

Metody analýzy rizik v kybernetické bezpečnosti

Bc. Jan Čížek

Diplomová práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně

Fakulta logistiky a krizového řízení

Ústav krizového řízení

Akademický rok: 2024/2025

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Bc. Jan Čížek
Osobní číslo:	L23073
Studijní program:	N1032A020002 Bezpečnost společnosti
Specializace:	Rizikové inženýrství
Forma studia:	Prezenční
Téma práce:	Metody analýzy rizik v kybernetické bezpečnosti

Zásady pro vypracování

- Proveďte rešerši vztahující se k dané problematice.
- Posuďte vhodnost vybraných metod analýzy rizik v kybernetické bezpečnosti.
- Proveďte komparaci výstupů vybraných metod.
- Navrhněte doporučení pro provádění analýzy rizik v kybernetické bezpečnosti.

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

Seznam doporučené literatury:

1. DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.
2. KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o. CZ.NIC, 2019. ISBN 978-80-88168-31-7.
3. OSTRUM, Lee T. a WILHELMSSEN, Cheryl A. *Risk assessment: tools, techniques, and their applications*. Second edition. Hoboken, NJ: Wiley, 2019. ISBN 978-1-119-48346-5.
4. SMEJKAL, Vladimír; SOKOL, Tomáš a KODL, Jindřich. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.
5. SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2022/2555: *o opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)*, 2022.

Další odborná literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **Ing. Petr Svoboda, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání diplomové práce: **2. prosince 2024**
Termín odevzdání diplomové práce: **25. dubna 2025**

L.S.

prof. Ing. Zuzana Tučková, Ph.D.
děkanka

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2024

PROHLÁŠENÍ AUTORA DIPLOMOVÉ PRÁCE

Beru na vědomí, že

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

Prohlašuji, že

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

V Uherském Hradišti, dne 25.4. 2025

.....
podpis autora

ABSTRAKT

Předložená diplomová práce se zabývá problematikou analýzy rizik v oblasti kybernetické bezpečnosti. Teoretická východiska jsou zaměřena na podstatu rizika, jeho definice, způsoby kvantifikace a relevantní standardy či normy. Praktická část práce se zaměřuje na identifikaci klíčových kritérií, která ovlivňují volbu metody analýzy rizik v kontextu kybernetické bezpečnosti. Pomocí metody multikriteriální analýzy byla určena nejvýznamnější kritéria, která hrají zásadní roli při výběru vhodného postupu. Na základě těchto kritérií a jejich kvantifikace byl následně navržen funkční koncept podpůrného nástroje, který usnadňuje organizacím rozhodování o volbě metody analýzy rizik s ohledem na jejich specifické potřeby.

Klíčová slova: analýza rizik, kybernetická bezpečnost, metody analýzy rizik, návrh nástroje, riziko

ABSTRACT

This thesis addresses the issue of risk analysis in the field of cybersecurity. The theoretical framework examines the nature of risk, its definitions, quantification methods, and relevant standards and norms. The practical part focuses on identifying key criteria influencing the selection of risk analysis methods in the context of cybersecurity. Using multi-criteria analysis, the most significant criteria were determined, playing a crucial role in choosing an appropriate approach. Based on these criteria and their quantification, a functional concept of a supportive tool was designed to facilitate organizations decision-making regarding the selection of risk analysis methods tailored to their specific needs.

Keywords: risk analysis, cybersecurity, risk analysis methods, supportive tool design, risk

Poděkování

Necht' je tato stránka skromnou poctou všem, kteří po mém boku kráčeli poskytující oporu v labyrintu poznání i na klikatých stezkách života. Bez jejich světla by má cesta byla temnější, bez jejich slov méně bohatá a bez jejich víry méně jistá. Každý krok na této pouti byl nejen mým vlastním úsilím, ale i ozvěnou jejich laskavosti, moudrosti a trpělivosti.

Necht' tato práce není jen výsledkem mého snažení, ale i odrazem podpory akademiků, přátel, rodiny i těch, jejichž přítomnost byla neviditelná, a přesto cenná. Vědomí, že mé kroky nesou ozvěnu tolika laskavých hlasů, mě naplňuje pokorou i vděčností.

Děkuji

„Ale žádný vysoko vzrostlý, vznešený strom se ještě nikdy nevzdal svých temných kořenů. Roste nejen nahoru, nýbrž také dolů. Jistě je naprosto důležité to, kam člověk jde; ale stejně důležitá mi připadá otázka: Kdo kam jde? A ono "kdo" vždycky vede k "odkud".“

- Carl Gustav Jung

„Kybernetická bezpečnost se týká každého z nás, kdo využívá jakékoliv prvky informační a komunikační technologie ve svém každodenním životě. Pokud si sami neuvědomíme, že jsme klíčovým, a v mnoha případech stěžejním prvkem kybernetické bezpečnosti (ať už ve svém soukromí či v práci), tak vlastně zvyšujeme pravděpodobnost úspěchu kybernetických útoků.“ (Kolouch, 2019)

OBSAH

ÚVOD.....	11
CÍL PRÁCE A POUŽITÉ METODY.....	12
I TEORETICKÁ ČÁST	14
1 KONCEPT RIZIKA.....	15
1.1 PRAVDĚPODOBNOST	16
1.1.1 Frekventistický přístup.....	17
1.1.2 Bayesovská analýza	18
1.2 DOPAD	20
1.3 METODA FUZZY LOGIKY	20
1.4 NORMATIVNÍ PŘÍSTUP K DEFINOVÁNÍ RIZIKA	21
1.4.1 ČSN ISO 31000:2018	21
2 VYMEZENÍ KYBERNETICKÉ BEZPEČNOSTI.....	23
2.1 KYBERNETICKÝ PROSTOR.....	23
2.2 KYBERNETICKÁ BEZPEČNOST	24
2.3 ISO 27000.....	26
2.4 NIS 2.....	26
2.5 NIST	28
3 PŘEHLED METOD.....	31
3.1 BUSINESS IMPACT ANALÝZA	31
3.2 MATICE RIZIK.....	34
3.3 ANALÝZA TYPU MOTÝLEK.....	36
3.3.1 FTA	37
3.3.2 ETA.....	37
3.4 LOPA	38
3.5 HRA	39
3.6 PIA A DPIA	40
3.7 GAP ANALÝZA.....	42
3.8 OCTAVE.....	42
3.9 CVSS.....	44
4 SHRUTÍ A REFLEXE	45
II PRAKTICKÁ ČÁST	46
5 KONCEPT VÝZKUMU	47
6 STANOVENÍ HODNOTICÍCH KRITÉRIÍ.....	50
6.1 IDENTIFIKOVANÁ KRITÉRIA A JEJICH POPIS.....	52

6.2	KVANTIFIKACE KRITÉRIÍ.....	64
7	MULTIKRITERIÁLNÍ ANALÝZA.....	69
7.1	STRUKTUROVÁNÍ KRITÉRIÍ DO SKUPIN	69
8	POROVNÁNÍ VÝSTUPŮ METOD.....	74
9	KONCEPCE APLIKACE PRO DOPORUČENÍ METOD ANALÝZY RIZIK	78
9.1	NÁVRH APLIKACE.....	79
9.2	NÁVRH NA ROZŠÍŘENÍ FUNKCIONALITY	82
10	SHRNUTÍ A DISKUZE	85
	ZÁVĚR.....	86
	SEZNAM POUŽITÉ LITERATURY	87
	SEZNAM OBRÁZKŮ	95
	SEZNAM TABULEK.....	96
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	97

ÚVOD

Neustálá proměnlivost a rostoucí sofistikovanost rizik v oblasti kybernetické bezpečnosti vypovídá o tom, že bezpečnost již není statickým cílem, nýbrž nepřetržitým procesem, který vyžaduje nejen adaptaci na nové hrozby, ale i soustavnou inovaci přístupů a strategií.

Tento proces zahrnuje širokou škálu metodik, nástrojů a postupů, jejichž cílem je řídit potenciální rizika. Tyto požadavky jsou navíc podpořeny legislativními rámci a normami, které organizacím ukládají povinnost provádět posuzování rizik.

Přestože dnešní legislativa či jiné regulace stanovují obecné požadavky pro identifikaci, analýzu a hodnocení rizik, často neudávají konkrétní návod, případně jaké metody by organizace měly zvolit, aby tyto úkoly splnily.

Tento prostor dává organizacím určitou volnost při interpretaci možností nakládání s riziky, na druhou stranu s sebou nese riziko, že použité metodologie mohou vést k rozdílným výsledkům, které nemusejí odrážet skutečnou podstatu hrozby. Různé přístupy mohou vést k odlišným závěrům ohledně závažnosti rizik, což může mít za následek nedostatečnou ochranu nebo naopak zbytečně nákladná opatření.

Vzhledem k tomu, že kybernetická rizika se vyvíjejí nejen technologicky, ale i v závislosti na sociálních, ekonomických a geopolitických faktorech, je zřejmé, že analýza rizik musí být nejen technicky precizní, ale také kontextově citlivá.

Výzva tedy nespočívá pouze v tom, jak efektivně aplikovat existující postupy, ale také v tom, zda jsou tyto postupy vůbec schopny držet krok s tempem změn v digitálním světě.

To vede k otázce, jaká metodika je pro konkrétní organizaci nejvhodnější a zda je vůbec možné najít univerzální přístup, který by vyhovoval různorodým potřebám a prostředím. Současně se nabízí zkoumání, která kritéria mohou být v různých oborech klíčová při výběru dané metody. Důležité je také posouzení, jak tyto faktory ovlivňují volbu metodiky a zda lze identifikovat obecně platné principy pro její výběr.

CÍL PRÁCE A POUŽITÉ METODY

Hlavním cílem je návrh nástroje pro identifikaci vhodných metod analýzy rizik v oblasti kybernetické bezpečnosti.

Za účelem dosažení hlavního cíle byly formulovány následující dílčí cíle:

1. Sumarizace metod analýzy rizik vhodných pro oblast kybernetické bezpečnosti.
2. Identifikace klíčových kritérií pro proces určení vhodnosti metod analýzy rizik.
3. Kvantitativní ohodnocení klíčových kritérií prostřednictvím expertních posudků.

V návaznosti na stanovené cíle byly formulovány výzkumné otázky:

Q1 – Které kritérium má největší vliv na výběr metody analýzy rizik v kontextu kybernetické bezpečnosti?

Q2 – Lze vyvinout nástroj, který usnadní výběr vhodné metody analýzy rizik v kybernetické bezpečnosti?

Pro naplnění cílů práce byly využity základní vědecké přístupy:

- **Bodovací analýza** – Doplnila Saatyho metodu a sloužila k určení důležitosti jednotlivých kritérií při výběru metod analýzy rizik. Bodovací analýza podpořila zodpovězení výzkumné otázky a poskytla doplňující perspektivu k hodnocení kritérií.
- **Brainstorming** – Aplikovaný k identifikaci klíčových kritérií ovlivňujících výběr metod analýzy rizik.
- **Dedukce a indukce** – Dedukce sloužila k odvození obecných závěrů z konkrétních teoretických předpokladů. Indukce umožnila formulaci obecných principů na základě analýzy konkrétních dat získaných z rozhovorů a literatury.
- **Flowcharting** – Tato metoda byla využita k vizualizaci a strukturování procesu sběru kritérií.
- **Kategorizace** – Kritéria byla rozdělena do sedmi skupin podle jejich společných charakteristik, což umožnilo zjednodušit jejich analýzu a aplikaci Saatyho metody pro stanovení jejich váhy.
- **Polostrukturované rozhovory** – Byly provedeny s cílem získat hlubší porozumění tematické oblasti a vytvořit pevné základy konceptu výzkumu.

- **Prototypování** – Tento přístup byl využit k vytvoření a testování základní verze navrhované aplikace, aby bylo možné ověřit její funkčnost a použitelnost.
- **Skupinové rozhodování** – Metoda byla použita k charakterizaci a popisu kritérií za účasti odborného týmu.
- **SMART** – Metoda byla aplikována za účelem definování procesu identifikace kritérií a jejich následné kvantifikace. Použití metody SMART bylo klíčové pro zajištění srozumitelnosti a přístupnosti celého procesu pro všechny zúčastněné strany.
- **Stanovení vah kritérií Saatyho metodou** – Metoda byla použita k určení vah kritérií prostřednictvím párového srovnání provedeného více hodnotiteli (Tabulky 15–18). Váhy byly vypočteny jako aritmetický průměr, čímž byla zajištěna jejich využitelnost pro základní výpočty v navržené aplikaci.
- **Syntéza** – Pomocí syntézy byly dílčí výsledky analýz sloučeny do uceleného konceptu.

I TEORETICKÁ ČÁST

1 KONCEPT RIZIKA

S pojmem rizika se setkáváme v odborné literatuře poměrně často. Definice rizika však může nabývat různých podob v závislosti na perspektivě, metodologickém přístupu či jiných cílech hodnocení. Rozdílný přístup k definování rizika odráží interdisciplinární povahu tohoto pojmu. Soudobí autoři se shodují, že riziko samo o sobě nemá jednotnou, všeobecně přijímanou definici. Sám Stanley Kaplan, ve své době přední přispěvatel do vědy o rizicích, napsal: „*Mnozí z vás si pamatují, že když byla Společnost pro analýzu rizik zcela nová, jednou z prvních věcí, které udělala, bylo založení výboru pro definici slova „riziko“. Tento výbor pracoval čtyři roky a pak to vzdal s tím, že v závěrečné zprávě uvedl, že je možná lepší riziko nedefinovat. Ať si ho každý autor definuje po svém, jen ať prosím každý jasně vysvětlí, co je to za způsob.*“ (Kaplan, 1997). Ve své další publikaci Kaplan (1980) tvrdí, že riziko je relativní vůči pozorovateli. Je čistě subjektivní – záleží na tom, kdo se dívá.

Některé definice rizika jsou založeny na pravděpodobnosti, náhodě nebo očekávaných hodnotách, jiné na nežádoucích událostech nebo nebezpečí a další na nejistotě. Někteří hodnotitelé považují riziko za subjektivní a epistemické, závislé na dostupných znalostech, zatímco jiné přiznávají riziku ontologický status nezávislý na hodnotitelích (Aven, 2012).

Abychom lépe porozuměli různým pohledům na riziko, může být užitečné podívat se na jeho etymologický původ. Pojem riziko lze vystopovat k italskému slovu *risco* nebo španělskému *riesco*. Obě slova vznikla pravděpodobně z latinského *rescum* (= to, co řeže). Tímto výrazem označovali námořníci útesy, které představovaly nebezpečí pro jejich lodě. (Liuzzo et al, 2014). Cattelan (2022) tvrdí, že latinské *rescum* mohlo být odvozeno od řeckého *πιζα*, které bylo používáno jako slovo pro *kořen, kámen* nebo jako metafora pro „*překážka, jíž se v moři nelze vyhnout.*“ Dále autor nabývá myšlenku, že řecké *πιζα* zřejmě našlo fonetický ekvivalent v arabském *rizq* (رزق), přičemž není zcela jasné, zda prostřednictvím středomořských kontaktů obou kultur převzala arabština tento termín z řečtiny, nebo zda tomu bylo naopak. V souladu s tímto slovem se taktéž odvíjí arabské *razaqa*, které je používáno ve významu „*Bůh, který poskytuje prostředky k obživě.*“ Tento pojem tedy na jedné straně vyjadřuje myšlenku „*šťěstí*“, „*zisku*“, „*prospěchu*“ nebo „*požehnání*“ (bezpečí před nástrahami života, jako v *πιζα* a později „*riziko*“). Na druhé straně však zůstává značně vzdálené od západního pojetí rizika, jakožto označení potenciální nežádoucí situace.

Samotný pojem riziko je velice často spojován s nedostatkem znalostí. Roeser et al. (2012) ve své knize vnesli myšlenku, že pokud bychom s jistotou věděli, že nastane v továrně výbuch, už bychom se nebavili o riziku. Podobná situace nastává, pokud bychom jistě věděli, že výbuch nenastane. Autorka dále tvrdí, že pokud mluvíme o riziku, například již zmíněné exploze, pak se jedná o situaci, kdy nevíme, zda exploze nastane. V tuto chvíli se tedy jedná o znalostech neznámého. Problém neznámého v těchto chvílích představuje problém, který vznáší řadu epistemologických otázek. Důležitost těchto otázek zdůrazňují i Ylönen a Aven (2022): „*Pro charakterizaci rizika je důležitý přístup epistemologie, zatímco pro koncept rizika kombinace přístupů ontologie a epistemologie*“. Ontologie se týká chápání reality a epistemologie k tomu, jak lze získat znalosti o této realitě. Tyto otázky však přesahují rozsah diplomové práce.

Mnozí odborníci se však shodují v jednom klíčovém aspektu, a to na existenci matematického vyjádření rizika. Uvádějí, že riziko lze kvantifikovat jako součin pravděpodobnosti výskytu dané události a jejího dopadu, případně následku. Ačkoli existují i komplexnější přístupy na výpočet rizika, zdá se, že většina vychází z tohoto základního principu. Rovnice byla odvozena na základě výstupů francouzského matematika Abraham de Moivre, který se zbýval otázkou pravděpodobnosti ve svých pojednáních o hazardních hrách (Large a Nielssen, 2012; Špaček, 2014).

$$R = P \times D$$

(1)

Kde: (R) = riziko, (P) = pravděpodobnost, (D) = dopad.

Pro hlubší porozumění tomuto vztahu se podíváme na jednotlivé přístupy k výpočtu pravděpodobnosti a následně na charakterizaci dopadu.

1.1 Pravděpodobnost

Jak udává ČSN EN IEC 31010 (2020), pravděpodobnost¹ vyjadřuje „*možnost, že se něco stane*“. Tento termín se může týkat pravděpodobné možnosti výskytu události nebo pravděpodobné možnosti výskytu specifikovaného následku. Zmíněná norma uvádí, že lze

¹ V angličtině označováno jako „*likelihood*“ nemá v některých jazycích přímý ekvivalent a často se nahrazuje termínem „*probability*“. V angličtině však „*probability*“ bývá úzce spojena s matematickým významem. V terminologii managementu rizik je „*likelihood*“ používáno tak, aby mělo širší interpretaci. (ČSN ISO 31000:2018)

pravděpodobnost klasifikovat jak **kvalitativně** (např. „*vysoce pravděpodobné*“) tak **kvantitativně** (přiřazení hodnot reprezentujících stupeň důvěry). Zdůrazňuje však, že v případě užití procentuálního vyjádření musí být uvedena povaha poměru. Jako konkrétní příklad udává nesprávné použití: „*pravděpodobnost nedodání dodávky dodavatelem je 5 %*“. Takové vyjádření považuje za nejasné, neboť z něj nelze pochopit, zda se jedná o vyjádření období či základního souboru.

Získávání dat o pravděpodobnosti může být poměrně problematické a existuje řada způsobů, a zdrojů, ze kterých můžeme tato data čerpat. Problematiku pravděpodobností také umocňuje používání alternativ jako je „frekvence“ nebo „náhoda“. To může vyvolávat dojem, že se jedná o synonyma pravděpodobnosti, tyto termíny jsou však výrazně odlišné. Aby bylo možné použít pravděpodobnost ve výpočtu rizik, je nezbytné, aby hodnotitelé rozuměli této terminologii (Hillson a Hulett, 2004).

Otázky spojené s pravděpodobnostmi, jež lze matematicky zhodnotit a tím ospravedlnit přesnost statistických metod, jsou odbornou komunitou poměrně široce probírány. Pokud by se měly binomicky rozdělit hlavní statistické metody pro získávání pravděpodobnosti, tak to budou metody **frekventistické** a metody založené na **Bayesovské** statistice. Vědní disciplína filozofie statistiky se zabývá aplikací těchto metod s důrazem na správnou interpretaci statistických postupů, jejich vstupních dat a výsledků (Vojáček, 2024).

1.1.1 Frekventistický přístup

Základní interpretace frekventistické pravděpodobnosti je vyjádřena jako: „*Relativní četnost výskytu jevu při mnoha opakováních náhodného pokusu.*“ (Pošík, 2015).

Tu můžeme vyjádřit klasickou Laplaceovou definicí pravděpodobnosti: „*Je-li základní prostor konečná neprázdná množina n elementárních jevů, které mají stejnou šanci výskytu, pak pravděpodobnost, že při realizaci náhodného pokusu nastane jev A je:*“

$$P(A) = \frac{m}{n} \quad (2)$$

Kde m je počet příznivých výsledků jevu A a n je počet všech možných výsledků.

Do těchto výpočtů můžeme využít například historická data organizací, které si mohou uchovávat interní databáze, například statistiky o chybovosti systémů ve výrobě. Tato data pak mohou využít v případě návrhu podobných systémů a výpočtu pravděpodobností poruch (Ostrom a Wilhelmsen, 2019).

Data nemusí uchovávat pouze příslušná organizace, ale existují i komerční či jiné veřejně dostupné zdroje dat. To mohou být různé pojišťovny, organizace zaměřené na sběr dat nebo příručky prevence ztrát (Ostrom a Wilhelmsen, 2019).

V oblasti kybernetické bezpečnosti může být konkrétním příkladem Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Ten každoročně vydává Zprávu o stavu kybernetické bezpečnosti. Ve své poslední zprávě z roku 2023 tvrdí, že od roku 2022 byl pozorován nárůst kybernetických incidentů téměř o 80 %. Mezi nejčastější druhy útoků patří podle NÚKIB různé variace phishingu a DDoS útoky. Druhým příkladem může být ENISA (Evropská agentura pro bezpečnost sítí a informací), která vydává veřejně dostupný registr rizik.

1.1.2 Bayesovská analýza

Bayesova věta pochází od reverenda Thomase Bayese, který její základy vytvořil před více než 250 lety, a Pierre-Simon Laplace ji později rozvinul a její finální podobu publikoval v roce 1812. Bayesova věta umožňuje aktualizovat pravděpodobnosti na základě nových důkazů (Ostrom a Wilhelmsen, 2019).

Bayesovská analýza je založena na apriorní a aposteriorní distribuční funkci. To znamená, že zvažuje změnu pravděpodobnosti před výzkumem a po výzkumu. Pomocí této analýzy jsme schopni odpovědět, jak se změnila pravdivost hypotézy vůči naměřeným datům. Bayesovská statistika je založena na Bayesově větě, která určuje pravděpodobnost, že dojde k určité události, s přihlédnutím k předchozím znalostem o souvisejících podmínkách (Vojáček, 2024; Hackenberger, 2019).

Matematické vyjádření:

$$P(A|B) = \frac{P(B|A) \times P(A)}{P(B)}$$

Kde: (3)

A a B jsou události, přičemž $P(B) \neq 0$

$P(A|B)$ je podmíněná, aposteriorní pravděpodobnost, kdy se událost A objeví, pokud nastala událost B

$P(B|A)$ je podmíněná aposteriorní pravděpodobnost, kdy se událost B objeví, pokud nastala událost A

$P(A)$ a $P(B)$ je apriorní vyjádření pravděpodobnosti A a B

Zajímavým popularizačním příkladem z oblasti pravděpodobnosti je takzvaný Monty Hallův problém, známý také jako problém tří dveří. Přestože řešení tohoto problému je poněkud neintuitivní, při použití Bayesovské analýzy se dostaneme k zajímavému pravděpodobnostnímu výsledku.

Formulace problému (matweb.cz):

Předpokládejme, že existují troje dveře. Za dvěma z nich jsou kozy a za jedněmi je výherní cena – auto. Soutěžící si nejprve vybere jedny dveře a ukáže na ně. Moderátor, který ví, co je za jednotlivými dveřmi, poté otevře jedny ze zbývajících dvou dveří. Za dveřmi, které se moderátor rozhodl otevřít, je koza. Soutěžící nyní má nové informace a může se rozhodnout, zda si ponechá svou původní volbu, nebo ji změní na druhé, dosud neotevřené dveře. Z hlediska pravděpodobnosti je výhodnější původní volbu změnit. Toto tvrzení lze podložit pomocí Bayesovské analýzy.

Původní výběr dveří odhaduje apriorní pravděpodobnost výhry na: $P_{auto} = \frac{1}{3}$.

A pravděpodobnost, že za dveřmi bude koza $P_{koza} = \frac{2}{3}$. Po otevření jedné dveří moderátorem a získání nové informace se pravděpodobnosti aktualizují (aposteriorní pravděpodobnost). Intuitivně by se mohlo zdát, že šance na výhru auta je nyní 50:50 mezi zbývajících dvěma dveřmi. Bayesovská analýza však ukazuje, že tomu tak není.

$$P(\text{auto}|\text{moderátor otevřel kozu}) = \frac{P(\text{moderátor otevřel kozu}|\text{auto}) \times P(\text{auto})}{P(\text{moderátor otevřel kozu})} = \frac{1}{3} \quad (4)$$

Aposteriorní pravděpodobnost, že soutěžící původně vybral auto, tedy zůstává $\frac{1}{3}$. Pokud však volbu dveří změní, pravděpodobnost výhry auta je $\frac{2}{3}$.

Novotný (2018) však rozvádí, že zde samozřejmě hraje roli několik proměnných například ohledně znalosti moderátora. Pokud moderátor chce soutěžícímu pomoci a zasáhne pouze v případě, že volil kozu, pak musí volbu jednoznačně změnit. Pokud však moderátor chce soutěžícího připravit o výhru a zasáhne pouze v případě, kdy první volba byla auto, pak soutěžící musí trvat na původní volbě. To dokazuje tvrzení, že riziko závisí na znalostech.

1.2 Dopad

ČSN ISO 31000 (2018) definuje následek jako „*výsledek události působící na cíle*“. Událost ve smyslu „*výskyt nebo změna určité množiny okolností*“. Rausand a Haugen (2020, str 44) pak definují jako dopad „*konkrétní poškození jednoho nebo více aktiv*.“ Dále rozvádějí myšlenku o problematice definice dle normy, čímž se shodují s Aven a Ylönen (2019), jejichž myšlenka bude rozvedena v kapitole 1.3.1. Rausand a Haugen (2020) opodstatňují svou definici, ohledně dopadu rizika, otázkou, že musíme identifikovat, kdo nebo co by mohlo být ovlivněno působením rizika. Otázku „kdo“ nebo „co“ proto nazývají aktivem, jež definují jako „*něco, čeho si vážíme a chceme zachovat*“.

Dopad můžeme klasifikovat dle jeho závažnosti. Závažnost může být vyjádřena finanční hodnotou nebo jako kategorie (např. katastrofální). Je však důležité jednotlivé kategorie podrobně popsat, aby relevantní stakeholderi všem formulacím porozuměli (Rausand a Haugen, 2020).

1.3 Metoda fuzzy logiky

Užití pojmů jako „*vysoce pravděpodobné*“ případně „*kritický dopad*“ nám nechává poměrně široký interpretační prostor. Pro takové případy můžeme užít fuzzy logiku, která je vhodná pro práci s neurčitostí. Zvláště při analýze rizik, kdy potřebujeme zohlednit nejen pravděpodobnost události, ale i její potenciální dopad, nám fuzzy logika umožňuje lépe modelovat nepřesnosti a subjektivní hodnocení. Díky tomu můžeme efektivněji klasifikovat a řídit rizika, i když pracujeme s informacemi, které nejsou jednoznačně kvantifikovatelné (Merola et al., 2024).

Kvůli tomuto problému byl vytvořen koncept fuzzy množin, tedy množin, u nichž příslušnost není pouze binární (ano/ne), ale plynulá. Podle tohoto přístupu mohou proměnné nabývat různých stupňů pravdivosti či nepravdivosti, vyjádřených hodnotami v rozmezí od 1 (pravda) do 0 (nepravda). Tím se usnadňuje vyjádření neurčitosti a umožňuje modelování kvalitativních a nejednoznačných informací (Merola et al., 2024).

Fuzzy logika je založena na teorii fuzzy množin. Termín „fuzzy“ označuje něco neostrého, matného, neurčitého či vágního. Tato teorie se zaměřuje na zachycení reality tak, jak se projevuje ve své nepřesnosti a neurčitosti (Doskočil a Lacko, 2022).

1.4 Normativní přístup k definování rizika

Mezinárodní standardy přistupují k definování rizika různými způsoby. Některé však poskytují komplexnější rámec pro jeho řízení. Mezi nejvýznamnější standardy v této oblasti patří ISO 9001, ISO 45001, ISO 14001, ISO 27000. Tyto normy integrují koncept **risk-based thinking**² (myšlení založené na riziku, dále jen RBT). Koncept, na kterém jsou normy založeny, vede organizace k systematickému a proaktivnímu přístupu k riziku. Organizace tak mohou předcházet dynamicky se vyvíjejícímu rizikovému prostředí (Matuszak-Flejszman, Paliwoda, 2021; iso.org).

Výše zmíněné standardy zakotvily koncept RBT do Demingova³ cyklu, který lze chápat jako neustálý proces, který obsahuje kroky stanovené v ČSN EN ISO 9001 (2016):

- **PLAN** „Plánuj – Stanov cíle systému a jeho procesů a zdroje potřebné pro dosažení výsledků v souladu s požadavky zákazníka a s politikami organizace, identifikuj rizika a příležitosti a zaměř se na ně.“
- **DO** „Dělej – zaváděj to, co bylo naplánováno.“
- **CHECK** „Kontroluj – monitoruj a (přichází-li to v úvahu) měř procesy a výsledné produkty a služby ve vztahu k politikám, cílům, požadavkům a plánovaným činnostem a podávej zprávy o výsledcích.“
- **ACT** „Jednej – podle potřeby přijímej opatření pro zlepšování výkonnosti.“

1.4.1 ČSN ISO 31000:2018

Mezinárodní norma o managementu rizik má tu výhodu, že poskytuje obecné zásady pro řízení rizik, které mohou být využity různými druhy organizací či jednotlivcem. Zmíněná norma definuje **riziko** jako: „účinek nejistoty na cíle“, jehož definici rozšiřuje o poznámky:

- „účinek je odchylka od očekávaného. Může být pozitivní, negativní nebo obojí a může řešit, vytvářet nebo vyústit v příležitosti a hrozby“.
- „Cíle mohou mít různá hlediska a kategorie a mohou být uplatňovány na různých úrovních“.

Implementaci procesu managementu rizik pro kybernetickou bezpečnost doporučuje řada autorů. Mezi nimi i Crotty a Daniel (2022), podle nichž proces napomáhá identifikaci aktiv

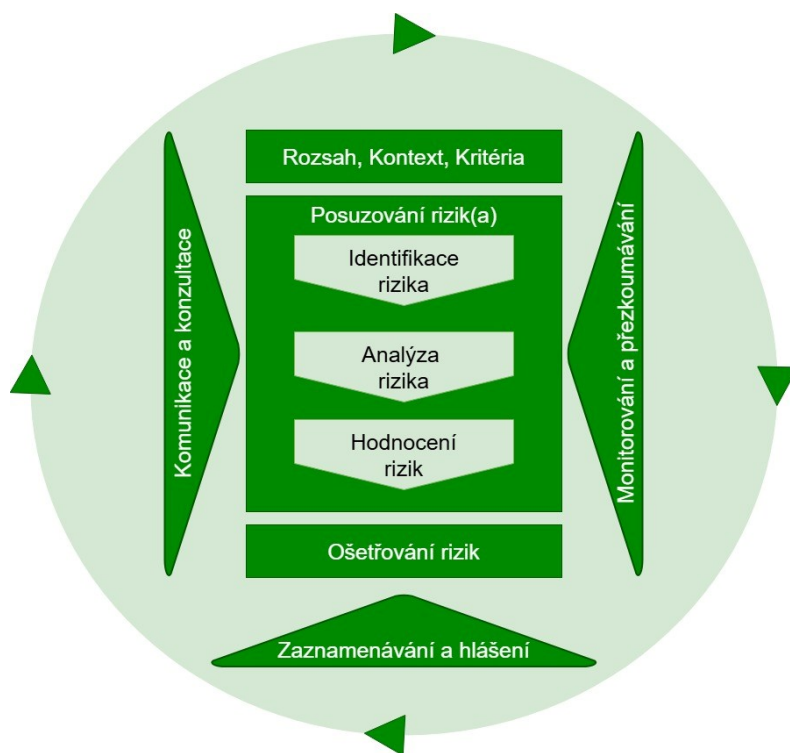
² ISO 9001 překládá jako „zvažování rizik“

³ Někdy označovaného jako PDCA cyklus

organizace, potenciálních hrozeb, zranitelností a pravděpodobným důsledkům, kterým může být organizace vystavena. Proces managementu rizik, jehož výsledky slouží jako základ pro vytvoření individuálního plánu řízení rizik, znázorněném na obrázku (1). Tento plán je zaměřen na prevenci, minimalizaci, přenos nebo akceptaci rizika v závislosti na jeho typu a úrovni, kterou je organizace ochotna přijmout.

Na druhou stranu autoři jako Aven a Ylönen (2019) argumentují, že některé části normy, jako třeba definice rizika, je poměrně problematická či zavádějící. Jako jeden z argumentů udávají problematiku o spojení konceptu rizika s formulacemi cílů („*Účinek nejistoty na cíle*“). Po podrobnějším zkoumání této definice podle autorů vyvstává otázka, zda riziko neexistuje, pokud nejsou definovány cíle.

Proces managementu rizik je soubor koordinovaných činností zaměřených na řízení a kontrolu organizace ve vztahu k rizikům. Pro zajištění účinného řízení rizik by mělo být v organizacích postupováno právě na základě procesu stanoveného v ČSN ISO 31000. Proces managementu rizik může být aplikován na strategické, provozní, programové nebo projektové úrovni, což znázorňuje obrázek 1 uvedený níže (ČSN ISO 31000:2018; Matuszak-Flejszman, Paliwoda, 2020).



Obrázek 1 Proces managementu rizik

(Zpracování: vlastní, na základě ČSN ISO 31000)

2 VYMEZENÍ KYBERNETICKÉ BEZPEČNOSTI

Podle Koloucha (2019) je potřeba pro definici kybernetické bezpečnosti nejprve určit, jak to sám autor nazývá, „*ono pomyslné hrací pole, ve kterém se tyto útočné a obranné akce odehrávají.*“

2.1 Kybernetický prostor

Kolouch (2019) konstatuje, že samotné definice podle Českého výkladového slovníku kybernetické bezpečnosti, případně podle Oxford Dictionary, neodrážejí komplexní a pochopitelnou definici kyberprostoru.

Na nejasnostech v oblasti kyberprostoru se shoduje i Hrůza (2013), který za nejasné považuje:

- Definici.
- Rozměr (konečnost/nekonečnost).
- Hranice (státy, organizace).
- Pravomoc a odpovědnost.

Kolouch (2019 str. 36) proto nabízí následující definici kyberprostoru:

„Kyberprostor je tvořen prvky informačních a komunikačních technologií, které vytvářejí pomocí protokolu TCP/IP celosvětovou, globální počítačovou síť, a jednotlivými počítačovými systémy, které jsou do této sítě připojeny a které v ní interagují. Kyberprostor je virtuální realitou, nemající konec ani začátek. Tato virtuální realita je však zcela závislá na materiální podstatě, tedy technologiích nacházejících se ve světě reálném.“

Z této definice plyne, že kyberprostor je určité nehmotné médium, které vzniklo díky médiu hmotnému (počítačové systémy, cloudová úložiště, prvky sítě). Kyberprostor se tedy adaptuje na změny v materiálním médiu, avšak při úplném kolapsu všech součástí materiálního média samotný kyberprostor taktéž přestane existovat.

Kybernetický prostor je prostorem veřejným. To znamená, že není vlastněn žádným národem, osobou či úřadem. Proto podle autorů musí být bezpečnostní aktivity v tomto prostoru koordinovány mezi zúčastněnými subjekty na různých úrovních. Z tohoto důvodu je potřeba, aby zúčastněné subjekty mezi sebou sdílely informace o rizicích a společně koordinovaly opatření proti potenciálnímu ohrožení (Doucek et al., 2019).

Kolektiv autorů pak stanovuje charakteristiky kybernetického prostoru jako (Doucek et al., 2019, str 18):

- *Anonymita – identita uživatele, který vyvíjí svoje aktivity v kybernetickém prostoru, není jasně prokazatelná a garantovaná žádnou autoritou.*
- *Asymetričnost – činnost v kybernetickém prostoru může mít významný dopad na ostatní uživatele sítě bez ohledu na význam a důvěryhodnost uživatele, který tuto aktivitu vyvinul.*
- *Neexistence hranic – aktivity v kybernetickém prostoru nejsou omezovány žádnou jurisdikcí nebo suverenitou, právním systémem nebo kulturou.*
- *Okamžitost – akce provedená v kybernetickém prostoru může mít okamžitě celosvětový dopad.*
- *Volný vstup i ukončení pobytu v něm – kdokoli, kdykoli může do kybernetického prostoru vstoupit, ale také v něm může kdykoli ukončit svoji aktivitu.*
- *Interakce – interaktivní činnosti v něm mohou vytvářet znalosti a mohou též vést k významnému ovlivnění ostatních uživatelů.*

2.2 Kybernetická bezpečnost

Podle Nařízení Evropského parlamentu a Rady (EU) 2019/881 lze **kybernetickou bezpečnost** chápat jako: “činnosti nezbytné k ochraně sítí a informačních systémů, jejich uživatelů a dalších osob dotčených kybernetickými hrozbami.” Stejně nařízení definuje **kybernetickou hrozbu** jako: “jakákoliv potenciální okolnost, událost nebo čin, které mohou poškodit, narušit nebo jinak nepříznivě ovlivnit sítě a informační systémy, jejich uživatele a další osoby.” (Evropský parlament a Rada EU, 2019)

V oblasti kybernetické bezpečnosti a ochrany informací je klíčové zajistit důvěrnost, integritu a dostupnost dat, což je známé jako paradigma CIA⁴. Tuto povinnost ukládá například český zákon o kybernetické bezpečnosti č. 181/2014 Sb. (Česko, 2014). Podle dokumentu ENISA kybernetická bezpečnost toto paradigma CIA nejen uplatňuje na vztahy a objekty v kyberprostoru, ale také jej rozšiřuje o ochranu soukromí jak fyzických, tak

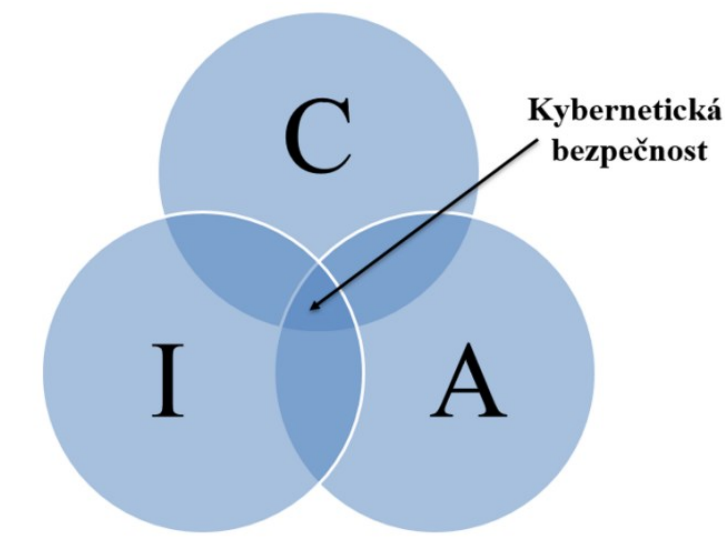
⁴ z anglického confidentiality, integrity, availability.

právnických osob (jednotlivců i korporací) (European Union Agency For Network And Information Security, 2015).

Důvěrnost (Confidentiality): Pojem charakterizuje zásadu, podle níž je přístup k informacím, datům či informačním a komunikačním technologiím (ICT) omezen výlučně na subjekty s příslušnou autorizací. Vzhledem k rozsáhlému objemu zpracovávaných informací se jeví jako účelné implementovat klasifikaci informací v souladu s ustanoveními zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti č. 412/2005 Sb., (Kolouch et al., 2022). Vyhláška č. 82/2018 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jako vyhláška o kybernetické bezpečnosti) stanovuje hodnocení důvěrnosti na základě TLP protokolu (Česko, 2018).

Integrita (Integrity): Pojem je definován dle výkladového slovníku kybernetické bezpečnosti jako: „*vlastnost přesnosti a úplnosti.*“ Kde autor dále rozšiřuje definici o „*Jistota, že data nebyla změněna.*“ Integrita může být zajištěna pomocí kontrolních či hashovacích funkcí, nebo redundancí (Jirásek et al., 2015). Stupnici pro hodnocení integrity stanovuje vyhláška o kybernetické bezpečnosti (Česko, 2018).

Dostupnost (Availability): Je zajištění garance přístupu k informacím, datům nebo počítačovému systému v okamžiku potřeby (Kolouch et al., 2022). I v případě dostupnosti je stupnice pro hodnocení aktiv stanovena v příloze vyhlášky o kybernetické bezpečnosti.



Obrázek 2 Triáda CIA

(Zdroj: Kolouch et al., 2022)

V odborné literatuře se vedle tradiční triády CIA objevuje její rozšíření označované jako **Parkerian hexad**. Tento koncept doplňuje původní prvky CIA o tři další (Pender-Bey, 2012):

- **P/C – Possession/Control** (držení/kontrola).
- **A – Authenticity** (autentičnost).
- **U – Utility** (užitečnost).

Rozšíření paradigmatu CIA o Parkerian hexad bylo diskutováno i v případě Národního úřadu pro kybernetickou a informační bezpečnost při přípravě nového zákona o kybernetické bezpečnosti. NÚKIB, jak sám deklaruje, usiluje o maximální transparentnost, a proto zveřejňuje podněty získané z veřejné konzultace k návrhu nového zákona o kybernetické bezpečnosti a příslušných souvisejících předpisů. Jeden z těchto podnětů uvádí: „*Je nezbytné si uvědomit, že k narušení dostupnosti, důvěrnosti či integrity informací a dat nemusí při úspěšném útoku vůbec dojít; útočník může systém pouze zneužít k různým účelům nebo jej kompromitovat a vyčkávat na vhodnou příležitost.*“ NÚKIB však tento návrh zamítl s tím, že daný koncept je pravidelně předmětem interních diskusí, přičemž se opakovaně dospělo k závěru, že triáda CIA zůstává pro hodnocení kybernetické bezpečnosti dostatečným rámcem (NÚKIB, 2024, str 5).

2.3 ISO 27000

Standardy z řady ISO/IEC 27000 poskytují přehled systémů řízení bezpečnosti informací, označovaný jako Information Security Management System (dále jen ISMS). Výhodou je využitelnost pro různé velikosti organizací. Organizace mohou použít standardy ISMS pro správu a bezpečnost svých aktiv, jako jsou například finanční údaje, duševní vlastnictví, informace o zaměstnancích a jiná data, která jim byla svěřena stakeholdery nebo dalšími třetími stranami (Smejkal et al., 2019).

2.4 NIS 2

Legislativní rámec, označovaný jako směrnice EU 2022/2555 – NIS 2, je určený ke zvýšení kybernetické bezpečnosti v celé Evropské unii. Tento dokument vychází z původní směrnice NIS, avšak rozšiřuje její oblast působnosti a zpřísňuje požadavky kladené na subjekty spadající pod působnost směrnice. Subjekty tak musí splňovat rozmanité množství technických, provozních a organizačních opatření pro řízení rizik kybernetické bezpečnosti.

Směrnice nařizuje subjektům řízení „všech rizik“, aby subjekty byly schopny čelit různému spektru hrozeb, od kybernetických útoků, až k fyzické bezpečnosti. Těmito kroky vytváří směrnice opatření pro komplexní zajištění ochrany a odolnosti daných subjektů (Cyber Risk GmbH; směrnice EU 2022/2555).

Opatření na řízení kybernetických rizik

Jak již bylo řečeno, směrnice klade důraz na přístup zohledňující všechny druhy rizik, jehož cílem je chránit sítě a informační systémy a fyzické prostředí uvedených systémů před incidenty, které podle normy zahrnují alespoň:

- a) politiku analýzy rizik a politiku bezpečnosti informačních systémů*
- b) řešení incidentů*
- c) řízení kontinuity provozu, jako je například správa zálohování a obnova provozu po havárii, krizové řízení*
- d) bezpečnost dodavatelského řetězce včetně bezpečnostních aspektů týkajících se vztahů mezi každým subjektem a jeho přímými dodavateli nebo poskytovateli služeb*
- e) zabezpečení pořízování, vývoje a údržby sítí a informačních systémů, včetně zveřejňování zranitelností a jejich řešení*
- f) politiky a postupy za účelem posouzení účinnosti opatření k řízení kybernetických bezpečnostních rizik*
- g) základní postupy kybernetické hygieny a školení v oblasti kybernetické bezpečnosti*
- h) politiky a postupy týkající se používání kryptografie a případně šifrování*
- i) bezpečnost lidských zdrojů, postupy kontroly přístupu a správa aktiv*
- j) v příslušných případech používání vícefaktorových autentizačních řešení nebo trvalých autentizačních řešení, zabezpečené hlasové, obrazové a textové komunikace a zabezpečených systémů nouzové komunikace v rámci subjektu. (Směrnice EU – NIS 2, 2022).*

Pro pochopení těchto opatření je zásadní definovat samotné pojmy, které směrnice používá.

Riziko = *potenciální ztráta nebo narušení v důsledku incidentu, přičemž toto riziko je vyjádřeno jako kombinace rozsahu takové ztráty nebo takového narušení a pravděpodobnosti vzniku incidentu (Směrnice EU – NIS 2, 2022).*

Incident = „událost narušující dostupnost, autenticitu, integritu nebo důvěrnost uchovávaných, předávaných nebo zpracovávaných dat nebo služeb, které jsou nabízeny prostřednictvím sítí a informačních systémů, nebo které jsou jejich prostřednictvím přístupné“ (Směrnice EU – NIS 2, 2022).

Nový zákon o kybernetické bezpečnosti

Legislativní rámec směrnice NIS 2 má být začleněn do nového zákona o kybernetické bezpečnosti. Vláda předložila návrh zákona Poslanecké sněmovně dne 25. července 2024, nicméně k 1. březnu 2025 jeho projednávání stále vázne. Podle informací na webu Poslanecké sněmovny proběhlo druhé čtení 21. ledna 2025 na 127. schůzi, přičemž pozměňovací návrhy byly rozeslány 22. ledna 2025 v 10:54 hod. Ke dni 1. března 2025 však Garanční výbor pro bezpečnost návrh zákona ještě neposoudil. Pro jeho dokončení je nadále potřeba absolvovat třetí čtení, poté bude předložen Senátu a následně prezidentovi k podpisu (Poslanecká sněmovna Parlamentu České republiky, psp.cz).

Nový český zákon o kybernetické bezpečnosti nebyl do této práce zařazen. Jeho přijetí, které má být v souladu se směrnicí NIS 2, se nadále odkládá kvůli probíhajícím diskusím mezi zákonodárci o jeho finální podobě, což znemožnilo jeho včasné a relevantní začlenění do diplomové práce.

2.5 NIST

Je vládní agenturou Spojených států amerických, zkratka představuje název Národní institut pro standardy a technologie (National Institute of Standards and Technology, dále jen „NIST“). Vydává soubor směrnic pro bezpečnost informací, které poskytují obecná doporučení pro provádění bezpečnostních kontrol a pomáhají organizacím chránit své informace před hrozbami (Barborík, b.r.).

V kontextu kybernetické bezpečnosti je NIST známý především díky svým publikacím z řady **Special Publication (SP) 800**, které obsahují směrnice, doporučení a osvědčené postupy pro ochranu informačních systémů a technologií. Mezi nejznámější patří například NIST Cybersecurity Framework.

NIST Cybersecurity Framework (CSF) dává průmyslu, vládním agenturám a dalším organizacím pokyny pro řízení rizik kybernetické bezpečnosti. Nabízí taxonomii výsledků kybernetické bezpečnosti na vysoké úrovni, kterou může využít každá organizace – bez ohledu na její velikost, odvětví nebo vyspělost – k lepšímu pochopení, posouzení, stanovení

priorit a komunikaci o svém úsilí v oblasti kybernetické bezpečnosti. CSF nepředepisuje, jak by mělo být výsledků dosaženo. Spíše odkazuje na online zdroje, které poskytují další pokyny k postupům a kontrolním mechanismům, které by mohly použít k dosažení těchto výsledků (NIST, 2024a).

CSF je navržen jako univerzální nástroj, jehož cílem je posílit kybernetickou bezpečnost napříč různými organizacemi – od malých veřejných škol až po rozsáhlé korporace. Jeho základ tvoří šest hlavních činností, které komplexně pokrývají oblast kybernetické bezpečnosti v rámci organizací (Polách, 2024):

- Govern (spravuj).
- Identify (identifikuj).
- Protect (ochraňuj).
- Detect (detekuj).
- Respond (reaguj).
- Recover (zotavuj se).

Mezi další významné publikace NIST patří:

NIST SP 800-82r3

Tento dokument obsahuje pokyny pro vytvoření bezpečné provozní technologie, přičemž zohledňuje její jedinečné požadavky na výkon, spolehlivost a bezpečnost. Dokument nabízí přehled o provozních technologiích a typických systémových topologiích, identifikuje běžné hrozby a zranitelnosti těchto systémů a doporučuje bezpečnostní opatření ke zmírnění souvisejících rizik (NIST, 2023).

NIST SP 800-50r1

Tato publikace nabízí federálním agenturám a organizacím směrnice pro tvorbu a správu komplexního přístupu k budování vzdělávacího programu zaměřeného na kybernetickou bezpečnost a ochranu soukromí. Přístup je navržen tak, aby vyhovoval potřebám jak velkých, tak malých organizací, včetně těch, které teprve zavádějí nový program. Vychází z obecně uznávaných standardů, předpisů, legislativy a osvědčených postupů. Doporučení lze přizpůsobit a začlenit do organizace jako součást širšího procesu řízení iniciativ pro zvyšování povědomí, školení a vzdělávání (NIST, 2024b).

Cílem programu je podpořit změny v chování zaměstnanců v oblasti řízení rizik a přispět k vytvoření organizační kultury, která klade důraz na bezpečnost a ochranu soukromí. Součástí pokynů jsou také navržené ukazatele a metody hodnocení, které organizacím umožňují průběžně zdokonalovat a aktualizovat program v souladu s měnícími se požadavky (NIST, 2024b).

NIST SP 800-184

Tento dokument je určen osobám, které mají odpovědnost za rozhodování v souvislosti s obnovou po kybernetických událostech. Má za cíl pomoci organizacím při zdokonalování jejich plánů, procesů a postupů pro zotavení po kybernetických událostech, aby mohly rychleji obnovit běžný provoz (NIST, 2016).

3 PŘEHLED METOD

Analýza rizik je „*systematická studie k identifikaci a popisu co se může pokazit a jaké mohou být příčiny, pravděpodobnosti a důsledky.*“ (Rausand a Haugen, 2020).

Dle Čermáka (2009) odborná literatura nepojednává o tom, kdo by měl analýzu rizik provádět. Podle prováděcího subjektu ji však můžeme rozdělit na interní, která je prováděna vlastními pracovníky, a externí, která je prováděna jako služba konzultanty společnosti. Mezi výhody analýzy rizik, prováděnou interními pracovníky, patří aspekty, jako znalosti prostředí a procesů a nižší cena. Na druhou stranu externí analýza může poskytnout zkušenosti z jiných společností a odbornost, na úkor její ceny.

Podle ISO 27005:2023 platí, že „*metody managementu rizik informační bezpečnosti mají být v souladu s přístupem a metodami používanými k řízení ostatních rizik organizace.*“ (ISO 27005:2023, str 19).

Požadavky na užití metody v rámci informační bezpečnosti pak klade norma ISO/IEC 27001:2022, kdy je organizace povinna zajistit takové posouzení rizik informační bezpečnosti, které je konzistentní, platné a srovnatelné s výsledky. Požadované vlastnosti výsledků stanoví následovně (ISO/IEC 27001:2022):

- **konzistence:** „*posouzení stejných rizik prováděná různými osobami nebo stejnými osobami při různých příležitostech ve stejném kontextu má vést k podobným výsledkům.*“
- **srovnatelnost:** „*mají být definována kritéria posuzování rizik, aby se zajistilo, že posouzení provedená pro různá rizika přinášejí srovnatelné výsledky, pokud představují rovnocenné úrovně rizika.*“
- **validita:** „*posouzení mají přinášet výsledky, které co nejvíce odpovídají skutečnosti.*“

Z důvodu splnění výše zmíněných požadavků budou v následujících kapitolách definovány některé metody analýzy rizik podle normy ČSN EN IEC 31010, která stanovuje techniky posuzování rizik.

3.1 Business impact analýza

Business impact analysis, v češtině normativně označována jako **analýza dopadu na podnikání** (dále jen BIA) „*se používá k určování kritičnosti a časových rámců obnovy*

procesů a přidružených zdrojů (např. osob, zařízení a informační technologie) k umožnění vhodného plánování pro narušující události.“ (ČSN EN IEC 31010, 2020, str 68).

„BIA analyzuje, jak by incidenty a události mohly ovlivnit funkce organizace, a identifikují a kvantifikují se způsobilosti, jež by byly potřebné k jejich zvládnutí. Specificky analýza BIA poskytuje dohodnuté porozumění:

- kritičnosti klíčových procesů podnikání, funkcí a přidružených zdrojů a klíčových vzájemných závislostí, jež v organizaci existují,
- jak bude narušující událost ovlivňovat kapacitu a způsobilost dosáhnout kritických cílů podnikání,
- kapacitě a způsobilosti potřebné ke zvládnutí dopadu narušení a obnovy na dohodnuté úrovni fungování.

Analýza BIA může být vykonávána s použitím dotazníků, rozhovorů, strukturovaných workshopů nebo kombinací všech“ (ČSN EN IEC 31010, 2020, str 68).

Během analýzy se nastavují cíle obnovy, které zahrnují určení maximálně přijatelného času prostojů (MTD), cílů obnovy dat (RPO), schopností obnovy (RTC) a dalších časových parametrů pro klíčové procesy organizace (Savolainen et al., 2024).

Podle Tjoa (et al., 2008) spočívají nejdůležitější kroky BIA v následujících krocích:

- (1) Určení aktiv organizace a jejich odpovědných vlastníků.
- (2) Výběr vhodných zaměstnanců pro efektivní sběr relevantních informací.
- (3) Identifikace scénářů, které by mohly významně ohrozit společnost, její aktiva nebo finanční stabilitu.
- (4) Stanovení časového období, ve kterém by narušení obchodních aktivit bylo nepřijatelné.



Obrázek 3 Postup BIA

(Zdroj: vlastní zpracování, dle Sikdar, 2011)

Hlavními výstupy analýzy BIA pro každou obchodní aktivitu: jsou maximální tolerovatelná doba přerušení (MTPD) a cíle bodu obnovy. MTPD stanovuje dobu, po jejímž překročení by přerušení určité obchodní činnosti mohlo ohrozit samotnou existenci společnosti. RPO pak definuje časový okamžik, kdy musí být po obnovení obchodní činnosti obnoveny základní informace (Tjoa et al., 2008).

Tabulka 1 Silné stránky a omezení metody BIA

Silné stránky	Omezení
✓ Porozumění procesům umožňující organizaci dosahovat cílů. ✓ Potřebné informace, které slouží plánování reakce na narušující událost. ✓ Porozumění klíčovým zdrojům požadovaných v případě narušení. ✓ Opětovné stanovení provozního procesu a zlepšení odolnosti organizace.	✓ Spoléhá na znalosti a vnímáních účastníků, nesoucí s sebou různé formy rizik ohledně příliš optimistickým očekáváním požadavků na zotavení. ✓ Skupinové rozhodování může ovlivňovat analýzu kritického procesu. ✓ Problematika se získáváním odpovídající úrovně porozumění o funkcích a činnostech organizace.

(Zdroj: ČSN EN IEC 31010)

Analýza tedy pomáhá organizaci identifikovat kriticky důležitá aktiva, která by případně mohla být nejzranitelnější vůči kybernetickým hrozbám. BIA je nepřetržitý proces, který musí být prováděn periodicky, aby nové dopady, které mohou být vneseny vnitřními nebo vnějšími změnami v podnikatelském prostředí, byly zachyceny, uvedeny a upozorněny na výkonné vedení. Aktualizace lze plánovat měsíčně nebo ročně podle stanovených požadavků (Sikdar, 2011).

3.2 Matice rizik

Matice rizik, která může být taktéž označována jako tepelná mapa, se využívá pro vizualizaci a klasifikaci významnosti rizika. Pro matici se zvolí stupnice charakterizující pravděpodobnost a dopad rizika. Podle zmíněné normy ISO mohou mít zvolené stupnice jakýkoliv počet bodů. Nejobvyklejší jsou však tři nebo pětibodové stupnice. Pro osy matice se mohou zvolit stupnice jak kvalitativní, kvantitativní, tak semi-kvantitativní. S buňkami v matici mohou být spojeny pravidla rozhodování (např. naléhavost odezvy). Výhodou použití matice je její jednoduchost a aplikovatelnost na jakékoliv úrovni. Může se taktéž používat jako nástroj pro třídění rizik nebo určení pozornosti. Výhodou je taktéž, že se může použít v případech, kdy není dostupný potřebný dostatek vstupních dat pro podrobnější analýzu (ČSN EN IEC 31010, 2020).

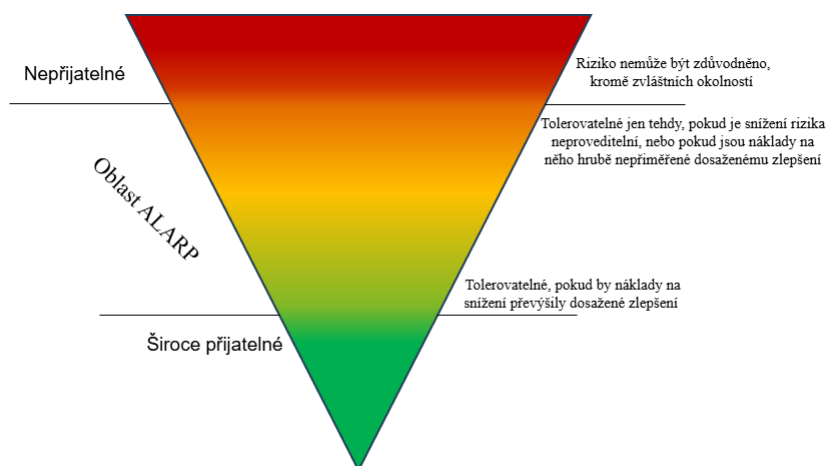
Tabulka 2 Příklad matice rizik

			Dopad				
			Zanedbatelný	Menší	Střední	Kritický	Katastrofální
			1	2	3	4	5
Pravděpodobno	Časté	5	Střední	Střední	Vysoké	Vysoké	Vysoké
	Pravděpodobné	4	Střední	Střední	Střední	Vysoké	Vysoké
	občasné	3	Nízké	Střední	Střední	Střední	Vysoké
	Ojedinělé	2	Nízké	Nízké	Střední	Střední	Střední
	Nepravděpodobné	1	Nízké	Nízké	Nízké	Střední	Střední

(Zdroj: vlastní zpracování)

Ve spojení s barevným škálováním rizika se používají principy ALARP (as low as reasonably practicable) a SFAIRP (so far as is reasonably practicable). ALARP vyžaduje snížení úrovně rizika natolik, aby bylo rozumně proveditelné. SFAIRP vyžaduje rozumně proveditelné zajištění bezpečnosti. Definici „rozumně proveditelné“ norma převádí na legislativu či judikaturu dané země (ČSN EN IEC 31010, 2020).

Tyto principy reprezentují prostor mezi rizikem „přijatelným“ a rizikem „nepřijatelným“ na následujícím obrázku.



Obrázek 4 Princip ALARP

(Zdroj: vlastní zpracování, na základě ČSN EN IEC 31010)

Využití matice rizik, přes její jednoduchost, vyžaduje například vyhláška 316/2021 Sb. Vyhláška o některých požadavcích pro zápis do katalogu cloud computingu, která požaduje ve své příloze č. 5 „zprávu nebo jiný doklad o zhodnocení přírodních zdrojů rizik a zdrojů rizik vyvolaných činností člověka musí obsahovat přehledně a srozumitelně“: podle bodu e) **označení rizika v matici rizik**. Dále rozvádí, že „přílohou zprávy budou zvolené škály pravděpodobnosti aktivace zdroje rizik a míry dopadu, kritéria pro hodnocení významnosti rizik a zpracovaná matice rizik, která kombinuje pravděpodobnost aktivace zdroje rizik a míru dopadu a ukazuje jaká rizika z toho vyplývají s jakou mírou přijatelnosti“ (Česko, 2021).

Tabulka 3 Silné stránky a omezení Matice rizik

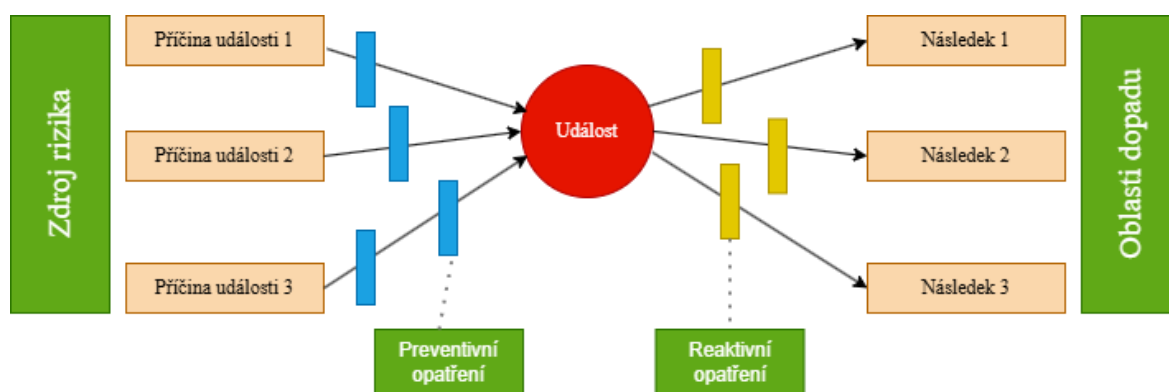
Silné stránky	Omezení
✓ Snadné použití. ✓ Rychlost analýzy. ✓ Vizuální zobrazení významnosti rizika.	✓ Správné stanovení stupnic může být obtížné. ✓ Validita stanoveného rizika závisí na stanovení stupnic. ✓ Subjektivnost.

(Zdroj: ČSN EN IEC 31010)

3.3 Analýza typu motýlek

Analýza typu motýlek, také známá jako Bow-tie analysis, se používá v případech, kdy je potřeba analyzovat událost s větším počtem příčin a možných následků. Analýza dokáže vizuálně zobrazit, že každá cesta od příčiny (útoku) k nežádoucímu následku, má patřičné prvky řízení rizika a faktory, které mohou způsobit selhání těchto prvků. Lze ji používat proaktivně, tedy k modelování potenciálních událostí, nebo i ke zpětné analýze již proběhlé události (ČSN EN IEC 31010, 2020).

Analýza představuje kombinaci dvou technik analýzy rizik. Je to jakási syntéza analýzy stromu poruch (FTA) a analýzy stromu událostí (ETA). Jednotlivé metody budou vysvětleny v následujících podkapitolách.



Obrázek 5 Schéma analýzy typu motýlek

(Zdroj: vlastní zpracování, na základě ČSN EN IEC 31010; Meland et al., 2019)

Levá strana diagramu je zaměřena na identifikaci hrozeb, které představují různé iniciační události nebo scénáře, které mohou potenciálně způsobit vrcholovou událost. Aby iniciační události přešly až k vrcholové události, jsou v diagramu vizualizovány preventivní opatření. Preventivní opatření si organizace zvolí k udržení kontroly nad hrozbami. Pravá strana diagramu znázorňuje potenciální události, které mohou nastat v případě působení vrcholové události. Ty se organizace snaží zmírnit nastavením reaktivních opatření nebo se jim zcela vyhnout (Majka, 2024).

Výhodu analýzy typu motýlek v kybernetické bezpečnosti vidí Meland et al. (2019) v provázanosti vztahů mezi preventivní bezpečností⁵ a následnou ochranou⁶ při posuzování rizik.

⁵ Bezpečnost ve smyslu „safety“

⁶ Ochrana jako „security“

Tabulka 4 Silné stránky a omezení Analýzy typu motýlek

Silné stránky	Omezení
✓ Srozumitelnost a vizuální reprezentace. ✓ Lze využít pro žádoucí i nežádoucí následky. ✓ Není potřeba vysoká úroveň znalostí.	✓ Nezobrazení nezávislých cest od příčin. (Kdy by byl využit v FTA logický prvek „AND“). ✓ Rozsáhlost při zobrazení příliš komplexního systému. ✓ Náchylnost na kvalitu vstupních informací.

(Zdroj: ČSN EN IEC 31010; Majka 2024)

3.3.1 FTA

Analýza stromu poruch je graficko-analytická metoda, která uplatňuje postup na základě zpětného rozboru události pomocí řetězce příčin, které mohou vést k vrcholové události. To znamená, že je to metoda deduktivní – zpracovává se shora dolů. Výstupem je rozvětvený graf, který používá předem dohodnutou symboliku, která pomáhá posoudit pravděpodobnost vrcholové události (Procházková, 2011).

Dohodnutá symbolika označuje pojem „hradla“, jehož definici stanovuje norma o FTA analýze, jako „značka, která se používá ke stanovení symbolické vazby mezi výstupní událostí a odpovídajícími vstupy“ (ČSN EN 61025:2007).

3.3.2 ETA

„Analýza stromu událostí je induktivní přístup modelování možných výstupů, které by mohly vyplývat z dané iniciační události a stavu zmírňujících faktorů, jakož i postup identifikace a posouzení četnosti nebo pravděpodobnosti různých možných výstupů dané iniciační události.“ (ČSN EN 62502:2011, str 12).

ETA využívá ke svému výstupu otázky „co se stane když“, díky které je pak vykonstruován strom možných výstupů. K tomu je potřeba vypracovat podrobný seznam všech iniciačních událostí, na které jsou dále zpracovávány posloupnosti jejich účinku. ETA tak identifikuje

všechny potenciální scénáře nehod, k čemuž využívá větve úspěchů nebo poruch (ČSN EN 62502:2011).

Analýza je úzce propojena s FTA, přičemž vrcholová událost (a její pravděpodobnost) se stává iniciační událostí pro ETA. Spojení obou analýz pak vzniká analýza typu motýlek, která byla popsána v kapitole 3.3.



Obrázek 6 Posloupnost ETA

(Zdroj: vlastní zpracování, na základě dle ČSN EN 62502:2011)

Pravděpodobnosti, které se využívají pro jednotlivé větve stromu událostí, jsou podmíněny posloupností předchozích událostí.

3.4 LOPA

Layers of protection analysis (Analýza ochranných vrstev) je považována za zvláštní formu semikvantitativního stromu událostí. Její atraktivitu ve využití v kybernetické bezpečnosti vyzdvihuje Allen (et. al 2024) slovy: „*Koncept vrstev ochrany přímo odpovídá mnohostrannému přístupu, který je nutný k ochraně citlivých informací, systémů a sítí.*“

Analýza je poměrně komplexní a umožňuje vypočítat dosaženou úroveň zabezpečení, identifikovat aktiva a stanovit vrstvy ochrany. Využití analýzy lze také na vyhodnocení účinnosti již zavedených bezpečnostních opatření a s tím spojenou identifikaci oblastí k možnému zlepšení (Allen et al, 2024).

LOPA se často využívá jako následující analýza, například po HAZOP, ve které byly identifikovány určité scénáře vyžadující další podrobnou analýzu. Pro provedení analýzy jsou zapotřebí vstupní informace jako pravděpodobnost různých iniciačních událostí kybernetických útoků a dostupnost ochranných vrstev pro stanovení celkového očekávaného rizika, které je následně posuzováno na základě vlastních kritérií přijatelnosti rizika organizace. Myšlenka využití metody LOPA v kybernetické bezpečnosti je podle autora poměrně nové (Alanen et. al, 2022).

Tabulka 5 Silné stránky a omezení LOPA

Silné stránky	Omezení
✓ Důkladnost oproti subjektivním kvalitativním úsudkům. ✓ Identifikace zdrojů napříč vrstvami ochrany. ✓ Zaměření na nejzávažnější následky.	✓ Zaměření pouze na: příčina-následek a scénář v čase. ✓ Kvantitativní použití neposuzuje společné prvky poruch. ✓ Složitost použití při rozmanitém počtu scénářů.

(zdroj: ČSN EN IEC 31010)

3.5 HRA

Human Reliability Analysis (Analýza bezporuchové činnosti člověka) je skupina technik, která se používá k vyhodnocení vlivu lidské chyby na systém.

Prvním krokem analýzy je provedení hierarchické analýzy jednotlivých kroků určité činnosti. Pro dílčí kroky se identifikuje potenciální chybovost, nejčastěji pomocí klíčových slov (příliš časně, příliš pozdě, špatný zásah). Zdroje těchto chyb se použijí ke snižování pravděpodobnosti jejich následujícího výskytu (ČSN EN IEC 31010, 2020).

Proces zahrnuje tyto fáze (Alijev, 2018):

Definice problému – jaké typy lidského zapojení se mají zkoumat?

Analýza úkolu – jak bude úkol proveden a jaký typ prostředků bude potřeba k podpoře výkonu?

Analýza lidských chyb – jaké chyby mohou nastat a jak je lze obnovit?

Reprezentace – jak lze tyto chyby výkonu úloh integrovat s jiným hardwarem, softwarem a událostmi prostředí, aby bylo možné vypočítat celkové pravděpodobnosti selhání systému?

Screening – existují nějaké chyby nebo úkoly, které nevyžadují podrobnou kvantifikaci?

Kvantifikace – jak pravděpodobné jsou jednotlivé chyby a selhání úloh?

Posouzení dopadů – které chyby nebo úkoly jsou nejdůležitější, tj. které nejvíce přispívají ke spolehlivosti nebo riziku?

Redukce chyb – jak lze dosáhnout vyšší lidské spolehlivosti?

Dokumentace – jaké podrobnosti o HRA je třeba zdokumentovat?

Tabulka 6 Silné stránky a omezení HRA

Silné stránky	Omezení
✓ Zdroje rizik způsobené lidskou činností. ✓ Na základě detailní analýzy lze odhadnout modifikaci rizika.	✓ Složitost použití v rutinních nebo složitých úkolech. ✓ V případě částečných dopadů na výkonnost je komplikovaná práce s analýzou. ✓ Nutnost názoru odborníka.

(zdroj: ČSN EN IEC 31010)

3.6 PIA a DPIA

Metoda analýzy dopadu na soukromí (PIA = Privacy Impact Analysis) a analýzy dopadu na ochranu údajů (Data Protection Impact Analysis) si kladou za cíl analyzovat incidenty a události a jejich vliv na soukromí osoby. Dále identifikují a kvantifikují potřebné způsobilosti ke zvládnutí těchto vlivů (ČSN EN IEC 31010, 2020).

Zmíněné analýzy tak pomáhají organizacím posuzovat rizika týkající se soukromí, zpracování a ukládání osobních údajů. Podle ISO tyto analýzy splňují požadavky, které jsou kladeny na organizace ohledně GDPR (ČSN EN IEC 31010, 2020).

Analýzu je nutno provádět na několika úrovních. Jednou z klíčových jsou kontroly, které nabývají následující charakter:

- **Kontrola zpracovávaných údajů** – šifrování, anonymizace, řízení přístupu, sledovatelnost.
- **Kontroly týkající se systému, v němž se zpracovávají údaje** – bezpečnost provozu, hardware, zálohování.

- **Organizační kontroly** – politika společnosti, personál, řízení incidentů.

Po určení nežádoucích událostí se musí určit následující (Commission Nationale de l'Informatique et des Libertés, 2018):

1. **Určení potenciálních dopadů na soukromí subjektů údajů:** Je třeba analyzovat, jaké důsledky by daná událost mohla mít na soukromí dotčených osob, pokud by k ní došlo.
2. **Odhad závažnosti události:** Tento odhad by měl zohlednit zejména škodlivou povahu potenciálních dopadů a případnou existenci kontrolních mechanismů, které by tyto dopady mohly zmírnit nebo změnit.
3. **Identifikace hrozeb a zdrojů rizik:** Je nutné určit hrozby pro podpůrná aktiva osobních údajů, které by mohly vést k identifikované nežádoucí události, a zároveň identifikovat zdroje rizik, jež by ji mohly vyvolat.
4. **Odhad pravděpodobnosti výskytu:** Tento krok zahrnuje posouzení pravděpodobnosti dané události s přihlédnutím k úrovni zranitelnosti prostředků podporujících osobní údaje, schopnostem zdrojů rizik tyto zranitelnosti zneužít a rovněž existujícím kontrolním mechanismům, které mohou tuto pravděpodobnost ovlivnit.

Tabulka 7 Silné stránky a omezení PIA/DPIA

Silné stránky	Omezení
✓ Hluboké porozumění citlivým údajům. ✓ Plán reakce na potenciální incident. ✓ Poskytuje potřebným orgánům informace o ochraně osobních údajů. (Splňuje požadavky na GDPR).	✓ V počáteční fázi mohou být podhodnoceny výpočty potenciální závažnosti rizika. ✓ Spoléhá na znalosti odborníků provádějících analýzu. ✓ Skupinová dynamika a časový tlak může nepříznivě ovlivnit analýzu.

(Zdroj: ČSN EN IEC 31010)

3.7 GAP analýza

GAP analýza umožňuje porovnávat zavedená bezpečnostní opatření organizace s legislativními požadavky⁷. Její doporučení stanovuje dokonce NÚKIB, jako ideální pro zpracování **prohlášení o aplikovatelnosti**. To je klíčový dokument ISMS, který stručně popisuje zavedená bezpečnostní opatření, způsob jejich implementace, nezavedená opatření včetně důvodů jejich vynechání a poskytuje aktuální přehled o stavu zabezpečení organizace. Společně s plánem zvládání rizik tvoří základní strategický podklad, který musí schválit výbor KB nebo jiný podobný orgán (NÚKIB, 2022).

GAP analýza tak identifikuje mezeru mezi současným stavem a požadovaným stavem zabezpečení. Prostřednictvím identifikovaných mezer se organizace snaží napravit současnou situaci tak, aby dosáhla žádoucího stavu (Kim a Ji, 2018).

Tabulka 8 Silné stránky a omezení GAP

Silné stránky	Omezení
✓ Popis aktuální úrovně zabezpečení. ✓ Může sloužit jako pomůcka pro hodnocení zranitelností. ✓ Jednoduchost a přehlednost.	✓ Potřebná znalost prostředí. ✓ Nehledá hlubší příčiny „proč“. ✓ Chybí plán k dosažení „výplně mezery“.

Zdroj: (NÚKIB, 2022; Kim a Ji, 2018)

3.8 OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation, volně přeloženo jako Operačně kritické hodnocení hrozeb, aktiv a zranitelností (OCTAVE), je přístupem pro analýzu a řízení rizik organizace, který vyvinula Carnegie Mellon University. Technika využívá znalosti lidí o bezpečnostních postupech a procesech organizace. Rizika pro nejkritičtější aktiva jsou použita k určení prioritních oblastí pro zlepšení a stanovení bezpečnostní strategie (Alberts et al., 2003).

⁷ Např. NIS 2, Zákon o KB

OCTAVE je zaměřen na organizační rizika a zaměřuje se na strategické otázky související s praxí. Jedná se o flexibilní hodnocení, které lze přizpůsobit většině organizací. OCTAVE je samořízený a vyžaduje, aby organizace řídila proces hodnocení a přijímala rozhodnutí o ochraně informací. Hodnocení vede interdisciplinární tým, který se nazývá analytický tým. Tým zahrnuje lidi jak z obchodních jednotek, tak z oddělení IT, protože při charakterizování globálního, organizačního pohledu na riziko bezpečnosti informací jsou důležité oba pohledy (Alberts et al., 2003).

Fáze 1: Vytvoření profilů hrozeb na základě aktiv – Jedná se o organizační hodnocení. Analytický tým určuje, co je pro organizaci důležité (informační aktiva) a co se aktuálně dělá pro ochranu těchto aktiv. Tým poté vybere ta aktiva, která jsou pro organizaci nejdůležitější (kritická aktiva), a popíše bezpečnostní požadavky pro každé kritické aktivum. Nakonec identifikuje hrozby pro každé kritické aktivum a vytvoří pro něj profil hrozeb.

Fáze 2: Identifikace zranitelností infrastruktury – Jedná se o hodnocení informační infrastruktury. Analytický tým zkoumá přístupové cesty v síti a identifikuje třídy komponent informačních technologií spojených s jednotlivými kritickými aktivy. Tým poté určuje, do jaké míry je každá třída komponent odolná vůči síťovým útokům.

Fáze 3: Vývoj bezpečnostní strategie a plánů – Během této části hodnocení analytický tým identifikuje rizika pro kritická aktiva organizace a rozhoduje, jak s nimi naložit. Tým vytváří strategii ochrany organizace a plány na zmírnění rizik pro kritická aktiva na základě analýzy shromážděných informací (Alberts et al., 2003).

Tabulka 9 Silné stránky a omezení OCTAVE

Silné stránky	Omezení
✓ zlepšování informačního systému řízení rizik. ✓ Existence formálních postupů pro proces „přijetí rizika“. ✓ Zaměření na hodnocení rizik informačních systémů.	✓ Časová náročnost. ✓ Závisí na detailní znalosti interních procesů. ✓ Nevhodná pro organizace s častými interními změnami.

Zdroj: (Stephanus, 2014; Khatibpour, 2024)

3.9 CVSS

Common Vulnerability Scoring System (CVSS) je metoda, která hodnotí systémy na základě jejich zranitelnosti. V samotném popisu metodiky je však zdůrazněno, že CVSS není mírou rizika (nist.gov, 2024). Například Spring et al. (2021) však tvrdí, že i přesto některé orgány tento přístup ke stanovení míry rizika přímo doporučují. Například vláda USA ve svých NIST standardech, nebo globální odvětví platebních karet⁸.

CVSS zohledňuje zranitelnost na základě tří metrik:

- základní metriky popisující charakteristiky zranitelnosti, které se v průběhu času nemění a nezávisí na běhovém prostředí,
- časové metriky upravují celkové skóre úplnosti dostupných informací o zranitelnosti, vyspělosti operačního kódu a dostupnosti oprav,
- environmentální metriky provádějí úpravy výsledného hodnocení s přihlédnutím k charakteristikám informačního prostředí.

Aplikace CVSS umožňuje podle Vasilyev et al. (2021) získat podrobné posouzení rizik kybernetické bezpečnosti a poskytuje výběr prostředků pro implementaci strategie víceúrovňové ochrany. CVSS umožňuje sestavení fuzzy kognitivních map pro všechny možné útoky a jejich implementační scénáře. Usnadňuje bezpečnostní analýzu, umožňuje stanovit hlavní prostředky spolu s nástroji ochrany ve fázi návrhu systému a zároveň pomáhá zvolit požadovanou úroveň detailu vektoru útoku (Vasilyev et al., 2021).

Tabulka 10 Silné stránky a omezení CVSS

Silné stránky	Omezení
✓ Mezinárodní uznávanost. ✓ Podpora automatizace. ✓ Kompatibilita s databázemi zranitelností.	✓ Skóre CVSS se může lišit v závislosti na kontextu hrozby. ✓ Nezohledňuje důležitost aktiv. ✓ Nutnost pochopení skórovacích faktorů.

(Zdroj: Goodman, 2024; nist.gov)

⁸ Global payment card industry

4 SHRNUTÍ A REFLEXE

V první kapitole této práce byla rozpracována problematika definice rizika. Riziko bylo následně teoreticky ukotveno prostřednictvím matematického vyjádření ve vzorci $Riziko = Pravděpodobnost \times Dopad$, který představuje základní rámec pro jeho analýzu. Současně byly detailně popsány přístupy k identifikování pravděpodobnosti a dopadu, které hrají roli v případě následujících výpočtů míry rizika v jednotlivých organizacích.

Druhá kapitola se věnovala vymezení kybernetické bezpečnosti jakožto samostatné disciplíny a představila její základní pojmy. V této souvislosti byly zmíněny mezinárodně uznávané standardy a rámce, jako například ISO 27000, směrnice NIS 2 a metodika NIST.

Třetí kapitola pak nabídla systematický přehled metod analýzy rizik aplikovaných v oblasti kybernetické bezpečnosti. Jednotlivé metody byly kvůli omezenému rozsahu textu popsány pouze stručně, což neumožnilo podrobné rozpracování teoretických základů ani diskusi o jejich praktické využitelnosti.

V oblasti analýzy rizik existuje široká škála metod a jejich variací, které zmiňuje současná odborná literatura. Z časových a prostorových důvodů nebylo možné v této práci podrobněji rozpracovat všechny dostupné přístupy. Mezi další významné metody, jež jsou často zmiňovány odbornou komunitou, ale nebyly v této diplomové práci detailněji popsány, patří například: ALE analysis, CRAMM, FRAP, CCTA, TARA. Nebo přístupy jako SIEM, Cyber kill chain či model FAIR.

Tyto metody jsou zde uvedeny pro úplnost a mohou být předmětem dalšího zkoumání v budoucím výzkumu.

II PRAKTICKÁ ČÁST

5 KONCEPT VÝZKUMU

Na základě poznatků získaných v teoretické části práce byla vytvořena základní formulace pro provedení polostrukturovaných rozhovorů. Pro tento účel byl vypracován souhrn otázek, které pokrývaly témata jako používané metody analýzy rizik, jejich teoretické ukotvení a vnímané nedostatky v praxi.

Na základě provedených rozhovorů s odborníky⁹, jejichž úkolem je analýza rizik v oblasti kybernetické bezpečnosti, byla identifikována značná mezera v povědomí o sofistikovaných metodách a přístupech k analýze.

Respondenti často uváděli, že při své práci využívají spíše intuitivní predikce nebo základní nástroje, jako jsou jednoduché matice rizik. Většina z nich však nebyla schopna tyto přístupy adekvátně pojmenovat či zařadit do teoretického rámce, jak je tomu běžné v akademickém prostředí.

Při diskusi o nedostacích tohoto přístupu k řízení rizik se opakovaně objevovala otázka, jakou metodiku by tedy bylo vhodné aplikovat. Tato otázka odhalila potřebu hlubšího zkoumání dostupných metod analýzy rizik. Dílčím cílem této diplomové práce se proto stala právě identifikace metod, které by byly alespoň částečně propojeny s výukou ve vzdělávací instituci, jež formují vzdělání autora již 5. rokem. Zároveň však, aby tyto metody zahrnovaly i nové, komplexnější přístupy, jež nebyly v rámci studia podrobněji probírány.

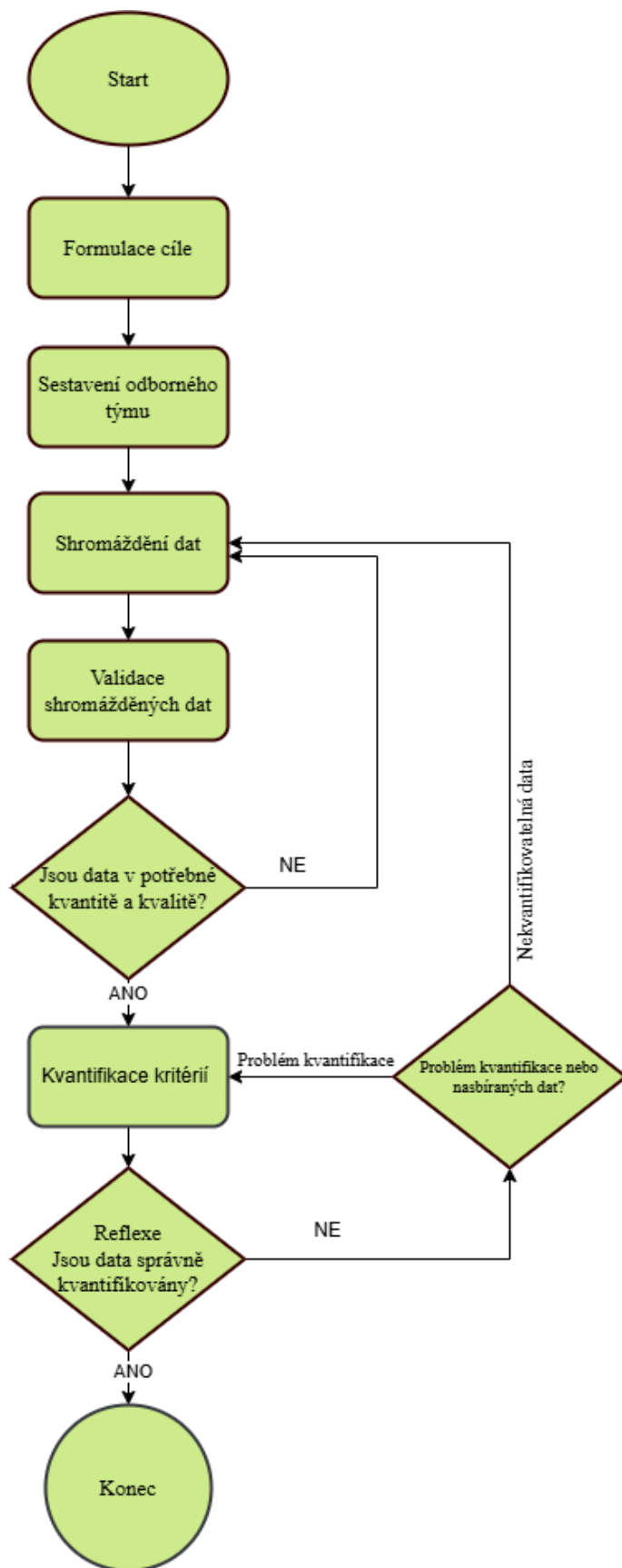
Tímto způsobem má práce ambici přispět k lepší přípravě na budoucí působení v organizacích, kde bude možné navrhnout vhodnou metodu analýzy rizik na základě konkrétních potřeb a požadavků.

Je však zřejmé, že poskytnutí univerzálního doporučení na „nejlepší“ metodu není reálné, neboť výběr vhodného přístupu závisí na specifickém vnitřním i vnějším prostředí dané organizace. Tento přístup podporuje kontingenční teorie managementu, která tvrdí, že efektivita organizačních rozhodnutí a metod je podmíněna přizpůsobením konkrétním podmínkám a kontextu organizace. V tomto ohledu je klíčové klást důraz na pochopení požadavků organizace, což umožňuje zúžit okruh potenciálních metod a lépe přizpůsobit jejich výběr.

⁹ Respondenti, kteří se podíleli na rozhovorech, pocházeli převážně z malých a středních podniků. Zjištěno bylo, že úroveň znalostí týkajících se metodik analýzy rizik vykazovala tendenci k růstu v závislosti na velikosti podniku.

Praktická část této práce je proto zaměřena na vytvoření přehledu kritérií rozhodujících při výběru metod analýzy rizik. Součástí je také návrh aplikace, která by organizacím usnadnila výběr vhodné metody v oblasti kybernetické bezpečnosti podle jejich konkrétních potřeb.

Prvním krokem v tomto procesu je obecná identifikace těchto kritérií, jejichž zjišťování bude probíhat podle metodického postupu znázorněného na následujícím diagramu.



Obrázek 7 Metodologický postup identifikace kritérií

(Zdroj: vlastní zpracování)

6 STANOVENÍ HODNOTICÍCH KRITÉRIÍ

Pro zajištění systematického přístupu k identifikaci hodnoticích kritérií bylo nezbytné jasně definovat cíl celého procesu. Pro formulaci cíle byla použita metoda SMART, která umožňuje stanovit cíle, aby byly:

- Specifické (Specific).
- Měřitelné (Measurable).
- Dosažitelné (Achievable).
- Realistické (Realistic).
- Časově ohraničené (Time-bound).

Díky této metodě byl zajištěn jasný směr procesu a následné efektivní hodnocení výsledků. Stanovení cíle bylo nezbytné pro následné kroky procesu, jelikož umožnilo všem participantům lépe porozumět celkovému konceptu a zajistilo jednotné vnímání a směřování.

Sestavení odborného týmu

Pro sestavení odborného týmu bylo potřeba stanovit specifické požadavky a základní charakteristiky odborníků. Mezi požadované předpoklady patřily:

- Odborné znalosti v příslušné oblasti (kybernetická bezpečnost, analýza rizik)
- Splňovat předpoklady k produktivnímu brainstormingu (komunikativnost, respekt k různorodým názorům, týmová spolupráce)

Odborný tým pro identifikaci kritérií byl sestaven ze sedmi lidí.

1. Facilitátor – Osoba, která řídí diskusi a zapisuje nápady (autor práce).
2. Participant 1 – Bezpečnostní analytik.
3. Participant 2 – Odborník v oblasti kybernetické bezpečnosti.
4. Participant 3 – Auditor.
5. Participant 4 – Odborník na krizové řízení.
6. Participant 5 – Právník.
7. Participant 6 – Softwarový architekt.

Shromáždění dat

K identifikaci klíčových kritérií byly využity dvě metody – metoda brainstormingu a metoda rozhovorů s relevantními odborníky.

Metoda brainstormingu umožnila na základě využití vzájemné interakce odborníků a rozvíjení vzájemných myšlenek identifikaci největšího množství kritérií.

Metoda rozhovorů byla aplikována s cílem identifikovat a doplnit případná opomenutá či nezohledněná kritéria, která mohla být přehlédnuta v předchozí fázi analýzy. Tento přístup byl zejména cenný pro získání inovativních podnětů a preciznější formulaci myšlenek některých participantů z brainstormingu.

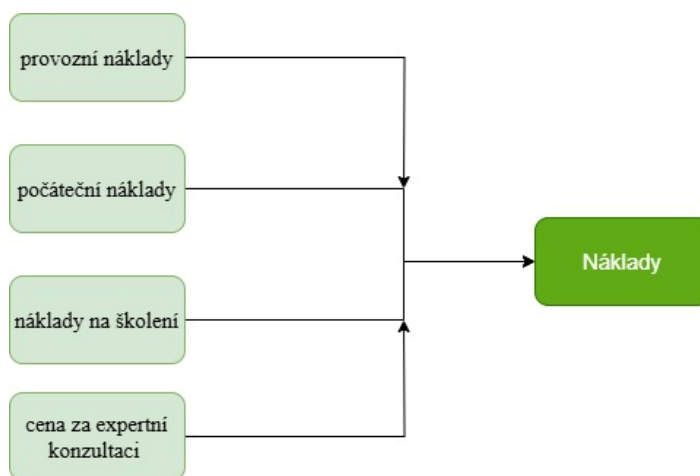
Výsledkem syntézy obou metod bylo identifikováno **64** individuálních výstupů.

Vzhledem k rozsáhlosti těchto výstupů, jejich komplexnosti a potřebě zajistit přehlednost a srozumitelnost pro další zpracování, bylo zapotřebí provést zjednodušení, aby se usnadnila následná analýza těchto dat. Zjednodušení spočívalo v kategorizaci identifikovaných výstupů do skupin podle jejich společných charakteristik.

Následně byla provedena validace těchto zjednodušených kritérií prostřednictvím konzultací s vybranými odborníky.

Validace shromážděných dat

Tento proces zahrnoval ověření, zda jsou nasbíraná data z metody brainstorming relevantní pro daný účel. Relevantnost dat byla konzultována s odborníkem na krizové řízení.



Obrázek 8 Seskupení kritérií

(Zdroj: vlastní zpracování)

Během shromažďování dat bylo nasbíráno několik lingvisticky proměnných. Tedy kdy bylo jedno téma vyjádřeno několika lingvistickými variacemi. Z důvodu vysokého počtu výstupů byla provedena simplifikace a seskupení. Tedy kdy kritéria jako: provozní náklady, počáteční náklady, náklady na školení, cena za expertní konzultaci – byly seskupeny pouze pod kritériem „náklady“. A složitá slovní spojení byla simplifikována, např. *„jak rychle dokážeme analýzu provést“* pod *„časová náročnost“*.

Po důkladném seskupení jednotlivých variací a následném odstranění duplicitních kritérií, která se navzájem překrývala pouze odlišnou formulací, bylo možné dospět k finálnímu souboru **22** kritérií. Tento proces nejen eliminoval redundantní prvky, ale zároveň přispěl k vyšší srozumitelnosti.

Každé z identifikovaných kritérií bylo kvalitativně popsáno a doplněno o zdůvodnění, aby bylo dosaženo určité relevance a význam pro provedení následující analýzy.

6.1 Identifikovaná kritéria a jejich popis

Identifikovaná kritéria byla náležitě popsána s cílem sjednotit interpretaci hodnotitelů a umožnit tak jejich následnou kvantifikaci.

1. Náklady

Zahrnuje finanční prostředky potřebné k implementaci a provádění vybrané metody, přičemž se bere v úvahu nejen počáteční investice, ale i dlouhodobé výdaje spojené s jejím udržováním a aktualizací. Mezi různé formy nákladů mohou patřit:

- Pořízení specializovaného softwaru (případně následující opakované platby při použití komerčních nástrojů), hardwaru nebo jiných nástrojů potřebných k provedení analýzy.
- Školení zaměstnanců.
- Najmutí externích odborníků.
- Alokace interních zdrojů.
- Potenciální ztráty (přízpůsobení systému), časové ztráty (náklady na testování).

Omezení kritéria:

Rozsah nákladů se může lišit v závislosti na komplexitě analyzovaného prostředí, velikosti organizace či specifických požadavcích na hloubku analýzy.

2. Časová náročnost

Doba potřebná k přípravě, provedení a vyhodnocení analýzy. Zahrnuje nejen samotnou délku trvání jednotlivých fází procesu analýzy, ale také faktory jako dostupnost potřebných dat, úroveň automatizace procesu či zkušenosti týmu provádějícího analýzu. Pod kritérium řadíme formy jako:

- Délka přípravy metody (včetně sběru dat).
- Trvání samotné analýzy (od zahájení po získání výsledků).
- Doba potřebná k vyhodnocení a interpretaci výsledků.
- Čas na školení týmu pro zvládnutí metody.
- Doba integrace metody do stávajícího prostředí firmy.

Omezení kritéria:

Omezení může spočívat v subjektivním odhadu času, protože přesné určení délky trvání analýzy závisí na proměnných, jako je zkušenost týmu, kvalita dostupných dat nebo neočekávané omezení, které nelze vždy předvídat.

Dále si je třeba uvědomit problematiku rozporu mezi kvalitou a rychlostí provedení analýzy. Metody s nízkou časovou náročností mohou produkovat méně přesné výsledky. Naopak komplexnější analýzy, které vyžadují více času, nemusí být proveditelné v situacích, kde je nezbytná okamžitá reakce na hrozbu.

Dále byla diskutována myšlenka, zda kritérium nezařadit pod „náklady“. Bylo však dosaženo závěru, že při působení rizika může být znatelný nepoměr mezi potřebou okamžité reakce versus dlouhodobou ekonomickou udržitelností. Například v situacích akutních kybernetických incidentů může být rychlost analýzy rozhodujícím faktorem bez ohledu na rozpočet, což zdůrazňuje nezávislost tohoto kritéria.

3. Lidské zdroje

Personální dostupnost v jednotlivých oborech jako „analýza rizik“ a „kybernetická bezpečnost“ může být nedostatečná. Seskupením obou oborů může nastat riziko nedostupnosti potřebných lidských zdrojů. Zmíněné kritérium proto zahrnuje faktory jako:

- Dostupnost personálu.

- Časová kapacita a flexibilita zaměstnanců vzhledem k jejich běžným úkolům. (Ne vždy je alokován jeden člověk pro pouhou analýzu rizik).
- Požadavky na koordinaci mezi interními týmy (IT oddělení s bezpečnostním oddělením), případně mezi interními i externími týmy (V případě provádění analýzy rizik externí společností je potřeba komunikace mezi interním a externím).

Omezení kritéria:

Přestože se nacházíme na pomyslné hranici překlenku éry umělé inteligence, v současné době stále úspěšnost analýzy rizik často spočívá na kvalitě lidského faktoru. Do budoucna by se toto kritérium díky rozmachu AI mohlo stát méně důležité.

Lidské zdroje jsou také omezeny jistou subjektivitou v hodnocení rizik, protože interpretace dat a rozhodování mohou být ovlivněny osobními předsudky či nedostatkem zkušeností, což může snížit objektivitu výsledků.

4. Přesnost výsledků

Toto kritérium odráží propracovanost metody a možnost poskytnutí spolehlivých a použitelných informací o potenciálních hrozbách a jejich dopadech. Zahrnuje míru, do jaké analýza dokáže odhadnout závažnost a budoucí scénáře rizik. Toto kritérium může zahrnovat i schopnost odhalit nejen zřejmé, ale i skryté druhy rizik.

- Schopnost metody identifikovat všechna relevantní rizika.
- Přesnost odhadu závažnosti a pravděpodobnosti hrozeb.
- Minimální míra falešně pozitivních nebo negativních výsledků.
- Robustnost metodiky vůči chybám nebo nekonzistentním datům.
- Hloubka analýzy.
- Schopnost predikce budoucích rizik na základě aktuálních trendů.
- Adaptabilita na nové typy kybernetických hrozeb a technologií.
- Objektivita výsledků

Omezení kritéria:

Jedním z hlavních omezení je závislost na kvalitě a dostupnosti vstupních dat. Pokud jsou data nepřesná, přesnost analýzy se výrazně snižuje bez ohledu na vhodnost použité metody. Přesnost výsledků může být dále ovlivněna subjektivní interpretací těchto výsledků. Navíc

míru chybovosti analýzy lze často spolehlivě posoudit až ex post, což značně omezuje možnost předem zaručit její přesnost.

5. Citlivost na kvalitu vstupních dat

Kritérium se zaměřuje na míru, v jaké je metoda ovlivněna charakterem a spolehlivostí vstupních dat. Zahrnuje schopnost metody produkovat validní výsledky i při použití dat, které mohou být neúplné nebo zastaralé. Předchozí kritérium – přesnost výsledků se soustředí na konečný výstup analýzy, citlivost na kvalitu vstupních dat se zabývá reakcí metody na vstupní data. Například dvě metody mohou za ideálních podmínek dosahovat stejné přesnosti, ale liší se v citlivosti.

- Odolnost metody vůči neúplným datům.
- Flexibilita při změnách dat.
- Požadavky na kvantitu vstupních dat.

Omezení kritéria:

Citlivost na kvalitu vstupních dat se může projevit až nějakou dobu po provedení samotné analýzy. Identifikace závadných vstupních dat může být vysoce problematická – zvláště u velkých organizací. Prokazatelnost, zda je metoda citlivá na vstupní data nebo přesná ohledně svých výpočtů nemusí být v praxi dosažitelná.

6. Odolnost vůči lidským chybám

Toto kritérium bylo zvoleno z důvodu variability lidských zkušeností a dovedností. Požadavky na zvolenou metodiku často zahrnují použitelnost i méně zkušenými pracovníky bez potřebného vzdělání nebo vědomostí. Kritérium tak zahrnuje míru, do které je metoda schopna pracovat s lidskými chybami nebo jak složitá je.

- Intuitivnost a jednoduchost použití metody nebo nástroje.
- Minimalizace manuálních zásahů do analytického procesu.
- Jasnost a srozumitelnost instrukcí a postupů.
- Mechanismy pro odhalení a opravu chyb (např. upozornění na anomálie, samokontrola výstupů).
- Přizpůsobení různým úrovním zkušeností uživatelů.

Omezení kritéria:

Snaha o maximalizaci odolnosti může vést k vyšší složitosti metody, což paradoxně zvyšuje nároky na technické dovednosti uživatelů a potenciálně tak zvyšuje i riziko pochybení. Striktní postupy, které by snižovaly míru lidské chybovosti, se mohou projevovat sníženou elasticitou metody. Tedy, kdy by se metoda těžce přizpůsobila prostředí organizace. Kritérium rovněž naráží na obtížnost předvídání všech typů lidských chyb, protože tyto mohou být ovlivněny faktory, jako je únava, stres nebo nedostatek školení, které nelze vždy předem otestovat.

Lidský faktor nebo lidské chyby se projevují jako velmi obtížně eliminovatelné. S přístupem softwarové podpory metodologie s kombinací se strojovým učením se však těmto chybám dá lépe vyhýbat.

7. Schopnost identifikovat nové hrozby

Schopnost metody odhalit a analyzovat nové hrozby, které doposud nebyly v organizaci známy (například zero-day zranitelnosti).

- Prediktivní modelování.
- Detekce nových rizik.
- Využití AI.

Omezení kritéria:

S potenciální schopností identifikace nových hrozeb se zvyšují požadavky na užití komplexnějších nebo pokročilých technologických postupů, které zvyšují požadavky na odborné znalosti. Identifikace nových hrozeb také může vést k řadě falešných poplachů, kvůli kterým se mohou zbytečně zvednout náklady. Otázka, zda je možné identifikovat zcela nové události, zvláště v kybernetické bezpečnosti, může být zavádějící. Řada kybernetických útoků se řadí pod kategorii černých labutí, které nemusejí být identifikovatelné.

8. Požadované znalosti

Různé metodiky budou vyžadovat různé odbornosti nebo znalosti pracovníků z oblastí jak kybernetické bezpečnosti, tak analýzy rizik. Požadované znalosti ovlivňují, jak efektivně a správně lze metodu aplikovat v praxi, ať už jde o technické dovednosti, porozumění

kybernetickým hrozbám nebo schopnost interpretovat výsledky. Toto kritérium hraje roli při volbě týmu, který bude metodu používat, a jeho vlastností a požadavků.

- Znalost kybernetického prostředí.
- Znalost metody.
- Schopnost interpretace dat.
- Zkušenosti s metodami.
- Požadavky na školení (včetně dostupnosti školitele) a dokumentaci.

Omezení kritéria:

Metody s nízkými požadavky na znalosti mohou být příliš zjednodušené a postrádat hloubku potřebnou pro komplexní analýzu, zatímco metody náročné na odbornost omezují okruh potenciálních uživatelů a zvyšují závislost na omezeném počtu expertů. Problematická může být i identifikace potřebných znalostí či kritérií výběru pracovníků. Zvýšení požadavků může tedy vést k nedostatku personálu, oproti tomu jejich snížením může být zvýšeno riziko chybovosti.

9. Srozumitelnost výstupů

Srozumitelnost výstupů může hrát klíčovou roli při předávání výsledků analýzy různým cílovým skupinám (vedení, stakeholders), které nemusejí být plně seznámeni s problematikou metodiky. Výsledky analýzy by v ideálním případě měly být schopny převést složité vstupy do podoby, která je pochopitelná a podporuje možnost dalšího rozhodování.

- Logická struktura výstupů.
- Dostupnost vysvětlení.
- Přizpůsobení cílové skupině.

Omezení kritéria:

Srozumitelnost výstupů může být omezena subjektivitou vnímání. Co se zdá srozumitelné pro jednu skupinu (např. analytiku), nemusí být srozumitelné pro skupinu jinou (např. management). To může vést k potřebě kompromisu mezi detailní analýzou a její jednoduchostí. Přílišná simplifikace může však vést ke ztrátě důležitých informací a dat,

kteřé jsou klíčové pro přesné posouzení rizik. Naopak nadměrná komplexnost může znesnadnit komunikaci s netechnickými uživateli a zpomalit rozhodovací proces.

Zmíněné však může záviset na schopnostech týmu, který danou analýzu provádí. Pokud výstupy formuluje tým, který nemá potřebné komunikační dovednosti, může narušit srozumitelnost jinak vhodné metody.

10. Možnost vizualizace výsledků

Prezentovat data a závěry analýzy pomocí grafických nástrojů může být užitečné právě pro netechnicky orientované cílové skupiny. Vizualizace výsledků se v reportingu využívá poměrně rozsáhle. Toto kritérium je tedy samostatně zvolené právě z důvodu tvorby reportů, dashboardů, grafů nebo diagramů. Dobrá vizualizace a srozumitelnost může urychlit rozhodovací procesy.

- Dostupnost grafických nástrojů.
- Přehled klíčových informací.
- Podpora rozhodování.
- Filtrování výstupů.

Omezení kritéria:

U některých metod nemusí být grafická vizualizace nezbytná nebo přinášet výraznou přidanou hodnotu. Pokud by však grafická vizualizace byla přínosná, nemusí být nástroje pro vizualizaci výsledků vždy součástí samotného softwaru nebo metody. V takových případech by bylo nutné využít další software, což by mohlo vést ke zbytečnému zkomplikování celého procesu.

11. Softwarová podpora

Dostupnost specializovaných softwarových nástrojů může urychlit celý proces analýzy. Softwarová podpora zahrnuje několik předpřipravených šablon nebo řešení, díky kterým nemusí být zapotřebí detailní metodologický postup nebo znalost výpočtů.

- Dostupnost specializovaných nástrojů.
- Automatizace procesů.
- Informační podpora a možné aktualizace.

Omezení kritéria:

Softwarová podpora může být omezena vysokými náklady na pořízení licence nebo se školením specializovaných nástrojů, což nemusí být dostupné pro všechny organizace. S takovým problémem se mohou potýkat zejména menší firmy s omezeným rozpočtem. Závislost na softwaru také přináší riziko, pokud dojde k výpadku systému nebo ukončení podpory dodavatelem.

12. Uživatelská přívětivost

Jak již bylo řečeno, menší organizace nemusí mít vyhrazený odborný tým pro provádění analýzy rizik v kybernetické bezpečnosti. Tato úloha může spočívat jako součást náplně práce jiného pracovníka. Proto se zmíněné kritérium zaměřuje na otázku, jak snadno a intuitivně mohou uživatelé (ať už techničtí experti, nebo méně zkušení pracovníci) metodu používat. Kritérium zohledňuje jednoduchost ovládání, přehlednost procesu a minimální potřebu pokročilých technických znalostí nebo rozsáhlého školení.

- Jednoduchost a intuitivnost použití.

Omezení kritéria:

Závislost na uživatelské přívětivosti závisí na individuálním pracovníkovi. Co může být přívětivé pro jednoho (např. preferující grafickou přehlednost), nemusí být vhodné pro druhého (např. preferující textové rozhraní). Uživatelská přívětivost může být také omezena kompromisem mezi jednoduchostí a hloubkou analýzy.

13. Uznávanost normy

Vyjadřuje pomyslné skóre, které konkrétní standard nebo metodologie analýzy rizik získaly v odborné komunitě nebo na mezinárodní úrovni. Zahrnuje faktory jako geografický rozsah použití, autoritu vydávající organizace, soulad s legislativou a důvěryhodnost.

- Mezinárodní versus lokální platnost.
- Adopce normy v praxi.
- Kompatibilita s právními požadavky.
- Historie a stabilita, aktualizace.

Omezení kritéria:

Vysoká uznávanost nemusí vždy zaručovat praktičnost metody. Některé široce uznávané normy mohou být příliš komplexní pro menší organizace s omezenými lidskými nebo finančními zdroji. Naopak méně uznávané normy mohou být jednodušší, ale postrádají flexibilitu pro mezinárodní prostředí nebo uznání při auditech od zahraničních partnerů.

14. Kompatibilita s jinými metodami

Efektivní integrace a spolupráce s jinými metodami, které jsou již například v organizaci využívány. Případně možnost navázání na provedenou analýzu jinou, podrobnější metodou, v případě potřeby.

- Technická integrace.
- Využití standardů (ISO 27000, NIS, NIST).
- Flexibilita při rozšiřování analýzy.
- Kompatibilita s existujícími procesy organizace.

Omezení kritéria:

Některé metody mohou být navrženy jako samostatné, bez potřeby další integrace nebo rozšíření. V případě rozšíření metody může být zapotřebí dalších školení, s kterými se budou zvyšovat i náklady. Přílišná snaha o kompatibilitu může oslabit specifické přínosy dané metody, pokud se její původní struktura příliš pozmění.

15. Použitelnost pro různé velikosti organizací

Použitelnost pro různé velikosti organizací vyjadřuje, do jaké míry je daná metoda analýzy rizik v kybernetické bezpečnosti vhodná a prakticky aplikovatelná pro organizace různých velikostí – od malých podniků přes střední firmy až po velké korporace.

- Škálovatelnost metody.
- Přizpůsobení specifickým potřebám.

Omezení kritéria:

Některé metody mohou být příliš komplexní nebo finančně náročné pro malé organizace, zatímco jiné mohou být příliš jednoduché, a tak nedostatečné pro potřeby velkých korporací s komplexnější infrastrukturou. Taktéž graficky složité metody se s rostoucí komplexností organizace zdají být méně přehledné.

16. Soulad s legislativou a normami

Současná legislativa vyžaduje po určitých organizacích řízení rizik v rámci kybernetické bezpečnosti. Toto kritérium klade důraz na zajištění bezpečnosti na základě platných legislativních předpisů nebo norem. Zahrnuje nejen přímou shodu s konkrétními zákony, ale i schopnost metody podpořit organizaci při prokazování souladu vůči regulačním orgánům nebo při auditech. Kritérium je zvláště důležité pro organizace působící v regulovaných odvětvích (např. finance, zdravotnictví) nebo na mezinárodní úrovni, kde je třeba sladit různé právní rámce a další požadavky.

- Shoda s příslušnou legislativou.
- Dodržení mezinárodních předpisů.
- Podpora při auditech a certifikacích.
- Aktualizovatelnost v souladu s novými předpisy.

Omezení kritéria:

Přestože legislativa nepodléhá častým změnám, zvolená metoda pro organizaci nemusí zcela reflektovat případné změny (například s příchodem nového zákona o KB). Některé metody mohou být navíc příliš obecně navrženy a postrádat tak specifické prvky, které zákon vyžaduje. Naopak metody, které splňují pouze legislativní nároky, nemusejí plně odrážet podstatu nových hrozeb.

17. Ověřitelnost výsledků

Schopnost ověřit výsledky poskytnuté metodou a tím zajistit jednoznačnost výstupů. Kritérium je důležité v případě ověřování výstupů interními auditory, externími konzultanty nebo regulačními orgány. Toto kritérium je zvláště důležité v regulovaných odvětvích nebo při spolupráci s externími partnery, kde je třeba transparentně prokazovat kvalitu a přesnost analýzy.

- Dokumentovatelnost postupu.
- Podpora pro audit.
- Jednoznačnost výstupů.

Omezení kritéria:

Časová a zdrojová náročnost při zajištění ověřitelnosti (např. detailní dokumentace) může prodloužit proces analýzy nebo zvýšit náklady. V dynamickém prostředí kybernetických hrozeb také mohou vstupní data rychle zestárnout, což snižuje relevanci ověření starších výsledků.

18. Míra subjektivity v hodnocení

Zvolené kritérium vyjadřuje, jak může být metoda ovlivněna osobními názory, zkušenostmi nebo odhady analytiků nebo jiných odborníků. Zmíněné kritérium může mít své výhody i nevýhody. Pokud by metoda vycházela pouze z objektivních dat a standardizovaných postupů, nemusí plně uchopit jiné neidentifikované prvky, které by zkušený odborník zachytil. Názor hodnotitele však může být i mylný.

- Závislost na odborném úsudku.
- Zapojení více hodnotitelů.
- Použití kvalitativních hodnocení.

Omezení kritéria:

Vysoká míra subjektivity může vést ke sporným výsledkům, což ztěžuje jejich ověřitelnost a obhajobu před třetími stranami. Na druhou stranu, metody s nízkou subjektivitou (například kvantitativní analýzy) však mohou být naopak příliš neflexibilní v situacích, kde chybí dostatek dat. Dalším omezením je, že úplné odstranění subjektivity není vždy možné ani žádoucí. Lidský úsudek může být cenný při identifikaci netradičních rizik.

19. Frekvence aktualizací metody

Kritérium označuje, jak často je metoda revidována, doplňována nebo přizpůsobována novým hrozbám, technologiím a jiným požadavkům.

- Pravidelnost revizí.
- Reakce na nové hrozby.
- Soulad s technologickým pokrokem.
- Zpětná vazba od uživatelů.

Omezení kritéria:

Časté aktualizace mohou vést k nestabilitě metody, protože opakované změny potenciálně ztěžují její osvojení týmy nebo vyžadovat neustálé přeškolení. Naopak nízká frekvence aktualizací může způsobit, že metoda ztratí relevanci vůči novým hrozbám.

20. Čas potřebný k aktualizaci dat

Zvolené kritérium bylo identifikované samostatně, oddělené od „časové náročnosti“, která byla zmíněna v bodě č. 2. A to z důvodu, že kritérium zdůrazňuje specifický aspekt, který může být klíčový v dynamických situacích (např. při reakci na nový útok). Navíc to může být důležité pro organizace, které pracují s velkým objemem dat nebo potřebují rychle reagovat na změny.

Čas potřebný k aktualizaci dat vyjadřuje dobu nezbytnou k zajištění, že vstupní data použítá pro analýzu rizik v kybernetické bezpečnosti zůstávají aktuální a relevantní vzhledem k měnícím se hrozbám, infrastruktuře nebo prostředí organizace.

- Doba získání nových dat (např. čas potřebný k aktualizaci logů, databází hrozeb nebo inventáře aktiv).
- Rychlost zpracování dat a jejich integrace do analýzy.
- Frekvence potřeby aktualizace.

Omezení kritéria:

Omezením může být závislost na dostupnosti a kvalitě zdrojů dat. Pokud organizace nemá přístup k aktuálním informacím (např. z monitoringu sítě), aktualizace může být zdlouhavá nebo nemožná. Dále čas potřebný k aktualizaci může být ovlivněn technickou infrastrukturou (např. pomalé systémy) nebo nedostatkem kvalifikovaného personálu.

21. Teoretické základy metody

Teoretické základy metody označují konceptuální, matematické nebo jiné odborné principy, na kterých je daná metoda postavena. Zahrnuje robustnost jejího konceptuálního rámce, soulad s uznávanými teoriemi a schopnost odůvodnit své postupy a výpočty.

- Vědecký základ.
- Odborná podpora.
- Metodologický postup.

Omezení kritéria:

Porozumění mezi teoretickým prostředím (jehož je ztělesněním akademické prostředí) a praxí může být problematické. Pokud je metoda akademicky robustní, může být složité ji aplikovat v praxi. Zejména pro organizace, kde provádí analýzu personál bez hlubokých teoretických znalostí. Naopak metody s méně propracovanými teoretickými základy mohou být sice praktičtější, ale mohou postrádat hloubku a obhájitelnost při auditu.

22. Druh standardizace

Druh standardizace označuje, na jakém standardizačním rámci je metoda založena, a zda je tento rámec uznáván na národní nebo mezinárodní úrovni.

- Mezinárodní, národní nebo odvětvové standardizace.
- Závazné či dobrovolné standardy.

Omezení kritéria:

Druh standardizace může omezovat flexibilitu metody. Mezinárodní standardy mohou být příliš obecné. Odvětvové standardy, které jsou sice konkrétní zase mohou být nepoužitelné mimo daný sektor.

Vnímání uznávanosti metody a její funkčnosti a využitelnosti v tak specifickém prostředí, čímž kybernetický prostor je, může být problematické. Standardizované metody mohou být neefektivní v rychle se měnících podmínkách kybernetických hrozeb. Naopak metody, které nejsou normované, nemusejí být vnímány důvěryhodně, přestože mohou být vhodnější. Vyhledávání vhodných nenormovaných metod a jejich prokazatelnost a důvěrnost se zdá být také problematická.

6.2 Kvantifikace kritérií

Pro kvantifikaci kritérií bylo užito dvou metod. Jednoduchá bodovací metoda a Saatyho metoda pro stanovení vah kritérií.

Stanovení vah bodovací metodou

Pro určení vah kritérií bylo osloveno 6 respondentů z řad odborné veřejnosti, přičemž jedním z hodnotitelů byl autor práce. Významnost jednotlivých kritérií byla hodnocena na škále přirozených čísel $<1; 5>$, kde hodnota 1 představuje nejnížší preferenci kritéria a hodnota 5 nejvyšší preferenci.

Tabulka 11 Stupnice bodovací metody

Slovní vyjádření	Hodnota
Nepodstatné	1
Méně důležité	2
Středně důležité	3
Velmi důležité	4
Klíčové	5

(Zdroj: vlastní zpracování)

Tabulka 12 Váhy kritérií dle bodovací metody

Číslo	Název kritéria	Hodnotitel 1	Hodnotitel 2	Hodnotitel 3	Hodnotitel 4	Hodnotitel 5	Hodnotitel 6	Hodnotitel 7	Průměrné hodnocení	Významnost
4	Přesnost výsledků	5	5	5	5	4	5	4	4,7143	1
16	Soulad s legislativou a normami	5	4	5	4	4	4	4	4,2857	2
17	Ověřitelnost výsledků	4	4	4	4	4	5	4	4,1429	3
7	Schopnost identifikovat nové hrozby	4	5	3	3	4	5	4	4,0000	4
1	Náklady	4	4	3	5	3	2	4	3,5714	5
2	Časová náročnost	4	3	5	4	5	1	2	3,4286	6
3	Lidské zdroje	3	3	3	4	4	4	3	3,4286	6
5	Citlivost na kvalitu vstupních dat	3	4	4	4	3	4	2	3,4286	6
6	Odolnost vůči lidským chybám	4	4	3	3	3	3	3	3,2857	9
8	Požadované znalosti	3	3	3	3	4	2	3	3,0000	10
21	Teoretické základy metody	2	3	5	2	4	3	2	3,0000	10
9	Srozumitelnost výstupů	3	4	3	3	2	3	2	2,8571	12
11	Softwarová podpora	2	3	4	2	3	3	3	2,8571	12
12	Uživatelská přívětivost	3	3	3	3	4	2	2	2,8571	12
20	Čas potřebný k aktualizaci dat	2	4	1	3	4	3	2	2,7143	15
18	Míra subjektivity v hodnocení	4	3	3	3	1	2	2	2,5714	16
13	Uznávanost normy	2	2	4	2	1	2	3	2,2857	17
15	Použitelnost pro různé velikosti organizací	2	3	2	2	2	3	1	2,1429	18
22	Druh standardizace	1	2	3	2	1	2	3	2,0000	19
14	Kompatibilita s jinými metodami	1	4	2	1	2	2	1	1,8571	20
10	Možnost vizualizace výsledků	1	3	2	1	3	1	1	1,7143	21
19	Frekvence aktualizací metody	2	3	2	1	1	1	1	1,5714	22

(Zdroj: vlastní zpracování)

Analýza výsledků

Nejvýznamnější kritéria (průměr $\geq 4,0$):

- Přesnost výsledků.
- Soulad s legislativou a normami.
- Ověřitelnost výsledků.
- Schopnost identifikovat nové hrozby.

Nejvýznamnější kritéria jasně ukazují na převahu technických a právních aspektů. Tato kritéria byla hodnotiteli ohodnocena nejkonzistentněji, což naznačuje, že dávají přednost metodám, které jsou spolehlivé, transparentní a v souladu s právními požadavky.

Středně významná kritéria (3,0–3,9)

- Náklady.
- Časová náročnost.
- Lidské zdroje.
- Citlivost na kvalitu vstupních dat.
- Odolnost vůči lidským chybám.
- Požadované znalosti.
- Teoretické základy metody.

Středně významná kritéria odrážejí důležitost ekonomických a uživatelských aspektů. Tato kritéria vykazují větší rozptyl v hodnocení, což naznačuje, že jejich význam se liší v závislosti na prioritách jednotlivých hodnotitelů a specifických potřebách organizací.

Méně významná kritéria ($<3,0$)

- Srozumitelnost výstupů.
- Softwarová podpora.
- Uživatelská přívětivost.
- Čas potřebný k aktualizaci dat.
- Míra subjektivity v hodnocení.
- Uznávanost normy.
- Použitelnost pro různé velikosti organizací.
- Druh standardizace.
- Kompatibilita s jinými metodami.
- Možnost vizualizace výsledků.
- Frekvence aktualizací metod.

Tato kritéria byla hodnotiteli ohodnocena jako méně podstatná, což naznačuje, že upřednostňují funkčnost a spolehlivost metod před jejich formou nebo častými změnami.

7 MULTIKRITERIÁLNÍ ANALÝZA

Pro multikriteriální analýzu byla zvolena Saatyho metoda, která umožňuje kvantifikovat identifikovaná kritéria pro výběr metod analýzy rizik v kybernetické bezpečnosti prostřednictvím párového srovnání.

V následující tabulce jsou stanoveny hodnoty intenzity významu, která umožňují kvantifikovat subjektivní preference rozhodovatele. Tato stupnice je založena na číselných hodnotách od 1 do 9, přičemž každá hodnota odpovídá určitému stupni preference jedné varianty nad druhou. Níže uvedená tabulka 13 shrnuje Saatyho stupnici intenzity významu variant, která byla použita při tvorbě matice párového porovnání v této práci.

Tabulka 13 Stupnice intenzity významu varianty

Číselné označení	Slovní popis
1	Varianty jsou stejně významné.
3	Varianta je mírně důležitější než jiná varianta.
5	Varianta je mnohem důležitější než jiná varianta.
7	Varianta je výrazně důležitější než jiná varianta.
9	Extrémní významnost jedné varianty nad jinou variantou.

(Zdroj: mff.cuni.cz)

7.1 Strukturování kritérií do skupin

Původní soubor 22 kritérií nebyl z hlediska přehlednosti a časové náročnosti proveditelný. Hodnotitelé nejprve museli být obeznámeni s principem multikriteriální analýzy a s charakteristikou jednotlivých kritérií. Z tohoto důvodu byla kritéria rozdělena do 7 skupin, aby se zajistila lepší orientace v jejich komplexním souboru. I přes snahu o simplifikaci se analýza stala časově náročnou, a to především kvůli nutnosti objasnit princip Saatyho metody odborné, avšak v této oblasti neznalé, komunitě hodnotitelů. Jednotlivým hodnotitelům musely být podrobně představeny charakteristiky jednotlivých kritérií, což samo o sobě zabralo čas. Navíc se nejednalo o stejnou skupinu, která kritéria

původně identifikovala, což vedlo k dlouhým diskuzím o významu a podobě jednotlivých kritérií.

Jednotlivá kritéria byla rozdělena do skupin na základě jejich charakteristik následovně:

K1 – Ekonomické aspekty

Jsou klíčové z důvodu omezenosti finančních zdrojů jednotlivých organizací. Náklady, čas a lidé rozhodují o tom, zda je metoda reálně použitelná, ať už jde o malou firmu nebo velkou instituci.

K2 – Technické vlastnosti

Technická kvalita metody určuje, jak dobře odhalí a zhodnotí rizika.

K3 – Uživatelské aspekty

Pokud metoda není srozumitelná, její úspěšné použití se snižuje bez ohledu na její kvalitu.

K4 – Kompatibilita a integrace

Metoda musí zapadnout do stávajících systémů a procesů organizace a respektovat právní rámec.

K5 – Důvěryhodnost a ověřitelnost

Závislost metody na možnosti ji ověřit, zejména při auditech nebo obhajobě rozhodnutí.

K6 – Aktualizace a údržba

Kybernetické hrozby se mění, takže metoda musí zůstat aktuální a přizpůsobivá.

K7 – Teoretické a metodologické aspekty

Pevné teoretické základy zajišťují, že metoda má vědecký základ a uznávanost.

Tabulka 14 Zařazení kritérií do skupin

K1 Ekonomické aspekty
K1.1 Náklady
K1.2 Časová náročnost
K1.3 Lidské zdroje
K2 Technické vlastnosti
K2.1 Přesnost výsledků
K2.2 Citlivost na kvalitu vstupních dat
K2.3 Odolnost vůči lidským chybám
K2.4 Schopnost identifikovat nové hrozby
K3 Uživatelské aspekty
K3.1 Požadované znalosti
K3.2 Srozumitelnost výstupů
K3.3 Možnost vizualizace výsledků
K3.4 Softwarová podpora
K3.5 Uživatelská přívětivost
K3.6 Uznávanost normy
K4 Kompatibilita a integrace
K4.1 Kompatibilita s jinými metodami
K4.2 Použitelnost pro různé velikosti organizací
K4.2 Soulad s legislativou a normami
K5 Důvěryhodnost a ověřitelnost
K5.1 Ověřitelnost výsledků
K5.2 Míra subjektivity v hodnocení
K5.3 Důvěryhodnost
K6 Aktualizace a údržba
K6.1 Frekvence aktualizací metody
K6.2 Čas potřebný k aktualizaci dat
K7 Teoretické a metodologické aspekty
K7.1 Teoretické základy metody
K7.2 Druh standardizace

(Zdroj: vlastní zpracování)

Tabulka 15 Saaty – respondent 1

	K1	K2	K3	K4	K5	K6	K7	Vektor	Váha
K1	1	1/7	1/5	7	1/5	5	3	0,9296	0,0923
K2	7	1	7	1	3	7	9	3,6869	0,3659
K3	5	1/7	1	1/5	1/7	5	5	0,9083	0,0902
K4	1/7	1	5	1	5	7	7	2,0914	0,2076
K5	5	1/3	7	1/5	1	7	5	1,8756	0,1862
K6	1/5	1/7	1/5	1/7	1/7	1	1/3	0,2344	0,0233
K7	1/3	1/9	1/5	1/7	1/5	3	1	0,3493	0,0347
								10,0757	1

(Zdroj: vlastní zpracování)

Tabulka 16 Saaty – respondent 2

	K1	K2	K3	K4	K5	K6	K7	Vektor	Váha
K1	1	1/5	1/3	1/3	1/5	3	3	0,6314	0,0634
K2	5	1	3	3	1	7	7	3,0035	0,3014
K3	3	1/3	1	1	1/3	5	5	1,3538	0,1359
K4	3	1/3	1	1	1/3	5	5	1,3538	0,1359
K5	5	1	3	3	1	7	7	3,0035	0,3014
K6	1/3	1/7	1/5	1/5	1/7	1	1	0,3095	0,0311
K7	1/3	1/7	1/5	1/5	1/7	1	1	0,3095	0,0311
								9,9650	1

(Zdroj: vlastní zpracování)

Tabulka 17 Saaty – respondent 3

	K1	K2	K3	K4	K5	K6	K7	Vektor	Váha
K1	1	1/3	3	7	1/3	9	3	1,8074	0,1972
K2	3	1	1/3	5	3	3	5	2,1678	0,2366
K3	1/3	3	1	5	3	7	3	2,2746	0,2482
K4	1/7	1/5	1/5	1	1/3	1/5	1/5	0,2580	0,0282
K5	3	1/3	1/3	3	1	5	3	1,4724	0,1607
K6	1/9	1/3	1/7	5	1/5	1	1/7	0,3581	0,0391
K7	1/3	1/5	1/3	5	1/3	7	1	0,8246	0,0900
								9,1630	1

(Zdroj: vlastní zpracování)

Tabulka 18 Saaty – respondent 4

	K1	K2	K3	K4	K5	K6	K7	Vektor	Váha
K1	1	1/3	7	1/7	1/7	1	1/3	0,5533	0,0624
K2	3	1	7	3	5	1	7	3,0035	0,3386
K3	1/7	1/7	1	1/3	1	1/3	3	0,4902	0,0553
K4	7	1/3	3	1	3	1/3	7	1,7436	0,1966
K5	7	1/5	1	1/3	1	5	3	1,3205	0,1489
K6	1	1	3	3	1/5	1	5	1,3687	0,1543
K7	3	1/7	1/3	1/7	1/3	1/5	1	0,3895	0,0439
								8,8694	1

(Zdroj: vlastní zpracování)

Tabulka 19 Rozptyl hodnot jednotlivých analýz

	K1	K2	K3	K4	K5	K6	K7
Analýza 1	0,0923	0,3659	0,0902	0,2076	0,1862	0,0233	0,0347
Analýza 2	0,0634	0,3014	0,1359	0,1359	0,3014	0,0311	0,0311
Analýza 3	0,1972	0,2366	0,2482	0,0282	0,1607	0,0391	0,0900
Analýza 4	0,0624	0,3386	0,0553	0,1966	0,1489	0,1543	0,0439
Rozdíl (MAX-MIN)	0,1349	0,1293	0,1930	0,1794	0,1525	0,1311	0,0589

(Zdroj: vlastní zpracování)

Jako největší rozdíl zde byl identifikován nesoulad pro skupinu kritérií č.3 - Uživatelské aspekty. Oproti tomu největší konzistentnost poukazuje na skupinu kritérií č.7 - Teoretické a metodologické aspekty.

Pro určení finální váhy jednotlivých kritérií byl použit aritmetický průměr vah získaných z analýz všech respondentů. Průměr tak zajišťuje, že finální váha kritéria je kompromisem mezi všemi hodnoceními, což zvyšuje robustnost výsledků. Z identifikovaných rozdílů je patrné, že mezi jednotlivými respondenty nejsou nijak extrémní aritmetické výkyvy. Rozumné rozmezí rozdílů potvrzuje vhodnost použití aritmetického průměru jako ideální variantu pro agregaci dat.

Tabulka 20 Průměr skupin kritérií

Kritérium	Průměr
K1	0,1038
K2	0,3106
K3	0,1324
K4	0,1420
K5	0,1993
K6	0,0619
K7	0,0499

SUMA	1
------	---

(Zdroj: vlastní zpracování)

Po výpočtu průměru vah jednotlivých kritérií byl ověřen jejich součet. Z výsledku vyplývá, že kritéria není potřeba dále normalizovat.

8 POROVNÁNÍ VÝSTUPŮ METOD

Pro efektivní výběr a doporučení metod analýzy rizik v rámci návrhu aplikace je nezbytné detailně porozumět tomu, jaké výstupy jednotlivé metody generují. Definice a porovnání těchto výstupů umožňuje lépe posoudit jejich přínos a relevanci vzhledem k identifikovaným kritériím. Tabulka 21 proto shrnuje charakteristiky výstupů vybraných metod analýzy rizik.

Tabulka 21 Výstup metod

Metoda	Výstupy
BIA (Business Impact Analýza)	✓ údaje o cílech, strategickém zaměření, prostředí, majetku a vzájemných propojenostech organizace ✓ přehled produktů, obchodních aktivit a služeb organizace a jejich propojení s podnikovým procesem ✓ vyhodnocení priorit stanovených při předchozím přezkoumání vedením ✓ podrobné informace o činnostech a funkcích organizace, včetně procesů, zdrojů, vazeb na jiné organizace, dodavatelských řetězců, outsourcovaných činností a zainteresovaných stran ✓ údaje umožňující zhodnotit finanční, právní a provozní dopady při ztrátě klíčových procesů ✓ připravený dotazník nebo jiný nástroj pro shromažďování informací ✓ výsledky z jiných analýz rizik a hodnocení kritických incidentů spojených s dopady narušujících událostí ✓ seznam osob z relevantních částí organizace nebo od zainteresovaných stran, které budou osloveny
Matice rizik	✓ zobrazení pravděpodobné možnosti výskytu následku a úroveň rizika pro různá rizika ✓ klasifikace významnosti pro každé riziko
Motýlek (Bow-Tie Analýza)	✓ Výstupem je diagram, který znázorňuje cesty rizika, stávající mechanismy pro jeho řízení a faktory, které by mohly způsobit selhání těchto mechanismů. Diagram zároveň ukazuje možné dopady a opatření, jež lze po vzniku události přijmout k jejich zmírnění
LOPA (Layer of Protection Analysis)	✓ Doporučení pro jakákoliv ošetření a odhady zbytkového rizika, ✓ Následek, který může nastat, pokud riziko není zabráněno a přejde do nežádoucího scénáře. ✓ Umožňující události a podmínky, které mohou přispět k iniciaci nežádoucí události. ✓ Frekvenci výskytu událostí. ✓ Tolerovatelnou frekvenci výskytu události.

Metoda	Výstupy
HRA (Analýza bezporuchové činnosti člověka)	✓ seznam potenciálních chyb nebo neobvyklých činností, které mohou nastat, spolu s metodami, jak je lze vylepšit úpravou návrhu systému ✓ způsoby, typy, příčiny a dopady lidských činností ✓ kvalitativní a kvantitativní hodnocení rizik vyplývajících z rozdílů ve výkonnosti
PIA/DPIA (Analýza dopadu na soukromí/Analýza dopadu na ochranu údajů)	✓ dokumenty obsahující popis shromážděných informací ✓ seznam procesů kritických informací a jejich vzájemných závislostí, seřazený podle priorit ✓ soubor scénářů, ve kterých je riziko při zpracování osobních údajů vyšší, než se předpokládalo ✓ dokumentované dopady úniku nebo ztráty osobních údajů na fyzickou osobu ✓ informace o podpůrných zdrojích a činnostech potřebných k omezení potenciálních dopadů na datový subjekt ✓ seznam produktů a služeb organizace, seřazený podle priorit ✓ hodnocení dopadů v čase a prostředcích, které nezaručují důvěrnost, integritu a dostupnost, spolu s následky pro datové subjekty ✓ časové rámce výpadků a zásahů, které mají být provedeny k obnovení ochranného prostředí nebo informací, včetně ohlášení příslušným orgánům
GAP Analýza	✓ Identifikace nedostatků a postup zajištění shody s požadavky
OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)	✓ Identifikovaná kritická aktiva ✓ identifikovaná slabá místa a hrozby pro tato aktiva ✓ vyhodnocení důsledků v případě uskutečnění identifikovaných hrozeb ✓ Inicie k neustálému zlepšování ✓ Porozumění organizaci ✓ Zaměření na kritická málo častá rizika ✓ Ochranné strategie a Plány zmírnění rizik
CVSS (Common Vulnerability Scoring System)	✓ kalkulace závažnosti zranitelností objevených na vlastních systémech

(Zdroj: ČSN EN IEC 31010; GENERAL ELECTRIC COMPANY, 2022; Pyka a Sobieski, 2012; nist.gov)

Vytyčení výstupů jednotlivých metod je klíčové z několika důvodů. Nejen že umožňuje organizacím lépe pochopit, jaké informace mohou od dané metody očekávat a jak tyto informace odpovídají jejich specifickým požadavkům. Popis výstupů také usnadňuje jejich propojení s hodnocením podle stanovených kritérií, což je zásadní pro funkčnost aplikace.

Tabulka 22 Porovnání metod na základě stanovených kritérií

Číslo	Název kritéria	BIA	Matice rizik	Motýlek	LOPA	HRA	PIA a DPIA	GAP	OCTAVE	CVSS
1	Náklady	Střední	Nízká	Střední	Střední	Vysoká	Vysoká	Nízká	Vysoká	Nízká
2	Časová náročnost	Střední	Nízká	Střední	Střední	Vysoká	Střední	Nízká	Vysoká	Nízká
3	Lidské zdroje	Střední	Nízké	Střední	Střední	Vysoká	Střední	Nízká	Střední	Nízká
4	Přesnost výsledků	Střední	Střední	Vysoká	Vysoká	Střední	Vysoká	Střední	Vysoká	Vysoká
5	Citlivost na kvalitu vstupních dat	Střední	Střední	Střední	Vysoká	Střední	Střední	Nízká	Vysoká	Střední
6	Odolnost vůči lidským chybám	Nízká	Nízká	Střední	Střední	Nízká	Nízká	Střední	Střední	Nízká
7	Schopnost identifikovat nové hrozby	NE	NE	NE	NE	NE	NE	NE	ANO	NE
8	Požadované znalosti	Nízká	Nízká	Střední	Vysoká	Vysoká	Vysoká	Nízká	Vysoká	Nízká
9	Srozumitelnost výstupů	Střední	Vysoká	Střední	Střední	Střední	Střední	Vysoká	Střední	Střední
10	Možnost vizualizace výsledků	NE	ANO	ANO	ANO	ANO	NE	NE	NE	ANO
11	Softwarová podpora	ANO	ANO	ANO	ANO	ANO	ANO	ANO	NE	ANO
12	Uživatelská přívětivost	Nízká	Vysoká	Střední	Střední	Nízká	Nízká	Vysoká	Střední	Vysoká
13	Uznávanost normy	Střední	Nízká	Vysoká	Vysoká	Vysoká	Vysoká	Střední	Vysoká	Vysoká
14	Kompatibilita s jinými metodami	Střední	Vysoká	Střední	Nízká	Střední	Nízká	Nízká	Střední	ANO
15	Použitelnost pro různé velikosti organizací	ANO	ANO	NE	ANO	ANO	ANO	ANO	ANO	ANO
16	Soulad s legislativou a normami	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO
17	Ověřitelnost výsledků	ANO	ANO	ANO	ANO	NE	ANO	ANO	ANO	
18	Míra subjektivity v hodnocení	Vysoká	Vysoká	Vysoká	Střední	Vysoká	ANO	Střední	Vysoká	Vysoká
19	Frekvence aktualizací metody	subj.	subj.	subj.	subj.	subj.	subj.	subj.	subj.	subj.
20	Čas potřebný k aktualizaci dat	Střední	Nízká	Střední	Střední	Vysoká	Vysoká	Střední	Vysoká	Střední
21	Teoretické základy metody	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO	ANO
22	Druh standardizace	Mezinárodní	Mezinárodní	Mezinárodní	Mezinárodní	Mezinárodní	Mezinárodní	Mezinárodní	Mezinárodní	Mezinárodní

(Zdroj: vlastní zpracování)

Tabulka č. 22 umožňuje porovnat klíčové vlastnosti jednotlivých metod a poskytuje tak datový základ pro rozhodovací algoritmus aplikace.

Hodnocení metod podle identifikovaných kritérií je aktuálně vyjádřeno pomocí kvalitativní škály „nízká“, „střední“, „vysoká“ doplněné o hodnocení („ano/ne“). Pro zvýšení přesnosti a použitelnosti těchto dat by bylo vhodné provést **fuzzifikaci** těchto pojmů, tedy převést vágní kategorie do číselného vyjádření formou fuzzy množin. Tento krok by umožnil lépe zachytit nejistotu a variabilitu spojenou s hodnocením jednotlivých kritérií.

Je však zřejmé, že hodnocení jednotlivých kritérií je vysoce individuální pro každou organizaci a závisí na jejích specifických podmínkách. Univerzální kvantifikace těchto aspektů proto není zcela reálná bez dalšího výzkumu. Přesto se domnívám, že na základě budoucích empirických dat by bylo možné jednotlivým metodám přiřadit konkrétnější hodnoty podle stanovených kritérií. Pokud by se například podařilo přiřadit metodám numerické skóre na škále 1–10 pro každé kritérium, mohlo by to vytvořit základ pro algoritmus aplikace, který by generoval datově podložená doporučení.

K dosažení takového cíle by však bylo nezbytné zapojit širší okruh odborníků a provést rozsáhlý sběr dat z reálných aplikací těchto metod v praxi. Takový proces by zahrnoval například analýzu časové náročnosti metody BIA v různých organizacích nebo posouzení finančních nákladů na implementaci OCTAVE v závislosti na velikosti firmy. Vzhledem k časovým a zdrojovým omezením této diplomové práce byla charakterizace metod provedena na základě nejlepšího uvážení autora, podloženého literární rešerší.

Přístup zvolený v tabulce č. 22 tak poskytuje předběžný rámec pro hodnocení metod, který může být v budoucnu dále rozpracován a validován prostřednictvím dalšího výzkumu.

9 KONCEPCE APLIKACE PRO DOPORUČENÍ METOD ANALÝZY RIZIK

Problematika řízení rizik v tak rozmanitém prostředí, jímž právě kybernetický prostor je, se stala v posledních letech velice diskutovanou. Metodika, která se zvolí pro analýzu kybernetických rizik může být poměrně zásadní. Dle rozhovorů s odborníky na kybernetickou bezpečnost vyplývá, že jsou stále nejvyužívanější kvalitativní metody, navzdory jejich kritice odbornou komunitou. Tyto kvalitativní přístupy stojí převážně na názoru a úsudku hodnotitele. To je v řadě případů opodstatněné, jelikož proměnlivost prostředí někdy nedovoluje použít relevantní empirická data pro hlubší analýzu. Na druhé straně povaha analýzy rizik, která stojí čistě na objektivní analýze statistických údajů, nezachycuje zcela různé formy emergentních rizik, pod které bychom mohli právě kybernetické útoky zařadit.

Jsem si vědom, že vytvoření zcela nové metody analýzy rizik by bylo příliš ambiciózní a časově náročné, vzhledem k rozsahu této práce a složitosti kybernetického prostředí. Nová metoda by pravděpodobně musela být syntézou již existujících přístupů, což by vyžadovalo rozsáhlé testování a validaci v reálných podmínkách, přesahující možnosti této diplomové práce. Místo toho jsem se rozhodl pro inovativní řešení návrhu aplikace, která na základě identifikovaných kritérií a jejich vah doporučí organizacím nejvhodnější metodu analýzy rizik.

Na základě identifikovaných požadavků a mezery na trhu by bylo přínosné vytvořit aplikaci, která by organizacím usnadnila výběr vhodné metodiky analýzy rizik tím, že by jim poskytla konkrétní doporučení. Tato aplikace by vycházela z identifikovaných kritérií a jejich vah, které byly stanoveny na základě hodnocení odborníků v rámci této práce.

Uživatel by prostřednictvím série cílených otázek, odrážejících klíčová kritéria jako velikost organizace, soulad s legislativou, časová náročnost nebo požadované znalosti, zadal specifika své organizace a její potřeby. Aplikace by následně na základě těchto vstupů a předem definovaných vah kritérií vyhodnotila, která metoda analýzy rizik je pro danou organizaci nejvhodnější.

Tímto způsobem by aplikace nejen usnadnila rozhodovací proces, ale také zajistila, že zvolená metodika bude co nejlépe odpovídat konkrétním požadavkům a omezením organizace, ať už jde o malou firmu s omezenými zdroji, nebo velkou korporaci s komplexní infrastrukturou.

9.1 Návrh aplikace

Návrh aplikace, jejímž cílem je pomoci organizacím vybrat nejvhodnější metodu pro hodnocení a řízení rizik, zejména v oblasti kybernetické bezpečnosti. Aplikace je aktuálně implementována jako webová stránka napsaná v HTML, CSS a JavaScriptu, což z ní činí jednoduchý, ale již funkční prototyp. Kód se skládá ze dvou hlavních částí:

Formulář pro zadání uživatelských preferencí

- Uživatel odpovídá na sadu otázek rozdělených do kategorií (základní informace o organizaci, zdroje a kapacity, požadavky na analýzu, priority a preference).
- Otázky zahrnují například velikost organizace, finanční možnosti, časovou náročnost analýzy nebo preference ohledně vizualizace výsledků.
- Uživatel také vybírá až tři hlavní priority, které hrají klíčovou roli při výpočtu doporučení.
- Po odeslání formuláře aplikace zpracuje odpovědi a přesměruje uživatele na stránku s výsledky.

Nástroj pro výběr metody analýzy rizik

Základní informace o organizaci

1. Jak velká je vaše organizace?

Vyberte možnost

2. Má vaše organizace pobočky nebo operace v různých geografických lokalitách?

Vyberte možnost

3. Má vaše organizace již zavedené procesy pro identifikaci, hodnocení a řízení rizik? 

Vyberte možnost

Obrázek 9 Návrh nástroje – část 1

(Zdroj: vlastní zpracování)

1 – výběr možností: Malá (do 50 zaměstnanců), Střední (50-250 zaměstnanců), Velká (více než 250 zaměstnanců)

2 – výběr možností: Ano, v jedné zemi, Ano, v několika zemích, Ne, pouze v ČR

3 – výběr možností: Ano, Částečně, Ne

Zdroje a kapacity

4. Jste ochotni investovat do specializovaného softwaru nebo externích odborníků pro analýzu rizik?

Vyberte možnost

5. Jaké jsou vaše finanční možnosti pro analýzu rizik?

Vyberte možnost

6. Máte vyhrazený tým pro analýzu rizik, nebo budou tuto úlohu plnit zaměstnanci s jinými povinnostmi?

Vyberte možnost

7. Jaká je dostupnost personálu pro provádění analýzy rizik?

Vyberte možnost

8. Jaké odborné znalosti má váš tým v oblasti kybernetické bezpečnosti a analýzy rizik?

Vyberte možnost

Obrázek 10 Návrh nástroje – část 2

(Zdroj: vlastní zpracování)

4 – výběr možností: Ano, pokud je to nutné, Pouze pokud je to nezbytné, Ne, preferujeme interní řešení.

5 – výběr možností: Velmi omezené, Střední, Vysoké.

6 – výběr možností: Vyhrazený tým, Zaměstnanci s jinými povinnostmi, Kombinace obou.

7 – výběr možností: Omezená, Střední, Plná.

8 – výběr možností: Základní, Středně pokročilé, Pokročilé (experti).

Požadavky na analýzu

9. Jak rychle potřebujete provést analýzu rizik?

Vyberte možnost

10. Preferujete kvalitativní nebo kvantitativní přístup k analýze rizik?

Vyberte možnost

11. Preferujete metodu s vizuálními nástroji (např. grafy, dashboardy) pro prezentaci výsledků?

Vyberte možnost

Obrázek 11 Návrh nástroje – část 3

(Zdroj: vlastní zpracování)

9 – výběr možností: Okamžitě (v řádu dní), V průběhu několika týdnů, Bez časového tlaku.

10 – výběr možností: Kvalitativní, Kvantitativní, Kombinace obou.

11 – výběr možností: Ano, nezbytné, Žádoucí, ale ne nutné, Není to důležité.

Priority a preference

12. Jaké jsou vaše hlavní priority při výběru metody analýzy rizik? (Vyberte 3 nejdůležitější)

- ☐ Nízké náklady
- ☐ Rychlost provedení
- ☐ Přesnost výsledků
- ☐ Snadné použití
- ☐ Soulad s normami
- ☐ Schopnost identifikovat nové hrozby
- ☐ Možnost vizualizace

Vyhodnotit a doporučit metodu

Obrázek 12 Návrh nástroje – část 4

(Zdroj: vlastní zpracování)

Stránka s výsledky

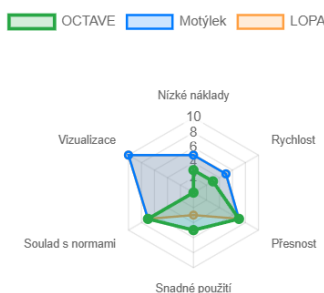
- Zobrazuje seznam tří doporučených metod (vybírání ze seznamu metod zmíněných v této práci) seřazených podle vypočteného skóre, přičemž nejvhodnější metoda je zvýrazněna zeleně.
- Součástí je také pavučinový graf, který vizuálně porovnává doporučené metody podle šesti vlastností (nízké náklady, rychlost, přesnost, snadné použití, soulad s normami, vizualizace).

Výsledek analýzy rizik

Doporučené metody:

1. OCTAVE (Skóre: 2.94)
2. Motýlek (Skóre: 2.32)
3. LOPA (Skóre: 2.32)

Na základě analýzy vašich odpovědí byly identifikovány tyto metody jako nejvhodnější. Nejlepší volba je označena zeleně.



Obrázek 13 Návrh nástroje – část 5

(Zdroj: vlastní zpracování)

Aplikace funguje na základě předdefinovaných dat (hodnocení metod a váhy kritérií), která jsou zakódována přímo v Javascriptu. Výpočet doporučení probíhá na straně klienta – JavaScript zpracovává uživatelské odpovědi, váží je podle priorit a generuje skóre pro jednotlivé metody.

9.2 Návrh na rozšíření funkcionality

Aplikace se prozatím nachází v návrhové, přesto funkční fázi. Přestože tento počáteční model již nabízí uživatelům doporučení metod na základě jejich odpovědí, pro její plnou funkčnost, přehlednost a integritu je třeba definovat její budoucí vývoj.

Cílem budoucího vývoje bude navržení komplexního, ale zároveň uživatelsky přívětivého nástroje pro návrh metod analýzy rizik. Budoucí rozvoj by měl zohlednit nejen technické vylepšení, ale i rozšíření funkcionalit či oblastí. Za předpokladu úspěšného průběhu by si uživatel mohl vybrat oblast, pro kterou by potřeboval personalizovaný návrh metody analýzy rizik, například v oblasti BOZP, kybernetické bezpečnosti a jiných oblastí. Dle zodpovězených otázek bude zachován koncept doporučení tří metod (dle skóre vypočítaného na základě vah jednotlivých odpovědí a kritérií), do budoucna by však aplikace mohla uživateli nabídnout i komplexní návod jednotlivých metod. Níže jsou uvedeny klíčové směry, kterými by se měl vývoj ubírat:

- **Rozšíření otázek**

Tento krok by mohl být klíčovým k jejímu dalšímu rozvoji a zvýšení přesnosti doporučení. Současný formulář obsahuje základní sadu otázek, které pokrývají klíčové aspekty organizace a jejích potřeb. V budoucnu by bylo vhodné přidat detailnější otázky zaměřené například na specifické odvětví.¹⁰

- **Rozšíření databáze metod a kritérií**

Současná verze aplikace zahrnuje omezený počet metod a kritérií. V budoucnu by mohla být databáze rozšířena o další specializované metody, včetně návodu a popisu.

- **Designová úprava**

Budoucí design by měl zahrnovat prvky od přehlednější navigace, vizuálních pomůcek (ikony, barevné odlišení sekcí), zlepšení vizualizace výsledků. Nebo možnost exportovat doporučení do formátů jako PDF, Excel a sdílet je zainteresovaným osobám.

Přidání vysvětlivek nebo bližší definování jednotlivých otázek by se mohlo jevit jako vhodné zejména pro osoby s nižší mírou odbornosti.

- **Změna programovacího jazyku a přidání backend**

Současná implementace v HTML s JavaScriptem je vhodná pro prototyp, avšak pro plnohodnotnou realizaci aplikace bude nutné zvolit robustnější jazyk.

Absence serverové části omezuje možnosti ukládání dat, správy uživatelů a historie doporučených analýz. Přidání backendu by umožnilo vytvořit uživatelské profily a případně sdílet výsledky mezi týmy. Backend by také mohl podporovat API (application programming interface) pro integraci s jinými nástroji, jako jsou systémy pro správu rizik.

- **Definování postupů na základě vybraných metod**

Aplikace aktuálně doporučuje metody, ale nenabízí konkrétní návod, jak je implementovat. V budoucnu by měla obsahovat podrobné postupy pro každou metodu – například šablony, příklady výpočtů nebo jiné „krok za krokem“ návody pro provedení analýz.

¹⁰ Zejména z důvodu požadavků NIS 2

- **Celkové zlepšení vstupních dat a provedení analýzy**

Přesnost doporučení závisí na kvalitě vstupních dat a algoritmu hodnocení. Budoucí verze by měla zahrnovat konkrétnější otázky, nebo pokročilejší výpočetní model, který by zohlednil vzájemné závislosti mezi faktory.

- **Vyzkoušení v praxi**

Pro ověření funkčnosti a přínosu aplikace je nezbytné otestovat ji v reálných podmínkách. Tento krok by zahrnoval pilotní nasazení v malých a středních organizacích různých odvětví, sběr zpětné vazby od uživatelů a analýzu výsledků. Testování by mělo zkoumat nejen technickou stabilitu, ale i praktičnost doporučených metod a jejich přínos pro řízení rizik. Na základě získaných dat by bylo možné upravit algoritmy, otázky i rozhraní tak, aby lépe odpovídaly skutečným potřebám.

10 SHRNUÍ A DISKUZE

Výzkum odhalil značné mezery v povědomí odborníků o sofistikovaných metodách analýzy rizik skutečnost, že v praxi převažuje využití intuitivních a základních přístupů, jako jsou jednoduché matice rizik.

Na základě brainstormingu bylo identifikováno 22 unikátních kritérií, která byla následně kvantifikována pomocí bodovací metody a Saatyho metody.

Dále byly porovnány výstupy metod. Do budoucna by však bylo vhodné provést empirický výzkum, který by zahrnoval sběr dat z reálných aplikací těchto metod v různých typech organizací (malé, střední, velké) a různých odvětvích, aby bylo možné posoudit, jak se jednotlivá kritéria projevují v praxi. Například by bylo možné analyzovat, jak dlouho trvá aplikace metody XY v různých týmech, a zohlednit faktory, jako jsou zkušenosti týmu nebo složitost analyzovaného prostředí. Kromě toho by bylo vhodné zapojit širší okruh odborníků z praxe prostřednictvím hloubkových rozhovorů a dotazníků.

Praktická část práce vyústila v návrh aplikace, která slouží jako nástroj pro organizace při rozhodování o nejvhodnější metodě analýzy rizik. Aplikace vychází z identifikovaných kritérií a jejich vah, přičemž prostřednictvím cílených otázek zohledňuje specifické požadavky jednotlivých organizací, jako je jejich velikost nebo dostupné zdroje.

Současná verze aplikace, implementovaná jako funkční prototyp v HTML, CSS a JavaScriptu, představuje Proof of Concept (PoC), který demonstruje potenciál navrženého řešení. Výstupy aplikace zahrnují doporučení tří metod seřazených podle skóre a vizuální srovnání jejich vlastností formou pavučinového grafu.

Tento PoC však představuje pouze počáteční krok, jehož účelem je ověřit koncept a identifikovat klíčové oblasti pro další rozvoj. Pro dosažení plné funkčnosti, robustnosti a uživatelské přívětivosti je nezbytné naplánovat její budoucí vývoj s využitím strukturovaných postupů.

ZÁVĚR

Na základě provedeného výzkumu tato studie uzavírá své zkoumání syntézou získaných teoretických poznatků, v rámci níž byly identifikovány klíčové prvky rizika, povědomí o kybernetické bezpečnosti spolu s vyjmenováním relevantních metod analýzy rizik.

Teoretická část tak vytvořila základ pro praktickou část diplomové práce, v níž byly metody implementovány do navržené aplikace. Tato aplikace, založená na definovaných kritériích s váhami stanovenými pomocí bodovací metody a Saatyho metody, využívá cíleně formulované otázky k tomu, aby organizacím umožnila výběr a doporučení optimální metody analýzy rizik v kontextu kybernetické bezpečnosti.

Výsledky této práce tak nejen propojují teoretické poznatky s praktickým využitím, ale také poskytují organizacím nástroj pro zlepšení jejich bezpečnosti. Tímto způsobem práce přispívá k rozšíření stávajících přístupů a otevírá prostor pro další vývoj již zmíněné aplikace. Lze tedy říci, že závěry práce nejenže zrcadlí komplexitu zkoumané oblasti, ale rovněž naznačují trajektorii pro další výzkum, jehož potenciál by mohl být dále rozvinut v rámci disertační práce.

Na závěr lze tedy konstatovat, že cíle diplomové práce byly naplněny. Primárním cílem bylo vytvoření funkčního konceptu aplikace, která usnadňuje rozhodování při výběru metody analýzy rizik v oblasti kybernetické bezpečnosti, což bylo úspěšně realizováno. Sekundární cíle byly dosaženy prostřednictvím výsledků, podložených multikriteriální analýzou, která definovala kritéria a jejich váhy použité v aplikaci.

Výzkumné otázky práce byly úspěšně zodpovězeny. První otázka, zaměřená na identifikaci klíčových kritérií ovlivňujících výběr metod analýzy rizik, byla zodpovězena kombinací dvou metodologických přístupů: Saatyho metodou pro stanovení vah kritérií a bodovací metodou. Druhá otázka, zkoumající možnost návrhu podpůrného nástroje, byla zodpovězena vytvořením funkčního konceptu aplikace, která prokazuje, že takové řešení je realizovatelné.

V současné podobě však nástroj není plně připraven pro plně funkční nasazení v organizacích. Jeho další vývoj, pilotní testování a naplnění vize popsané v kapitole 9.2 jsou nezbytnými kroky k dosažení plného potenciálu tohoto řešení v budoucnosti.

Tímto způsobem byla ambice práce splněna v souladu s předpoklady a očekáváními.

SEZNAM POUŽITÉ LITERATURY

ALANEN, J.; LINNOSMAA, J.; PÄRSSINEN, J., KOTELBA, A., & HEIKKILÄ, E. (2022). *Review of cybersecurity risk analysis methods and tools for safety critical industrial control systems*. VTT Technical Research Centre of Finland. VTT Research Report No. VTT-R-00298-22

ALBERTS, Christopher; DOROFEE, Audrey; STEVENS, James a WOODY, Carol, 2003. *Introduction to the OCTAVE® Approach*. Carnegie Mellon University, Software Engineering Institute. Dostupné také z: <https://insights.sei.cmu.edu/library/introduction-to-the-octave-approach/>.

ALIYEV, Ilgar, 2018. *Cyber-risk management techniques - Human reliability assessment (HRA)*, Dostupné z: <https://www.linkedin.com/pulse/cyber-risk-management-techniques-human-reliability-ilgar-aliyev/>

ALLEN, David; EL, Hawraa, CHANDRASHEKHAR, Amulya, 2024. *Unlocking the Power of CyLOPA: Your Cyber Risk Assessment Ally*. Dostupné z: <https://www.linkedin.com/pulse/unlocking-power-cylopa-your-cyber-risk-assessment-allen-msc-ceng-xqgwe/>

AVEN, Terje a YLÖNEN, Marja, 2019. The strong power of standards in the safety and risk fields: A threat to proper developments of these fields? Online. Roč. 189, s. 279-286. ISSN 09518320. Dostupné z: <https://doi.org/10.1016/j.res.2019.04.035>. [cit. 2025-02-17].

AVEN, Terje, 2012. The risk concept—historical and recent development trends. Online. Roč. 99, s. 33-44. ISSN 09518320. Dostupné z: <https://doi.org/10.1016/j.res.2011.11.006>. [cit. 2025-01-26].

BARBORÍK, Denis. *Co je to NIST a jak souvisí s ISO/IEC 27001*. Online. Dostupné z: <https://www.cems-cz.com/blog/885-co-je-to-nist-a-jak-souvisi-s-iso-iec-27001>. [cit. 2025-03-01].

CATTELAN, Valentino. IN THE NAME OF GOD: MANAGING RISK IN ISLAMIC FINANCE. *Ianus - Diritto e Finanza*. Č. 26 (16), s. 149-164. ISSN 1974-9805.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, 2018. *PIA methodology*. Dostupné také z: <https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-pia-1-en-methodology.pdf>.

CROTTY, James a DANIEL, Elizabeth, 2022. Cyber threat: its origins and consequence and the use of qualitative and quantitative methods in cyber risk assessment. Online. *Applied Computing and Informatics*. 2022-12-26. ISSN 2634-1964. Dostupné z: <https://doi.org/10.1108/ACI-07-2022-0178>. [cit. 2025-02-17].

CROTTY, James a DANIEL, Elizabeth, 2022. Cyber threat: its origins and consequence and the use of qualitative and quantitative methods in cyber risk assessment. Online. *Applied Computing and Informatics*. 2022-12-26. ISSN 2634-1964. Dostupné z: <https://doi.org/10.1108/ACI-07-2022-0178>. [cit. 2025-02-22].

CYBER RISK GMBH. *The NIS 2 Directive*. Online. Dostupné z: <https://www.nis-2-directive.com/>. [cit. 2025-02-18].

ČERMÁK, Miroslav, 2009. *Řízení informačních rizik v praxi*. V Tribunu EU vyd. 1. Knihovnicka.cz. Brno: Tribun EU. ISBN 978-807-3997-311.

ČESKO, 2014. *Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*. Dostupné z: <https://www.zakonyprolidi.cz/cs/2014-181>

ČESKO, 2018. *Vyhláška č. 82/2018 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)*. Dostupné z: <https://www.zakonyprolidi.cz/cs/2018-82>

ČESKO. *Vyhláška č. 316/2021 Sb. Vyhláška o některých požadavcích pro zápis do katalogu cloud computingu*. Dostupné z: <https://www.zakonyprolidi.cz/cs/2021-316#Top>

ČSN EN IEC 31010 ed. 2 *Management rizik – Techniky posuzování rizik*. Praha: Český normalizační institut, 2020.

ČSN EN ISO 9001:2016. *Systémy managementu kvality – Požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2016

ČSN EN ISO/IEC 27001 *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Systémy managementu informační bezpečnosti - Požadavky*, 2023

ČSN EN ISO/IEC 27005 *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Pokyny pro management rizik informační bezpečnosti*, 2023.

ČSN ISO 31000 *Management rizik - Směrnice*, 2018. Česká agentura pro standardizaci, 2018.

DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk, 2019. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing. ISBN 978-80-88260-39-4.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY, 2015. *Definition of Cybersecurity: Gaps and overlaps in standardisation*. Dostupné také z: https://www.enisa.europa.eu/sites/default/files/publications/Cybersecurity_Definition_Gaps_v1_0.pdf.

EVROPSKÝ PARLAMENT, RADA EVROPSKÉ UNIE, 2019. *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2019/881: o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“)*. In: <http://data.europa.eu/eli/reg/2019/881/oj>.

GENERAL ELECTRIC COMPANY, 2022. *Layers of Protection Analysis*. Dostupné také z: https://www.gevernova.com/software/documentation/predix-apm/v46x/pdf/Layers_of_Protection_Analysis.pdf.

GOODMAN, Courtney. *What is the Common Vulnerability Scoring System (CVSS)?* Online. Dostupné z: <https://www.balbix.com/insights/understanding-cvss-scores/>. [cit. 2025-04-09].

HILLSON, D.; HULETT, D. T., 2004. *Assessing risk probability: alternative approaches*. PMI® Global Congress 2004—EMEA, Prague, Czech Republic. Newtown Square, PA: Project Management Institute

HRŮZA, Petr, 2013. *Kybernetická bezpečnost II*. Brno: Univerzita obrany. ISBN 978-80-7231-931-2.

International Organization for Standardization: *RISK-BASED THINKING IN ISO 9001:2015*. Dostupné také z: https://committee.iso.org/files/live/sites/tc176sc2/files/documents/ISO%209001%202015%20-%20Implementation%20guidance%20docs/ISO9001_2015_and_Risk.docx.

JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef, 2015. *Výkladový slovník Kybernetické bezpečnosti*. Policejní akademie ČR v Praze Česká pobočka AFCEA. Dostupné také z: https://cybersecurity.cz/data/slovník_v310.pdf.

HACKENBERGER, Branimir, 2019. *Bayes or not Bayes, is this the question?* Online. *Croatian Medical Journal*. Roč. 60, č. 1, s. 50-52. ISSN 0353-9504. Dostupné z: <https://doi.org/10.3325/cmj.2019.60.50>. [cit. 2025-02-24].

KAPLAN, Stanley a GARRICK, John, 1981. *On The Quantitative Definition of Risk*. Online. *Society for Risk Analysis*. Dostupné z: <https://www.nrc.gov/docs/ML1216/ML12167A133.pdf>. [cit. 2025-01-26].

KAPLAN, Stanley, 1997. The Words of Risk Analysis, *Risk Analysis*, vol.17, pp 407-417

KIM, Sora; JI, Yingru, 2018. *Gap Analysis*. The Chinese University of Hong Kong. Dostupné z: <https://www.com.cuhk.edu.hk/wp-content/uploads/2022/11/sora-ch-2019-gap.pdf>

KOLOUCH, Jan a BAŠTA, Pavel, 2019. *CyberSecurity*. CZ.NIC ;. Praha : CZ.NIC, z.s.p.o. ISBN 978-80-88168-34-8.

KOLOUCH, Jan; MINAŘÍKOVÁ, Petra a RYDVALOVA, Marketa, 2022. *Základy kybernetické bezpečnosti*. Dostupné také z: <https://moodle.cybersecurity-fundamentals.eu/course/index.php?categoryid=4>.

LARGE, Matthew M a NIELSSEN, Olav B, 2012. Comment on risk assessment: predicting violence. Online. *Evidence Based Mental Health*. 2012-01-17, roč. 15, č. 1, s. 4-4. ISSN 1362-0347. Dostupné z: <https://doi.org/10.1136/ebmh.2011.100174>. [cit. 2025-02-21].

LIUZZO, Gaetano; BENTLEY, Stefano; GIACOMETTI, Federica; BONFANTE, Elena a SERRAINO, Andrea, 2014. *The term risk: etymology, legal definition and various traits*. Online. *Italian Journal of Food Safety*. 2014-01-21, roč. 3, č. 1. ISSN 2239-7132. Dostupné z: <https://doi.org/10.4081/ijfs.2014.2269>. [cit. 2025-01-24].

MAJKA, Marcin, 2024. *Bow-Tie Analysis*. Dostupné z: https://www.researchgate.net/publication/383311853_Bow-Tie_Analysis

MATUSZAK-FLEJSZMAN, Alina; PALIWODA, Beata *Maturity of Risk-Based Thinking in Organizations*. Proceedings of the 37th International Business Information Management Association (IBIMA), 2021, Cordoba, Spain, ISBN: 978-0-9998551-6-4, ISSN: 2767-9640

MATUSZAK-FLEJSZMAN, Alina; PALIWODA, Beata, 2020. *"Influence of The Implemented Management Systems on Risk-Based Thinking in Organizations – A Review"* Proceedings of the 36th International Business Information Management Association (IBIMA), ISBN: 978-0-9998551-5-7.

MATWEB.CZ. *Problém tří dveří*. Dostupné také z: <https://www.matweb.cz/tri-dvere/>.

MELAND, Per Håkon; BERNSMED, Karin; FRØYSTAD, Christian; LI, Jingyue a SINDRE, Guttorm, 2019. *An experimental evaluation of bow-tie analysis for security*. Online. 2019-06-20, roč. 27, č. 4, s. 536-561. ISSN 2056-4961. Dostupné z: <https://doi.org/10.1108/ICS-11-2018-0132>. [cit. 2025-02-23].

MEROLA, Francesco; BERNARDESCHI, Cinzia a LAMI, Giuseppe, 2024. *A Risk Assessment Framework Based on Fuzzy Logic for Automotive Systems*. Online. *Safety*. Roč. 10, č. 2. ISSN 2313-576X. Dostupné z: <https://doi.org/10.3390/safety10020041>. [cit. 2025-03-01].

MFF.CUNI.CZ. *VÍCEKRITERIÁLNÍ ROZHODOVÁNÍ*. Dostupné také z: <https://www.karlin.mff.cuni.cz/~kopa/VRfinal.pdf>.

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, 2024. *Podněty z veřejné konzultace k návrhu nového zákona o kybernetické bezpečnosti a souvisejících předpisů*. Dostupné z: https://portal.nukib.gov.cz/storage/uploads/2024/08/26/Souhrnne-vyporadani-verejne-konzultace-nZKB_uid_66cc4c8750ff5.pdf

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, 2024. *Zpráva o stavu kybernetické bezpečnosti ČR za rok 2023*. Dostupné také z: <https://nukib.gov.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/>.

NIST. 2016. *Guide for Cybersecurity Event Recovery*. NIST Special Publication 800-184 [online]. Gaithersburg, MD: National Institute of Standards and Technology. Dostupné z: <https://doi.org/10.6028/NIST.SP.800-184>.

NIST. 2023, *Guide to Operational Technology (OT) Security*. NIST Special Publication 800-82, Revision 3 [online]. Gaithersburg, MD: National Institute of Standards and Technology. Dostupné z: <https://doi.org/10.6028/NIST.SP.800-82r3>.

NIST. 2024a *Cybersecurity Framework Version 1.1*. NIST Cybersecurity White Paper CSWP.29 [online]. Gaithersburg, MD: National Institute of Standards and Technology. Dostupné z: <https://doi.org/10.6028/NIST.CSWP.29>.

NIST. 2024b *Building a Cybersecurity and Privacy Learning Program*. NIST Special Publication 800-50, Revision 1 [online]. Gaithersburg, MD: National Institute of Standards and Technology,. Dostupné z: <https://doi.org/10.6028/NIST.SP.800-50r1>

NIST.GOV. *Vulnerability Metrics*. Online. Dostupné z: <https://nvd.nist.gov/vuln-metrics/cvss>. [cit. 2025-03-05].

NOVOTNÝ, Jan, 2018. *Problém dvou obálek, problém tří dveří a Jánošíkův paradox*. Katedra fyziky, chemie a odborného vzdělávání, Masarykova univerzita, Brno. Veletrh nápadů učitelů fyziky 23. Dostupné z: https://home.pf.jcu.cz/~vnufcb/CD/pdf/VNUF23_26.pdf

NÚKIB, 2022. *PRŮVODCE ŘÍZENÍM AKTIV A RIZIK DLE VYHLÁŠKY O KYBERNETICKÉ BEZPEČNOSTI*. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/Prvodce%20zenm%20aktiv%20a%20rizik%20dle%20vyhlky%20o%20kybernetick%20bezpenosti.pdf

OSTROM, Lee T. a WILHELMSSEN, Cheryl A., 2019. *Risk assessment: tools, techniques, and their applications*. Second edition. Hoboken, NJ: Wiley. ISBN 978-1-119-48346-5.

PENDER-BEY, Georgie, 2012. *THE PARKERIAN HEXAD*. Information Security Program at Lewis University. Dostupné také z: <https://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf>.

POLÁCH, David, 2024. *Cyber Security Framework 2 – americká obdoba NIS2 a ISO 27001?* Online. Dostupné z: <https://cybrela.com/cyber-security-framework-2-obdoba-nis2-a-iso-27001/>. [cit. 2025-03-01].

POSLANECKÁ SNĚMOVNA PARLAMENTU ČESKÉ REPUBLIKY. *Vládní návrh zákona o kybernetické bezpečnosti - EU, Sněmovní tisk 759*. Online. Dostupné z: <https://www.psp.cz/sqw/historie.sqw?o=9&t=759>. [cit. 2025-03-01].

POŠÍK, Petr, 2015. *Opakování základů teorie pravděpodobnosti*. katedra kybernetiky FEL CVUT. Dostupné z: https://cw.fel.cvut.cz/b182/_media/courses/a6m33ssl/basicprob-rehersal-short-handouts.pdf

PROCHÁZKOVÁ, Dana, 2011. *Analýza a řízení rizik*. Praha: České vysoké učení technické v Praze. ISBN 978-80-01-04841-2.

PYKA, Marek a SOBIESKI, Šcibor, 2012. *Implementation of the OCTAVE Methodology in Security Risk Management Process for Business Resources*. Online. *Internet - Technical*

Developments and Applications 2. Advances in Intelligent and Soft Computing. S. 235-252. ISBN 978-3-642-25354-6. Dostupné z: https://doi.org/10.1007/978-3-642-25355-3_21. [cit. 2025-03-21].

RAUSAND, Marvin a HAUGEN, Stein, 2020. *Risk assessment: theory, methods, and applications*. Second edition. Wiley series in statistics in practice. Hoboken, NJ: Wiley. ISBN 978-111-9377-238.

ROESER, Sabine; HILLERBRAND, Rafaela; SANDIN, Per a PETERSON, Martin, 2012. *Handbook of Risk Theory, Epistemology, Decision Theory, Ethics, and Social Implications of Risk*. Online. ISBN 978-94-007-1432-8. Dostupné z: <https://doi.org/10.1007/978-94-007-1433-5>. [cit. 2025-02-04].

SAVOLAINEN, Timo; MCCARTHY, Nora; NEVILLE, Karen a RUOSLAHTI, Harri, 2024. *Business Continuity Management of Critical Infrastructures from the Cybersecurity Perspective*. Online. 2024 IEEE Global Engineering Education Conference (EDUCON). 2024-5-8, s. 1-6. ISBN 979-8-3503-9402-3. Dostupné z: <https://doi.org/10.1109/EDUCON60312.2024.10578811>. [cit. 2025-02-21].

SIKDAR, Priti, 2011. *Alternate Approaches to Business Impact Analysis*. Online. Information Security Journal: A Global Perspective. 2011-05-17, roč. 20, č. 3, s. 128-134. ISSN 1939-3555. Dostupné z: <https://doi.org/10.1080/19393555.2010.551274>. [cit. 2025-02-21].

SMEJKAL, Vladimír; SOKOL, Tomáš a KODL, Jindřich, 2019. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-765-8.

SPRING, Jonathan; HATLEBACK, Eric; HOUSEHOLDER, Allen; MANION, Art a SHICK, Deana, 2021. *Time to Change the CVSS?* Online. Roč. 19, č. 2, s. 74-78. ISSN 1540-7993. Dostupné z: <https://doi.org/10.1109/MSEC.2020.3044475>. [cit. 2025-03-05].

STEPHANUS, Stephanus, 2014. *Implementation Octave-S and Iso 27001 controls in Risk Management Information Systems*. Online. ComTech: Computer, Mathematics and Engineering Applications. 2014-12-31, roč. 5, č. 2, s. 685-693. ISSN 2476-907X. Dostupné z: <https://doi.org/10.21512/comtech.v5i2.2225>. [cit. 2025-04-09].

ŠPAČEK, Miroslav, 2014. *Pravděpodobnostní přístupy k analýze rizik investičních projektů a jejich využití v praxi*. Plzeň: Nava. ISBN 978-80-7211-472-6.

TJOA, Simon; JAKOUBI, Stefan a QUIRCHMAYR, Gerald, 2008. *Enhancing Business Impact Analysis and Risk Assessment Applying a Risk-Aware Business Process Modeling and Simulation Methodology*. Online. 2008 Third International Conference on Availability, Reliability and Security. S. 179-186. ISBN 978-0-7695-3102-1. Dostupné z: <https://doi.org/10.1109/ARES.2008.206>. [cit. 2025-02-21].

VASILYEV, Vladimir; KIRILLOVA, Anastasia; VULFIN, Alexey a NIKONOV, Andrey, 2021. Cybersecurity Risk Assessment Based on Cognitive Attack Vector Modeling with CVSS Score. Online. 2021 International Conference on Information Technology and Nanotechnology (ITNT). 2021-9-20, s. 1-6. ISBN 978-1-6654-3217-7. Dostupné z: <https://doi.org/10.1109/ITNT52450.2021.9649191>. [cit. 2025-03-05].

VOJÁČEK, Jan, [2024]. *Statistika pro nematematiky: pravděpodobnostní myšlení a základy statistiky nejen v moderní medicíně*. Praha: Maxdorf. ISBN 978-80-7345-785-3.

YLÖNEN, Marja a AVEN, Terje, 2023. A framework for understanding risk based on the concepts of ontology and epistemology. Online. *Journal of Risk Research*. 2023-06-03, roč. 26, č. 6, s. 581-593. ISSN 1366-9877. Dostupné z: <https://doi.org/10.1080/13669877.2023.2194892>. [cit. 2025-01-24]

SEZNAM OBRÁZKŮ

Obrázek 1 Proces managementu rizik	22
Obrázek 2 Triáda CIA.....	25
Obrázek 3 Postup BIA	32
Obrázek 4 Princip ALARP	35
Obrázek 5 Schéma analýzy typu motýlek.....	36
Obrázek 6 Posloupnost ETA.....	38
Obrázek 7 Metodologický postup identifikace kritérií	49
Obrázek 8 Seskupení kritérií.....	51
Obrázek 9 Návrh nástroje – část 1	79
Obrázek 10 Návrh nástroje – část 2	80
Obrázek 11 Návrh nástroje – část 3	80
Obrázek 12 Návrh nástroje – část 4	81
Obrázek 13 Návrh nástroje – část 5	82

SEZNAM TABULEK

Tabulka 1 Silné stránky a omezení metody BIA	33
Tabulka 2 Příklad matice rizik	34
Tabulka 3 Silné stránky a omezení Matice rizik	35
Tabulka 4 Silné stránky a omezení Analýzy typu motýlek	37
Tabulka 5 Silné stránky a omezení LOPA	39
Tabulka 6 Silné stránky a omezení HRA	40
Tabulka 7 Silné stránky a omezení PIA/DPIA	41
Tabulka 8 Silné stránky a omezení GAP	42
Tabulka 9 Silné stránky a omezení OCTAVE	43
Tabulka 10 Silné stránky a omezení CVSS	44
Tabulka 11 Stupnice bodovací metody	65
Tabulka 12 Váhy kritérií dle bodovací metody	66
Tabulka 13 Stupnice intenzity významu varianty	69
Tabulka 14 Zařazení kritérií do skupin	71
Tabulka 15 Saaty – respondent 1	71
Tabulka 16 Saaty – respondent 2	72
Tabulka 17 Saaty – respondent 3	72
Tabulka 18 Saaty – respondent 4	72
Tabulka 19 Rozptyl hodnot jednotlivých analýz	72
Tabulka 20 Průměr skupin kritérií	73
Tabulka 21 Výstup metod	74
Tabulka 22 Porovnání metod na základě stanovených kritérií	76

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ALARP	As low as resonably practicable
BIA	Business Impact Analýza
CIA	Důvěrnost (Confidentiality), Integrita (Integrity) Dostupnost (Availability)
CSF	Cybersecurity Framework
DDoS	Distributed Denial of Service
DPIA	Posouzení vlivu na ochranu osobních údajů
ENISA	Evropská agentura pro bezpečnost sítí a informací
ETA	Analýza stromu událostí
FTA	Analýza stromu poruchových stavů
GDPR	Obecné nařízení o ochraně osobních údajů
HRA	Analýza bezporuchové činnosti člověka
ICT	Informační a komunikační technologie
ISMS	Systém řízení bezpečnosti informací
ISO	Mezinárodní organizace pro normalizaci
KB	Kybernetická bezpečnost
LOPA	Layers of protection analysis
MTD	Maximálně přijatelný času prostojů
MTPD	Maximální tolerovatelná doba přerušení
NIS	Network Information Security
NIST	Národní institut standardů a technologie
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OCTAVE	Operačně kritické hodnocení hrozeb, aktiv a zranitelností
PIA	Posouzení dopadů na soukromí
PoC	Proof of Concept
RBT	Risk Based Thinking
RPO	Cíl obnovy dat
RTC	Schopnost obnovy
SFAIRP	So far as is resonably practicable
SP	Special Publication
TCP/IP	Transmission Control Protocol / Internet Protocol
TLP	Traffic Light Protocol

Použité zkratky ve vzorcích

R	Riziko
P	Pravděpodobnost
D	Dopad
m	Počet příznivých výsledků jevu A
n	Počet všech možných výsledků
A a B	Vyjádření události
$P(A B)$	Podmíněná, aposteriorní pravděpodobnost, kdy se událost A objeví, pokud nastala událost B
$P(B A)$	Podmíněná aposteriorní pravděpodobnost, kdy se událost B objeví, pokud nastala událost A
$P(A)$ a $P(B)$	Apriorní vyjádření pravděpodobnosti A a B