Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informačních technologií

Využití teorie her k detekci anomálií

Diplomová práce

Autor práce: Bc. Dominik Búzik
Studijní obor: Aplikovaná Informatika

Vedoucí práce: doc. RNDr. Kamila Štekerová, Ph.D., MSc.

Hradec Králové srpen 2022

Prohlášení

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a s použitím uvedené literatury.

. . . . . .

V Hradci Králové dne 9. srpna 2022 Dominik Búzik

Poděkování

Děkuji vedoucí práce doc. RNDr. Kamile Štekerové, Ph.D., MSc. za metodické vedení práce, cenné rady, připomínky, věnovaný čas a poskytnutí vhodných studijních materiálů.

Anotace

Datová věda je v posledních letech velmi vyhledávaným vědním oborem. Díky vývoji v oblastech Internet of Things, elektronickému obchodování či rozvoji sociálních sítí vzniká obrovské množství dat, které je možné zpracovat pro získání informací a vědomostí. Tyto zpracovaná data mohou posloužit například k lepšímu rozhodování ve firmách, zlepšení zdravotní péče či zlepšování firemních procesů. Teorie her se zabývá modelováním konfliktních rozhodovacích situací, proto je vhodné situace v oblastech, kde je nutné činit informovaná rozhodnutí, modelovat jako hru. Takovou rozhodovací situací je například detekce anomálií. Tato diplomová práce se zabývá využitím teorie her v oblasti detekce anomálií. Teoretická část se zabývá základy práce s daty, metodami strojového učení a vybranou oblastí datové vědy - detekcí anomálií. Dále jsou popsány základy teorie her a způsoby řešení her. V praktické části je formou systematické rešerše pomocí metodiky PRISMA zkoumáno uplatnění teorie her v oblasti detekce anomálií.

Annotation

Title: Game-Theoretic Approaches for Anomaly Detection

Data Science has been highly sought-after scientific field in recent years. Thanks to development in areas such as Internet of Things, electronic trading or the development of social networks, a huge amount of data is created that can be processed to obtain information and knowledge. This processed data can be used, for example, to make better business decisions, improve health care or improve business processes. Game Theory is focused on the modeling of conflictual decision-making situations, therefore it is appropriate to model the situation in areas where it is necessary to make informed decisions as a game. Such a decision-making situation is, for example, the detection of anomalies. This Diploma Thesis deals with the use of Game Theory in the field of anomaly detection. The theoretical part deals with the basics of working with data, machine learning methods and selected area of Data Science - anomaly detection. Furthermore, the basics of Game Theory and methods of solving games are described. In the practical part, the application of Game Theory in the field of anomaly detection is investigated in the form of a systematic research using the PRISMA methodology.

Obsah

1 Úvod **1**

2 Datová věda **2**

2.1 Vlastnosti dat . . . 3
2.2 Ukládání dat . . . 4
2.3 Nástroje pro práci s daty . . . 5
2.4 Práce s daty . . . 7
2.4.1 Shromáždění dat . . . 8
2.4.2 Příprava dat . . . 9
2.4.3 Explorace dat . . . 11
2.5 Oblasti využití datové vědy . . . 12

3 Strojové učení **14**

3.1 Algoritmy strojového učení . . . 15
3.1.1 Analýza hlavních komponent . . . 16
3.1.2 Shluková analýza . . . 17
3.1.3 Predikce . . . 18
3.1.4 Klasifikace . . . 19
3.1.5 Zpracování přirozeného jazyka . . . 22
3.1.6 Asociační analýza . . . 22
3.1.7 Neuronové sítě . . . 23

4 Detekce anomálií **25**

5 Teorie her **29**

5.1 Základní pojmy . . . 29
5.1.1 Hráč . . . 30
5.1.2 Hra . . . 30
5.1.3 Užitek . . . 30
5.1.4 Klasifikace her . . . 31
5.2 Reprezentace her . . . 32
5.2.1 Hra v normálním tvaru . . . 32
5.2.2 Hra v rozvinutém tvaru . . . 32
5.3 Řešení her v normálním tvaru . . . 33
5.3.1 Dominovanost . . . 33

5.3.2 Nashova rovnováha 34
5.3.3 Hledání řešení ve smíšených strategiích 37
5.4 Řešení her v rozvinutém tvaru 37
5.5 Další typy her 38

6 Systematická rešerše **40**
6.1 Metodika PRISMA 40
6.2 Metodika zpracování 41
6.3 Výběr a analýza článků 42

7 Souhrn výsledků **57**
7.1 Odpověď na otázku 1: Oblasti využití detekce anomálií 57
7.2 Odpověď na otázku 2: Typy detekce anomálií a her 58
7.3 Odpověď na otázku 3: Přínos použití teorie her 59

8 Závěr **60**

Literatura **61**

Seznam obrázků

1 Ukázka zápisníku Deepnote 7
2 Životní cyklus datové vědy 8
3 Přehled typů metod strojového učení 14
4 PCA: Atributy dat a komponenty 16
5 Matice záměn 19
6 Metoda podpůrných vektorů 21
7 One-class SVM 21
8 Architektura MLP 24
9 Architektura BiGAN 24
10 Kontextová anomálie teploty v čase 25
11 Kolektivní anomálie v elektrokardiogramu 26
12 Strom hry obchodního řetězce 38
13 Vývojový diagram PRISMA 43
14 Počty nalezených článků dle roku vydání 43

Seznam tabulek

1 Souhrn pěti základních hodnot 12
2 Analýza článků zahrnutých v rešerši 44

1 Úvod

Datová věda se v posledních letech stala velmi atraktivním vědním oborem. Díky rozvoji sociálních sítí, elektronické komunikace, obchodování po síti Internet či rozšíření sítí Internet of Things do oblastí běžného života, průmyslu, zabezpečení nebo zdravotnictví vzniká obrovské množství dat. Z těchto dat je možné získat mnoho informací a znalostí, které nám mohou přinést zlepšení v nejen v těchto oblastech. S vývojem stále výkonnějších počítačů a metod strojového učení je možné snadněji analyzovat velké množství dat v krátkém čase, díky čemuž je možné zlepšovat stávající firemní procesy, činit informovaná rozhodnutí, zlepšovat zdravotní péči či uživatelský zážitek při používání produktů. Zvláště v oblasti rozhodování nachází vhodné využití vědní disciplína teorie her, která se zabývá studiem konfliktních rozhodovacích situací. V teorii her jsou informace klíčovým prvkem pro učinění správného rozhodnutí, proto je vhodné metody těchto oborů využívat současně.

Cílem této diplomové práce je popsat a zhodnotit možnosti uplatnění teorie her v aplikační oblasti datové vědy - detekce anomálií. V teoretické části bude čtenář seznámen se základními principy práce s daty, algoritmy strojového učení používanými v datové vědě a problematikou oblasti detekce anomálií. Seznámení s algoritmy strojového učení používanými v datové vědě je důležité pro orientaci v praktické části, neboť se zde mohou vyskytnout. Dále bude čtenář seznámen se základními pojmy teorie her a způsoby řešení her. V praktické části bude formou systematické rešerše pomocí metodiky PRISMA představeno uplatnění teorie her v oblasti detekce anomálií. V závěru budou shrnuta zjištění o využití metod detekce anomálií a uplatnění teorie her v této oblasti.

2 Datová věda

V dnešní době je každý den na světě vyprodukováno obrovské množství dat různých typů a forem. Data mohou být produkována záměrně - mohou to být textové či jiné dokumenty, záznamy hovorů, obrázky, zvukové soubory a spousty jiných typů dat. Data jsou generována také pouhou aktivitou - mohou to být záznamy ze senzorů vibrací pracovních strojů, data z osobních fitness náramků, aktivita uživatelů na webových stránkách, data generovaná senzory IoT zařízení, záznamy z autonomních vozidel a mnoho dalších. Data generovaná každodenním děním lze zachytávat a převádět na strojově zpracovatelná data. Proces převodu na strojově zpracovatelná data se nazývá datafikace [1]. Tato na první pohled nezajímavá data je však možné zpracovat, analyzovat a získat z nich velmi cenné informace a znalosti.

Procesem zpracování a analýzy dat se zabývá datová věda. Datová věda není nijak nová záležitost. Již v roce 1962 John W. Tukey ve svém článku „The Future of Data Analysis“ [2] zmiňuje důležitost rozvoje datové analýzy, neboli získávání vědomostí z dat, jako samostatné vědy, nejen jako součást matematické statistiky. V průběhu následujících let byl termín „Data Science“ používán v mnoha publikacích, dle Howarda Wainera [3] byl tento termín poprvé použit ještě dříve, než John W. Tukey vydal svůj článek - v roce 1960 Peterem Naurem: „Data science is the study of the generalizable extraction of knowledge from data“.

Díky rozvoji počítačových technologií se klade na datovou analýzu mnohem větší důraz než dříve. Data, která byla mnohdy opomíjena, v sobě mohou obsahovat skryté znalosti. Díky nízkým cenám počítačů a datových úložišť je mnoho společností schopných ukládání velkého množství těchto dat. Strojové zpracování dat bylo dříve výsadou jen několika největších firem, například Google či IBM. Tyto firmy disponovaly dostatečným výpočetním výkonem i prostorem pro data, aby je mohly zpracovávat. Postupem času se však staly výkonné počítače dostupnými pro všechny, ať již formou pronajmutí výpočetního výkonu - cloud computingem[1], či zakoupením fyzického vybavení. Díky současnému rozvoji se může tomuto tématu věnovat mnohem více lidí. [4]

Datová věda v sobě kombinuje několik různých oborů, jako je matematika, statistika, ale také informatika. Výsledkem práce datových vědců a vědkyň jsou informace, získané pomocí průzkumu dat, které napomáhají například k činění informovaných

[1] Cloud computing je forma dodávání výpočetního výkonu či úložiště ze vzdáleného umístění přes síť Internet

rozhodnutí. Datová věda umožňuje lidem prozkoumávat svět pomocí dat v několika směrech. Hlavními směry jsou [4]:

- **Zkoumání reality** nám umožňuje objevovat reakce okolí na předchozí události a pomocí pochopení těchto reakcí přizpůsobovat následující události. Tato strategie chování se využívá v různých formách testování (softwarové, zkoumání reakce trhu na nový výrobek a podobně).
- **Rozpoznávání vzorů** je velmi důležitá oblast například v medicíně, kde pomáhá stanovit diagnózu na základě analýzy a klasifikace obrazových dat.
- **Predikce** budoucích událostí je oblast, které se velmi věnuje statistická analýza. Statistická analýza se zakládá na historických datech (například časových řadách), pomocí kterých se snaží vytvářet dostatečně robustní modely, díky kterým by lidé byli schopni na základě minulých událostí reagovat na události, které mohou teprve nastat. Pro dostatečnou přesnost těchto modelů je zapotřebí mnoha vhodně připravených dat. Použitím metod datové vědy je možné identifikovat důležitá data, která tyto modely mohou obohatit.
- **Snaha o porozumění lidem a světu.** Tímto směrem se zabývají například oblasti strojového učení, které se věnují zpracování a generování přirozeného jazyka či rozpoznávání obrazu.

2.1 Vlastnosti dat

Základem pro metody datové vědy jsou samotná data. Jak již bylo napsáno, data mohou nabývat různých forem:

- **strukturovaná data** mají často podobu matice, kde řádky jsou jednotlivé záznamy a sloupce jsou vlastnosti těchto záznamů,
- **polostrukturovaná data** mají často formu dokumentu, například soubory JSON či XML,
- **nestrukturovaná data** jsou data v jejich originálním formátu (obrazová, zvuková data, různé dokumenty atd.).

Data lze dle [5] rozdělit na několik typů:

- **Kvantitativní data** jsou číselné hodnoty, které lze zařadit na nějakou stupnici. S kvantitativními daty lze bez jakýchkoliv úprav provádět matematické operace, porovnávat je mezi sebou či je řadit. Příkladem kvantitativních dat jsou například rozměry, váha, věk, vzdálenost či počet.

- **Kategorická data** popisují vlastnosti objektů. Podle jednotlivých vlastností je možné objekty přiřazovat do určitých kategorií. Kategorická data se dále dělí na nominální a ordinální. Nominální kategorická data nemají žádné pořadí, například názvy měst. Ordinální kategorická data mají určité pořadí, například rozdělení velikosti na malou, střední a velkou. Pro statistickou analýzu je lze překódovat do numerických hodnot. Příkladem kategorických dat je například věk, pohlaví, úroveň vzdělání, barva či země původu.

2.2 Ukládání dat

Pro ukládání dat se běžně používají systémy řízení báze dat. Tyto systémy se starají o ukládání dat do databáze, což je systém souborů s danou strukturou záznamů. Pojmem databáze se často označují jak samotná data, tak i systém řízení báze dat. Jedním z hlavních aktuálně používaných typů databází jsou relační databáze. Pro ukládání dat používají tabulky se sloupci, kde jednotlivé řádky reprezentují datové položky. Data uložená v relační databázi mají přesně definovaný formát, jsou tedy strukturovaná. Pro práci s nimi se používá jazyk SQL. Druhým velmi často používaným typem databáze je ne-relační (označován jako NoSQL). Jak uvádí [6], data v NoSQL databázi mohou být ukládána různými způsoby, například formou klíč-hodnota, formou dokumentů (ve formátu JSON či XML) a jinými. Data v NoSQL databázi mohou být strukturovaná či polostrukturovaná.

V klasických produkčních databázích se většinou nacházejí data aktuální, která se mohou často a rychle měnit či přibývat. Pro další analýzu je však vhodné mít nejen data aktuální, ale také historická. Pro ukládání takových dat se používá datový sklad (anglicky Data Warehouse). Dle [7] je datový sklad zvláštní typ databáze, který je určený pro analýzu dat. Data jsou do datového skladu ukládána pomocí tzv. datové pumpy z různých provozních databází. Datová pumpa pro svou činnost využívá ETL nástroje (zkratka slov „Extraction“, „Transformation“ a „Loading“). ETL nástroje, jak z významu zkratky vyplývá, vykonávají tři důležité kroky: extrakci dat určených k uložení, jejich transformaci (očištění, formátování) a samotné ukládání. Tento proces ukládání se děje periodicky, data obsažená v datovém skladu tak nemusí být aktuální. Data uložená v datovém skladu jsou strukturovaná a očištěná, což ulehčuje jejich následnou analýzu. Příkladem implementace datového skladu je například Oracle Autonomous Data Warehouse či Google BigQuery.

Zcela jiným přístupem ke skladování dat je datové jezero (anglicky Data Lake). Datové jezero je, jak uvádí [8] způsob ukládání dat do úložiště, při kterém se do jednoho úložiště ukládají jak data strukturovaná, tak polostrukturovaná či nestruk-

turovaná. Cílem této metody je mít jedno velké centralizované úložiště, ve kterém se mohou nacházet jak data připravená pro pozdější využití, tak i data surová, ať již ve formě dokumentů či například obrázků, zvukových a jiných souborů, ukládaných v původním formátu. Příkladem takového typu úložiště je například Azure Data Lake či Amazon AWS S3.

Datové sklady a datová jezera se liší nejen typem dat, která v nich mohou být uložena, ale také metodologií přístupu k nim. Podle [9] má datový sklad již při jeho vytvoření definován schéma, které definuje sloupce tabulek s daty. Toto schéma je tedy navrženo tak, aby se ukládala pouze data, která byla při návrhu datového skladu identifikována jako důležitá. Přístup, kdy ukládaná data mají předem danou strukturu, se anglicky nazývá Schema on Write. Naopak datové jezero umožňuje ukládat všechny možné druhy dat, bez ohledu na strukturu či datový typ. Tento přístup umožňuje mnoho možností načítání různých dat bez ohledu na jejich souvislost, což může být vhodné například pro hledání skrytých souvislostí mezi daty. Takový přístup se anglicky nazývá Schema on Read.

2.3 Nástroje pro práci s daty

Pro práci s daty existuje mnoho programů a jazyků. Výběr vhodného programu či jazyka záleží na typu dat, se kterými pracujeme a na problému, který řešíme. Pro obecné použití se však nabízí několik programovacích jazyků a programů, které budou na následujících řádcích představeny.

Zřejmě nejjednodušším programovacím jazykem pro použití v datové vědě je Python. Tento interpretovaný, objektově orientovaný programovací jazyk je díky velkému množství podpůrných knihoven a dobré čitelnosti kódu velmi oblíbený. Je často používán pro manipulaci s daty, interpretaci dat pomocí grafů či implementaci strojového učení. Mezi velmi často používané knihovny patří:

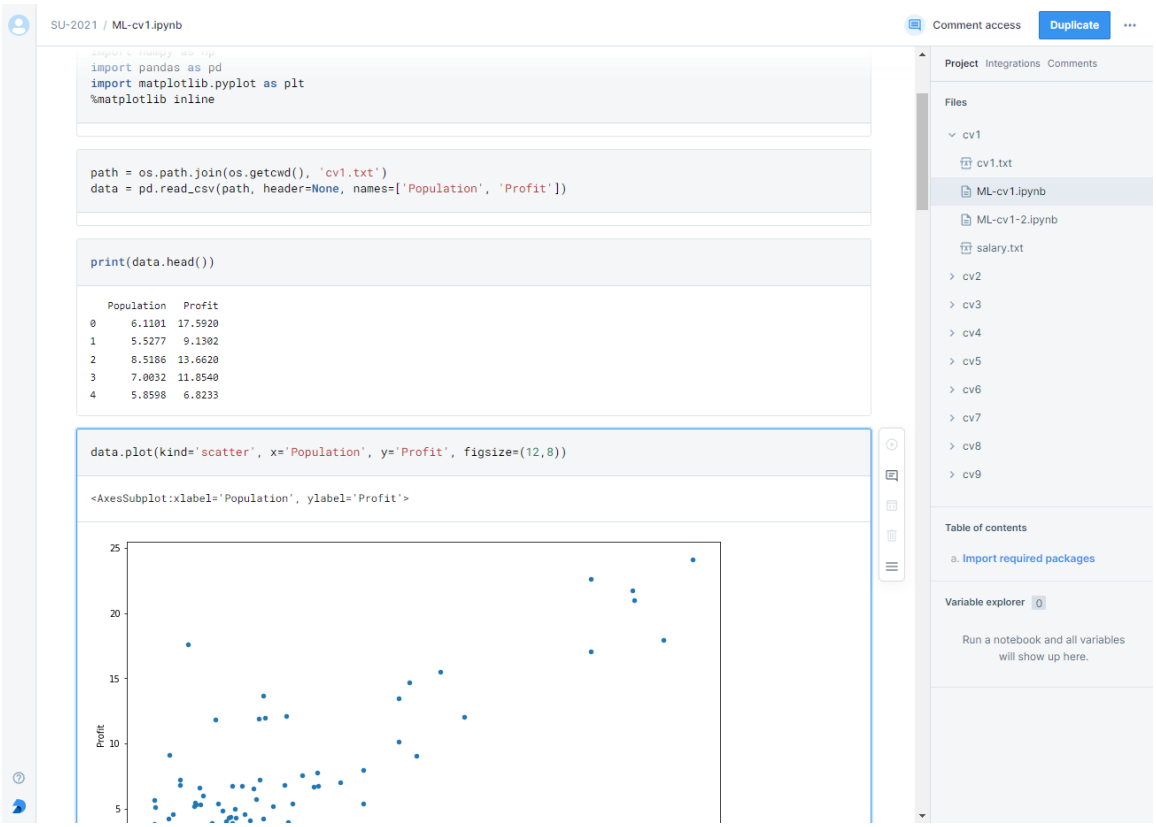
- **NumPy**, celým názvem Numerical Python, slouží k provádění matematických operací s maticemi.
- **Pandas** je knihovna, která umožňuje práci s daty v mnoha různých formátech. Umožňuje manipulaci, vizualizaci a analýzu dat.
- **SciPy** obsahuje funkce pro vědecké a technické výpočty.
- **Scikit-learn** je knihovna, která obsahuje funkce pro strojové učení. Součástí je mnoho funkcí například pro klasifikaci, regresi či shlukování.
- **Matplotlib** je knihovna používaná pro vizualizaci dat pomocí různých druhů grafů.

Možnou nevýhodou jazyka Python je výkon, neboť je to jazyk interpretovaný. Avšak díky jednoduchosti použití i pro začátečníky je velice oblíbeným nástrojem. [10]

Dalším velmi oblíbeným programovacím jazykem je jazyk R. Tento jazyk je často využíván pro statistickou analýzu a vizualizaci dat. Zajímavostí je dle [5] provázanost s jazykem Python, kdy v Pythonu lze volat funkce knihoven R. Pro jazyk R existuje mnoho dalších knihoven, které rozšiřují jeho možnosti práce s daty.

Pro statistickou analýzu a matematické operace existuje mnoho programů. Mezi nejznámější dle [5] patří aplikace Matlab, která je založena na práci s maticemi. V datové vědě lze použít například pro zpracování dat, využití algoritmů strojového učení či vytváření prediktivních modelů. Pro statistickou analýzu či použití algoritmů strojového učení je často používán program IBM SPSS. Velmi oblíbeným nástrojem pro vizualizaci a průzkumnou analýzu dat je také program Microsoft Excel.

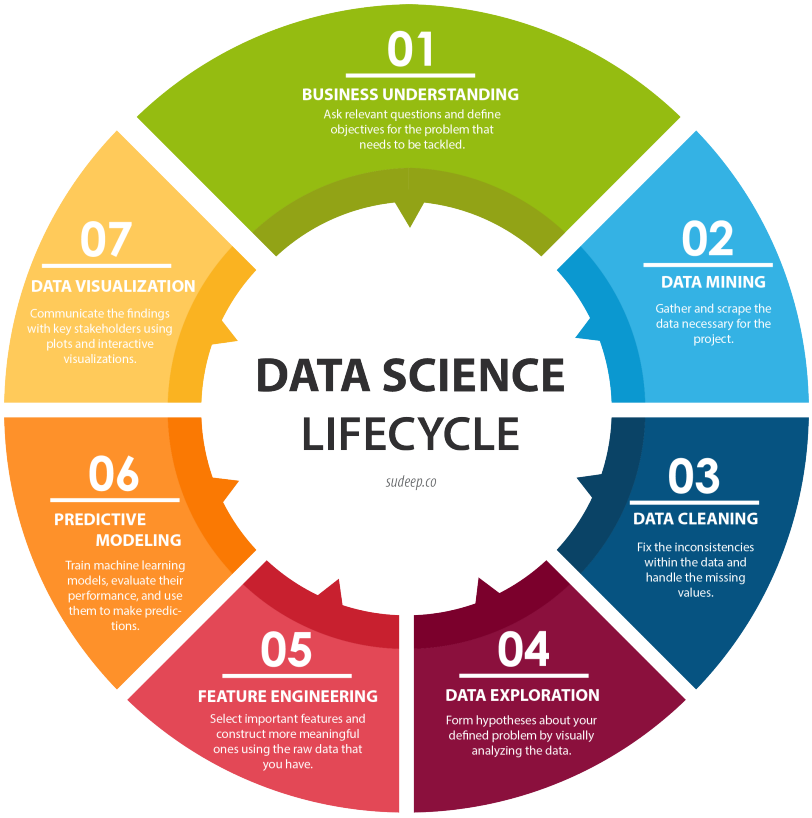
Pro efektivní práci s daty a jejich prezentaci je velmi vhodné používat tzv. zápisník (anglicky notebook). Jak uvádí [11], tento zápisník představuje interaktivní pracovní nástroj, který významně ulehčuje práci v týmu. Podstatou tohoto nástroje je jeho univerzálnost. Do zápisníku je možné zapisovat formátovaný text, ale také programový kód, který je možné v zápisníku spustit a následně lze zobrazit jeho výstupy. Výstupy vykonaného kódu mohou být nejen textové, ale také grafické. Díky možnosti zobrazení a úpravy kódu a následnému zobrazení jeho výsledků je zajištěna reprodukovatelnost, která je pro výzkum velmi důležitá. Mezi největší výhody zápisníku patří přenositelnost, možnost sdílení s více členy týmu a možnost srozumitelné prezentace získaných výsledků včetně postupů, kterými jich bylo dosaženo. Zápisníky mohou být spouštěné v lokálním prostředí, ale také mohou být hostované ve vzdáleném prostředí. Mezi nejvíce používané zápisníky patří Jupyter Notebook, Kaggle, DeepNote či Google Collab.



Obrázek 1: Ukázka zápisníku Deepnote. Zdroj: vlastní zpracování

2.4 Práce s daty

Hlavním zájmem datové vědy je hledání informací či odpovědí na otázky, které pomohou lidem s pochopením procesů či s učiněním informovaného rozhodnutí. Proto je důležité určit důležité otázky, na které chceme najít odpovědi či specifikovat problém, který chceme vyřešit. Jak uvádí [12], prvním krokem v procesu hledání řešení pomocí datové vědy je tedy právě identifikace problémových oblastí, pro které chceme najít řešení, otázek, pro které chceme najít odpovědi, či podmínek, které dané řešení musí splňovat. Po určení prvotního problému je nutné detailně specifikovat kroky, které povedou k nalezení řešení a metriky, pomocí kterých bude určena úspěšnost řešení. Po určení těchto důležitých kritérií se lze zaměřit na prostředky a data, pomocí kterých bude možné hledaná řešení či odpovědi nalézt. Tyto kroky jsou také ilustrovány na obrázku 2.



Obrázek 2: Životní cyklus datové vědy. Zdroj: [13]

Hlavními kroky pro práci s daty jsou:

1. **Shromáždění dat:** proces, při kterém získáme všechna data, která budou potřeba pro nalezení hledané odpovědi či řešení.
2. **Příprava dat:** vyčištění a sjednocení dat tak, aby bylo možné je porovnávat.
3. **Explorace dat:** prozkoumání vlastností dat.

Po provedení těchto kroků je možné data použít pro vytvoření modelů sloužících k nalezení řešení.

2.4.1 Shromáždění dat

Shromáždění potřebných dat pro daný problém je velmi časově náročný proces. Data jsou často shromážděná do datových sad velkých rozměrů. Data, která jsou potřebná k nalezení řešení daného problému se často týkají osob či organizací. Pokud tato data nejsou již ošetřena, je nutné pro jejich použití podniknout kroky, které zamezí jejich identifikaci. V České republice se tomuto tématu věnuje Obecné nařízení o ochraně

osobních údajů, označováno anglickou zkratkou GDPR (General Data Protection Regulation). Prakticky se jedná o techniky:

- **Anonymizace**, při jejichž použití dojde k nevratné ztrátě možnosti identifikace jednotlivce. [14]
- **Pseudonymizace**, při jejichž použití dojde k náhradě osobních informací pseudonymy. Po pseudonymizaci nelze jednotlivce identifikovat bez použití dalších informací. Osobní data jsou například zašifrována a bez použití klíče je nelze použít k identifikaci. Informace, které lze použít pro zpětnou identifikaci musí být odděleny od zbytku dat. [15]

Pro získání dat existuje několik možností. Mnoho velkých firem poskytuje data, která je možné zveřejnit, například pomocí aplikačního programového rozhraní či jako balíku dat ke stažení, viz [5]. Jiným zdrojem dat mohou být státní organizace. Na internetových stránkách Národního katalogu otevřených dat [16] je k dispozici mnoho datových sad, rozdělených přehledně dle témat, klíčových slov či formátů dat včetně pravidel, při jejichž dodržení je možné takto získané datové sady používat. V případě řešení problému pro určitou organizaci je možné získat přístup k vnitřním datům dané organizace, se kterými lze následně pracovat.

Po úvodní fázi, při které se identifikují problémy k řešení, je nutné určit, jaká data budou k řešení potřeba. Jak uvádí [17], potřebná data jsou často umístěna na různých úložištích, ke kterým nemusíme mít přístup. Data jsou často duševním vlastnictvím, proto je k jejich získání a použití nutné získat souhlas vlastníka a seznámit se s pravidly nakládání s nimi.

Pro cvičné aplikace, jako je například vyzkoušení různých algoritmů, existuje mnoho datových sad, které jsou často již alespoň částečně předpřipravené k použití. Vhodné datové sady jsou k nalezení například na internetových stránkách Kaggle (www.kaggle.com). Pro konkrétní aplikace je však použití cvičných datových sad nevhodné.

2.4.2 Příprava dat

Po získání potřebných dat je nutné je připravit pro použití. Pro propojení dat z různých zdrojů je nutné najít společné vlastnosti, pomocí kterých je toto propojení možné, například seskupením pomocí společného atributu. Při propojování je často užitečné vytvořit nové atributy, které v sobě zahrnou data z propojených zdrojů. Například při propojení dat o zákaznících a jejich nákupech je vhodné vytvořit nové atributy popisující souhrn či průměr jejich útrat [18]. Při práci s numerickými daty

je vhodné předem určit, v jakých jednotkách budou data zapsána a všechna data do těchto jednotek převést. Toto sjednocení jednotek umožní smysluplné porovnávání. Stejně tak je vhodné sjednotit formát zápisu kalendářních dat, reprezentaci numerických hodnot či názvů (často je používáno více názvů pro totožnou entitu, například kvůli chybnému zapsání názvu či různému použití velkých a malých písmen) [5]. Kategorická data je často vhodné překódovat na numerické hodnoty. Překódování dat není nutnou podmínkou, ale mnoho statistických programů jej pro svou práci požaduje. Při překódování ordinálních dat je vhodné volit hodnoty tak, aby korespondovaly s významem dat, například při překódování velikosti bude hodnota 1 odpovídat malé velikosti, hodnota 2 střední velikosti a tak dále.

Získaná data mohou obsahovat prázdné hodnoty. Důvody vzniku prázdných hodnot jsou různé, například prázdné datum úmrtí v záznamu živého člověka či záměrně nevyplněné pole v dotazníku. Problém chybějících hodnot lze dle [5] řešit odstraněním záznamů s chybějícími hodnotami a nebo jejich nahrazením. Záznamy s chybějícími daty je možné odstranit v případě, že po odstranění zůstane dostatečně velký objem dat. Pro co nejmenší zkreslení vlastností dat je ale vhodnější nahradit chybějící data. Tento proces nahrazení se nazývá imputace. Nejjednodušším způsobem nahrazení dat je použití střední hodnoty daného atributu. Mezi jiné způsoby doplnění chybějících hodnot patří také použití lineární regrese pro predikci chybějící hodnoty, doplnění náhodně zvolené hodnoty z množiny hodnot daného atributu či využití heuristiky, kdy při dostatečné znalosti oblasti, ke které se daný atribut vztahuje, můžeme odhadnout přibližnou hodnotu.

Pro objektivní srovnání prvků s různými rozměry se používá standardizace dat. Tato metoda statistické analýzy umožňuje převést hodnoty atributů z různých měřítek na jednotné měřítko. Pro standardizaci se nejčastěji používají tyto metody:

- **Standardizace rozpětím**, také označovaná jako „min-max normalizace“, transformuje hodnoty daného atributu na hodnotu v rozpětí 0-1. Provádí se dle vzorce

$$u_i = \frac{x_i - min(x_i)}{max(x_i) - min(x_i)}, \tag{1}$$

  kde $\min(x_i)$ značí minimální hodnotu a $\max(x_i)$ maximální hodnotu daného atributu.

- **Standardizace vzhledem k průměru** transformuje hodnoty daného atributu tak, že průměrná hodnota se po transformaci bude rovnat nule. Provádí se dle

vzorce

$$u_i = \frac{x_i - \mu}{max(x_i) - min(x_i)}, \tag{2}$$

kde $\min(x_i)$ značí minimální hodnotu, $\max(x_i)$ maximální hodnotu a μ značí průměrnou hodnotu daného atributu.

- **Standardizace směrodatnou odchylkou**, také označovaná jako Z-skóre, transformuje hodnoty daného atributu tak, aby výsledné rozdělení mělo průměr 0 a směrodatnou odchylku 1. Provádí se dle vzorce

$$z_i = \frac{x_i - \mu}{\sigma}, \tag{3}$$

kde μ značí průměrnou hodnotu a σ značí směrodatnou odchylku hodnot daného atributu.

Po provedení standardizace jsou atributy převedeny na jednotné měřítko, což ulehčí nalezení odlehlých hodnot. Odlehlé hodnoty jsou naměřené hodnoty, které se významně liší od ostatních hodnot daného atributu. Odlehlé hodnoty mohou být způsobeny chybou v měření či zaznamenání, ale mohou také být zcela validní. Proto je nutné se rozhodnout, zda takovou hodnotu odstranit či nikoliv. Například při použití metod pro detekci anomálií jsou odlehlé hodnoty v datové sadě velmi důležité a jejich odstraněním by došlo k nepoužitelnosti datové sady.

2.4.3 Explorace dat

Pro bližší porozumění datům, hledání souvislostí mezi daty a vytváření předpokladů je důležité se seznámit s jejich vlastnostmi. Prvotním krokem je seznámit se se samotnou datovou sadou: kdy byla data vytvořena, jak je datová sada veliká, jaký je význam jednotlivých atributů. Poté je vhodné se seznámit se základními statistickými vlastnostmi jednotlivých atributů. Pro ilustraci byla použita datová sada měření těla, měrné jednotky jsou palce [19]. Pro jednoduchost byly vybrány jen atributy věk, celková výška a obvod boků. Kategorická data je možné zkoumat pomocí četnosti prvků dané kategorie z celkového počtu. Jednoduchým způsobem zkoumání kvantitativních dat je souhrn pěti základních hodnot [5]:

- minimální hodnota,
- první kvartil, značen jako Q_1, vyjadřuje hodnotu, která je vyšší než 25 % všech hodnot,
- medián, v seřazeném souboru hodnot označuje hodnotu uprostřed,

- třetí kvartil, značen jako Q_3, vyjadřuje hodnotu, která je vyšší než 75 % všech hodnot,
- maximální hodnota.

Tento souhrn lze přehledně zobrazit tabulkou, jak je názorně předvedeno v tabulce 1:

Tabulka 1: Souhrn pěti základních hodnot

	Min	Q_1	Medián	Q_3	Max
věk	1	7	11	21	68
celková výška	19	40	48	55	89
obvod pasu	7	12	18	24	63

Kromě tohoto souhrnu je vhodné také určit střední hodnotu a rozptyl. Střední hodnota se určuje dle vzorce

$$\mu = \frac{1}{n} \sum_{i=1}^{n} x_i, \tag{4}$$

kde n je počet prvků v souboru a x_i jsou jednotlivé hodnoty daného atributu. Rozptyl se určuje dle vzorce

$$\sigma^2 = \frac{1}{n} \sum_{i=1}^{n} (x_i - \mu)^2. \tag{5}$$

Rozptyl udává, jak jsou hodnoty v souboru rozptýleny kolem střední hodnoty. Odmocněním hodnoty rozptylu získáme směrodatnou odchylku. Data ale nelze hodnotit jen dle těchto statistických vlastností, neboť různá data mohou mít stejné charakteristiky. Pro vizualizaci dat je možné použít histogram [4].

2.5 Oblasti využití datové vědy

Metody datové vědy díky rozvoji strojového učení a výpočetního výkonu našly uplatnění v mnoha oborech. Těmito obory jsou [20]:

- **Finance, bankovnictví**: ve finančním sektoru se metody datové vědy využívají například pro analýzu rizik, rozhodování o půjčkách či odhalování podvodů. Mezi využívané metody patří klasifikace, predikce, shlukování či zpracování přirozeného jazyka. Jak uvádí [21], v oblasti odhalování podvodů se intenzivně používá také detekce anomálií. V této oblasti je využívána pro zjišťování zneužití platebních karet z dat o výši a četnosti útrat či zjišťování pojistných podvodů zkoumáním dokumentů o pojistných událostech.
- **Zdravotnictví**: ve zdravotnictví našly uplatnění metody klasifikace pro analýzu lékařských snímků, asociační metody pro genetický výzkum či metody

predikce pro vývoj léků. V této oblasti je detekce anomálií používána v oblasti zkoumání kardiologických problémů [22], hledání chyb ve zdravotních záznamech či celkové analýze zdravotního stavu pacientů [21].

- **Marketing**: metody datové vědy jsou v marketingu hojně využívány. Klasifikační, prediktivní a asociační metody jsou využívány pro cílené reklamy. Shlukovací a asociační metody jsou využívány pro profilování zákazníků, segmentaci trhu či analýzu nákupního košíku. Metody zpracování přirozeného jazyka jsou využívány pro analýzu sentimentu. Doporučující systémy využívají shlukovací, prediktivní a asociační metody pro doporučování obsahu.
- **Zpracování textu**: pro získávání informací z textu, sumarizaci, strojový překlad, spamové filtry a mnohé další úlohy je využíváno zpracování přirozeného jazyka.
- **Doprava**: pro optimalizaci dopravních tras a plánování času jsou využívány prediktivní metody.
- **Průmysl**: v průmyslovém prostředí je kladen velký důraz na minimalizaci poškození způsobeného opotřebením strojů. Opotřebení lze sledovat pomocí množství senzorů, například senzory průtoku či otřesů. Dle [23] lze v zaznamenaných datech hledat anomálie, které mohou indikovat budoucí selhání stroje a včasným varováním tomuto selhání zabránit. Zároveň lze tímto způsobem odhalit poškození či nedovolenou manipulaci se senzory, jejichž selhání může zapříčinit nefunkčnost sledování poškození.

Existuje mnoho dalších odvětví, ve kterých je možné použít metody datové vědy, neboť mnoho firem a organizací denně zaznamenávají obrovské množství dat, ze kterých lze získat cenné informace, které mohou posloužit pro zvýšení efektivity své činnosti.

3 Strojové učení

Po nalezení vhodných dat, jejich zpracování a exploraci je možné tato data použít pro vytvoření modelu, jehož výsledky bude možné použít pro hledání odpovědí na stanovené otázky. Výběr správného modelu záleží na problému, který je řešen, často se používá více modelů. Modely mohou být implementovány pomocí metod strojového učení, které často využívají statistických metod. Metody strojového učení využívané v zde prezentovaných technikách modelování se dělí na dvě skupiny:

- **Učení s učitelem**: pro vytvoření modelu jsou dostupná vstupní data a očekávané výstupy.
- **Učení bez učitele**: pro vytvoření modelu jsou dostupná jen vstupní data bez očekávaných výstupů, cílem je zjednodušit reprezentaci dat či najít skryté struktury v datech.

Obrázek 3: Přehled typů metod strojového učení. Zdroj: [24]

Nejčastěji používané modelovací techniky jsou [20]:

- **Redukce dimenzionality dat**: Jedná se o techniky přípravy dat. Data mají často mnoho atributů, které přinášejí malou či žádnou hodnotu k řešení problému, čímž mohou komplikovat nalezení vhodného řešení. Pomocí metod redukce dimenzionality dat je možné vybrat jen ty parametry, které jsou důležité pro nalezení řešení.
- **Shlukování**: Shlukování je metoda, pomocí které rozdělujeme množinu prvků do předem neznámých homogenních shluků tak, aby si prvky v rámci shluku byly maximálně podobné a mezi shluky byly maximálně odlišné. Toto rozdělení probíhá na základě vzdáleností prvků tak, aby vzdálenosti mezi prvky v rámci shluku byly minimální a vzdálenosti mezi shluky maximální. Model vzniká učením bez učitele.
- **Predikce**: Predikce slouží k nalezení předpokládané výstupní hodnoty na základě matematické funkce popisující dostupná data.
- **Klasifikace**: Tato technika umožňuje rozdělování prvků (kategorizaci) do předem daných tříd na základě jejich vlastností. Zařazení může probíhat právě do jedné třídy nebo do více tříd. Model se vytváří za pomoci tréninkových dat, která obsahují jejich klasifikaci do tříd, jedná se tedy o model učení s učitelem.
- **Zpracování přirozeného jazyka**: Tato technika slouží k analýze textových dokumentů. Na základě této analýzy jsou z textu extrahována důležitá data, která je následně možné použít jako vstup pro jiné modelovací techniky, manipulaci s textem či generování nového textu.
- **Asociační analýza**: Tato technika se zaměřuje na zkoumání závislostí dat na jiných datech. Příkladem je analýza nákupního košíku, ve které se zkoumají asociace mezi společně zakoupenými produkty.

Tyto modelovací techniky samozřejmě nejsou jediné, ale jsou často používané. Pro nalezení řešení také často nestačí využít jen jednu techniku, ale jejich kombinaci.

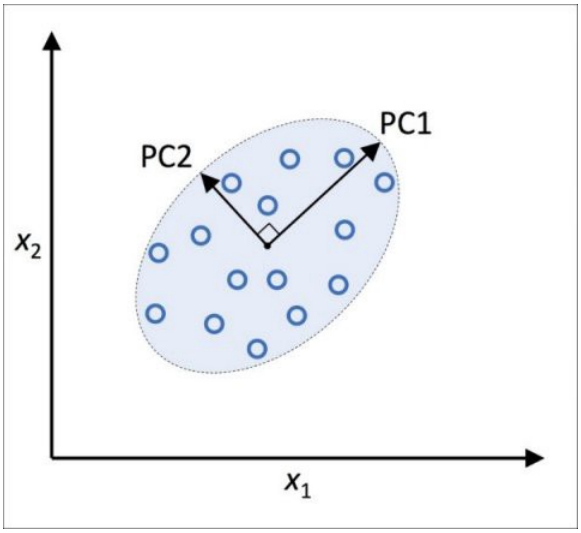
3.1 Algoritmy strojového učení

Pro každou metodu modelování dat existuje několik algoritmů či metod, které je možné použít. V této části jsou představeny často používané algoritmy a přístupy k jednotlivým modelovacím metodám.

3.1.1 Analýza hlavních komponent

Pro redukci dimenzionality dat lze využít výběr důležitých proměnných pomocí korelace nebo extrakci příznaků metodou analýzy hlavních komponent (anglicky Principal Component Analysis, zkráceně PCA). Extrakcí příznaků rozumíme nahrazení existujících proměnných jejich kombinací.

Analýza hlavních komponent je metoda, která reprezentuje původní, vzájemně korelovaná data pomocí komponent, což jsou nové, nekorelované proměnné, které vystihují proměnlivost původních dat. Jak uvádí [25], tyto komponenty jsou na sebe kolmé projekce dat do prostoru menší dimenze. První hlavní komponenta vysvětluje největší část rozptylu dat, každá další komponenta je kolmá na předchozí komponentu a vysvětluje část zbývajícího rozptylu, který není obsažen v předchozí komponentě.



Obrázek 4: PCA: Atributy dat a komponenty. Zdroj: [25]

Pro provedení algoritmu PCA je nejdříve nutné standardizovat data vzhledem k průměru. Poté se určí kovarianční matice, značená Σ. Kovariance vyjadřuje vzájemnou závislost veličin X a Y. Pokud je hodnota kovariance kladná, hodnoty X a Y se pohybují stejným směrem; pokud je záporná, hodnoty X a Y se pohybují směrem opačným. V případě nulové hodnoty jsou X a Y vzájemně nezávislé.

Z kovarianční matice se následně určí vlastní vektory (nazývané eigenvektory). Vlastní vektor matice Σ je takový nenulový vektor u, pro které existuje vlastní číslo λ tak, že platí $\Sigma u = \lambda u$. Tyto vlastní vektory lze získat singulárním rozkladem. Při použití funkce svd z knihovny NumPy jsou výstupem tohoto rozkladu matice U, S, V. Matice U je rozměru $n \times n$ a její sloupce jsou jsou vektory u. Pro výpočet nových

dat je vybráno prvních k sloupců matice U, které utvoří matici U_k rozměru $n \times k$ a použije se pro výpočet nových dat dle vzorce

$$x' = x \cdot U_k, \tag{6}$$

kde x je jeden řádkový vektor původních dat. Stejným způsobem lze transformovat celou sadu dat.

3.1.2 Shluková analýza

Shluková analýza je metoda, kterou je tvořen disjunktní rozklad množiny objektů dle jejich příznaků do předem neznámých homogenních shluků. Při vytváření shluků požadujeme maximální podobnost objektů v rámci shluku a maximální nepodobnost objektů mezi shluky. Shlukování se dělí na hierarchické a nehierarchické.

Hierarchické shlukování

Hierarchické shlukování může být provedeno dvěma způsoby [26]:

- **Aglomerativní**: také nazýván „zdola nahoru“, spočívá v postupném seskupování jednočlenných shluků. Na začátku každý objekt představuje samostatný shluk. Postupně se spojují nejbližší shluky tak, že na konci procesu vznikne jeden velký shluk. Tento postup se zaznamenává do dendrogramu, což je typ stromového grafu zobrazující hierarchii shluků. Oříznutím dendrogramu je získán požadovaný počet shluků.
- **Divizní**: také nazýván „shora dolů“, spočívá v postupném rozdělování jednoho výchozího shluku na více menších shluků. Nové shluky vznikají oddělením nejvíce nepodobných shluků.

Pro měření vzdáleností shluků se používají čtyři metody:

- **Metoda nejvzdálenějšího souseda** určuje vzdálenost mezi nejvzdálenějšími objekty z různých shluků.
- **Metoda nejbližšího souseda** určuje vzdálenost mezi nejbližšími objekty z různých shluků.
- **Metoda průměru** používá průměrnou vzdálenost všech dvojic objektů z různých shluků.
- **Metoda centroidů** používá vzdálenost center dvou různých shluků.

Metoda k-průměrů

Metoda k-průměrů je dle [27] nehierarchická shlukovací metoda, která rozděluje data do předem stanoveného počtu k shluků. Na počátku se náhodně zvolí k centroidů a k nim se následně přiřadí nejbližší objekty. Poté se přepočítá poloha centroidů do center nově vytvořených shluků. Tento proces se opakuje, dokud se nepřestane měnit pozice centroidů.

3.1.3 Predikce

Predikce slouží k predikování budoucích hodnot na základě dostupných hodnot z minulosti. Mezi metody predikce patří lineární regrese. Lineární regrese se dělí na jednoduchou a vícerozměrnou.

Lineární regrese

Jednoduchá lineární regrese zkoumá lineární závislost mezi nezávislou veličinou X a na ní závislou veličinou Y. Dle [28] je tento vztah popsán přímkou:

$$\hat{y} = \beta_0 + \beta_1 x, \tag{7}$$

kde $\hat{y}$ je očekávaná hodnota Y pro $X = x$, β_0 je absolutní člen udávající posun přímky po ose y a β_1 je regresní člen neboli směrnice přímky. Tato přímka se určuje aproximací daných hodnot metodou nejmenších čtverců. Vícerozměrná lineární regrese zkoumá lineární závislost mezi několika nezávislými veličinami X_1, X_2, …, X_n a závislou veličinou Y. Výstupní proměnnou chápeme jako lineární kombinaci hodnot vstupních proměnných. Tento vztah je popsán jako:

$$\hat{y} = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_n x_n. \tag{8}$$

Koeficienty β_0, β_1, …, β_n jsou odhadovány tak, aby odchylky modelu od skutečnosti

$$S = \sum_{i=1}^{n} (y_i - \hat{y}_i)^2 \tag{9}$$

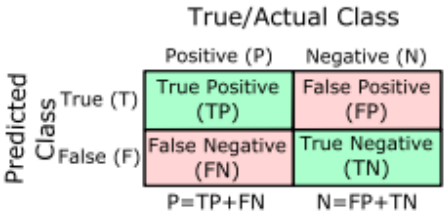
byly minimální.

Sestup gradientu

Algoritmy strojového učení používají pro optimalizaci koeficientů algoritmus sestupu gradientu. Jak uvádí [29], cílem tohoto algoritmu je měnit hodnoty koeficientů tak, aby došlo k minimalizaci takzvané nákladové funkce. V případě lineární regrese je nákladovou funkcí odchylka modelu od skutečnosti, viz (9) či průměrná odchylka modelu od skutečnosti. Algoritmus sestupu gradientu funguje iterativně, v každé iteraci upravuje hodnoty koeficientů tak, aby konvergovaly k lokálnímu minimu nákladové funkce.

3.1.4 Klasifikace

Klasifikace spočívá v rozdělení prvků do kategorií či tříd dle jejich vlastností. Toto rozdělení provádí klasifikátor, což je algoritmus, který mapuje vstupní data na kategorie. Pro hodnocení úspěšnosti klasifikátoru se používá matice záměn, která poskytuje několik metrik, dle kterých lze úspěšnost hodnotit. Matici záměn pro binární klasifikaci lze sestavit dle obrázku 5. Matice záměn se skládá z počtu skutečných/predikova-



Obrázek 5: Matice záměn. Zdroj: [30]

ných správně/nesprávně klasifikovaných příkladů. Z těchto hodnot je možné odvodit metriky [30]:

- **Správnost**: podíl správně klasifikovaných příkladů

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}, \tag{10}$$

- **preciznost**: podíl skutečně pozitivních mezi všemi pozitivně predikovanými příklady

$$Precision = \frac{TP}{TP + FP}, \tag{11}$$

- **senzitivita**: podíl predikovaných pozitivních mezi všemi skutečně pozitivními příklady
$$Sensitivity = \frac{TP}{TP + FN}, \tag{12}$$
- **specificita**: podíl predikovaných negativních mezi všemi skutečně pozitivními příklady
$$Specificity = \frac{TN}{FP + TN}. \tag{13}$$

Mezi základní klasifikační algoritmy patří rozhodovací stromy, logistická regrese a metoda podpůrných vektorů.

Rozhodovací stromy

Rozhodovací strom je jednoduchá klasifikační metoda, kterou tvoří graf typu strom. Tento graf se skládá z kořene, vrcholů a listů. Kořen reprezentuje atribut, který nejlépe rozlišuje příklady na pozitivní a negativní. Jak uvádí [31], vrcholy představují testy hodnot atributů a listy představují zařazení objektů do tříd. Klasifikace probíhá testováním atributů příkladů a zařazením do dané kategorie dle výsledků. Výhodou rozhodovacího stromu je jeho přehlednost.

Logistická regrese

Logistická regrese je používána pro binární klasifikaci. Dle [32] se pomocí této metody predikuje pravděpodobnost příslušnosti ke třídě. Princip fungování je obdobný jako u lineární regrese. Lineární regrese aproximuje datové body pomocí přímky, což ale nemusí vystihovat data pro binární klasifikaci. Z tohoto důvodu se v logistické regresi využívá logistická funkce zvaná sigmoid. Klasifikace se poté provádí dle vzorce

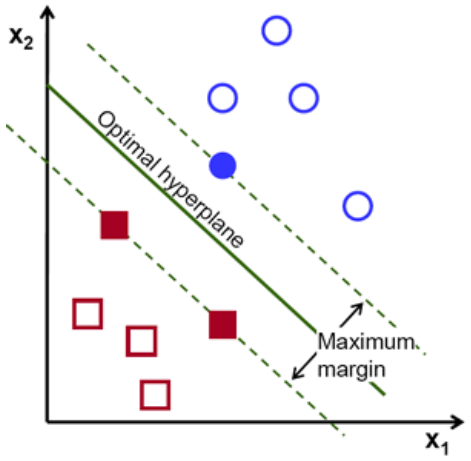
$$p = \frac{1}{1 + e^{-\hat{y}}}, \tag{14}$$

kde $\hat{y}$ je rovnice lineární regrese (7) a p vyjadřuje pravděpodobnost, že příklad je pozitivní.

Metoda podpůrných vektorů

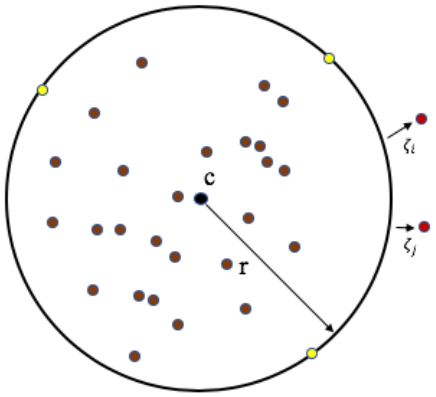
Metoda podpůrných vektorů (anglicky Support Vector Machine, zkráceně SVM) je využívána pro regresní analýzu a binární klasifikaci, z tohoto důvodu je používána také pro detekci anomálií. Jak uvádí [33], cílem metody podpůrných vektorů je nalézt v N-dimenzionálním prostoru takovou nadrovinu, která nejlépe rozdělí data do

dvou opačných poloprostorů. Forma nadroviny záleží na dimenzi prostoru dat, ve 2D prostoru je nadrovinou přímka, ve 3D prostoru je to rovina. Optimální nadrovina je taková, která má na obou stranách co největší pásmo bez datových bodů (anglicky maximal margin). Body ohraničující toto pásmo se nazývají podpůrné vektory a slouží k popisu hledané nadroviny.



Obrázek 6: Metoda podpůrných vektorů. Zdroj: [33]

One-class SVM je upravená metoda SVM určená pro rozlišení jedné konkrétní třídy dat od ostatních. Dle [34] probíhá trénování této metody strojového učení bez učitele pouze na třídě normálních dat. Cílem je z dat určit hypersféru, která bude uvnitř obsahovat data jedné třídy (normální data) a mimo ní budou data ostatních tříd (anomálie). Ve 2D prostoru má hypersféra tvar kružnice, ve 3D prostoru má tvar koule. Stejně jako v případě SVM hypersféru definují podpůrné vektory.



Obrázek 7: One-class SVM. Zdroj: [35]

3.1.5 Zpracování přirozeného jazyka

Hlavním cílem zpracování přirozeného jazyka je porozumění přirozenému jazyku strojem. Pro toto porozumění je vhodné data zpracovat tak, aby bylo možné je následně použít. Toto zpracování dat se provádí několika metodami:

- **Tokenizace** je metoda rozdělení textu do menších částí, nazývaných tokeny. Rozdělení probíhá na jednotlivé věty či slova. Pomocí tohoto rozdělení lze následně určit frekvence výskytu slov či vět. [36]
- **Odstranění stop-slov** je metoda, kterou se z textu odstraňují slova, která nenesou významovou informaci, ale mají pouze syntaktický význam. Pro tento účel jsou vytvořeny slovníky stop-slov. Odstraněním stop-slov se sníží počet slov určených ke zpracování a tím se ušetří strojový čas. [36]
- **Normalizace** je metoda nahrazení různých tvarů slov jednotným tvarem. Normalizaci lze provést dvěma způsoby [37]:
  - **stematizací**, neboli hledáním kořene slov pomocí ořezání částí slov. Problémy této metody mohou být nedostatečné či přílišné ořezání,
  - **lemmatizací**, neboli převodem slov na základní gramatický tvar.
- **Tagování slovních druhů** je důležité pro porozumění významu slov ve větě. Také je důležité pro správnou lemmatizaci slov, například anglické slovo „leaves“ lze lemmatizovat na slovo „leaf“ či „leave“, dle slovního druhu. [37]
- **Vektorizace** je metoda převodu tokenů na numerickou reprezentaci - pole či matici. Základní metodou je metoda „Bag of Words“, která převádí věty na vektory dle výskytu slov ze seznamu všech slov v textu. Vektorizovaný text lze poté dále zpracovat klasifikátorem. [38]

Po předzpracování lze data použít pro získávání informací o entitách (lidech, místech, organizacích), analýzu sentimentu, sumarizaci textu či určování tématu textu.

3.1.6 Asociační analýza

Asociační analýza je metoda určená pro hledání skrytých závislostí dat na jiných datech. Nejčastěji používaným algoritmem je Apriori, představený v roce 1994 [39]. Algoritmus Apriori je využíván například pro analýzu nákupního košíku, která se zabývá hledáním často společně nakupovaných produktů, takzvaných sad položek (anglicky itemset).

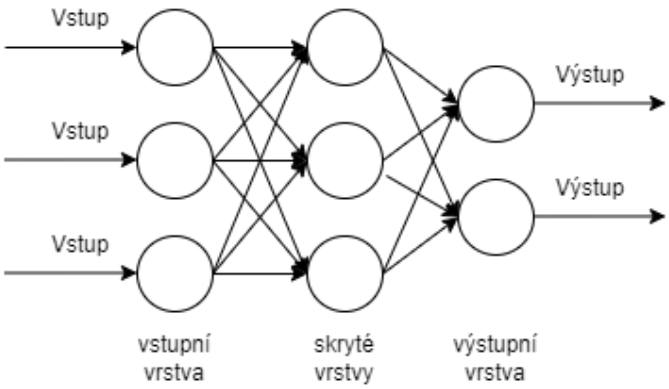
Pro použití algoritmu Apriori, viz [40] je nutné mít záznamy transakcí se zakoupenými produkty. Z těchto dat se pro každý produkt určí podpora (anglicky support), což je parametr udávající počet výskytů jednotlivých produktů v transakcích. Po určení parametru podpory produktů je nutné ručně zvolit hodnotu minimální podpory, pomocí které jsou následně vyfiltrovány položky s nízkým počtem výskytů. Po vyfiltrování položek je určena podpora pro sady dvou položek a následně jsou filtrovány pomocí minimální podpory. Tento proces se opakuje pro sady tří, čtyř, ..., k položek, dokud nejsou nalezeny žádné větší sady položek s podporou větší než minimální. Po určení často nakupovaných sad položek se z těchto určí asociační pravidla ve formátu produkt X $\Rightarrow$ produkt Y, tedy pokud byl zakoupen produkt X, bude zřejmě také zakoupen produkt Y. Pro tato pravidla se určí spolehlivost (anglicky confidence), vyjádřená podílem nákupů obsahující produkty X a Y a nákupů obsahující produkty X. Sady položek lze poté filtrovat pomocí ručně zvoleného parametru minimální spolehlivosti.

3.1.7 Neuronové sítě

Neuronové sítě jsou inspirovány neuronovými sítěmi živých organismů. Základní výpočetní jednotkou neuronové sítě je perceptron. Perceptron je model neuronu, který se skládá z několika vstupů opatřených vahami, aktivační funkce a výstupu. Na základě vstupních dat se síť trénuje - upravuje hodnoty vah jednotlivých vstupů a dle aktivační funkce dochází v neuronu k výpočtu výstupní hodnoty. Neurony jsou v síti propojeny ve vrstvách, výstupy neuronů jedné vrstvy slouží jako vstupy neuronů v další vrstvě. Níže jsou popsány typy neuronových sítí, které se objevily v praktické části.

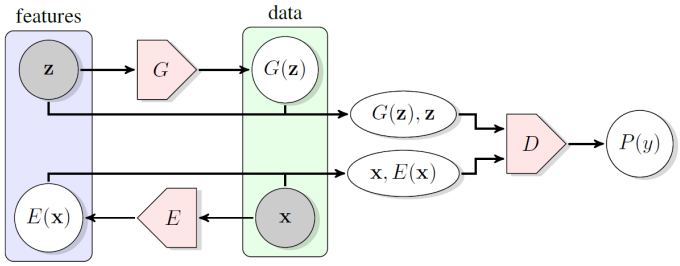
Základní metoda se nazývá Multi Layer Perceptron (zkráceně MLP), což je acyklická síť, která se skládá ze vstupní vrstvy, několika skrytých vrstev a výstupní vrstvy. V této síti jsou uzly z každé vrstvy propojeny se všemi uzly v následující vrstvě.

Druhým typem neuronové sítě používaným v praktické části je Bidirectional Generative Adversarial Network (zkráceně BiGAN). Jak uvádí [41], GAN je architektura neuronové sítě skládající se ze dvou modelů - generátoru a diskriminátoru. Úlohou generátoru je naučit se vlastnosti poskytnutých vstupních dat a na základě získaných znalostí vytvářet data nová, s podobnými vlastnostmi jako vstupní data. Úlohou diskriminátoru je naučit se na základě původních vstupních dat a dat vygenerovaných generátorem mezi nimi rozlišovat. Učení GAN probíhá jako soutěž mezi generátorem a diskriminátorem, kdy generátor se snaží generovat více věrohodná data, zatímco diskriminátor se snaží lépe rozlišovat mezi reálnými a generovanými daty. BiGAN



Obrázek 8: Architektura MLP. Zdroj: vlastní zpracování

je dle [42] rozšíření základní GAN o enkodér, který je v podstatě inverzí generátoru - snaží se mapovat data na vlastnosti. Diskriminátor tak pracuje nejen s daty z generátoru, ale také s daty z enkodéru.



Obrázek 9: Architektura BiGAN. Zdroj: [42]

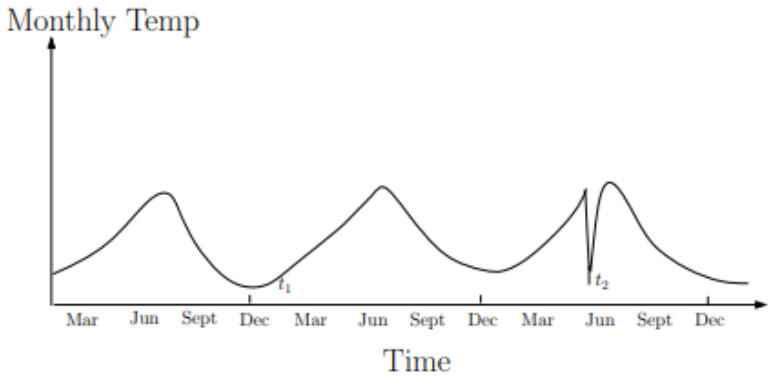
Třetí využívanou neuronovou sítí je autoenkodér. Jak uvádí [43], autoenkodér je síť, která se učí bez učitele. Skládá se ze dvou částí: enkodéru a dekodéru. Úlohou enkodéru je naučit se redukovat vstupní data a zakódovat je do komprimované formy. Úlohou dekodéru je z těchto zakódovaných dat rekonstruovat data do původní podoby s minimální ztrátou. Efektivita sítě je měřena pomocí rekonstrukční ztráty.

4 Detekce anomálií

Detekce anomálií označuje proces objevování neobvyklých jevů či událostí v datech. Tyto neobvyklé jevy se nazývají anomálie či odlehlé hodnoty. Anomálie představují jednotlivá data či vzory, které se odlišují od dat, která jsou považována za normální. Příčiny vzniku anomálií mohou být nahodilé, například chyby při přenosu dat či poškození senzorů, ale důvodem vzniku anomálií může být také podvodná činnost například v bankovnictví a v zabezpečovacích systémech či výskyt nemoci v lékařských záznamech zdravotního stavu pacienta.

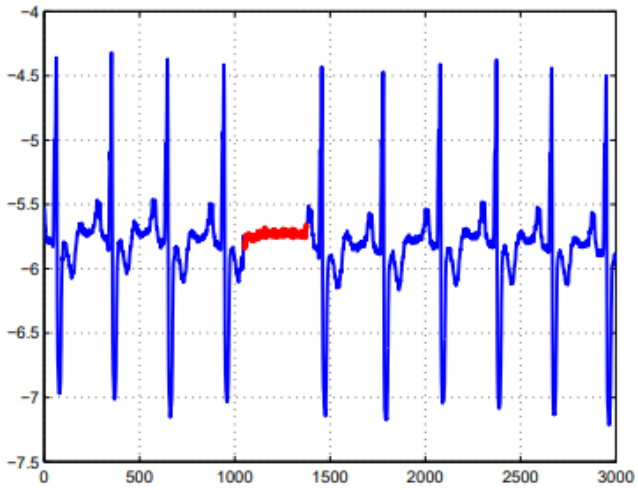
Anomálie lze dle [44] rozdělit na tři druhy:

- **Bodové** anomálie jsou taková jednotlivá data, která se výrazně odlišují od ostatních. Příkladem bodové anomálie je velmi vysoká platba na bankovním účtu, kde jsou běžně prováděny výrazně nižší transakce.
- **Kontextové** anomálie jsou data, která se v datovém souboru mohou běžně vyskytovat, ale jejich odlišnost vychází z kontextu, nejčastěji časového či prostorového. Příkladem budiž sledovaná teplota v časovém průběhu na obrázku 10. Teploty t_1 a t_2 jsou stejné, avšak v časovém kontextu je teplota t_2 anomálií, neboť je v daném měsíci neobvyklá.



Obrázek 10: Kontextová anomálie teploty v čase. Zdroj: [21]

- **Kolektivní** anomálie se skládají ze skupiny hodnot. Tyto hodnoty samostatně anomáliemi nejsou, ale při zkoumání celé skupiny mezi jednotlivými prvky vyvstane neočekávaný vztah. Na obrázku 11 je vidět elektrokardiogram nepravidelné srdeční aktivity. Jednotlivé hodnoty by anomálii nepředstavovaly, ale jako sekvence hodnot již anomálii představují.



Obrázek 11: Kolektivní anomálie v elektrokardiogramu. Zdroj: [21]

Detekci anomálií lze na základě dostupnosti trénovacích dat rozdělit dle [21] do tří kategorií:

- **Detekce anomálií s učitelem:** tento způsob lze použít, pokud jsou k dispozici data označená jako normální a anomálie. Za pomoci označených dat je možné sestavit klasifikační model, který následně o nových datech rozhoduje, zda jsou normální či nikoli. Tento přístup má ale své problémy. Pro správné naučení klasifikačního modelu je nutné mít dostatečný počet označených normálních dat a anomálií. Anomálie se na rozdíl od běžných dat vyskytují vzácně, z tohoto důvodu jsou často v souboru dat určených k učení zastoupeny výrazně méně. Dalším problémem je také rozmanitost anomálií, které se mohou vyskytnout.
- **Detekce anomálií pomocí kombinace s učitelem a bez učitele:** na rozdíl od detekce anomálií s učitelem jsou pro sestavení modelu k dispozici pouze označená normální data. Výhodou tohoto způsobu detekce je vyšší přizpůsobitelnost neznámým anomáliím.
- **Detekce anomálií bez učitele:** tento způsob nevyžaduje označená trénovací data, je tak univerzálně použitelný. Základním předpokladem je, že většina dat je normálních. Na základě tohoto předpokladu jsou data, která se výrazně liší od ostatních dat označena jako anomálie. Pro detekci se používají různé metody, například statistické či shlukovací.

Výsledkem detekce anomálií je rozhodnutí o tom, zda zkoumaná data jsou či nejsou anomálií. Zkoumaná data mohou být jednoduše označena jako normální či anomálie,

nebo mohou být ohodnocena pomocí skóre. Skóre značí míru odlehlosti od normálních dat. Ohodnocení dat pomocí skóre přináší možnost anomálie řadit, spolu s tím je ale nutné určit prahovou hodnotu odlehlosti, která rozděluje anomálie od normálních dat.

Pro detekci anomálií lze, jak uvádí [21] využít různé algoritmy založené na klasifikaci, například metodu podpůrných vektorů, kterou lze nalézt hranici mezi normálními daty a anomáliemi a poté tuto hranici použít pro klasifikaci nových dat. Také lze použít algoritmy založené na měření vzdálenosti mezi prvky či hustoty jejich okolí, jako je například metoda Local Outlier Factor, která využívá předpokladu, že anomálie jsou vzdáleny ostatním prvkům a tedy jejich okolí má nízkou hustotu prvků. Dále lze použít shlukovou analýzu, při které se předpokládá, že normální data patří do shluku a anomálie ne. Anomálie lze také detekovat pomocí statistických metod, například pro jednorozměrná data porovnáním Z-skóre prvků s předem určenou prahovou hodnotou. Další využívanou statistickou metodou je sekvenční testování hypotéz.

Sekvenční testování hypotéz, jak uvádí [45] je metoda statistické analýzy, která nemá předem definovanou velikost vzorku. Data jsou analyzována postupně v krocích a pokračování či zastavení analýzy záleží na výsledcích předchozích kroků. Cílem sekvenčního testování hypotéz je rozhodnout, zda zkoumaná množina hodnot $\{x_1, x_2, \ldots, x_i\}$ patří do jedné ze dvou tříd - v případě detekce anomálií do tříd normální data nebo anomálie. V každém kroku i se na základě hodnot $x_1, \ldots, x_i$ pomocí rozhodovací funkce rozhoduje o zařazení do třídy. Pokud nelze rozhodnout, pokračuje se v rozhodování na hodnotě x_{i+1}.

Metoda CUSUM je technika používaná pro sekvenční testování hypotéz. Je založena na kumulativním součtu hodnot S_i. Jednotlivé hodnoty x_i mají přiřazeny váhu ω. Výpočet kumulovaných hodnot probíhá dle [46]

$$\begin{aligned} S_{H0} = S_{L0} = 0, \\ S_{Hi+1} = \max(0, S_{Hi} + x_{i+1} - \omega), \\ S_{Li+1} = \min(0, S_{Li} + x_{i+1} - \omega). \end{aligned} \tag{15}$$

Hodnota S_H značí odchýlení hodnot v kladném směru, hodnota S_L odchýlení v záporném směru. Překročením stanovených hranic dojde k detekci anomálie.

Zvláštní metodou je algoritmus Isolation Forest, která nepracuje se vzdáleností či hustotou okolí prvků, není třeba ji trénovat pro další použití a díky lineární složitosti je dobře škálovatelná i pro velké množství dat. Algoritmus Isolation Forest je založen

na předpokladu, že anomálie se vyskytují v malém počtu a mají výrazně odlišné hodnoty od normálních dat. Jak uvádí [47], algoritmus funguje na principu vytváření binárních rozhodovacích stromů. Z dat se vybere náhodně atribut a hraniční hodnota, dle které se data rozdělí do binárního stromu. Tímto způsobem se vytvoří zvolený počet stromů, které dohromady tvoří les. Rozdělení dat na normální a anomálie poté probíhá tak, že u každého prvku se zkoumá délka cesty každým stromem. Délka cesty stromem je definována počtem uzlů, kterými je nutné projít, než je dosaženo listu, ve kterém je prvek zařazen. Čím kratší je délka cesty prvku, tím odlišnější je hodnota atributu daného prvku od ostatních. Pokud má více atributů prvku krátké délky cest, pravděpodobně se jedná o anomálii.

5 Teorie her

Teorii her je možné dle [48] definovat jako vědní disciplínu, která se zabývá studiem konfliktních rozhodovacích situací. Konfliktní rozhodovací situace je taková situace, ve které se střetávají zájmy několika subjektů, které se musí nějakým způsobem o něčem rozhodnout. Konfliktní situace jsou reprezentovány matematickými modely, které jsou používány pro hledání optimálních strategií. Teorie her tedy patří mezi vědní obory aplikované matematiky.

Jedním z prvních příspěvků do teorie her byl ekonomický model duopolu, tedy model zabývající se stanovením rozsahu výroby při konkurenci dvou firem z roku 1838, jehož autorem byl francouzský matematik Augustin Cournot [49]. V roce 1928 napsal John von Neumann článek [50], ve kterém formuloval hru jako matematický problém a dokázal větu o minimaxu. Následně v roce 1944 spolu s Oskarem Morgensternem napsal knihu „Theory of Games and Economic Behavior“ (česky Teorie her a ekonomického chování) [51], která ustanovila vědní disciplínu teorie her.

Teorie her má mnoho využití. Jedním z nejstarších příkladů využití je v oboru salonních her, kde se využívá pro jejich rozbory. Autoři [52] uvádí využití v logistice pro určení tras či v informatice v oblasti počítačových sítí, sdílení souborů nebo zabezpečení. Velké využití má také v oboru ekonomie, kde se využívá pro zkoumání chování firem či aukcí. V politologii se využívá pro analýzy hlasování a vyjednávání, viz [48].

5.1 Základní pojmy

Hra modeluje konfliktní situace z reálného života, ve které se hráči nějak musí rozhodovat. Pro modelování konfliktní situace je dle [53] nutné:

1. definovat konflikt, který chceme modelovat,
2. vymezit pojmy hra, hráč, strategie a výplata,
3. sestavit optimalizační úlohu, kterou chceme vyřešit,
4. najít matematický nástroj, kterým se pokusíme co nejpřesněji danou optimalizační úlohu vyřešit,
5. interpretovat výsledek a posoudit, zda výsledek daný konflikt řeší.

Hra se tedy skládá z hráčů, kteří si vybírají svou strategii z prostoru možných strategií. Tuto strategii si vybírají na základě hodnot výplatní funkce. Strategie s nejvyšší hodnotou výplatní funkce se nazývá optimální strategie. [48]

5.1.1 Hráč

Hráči jsou účastníci konfliktní rozhodovací situace. Hráči se dle [53] dělí na:

- **Inteligentní**, neboli takové, kteří analyzují situaci a vybírají takovou strategii, která jim maximalizuje hodnotu výplatní funkce. Takové chování se dle [48] nazývá racionální.
- **P-inteligentní**, neboli takové hráče, kteří se s pravděpodobností p chovají inteligentně a s pravděpodobnostní $1 - p$ se chovají neinteligentně.
- **Neinteligentní** hráči se chovají náhodně, nezávisle na výplatní funkci. Pokud je ve hře více neinteligentních hráčů, je možné je pro zjednodušení nahradit jedním hráčem.

5.1.2 Hra

Hra se skládá z alespoň dvou hráčů, kteří si vybírají svou strategii z prostoru možných strategií. Tuto strategii si vybírají na základě hodnot výplatní funkce. Strategie s nejvyšší hodnotou výplatní funkce se nazývá optimální strategie. Každá hra má svá pravidla, která všichni hráči znají a musí se jimi řídit. [48]

Hru N hráčů v normálním tvaru lze dle [53] popsat pomocí tří množin:

- Množinou hráčů $H = \{1, 2, \ldots, N\}$,
- množinou prostorů strategií $X = \{X_1, X_2, \ldots, X_N\}$, kde X_i reprezentuje prostor možných strategií hráče $i,\ i\ \in H$,
- množinou $M = \{M_1, M_2, \ldots, M_N\}$, kde M_i reprezentuje výplatní funkci hráče $i,\ i\ \in H$. Hodnota výplatní funkce je výplata hráče.

Formálně lze tuto hru zapsat jako uspořádanou (2N+1)-tici

$$G = \{H, X, M\}. \tag{16}$$

5.1.3 Užitek

Cílem inteligentního hráče je vybrat takovou strategii, která maximalizuje hodnotu výplatní funkce. Tato hodnota reprezentuje užitek, který hráč z řešení hry má. Dle [48] se užitkem zabývá ekonomická teorie užitku. Užitek je dle této teorie stupeň uspokojení ze spotřeby určitého statku či služby. Užitek je velmi subjektivní pojem, neboť jedna osoba může mít ze spotřeby statku či služby vyšší stupeň uspokojení než někdo jiný.

Určit míru užitku může být obtížné. Jak uvádí [48], v případě firem je užitek jednoduché vyjádřit peněžními prostředky. Užitek, který je možné vyčíslit a porovnávat v nějakých jednotkách se nazývá kardinální. Dle [53] je však často užitek těžko měřitelný. Příkladem může být dobrý pocit z vykonané činnosti. Takový pocit lze těžko vyčíslit, je ale možné jej porovnávat. V některých případech je složité určit, zda je užitek kladný či záporný, například při výhře nad mladším sourozencem. Užitek, který nelze vyčíslit, ale lze porovnat, se nazývá ordinální.

5.1.4 Klasifikace her

Hry lze klasifikovat mnoha způsoby, například [53] uvádí tyto pohledy:

- **Kooperativní, nekooperativní**: takové hry, ve kterých hráči mohou či nemohou uzavírat dohody.
- **Jednokolové, vícekolové**: v jednokolové hře hráči odehrají pouze jednu hru, nemusí tedy brát v potaz následky jejich volby strategie na další kola. Ve vícekolové hře hráči využívají zkušeností z předchozích kol a berou v potaz následky jejich vybrané strategie na další kola. Zvláštním typem vícekolové hry je evoluční hra, ve které hráči kopírují strategie úspěšnějších hráčů.
- **Symetrické, asymetrické**: symetrické hry se vyznačují stejnou množinou strategií, ze kterých mohou všichni hráči vybírat, popřípadě mají také všichni hráči stejné výplatní funkce. V asymetrických hrách tyto předpoklady neplatí.
- **Hry s nulovým, nenulovým součtem**: hry s nulovým součtem jsou takové, ve kterých platí, že součet výplat všech hráčů se rovná nule či jakékoli předem dané konstantě (lze nazývat také jako hry s konstatním součtem). Pro hry s nenulovým součtem nelze výsledný součet výplat předem určit.
- **Hry s úplnou (dokonalou)/částečnou informací**: takové hry, ve kterých hráči mohou nebo nemohou znát všechny možné průběhy hry. Hry s částečnou informací jsou takové, ve kterých hráč nezná nějaké informace, například množinu strategií protihráče.
- **Nekonečné hry**: teoretický koncept pro zkoumání chování modelů v extrémních podmínkách.
- **Konečné, diskrétní, spojité hry**: takové hry, ve kterých je množina strategií hráčů konečná, spočetná či nespočetná.

- **Simultánní, metahry (sekvenční)**: v simultánních hrách všichni hráči volí svou strategii současně, neznají tedy zvolenou strategii ostatních hráčů. V metahrách hrají hráči postupně, mohou tedy znát strategie předešlých hráčů.

5.2 Reprezentace her

Pro hledání teoretického řešení je nutné hry nějakým způsobem reprezentovat. Obvyklými způsoby jsou reprezentace hry v normálním a v rozvinutém tvaru, kterými se bude tato podkapitola zabývat.

5.2.1 Hra v normálním tvaru

Hra v normálním tvaru, někdy také nazývána ve strategickém tvaru, je způsob zápisu her používaný pro simultánní hry, ve kterých si všichni hráči volí strategii současně. Tato forma zápisu hry spočívá v definování matice výplat. Jak uvádí [48], v případě hry dvou hráčů s konečným prostorem strategií si první hráč vybírá z m možných strategií a druhý hráč z n možných strategií, ke kterým lze přiřadit výplatní funkce. Matice výplat má tedy tvar $m \times n$ a skládá se z hodnot výplatních funkcí možných strategií. Formálně lze zapsat jako $A = (a_{ij}),\ i\ = 1, 2, \ldots, m;\ j = 1, 2, \ldots, n$. První hráč vybírá svou strategii určením i-tého řádku, druhý hráč určením j-tého sloupce. Hodnota výplatní funkce poté odpovídá prvku a_{ij} matice výplat A každého hráče.

$$A\ = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix} \tag{17}$$

V případě hry s velkým množstvím hráčů či strategií je problém takovou hru popsat v normálním tvaru. Například dle [52] je ve hře n hráčů, kdy každý má dvě strategie, nutné definovat 2^n strategií a jejich výplatních funkcí.

5.2.2 Hra v rozvinutém tvaru

Hra v rozvinutém (extenzivním, rozšířeném) tvaru, jak uvádí [48], je způsob zápisu používaný pro tahové hry, ve kterých se hráči střídají při volbě strategií. Rozdíl oproti hrám v normálním tvaru je možnost přizpůsobení volby strategie hráče na základě předchozích tahů ostatních hráčů. Dle míry znalosti předchozích tahů protihráčů se

hry v rozvinutém tvaru dělí na hry s dokonalou informací a na hry s nedokonalou informací. Hrou s dokonalou informací je například hra šachy, neboť všichni hráči znají svou pozici na hrací ploše a všechny tahy, které tomuto stavu předcházely. Naopak karetní hry jsou příkladem her s nedokonalou informací, neboť hráči neznají karty ostatních hráčů.

Hru v rozvinutém tvaru je možné znázornit pomocí grafu, konkrétně orientovaného stromu, který obsahuje možné strategie a výplaty. Orientovaný strom se skládá z kořene, uzlů a hran. Kořen reprezentuje počátek hry. Uzly mohou být rozhodovací nebo konečné. V rozhodovacích uzlech se hráč rozhoduje, kterou strategii zvolí, možné strategie jsou znázorněny pomocí hran vycházejících z uzlu. Z konečných uzlů (listů) již žádné hrany nevycházejí, když je jich dosaženo, hra končí a hráči dostanou své výplaty, viz [52]

5.3 Řešení her v normálním tvaru

Ve hrách v normálním tvaru lze hledat řešení několika způsoby. Pokud je to možné, lze je hledat pomocí dominovanosti. Pokud hru nelze takto řešit, je nutné v ní hledat řešení pomocí Nashovy rovnováhy v ryzích či smíšených strategiích.

5.3.1 Dominovanost

Jedním ze základních způsobů je řešení pomocí dominantní strategie. Dle [52] si při tomto způsobu řešení hráč vybírá takovou strategii, která mu přinese nejvyšší užitek. Při výběru své strategie nebere ohled na strategii, kterou si vybere protihráč. Her, které by splňovalo podmínku jedné dominantní strategie pro každého hráče ale není mnoho.

V některých hrách s nulovým součtem je možné matici výplat při hledání řešení zjednodušit či ve výjimečných případech najít řešení, jak uvádí [48]. První hráč nebude vybírat takovou strategii, která mu přinese méně užitku než ostatní strategie, stejně tak druhý hráč nebude volit strategii, která mu přinese vyšší ztrátu než ostatní. Tyto strategie se nazývají silně dominované a je možné je z výběru strategií odebrat. Dále také existují slabě dominované strategie, to jsou takové strategie, které přinesou prvnímu hráči stejný nebo menší užitek, analogicky druhému hráči přinesou stejnou či větší ztrátu. Tyto strategie nelze jednoduše odebrat, neboť bychom mohli přijít o možné řešení.

5.3.2 Nashova rovnováha

Pro nalezení optimálního řešení konečné hry v normálním tvaru se používá Nashova rovnováha. Dle [48] lze Nashovu rovnováhu popsat jako takové řešení, při kterém platí, že pokud se některý z hráčů samostatně nebude držet své optimální strategie, tak jeho výhra zůstane stejná nebo bude nižší. Je to tedy kombinace optimálních strategií všech hráčů.

Nashova rovnováha ve hře s konstantním součtem

Hra s konstantním součtem představuje antagonistický konflikt - co jeden hráč získá, to druhý ztratí. Jak uvádí [48], Nashova rovnováha ve hře dvou hráčů s konstantním součtem nastane v případě, že nalezneme strategie $x^O \in X$ a $y^O \in Y$ pro které platí:

$$f_1(x, y^O) \leq f_1(x^O, y^O) \text{ a } f_2(x^O, y) \leq f_2(x^O, y^O). \tag{18}$$

Jednoduchou úpravou lze toto upravit na hru s nulovým součtem, kdy označíme $f_1(x, y) = f(x, y)$ a $f_2(x, y) = -f(x, y)$. Poté lze Nashovu rovnováhu definovat jako

$$f(x, y^O) \leq f(x^O, y^O) \leq f(x^O, y). \tag{19}$$

Tyto optimální strategie se nazývají rovnovážné strategie.

Nashovu rovnováhu v ryzích strategiích je možné určit pomocí nalezení sedlového bodu matice A. Sedlový bod je takový prvek a_{ij} matice A, pro který platí

$$\max_i \min_j a_{ij} = \min_j \max_i a_{ij}, \tag{20}$$

neboli platí, že je to největší prvek ve svém řádku a zároveň nejmenší prvek ve svém sloupci. Tento princip se také nazývá minimax, který je popisován jako pesimistický pohled na svět. Hráč předpokládá, že jeho soupeř vybere pro něj nejhorší variantu. Z tohoto důvodu se snaží maximalizovat svou minimální výplatu: z řádkových strategií vybere minima a z těchto vybere maximum. Druhý hráč se analogicky snaží minimalizovat ztrátu, tedy ze sloupcových strategií vybere maxima a z těchto vybere minimum. Hodnota výplatní funkce v sedlovém bodě se nazývá cena hry. Ve hrách s konstantním součtem mohou nastat tři situace:

- hra má právě jedno Nashovo rovnovážné řešení,
- hra má více alternativních Nashových rovnovážných řešení,
- hra nemá Nashovo rovnovážné řešení v ryzích strategiích.

Pokud konečná hra nemá Nashovo rovnovážné řešení v ryzích strategiích, platí, že má řešení ve smíšených strategiích. Smíšené strategie vyjadřují pravděpodobnosti, že je hráč zvolí. [48]

Tyto tři situace jsou předvedeny v následujícím příkladu, převzatém z [48]:

Příklad 1. Mějme tři hry dané maticemi výplat A, B, C. Kulatými závorkami označme řádková minima, hranatými závorkami sloupcová maxima.

$$A = \begin{pmatrix} (1) & [4] & 3 \\ (2) & [4] & [5] \\ [3] & (0) & 2 \end{pmatrix}, B = \begin{pmatrix} 1 & (0) & 4 \\ [6] & [(3)] & 4 \\ 5 & (1) & [6] \end{pmatrix}, C = \begin{pmatrix} [3] & [(2)] & [(2)] \\ [3] & (1) & (1) \\ 2 & 0 & (-1) \end{pmatrix}$$

Jak je vidět, matice A nemá žádné Nashovo rovnovážné řešení v ryzích strategiích, matice B má právě jedno rovnovážné řešení a matice C má dvě rovnovážná řešení.

Nashova rovnováha ve hře s nekonstantním součtem

Hra s nekonstantním součtem představuje neantagonistický konflikt - zájmy hráčů nejsou v protikladu, výhra jednoho hráče není prohrou druhého. Stále platí, že při odchýlení od optimální strategie si hráč nemůže polepšit. Při tomto typu konfliktu může být hra kooperativní (hráči mohou spolupracovat) nebo nekooperativní (hráči spolupracovat nemohou). Protože mezi hodnotami výplatních funkcí hráčů není vztah, je nutné hru reprezentovat dvěma maticemi A, B či zjednodušeně dvojmaticí. Taková hra se také nazývá dvojmaticová či bimaticová.

V nekooperativní hře s nekonstantním součtem hráči nemohou spolupracovat. Jak uvádí [48], u tohoto typu her je možné hledat Nashovo rovnovážné řešení podobně jako při antagonistickém konfliktu. Rovnovážné strategie x^O, y^O jsou takové, pro které platí:

$$f_1(x, y^O) \leq f_1(x^O, y^O) \text{ a } f_2(x^O, y) \leq f_2(x^O, y^O) \tag{21}$$

pro $\forall x \in X,\ \forall y \in Y$. Nashovo rovnovážné řešení v ryzích strategiích je možné, stejně jako tomu bylo u her s konstatním součtem, hledat pomocí sedlového bodu. Hledání sedlového bodu probíhá tak, že první hráč si ve své matici A označí sloupcová maxima a druhý hráč si ve své matici B označí řádková maxima. Sedlový bod se poté nachází v průsečíku těchto označených maxim. V nekooperativních hrách s nekonstantním součtem mohou nastat čtyři situace:

- hra má právě jedno Nashovo rovnovážné řešení,

- hra má více rovnovážných řešení a právě jedno řešení je výhodnější pro oba hráče (dominuje ostatním řešením),
- hra má více rovnovážných řešení a alespoň dvě řešení jsou nejvýhodnější pro oba hráče (nejsou dominovaná) - hráči neví, které řešení zvolit,
- hra nemá Nashovo rovnovážné řešení v ryzích strategiích.

Na následujících příkladech budou popsány některé z možných situací.

Příklad 2. Jednou z nejznámějších her s jedním Nashovým rovnovážným řešením v ryzích strategiích je hra zvaná vězňovo dilema. V této hře jsou dva zločinci vyslýcháni policií. Oba mohou buď nevypovídat (označme N) nebo zradit druhého (označme Z). Pokud jeden druhého zradí, zrádce bude volný a druhý bude odsouzen na tři roky ve vězení. Pokud oba zradí, oba budou odsouzeni na dva roky. V případě, že ani jeden nebude vypovídat, budou oba odsouzeni na jeden rok. Tresty lze zobrazit jako dvojmatici, maxima prvního hráče označíme kulatými závorkami, maxima druhého hráče hranatými závorkami:

$$\begin{array}{c} \\ N \\ Z \end{array} \begin{array}{c} \begin{array}{cc} N & Z \end{array} \\ \begin{pmatrix} -1;-1 & -3;[0] \\ (0);-3 & (-2);[-2] \end{pmatrix} \end{array}$$

Oba hráči přemýšlejí takto: pokud nebude protihráč vypovídat, vyplatí se zradit - lepší být na svobodě, než rok ve vězení. Pokud protihráč zradí, vyplatí se také zradit - lepší být ve vězení dva roky než tři. Jak je z označení maxim patrné, vězňovo dilema má jedno Nashovo rovnovážné řešení - oba by měli zradit, přesto že by pro oba bylo lepší spolupracovat.

Příklad 3. Pro ilustraci situace, ve které nastanou dvě Nashova rovnovážná řešení, která si navzájem nedominují je vhodná hra nazvaná manželský spor (často také jako souboj pohlaví). Dva hráči, ona a on, se rozhodují nad večerním programem. Ona by ráda šla do divadla, on by rád šel na fotbalový zápas. Pokud by jeden z hráčů šel tam, kam chce druhý, bude z toho mít menší užitek oproti preferované aktivitě. Pokud oba zvolí rozdílnou možnost, večer si neužijí a budou mít užitek nulový. Toto lze popsat následující dvojmaticí:

$$\begin{array}{c} \\ D \\ F \end{array} \begin{array}{c} \begin{array}{cc} D & F \end{array} \\ \begin{pmatrix} (1);[2] & 0;0 \\ 0;0 & (2);[1] \end{pmatrix} \end{array}$$

Z dvojmatice je patrné, že hra má dvě rovnovážná řešení, která si ale nedominují a nelze tak hru vyřešit v čistých strategiích.

5.3.3 Hledání řešení ve smíšených strategiích

Ne vždy se podaří ve hrách najít sedlový bod. V případě, že hra nemá rovnovážné řešení v ryzích strategiích, je nutné jej hledat ve smíšených strategiích. Platí, že každá konečná hra má vždy alespoň jedno Nashovo rovnovážné řešení ve smíšených strategiích. Smíšené strategie reprezentují pravděpodobnosti, se kterými by měl hráč tu kterou strategii zahrát. Hledání řešení je nejlépe představit na příkladu, popsaném dle [54]:

Příklad 4. Jak bylo v předchozím příkladu ukázáno, hra manželský spor nemá řešení v ryzích strategiích. Řešení lze tedy nalézt ve smíšených strategiích. Toto řešení reprezentuje pravděpodobnosti $(p, 1-p)$, se kterými by měl první hráč volit první či druhou strategii, totéž platí pro druhého hráče s pravděpodobnostmi $(q, 1-q)$.

$$\begin{array}{ccc} & D & F \\ D & (1);[2] & 0;0 \\ F & 0;0 & (2);[1] \\ & q & 1-q \end{array} \begin{array}{c} \\ p \\ 1-p \end{array}$$

Řešení ve smíšených strategiích je možné získat výpočtem rovnic, které se skládají z užitků hráče v případě, že čelí jedné či druhé strategii:

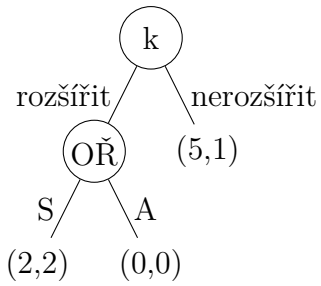
$$\begin{aligned} 1 \cdot p + 0 \cdot (1-p) &= 0 \cdot p + 2 \cdot (1-p) \\ 2 \cdot q + 0 \cdot (1-q) &= 0 \cdot q + 1 \cdot (1-q). \end{aligned}$$

Řešením rovnic dojdeme k výsledku $p = \frac{2}{3}$, $q = \frac{1}{3}$, řešení je tedy $\left(\left(\frac{2}{3}, \frac{1}{3}\right), \left(\frac{1}{3}, \frac{2}{3}\right)\right)$.

5.4 Řešení her v rozvinutém tvaru

Řešení her v rozvinutém tvaru je hledáno metodou zpětné indukce. Jak uvádí [52], princip této metody spočívá v rozložení hry na podhry. Podhra je část hry, která má jako kořen zvolený uzel a obsahuje všechny následující strategie. Řešení hry je tak hledáno postupným řešením podher - nejdříve určíme optimální strategii v poslední podhře, poté určíme optimální strategii v podhře, která předchází poslední podhře a tak dále až ke kořenu původní hry.

Příklad 5. Příkladem reprezentace a řešení hry je například hra obchodního řetězce [55]. Obchodní řetězec (OŘ) má v K městech pobočku. V každém městě k je také konkurenční hráč k, který se může rozhodnout, zda se rozšíří či nikoli. Pokud se hráč k rozhodne nerozšířit, jeho výplata bude 1 a výplata OŘ bude 5. Pokud se rozhodne rozšířit, bude si muset řetězec zvolit cenovou strategii - buď spolu budou spolupracovat (S), což každému přinese výplatu 2, nebo zvolí agresivní strategii (A) a výplata obou hráčů bude nulová. Řešení této hry metodou zpětné indukce je takové, že OŘ bude vždy raději spolupracovat než volit agresivní cenovou politiku a konkurenční hráč se vždy rozhodne rozšířit.



Obrázek 12: Strom hry obchodního řetězce. Zdroj: vlastní zpracování

5.5 Další typy her

V této podkapitole jsou popsány typy her, které se vyskytují ve zkoumané literatuře v rámci systematické rešerše v praktické části této diplomové práce.

Stackelbergova hra

Jak uvádí [56], Stackelbergův model je asymetrická hra, ve které jsou dva druhy hráčů - hráč v postavení vůdce a ostatní hráči v postavení následníka. Řešení Stackelbergovy hry se nazývá Stackelbergova rovnováha. Vedoucí hráč si jako první zvolí svou optimální strategii a následně si ostatní hráči dle vybrané strategie vedoucího hráče vyberou své optimální strategie. Řešení může být buď silná nebo slabá Stackelbergova rovnováha. V případě silné Stackelbergovy rovnováhy si hráči v roli následníka zvolí takovou strategii, která se jeví jako optimální i z pohledu hráče v roli vůdce. Při slabé rovnováze si hráč v roli následníka zvolí takovou strategii, která je z pohledu hráče v roli vůdce nejhorší možná. Existuje také Bayesovská Stackelbergova hra, ve které mohou mít hráči v roli následníka různý typ a tedy i různé sady strategií.

Shapleyho hodnota

Shapleyho hodnota je způsob řešení spravedlivého rozdělení hodnoty výplatní funkce v kooperativní hře. Rozdělení probíhá mezi členy koalice dle jejich podílu na výsledku hry. Dle [52] lze Shapleyho hodnotu definovat jako mezní hodnotu výplatní funkce každého hráče. Jedním ze způsobů přiřazení hodnoty výplatní funkce je přírůstkové sdílení nákladů. Tato metoda spočívá v seřazení hráčů a, například $a_1, a_2, \ldots, a_n$ a postupném přiřazování hodnot $c(\{a_i\})$ - tedy hráč a_1 dostane hodnotu $c(\{a_1\})$, hráč a_2 dostane $c(\{a_1, a_2\}) - c(\{a_1\})$ a tak dále. Nevýhodou této metody je závislost pořadí hráčů na hodnotě výplatní funkce. Shapleyho hodnota řeší tento problém výběrem náhodného seřazení hráčů ze všech možných kombinací a přiřazení očekávané hodnoty výplatní funkce v tomto vybraném seřazení.

6 Systematická rešerše

Praktická část této diplomové práce se věnuje provedení systematické rešerše tématu využití teorie her v oblasti detekce anomálií. Tato oblast se jeví jako velmi vhodná pro využití teorie her, neboť se zabývá konfliktní situací hledání a rozhodování o normalitě nalezených nestandardních hodnot. Literární rešerše má za cíl pomocí průzkumu existující literatury k vybrané oblasti zájmu vytvořit shrnutí zjištěných poznatků. Cílem této rešerše je nalézt oblasti, ve kterých je detekce anomálií využívána spolu s teorií her, aktuálně používané metody detekce anomálií, typy her a zjistit, zda využití teorie her přineslo zlepšení fungování detekce anomálií.

6.1 Metodika PRISMA

Metodika PRISMA (zkratka anglického názvu Preferred Reporting Items for Systematic Reviews and Meta-Analyses) vznikla jako reakce na nepříliš vysokou kvalitu systematických přehledů. Systematické přehledy se využívají hlavně ve zdravotnictví, kde je zdravotníci využívají pro získání a udržování přehledu o aktuálním vývoji zvoleného oboru. Také se používají jako podklady pro zavádění doporučených postupů či pro podporu dalšího výzkumu. V roce 1987 a následně v roce 1996 [57] byla provedena analýza kvality 50 článků v lékařských časopisech dle stanovených kritérií. Žádný z vybraných článků nesplnil všechna kritéria. V návaznosti na toto zjištění vznikla metodika QUOROM (zkratka anglického názvu QUality Of Reporting Of Meta-analyses), ze které v roce 2009 vznikla metodika PRISMA.

Tato metodika byla vypracována tak, aby poskytla autorům systematických přehledů vedení při tvorbě jejich prací. Práce vytvořené na základě doporučení této metodiky by měly transparentně a detailně uvádět důvody vzniku, výzkumné otázky, použité metody pro vytvoření přehledu a výsledky. Díky tomuto přístupu je následně možné reprodukovat výsledky zpracovaného přehledu a tím ověřit jeho důvěryhodnost a přesnost. Díky obecnosti zpracování se tato metodika rozšířila i mimo medicínu do ostatních oborů. Postupem času se tato metodika vyvíjela, aktuální verze se nazývá PRISMA 2020. [58]

Metodika PRISMA se skládá ze několika částí:

- kontrolní seznam pro práci,
- zásady pro vypracování práce,
- vývojový diagram pro zachycení průběhu získávání dat.

Kontrolní seznam je velmi užitečná pomůcka při tvorbě přehledu. Je doporučeno jej používat od započetí práce a postupně zaznamenávat splnění jednotlivých bodů spolu s referencí na místo v práci, kde ke splnění došlo. Tento seznam obsahuje celkem 27 bodů rozdělených do sedmi částí. Jednotlivé body se postupně věnují vývoji práce tak, aby obsahovala všechny důležité údaje v každé z částí zpracovávání dat. Zásady pro vypracování práce poskytují velmi podrobný popis jednotlivých bodů uvedených v kontrolním seznamu. Ke každému bodu je kromě detailního popisu k dispozici také příklad, na kterém je názorně předvedeno splnění požadavků v daném bodě. Vývojový diagram slouží k systematickému zachycení průběhu vyhledávání informací pro použití v systematickém přehledu. Obsahuje informace o:

- počtu záznamů, které byly nalezeny v prohledávaných databázích,
- počtu záznamů určených k prozkoumání dle názvu či abstraktu,
- počtu záznamů určených k prozkoumání plného textu
- počtu vyřazených záznamů z důvodu duplicity, nerelevance, nedostupnosti plného textu či jiných důvodů.

6.2 Metodika zpracování

Při tvorbě této literární rešerše byla použita metodika PRISMA, popsaná výše. Postup vyhledání a selekce relevantní literatury je popsán na obrázku 13. Relevantní literatura byla vyhledána ve víceoborových bibliografických databázích Scopus a Web of Science a v databázi ACM Digital Library, která je zaměřena na tématiku výpočetních a informačních technologií. Vyhledání literatury bylo provedeno za použití následujících klíčových slov a logických operátorů: („game theory“ OR „game theoretic“ OR „game-theoretic“) AND „anomaly detection“.

Kritéria pro zařazení

Do literární rešerše byly zařazeny všechny publikace, které splňovaly následující kritéria:

- typ publikace: článek v odborném časopise,
- jazyk publikace: anglický,
- datum vydání mezi roky: 2017-2022,
- dostupnost: celý text.

Z vyhledávání byly vyřazeny

- sborníky z konferencí,
- průzkumy,
- články zaměřené pouze na detekci anomálií (bez spojitosti s teorií her).

Vyhledání a zpracování článků bylo prováděno v období březen-květen 2022. Cílem rešerše je nalézt odpovědi na tři výzkumné otázky:

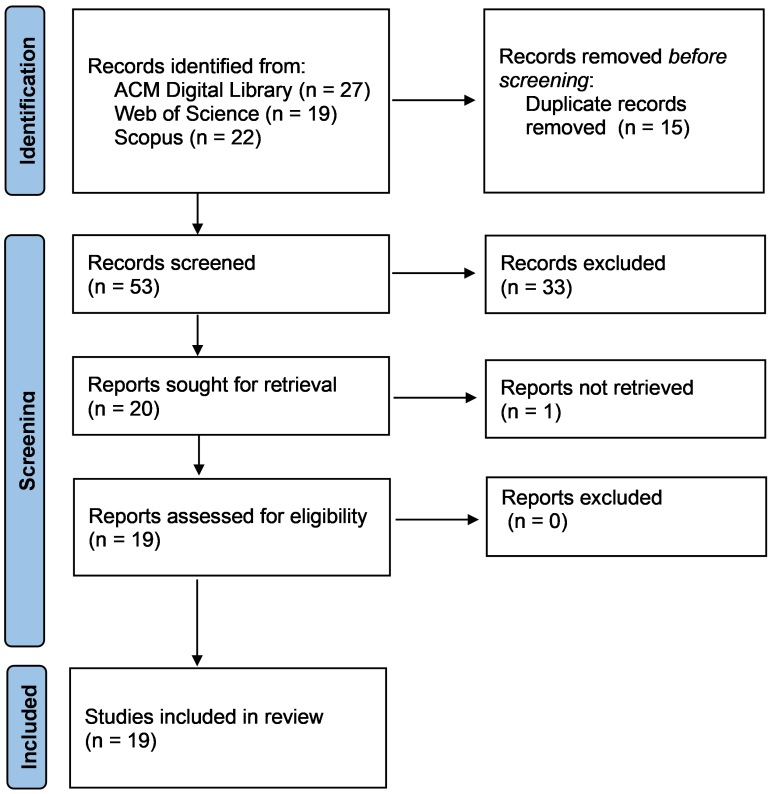
1. **Otázka 1:** V jakých oblastech je používána detekce anomálií s využitím teorie her?
2. **Otázka 2:** Jaké typy detekce anomálií a her jsou používány?
3. **Otázka 3:** Přineslo použití teorie her při detekci anomálií lepší výsledky?

6.3 Výběr a analýza článků

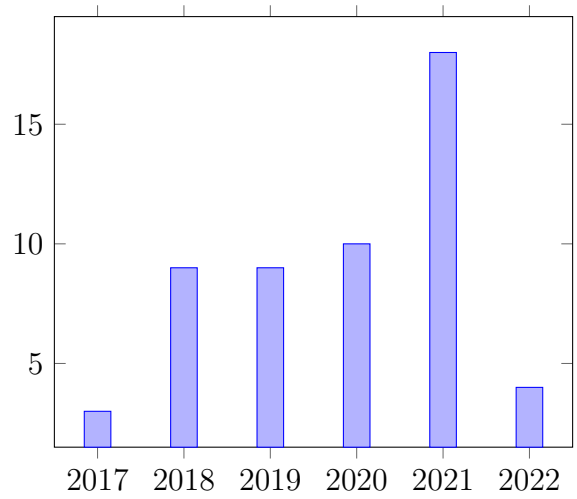
Výsledkem vyhledávání bylo celkem 68 nalezených článků, z toho 27 článků v databázi ACM Digital Library, 19 článků v databázi Web of Science a 22 článků v databázi Scopus. Následně bylo kontrolou duplikátů odstraněno 15 článků, čímž bylo nalezeno celkem 53 článků určených pro výběr relevantních článků dle názvu a abstraktu (anglicky screening). Po výběru relevantních článků dle přečtení abstraktů bylo do rešerše zařazeno celkem 19 článků.

Na grafu 14 lze vidět počty článků nalezených dle hledaných kritérií v jednotlivých letech. Zájem výzkumníků o toto téma roste zejména díky rozvoji oblasti IoT, mimo jiné z důvodu nutnosti řešení otázky zabezpečení množství zařízení a senzorů s omezenými výpočetními a energetickými možnostmi.

U všech článků bylo sledováno několik parametrů: rok vydání, metoda detekce anomálií, typ hry, oblast, cíl práce a výsledek. Souhrn studovaných článků a sledovaných parametrů je uveden v tabulce 2.



Obrázek 13: Vývojový diagram PRISMA. Zdroj: [58]



Obrázek 14: Počty nalezených článků dle roku vydání. Zdroj: vlastní zpracování

Tabulka 2: Analýza článků zahrnutých v rešerši

Autor, rok	**Metoda detekce**	**Teorie her**	**Aplikační oblast**	**Shrnutí obsahu**
Antwarg et al., 2021 [59]	strojové učení - autoenkodér	Shapleyho hodnota	neuvedeno	**Cíl:** Představit metodu vysvětlení důvodu vzniku anomálií detekovaných autoenkodéry, bez ohledu na jejich vnitřní strukturu. Pro toto vysvětlení jsou použity Shapleyho hodnoty vlastností rekonstruovaných dat a porovnání s hodnotami původních dat. Vysvětlení důvodu vzniku anomálií má za cíl zvýšit důvěru v metody strojového učení a přinést porozumění rozhodnutím detekčního systému. **Výsledek:** Metoda byla otestována na čtyřech datasetech z různých oblastí (reklamace, útoky na síť, transakce na platebním účtu a vygenerovaný dataset) s různou velikostí a počtem vlastností. Výsledné vlastnosti se shodovaly s očekávanými. Výstupy kontroly datasetu reklamací byly konzultovány s experty v této oblasti, kterým byla poskytnutá vysvětlení nápomocná při identifikaci složitých případů neoprávněných reklamací.

Pokračování na další straně

Tabulka 2 – *Pokračování*

Autor, rok	**Metoda detekce**	**Teorie her**	**Aplikační oblast**	**Shrnutí obsahu**
Arfaoui et al., 2019 [60]	statistická (EWMA, Manhattanská vzdálenost)	opakovaná hra více hráčů s možností spolupráce; senzory se na základě svého stavu (síla signálu, stav baterie, volná paměť, časová náročnost) rozhodují, zda budou s ostatními spolupracovat = porovnají si data ze senzorů a zlepší přesnost detekce, nebo zda provedou detekci pouze lokálně	WBAN (Wireless Body Area Network), IoT, zdravotnictví	**Cíl:** Vytvořit systém detekce anomálií v oblasti IoT ve zdravotnictví. Lokální detekce anomálií využívá časoprostorové informace k rozlišení vadných senzorů od změny zdravotního stavu pomocí korelace dat mezi senzory. Globální detekce agreguje detekované anomálie a pomocí Manhattanské vzdálenosti naměřených parametrů rozhoduje o typu anomálie. Teorie her se využívá pro zlepšení přesnosti detekce sdílením dat mezi senzory. **Výsledek:** Systém byl otestován na datasetu vytvořeném z reálných dat z jednotek intenzivní péče. Testování proběhlo bez možnosti kolaborace senzorů a s kolaborací senzorů pro porovnání efektivity využití teorie her. Detekce bez možnosti kolaborace identifikovala v datech čtyři anomálie, s možností kolaborace pouze dvě. Využitím teorie her došlo ke snížení falešně pozitivních výsledků a zvýšení přesnosti. Při porovnání se třemi dalšími přístupy pomocí ROC křivek dosáhl představený systém nejnižší podíl falešně pozitivních výsledků.

Pokračování na další straně

Tabulka 2 – *Pokračování*

Autor, rok	**Metoda detekce**	**Teorie her**	**Aplikační oblast**	**Shrnutí obsahu**
Bulla a Birje, 2021 [61]	strojové učení (LSTM autoenkodér a One-Class SVM)	Shapleyho hodnota	IoT, Fog computing, prediktivní údržba	**Cíl:** Vytvořit systém prediktivní údržby fog computing infrastruktury a smart zařízení. Systém pomocí LSTM autoenkodéru a One-Class SVM detekuje anomálie a pomocí algoritmu SHAP (využívajícího Shapleyho hodnot) provádí analýzu hlavní příčiny nalezených anomálií. **Výsledek:** Systém byl otestován na veřejně dostupném datasetu a detekce porovnána se třemi dalšími metodami strojového učení (RNN, LSTM, autoenkodér). V porovnání má nejnižší RMSE a nejvyšší preciznost.
Cinque et al., 2020 [62]	statistická	koaliční - volba důležitých parametrů	detekce zneužití dat a selhání v záznamech kritických systémů	**Cil:** Detekovat zneužití dat a selhání systému. Detekce probíhá pomocí výběru sledovaných vlastností formou koaliční hry a následně pomocí určení skóre dat a porovnávání s hranicemi. **Výsledek:** Představený systém porovnán se čtyřmi dalšími algoritmy pomocí metrik preciznosti, senzitivity a správnosti. V těchto metrikách představený systém překonává tři ze čtyř algoritmů, ve správnosti je nejlepší.

Pokračování na další straně

Tabulka 2 – *Pokračování*

Autor, rok	**Metoda detekce**	**Teorie her**	**Aplikační oblast**	**Shrnutí obsahu**
Ghafouri et al., 2019 [63]	statistická - sekvenční testování (CUSUM)	Stackelbergova hra dvou hráčů, útočník má úplnou informaci	sledování prostředí	**Cíl:** Nalézt a ověřit algoritmus, který vypočítá optimální hraniční hodnotu (rozdělující normální data a anomálie) pro statistickou detekci anomálií v závislosti na čase. Optimální hodnota je založena na kompromisu mezi zpožděním detekce (čas mezi začátkem útoku a detekcí) a pravděpodobností falešně pozitivních výsledků. Problém je modelován jako Stackelbergova hra, kdy útočník volí čas a typ útoku a obránce volí hraniční hodnotu detekce tak, aby minimalizoval škodu a pravděpodobnost falešně pozitivních výsledků. **Výsledek:** Funkce algoritmu byla otestována na reálných datech systému distribuce vody, kdy se útočník snaží v určitém čase a s určitou intenzitou kontaminovat vodu. Použití optimální hraniční hodnoty závislé na denní době přineslo výrazně nižší způsobenou škodu v porovnání s pevnou optimální hraniční hodnotou.

Pokračování na další straně

Tabulka 2 – *Pokračování*

Autor, rok	**Metoda detekce**	**Teorie her**	**Aplikační oblast**	**Shrnutí obsahu**
Huang et al., 2020 [64]	statistická (LSMAD RX)	hra více hráčů (superpixely) s možností spolupráce; hráči volí, zda budou anomálie či pozadí	detekce objektů v obraze	**Cíl:** Vytvořit systém detekce objektů v hyperspektrálních snímcích. Ze snímků jsou extrahovány tři vrstvy, ve kterých jsou pomocí modelování problému detekce anomálií jako hry odlišeny oblasti s pozadím od oblastí s objekty (anomáliemi). Výsledky těchto tří her jsou zkombinovány do jedné mapy detekcí. **Výsledek:** Výsledný systém otestován na čtyřech snímcích a porovnán s pěti dalšími algoritmy pomocí ROC křivek a času detekce. Představený systém překonal všechny ostatní algoritmy v efektivitě, v rychlosti detekce byl třetí nejrychlejší.
Martakis et al., 2022 [65]	strojové učení (SVM)	Shapleyho hodnota	průmysl - detekce závad na zařízení či senzorech	**Cíl:** Vytvořit framework pro detekci poškození senzorů sledujících kritickou infrastrukturu, např. mosty, pomocí využití SVM a algoritmu XGBoost. Rozhodování frameworku má být vysvětlitelné, toho je dosaženo výběrem vlastností vstupních dat a jejich Shapleyho hodnotami, které určují podíl vlastností na výsledném zařazení. **Výsledek:** Framework otestován na dvou případových studiích dat ze senzorů na lanových mostech. V obou případech byl výsledek detekce anomálií dobrý.

Pokračování na další straně

Tabulka 2 – *Pokračování*

Autor, rok	**Metoda detekce**	**Teorie her**	**Aplikační oblast**	**Shrnutí obsahu**
Mishra a Smirnova, 2021 [66]	neuvedeno	sekvenční hra dvou hráčů; útočník útočí nebo neútočí, organizace prověřuje nebo neprověřuje transakci v případě, že byla/nebyla zaznamenána neobvyklá aktivita	detekce narušení systému (IDS)	**Cíl:** Optimalizace IDS využívajících detekci anomálií pomocí teorie her tak, aby byla nalezena rovnováha mezi úspěšností detekce a FP hlášeními na základě ceny prověření FP vs. ceny nezachyceného útoku. **Výsledek:** Výsledkem je model strategických interakcí mezi organizací a útočníkem. Při použití zjištěné reálné ceny kontroly transakcí a ROC křivky použité detekce anomálií (zobrazuje TP a FP - efektivitu) lze tento model použít pro optimalizaci nastavení detekce anomálií.
Neshenko et al., 2021 [67]	strojové učení - neuronová síť a enkodér	Shapleyho hodnota	IoT, průmysl	**Cíl:** Vytvořit systém detekce anomálií v datech ze senzorů v úpravnách vody. Detekce probíhá pomocí neuronové sítě typu BiGAN a enkodéru a následně je pomocí statistické metody CART a Shapleyho hodnot určeno, zda se jedná o lokální anomálii nebo útok na sledovaný objekt. **Výsledek:** Systém byl otestován na reálných datech získaných z malé úpravny vody. Ve srovnání s nejmodernějšími systémy byla preciznost detekce mírně nižší - 0,81, ale senzitivita byla mírně vyšší - 0,84. Preciznost a senzitivita identifikace škodlivých senzorů však byla vyšší (0,38 a 0,49) oproti porovnávaným systémům. Představený systém je tak podobně efektivní jako nejmodernější systémy.

Pokračování na další straně

Tabulka 2 – *Pokračování*

Autor, rok	**Metoda detekce**	**Teorie her**	**Aplikační oblast**	**Shrnutí obsahu**
Rani et al., 2019 [68]	neuvedeno	vícekolová nekooperativní hra dvou hráčů s nenulovým součtem (vedoucí shluku a jednotlivé prvky ve shluku); prvek může být normální nebo škodlivý, vedoucí shluku řadí prvek do tří kategorií: normální, podezřelý a škodlivý	IoT, Wireless Sensor Network (WSN)	**Cíl:** Vytvořit energeticky úsporný systém senzorů (EETE), který pomocí teorie her tvoří shluky o dostatečné velikosti a udržuje informace o důvěryhodnosti jednotlivých prvků. Na základě této důvěryhodnosti následně detekuje škodlivé prvky. **Výsledek:** Představený systém byl porovnán se systémy TDDG, HIDS, CWSN a LHIDS. V účinnosti detekce překonává LHIDS i při zvýšeném počtu škodlivých prvků. EETE má nižší či srovnatelnou spotřebu s TDDG, v závislosti na počtu prvků. EETE potřebuje výrazně nižší čas na detekci škodlivých prvků, bez ohledu na procento jejich zastoupení. EETE tedy překonává porovnávané systémy v úspěšnosti detekce a době potřebné pro detekci, době určení důvěryhodnosti prvků a spotřebě energie.
Saraeian a Shirazi, 2020 [69]	strojové učení - klasifikace	nekooperativní hra dvou hráčů s nenulovým součtem, s úplnou informací	průmysl	**Cíl:** Rozšířit Business Process Management systém o bezpečnostní modul, který detekuje narušení výrobních procesů. Ze záznamů zjistí průběh procesů a porovná jej s předpokládaným chováním. Detekce je optimalizována pomocí teorie her nalezením Nashova rovnovážného řešení s pravděpodobnostmi spuštění detekce. **Výsledek:** Při porovnání s jinými algoritmy systém přinesl snížení časové náročnosti. Přesnost detekce se pohybovala mezi 97-98 % s velmi nízkým počtem falešně pozitivních výsledků.

Pokračování na další straně

Tabulka 2 – *Pokračování*

Autor, rok	**Metoda detekce**	**Teorie her**	**Aplikační oblast**	**Shrnutí obsahu**
Sedjelmaci et al., 2017 [70]	strojové učení - neuronová síť	vícekolová hra více hráčů (obránci, útočníci) s úplnou informací	IoT	**Cíl:** Vytvořit takový systém detekce narušení, který se snaží rozpoznat známé typy útoků. Pouze při neznámém útoku spustí detekci anomálií, čímž šetří energii. Systém detekce je modelován jako hra útočníka a obránce. Při dosažení Nashova rovnovážného řešení útočník použije nový útok a obránce spustí detekci anomálií s cílem naučit se jej. Pro snížení FP hlášení je použit systém reputace, který zařazuje jednotlivé prvky sítě do tří kategorií důvěryhodnosti. **Výsledek:** Vytvořený systém je porovnán se třemi používanými hybridními systémy. V simulovaném prostředí je úspěšnost detekce podobná, při různých počtech senzorů se liší cca o 1 % a i při vysokém počtu senzorů přesahuje 92 %. Falešně pozitivní výsledky nepřesahují 3 %. Rychlost detekce představeného systému je výrazně vyšší než ostatní, systému trvá detekce až o polovinu méně času než ostatní systémy. Výrazně je také snížena spotřeba energie, a to minimálně o polovinu i při vysokém počtu senzorů.

Pokračování na další straně

Tabulka 2 – *Pokračování*

Autor, rok	**Metoda detekce**	**Teorie her**	**Aplikační oblast**	**Shrnutí obsahu**
Subba et al., 2018 [71]	na úrovni prvku specifikační pravidla, na úrovni vedoucího shluku specifikační pravidla a klasifikace neuronovou sítí	nekooperativní hra dvou hráčů (monitorovaný senzor a IDS agent) s neúplnou informací	Wireless Sensor Networks (WSN), IoT	**Cíl:** Vytvořit framework pro detekci narušení sítě na základě pravidel a strojového učení s využitím modelování situace jako hry pro snížení síťového provozu nutného pro tuto detekci. Framework by měl splňovat požadavky na nízkou energetickou náročnost, výpočetní výkon a nízkou zátěž sítě. Framework se skládá ze tří úrovní: senzor, vedoucí shluku a základní stanice. **Výsledek:** Framework otestován simulací pěti různých typů útoků a porovnán se dvěma hybridními systémy, jedním hierarchickým systémem a jedním systémem založeným na teorii her. Detekce narušení porovnatelná s hierarchickým systémem, ale s nižší spotřebou energie, překonala ostatní. FP hlášení porovnatelná se systémem založeným na teorii her, nižší než ostatní. Spotřeba nižší než ostatní systémy.

Pokračování na další straně

Tabulka 2 – *Pokračování*

Autor, rok	**Metoda detekce**	**Teorie her**	**Aplikační oblast**	**Shrnutí obsahu**
Wang et al., 2019 [72]	kombinace statistické metody a strojového učení	hra dvou hráčů s neúplnou informací, hráči nemusí být racionální; útočník se rozhoduje, zda zaútočí či ne, obránce se rozhoduje, zda pakety propustí, zablokuje nebo spustí detekční modul se strojovým učením	IoT	**Cíl:** Vytvořit systém detekce škodlivosti přijímaných dat od jiných senzorů v síti. Systém se skládá ze statistické detekce anomálií, dle jejího výsledku se poté rozhoduje, zda spustí detekci strojovým učením. Rozhodování je modelováno jako hra. Detekce strojovým učením spotřebuje mnohem více energie, proto není spouštěna pořád. K rozhodování pomáhá zpětná vazba ze spouštění detekce strojovým učením. **Výsledek:** Funkce ověřena simulací, v porovnání se statistickou detekcí, detekcí strojovým učením a v jiném díle představenou detekcí založené na teorii her přinesl systém vyšší úspěšnost a nižší spotřebu energie.
Wu a Wang, 2018 [73]	statistická (CUSUM)	nekonečná hra dvou hráčů (útočník, obránce) s nenulovým součtem; obránce volí hraniční hodnotu detekce, útočník rozdělení prostředků	bezpečnost počítačových či senzorových sítí	**Cíl:** Modelováním situace útoku na síť jako hry nalézt optimální hraniční hodnotu detekce anomálií a optimální rozdělení prostředků pro napadení jednotlivých částí sítě s cílem způsobit co největší poškození. **Výsledek:** Dokázána existence Nashova rovnovážného řešení, představen algoritmus pro jeho výpočet. Algoritmus byl otestován simulací DDoS útoku na distribuovaný DNS a na síť o velikosti 100 prvků. V obou případech bylo nalezeno Nashovo rovnovážné řešení.

Pokračování na další straně

Tabulka 2 – *Pokračování*

Autor, rok	**Metoda detekce**	**Teorie her**	**Aplikační oblast**	**Shrnutí obsahu**
Wu a Wang, 2018 [74]	statistická - testování hypotéz	opakovaná hra dvou racionálních hráčů; obráncova strategie je volba hraniční hodnoty detekce, útočníkova strategie je rozložení zdrojů mezi prvky sítě	IoT	**Cíl:** Představit kolaborativní metodu detekce anomálií - plně distribuovanou formu centralizované metody, kdy na rozdíl od centralizované metody detekci provádí každý prvek v síti na základě informací od sousedních prvků. Modelováním situace jako hry je hledána optimální hranice detekce. **Výsledek:** Metoda byla analyzována a otestována na simulované síti, kdy byl sledován počet iterací nutných k nalezení Nashova rovnovážného řešení a vývoj užitku obránce.
Yan et al., 2019 [75]	neuvedeno	Stackelbergova hra s nulovým součtem a racionálními hráči; auditor se snaží nalézt takové rozdělení budgetu, aby co nejvíce snížil výplatu útočníkům	bezpečnostní audit, průmysl	**Cíl:** Detekce anomálií registruje různé události a přiřazuje jim priority. Pro kontrolu detekcí je vyhrazen omezený počet pracovníků a čas. Cílem práce je pomocí modelování interakce mezi auditory a útočníky nalézt způsob rozdělení počtu pracovníků mezi priority tak, aby útočníci způsobili co nejmenší škodu. **Výsledek:** Funkce představeného heuristického algoritmu byla nejdříve ověřena na malém datasetu porovnáním výsledků se známým optimálním řešením. Následně byl algoritmus použit na dvou datasetech z reálného prostředí a porovnán se třemi běžně používanými přístupy. V tomto porovnání představený algoritmus výrazně překonal výsledky ostatních přístupů.

Pokračování na další straně

Tabulka 2 – *Pokračování*

Autor, rok	**Metoda detekce**	**Teorie her**	**Aplikační oblast**	**Shrnutí obsahu**
Yang et al., 2017 [76]	statistická; založená na predikci budoucího stavu parametrů dat a sekvenčním testování hypotéz	nekonečná, opakovaná hra dvou racionálních hráčů s úplnou informací; cílem útočníka je maximalizovat průměrnou hodnotu vložených falešných dat, cílem obránce je co nejrychleji odhalit kompromitovaná data a tím minimalizovat objem falešných dat	IoT, sledování prostředí	**Cíl:** Vytvořit systém detekce narušení integrity agregovaných dat získaných ze senzorů. Ověřit funkci systému formulací problému jako nekonečná opakovaná hra s dokonalou informací. **Výsledek:** Funkce představeného systému byla teoreticky ověřena pomocí formulace strategií a nalezení Nashovy rovnováhy. Dále byla funkce ověřena v několika simulovaných scénářích.

Pokračování na další straně

Tabulka 2 – *Pokračování*

Autor, rok	**Metoda detekce**	**Teorie her**	**Aplikační oblast**	**Shrnutí obsahu**
Yang et al., 2021 [77]	strojové učení (k-průměry)	evoluční hra mezi důvěryhodnými senzory	IoT, WSN	**Cíl:** Vytvořit systém bezpečné komunikace mezi senzory. Senzory vytvářejí shluky, v rámci shluku si udržují informace o důvěryhodnosti ostatních senzorů pomocí fuzzy logiky. Z těchto informací jsou následně pomocí metody k-průměrů identifikovány škodlivé senzory, které mohou ovlivňovat bezpečnost zahazováním paketů či jejich zpožděním. Volba vedoucích shluků je modelována pomocí evoluční hry mezi důvěryhodnými senzory. **Výsledek:** Systém byl analyzován pomocí simulace a porovnán se dvěma dalšími algoritmy (TKFCC, SCCT). Představený systém oproti ostatním algoritmům výrazně snížil počet útoků na síť a to i při vyšším počtu škodlivých senzorů. Doba životnosti sítě byla vyšší než při použití TKFCC, ale nižší než při použití SCCT z důvodu menšího počtu adeptů na vedoucího shluku. Snaha nepoužívat nedůvěryhodné senzory ke komunikaci vede také k nejnižší propustnosti sítě, ale k nejlepšímu využití energie díky omezení nutnosti opakovaného přenosu dat.

7 Souhrn výsledků

V této kapitole jsou shrnuty výsledky systematické rešerše. V jednotlivých podkapitolách jsou uvedeny odpovědi na stanovené výzkumné otázky, viz podkapitola 6.2.

7.1 Odpověď na otázku 1: Oblasti využití detekce anomálií

Největší oblastí využití detekce anomálií ve zkoumané literatuře je Internet of Things, tomuto tématu se věnuje 13 článků. Další oblasti využití, kterým se autoři článků věnovali jsou průmysl, zdravotnictví a detekce objektů v obrazu. Některé práce se v souvislosti s detekcí věnovali využití teorie her k vysvětlení vlivů, které vedly k detekci anomálie.

Díky dobré dostupnosti a nízké ceně jsou malá, energeticky nenáročná zařízení a senzory používána ke sledování okolí či zařízení. Počítačové sítě složené z těchto prvků (anglicky Wireless Sensor Network, zkráceně WSN) jsou však často vystaveny vnějším vlivům a mají nedostatečné zabezpečení proti fyzickému přístupu. Z těchto důvodů se mohou v datech komunikovaných mezi zařízeními vyskytovat různé druhy anomálií, jako jsou data z poškozených senzorů či různé formy útoků na síť.

Články věnující se zabezpečení sítí IoT mají za cíl zajistit stabilitu sítě a důvěryhodnost dat ze senzorů. Anomálií v této oblasti může být útok na síť či poškození některého prvku. Detekce anomálií je prováděna na několika úrovních. Na úrovni prvků sleduje každý prvek sítě chování ostatních prvků (například síla signálu, délka a pravidelnost komunikace) v jeho okolí. Na úrovni shluků je detekce prováděna vedoucím shluku na základě agregovaných dat z ostatních prvků ve shluku. Na úrovni sítě detekci provádí k tomuto účelu určený prvek, který má výrazně vyšší výkon a není omezen spotřebou energie. Detekci provádí na základě agregovaných dat z celé sítě. Specifikem detekce anomálií v IoT je důraz na optimalizaci spotřeby energie jednotlivých prvků pro jejich co nejdelší provoz a současně zachování dostatečné výkonnosti detekce.

V oblasti průmyslu je detekce anomálií důležitá pro udržení bezpečnosti sledovaných výrobních procesů či zařízení. Díky zjištěným anomáliím je možné identifikovat útok na zařízení, jeho selhání či selhání senzorů určených ke sledování a včasnou reakcí minimalizovat vzniklé škody. Ve zkoumané literatuře jsou popsány způsoby detekce anomálií ve výrobních procesech či zařízeních kritické infrastruktury, jako jsou například úpravny vody.

V oblasti zdravotnictví je detekce anomálií využívána pro sledování zdravotního stavu pacientů pomocí senzorů. Zdravotní stav pacienta je sledován množstvím sen-

zorů rozmístěných po těle, které sledují jeho různé vlastnosti - srdeční tep, krevní tlak, teplotu a jiné. Díky nepřetržitému sledování je možné včas zachytit změnu zdravotního stavu nebo poškození senzorů a tím zlepšit lékařskou péči.

7.2 Odpověď na otázku 2: Typy detekce anomálií a her

Mnoho vybraných článků využívá metody detekce, které se vyskytly ve výběru pouze jednou, bylo však nalezeno několik metod, které se v článcích opakují. Mezi tyto metody patří sekvenční testování hypotéz a technika Cumulative Sum (CUSUM), které jsou popsány v kapitole 4. Dále jsou ve zkoumané literatuře využívány metody strojového učení: klasifikační neuronové sítě typu MLP a BiGAN, autoenkodéry, Support Vector Machines (SVM) a rozšíření One-class SVM. Tyto metody jsou popsány v podkapitole 3.1.

Využití teorie her

Z výsledků literární rešerše vyplývá, že teorie her je využívána několika způsoby: k modelování problému detekce anomálií jako hry mezi útočníkem a obráncem, pro optimalizaci spotřeby energie a nákladovou efektivitu či pro vysvětlení příčin detekce anomálie.

Autoři prací v rešerši využívají poznatků z teorie her k různým způsobům vylepšení detekce anomálií. Autoři často využívají teorii her v kombinaci se statistickou detekcí anomálií, kde je problém detekce modelován jako hra mezi útočníkem a obráncem (viz [63, 66, 70, 71, 72, 73, 74, 75, 76]), kdy cílem obránce je nalézt optimální hraniční hodnoty detekčního algoritmu a cílem útočníka je zvolit takové rozložení prostředků mezi jednotlivé prvky sítě, aby způsobil co největší poškození.

Dalším využitím teorie her je optimalizace spotřeby energie v oblasti IoT. Detekce anomálií, obzvláště při využití metod strojového učení je energeticky náročná činnost. Autoři se proto ve svých pracích často věnují vylepšení životnosti prvků sítě snížením spotřeby energie pomocí omezení sdílení dat vylepšujících detekci mezi senzory [60], volbou použitého detekčního mechanismu [72] či omezením spouštění energeticky náročného algoritmu pouze za účelem rozpoznání neznámého typu útoku [70]. Autoři se tak snaží najít kompromis mezi spotřebou energie prvků v síti a dostatečnou úrovní zabezpečení pomocí modelování problému jako hry a hledáním řešení ve formě Nashovy rovnováhy.

Autoři článků [66] a [75] se věnují využití teorie her pro optimalizaci detekce tak, aby byla nákladově efektivní. Autoři prvního článku se věnují optimalizaci detekčního

algoritmu s ohledem na falešně pozitivní hlášení. Každé hlášení je prověřováno a prověřování falešně pozitivních výsledků negativně ovlivňuje dobu, než dojde k prověření opravdové anomálie. Autoři druhého článku se věnují rozdělení omezeného počtu pracovníků a jejich času mezi jednotlivé priority detekovaných anomálií s cílem minimalizovat škodu způsobenou neprověřenými detekcemi. V souvislosti s optimalizací spotřeby energie a nákladově efektivní detekcí autoři využili také model Stackelbergovy hry.

Autoři se kromě samotné detekce anomálií věnovali také hledání příčin vzniku anomálií a podílu jednotlivých částí sledovaného systému na vzniku nalezených anomálií. V případě detekčních systémů založených na neuronových sítích nelze jednoduše vysvětlit, jakým způsobem systém dospěl k rozhodnutí o detekci. Pro zvýšení důvěry v detekční systémy se autoři snažili nalézt vlastnosti dat, které nejvíce přispěly k detekci. K tomuto účelu byla využita Shapleyho hodnota. Jak uvádí [78], Shapleyho hodnota je v kooperativních hrách využívána pro rozdělení hodnoty výplatní funkce mezi členy koalice dle jejich podílu na výsledku hry. Pomocí těchto hodnot byli autoři schopni vysvětlit důvody detekce anomálie [59, 61], identifikovat vadné senzory [65] či rozlišit, zda jde o vadu senzoru či útok na síť [67].

7.3 Odpověď na otázku 3: Přínos použití teorie her

Metody byly porovnávány pomocí metrik typu preciznost, senzitivita, či správnost. Mezi další způsoby porovnání patří ROC křivka (anglicky Receiver Operating Characteristic curve), která slouží k hodnocení a grafickému znázornění chování algoritmu při různých nastaveních jeho parametrů. Zobrazuje senzitivitu detekce (True Positive Rate, zkráceně TPR) a pravděpodobnost falešného poplachu (False Positive Rate, zkráceně FPR), určenou jako podíl falešně pozitivních výsledků a negativních výsledků. Z výsledků testování ve zkoumaných pracích lze usuzovat, že využití teorie her přineslo zlepšení v oblastech přesnosti detekce, optimalizace algoritmů, snížení spotřeby a vysvětlitelnosti rozhodování. Představené metody podávaly minimálně stejně dobré výkony jako (v době vydání článků) nejmodernější metody bez využití teorie her, v některých případech tyto konkurenční metody výrazně překonávaly.

8 Závěr

Předložená diplomová práce si klade za cíl popsat možnosti uplatnění teorie her v oblasti detekce anomálií. V tomto kontextu byla nejprve teoreticky popsána datová věda, základy práce s daty a oblasti využití v kapitole 2. Pro získávání informací a znalostí z dat v oblasti datové vědy je používáno strojové učení. Nástroje a metody strojového učení používané v oblasti datové vědy jsou popsány v kapitole 3. Oblast vybraná pro zkoumání využití teorie her v datové vědě, kterou je detekce anomálií a metody v ní používané jsou popsány v kapitole 4.

Dále byl čtenář v kapitole 5 seznámen se základními pojmy teorie her, způsoby reprezentace her a řešením her v normálním a rozšířeném tvaru, včetně příkladů.

Kapitola 6 je věnována systematické rešerši na téma uplatnění teorie her v oblasti detekce anomálií. Nejdříve je popsána metodika PRISMA, která byla použita při tvorbě rešerše. Následně zde byly určeny bibliografické databáze, klíčová slova a kritéria, podle kterých byly do rešerše zařazeny články určené k analýze. Poté byly stanoveny výzkumné otázky, na které byly hledány odpovědi. Tato kapitola obsahuje také vývojový diagram popisující postup výběru vhodných článků a souhrnnou tabulku se sledovanými parametry k jednotlivým článkům.

Souhrn poznatků o používaných metodách detekce anomálií, typy her a posouzení přínosu použití teorie her v oblasti detekce anomálií je popsán v kapitole 7. Na základě provedené analýzy bylo zjištěno, že metody uvedené v článcích podávaly ve srovnání s jinými metodami minimálně stejně dobré výsledky.

Diplomová práce se zabývá komplexním tématem a je zaměřena pouze na jednu oblast datové vědy. Další rozvoj zkoumaného tématu je zcela jistě možný, pokračování se může zabývat například jen opakováním stejného postupu na jinou zvolenou oblast datové vědy a následně porovnat zjištěné uplatnění teorie her. Jiným rozvojem tématu může také být vlastní implementace detekce anomálií s využitím teorie her a zkoumání její úspěšnosti.

Literatura

1. MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. *Big Data: A Revolution that Will Transform how We Live, Work, and Think*. Houghton Mifflin Harcourt, 2013. ISBN 978-0-544-00269-2.
2. TUKEY, John W. The Future of Data Analysis. *The Annals of Mathematical Statistics* [online]. 1962-03, roč. 33, č. 1, s. 1–67 [cit. 2021-11-27]. ISSN 0003-4851, ISSN 2168-8990. Dostupné z DOI: 10.1214/aoms/1177704711.
3. WAINER, Howard. *Truth or Truthiness: Distinguishing Fact from Fiction by Learning to Think Like a Data Scientist*. Cambridge University Press, 2016. ISBN 978-1-107-13057-9. Google-Books-ID: KlRyCwAAQBAJ.
4. IGUAL, Laura et al. *Introduction to Data Science: A Python Approach to Concepts, Techniques and Applications*. 1st ed. 2017 edition. New York, NY: Springer, 2017-03. ISBN 978-3-319-50016-4.
5. SKIENA, Steven S. *The Data Science Design Manual* [online]. Cham: Springer International Publishing, 2017 [cit. 2022-01-29]. Texts in Computer Science. ISBN 978-3-319-55443-3 978-3-319-55444-0. Dostupné z DOI: 10.1007/978-3-319-55444-0.
6. *Databáze NoSQL – co je NoSQL? | Microsoft Azure* [online]. [cit. 2022-01-28]. Dostupné z: https://azure.microsoft.com/cs-cz/overview/nosql-database/.
7. *What is a Data Warehouse?* [online]. [cit. 2022-01-28]. Dostupné z: https://www.oracle.com/cz/database/what-is-a-data-warehouse/.
8. *Databases vs. Data Warehouses vs. Data Lakes* [MongoDB] [online]. [cit. 2022-01-28]. Dostupné z: https://www.mongodb.com/databases/data-lake-vs-data-warehouse-vs-database.
9. VERMEULEN, Andreas François. *Practical Data Science: A Guide to Building the Technology Stack for Turning Data Lakes into Business Assets*. 1st ed. edition. New York, NY: Apress, 2018-02-22. ISBN 978-1-4842-3053-4.
10. HOODA, Saurabh. *Python Data Science for Beginners* [KDnuggets] [online]. [cit. 2022-01-30]. Dostupné z: https://www.kdnuggets.com/python-data-science-for-beginners.html/.

11. MYERS, Astasia. *Data Science Notebooks — A Primer* [Memory Leak] [online]. 2020-04-29. [cit. 2022-01-30]. Dostupné z: https://medium.com/memory-leak/data-science-notebooks-a-primer-4af256c8f5c6.

12. EUNICE, Tommy et al. *Translate a business problem into an AI and data science solution - IBM Garage Practices* [online]. [cit. 2022-01-30]. Dostupné z: https://www.ibm.com/garage/method/practices/discover/business-problem-to-ai-data-science-solution/.

13. KRUMM, Alison. Data Science Lifecycle. In: *Cortell Intelligent Business Solutions* [online]. Midrand: Cortell, 2018 [cit. 2022-08-05]. Dostupné z: http://www.cortell.co.za/wp-content/uploads/2018/06/chart.png.

14. GROSSMANN, Wilfried. *Anonymization* [CROS - European Commission] [online]. 2019-04-28. [cit. 2022-02-01]. Dostupné z: https://ec.europa.eu/eurostat/cros/content/anonymization_en.

15. GROSSMANN, Wilfried. *Pseudonymisation* [CROS - European Commission] [online]. 2019-05-08. [cit. 2022-02-01]. Dostupné z: https://ec.europa.eu/eurostat/cros/content/pseudonymisation_en.

16. *Portál otevřených dat České republiky* [online]. [cit. 2022-02-03]. Dostupné z: https://data.gov.cz/.

17. BIDDLE, Edd et al. *Understand data needs to support AI and data science solutions - IBM Garage Practices* [online]. [cit. 2022-02-01]. Dostupné z: https://www.ibm.com/garage/method/practices/think/data-needs-for-ai-data-science/.

18. BIDDLE, Edd; CHRISTENSEN, Paul. *Prepare your data for AI and data science - IBM Garage Practices* [online]. [cit. 2022-02-09]. Dostupné z: https://www.ibm.com/garage/method/practices/code/data-preparation-ai-data-science/.

19. KIRU, Muhammad. *Body Measurements Datasets* [online]. Mendeley, 2021-07-15 [cit. 2022-02-19]. Dostupné z DOI: 10.17632/BJV6C9PMP4.1.

20. BIDDLE, Edd. *Select and develop an AI and data science model - IBM Garage Practices* [online]. [cit. 2022-02-20]. Dostupné z: https://www.ibm.com/garage/method/practices/reason/model-selection-development-ai-data-science/.

21. CHANDOLA, Varun et al. Anomaly Detection: A Survey. *ACM Comput. Surv.* 2009-07, roč. 41. Dostupné z DOI: 10.1145/1541880.1541882.

22. ŠABIĆ, Edin et al. Healthcare and anomaly detection: using machine learning to predict anomalies in heart rate data. *AI & SOCIETY* [online]. 2021-03, roč. 36, č. 1, s. 149–158 [cit. 2022-06-16]. ISSN 0951-5666, ISSN 1435-5655. Dostupné z DOI: 10.1007/s00146-020-00985-1.

23. LAI, Yingxu et al. Industrial Anomaly Detection and Attack Classification Method Based on Convolutional Neural Network. *Security and Communication Networks* [online]. 2019-09, roč. 2019, e8124254 [cit. 2022-06-16]. ISSN 1939-0114. Dostupné z DOI: 10.1155/2019/8124254.

24. KIM, Ki-Jo; TAGKOPOULOS, Ilias. Application of machine learning in rheumatic disease research. *The Korean Journal of Internal Medicine*. 2018-12-31, roč. 34. Dostupné z DOI: 10.3904/kjim.2018.349.

25. LI, Lorraine. *Principal Component Analysis for Dimensionality Reduction* [Medium] [online]. 2019-05-27. [cit. 2022-02-24]. Dostupné z: https://towardsdatascience.com/principal-component-analysis-for-dimensionality-reduction-115a3d157bad.

26. CHAUHAN, Nagesh Singh. *What is Hierarchical Clustering?* [KDnuggets] [online]. [cit. 2022-02-25]. Dostupné z: https://www.kdnuggets.com/what-is-hierarchical-clustering.html/.

27. HAYASAKA, Satoru. *What is Clustering and How Does it Work?* [KDnuggets] [online]. [cit. 2022-02-25]. Dostupné z: https://www.kdnuggets.com/what-is-clustering-and-how-does-it-work.html/.

28. SKALSKÁ, Hana. *Aplikovaná statistika*. Hradec Králové: Gaudeamus, 2013. ISBN 978-80-7435-320-8. OCLC: 886601186.

29. MCDONALD, Conor. *Machine learning fundamentals (I): Cost functions and gradient descent* [Medium] [online]. 2021-04-03. [cit. 2022-03-05]. Dostupné z: https://towardsdatascience.com/machine-learning-fundamentals-via-linear-regression-41a5d11f5220.

30. THARWAT, Alaa. Classification assessment methods. *Applied Computing and Informatics* [online]. 2020-01-01, roč. 17, č. 1, s. 168–192 [cit. 2022-03-05]. ISSN 2210-8327. Dostupné z DOI: 10.1016/j.aci.2018.08.003.

31. PATEL, Harsh; PRAJAPATI, Purvi. Study and Analysis of Decision Tree Based Classification Algorithms. *International Journal of Computer Sciences and Engineering*. 2018, roč. 6, s. 74–78. Dostupné z DOI: 10.26438/ijcse/v6i10.7478.

32. SHAH, Kanish et al. A Comparative Analysis of Logistic Regression, Random Forest and KNN Models for the Text Classification. *Augmented Human Research* [online]. 2020-03-05, vol. 5, no. 1, s. 12 [cit. 2022-03-06]. ISSN 2365-4325. Dostupné z DOI: 10.1007/s41133-020-00032-0.

33. GANDHI, Rohith. *Support Vector Machine — Introduction to Machine Learning Algorithms* [Medium] [online]. 2018-07-05. [cit. 2022-07-26]. Dostupné z: https://towardsdatascience.com/support-vector-machine-introduction-to-machine-learning-algorithms-934a444fca47.

34. KILARU, Vasudeva. *One Class Classification Using Support Vector Machines* [Analytics Vidhya] [online]. 2022-06-03. [cit. 2022-07-26]. Dostupné z: https://www.analyticsvidhya.com/blog/2022/06/one-class-classification-using-support-vector-machines/.

35. GUPTA, Jayant. One-class data description. In: *Wikipedia* [online]. 2019-09-02 [cit. 2022-07-26]. Dostupné z: https://en.wikipedia.org/w/index.php?title=File:One-class_data_description_TAX.png&oldid=913742868.

36. GOYAL, Chirag. *Text Cleaning and Preprocessing | Guide to Master NLP (Part 3)* [Analytics Vidhya] [online]. 2021-06-15. [cit. 2022-03-07]. Dostupné z: https://www.analyticsvidhya.com/blog/2021/06/part-3-step-by-step-guide-to-nlp-text-cleaning-and-preprocessing/.

37. YSE, Diego Lopez. *Text Normalization for Natural Language Processing (NLP)* [Medium] [online]. 2021-03-12. [cit. 2022-03-07]. Dostupné z: https://towardsdatascience.com/text-normalization-for-natural-language-processing-nlp-70a314bfa646.

38. PANTOLA, Paritosh. *Natural Language Processing: Text Data Vectorization* [Medium] [online]. 2018-06-14. [cit. 2022-03-07]. Dostupné z: https://medium.com/@paritosh_30025/natural-language-processing-text-data-vectorization-af2520529cf7.

39. AGRAWAL, Rakesh; SRIKANT, Ramakrishnan. Fast algorithms for mining association rules. In: *Proc. of 20th Intl. Conf. on VLDB* [online]. 1994, s. 487–499 [cit. 2022-03-10]. Dostupné z: https://www.vldb.org/conf/1994/P487.PDF.

40. KORSTANJE, Joos. *The Apriori algorithm* [Medium] [online]. 2021-09-24. [cit. 2022-03-10]. Dostupné z: https://towardsdatascience.com/the-apriori-algorithm-5da3db9aea95.

41. BROWNLEE, Jason. *A Gentle Introduction to Generative Adversarial Networks (GANs)* [Machine Learning Mastery] [online]. 2019-06-16. [cit. 2022-07-25]. Dostupné z: https://machinelearningmastery.com/what-are-generative-adversarial-networks-gans/.

42. TSANG, Sik-Ho. *Review — BiGAN: Adversarial Feature Learning (GAN)* [Nerd For Tech] [online]. 2021-05-08. [cit. 2022-07-25]. Dostupné z: https://medium.com/nerd-for-tech/review-bigan-adversarial-feature-learning-gan-535eb76be2ca.

43. BADR, Will. *Auto-Encoder: What Is It? And What Is It Used For? (Part 1)* [Medium] [online]. 2019-07-01. [cit. 2022-07-25]. Dostupné z: https://towardsdatascience.com/auto-encoder-what-is-it-and-what-is-it-used-for-part-1-3e5c6f017726.

44. KAMPAKIS, Stylianos. *What is anomaly detection, and why you need it.* [online]. 2020-02. [cit. 2022-06-13]. Dostupné z: https://thedatascientist.com/anomaly-detection-why-you-need-it/.

45. WALD, Abraham. *Sequential analysis*. New York; London: J. Wiley & Sons ; Chapman & Hall, 1947. Dostupné také z: http://archive.org/details/in.ernet.dli.2015.90255. OCLC: 529524.

46. *Keeping the Process on Target: CUSUM Charts* [BPI Consulting] [online]. 2014-08-29. [cit. 2022-07-24]. Dostupné z: https://www.spcforexcel.com/knowledge/variable-control-charts/keeping-process-target-cusum-charts.

47. LIU, Fei Tony et al. Isolation Forest. In: *2008 Eighth IEEE International Conference on Data Mining* [online]. Pisa, Italy: IEEE, 2008-12, s. 413–422 [cit. 2022-06-16]. ISBN 978-0-7695-3502-9. Dostupné z DOI: 10.1109/ICDM.2008.17.

48. DLOUHÝ, Martin; FIALA, Petr. *Úvod do teorie her*. 2. vydání. Praha: Oeconomica, 2009. ISBN 978-80-245-1609-7.

49. COURNOT, Antoine-Augustin. *Recherches sur les principes mathématiques de la théorie des richesses* [online]. Paris: L. Hachette, 1838 [cit. 2022-03-18]. Dostupné z: http://gallica.bnf.fr/ark:/12148/bpt6k6117257c.

50. VON NEUMANN, John. Zur Theorie der Gesellschaftsspiele. *Mathematische Annalen* [online]. 1928-12-01, Jg. 100, Nr. 1, s. 295–320 [cit. 2022-03-18]. ISSN 1432-1807. Dostupné z DOI: 10.1007/BF01448847.

51. VON NEUMANN, John; MORGENSTERN, Oskar. *Theory of games and economic behavior* [online]. Princeton: Princeton University Press, 1944 [cit. 2022-03-18]. Dostupné z: https://jmvidal.cse.sc.edu/library/neumann44a.pdf.

52. NISAN, Noam et al. (ed.). *Algorithmic Game Theory* [online]. 1. vyd. Cambridge University Press, 2007-09-24 [cit. 2022-05-13]. ISBN 978-0-521-87282-9 978-0-511-80048-1. Dostupné z DOI: 10.1017/CBO9780511800481.

53. CHVOJ, Martin. *Pokročilá teorie her ve světě kolem nás*. Praha: Grada, 2013. ISBN 978-80-247-4620-3.

54. OSBORNE, Martin J.; RUBINSTEIN, Ariel. *A course in game theory* [online]. Ve spol. s LIBRARY GENESIS. Cambridge, Mass. : MIT Press, 1994 [cit. 2022-05-13]. ISBN 978-0-262-15041-5 978-0-262-65040-3. Dostupné z: https://arielrubinstein.tau.ac.il/books/GT.pdf.

55. SELTEN, Reinhard. The chain store paradox. *Theory and Decision* [online]. 1978-04, vol. 9, no. 2, s. 127–159 [cit. 2022-05-26]. ISSN 0040-5833, ISSN 1573-7187. Dostupné z DOI: 10.1007/BF00131770.

56. WILCZYŃSKI, Andrzej et al. Stackelberg Security Games: Models, Applications and Computational Aspects. *Journal of Telecommunications and Information Technology* [online]. 2016-09-30, roč. 3, s. 70–79 [cit. 2022-07-28]. Dostupné z: https://www.researchgate.net/publication/308937195_Stackelberg_Security_Games_Models_Applications_and_Computational_Aspects.

57. MOHER, David et al. Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *Journal of Clinical Epidemiology* [online]. 2009-10-01, roč. 62, č. 10, s. 1006–1012 [cit. 2022-05-30]. ISSN 0895-4356, ISSN 1878-5921. Dostupné z DOI: 10.1016/j.jclinepi.2009.06.005.

58. PAGE, Matthew J. et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ* [online]. 2021-03-29, vol. 372, n71 [cit. 2022-05-30]. ISSN 1756-1833. Dostupné z DOI: 10.1136/bmj.n71.

59. ANTWARG, Liat et al. Explaining anomalies detected by autoencoders using Shapley Additive Explanations. *EXPERT SYSTEMS WITH APPLICATIONS* [online]. 2021-12-30, roč. 186 [cit. 2022-06-18]. ISSN 0957-4174. Dostupné z DOI: 10.1016/j.eswa.2021.115736.

60. ARFAOUI, Amel et al. Game-based adaptive anomaly detection in wireless body area networks. *COMPUTER NETWORKS* [online]. 2019-11-09, roč. 163 [cit. 2022-06-18]. ISSN 1389-1286. Dostupné z DOI: 10.1016/j.comnet.2019.106870.

61. BULLA, C.; BIRJE, M.N. Improved data-driven root cause analysis in fog computing environment. *Journal of Reliable Intelligent Environments* [online]. 2021 [cit. 2022-06-19]. Dostupné z DOI: 10.1007/s40860-021-00158-x.

62. CINQUE, Marcello et al. Security Log Analysis in Critical Industrial Systems Exploiting Game Theoretic Feature Selection and Evidence Combination. *IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS* [online]. 2020, roč. 16, č. 6, s. 3871–3880 [cit. 2022-06-19]. ISSN 1551-3203. Dostupné z DOI: 10.1109/TII.2019.2944477.

63. GHAFOURI, Amin et al. A game-theoretic approach for selecting optimal time-dependent thresholds for anomaly detection. *AUTONOMOUS AGENTS AND MULTI-AGENT SYSTEMS* [online]. 2019, roč. 33, č. 4, s. 430–456 [cit. 2022-06-21]. ISSN 1387-2532. Dostupné z DOI: 10.1007/s10458-019-09412-2.

64. HUANG, Zhihong et al. Game Theory-Based Hyperspectral Anomaly Detection. *IEEE TRANSACTIONS ON GEOSCIENCE AND REMOTE SENSING* [online]. 2020-04, roč. 58, č. 4, s. 2965–2976 [cit. 2022-06-21]. ISSN 0196-2892. Dostupné z DOI: 10.1109/TGRS.2019.2958359.

65. MARTAKIS, Panagiotis et al. A semi-supervised interpretable machine learning framework for sensor fault detection. *SMART STRUCTURES AND SYSTEMS* [online]. 2022-01, roč. 29, č. 1, s. 251–266 [cit. 2022-06-22]. ISSN 1738-1584. Dostupné z DOI: 10.12989/sss.2022.29.1.251.

66. MISHRA, Birendra; SMIRNOVA, Inna. Optimal configuration of intrusion detection systems. *INFORMATION TECHNOLOGY & MANAGEMENT*

[online]. 2021-12, roč. 22, č. 4, s. 231–244 [cit. 2022-06-22]. ISSN 1385-951X. Dostupné z DOI: 10.1007/s10799-020-00319-z.

67. NESHENKO, Nataliia et al. A behavioral-based forensic investigation approach for analyzing attacks on water plants using GANs. *FORENSIC SCIENCE INTERNATIONAL-DIGITAL INVESTIGATION* [online]. 2021-09, roč. 37 [cit. 2022-06-23]. Dostupné z DOI: 10.1016/j.fsidi.2021.301198.

68. RANI, Rinki et al. Trust Evaluation for Light Weight Security in Sensor Enabled Internet of Things: Game Theory Oriented Approach. *IEEE INTERNET OF THINGS JOURNAL* [online]. 2019, roč. 6, č. 5, s. 8421–8432 [cit. 2022-06-23]. ISSN 2327-4662. Dostupné z DOI: 10.1109/JIOT.2019.2917763.

69. SARAEIAN, Shideh; SHIRAZI, Babak. Process mining-based anomaly detection of additive manufacturing process activities using a game theory modeling approach. *COMPUTERS & INDUSTRIAL ENGINEERING* [online]. 2020-08, roč. 146 [cit. 2022-06-25]. ISSN 0360-8352. Dostupné z DOI: 10.1016/j.cie.2020.106584.

70. SEDJELMACI, H. et al. An accurate security game for low-resource iot devices. *IEEE Transactions on Vehicular Technology* [online]. 2017, roč. 66, č. 10, s. 9381–9393 [cit. 2022-06-26]. Dostupné z DOI: 10.1109/TVT.2017.2701551.

71. SUBBA, Basant et al. A Game Theory Based Multi Layered Intrusion Detection Framework for Wireless Sensor Networks. *INTERNATIONAL JOURNAL OF WIRELESS INFORMATION NETWORKS* [online]. 2018-12, roč. 25, č. 4, s. 399–421 [cit. 2022-06-26]. ISSN 1068-9605. Dostupné z DOI: 10.1007/s10776-018-0403-6.

72. WANG, Bizhu et al. Loose Game Theory Based Anomaly Detection Scheme for SDN-Based mMTC Services. *IEEE ACCESS* [online]. 2019, roč. 7, s. 139350–139357 [cit. 2022-06-27]. ISSN 2169-3536. Dostupné z DOI: 10.1109/ACCESS.2019.2943056.

73. WU, Hao; WANG, Zhonghua. Multi-source fusion-based security detection method for heterogeneous networks. *COMPUTERS & SECURITY* [online]. 2018-05, roč. 74, s. 55–70 [cit. 2022-06-28]. ISSN 0167-4048. Dostupné z DOI: 10.1016/j.cose.2018.01.003.

74. WU, Hao; WANG, Wei. A Game Theory Based Collaborative Security Detection Method for Internet of Things Systems. *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY* [online]. 2018, roč. 13, č. 6, s. 1432–1445 [cit. 2022-06-28]. ISSN 1556-6013. Dostupné z DOI: 10.1109/TIFS.2018.2790382.

75. YAN, Chao et al. Database Audit Workload Prioritization via Game Theory. *ACM TRANSACTIONS ON PRIVACY AND SECURITY* [online]. 2019, roč. 22, č. 3 [cit. 2022-06-28]. ISSN 2471-2566. Dostupné z DOI: 10.1145/3323924.

76. YANG, L. et al. Robust detection of false data injection attacks for data aggregation in an Internet of Things-based environmental surveillance. *Computer Networks* [online]. 2017, roč. 129, s. 410–428 [cit. 2022-06-29]. Dostupné z DOI: 10.1016/j.comnet.2017.05.027.

77. YANG, Liu et al. An Evolutionary Game-Based Secure Clustering Protocol With Fuzzy Trust Evaluation and Outlier Detection for Wireless Sensor Networks. *IEEE SENSORS JOURNAL* [online]. 2021-06-15, roč. 21, č. 12, s. 13935–13947 [cit. 2022-06-29]. ISSN 1530-437X. Dostupné z DOI: 10.1109/JSEN.2021.3070689.

78. GOPINATH, Divya. *The Shapley Value for ML Models* [Medium] [online]. 2021-10-26. [cit. 2022-07-28]. Dostupné z: https://towardsdatascience.com/the-shapley-value-for-ml-models-f1100bff78d1.

Univerzita Hradec Králové
Fakulta informatiky a managementu

Zadání diplomové práce

Autor:	**Bc. Dominik Búzik**
Studium:	I2000031
Studijní program:	N1802 Aplikovaná informatika
Studijní obor:	Aplikovaná informatika
Název diplomové práce:	**Využití teorie her k detekci anomálií**
Název diplomové práce AJ:	Game-Theoretic Approaches for Anomaly Detection

Cíl, metody, literatura, předpoklady:

Cílem práce je popsat a zhodnotit možnosti uplatnění teorie her ve vybrané aplikační oblasti (detekce anomálií v datech).

Osnova:
1.Úvod
2.Teoretická část
2.1. Datová věda
2.2. Teorie her
2.3. Metodika PRISMA
3. Praktická část
3.1. Stanovení výzkumných otázek
3.2. Systematická rešerše
4. Výsledky
5. Závěr

Page, M.J., McKenzie, J.E., Bossuyt, P.M. et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. Syst Rev 10, 89 (2021). https://doi.org/10.1186/s13643-021-01626-4
Nisan, N., Roughgarden, T., Tardos, E., & Vazirani, V. (Eds.). (2007). Algorithmic Game Theory. Cambridge: Cambridge University Press. doi:10.1017/CBO9780511800481

Zadávající pracoviště:	Katedra informačních technologií, Fakulta informatiky a managementu
Vedoucí práce:	doc. RNDr. Kamila Štekerová, Ph.D., MSc.
Oponent:	Ing. Marek Zanker
Datum zadání závěrečné práce:	9.9.2021