 a 2,1 % v roce 2024 odráží předpokládané zmírnění cen energetických a potravinářských komodit. Inflace bez energií a potravin zůstane do konce roku 2022 velmi zvýšená, ale poté by měla klesat. Ve srovnání s projekcemi z března 2022 byla inflace revidována směrem vzhůru, což odráží nedávné údaje, vyšší ceny energií a potravin, trvalejší proinflační tlaky kvůli narušení dodávek, růst mezd a oslabení eura.

### **Kybernetické útoky**

Salomon (2022, str. 3) upozorňuje na nutnost zaměřit se na digitální provozní odolnost a dodává, že kybernetičtí podvodníci využívají kritické mezinárodní situace, jako je válka na Ukrajině, k cílení na klienty českých bank, zejména na rusky a ukrajinsky hovořící občany. Hackeři využívají nepozornosti a strachu klientů o budoucnost a pod záminkou, že jsou jejich peníze v ohrožení, je nutí sdělit citlivé údaje, které následně zneužijí pro získání jejich úspor. Dle výroční zprávy ČNB (2022, str. 63) je zvýšení kybernetické odolnosti finančního sektoru klíčové pro hladký chod finančního trhu. ČNB proto prioritizuje schopnost úvěrových institucí řídit kybernetická rizika, včetně přípravy na kybernetické útoky a selhání klíčových IT dodavatelů.

### **Geopolitická krize a náhlý pád Sberbank CZ**

Dle Strašáka (2022) byla Sberbank CZ solidní bankou, ale vzhledem k faktu, že byla ruského původu, se stala cílem nespokojených klientů v reakci na invazi Ruska do Ukrajiny. Klienti začali masově rušit své účty a vybírat peníze, což vedlo k uzavření poboček, zastavení internetového bankovníctví a omezení transakcí platebními kartami. To vnímá i ředitel divize řízení rizik, který dodává, viz příloha č. 2, že „*pád Sberbank CZ navýšil počet klientů*“. ČNB (2022) dodává, že vzhledem ke zhoršení likviditní situace v souvislosti s významným odlivem vkladů odebrala ČNB Sberbank CZ bankovní licenci, což znamená, že Sberbank CZ již nesmí vykonávat bankovní činnosti, jako je přijímání vkladů a poskytování úvěrů. V současné době je Sberbank CZ v likvidaci a pražský městský soud vyhlásil konkurz. Majetek banky bude zlikvidován a výtěžek bude rozdělen mezi věřitele.

#### **Příležitosti**

I z této situace mohou vyvstat příležitosti. V období geopolitického napětí a nestability je ještě důležitější poskytování digitálních bankovních služeb, a to z důvodu bezpečnosti, přístupnosti, pružnosti a rychlosti komunikace. Digitální služby jsou také schopny zachovat kontinuitu obchodních operací. S výše zmíněným souhlasí i ředitel řízení rizik „Banky X“, který digitalizaci označil jako klíčový trend, viz příloha č. 2. Jako další příležitost se jeví možnost získání nových klientů z banky Sberbank CZ, která již v České republice nesmí provozovat bankovní činnosti.

#### **Hrozby**

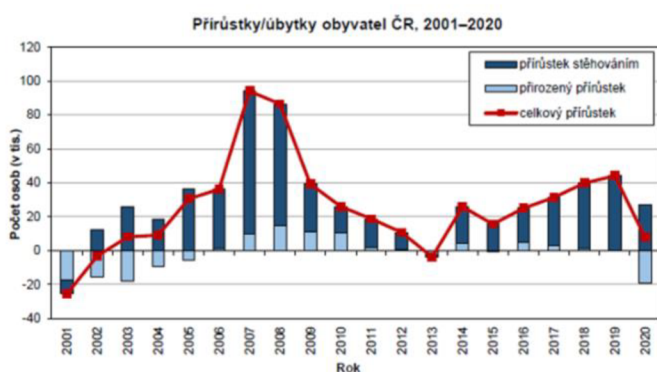
Co se týče hrozeb, tak jak již bylo zmíněno výše, „Banka X“ může být vystavena většímu riziku kybernetických útoků, což může vést k finančním ztrátám, narušení reputace či právním důsledkům. V rámci geopolitického napětí může dojít ke zvýšení regulatorních požadavků, což by mohlo omezit schopnost „Banky X“ poskytovat úvěry a jiné finanční služby.

## Sociální faktory

V návaznosti na rozhovory se ředitelem řízení rizik „Banky X“, dle přílohy č. 2 vyplynulo, že v rámci sociálních faktorů je pro „Banku X“ klíčové sledovat změny ve spotřebitelském chování a preferencích a také změny v demografickém vývoji, které mohou mít dopad na cílové trhy a produkty, jako například růst populace či migrační změny. Na základě tohoto faktu jsou tyto vlivy detailně vypracovány.

Dle dat ČSÚ (2023) od počátku 21. století až do konce druhé dekády došlo v České republice k pravidelnému ročnímu nárůstu populace, s výjimkou roku 2013, kdy došlo ke zmenšení o 3,7 tisíce obyvatel. Za posledních deset let (2011–2020) počet obyvatel vzrostl o 215 tisíce obyvatel (2 %). K růstu populace přispělo migrační saldo (221,7 tisíce), zatímco přirozený růst byl záporný (-6,6 tisíce). Epidemie covid-19 ovlivnila saldo zahraniční migrace (-39 %). Celkový přírůstek obyvatel v roce 2020 byl 7,8 tisíce, nejmenší v poslední dekádě (kromě roku 2013). Trend je zobrazen níže v grafické podobě.

Graf 1 Přírůstky/úbytky obyvatel ČR, 2001–2020



Zdroj: ČSÚ (2023)

Z dat ČSÚ (2023) týkajících se přírůstku a úbytku obyvatel dále vyplývá, že v roce 2020 se populace České republiky ve třech hlavních věkových skupinách vyvíjela podobně jako v předchozích letech. Dětská populace (0–14 let) rostla od roku 2008, v roce 2020 dosáhla 1,72 milionu osob, což představuje 16,1 % všech obyvatel. Skupina seniorů nad 65 let také zaznamenala vzestup s 2,16 milionu osob, což bylo poprvé v historii přes 20 % populace. Počet obyvatel v produktivním věku (15–64 let) se však snížil o 28,4 tisíce na 6,82 milionu osob, tvořících 63,8 % populace. Tento trend vedl k postupnému stárnutí populace.

Průměrný věk obyvatel ČR vzrostl na posledních deset let o necelé dva roky na 42,6 let. Věkový medián stoupl z 39,8 let na 43,3 let, což znamená, že polovina populace byla starší než 43,3 let. Index ekonomické závislosti, který udává počet neproduktivních osob na 100 ekonomicky produktivních, se postupně zvyšoval z 55 na 69.

## Příležitosti

S nárůstem digitálních technologií a pohodlným přístupem k internetu roste i očekávání klientů ohledně snadného a rychlého přístupu k finančním službám. Tuto příležitost identifikoval také ředitel divize řízení rizik „Banky X“, viz příloha č. 2. Banky mohou využít tuto příležitost a investovat do modernizace svých online a mobilních aplikací. Toto téma bude detailněji zpracováno v následující kapitole. Další příležitost byla identifikována v podobě potřeby finančního poradenství pro seniory. S rostoucím počtem seniorů v populaci se zvyšuje potřeba specializovaného finančního poradenství pro tuto skupinu klientů. Banky mohou vytvářet produkty a služby, které lépe odpovídají potřebám seniorů a pomáhají jim lépe spravovat jejich finanční situaci. Následující příležitost se týká rozvoje inovativních finančních produktů. S rostoucí digitalizací a technologickým pokrokem se otevírají nové možnosti pro vytváření inovativních finančních produktů, které mohou bankám pomoci oslovit nové trhy a získat nové zákazníky. V rámci změn v životních stylech a spotřebních preferencích mohou s proměnou společnosti vzniknout nové segmenty klientů s odlišnými finančními potřebami. Banky mohou využít tuto příležitost a vytvářet produkty a služby, které lépe vyhovují těmto novým potřebám.

## Hrozby

V oblasti stárnutí populace může růst počtu osob ve věkové skupině nad 65 let a snižující se podíl obyvatel v produktivním věku vést ke zvýšení poptávky po finančních produktech spojených s důchodovým zabezpečením, zároveň může snížit poptávku po produktech, jako jsou hypotéka nebo spotřebitelské úvěry. Další hrozba byla identifikována v rámci nízké natality. Pokles počtu dětí a mladých lidí může ovlivnit poptávku po dětských spořicíh účtech a dalších produktech pro mladé klienty. „Banka X“ by na základě tohoto zjištění mohla zahrnout do nabídky svých produktů také stavební spoření či kreditní karty, které momentálně nenabízí. „Banka X“ by tak mohla zacílit na tento segment a získat potenciální nové zákazníky. V rámci ekonomické nestability, která byla jako hrozba identifikována také v rozhovoru s ředitelem divize řízení rizik viz příloha č. 2, může fluktuace v ekonomice ovlivnit finanční situaci obyvatelstva, což může mít dopad na poptávku po úvěrech, spořicíh produktech a dalších finančních službách.

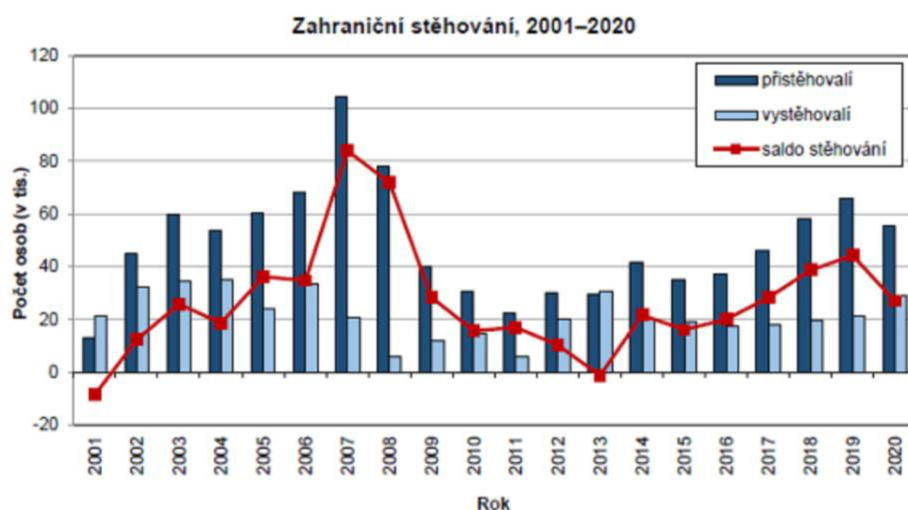
Výše uvedené hrozby a příležitosti v sociálním faktoru mohou mít vliv na strategii banky, portfolio finančních produktů, cílení trhů a způsob komunikace s klienty. Pro banku je důležité sledovat sociální vývoj a změny ve spotřebitelském chování, aby byla schopna efektivně reagovat na měnící se potřeby svých zákazníků a udržet si konkurenční výhodu na trhu.

## Zahraniční migrace

Z dat ČSÚ vyplývá, že zahraniční migrace převažuje zejména u osob v produktivním věku (20–34 let). Banka by měla být schopna poskytovat efektivní a snadné možnosti pro mezinárodní platby a transakce, aby uspokojila potřeby této rostoucí skupiny klientů. V následujícím grafu lze vyčíst trend zahraničního stěhování v letech 2001–2020.



Graf 2 Zahraniční stěhování, 2001–2020



Zdroj: ČSÚ (2023)

Dle informací z ČSÚ lze vyčíst, že zahraniční migrace pravidelně přispívá k růstu populace České republiky. V roce 2020 se do ČR přistěhovalo celkem 55,7 tisíce osob, což představuje potenciální zvýšení počtu klientů banky, což je to identifikováno jako příležitost. Tento růst populace může vést ke zvýšené poptávce po bankovních službách a produktech, jako jsou běžné účty, půjčky či spořicí účty.

Tabulka č. 4 Nejčtenější státní občanství migrantů v saldu zahraniční migrace, 2001–2020

Tab.: Nejčtenější státní občanství migrantů v saldu zahraniční migrace, 2001–2020

Rok	1.	2.	3.	4.	5.
2001	Vietnam 1 404	Česko 692	Rumunsko 119	Kazachstán 20	Írák 16
2002	Ukrajina 4 962	Vietnam 4 409	Polsko 541	Rusko 520	Moldavsko 420
2003	Ukrajina 10 062	Slovensko 5 573	Vietnam 2 649	Česko 1 554	Rusko 834
2004	Ukrajina 11 357	Vietnam 3 687	Česko 1 615	Rusko 1 316	Polsko 747
2005	Ukrajina 12 483	Slovensko 8 161	Vietnam 3 489	Rusko 1 994	Německo 1 332
2006	Ukrajina 12 993	Slovensko 6 152	Vietnam 4 083	Rusko 2 214	Moldavsko 1 143
2007	Ukrajina 30 902	Slovensko 13 129	Vietnam 11 281	Rusko 5 765	Mongolsko 2 879
2008	Ukrajina 18 575	Vietnam 13 299	Slovensko 7 007	Rusko 5 728	Mongolsko 3 497
2009	Ukrajina 8 051	Rusko 4 106	USA 2 454	Vietnam 2 269	Slovensko 1 442
2010	Rusko 3 670	Ukrajina 3 432	USA 1 673	Vietnam 1 386	Kazachstán 712
2011	Slovensko 3 389	Rusko 2 123	Ukrajina 1 889	USA 1 311	Německo 972
2012	Slovensko 3 959	Rusko 1 566	Německo 1 050	USA 765	Bulharsko 703
2013	Slovensko 4 841	Německo 1 299	Bulharsko 872	Rumunsko 865	Maďarsko 337
2014	Slovensko 5 574	Ukrajina 3 957	Rusko 3 105	Německo 1 396	Rumunsko 1 091
2015	Slovensko 5 202	Ukrajina 2 246	Rumunsko 1 238	Bulharsko 921	Německo 845
2016	Slovensko 5 292	Ukrajina 3 335	Rumunsko 1 527	Bulharsko 1 211	Maďarsko 875
2017	Ukrajina 7 690	Slovensko 4 356	Rumunsko 1 602	Bulharsko 1 437	Rusko 1 346
2018	Ukrajina 13 204	Slovensko 5 246	Rumunsko 2 018	Bulharsko 1 869	Rusko 1 683
2019	Ukrajina 18 241	Slovensko 4 602	Rusko 2 727	Rumunsko 2 024	Bulharsko 1 553
2020	Ukrajina 15 959	Slovensko 3 009	Rusko 2 171	Rumunsko 1 341	Maďarsko 1 110

Zdroj: ČSÚ (2023)

Z údajů zpracovaných ČSÚ lze vypořadovat, že dominující státní občanství migrantů zahrnuje občany Ukrajiny, Slovenska, Ruska a Rumunska. Tato různorodost kultur a jazyků vyžaduje,



aby banka byla schopna komunikovat a poskytovat služby v různých jazycích a přizpůsobit se specifickým potřebám a preferencím různých skupin migrantů. Doplnující tabulka zobrazuje počet cizinců v ČR v následujících letech 2020–2023.

Tabulka 4 Počet cizinců v ČR – předběžné čtvrtletní údaje 2020–2023

Datum Date	Celkem Total	Muži Males	Ženy Females	Trvalý pobyt Permanent stay	Ostatní typy pobytu Other types of stay	Ukrajina Ukraine	Slovensko Slovakia	Vietnam Viet Nam	Rusko Russian Federation	Rumunsko Romania	Polsko Poland	Bulharsko Bulgaria	Německo Germany	Ostatní Other
31.03.2023	1 010 692	514 766	495 926	339 392	672 300	527 268	117 492	66 751	42 985	20 010	17 823	17 756	13 724	186 883
31.12.2022	1 116 154	545 001	570 553	334 154	782 000	636 282	117 265	66 340	43 498	19 724	17 884	17 673	14 032	183 456
30.09.2022	1 091 098	534 368	556 732	331 350	759 748	615 616	116 716	65 938	44 059	19 512	17 934	17 601	14 183	179 539
30.06.2022	1 053 568	518 576	534 992	328 332	725 236	579 843	116 173	65 527	45 513	19 268	17 952	17 559	14 453	177 280
31.03.2022	922 516	463 251	459 265	325 148	597 368	452 657	115 327	65 130	46 098	18 978	17 926	17 404	14 586	174 410
31.12.2021	660 849	373 463	287 386	321 892	338 957	196 875	114 630	64 851	45 365	18 806	17 936	17 295	14 792	170 299
30.09.2021	647 650	365 658	281 992	319 090	328 560	189 912	113 760	64 576	45 176	18 541	17 861	17 129	14 997	165 698
30.06.2021	668 238	381 287	286 951	315 137	353 101	183 250	126 720	64 261	45 488	19 086	20 805	18 245	20 799	169 584
31.03.2021	656 301	374 047	282 254	311 967	344 334	176 204	125 527	63 921	44 332	18 707	20 758	18 060	20 769	168 023
31.12.2020	634 790	362 336	272 454	309 608	325 182	165 654	124 544	62 884	41 907	18 396	20 733	17 917	20 861	161 894
30.09.2020	616 659	352 516	264 143	306 853	309 806	158 300	123 266	62 523	37 827	17 979	20 588	17 733	21 004	157 439
30.06.2020	618 131	352 724	265 407	304 543	313 588	157 289	120 558	62 525	40 875	17 313	20 846	17 346	20 673	160 706
31.03.2020	604 076	345 683	258 393	302 885	301 191	151 481	121 036	62 290	39 363	17 188	21 209	17 383	20 747	153 399

Zdroj: Ředitelství služeb cizinecké policie, ČSÚ (2023)

Z údajů je patrný významný nárůst migrace občanů Ukrajiny v souvislosti s válkou v jejich zemi. Lze pozorovat rostoucí trend, kdy k 31. 12. 2020 bylo zaznamenáno 165 554 občanů Ukrajiny, kdežto k 31. 3. 2023 to bylo již 527 268 Ukrajinců. Další zastoupení cizinců v ČR dle tabulky jsou občané Slovenska. K 31. 3. 2023 bylo zaznamenáno 117 492 občanů SR. Tento trend potvrzuje i ředitel divize řízení rizik, viz příloha č. 2, který hovoří o tom, že vysoká imigrace zvýšila počet nových klientů.

#### Příležitosti

Rozvoj nových služeb v rámci zvýšené migrace podnikatelů a pracovníků z jiných zemí může vytvářet příležitosti pro banku rozvíjet nové bankovní produkty a služby, které uspokojí potřeby cizinců v České republice. To může zahrnovat speciální účty pro cizince, mezinárodní platby, multi-měnové účty nebo služby pro zprostředkování práce. Další identifikovaná příležitost je finanční poradenství pro cizince, kdy cizinci, kteří se přistěhují do České republiky, mohou potřebovat poradenství a informace ohledně finančních záležitostí, daňových pravidel, pojištění apod. Banka by mohla nabídnout specializované finanční poradenství pro cizince, což by jí mohlo poskytnout konkurenční výhodu. Pro online a mezinárodní bankovníctví platí, že s rostoucím počtem cizinců, kteří si otevírají účty u „Banky X“, by banka měla zlepšit své online bankovníctví a nabízet služby v anglickém jazyce, aby lépe obsloužila mezinárodní klientelu.

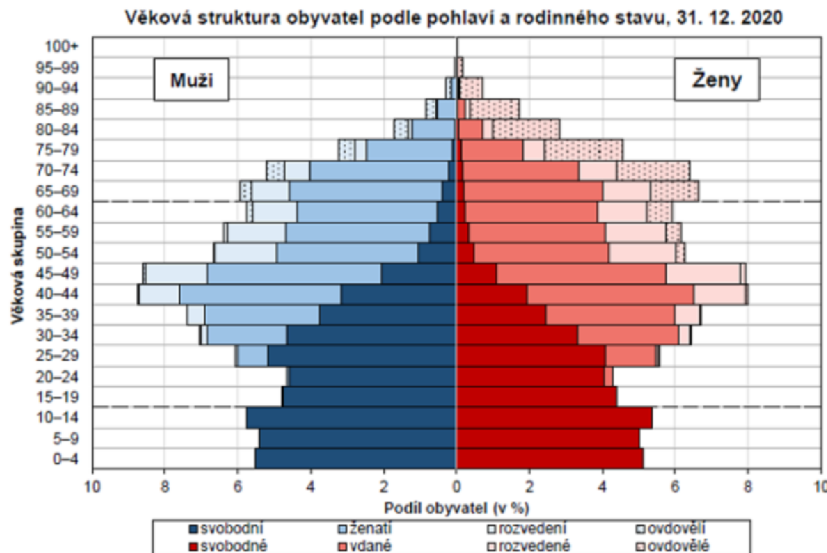
#### Hrozby

Co se týče hrozeb, jako první byly identifikovány změny v imigrační politice. Banka by měla sledovat změny v imigrační politice České republiky, protože restriktivnější politika může omezit příliv nových klientů z ciziny a snížit poptávku po specifických bankovních službách pro cizince. Další hrozba se týká snížené mobility. Pandemie covid-19 ukázala, že krize může dramaticky ovlivnit migrační toky. Banka by měla být připravena na sníženou mobilitu a případné omezení migračních pohybů, což by mohlo ovlivnit počet nových klientů a jejich finanční aktivity. Jako poslední hrozba bude popsána konkurence. S rostoucím počtem cizinců přicházejících do České republiky bude banka čelit větší konkurenci od jiných bank, které se budou snažit oslovit tuto cílovou skupinu. Banka by měla inovovat a nabízet unikátní služby, aby udržela svůj tržní podíl.

## Věková struktura obyvatel podle pohlaví a rodinného stavu

Struktura obyvatel podle rodinného stavu se také měnila. Svobodných a rozvedených osob přibývalo, zatímco počet a podíl osob vdaných/ženatých klesal. Tento trend byl důsledkem nízké sňatečnosti, vysoké rozvodovosti, dlouhého průměrného věku a odkládání sňatků způsobeného opatřeními proti šíření covid-19 v roce 2020. Věková struktura obyvatel podle pohlaví a rodinného stavu je zobrazena v následujícím obrázku.

Graf č. 3 Věková struktura obyvatel podle pohlaví a rodinného stavu



Zdroj: ČSÚ (2023)

Na základě dat z ČSÚ (2023) byla populace osob ve věku 15 let a více rozdělena podle rodinného stavu následovně: 32,1 % osob bylo svobodných (nárůst o 2,5 procentního bodu od roku 2011), 46,1 % ženatých nebo vdaných (snížení o 3,6 procentního bodu od roku 2011), 13,7 % rozvedených (nárůst o 1,6 procentního bodu od roku 2011) a 8,1 % ovdovělých (snížení o 0,4 procentního bodu od roku 2011). Struktura obyvatel podle rodinného stavu se tradičně liší mezi muži a ženami. U mužů je vyšší podíl svobodných a nižší podíl ovdovělých o zhruba 10 procentních bodů ve srovnání s ženami. Rozdíl mezi procentním zastoupením osob ženatých/vdaných a rozvedených podle pohlaví je nižší, kolem 3 procentních bodů – osob žijících v manželství je relativně více u mužů a rozvedených oproti tomu u žen. Z výše uvedených dat lze stanovit příležitosti a hrozby pro „Banku X“.

Na základě dat z ČSÚ (2023) byla populace osob ve věku 15 let a více rozdělena podle rodinného stavu následovně: 32,1 % osob bylo svobodných (nárůst o 2,5 procentního bodu od roku 2011), 46,1 % ženatých nebo vdaných (snížení o 3,6 procentního bodu od roku 2011), 13,7 % rozvedených (nárůst o 1,6 procentního bodu od roku 2011) a 8,1 % ovdovělých (snížení o 0,4 procentního bodu od roku 2011). Struktura obyvatel podle rodinného stavu se tradičně liší mezi muži a ženami. U mužů je vyšší podíl svobodných a nižší podíl ovdovělých o zhruba 10 procentních bodů ve srovnání s ženami. Rozdíl mezi procentním zastoupením osob ženatých/vdaných a rozvedených podle pohlaví je nižší, kolem 3 procentních bodů – osob žijících v manželství je relativně více u mužů a rozvedených oproti tomu u žen. Z výše uvedených dat lze stanovit příležitosti a hrozby pro „Banku X“.

## Příležitosti

V oblasti růstu populace svobodných a rozvedených osob může banka s rostoucím počtem svobodných a rozvedených osob identifikovat nové trhy a přizpůsobit své finanční produkty a služby, aby lépe vyhovovaly potřebám těchto skupin klientů. Může se zaměřit na produkty spojené s individuálním finančním plánováním, investicemi či úvěrovými produkty vhodnými pro tuto skupinu zákazníků.

S narůstajícím počtem mladých a technologicky zdatných zákazníků, kteří jsou svobodní nebo rozvedení, roste i poptávka po moderních a uživatelsky přívětivých digitálních bankovních službách. Banky mohou investovat do online aplikací a inovativních technologií, aby oslovily tuto skupinu klientů.

S nárůstem počtu svobodných a rozvedených osob se zvyšuje potřeba finančního poradenství v oblasti správy osobních financí, plánování na stáří a investic. Banky mohou poskytovat specializované poradenství a produkty, které budou odpovídat potřebám této klientely.

Vzhledem k trendu klesajícího počtu osob vdaných/ženatých a rostoucím podílu svobodných a rozvedených, banky mohou vyvíjet nové finanční produkty, které osloví mladé generace a nabídnou jim přizpůsobené služby, jako jsou studentské účty nebo inovativní půjčky.

## Hrozby

S klesajícím podílem osob vdaných/ženatých a ovdovělých se může snížit poptávka po tradičních bankovních účtech, jako jsou společné účty manželů nebo důchodové plány pro ovdovělé. Banky budou muset vyvinout strategie, jak udržet zájem klientů o tyto produkty.

Pokles počtu sňatků a narozených dětí, zejména v souvislosti s opatřeními proti covid-19, může ovlivnit poptávku po produktech spojených s financováním svateb, rodinných úvěrů a spořicích plánech pro děti.

## Dílčí závěr

Analýza sociálních faktorů ukázala několik významných příležitostí i hrozeb pro Banku X. Změny ve struktuře populace, včetně stárnutí populace, rostoucího počtu svobodných a rozvedených jedinců, a zvýšené migrace, představují významné sociální faktory, které mohou ovlivnit poptávku po bankovních produktech a službách.

Příležitosti zahrnují rozvoj nových online a mobilních aplikací, které vyhovují rostoucím očekáváním klientů pro digitální finanční služby. Také se ukázala možnost vytvořit specializované finanční produkty a služby pro seniory, cizince a svobodné či rozvedené jedince. Další příležitostí je využití technologického pokroku pro vývoj inovativních finančních produktů.

Nicméně analýza také identifikovala řadu hrozeb. Stárnutí populace může vést k nárůstu poptávky po produktech spojených s důchodovým zabezpečením a k poklesu poptávky po produktech, jako jsou hypotéky a spotřebitelské úvěry. Nízká natalita může ovlivnit poptávku po dětských spořicích účtech a dalších produktech pro mladé klienty. Další hrozby zahrnují potenciální změny v imigrační politice, sníženou mobilitu kvůli pandemii a zvýšenou konkurenci z jiných bank.

Výsledkem je, že Banka X by měla pružně reagovat na tyto sociální vývoje a dynamicky přizpůsobovat své strategie a nabídky produktů, aby efektivně oslovila nové trhy a udržela si konkurenceschopnost. To zahrnuje sledování změn a reagování na změny ve spotřebitelském chování, investování do digitálních technologií a vytváření specializovaných finančních produktů a služeb pro různé skupiny klientů.

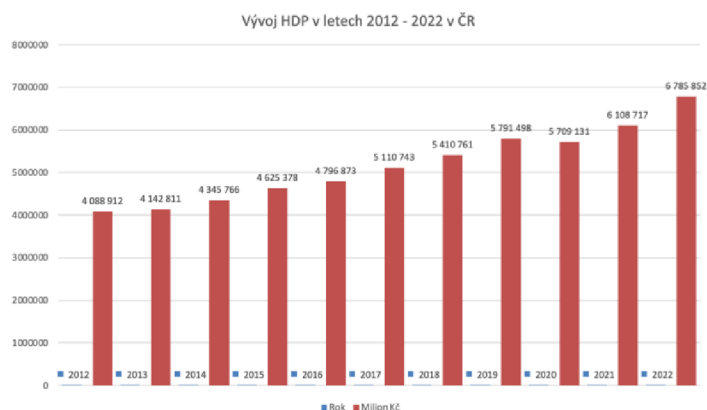
## Ekonomické faktory

V rámci ekonomických faktorů bude rozpracován vývoj HDP, inflace a úrokových sazeb, jelikož ty dle rozhovoru v příloze č. 2 s ředitelem divize řízení rizik „Banky X“ mohou ovlivnit zisky a náklady banky. Na základě informací z výše uvedeného rozhovoru budou v rámci ekonomických faktorů dále detailně popsána míra nezaměstnanosti a zaměstnanosti jakožto klíčové ukazatele, které ovlivňují úvěrové portfolio a poptávku po finančních produktech.

## Vývoj HDP

Dle dat ČSÚ (2023) vyplývá, že dlouhodobý trend za posledních několik desetiletí rosti. Počínaje 90. lety 20. století prošla ekonomika značnými změnami a transformací z plánované ekonomiky na tržní. To vedlo k postupnému zvyšování HDP. V následujícím grafu je zaznamenán trend vývoje v letech 2012–2022.

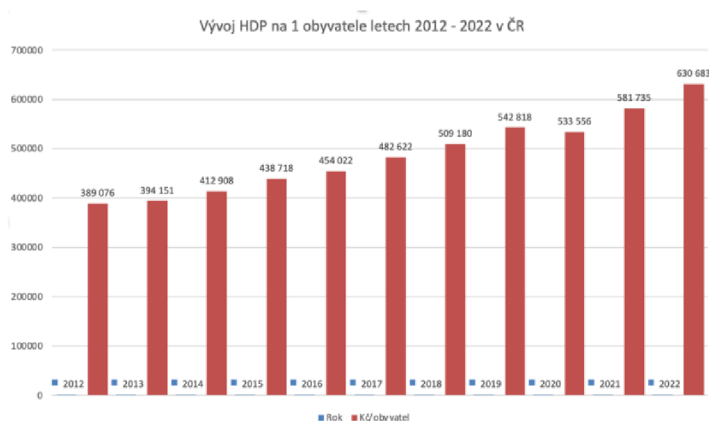
Graf 3 Vývoj HDP v letech 2012–2022 v ČR



Zdroj: ČSÚ (2023), vlastní zpracování

Ve výše uvedeném grafu lze sledovat vývoj HDP v posledních deseti letech, kdy Česká republika, stejně jako mnoho jiných zemí, čelila ekonomickým výzvám. Pandemie covid-19 měla negativní dopad na ekonomiku v roce 2020, což vedlo k poklesu HDP. Nicméně ekonomika se začala zotavovat v následujícím období, v roce 2021 a 2022 se očekávala pozitivní míra růstu. Další graf reprezentuje vývoj HDP na 1 obyvatele v letech 2012 až 2022.

Graf 4 Vývoj HDP na 1 obyvatele v letech 2012–2022 v ČR



Zdroj: ČSÚ (2023), vlastní zpracování

I z těchto dat lze dále vyčíst, že dlouhodobý trend v rámci HDP na obyvatele rostl v souladu s celkovým růstem HDP. To naznačuje, že se zvyšoval životní standard obyvatel. V důsledku pandemie bylo očekáváno, že HDP na obyvatele se v roce 2020 sníží, ale následně by se mělo zlepšit s oživením ekonomiky.

V rámci poskytnutí aktuálních dat budou prezentovány také z 2. čtvrtletí 2023. Data byla čerpána z ČSÚ (2023). Předběžné údaje ukazují, že ve druhém čtvrtletí došlo k mezičtvrtletnímu nárůstu HDP o 0,1 %, zatímco meziročně klesl o 0,6 %. V následující tabulce bude znázorněn přehled identifikovaných příležitostí a hrozeb na základě získaných dat týkajících se vývoje HDP.

#### Příležitosti

Jako příležitost lze identifikovat růst HDP v dlouhodobém trendu, jelikož naznačuje stabilní a rostoucí ekonomiku. To může přinést nové podnikatelské příležitosti pro banku. S rostoucím HDP se také může zvyšovat poptávka po úvěrových produktech a bankovních službách. Další příležitost je ve zlepšující se HDP na obyvatele, což ukazuje na potenciálně rostoucí příjmy a vyšší životní standard obyvatelstva. To může podpořit větší poptávku po hypotékách, spotřebitelských úvěrech a investičních produktech. Ekonomické oživení po pandemii covid-19 by mohlo vést k rostoucí aktivitě podniků a jednotlivců, což může vytvořit příležitost pro banku v oblasti investičního bankovníctví, správy aktiv a dalších finančních služeb.

Z pohledu ECB.europa.eu (2022) by reálný HDP eurozóny měl v roce 2022 vzrůst o 2,8 %, v letech 2023 a 2024 pak o 2,1 %. Ve srovnání s projekcemi z března 2022 byl výhled hospodářského růstu snížen pro roky 2022 a 2023, především kvůli dopadům války na Ukrajině, zatímco růst pro rok 2024 byl revidován směrem vzhůru.

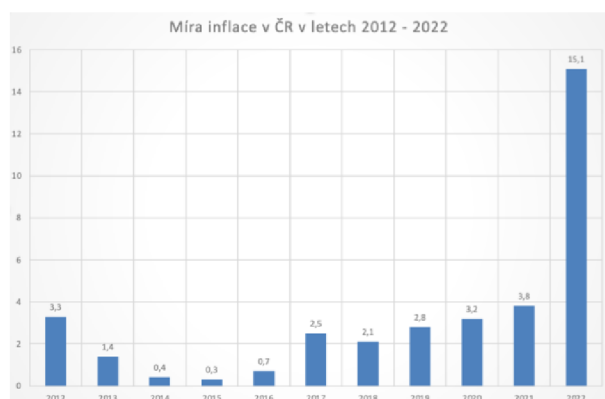
#### Hrozby

Naopak jako hrozba může být identifikován pokles HDP v důsledku pandemie, což může znamenat sníženou schopnost klientů splácet úvěry a zvýšené riziko nesplácení úvěrů. To může vést k růstu problematických úvěrů a negativně ovlivnit kvalitu aktiv banky.

## Vývoj inflace

Dle informací ČNB (2023) má centrální banka jako hlavní cíl stanoven péči o cenovou stabilitu v ekonomice, což je také zakotveno v § 2 zákona o ČNB. To znamená, že se zaměřuje na kontrolu inflace, opakujícího se růstu většiny cen v zemi. ČNB provádí měnovou politiku v režimu cílování inflace, kdy sleduje vývoj spotřebitelských cen a snaží se udržet míru inflace v rámci stanoveného cíle. Pro dosažení svého cíle sleduje ČNB nejen samotnou inflaci, ale také inflační očekávání domácností, podniků a finančních trhů. To umožňuje lépe předvídat budoucí vývoj cen a přizpůsobit svou měnovou politiku aktuálním ekonomickým podmínkám. Na základě přístupných dat z ČSÚ (2023) byl vytvořen graf týkající se vývoje inflace v ČR.

Graf 5 Míra inflace v ČR v letech 2012–2022



Zdroj: ČSÚ (2023), vlastní zpracování

[https://www.czso.cz/csu/czso/hmu\\_cr](https://www.czso.cz/csu/czso/hmu_cr)

Dle dat ČSÚ (2023) byla Česká republika v rámci dlouhodobého trendu schopna udržet inflaci v relativně nízkých číslech po vstupu do EU. V posledních letech byla inflace poměrně stabilní, ale v roce 2022 se očekávalo zvýšení kvůli oživení ekonomiky a růstu cen. Dle článku ČNB (2023) vysoká inflace a rostoucí úrokové sazby mají dopad na bankovníctví, především na úrokové sazby u půjček. V důsledku vysoké inflace centrální banky často zvyšují úrokové sazby, což způsobuje zvýšení nákladů na úvěry. To může způsobit, že nové úvěry budou dražší a méně dostupné pro klienty. MFČR (2023) predikuje, že v roce 2024 by inflační růst mohl dosáhnout horní poloviny inflačního cíle stanoveného ČNB. Průměrná inflace v tomto roce může dosáhnout 10,9 % a v roce 2024 poklesnout na 2,4 %, což značí výrazné zpomalení inflace v následujícím roce. Na základě dat získaných z ČSÚ o míře inflace v České republice a rozhovoru s generálním ředitelem „Banky „X“ v tiskové zprávě „Skupiny Y“ (2023) lze identifikovat následující příležitosti a hrozby související s vývojem inflace.

### Příležitosti

Banka má příležitost vyvíjet a nabízet nové finanční produkty a služby, které budou klientům pomáhat zvládnout náročnou ekonomickou situaci, např. úvěry s nízkým úrokem nebo nové způsoby investování. Vysoká míra inflace může vést k rostoucímu zájmu o investice a produkty, které klientům umožní chránit své peníze před inflačním efektem. Výroční zpráva (2020, str. 4) uvádí, že „Banka X“ na tuto skutečnost reagovala tak, že rozšířila své služby o jednorázové investování do podílových fondů.



Možnost nabídnout klientům flexibilní splátkové podmínky, jako jsou splátkové prázdniny nebo snížení měsíčních splátek, může zvýšit jejich loajalitu a spokojenost. V rámci snížení měsíčních splátek pro klienty s neočekávanými náklady nabízí banka přizpůsobení se klientům, kteří mají neočekávané výdaje. Může tak zabránit většímu zadlužení a ztrátě klientů. Jako poslední příležitost byla identifikována podpora klientů s nejistými finančními vyhlídkami, kdy banka může klientům poskytnout poradenství a podporu v plánování financí, aby lépe zvládli nejistotu spojenou s inflací a změnami na trhu.

### Hrozby

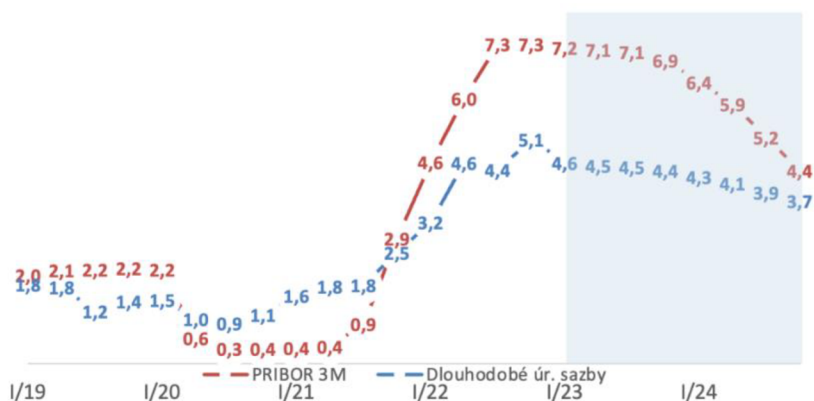
Pokud inflace způsobí vysokou míru cenového růstu, může to mít negativní dopad na platební schopnost klientů a zvýšit riziko nesplácení úvěrů. Pokud se inflace drží na vyšší úrovni a lidé očekávají další zvyšování cen, mohou být opatrnější při zadlužování na delší dobu, což může vést ke snížení poptávky po dlouhodobých úvěrech. Pokud dojde k výraznému nárůstu cen hypoték, může to odradit potenciální klienty od nakupování nemovitostí, což může snížit poptávku po hypotečních úvěrech. Růst cen energií může zvýšit náklady na provoz banky a omezit finanční prostředky dostupné pro investice do nových produktů a služeb. Při vysoké inflaci se reálné výnosy z investičních produktů mohou snižovat, což může odradit některé klienty od investování a hledání jiných možností uchování hodnoty svých peněz.

### Vývoj úrokové sazby

Prognózy ČNB mají zásadní dopady na banku a její fungování. Pokud úrokové sazby výrazně vzrostou nebo klesnou, může to negativně ovlivnit finanční výsledky banky. Tato hrozba se může zvýšit v časech hospodářské nejistoty nebo změn měnové politiky.

Vysoká míra inflace může vést k růstu úrokových sazeb, což se promítá do nákladů banky na financování. Dle dat MF ČR (2023) lze v níže uvedeném obrázku sledovat predikce MF ČR (Ministerstvo financí České republiky).

Graf 6 Výpočty a predikce MF ČR



Zdroj: MF ČR (2023)

Tento graf reprezentuje dvě linie. Červená linie značí PRIBOR (Prague InterBank Offered Rate), což v překlade znamená průměrná úroková sazba, za kterou si banky v České republice navzájem půjčují peníze na mezibankovním trhu (hyponamiru.cz, 2023). 3M znamená 3měsíční sazba. Sazby se pohybovaly v rozmezí od 2,0 % do 2,2 % mezi lety 2019 a 2020, pak ale poklesla na 0,3 % ve třetím čtvrtletí 2020, což mohl být důsledek ekonomické reakce

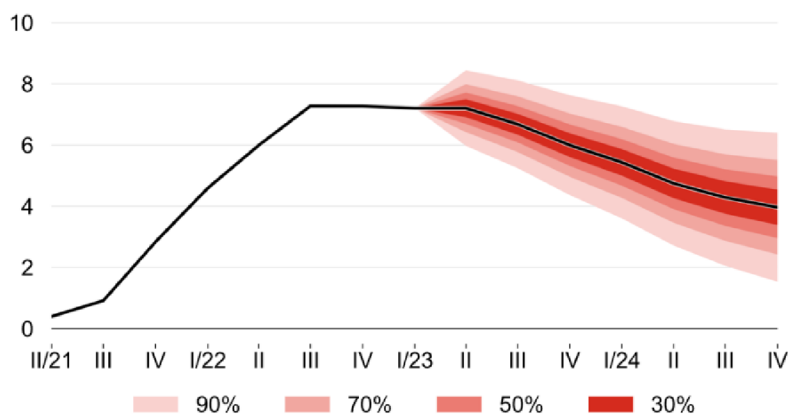
na pandemii covid-19. Od roku 2021 začaly sazby opět růst. Dosáhly 4,6 % ve druhém čtvrtletí 2022 a očekává se další nárůst. Modrá linie značí dlouhodobé úrokové sazby. Tyto sazby byly stabilní na 1,8 % v prvním a druhém čtvrtletí roku 2019, poté však klesly na 1,2 % ve třetím čtvrtletí a opět stouply na 1,4 % ve čtvrtém čtvrtletí. V průběhu roku 2020 došlo k mírným výkyvům mezi 1,0 % a 1,6 %. Od roku 2021 začaly sazby opět růst. Dosahují 5,1 % v prvním čtvrtletí 2023.

Růst úrokových sazeb může signalizovat zvyšující se inflaci, viz graf č. 6 Míra inflace v ČR v letech 2012–2022, kdy centrální banka zvyšuje sazby, aby omezila množství peněz v oběhu a tím omezila inflaci. Jako další v rámci úrokových sazeb bude zpracována prognóza pro vývoj úrokové sazby do prvního kvartálu roku 2024 (ČNB, 2023).

Graf 7 Prognóza úrokové sazby

### Úrokové sazby 3M PRIBOR (%)

S prognózou je konzistentní nejprve stabilita tržních úrokových sazeb následovaná jejich postupným poklesem.



Zdroj: ČNB (2023)

V roce 2023 jsou úrokové sazby relativně vysoké, 6,9 %. To znamená, že úrokové sazby jsou pravděpodobně vyšší i pro banku, což může mít vliv na náklady na financování a úvěrové produkty. Dle analytiků dojde v roce 2024 k mírnému snížení úrokových sazeb na 4,6 %. Nižší úrokové sazby mohou být pro banku výhodné, protože mohou snížit náklady na půjčování a zvýšit atraktivitu úvěrových produktů pro zákazníky. Další graf, který bude zpracován, se týká klientských úrokových sazeb (MFČR, 2023).



Graf 8 Klientské úrokové sazby

		2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
										Predikce	Predikce
<b>Klientské úrokové sazby</b>											
Úvěry domácnostem	v % p.a.	5,15	4,65	4,10	3,76	3,66	3,53	3,31	3,42	.	.
Úvěry nefinančním podnikům	v % p.a.	2,18	1,95	2,02	2,51	2,71	2,22	2,22	4,95	.	.
Vklady domácností	v % p.a.	0,65	0,47	0,36	0,33	0,39	0,35	0,26	1,13	.	.
Vklady nefinančních podniků	v % p.a.	13,01	11,21	9,62	8,75	8,67	8,27	7,74	9,06	.	.

Zdroj: MFČR (2023)

Z výše uvedeného grafu lze pozorovat trend v klientských úrokových sazbách. V oblasti úvěrů domácnostem se sazba obecně snižovala. V roce 2015 byla na úrovni 5,15 %, což byla nejvyšší hodnota v daném časovém období. Od tohoto bodu začala sazba klesat. Nejnižší hodnota byla zaznamenána v roce 2021, kdy sazba dosáhla 3,31 %. Poté došlo k mírnému nárůstu na 3,42 % v roce 2022. Co se týče úvěrů nefinančním podnikům, tato sazba byla variabilní. V roce 2015 byla na úrovni 2,18 %, klesla na 1,95 % v roce 2016, pak postupně stoupala až na 2,71 % v roce 2019. V roce 2020 došlo k poklesu na 2,22 %, ale v roce 2022 se sazba zvýšila na 4,95 %, což bylo nejvyšší v daném časovém období. Tento trend naznačuje, že úrokové sazby pro úvěry nefinančním podnikům nejdříve klesaly, ale poté začaly stoupat. U vkladů domácností lze pozorovat, že se tato sazba postupně snižovala. V roce 2015 byla sazba na úrovni 0,65 %, což bylo nejvyšší pro dané období. Od tohoto bodu začala sazba klesat a dosáhla nejnižšího bodu v roce 2021, kdy byla sazba 0,26 %. V roce 2022 došlo k nárůstu na 1,13 %. V oblasti vkladů nefinančních podniků sazba klesala od roku 2015, kdy dosáhla 13,01 %, což bylo nejvyšší pro dané období, a pokračovala v klesání až do roku 2022, kdy dosáhla 9,06 %. To ukazuje na klesající trend pro vklady nefinančních podniků. V návaznosti na výše uvedených údajů a rozhovoru s ředitelem řízení rizik, viz příloha č. 2, byly identifikovány následující příležitosti a hrozby pro „Banku X“.

#### Příležitosti

Pokud ekonomika očekává růst úrokových sazeb, banka by mohla mít příležitost k větším ziskům z úrokových výnosů. V rámci makroekonomické stabilizace lze říci, že pokud se ekonomika stabilizuje a inflace je pod kontrolou, může banka profitovat z lepších podmínek pro poskytování úvěrů a vkladů.

#### Hrozby

Na druhé straně, pokud ekonomika očekává růst úrokových sazeb, mohou se zvýšit náklady na financování banky, což by mohlo snížit ziskovost. Vysoká inflace může vést k nestabilitě a nejistotě, což by mohlo mít negativní dopad na bankovní sektor a způsobit ztrátu důvěry vkladatelů.

#### Míra zaměstnanosti

Na základě dostupných dat ČSÚ (2023x) bylo porovnáno období únor 2022 až únor 2023. Podíl zaměstnaných k celé populaci 15–64letých dosáhl 75,4 %, což je mírný nárůst o 0,2 procentního bodu ve srovnání s únorovými daty z roku 2022. Míra zaměstnanosti mužů činila 81,4 %, zatímco u žen dosáhla 69 %. Tento rozdíl ukazuje na stále existující genderovou nerovnost na trhu práce, což může mít vliv na finanční potřeby a preferenční chování podle pohlaví.

Míra zaměstnanosti osob ve věku 15–29 let byla 41,6 %, ve věku 30–49 let 87,6 % a osob ve věku 50–64 dosáhla 81,6 %. Tato data ukazují, že mladší věkové skupiny mají nižší míru zaměstnanosti než ostatní, což může ovlivnit jejich finanční situaci a potřeby. Lidé v této věkové skupině mohou mít problém se splácením půjček, mohou mít také méně zkušeností v oblasti finanční gramotnosti. Dle rozhovoru s generálním ředitelem v tiskové zprávě (2023, str. 58) si je „Banka X“ tohoto faktu vědoma a od loňského roku nabízí účty pro rodiny a malé děti, aby měly možnost učit se pracovat s financemi již od útlého věku. Dle výroční zprávy „Banky X“ (2020, str. 4) díky tomu, že disponenty se mohou stát děti už od 10 let a pro internetové bankovníctví existuje také dětská verze aplikace, přibylo „Bance X“ za jeden rok 72 tisíc nových klientů. Jako příležitost pro banku může být také rozšíření produktu o studentské účty či spoření s výhodnými podmínkami, které by tuto věkovou skupinu mohly oslovit.

### Příležitosti

V rámci mírného nárůstu zaměstnanosti lze sledovat, že nárůst podílu zaměstnaných k celé populaci 15–64letých na 75,4 % může signalizovat zlepšení ekonomické situace. To by mohlo vést ke zvýšení poptávky po bankovních produktech a službách. Další příležitost se týká rodinných a dětských účtů. Banka úspěšně zavedla účty pro rodiny a malé děti, což přilákalo 72 tisíc nových klientů. To ukazuje, že banka může úspěšně oslovovat mladé klienty a jejich rodiny. S tím také souvisí třetí identifikovaná příležitost, tou je potenciální rozšíření nabídky pro mladé lidi. Existující úspěch s účty pro děti a rodiny totiž naznačuje potenciální příležitost pro rozšíření nabídky produktů pro mladé lidi. Může se to týkat nabídky studentských účtů či spořicí účty s výhodnými podmínkami, jako je např. roční úrok 5 %.

### Hrozby

Jako hrozba byla identifikována genderová nerovnost na trhu práce. Rozdíl v míře zaměstnanosti mezi muži a ženami ukazuje na stále existující genderovou nerovnost na trhu práce, což může vést k odlišným finančním potřebám a preferencím. To by mohlo vyžadovat specifické produkty a služby pro každé pohlaví. Další hrozba, tedy nižší míra zaměstnanosti u mladších věkových skupin značí, že tato skupina má nižší míru zaměstnanosti než ostatní, což může negativně ovlivnit jejich finanční situaci a potřeby. Tito lidé pak mohou mít potíže se splácením půjček. S mladší věkovou skupinou souvisí také poslední identifikovaná hrozba, což je finanční gramotnost. Tato skupina může mít méně zkušeností v oblasti finanční gramotnosti. To může vést k potenciálnímu riziku špatného rozhodování a řízení jejich finanční situace.

### Míra nezaměstnanosti

Dle dat ČSÚ (2023x) bylo v rámci tohoto aspektu bylo porovnáváno stejné období, tedy únor 2022 až únor 2023. Podíl nezaměstnaných k ekonomicky aktivním, tedy součtu zaměstnaných a nezaměstnaných, dosáhl 2,5 %, což je stejná hodnota jako v únoru předchozího roku. To naznačuje relativně nízkou míru nezaměstnanosti v zemi, což může signalizovat stabilní ekonomické podmínky a potenciálně menší riziko výpadku splácení úvěrů. Míra nezaměstnanosti mužů dosáhla 2,1 %, u žen 2,9 %. Opět je zde patrná genderová nerovnost na trhu práce, což může ovlivnit ekonomickou nezávislost a platební schopnost jednotlivých klientů. Stabilní ekonomické podmínky mohou pro banku znamenat menší riziko nemožnosti splácení úvěrů ze strany klientů. Dle MFČR (2023) se na trhu práce stále vyskytuje problém spojený s nedostatkem zaměstnanců. I přes skutečnost, že hospodářství prochází mírným poklesem, očekává se, že míra nezaměstnanosti v roce 2023 nebude dramaticky růst. Z 2,3 %

v předešlém roce by letos mohla dosáhnout na 3,0 %. Predikce na rok 2024 naznačuje, že by se mohla snížit na průměrných 2,8 %.

### Příležitosti

První identifikovaná příležitost, tedy nízká míra nezaměstnanosti, která činí 2,5 %, ukazuje na nízkou míru nezaměstnanosti v zemi, což může znamenat, že většina lidí má pravidelný příjem. To může zvýšit poptávku po bankovních produktech a službách a snížit riziko nesplácení úvěrů. Stabilní míra nezaměstnanosti může signalizovat stabilní ekonomické podmínky v zemi, což může vést ke zvýšené důvěře spotřebitelů a zvýšení poptávky po finančních produktech a službách.

### Hrozby

Míra nezaměstnanosti mezi muži a ženami ukazuje na genderovou nerovnost na trhu práce. Vyšší míra nezaměstnanosti mezi ženami může vést k nižší ekonomické nezávislosti a platební schopnosti, což by mohlo žádat specifické produkty a služby pro ženy.

### Dílčí závěr

Zvýšená poptávka po bankovních produktech a službách může vést k vyššímu zisku a růstu tržního podílu banky. Banka má také příležitost využít své schopnosti a zkušenosti k rozšíření svého portfolia produktů a služeb a ke zvýšení své konkurenceschopnosti.

Hrozby však představuje pokles HDP, vysoká inflace, růst úrokových sazeb a nerovnost na trhu práce. Tyto faktory mohou vést ke zvýšenému riziku nesplácení úvěrů, ztrátě důvěry vkladatelů a k poklesu poptávky po bankovních produktech a službách. To by mohlo negativně ovlivnit finanční výkon a postavení banky na trhu.

Banka by měla aktivně sledovat ekonomické trendy a potřeby klientů a přizpůsobovat své strategie a nabídky produktů a služeb, aby mohla efektivně reagovat na měnící se ekonomické podmínky a konkurenční prostředí. Jedná se o kontinuální proces, který vyžaduje pružnost a inovativní přístup.

Celkově je ekonomický faktor klíčový pro úspěch a růst banky. Jeho správné pochopení a využití může být rozhodující pro budoucí vývoj a konkurenceschopnost banky.

### Technologické faktory

Technologický aspekt STEP analýzy se zabývá technologiemi a jejich dopady na organizaci. Faktor bude dále zkoumán jak z pohledu aktuálních technologií, tak trendů v digitální bankovníctví. Z dat výroční zprávy „Banky X“ (2020, str. 12) vyplývá, že technologická infrastruktura a informační systémy jsou základními nástroji pro řízení rizik a reportování těchto událostí vedení. Technologie jsou také důležité pro implementaci technických opatření na snížení rizik, ať už jako prevence či v rámci nápravných aktivit. Technologické nástroje hrají také roli v řízení kontinuity podnikání a reagování na mimořádné události s pomocí předem vypracovaných a pravidelně aktualizovaných pohotovostních plánů.

V návaznosti na výroční zprávu (2021) se „Banka X“ úspěšně přizpůsobila zhoršené ekonomické situaci v ČR způsobené bojem proti epidemii koronaviru. Investice do digitálních distribučních kanálů umožnily „Banka X“ fungovat bez výrazného dopadu na dostupnost služeb během pandemie. Tento aspekt zvýšil růst a urychlil přijetí digitálního bankovníctví mezi zákazníky. Orientace na digitální kanály, zejména mobilní aplikaci, v kombinaci s optimalizací provozních nákladů přispěla k růstu kladných výsledků hospodaření.

## Trendy v digitálním bankovníctví

Na základě rozhovoru s generálním ředitelem „Banky X“ pro výroční zprávu „Skupiny Y“ (2023, str. 59) je patrné, že digitalizace a přístupnost služeb pro klienty jsou jedním z hlavních pilířů a strategií „Banky X“. Na online bankovníctví byl kladen velký důraz již od založení banky a všechny služby, které banka v té době nabízela (běžný a spořicí účet) byly od začátku přístupné prostřednictvím digitálních kanálů. Dle výroční zprávy (2023, str. 4) v roce 2020 překročil počet uživatelů aplikace internetového bankovníctví 600 tisíc lidí.

Digitalizace bankovníctví je trend, který banky všude na světě sledují a dle informací získaných z dokumentu „Skupiny Y“ (2021, str. 17) a z výše uvedených informací je zřejmé, že „Banka X“ si je tohoto faktu velmi dobře vědoma. Mobilní platforma „Banky X“ je klíčovým nástrojem pro růst prodeje. Prostřednictvím mobilní aplikace prodala od srpna 2019 více než 5,2 tisíce kontokorentů, z toho 43 % aktivací proběhlo přes mobilní aplikaci. Od června 2018 nabízí „Banka X“ možnost vyplnění kompletní žádosti o spotřebitelský úvěr v rámci mobilní aplikace a od března 2017 bylo prodáno 24 tisíc cestovních pojištění, z čehož 72 % nákupů bylo uskutečněno v mobilní aplikaci. „Banka X“ zaznamenává desítky interakcí s klientem v rámci online bankovníctví na denní bázi, což je oproti předchozích letem velký nárůst.

Oblibu digitalizace potvrzují i data ČSÚ (2023x), dle kterých využívalo internetové bankovníctví v roce 2010 21 % Čechů, v roce 2022 bylo zaznamenáno již 71 %. Více těchto služeb využívají muži než ženy (74 % oproti 68 %). Statistiky dále uvádějí, že nejpočetnější skupinou uživatelů jsou mladí lidé ve věku 25–34 let (95 % z této skupiny). Je zde také patrná souvislost mezi vzděláním a používáním internetového bankovníctví. Z vysokoškolsky vzdělaných lidí (věk 25–64) využívá služby internetového bankovníctví 97 % osob. Se základním vzděláním ve stejné věkové skupině je to již pouze 48 % osob. V roce 2021 bylo využívání internetového bankovníctví v ČR (73 %) výrazně nad průměrem v rámci EU (58 %). Češi prostřednictvím internetového bankovníctví také sjednávali online pojištění (10 % Čechů v roce 2022), online půjčky či nakupovali cenné papíry (2,4 % Čechů v roce 2022).

Data ČSÚ (2023) uvádí, že v roce 2020 mělo připojení k internetu 82 % českých domácností, což značí výrazný nárůst od předchozích let. V roce 2020 79 % českých domácností vlastnilo počítač. Pandemie covidu-19 změnila chování na internetu, kdy 64 % obyvatel používalo internetové bankovníctví. Pandemie covidu-19 způsobila zvýšené využívání online služeb, včetně online bankovníctví, což banky musí brát v úvahu při plánování budoucích služeb a krizových reakcí. Je možné sledovat trend ve výrazném poklesu v počtu telefonních stanic z 2,3 milionu v roce 1995 na 530 tisíc v roce 2020. Počet uživatelů chytrých telefonů s internetem vzrostl z 1 milionu v roce 2012 na 6,4 milionu v roce 2020. Tento významný nárůst znamená, že mobilní bankovníctví může být klíčovým kanálem pro poskytování bankovních služeb. V České republice došlo v období mezi lety 1995 a 2020 k výraznému nárůstu v používání informačních technologií a mobilních telefonů. Tento trend je ovlivněn technologickým vývojem a sociálními a ekonomickými změnami, zejména pandemií covidu-19. Lze pozorovat, že technologie hrají stále důležitější roli v běžném životě Čechů.

## Příležitosti

Tyto skutečnosti indikují, že digitalizace je obrovská inovace a změna, která samozřejmě zasahuje i do spotřebitelského chování. Poptávka po digitálních finančních službách a mobilním bankovním neustále roste. V minulé dekádě chodili klienti na pobočky mnohem častěji, než je tomu dnes. V dnešní době musí naopak banky vymýšlet strategie a způsoby, jak oslovit a zaujmout klienta, aby si ideálně z pohodlí domova mohl vybrat produkt z bankovního portfolia, který je šitý na míru a dosažitelný pomocí pár kliknutí v mobilní aplikaci. Je tedy velice důležité, aby banka pokračovala v rozšiřování nabídky produktů či služeb na mobilní platformě. Nezbytné je také pokračovat ve vývoji a aktualizaci, aby bylo možné uspokojit rostoucí poptávku. V rámci digitalizace je také zapotřebí využívat nové technologie, jako je například automatizace procesů či využití chatbotů, kteří mohou interakci zefektivnit. Tuto příležitost také identifikoval ředitel divize řízení rizik operačních rizik „Banky X“, viz příloha č. 2. Pro banku je také extrémně důležité věnovat pozornost změnám v technologiích, jako jsou např. různé zabezpečovací protokoly, algoritmy pro umělou inteligenci nebo trendy v „user experience“ UX či „user interface“ UI designu mohou mít významný dopad, jak „Banka X“ poskytuje své služby.

Kryptoaktiva jsou pro „Banku X“ také velká příležitost, zároveň však také hrozba. Vávra (2022) uvádí, že momentální přístup „Banky X“ je vůči kryptoměnám restriktivní, jelikož zahájila blokování bankovních převodů směřujících na burzy kryptoměn. Přestala také umožňovat svým klientům používat funkci okamžitých plateb pro investici do kryptoměn, jako jsou např. Bitcoin a Ethereum. Toto opatření bylo zdůvodněno zvýšeným rizikem praní špinavých peněz při obchodování s virtuálními měnami. Autor článku dále uvádí, že „Banka X“ je příliš svázaná současnou legislativou a také rozhodnutím její korespondenční banky, která zpracovává zahraniční platby a je vůči kryptoměnám negativně naladěná. Nicméně „Banka X“ si uvědomuje obrovský potenciál a na alternativním řešení pracuje, současný stav není vyhovující a „Banka X“ vnímá potřebu změny. Tento názor sdílí také generální ředitel „Banky X“, který ve výroční zprávě (2023) dodává, že jako hlavní riziko vnímá fakt, že tato oblast není dostatečně regulovaná, na rozdíl od ostatních investic, které jsou regulovány striktně. Vzniká tedy situace, kdy do kryptoaktiv investují lidé, kteří nemají dostatečné znalosti a hrozí tak ztráta jejich financí. S tímto názorem souhlasí i vedoucí operačních rizik, viz příloha č. 1.

## Hrozby

V rámci hrozeb bude detailně popsána kybernetická bezpečnost, jelikož tato hrozba byla také identifikována v rozhovoru s vedoucím oddělení operačních rizik v příloze č. 2, otázka č. 18. Vzhledem k faktu, že využití digitálních platforem je stále běžnější a populárnější, roste také riziko kybernetických útoků, které se stávají sofistikovanějšími. Banka musí neustále podvodné praktiky monitorovat a být schopna pružně reagovat, aby byla schopna ochránit osobní údaje a finance svých zákazníků. Je zapotřebí neustále investovat do nových technologií a systémů, které dokáží zabezpečit citlivá data a zabránit kybernetickým útokům.

Jedna ze strategií kybernetické bezpečnosti, kterou banka aplikuje, je komunikace s klienty prostřednictvím e-mailů, které mají za cíl klienty naučit, jakým způsobem banka s klienty komunikuje a jak se vyhnout podvodům. V těchto emailech „Banka X“ např. edukuje, jak poznat phishing – podvodný email, který se snaží napodobit bankovní komunikaci. Dále „Banka X“ zdůrazňuje, že nikdy neposílá svým klientům odkazy na přihlášení do internetového bankovního či mobilní aplikace.

Další informace v rámci této komunikace je upozornění, aby klienti nikdy nesdíleli své přihlašovací údaje do bankovního, ani číslo platební karty se všemi údaji. Podvodníci mohou využít také vishingu, což je velmi podobná podvodná praktika jako phishing, místo emailu je útok proveden prostřednictvím telefonních hovorů. Klímová (irozhlas.cz, 2023) konstatuje,

že loni podal Finanční analytický úřad (FAÚ) rekordní počet trestních oznámení kvůli podezření na podvody a praní špinavých peněz. Bylo jich 911 a celkem zajistili 2,6 miliardy korun, což je o zhruba 600 milionů více než za rok předchozí. Velká část případů se týkala právě phishingu a vishingu.

## **Dílčí závěr**

Na základě technického faktoru lze shrnout, že digitalizace a technologický vývoj mají pro banku klíčový význam, a to jak v kontextu růstu a vývoje jejích služeb, tak i v kontextu zabezpečení a ochrany proti rizikům.

Digitalizace bankovních služeb představuje významnou příležitost pro banku, a to jak z hlediska uspokojování rostoucí poptávky po digitálních službách a mobilním bankovníctví, tak z hlediska efektivity operací prostřednictvím automatizace procesů a využití chatbotů. Je nezbytné, aby banka pokračovala v rozšiřování nabídky produktů či služeb na mobilní platformě a sledovala nejnovější trendy v oblasti UX/UI designu. S tímto názorem souhlasí také vedoucí operačních rizik, viz příloha č. 1.

Naproti tomu banka musí čelit i významným rizikům, včetně kybernetické bezpečnosti. S rostoucím využitím digitálních platform roste také riziko kybernetických útoků. Je tedy nezbytné investovat do nových technologií a systémů pro zabezpečení citlivých dat a ochranu proti kybernetickým útokům.

Souhrnně řečeno, technický faktor vyžaduje od banky neustálý rozvoj a adaptaci v kontextu rychle se vyvíjejících technologií, včetně digitálních a mobilních platform, kryptoaktiv a kybernetické bezpečnosti.

### **3.2.1 Analýza rizik**

STEP analýza umožnila identifikovat příležitosti a hrozby spojené s vybranými oblastmi, konkrétně sociální, technicko-technologickými a ekonomickou. Tyto příležitosti a hrozby mohou ovlivnit činnost banky a její strategické cíle. Na základě STEP analýzy a rozhovoru s ředitelem divize řízení rizik a vedoucím oddělení řízení operačních rizik bylo identifikováno 30 příležitostí a 28 hrozeb. K naplnění cíle této práce budou dále zkoumány hrozby, na základě kterých byla identifikována rizika a dopad, který by mohl nastat v jejich důsledku.

Jako další krok v rámci kvantifikace rizik bude aplikována matice rizik (MR). Šenovský (2021) konstatuje, že tato metoda je jedním z nejpoužívanějších nástrojů pro hodnocení rizik. Fotr et al. (2020, str. 288) dodávají, že matice rizik se řadí mezi nástroje expertního hodnocení, které vyžaduje komplexní znalosti z dané oblasti. MR bude mít jasně stanoveny klasifikačními parametry. Cílem využití matice rizik je zjistit nejvyšší míru rizika a tím tak stanovit, která rizika mohou mít na organizaci nejkritičtější dopad. Pro tato rizika budou zpracována opatření na snížení rizika. Pro přehlednost vstupů jsou následující informace dohledatelné v příloze č. 4 a č.5.

### **Sociální rizika**

R1 – Profil klientů může být ohrožen stárnutím populace, což povede ke změně potřeb klientů. Dopad: Snížení poptávky po některých produktech.

R2 – Produkty pro mladé rodiny nebo děti mohou být ohroženy nízkou porodností, což vede k dlouhodobému snížení poptávky. Dopad: Snížení poptávky po stávajících produktech pro mladé rodiny.

## **Ekonomická rizika**

R3 – Solventnost klientů může být ohrožena ekonomickou nestabilitou, což znamená riziko zvýšení nesplacených úvěrů. Dopad: Zvýšení nesplacených úvěrů a zvýšení nákladů na vymáhání pohledávek.

R4 – Demografická struktura klientů může být ohrožena změnami v imigrační politice. Dopad: Náhlý příliv klientů z nových demografických skupin, na které by banka nebyla připravená.

R5 – Počet nových klientů může být ohrožen sníženou mobilitou a omezeními migračních pohybů, jak bylo vidět během pandemie covid-19. Dopad: Výrazný pokles v nových účtech a úvěrových žádostech v důsledku omezení mobility.

R6 – Podíl na trhu a příjmy mohou být ohroženy konkurencí, což vede k možnosti ztráty tržního podílu. Dopad: Snížení příjmů, zvýšení nákladů na získání a udržení zákazníka.

R7 – Snížená poptávka po tradičních bankovních produktech může ohrozit příjmy. Dopad: Odliv zákazníků, snížené příjmy.

R8 – Produkty orientované na rodinný život mohou být ohroženy odkládáním sňatků a porodů. Dopad: Snížení poptávky pro produktech orientovaných na rodiny (společné účty, dětské účty, hypotéky, sloučení půjček apod.).

R9 – Problém správy úvěrů může být ohrožen růstem problematických úvěrů a nedostatečnými kontrolními mechanismy. Dopad: Navýšení nákladů na vymáhání pohledávek, snížené příjmy.

R10 – Bankovní segment může být ohrožen nestabilitou v ekonomické situaci a závislostí na jediném tržním segmentu. Dopad: Masivní odliv klientů a snížené tržby.

R11 – Úrokové příjmy mohou být ohroženy poklesem poptávky po dlouhodobých úvěrech v důsledku omezené produktové diverzifikace. Dopad: Snížení úrokových příjmů a možná finanční ztráta.

R12 – Tržní podíl může být ohrožen zvýšením cen hypoték a neschopností banky pružně reagovat. Dopad: Ztráta tržního podílu a snížení tržeb.

R13 – Provozní náklady mohou být ohroženy prudkým nárůstem cen energie a vysokými energetickými nároky banky. Dopad: Zvýšené provozní náklady a snížený zisk.

R14 – Absence informací o alternativních investičních produktech může být ohrožena negativními výnosy z investičních produktů. Dopad: Masivní odliv investic a kapitálu.

R15 – Dlouhodobě fixované náklady financování banky mohou být ohroženy růstem úrokových sazeb. Dopad: Zvýšení nákladů na financování a potenciální bankrot.

R16 – Úspory klientů banky mohou být ohroženy vysokou inflací, pokud nejsou inflací korigovány. Dopad: Masivní odliv úspor a kapitálu.

R17 – Nepružný trh práce může být ohrožen nižší mírou zaměstnanosti mladších věkových skupin. Dopad: Ekonomická nestabilita a zvýšené sociální napětí.

R18 – Finanční vzdělání a dostupné zdroje pro mladší věkové skupiny mohou být ohroženy špatným finančním rozhodováním. Dopad: Větší ekonomická nestabilita a potenciální finanční ztráty.

R19 – Genderová nerovnost v míře nezaměstnanosti může být ohrožena předsudky zaměstnavatelů. Dopad: Prohloubení sociálních a ekonomických nerovností.

### **Technologická rizika:**

R20 – Kybernetická bezpečnost je ohrožena nárůstem kybernetických útoků, což může narušit poskytování služeb a způsobit finanční ztráty. Dopad: Významné finanční ztráty způsobené narušením služeb a ztráta důvěry klientů.

R21 – Změna regulace může vést k vyšším nákladům na dodržování pravidel a potřebě adaptace produktů a služeb. Dopad: Zvýšení operativních nákladů a potřeba přepracování obchodní strategie.

R22 – Rychlý technologický vývoj může znamenat potřebu zvýšených investic do inovací a hrozbu neschopnosti držet krok s konkurencí. Dopad: Ztráta konkurenceschopnosti a potřeba větších investic do technologického vývoje.

### **Ostatní rizika:**

R23 – Nefunkčnost hardwaru či bankovní aplikace může vést k ztrátě nebo narušení informačních systémů. Dopad: Přerušování všech bankovních transakcí a ztráta důvěry zákazníků.

R24 – Požár v budově může způsobit poškození majetku a infrastruktury a potenciální zranění zaměstnanců. Dopad: Finanční ztráty v důsledku poškození majetku a možné náklady na léčbu zraněných zaměstnanců.

R25 – Výpadek elektrického proudu může vést k zpoždění nebo přerušování klíčových obchodních operací. Dopad: Zastavení všech bankovních operací a transakcí v důsledku výpadku energie.

R26 – Nepřítomnost většího počtu zaměstnanců, např. kvůli nemoci, může způsobit narušení klíčových operací a služeb. Dopad: Zpoždění v provádění transakcí a ztráta efektivity v poskytování služeb.

R27 – Nedostupnost hlavních pracovních systémů může způsobit ztrátu dat nebo narušení informačních systémů. Dopad: Pozastavení všech transakcí a narušení služeb zákazníků.

R28 – Teroristický útok nebo podezřelé chování ve veřejném prostoru může ohrozit bezpečnost zaměstnanců a klientů. Dopad: Možné zranění zaměstnanců a klientů, materiální škody a významná ztráta důvěry veřejnosti.

### **Výpočet míry rizika**

Jednotlivá rizika ve výše uvedeném seznamu byla ohodnocena pomocí výpočtu míry rizika. Tato rizika byla klasifikována s ředitelem divize řízení rizik, vedoucím oddělení řízení operačních rizik a manažerem tržních rizik „Banky X“ v rámci brainstormingu. Manažeři v rámci tohoto hodnocení uplatnili své vlastní zkušenosti. Pro kvantifikaci rizik byla stanovena klasifikační stupnice a stupnice pro hodnocení rizik. Klasifikační stupnice obsahuje stupnici čísel 1–5, kdy 1 reprezentuje nejnižší hodnoty pravděpodobnosti výskytu či dopadu a číslo 5 představuje nejvyšší hodnotu. Cílem této metody je zjistit u každého rizika pravděpodobnost výskytu a velikost dopadu.



Tabulka 5 Klasifikační stupnice

Klasifikační stupeň	Pravděpodobnost výskytu	Velikost dopadu
1	Vzácné	Zanedbatelná
2	Nepravděpodobné	Malá
3	Možné	Střední
4	Pravděpodobné	Významná
5	Jisté	Katastrofální

Zdroj: autor, vlastní zpracování

Pravděpodobnost výskytu je klasifikována následovně: Vzácná (1), Nepravděpodobná (2), Možné (3), Pravděpodobná (4), Jistá (5).

Závažnost (velikost) dopadu je klasifikována následovně: Zanedbatelná (1), Malá (2), Střední (3), Významná (4), Katastrofální (5).

Ve stupnici pro hodnocení rizik je stupnice 1 až 25, dle míry rizika od nízkého až po kritická. Rizika budou také barevně odlišena dle významnosti rizika. Součinem těchto hodnot lze identifikovat riziko s nejvyšší mírou dopadu (RPN). Vzhledem k velikosti byla výsledná tabulka výpočtu míry rizika na základě identifikovaných hrozeb přesunuta do přílohy č. 5. Rizika s nejvyšší mírou rizika (RPN) budou rozepsána níže v textu.

Tabulka 6 Stupnice pro hodnocení rizik

Míra rizika	Popis	Rozmezí	Barevné označení
Nízké	Riziko je akceptovatelné	1–6	
Střední	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti je riziko akceptovatelné	7–13	
Vysoké	Riziko je dlouhodobě nepřijatelné, jsou nutné systematické kroky potřebné k jeho odstranění	14–19	
Kritické	Riziko je nepřijatelné, neprodleně musí být odstraněno	20–25	

Zdroj: zákonyprolidi.cz (2023)

Míra rizika je vypočítána pomocí následujícího vzorce:

$$\text{Riziko} = \text{pravděpodobnost výskytu} * \text{dopad}$$

## **Opatření vedoucí ke snížení rizik**

Po hodnocení rizik následuje další krok v rámci procesu řízení rizik, a sice ošetření rizik. Přístupy akceptace rizika, zmírnění rizika, přenos rizika nebo vyhnutí se riziku budou aplikovány na ta rizika, která mají nejvyšší míru rizika, tedy R3 – Riziko snížení solvence klientů kvůli ekonomické nestabilitě, R6 – Ztráta tržního podílu kvůli konkurenci, R10 – Finanční ztráta kvůli ekonomické nejistotě, R20 – Finanční ztráta kvůli kybernetickým incidentům. Bude zohledněn jak krátkodobý, tak dlouhodobý horizont.

### **R3: Riziko snížení solvence klientů kvůli ekonomické nestabilitě (RPN 20)**

- Zainteresované strany: Management banky, akcionáři, věřitelé, klienti a regulátoři.
- Krátkodobý horizont: Riziko je akceptováno. K 31. 12. 2020 banka disponovala základním kapitálem ve výši 500 021 tis. Kč a celkovým vlastním kapitálem 11 137 384 tis. Kč. Celková kapitálová přiměřenost se zvýšila z 15,4 % v roce 2019 na 15,8 % v roce 2020. To může naznačovat, že banka je lépe připravena na pokrytí potenciálních ztrát v důsledku nesolventnosti klientů. Kapitálová přiměřenost dále poskytuje bance dostatečnou finanční pružnost k absorpci potenciálního nárůstu nesplacených úvěrů v krátkodobém horizontu.
- Dlouhodobý horizont: Riziko je zmírňováno. Investování do sofistikovaných analytických nástrojů a technologií může pomoci při identifikaci potenciálních rizikových skupin klientů a zároveň umožnit proaktivní řešení. To může zahrnovat využití umělé inteligence a strojového učení k analýze vzorců chování klientů a včasné identifikaci rizik.

### **R6: Ztráta tržního podílu kvůli konkurenci (RPN 20)**

- Zainteresované strany: Management banky, marketingový tým, akcionáři, klienti a konkurenční banky.
- Krátkodobý horizont: Riziko je zmírňováno. Banka plánuje zintenzivnit své marketingové aktivity, využívá k tomu část svého emisního ážia 4 962 562 tis. Kč. Zvýšené marketingové aktivity, zejména v oblasti digitálních kanálů, jsou vhodným krokem. Z výroční zprávy vyplývá, že banka má silnou pozici v digitálních službách, což může posílit její konkurenceschopnost.
- Dlouhodobý horizont: Riziko je zmírňováno. Investice do inovací a vývoj nových digitálních produktů je důležitý pro udržení konkurenceschopnosti. To by také mohlo přilákat nové klienty a udržet stávající. Zároveň je třeba sledovat trendy na trhu a poptávku zákazníků.

### **R10: Finanční ztráta kvůli ekonomické nejistotě (RPN 20)**

- Zainteresované strany: Management banky, akcionáři, věřitelé, klienti a ekonomičtí analytici.
- Krátkodobý horizont: Riziko je přeneseno. Banka může uzavřít pojištění proti rizikům mimořádných ekonomických událostí, využívajíc k tomu část svého vlastního kapitálu.
- Dlouhodobý horizont: Riziko je zmírňováno. Zlepšení procesů řízení rizik a strategického plánování je klíčové. Toto by mělo zahrnovat pravidelné přehodnocení rizikového profilu banky a její strategie na základě měnící se ekonomické situace. Banka by měla zvážit diverzifikaci svých investic a optimalizaci svých finančních rezerv, aby byla schopná lépe absorbovat potenciální finanční ztráty v důsledku ekonomické nejistoty. To může také zahrnovat pravidelný monitoring a posuzování ekonomických ukazatelů a trendů.

## **R20: Finanční ztráta kvůli kybernetickým incidentům (RPN 25)**

- Zainteresované strany: Management banky, IT tým, zaměstnanci banky, akcionáři, klienti a externí IT bezpečnostní firmy.
- Krátkodobý horizont: Riziko je zmírňováno. Banka může využít část svého emisního ážia na posílení svých IT bezpečnostních týmů a zlepšení bezpečnostních protokolů. Banka by měla posílit své IT bezpečnostní týmy a zlepšit bezpečnostní protokoly, aby minimalizovala riziko kybernetických incidentů.
- Dlouhodobý horizont: Kromě uzavření pojištění proti kybernetickým rizikům je třeba dále investovat do rozvoje infrastruktury a vzdělávání zaměstnanců v oblasti kybernetické bezpečnosti. Správní náklady na jednoho zaměstnance se snížily z 1 595 tis. Kč v roce 2019 na 1 413 tis. Kč v roce 2020. To může signalizovat zlepšenou efektivitu, ale je důležité sledovat, zda snižování nákladů nevede k omezení investic do IT bezpečnosti. Banka by měla také pravidelně sledovat a aktualizovat svou kybernetickou strategii v závislosti na vývoji technologií a potenciálních hrozbách.

### **3.2.2 What-if analýza**

Tato metoda byla zvolena, jelikož tento typ analýzy je užitečný pro identifikaci a hodnocení potenciálních dopadů rizik, což umožňuje připravit efektivní opatření. Oblastí zájmu what-if analýzy budou interní systémy banky, jelikož v matici rizik byly ohodnoceny nejvyšší mírou rizika, tedy RPN 25. Níže budou vypracovány tři scénáře, které by mohly nastat, pokud by se toto riziko projevilo. V tomto konkrétním případě bude blíže zkoumána situace, která souvisí s kybernetickým incidentem a chybou interního systému nastanou následující situace:

#### **Scénář č. 1: Co se stane, když dojde k chybě interního systému banky a dočasně nebudou dostupné její služby?**

- Může nastat frustrace a nespokojenost zákazníku z důvodu nedostupnosti služeb.
- Mohou nastat ztráty z obchodů a transakcí, které nemohou být provedeny během výpadku.
- V očích veřejnosti a zákazníků může dojít k poškození reputace a snížení důvěryhodnosti banky.

V rámci opatření tohoto krizového scénáře by bylo vhodné vytvořit plán kontinuity podnikání, který umožní rychlé obnovení služeb v případě výpadku. Tento plán by měl zahrnovat záložní servery, dodatečné zdroje energie a komunikační strategie pro informování zákazníků o situaci.

#### **Scénář č. 2: Co se stane, když dojde ke ztrátě dat z interního systému banky a chyba způsobí trvalé poškození nebo ztrátu dat?**

- Může nastat neschopnost obnovení historie transakcí nebo jiných bankovních záznamů.
- Dále finanční a právní komplikace z důsledku ztráty důležitých dat.
- Snížení důvěry zákazníků, když si uvědomí, že jejich finanční záznamy nejsou v bezpečí.

V rámci opatření je potřebné pravidelné zálohování dat na více lokacích, včetně off-site záloh. Je také nezbytné implementovat rychlý postup pro obnovení dat z těchto záloh v případě potřeby.

### **Scénář č. 3: Co se stane, když chyba v interním systému banky způsobí únik citlivých informací o zákaznících?**

- Může dojít ke ztrátě důvěry zákazníků v bezpečnostní postupy banky.
- Mohou vzniknout právní postihy a pokuty v důsledku porušení právních předpisů o ochraně dat.
- Může vzniknout Riziko finančních podvodů a zneužití uniklých informací nepřátelskými aktéry.

V rámci opatření je potřeba implementovat pokročilá bezpečnostní opatření, jako jsou šifrování, striktní řízení přístupových oprávnění, auditování přístupů k informacím, implementaci Data Leakage Prevention nástrojů či monitorování síťového provozu. Dále je potřeba vytvořit tým reagující na incidenty, který bude rychle reagovat na bezpečnostní hrozby a minimalizovat škody.

### **3.3 Identifikování krizových scénářů a plánů**

Proces tvorby krizových scénářů a plánování je klíčovým prvkem continuity podnikání a provozu v organizaci. Jeho cílem je minimalizovat dopady mimořádných situací na chod organizace a zajistit rychlé a efektivní řešení nečekaných událostí. V předchozích kapitolách byly na základě vybraných oblastí STEP analýzy identifikovány vnější vlivy, které přímo působí na činnost banky. Dílčím cílem této analýzy bylo stanovit hrozby a příležitosti, které mohou organizaci významně ovlivnit v budoucích aktivitách. Následně bude ohodnocena pravděpodobnost a dopad hrozeb. Pro rizika s nejvyšší mírou rizika týkající se kybernetických incidentů budou následně zpracovány krizové scénáře.

Pro krizové scénáře budou následně podrobně vypracovány krizové plány, které odpovídají konkrétním situacím. Krizový plán bude obsahovat konkrétní kroky a opatření, které by banka měla podniknout v případě vzniku krize, s cílem minimalizovat negativní dopady a co nejrychleji obnovit běžný chod a činnost organizace. Důraz bude kladen na efektivní komunikaci, koordinaci a spolupráci mezi všemi zainteresovanými stranami včetně zaměstnanců, vedení společnosti, zákazníků a dalších klíčových partnerů. Krizový plán by měl být srozumitelný, přístupný a pravidelně aktualizován, aby byl schopen efektivně reagovat na různé krizové situace. Následovat budou doporučení týkající se postupu v rámci možné implementace navržených scénářů a plánů.

V rámci výzkumu bylo zjištěno, že krizový scénář pro nedostupnost systému má banka vypracovaný velmi obecně, níže proto bude navržena rozšířená verze. Pro scénář č. 2, tedy co se stane, když chyba způsobí trvalé poškození nebo ztrátu dat, a scénář č. 3, tedy co se stane, když chyba v zabezpečení banky způsobí únik citlivých informací o zákaznících, připravené scénáře k dispozici nejsou. Tyto chybějící scénáře budou vypracovány v následující kapitole.

#### **3.3.1 Tvorba krizových scénářů**

V návaznosti na výše uvedené krizové scénáře bude podrobněji vypracován scénář „Nedostupnost – ztráta systému“, který je aktualizovanou verzí současného scénáře. Na základě výsledků matice rizik vyšla tato varianta jako nejpravděpodobnější a s nejvyšším rizikem. Dále budou vypracovány krizové scénáře „Ztráta dat v interním systému banky“ a „Únik citlivých informací o zákaznících“, které také spadají do kategorie kybernetických incidentů.

### 3.3.2 Krizový scénář č. 1 Nedostupnost – ztráta systému

Mobilní aplikace internetového bankovníctví „Banky X“ náhle přestane reagovat. Zákazníci nemohou přistupovat ke svým účtům, provádět transakce ani prověřovat své zůstatky. Mobilní aplikace internetového bankovníctví "Banky X" může čelit selhání v důsledku softwarových chyb, škodlivého software, kybernetických útoků, selhání serverů nebo přetížení systému způsobeného neočekávaným zvýšeným provozem. Nedostupnost mobilní aplikace by mohla vést k frustraci a nespokojenosti zákazníků, potenciálním finančním ztrátám kvůli zpožděním v transakcích a ztrátě důvěry v Banku X.

V případě nedostupnosti mobilní aplikace by někteří zákazníci zvolili jiný způsob komunikace s bankou, čímž by mohlo dojít k přetížení pobočkové sítě, internetové aplikace či zákaznických telefonních linek. Celý problém by tak mohl vést k dominovému efektu a paralýze interních bankovních systémů.

První hodiny po detekci problému jsou klíčové pro identifikaci a hodnocení rozsahu problému. Během následujících 4–6 hodin je důraz kladen na rychlé nalezení řešení. V následujících 24 hodinách je možné aktivovat nouzové plány a komunikovat s uživateli aplikace. Plná obnova může trvat i několik dní, v závislosti na závažnosti problému.

Banka X implementovala robustní bezpečnostní postupy, pravidelné testování zátěže, monitoring aplikace a pravidelné zálohování dat. Jakmile je detekován problém s mobilní aplikací, krizový tým Banky X je okamžitě aktivován. Prioritou je identifikace problému, následně komunikace s uživateli a implementace potřebných opravných kroků. Paralelně se provádějí kroky k obnově plné funkčnosti aplikace.

Manažer IT oddělení má pravomoc rozhodovat o technických aspektech řešení problému. Oddělení zákaznické podpory je zodpovědné za komunikaci s uživateli, zatímco CEO má konečné slovo v otázkách týkajících se vnější komunikace a strategie obnovy.

#### Návrh krizového plánu pro krizový scénář č. 1 Nedostupnost – ztráta systému

V této části bude na základě popisu krizového scénáře „Nedostupnost – ztráta systému“ vytvořen krizový plán. Během tvoření tohoto krizového plánu budou aplikovány poznatky z teorie. Krizový plán bude navržen tak, aby splňoval veškeré atributy, které by tento dokument měl obsahovat, viz kapitola v teoretické části pod názvem „Plánování a struktura krizových plánů.“

#### Předpoklad

Mobilní aplikace internetového bankovníctví „Banky X“ je nedostupná po dobu několika hodin během hlavního provozního času, což může mít dopad na zákazníky, provoz a také finanční výsledky.

#### Detekce

- Detekce anomálií v provozu a dostupnosti systému.
- Prvotní nahlášení incidentu klíčovými stakeholdery, množí se hovory na zákaznické lince.
- Stanovení důvodného podezření na externí nebo interní příčinu výpadku.

#### Analýza a klasifikace

- Sestavení krizového týmu pro analýzu a reakci.
- Stanovení rozsahu, dopadu a časového odhadu obnovy.
- Aktualizace informací o dopadu na data, systémy a uživatele.

### **Plán reakce**

- Registrace incidentu v interních systémech.
- Přezkoumání a konsolidace shromážděných informací.
- Vytvoření plánu komunikace s interními a externími stranami.
- Identifikace a plánování krátkodobých a dlouhodobých řešení.
- Kontaktování klíčových dodavatelů zasažených systémů.

### **Komunikace**

- Komunikace s interními týmy, partnery a zákazníky o stavu a očekávaném čase obnovení.
- Nutná komunikace s regulačními úřady nebo dalšími relevantními institucemi (NÚKIB, ČNB).

### **Zvládnutí incidentu**

- Aktivace nouzových a kontingenčních plánů.
- Izolace postižených systémů a implementace krátkodobých (workaround) nápravných opatření.
- Kontinuální monitorování a aktualizace postupů na základě nově získaných informací.

### **Obnova**

- Postupné obnovení funkčnosti systému ze záloh.
- Ověření funkčnosti a bezpečnosti před plným nasazením do provozu.
- Monitorování systému po obnovení pro identifikaci potenciálních problémů.

### **Post-mortem**

- Hodnocení celkového dopadu incidentu.
- Analýza příčin incidentu a vyvození závěrů.
- Aktualizace interních postupů a směrnic na základě získaných zkušeností.

### **Kontinuálně**

- Udržování databáze incidentů pro budoucí referenci a analýzu.
- Aktualizace postupů a školení týmu na základě získaných zkušeností.

### **3.3.3 Krizový scénář č. 2 Ztráta dat v interním systému banky**

Tento scénář popisuje situaci, kdy banka ztratí přístup ke svým datům kvůli technickým, softwarovým, nebo hardwarovým selháním, aniž by tato data byla vystavena vnější hrozbě. Scénář se spouští, když je zjištěno, že kritická data byla poškozena, smazána nebo jinak ztracena bez možnosti obnovy ze zálohy v předem definovaném časovém rámci.

Co se týče důsledků, mohou být následky těchto krizových situací závažné. Ztráta kritických dat, dočasné zastavení bankovních operací, ztráta důvěry zákazníků a potenciální finanční ztráty či pokuty za nedodržení regulačních standardů byly identifikovány jako hlavní důsledky.

První hodiny po detekci krize jsou věnovány identifikaci problému. V následujících 4–6 hodinách jsou vyvíjeny snahy o rychlou obnovu. Během následujících 24 hodin je prováděna implementace nouzových plánů a komunikace s veřejností, a během následujícího týdne se usiluje o kompletní obnovu a návrat k normálnímu provozu.

K snížení možnosti výskytu krize a jejího dopadu byla navržena některá opatření. Mezi tato opatření patří pravidelné zálohování dat, mandatorní zaznamenávání všech provedených transakcí do logů, kontrolní mechanismy pro aktualizace software, pravidelné testování a revize krizových plánů a školení zaměstnanců v oblasti IT bezpečnosti.

V případě krize byl navržen konkrétní postup: aktivace krizového týmu, detekce a analýza problému, rychlá komunikace s veřejností, pokus o rychlou obnovu dat, implementace dočasných řešení, a nakonec kompletní obnovu a návrat k normálnímu provozu.

Manažerské pravomoci a odpovědnosti byly také definovány. Manažerovi IT oddělení byla udělena pravomoc rozhodnout o postupech technického řešení, zatímco CEO byla udělena pravomoc schválit veškerou komunikaci s veřejností a rozhodnout o dalším postupu. Oddělení PR a komunikace má odpovědnost za správnou informaci veřejnosti a CFO má odpovědnost za finanční aspekty řešení krize.

## **Návrh krizového plánu pro scénář č. 2 Ztráta dat v interním systému banky**

### **Detekce**

- Prvotní nahlášení: Zajišťuje IT tým okamžitě po zjištění ztráty dat. Komunikace probíhá prostřednictvím interního komunikačního kanálu, např. e-mail nebo telefon.
- Analyzovat předchozí a aktuální události: Prohledání logů a hlášení pro indikátory možného útoku nebo selhání.
- Hrubý popis podezření: Vytvoření časové osy událostí a formulace hypotéz o možném zdroji a cíli útoku.
- Odhad typu incidentu: Určení, zda se jedná o bezpečnostní incident (tzn. skutečné narušení bezpečnosti banky, např. kybernetický útok) nebo bezpečnostní událost (tzn. nemá reálný dopad na bezpečnost banky, např. technická chyba).

### **Analýza a klasifikace**

- Vybrat team pro investigaci: IT bezpečnostní tým a případně externí specialisté.
- Stanovit rozsah a časový odhad: Určit, které systémy a logy jsou postiženy, kdy byla data naposledy v pořádku, které systémy budou detailně zkoumány.
- Aktualizace informací: Na základě získaných informací upravovat hypotézy a odhady.

### **Plán reakce**

- Revidovat informace: Sestavit a shrnout získané informace.
- Připravit plán komunikace: Vytvořit strategii pro informování všech zainteresovaných stran, včetně zákazníků, zaměstnanců a regulatorních orgánů.
- Stanovit plán řešení: Včetně nouzových, dočasných i trvalých opatření.

### **Komunikace**

- Odsouhlasit plán komunikace: Schválení vrcholovým managementem.
- Informovat příslušné úřady: Podle regulatorních požadavků.
- Informovat zasažené strany: Zákazníci, partneři a další zainteresované strany.

### **Zvládnutí incidentu**

- Úvodní zásah: Zaměření na okamžité řešení problému.
- V případě kybernetického útoku izolace nakažených zařízení: Zajištění, aby incident dále nešířil. Reimaging infikovaných systémů: Kompletní obnova pevných disků.
- Implementace nouzových a dočasných opatření: Rekonstrukce transakcí či obnova ze zálohy.

### **Obnova**

- Obnovit data a systémy: Pomocí posledních funkčních záloh.
- Testování a monitorování: Zajištění, že systémy fungují správně a bezpečně.

### **Post-mortem**

- Vyčíslit škody a náklady: Stanovit finanční a reputační dopad.
- Vyhodnocení: Jak dobře se banka vypořádala s incidentem a co lze zlepšit.
- Zpráva o incidentu: Vytvoření oficiálního dokumentu o incidentu pro interní i externí použití.

### **Kontinuálně**

- Vedení záznamů: Uchování veškerých relevantních informací pro budoucí referenci a jako učební příležitost pro banku.

### **3.3.4 Krizový scénář č. 3 Únik citlivých informací o zákaznících**

Tato situace představuje scénář, kdy osobní a finanční údaje zákazníků uniknou z interního systému banky a dostanou se do rukou neoprávněných osob nebo veřejnosti, což může ohrozit soukromí zákazníků a reputaci banky. Scénář se aktivuje ihned po zjištění úniku citlivých informací o zákaznících. Únik citlivých informací může vést k finančním ztrátám pro zákazníky a banku, ztrátě důvěry zákazníků v banku, možným právním postihům a dlouhodobému poškození reputace Banky X.

Bezprostřední reakce v prvních hodinách po detekci je kritická pro minimalizaci škody. Během následujících 4–6 hodin je důraz kladen na identifikaci zdroje úniku a zajištění dat. V následujících 24 hodinách může být nezbytné informovat zákazníky, regulační orgány a veřejnost.

Banka X zavedla víceúrovňová bezpečnostní opatření, pravidelné školení zaměstnanců, audit bezpečnostních postupů a postupy pro rychlé reagování na bezpečnostní incidenty. Po detekci úniku je okamžitě aktivován krizový tým Banky X. Je provedena analýza rozsahu úniku, identifikace postižených zákazníků a přijata opatření k zajištění dalších dat. Současně je zahájena komunikace s postiženými zákazníky a veřejností, a jsou přijata opatření k nápravě situace.

Manažer bezpečnostního týmu má pravomoc rozhodovat o technických krocích potřebných k zajištění dat. Oddělení PR je zodpovědné za komunikaci s veřejností, zatímco CEO má konečné slovo v otázkách týkajících se vnější komunikace a strategie nápravy. Manažer oddělení zákaznického servisu koordinuje komunikaci s postiženými zákazníky.

### **Návrh krizového plánu pro scénář č. 3 Únik citlivých informací o zákaznících**

#### **Detekce**

1. Prvotní nahlášení: Zodpovědný zaměstnanec by měl okamžitě hlásit podezření na únik prostřednictvím interního bezpečnostního portálu a na lince pro hlášení incidentů. Toto by mělo být provedeno neprodleně po zjištění incidentu.
2. Analyzovat předchozí události: Zkontrolovat hlášení a varování v bezpečnostních nástrojích banky za poslední období, zda neexistují dřívější indikátory útoku.
3. Analyzovat aktuální události: Zhodnotit aktuální stav IT systému a porovnat s normálním chodem, pro identifikaci neobvyklých aktivit.
4. Vytvořit hrubý popis: Založit časovou osu posledních událostí, vytvořit hypotézu o možném zdroji a cíli úniku dat.
5. Odhadnout charakter události: Určit, zda se jedná o bezpečnostní incident (útok byl úspěšný) nebo pouze o bezpečnostní událost (pouze pokus o útok).

#### **Analýza a klasifikace**

1. Tým pro úvodní investigaci: Rychle vybrat členy interního IT a bezpečnostního týmu pro detailní analýzu.
2. Stanovit prvotní rozsah: Zaměřit se na hlavní systémy, které mohou být ohroženy, a zkontrolovat relevantní logy a důkazy.
3. Aktualizace informací: Průběžně aktualizovat informace podle vývoje situace, modifikovat rozsah analýzy a odhadnout dopad.



4. Typ a dopad útoku: Na základě analýzy určit typ úniku, jeho dopad na data, systémy a uživatele a odhadnout potenciální ztráty.
5. Prioritizace: Na základě závažnosti a dopadu incidentu určit prioritu a eskalační úroveň.
6. Revidování rozhodnutí: Na základě nových informací přehodnotit, zda se jedná o bezpečnostní incident nebo událost.

### **Plán reakce**

1. Konsolidace informací: Sestavit veškeré zjištěné informace a reporty do jednotného dokumentu.
2. Registrovat incident: Formálně zaregistrovat incident v interním systému pro správu incidentů.
3. Plán komunikace: Vytvořit plán komunikace s jasnými pokyny k tomu, kdo má být informován, kdy, jak často a prostřednictvím jakých komunikačních kanálů.
4. Stanovit řešení: Identifikovat nezbytná nouzová a dočasná řešení a stanovit časový plán pro jejich realizaci.

### **Komunikace**

1. Odsouhlasit plán: Plán komunikace by měl být rychle odsouhlasen vrcholovým vedením banky.
2. Nahlášení: Co nejdříve informovat příslušné orgány, zasažené strany a veřejnost podle potřeby.
3. Zvládnání incidentu: Vytvořit jasný plán kroků k řešení incidentu, včetně obnovy postižených systémů a dat.

### **Obnova**

1. Návrat k normálnímu provozu: Po zvládnutí incidentu obnovit postižené systémy a data, provést testy a průběžně monitorovat systémy, aby bylo zjištěno, zda bylo vše úspěšně odstraněno.

### **Post-mortem**

1. Hodnocení: Vyhodnotit, jak byl incident zvládnut, určit příčiny a dopady a vytvořit zprávu o incidentu.
2. Závěrečné schůzky: Uspořádat schůzky s týmem pro vyhodnocení a stanovení dalších kroků.

### **Kontinuálně**

1. Vedení záznamů: Udržovat průběžné záznamy o všech incidentech a jejich řešení, pro lepší připravenost na budoucí incidenty.

## **3.4 Doporučení**

Před zahájením jakýchkoliv testovacích aktivit by měly být všechny scénáře pečlivě prozkoumány, schváleny managementem a následně sdíleny v rámci organizace. Tímto způsobem bude zabezpečeno, že všechny scénáře jsou relevantní a reflektují skutečné hrozby a rizika. Scénáře by měly být testovány buď teoreticky (table-top cvičení), nebo prakticky (skutečná simulace krizové situace). Toto testování pomůže zjistit, jak efektivní jsou výše vypracované postupy v reálných situacích. Testování pomůže ověřit kvalitu procesů a také

funguje jako nástroj vzdělávání pro všechny zainteresované strany. Četnost těchto simulací připraví zaměstnance na to lépe reagovat na skutečné incidenty. Po každém testu by měla být provedena důkladná analýza, která zhodnotí efektivitu postupů, dobu reakce a celkovou kvalitu reakce. Na základě této zpětné vazby mohou být postupy upraveny. Na základě výsledků testování by mělo být jasné, zda doporučené scénáře a postupy odpovídají aktuálním potřebám a požadavkům oblasti řízení rizik v bankovním sektoru. Pokud je to žádoucí, měly by být provedeny nezbytné úpravy a implementace nových opatření, a to v rámci zachování aktuálnosti a připravenosti na budoucí hrozby. V rámci kontinuálního zlepšování by testování a analýza měly být prováděny pravidelně, aby se zajistilo, že navržené postupy jsou stále aktuální a odpovídají měnícím se okolnostem. Tímto způsobem bude zajištěno, že reakce na budoucí incidenty bude vždy optimální.

### **3.5 Zhodnocení stavu připravenosti**

Banka X má v současné době solidní přístup k připravenosti na kritická rizika. Byl vypracován komplexní plán kontinuity podnikání, s důrazem na IT oblast díky existenci plánu obnovy po havárii (DRP), který je pravidelně aktualizován a reflektuje technologické a organizační změny. Tento plán pečlivě zpracovává jak obnovu IT systémů po krizových situacích, tak i specifické postupy při přechodech mezi různými datovými centry.

Dále banka investuje do pravidelných školení zaměstnanců a simulací krizových situací. Toto vše zajišťuje kooperativní spolupráci mezi odděleními a kontinuální revizi plánů, aby byla zajištěna jejich aktuálnost a relevance v měnícím se prostředí.

Nicméně i přes výše zmíněné kroky existují oblasti, kde je možné identifikovat prostor pro zlepšení. Zejména je důležité zaměřit se na konkrétnější a podrobnější krizové scénáře, zejména v oblasti kybernetické bezpečnosti, kde byly identifikovány konkrétní mezery. Toto je v souladu s obecným doporučením, že proces tvorby, testování a revize krizových scénářů je klíčový pro kontinuitu podnikání a provozu.

Pro úplnost je nezbytné pravidelně testovat krizové scénáře a plány, a to jak teoreticky, tak prakticky, a provádět jejich důkladné vyhodnocení. To zajistí, že všechny postupy jsou aktuální, efektivní a odpovídají reálným potřebám banky v kontextu řízení rizik.

## 4 Závěr

Tato diplomová práce se zaměřila na problematiku řízení rizik a krizového řízení ve finančním sektoru, konkrétně v organizaci „Banka X“. Cílem práce bylo identifikovat a ohodnotit rizika, ke kterým dochází při provozu banky, a na základě těchto informací posoudit míru připravenosti na jejich působení. V teoretické části práce byla provedena literární rešerše, která poskytla potřebné teoretické pozadí pro praktickou část práce. První kapitola se věnovala oblasti řízení rizik. Nejprve byl popsán koncept a definice řízení rizik, poté byly vymezeny základní pojmy v této oblasti. V další podkapitole byly představeny koncepty a principy Enterprise Risk Managementu a Business Continuity Managementu, které se při řízení rizik často používají. Obsáhlou kapitolou je proces řízení rizik a jeho jednotlivé fáze.

V další kapitole byl popsán koncept krizového řízení. Bylo definováno, co je krize a byly zde představeny různé typy krizí. Následuje popis různých fází krizového řízení a jejich význam. Jako další navazují různé strategie pro krizové řízení a dále bylo vysvětleno, co je krizová komunikace a proč je důležitá. Následující podkapitola popsala roli centrální banky v řízení krizí ve finančním sektoru. Rovněž byly popsány krizové scénáře a plány, postup tvorby krizových scénářů a jak plánovat a strukturovat krizové plány. Teoreticko-metodologickou část uzavírá kapitola týkající se metodiky.

Praktická část byla provedena na základě analýzy primárních zdrojů, zejména kvalitativního výzkumu v rámci polostrukturovaných rozhovorů a brainstormingu s vybranými manažery banky. V první kapitole praktické části práce byla představena organizace, její současný stav a organizační struktura. V další kapitole byla provedena analýza vnějšího prostředí banky pomocí STEP analýzy, která zahrnuje sociální, technicko-technologické, ekonomické a politické faktory. Pro potřeby této diplomové práce byl detailně zpracován sociální, technologický a ekonomický faktor. Na základě toho byly identifikovány příležitosti a hrozby, které mohou ovlivňovat fungování banky a její odolnost vůči různým rizikům. Bylo zjištěno, že banka je vystavena různým vnějším hrozbám, jako jsou ekonomické výkyvy, politická nestabilita, technologický pokrok a změny v přístupu společnosti k finančním institucím v rámci digitalizace služeb. Tyto hrozby byly následně ohodnoceny v rámci brainstormingu s vybranými manažery banky. Tímto bylo možné určit nejkritičtější rizika.

Bylo zjištěno, že nejkritičtější riziko pro banku představují rizika spojená s kybernetickou bezpečností, rizikem snížení solvence klientů kvůli ekonomické nestabilitě, ztráta tržního podílu kvůli konkurenci a finanční ztráty kvůli ekonomické nejistotě. Pro tato rizika byla vypracována opatření, která by měla přispět k jejich minimalizaci.

Krizové scénáře byly vypracovány na základě vybraného rizika s nejvyšší mírou dopadu a pravděpodobnosti. Tyto scénáře popisují konkrétní průběh kritické situace. Navazuje vyhotovení krizových plánů, který poskytují postupné instrukce a doporučené kroky k řešení krizových situací.

Z výsledků analýzy a doporučení plyne, že ačkoli má „Banka X“ robustní přístup k připravenosti a řízení rizik, neustálý vývoj v oblasti kybernetických hrozeb a měnící se vnější faktory zdůrazňují potřebu pravidelné revize, testování a adaptace jejích postupů, aby zůstala na špičce v oblasti řízení rizik a krizového řízení.

Jako omezení práce je vnímána skutečnost, že byla provedena pouze na jedné bance, a tak nemůže být považována za kompletní a vyčerpávající. V budoucnu by bylo vhodné rozšířit vzorek a provedení analýz na další finanční instituce a srovnat výsledky.

# Literatura

## Monografie

AGNES, M. *Crisis Ready: Building an Invincible Brand in an Uncertain World*. Herndon: Mascot Books, 2018. 288 s. ISBN 978-1-68401-413-2.

AKINFENWA, A. *Risk Assessment: An in depth guide to principles, methods, best practices, and interview questions and answers*. Unknown: Absolute Author Publishing House, 2023. 34 s. ISBN 978-1649537539.

ALI M. Z., JOHN S., J. *Risk Management Key Notes:1*. Unknown: Independently Published, 2020, 62 s. ISBN 979-8713939052.

ANTUŠÁK, E., VILÁŠEK, J. *Základy teorie krizového managementu*. 1.vyd. Praha: Karolinum, 2016. 134 s. ISBN 978-80-246-3443-2.

BALOG, M., IAKOVETS A. *Risk management: theory, background, practice*. Prague: Leges, 2020. 135 s. ISBN 978-80-7502-463-3.

BEDNÁŘ, V. *Vedení v krizi: jak zvládnout zaměstnance v nesnadných časech*. Praha: Management Press, 2022. 240 s. ISBN 978-80-7261-592-6.

BEVOC, S. *Office Management, Operations Management, Crisis Management, and Project Management in Organizations*. Troy: NutriNiche Systém Llc, 2016. 61 s. ISBN 978-1519057686.

CALDER, A. *ISO 22301:2019 and business continuity management – Understand how to plan, implement and enhance a business continuity management system (BCMS)*. Cambridgeshire: IT Governance Publishing Ltd, 2021. 154 s. ISBN 978-1-78778-299-0.

CANE, P. *Product Harm Management: How to Lead a Company during Crisis*. Unknown: Independently published, 2019. 110 s. ISBN 978-1707455348.

COPELLO, F. *Internal Controls – A Practical View: An uncomplicated and objective guide to risk management*. Passo: Porto Alegre, 2019. 96 s. ISBN 978-85-5996-929-130.

CRANDALL, W. R., PARNELL, J. A., SPILLAN, J. E., *Crisis Management: Leading in the New Strategy Landscape*. 2nd Edition. Los Angeles: SAGE Publications, Inc., 2014. 384 s. ISBN 978-1412991681.

DARE, N. *Leadership Sustainability – Crisis and Emergency Management : How To Prepare Your Business To Survive Any Crisis*. Unknown: Independently Published. 2022. 51 s. ISBN 9798413822067.

FOTR, J., HNILICA J. *Aplikovaná analýza rizika ve finančním managementu a investičním rozhodování*. 2., aktualiz. a rozš. vyd. Praha: Grada, 2014. 304 s. ISBN 978-80-247-5104-7.

FOTR, J., VACÍK, E., SOUČEK I., ŠPAČEK M., HÁJEK S. *Tvorba strategie a strategické plánování: teorie a praxe. 2.*, aktualizované a doplněné vydání. Praha: Grada Publishing, 2020. 416 s. ISBN 978-80-271-2499-2.

FRASER J. R. S., QUAIL R., SIMKINS, B. *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*, 2nd edition. Hoboken: Wiley, 2021. 944 s. ISBN 978-1119741480.

GEARY, J. *How to be a Chief Risk Officer: A handbook for the modern CRO*. Seattle: Kindle Direct Publishing, 2022. 242 s. ISBN 978-1-9997683-3-1.

GOZORA, V. *Krizový manažment podniku*. Praha: Wolters Kluwer, 2017. 184 s. ISBN 978-80-7552-805-6.

HARAZIN, L. et al. *Modelové scénáře pro vybrané zátěžové situace: Model scenarios for selected stress situations: monografie*. Praha: Policejní akademie České republiky v Praze. 2018. 312 s. ISBN 978-80-7251-489-2.

HEMUS, J. *Crisis Proof: How to prepare for the worst day of your business life*. Yarmouth: Rethink Press, 2020. 268 s. ISBN 978-1781335109.

KARLÍČEK, M. *Marketingová komunikace: jak komunikovat na našem trhu. 2.*, aktualizované a doplněné vydání. Praha: Grada Publishing, 2016. 224 s. ISBN 978-80-247-5769-8.

KOLOUCH, J. BAŠTA, P. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. 560 s. ISBN 978-80-88168-31-7.

MARKS, N. *Risk Management for Success*. Unknown: Independently published, 2020. 183 s. ISBN 979-8692068781.

MURRAY, M.L. *Prepared Leadership, Amazing Crisis Management and Emergency Planning*. Unknown: Independently published, 2022. 63 s. ISBN 979-8356246661.

MYŠKOVÁ, R. *Analytické přístupy pro podporu řízení podniku*. Brno: Akademické nakladatelství CERM, 2022. 134 s. ISBN 978-80-7623-093-4.

OLAFSSON, G. R., *The Crisis Leader: The Art of Leadership in Times of Crisis*. 2nd edition. Chicago: Lorien Consulting, 2013. 178 s. ISBN 978-1499217032.

OŠKRDAL, V., DOUCEK, P. *Praktické řízení ICT projektů*. Praha: Oeconomica, nakladatelství VŠE, 2014. 255 s. ISBN 978-80-245-2073-5.

PAULA, D. *Principles of Risk Management: A Practical Introduction to Managing Risk | For Beginners*. Unknown: Independently Published, 2023. 87 s. ISBN: 979-8375286143.

PŘIKRYLOVÁ, J. *Moderní marketingová komunikace. 2.*, zcela přepracované vydání. Praha: Grada Publishing, 2019. 344 s. ISBN 978-80-271-0787-2.

ROBERTSON, J. *Executing crisis: a C-suite crisis leadership survival guide*. Brookfield, Connecticut: Rothstein Publishing, 2020. 270 s. ISBN 978-1-944480-64-6.

ROLÍNEK, L. *Krize malých a středních podniků, příčiny a jejich řešení*. Praha: Wolters Kluwer, 2016. 152 s. ISBN 978-80-7552-448-5.

RUBENS, D. *Strategic Risk and Crisis Management: A Handbook for Modelling and Managing Complex Risks*. 1st Edition. Unknown: Kogan Page, 2023. 352 s. ISBN 978-1398609754.

SHAYB, H. A. *Enterprise Crisis Management*. Independently Published. Israel: Independently Published, 2021. 416 s. ISBN 978-9655998139.

SHUAIB, Y.A. *Award-winning crisis communication strategies*. Abuja: Image Merchants Promotions Limited, 2020. 186 s. ISBN 9789770499.

SMEJKAL, V., RAIS K. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013. 488 s. ISBN 978-80-247-4644-9.

SMITH, P., G. MERRIT, G., M. *Proactive Risk Management: Controlling Uncertainty in Product Development*. New York: Productivity Press, 2020. 256 s. ISBN 9780367807542.

SOBIA, P. *Learn Risk Analysis & Evaluation from A to Z: Became An Expert of the Fundamental Techniques and Tools in Risk Management*. Unknown: Independently Published, 2022. 79 s. ISBN 979-8370721830.

TOMANDL, J. ČUŘÍK, J. MARŠOVSKÁ, K., FOJTOVÁ, T. *Krizová komunikace: principy – zkušenosti – postupy*. Brno: Masarykova univerzita, 2020. 220 s. ISBN 978-80-210-9636-3.

VÁCHAL, J., VOCHOZKA M. *Podnikové řízení*. Praha: Grada, 2013. 688 s. ISBN 978-80-247-4642-5.

VÁVROVÁ, E. *Finanční řízení komerčních pojišťoven*. 1. vyd. Praha: Grada Publishing, 2014. 190 s. 5627. ISBN 978-80-247-4662-3.

WHEELER, A. *Crisis Communications (PRCA Practice Guides)*. Bingley: Emerald Publishing Limited, 2019. 152 s. ISBN 978-1787566187.

WILLIE, J. *Crisis management in organizations*. Unknown: Independently published, 2023. 80 s. ISBN 979-8376706077.

### **Odborné časopisy**

COOMBS, W. T., LAUFER D. Global Crisis Management – Current Research and Future Directions. *Journal of International Management*, vol. 24, issue 3, p. 199-203. DOI <https://doi.org/10.1016/j.intman.2017.12.003>.

ERIKSSON, K. Organisational learning without fire? Risk analyses as a basis for developing crisis management capabilities. *Safety Science*, 2023, vol. 163. DOI <https://doi.org/10.1016/j.ssci.2023.106144>.



LIMA, P. F. A., CREMA M., VERBANO C., Risk management in SMEs: A systematic literature review and future directions. *European Management Journal*, 2020, vol. 38, Issue 1, p. 78-94. DOI <https://doi.org/10.1016/j.emj.2019.06.005> .

MACHADO, P. G., RIBIERO, C. D., NASCIMENTO, C. A. O. Risk analysis in energy projects using Bayesian networks: A systematic review. *Energy Strategy Reviews*, 2023, vol. 47. DOI <https://doi.org/10.1016/j.esr.2023.101097>.

MALDONADO, T., VERA, D. Leadership skills for international crises: The role of cultural intelligence and improvisation. *Organizational Dynamics*, 2014, vol. 43, issue 4, p. 257-265. DOI <https://doi.org/10.1016/j.orgdyn.2014.09.002> .

THANI, F. B. H. A., OBEIDAT, A. M. The Impact of Strategic Leadership on Crisis Management, *International Journal of Asian Social Science*, 2020, 10(6), pp. 307–326. DOI 10.18488/journal.1.2020.106.307.326.

TOKASIS, V., POLYCHRONIOU, P., BOUSTRAS, G. Crisis management in public administration: The three phases model for safety incidents. *Safety Science*, 2019, vol. 113, p. 37-43. DOI <https://doi.org/10.1016/j.ssci.2018.11.013>.

WONG, W. N. Z. Transforming corporate performance: A business continuity management approach. *Organizational Dynamics*, 2019, vol. 48, Issue 2, p. 29-36. DOI <https://doi.org/10.1016/j.orgdyn.2018.08.004>.

YUN, J. The effect of enterprise risk management on corporate risk management. *Finance Research Letters*, 2023, vol. 55, Part B. DOI <https://doi.org/10.1016/j.frl.2023.103950>.

ZHU, D., LI, Z., MISHRA, A.R., Evaluation of the critical success factors of dynamic enterprise risk management in manufacturing SMEs using an integrated fuzzy decision-making model. *Technological Forecasting and Social Change*, 2023, vol. 186, Part A. DOI <https://doi.org/10.1016/j.techfore.2022.122137>.

## Normy

ČSN ISO 31000 (01 0351). Management rizik-směrnice. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2018.

## Internetové zdroje

ALEXANDER, A. Business Continuity Management Process. *Amazon.com* [online]. 2018 [cit. 2023-08-27]. Dostupný z WWW: [https://www.amazon.com/Business-Continuity-Management-Process-Alexander-ebook/dp/B07F5GDKBT#detailBullets\\_feature\\_div](https://www.amazon.com/Business-Continuity-Management-Process-Alexander-ebook/dp/B07F5GDKBT#detailBullets_feature_div).

BANKY.CZ. Přehled Banky X. *Banky.cz* [online]. 2023 [cit. 2023-08-27]. Dostupný z WWW: <https://www.banky.cz/BankaX>.

BANKY.CZ. Ruské sankce a banky Sberbank, Expo bank – co to znamená pro vaše osobní finance? *Banky.cz* [online]. 2022 [cit. 2023-08-27]. Dostupný z WWW:

<https://www.banky.cz/clanky/ruske-sankce-a-banky-sberbank-expo-bank-co-to-znamenapro-vase-osobni-finance/>.

CZECH NATIONAL BANK. Annual report of the Czech national bank 2022. *Cnb.cz* [online]. 2022 [cit. 2023-08-27]. Dostupný z WWW: [https://www.cnb.cz/export/sites/cnb/en/about\\_cnb/.galleries/performance/annual\\_reports/download/vz\\_2022\\_en.pdf](https://www.cnb.cz/export/sites/cnb/en/about_cnb/.galleries/performance/annual_reports/download/vz_2022_en.pdf).

ČESKÁ NÁRODNÍ BANKA. Co opatření ČNB vůči Sberbank CZ znamená? *Cnb.cz* [online]. 2022 [cit. 2023-08-27]. Dostupný z WWW: <https://www.cnb.cz/cs/casto-kladene-dotazy/Co-opatreni-CNB-vuci-Sberbank-CZ-znamenat/>.

ČESKÁ NÁRODNÍ BANKA. ČNB zahájila kroky k odejmutí licence Sberbank CZ. *Cnb.cz* [online]. 2022 [cit. 2023-08-27]. Dostupný z WWW: <https://www.cnb.cz/cs/cnb-news/tiskove-zpravy/CNB-zahajila-kroky-k-odejmuti-licence-Sberbank-CZ/>.

ČESKÁ NÁRODNÍ BANKA. Prognóza ČNB-léto 2023. *Cnb.cz* [online]. 2023 [cit. 2023-08-27]. Dostupný z WWW: <https://www.cnb.cz/cs/menova-politika/prognoza/>.

ČESKÁ NÁRODNÍ BANKA. Tvorba plánů pro řešení krize. *Cnb.cz* [online]. 2023 [cit. 2023-08-27]. Dostupný z WWW: <https://www.cnb.cz/cs/reseni-krize-na-ft/tvorba-planu-pro-reseni-krize/>.

ČESKÁ NÁRODNÍ BANKA. Zajištění kontinuity zpracování při krizových situacích. *Cnb.cz* [online]. 2023 [cit. 2023-08-27]. Dostupný z WWW: <https://www.cnb.cz/cs/financni-trhy/skd/zajisteni-kontinuity-zpracovani-pri-krizovych-situacich/>.

ČESKÝ STATISTICKÝ ÚŘAD. Hlavní makroekonomické ukazatele. *Cnb.cz* [online]. 2023 [cit. 2023-08-27]. Dostupný z WWW: [https://www.czso.cz/csu/czso/hmu\\_cr](https://www.czso.cz/csu/czso/hmu_cr).

ČESKÝ STATISTICKÝ ÚŘAD. Informační technologie. *Czso.cz* [online]. 2023 [cit. 2023-08-27]. Dostupný z WWW: [https://www.czso.cz/documents/10180/150808213/3202032106\\_inf.pdf/e9954f37-ef16-4abd-b29e-a4fe98c5f118?version=1.3](https://www.czso.cz/documents/10180/150808213/3202032106_inf.pdf/e9954f37-ef16-4abd-b29e-a4fe98c5f118?version=1.3).

ČESKÝ STATISTICKÝ ÚŘAD. Míry zaměstnanosti, nezaměstnanosti a ekonomické aktivity – květen 2023. *Czso.cz* [online]. 2023 [cit. 2023-08-27]. Dostupný z WWW: <https://www.czso.cz/csu/czso/cris/miry-zamestnanosti-nezamestnanosti-a-ekonomicke-aktivity-kveten-2023>.

ČESKÝ STATISTICKÝ ÚŘAD. Míry zaměstnanosti, nezaměstnanosti a ekonomické aktivity - únor 2023. *Czso.cz* [online]. 2023 [cit. 2023-08-27]. Dostupný z WWW: <https://www.czso.cz/csu/czso/cris/miry-zamestnanosti-nezamestnanosti-a-ekonomicke-aktivity-unor-2023>.



ČESKÝ STATISTICKÝ ÚŘAD. Používání internetového bankovníctví a jiných finančních služeb. *Czso.cz* [online]. 2022 [cit. 2023-08-27]. Dostupný z WWW: <https://www.czso.cz/csu/czso/11-pouzivani-internetoveho-bankovnictvi-a-jinych-financnich-sluzeb-pd3xgddjzf>.

DEUSCHEL, R. All About Crisis Management: How To Create And Maintain An Effective Crisis Management Programme. *Amazon.com* [online]. 2021 [cit. 2023-08-27]. Dostupný z WWW: <https://shorturl.at/rsEMU>.

DUMITRASCU, S. Risk Management: A Practical Guide (Advance Book 6). *Amazon.com* [online]. 2018 [cit. 2023-08-27]. Dostupný z WWW: <https://shorturl.at/koAJ3>.

ELLIOT, D. W. What's the Plan?: An introduction to Business Continuity Planning (Forward Looking Guides). *Amazon.com* [online]. 2020 [cit. 2023-08-27]. Dostupný z WWW: <https://shorturl.at/glpUW>.

EVROPSKÁ CENTRÁLNÍ BANKA BANKOVNÍ DOHLED. Priority SSM v oblasti dohledu na období 2023–2025. *Bankingsupervision.europa.eu* [online]. 2022 [cit. 2023-08-27]. Dostupný z WWW: [https://www.bankingsupervision.europa.eu/banking/priorities/html/ssm.supervisory\\_priorities\\_202212~3a1e609cf8.cs.html](https://www.bankingsupervision.europa.eu/banking/priorities/html/ssm.supervisory_priorities_202212~3a1e609cf8.cs.html).

EVROPSKÁ CENTRÁLNÍ BANKA EUROSISTÉM. Makroekonomické projekce, shrnutí. *Ecb.europa.eu* [online]. 2022 [cit. 2023-08-27]. Dostupný z WWW: [https://www.ecb.europa.eu/pub/projections/html/ecb.projections202206\\_eurosystemstaff~2299e41f1e.cs.html](https://www.ecb.europa.eu/pub/projections/html/ecb.projections202206_eurosystemstaff~2299e41f1e.cs.html).

GARTNER PEER INSIGHTS. What are IRM (Integrated Risk Management) Solutions? *Gartner.com* [online]. 2023 [cit. 2023-08-27]. Dostupný z WWW: <https://www.gartner.com/reviews/market/integrated-risk-management>.

HYPO NA MÍRU. Přibor. *Hyponamiru.cz* [online]. 2023 [cit. 2023-08-27]. Dostupný z WWW: <https://www.hyponamiru.cz/slovník-pojmu/pribor/>.

IBNALKADI, H., IBNALKADI, M. Introduction to Enterprise & Model Risk Management. *Amazon.com* [online]. 2020 [cit. 2023-08-27]. Dostupný z WWW: <https://shorturl.at/oBVX9>.

JANOUSH, M. Příběh Banky X. Bývalý ředitel vyprávěl o jejím vzniku. *Mesec.cz* [online]. 2014 [cit. 2023-08-27]. Dostupný z WWW: <https://www.mesec.cz/clanky/pribeh-BankyX-byvaly-reditel-vypravel-o-jejim-vzniku/>.

KLÍMOVÁ, J. V Česku bují kyberútoky na bankovní účty. FAÚ podal loni rekordní počet trestních oznámení. *Irozhlaz.cz* [online]. 2023 [cit. 2023-08-27]. Dostupný z WWW: [https://www.irozhlaz.cz/ekonomika/bnky-kyberutoky-financi-analyticky-utvar\\_2303210900\\_vik](https://www.irozhlaz.cz/ekonomika/bnky-kyberutoky-financi-analyticky-utvar_2303210900_vik).

MANAGEMENT MANIA. Brainstorming. *Managementmania.com* [online]. 2016 [cit. 2023-08-27]. Dostupný z WWW: <https://managementmania.com/cs/brainstorming>.

MANAGEMENT MANIA. Co – když analýza What-if Analysis. *Managementmania.com* [online]. 2016 [cit. 2023-08-27]. Dostupný z WWW: <https://managementmania.com/cs/co-kdyz-analyza-what-if-analysis>.

MAZAREANU, V. Risk Management – From Theory To a Healthy Business. *Amazon.com* [online]. 2020 [cit. 2023-08-27]. Dostupný z WWW: <https://www.amazon.com.au/RISK-MANAGEMENT-THEORY-HEALTHY-BUSINESS-ebook/dp/B08KPKP35P>

MINISTERSTVO FINANCÍ ČESKÉ REPUBLIKY. Makroekonomická predikce - duben 2023. *Mfcr.cz* [online]. 2023 [cit. 2023-08-27]. Dostupný z WWW: <https://www.mfcr.cz/cs/rozpocetova-politika/makroekonomika/makroekonomicka-predikce/2023/makroekonomicka-predikce-duben-2023-50912>.

OZAK, O. Crisis Management: Navigating Through Turbulent Times. *Amazon.com* [online]. 2023 [cit. 2023-08-27]. Dostupný z WWW: <https://t.ly/le12K>.

PODNIKATEL.CZ. Zákon o krizovém řízení a o změně některých zákonů (krizový zákon) - Díl 3 - Česká národní banka. *Podnikatel.cz* [online]. 2023 [cit. 2023-08-27]. Dostupný z WWW: <https://www.podnikatel.cz/zakony/zakon-o-krizovem-rizeni-a-o-zmene-nekterych-zakonu-krizovy-zakon/f2060061/>.

RISK MANAGEMENT TOOLKIT. Brainstorming. *Mitre.org* [online]. 2023 [cit. 2023-08-27]. Dostupný z WWW: <http://www2.mitre.org/work/sepo/toolkits/risk/procedures/brainstorming.html>.

SPIŠÁK, J. Vojenské aspekty na Ukrajině. *Vojenskerozhledy.cz* [online]. 2022 [cit. 2023-08-27]. Dostupný z WWW: <https://www.vojenskerozhledy.cz/kategorie-clanku/ozbrojene-konflikty/vojenske-aspekty-valky-ukrajina>.

VÁVRA, J. Banka X trestá kryptoinvestory. Některým z nich odpírá okamžité platby. *E15.cz* [online]. 2023 [cit. 2023-08-27]. Dostupný z WWW: <https://www.e15.cz/>

ZÁKONY PRO LIDI. Vyhláška č. 82/2018 Sb. *Zakonyprolidi.cz* [online]. 2018 [cit. 2023-08-27]. Dostupný z WWW: <https://www.zakonyprolidi.cz/cs/2018-82#f6228905>.

ZÁKONY PRO LIDI. Zákon č. 240/2000 Sb. *Zakonyprolidi.cz* [online]. 2022 [cit. 2023-08-27]. Dostupný z WWW: <https://www.zakonyprolidi.cz/cs/2000-240>.

## Další zdroje

Webové stránky Banky X.

Výroční zpráva Banky X za rok 2020.

Tisková zpráva Banky X, 2023.

Výroční zpráva Skupiny Y za rok 2022.

Plán kontinuity podnikání Banky X.

Bezpečnostní manuál pro případ mimořádných událostí Banky X.

## **Přílohy**

Příloha č. 1 Polostrukturovaný rozhovor s vedoucím oddělení řízení operačních rizik v "Bance X" II

Příloha č. 2 Polostrukturovaný rozhovor s ředitelem divize Řízení rizik „Banky X“ IV

Příloha č. 3 Seznam všech identifikovaných příležitostí a hrozeb VIII

Příloha č. 4 Výpočet míry rizika na základě identifikovaných hrozeb X

Příloha č. 5 Matice rizik XII

Příloha č. 1 Polostrukturovaný rozhovor s vedoucím oddělení řízení operačních rizik v „Bance X“

**Jak charakterizujete svůj přístup k identifikaci a řízení operačních rizik v „Bance X“?**

*„V „Bance X“ upřednostňujeme kombinaci kvantitativních a kvalitativních metod, s důrazem na pravidelnou komunikaci mezi odděleními.“*

**Které technologické nástroje „Banka X“ v současnosti používá pro monitorování operačních rizik?**

*„Využíváme integrovaný software pro řízení rizik, který zahrnuje funkce AI pro analýzu vzorců a detekci anomálií.“*

**Máte zavedené konkrétní strategie pro posilování kultury řízení rizik mezi zaměstnanci?**

*„Ano, organizujeme pravidelné školení a workshopy, kde zdůrazňujeme význam individuálního přístupu k rizikům.“*

**Jak často provádíte revizi plánů kontinuity podnikání s ohledem na operační rizika?**

*„Revize provádíme každý rok, a v případě významných změn na trhu nebo v regulačním prostředí.“*

**Jak „Banka X“ postupuje při identifikaci nových a rozvíjejících se rizik?**

*„Máme tým, který sleduje tržní trendy a technologické inovace, aby proaktivně identifikoval potenciální rizika.“*

**Které klíčové metriky používáte pro hodnocení operačního rizika v „Bance X“?**

*„Kromě tradičních metrik, jako jsou finanční ztráty, sledujeme i úroveň stížností klientů a výkonnost interních procesů.“*

**Jaký význam přikládáte externím auditům v kontextu operačního rizika?**

*„Považujeme je za nezbytné, protože nám poskytují nezávislý pohled na naše postupy a identifikují potenciální slabiny.“*

**Jaký vliv má digitalizace bankovních služeb na operační rizika „Banky X“?**

*„Zatímco digitalizace přináší výhody v podobě efektivity, zvyšuje také rizika spojená s kybernetickou bezpečností.“*

**V jaké míře zapojujete oddělení IT při řízení operačních rizik?**

*„Oddělení IT je klíčovým partnerem. Spolupracujeme na implementaci bezpečnostních opatření a monitorování systémů.“*

**Jak se „Banka X“ připravuje na budoucí výzvy v oblasti operačního rizika?**

*„Investujeme do výzkumu a vývoje, sledujeme mezinárodní best practices a pravidelně revidujeme naše strategie.“*

**Jaké jsou hlavní výzvy při zavádění nových technologií a digitálních inovací v kontextu operačního rizika?**

*„Při zavádění nových technologií a digitálních inovací se objevují různé výzvy v kontextu operačního rizika. Je nezbytné provést důkladnou analýzu rizik spojených s novými technologiemi a zavést odpovídající kontroly a bezpečnostní opatření. Dále je třeba zajistit, aby*

*byli zaměstnanci dostatečně školeni a informováni o bezpečnostních postupech při používání nových technologií. Je také důležité sledovat vývoj technologií a inovačních trendů a přizpůsobit naše řízení rizik tomuto dynamickému prostředí. “*

***Momentálně nenabízíte možnost platby spojené s kryptoměnovými burzami. Můžete mi k tomuto tématu říct více informací? Jaká jsou hlavní rizika, která v této souvislosti identifikujete?***

*Rozumím, že kryptoměny jsou zajímavým fenoménem a mnozí z našich klientů by chtěli pomocí kryptoměny platit. V současné době ale nepodporujeme platby spojené s kryptoměnovými burzami. Důvod je ten, že se snažíme chránit naše klienty před riziky, jako je kybernetický útok nebo nestabilní hodnota kryptoměn. Jako další rizika vidíme nestabilní hodnoty a regulatorní nejistotu. Sledujeme pečlivě tržní trendy, abychom do budoucna byli schopni tyto rizika minimalizovat.*

***Jaký je váš přístup k rozvoji a posilování bezpečnostní kultury?***

*„Můj přístup k rozvoji a posilování bezpečnostní kultury je založen na aktivní komunikaci, vzdělávání a osvědčených postupech. Vytváříme prostředí, které klade důraz na bezpečnost a zodpovědnost všech zaměstnanců v bance. To zahrnuje pravidelné školení zaměstnanců o bezpečnostních postupech, podporu pro hlášení rizikových situací a zajištění, aby se bezpečnostní záležitosti staly součástí každodenní pracovní kultury. “*

***Jaké jsou vaše metody a postupy pro monitorování a reportování operačního rizika?***

*„Pro monitorování a reportování operačního rizika v Bance X používáme systém sledování klíčových rizikových ukazatelů a pravidelné sestavování rizikových reportů. Sledujeme ukazatele v reálném čase, abychom byli schopni identifikovat případné anomálie nebo vzorce rizikového chování. Naše reporty jsou strukturované a obsahují podrobné informace o identifikovaných rizicích, jejich vývoji a dopadu na banku. “*

***Jaký je váš přístup k hodnocení a správě operativních rizik ve spolupráci se zainteresovanými odděleními a týmy?***

*„Mým přístupem k hodnocení a správě operativních rizik je spolupráce a komunikace se zainteresovanými odděleními a týmy v bance. Pravidelně konzultuji s vedoucími oddělení a týmy, abych získal jejich perspektivu na operační rizika v jejich oblastech a sdílel relevantní informace o rizicích a opatřeních. Společně se snažíme identifikovat nejlepší přístupy a spolupracovat na řešeních pro správu a minimalizaci rizik. “*

***Jaký je váš pohled na roli technologií jako nástroje pro řízení a snižování operačního rizika?***

*„Považuji technologie za důležitý nástroj pro řízení a snižování operačního rizika v Bance X. Moderní technologie, jako jsou automatizace procesů, analýza dat a umělá inteligence, mohou výrazně zlepšit naši schopnost identifikovat, monitorovat a řídit rizika. Využíváme technologická řešení pro detekci anomálií, sledování klíčových rizikových ukazatelů a rychlou reakci na potenciální rizikové události. Nicméně je důležité zajistit, aby byly technologie správně implementovány a aby byla zajištěna jejich bezpečnost a spolehlivost. “*

**Jaké jsou hlavní povinnosti a odpovědnosti spojené s vaší rolí?**

*„Mám na starosti celkové řízení rizik v bance. Mé povinnosti zahrnují identifikaci, hodnocení a řízení operačního rizika, finančního rizika, kreditního rizika, likviditního rizika a dalších relevantních rizikových oblastí. Také jsem odpovědný za vytváření a implementaci směrnic a postupů pro řízení rizik a zajištění souladu s příslušnými regulačními požadavky.“*

**Jaký je váš přístup k identifikaci a hodnocení rizik?**

*„Můj přístup k identifikaci a hodnocení rizik je založen na systematickém přístupu. Spolupracuji s různými odděleními a týmy v bance, abychom identifikovali potenciální rizika a provedli jejich kvalitativní a kvantitativní hodnocení. Používáme metody, jako jsou rizikové analýzy, scénářové analýzy a modelování rizik, abychom získali co nejkomplexnější a přesné informace o rizikovém prostředí.“*

**Jaké strategie a opatření máte v plánu pro řízení operačního rizika?**

*„Pro řízení operačního rizika v Bance X plánujeme implementovat strategie a opatření založené na nejlepších postupech a osvědčených metodách. To zahrnuje vytváření efektivních interních kontrolních opatření, pravidelné školení zaměstnanců o bezpečných pracovních postupech, důkladné monitorování klíčových rizikových ukazatelů a analýzu rizikových událostí. Také hodláme spolupracovat s technologickými týmy pro implementaci pokročilých technologických řešení pro detekci a prevenci operačního rizika.“*

**Jaké jsou hlavní výhody a výzvy spojené s implementací efektivního systému řízení operačního rizika?**

*„Implementace efektivního systému řízení operačního rizika přináší několik výhod. Patří sem snížení frekvence a dopadu operačních rizikových událostí, zvýšení bezpečnosti a spolehlivosti našich operací, zlepšení dodržování předpisů a regulací, a posílení důvěry klientů a investorů v naši banku. Nicméně, existují také výzvy, jako je nutnost kontinuálního monitorování a aktualizace systému, správná komunikace a spolupráce mezi odděleními a potřeba dostatečných finančních a lidských zdrojů pro implementaci a provoz systému řízení rizik.“*

**Jaký je váš přístup ke krizovému řízení a kontinuitě podnikání v případě vzniku nečekaných událostí?**

*„Můj přístup ke krizovému řízení a kontinuitě podnikání je založen na plánování, připravenosti a rychlé reakci. Spolupracuji s týmy zodpovědnými za krizové řízení a vypracováváme plány pro zvládání rizikových situací. To zahrnuje identifikaci klíčových procesů a funkcí, zavedení opatření pro minimalizaci přerušení činnosti a přípravu na obnovení operací po krizové události. Dále provádíme pravidelné simulace a cvičení, abychom ověřili účinnost našich plánů a zlepšili naše reakční schopnosti.“*

**Jak vypadá organizační struktura řízení rizik a rozdělení zodpovědností?**

*„Tým je rozdělen do těchto oddělení. Řízení retailových rizik. Tato část týmu se specializuje na řízení rizik spojených s našimi retailovými produkty a službami. Naše hlavní prioritou je monitorovat a hodnotit rizika související s úvěrovou činností, správou klientů a dalšími retailovými operacemi. Dále je to řízení rizik nových produktů a komerčních operací: zde se zaměřujeme na řízení rizik spojených s novými produkty, které banka nabízí, a komerčními operacemi. Naše týmové úsilí směřuje k posouzení a hodnocení rizik, která se vztahují k novým*

*investičním nástrojům, finančním derivátům a dalším komerčním aktivitám. Další je řízení operačních rizik. Tato část týmu je zodpovědná za identifikaci a řízení operačních rizik v naší bance. Soustředíme se na monitorování a hodnocení rizik spojených s procesy, systémy a interními kontrolami. Naším cílem je minimalizovat možné operativní problémy a zajistit bezproblémový průběh našich operací. Řízení tržních rizik a stres testů, tady se zaměřujeme na řízení rizik spojených se změnami na finančních trzích a provádění stres testů. Analyzujeme vlivy tržních podmínek na bankovní portfolia a provádíme simulace a testování za různých stresových scénářů. V oddělení podpory klientských procesů a manuální schvalování se věnujeme podpoře různých klientských procesů a schvalování operací, které vyžadují manuální přezkoumání. Zajišťujeme, aby tyto procesy byly řádně provedeny, a monitorujeme případná rizika spojená s manuálními operacemi. Treasury back office se specializuje na správu a provoz treasury operací. Zabezpečujeme správné zpracování a evidenci transakcí, likviditu a řízení rizik spojených s investicemi a financováním. Poslední část týmu se stará o celkový provoz a chod naší banky. Zajišťujeme, aby všechny operace a služby probíhaly bez problémů a efektivně.“*

**Mohl byste mi sdělit váš názor na hrozby a příležitosti, které se bezprostředně týkají banky?**

*„Pokud jde o hrozby, identifikujeme několik klíčových rizik. Za prvé, ekonomickou nestabilitu. Další hrozbou je rychle se měnící regulační prostředí, které může přinést vyšší náklady a omezení našich aktivit. Neméně důležité jsou kybernetické hrozby, které mohou vážně ohrozit naši bezpečnost a důvěryhodnost klientů. Konkurence v bankovním odvětví se stále zvyšuje, což může mít negativní dopad na naši tržní pozici.“*

**Vidíte nějaké příležitosti, které by mohly pro banku vyplývat ze současného makroekonomického prostředí?**

*„Ano, v současném prostředí identifikujeme několik zajímavých příležitostí. Digitalizace je klíčovým trendem, který nám poskytuje možnost zlepšit naše služby a procesy a tím zvýšit spokojenost zákazníků a efektivitu banky. Implementace nových technologií, jako automatizace procesů nebo umělá inteligence, nám může umožnit rozšířit nabídku produktů a zlepšit interní operace. Rostoucí trhy nám poskytují příležitost expanze na nové trhy s rostoucí poptávkou po finančních službách.“*

**Jaké strategie a opatření pro tyto hrozby a příležitosti plánujete implementovat?**

*„Je klíčové, abychom byli proaktivní a připraveni na změny v makroekonomickém prostředí. Pro hrozby, jako je ekonomická nestabilita a regulace, musíme mít připravené plány, jak minimalizovat negativní dopady našich aktivit a portfolio. Pro kybernetické hrozby musíme posílit naše bezpečnostní opatření a investovat do moderních technologií, které nám pomohou chránit naše klienty. Co se týče příležitostí, musíme strategicky využít digitalizaci a nové technologie k rozšíření nabídky a zvýšení efektivity. Na nových trzích musíme provést pečlivý průzkum a přizpůsobit naše produkty a služby potřebám těchto trhů.“*

**Jak vnímáte vliv sociálních a ekonomických faktorů na banku?**

*„Sociální a ekonomické faktory hrají v současném makroekonomickém prostředí klíčovou roli pro naši banku. Co se týče sociálních faktorů, je důležité sledovat změny ve spotřebitelském chování a preferencích. Růst popularity online bankovníctví a mobilních platforem nám ukazuje, že naši klienti očekávají snadný a rychlý přístup k finančním službám. Dále je třeba sledovat změny v demografické struktuře, zejména s ohledem na stárnutí populace a jeho dopad“*



na naše cílové trhy a produkty. Dále sledujeme růst populace, věkovou strukturu a migrační trendy.

V ekonomických faktorech musíme sledovat vývoj HDP, inflace a úrokových sazeb, které mohou ovlivnit naše zisky a náklady. Nezaměstnanost a zaměstnanost jsou také klíčové ukazatele, které ovlivňují naše úvěrové portfolio a poptávku po finančních produktech. Rovněž sledujeme ekonomickou stabilitu, která může mít dopad na globální ekonomiku.

### **Jaký vliv má dle Vás válka na Ukrajině na činnost banky?**

*Zdražení energií zvýšilo rapidně náklady na provoz IT systémů a pobočkové sítě, vysoká inflace tlačí na navýšení cen všech komodit a služeb. Zaměstnanci požadují vyšší platy a zvyšují tím náklady. Dále vnímáme odliv ruského kapitálu, vysoká imigrace naopak zvýšila počet klientů, pád Sberbank CZ navýšil počet klientů. Nejistá bezpečnostní a ekonomická situace snižuje investice, vysoké úroky ČNB snižují investice, a to má dopad na bilanci banky, lidé se snaží více šetřit, jejich chování se mění, kybernetické hrozby z východu nutí k novým investicím do bezpečnosti.*

### **Mohli bychom se blíže zastavit u tématu inflace? Jak banka reaguje na její vývoj a jaký vliv má na poptávku vašich produktů?**

*„Inflace je jedním z faktorů, kterým jako ředitel divize Řízení rizik věnuji zvláštní pozornost. Naše banka uznává význam cenové stability a jejího vlivu na ekonomiku i naše klienty. Pravidelně monitorujeme vývoj inflace a snažíme se předvídat její budoucí vývoj, abychom lépe mohli přizpůsobit naši měnovou politiku a investiční nabídky situaci na trhu. Míra inflace může mít významný dopad na poptávku našich klientů po investičních produktech. Vysoká míra inflace může snižovat reálný výnos z některých tradičních spořicíh možností, což může klienty motivovat hledat jiné investiční příležitosti, které by jim umožnily lépe uchovat hodnotu jejich úspor v době inflace. To může zvýšit zájem o akcie, podílové fondy, nemovitosti nebo komodity, které mají potenciál růstu v době inflace“.*

### **Jak banka reaguje na tuto situaci a jaké investiční produkty nabízíte, které by mohly klienty zajímat v době vysoké inflace?**

*„S ohledem na vývoj inflace průběžně aktualizujeme naši nabídku investičních produktů, abychom reflektovali potřeby našich klientů. V době vysoké inflace nabízíme klientům různé investiční možnosti, které mají potenciál lépe chránit jejich úspory před cenovou inflací. V současné době nabízíme možnost investování na míru, podílové fondy či doplňkové penzijní spoření.“*

### **Jaké kroky a strategie plánujete implementovat v reakci na tyto sociální a ekonomické faktory?**

*V reakci na sociální faktory plánujeme dále investovat do digitálních kanálů a zlepšit uživatelský zážitek našich klientů. Chceme nabídnout moderní a inovativní způsoby bankovníctví, které odpovídají očekáváním a potřebám našich zákazníků. Zároveň se zaměříme na segmentaci našich produktů a služeb, aby byly vhodně přizpůsobeny různým věkovým a demografickým skupinám.*

*V ekonomických faktorech plánujeme pružnou strategii, která nám umožní efektivně reagovat na změny v ekonomice.*

### **Jak se Vaše strategie a činnost přizpůsobuje novým legislativním předpisům v oblasti bankovníctví a ochrany spotřebitelů?**

*„Jsme pečlivě informováni o nových bankovních a spotřebitelských předpisech a úzce spolupracujeme s právním oddělením. Aktivně se podílíme na jejich implementaci a zajišťujeme, že naše činnost je v souladu s aktuální legislativou. Tím chráníme jak banku, tak i naše zákazníky.“*

**Jaký je vliv politických změn na bankovní sektor a vaše podnikání?**

*„Sledujeme politickou stabilitu a změny v regulacích, které ovlivňují bankovní sektor. Politická rozhodnutí, například v oblasti fiskální politiky nebo regulace datové ochrany, mají významný dopad na naše podnikání. Jsme připraveni reagovat a přizpůsobit se těmto změnám.“*

**Máte nějaké doplňující komentáře nebo myšlenky ohledně hrozeb a příležitostí v makroekonomickém prostředí?**

*„Rád bych zdůraznil, že hodnocení hrozeb a příležitostí v makroekonomickém prostředí je proces, který vyžaduje pravidelné aktualizace a analýzy. Musíme být schopni rychle reagovat na změny v ekonomice, technologiích, regulačním prostředí a preferencích zákazníků. Spolupráce mezi různými odděleními banky, jako je rizikový management, obchodní strategie a inovace, je klíčová pro úspěch v tomto rychle se měnícím prostředí.*

*Je také důležité zapojit se do dialogu s našimi klienty a investory, abychom lépe porozuměli jejich potřebám a očekáváním. Poskytování udržitelných a odpovídajících finančních produktů nám umožní posílit naši konkurenceschopnost a dlouhodobou udržitelnost.*

Zdroj: vlastní zpracování

Příloha č. 3 Seznam všech identifikovaných příležitostí a hrozeb

<b>Příležitosti</b>	<b>Hrozby</b>
<b>Sociální faktor</b>	
Růst popularity online bankovníctví a mobilních platforem	Stárnutí populace
Finanční poradenství pro seniory	Nízká porodnost
Rozvoj inovativních finančních produktů	Ekonomická nestabilita
Změny v životních stylech a spotřebních preferencích	
Rozvoj nových služeb	Změny v imigrační politice
Finanční poradenství pro cizince	Snížená mobilita
Online a mezinárodní bankovníctví	Konkurence
Růst populace svobodných a rozvedených osob	Snížená poptávka po tradičních bankovních produktech
Růst popularity online bankovníctví a digitálních platforem	Odkládání sňatků a porodů
Finanční poradenství pro svobodné a rozvedené osoby	
Rozvoj inovativních finančních produktů pro mladé generace	
<b>Ekonomický faktor</b>	
Nové podnikatelské příležitosti	Snížená schopnost klientů splácet úvěry a zvýšené riziko nesplácení úvěrů
Rostoucí životní standard obyvatel	Růst problematických úvěrů
Ekonomické oživení po pandemii covid -19	Potenciální nejistota v souvislosti s dalším vývojem ekonomické situace
Nové produkty a služby	Riziko nesplácení úvěrů
Zájem o investiční produkty	Pokles poptávky po dlouhodobých úvěrech
Růst poptávky po doplňkovém penzijním spoření	Zvýšení cen hypoték
Flexibilní splátkové podmínky	Nárůst cen energií
Snížení měsíčních splátek pro klienty s neočekávanými náklady	Nízké reálné výnosy z investičních produktů
Podpora klientů s nejistými finančními vyhlídkami	
Růst úrokových sazeb	Růst úrokových sazeb
Makroekonomická stabilita	Inflace
Mírný nárůst zaměstnanosti	Genderová nerovnost na trhu práce
Úspěch rodinných a dětských účtů	Nižší míra zaměstnanosti u mladších věkových skupin
Potenciální rozšíření nabídky pro mladé lidi	Nezkušenost mladších věkových skupin v oblasti finanční gramotnosti
Nízká míra nezaměstnanosti	Genderová nerovnost v míře nezaměstnanosti
Stabilní ekonomické podmínky	

<b>Technicko-technologický faktor</b>	
Nové technologie a inovace	Kybernetická bezpečnost
Zlepšení uživatelské zkušenosti	Regulace
Dostupnost dat	Technologický vývoj
<b>Ostatní</b>	
	Nefunkčnost hardwaru nebo bankovní aplikace
	Požár v budově
	Výpadek elektrického proudu
	Nepřítomnost většího počtu zaměstnanců (např. kvůli nemoci)
	Nedostupnost hlavních pracovních systémů
	Teroristický útok

Zdroj: vlastní zpracování

Příloha č. 4 Výpočet míry rizika na základě identifikovaných hrozeb

Pořadí	Riziko	Pravděpodobnost (1-5)	Dopad (1-5)	Míra rizika (RPN)
R1	Ztráta příjmů z důchodových produktů kvůli stárnutí populace	4	3	12
R2	Snížená poptávka po úvěrech kvůli nízké porodnosti	3	2	6
R3	Riziko snížení solvence klientů kvůli ekonomické nestabilitě	4	5	20
R4	Ztráta klientů z důvodu změn v imigrační politice	2	2	4
R5	Snížená schopnost expanze kvůli snížené mobilitě	3	3	9
R6	Ztráta tržního podílu kvůli konkurenci	4	5	20
R7	Pokles příjmů kvůli snížené poptávce po tradičních produktech	3	4	12
R8	Snížená poptávka po úvěrech kvůli odkládání sňatků a porodů	3	3	9
R9	Ztráta aktiva kvůli růstu problematických úvěrů	4	4	16
R10	Finanční ztráta kvůli ekonomické nejistotě	4	5	20
R11	Pokles příjmů kvůli snížené poptávce po dlouhodobých úvěrech	3	3	9
R12	Pokles příjmů kvůli zvýšení cen hypoték	3	4	12
R13	Zvýšení provozních nákladů banky	2	3	6
R14	Snížení poptávky po investičních produktech a snížení provizních příjmů	3	4	12
R15	Snížení poptávky po úvěrových produktech a zvýšení nákladů na financování	4	4	16
R16	Snížený zisk kvůli inflaci	4	4	16
R17	Snížená poptávka po některých produktech kvůli nižší míře zaměstnanosti u mladších skupin	2	2	4

R18	Vyšší náklady na vzdělávání kvůli nezkušenosti mladších věkových skupin v oblasti finanční gramotnosti	3	3	9
R19	Snížená efektivita kvůli genderové nerovnosti v míře nezaměstnanosti	2	3	6
R20	Finanční ztráta kvůli kybernetickým incidentům	5	5	25
R21	Vyšší provozní náklady kvůli regulaci	4	3	12
R22	Ztráta tržního podílu kvůli technologickému vývoji	4	4	16
R23	Ztráta klientů a příjmů kvůli nefunkčnosti hardwaru nebo bankovní aplikace	3	4	12
R24	Finanční a operativní ztráta kvůli požáru v budově	2	5	10
R25	Ztráta operativní efektivity kvůli výpadku elektrického proudu	2	4	8
R26	Snížená efektivita kvůli nepřítomnosti většího počtu zaměstnanců	3	3	9
R27	Ztráta operativní efektivity kvůli nedostupnosti hlavních pracovních systémů	3	4	12
R28	Finanční a operativní ztráta kvůli teroristickému útoku	1	5	5

Zdroj: vlastní zpracování

Příloha č. 5 Matice rizik

Pravděpodobnost výskytu	Závažnost důsledků				
	Zanedbatelná (1)	Malá (2)	Střední (3)	Významná (4)	Katastrofální (5)
Jistá (5)					<b>R20</b>
Pravděpodobná (4)			<b>R1, R21</b>	<b>R9, R15, R16, R22</b>	<b>R3, R6, R10</b>
Možná (3)		<b>R2</b>	<b>R5, R8, R11, R18, R26</b>	<b>R7, R12, R14, R23, R27</b>	
Neppravděpodobná (2)		<b>R4, R17</b>	<b>R13, R19</b>	<b>R25</b>	<b>R24</b>
Vzácná (1)					<b>R28</b>

Zdroj: vlastní zpracování



## DIPLOMOVÁ PRÁCE



**Identifikování rizik a zpracování krizových scénářů a plánů v podniku**

**Bc. Daniela Mertlová, KEMMA05**



# Řešená problematika

## úvod

Cíl diplomové práce:

- Identifikování kritických rizik v organizaci
- Analýza a hodnocení rizik
- Posouzení stavu připravenosti na rizika

## problém

Problém spočívá v identifikaci a předvídání potenciálních rizik a následném vytváření efektivních krizových scénářů a plánů pro jejich řešení.

## přístup

- Brainstorming
- Polostrukturované rozhovory
- Analýza firemních dokumentů

# Postup řešení

## zdroj

- Literární publikace
- Odborné články, studie
- Internetové zdroje
- Zákony, normy
- Veřejně dostupné dokumenty společnosti

## získávání

- Metoda komparace
- Metoda řešerše
- Provedení polostrukturovaných rozhovorů, brainstormingu v rámci vlastního výzkumu

## zpracování

- Identifikace rizik pomocí STEP analýzy a polostrukturovaných rozhovorů
- Hodnocení rizik pomocí matice rizik a vstupů z brainstormingu
- Tvorba opatření na nejkritičtější rizika
- Tvorba krizových scénářů a plánů na nejkritičtější rizika

# Výsledky práce- analýza rizik

V rámci výzkumu bylo identifikováno 30 příležitostí a 28 hrozeb.

Příležitosti	Hrozby
<b>Sociální faktor</b>	
Růst popularity online bankovníctví a mobilních platforem	Stárnutí populace
Finanční poradenství pro seniory	Nízká porodnost
Rozvoj inovativních finančních produktů	Ekonomická nestabilita
Změny v životních stylech a spotřebních preferencích	
Rozvoj nových služeb	Změny v imigrační politice
Finanční poradenství pro cizince	Snížená mobilita
Online a mezinárodní bankovníctví	Konkurence
Růst populace svobodných a rozvedených osob	Snížená poptávka po tradičních bankovních produktech
Růst popularity online bankovníctví a digitálních platforem	Odkládání sňatků a porodů
Finanční poradenství pro svobodné a rozvedené osoby	
Rozvoj inovativních finančních produktů pro mladé generace	
<b>Ekonomický faktor</b>	
Nové podnikatelské příležitosti	Snížená schopnost klientů splácet úvěry a zvýšené riziko nesplácení úvěrů
Rostoucí životní standard obyvatel	Růst problematických úvěrů
Ekonomické oživení po pandemii Covid -19	Potenciální nejistota v souvislosti s dalším vývojem ekonomické situace
Nové produkty a služby	Riziko nesplácení úvěrů
Zájem o investiční produkty	Pokles poptávky po dlouhodobých úvěrech
Růst poptávky po doplňkovém penzijním spoření	Zvýšení cen hypoték
Flexibilní splátkové podmínky	Nárůst cen energií
Snížení měsíčních splátek pro klienty s neočekávanými náklady	Nízké reálné výnosy z investičních produktů
Podpora klientů s nejistými finančními vyhlídkami	
Růst úrokových sazeb	Růst úrokových sazeb
Makroekonomická stabilita	Inflace
Mírný nárůst zaměstnanosti	Genderová nerovnost na trhu práce

Úspěch rodinných a dětských účtů	Nižší míra zaměstnanosti u mladších věkových skupin
Potenciální rozšíření nabídky pro mladé lidi	Nezkušenost mladších věkových skupin v oblasti finanční gramotnosti
Nízká míra nezaměstnanosti	Genderová nerovnost v míře nezaměstnanosti
Stabilní ekonomické podmínky	
<b>Technico-technologický faktor</b>	
Nové technologie a inovace	Kybernetická bezpečnost
Zlepšení uživatelské zkušenosti	Regulace
Dostupnost dat	Technologický vývoj
<b>Ostatní</b>	
	Nefunkčnost hardwaru nebo bankovní aplikace
	Požár v budově
	Výpadek elektrického proudu
	Nepřítomnost většího počtu zaměstnanců (např. kvůli nemoci)
	Nedostupnost hlavních pracovních systémů
	Teroristický útok

## Výsledky práce – hodnocení rizik

Následně byla rizika ohodnocena pomocí expertů a byla vypočítána míra jednotlivých rizik. Níže je tabulka nejkritičtějších rizik.

Pořadí	Riziko	Pravděpodobnost (1-5)	Dopad (1-5)	Míra rizika (RPN)
R3	Riziko snížení solvence klientů kvůli ekonomické nestabilitě	4	5	20
R6	Ztráta tržního podílu kvůli konkurenci	4	5	20
R10	Finanční ztráta kvůli ekonomické nejistotě	4	5	20
R20	Finanční ztráta kvůli kybernetickým incidentům	5	5	25

# Výsledky práce – Opatření vedoucí ke snížení rizik

Na základě nejkritičtějších rizik vznikla následná doporučení k opatření vedoucí ke snížení rizik:

	Stakeholderi	Krátkodobé opatření	Dlouhodobé opatření
<b>R3: Snížení solvence klientů</b>	Pojištění proti kybernetickým rizikům a kontinuální investice do vzdělávání a technologie.	Akceptace rizika díky silnému kapitálu banky.	Využití analytických nástrojů a umělé inteligence pro identifikaci a předcházení rizikům.
<b>R6: Ztráta tržního podílu kvůli konkurenci</b>	Management banky, marketingový tým, akcionáři, klienti a konkurenční banky.	Zesílené marketingové aktivity.	Investice do digitální inovace a sledování tržních trendů.
<b>R10: Finanční ztráta kvůli ekonomické nejistotě</b>	Management banky, akcionáři, věřitelé, klienti a ekonomičtí analytici.	Přenesení rizika prostřednictvím pojištění.	Diverzifikace investic a zlepšení strategického řízení rizik.
<b>R20: Ztráta kvůli kybernetickým incidentům</b>	Management banky, IT tým, zaměstnanci banky, akcionáři, klienti a externí IT bezpečnostní firmy.	Posílení IT bezpečnosti.	Pojištění proti kybernetickým rizikům a kontinuální investice do vzdělávání a technologie.

# Výsledky práce – krizové scénáře a plány

Na základě nejkritičtějších rizik byly vypracovány krizové scénáře a plány.

Pomocí What-if analýzy byly vytvořeny další scénáře týkající se kybernetické bezpečnosti:

- **Scénář č. 1:** Co se stane, když dojde k chybě interního systému banky a dočasně nebudou dostupné její služby?
- **Scénář č. 2:** Co se stane, když dojde ke ztrátě dat z interního systému banky a chyba způsobí trvalé poškození nebo ztrátu dat?
- **Scénář č.3:** Co se stane, když chyba v interním systému banky způsobí únik citlivých informací o zákaznících?

# Výsledky práce – krizové scénáře a plány - zhodnocení

## 1. Základní zhodnocení:

- Scénář pro nedostupnost systému existuje, ale je příliš obecný.
- Chybějící scénáře pro ztrátu dat a únik informací.

## 2. Aktualizace stávajících scénářů:

- "Nedostupnost – ztráta systému" byl aktualizován na základě nových rizikových hodnocení.

## 3. Nově vypracované scénáře:

- "Ztráta dat v interním systému banky".
- Únik citlivých informací o zákaznících".

## 4. Důraz na implementaci:

- Efektivní komunikace, koordinace a aktualizace krizových plánů pro rychlou a účinnou reakci na mimořádné události.

# Závěrečná doporučení

Na základě výsledků vyplývají následná doporučení:

**1. Příprava scénářů** vyžaduje pečlivé prozkoumání, schválení managementem před vlastní realizací. Scénáře musí reflektovat skutečné hrozby a rizika. Je zapotřebí jak teoretický (table-top cvičení), tak praktické (simulace krizových situací). Je nutná analýza po testu (hodnocení efektivnosti, reakční doby, kvality reakce), revize postupů a aktualizace a připravenost.

**2. V rámci zhodnocení stavu připravenosti** lze vyhodnotit **kladné stránky** a **oblasti ke zlepšení**.



- Komplexní plán kontinuity podnikání.
- Pravidelná aktualizace plánů obnovy po havárii (DRP).
- Investice do školení a simulací.
- Kooperace mezi odděleními.



- Detailnější krizové scénáře a plány (zejména kybernetická bezpečnost).
- Pravidelné testování scénářů.



# DEKUI ZA POZORNOST

VŠEM  
VYSOKÁ  
ŠKOLA  
EKONOMIE  
A MANAGEMENTU