Jak umělá inteligence (AI) ovlivňuje bezpečnost

Moláčková Nikola

Bakalářská práce
2024

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav bezpečnostního inženýrství

Akademický rok: 2023/2024

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Nikola Moláčková**
Osobní číslo:	**A21030**
Studijní program:	**B1032A020001 Bezpečnostní technologie, systémy a management**
Forma studia:	**Prezenční**
Téma práce:	**Jak umělá inteligence (AI) ovlivňuje bezpečnost**
Téma práce anglicky:	**How artificial intelligence (AI) affects security**

Zásady pro vypracování

1. Specifikujte oblasti bezpečnosti, které již využívají prvky umělé inteligence.
2. Popište jednotlivé hrozby a rizika spojená s využitím umělé inteligence.
3. Na modelových příkladech definujte přínosy a rizika využití umělé inteligence.
4. Definujte příležitosti využití nových poznatků z umělé inteligence v oblastech bezpečnosti.
5. Zpracujte soubor doporučení pro zaměstnance a zaměstnavatele, jak využít umělé inteligence ke svému prospěchu, a také jak předcházet hrozbám, které souvisí s umělou inteligencí.

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

Seznam doporučené literatury:

1. Vladimír Smejkal. Kybernetická kriminalita (3. vydání). Vydavatelství a nakladatelství Aleš Čeňek, s.r.o., 2022
2. Luděk Lukáš a kolektiv. Bezpečnostní technologie, systémy a management III. Radim Bačuvčík – VeRBuM. 2013
3. Luděk Lukáš a kolektiv. Bezpečnostní technologie, systémy a management IV. Radim Bačuvčík – VeRBuM. 2014
4. Sojka. Hashdork. Umělá inteligence v kybernetické bezpečnosti. Publikováno 11-09-2022. Dostupné z: https://hashdork.com/cs/artificial-intelligence-in-cybersecurity/, citace [9.11.2023]
5. Evropský parlament. Akt EU o umělé inteligenci: První nařízení o AI na světě. Publikováno 14-06-2023. Dostupné z: https://www.europarl.europa.eu/news/cs/headlines/society/20230601STO93804/akt-eu-o-umele-inteligenci-prvni-narizeni-o-ai-na-svete, citace [9.11.2023]

Vedoucí bakalářské práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **8. prosince 2023**
Termín odevzdání bakalářské práce: **28. května 2024**

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
DĚKAN
L.S.

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

Ing. Jan Valouch, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 8. prosince 2023

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 25.7.2024

Nikola Moláčková v.r.
podpis studenta

ABSTRAKT

Abstrakt česky: Tato bakalářská práce se zaměřuje na vliv umělé inteligence (AI) na bezpečnost v různých kontextech. V současné době se implementace AI stává běžnou praxí napříč mnoha odvětvími, což přináší nejen významné přínosy, ale i potenciální rizika. Práce se zaměřuje na využití umělé inteligence (AI) v oblasti bezpečnosti, zkoumá potenciální přínosy a rizika spojená s touto technologií a nabízí doporučení pro její bezpečné a efektivní nasazení. Modelové příklady ukazují přínosy a rizika využití AI na konkrétních případech, jako je detekce kybernetických útoků pomocí hlubokého učení nebo autonomní drony používané k monitorování kritické infrastruktury. Práce také diskutuje příležitosti pro využití nových poznatků z AI v bezpečnostních aplikacích, zahrnující automatizaci bezpečnostních procesů a predikci hrozeb.

Klíčová slova: umělá inteligence, bezpečnost, implementace, přínosy, rizika, hrozby

ABSTRACT

Abstrakt ve světovém jazyce: This bachelor's thesis focuses on the impact of artificial intelligence (AI) on security in various contexts. Currently, the implementation of AI is becoming common practice across many industries, bringing not only significant benefits but also potential risks. The thesis examines the use of AI in the field of security, exploring the potential benefits and risks associated with this technology and offering recommendations for its safe and effective deployment. Model examples illustrate the benefits and risks of using AI in specific cases, such as detecting cyber attacks through deep learning or using autonomous drones to monitor critical infrastructure. The thesis also discusses opportunities for utilizing new AI insights in security applications, including the automation of security processes and threat prediction.

Keywords: artificial intelligence, security, implementation, benefits, risks, threats

Mé poděkování patří Ing. Davidu Malaníkovi, Ph.D. za odborné vedení, trpělivost a ochotu, kterou mi v průběhu zpracování bakalářské práce věnoval. Taktéž bych chtěla vyjádřit své díky panu Ing. Lukáši Kotkovi a paní Ing. Doře Kotkové, kteří mi ochotně pomáhali s analýzou rizik. V neposlední řadě děkuji své rodině za velkou podporu jak při studiu, tak při psaní této bakalářské práce.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Obsah

ÚVOD

Umělá inteligence (AI) se v posledních letech stává neoddělitelnou součástí mnoha průmyslových odvětví a její vliv na bezpečnostní sféru je značný. Tento fenomén, podpořený rostoucí schopností AI systémů zpracovávat a analyzovat velké objemy dat, vede k inovacím, které mohou významně přispět k ochraně kritických infrastruktur, kybernetické bezpečnosti a osobní bezpečnosti. V rámci této bakalářské práce se autorka zaměřuje na komplexní analýzu vlivu AI na bezpečnost v různých kontextech. Cílem je identifikovat jak přínosy, které mohou technologie AI přinést, tak rizika, jež jsou s jejich nasazením spojena.

Práce se nejprve věnuje teoretickému základu umělé inteligence, kde je představena její definice, typy a historický vývoj. Následuje přehled konkrétních aplikací AI v oblasti bezpečnosti, včetně kybernetické bezpečnosti, fyzické bezpečnosti a národní bezpečnosti. V těchto kapitolách jsou rozebírány reálné příklady využití AI, jako je detekce kybernetických útoků pomocí strojového učení, autonomní dohledové systémy a predikce hrozeb pomocí hlubokého učení. Důležitou částí práce je také analýza potenciálních hrozeb a rizik, které mohou vyplývat z nesprávného nebo neopatrného nasazení AI technologií. Autorka se zde věnuje nejen technickým rizikům, ale i etickým otázkám, jako je diskriminace, předsudky v datech a problém transparentnosti rozhodovacích procesů AI.

Konečným cílem této práce je nabídnout doporučení pro bezpečné a efektivní nasazení AI v bezpečnostních aplikacích. Na základě teoretických znalostí i praktických příkladů autorka navrhuje strategie, které mohou organizace použít k minimalizaci rizik a maximalizaci přínosů AI technologií. Tato doporučení jsou klíčová pro vytvoření rámce, který zajistí, že AI bude implementována způsobem, který je nejen technicky pokročilý, ale i eticky odpovědný a bezpečný.

I. TEORETICKÁ ČÁST

1 ÚVOD DO UMĚLÉ INTELIGENCE

Stejně jako v počátcích internetu a Bluetooth, kdy lidé rychle začali tyto technologie používat, nyní rychle roste počet uživatelů implementujících AI do chytrých domácností a firemních systémů. Propojování komunikačních technologií, jako jsou Bluetooth, WiFi, LAN, WAN a internet, spolu s rostoucím využíváním cloudových služeb a IoT, znamená, že vše je propojeno – od kávovarů až po televize a chytré osvětlení. S tímto nárůstem užívání AI však roste i riziko, protože implementace AI do těchto zařízení zvyšuje potenciální bezpečnostní hrozby.[1]

Umělá inteligence (AI) je stěžejním tématem dnešní doby a již mnoho odborníků si myslí, že se jedná o budoucnost informačních technologií. Vědci a inženýři dlouhodobě pracují na vývoji inteligentních systémů, které dokážou napodobovat kognitivní schopnosti člověka. Cílem je vytvořit programy a stroje, jež budou schopné se učit, poznávat a poskytovat chytrou asistenci v široké škále aplikací. Umělá inteligence už dnes například pomáhá ve zdravotnictví se správnou diagnózou, ve finančním odvětví s analýzou dat a řízením investic nebo v marketingu s tvořením nejrůznějších textů. Oborů, kde se umělá inteligence objevuje je čím dál tím více a její implementace do nejrůznějších systémů je dnes běžná. Díky svým schopnostem rychle se učit z dat a pružně reagovat na nové podněty, nachází čím dál širší uplatnění. Systémy založené na umělé inteligenci dokážou analyzovat obrovské množství dat, rozpoznávat vzory a na jejich základě přijímat rychlá a efektivní rozhodnutí. To vede k inovacím a zvyšování efektivnosti v mnoha oblastech lidské činnosti. Pojem výpočetní stroj se objevil již v roce 1940, avšak reálné výsledky se objevily až ve druhé polovině 20. století. [2] Od té doby se setkáváme se spoustou milníků a pokroků, hlavně kvůli vynálezu a rychlému vývoji počítačů a počítačových systémů.[2]

1.1 Definice umělé inteligence

Jako první definice umělé inteligence se považuje tvrzení od jednoho ze zakladatelů, který ji popsal jako: *„vědu o výrobě strojů, která by dělala věci, které by vyžadovaly inteligenci, kdyby ji dělali lidé*“.[2] Jádro této definice nemá daleko k pravdě, avšak se musí přizpůsobit dnešnímu světu a jeho požadavkům.[2][3]

Umělá inteligence (AI) je schopnost strojů napodobovat ne-li předčit, lidské schopnosti, jako je učení se, uvažování, plánování, tvoření a podobně. Jejím cílem je umožnit technickým systémům reagovat **v reálném čase** na nejrůznější podněty, jež mu zadá uživatel (či jiný

vstup – kamera, senzor apod.) a řešit na základě těchto vstupů problémy, dosahovat konkrétních cílů či automatizovat procesy. Na základě těchto vstupů je umělá inteligence poté schopna maximalizovat šance na úspěšný a správný výstup – dále také interpretovat a analyzovat tato data pro budoucí učení a přizpůsobení se.[3]

1.2 Typy umělé inteligence

1. Úzká umělá inteligence (ANI)

Artificial narrow inteligence je druh umělé inteligence, která dnes existuje a běžně se používá, známá také jako „slabá“ umělá inteligence. Ačkoli úzké AI mohou být řízeny složitými a vysoce komplexními algoritmy a neuronovými sítěmi, jsou stále individuálně zaměřené na konkrétní cíle (mohou zpracovávat široké spektrum dat a úloh, ale pouze pro specifický účel nebo cíl). Příkladem úzké umělé inteligence může být rozpoznávání obličejů, vyhledávání na internetu nebo samořídící auta. ANI je klasifikována jako slabá nikoliv proto, že by měla málo prostoru nebo moci, ale protože ještě není tak dobrá jako celkové myšlení člověka.[2] Filozof John Searle popisuje úzkou AI jako *„užitečnou pro testování hypotézy mysli, ale ve skutečnosti by to nebyla mysl“*.[2]

2. Umělá inteligence (AGI)

Artificial general inteligence by na rozdíl od ANI měla být schopna vykonávat všechny intelektuální úkoly, které může dělat člověk. AGI je také schopna se učit ze zkušeností, rozpoznávat vzorce, ale má schopnost to posunout na vyšší úroveň – je schopna extrapolovat (přiblížit se k hodnotám a informacím mimo její rozsah dat) znalosti přes jiné úkoly a situace, které již ovládá. Jinak řečeno, je schopna se přizpůsobovat neznámým úkolům a situacím. K něčemu takovému je ale třeba superpočítač jako je Summit Supercomputer, který jako jeden z mála ukazuje AGI. Tento počítač dokáže za jednu sekundu provést 200 kvadrilionových výpočtů (čehož by člověk byl schopen až za milion let). Pro superpočítače je ale třeba obrovská výpočetní kapacita, která existuje jen na superpočítačových úrovních, a proto se s AGI běžně nesetkáme.[2]

3. **Umělá inteligence (ASI)**

Artificial super inteligence je pro dnešní dobu zatím sci-fi, ale ne nereálná záležitost. Jde o umělou inteligenci, která je plně samostatná a uvědomuje si samu sebe. Je schopna předčit lidské schopnosti, napodobit jakékoliv lidské chování a důležité říci – je schopna ovlivnit budoucnost lidstva.[2] Jak pravil Stephen Hawking: „*Vzhledem k velkému potenciálu umělé inteligence je důležité prozkoumat, jak ji využít a zároveň se vyhnout potenciálním nástrahám.“*.[2]

1.3 Historie umělé inteligence

Historie umělé inteligence je velmi rozmanitá, a ačkoliv se to bude zdát nemožné, sahá až do roku 1920. V tomto roce poprvé zazněl pojem robot, a to ve vědecko-fantastickém dramatu R.U.R od Karla Čapka. V této době se zdál pojem robot a umělá inteligence jako velmi vzdálená a občas až nemožná budoucnost. Už ale o pár let později se začalo hovořit o pojmu univerzální (výpočetní) stroj, který vyřknul britský matematik a logik Alan Turing, jež tímto oficiálně odstartoval éru umělé inteligence. V roce 1950 pan Turing položil otázku „Mohou stroje myslet?“ a tím vstoupil do světa filozofie a kognitivních věd. Na otázku se ovšem nesnažil odpovědět přímo a místo toho vytvořil experiment pojmenovaný Turingův test, kterým později hodnotil inteligentní stroje.[4][5][6]

Pojmy umělá inteligence a strojové učení byly poprvé použity v roce 1956 na Dartmouthské konferenci, přičemž byl tento moment označen za oficiální začátek umělé inteligence. Na této konferenci se skupina vědců začala poprvé zaobírat tématem strojové učení a AI. Právě na této konferenci se objevila hlavní osobnost té doby profesor matematiky a zakladatel dvou významných laboratoří na vývoj umělé inteligence John McCarthy, někdy přezdívaný jako otec oboru AI, který se věnoval několika výzkumům spolu s dalšími (jako například Marvin Minsky, Allen Newel, Herbert Simon, či John von Neumann) několik desítky let.[7] Přínos této konference shrnul profesor Josef Kelemen větou: *„Na tomto setkání mladých nadšenců, kteří měli do té doby umělou inteligenci spíše jako koníčka než jako seriózní vědeckou a technickou disciplínu, navíc se jí zabývali izolovaně, znamenal seminář nejenom konstituci jejich oboru a jeho profesionalizaci, nýbrž i možnost začít s koordinovanými aktivitami.“*.[7]

V roce 1960 byl postaven první počítač využívající strojové učení MENACE, který byl sestrojen Donaldem Michiem z 304 krabiček od sirek, jež využíval náhodnou strategii a později se naučil, jak nad člověkem vyhrát. O 6 let později vzniká první konkrétní aplikace,

která byla založena právě na konceptech umělé inteligence, sebe učení a neuronové síti. První takovou aplikací, kterou bychom dnes mohly nazvat chatgpt byla ELIZA – psychoterapeutický simulátor vytvořen Josephem Winogradem založený na chytrém sytému pravidel.[4][5][6][8]

V roce 1972, se sice tehdejší AI dostala do světa medicíny a překladů, ve kterých je dodnes, avšak tyto systémy se zabývaly pouze řešením složitých matematických problémů. Proto jsou sedmdesátá léta označena jako „AI zima" – v této době začal úpadek výzkumů zabývající se umělou inteligencí především z důvodu nedostatku financí a výpočetní techniky (kvůli nedostatečné paměťové kapacitě). Toto období úpadku a skeptičnosti umělé inteligence trvalo (až na pár světlých momentů) do 90. let. AI zima sice zpomalila, téměř zastavila výzkum, ale zároveň otevřela světu možnosti hledání nových cest, sebereflexe a myšlenek, které přinesly základ pro novou éru umělé inteligence, jež přišla v následujících letech.[4][5][6]

Rok 1997 je začátkem období rozkvětu umělé inteligence z důvodu příchodu prvního superpočítače od firmy IBM s názvem Deep Blue. Právě v tomto roce byl Deep Blue schopen analyzovat více než 200 milionů tahů za sekundu a tím porazit tehdejšího světového šampiona v šachu Garryho Kasparova.[4][5][6]

Jaro, tak by se dala nazvat léta po roce 2000. Započalo období rychlého vývoje, optimismu a pokroku. Začátkem nového tisíciletí započaly časy průlomů, které umělou inteligenci znovu vyzdvihly do popředí technologického vývoje. V té době se zde začaly objevovat nové algoritmy jako například SVM (Support Vector Machines), které využíváme dodnes na rozpoznání psaného textu či klasifikaci obrázků. Poté už byl vývoj všemožných aplikací jen v rozkvětu. Japonská firma Sony uvedla na trh domácího mazlíčka AIBO, jež byl schopen reagovat na více než sto hlasových příkazů. Hned poté v roce 2005 započal trend samořídících automobilů, které na trh uvedla automobilka Stanley. Poté Apple uvedl svého dones populárního asistenta Siri.[4][5][6]

Éra, která probíhala mezi lety 2000-2020 se nazývá éra hlubokého učení, jehož vzestup začal primárně v roce 2012, protože firma AlexNet přišla s metodou prvních umělých neuronových sítí a tím dala najevo zastaralost do té doby nenahraditelnému strojovému učení. Ani ne o 3 roky později se teorie neuronových sítí a hlubokého učení potvrdila, a to programem AlphaGo od Google DeepMind, která porazila světového šampiona Lee Sedola v čínské hře Go.[9] Od té doby byly představeny nejrůznější programy, hry a stroje, které právě

hlubokého učení a neuronových sítí využívalo. Díky těmto pokrokům je umělá inteligence dnes nedílnou součástí našich každodenních životů a nastávají zde větší a větší otázky bezpečnosti. Samozřejmě ale AI spolu se svými riziky přináší řadu výhod a umožňuje technologický pokrok v mnoha oborech. [4][5][6]

1.4 Turingův test

Turingův test, který je pojmenován po jeho autorovi, je test, který spočívá v konverzaci mezi strojem a člověkem. V tomto testu si lidský tazatel povídá se subjektem A a subjektem B, zatímco jeden z nich je stroj a druhý člověk. Pokud se tazateli nepovede posoudit, zda hovoří se strojem, test bude úspěšný a naopak. Argumentem v tomto testu je fakt, že pokud se stroji povede být nerozeznatelný od člověka, dosáhl lidské inteligence.[4][5][6][11]

Tento test měl za úkol ovlivnit pohled na vědomí strojů a také podstatu inteligence. Inteligentní stroj můžeme považovat za inteligentní pokud, zjednodušeně řečeno, jeho odpovědi na různorodé otázky nedokážeme odlišit od odpovědí člověka. Princip Turingova testu je velmi jednoduchý a probíhá tak, že do oddělených místností umístíme testujícího člověka a také stroj (počítač), který chceme ohodnotit pomocí Turingova testu a do druhé místnosti tazatele. Tazatel posílá otázky směřující na stroj a člověka a jeho úkolem je posoudit, s kým konverzuje. Odpovědi se poté vrátí tazateli v tištěné (neutrální) formě a jak již bylo uvedeno, pokud se podaří určit, zda konverzace proběhla se strojem či člověkem, pak je Turingův test úspěšný. [4][5][6][11]

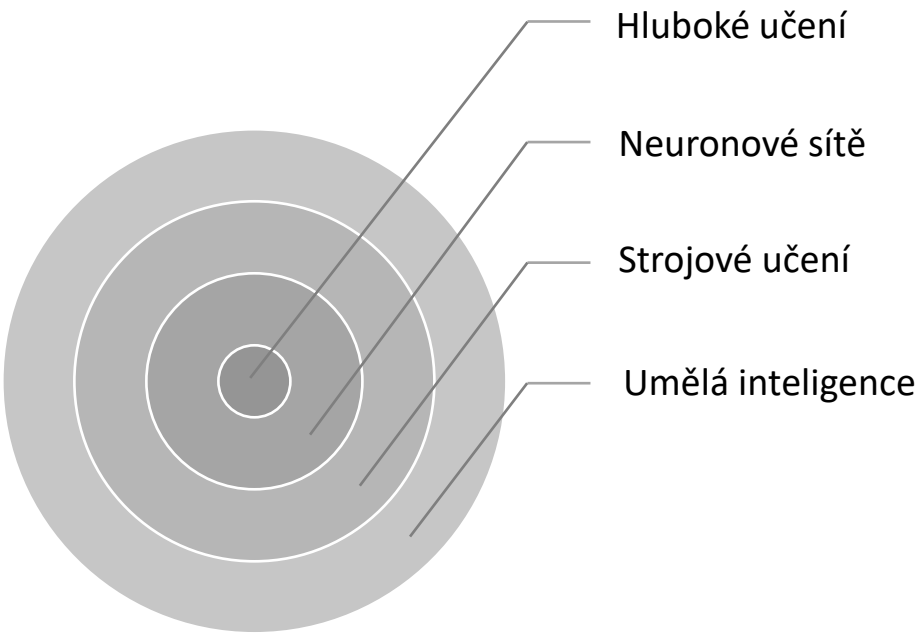
1.5 Základní pojmy umělé inteligence

V této kapitole budou popsány základní pojmy a principy umělé inteligence pro pochopení umělé inteligence jako celku. Kapitola bude sloužit jako přehled nejdůležitějších definic a konceptů, které formulují základní stavební kameny, na nichž stojí současná i budoucí řešení AI včetně strojového učení, neuronových sítí, algoritmů a podobně.

Prvním důležitým pojmem je **model umělé inteligence** – model AI je matematický nebo statický model, založený na algoritmech strojového učení, neuronových sítích nebo jiných výpočetních metodách, který simuluje konkrétní chování lidské inteligence – zpracovává data, učí se z nich a poté provádí úkoly, které by jinak vyžadovaly lidskou inteligenci.

1.5.1 Strojové učení (Machine Learning)

Strojové učení umožňuje AI modelům učit se na základě vstupních dat nebo předešlých výstupů, a to bez nutnosti programování. AI si ukládá algoritmy a předešlé zkušenosti, uspořádá je do souvislostí a poté vyhodnotí (typicky k tomu využívá služeb cloud). Při těchto postupech se zpracovává pro člověka nemyslitelné množství dat, které AI přinesou zcela nový pohled – příkladem může být využití ML pro e-shopy, kdy AI porovnává a pozoruje chování zákazníků, přičemž je potom schopna odvodit například další produkt, který by si zákazník mohl koupit. Tyto znalosti dokáže ML rozšiřovat a zlepšovat i bez lidské pomoci, avšak s nimi samo o sobě neumí pracovat – o to se stará AI, která přijaté poznatky aplikuje do praxe. Strojové učení je tedy nástrojem umělé inteligence, která jí pomáhá se orientovat ve světě a umožňuje jí se učit z nabytých poznatků. Je důležité říci, že AI modely jsou schopny automatizovaně vykonávat úkoly, rozhodovat se a optimalizovat svůj výkon v čase, pouze pokud jsou schopné machine learning (ML). Zatímco všechny ML modely jsou považovány za AI, ne všechny AI obsahují ML. Na obrázku číslo 1 je vidět vztah mezi umělou inteligencí, strojovým učením a hlubokým učením, které bude popsáno níže v textu.[11][12][13][14]



Obrázek 1 Vztah mezi AI, ML, ANN, DL [vlastní]

Aplikace strojového učení nám poskytují nesmírnou řadu možností pro její využití a otvírají dveře k mnoha možným inovacím v nejrůznějších oblastech. Například rozpoznání obrazu, jež pracuje na základě strojového učení, se stalo zásadním v mnoha oblastech bezpečnosti – **veřejná bezpečnost a dozor** (monitorování veřejných prostorů a analýza chování osob s možností identifikace podezřelé osoby), **bezpečnostní kontroly na letištích** (využití pro automatické skenování a hledání nebezpečných předmětů v zavazadlech), **kontrola přístupu** (biometrické ověřování osob), **forenzní analýzy** (identifikace podezřelých a obětí na základě fotografií či videí), **obrana a vojenský sektor** (identifikace cílů, analýza satelitních a leteckých snímků), **kybernetická bezpečnost** (detekce a prevence online podvodů – phishing) a mnoho dalších. Dalším využitím ML, konkrétně rozpoznání obrazu, je AI technologie pro **zdravotnictví** (analýza snímků RTG apod.). Dalším příkladem je **zpracování přirozeného jazyka** (NLP) a chatboti, kteří hrají klíčovou roli v zjednodušení, zrychlení a zefektivnění práce s texty. NLP umožňuje počítačům analyzovat a interpretovat lidský jazyk, což vede k vývoji pokročilých chatbotů a digitálních asistentů. Tyto technologie mohou automaticky odpovídat na dotazy zákazníků, analyzovat sentiment v textech, a dokonce generovat textový obsah. Výsledkem je výrazné zlepšení v komunikaci s uživateli, efektivnější zpracování velkých objemů textových dat a zvýšená produktivita v různých oblastech, od zákaznické podpory po analýzu dat. Vše uvedené jsou pouze základní příklady a je třeba si uvědomovat, mimo všechny výhody, které AI přináší, také řadu možných hrozeb a problémů, které sebou implementace AI může přinést. [10][15][16]

Jak strojové učení funguje? Během trénování modelu vstupními daty (trénovací data) je umělé inteligenci zadán taktéž výstup, aby si ho AI spojila s konkrétním vstupem (anotovaná data – označení dat) - to umožňuje modelu reagovat na neznámé vstupy, protože si je schopen nalézt podobnosti. Algoritmy modelů strojového učení jsou navrženy tak, aby byly schopny klasifikovat věci, předpovídat výsledky a hledat vzorce.[14]

Dle požadovaného výsledku a v závislosti na povaze dat můžeme využít jeden ze čtyř učebních modelů – **s dohledem**, **bez dohledu** a **zesilovací model** (učení se posilováním).[14]

Model s dohledem: V této metodě je stroj učen pomocí příkladů dat, které označuje učitel, kde každý vstup má přiřazený požadovaný výstup – ty určuje právě učitel a tím v podstatě navádí model ke správným odpovědím, aby je mohl později algoritmus vytvářet samostatně. Tyto algoritmy se využívají také tam, kdy je předvídaným výsledkem číslo – například rozpoznání SPAM e-mailu, předvídání počtu dopravních nehod nebo předvídání prodejní ceny pozemků na základě polohy, stavu, velikosti a podobně. Tato technika se nazývá **lineární**

regrese (dvě a více hodnot se navzájem ovlivňují). Jinými technikami pro tyto detekční algoritmy je klasifikační nebo shlukovací. Dalším příkladem může být požadavek, aby stroj rozeznal sedmikrásku od heřmánku – poskytneme mu dvojice obrázků těchto květin a označíme správnou identifikaci. Stroj poté analyzuje tato tréninková data a začne rozpoznávat podobnosti, rozdíly a vzory, dokud není schopen odpovídat na složité otázky. Tato metoda je používána v běžných aplikacích, například v systémech pro doporučení produktů nebo v navigačních aplikacích jako Waze.[12][13][14]

Model bez dohledu: V učení bez učitele nejsou k dispozici správné odpovědi, což zcela odlišuje situaci od učení s učitelem. V tomto případě nelze model konstruovat na základě správných odpovědí v tréninkových datech, což komplikuje vyhodnocování jeho výkonnosti, protože není možné ověřit, zda je naučený model úspěšný. Typické metody učení bez učitele se zaměřují na učení určité "struktury", na které jsou data založena. To může zahrnovat vizualizaci, kde jsou podobné nebo stejné položky umístěny blízko sebe a odlišné položky dál od sebe, nebo klastrování, kdy se data používají k identifikaci skupin položek („klastrů“), které jsou podobné, ale jsou různé od dat v klastrech jiných. Příkladem může být analýza zákazníků v supermarketu – využití zákaznických kartiček pro kategorizování oblíbených produktů apod.[12][13][14]

Dalším učením bez učitele se nazývá **generativní modelování** – tyto modely se učí pravidla a statistiky a jsou poté schopny na základě vstupních dat generovat data nová (například obrázky), která jsou podobná těm, na kterých model trénoval. Tato technika je využívána v oblastech **GANs** (Generativní Adversariální sítě) – typ umělé neuronové sítě, která se skládá z generátoru a diskriminátoru. Sítě jsou navrženy tak, aby spolu soupeřily a tím se realisticky učily novým znalostem.[12][13][14]

Zesilovací model: Na rozdíl od učení s dohledem, kde stroj dostává správné odpovědi a učí se korelacím mezi nimi, posilované učení nepoužívá klíč k odpovědi. Místo toho se zaměřuje na soubor možných akcí, pravidel a konečných stavů. Když je cíl algoritmu pevný nebo binární, mohou se stroje učit pomocí příkladů. Avšak pokud je požadovaný výsledek proměnlivý, systém se musí učit zkušenostmi a odměnou. V posilovaném učení je "odměna" často numerická a je zapracována do algoritmu jako něco, co systém usiluje získat.[12][13][14]

Tento model je často přirovnáván k tomu, jak se někdo učí hrát šachy. Místo aby jim byly ukázány všechny možné tahy, jsou jim vysvětlena pravidla a dovednost si budují praxí. Odměny přicházejí v podobě vítězství ve hře a získání soupeřových kamenů. [14]

Je nutné upozornit na fakt, že umělá inteligence může dělat chyby a přesnost predikcí naučených pomocí ML se může lišit v tréninkových datech a v samotných testovacích datech – takzvaně se „přetrénovat“ (overfitting). To znamená, že se stroj snaží být až moc chytrý a vymýšlí si zvláštní pravidla, dokud nenajde takové, které přesně odpovídají trénovacím datům. Například umělé neuronové sítě požadují obrovské množství dat, aby poté byly schopny vygenerovat přesné prognózy.[12][13][14]

1.5.2 Hluboké učení a neuronové sítě

Hluboké učení je podmnožina strojového učení, která využívá pokročilé neuronové sítě – matematické modely, které jsou inspirovány lidským mozkem, a má obrovský dopad na lidský život. Hluboké učení zpracovává a interpretuje data hierarchicky, což vylepšuje výkonnost a hledání vzorců v různých oblastech. Často používaným algoritmem je sigmoidní funkce, kvadratická ztrátová funkce, křížová entropie (měří rozdíl mezi dvěmi pravděpodobnostními rozděleními), ReLu (Rectified Linear Unit) a tanh (hyperbolický tangens). Dalším důležitým algoritmem je **zpětné šíření chyby** – identifikace, oprava a následné poučení se z vlastních chyb. **Stochastický gradientní sestup** – neustálé updatování parametrů modelu pomocí vypočteného gradientu. To umožňuje minimalizaci chyb, efektivní a rychlé trénování modelu. Hluboké učení vyžaduje obrovské množství výpočetního výkonu, proto je nyní vývoj zaměřen na vývoj hardwaru a efektivnějších algoritmů. Výzkum je teď také zaměřen na vývoj metod, které umožní lepší **transparentnost** a **interpretaci** modelů, protože v oblastech jako je bezpečnost, právo či zdravotnictví, je kriticky důležitá spolehlivost. Mezi typy hluboce učících se modelů patří konvoluční neuronová síť (CNN), rekurentní neuronová síť (RNN), autoenkodéry, generativní konkurenční sítě (GAN). [17]

1.5.3 Zpracování přirozeného jazyka

Zpracování přirozeného jazyka (NLP, z anglického "Natural Language Processing") je technologie, která umožňuje počítačům porozumět lidské řeči tak, jak ji běžně používáme v každodenní komunikaci. NLP je klíčovým prvkem pro inteligentní domácí asistenty jako jsou Google Assistant, Siri od Apple, nebo Amazon Alexa. Tyto systémy dokáží přirozeně

komunikovat a reagovat na lidské dotazy díky využití NLP, což jim umožňuje nejen "číst" text, ale i učit se z něj a rozumět jeho kontextu a významu.[18][19]

NLP funguje tak, že kombinuje poznatky z lingvistiky a informatiky, aby vytvořil modely schopné analyzovat strukturu jazyka, rozpoznávat význam slov a frází a správně na ně reagovat. Tyto modely jsou trénovány na obrovských datech získaných také z internetové komunikace, což jim umožňuje adaptovat se na variabilitu v jazyce, včetně hovorových výrazů a slangových termínů.[18][19]

Jedním z praktických příkladů využití NLP je funkce autokorekce na našich telefonech, která nám pomáhá opravovat gramatické chyby a překlepy během psaní textových zpráv. Tato technologie neustále vylepšuje naše textové komunikace tím, že se učí z našich interakcí a přizpůsobuje se našemu stylu psaní.[18][19]

2 VYUŽITÍ UMĚLÉ INTELIGENCE V OBLASTECH BEZPEČNOSTI

Umělá inteligence se v bezpečnostních aplikacích využívá v různých formách, od detekce malwaru a phishingových útoků, přes monitorování síťového provozu a identifikaci anomálií, až po biometrické bezpečnostní systémy, jako je rozpoznávání obličeje nebo otisků prstů. Tyto systémy využívají algoritmy strojového učení k výraznému zlepšení schopnosti identifikovat a reagovat na bezpečnostní hrozby v reálném čase.

2.1.1 Kybernetická bezpečnost

První kapitolou bude popis oblastí kybernetické bezpečnosti, kde je možné využít (či už je využívána) umělá inteligence. Kybernetická bezpečnost se zabývá ochranou dat, sítí, zařízení a jiných informačních systémů a zahrnuje takové opatření, které brání tyto systémy proti útokům malware, ransomware, phishing a mnoho dalších. Bezpečnost kybernetického prostoru je důležitá pro ochranu soukromých dat, firemních informací, národních bezpečnostních zájmů apod. Skutečnost, že implementace do kybernetické sféry může být užitečná, avšak velmi nebezpečná je známý fakt, o kterém se mluví ve velmi malém měřítku. V této kapitole budou uvedeny veškeré oblasti informační a kybernetické bezpečnosti, ve kterých je možné použít technologie umělá inteligence a níže v práci bude k těmto oblastem přidán popis existujících a možných hrozeb či rizik.[1]

Prvním pozitivním vlivem v kybernetické bezpečnosti je využití kombinace AI a ML, která je schopná se učit z databáze již proběhlých útoků a tím rozeznat a detekovat obvyklé chování aplikace od útoků malware a následně na útoky navrhnout reakci (obranu). Toto usnadňuje práci bezpečnostním expertům, kteří se nemusí starat o staré a známé malware útoky a mohou se věnovat komplexnějším problémům spojených s ochranou kybernetické infrastruktury. Toto vede ke skutečnosti, že umělá inteligence dokáže tyto nové útoky pomáhat odhalit, protože vidí vzorce a varovné příznaky dříve než člověk a následně je způsobilá na navržení řešení pro obranu či dokonce predikci budoucí podoby útoků. Další výhodou, co se týče detekce malware, je možnost umělé inteligence nejen hledat malware jako celek, ale také je schopna se zaměřit na samotný základ každého programu – na jeho kód. V kódu je AI schopna posloužit jako nástroj kontroly a nalézt zranitelnosti již při vývoji.[16][20]

Právě tato schopnost umělé inteligence způsobuje revoluci ve vývoji aplikací, protože právě aplikace vždy čelily nejrůznějším bezpečnostním problémům od narušení soukromí, krádeže

dat, útoků malware po problémy s ověřením uživatelů. Ve fázi kódování je AI tedy využívána na detekci a předvídání potencionálních hrozeb a bezpečnostních chyb v programu, které by snadno mohli lidští vývojáři přehlédnout. K tomuto účelu je využívána aplikace DAST (Dynamic Application Security Testing), proces testování, který slouží právě pro detekci slabých míst a zranitelností v aplikacích. Na rozdíl od DAST, která simuluje útoky na běžících aplikacích SAST (Static Application Security Testing) analyzuje přímo zdrojový kód aplikace (tedy na kódu, který není spuštěný).[21]

Dalšími způsoby, jak může AI pomáhat vývojářům aplikací, a tak vlastně chránit uživatelská data proti zneužití či krádeži jsou následující: Automatická kontrola a analýza kódu; Sepsání doporučení pro nové bezpečnostní hrozby; Generování oprav; Modelování hrozeb (simulace) a analýza rizik; Přizpůsobení bezpečnostních protokolů (například správa relací, zálohování a šifrování dat, zabezpečení API nebo ověření a autentizace uživatelů); Monitoring celého procesu vývoje; Kontrola bezpečnostních standardů (GDPR, HIPPA, PCI DSS atd.); Zajištění kompatibility a účinnosti.[21]

Protože se zaměstnavatelé snaží chránit své sítě, systémy a jiná aktiva, aplikují systémy umělé inteligence pro odhalování a reakci na možné kybernetické hrozby. Systémy AI jsou schopny blokovat konkrétní IP adresy nebo ukončit podezřelé aktivity a relace. To umožňuje organizacím okamžitě přijmout proti těmto hrozbám opatření, zatímco by jiné bezpečnostní systémy neměly šanci reagovat stejně rychle.[22]

Mimo detekci hrozeb, je umělá inteligence schopna analyzovat rizika a přicházet s novými bezpečnostními strategiemi. Nástroje pro analýzu rizik jsou schopny analyzovat nesmírně velké množství dat o prostředí společnosti a na základě těchto dat dále vytvořit hodnocení rizik. Díky AI je proces hodnocení rizik mnohem rychlejší a efektivnější. Je možné posoudit pravděpodobnost a závažnost konkrétních rizik a organizace poté jen stanoví odpovídající způsoby pro ochranu konkrétních aktiv a minimalizaci nejzávažnějších rizik. Taktéž právě z důvodu možnosti analýzy obrovského množství dat, je AI schopna přijít na rizika, která by mohl člověk přehlédnout či je podcenit. Toto je užitečné pro organizace z důvodu zkrácení doby potřebnou pro analýzy, a tedy zkrácení doby pro zavedení protiopatření.[22]

Modely umělé inteligence se strojovým učením jsou mimořádné nástroje, které mimo to, že dokáží detekovat, reagovat a učit se z již existujících hrozeb, tak také dokáží rozpoznat složité vzorce, předvídat výstupy a časem být mnohem chytřejší. Dalším typickým příkladem využití strojového učení v informační bezpečnosti je **spamový filtr**. Tento filtr slouží

k filtrování nežádoucích (SPAM) e-mailů. Tato technologie se buď pomocí regesivní, klasifikační nebo shlukovací metody naučí vzory toho, jak nežádoucí e-mail vypadá a poté upozorňuje uživatele na možnou hrozbu. Také je tento algoritmus schopen předvídat a upozorňovat na phishingové útoky (e-mailové zprávy s cílem ukrást osobní soukromé informace jako jsou hesla, bankovní účty apod.) nebo pharming (odkaz například na bankovnictví je zaměněn za internetovou stránku útočníka, která má poté stejný cíl jako phishing).[22]

Výzvy a úvahy – Integrace umělé inteligence do vývojových nástrojů vyžaduje specializované dovednosti a zdroje – musí být zajištěna kompatibilita i účinnost kvůli náročnosti na výpočetní zdroje. Vývoj softwaru musí být vždy o krok napřed – AI se vyvíjí velmi rychle, ale stejně tak i kybernetičtí útočníci, to vyžaduje neustálou aktualizaci a přizpůsobení modelů umělé inteligence, aby byl systém schopen odolávat i novým a sofistikovanějším hrozbám. Důvěra v kvalitu dat a interpretace umělé inteligence – trénovací a testovací data musí být stoprocentní, nesmíme se spoléhat na něco, co nemusí dodat správný výsledek. Nákladnost na implementaci – ta může být velmi finančně náročná pro malé a střední firmy, je třeba tedy implementovat AI tam, kde je největší pravděpodobnost rizika, využít opensource nástrojů, partnerství s jinými vývojáři a podobně.[16][23]

Bodové shrnutí využití AI v kybernetické bezpečnosti:

1. Detekce, prevence a reakce na malware či kybernetické útoky;
2. Vývoj a kontrola aplikací – detekce a predikce potencionálních chyb přímo v kódu (minimalizace zranitelnosti), kontrola bezpečnostních standardů;
3. Ochrana dat, cloudu atd.
4. Analýza rizik

2.1.2 Fyzická (osobní) bezpečnost

Umělá inteligence se dá do fyzické bezpečnosti implementovat v různých kontextech a pro různé účely a již se stává její neoddělitelnou součástí. Jak již bylo řečeno, rozpoznání obrazu pomocí strojového učení je jednou z klíčových vlastností AI. CCTV jsou dnes běžnou součástí měst a dají se považovat za nejlevnější a nejvíce dostupnou metodu monitorování. Protože se technologie posouvá čím dál rychleji na nové úrovně, tak také kvalita kamerových systémů a jimi natáčeného obrazu jde kupředu. Tohoto se využívá v bezpečnostních kamerách. Moderní algoritmy umělé inteligence umožňují nejen pokročilou analýzu obrazů a videí, ale také detekci specifických vzorců chování a rozpoznávání osob. Tyto systémy jsou využívány k rozeznání neobvyklých aktivit nebo hrozeb v reálném čase, což umožňuje

rychlou reakci na nejrůznější bezpečnostní incidenty, jako například identifikace neobvyklých pohybů, zdržování v omezeném, zalidněném prostoru nebo upozornění na opuštěný podezřelý balíček, zavazadlo apod. Bezpečnostní kamery, které využívají strojového učení pro rozpoznání vzorců chování jsou takto poté schopny predikovat možný teroristický útok, rozeznat kriminalitu například v podobě únosů, krádeží, loupeží nebo organizovaných zločinů. Dále jsou tyto technologie také schopny rozeznávat hlasové či jiné zvukové vjemy jako je křik, rozbití okna apod. To umožňuje bezpečnostním složkám rychlou, a hlavně včasnou reakci na tyto události, které mohou mít také podobu přírodních katastrof (požáry, povodně aj.), či jiných známých mimořádných událostí (MU), které také AI dokáže na základě předešlých incidentů predikovat a také navrhovat včasné řešení v podobě evakuačních nebo jiných zásahových plánů. Technologie byla použita k řešení několika významných případů, včetně bombového útoku na bostonský maraton a teroristického útoku na londýnský most v roce 2017.[21][22][24][25]

Dalším významných využitím umělé inteligence je v systémech kontroly vstupu (SKV), kde pomocí biometrické autentizace chrání citlivé oblasti, prostory firem či jiných organizací. Tato technologie přináší vysokou úroveň zabezpečení a minimalizuje riziko neautorizovaného přístupu. Biometrická autentizace může mít podobu rozpoznání obličeje, otisku prstů, dlaně apod. Implementace AI do těchto systémů přináší přesnější funkcionalitu, pokud jsou systémy řádně chráněny.

Průzkum nebezpečných oblastní pomocí dronů či autonomních vozidel, které využívají technologií umělé inteligence, je další oblastí fyzické bezpečnosti, která nám umožní rychleji a efektivněji hledat hrozby. Tyto vozidla a drony jsou schopny proniknout do nebezpečných zón, kde by bylo příliš rizikové nasadit lidské pátrací týmy, jako například oblasti postižené přírodními katastrofami, zamořené toxickými látkami, radiací nebo v oblastech, kde je velké riziko ozbrojených konfliktů. Dále jsou tyto systémy schopny monitorovat hranice států a tím odhalovat nedovolené překročení, nelegální převoz zboží, či možný únik zločinců. Co se poté týče dopravní infrastruktury, AI přináší možnosti pro zvýšení bezpečnosti na silnicích. To znamená monitorování dopravních situací, identifikace rizikových míst nebo pomoc při řízení dopravního toku.[112][123]

Nakonec, AI také hraje důležitou roli v podpoře školení a výcviku zaměstnanců v bezpečnosti a ochraně zdraví při práci (BOZP). Využití umělé inteligence v této sféře otevírá nové možnosti pro rozvoj a implementaci školicích programů, které jsou mnohem efektivnější a interaktivnější než tradiční metody. Jednou z takových možností je vytváření realistických

tréninkových simulací, které umožní personálu projít nejrůznějšími scénáři, aniž by přišel kdokoliv k úrazu. Tyto simulace mohou zahrnovat širokou škálu situací, od rutinních bezpečnostních kontrol až po krizové reakce na mimořádné události, jako jsou požáry, teroristické útoky nebo přírodní katastrofy. Tyto simulace je poté možné dynamicky upravovat pro specifické potřeby a tím zajistit ještě více efektivní školení. Na to navazuje možnost tyto simulace analyzovat a data poté shromažďovat pro budoucí zpětnou vazbu a personalizaci.[114]

Bodové shrnutí využití AI v národní bezpečnosti:

1. Osobní bezpečnostní aplikace a nositelná bezpečnostní technologie – náramky, řetízky apod. - AI poháněné osobní asistenty mohou pomoci starším osobám nebo osobám se speciálními potřebami v nouzových situacích;
2. Domácí bezpečnostní systémy;
3. Prevence finančních podvodů a ochrana identity;
4. Snaha o zvýšení automobilové bezpečnosti;
5. Kybernetická bezpečnost a ochrana osobních dat;
6. Vzdělávání a osvěta v oblasti bezpečnosti – AI může být využita pro vývoj vzdělávacích programů a simulací, které učí uživatele, jak rozpoznat a reagovat na různé bezpečnostní situace;
7. Detekce nebezpečných situací ve veřejných prostorech – AI může pomoci monitorovat veřejné prostory a identifikovat potenciální hrozby nebo nebezpečné situace, jako jsou podezřelé balíčky, chování a jiné anomálie;

A další.

2.1.3 Národní bezpečnost

Tato kapitola se zaměřuje na implementaci umělé inteligence do národní bezpečnosti v obecném měřítku, přičemž níže v kapitolách Modelové příklady a Příležitosti využití nových poznatků z AI v oblastech bezpečnosti, budou uvedeny a rozepsány již konkrétní případy.

Jedna z již známých technologií umělé inteligence je rozpoznání obličejů a analýza chování pro identifikaci nejrůznějších anomálií v chování. Pro účely národní bezpečnosti, je tato technologie převážně využívána pro identifikaci teroristických a jiných kriminálních aktivit. Právě analýza vizuálních dat a behaviorálních vzorců umožňuje efektivnější identifikaci možných hrozeb ještě předtím, než nastanou.

Další významnou a méně známou disciplínou, ve které našla umělá inteligence své uplatnění je kontrarozvědka (counterintelligence, dále CI). AI v tomto odvětví ovlivňuje sběr zpravodajských informací i jejich zpracování. Integrace AI do CI operací značně rozšířila možnosti právě díky schopnosti systematicky analyzovat obrovské množství dat a na základě výstupů vytvářet možné predikce proti špionážím, kybernetickým útokům a jiným kriminálním aktivitám cílených na národní bezpečnost. Mezi další způsoby, jak AI doplňuje tradiční metody zpravodajství je automatizovaný sběr informací – ten umožňuje botům a web crawlerům prohledávat dostupné informace na internetu (online fóra, sociální sítě apod.) za účelem hledání nových zranitelností a potencionálních hrozeb.[30][31][48][49][50][51][52][53]

Zpracování přirozeného jazyka (NLP) je technika, která umožňuje modelům AI vytvářet textové či hlasové zprávy. V kontextu národní bezpečnosti se této techniky využívá pro automatizovanou analýzu obrovského množství jak psaných, tak mluvených dat za účelem vyhledávání klíčových slov a lingvistických anomálií. To umožňuje odhalovat podezřelé (i skryté) komunikační kanály, které jsou využívány špiony.[48][53]

Zapojení umělé inteligence do CI operací znamená významný pokrok v možnostech odhalování, předcházení a minimalizaci špionážních činností. Tato technologie umožňuje zpravodajským službám efektivně zpracovávat obrovské objemy dat, s větší přesností rozpoznávat potenciální hrozby a rychleji odhalovat i reagovat na nové výzvy. Současně je zde nutnost zodpovědného přístupu k vývoji AI – zaobírat se etickými úvahami a potřebami sloučení bezpečnostních opatření s ochranou práv na soukromí. Vzhledem k tomu, že technologie AI se neustále vyvíjí, její význam v oblasti CI bude nadále klíčový pro zajištění národní bezpečnosti.[48][49][50][51][52][53]

Bodové shrnutí využití AI v národní bezpečnosti:

1. Rozpoznání obličeje, anomálií – odhalování teroristických a jiných kriminálních útoků jak v kybernetickém prostoru, tak v kritické infrastruktuře;
2. Predikce;
3. Podpora rozhodování ve vojenských krizových situacích;
4. Bezpilotní automatické systémy (obranné, zbraňové, průzkumné (drony))– záchranné, průzkumné akce (např. v horách a jiných podobně nepřístupných oblastech);

5. Kontrola a dohled nad komunikacemi, sociálními sítěmi apod. – AI může monitorovat a analyzovat komunikaci pro identifikaci hrozeb, šíření dezinformací nebo podezřelých vzorců chování (špionáž, terorismus, a jiné útoky);
6. Špionáž pro vojenské zpravodajství, mezinárodní spolupráce v odhalování zločinu, humanitární mise;
7. Detekce a neutralizace dronů nebo nejrůznějších zbraňových systémů;
8. Vzdělávání a školení bezpečnostních sil – využití AI pro vytváření realistických tréninkových simulací a poskytování personalizovaného školení pro vojenský a bezpečnostní personál;
9. Optimalizace logistiky a zásobování – jak pro armádu, tak pro občany při mimořádných událostech;
10. Detekce a analýza chemických, biologických, radiologických a jaderných hrozeb;

A další.

3 HROZBY A RIZIKA SPOJENÁ S VYUŽITÍM UMĚLÉ INTELIGENCE

3.1 Hrozba

Hrozba je jakýkoliv jev, který má potenciál ohrozit člověka, majetek, zdraví či jiné hodnoty chráněné státem. Definice podle Ministerstva vnitra zní: *„Jakýkoli fenomén, který má potenciální schopnost poškodit zájmy a hodnoty chráněné státem. Míra hrozby je dána velikostí možné škody a časovou vzdáleností (vyjádřenou obvykle pravděpodobností čili rizikem) možného uplatnění této hrozby.“* [40] V případě umělé inteligence jsou hrozby všechny události, které mohou potenciálně negativně ovlivnit tyto systémy a jejich provoz. Tyto události zahrnují širokou škálu situací od technologických selhání až po záměrné útoky, a mohou pocházet jak z interního, tak z externího prostředí. Mezi příklady patří chybná konfigurace AI algoritmů, narušení datových sad, které mohou vést ke zkresleným výsledkům, a útoky, jako jsou ty založené na otrávení dat nebo sociální inženýrství, cílící na zaměstnance, kteří pracují s AI. Rovněž je nutné brát v úvahu nepředvídatelnost AI systémů, kdy se chování modelů může v reálném světě značně lišit od testovacích scénářů v laboratorních podmínkách, a bezpečnostní rizika, která mohou vést k neautorizovanému přístupu nebo úniku informací. Vzhledem k rostoucí integraci AI do kritických systémů a infrastruktur je důležité tyto hrozby řádně identifikovat, hodnotit a minimalizovat prostřednictvím pečlivě navržených bezpečnostních strategií a protokolů.

Hrozby v oblasti kybernetické bezpečnosti a bezpečnosti informačních systémů v rámci umělé inteligence lze klasifikovat do několika kategorií, které nám umožňují pochopit jejich původ a potenciální motivy.[42] Tyto hrozby rozdělujeme do čtyř hlavních skupin:

Externí náhodné hrozby zahrnují faktory mimo kontrolu organizace, jako jsou přírodní pohromy – povodně, zemětřesení nebo bouřky, které mohou nepředvídatelně ohrozit infrastrukturu a data.[32][42]

Externí úmyslné hrozby jsou často dílem aktérů s cílem poškodit organizaci nebo získat neoprávněný přístup k informacím. Hacking, prováděný jednotlivci nebo organizovanými skupinami, patří mezi nejvýznamnější z této kategorie, protože útočníci aktivně hledají způsoby, jak prolomit bezpečnostní opatření.[32][42]

Interní náhodné hrozby obvykle vycházejí z vnitřního prostředí organizace a zahrnují technická selhání, jako jsou chyby softwaru nebo hardware, nebo lidskou chybu, která může být způsobena neúmyslně zaměstnanci.[32][42]

Interní úmyslné hrozby představují sabotáž nebo jiné škodlivé činy provedené vědomě zaměstnanci nebo insidery, kteří mohou zneužít své postavení a přístup k citlivým informacím nebo systémům.[32][42]

Rozpoznání a kategorizace těchto hrozeb je klíčové pro efektivní plánování bezpečnostních opatření a reakčních plánů, umožňuje organizacím lepší přípravu a zvýšení odolnosti proti potenciálním bezpečnostním incidentům. Tabulka níže popisuje tento vztah, přičemž jsou uvedeny příklady hrozeb spojených s AI. Informace v tabulce jsou čerpány ze stejného zdroje, jako předchozí kapitoly.

Tabulka 1 Druhy hrozeb a jejich vztahy

HROZBY	Náhodné	Úmyslné
Externí	Externí programátor nevěděl, jaký bude úplný účel systému, a proto testování v prostředí organizace vedlo k nesprávné funkčnosti.	Útoky na AI systém, jako je například otrávení dat (data poisoning).
Interní	Chyba v kódu při implementaci algoritmu AI vedoucí k chybným výstupům.	Interní manipulace s tréninkovými daty pro vytvoření zaujatého modelu.

V rámci komplexní analýzy hrozeb v oblasti umělé inteligence rozlišujeme mezi aktivními a pasivními hrozbami, s důrazem na jejich interakci s klíčovými složkami AI systémů.

Aktivní hrozby v oblasti umělé inteligence představují zásahy, které mění funkční stav AI systému a mohou vést k porušení jeho integrity nebo dostupnosti. Takové hrozby mohou zasáhnout procesy strojového učení, manipulovat s datovými sadami nebo zasahovat do operačního prostředí AI, což může způsobit nepředvídatelné chování nebo znefunkčnění AI systému. Například, útočník může injektovat škodlivá data během fáze tréninku AI, což vede k sestavení zavádějících nebo nepřesných modelů.[32]

Pasivní hrozby jsou v kontextu umělé inteligence obzvláště závažné, jelikož se týkají neoprávněného sběru a analýzy dat bez narušení systému AI. Tyto hrozby často cílí na modely strojového učení s cílem získat citlivé informace prostřednictvím technik jako jsou útoky na soukromí modelů nebo inverzní útoky, které se snaží rekonstruovat trénovací data.[32]

Také je důležité si uvědomit, že hrozby mohou působit na různé **komponenty** AI systémů, včetně **operačních systémů**, které podporují AI aplikace, **databází** používaných pro učení a ukládání dat AI, **síťových infrastruktur**, které umožňují výměnu dat, a na samotné **uživatelské rozhraní**. Identifikace a pochopení, jak se tyto hrozby projevují a působí na různé aspekty AI, je nezbytné pro tvorbu účinných obranných strategií, zajišťující, že systémy umělé inteligence zůstanou důvěryhodné – tedy bezpečné, spolehlivé, transparentní, diskrétní, odpovědné a spravedlivé.[32]

Umělá inteligence se stává součástí našeho každodenního života, a proto je nezbytné stanovit pravidla pro její používání a zároveň vyzdvihnout hrozby, které sebou AI nese. Níže budou popsány hrozby spojené s užíváním umělé inteligence, přičemž veškeré informace vyplývají z těch, které již byly uvedeny v této práci.

Mezi hlavní přínosy AI patří možnost využití těchto technologií jako nástroje k predikci hrozeb v organizacích, spolu s použitím těchto systémů pro návrh řešení pro dané hrozby. Dále je AI schopna poskytnou kvalitnější zdravotní péči, přináší autonomní vozidla a drony, které jak bylo zmíněno, slouží také k prozkoumávání nebezpečných oblastí pro člověka, což zvyšuje bezpečnost občanů. Usnadnit může také přístup ke vzdělávání a nejrůznějším informacím, či vzdělávání v oblastech jako je BOZP. V organizacích a podnikách pomáhá AI k výrobě nových výrobků, analýze nákupů a chování svých zákazníků, optimalizaci a plynulosti prodeje a zároveň je schopna šetřit energii a jiné zdroje.

Dále je umělá inteligence schopna predikce a včasné reakce na nové i staré kybernetické útoky spolu s ochranou proti SPAMU či dezinformacím. Předpokládat se také dá použití těchto technologií v prevenci proti kriminalitě včetně například analýzy rizika úniku vězňů.

Využití AI technologií je mnoho a budou stále přibývat. Její implementace do systémů je velmi přínosná, avšak sebou nese značné množství hrozeb – vše co má implementovanou umělou inteligenci, je napadnutelné v případě nedostatečného zabezpečení. Zdravotnictví, školství, silniční a železniční doprava nebo dokonce elektrárny mohou v budoucnu používat AI za účelem automatizace rutinních procesů apod. To dává ale prostor teroristickým

organizacím či jednotlivcům pro hledání slabých míst v těchto systémech, za účelem jejich zneužití či kompletního vyřazení z provozu. Co se týče oblastí kritické infrastruktury, jež budou využívat umělé inteligence, bude robustní zabezpečení systémů využívající AI zcela nezbytné.

Problémem může být i nedostatečné využívání těchto systémů. Kromě promarněných příležitostí to také může znamenat otevřené dveře pro útočníky, kteří těchto systémů využívají – to znamená, že systémy bez implementované umělé inteligence budou v budoucnosti zranitelnější, jelikož nebudou schopné držet krok s nově se vyvíjejícími hrozbami, které může generovat právě AI. Firmy, které neimplementují AI modely a nevyužívají je pro neustálé aktualizace svých bezpečnostních systémů, se tak stanou atraktivnějšími cíli pro kybernetické útočníky.

Spolu s hrozbami spojenými hlavně s kybernetickou sférou, je zde také otázka, zda umělá inteligence nevezme pracovní místa, která nebude možné nahradit. Občané by pak ztráceli práci jak na běžícím pásu a neměli by možnost náhrady ve svém oboru. Nárůst nezaměstnanosti je varianta velmi očekávaná, protože stroje, které budou schopny nahradit člověka v určitém sektoru, nebudou muset dostávat výplatu, neunaví se a nebudou si stěžovat. To sice znamená zvýšení zisků pro firmy a větší produktivitu práce, ale co se stane s původními zaměstnanci? Nebude to znamenat přílišnou závislost na technologii? Tyto skutečnosti mohou znamenat pokles či úplnou ztrátu lidských dovedností, nedostatečný rozvoj v manuálních pracích nebo ztrátu schopnosti řešit problémy a krize bez technologické pomoci. Například architekti se přestanou učit dělat výkresy, protože je za ně bude schopná rychleji a kvalitněji zpracovat umělá inteligence, doktoři se přestanou vzdělávat v různých oblastech, protože bude AI schopna efektivněji hledat řešení na různé zdravotní problémy, či zdravotnické stroje budou dělat práci přímo fyzicky za ně. Další oblastí, kterou vývoj technologií AI zasáhne jsou oblasti umění, designu nebo tvůrčího psaní – tyto umělecké výtvory začnou být nekreativní a budou postrádat lidský dotek. Ano, obrazy, co vytvoří umělá inteligence jsou naprosto úchvatné, avšak to je jen spleť pixelů, kterou vytvořil stroj a ne dílo, na kterém usilovně někdo pracoval.

Hrozby, které jsou spojeny s využitím AI jsou popsány níže v Tabulce 1 Hrozby – veškeré informace použity v tabulce vychází z poznatků, které jsou použity v této práci. [34]

3.1.1 Hrozby spojené s využitím umělé inteligence

Tabulka 2 Hrozby

Kategorie, hrozby	Popis hrozeb
Vnější hrozby	
Vytváření a šíření dezinformací (deepfakes, hoax)	Využití AI pro vytváření a šíření falešných informací, například prostřednictvím deepfakes technologií, představuje vážnou hrozbu pro společnost, jelikož může podkopávat důvěru v média a ovlivňovat veřejné mínění.
Vytváření sofistikovanějších malware	AI má schopnost detekovat malware pomocí specifických anomálií v chování systémů. Kromě toho však AI může tuto schopnost obrátit ve svůj prospěch: je schopna nejen napodobit existující útoky, ale také je dále rozvíjet. Tímto způsobem umělá inteligence přispívá k tvorbě zcela nových typů kybernetických útoků. Tyto nově vyvinuté útoky jsou obzvlášť nebezpečné, protože jsou zatím neznámé a mohou uniknout stávajícím bezpečnostním opatřením.
Nelegální vývoj autonomních zbrání	Podobně jako v případě vyvíjení zcela nových typů kybernetických útoků, je třeba zdůraznit i schopnost umělé inteligence generovat kódy pro nelegální autonomní zbraně, které se mohou velmi snadno dostat do rukou teroristů.
Napadení autonomních dronů	Umělá inteligence se stává součástí mnoha technologických aplikací a ani drony nejsou výjimkou. Tato integrace však přináší rizika spojená se zneužitím technologie, zejména pokud je zabezpečení nedostatečné. Útok na vojenské bojové drony může mít fatální následky, což zdůrazňuje potřebu robustního zabezpečení v těchto systémech.
Napadení autonomních vozidel	Podobně jako s drony, je zde riziko napadení. Autonomní vozidla obsahují technologie umělé inteligence, která sbírají data, vyhodnocují je a na základě toho se poté rozhodují (například pomocí senzorů pozná chodce na přechodu apod.). To ale znamená opět potřebu kvalitního zabezpečení, aby tyto vozidla nebyly napadnutelná a poté zneužitá (například pro teroristický útok)
Použití pro hledání zranitelností v systémech	AI je schopna identifikovat specifické vzorce v systémech, což umožňuje předcházet potenciálním kybernetickým útokům. Tuto schopnost však mohou zneužít i útočníci, kteří využívají AI k vyhledání zranitelností v těchto systémech. Následně tyto zranitelnosti využijí k provedení útoků, během kterých mohou krást citlivá data nebo dokonce získat plnou kontrolu nad postiženým systémem.
Využití pro automatizaci kybernetických útoků	Umělá inteligence může být využita k automatizaci kybernetických útoků, což umožňuje útočníkům provádět sofistikované a koordinované útoky ve velkém měřítku bez nutnosti lidského zásahu. Tato schopnost zvyšuje frekvenci a účinnost útoků, čímž se zvyšuje i riziko pro veřejné i soukromé organizace.

Napadení zdravotních přístrojů	Kybernetické útoky na zdravotní přístroje mohou mít závažné důsledky pro pacienty, neboť kompromitace těchto zařízení může vést k nesprávné diagnóze, chybné operaci nebo jiným lékařským chybám. Zneužití umělé inteligence v tomto kontextu zvyšuje riziko nedovolených zásahů do zvláštních osobních údajů.
Napadení a sabotáž průmyslových zařízení a přístrojů	Sabotáž nebo útoky na průmyslová zařízení a přístroje mohou mít devastující důsledky na výrobní procesy a dodavatelské řetězce. Použití umělé inteligence k identifikaci slabých míst a koordinaci útoků může vést k výpadkům, ztrátám nebo ohrožení bezpečnosti pracovníků a veřejnosti.
Vnitřní hrozby	
Únik osobních údajů	Únik osobních údajů představuje závažné riziko zneužití citlivých informací, které může vést k finančním ztrátám, krádežím identity a narušení soukromí jednotlivců. Tyto incidenty často vyplynou z nedostatečných bezpečnostních opatření nebo cílených kybernetických útoků.
Nelegální sběr osobních údajů	Stejně jako únik citlivých informací, tak také nelegální sběr je velkým rizikem pro ochranu soukromí jednotlivců. Může dojít k finančním ztrátám, krádežím identity a jiným stejně závažným hrozbám spojených s osobními údaji.
Nelegální úprava osobních údajů	Neoprávněná modifikace osobních údajů může mít za následek závažné důsledky, včetně falešných obvinění, poškození reputace a právních nejasností pro jedince, jejichž údaje byly pozměněny.
Vytváření falešných dokumentů	Využití technologií pro generování podvodných dokumentů, jako jsou občanské průkazy, pasy nebo jakékoliv finanční dokumenty, představuje seriózní bezpečnostní hrozbu s dopadem na jak individuální, tak i na institucionální úrovni.
Vytváření podvodných aplikací a software	Tvorba těchto aplikací a software, které se tváří jako legitimní, může způsobit ztrátu osobních údajů, financí či dokonce soukromí.
Obcházení bezpečnostních opatření	Obcházení bezpečnostních opatření za účelem neautorizovaného přístupu, může být velkou bezpečnostní hrozbou pro organizace.
Prodej „jailbreaků“ pro odblokování omezení AI modelů	Prodej nástrojů umožňujících obejít omezení implementovaná v AI modelech zvyšuje riziko zneužití těchto technologií, jako je například neetické jednání modelů AI.
Sociální a ekonomické důsledky	
Ztráta pracovních míst	Automatizace procesů prostřednictvím umělé inteligence může vést k masivní ztrátě pracovních míst v odvětvích, kde jsou rutinní (opakující se) úkoly nahrazovány stroji.
Diskriminace	Používání AI v procesech rozhodování, jako je výběr zaměstnanců nebo poskytování úvěrů, může neúmyslně zesílit existující předsudky, pokud nejsou algoritmy správně kalibrovány.

Právní výzvy	
Nedostačující právní regulace	Absence adekvátních právních rámců pro nové technologie AI může způsobit právní nejistoty ohledně odpovědnosti a správného využívání těchto systémů.

3.1.2 Další možné hrozby spojené s používáním umělé inteligence

Dark Web jsou webové stránky, které jsou veřejně viditelné ale skrývají adresy internetového protokolu (IP) serverů, které provozují tyto weby. Jedná se o skryté sítě, které se vyhýbají přítomnosti na viditelném webu a jejich URL adresy nesou příponu .onion. – prohlížeč TOR.[1] Blog Kaspersky se zabývá tím, jak kyberzločinci využívají AI pro generování polymorfního malwaru, automatizaci škodlivých úkolů a obcházení bezpečnostních opatření. Dále popisuje vytváření a prodej "jailbreaků" pro odblokování omezení AI modelů, vývoj AI řízeného softwaru pro škodlivé účely a zneužití open-source nástrojů pro kyberútoky. Zmiňuje se také o vzniku neomezených ChatGPT navržených pro kriminální aktivity a o prodeji ukradených nebo podvodně vytvořených účtů ChatGPT.[38]

Dalším klíčovým fenoménem současné doby jsou inteligentní města, známá také jako koncept Průmysl 4.0, který reflektuje rostoucí trend propojení různých systémů a technologií. Tento fenomén má své kořeny v nástupu internetu a následně v rozvoji Internetu věcí (IoT). V současnosti se umělá inteligence (AI) stává nedílnou součástí těchto systémů, což přináší nejen technologické inovace, ale také nové bezpečnostní výzvy.[1]

Implementace AI v inteligentních městech a průmyslových procesech zvyšuje efektivitu a automatizaci, avšak zároveň vystavuje tyto systémy novým hrozbám. Mezi hlavní bezpečnostní rizika patří ztráta dat, narušení soukromí a zvýšené riziko kybernetických útoků, včetně teroristických aktivit využívajících rozsáhlé propojení těchto technologií. AI tedy nejen zlepšuje funkčnost a propojení systémů, ale zároveň vyžaduje zvýšenou pozornost na otázky kybernetické bezpečnosti a ochrany kritických infrastruktur.[1]

Nelegální odposlech je další rozsáhlou kapitolou, kterou je třeba diskutovat. Odposlech může nastat třemi různými způsoby – prostorový odposlech, odposlech mobilních telefonů a spyware. V souvislosti se systémy, které používají AI to bude znamenat nutnost většího

zabezpečení počítačových dat, počítačového systému a elektronickou komunikaci v jakémkoliv podání.[1]

Další významnou bezpečnostní hrozbou, kterou je nezbytné podrobně diskutovat v kontextu systémů využívajících umělou inteligenci (AI) je **nelegální odposlech**. Využití AI v zabezpečení systémů může nabídnout inovativní přístupy k detekci a prevenci odposlechů, ale zároveň může být AI také zneužita k sofistikovanějším formám útoků. **Prostorový odposlech** zahrnuje naslouchání nebo záznam rozhovorů pomocí mikrofonů nebo jiných zvukových zařízení, kde AI může být využita jak k efektivnější analýze zvukových signálů, tak ke generování deepfake zvuků. Dále AI dokáže odposlouchávat **mobilní komunikaci** pomocí pokročilých algoritmů strojového učení, které analyzují síťový provoz a identifikují zranitelnosti v mobilních sítích. Tyto technologie mohou být zneužity k zachycení hovorů a zpráv, zejména prostřednictvím útoků typu man-in-the-middle (MitM), kde útočník přesměruje komunikaci přes svůj vlastní server. Účelem těchto odposlechů může být získání citlivých informací, jako jsou obchodní tajemství nebo osobní údaje, které mohou být dále prodány nebo zneužity k vydírání. Obrana proti těmto hrozbám zahrnuje použití šifrovacích technik pro ochranu dat během přenosu, pravidelnou aktualizaci softwaru a firmware zařízení, a implementaci systémů detekce průniku využívajících AI, které mohou v reálném čase monitorovat a analyzovat síťový provoz, detekovat anomálie a potenciální útoky. Použití **spyware** představuje další hrozbu, kdy AI může zlepšit schopnosti spyware v obcházení detekčních systémů a shromažďování dat, zatímco antimalware s AI může efektivněji detekovat a eliminovat spyware prostřednictvím dynamické analýzy. **Odposlech datové komunikace**, známý také jako sniffing, zahrnuje zachycení a analýzu datových paketů přenášených sítí, kde AI může automatizovat analýzu zachycených dat a předvídat vhodné okamžiky pro odposlech, ale také může vylepšit systémy detekce průniku a optimalizovat šifrovací procesy pro zajištění nečitelnosti dat.[1]

Každý z těchto způsobů odposlechů představuje specifické hrozby, které vyžadují rozdílné přístupy k zabezpečení. Využití AI v této oblasti přináší nové možnosti jak pro útočníky, tak pro obránce, a je tedy klíčové, aby byly neustále vyvíjeny a aktualizovány metody zabezpečení, které mohou čelit stále sofistikovanějším hrozbám v oblasti nelegálního odposlechu.[1]

3.2 Riziko

Riziko je míra pravděpodobnosti, zda vznikne událost, která je nežádoucí z bezpečnostních hledisek a je odvozena od konkrétní hrozby. Definice podle Ministerstva vnitra zní: *„Možnost, že s určitou pravděpodobností vznikne událost, kterou považujeme z bezpečnostního hlediska za nežádoucí. Riziko je vždy odvoditelné a odvozené z konkrétní hrozby. Míru rizika, tedy pravděpodobnost škodlivých následků vyplývajících z hrozby a ze zranitelnosti zájmu, je možno posoudit na základě tzv. analýzy rizik, která vychází i z posouzení naší připravenosti hrozbám čelit.“*.[39]

V kontextu umělé inteligence můžeme riziko definovat jako potenciál negativních následků, ke kterým může dojít v důsledku interakce systémů AI s jejich prostředím. Tato rizika mohou nabývat mnoha forem, od drobných technických komplikací až po významné bezpečnostní incidenty s širokým spektrem dopadů. Patří mezi ně například nesprávné rozhodování způsobené zkreslenými daty, zneužití AI systémů prostřednictvím kybernetických útoků, nebo nepředvídané etické dilema vznikající z autonomních rozhodnutí AI. Rizika mohou pocházet jak z vnitřních operací a struktury systémů AI, tak z externích faktorů, včetně manipulace údajů a sociálně inženýrských útoků. V důsledku schopnosti AI systémů učit se a adaptovat se, může být jejich chování v reálném světě nejisté a může se lišit od původních očekávání stanovených během fáze návrhu a testování.[41]

Kromě toho, jak AI postupně proniká do kritických sektorů a infrastruktur, roste potřeba uceleného řízení rizik, které zohledňuje všechny aspekty vývoje, nasazení a provozu AI systémů. To vyžaduje komplexní přístupy a strategie, které budou zahrnovat přesné a transparentní hodnocení potenciálních rizik, jejich řízení a prostřednictvím bezpečnostních protokolů, a to v souladu s nejnovějšími standardy a osvědčenými postupy v oblasti kybernetické bezpečnosti a ochrany soukromí.[41]

3.2.1 Doporučení pro řízení rizik umělé inteligence

Ve vývoji umělé inteligence hrají data zásadní roli, a jak se ukazuje, chování a interpretace dat může být odlišné mezi kontrolním prostředím laboratoře a dynamickým prostředím reálného světa. Je zásadní, aby byl účel, pro který je AI systém vytvářen, jasně definován a komunikován v rámci celého cyklu vývoje a nasazení. To zahrnuje identifikaci potřeb zákazníků a očekávání vůči systému, aby bylo zajištěno, že systém bude po nasazení fungovat dle specifikací a bude splňovat požadované funkce a cíle. Nejedná se pouze o technické

testování, ale také o ověření, že AI plní svůj zamýšlený účel v různých podmínkách a scénářích, se kterými se může setkat ve skutečném provozu.[42][43]

Dále je kriticky důležité, aby datasety, na kterých jsou AI systémy trénovány a testovány, byly reprezentativní pro skutečné podmínky použití. Nereprezentativní nebo zkreslené datové sady mohou vést k diskriminačním výstupům, jako je rasismus nebo xenofobie. AI systémy, které se spoléhají na takovéto data, mohou vytvářet a upevňovat předsudky, které ovlivňují rozhodování a chování systému. Aby se předešlo těmto nežádoucím tendencím, je nezbytné pečlivě vybírat a zpracovávat data s důrazem na diverzitu a objektivitu.[42][43][44]

Podle zdrojů, jako jsou publikace NIST [44] a články na webu Clever&Smart [42][43], které se zabývají řízením rizik umělé inteligence, musí být v procesu vývoje a nasazení AI přijata opatření k zajištění správného zacházení s daty a jejich validitou. V tomto kontextu je důležité aplikovat principy a praxe, které podporují spravedlnost, transparentnost a odpovědnost v celém životním cyklu AI systému. Implementace komplexního přístupu k řízení rizik v AI je zásadní k minimalizaci negativních sociálních dopadů a podpoře důvěry a bezpečnosti v technologie AI.[41][44][45][46][47]

3.2.2 Analýza rizik

Tato kapitola se zaměřuje na analýzu rizik spojených s implementací umělé inteligence. Pro analýzu rizik byly v rámci této práce vybrány následující 3 oblasti, u kterých v současné době pozorujeme nejvýznamnější růst. V kompletní analýze rizik by byla zahrnuta kompletní škála aktiv a jejich hrozeb – v této práci jsou hrozby uvedené u vybraných aktiv pouze příkladem, které ilustrují důležité aspekty, nad kterými je třeba se zamyslet při implementaci AI a na které je aplikována analýza rizik. V budoucnu je možné tyto oblasti rozšířit a zabývat se jimi více do hloubky.

V rámci této analýzy jsou použity tabulky, které kvantifikují pravděpodobnost (značené P) a dopad (značeno D). Při vynásobení těchto aspektů vyjde riziko v číselné podobě, které je označeno písmenem R.

V této analýze rizik se nesoustředíme na specifické zranitelnosti jednotlivých systémů AI, neboť tato oblast vyžaduje vysokou míru specializace a individuálního přístupu. Komplexnost systémů umělé inteligence a diverzita jejich aplikací v různých organizacích a firmách znamenají, že každý subjekt bude mít odlišné bezpečnostní potřeby a požadavky.

Zranitelnosti v systémech AI mohou být velice specifické a závislé na konkrétním nasazení, konfiguraci, využitých datech a provozním prostředí. Detailní identifikace a řešení těchto zranitelností by vyžadovalo rozsáhlé zdroje a odborné znalosti specifické pro dané technologické řešení, což by přesahovalo rámec obecné analýzy rizik. Proto se tato analýza zaměřuje na spektrum potenciálních hrozeb, příčin, pravděpodobnosti a jejich dopadům. Organizace musí adaptovat zjištění na jejich specifické kontexty a vytvářet zabezpečovací opatření, která jsou pro ně nejrelevantnější.

Tabulka 2 je zaměřena na oblast zdravotnictví, přičemž bylo zvolené aktivum „život a zdraví pacientů“. Zdravotnictví je jedním z prvků kritické infrastruktury, kam můžeme dále zařadit dopravu, energetiku, telekomunikaci apod. Všechny tyto oblasti by měli velmi rozsáhlou analýzu rizik, která není předmětem této práce, a proto je zde uvedeno pouze jedno aktivum pro oblast zdravotnictví, jedno aktivum pro dopravu a příklady hrozeb, které na dané aktivum mohou působit. Hrozby u této kapitoly jsou brány jako ohrožení života a zdraví až po úmrtí, přičemž úmrtí je samozřejmě nejzávažnější hrozbou, ale její příčiny by se v tabulce opakovali, proto není uvedená.

Pro tabulky číslo 3, 5 a 7 platí stejná pravidla. Hrozby jsou pouze příkladem. Cílem je poskytnout čtenáři metodologický základ pro vlastní analýzu rizik, která by měla být součástí proaktivní strategie řízení rizik v jakékoliv organizaci implementující AI systémy.

3.3 Oblast zdravotnictví

Tabulka 3 Zdravotnictví: Aktiva – život a zdraví pacientů

Aktivum	Hrozba	Příčina	P	D	R
Život a zdraví pacientů	Chybná diagnóza	Nesprávná data nebo chyby v algoritmu	3	4	12
		Napadení autonomních zdravotnických přístrojů (kybernetické útoky)	4	5	20
		Manipulace s daty , které ovlivňují zdravotnické přístroje a jejich rozhodování	3	5	15
		Chyby v diagnostických algoritmech	4	4	16
		Selhání systémů	4	4	16
		Chyby při vývoji a testování AI modelů	3	3	9
		Nedostatečná koordinace mezi zdravotním personálem a AI systémy	4	3	12
		Chyby v interpretaci výsledků AI systémů (nedostatečná školení)	4	4	16
	Chybný léčební plán	Nesprávná data, chyby v algoritmu nebo nelegální manipulace s osobními údaji	3	4	12
	Nesprávné dávkování léků	Nesprávná data, chyby v algoritmu nebo nelegální manipulace s osobními údaji	2	5	10
	Selhání robotických zařízení	Technické selhání, sabotáž nebo napadení zdravotnických přístrojů	2	5	10
	Závislost na technologii	Nedostatečný lidský dohled	3	3	9
	Diskriminace	Modely AI budou dělat rozhodnutí pouze na základě předchozích výsledků	3	3	9
	Chyby v predikci výsledků léčby	Zkreslená nebo neúplná data	3	5	15

3.4 Oblast doprava

Tabulka 4 Doprava: Aktivum – Autonomní vozidla

Aktivum	Hrozba	Příčina	P	D	R
Autonomní vozidla	Útoky na senzory a vstupní data	Fyzické manipulace se senzory	2	5	10
		Zaslání falešných signálů do senzorů (nesprávná data o okolním prostředí)	4	5	20
		Záměrné narušení čtení senzorů (např. překrytím značky STOP)	3	5	15
	Manipulace s mapovými daty	Změna mapových dat nebo GPS souřadnic prostřednictvím hacknutí serveru poskytující mapové aktualizace	4	4	16
		Vkládání falešných bodů zájmů pro senzory, které mohou ovlivnit navigaci.	4	4	16
	Větší nehodovost	Závislost na AI a ztráta lidských dovedností	5	5	25
	Adversariální útoky na algoritmy AI	Vkládání malých změn do vstupních dat, které zcela ovlivní rozhodovací procesy	5	5	25
	Nedostatečná interpretovatelnost AI rozhodnutí	Chybějící nebo neúplná dokumentace rozhodovacích procesů	3	5	15
	Instalace defektivního firmware	Úmyslná sabotáž, aktualizace firmware probíhá na nezabezpečeném kanálu, který může být napaden, nedostatečné testování před nasazením	5	5	25
	Ovládnutí vozidla	Zneužití slabin v softwaru, útočníci získají přístup k vnitřní síti vozidla, špatně zabezpečené komunikační kanály vozidla	5	5	25

Tabulka 5 Pravděpodobnost a dopad pro oblast zdravotnictví a doprava

Stupeň	**Pravděpodobnost**	**Kritérium**
1	Velmi nízká	Uplatnění hrozby je vysoce nepravděpodobné nebo žádné
2	Nízká	Výskyt méně než 1 x za rok
3	Střední	Výskyt zhruba 1x za rok
4	Vysoká	Výskyt zhruba 1x za měsíc
5	Velmi vysoká	Výskyt zhruba 1x týdně
Stupeň	**Dopad**	**Kritérium**
1	Velmi nízký	Menší úrazy nebo nemoci, které nepotřebují zásadní léčbu a nevedou k významnému narušení osobního života nebo práce.
2	Nízký	Úrazy nebo nemoci, které vyžadují léčbu, ale jsou plně vyléčitelné bez dlouhodobých následků.
3	Střední	Vážnější úrazy nebo nemoci, které mohou vést ke krátkodobé pracovní neschopnosti a možným dlouhodobým následkům.
4	Vysoký	Závažné úrazy nebo nemoci s dlouhodobou nebo trvalou pracovní neschopností a významným vlivem na osobní život.
5	Velmi vysoký	Úmrtí nebo úrazy či nemoci, které mají trvalý a zásadní dopad na kvalitu života.

3.5 Technologická oblast

Tabulka 6 Technologie: Aktivum – data

Aktivum	Hrozba	Příčina	P	D	R
Data	Únik nebo kompletní ztráta dat	Hledání zranitelností v systémech (neoprávněný přístup)	5	5	25
		Použití sofistikovanějších kybernetických útoků	5	5	25
		Použití podvodných software a aplikací	3	5	15
		Prodej jailbreaků	4	3	12
		Nedbalost zaměstnanců	4	5	20
		Nedostatečné šifrování	3	5	15
	Neoprávněná modifikace dat	Vytvoření falešných přístupových práv	3	5	15
		Zneužití slabin v systémech pro ukládání dat	3	5	15
	Nekvalitní nebo nesprávná data	Chyby při sběru dat	4	1	4
		Data jsou zastaralá	3	2	6
		Nedostatečné školení a kvalifikace zaměstnanců	4	3	12

Tabulka 7 Pravděpodobnost a dopad pro technologickou oblast (aktivum data)

Stupeň	Pravděpodobnost	Kritérium
1	Velmi nízká	Uplatnění hrozby je vysoce nepravděpodobné nebo žádné
2	Nízká	Výskyt méně než 1 x za rok
3	Střední	Výskyt zhruba 1x za rok
4	Vysoká	Výskyt zhruba 1x za měsíc
5	Velmi vysoká	Výskyt zhruba 1x týdně
Stupeň	**Dopad**	**Kritérium**
1	Velmi nízký	Drobné porušení informační bezpečnosti nebo soukromí bez závažných důsledků.
2	Nízký	Porušení bezpečnosti, které vede k malému úniku dat, s omezenými důsledky na jednotlivce nebo organizaci.
3	Střední	Únik dat nebo porušení soukromí s důsledky pro střední skupinu lidí, což vede k právním problémům a narušení důvěry.
4	Vysoký	Velký únik dat nebo vážné porušení soukromí, které má vliv na větší skupinu lidí a způsobuje vážné právní a reputační škody.
5	Velmi vysoký	Masivní únik dat nebo kritické porušení soukromí a bezpečnosti, které ohrožuje reputaci organizace a vede k významným právním důsledkům a ztrátě důvěry.

Tabulka 8 Technologie: Aktivum – Infrastruktura systémů AI

Aktivum	Hrozba	Příčina	P	D	R
Infrastruktura systémů AI	Kybernetické útoky	Nedostatečné zabezpečení	5	5	25
		Zranitelnosti v systémech	5	5	25
	Selhání systémů	Chyby v algoritmech nebo implementaci	4	3	12
		Nesplňující nároky na výkon a kapacitu systémů	5	3	15
	Selhání hardware	Nedostatečná údržba a aktualizace zařízení	5	4	20
		Vysoké nároky na výpočetní výkon a kapacitu	5	4	20
		Nedostatečná optimalizace	5	4	20
	Selhání sítě	Přetížení sítě	5	5	25
	Nedostatečná škálovatelnost	Rychlý nárůst objemu dat a provozu	5	5	25
	Změna přístupu k AI	Nová nařízení EU, která funkce může omezit nebo kompletně zakázat	3	5	15

Tabulka 9 Pravděpodobnost a dopad pro technologickou oblast (aktivum infrastruktura systémů AI)

Stupeň	**Pravděpodobnost**	**Kritérium**
1	Velmi nízká	Uplatnění hrozby je vysoce nepravděpodobné nebo žádné
2	Nízká	Výskyt méně než 1 x za rok
3	Střední	Výskyt zhruba 1x za rok
4	Vysoká	Výskyt zhruba 1x za měsíc
5	Velmi vysoká	Výskyt zhruba 1x týdně
Stupeň	**Dopad**	**Kritérium**
1	Velmi nízký	Drobné poškození nebo narušení, které lze snadno a levně opravit nebo nahradit.
2	Nízký	Poškození, které vyžaduje opravu nebo náhradu, ale nevede k významnému narušení.
3	Střední	Poškození nebo narušení, které má střední dopad a způsobuje značné náklady na opravy nebo náhrady.
4	Vysoký	Závažné poškození nebo narušení, které způsobuje dlouhodobý výpadek a vysoké náklady na opravy nebo náhrady.
5	Velmi vysoký	Kritické poškození nebo narušení, které ohrožuje dlouhodobé přežití organizace nebo jednotlivce a vyžaduje rozsáhlé náklady na obnovu.

4 MODELOVÉ PŘÍKLADY

4.1 AI v kybernetické bezpečnosti: Detekce a prevence útoků

Příležitosti: Rozpoznávání a eliminace potenciálních bezpečnostních hrozeb, včetně phishingu, DDoS útoků a dalšího škodlivého softwaru, se v posledních letech stalo mnohem snazším, a to díky pokrokům v oblasti umělé inteligence. Díky AI, která využívá rozsáhlé sady tréninkových dat a již známé vzorce chování, jsou tyto systémy schopné varovat před potenciálními hrozbami dříve, než se vůbec projeví. To je uskutečněno pomocí technik hlubokého učení, které napodobují funkce lidského mozku prostřednictvím tzv. neuronových sítí. Tyto sítě se postupem času samy vylepšují, čímž se stávají odolnějšími, inteligentnějšími a efektivnějšími. Systémy založené na hlubokém učení mají schopnost současně analyzovat data z mnoha různých zdrojů a systémů, což umožňuje odborníkům na kybernetickou bezpečnost rychleji identifikovat a reagovat na hrozby ještě předtím, než se mohou rozvinout v závažné bezpečnostní incidenty.[48][49][50][51]

Rizika: Falešně pozitivní a falešně negativní výsledky jsou jedním z hlavních problémů spojených s AI v bezpečnosti. Falešně pozitivní výsledek nastane, když AI nesprávně identifikuje legitimní aktivitu jako útok, což může vést k zbytečným vyšetřováním a přerušení obchodních procesů. Na druhé straně, falešně negativní výsledky znamenají, že skutečné útoky nejsou detekovány, což zanechává organizaci zranitelnou vůči hrozbám. Právě účinnost a správné výsledky AI modelů závisí na kvalitě a rozsahu trénovacích dat, na kterých jsou modely trénovány. Pokud trénovací data obsahují předsudky, neúplné nebo zastaralé informace, může to vést k nesprávným predikcím nebo nedostatečné schopnosti detekce nových a sofistikovaných útoků.[48][49][50][51]

Dalším rizikem je fakt, že AI systémy samotné mohou být cílem útoků. Útočníci mohou použít techniky jako jsou adversarial attacks, při kterých jsou do systému vkládány manipulované vstupy, aby bylo dosaženo falešných výsledků nebo aby šel systém zcela obejít. To zdůrazňuje potřebu robustního zabezpečení a pravidelné aktualizace AI modelů proti novějším typům kybernetických útoků.[48][49][50][51]

Používání AI v bezpečnostním kontextu přináší otázky týkající se soukromí, etiky a právní odpovědnosti. Je důležité zajistit, aby byly všechny operace AI v souladu se zákony a regulacemi týkajícími se ochrany dat a soukromí. Navíc je důležité pečlivě zvážit, jakým

způsobem jsou data sbírána, ukládána a analyzována, aby byla respektována práva jednotlivců.[48][49][50][51]

Možný vývoj: Systémy autentizace využívající umělou inteligenci mohou pro zajištění bezpečnější a přesnější autentizace využívat biometrická data, analýzu chování a další pokročilé techniky. Díky použití algoritmů strojového učení pro analýzu chování uživatelů a identifikaci potenciálních anomálií budou tyto systémy schopny rozpoznat podvodné aktivity a zabránit neoprávněným přístupům, které by kybernetický specialista neměl šanci vyhledat. Toto může být využíváno například pro přihlašování do firemních počítačů, účtů, databází atp.[48][49]

Dalším možným pokrokem ve vývoji bude jistě zvětšená automatizace, což sníží potřebu lidského zásahu v procesech zabezpečování. To ale může vyvolat otázky týkající se transparentnosti, odpovědnosti nebo předsudků.[48][49]

Jak se bezpečnostní prostředí vyvíjí a stává se složitějším, pravděpodobně dojde k větší spolupráci mezi průmyslem a vládou ve vývoji a implementaci bezpečnostních systémů poháněných AI. To by umožnilo efektivnější detekci a prevenci hrozeb, ale může také vyvolat obavy ohledně soukromí a občanských svobod.[48][49]

4.2 AI v bezpečnosti státu a kritické infrastruktuře

Příležitosti: Implementace AI do autonomních systémů a dronů přináší širokou škálu aplikací, které výrazně zvyšují jejich efektivitu a schopnost provádět složité úkoly. AI umožňuje autonomním dronům navigovat v komplexních prostředích, zpracovávat data v reálném čase a přizpůsobovat se měnícím se podmínkám, což je klíčové pro úspěšné monitorovací a průzkumné mise. Tato technologie může být využita například při záchranných operacích nebo monitorování kritické infrastruktury. Dále jsou AI systémy schopny analyzovat velké množství dat za účelem detekce anomálií a potenciálních hrozeb v reálném čase. Tento přístup je klíčový pro ochranu kritické infrastruktury před kybernetickými útoky. AI může automatizovat reakce na incidenty a minimalizovat tak dopady kybernetických útoků, což významně zvyšuje odolnost infrastruktury.[52][53]

Pokroky v technologiích, jako jsou rozšířená a virtuální realita, umožňují vývoj realistických výcvikových programů, které připravují vojenský personál na situace, jež by jinak nebylo možné simulovat. Tyto technologie zvyšují efektivitu a připravenost vojáků pro reálné bojové situace a zároveň zlepšují jejich schopnost koordinace, jak mezi sebou navzájem, tak i

s ostatními bezpečnostními složkami, díky rychlejšímu a efektivnějšímu sdílení informací.[52][53]

Rizika: Implementace umělé inteligence (AI) v bezpečnostních a autonomních systémech přináší celou řadu etických a právních výzev. Autonomní systémy schopné rozhodovat o životech a smrti bez lidského zásahu vyvolávají zásadní otázky týkající se odpovědnosti a etiky. Mezinárodní právo zatím není plně přizpůsobeno těmto technologiím, což může vést k právním nejasnostem a sporům. Kromě toho je AI vystavena riziku zneužití pro kybernetické útoky a špionáž. Škodliví aktéři mohou využít AI k vytváření sofistikovaných, obtížně detekovatelných útoků, čímž ohrožují kritickou infrastrukturu a národní bezpečnost. Automatizované špionážní operace představují další vrstvu rizik pro státy.[52][53]

Přílišná závislost na technologii AI může oslabit schopnost reagovat na situace bez její podpory, což je problém zejména v případě poruch nebo útoků. AI systémy jsou navíc zranitelné vůči různým typům útoků, což může umožnit nepřátelským entitám proniknout do kritických systémů. Nedostatečná kvalita algoritmů použitých v AI systémech může vést k chybám a nesprávným rozhodnutím, což má závažné následky pro národní bezpečnost. Neadekvátní správa dat může rovněž vést k neoprávněnému sběru a zneužívání citlivých informací, čímž je ohrožena bezpečnost státu.[52][53]

Závody ve zbrojení s AI technologiemi mohou destabilizovat globální bezpečnostní prostředí. Vývoj a nasazení AI řízených zbraní může vyvolat napětí mezi státy a eskalovat konflikty. Riziko nechtěné eskalace konfliktů je zvýšené, protože AI systémy mohou jednat rychleji než lidé a jejich rozhodnutí mohou být nepředvídatelná.[52][53]

Pokroky v technologiích, jako jsou rozšířená a virtuální realita, umožňují vývoj realistických výcvikových programů, které připravují vojenský personál na situace, jež by jinak nebylo možné simulovat. Tyto technologie zvyšují efektivitu a připravenost vojáků pro reálné bojové situace a zároveň zlepšují jejich schopnost koordinace, jak mezi sebou navzájem, tak i s ostatními bezpečnostními složkami, díky rychlejšímu a efektivnějšímu sdílení informací.[52][53]

AI má také potenciál zásadně ovlivnit kritickou infrastrukturu v oblastech, jako je doprava, zdravotnictví, energetika a potravinářství. Například v dopravě může AI optimalizovat řízení dopravy, předcházet nehodám a zlepšovat logistiku. Ve zdravotnictví může AI napomáhat v diagnostice nemocí, optimalizovat léčebné postupy a zefektivňovat správu zdravotnických zařízení. V energetice může AI přispět k optimalizaci výroby a distribuce energie, čímž se

zvýší energetická účinnost a spolehlivost. V potravinářství může AI pomoci při monitorování a řízení produkce potravin, čímž se zlepší efektivita a bezpečnost potravinového řetězce. To ale znamená, že všechny tyto oblasti kritické infrastruktury budou obsahovat systémy umělé inteligence a tím se stanou více náchylnými na již zmíněná rizika.[52][53]

Možný vývoj: Pokračující výzkum a vývoj v oblasti AI povede k sofistikovanějším a efektivnějším bezpečnostním systémům. Tyto technologie budou schopny lépe předpovídat hrozby, chránit citlivé infrastruktury a zlepšovat operace v reálném čase. Vývoj AI přinese nové aplikace v oblasti zpravodajství a vojenských operací. Například pokroky v strojovém učení a analýze dat mohou vést k vytvoření pokročilých systémů pro detekci anomálií, které umožní identifikovat hrozby dříve a s větší přesností. Významný posun se očekává také v oblasti autonomních systémů a dronů, které budou schopny provádět složité mise s minimálním lidským zásahem.[52][53]

Budoucí vývoj AI v bezpečnostním kontextu bude zahrnovat větší mezinárodní spolupráci a tvorbu regulačních rámců. Státy budou muset spolupracovat na vytvoření norem a dohod pro odpovědné využívání AI v oblasti národní bezpečnosti, aby se minimalizovala rizika a maximalizovaly přínosy těchto technologií. Mezinárodní organizace, jako OSN a NATO, mohou hrát klíčovou roli v koordinaci těchto snah a v zajišťování, že AI technologie jsou využívány v souladu s mezinárodními právními a etickými standardy. Současně bude nutné vyvinout nové mechanismy pro sledování a regulaci použití AI, aby se zabránilo zneužití těchto technologií. Státy budou muset neustále přizpůsobovat své bezpečnostní strategie a infrastrukturu, aby čelily novým hrozbám spojeným s AI. To zahrnuje nejen technologický pokrok, ale také změny v legislativě, mezinárodních dohodách a institucionálních strukturách. Flexibilita a schopnost rychle reagovat na nové výzvy budou klíčové pro udržení národní bezpečnosti v éře AI. Například implementace adaptivních systémů řízení rizik a vývoj nových protokolů pro rychlou reakci na kybernetické útoky budou nezbytné. Státy budou muset investovat do školení a výcviku svých bezpečnostních složek, aby byly schopny efektivně využívat nové AI technologie a zároveň si zachovaly schopnost jednat nezávisle na těchto systémech v případě jejich selhání.[52][53][54]

Další významný vývoj se očekává v oblasti zabezpečení dat a ochrany osobních údajů. AI technologie budou stále více využívány pro správu a ochranu citlivých informací, což vyžaduje vytvoření robustních bezpečnostních protokolů a standardů pro zpracování dat. Vývoj v oblasti kvantové kryptografie a dalších pokročilých šifrovacích technik bude klíčový pro

zajištění, že data zůstanou chráněna před stále sofistikovanějšími kybernetickými hrozbami.[53]

4.3 AI ve finančním sektoru – detekce podvodů a praní peněz

Příležitosti: Již je známou informací, že je AI schopna zpracovávat a analyzovat obrovské množství dat v reálném čase a tím pomoci v detekci podvodů, hrozeb apod. O čem se ale už tolik neví, je fakt, že je AI schopna detekovat podvody, a dokonce i **praní peněz** (AML – Anti-Money Laundering). Technologie AML se za posledních 10 let moc nezměnily. Procesy, které kontrolovaly transakce často vytvářely falešně pozitivní výstupy a tím čelily značné kritice, především proto, že objem a rychlost finančních transakcí značně vzrostla. Podobně, rostoucí využívání kryptoměn a decentralizovaných finančních platforem obchází tradiční finanční regulace (vzorce, pravidla), čímž vznikají takzvané slepé skvrny pro detekci praní peněz. Příkladem těchto pravidel je detekce velkých vkladů v hotovosti nebo převod peněz do zemí s velký rizikem. Toto je ale pravidlo, který každý zkušený člověk, který pere peníze, dokáže obejít. Tento problém ale pokroky v analýze dat, strojovém učení a celosvětové spolupráci pomoci orgánům se úspěšně minimalizuje.[54][55]

Příchod pokročilých modelů umělé inteligence přinesl významné zlepšení při řešení problémů v různých oblastech, zejména ve způsobech, jakými pracujeme s daty a přizpůsobuje se novým výzvám. Díky schopnosti AI analyzovat obrovské objemy dat se nám otevřely nové možnosti ve zlepšení procesů péče o zákazníky, hodnocení rizik a monitorování aktivit, což umožňuje hlubší a přesnější pochopení dané problematiky. AI také ukázalo svou schopnost rychle se přizpůsobovat měnícímu se prostředí, vstupům a stále se vyvíjejícím profilům rizik, což umožňuje efektivněji reagovat na nové výzvy. Automatizace úkolů, které byly dříve zpracovány ručně, nejenže zvýšila efektivitu, ale také poskytla zaměstnancům více prostoru pro jejich profesní růst a zaměření se na složitější a strategičtější úkoly. Navíc došlo k významnému snížení chyb a zlepšení konzistence v rozhodovacích procesech, což celkově zvyšuje kvalitu a spolehlivost práce. Díky těmto pokrokům v AI jsme schopni lépe čelit současným a budoucím výzvám.[54][55]

Rizika: Riziko falešně negativních nebo pozitivních identifikací, které mohou vést k nespravedlivému zacházení s nevinnými klienty nebo přehlédnutí skutečných podvodů, otázky soukromí a správného použití osobních a finančních dat jsou rizika, které tu budou i po nasazení propracovanějších AI modelů. Hlavní výzvy a omezení AI pro AML zahrnují kvalitu a dostupnost dat, vysvětlitelnost a transparentnost (mnoho pokročilých AI systémů funguje jako

"černé skříňky", což ztěžuje pochopení logiky rozhodnutí modelu), etické a právní otázky (AI musí předcházet nezákonné diskriminaci nebo profilování) a spolupráci mezi lidmi a AI (řádná školení pro zaměstnance, aby se předcházelo chybným výstupům, či špatnému zacházení s AI).[54][55]

Možný vývoj: S rychle rostoucí popularitou v AI modelech přijde i na budoucí vývoj v oblastech detekce a prevence podvodů či praní peněz. Mezi očekávaný vývoj patří i technologie **Explainable AI (XAI)** – modely, které jsou schopny vysvětlit své rozhodovací procesy a tím umožnit odborníkům plně pochopit jaké faktory ovlivňují rozhodování a výstupy. Právě XAI je schopna eliminovat „černou skříňku“ a tím vysoce zvýšit důvěru v její používání převážně v kritických oblastech jako je právě například finanční sektor.[55]

Dalším klíčovým nástrojem, který umožní vizualizaci vztahů, propojené entity a spojení v rozsáhlých datech je **analýza grafů a sítí**. Ty budou schopny odhalit organizované sítě podvodů, které by mohli naznačovat financování teroristických skupin a podobné nelegální aktivity, které by za normálních okolností nebyly detekovatelné pomocí klasických nástrojů založených na jednoduchých pravidlech.[55]

Zlepšení spolupráce mezi finančními institucemi bez ohrožení soukromí dat je jedním z největších rizik. Toto riziko snižuje na minimální úroveň **federované učení** a **decentralizovaný přístup** ke strojovému učení. Tento model umožňuje trénovat AI modely lokálně v jednotlivých institucích, přičemž sdílené jsou pouze aktualizace modelu. To umožňuje učení modelů napříč sítí finančních institucí, mezitím co citlivé údaje zůstávají lokálně v jednotlivých institucích.[55]

4.4 AI ve fyzickém zabezpečení: Chytré dohledové systémy

Příležitosti: Chytré dohledové systémy, poháněné umělou inteligencí (AI), přinášejí řadu významných příležitostí. Tyto technologie umožňují automatické rozpoznávání objektů a osob, což zvyšuje účinnost a rychlost reakce bezpečnostních složek. Schopnost AI analyzovat velké objemy dat v reálném čase umožňuje rychle identifikovat potenciální hrozby a předejít bezpečnostním incidentům. Například moderní kamerové systémy mohou automaticky detekovat podezřelé chování, sledovat pohyb osob v chráněných oblastech a okamžitě upozornit operátory na potenciální nebezpečí.[56][57]

Rizika: S nasazením AI v chytrých dohledových systémech se však pojí i značná rizika. Jedním z hlavních problémů je ochrana osobních údajů a soukromí. Dohledové systémy mohou shromažďovat a analyzovat velké množství osobních dat, což zvyšuje riziko jejich zneužití. Nedostatečná regulace a kontrola nad těmito systémy může vést k neoprávněnému sledování a porušení práv na soukromí jednotlivců. Navíc existuje riziko, že chyby v algoritmech nebo nedostatečně trénované modely povedou k nesprávným rozhodnutím a falešným poplachům, což může mít vážné následky pro bezpečnost a soukromí osob. Obavy z ochrany soukromí, zejména pokud je dohled prováděn ve veřejných nebo poloveřejných prostorech, jsou opodstatněné, protože existuje riziko chybné identifikace a následných nesprávných akcí. Potenciální zneužití systémů pro masový dohled a kontrolu může vést k významnému omezení občanských svobod a demokratických principů.[56][58][59]

Možný vývoj: Nepřetržitý výzkum a rozvoj v oblasti AI a strojového učení vedou k stále sofistikovanějším a efektivnějším chytrým dohledovým systémům. Očekává se, že tyto systémy budou v budoucnu využívat pokročilé technologie hlubokého učení a rozpoznávání obrazu pro ještě přesnější detekci a analýzu bezpečnostních hrozeb. Nové algoritmy umožní těmto systémům identifikovat složité vzory chování a predikovat potenciální bezpečnostní incidenty s větší rychlostí a přesností. Další významný pokrok se projeví ve zlepšení interoperability mezi různými dohledovými systémy a zařízeními, což umožní sdílení a analýzu dat napříč platformami a lokalitami, čímž se zvýší efektivita a schopnost rychlé reakce na incidenty. To bude zahrnovat integraci s dalšími technologiemi, jako jsou senzory internetu věcí (IoT) a kvantové výpočetní techniky, což umožní vytvořit vícevrstevné bezpečnostní sítě.[56][58]

Chytré dohledové systémy se budou dále rozšiřovat do různých sektorů, včetně zdravotnictví, dopravy a energetiky. Ve zdravotnictví mohou být tyto systémy využívány k monitorování pacientů a identifikaci abnormálních chování, což umožní rychlejší zásahy zdravotnického personálu. V dopravě mohou chytré dohledové systémy zlepšit řízení provozu a zvýšit bezpečnost na silnicích pomocí real-time analýzy dat z kamerových systémů. V energetickém sektoru mohou dohledové systémy monitorovat infrastrukturu a předcházet potenciálním hrozbám pro energetické sítě.[60]

S rozvojem AI v chytrých dohledových systémech bude nutné řešit i etické a právní výzvy, které tyto technologie přinášejí. Bude zapotřebí vyvinout nové regulační rámce, které zajistí ochranu soukromí a osobních údajů. Mezinárodní spolupráce bude klíčová při tvorbě norem

a dohod, které budou regulovat používání AI v dohledových systémech a zajistí, že technologie budou používány odpovědně a v souladu s právními předpisy.[61][62][63][64][65]

Pokračující pokrok v oblasti kybernetické bezpečnosti bude hrát klíčovou roli při ochraně dat shromažďovaných chytrými dohledovými systémy. Implementace pokročilých šifrovacích technik a kvantové kryptografie bude nezbytná pro zajištění, že citlivá data zůstanou chráněna před kybernetickými hrozbami. Důraz na bezpečnost dat a ochranu soukromí bude klíčovým faktorem při dalším vývoji a implementaci chytrých dohledových systémů.[56][60][61][62][63][64][65]

4.5 AI v zdravotnictví: Diagnostika a personalizovaná medicína

Příležitosti: Umělá inteligence (AI) nabízí v oblasti zdravotnictví mnoho příležitostí, zejména v diagnostice a personalizované medicíně. AI umožňuje analýzu obrovského množství lékařských dat, což napomáhá přesnější diagnostice nemocí a predikci zdravotních rizik. Například, algoritmy strojového učení mohou analyzovat snímky z lékařských vyšetření a identifikovat vzory, které mohou indikovat přítomnost nemocí dříve, než by to bylo možné pomocí tradičních metod.[66]

Personalizovaná medicína, podpořená AI, umožňuje vytvoření léčebných plánů na míru pro jednotlivé pacienty na základě jejich genetických informací, životního stylu a dalších relevantních dat. To může vést k efektivnějšímu léčení a snížení vedlejších účinků. AI také umožňuje monitorování pacientů v reálném čase, což je klíčové pro řízení chronických onemocnění a prevence akutních zdravotních událostí.[66]

Rizika: S nasazením AI ve zdravotnictví se pojí významná rizika, která je nutné pečlivě zvážit. Jedním z hlavních problémů je bezpečnost a ochrana dat pacientů. AI systémy zpracovávají obrovské množství citlivých informací, které mohou být v případě nedostatečného zabezpečení zneužity. Potenciál zkreslení v důsledku trénovacích dat je další vážné riziko. Pokud jsou trénovací data neúplná nebo zkreslená, AI může poskytovat nesprávné diagnózy a léčebná doporučení. Navíc závislost na technologii může vést k potenciální ztrátě lidského prvku v péči, což může ovlivnit vztah mezi pacientem a lékařem a snížit empatii v péči o pacienty.[67]

Dalším problémem je etické dilema kolem rozhodování založeného na algoritmech. Algoritmy mohou učinit rozhodnutí, která jsou obtížně interpretovatelná a mohou vést k nespravedlivým výsledkům. Například diskriminace pacientů je reálnou hrozbou, pokud AI

systémy neúmyslně zvýhodňují nebo znevýhodňují určité skupiny na základě historických dat. Stejně tak může dojít k diskriminaci klinik, kdy systém může začít automaticky předpokládat, že každý pacient má určitou diagnózu, pokud daná klinika často léčí specifické onemocnění. Tento problém může vést k nesprávným diagnózám a léčbám.[68]

Dalším rizikem je možnost hacknutí systémů. AI systémy mohou být cílem kybernetických útoků, což může vést k úniku citlivých informací nebo manipulaci s daty. Nedostatečná regulace a kontrola nad těmito systémy může vést k neoprávněnému sledování a porušení práv na soukromí jednotlivců. Takové incidenty mohou mít závažné následky pro bezpečnost a soukromí pacientů a mohou podkopat důvěru ve zdravotnické technologie.[69][70][71][72]

Možný vývoj: Budoucnost AI ve zdravotnictví slibuje výrazné inovace a zlepšení v různých oblastech, včetně diagnostiky, léčby, správy zdravotnických dat a péče o pacienty. Jednou z nejdůležitějších oblastí vývoje bude zlepšení přesnosti a rychlosti diagnostických nástrojů. Algoritmy hlubokého učení budou schopny analyzovat rozsáhlé množství dat z různých zdrojů, jako jsou genetická data, snímky z lékařských vyšetření a elektronické zdravotní záznamy, což povede k rychlejšímu a přesnějšímu určení diagnózy a personalizovaným léčebným plánům.[66] Automatizace administrativních úkolů pomocí AI sníží administrativní zátěž pro zdravotnický personál, což jim umožní více se soustředit na péči o pacienty. To zahrnuje správu zdravotnických záznamů, plánování návštěv pacientů a správu pojištění, což zvýší efektivitu zdravotnických systémů. [68]

4.6 Další modelové příklady

Tabulka 10 Další modelové příklady

Příklad	Příležitosti	Rizika	Možný vývoj
AI v energetice	Predikce spotřeby, optimalizace distribuce energie, správa obnovitelných zdrojů.	Kybernetické útoky na energetické sítě, vysoké náklady na implementaci. Blackout AI systému.	Zlepšení efektivity, snížení emisí, stabilizace sítě.
AI v logistice	Optimalizace tras, prediktivní údržba, řízení zásob.	Závislost na technologii, kybernetické útoky.	Zvýšení efektivity, snížení nákladů, rychlejší doručení.
AI v dopravě	Autonomní vozidla, optimalizace dopravního provozu.	Bezpečnostní rizika, právní odpovědnost, ztráta pracovních míst (taxi).	Zlepšení bezpečnosti, snížení dopravních zácp a emisí.
AI v IoT	Automatizace domácností, průmyslová automatizace, prediktivní údržba.	Zranitelnost vůči kybernetickým útokům, soukromí uživatelů, nedostatečná kompatibilita.	Inteligentní města, rozšíření chytrých zařízení a sítí.
AI ve stavebnictví	AI pro plánování projektů, správu zdrojů a predikci rizik.	Ztráta pracovních míst pro tradiční role v odvětví.	Vytváření nových pracovních míst v oblasti AI a robotiky ve stavebnictví.

5 PŘÍLEŽITOSTI VYUŽITÍ NOVÝCH POZNATKŮ Z AI V OBLASTECH BEZPEČNOSTI

Rozvoj AI otevírá nové možnosti pro predikci a prevenci bezpečnostních hrozeb, automatizaci bezpečnostních procesů a vytváření dynamických obranných mechanismů. Příležitosti zahrnují vylepšení existujících bezpečnostních politik a vývoj nových technologií založených na AI – organizace lépe čelí novým a vyvíjejícím se hrozbám. Níže budou blíže popsány příležitosti v konkrétních oblastech bezpečnosti.

5.1 Rozvoj nepřátelské AI a obranných strategií

S rozvojem AI se zvyšuje i riziko nepřátelských AI útoků (Rise of Adversarial AI), které jsou schopné oklamat obranné systémy. Obrana proti těmto hrozbám vyžaduje strategické investice do robustních systémů a rozvoj odolných AI modelů. Tyto zásadní změny otvírají novou kapitolu v ochraně kybernetických prostor, a to také příchodem nové směrnice NIS2. Ta stanovuje nová pravidla a požadavky pro organizace na kybernetickou bezpečnost a tím zase dává bezpečnosti v digitálním prostředí novou úroveň. Implementace NIS2 nejen nařizuje splnění nových požadavků, ale také vyžaduje změnu přístupů a postoje ke kybernetické bezpečnosti. Tyto požadavky má za úkol kontrolovat Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB).[84]

Umělá inteligence je schopna posílit jak obranu, tak útok a tím transformuje celou kybernetickou bezpečnost. Detekční postupy proti hrozbám, u kterých kdysi platila pravidla a určité šablony, již nejsou dostačující. Implementace AI detekčních software je tedy více než nezbytná pro bezpečný chod organizací a samozřejmě kvůli zachování bezpečnosti jejich kybernetických prostor a citlivých informací.[73]

Představme si **hypotetický příklad**, který ilustruje rozvoj nepřátelské AI – Banka má implementovány systémy umělé inteligence a využívá je pro detekci a prevenci kybernetických útoků. Jejich systémy jsou vybaveny AI detekčními technologiemi proti podvodům, nebezpečným anomáliím (např. podezřelé transakce) či systémy pro ochranu a správu citlivých dat, které avšak přestávají splňovat požadavky na kybernetickou bezpečnost podle NIS2 a tím se stávají atraktivním cílem pro nepřátelské AI, která jsou schopny se adaptovat a obcházet tradiční a zastaralé obranné mechanismy. Tato AI využívá technik strojového učení k analýze obranných systémů a k následnému vytváření útoků, které jsou speciálně navrženy, aby systém banky oklamaly. Příkladem techniky pro oklamání systémů AI je

addversial attack – útok, který poskytuje modelu umělé inteligence zavádějící data, které mají za cíl model vést k nesprávným výstupům. Existují různé typy těchto útoků, ale v tomto případě by útočník pravděpodobně využil transakční zprávy tak, aby AI systém, který banka používá pro detekci podvodů, tuto transakci chybně identifikoval jako legitimní. V důsledku toho by mohl útočník převést finanční prostředky z účtu oběti bez vzbuzení podezření. Další relevantní příklad v bankovním sektoru by se týkal použití adversarial útoků k oklamání systémů založených na AI, které banky používají pro ověřování identity a kontrolu KYC (Know Your Customer). Útočník by mohl upravit digitální obrázky občanských průkazů nebo pasů předložených elektronicky během procesu ověřování tak, aby systém nesprávně potvrdil identitu útočníka jako legitimního klienta banky. Tato manipulace by umožnila útočníkům otevřít účty nebo získat finanční služby pod cizí identitou, což by mohlo vést k finančnímu zneužití nebo praní peněz.[74][75][76]

Příkladem obrany proti adversarial útoku je **adversarial training** – v podstatě opak adversarial útoku – model je explicitně trénován, aby nebyl náchylný na tyto útoky tím, že jsou mu záměrně překládány „otrávená data“, aby se stal odolnějším a poznal zavádějící data. Dalším způsobem, jak předejít adversarial útokům je metoda **defensive distillation** – metoda spočívá v trénování modelů pomocí soft labelů (určitá pravděpodobnost, tříděná podle konkrétních kategorií), které jsou generovány z modelu původního (originálního). Toto vytváří zcela nový model, který nese značně méně informací o trénovacích datech než model původní, což útočníkům ztěžuje pokusy o napadení a modelu samotnému to zvyšuje výkon.[76][77]

5.2 Synergie mezi AI a lidskými experty

AI rozšiřuje možnosti lidských expertů v oblasti kybernetické bezpečnosti tím, že automatizuje rutinní úkoly a umožňuje jim se zaměřit na nové hrozby a rizika. Tím, že umělá inteligence dokáže pracovat v reálném čase, je odezva na hrozbu okamžitá. Díky integraci behaviorální analýzy dokáže rozpoznat známé znaky a chování, a tím rychle predikovat potenciónální problém rozeznáním odchylky od normálního chování jednotlivců. AI je schopna uchovávat tyto nepravidelnosti a tím zlepšit detekci potenciálních hrozeb. Tento cílený přístup představuje snížení časového okna zranitelnosti, což znamená aktivní a preventivní postoj ke kybernetické bezpečnosti. Tím se zdůrazňuje důležitost prevence, predikce a rychlé reakce na možné bezpečnostní incidenty. Toto usnadňuje například expertům na kybernetickou bezpečnost práci tím, že se mohou zaměřit na složitější analýzy a strategické

rozhodování, mezitím, co umělá inteligence bude provádět pravidelné kontroly, aktualizace a reakce na známé hrozby a nechá prostor expertům, pro práci s novými predikcemi v kybernetickém prostoru.

5.3 Zajištění soukromí a ochrana dat pomocí AI

Organizace čím dál tím více využívají pokročilé technologie, jako je federované učení – decentralizovaný systém, který spojuje více výpočetních a IoT zařízení, které fungují jako výuková síť – normální model strojového učení funguje tak, že modelu poskytneme zdroje dat, ale u federovaného stylu učení dáváme model strojového učení přímo do zdroje dat.[78] To umožňuje každému uživateli trénovat vlastní kopii modelu díky lokálním datům – ty jsou poté odesílány do hlavního serveru nebo jiného zařízení, které vyhodnocuje parametry a následně aktualizuje globální (hlavní) model. Tento model se používá ke zvýšení přesnosti a kvality trénovacích dat. Tohoto stylu učení, lze využít ve firmách, kde se pracuje s velkým množstvím citlivých informací (například s osobními údaji klientů) a umožňuje udržovat klientské modely zvlášť od modelů centrálních (chrání soukromí při zpracování dat), které by následně plnily své úkoly (predikce a podobně). Toto učení je výhodné pro zvýšení ochrany soukromí klientů a zároveň zajištění bezpečnosti dat bez kompromitování osobních informací.[78]

Další technologií, která zajišťuje větší bezpečnost dat je homomorfní šifrování. Toto šifrování samo o sobě dokáže provádět výpočty a jiné operace se šifrovanými daty, a to i bez znalosti jejího obsahu (bez dešifrování). Tato technika je využívána při zpracování citlivých dat, převážně v cloudových službách a v kombinaci s umělou inteligencí zajišťuje velkou bezpečnost dat a také zlepšuje bezpečnost a soukromí datových analýz.[78]

Umělá inteligence (AI) zlepšuje šifrování informací prostřednictvím inovativního vývoje šifrovacích algoritmů, které jsou pro potenciální hackery obtížněji prolomitelné. Může rovněž asistovat při identifikaci a opravě bezpečnostních slabých míst v šifrovacích protokolech a pro zajištění bezpečného ukládání dat umožňuje AI dynamickou adaptaci bezpečnostních opatření v souladu s aktuálními hrozbami, čímž je zajištěno, že ochrana dat je neustále na maximální úrovni.[78][79]

Schopnost zajištění soukromí a ochrana dat je jedna z předností umělé inteligence, která může mít, při nesprávném používání, fatální následky. Proto Evropský parlament 13. března 2024 schválil nařízení o problematice **Aktu EU o umělé inteligenci** (AI act), který by měl

být platný od roku 2026, přičemž některé regulace budou platné dříve – konkrétně ohledně zakázané umělé inteligence. Toto nařízení bude v EU i ve světě regulovat systémy umělé inteligence ve vztahu k ochraně osobních údajů (GDPR), technické dokumentaci, trénovacím datům a podobně. AI act definuje stupně rizikovosti a nová pravidla, která uživatelé musí dodržovat při implementaci a následném používání AI. To má zajistit, aby systémy umělé inteligence, používané v České republice, byly bezpečné, sledovatelné, transparenční a nediskriminační.[80][81][86]

Jak již bylo zmíněno, umělá inteligence používá federovaného učení, které slouží k vyhodnocování soukromých informací bez jejich narušení a jiné styly učení, které modelům umožňují efektivní analýzu dat a jejich následné zpracování. AI act bude tyto techniky modelů regulovat a nastavovat jim podmínky, které zajistí stoprocentní integritu a transparentnost. Také bude řídit požadavky pro modely, které spadají do kategorie s vysokým rizikem – konkrétně jak bude probíhat hodnocení rizik, testování obrany a protiútoků či jak bude systém hlásit incidenty. Jedním z dalších pravidel, které bude AI act kontrolovat, je registrace umělých inteligencí v databázi EU, vytváření nezákonného obsahu (deepfakes), autorská práva nebo ochrana soukromí.[80][81][82]

Jak již bylo řečeno, AI act bude regulovat a popisovat jednotlivé typy rizikovosti AI modelů. Úrovně rizik plynoucích z AI jsou následující:

1. **Nepřijatelné riziko –** Tyto systémy jsou přímo považovány za hrozbu pro člověka a budou zcela zakázány. Mezi zakázané AI budou patřit: systémy, které používají manipulaci nebo využívají zranitelných skupin (děti, ZTP osoby apod.); biometrické systémy, které pracují „zpětně“ nebo používají citlivé údaje jako je pohlaví, věk, rasa, náboženství a podobně; systémy, které kategorizují lidi na základě jejich chování nebo sociálního postavení.[46][47]

   * Biometrické systémy, které pracují „zpětně“ budou povoleny pouze policejním složkám, pro identifikaci pachatelů nebo stíhání závažných trestních činů.[46]
2. **Vysoké riziko –** Systémy, které spadají do této kategorie, jsou takové, které mají negativní dopad na základní práva občanů a na bezpečnost. Dělí se na dvě kategorie:
   a. **Výrobky využívající systémy AI**, na které se vztahuje právní předpis EU o bezpečnosti výrobků. Patří sem automobily, dětské hračky, zdravotnické pomůcky, nebo výrobky pro letadlový a kosmický průmysl.
   b. **Systémy, které musí být registrovány v databázi EU** (8 kategorií):
      i. Biometrická identifikace, kategorizace osob;

ii. Kritická infrastruktura (správa a provoz);
iii. Odborná příprava, vzdělávání;
iv. Výdělečné činnosti (zaměstnanost, řízení pracovních sil);
v. Soukromé a veřejné služby, dávky;
vi. Vymáhání práva;
vii. Ochrana hranic (řízení migrace, azyl)
viii. Pomoc s právním výkladem a vymáháním [46]

Tyto systémy budou posuzovány před i po uvedení na trh, a to po celou dobu jejich životnosti.[46]

3. **Omezené a minimální riziko –** Do této kategorie spadají generativní umělé inteligence (ChatGPT, Gemini apod.). U této kategorie je kladen důraz na to, aby uživatel vždy věděl, že je v interakci se systémem umělé inteligence a také kdo je za AI systém zodpovědný. Mezi tyto systémy spadá i biometrický kategorizační systém (například rozpoznávání květin) či deepfakes.[47]
   Systémy, které nebudou spadat do žádné kategorie, nebudou mít žádnou speciální právní úpravu a bude pouze důležité, aby uživatel věděl, že komunikuje s robotem či chatbotem.[47][82]

5.4 Nedostatek kvalifikovaných pracovníků a role AI

S narůstajícím počtem kybernetických hrozeb se AI stává klíčovým nástrojem pro překlenutí mezery v dostupnosti kvalifikovaných bezpečnostních expertů. AI může pomoci minimalizovat nedostatek pracovníků v oblasti kybernetické bezpečnosti tím, že automatizuje složité úkoly a usnadní rozhodovací procesy. Taktéž nástroje, jež jsou řízené pomocí AI, posílí profesionály tím, že rozšíří jejich možnosti pro reakci na hrozby a také pomohou s rozhodováním.[83][87][90][91][92]

Dále je umělá inteligence schopna pomoci se školením zaměstnanců v oblasti kybernetické bezpečnosti, a to například pomocí simulačních platforem, které ukáží jak zaměstnavatelům, tak zaměstnancům realistické scénáře a pomohou jim se vyškolit, připravit a přizpůsobit vyvíjejícím se hrozbám. Tyto platformy pro školení, jsou založeny na hlubokém učení a dokáží se přizpůsobit požadavkům a schopnostem jednotlivým osobám. To umožní personalizované a rychlejší učení a zajistí pochopení jakýchkoliv nedostatků v oboru.[83][87][90][91][92]

AI hraje stále důležitější roli v kybernetické bezpečnosti, poskytuje nové nástroje pro detekci a obranu proti hrozbám a umožňuje efektivnější využívání lidských zdrojů. Současně je zřejmé, že vývoj a implementace AI v bezpečnostních systémech musí být doprovázena důkladnou kontrolou a strategickým plánováním, aby se minimalizovala rizika a maximalizovaly příležitosti, které AI přináší.[83][87][90][91][92]

5.5 Národní bezpečnost a obrana

Umělá inteligence přináší řadu příležitostí do národní bezpečnosti a armády, jak ukazuje diskuse na workshopu zaměřeném na využití AI v Armádě ČR. [93] Zástupci armády, včetně expertů na technologie AI, zde zdůrazňovali potřebu integrace nových technologií do vojenského sektoru. Důležitým aspektem je autonomie systémů bez posádky, které musí být schopny reagovat na své okolí podobně, jak by to udělal voják, a spolupracovat s dalšími autonomními systémy, aby mohly plně využít svůj potenciál.[93]

Náčelník generálního štábu zdůraznil význam spolupráce s veřejným a privátním sektorem a poukázal na potřebu navrhovat technologie, které vypadají jako sci-fi, ale jsou klíčové pro budoucnost armády. V kontextu konfliktu na Ukrajině poukázal na to, že armáda nesmí spoléhat pouze na nové technologie, ale musí je chápat jako doplněk k tradičním schopnostem. Autonomní systémy musejí být schopny dosáhnout vysoce autonomního stavu chování, aby plně uplatnily svůj potenciál.[93]

Umělá inteligence má také klíčovou roli ve výcviku, kde se očekává významný pokrok v používání simulačních technologií, virtuální reality a personalizovaného učení. Výcvikové programy využívající rozšířenou a virtuální realitu, která připraví vojáka na situace, které by si jinak nikdy nemohl vyzkoušet, čímž se zvyšuje efektivita a připravenost pro reálné bojové situace.[94]

Umělá inteligence je vnímána jako klíčový prvek pro budoucnost vojenských operací, zvyšování efektivity a přesnosti, a zároveň nabízí nové možnosti ve výcviku a přípravě vojenského personálu.[94]

5.5.1 Autonomní systémy a drony pro průzkum a monitorování.

Implementace umělé inteligence (AI) do autonomních systémů a dronů pro průzkum a monitorování nabízí široké spektrum aplikací a významně zvyšuje jejich efektivitu, adaptabilitu a schopnost provádět složité úkoly. Tato integrace AI s drony umožňuje vytvářet systémy, které mohou autonomně navigovat v komplexních prostředích, zpracovávat data v reálném

čase a adaptovat se na měnící se podmínky, což je klíčové pro úspěšné monitorovací a průzkumné mise.[95]

5.5.1.1 Významné aspekty a aplikace

1. **Autonomní navigace a vyhýbání se překážkám**: AI umožňuje dronům inteligentně se rozhodovat v reálném čase, analyzovat své okolí, detekovat překážky a autonomně plánovat nejefektivnější trasu k dosažení cíle. Tato schopnost je zásadní v aplikacích jako jsou záchranné operace, monitorování a dohled.[95]

2. **Rozpoznávání a sledování objektů**: Díky pokrokům v algoritmech AI mohou drony s přesností identifikovat a sledovat různé objekty. Tato schopnost má obrovské využití v oblastech jako vyhledávání a záchrana, dohled a monitorování. Systémy založené na AI umožňují dronům identifikovat jednotlivce nebo objekty zájmu, sledovat jejich pohyby a v reálném čase poskytovat cenné informace operátorům.[95]

3. **Automatizovaný sběr a analýza dat:** Autonomní drony vybavené AI mají potenciál zefektivnit sběr a analýzu dat v několika odvětvích. Například v zemědělství mohou drony programované pro sběr leteckých snímků a senzorových dat, která jsou poté zpracovávána pomocí algoritmů AI pro monitorování zdraví plodin, detekci anomálií a optimalizaci alokace zdrojů.[95][96]

5.5.1.2 Výzvy a etické úvahy

Používání AI v dronech přináší také výzvy a etické úvahy, zejména v oblastech soukromí a bezpečnosti. Je důležité zabývat se obavami o soukromí, neboť drony vybavené pokročilými kamerami a technologií rozpoznávání obličeje mohou zasahovat do soukromí jedinců. Regulační a právní výzvy spojené s integrací AI v dronech zahrnují vytváření pravidel pro operace dronů, včetně regulací vzdušného prostoru, požadavků na certifikaci a zákony o ochraně dat. Zajištění bezpečnosti a ochrany před neoprávněným přístupem a zneužitím je kritické. [97]

Používání AI v autonomních vozidlech a dronech představuje značné etické a právní výzvy, zejména pokud jde o otázky bezpečnosti, odpovědnosti a zodpovědnosti. Když AI poháněné zařízení, jako je dron nebo autonomní vozidlo, způsobí nehodu, otázka "Kdo je viník?" se stává složitou. Právní systémy se snaží přizpůsobit těmto novým technologiím, ale zatím neexistuje jednotný přístup k určení odpovědnosti. Jedním z klíčových etických zvážení je otázka bezpečnosti. Zatímco autonomní vozidla či drony mají potenciál výrazně snížit počet

nehod způsobených lidskou chybou, mohou také čelit technickým výzvám, které mohou vést k nehodám. V případě nehody zahrnující autonomní vozidlo bude nutné určit, kdo ponese zodpovědnost za škody: výrobce vozidla, vývojáře softwaru nebo vlastníka vozidla.[1]

V současné době právní systémy zkoumají různé metody řešení těchto otázek, ale stále ještě neexistuje globálně přijímaný standard pro určení odpovědnosti v případě nehod způsobených AI. EU chce tyto nejistoty neutralizovat přijetím směrnice Evropského parlamentu a Rady o přizpůsobení pravidel mimosmluvní občanskoprávní odpovědnosti umělé inteligence (AI act), která bude řešit právní otázky odpovědnosti za nehody, které způsobily systémy umělé inteligence. Hlavním cílem bude stanovení výše škody, způsoby prokázání zavinění či prokázání nedostatečné péče. Směrnice AI act je ale zatím pouze v přípravné fázi (očekávaný rok přijetí je 2026), to ale znamená, že první případy, které se objeví do roku přijetí, budou muset náhrady škody vyvíjet a přizpůsobovat za běhu.[98]

5.5.1.3 Budoucí perspektivy

Vývoj v oblasti AI a technologie dronů slibuje ještě sofistikovanější aplikace. Pokroky v algoritmech AI a hardwaru, včetně rychlejších procesorů a efektivnějších senzorů, umožní dronům vykonávat ještě komplexnější úkoly, včetně plně autonomních dlouhých letů, zlepšené energetické účinnosti a zvýšené adaptability na rozmanité prostředí.[97]

Specifické příklady použití AI ve dronových technologiích zahrnují boj proti pytláctví slonů v Africe s využitím dronů Neurala pro monitorování stád slonů a detekci možných pytláků, trénink dronů na leteckých snímcích pomocí AI a strojového učení společností Scale AI pro identifikaci a mapování objektů, nebo vývoj autonomních dronů s použitím „tekutých neuronových sítí“, které umožňují adaptaci na nová prostředí a scénáře.[99]

Vzhledem k těmto pokrokům a aplikacím je zřejmé, že integrace AI do autonomních dronů otevírá nové možnosti pro průzkum a monitorování, zatímco zároveň klade důraz na potřebu řešit výzvy a etické otázky související s jejich používáním.

5.5.2 Protidronový systém

Protidronová technologie je nezbytná pro zajištění bezpečnosti a ochrany v éře, kdy jsou drony stále dostupnější a jejich technologie se neustále vyvíjí. Adaptace a integrace AI do protidronových systémů umožňuje efektivně čelit těmto novým hrozbám a zajišťuje vysokou úroveň ochrany pro kritickou infrastrukturu, vojenské zařízení a veřejná prostranství.[100]

Krom schopnosti operovat v rojích a autonomní navigace, tak již zvládají sebeopravy a adaptace komunikačních frekvencí.[100]

Jak se drony stávají inteligentnějšími a dostupnějšími, tradiční metody jako rušení signálu, spoofing (vydávání se, za někoho jiného) a fyzické zachycení často nestačí. AI drony se snadno vyhnou takovým metodám díky pokročilým navigačním systémům a mohou operovat mimo dosah tradičních záchytných metod. Vzniká tak potřeba sofistikovanějších řešení, jako je analýza protokolů, která nabízí cílenou a adaptabilní strategii pro efektivní neutralizaci AI poháněných dronů bez nežádoucích vedlejších efektů.[100]

Dedrone je příkladem firmy, která vyvíjí pokročilé AI/ML řešení pro ochranu vzdušného prostoru, přičemž klade důraz na přesnost a spolehlivost při detekci dronů a minimalizaci falešných poplachů. Dedrone nabízí flexibilní sady řešení pro různé bezpečnostní požadavky, od leteckého dohledu po kompletní obranné systémy.[101][102][103][104][105]

5.6 Veřejná bezpečnost a dohled

V současné době je využívání umělé inteligence v oblastech veřejné bezpečnosti a dohledu stále častější. Klíčovou aplikací těchto systémů, je strojové učení, které umožňuje rozpoznávání objektů a tváří v reálném čase. To přináší zlepšení městského dohledu a efektivnější hledání hrozeb či podezřelých osob. Systémy městského kamerového dohledového systému (MKDS) umožňují zvýšit schopnost identifikace nelegálních aktivit, přičemž právě schopnost AI analyzovat velké objemy dat (z veřejných kamer, sociálních médií atd.) umožňuje proaktivní přístup ke zločinu, včetně čtení SPZ nebo dokonce predikce a reakce na mimořádné události.[106]

IP kamery mají čím dál větší paměťovou kapacitu, a proto je možné, aby programy umělé inteligence běželi přímo v procesoru kamery, konkrétně v obrazovém a/nebo zvukovém senzoru. Díky tomu není třeba nepřetržitě posílat záznamy do centrálního serveru – šetří se datový přenos, je více zachována ochrana soukromí a také jsou prakticky eliminovány falešné poplachy. Tyto kamery dokáží v reálném čase zpracovávat data a upozornit operátora pouze v případě určitých nadefinovaných stavů (např. do střežené zóny vjelo auto, člověk přelézá plot, na veřejném místě se objevila zbraň…). Samozřejmě kamery nedokáží zpracovávat náročnější operace, a proto právě ty probíhají na serveru.[106][107]

Nicméně implementace AI systémů do bezpečnosti veřejných prostor přináší výzvy v souvislosti s ochranou osobních údajů. Mohou kamery s implementovanou umělou inteligencí

monitorovat prostory 24/7? Diskuse o rovnováze mezi zajištěním bezpečnosti a zachováním soukromí jedinců je stále otevřená. GDPR *(„Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES“)[108]* je soubor přísných pravidel, které upravují, jak se má nakládat s osobními informacemi v EU. V kontextu AI a veřejné bezpečnosti musí být zajištěno, že jakékoli použití technologie pro sledování a analýzu je v souladu s těmito principy. To zahrnuje zajištění, že občané jsou informováni o tom, jak jsou jejich údaje používány, a že existují silná zabezpečovací opatření pro ochranu těchto údajů před neoprávněným přístupem nebo únikem. [107][108][109]

5.7 Osobní bezpečnost

Je hned několik oblastí, kde najde AI své uplatnění v oboru osobní bezpečnosti. Prvním z nich jsou inteligentní domácí bezpečnostní systémy, které stejně jako u MKDS zajišťují dohled nad domácnostmi a jsou schopny detekovat podezřelé anomálie či rozpoznat tváře. To poskytuje lidem v domácnostech nonstop přehled a také jim umožňuje rychleji reagovat na možné hrozby.[110]

Druhou oblastí, kde AI pomáhá s osobní bezpečností jsou aplikace nebo nositelná zařízení, které mají integrovanou umělou inteligenci. Tyto systémy dokáží poskytnout informace záchranářům v reálném čase (např. polohu, nejefektivnější cestu na místo nehody nebo predikce k zajištění lepší péče o pacienta).[111]

V neposlední řadě jsou na místě samozřejmě autonomní vozidla, která slibují větší bezpečnost pro své pasažéry. Tato vozidla jsou schopna reagovat na dopravní podmínky, vyhnout se nebezpečí a mnohem více. Tato vozidla jsou ale ještě stále ve vývoji a než se podaří vyvinout autonomní vozidlo na úrovni 5, bude stále vzrůstat náročnost těchto systémů – to především na kybernetickou bezpečnost, jež se ověřilo už v roce 2015, kdy značka Fiat musela svolat zpět 1,4 milionu vozidel, protože se dali hacknout a poté ovládat na dálku.[112]

Dalšími problémy, se kterými se výrobci autonomních vozidel potýkají, je neustále se měnící prostředí – tím je myšleno počasí, osvětlení, provoz nebo stav vozovky. Proto se společnosti (převážně výzkumníci z Illinois) snaží vyvinout systém, který bude schopen zpracovávat miliony řádků kódu pomocí desítek procesorů a akcelerátorů. Obecně jsou autonomní vozidla stále nebezpečnější než lidé, právě kvůli nedostatku dat, které se týkají mimořádných situací a stále měnícího se prostředí – pravděpodobnost nehod je proto vyšší.[113]

5.8 Bezpečnost na pracovištích

V současné době se umělá inteligence (AI) stává neodmyslitelnou součástí mnoha pracovišť a přináší s sebou značné přínosy v podobě efektivity, automatizace procesů a schopnosti zpracovávat a analyzovat velké objemy dat v reálném čase. Její integrace do různých průmyslových odvětví, od výroby přes zdravotnictví až po finanční služby, transformuje tradiční pracovní postupy a otevírá dveře novým možnostem zvyšování produktivity a inovací.

Avšak s rostoucím nasazením AI na pracovištích se zvyšuje i důraz na aspekty bezpečnosti. Mezi všemi přínosy, které AI nabízí se musí organizace také zabývat dopady, které může AI mít na BOZP. Od kybernetické bezpečnosti a ochrany dat po fyzickou bezpečnost a etické otázky, je zásadní, aby organizace proaktivně přistupovaly k zavádění bezpečnostních opatření a pravidel.[114][115][116]

Stejně jako umělá inteligence může snižovat fyzická rizika v podobě automatizace nebezpečných úkonů pro lidské pracovníky apod., tak také dokáže způsobovat rizika nová. Pokud například autonomní stroje či vozidla nebudou pod drobnohledem a pravidelně kontrolovány, mohou způsobit velké havárie a škody jak na majetku, tak na životech.[114][115][116]

Kapitoly níže popisují klíčové aspekty, jak se zákoník práce a regulace dotýkají využití umělé inteligence na pracovišti a jak mohou tyto technologie formovat budoucnost pracovního práva a ochrany zdraví při práci. Průnik AI do pracovních procesů nabízí nejen příležitosti pro zlepšení efektivity a bezpečnosti, ale také přináší nové výzvy v ochraně práv zaměstnanců a zachování etických standardů. Od aplikací v náboru a výběru zaměstnanců, přes biometrické přístupy a chytré kamerové systémy, až po podporu whistleblowerů, každý z těchto aspektů odráží důležitost pečlivého zvážení etických, právních a sociálních implikací AI. Zároveň je zřejmé, že přizpůsobení stávajících právních rámců a vytvoření nových regulací jsou nezbytným krokem k zajištění, že využití AI bude sloužit jako nástroj pro podporu a ochranu pracovníků, nikoli jako zdroj potenciálních rizik.[114][115][116]

5.8.1 Zákoník práce a AI

Zákoník práce je soubor informací, které řeší vztah mezi zaměstnavatelem a zaměstnancem včetně ochrany zdraví při práci. Umělá inteligence je schopna pomáhat vytvářet lepší a bezpečnější pracovní prostředí – například pomocí simulace scénářů, automatizací nebezpečných úkonů nebo pomocí monitorování zaměstnanců a vyhodnocování situací v reálném čase.

Jednou z klíčových oblastí, kde AI ovlivňuje pracovní právo, je nábor a výběr zaměstnanců. Algoritmy a nástroje strojového učení jsou stále častěji využívány k analýze životopisů, předpovědi výkonnosti pracovníků nebo dokonce provádění analýzy obličeje během pohovorů k hodnocení stability, optimismu nebo pozornosti kandidátů. Ačkoli je použití AI zamýšleno ke zjednodušení procesů a zajištění spravedlivějších pracovních postupů, bylo kritizováno za možnost umožnění systémové diskriminace a replikaci lidských předsudků. Kritickým bodem je, jak jsou algoritmy programovány, protože mohou odrážet předsudky obsažené v datech, na kterých jsou trénovány. Například stát Illinois v USA nebo New York přijímají legislativu zaměřenou na používání AI v pracovním prostředí, která se například týká právě použití AI v náborových systémech.[117][118]

5.8.2 Biometrický přístup, chytré kamerové systémy, GDPR

GDPR (Obecné nařízení o ochraně osobních údajů) klade důraz na ochranu osobních údajů občanů EU, včetně biometrických údajů, které mohou být použity k jednoznačné identifikaci osob. Využití AI pro biometrický přístup nebo pro chytré kamerové systémy na pracovištích přináší zvýšenou úroveň bezpečnosti, ale také vyžaduje pečlivé zvážení ochrany soukromí a dat. Je důležité, aby systémy byly navrženy a provozovány tak, aby respektovaly zásady transparentnosti, zajišťovaly vysokou úroveň ochrany dat a poskytovaly zaměstnancům kontrolu nad jejich osobními údaji.[119]

5.8.3 Whistleblower

Role whistleblowerů (oznamovatelů) je v kontextu AI zásadní, protože mohou odhalovat neetické využívání technologií, porušování právních předpisů týkajících se ochrany osobních údajů (GDPR) nebo jiná rizika a nebezpečí spojená s implementací AI na pracovištích. Podpora a ochrana whistleblowerů jsou klíčové pro zajištění transparentnosti a etického používání AI v průmyslu. V mnoha jurisdikcích existují zákony chránící whistleblowerů před odvetou, což umožňuje bezpečné a důvěrné hlášení potenciálních problémů.[114][120]

PRAKTICKÁ ČÁST

6 JAK BEZPEČNĚ A EFEKTIVNĚ IMPLEMENTOVAT UMĚLOU INTELIGENCI

6.1 Checklist

Tabulka 11 Checklist na fáze projektu

Fáze 1: Příprava a plánování	Status
Identifikace činností, které lze automatizovat	
Stanovení cílů implementace	
Výběr funkcí, technologií a nástrojů AI	
Fáze 2: Sestavení týmu, harmonogramu a rozpočtu	
Určení týmu a odborníků	
Rozdělení klíčových rolí	
Plánování harmonogramu	
1: Příprava a Plánování (1-2 měsíce)	
2: Vývoj a Prototypování (3-6 měsíců)	
3: Nasazení a Implementace (1-3 měsíce)	
4: Hodnocení a Iterace (1-2 měsíce)	
Plánování rozpočtu	
1: Výzkum a vývoj	
2: Nákup nebo licencování software a technologií	
3: Hardware	
4: Externí konzultace a služby	
5: Školení a vzdělávání	
6: Integrace systémů	
7: Zabezpečení a ochrana dat	
8: Testování kvality	
9: Údržba a podpora	
10: Právní a regulační shody	
Fáze 3: Testování a vzdělávání	
Ověřit funkčnost na malém objemu dat	
Provést penetrační testování	
Vzdělávání a rozvoj dovedností zaměstnanců	
Testování AI systému	
Zpětná vazba	
Fáze 4: Implementace a hodnocení	
Hodnocení zákazníkem	
Hodnocení od zaměstnanců	
Ověření právní a regulační shody	
Fáze 5: Monitorování a kontinuální zlepšování	
Na základě zpětné vazby provést úpravy	
Najmutí whistleblowerů	

6.2 Souhrn pro rozhodovací strom

Tabulka 12 Souhrn pro rozhodovací strom

Rozhodovací bod	Popis	Rizika	Doporučení
FÁZE 1			
Identifikace činnosti	Identifikace činností, které lze automatizovat.	Nesprávná identifikace může vést k neefektivní implementaci a nevyužití potenciálu AI.	Proveďte důkladnou analýzu současných procesů a konzultujte s odborníky.
Stanovení vstupů	Určení dat a informací potřebných pro trénování a provoz AI systémů.	Nekvalitní nebo nedostatečná data mohou vést k nízké přesnosti nebo nefunkčnosti AI modelů.	Zajistěte kvalitní, přesná a detailní data.
Stanovení cílů	Definování konkrétních cílů a metrik úspěchu pro AI projekty.	Nejasné cíle mohou vést k nesprávnému použití AI modelů.	Stanovte jasné, měřitelné a dosažitelné cíle.
Výběr funkcí	Určení klíčových funkcí a schopností AI systémů, které budou implementovány.	Výběr nesprávných funkcí může vést k nedostatečnému pokrytí potřeb uživatelů.	Proveďte analýzu potřeb uživatelů a trhu.
FÁZE 2			
Určení týmu	Výběr odborníka/ů a stanovení klíčových rolí (kdo se o co bude starat).	Nedostatečné dovednosti v týmu mohou ohrozit úspěch projektu.	Zajistěte, aby tým zahrnoval odborníky na AI, data, IT a bezpečnost.
Plánování časového harmonogramu	Vytvoření časového plánu pro všechny fáze implementace.	Špatné plánování může vést k zpožděním a překročení rozpočtu.	Stanovte realistické termíny a zahrňte rezervy pro nečekané události.
Plánovaní rozpočtu	Stanovení rozpočtu pro všechny aspekty AI projektu.	Nedostatečné financování může vést k neúplné nebo nekvalitní implementaci.	Vytvořte detailní rozpočet a zahrňte všechny náklady, včetně těch skrytých.
Zajištění bezpečnosti a spolehlivosti systému	Implementování bezpečnostních opatření a testování spolehlivosti systému.	Zranitelnosti mohou vést k bezpečnostním incidentům a ztrátě dat.	Implementujte vícevrstvá bezpečnostní opatření a pravidelně testujte systém.
Zálohování a obnova dat	Vytvoření strategie pro zálohování a obnovu dat.	Ztráta dat může způsobit kritické přerušení operací a nefunkčnost systému.	Zajistěte pravidelné zálohování a testujte obnovitelnost dat.
FÁZE 3			
Vzdělávání a rozvoj	Zajištění školení a rozvoje dovedností pro uživatele a tým.	Nedostatečné školení může vést k neefektivnímu a nebezpečnému používání systému.	Poskytněte pravidelná školení a aktualizace pro všechny zúčastněné strany.
Testování systému AI	Pravidelné testování a ladění AI systémů.	Chyby a nesprávné výsledky mohou vést k nesprávným	Provádějte důkladné testování a využívejte zpětnou vazbu pro zlepšení.

		rozhodnutím a nefunkčnosti modelů.	
Integrace a zpětné vazby	Integrace AI systémů do stávajících procesů a sběr zpětné vazby.	Problémy s integrací mohou narušit stávající operace.	Plánujte postupnou integraci a pravidelně vyhodnocujte zpětnou vazbu.
FÁZE 4			
Komunikace se zákazníky	Informování zákazníků o nových funkcích a změnách.	Nedostatečná komunikace může vést k neporozumění a nesprávnému používání.	Zajistěte pravidelnou komunikaci se zákazníky.
Právní a regulační shoda	Zajištění souladu s právními a regulačními požadavky.	Nesoulad může vést k právním postihům a pokutám.	Pravidelně revidujte a aktualizujte postupy podle platných předpisů.
FÁZE 5			
Monitorování výkonu a efektivity AI	Průběžné sledování a vyhodnocování výkonu a efektivity AI systémů.	Neefektivní systém může vést k plýtvání zdroji a nespokojenosti uživatelů.	Implementujte systémy pro průběžné monitorování a reportování výkonu.
Podpora a ochrana whistleblowerů	Vytvoření mechanismů pro podporu a ochranu těch, kteří hlásí problémy nebo špatné zacházení.	Bez ochrany mohou být whistlebloweři vystaveni odvetě a problémy mohou být zametány pod koberec.	Vytvořte jasné politiky a procesy pro hlášení problémů a zajistěte ochranu whistleblowerů.

6.3 Popis tabulky a rozhodovacího stromu

Rozhodovací strom a souhrnná tabulka, které byly vytvořeny jako součást této práce, slouží jako nástroj pro strukturované plánování a implementaci AI systémů v organizaci. Tyto nástroje poskytují přehled klíčových kroků, rozhodovacích bodů a doporučených akcí, které by měly být zváženy během celého procesu implementace. Je důležité si uvědomit, že diagram a tabulka jsou pouze příkladem a mohou se lišit v závislosti na složitosti projektu, dostupných zdrojích a specifických potřebách. Flexibilita a připravenost na neočekávané výzvy jsou klíčové pro úspěšnou implementaci AI.

6.3.1 Fáze 1: Identifikace a plánování

První fáze je zaměřena na identifikaci hlavních činností a procesů, které budou AI systémy podporovat (automatizovat) nebo zlepšovat. To zahrnuje určení dat potřebných pro trénování a provoz AI systémů, definování konkrétních cílů a metrik úspěchu, a určení klíčových funkcí a schopností AI systémů. Každá firma je unikátní, a proto je tento výběr pouze orientační. Firma si výběr přizpůsobí a rozšíří dle svých požadavků. Nesprávná identifikace nebo nedostatečné stanovení vstupů a cílů může vést k neefektivní implementaci a nevyužití plného potenciálu AI, proto je tato fáze velmi důležitá.

6.3.2 Fáze 2: Příprava a zabezpečení

Druhá fáze se zaměřuje na praktické aspekty plánování a přípravy implementace AI. Tento krok zahrnuje sestavení týmu odborníků, vytvoření časového plánu, plánování rozpočtu a zajištění bezpečnosti a spolehlivosti systému. Klíčovou součástí této fáze je také vytvoření strategií pro zálohování a obnovu dat. Pravidelné zálohování a testování obnovitelnosti dat jsou nezbytné pro ochranu proti ztrátě dat a zajištění kontinuity operací. Tato fáze vyžaduje realistické plánování a zahrnutí rezerv pro neočekávané události. Je důležité mít na paměti, že náklady mohou být velmi variabilní a závislé na specifikách projektu, velikosti firmy, odvětví, ve kterém firma působí, a konkrétních cílech, kterých chce dosáhnout. Doporučuje se vytvořit detailní rozpočtový plán s dostatečnou rezervou pro neočekávané výdaje a případné výzvy, které mohou nastat během implementace AI.

Bezpečnost je v této fázi kritickým faktorem a zahrnuje následující kroky:

Analýza rizik: Tento krok zahrnuje identifikaci a hodnocení potenciálních rizik spojených s implementací AI. To může zahrnovat rizika spojená s ochranou dat, možnostmi zneužití systému, chybami v algoritmech a nepředvídatelným chováním AI systémů.

Identifikace bezpečnostních požadavků: Stanovte bezpečnostní požadavky, které musí AI systém splňovat, včetně ochrany osobních údajů, integrity dat a dostupnosti systémů.

Návrh a implementace bezpečnostních opatření: Navrhněte a implementujte bezpečnostní opatření, která zabrání nebo minimalizují identifikovaná rizika. To může zahrnovat šifrování dat, autentizační mechanismy, systémy pro detekci a reakci na incidenty a pravidelné aktualizace softwaru.

Dopad AI na soukromí: Zvažte, jak AI systém zpracovává a ukládá osobní údaje a zda jsou dodržovány příslušné zákony a normy o ochraně dat.

Testování a validace: Pravidelně testujte AI systém na bezpečnostní slabiny a ověřte, že jsou bezpečnostní opatření efektivní. To zahrnuje penetrační testování a testování odolnosti proti nejrůznějším útokům.

Školení uživatelů a zúčastněných stran: Vzdělávejte uživatele a další zainteresované strany o bezpečnostních aspektech AI systémů a o tom, jak se vyhnout rizikům spojeným s jejich používáním.

Zavedení etických zásad: Definujte a dodržujte etické zásady pro používání AI, zahrnující transparentnost, spravedlnost a odpovědnost.

Monitorování a aktualizace: Pravidelně monitorujte výkon a bezpečnost AI systémů a provádějte potřebné aktualizace softwaru a bezpečnostních protokolů k zajištění trvalé ochrany.

Incidentní řízení a reakční plány: Vypracujte a testujte plány pro řešení bezpečnostních incidentů spojených s AI, včetně protokolů pro okamžité reakce a obnovu systému.

Dodržování regulatorních a právních požadavků: Zajistěte, aby byly všechny aspekty používání AI v souladu s místními zákony a mezinárodními normami.

6.3.3 Fáze 3: Vývoj, testování a vzdělávání

Třetí fáze zahrnuje vzdělávání a rozvoj dovedností pro uživatele a tým, pravidelné testování AI systémů a jejich integraci do stávajících procesů. Pilotní testování je klíčovým krokem, který zahrnuje výběr omezené oblasti nebo procesu jako testovacího prostředí pro AI systém. Je důležité zajistit kvalitní a reprezentativní dataset pro testování, včetně historických dat. Během pilotního testování pečlivě monitorujte výkon systému a sbírejte zpětnou vazbu od uživatelů. Validace výsledků a penetrační testování zaměřené na bezpečnostní aspekty jsou nezbytné pro ověření spolehlivosti a bezpečnosti systému. Na základě získané zpětné vazby proveďte nezbytné úpravy AI systému. Tento cyklus může být opakován vícekrát, dokud nebudou dosaženy uspokojivé výsledky.

6.3.4 Fáze 4: Nasazení a hodnocení

Čtvrtá fáze zahrnuje komunikaci se zákazníky o nových schopnostech a změnách, a zajištění souladu s právními a regulačními požadavky. Nedostatečná komunikace může vést k neporozumění a nesprávnému používání systémů zákazníky, zatímco nesoulad s právními předpisy může vést k právním postihům a pokutám. Pravidelná a jasná komunikace se zákazníky a důsledná revize a aktualizace postupů podle platných předpisů jsou nezbytné pro úspěch této fáze.

6.3.5 Fáze 5: Monitorování a údržba

Pátá fáze je zaměřena na monitorování výkonu a efektivity AI systémů a podporu a ochranu whistleblowerů. Průběžné sledování a vyhodnocování výkonu zajišťuje, že systémy fungují optimálně a že případné problémy jsou rychle identifikovány a řešeny. Vytvoření mechanismů pro podporu a ochranu whistleblowerů je důležité pro zajištění, že všechny problémy a nesrovnalosti jsou hlášeny a řešeny bez rizika odvety pro oznamovatele.

ZÁVĚR

Závěrem této bakalářské práce lze konstatovat, že umělá inteligence má potenciál zásadně transformovat oblast bezpečnosti a přinést inovace, které mohou výrazně zlepšit schopnost detekovat, předcházet a reagovat na různé hrozby. V průběhu práce bylo demonstrováno, jak mohou AI technologie přispět k vyšší efektivitě a rychlosti reakce na kybernetické útoky, zlepšit fyzickou bezpečnost prostřednictvím autonomních dohledových systémů a podpořit národní bezpečnost pomocí pokročilých analytických nástrojů.

Nicméně, s těmito technologickými pokroky přicházejí i nová rizika. Potenciální zneužití AI, chyby v algoritmech, etické problémy a nedostatek transparentnosti jsou faktory, které mohou ohrozit nejen technickou, ale i sociální a etickou stabilitu. Proto je nezbytné, aby organizace věnovaly dostatečnou pozornost bezpečné implementaci AI, zahrnující pravidelný monitoring, aktualizace systémů a důkladné školení zaměstnanců. Jen tak lze zajistit, že AI bude sloužit jako nástroj pro zvýšení bezpečnosti, aniž by představovala nová, nepředvídaná rizika.

Důkladná analýza a pochopení obou stran – přínosů a rizik – jsou klíčové pro odpovědné využívání umělé inteligence. Z této práce vyplývá, že při správné aplikaci může AI přinést významné zlepšení v oblasti bezpečnosti a zároveň vytvořit nové možnosti pro ochranu kritických infrastruktur a osobních dat. Budoucí výzkum a vývoj by měly pokračovat v hledání rovnováhy mezi technologickým pokrokem a bezpečnostními opatřeními, což zajistí, že AI bude moci být nasazena bezpečně a efektivně v souladu s nejnovějšími standardy a etickými normami.

SEZNAM POUŽITÉ LITERATURY

[1] SMEJKAL, V. Kybernetická kriminalita. 3. vyd. Plzeň: Aleš Čeněk, 2022. 1166 s. ISBN 978-80-7380-849-5.

[2] SAP. What is Artificial Intelligence? [online]. SAP, n.d. Dostupné z: https://www.sap.com/cz/products/artificial-intelligence/what-is-artificial-intelligence.html [cit. 2024-05-20].

[3] Evropský parlament. Umělá inteligence: definice a využití [online]. 4.9.2020, aktualizováno 21.11.2023. Dostupné z: https://www.europarl.europa.eu/news/cs/headlines/society/20200827STO85804/umela-inteligence-definice-a-vyuziti [cit. 2024-05-20].

[4] KUBÍČEK. Historie umělé inteligence [online]. n.d. Dostupné z: https://kubicek.ai/historie-umele-inteligence/ [cit. 2024-05-20].

[5] MLCollage. Historie umělé inteligence [online]. n.d. Dostupné z: https://www.mlcollege.com/historie-umele-inteligence/ [cit. 2024-05-20].

[6] Rascasone. Umělá inteligence (AI) trendy [online]. n.d. Dostupné z: https://www.rascasone.com/cs/blog/umela-inteligence-ai-trendy [cit. 2024-05-20].

[7] KAPOUN, Jan. Průkopníci informačního věku: John McCarthy. ComputerWorld [online]. 14.3.2012. Dostupné z: https://www.computerworld.cz/clanky/prukopnici-informacniho-veku-john-mccarthy/ [cit. 2024-05-20].

[8] Barton Studio. Historie umělé inteligence [online]. 16.8.2023. Dostupné z: https://www.bartonstudio.cz/historie-umele-inteligence/ [cit. 2024-05-20].

[9] Patria.cz. Korejský 18násobný světový mistr hry Go byl poražen strojem od Google [online]. 9.3.2016. Dostupné z: https://www.patria.cz/zpravodajstvi/3148287/korejsky-18nasobny-svetovy-mistr-hry-go-byl-porazen-strojem-od-google.html [cit. 2024-05-20].

[10] Deeply. Vše o umělé inteligenci [online]. 2023. Dostupné z: https://deeply.cz/vse-o-umela-inteligence/ [cit. 2024-05-20].

[11] Elements of AI. Elements of AI [online]. 2023. Dostupné z: https://course.elementsofai.com/cs/1/3 [cit. 2024-05-20].

[12] Rascasone. Strojové učení (ML) metody klasifikace [online]. 13.4.2021. Dostupné z: https://www.rascasone.com/cs/blog/strojove-uceni-ml-metody-klasifikace [cit. 2024-05-20].

[13] IBM. AI model [online]. n.d. Dostupné z: https://www.ibm.com/topics/ai-model [cit. 2024-05-20].

[14] SAP. What is Machine Learning? [online]. n.d. Dostupné z: https://www.sap.com/cz/products/artificial-intelligence/what-is-machine-learning.html [cit. 2024-05-20].

[15] Shaip. What is AI Image Recognition and How Does it Work? [online]. 17.5.2022. Dostupné z: https://cs.shaip.com/blog/what-is-ai-image-recognition-and-how-does-it-work/ [cit. 2024-05-20].

[16] Hashdork. Artificial intelligence in cybersecurity [online]. 11.9.2023. Dostupné z: https://hashdork.com/cs/artificial-intelligence-in-cybersecurity/ [cit. 2024-05-20].

[17] Deeply. Hluboké učení [online]. n.d. Dostupné z: https://deeply.cz/hluboke-uceni/ [cit. 2024-05-20].

[18] Deeply. Zpracování přirozeného jazyka [online]. n.d. Dostupné z: https://deeply.cz/blog/zpracovani-prirozeneho-jazyka [cit. 2024-05-20].

[19] Unite AI. Co je zpracování přirozeného jazyka [online]. n.d. Dostupné z: https://www.unite.ai/cs/co-je-zpracovani-prirozeneho-jazyka/ [cit. 2024-05-20].

[20] NGSS. Umělá inteligence a kybernetická bezpečnost [online]. 24.2.2023. Dostupné z: https://www.ngss.cz/clanek/umela-inteligence-a-kyberneticka-bezpecnost-2023-02-24 [cit. 2024-05-20].

[21] Unite AI. 10 Ways Artificial Intelligence is Shaping Secure App Development [online]. 17.11.2023. Dostupné z: https://www.unite.ai/cs/10-ways-artificial-intelligence-is-shaping-secure-app-development/ [cit. 2024-05-20].

[22] Rezac, J. Závěrečná práce [online]. 2021. Ambis. Dostupné z: https://is.ambis.cz/th/fendi/Zaverecna_prace_Jan_Rezac_49399.pdf [cit. 2024-05-20].

[23] Unite AI. Nové hranice v generativním AI daleko od cloudu [online]. n.d. Dostupné z: https://www.unite.ai/cs/nové-hranice-v-generativním-AI-daleko-od-cloudu/ [cit. 2024-05-20].

[24] ČERVENKA, Tomáš. Závěrečná práce [online]. 2020. Univerzita Karlova. Dostupné z: https://dodo.is.cuni.cz/bitstream/handle/20.500.11956/116834/120352629.pdf?sequence=1&isAllowed=y [cit. 2024-05-20].

[25] Mach, Václav. Český minority report IURE [online]. 12/2023. Dostupné z: https://digitalnisvobody.cz/wp-content/uploads/2024/01/cesky_minority_report_iure_23.pdf [cit. 2024-05-20].

[26] CAMPBELL, Jason R., HENDRIX, Michael T., KIM, Emily S., MOORE, Natalie A. Counterintelligence Artificial Intelligence and National Security: Synergy and Challenges [online]. Preprint. March 2024. DOI: 10.13140/RG.2.2.29778.36583. Dostupné z: https://www.researchgate.net/publication/362438500_Counterintelligence_Artificial_Intelligence_and_National_Security_Synergy_and_Challenges [cit. 2024-05-20].

[27] SRIVASTAVA, Kushal. Artificial Intelligence and National Security: Perspective of the Global South. International Journal of Law in Changing World. 2023, 2(2), 77-87. DOI: 10.54934/ijlcw.v2i2.63. Dostupné z: https://www.researchgate.net/publication/374918858 [cit. 2024-05-20].

[28] POTTER, Kaledio, LETHO, Julia R., RUSSELL, E. AI and National Security: The Geopolitical Implications of Autonomous Weapons and Cybersecurity. The Open Artificial Intelligence Journal. October 2023. DOI: 10.13140/RG.2.2.27455.60983. Dostupné z: https://www.researchgate.net/publication/374918858 [cit. 2024-05-20].

[29] SCHMIDT, Eric. AI, Great Power Competition & National Security. Dædalus, the Journal of the American Academy of Arts & Sciences. 2022, 151(2), 288-294. DOI: 10.1162/DAED_a_01916. Dostupné z: https://www.researchgate.net/publication/364726744_AI_Great_Power_Competition_National_Security [cit. 2024-05-20].

[30] FBI. Counterintelligence [online]. n.d. Dostupné z: https://www.fbi.gov/investigate/counterintelligence [cit. 2024-05-20].

[31] Bezpečnostní informační služba (BIS). Kontraspionáž [online]. n.d. Dostupné z: https://www.bis.cz/kontraspionaz/ [cit. 2024-05-20].

[32] Clever and Smart. Analýza rizik, identifikace hrozeb [online]. 26. 06. 2009, aktualizováno 13.10.2012. Dostupné z: https://www.cleverandsmart.cz/analyza-rizik-identifikace-hrozeb/ [cit. 2024-05-20].

[33] ČERMÁK, Miroslav. Řízení informačních rizik v praxi. Brno: Tribun EU, 2023. Knihovnicka.cz. ISBN 978-80-263-1794-4.

[34] Generali Česká pojišťovna. Kybernetická hrozba umělé inteligence [online]. n.d. Dostupné z: https://www.generaliceskaprofi.cz/ze-zivota/kyberneticka-hrozba-umele-inteligence [cit. 2024-05-20].

[35] Vláda České republiky. Národní akční plán umělé inteligence květen 2019 [pdf]. 2019. Dostupné z: https://vlada.gov.cz/assets/evropske-zalezitosti/umela-inteligence/NAIS_kveten_2019.pdf [cit. 2024-05-20].

[36] NGSS. Umělá inteligence a kybernetická bezpečnost [online]. 24.2.2023. Dostupné z: https://www.ngss.cz/clanek/umela-inteligence-a-kyberneticka-bezpecnost-2023-02-24 [cit. 2024-05-20].

[37] KUBÍČEK. 100 zaměstnání, kde se bez AI neobejdete [online]. n.d. Dostupné z: https://kubicek.ai/100-zamestnani-kde-se-bez-ai-neobejdete/ [cit. 2024-05-20].

[38] Kaspersky Daily. AI in Darknet [online]. n.d. Dostupné z: https://dfi.kaspersky.com/blog/ai-in-darknet [cit. 2024-05-20].

[39] Ministerstvo vnitra ČR. Riziko [online]. 2003. Dostupné z: https://www.mvcr.cz/clanek/riziko.aspx [cit. 2024-05-20].

[40] Ministerstvo vnitra ČR. Hrozba [online]. 2003. Dostupné z: https://www.mvcr.cz/clanek/hrozba.aspx [cit. 2024-05-20].

[41] LUKÁŠ, Luděk a kolektiv. Bezpečnostní technologie, systémy a management III. Zlín: VeRBuM, 2013. ISBN 978-80-87500-35-4.

[42] Clever and Smart. Řízení rizik umělé inteligence [online]. 3.5.2023. Dostupné z: https://www.cleverandsmart.cz/rizeni-rizik-umele-inteligence/ [cit. 2024-05-20].

[43] Clever and Smart. Řízení rizik umělé inteligence - 2. díl [online]. 12.6.2023. Dostupné z: https://www.cleverandsmart.cz/rizeni-rizik-umele-inteligence-2-dil/ [cit. 2024-05-20].

[44] National Institute of Standards and Technology. NIST Special Publication on Artificial Intelligence NIST.AI.100-1 [pdf]. 1/2023. Dostupné z: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf [cit. 2024-05-20].

[45] Investigace.cz. Testování hranic AI: rizika zneužití chatbotu [online]. 14.8.2023. Dostupné z: https://www.investigace.cz/testovani-hranic-ai-rizika-zneuziti-chatbotu/ [cit. 2024-05-20].

[46] Dreport. Představení systému AI s vysokým rizikem [online]. n.d. Dostupné z: https://www.dreport.cz/blog/predstaveni-systemu-ai-s-vysokym-rizikem/ [cit. 2024-05-20].

[47] Dreport. Představení AI systému s nepřijatelným, omezeným a minimálním rizikem [online]. n.d. Dostupné z: https://www.dreport.cz/blog/predstaveni-ai-systemu-s-neprijatelnym-omezenym-a-minimalnim-rizikem/ [cit. 2024-05-20].

[48] RIZVI, Mohammed. Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention. International Journal of Advanced Engineering Research and Science (IJAERS). 2023, 10(5), 55-60. DOI: 10.22161/ijaers.105.8. Dostupné z: https://www.researchgate.net/publication/371131032_Enhancing_cybersecurity_The_power_of_artificial_intelligence_in_threat_detection_and_prevention [cit. 2024-05-20].

[49] RAJ, Rohit; KUMAR, Jayant; KUMARI, Akriti. How AI Used to Prevent Cyber Threats. International Research Journal of Computer Science (IRJCS). 2022, 9(7), 146-151. DOI: 10.26562/irjcs.2022.v0907.002. Dostupné z: https://www.researchgate.net/publication/362468803_How_AI_Used_to_Prevent_Cyber_Threats [cit. 2024-05-20].

[50] AL-HAWAMLEH, Ahmad Mtair. Predictions of Cybersecurity Experts on Future Cyber-Attacks and Related Cybersecurity Measures. International Journal of Advanced Computer Science and Applications (IJACSA). 2023, 14(2), 801-812. DOI: 10.14569/IJACSA.2023.0140292. Dostupné z: https://www.researchgate.net/publication/370401571_Predictions_of_Cybersecurity_Experts_on_Future_Cyber-Attacks_and_Related_Cybersecurity_Measures [cit. 2024-05-20].

[51] BHARADIYA, Jasmin Praful. AI-Driven Security: How Machine Learning Will Shape the Future of Cybersecurity and Web 3.0. American Journal of Neural Networks and Applications. 2023, 9(1), 1-7. DOI: 10.11648/j.ajnna.20230901.11. Dostupné z: https://www.researchgate.net/publication/371562853_AI-Driven_Security_How_Machine_Learning_Will_Shape_the_Future_of_Cybersecurity_and_Web_30 [cit. 2024-05-20].

[52] SCHMIDT, Eric. AI, Great Power Competition & National Security. Dædalus, the Journal of the American Academy of Arts & Sciences. 2022, 151(2), 288-295. DOI: 10.1162/DAED_a_01916. Dostupné z: https://www.researchgate.net/publication/371131032_AI_Great_Power_Competition_National_Security [cit. 2024-05-20].

[53] SRIVASTAVA, Kushal. Artificial Intelligence and National Security: Perspective of the Global South. International Journal of Law in Changing World. 2023,

2(2), 77-87. DOI: 10.54934/ijlcw.v2i2.63. Dostupné z: https://www.researchgate.net/publication/377499536_Artificial_Intelligence_and_National_Security_Perspective_of_the_Global_South [cit. 2024-05-20].

[54] ZIADÉ, M. Fouad; DAHER, Malak Mohamad; ZIADÉ, Abdallah M. Artificial Intelligence for Money Laundering Detection. In: Artificial Intelligence and Data Science in Financial Services [online]. 2024. DOI: 10.4018/979-8-3693-1046-5. Dostupné z: https://www.researchgate.net/publication/377499536_Artificial_Intelligence_for_Money_Laundering_Detection [cit. 2024-05-20].

[55] ODEYEMI, Olubusola; MHLONGO, Noluthando Zamanjomane; NWANKWO, Ekene Ezinwa; SOYOMBO, Oluwatobi Timothy. Reviewing the Role of AI in Fraud Detection and Prevention in Financial Services. International Journal of Science and Research Archive. 2024, 11(01), 2101-2110. DOI: 10.30574/ijsra.2024.11.1.0279. Dostupné z: https://www.researchgate.net/publication/371562853_Reviewing_the_Role_of_AI_in_Fraud_Detection_and_Prevention_in_Financial_Services [cit. 2024-05-20].

[56] ARDABILI, Babak Rahimi; PAZHO, Armin Danesh; NOGHRE, Ghazal Alinezhad; NEFF, Christopher Gorman et al. Understanding Policy and Technical Aspects of AI-Enabled Smart Video Surveillance to Address Public Safety [online]. Preprint. March 2023. DOI: 10.48550/arXiv.2302.04310. Dostupné z: https://www.researchgate.net/publication/369550562_Understanding_Policy_and_Technical_Aspects_of_AI-Enabled_Smart_Video_Surveillance_to_Address_Public_Safety [cit. 2024-05-20].

[57] BHAVYASRI, J.; RAMAIAH, G. N. Kodanda; RASADURAI, K. AI Based Smart Surveillance System. International Journal of Scientific Research in Science, Engineering and Technology. 2023, 10(1), 10-15. DOI: 10.32628/IJSRSET229672. Dostupné z: https://www.researchgate.net/publication/371499536_AI_Based_Smart_Surveillance_System [cit. 2024-05-20].

[58] Security Magazine. The Evolution of AI and Physical Security [online]. n.d. Dostupné z: https://www.securitymagazine.com/articles/100128-the-evolution-of-ai-and-physical-security [cit. 2024-05-20].

[59] YOUVAN, Douglas C. Shadows and Silhouettes: The Invisible Filter on National Security Figures in AI Recognition [online]. Preprint. March 2024. DOI:

10.13140/RG.2.2.29898.38081. Dostupné z: https://www.researchgate.net/publication/379345059_Shadows_and_Silhouettes_The_Invisible_Filter_on_National_Security_Figures_in_AI_Recognition [cit. 2024-05-20].

[60] Forbes Tech Council. How AI is Disrupting the Business of Physical Security [online]. 2023. Dostupné z: https://www.forbes.com/sites/forbestechcouncil/2023/09/27/how-ai-is-disrupting-the-business-of-physical-security/ [cit. 2024-05-20].

[61] G4S. Artificial Intelligence and its Applications in Physical Security [online]. n.d. Dostupné z: https://www.g4s.com/en-gb/what-we-do/security-solutions/commercial-security-systems/tech-talks/artificial-intelligence-and-its-applications-in-physical-security [cit. 2024-05-20].

[62] Unite AI. AI přeplňuje možnosti bezpečnostních kamer [online]. n.d. Dostupné z: https://www.unite.ai/cs/ai-přeplňuje-možnosti-bezpečnostních-kamer/ [cit. 2024-05-20].

[63] Appinventiv. AI in Surveillance System [online]. n.d. Dostupné z: https://appinventiv.com/blog/ai-in-surveillance-system/ [cit. 2024-05-20].

[64] AITech. AI Smart Surveillance [online]. n.d. Dostupné z: https://www.ai-tech.vision/products/ai-smart/ai-smart-surveillance/ [cit. 2024-05-20].

[65] Viso. Computer Vision Applications in Surveillance and Security [online]. n.d. Dostupné z: https://viso.ai/applications/computer-vision-applications-in-surveillance-and-security/ [cit. 2024-05-20].

[66] Siemens Advanta. Generative AI in Healthcare [online]. n.d. Dostupné z: https://www.siemens-advanta.com/featured-articles/generative-ai-healthcare?acz=1&gad_source=1&gclid=Cj0KCQjw3ZayBhDRARIsAPWzx8qdLo8G67v0_GVK5Ca3cX1-jkKGdrtCSBPgzC7_pSOvld5JzNN5T68aAhyuEALw_wcB [cit. 2024-05-20].

[67] Foreseemed. Artificial Intelligence in Healthcare [online]. n.d. Dostupné z: https://www.foreseemed.com/artificial-intelligence-in-healthcare [cit. 2024-05-20].

[68] Thomson Reuters. AI Usage in Healthcare [online]. 27.8.2023. Dostupné z: https://www.thomsonreuters.com/en-us/posts/technology/ai-usage-healthcare/ [cit. 2024-05-20].

[69] Netguru. Artificial Intelligence in Hospitals [online]. 2.4.2024. Dostupné z: https://www.netguru.com/blog/artificial-intelligence-in-hospitals [cit. 2024-05-20].

[70] LAPU. AI in Health Care Industry [online]. n.d. Dostupné z: https://www.lapu.edu/ai-health-care-industry/ [cit. 2024-05-20].

[71] IBM. AI Healthcare Benefits [online]. 11.6.2023. Dostupné z: https://www.ibm.com/think/insights/ai-healthcare-benefits [cit. 2024-05-20].

[72] HealthITAnalytics. Top 12 Ways Artificial Intelligence Will Impact Healthcare [online]. 23.4.2024. Dostupné z: https://healthitanalytics.com/news/top-12-ways-artificial-intelligence-will-impact-healthcare [cit. 2024-05-20].

[73] Data Platform Cloud IBM. Federated Learning [online]. 14.8.2023. Dostupné z: https://dataplatform.cloud.ibm.com/docs/content/wsj/analyze-data/fl-homo.html?context=wx&locale=cs&audience=wdp [cit. 2024-05-20].

[74] Built In. AI in Banking [online]. 13.3.2023. Dostupné z: https://builtin.com/artificial-intelligence/ai-in-banking [cit. 2024-05-20].

[75] CC. Umělá inteligence čím dál více proniká do bankovního sektoru: největší hráči na trhu se bez ní neobejdou [online]. 13.2.2024. Dostupné z: https://cc.cz/brandstory/umela-inteligence-cim-dal-vice-pronika-do-bankovniho-sektoru-nejvetsi-hraci-na-trhu-se-bez-ni-neobejdou/ [cit. 2024-05-20].

[76] OpenAI. Attacking Machine Learning with Adversarial Examples [online]. 24.2.2017. Dostupné z: https://openai.com/research/attacking-machine-learning-with-adversarial-examples [cit. 2024-05-20].

[77] Nature. [online]. 29.8.2022. Dostupné z: https://www.nature.com/articles/s41467-022-33266-0 [cit. 2024-05-20].

[78] Data Platform Cloud IBM. Federated Learning [online]. 14.8.2023. Dostupné z: https://dataplatform.cloud.ibm.com/docs/content/wsj/analyze-data/fl-homo.html?context=wx&locale=cs&audience=wdp [cit. 2024-05-20].

[79] Unite AI. Co je federované učení? [online]. n.d. Dostupné z: https://www.unite.ai/cs/co-je-federované-učení/?fbclid=IwAR1mli4il_R3RZ0FAIKZpfxImJMjRPJ8wNZKYw3z4dgPmYHYOSeCPZrQFds [cit. 2024-05-20].

[80] Evropský parlament. Akt EU o umělé inteligenci: první nařízení o AI na světě [online]. 14.6.2023. Dostupné z: https://www.europarl.europa.eu/topics/cs/article/20230601STO93804/akt-eu-o-umele-inteligenci-prvni-narizeni-o-ai-na-svete?fbclid=IwAR22CU8pgSTs_GgAid0DVvO40RCO6IQaw-9wbmL5jSfnzSlt5OYNveD8s4I [cit. 2024-05-20].

[81] Asociace AI. EU AI Act [online]. 1.4.2024. Dostupné z: https://asociace.ai/eu-ai-act/?fbclid=IwAR11c7JTdI-J0TVlXBNP_rc_39sznZqwU77NdT7V0Pu3FBGsakfcfx_odD0 [cit. 2024-05-20].

[82] Digital Strategy EU. Regulatory Framework for AI [online]. n.d. Dostupné z: https://digital-strategy.ec.europa.eu/cs/policies/regulatory-framework-ai [cit. 2024-05-20].

[83] Rank Tracker. The Intersection of AI and Cybersecurity: Shaping a New Era of Protection [online]. 8.8.2023. Dostupné z: https://www.ranktracker.com/cs/blog/the-intersection-of-ai-and-cybersecurity-shaping-a-new-era-of-protection/ [cit. 2024-05-20].

[84] InSmart. Kyberbezpečnost v roce 2024 [online]. 4.1.2024. Dostupné z: https://insmart.cz/kyberbezpecnost-v-roce-2024/ [cit. 2024-05-20].

[85] Unite AI. Trendy kybernetické bezpečnosti v roce 2024 [online]. n.d. Dostupné z: https://www.unite.ai/cs/Trendy-kybernetické-bezpečnosti-v-roce-2024/ [cit. 2024-05-20].

[86] GDPR.cz. Umělá inteligence v kybernetické bezpečnosti: nepřítel nebo pomocník [online]. 16.11.2023. Dostupné z: https://www.gdpr.cz/umela-inteligence-v-kyberneticke-bezpecnosti-nepritel-nebo-pomocnik [cit. 2024-05-20].

[87] NCP40.cz. Generativní AI v kybernetické bezpečnosti: nové výzvy a možnosti [online]. n.d. Dostupné z: https://www.ncp40.cz/aktuality/generativni-ai-v-kyberneticke-bezpecnosti-nove-vyzvy-a-moznosti [cit. 2024-05-20].

[88] Ministerstvo obrany ČR. Národní centrum kybernetických operací vypracovalo strategii kybernetické obrany ČR [online]. 6.8.2018. Dostupné z: https://mocr.army.cz/informacni-servis/zpravodajstvi/narodni-centrum-kybernetickych-operaci-vypracovalo-strategii-kyberneticke-obrany-cr-201906/ [cit. 2024-05-20].

[89] Unite AI. Jak AI snižuje náklady na únik dat [online]. n.d. Dostupné z: https://www.unite.ai/cs/jak-ai-snižuje-náklady-na-únik-dat/?fbclid=IwAR19xy-MvoGiBAqtZHQBBFNQKwGHePTv5_3SZo_1GFwcSj-anaf0KfSekAgI [cit. 2024-05-20].

[90] Techwire Asia. How can AI and cybersecurity bridge APAC's talent gap [online]. 19.8.2023. Dostupné z: https://techwireasia.com/09/2023/how-can-ai-and-cybersecurity-bridge-apacs-talent-gap/ [cit. 2024-05-20].

[91] World Economic Forum. Cybersecurity and AI: Challenges and Opportunities [online]. 5.6.2023. Dostupné z: https://www.weforum.org/agenda/2023/06/cybersecurity-and-ai-challenges-opportunities/#:~:text=URL%3A%20https%3A%2F%2Fwww.weforum.org%2Fagenda%2F2023%2F06%2Fcybersecurity [cit. 2024-05-20].

[92] Cybersecurity Dive. Cybersecurity Talent Gap: Worker Shortage [online]. 5.1.2023. Dostupné z: https://www.cybersecuritydive.com/news/cybersecurity-talent-gap-worker-shortage/639724/ [cit. 2024-05-20].

[93] Novinky. Umělá inteligence pomůže armádě při výcviku i překonávání nedostatků [online]. 3.4.2022. Dostupné z: https://www.novinky.cz/clanek/internet-a-pc-umela-inteligence-pomuze-armade-pri-vycviku-i-prekonavat-nedostatky-40392622 [cit. 2024-05-20].

[94] Armáda ČR. Umělá inteligence a průlomové technologie pro vojáky: Armáda podepsala memorandum o spolupráci s ČVUT [online]. 25.4.2023. Dostupné z: https://acr.army.cz/informacni-servis/zpravodajstvi/umela-inteligence-a-prelomove-technologie-pro-vojaky--armada-podepsala-memorandum-o-spolupraci-s-cvut--243412/ [cit. 2024-05-20].

[95] Analytics Insight. Future Role of AI in Autonomous Drones [online]. 5.1.2023. Dostupné z: https://www.analyticsinsight.net/future-role-of-ai-in-autonomous-drones/ [cit. 2024-05-20].

[96] GAO RFID. Columbia Leads RFID, BLE, IOT Drones [online]. n.d. Dostupné z: https://gaorfid.com/cs/columbia-leads-rfid-ble-iot-drones/ [cit. 2024-05-20].

[97] BBVA OpenMind. AI and Drones [online]. 11.12.2023. Dostupné z: https://www.bbvaopenmind.com/en/technology/artificial-intelligence/ai-and-drones/ [cit. 2024-05-20].

[98] Právní Prostor. Směrnice o odpovědnosti za umělou inteligenci [online]. 8.11.2023. Dostupné z: https://www.pravniprostor.cz/clanky/pravo-it/smernice-o-odpovednosti-za-umelou-inteligenci [cit. 2024-05-20].

[99] MIT News. Drones Navigate Unseen Environments with Liquid Neural Networks [online]. 19.4.2023. Dostupné z: https://news.mit.edu/2023/drones-navigate-unseen-environments-liquid-neural-networks-0419 [cit. 2024-05-20].

[100] Sentrycs. The Evolution of AI in Drones: Implications [online]. n.d. Dostupné z: https://sentrycs.com/the-counter-drone-blog/the-evolution-of-ai-in-drones-implications- [cit. 2024-05-20].

[101] Dedrone. [Hlavní stránka] [online]. n.d. Dostupné z: https://www.dedrone.com [cit. 2024-05-20].

[102] Drone Operator. How Do Drones Communicate? Unraveling the Mystery [online]. 17.9.2023. Dostupné z: https://www.drone-operator.com/how-do-drones-communicate-unraveling-the-mystery/ [cit. 2024-05-20].

[103] Elsight. Drone Connectivity for Unmanned Aerial Vehicles Explained [online]. 6.7.2023. Dostupné z: https://www.elsight.com/blog/drone-connectivity-for-unmanned-aerial-vehicles-explained/ [cit. 2024-05-20].

[104] Defense One. Pentagon Already Testing Tomorrow's AI-Powered Swarm Drones Ships [online]. 22.1.2024. Dostupné z: https://www.defenseone.com/technology/2024/01/pentagon-already-testing-tomorrows-ai-powered-swarm-drones-ships/393528/ [cit. 2024-05-20].

[105] Swyvl. The Dawn of a New Era: AI Drones and the Future of Autonomous Mapping [online]. 28.11.2023. Dostupné z: https://www.swyvl.io/blog/the-dawn-of-a-new-era-ai-drones-and-the-future-of-autonomous-mapping [cit. 2024-05-20].

[106] Securitas. Technologie na odhalení zbraní už testuje pražský IKEM [online]. 17.12.2020. Dostupné z: https://www.securitas.cz/novinky--blog/blog/technologie-na-odhaleni-zbrani-uz-testuje-prazsky-ikem/ [cit. 2024-05-20].

[107] Securitas. Moderní chytré kamery: Jak funguje analýza s pomocí AI [online]. 14.7.2022. Dostupné z: https://www.securitas.cz/novinky--blog/blog/moderni-chytre-kamery--jak-funguje-analyza-s-pomoci-ai/ [cit. 2024-05-20].

[108] Ministerstvo vnitra ČR. Co je GDPR [online]. n.d. Dostupné z: https://www.mvcr.cz/gdpr/clanek/co-je-gdpr.aspx [cit. 2024-05-20].

[109] ePrávo. Umělá inteligence a právo: patrně první rozsudek ve věci umělé inteligence [online]. 3.11.2023. Dostupné z: https://www.epravo.cz/top/clanky/umela-inteligence-a-pravo-patrne-prvni-rozsudek-ve-veci-umele-inteligence-117132.html [cit. 2024-05-20].

[110] MDPI. [online]. 2023. Dostupné z: https://www.mdpi.com/1424-8220/23/15/6979 [cit. 2024-05-20].

[111] Surec. Benefits of AI-Powered Emergency Response Apps [online]. n.d. Dostupné z: https://surec.ca/benefits-of-ai-powered-emergency-response-apps/ [cit. 2024-05-20].

[112] Securities.io. AI za volantem: Jak umělá inteligence řídí vývoj autonomních vozidel [online]. n.d. Dostupné z: https://www.securities.io/cs/ai-za-volantem-toho%2C-jak-umělá-inteligence-řídí-vývoj-autonomních-vozidel/ [cit. 2024-05-20].

[113] Unite AI. Škálovatelné nástroje pro bezpečnost autonomních vozidel vyvinuté výzkumníky [online]. n.d. Dostupné z: https://www.unite.ai/cs/škálovatelné-nástroje-pro-bezpečnost-autonomních-vozidel-vyvinuté-výzkumníky/ [cit. 2024-05-20].

[114] Bezpečnost Práce. Jak AI mění BOZP [online]. 2.5.2023. Dostupné z: https://www.bezpecnostprace.info/umela-inteligence-ai/jak-ai-meni-bozp/ [cit. 2024-05-20].

[115] Bezpečnost Práce. Umělá inteligence (AI) studie REDECA [online]. 2.11.2023. Dostupné z: https://www.bezpecnostprace.info/umela-inteligence-ai/studie-redeca/#tab1 [cit. 2024-05-20].

[116] EU-OSHA. Impact of Artificial Intelligence on Occupational Safety and Health [online]. 7.1.2021. Dostupné z: https://osha.europa.eu/cs/publications/impact-artificial-intelligence-occupational-safety-and-health [cit. 2024-05-20].

[117] American Bar Association. AI in the Workplace [online]. 10.6.2022. Dostupné z: https://www.americanbar.org/groups/labor_law/publications/labor_employment_law_news/spring-2022/ai-in-the-workplace/ [cit. 2024-05-20].

[118] UK Parliament, House of Commons Library. Research Briefing: CBP-9817 [online]. 11.8.2023. Dostupné z: https://commonslibrary.parliament.uk/research-briefings/cbp-9817/ [cit. 2024-05-20].

[119] IEEE Xplore. [online]. 2019. Dostupné z: https://ieeexplore.ieee.org/abstract/document/8622621 [cit. 2024-05-20].

[120] Bezpečnost Práce. Whistleblowing: ochrana oznamovatelů [online]. 2.2.2024. Dostupné z: https://www.bezpecnostprace.info/pracovni-pravo/whistleblowing-ochrana-oznamovatelu [cit. 2024-05-20].

[121] Seznam.cz. Romeo: Jak umělá inteligence pomáhá v oblasti bezpečnosti a prevenci kriminality [online]. 4.3.2023. Dostupné z:

https://medium.seznam.cz/clanek/romeo-jak-umela-inteligence-pomaha-v-oblasti-bezpecnosti-a-prevenci-kriminality-4090 [cit. 2024-05-20].

[122] KOVÁŘ, David. Umělá inteligence k předpovídání trestné činnosti: skutečnost nebo fikce? [online]. 13.12.2023. AI Novinky. Dostupné z: https://ainovinky.cz/umela-inteligence-k-predpovidani-trestne-cinnosti-skutecnost-nebo-fikce/ [cit. 2024-05-20].

[123] HOLUB, Dušan. Využití umělé inteligence u dronů [online]. 2021. Západočeská univerzita V Plzni. Dostupné z: https://courseware.zcu.cz/CoursewarePortlets2/DownloadDokumentu?id=210374 [cit. 2024-05-20].

[124] Evropský parlament. Umělá inteligence: Jaké jsou výhody a nevýhody [online]. Vytvořeno 23.9.2020, aktualizováno 21.11.2023. Dostupné z: https://www.europarl.europa.eu/news/cs/headlines/society/20200918STO87404/umela-inteligence-jake-jsou-vyhody-a-nevyhody [cit. 2024-05-20].

[125] VACÍKOVÁ, Michala. [online]. 2017. Masarykova univerzita. Dostupné z: https://nlp.fi.muni.cz/uui/referaty2017/michala_vacikova/referat.pdf [cit. 2024-05-20].

[126] MagicSky. Jaké jsou výhody a nevýhody umělé inteligence [online]. n.d. Dostupné z: https://magicsky.cz/blogs/news/jake-jsou-vyhody-a-nevyhody-umele-inteligence [cit. 2024-05-20].

[127] Mali Computer. Umělá inteligence: Co to vlastně je a co nás čeká? [online]. n.d. Dostupné z: https://www.malicomputer.cz/blog/umela-inteligence-co-to-vlastne-je-a-co-nas-ceka/ [cit. 2024-05-20].

[128] VALUT, Zdeněk. Jaké výhody a úskalí sebou přináší umělá inteligence [online]. 28.4.2023. LinkedIn. Dostupné z: https://cz.linkedin.com/pulse/jaké-výhody-úskalí-sebou-přináší-umělá-inteligence-ydealcz [cit. 2024-05-20].

[129] ČVUT. Akce: Staň se na den expertem či expertkou na AI [online]. n.d. České vysoké učení technické v Praze. Dostupné z: https://kyr.fel.cvut.cz/akce-stan-se-na-den-expertem-ci-expertkou-na-ai-stredoskolakum-ukazala-vyhody-i-nevyhody-umele [cit. 2024-05-20].

[130] Infosys BPM. Artificial Intelligence in Physical Security Systems [online]. n.d. Dostupné z: https://www.infosysbpm.com/blogs/annotation-services/artificial-intelligence-in-physical-security-systems.html [cit. 2024-05-20].

[131] USAID. USAID Artificial Intelligence Ethics Checklist [online]. 2023. Dostupné z: https://www.usaid.gov/sites/default/files/2023-12/USAID%20Artificial%20Intelligence%20Ethics%20Checklist.pdf [cit. 2024-05-20].

[132] EY Česká republika. Jan Pich: Umělá inteligence je pouze tak dobrá, jaká jsou data [online]. n.d. Dostupné z: https://www.ey.com/cs_cz/technology/jan-pich-umela-inteligence-je-pouze-tak-dobra-jaka-jsou-data [cit. 2024-05-20].

[133] Sedlakova Legal. Implementace umělé inteligence v právní praxi [online]. n.d. Dostupné z: https://www.sedlakovalegal.cz/uploads/Am7f0T9IKCzaToSop-KunsvfsLrPrPPHF.pdf [cit. 2024-05-20].

[134] SystemOnline. AI se sama do firmy nenasadí, potřebujete strategii: Jednotlivé výzvy – řešení [online]. n.d. Dostupné z: https://m.systemonline.cz/business-intelligence/ai-se-sama-do-firmy-nenasadi-potrebujete-strategii.htm [cit. 2024-05-20].

[135] Deloitte Česká republika. Trustworthy AI: Dokumenty - AI Act, implementace do corporate governance procesů, evaluace rizik, digitální/ovládací prvky AI/algoritmy [online]. n.d. Dostupné z: https://www2.deloitte.com/cz/cs/pages/risk/solutions/trustworthy-ai.html [cit. 2024-05-20].

[136] Cesta do Cloudu. Jak vaší firmě pomůže umělá inteligence a proč potřebuje cloud [online]. n.d. Dostupné z: https://www.cestadocloudu.cz/blog/jak-vasi-firme-pomuze-umela-inteligence-a-proc-potrebuje-cloud/ [cit. 2024-05-20].

[137] Eprávo. Proč a jak nastavit pravidla pro užívání AI ve vaší společnosti [online]. n.d. Dostupné z: https://www.epravo.cz/top/clanky/proc-a-jak-nastavit-pravidla-pro-uzivani-ai-ve-vasi-spolecnosti-117011.html [cit. 2024-05-20].

[138] Globema. Cloud vs. on-premise: Stručná příručka [online]. n.d. Dostupné z: https://www.globema.cz/cloud-vs-premise-strucna-prirucka/ [cit. 2024-05-20].

[139] PCWorld. Kybernetická bezpečnost: Člověk vs. umělá inteligence [online]. n.d. Dostupné z: https://www.pcworld.cz/clanky/kyberneticka-bezpecnost-clovek-vs-umela-inteligence/ [cit. 2024-05-20].

[140] YouTube. What is AI? [online video]. Dostupné z: https://www.youtube.com/watch?v=Bc3stMxxW0s [cit. 2024-05-20].

[141] ComputerWorld. Umělá inteligence v kybernetické válce [online]. n.d. Dostupné z: https://www.computerworld.cz/clanky/umela-inteligence-v-kybernetickevalce/ [cit. 2024-05-20].

[142] RMOL. Motorem současného vývoje IT bezpečnosti je umělá inteligence [online]. n.d. Dostupné z: https://www.rmol.cz/novinky/motorem-soucasneho-vyvoje-it-bezpecnosti-je-umela-inteligence [cit. 2024-05-20].

[143] MBI. Rizika kybernetické bezpečnosti spojená s aplikací umělé inteligence v autonomních vozidlech [pdf]. 2021. Dostupné z: https://www.mbi.expert/wp-content/uploads/2021/04/Rizika-kyberneticke-bezpecnosti-spojena-s-aplikaci-umele-inteligence-v-autonomnich-vozidlech.pdf [cit. 2024-05-20].

[144] Feedit. Umělá inteligence je velká příležitost, ale také hrozba, varuje IT společnost Eviden [online]. 31.7.2023. Dostupné z: https://feedit.cz/2023/07/31/umela-inteligence-je-velka-prilezitost-ale-take-hrozba-varuje-it-spolecnost-eviden/ [cit. 2024-05-20].

[145] Root.cz. Postřehy z bezpečnosti: Umělá inteligence na dráze zločinu [online]. n.d. Dostupné z: https://www.root.cz/clanky/postrehy-z-bezpecnosti-umela-inteligence-na-draze-zlocinu/ [cit. 2024-05-20].

[146] ITPoint. Kyberbezpečnost a AI [online]. n.d. Dostupné z: https://www.itpoint.cz/gfi/?i=kyberbezpecnost-ai-15264 [cit. 2024-05-20].

[147] Centrum kyberbezpečnosti. Bez umělé inteligence (AI) bude kyberbezpečnost nemyslitelná [online]. n.d. Dostupné z: https://centrumkyberbezpecnosti.cz/bez-umele-inteligence-ai-bude-kyberbezpecnost-nemyslitelna/ [cit. 2024-05-20].

[148] CISA. Artificial Intelligence [online]. n.d. Dostupné z: https://www.cisa.gov/ai [cit. 2024-05-20].

[149] IBM. AI Cybersecurity [online]. n.d. Dostupné z: https://www.ibm.com/ai-cybersecurity#3 [cit. 2024-05-20].

[150] Innefu. Artificial Intelligence in Defence Technology [online]. n.d. Dostupné z: https://www.innefu.com/blog/artificial-intelligence-in-defence-technology [cit. 2024-05-20].

[151] SDI. The Most Useful Military Applications of AI [online]. n.d. Dostupné z: https://sdi.ai/blog/the-most-useful-military-applications-of-ai/ [cit. 2024-05-20].

[152] FlySight. Artificial Intelligence in Military Technology: 8 Applications Examples [online]. n.d. Dostupné z: https://www.flysight.it/artificial-intelligence-in-military-technology-8-applications-examples/ [cit. 2024-05-20].

[153] LinkedIn. Top 10 AI Applications for Military Use [online]. n.d. Dostupné z: https://www.linkedin.com/pulse/top-10-ai-applications-military-use-markets-us-icjgf [cit. 2024-05-20].

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AI	Artificial Intelligence
ML	Machine Learning
DL	Deep Learning
ANN	Artificial Neural Network
NLP	Natural Language Processing
AGI	Artificial General Intelligence
ASI	Artificial Super Intelligence
ANI	Artificial Narrow Intelligence
IoT	Internet of Things
GDPR	General Data Protection Regulation
SIEM	Security Information and Event Management
DAST	Dynamic Application Security Testing
SAST	Static Application Security Testing
BOZP	Bezpečnost a ochrana zdraví při práci
CCTV	Closed-Circuit Television
API	Application Programming Interface
GAN	Generative Adversarial Networks
CNN	Convolutional Neural Networks
RNN	Recurrent Neural Networks
SVM	Support Vector Machines
SKV	Systém Kontroly Vstupu
CI	Counter Intelligence
URL	Uniform Resource Locator
IP	Internet Protocol

MitM	Man in the Middle
NIS	Network a Information Security
NÚKIB	Národní Úřad pro Kybernetickou a Informační Bezpečnost
NIST	National Institute of Standards and Technology
OSN	Organizace Spojených Národů
NATO	North Atlantic Treaty Organization
AML	Anti Money Laundering
EU	Evropská Unie
KYC	Know Your Customer
SPZ	Státní Poznávací Značka

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: VÝVOJOVÝ DIAGRAM

Přiloženo jako soubor typu JPG na CD v práci ve složce Prilohy.zip.