

Umělá inteligence v oblasti ochrany obyvatelstva

Bc. Petr Kociňák

Diplomová práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně

Fakulta logistiky a krizového řízení

Ústav ochrany obyvatelstva

Akademický rok: 2024/2025

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Bc. Petr Kociňák
Osobní číslo:	L23308
Studijní program:	N1032A020002 Bezpečnost společnosti
Specializace:	Ochrana obyvatelstva
Forma studia:	Prezenční
Téma práce:	Umělá inteligence v oblasti ochrany obyvatelstva

Zásady pro vypracování

- Popište vývoj umělé inteligence.
- Zpracujte literární rešerši zaměřenou na problematiku umělé inteligence v oblasti ochrany obyvatelstva.
- Zhodnotte nasazení prvků umělé inteligence v ochraně obyvatelstva.
- Na základě zjištění plynoucích z předchozích bodů navrhnete doporučení/opatření pro zlepšení stávající situace.

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

Seznam doporučené literatury:

1. KNIHOVÁ, Ladislava. *AI marketing playbook: jak ChatGPT a umělá inteligence mění svět marketingu*. Praha: Grada, 2024. ISBN 978-802-7152-261.
2. MAŘÍK, Vladimír; TRČKA, Michal a ČERNÝ, David. *Proč se nebát umělé inteligence?: AI pohledem nejen českých odborníků*. Brno: Jota, 2024. ISBN 978-80-7689-459-4.
3. NEUMAN, W. Russell. *Evolutionary Intelligence: How Technology Will Make us Smarter*. Cambridge, Massachusetts: The MIT Press, 2023. ISBN 978-0-262-04848-4.
4. RUSSELL, Stuart J. *Jako člověk: umělá inteligence a problém jejího ovládnutí*. Žilina: Argo, 2021. ISBN 978-80-7363-810-8.
5. SHARMA, Abhinav; JAIN, Arpit; ARYA, Ashwini Kumar a RAM, Mangey (ed.). *Artificial Intelligence for Signal Processing and Wireless Communication*. De Gruyter Series on the Applications of Mathematics in Engineering and Information Sciences. Berlin: De Gruyter, 2022. ISBN 978-3-11-073882-7.

Další doporučená literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **Ing. Pavel Tomášek, Ph.D.**
Ústav ochrany obyvatelstva

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

L.S.

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

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2024

PROHLÁŠENÍ AUTORA DIPLOMOVÉ PRÁCE

Beru na vědomí, že

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

Prohlašuji, že

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

V Uherském Hradišti, dne 25.04.2025

.....
podpis autora

ABSTRAKT

Tato práce se zaměřuje na využití umělé inteligence, dále jen (AI) v oblasti ochrany obyvatelstva, zejména v kontextu krizového řízení a první pomoci. Cílem práce bylo analyzovat současný stav implementace AI v mobilních aplikacích určených pro tyto účely a navrhnout koncept ideální aplikace, která by mohla zvýšit efektivitu zásahů a zlepšit koordinaci mezi uživateli a Integrovaným záchranným systémem, dále jen (IZS).

Teoretická část práce představuje vývoj AI, její současné technologie a etické problémy spojené s jejím používáním. Praktická část se zaměřuje na analýzu vybraných aplikací, jako jsou Záchranka, PulsePoint Respond, EchoSOS, GoodSAM a Life360 - z hlediska jejich funkčnosti, přínosů a omezení. Na základě této analýzy byl navržen koncept aplikace „True Life Guardian“, která integruje pokročilé funkce, jako je prediktivní analýza, automatizované rozhodování a zpracování velkých objemů dat.

Analýza SWOT navrhované aplikace identifikovala klíčové silné a slabé stránky a zdůraznila potřebu technologických inovací a širší meziinstitucionální spolupráce. Výsledky práce potvrdily, že AI má značný potenciál pro další zefektivnění krizového řízení a že navrhovaný koncept aplikace může být cenným příspěvkem k modernizaci nástrojů ochrany obyvatelstva.

Klíčová slova: umělá inteligence, ochrana obyvatelstva, krizové řízení, první pomoc, mobilní aplikace

ABSTRACT

This thesis focuses on the use of artificial intelligence, hereafter referred to as (AI) in the field of public protection, particularly in the context of crisis management and first aid. The aim of the work was to analyse the current state of AI implementation in mobile applications designed for these purposes and to propose a concept of an ideal application that could increase the efficiency of interventions and improve coordination between users and the Integrated Rescue System, hereafter referred to as (IRS).

The theoretical part of the thesis presents the development of AI, its current technologies, and ethical issues related to its use. The practical part focuses on the analysis of selected applications such as Záchranka, PulsePoint Respond, EchoSOS, GoodSAM, and Life360 - in terms of their functionality, benefits, and limitations. Based on this analysis, the concept of a "True Life Guardian" application was proposed, which integrates advanced features such as predictive analytics, automated decision-making, and big data processing.

A SWOT analysis of the proposed application identified key strengths and weaknesses and highlighted the need for technological innovation and wider inter-institutional collaboration. The results of the work confirmed that AI has considerable potential to further streamline crisis management and that the proposed application concept can be a valuable contribution to the modernization of public protection tools.

Keywords: artificial intelligence, public protection, crisis management, first aid, mobile application

Na tomto místě bych rád poděkoval mému vedoucímu diplomové práce panu Ing. Pavlu Tomáškoví, Ph.D. za cenné rady, odborné vedení, podporu a trpělivost při zpracování této práce. Jeho vstřícnost, podnětné připomínky a profesionální přístup mi byly velkou oporou a motivací při řešení zvoleného tématu.

Rád bych mu také poděkoval za důvěru, kterou mi během zpracování této práce projevil, a za čas, který mi věnoval.

OBSAH

ÚVOD.....	13
CÍL PRÁCE A POUŽITÉ METODY	14
I TEORETICKÁ ČÁST	16
1 VÝVOJ UMĚLÉ INTELIGENCE	17
1.1 HISTORIE UMĚLÉ INTELIGENCE.....	17
1.2 BUDOUCNOST UMĚLÉ INTELIGENCE	19
1.3 ETICKÉ VÝZVY UMĚLÉ INTELIGENCE	20
1.3.1 Právní a regulační rámce pro umělou inteligenci.....	22
1.3.2 Umělá inteligence a lidská práva	23
1.3.3 Umělá inteligence a dezinformace	25
1.4 TECHNOLOGIE UMĚLÉ INTELIGENCE	26
1.4.1 Strojové učení a hluboké učení	27
1.4.2 Generativní umělá inteligence – ChatGPT a jeho využití v praxi	28
1.4.3 Umělá inteligence v reálném čase – Nasazení v rámci integrovaného záchranného systému	29
2 VYUŽITÍ UMĚLÉ INTELIGENCE V OBLASTI OCHRANY OBYVATELSTVA.....	31
2.1 LITERÁRNÍ REŠERŠE K VYUŽITÍ UMĚLÉ INTELIGENCE V OCHRANĚ OBYVATELSTVA.....	32
2.2 KRIZOVÉ ŘÍZENÍ S PODPOROU UMĚLÉ INTELIGENCE	33
2.2.1 Predikce přírodních katastrof s pomocí umělé inteligence	34
2.2.2 Řízení krizových situací s využitím umělé inteligence.....	35
2.2.3 Plánování obnovy po katastrofách s pomocí umělé inteligence	36
2.3 BEZPEČNOST OBYVATELSTVA A VEŘEJNÝ DOHLED S VYUŽITÍM UMĚLÉ INTELIGENCE	38
2.3.1 Monitorování veřejných prostor.....	39
2.3.2 Prediktivní modely pro prevenci kriminality	40
2.3.3 Umělá inteligence v boji proti terorismu a extremismu.....	41
2.3.4 Ochrana soukromí a etické výzvy veřejného dohledu	42
3 VÝZVY A OMEZENÍ UMĚLÉ INTELIGENCE V OCHRANĚ OBYVATELSTVA.....	44
3.1 TECHNOLOGICKÉ LIMITY A SPOLEHLIVOST UMĚLÉ INTELIGENCE SYSTÉMŮ	45
3.2 NEDOSTATEK DAT A JEJICH KVALITA	46
3.3 ODOLNOST UMĚLÉ INTELIGENCE VŮČI KYBERNETICKÝM HROZBÁM.....	47
4 DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI	49
II PRAKTICKÁ ČÁST.....	51
5 APLIKACE PRO POSKYTOVÁNÍ PRVNÍ POMOCI	52
5.1 APLIKACE ZÁCHRANKA	53

5.2	PULSEPOINT RESPOND	59
5.3	ECHOSOS	64
5.4	GOODSAM	69
5.5	LIFE360.....	74
6	NÁVRH IDEÁLNÍ APLIKACE TRUE LIFE GUARDIAN APP.....	79
6.1	KLÍČOVÉ VLASTNOSTI APLIKACE.....	81
6.2	UMĚLÁ INTELIGENCE V APLIKACI.....	83
6.3	SWOT ANALÝZA APLIKACE TRUE LIFE GUARDIAN.....	87
	ZÁVĚR	105
	SEZNAM POUŽITÉ LITERATURY.....	107
	SEZNAM OBRÁZKŮ	115
	SEZNAM TABULEK.....	116
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	117

ÚVOD

Mimořádné události, jako jsou přírodní katastrofy, havárie, technické poruchy nebo jiné krizové situace, mohou udeřit kdykoli a kdekoli a zasáhnout jednotlivce i celé komunity. Klíčem ke zvládnutí těchto situací je včasná reakce, účinné krizové řízení a dostupnost správných informací. V posledních letech se v této oblasti stále více využívají moderní technologie, zejména umělá inteligence, dále jen (AI), která má potenciál výrazně zefektivnit rozhodovací procesy, předvídat vývoj událostí a podpořit koordinaci mezi obyvatelstvem a záchrannými složkami.

Zejména mobilní aplikace využívající AI začínají hrát důležitou roli při ochraně obyvatelstva, a to nejen v oblasti prevence, ale i při samotné reakci na krizové situace a následné obnově. Aplikace jako Záchranka, PulsePoint Respond, EchoSOS, GoodSAM nebo Life360 nabízejí nové způsoby, jak rychle přivolat pomoc, sdílet polohu nebo varovat před hrozcím nebezpečím. Jejich analýzou můžeme lépe pochopit výhody, ale i omezení současných řešení.

S vývojem AI se zvyšují i očekávání veřejnosti a odborníků ohledně funkčnosti a spolehlivosti těchto nástrojů. Už nejde jen o jednoduchá oznámení nebo funkce založené na poloze, AI nyní dokáže například předvídat pravděpodobnost určitého typu události na základě historických dat, automaticky rozpoznávat rizikové chování nebo personalizovat krizová doporučení podle individuální situace uživatele. Takový vývoj klade nové nároky nejen na samotnou technologii, ale také na otázky etiky, bezpečnosti dat a důvěry veřejnosti v algoritmičké rozhodování v kritických okamžicích.

Cílem této práce je nejen zhodnotit současný stav využití AI pro ochranu obyvatelstva, ale také navrhnout vlastní koncept ideální aplikace pro krizové řízení a první pomoc - aplikaci „True Life Guardian“. Práce vychází z teoretického rámce vývoje AI, jejích technologických možností a etických otázek spojených s jejím využitím. Na základě analýzy vybraných aplikací a poznatků je navrženo řešení, které by mohlo účinně reagovat na současné i budoucí výzvy v oblasti ochrany obyvatelstva.

Vzhledem k rostoucím rizikům a měnící se povaze hrozeb je důležité nejen vyhodnocovat současná technologická řešení, ale také aktivně hledat nové způsoby využití potenciálu AI k záchraně životů a minimalizaci škod. Výsledkem této práce je proto návrh nástroje, který kombinuje prvky AI, krizového řízení a uživatelsky přívětivého prostředí s cílem podpořit připravenost a reakci běžných občanů i profesionálních záchranných služeb.

Cíl práce a použité metody

Diplomová práce se zaměřuje na možnosti využití AI v oblasti ochrany obyvatelstva, konkrétně prostřednictvím mobilních aplikací pro první pomoc a krizovou komunikaci. V souvislosti s rostoucím rizikem přírodních katastrof, kybernetických hrozeb a dalších mimořádných událostí se digitální nástroje jeví jako důležitá součást moderního krizového řízení. Tato práce analyzuje stávající mobilní aplikace pro krizovou komunikaci a první pomoc (Záchranka, PulsePoint Respond, EchoSOS, GoodSAM a Life360) a poté navrhuje koncept inovativní aplikace s AI True Life Guardian, která by mohla zefektivnit reakci na mimořádné události.

Cíl práce:

Cílem diplomové práce je analyzovat vybrané mobilní aplikace určené pro poskytování první pomoci a krizovou komunikaci (Záchranka, PulsePoint Respond, EchoSOS, GoodSAM a Life360) z hlediska jejich funkčnosti, přínosů a omezení. Na základě této analýzy je následně navržena ideální podoba nové aplikace s názvem True Life Guardian, která by s využitím AI efektivněji podporovala ochranu obyvatelstva v krizových situacích.

Dílčí cíle:

Provést literární rešerši zaměřenou na vývoj a aktuální využití AI v oblasti ochrany obyvatelstva.

- Identifikovat a popsat nejvíce využívané aplikace pro první pomoc a krizové situace.
- Analyzovat vybrané aplikace z hlediska jejich silných a slabých stránek a poskytnout návrhy na jejich zlepšení.
- Navrhnout koncepční podobu aplikace True Life Guardian s důrazem na prediktivní a analytické schopnosti využívající AI.
- Realizovat SWOT analýzu navržené aplikace a zhodnotit možnosti jejího rozvoje.
- Zhodnotit reálnou možnost implementace této aplikace jako samostatného řešení, či jako rozšíření stávajících nástrojů (např. Záchranka).
- V následujících částech je popsán hlavní cíl práce, dílčí cíle a dále metody použité k jejich dosažení. Důraz je kladen na propojení teoretického rámce

s praktickou aplikací, komparaci současných řešení a syntézu návrhového řešení s využitím AI.

Použité metody

- Při zpracování diplomové práce byly použity následující výzkumné a analytické metody:
- Literární rešerše – pro zajištění teoretického rámce a identifikaci současných trendů, konceptů a aplikací v oblasti AI a krizového řízení. Byly využívány odborné knihy, články, zprávy a online databáze (s důrazem na zdroje od roku 2015).
- Analýza případových studií a existujících aplikací – komparativní přístup umožnil porovnat funkce pěti významných aplikací (Záchranka, PulsePoint Respond, EchoSOS, GoodSAM a Life360) z hlediska jejich relevance pro ochranu obyvatelstva.
- SWOT analýza – systematické vyhodnocení silných a slabých stránek, příležitostí a hrozeb navržené aplikace True Life Guardian s využitím vícekritériálního rozhodování. Výsledkem bylo zvolení strategie typu WO (využití příležitostí k překonání slabin).
- Analytické a syntetické metody – pro zpracování získaných poznatků, identifikaci souvislostí a formulaci návrhů a závěrů.
- Koncepční návrh – byl použit při návrhu ideální aplikace, jejích klíčových funkcí, způsobů využití AI a možností začlenění do současného systému ochrany obyvatelstva.

I. TEORETICKÁ ČÁST

1 VÝVOJ UMĚLÉ INTELIGENCE

Umělá inteligence, dále jen (AI) je věda o aplikaci a vývoji systémů, které lze snadno použít k provádění všech úkolů, které vyžadují lidskou inteligenci. Jak říkají Stuart Russell a Peter Norvig ve své knize *Artificial Intelligence: A Modern Approach* (2020), AI zahrnuje širokou škálu metod a přístupů od řešení problémů a logického odvozování až po strojové učení, rozpoznávání vzorů a plánování (Russell et al., 2021).

Takový vývoj v oblasti AI se připisuje četným technologickým a teoretickým pokrokům, které položily základy pro nové aplikace a přístupy. Mezi důležité mezníky tohoto vývoje patří: strojové učení, hluboké učení a generativní modely. Tyto technologie mohou způsobit revoluci v řadě průmyslových odvětví, která potenciálně ovlivňují také krizové řízení a sektor veřejné bezpečnosti, a jsou využívány v národní bezpečnosti i dalších oblastech souvisejících s veřejnou bezpečností (Sharma et al., 2022).

S neustálým pokrokem technologie AI lze vidět, že život bude podle technologie formován i dál v budoucnu. Již nyní AI přebírá klíčovou roli v konkrétních oblastech zdravotnictví, pomáhá s diagnostikovaním nemocí a ve finančním aparátu pomáhá s analýzou rizik a průběžného předvídání tržních trendů. V oblasti ochrany obyvatelstva nabízí AI pokročilé výhody, protože pokud jde o předpovídání důležitých přírodních katastrof, může poskytnout případnou pomoc na pracovišti. Dále napomáhá při řešení krizových situací a odstraňování následků mimořádných katastrof. Díky těmto pokrokům se AI stává nejen klíčovou součástí běžného života, ale i její role má v budoucnu potenciál se dále rozšiřovat (Russell et al., 2021).

Vyvíjející se pokroky AI vyvolávají otázky týkající se inteligence, etiky a možností budoucího soužití lidí a strojů. A protože stále více lidí je nahrazováno stroji, které mohou vykonávat práci, kterou kdysi vykonávali oni sami, je třeba se zabývat otázkou, jak bude AI začleněna do našich sociálních a politických institucí (Neuman, 2023).

1.1 Historie umělé inteligence

Historie AI je bohatá a fascinující, přičemž k prvním významným mezníkům došlo ve 40. a 50. letech 20. století, kdy vědci jako Alan Turing začali pokládat základy tohoto oboru. Na základě Turingovy teorie „Turingova stroje“ a následného návrhu testu nazvaného Turingův test je jednou z důležitých otázek pro návrh testů úvaha, zda se stroje mohou učit podobně

jako lidé inteligentnímu chování. Tento test se stal první snahou o zjištění, zda je možné sestavit stroj, který by dokázal „myslet“ stejně jako člověk (Russell et al., 2021).

Rok 2015 byl v historii AI velmi důležitým mezníkem, protože bylo dosaženo mnoha průlomových objevů v oblasti hlubokého učení. Jedná se o podmnožinu strojového učení - tzv. hluboké učení - kde jsou víceúrovňové neuronové sítě schopny řešit složité problémy. Lecun, Bengio a Hinton zdůraznili přelomový rok, kdy hluboké učení začalo ovládat oblast zpracování obrazu, rozpoznávání řeči a další aplikace. To vše bylo umožněno pokrokem v oblasti hardwaru a dostupností výkonných souborů dat, díky čemuž se hlubokému učení podařilo dosáhnout takové úrovně přesnosti, o které se dříve jen zdálo (Lecun et al., 2015).

Výzkum AI v oblasti generativních modelů schopných generovat realistické obrázky, texty a videa získal po roce 2015 na popularitě. Koncept generativních adversariálních sítí (GAN) představili Goodfellow a et al., v roce 2014 a ukázal neuvěřitelně super výsledky s novými daty, co ho uchvátila. Stala se z nich super zbraň na tvorbu krásných obrázků, co hodně ovlivňuje vědu, design a simulace (Yao et al., 2023).

Další velký krok pro AI byl v roce 2016, když AlphaGo od DeepMind porazil světového šampiona ve hře Go. Jednalo se o přelomový úspěch; dlouho se mělo za to, že ve hře Go, která je nesmírně složitá, není v silách stroje zvítězit. AlphaGo proto dosáhl nejen potenciálního uplatnění AI v logických hrách, ale také ukázal, že AI je schopna učení velkých dat a dokáže rozpoznat vzory v neznámých situacích (Silver, 2016).

Současně jsme zažili revoluci ve zpracování NLP. Nejmodernější modely, jako je BERT (Devlin et al., 2019) a GPT (Brown et al., 2020), například zlepšily schopnost strojů číst a psát a chápat kontext vět. Tyto technologie vytvořily základ pro vytváření asistentů, strojového překladu a zpracování velkého množství textových dat, které přímo ovlivnily tvorbu digitálních služeb a produktů (Devlin, 2019).

ChatGPT od OpenAI je modelem AI, který podle Knihovny slouží jako pokročilé extenze zpracování přirozeného jazyka. Jedná se o nástroj poháněný AI, který komunikuje s uživateli prostřednictvím konverzačního textu pomocí NLP nebo technologie zpracování přirozeného jazyka. ChatGPT funguje na principu strojového učení a čte, syntetizuje a generuje texty pomocí rozsáhlé sady dat, na kterých byl trénován. Používá se v mnoha oblastech, včetně zákaznické podpory, marketingu, tvorby obsahu a vzdělávání, kde může fungovat jako užitečný pomocník při řešení složitých úkolů. Knihovna také zdůrazňuje, že

ChatGPT je příkladem toho, jak AI přetváří komunikační procesy a interakci mezi lidmi a stroji (Knihová, 2024).

1.2 Budoucnost umělé inteligence

Oblast AI je velmi rychle se rozvíjející oblastí, kdy dnešní i budoucí předpovědi jsou provedeny za předpokladu současné trajektorie vědeckého vývoje. Posouvání hranic inteligentnějšího, autonomnějšího a adaptivnějšího vývoje systémů, které budou schopny reagovat na složité hrozby/výzvy, kterým bude naše společnost čelit (Neuman, 2023).

Jeden z nejvýznamnějších trendů současnosti, Algoritmy pokročilé AI byly vycvičeny na vzorcích a trendech historických dat, což pomáhá technologii AI zlepšovat předpovědi přírodních katastrof, epidemických hrozeb a kybernetických útoků. V kombinaci s neuronovými sítěmi poskytují metody strojového učení AI modelům schopnost analyzovat komplikované a dynamické systémy a rozpoznávat rizikové prvky přesněji než kdy dříve. To by mohlo pomoci s lepším plánováním preventivních opatření a zmírňováním škod (Neuman, 2023).

Jedním z těchto faktorů je rostoucí autonomie systémů. Během krizového řízení, zejména při monitorování bezpečnostních hrozeb v neustále se měnícím prostředí a koordinaci záchranných misí, se jako nenahraditelné nástroje objevují pokročilé robotické technologie včetně autonomních dronů a chytrých senzorů. Takové technologie mohou urychlit analýzu oblastí postižených katastrofami, zlepšit identifikaci osob ohrožených poškozením a optimalizovat proces evakuace. S rychlým pokrokem AI se očekává, že tyto systémy budou nakonec schopny nezávisle rozhodovat o zásazích na základě složitých datových vstupů, což umožní ještě účinnější a přesnější možnosti léčby (Sharma et al., 2022).

V budoucnu bude velkou roli hrát vývoj kolaborativní AI, tedy systémy, které budou schopny efektivně spolupracovat s lidskými operátory. V rámci zasazení daného tématu lze relevantní technologie začít využívat jak k rozhodování u mimořádných událostí, tak ke kvalitnější koordinaci složek záchranných služeb a agentur zabývajících se bezpečností. Příkladem můžou být inteligentní asistenční platformy ovládající pomoc s informováním o situaci v reálném čase za pomoci doporučení založených na historických datech a aktuálních hrozbách (Russell, 2021).

Tento výzkum také ukazuje, že etický rámec a následná regulace jsou ještě potřebnější, protože AI musí v budoucnu hrát významnější roli v ochraně obyvatelstva. Tyto principy by

měly zajistit, že nasazení nových technologií bylo nejen transparentní, ale také obsahovalo bezpečné prvky a určitou spravedlnost. Zaměřování se na problém správy – kdo ovládá AI, jak je využívána, a volá po regulaci, která zabrání tomu, aby se AI stala hrozbou pro společnost (Russell, 2021).

Analýza se zaměřením na řízení rizik a konkrétní tvorbu pravidel zabraňujících AI mít špatné účinky na ochranu populace. V současné době se zdůrazňuje, že odpovědnost mají jak vývojáři, tak i uživatelé takových technologií. Systémy záznamů pro krizové situace rozhodují, pro jakou technologii, včetně strukturovaných protokolů je potřeba nasadit AI v krizových situacích, které mají za úkol chránit soukromí, minimalizovat škody způsobené nesprávným rozhodováním a popřípadě určit kdo ponese odpovědnost za použití těchto inovací, to vše bude při zavádění AI nejdůležitější,“ řekl (Russell, 2021).

Dalším zásadním problémem je interoperabilita systémů AI, kdy schopnost různých systémů sdílet mezi sebou informace a navazovat spolupráci je při reakci na krize velmi důležité. Zde je obzvláště důležité, že když v souvislosti s používáním AI ve veřejných službách, se vyskytuje standardizace datových formátů, komunikačních protokolů a bezpečnostních postupů tak, je potřeba mít zásadní informace a interoperabilitu zařazenou v důležitých tématech (Binns, 2017).

Závěrem lze konstatovat, že se očekává, pokračující trend důležitosti AI v ochraně obyvatelstva, od možného předvídání rizik až po samotné krizové řízení. Pokroky v této oblasti poskytují nejen významné cesty pro případné zvýšení bezpečnosti ale i maximalizaci účinnosti terapií. Cílem by stále mělo být zdůraznění zodpovědného používání těchto technologií. Zásadní bude zajistit, aby fungovaly tak, že nebude poškozena žádná lidská hodnota nebo nabízení náhledu na volby, které nemají potenciál být zneužity (Binns, 2017).

1.3 Etické výzvy umělé inteligence

Etické obavy kolem AI se v posledních několika letech staly nejen velkým tématem ve výzkumu, ale i v diskursu široké veřejnosti a odborníků. Bylo zdůrazněno od (Floridi a Cows, 2020), že zrychlený vývoj spojený s AI s sebou nese rizika, která by mohla ohrozit práva jednotlivců, stejně jako bezpečnost veřejnosti a spravedlivé rozdělení výhod, které technologie nabízí. Klíčovým problémem, který je v tomto ohledu často označován, je ochrana soukromí. Systémy AI obvykle pracují s velkým množstvím osobních a citlivých dat, která mohou být řádně chráněna, a pokud ne, mohou být snadno zneužita. Ve Skutečnosti je otázkou, kdo má a vlastní k těmto údajům přístup a jak je prováděno jejich

následné zpracování. Nedostatek důležitého ochranného rámce může mít za následek ohrožení bezpečnosti osobních informací a soukromí, zejména v oblastech, kde jsou tyto specifická data využívána pro modelové školení, dále může mít nejen dopad na životy lidí, ale může zde i figurovat analýza chování, hodnocení kreditů nebo předvídání konkrétních zločinů (Floridi a Cows, 2020).

Dalším z řady velkých problémů je etika, kdy se daný problém týká transparentnosti a odpovědnosti za rozhodnutí, která AI učiní. Vzhledem ke stále více se vyskytujícím algoritmům produkujícím výsledky nebo určení, aniž by veřejnost nebo subjekty kterých se daná problematika týká, dostali šanci pochopit, jak vlastně byla tyto určení zavedena. Tento specifický prvek „černé skříňky“ v AI, kde procesy řídící a manipulující rozhodování zůstávají skryté. Zůstává otázkou, zdali jsou problémy vyvolány se spravedlností a rovností. Např. u prediktivních policejních systémů nebo u automatizované kontroly žádostí o úvěr, může nevědomost o tom, jak tyto algoritmy fungují, vést k zcela nepochopitelné a neúmyslné diskriminaci nebo nespravedlivému rozhodnutí (O'Neil, 2016).

Zkreslení školicích dat je zásadní problém, který ovlivňuje etiku AI. Systémy v konkrétní technologii se učí na základě historických dat, a pokud data obsahují konkrétní historické zkreslení nebo sociální nerovnosti, vytvořené modely mohou tyto zkreslení reprodukovat nebo dokonce posílit. Například algoritmy testování kriminality nebo sociálního chování mohou nést rasové nebo genderové stereotypy a mít negativní dopad na určité segmenty populace (Barocas et al., 2019).

Proto je nezbytné, aby systémy AI byly navrženy s ohledem na minimalizaci rizika předsudků a zajištění, že se všemi občany se bude zacházet stejně bez ohledu na rasu, pohlaví, národnost nebo jiné vlastnosti (Barocas et al., 2019).

Bylo to v souvislosti s potřebou vyvinout etické rámce a předpisy, které by zajistily bezpečné, transparentní a spravedlivé používání AI. Nabývají na významu zejména v oblasti ochrany obyvatelstva, kde existují potenciální budoucí důsledky zneužití AI, které mohou významně ovlivnit veřejnou bezpečnost a důvěru v instituce. AI má také hrát klíčovou roli při rychlém odhalování hrozeb – ale musí být navržena tak, aby prosazovala lidská práva a nezneužívala informace neetickým způsobem. Například nasazení AI pro objekty krizové analýzy, řízení mimořádných událostí nebo specifické zabezpečení před přírodními katastrofami musí být zajištěno, aby byl k dispozici nejen efektivní systém, ale aby byly opravdu zabezpečeny osobní údaje. Rozhodovací procesy by měli odrážet transparentnost

a rizika a přínosy byly zde posuzovány stejně i pro různé skupiny obyvatelstva (Barocas et al., 2019).

Floridi a Cows také zvažují otázku, jak A.I. může změnit povahu lidské odpovědnosti. Koneckonců, po několika desetiletích by AI také rozhodovala a bude následovat otázka, kdo nese odpovědnost za chyby, které stroj dělá. Odpovědnost musí být také jasně definována, zejména proto, aby mohla existovat náprava v případech, kdy AI vede k nesprávným rozhodnutím nebo špatným následkům. Jelikož rozhodnutí týkající se AI mohou přímo ovlivnit zdraví a bezpečnost lidí, je to zvláště důležité v kontextu ochrany obyvatelstva (Floridi a Cows, 2020).

Prostřednictvím těchto výzev lze usoudit, že potřeba nových komplexních rámců správy a následná regulace AI umožní odpovědné inovace a zároveň ochrání v případě problému veřejnost před potenciálními následky. Tyto rámce zahrnují nejen technické, legislativní a etické normy, ale taky umožňují AI sloužit k veřejnému prospěchu, aniž by byly zavedeny nadměrná rizika. Je nezbytné hlídat nejen vývoj a poskytování technologií AI, ale i vše ostatní tak, aby bylo v souladu s lidskými právy, obsahovalo transparentnost a spravedlnost. Je také důležité zaměřit se na vývin jasných etických zásad a pravidel k zajištění rovnosti, spravedlivého přístupu a podporu ochrany občanů před diskriminací (Binns, 2017).

1.3.1 Právní a regulační rámce pro umělou inteligenci

Právní a regulační rámec pro AI v České republice se v průběhu posledních let vyvíjí podle legislativy EU a v souladu se národními strategiemi. Tím, že příchod AI nabídl nové technologické příležitosti, vyvolalo to řadu otázek v oblasti etiky, zásadní bezpečnosti a důležitosti ochrany osobních údajů. Je také potřeba si všimnout, že právní základ pro zajištění zodpovědného vývoje a nasazení AI byl měl být stejný napříč všemi sektory. Za tímto účelem se ČR rozhodla čerpat informace nejen z vlastní iniciativy, ale i ze svých závazků vyplývajících z předpisů přijatých v EU (Úřad vlády ČR, © 2025).

Na úrovni Evropské unie je jedním z nejdůležitějších právních předpisů zákon o AI (dále jen AI zákon), tedy první na světě komplexní regulace této technologie. Na základě rizika, které tyto systémy představují, tato legislativa stanoví přísná pravidla pro vysoce rizikové systémy AI, jako jsou systémy používané ve zdravotnictví, kritické infrastruktury nebo veřejné správě. Zákon o AI se také snaží zakázat některé neetické praktiky, jako je biometrická identifikace v reálném čase nebo manipulativní systémy AI. Česká republika

bude muset toto nařízení zavést do svého právního řádu, jehož plná účinnost se očekává v roce 2026 (Úřad vlády ČR, © 2025).

Národní strategie pro AI byla schválena v roce 2019 a stanovuje prioritní kroky pro rozvoj AI na národní úrovni v České republice. Strategie klade důraz na inovace, vzdělávání a propojení akademické sféry s průmyslem a podstatou společnosti. Řeší také etické obavy týkající se AI a uznává nezbytnost regulace za okolností, které by mohly ohrozit práva občanů. Konkrétně v tomto ohledu čtená specializovaná pracoviště, např. Národní centrum AI, regulační systémy, které mají právo dát společností příležitost otestovat technologie AI před jejich implementací do praxe (European commission, © 2025).

Kromě evropské legislativy musí AI také dodržovat obecná právní ustanovení, jako je GDPR (General Data Protection Regulation) související s individuálním automatizovaným rozhodováním a profilováním. Takové systémy AI, které zpracovávají osobní údaje, musí být transparentní a uživatel by měl mít možnost ovlivnit, jak jsou jeho osobní údaje zpracovávány. Zvláštní pozornost je také věnována odpovědnosti za škody způsobené AI. Tato problematika ještě nebyla plně harmonizována, ale vzhledem k velmi zastřeným mezerám v zákoně očekávejte, že se v budoucnu dočkáme nové legislativy na úrovni EU (European Commission, © 2025).

Česká republika už se nachází v konkrétním bodu práce na přizpůsobení svého právního prostředí pro AI. Nejedná se ale o to, že by už byly všechny přípravy byly dokončeny, ale že se tu stále vyskytují klíčové problémy, které bývají u zajištění odpovědnosti za škody způsobené autonomními systémy. Základní etické důsledky AI a její hromadné kontrolování, bude potřeba vyvážit s transparentností a ochranou základních práv člověka tak, aby dané technologie byly schopné v budoucnu ji efektivně využívat (Úřad vlády ČR, © 2025).

1.3.2 Umělá inteligence a lidská práva

Rozšířené používání AI má významný dopad na lidská práva s novými příležitostmi pro jejich ochranu, ale také s řadou etických a právních problémů spojených s jejich používáním. AI je již dobrá v odhalování porušování lidských práv, pomáhá monitorovat cenzuru a analyzuje velké soubory dat, aby zjistila, kde dochází k represivním praktikám, díky pokročilým algoritmům. To vyžaduje regulaci a ostražitost, aby se zajistilo, že se občané neocitnou na přijímací straně drtivých technologií používaných pro hromadné sledování, diskriminační rozhodnutí nebo manipulaci s veřejností (Stahl a Brooks, 2023).

Diskriminace je jedním z hlavních rizik AI vyplývajících z poškozených datových souborů a algoritmických zkreslení. Systémy AI, pro které je využití v oblastech jako jsou určitá zaměstnání typu: Zdravotnictví, odvětví spravedlnosti, se může vyskytovat sociální nerovnost, pokud dané systémy nejsou správně navrženy a otestovány. Příkladem bývá analýza náborových procesů, aby se zjistilo, zdali některé modely chtějí diskriminovat ženy nebo specifické etnické menšiny, v důsledku historických fakt ve vstupních datech lze konstatovat přenos určitých vzorců. Tím pádem je vyžadováno přísné dodržování předpisů a auditovatelnosti rozhodování AI (Gordon a Eubanks, 2018).

Dalším souborem výzev, kterým obyvatelstvo čelí, je ochrana soukromí a prevence nezákonného sledování. Takové monitorování populace v měřítku, které tu ještě nikdy předtím neexistovalo, umožňuje jak státním, tak soukromým subjektům sledovat data pomocí nových technologií, jako je rozpoznávání obličejů a prostřednictvím analýzy velkých souborů dat. S tím se vyskytnul problém hromadného sledování a neoprávněného shromažďování osobních údajů. Lze také vidět, že autoritářské vlády zneužívají tyto technologie způsobem, který porušuje svobodu projevu. Monitorování disidentů začíná být taky problémem, a proto se objevuje otázka mezinárodní regulace a přínosu přísnějších pravidel pro používání těchto technologií (Topal, 2022).

Existence nástroje sloužícího k ochraně lidských práv prostřednictvím AI už je reálnou záležitostí. Organizace pracující s tímto problémem mají k dispozici dané nástroje k analýze příslušných příspěvků na internetu, identifikaci projevů nenávisti a důsledný dohled na porušování mezinárodního práva. Pojem automatizace strojového učení, kdy je zpracováno svědectví o válečných zločinech, může následně pomoci při identifikaci podezřelého pachatele. Technologie NLP jako bonus poskytují zařízení k předělání klíčových dokumentů, a tím pádem se zasaženým skupinám umožňuje získat přístup k právní pomoci mnohem snáze (Gordon a Eubanks, 2018).

Otázkou zůstává, zdali AI může způsobit revoluci v oblasti lidských práv. Její implementace by měla dávat přednost transparentnosti, odpovědnosti a následné regulaci. Vlády společně s mezinárodními organizacemi by měli spolupracovat při zajištění globálních právních rámců zabráňujících zpronevěření AI k potlačování občanských práv. Zároveň je důležité umožnit odhalení potenciálního zneužívání veřejným orgánem a případným použitím stejných technologií k ochraně lidských práv (Stahl a Brooks, 2023).

1.3.3 Umělá inteligence a dezinformace

AI hraje stále větší roli v šíření a odhalování dezinformací. Současné generativní modely, jako jsou jazykové modely (např. GPTSMX) a technologie pro syntézu obrázků a videí (tzv. deepfake), umožňují generování realistického, ale také falešného obsahu ve velkém měřítku. Ty mohou být použity k tomu, aby se nepodařilo manipulovat veřejným míněním, šířit propagandu nebo se zapojit do podvodného chování. AI tak nejen pomáhá při generování falešných zpráv, ale je také nezbytnou zbraní v boji proti ní (Birrer a Just, 2024).

Technologie Deepfake je jedním z nejnebezpečnějších jevů v dezinformačním vesmíru. Umožňuje produkci realistického videa a zvuku jednotlivců, jejichž identitu lze zfalšovat. Měli bychom se z tohoto pokroku radovat – a především z politické stability, důvěry ve veřejné instituce a také kybernetické bezpečnosti, ale také bychom se měli bát. Deepfake videa byla velmi užitečná při vytváření zmanipulovaných voleb, při manipulativních hovorech s telefonním číslem někoho jiného, a dokonce i při stříhání neprospěšného materiálu. Je však obtížné je odhalit, ale systémy AI založené na strojovém učení jsou dostatečně schopné najít nekonzistence v obrazech, zvucích a výrazech obličeje (Birrer a Just, 2024).

Sociální média se ukázala jako klíčová platforma pro šíření dezinformací a AI má v tomto prostředí dvojí roli. Za prvé, algoritmy těchto platform odměňují senzacechtivý obsah, který může způsobit, že se falešné zprávy budou šířit jako požár. Naproti tomu společnosti jako jsou Meta, Google a Twitter používají AI k automatické detekci a označování zavádějícího obsahu. Systémy pro zpracování NLP zkoumají texty, vyhodnocují důvěryhodnost zdrojů a identifikují potenciálně falešný obsah (Shu et al., 2017).

Zatímco textové dezinformace jsou jednou z největších hrozeb, AI také otevírá stavidla pro generování obrázků a videí. Generování hyperrealistického, ale falešného obsahu se stalo pozoruhodně jednoduchým. Obvykle to vyžaduje jen několik kliknutí myši nebo několik instrukcí a nejsou nutné žádné speciální kódovací dovednosti. Obrázky lidí, které jsou generovány technologií AI, jsou často identifikovatelné podivnými ilustrativními pohyby rukou nebo očí. Falešné video nebo zvuk jsou navíc často označeny nesprávným měkkým nebo tvrdým podpisem. Ale obsah pochybného původu, který se dnes objevuje, spouští poplašné zvonky i v těch nejmodernějších, okamžitých poplašných zvoncích. Falešné obrázky, například během krizí, mohou v lidech vyvolat paniku nebo ovlivnit veřejné

mínění. K boji s těmito hrozbami se používají techniky ověřování zdrojů a detekční algoritmy, které těží metadata a odhalují anomálie v obrazech (Aliabadi, 2024).

V rámci pokroků ve specifických metodách detekce představuje specifické řešení dezinformací pořád určitou výzvu. Systémy AI se musí pravidelně aktualizovat, aby případná reakce na nové strategie rozesílání falešných zpráv byla už v základu vytvoření objevena. Mezi další zásadní aspekt patří mediální gramotnost, kdy se jedná o vzdělávání veřejnosti jako celku v specifickém kritickém myšlení a zdali jsou si schopni správně ověřovat informace. Lze konstatovat, že pokud dané metody jsou spárované s technologickými řešeními, může se zde vyskytnout dlouhodobý problém, který by mohl vést k oslabení účinků, které v dnešní době mají dezinformace na naši společnost (Shu et al., 2017).

1.4 Technologie umělé inteligence

Technologie je základem vývoje systémů, schopných provádět náročné úkoly. Mezi jednu z nejdůležitějších patří Strojové učení, umožňující systémům získávat vědomosti prostřednictvím analýzy dat, bez potřeby předešlého explicitního naprogramování. Tím se poskytuje strojům schopnost identifikovat konkrétní vzory, kde přichází následné zlepšení jejich výkonu v opakujících se úlohách. Strojové učení lze využít při analýze finančních trhů, určitého předpovídání chování zákazníků nebo při vybudování systémů, které mají za úkol detekovat bezpečnostní anomálie (Russell et al., 2021).

V rámci kritických technologií lze najít druh strojového učení, spadá do něj hluboké učení. V technice figuruje věc, která využívá vícevrstvé neuronové sítě, které jsou podobné tomu, jak funguje lidský mozek. Podle těchto sítí bylo možné interpretovat složité datové struktury, obsahující obrázky, hlasové záznamy nebo přirozenou řeč (Yao Kan a Zheng Yuebing 2023).

Více aplikovatelný obor je zpracování přirozeného jazyka neboli zpracování NLP. Je to obor věnovaný studiu lidského jazyka a aplikacím tohoto studia. Asistenti pro psaní AI (jako ChatGPT), software pro překlad jazyků a textová analýza velkých dat spoléhají na technologie NLP. Příkladem může být analýza sentimentu textu na sociálních sítích a automatická klasifikace textu (Russell a Norvig, 2020).

AI je vlastně širším oborem, zahrnujícím pod pole, jako je počítačové vidění, které se zaměřuje na analýzu a interpretaci vizuálních dat. Automatizované počítačové vidění

umožňuje detekci objektů na fotografiích. Rozpoznávání pohybů a sledování situace (v reálném čase) zvládá podobným způsobem. Strojové učení, forma AI, která stojí za vozidly ovládané touto technologií (LeCun et al., 2015).

Mezi dva základní stavební kameny AI patří: systémy agentů a plánování. Agent je bývá softwarová nebo hardwarová entita obdařená speciálními schopnostmi, reflexy, které mohou přijímat akce nebo rozhodnutí po obdržení vstupů z konkrétního prostředí. Dané systémy spoléhají na algoritmus, který dále zvyšuje své úsilí a strategické kroky k dosažení definovaných cílů. V dnešní robotice se systémy agentů používají k efektivní navigaci v neznámém prostředí a zároveň je lze využít k optimalizaci dodavatelských řetězců v logistice (Russell et al., 2021).

Další důležitou oblastí výzkumu AI je (Reinforcement Learning). Tato metoda se podobá tomu, jak funguje lidské učení – metodou pokusů a omylů. V simulovaném prostředí umožní posilovací učení agentům objevit optimální strategie fungujících prostřednictvím teorie odměn a trestů. Jedná se o velmi běžný přístup; jako příklad bývá uváděn uplatnění v autonomních systémech, jako jsou roboti a drony, ale možností jsou už i videohry, kde je AI téměř schopné ovládnout hry tak, že porazí i člověka. Mezi nejznámější hry patří šachy a poker (Sutton a Barto, 2018).

1.4.1 Strojové učení a hluboké učení

Systémy AI jako jsou strojové učení dále jen (ML) a hluboké učení dále jen (DL) bývají pokládány jako dvě nezbytné technologie, které výrazně formují a mění zavedený vývoj moderních AI systémů. Možnost strojové učení zlepšovat systémům výkon na základě provedené analýzy dat, lze i bez nutnosti je explicitně programovat. Hluboké učení, vedené jako podmnožina strojového učení, využívá potřebné neuronové sítě s více vrstvami k efektivnějšímu zpracování náročných datových vzorců. Technologie s tímto obsahem nacházejí široké uplatnění v mnoha specifických oblastech, počínaje od průmyslu, přecházející ke zdravotnictví až po jeden z nejdůležitějších prvků ochrany obyvatelstva a tím je kybernetická bezpečnost (Goodfellow et al., 2016).

Technologie Hluboké učení nevyužívá konvenční techniky strojového učení, ale místo toho pracuje s hlubokými neuronovými sítěmi (DNN), jedná se vlastně o neuronové sítě s více vrstvami. Protože tyto sítě modelují dohledatelnost po celém světě, zachycují jemnou složitost, která vede k velmi přesným modelům pro vysoce hodnotné úkoly, jako je rozpoznávání obrázků, procesory přirozeného jazyka a systémy automatického řízení. V této

oblasti bylo dosaženo značného úspěchu s konvolučními neuronovými sítěmi (CNN), které jsou nezbytné pro analýzu obrazových dat, a rekurentními neuronovými sítěmi (RNN), u nichž se vyskytuje aplikování v časových řadách a sekvenčním zpracování dat (Goodfellow et al., 2016).

Jedním z nejdůležitějších aspektů krásného pokroku v hlubokém učení v posledních několika letech je obrovské množství výpočetního výkonu a snadný přístup k masivním datům. GPU (grafické procesorové jednotky) a specializované čipy AI umožňují efektivněji trénovat neuronové sítě. V kontextu těchto faktorů se hluboké učení stalo hlavní hnací silou inovací v AI (LeCun et al., 2015).

Systémy ML a DL mají mnoho výhod, ale mají také řadu výzev a nedostatků. Trénink hlubokých neuronových sítí vyžaduje obrovské množství výpočetního výkonu a energie, což se promítá do vysokých nákladů a také do ekologické stopy. Další největší výzvou je interpretovatelnost modelu; hluboké neuronové sítě se často chovají jako „černá skříňka“, což může komplikovat jejich aplikaci v základních oblastech, jako je zdravotnictví nebo autonomní řízení. V tomto ohledu se tedy vyvinuly výzkumné práce na daných modelech AI zaměřené na lepší pochopení rozhodovacích procesů (Marcinkevičs et al., 2023).

1.4.2 Generativní umělá inteligence – ChatGPT a jeho využití v praxi

Generativní AI popisuje radikální přístup v této technologii, a to vytváření nových textů, obrázků, hudby, a dokonce i nových videí na základě existujících vzorů a dat. Jedním z nejznámějších modelů, používající danou technologii je ChatGPT, který vytvořila společnost OpenAI. Pro správné porozumění a vytvoření lidského jazyka je využito technologie hluboké neuronové sítě. ChatGPT se dnes používá k mnoha účelům, mezi nejznámější patří podpora při hovorech, specifický marketingový obsah, možnost širšího vzdělávání a plnohodnotná automatizace administrativních procesů (Pugachev et al., 2023).

Generativní AI funguje pomocí složitých transformačních modelů včetně různých variant architektury generativního předškolního transformátoru (dále jen GPT). Modely jsou dále trénovány na obrovském množství dat, zejména obsahující data textů a kontextů. Tyto modely získávají pochopení v kontextu na vysoké úrovni, kdy jejich předností je schopnost se průběžně učit novým věcem z velkého objemu dat po celý svůj život (Pugachev et al., 2023).

Praktické využití ChatGPT

Využití generativní AI se čím dál víc objevuje v marketingovém a mediálním světě, kdy dochází k automatickému generování článků, blogových příspěvků a reklamních textů. ChatGPT a jemu podobné modely začali usnadňovat generování textu souvisejícího se zadanými klíčovými slovy nebo tématy uživatelem. Model umožňuje také mít text v tónu a stylu, který si uživatel přeje (Knihová, 2024).

Značné usnadnění práce programátorům při psaní kódu je další významnou aplikací generativní AI. Tato technologie má schopnost pracovat se zdrojovým kódem, kdy nemá problém psát určité algoritmy, vyhledávat a opravovat chyby ve zdrojovém kódu anebo pomáhat při vytváření softwarových aplikací. Vše, co je využito ve vývoji této technologie se stalo nezbytným díky systémům založeným na GPT (Pugachev et al., 2023).

Generativní AI obsahuje nespočet výhod, ale na druhou stranu se zde objevují i zjevné nevýhody. Jedním z hlavních problémů je možné šíření dezinformací, protože modely jako ChatGPT mají sice určitou schopnost produkovat velké množství informací, ale při jejich generování mají tendenci zapomínat na soukromí a autorská práva která se na ně vztahují. Existují také určité obavy z dopadů AI na trh práce, kdy automatizace v některých odvětvích může vést k zániku určitých pracovních míst bez možnosti náhrady na jiných pozicích (Bender et al., 2021).

1.4.3 Umělá inteligence v reálném čase – Nasazení v rámci integrovaného záchranného systému

Tento projekt pokládá základy pro strategickou implementaci AI v reálném čase v IZS, což znamená významný pokrok v úsilí o krizové řízení a ochranu obyvatelstva. Tato řešení, poháněná moderními systémy AI, umožňují rychlou analýzu dat, predikci hrozeb, optimalizaci zásahů a podporu rozhodování v citlivých scénářích, kde pouhá vteřina může znamenat rozdíl mezi životem a smrtí nebo záchranou majetku. AI, alespoň částečně poháněná pokročilými algoritmy strojového učení a efektivním zpracováním velkých objemů dat, se rychle objevuje jako nedílný nástroj pro hasiče, záchrannou zdravotnickou službu a policejní oddělení při řešení mimořádných událostí (Evropská unie, © 2020).

Největší AI v IZS je předvídání krizových situací, kdy AI může pomoci vyhnout se katastrofám nebo je snížit. Systémy založené na strojovém učení jsou trénovány na historických datových sadách, meteorologických podmínkách a geolokačních datech, což podnikům umožňuje získat předem upozornění na možné povodně, požáry nebo dopravní nehody. Abychom uvedli příklad v oblasti lesních požárů, modely AI mohou předpovídat

šíření požáru na základě směru větru, vlhkosti a terénu. To zase umožňuje efektivnější nasazení hasičských jednotek, kdykoli a kdekoli to bude potřeba (Evropská unie, © 2020).

Oblastí revolučních změn, které přináší AI, je koordinace zásahů dispečerů. Systémy řízené AI využívající kombinaci dopravních dat v reálném čase, senzorických vstupů a videozáznamů umožňují automatické vyhodnocení situace výskytu a směřování nejbližších a nejvhodnějších záchranných jednotek. To zase znamená, že v případě dopravní nehody je systém okamžitě schopen analyzovat, kolik je zraněných, zda jsou záchranáři k dispozici, jak silné jsou dopravní zácpy a jakou trasu by tam měla sanitka dostat. Tím se výrazně zkrátí doba příjezdu a zvýší se účinnost zásahu (Papaioannuo et al., 2024).

Externí AI se používá v terénu k podpoře záchranářů a hasičů při jejich zásazích. Hasičské drony s touto technologií mohou mapovat místa požáru, detekovat osoby v nebezpečných situacích a analyzovat stabilitu budov po zemětřesení, čímž minimalizují riziko pro personál zásahové jednotky. Asistenti založení na AI jsou využíváni ve zdravotnictví k neustálému sledování vitálních funkcí pacienta a následnému doporučování nejúčinnější léčby. Některé země již mají tísňové linky spojené s AI, které dokážou rozpoznat srdeční infarkt nebo jinou život ohrožující situaci analýzou tónu hlasu volajícího, takže pomoc může být odeslána bez prodlení (Papaioannuo et al., 2024).

Vlnění výše zmíněných výhod, etický systém a bezpečnostní otázky spojené s implementací AI do IZS jsou stále aktuální. Rizikové diskuse o ochraně soukromí a možném zneužití těchto technologií, konkrétně automatizované rozhodování, hromadné sledování a sběr osobních údajů. Proto je třeba věnovat zvláštní pozornost zajištění toho, aby AI byla nasazena způsobem, který je transparentní, respektuje právní stát a je založen na přístupu zaměřeném na lidská práva (Evropská unie, © 2020).

To přináší významné změny v přístupu k řešení krizí, protože nastala nová éra v IZS a AI. Tyto vznikající technologie začínají rychleji, přesněji a efektivněji reagovat na různé hrozby, které by mohly opravdu ohrozit občany. Kromě zvýšení úrovně bezpečnosti obyvatelstva, mají za cíl pomáhat a optimalizovat záchranné operace, když každá vteřina rozhoduje mezi životem nebo smrtí (Papaioannuo et al., 2024).

2 VYUŽITÍ UMĚLÉ INTELIGENCE V OBLASTI OCHRANY OBYVATELSTVA

AI je nejnovějším prostředkem ochrany obyvatelstva, protože byla vycvičena k analýze obrovského množství dat a poskytuje přesné časové předpovědi. Vzhledem k tomu, že dnešní svět čelí mnoha výzvám, ať už jsou to přírodní katastrofy, pandemie nebo změna klimatu, existuje naléhavá potřeba vyvinout inovativní a rychlé prostředky na ochranu lidských životů a majetku. AI je mocný nástroj pro řešení krizového řízení, který umožňuje efektivnější způsob práce a zároveň posouvá rozhodovací procesy a předpovídá budoucí rizika. Tak například aplikace strojového učení a datové analýzy mohou výrazně pomoci umožnit reagovat na neočekávané a poskytovat životní informace, které hrozí během krize (Floridi a Cows, 2020).

AI se v dnešní době využívá k monitorování přírodních katastrof, mezi které patří například zemětřesení, záplavy nebo hurikány. S pomocí pokročilých algoritmů AI a získaných dat ze satelitních snímků a informací vytvořenými senzory lze provést varování v reálném čase. Tím se umožňuje lepší příprava v případě výskytu ohrožení u lidí. Takové aplikace jsou opravdu klíčové, protože ve zranitelných oblastech, kde je omezená infrastruktura, je potřeba rychlé reakce, která může znamenat rozdíl mezi životem a smrtí (Yao Kan a Zheng Yuebing, 2023).

Jednou z důležitých oblastí použití AI je sledování a predikce šíření epidemií. Data do října 2023 jsou například nasazeny systémy strojového učení – během pandemie COVID-19 systémy strojového učení umožňovaly sledovat šíření viru, předpovídat vývoj pandemie a optimalizovat zdroje zdravotní péče. Tyto typy technologií umožnily zdravotnickým institucím reagovat mnohem rychleji a nasadit potřebné zdroje mnohem efektivněji (Vaishya a Javaid, 2020).

Technologie představuje několik výzev, zejména v oblasti etiky, odpovědnosti a odpovědnosti. Je nezbytné zajistit, aby rozhodování založené na AI bylo prováděno zcela transparentně a spravedlivě a aby byla chráněna práva obyvatel. Účelem tohoto rámce je definovat standardy, které zaručují, že AI, když se použije, nebude používána k nezákonným účelům, jako je nezákonné sledování a diskriminace, v případě veřejného sledování jako příklad. Tyto problémy jsou zvláště důležité tam, kde AI volá po prioritě přístupu k veřejným zdrojům nebo prioritě ochranných opatření (Floridi a Taddeo, 2016).

2.1 Literární rešerše k využití umělé inteligence v ochraně obyvatelstva

Cílem této literární rešerše je podrobit analýze dostupnou odbornou literaturu a vědecké studie, které se zabývají využitím AI v oblasti ochrany obyvatelstva. Rešerše se soustředí na stávající výzkumy, aplikace AI v krizovém řízení a veřejné bezpečnosti, a také se zaměřuje na etické a právní otázky spojené s tímto využitím.

Metodologie literární rešerše

Literární rešerše byla provedena na základě odborných publikací, recenzovaných článků a výzkumných studií, které jsou dostupné v databázích jako Springer Nature, Science Direct, Scopus a SSRN. Při vyhledávání byly používány klíčové termíny jako "AI v řízení katastrof", "AI v krizovém managementu", "strojové učení pro plánování nouzových situací" a "systémy AI pro veřejnou bezpečnost". Do rešerše byly zařazeny pouze publikace vydané po roce 2015, což by mělo za cíl zajistit aktuálnost informací.

Současný stav výzkumu

V poslední době jsme všichni mohli sledovat dynamický rozvoj AI v krizovém managementu a ochraně obyvatelstva. Ve skutečnosti se algoritmy strojového učení již dlouho používají k předpovídání přírodních katastrof k modelování krizových situací a optimalizaci záchranných operací. Neuronové sítě se například používají k předpovídání záplav a požárů – umožňují efektivnější a přesnější rozptýlení zdrojů (Sharma et al., 2022).

Zajímavý způsob šíření dat v těchto oblastech je dán dalším výzkumem otevřeného veřejného sledování lidí a poplachové analýzy bezpečnostních hrozeb. Potenciální rizika, jako jsou teroristické útoky nebo kybernetické hrozby, jsou rychleji zmírňována díky automatizovanému rozpoznávání obrazu a systémům zpracování přirozeného jazyka (Mařík et al., 2023).

Klíčové oblasti aplikace AI:

- Na základě provedené analýzy lze vymezit několik klíčových oblastí, kde AI přináší přínos pro ochranu obyvatelstva:
- Predikce a prevence katastrof – Použití AI pro modelování povodní, požárů, zemětřesení a jiných mimořádných událostí.
- Krizové řízení a optimalizace zásahů – AI pomáhá koordinovat záchranné složky a analyzovat dostupné zdroje.

- Veřejný dohled a bezpečnost – Rozpoznávání rizikových situací pomocí video analytiky a detekce anomálií.
- Etické a právní aspekty – Ochrana soukromí a regulace využití AI v monitorovacích systémech.

Shrnutí

Přehled literatury potvrdil trend, že AI se stále více stává nepostradatelnou pro efektivní práci v krizovém řízení a pro ochranu populace. Předběžný výzkum ukazuje, jaký je její pozitivní dopad na předvídání katastrof, zlepšení v časové reakci, akci v zásahu a na celkové posílení veřejné bezpečnosti. Jak se však objevuje je potřeba vzít v úvahu také etické a právní otázky, protože jsou zásadní ve směru úspěšného používání daných technologií. Další studie mají být orientovány na zvýšení přesnosti modelů AI a transparentnosti v jejich rozhodovacích procesech.

2.2 Krizové řízení s podporou umělé inteligence

Jednou disciplínou v tomto ohledu je krizové řízení, které pracuje v rámci přípravy, reakce a obnovy přírodních nebo člověkem způsobených katastrof. AI se v posledních letech prosazuje mezi základní nástroje využívané pro zefektivnění krizového řízení. AI má schopnost pracovat s obrovským množstvím dat neskutečně velikou rychlostí, zároveň může detekovat vzorce a podle nich vytvářet vysoce přesné předpovědi, což umožňuje získat inovativní scénáře, které dříve ještě nebyly k dispozici. Tím vzniká lepší schopnost krizových týmů reagovat bez prodlevy na nečekané situace (Mařík et al., 2024).

Je také široce používána i v jiných částech krizového řízení, než je např. predikce katastrof, lze ji najít při návrhu intervence a efektivity alokace zdrojů. Možnost metody strojového učení analyzovat historická data ve všech případech povodní, zemětřesení nebo epidemií, a má za cíl dokázat předpovědět, kdy a kde se podobné události v budoucnu pravděpodobně vyskytnou. Tyto poznatky lze využít nejen k provádění preventivních opatření, která pomáhají zmírňovat ztráty ale i ke potenciální záchraně životů (Neuman, 2023).

AI získala výjimečnou výhodu v možnosti kombinování dat z různých zdrojů, mezi které patří satelitní snímky, meteorologická data, určitá sociální média a specifická data od záchranných služeb. Krizoví manažeři mají tak možnost brát z konsolidovaného pohledu na

současnou situaci vyskytující se v reálném čase, které jim poskytuje možnost přijímat rozhodnutí na základě více informací (Sharma et al., 2022).

V oblasti ochrany obyvatelstva AI nejen že urychluje reakci na katastrofy, ale také má za cíl zvyšovat povědomí veřejnosti. Zde lze najít systémy přizpůsobené konkrétním čtvrtím, které budou mít možnost posílat varování ohroženým obyvatelům prostřednictvím specifických mobilních aplikací, čímž se zvyšuje pravděpodobnost vzniku včasné reakce a následné evakuace (Mařík et al., 2024).

2.2.1 Predikce přírodních katastrof s pomocí umělé inteligence

Jednou z hlavních oblastí, kde se používá AI, je předpovídání přírodních katastrof. K předpovídání a snížení dopadu katastrof, jako jsou zemětřesení, záplavy, hurikány nebo požáry, to lze provést pomocí pokročilých algoritmů strojového učení, pomocí analýzy velkých dat a také nasazením satelitních technologií. Celá aplikační oblast, která využívá AI k modelování složitých přírodních procesů, je sama o sobě cennou revolucí, protože zdůrazněnou funkcí je schopnost zpracování a analýzy velkého množství dat, které by tradiční metody nebyly schopny efektivně využít (Sun et al., 2020).

Nejlepším způsobem, jak zabránit většině druhům přírodních katastrof, mají být neuronové sítě, které pracují s minulými událostmi a specifickými vzory. Příkladem lze uvést systémy detekce zemětřesení, které využívají seismografická data společně se systémy AI. Algoritmy daného typu dokážou detekovat menší otřesy, vzájemně navazující obvykle na větší zemětřesení, čím se stávají důležité pro zachránění životů, včasného upozornění a přípravy na přicházející katastrofy. Stejným způsobem se AI používá i při analýze klimatických dat, kdy si bere vzorce srážek, průtoky řek a hydrologické stavy, tak aby bylo možné předpovědět možné povodně (Comes, 2024).

Analýza předpovědí hurikánů a tropických bouří patří mezi další zajímavé domény s nedávným pokrokem v používání AI. Nyní jsou využívány satelitní snímky s radarovými daty použitelné pro předpověď počasí, tak aby byly schopné vytvořit přesné modely, zjišťující dráhu a specifickou intenzitu jakékoli bouře, která se může v nedohledné době přiblížit. Čas k vytvoření modelů se v dnešní době se značně zkrátil, díky využití technologie hlubokého učení, která má velký dopad na včasné varování obyvatelstva a jeho přípravu na evakuaci (Sun et al., 2020).

V případě lesních požárů lze využít AI. Moderní systémy sbírají satelitní snímky následně je spojují s daty z dronů a senzory, které mají za úkol sledovat změny teploty,

vlhkosti nebo případný výskyt kouře. Kombinace všech těchto strategií umožňuje rychlejší detekci požáru, dále napomáhá včas objevit meteorologické jevy a tím pádem dokáže snížit závažnost případného dopadu. Integrace AI navíc může pomoci s plánováním rozmístění zdrojů, případná výpomoc taky přichází při koordinaci se záchrannými týmy (Poorani et al., 2024).

2.2.2 Řízení krizových situací s využitím umělé inteligence

AI se nyní připravuje na výraznou změnu v krizovém řízení, kdy bude stále důležitější její přítomnost u krizových situací, jako jsou přírodní katastrofy, průmyslové havárie nebo pandemie. Dále AI dokáže výrazně urychlovat rozhodovací procesy, které vedou ke zlepšení efektivního nasazování zdrojů. Zmíněná technologie pomáhá nejen při přípravě na krizové události, ale také při jejich řešení, kdy funguje jako výborná podpora záchranářům, krizovým manažerům a bezpečnostním složkám (Mařík et al., 2024).

Systémy strojového učení mají schopnost sbírat data z více zdrojů, mezi ně se řadí satelitní snímky, kamery, internet věcí, dále jen (IoT) senzory nebo sociální sítě. Získané informace pak mají za následek vytvoření přesného obrazu o aktuální situaci a kde se nachází nejvíce postižené oblasti. Například během pandemie COVID-19 byly využity různé systémy obsahující AI ke nepřetržitému sledování šíření této nemoci, následné modelování scénářů a projektování různých potřeb vztahujícím se k lékařským kapacitám (Russell, S. a Norvig, P, 2021).

Dalším příkladem využití moderních technologií jsou autonomní systémy, jako jsou drony a roboti, kteří mohou provádět průzkum v místech, kam se lidé nedostanou. Tyto inovativní technologie usnadňují mapování terénu, lokalizaci přeživších a doručování zásob do ohrožených oblastí. Například v oblastech postižených zemětřesením mohou drony vybavené termovizními kamerami rychle identifikovat místa, kde by se mohli nacházet zasypaní lidé (Sharma et al., 2022).

Nové moderní technologie ve vojenském sektoru obsahují autonomní systémy, drony a roboty, kteří dokážou provádět průzkum v zónách kam lidé nemají přístup. Dnes nám nové technologie napomáhají zmapovat postižené oblasti, kde lze najít přeživší, kteří potřebují nutnou zásilku potřebných zásob k přežití. V oblastech zasaženými mimořádnými událostmi jako jsou například zemětřesení, lze využít drony s termovizními kamerami pro rychlé detekování oblasti, kde se mohou nacházet jedinci uvěznění nebo pohřbeni pod sutinami (Sharma et al., 2022).

Nástroje AI nejen že umožňují podporovat krizové týmy v rozhodování, ale lze i využít algoritmy, které mohou vytvářet a simulovat různé možnosti krizových situací, které umožní předvídat těmto týmům výsledky určitých rozhodnutí a poté na ně zvolit nejlepší strategie. Příkladem může být optimalizování tras během evakuace, kdy se vytváří schopnost vyhnout dopravním zácpám a přeplněným krytům (Neuman, 2023).

Chatboti a virtuální asistenti jsou také nenahraditelnou součástí u poskytování aktuálních informací a nutných pokynů populaci. V nouzových situacích mohou být tyto nástroje efektivním řešením na často kladené otázky. Další využití je při sdílení informací o bezpečnostních opatřeních nebo u koordinace dobrovolníků. Tato strategie fungovala již v minulosti, například při rozsáhlých lesních požárech v Kalifornii, kdy pomocí systémů AI, byla přivolána pomoc obyvatelům a následně jim byla poskytnuta i při útěku (Russell a Norvig, 2021).

Hlavní výhodou AI je potenciál modelovat a předpovídat vývoj krizových scénářů. Na těchto krizových scénářích mohou krizové týmy simulovat několik scénářů za pomoci modelů založených na posíleném učení a tím získávají schopnost si přizpůsobit své plány proti neočekávanému. Pomocí AI je možnost detekovat pohyb šíření lesních požárů už na základě meteorologické podmínek, což přispívá ke strategickému pohybu hasičských týmů (Russell a Norvig, 2021).

Díky pokroku v oblasti AI se řízení krizových situací stává stále účinnějším, což vede k větší k novým možnostem, jak lépe ochránit obyvatelstvo před následky katastrof. V tomto trendu lze však pokračovat pouze tehdy, bude-li v oblasti technologií zaznamenán určitý pokrok a budou vytvářeny etické standardy a legislativní rámce, které umožní využití AI ve prospěch společnosti a tím se zároveň omezí rizika nežádoucích vlivů (Mařík et al., 2024).

2.2.3 Plánování obnovy po katastrofách s pomocí umělé inteligence

Plán obnovy po katastrofě je důležitou součástí krizového řízení. Jeho primárním cílem je omezit trvalé následky incidentů, aby bylo možné včas se soustředit na obnovu základních potřeb společnosti. AI má v tomto kontextu nepostradatelnou roli, protože zavádí nové schopnosti, které dramaticky vylepšují inovativní procesy a podporuje stanovování priorit a přidělování podstatných zdrojů pro jednotlivé úkoly. To znamená, že AI dokáže takticky navrhnout správná řešení, jak přerozdělovat tyto zdroje, a dále přispívat k urychlení celého procesu obnovy (Sun et al., 2020).

Analýza dat a modelování katastrof je jednou z významných aplikací AI v této oblasti. Předpokládá se, že výkonné algoritmy by mohly také pomoci předpovědět oblasti, které nejvíce potřebují okamžitou pomoc, a klíčové části infrastruktury, které je třeba co nejrychleji obnovit. Tento přístup by prý mohl pomoci i při rozhodování v krizových situacích, a upevnit tak pole působnosti AI, pokud jde o analýzu rizik a obnovu po katastrofách (Comes, 2024).

Je povzbudivé vidět rozmanité a inovativní způsoby, jakými se AI uplatňuje, a to i při využití v oblasti scénářů obnovy. Vytvářením různých scénářů dobrých i špatných na základě minulé historie a současných podmínek by mohli být manažeři pro mimořádné události lépe vybaveni pro řešení různých potenciálních budoucích výzev. Tyto simulace využívají data z minulých katastrof k vývoji modelů, které umožňují simulaci různých scénářů. To zase může pomoci vést k efektivnějšímu využívání lidských a materiálních zdrojů (Poorani et al., 2024).

Úloha AI při monitorování a vyhodnocování procesu obnovy, zejména po katastrofách, je oblastí, která může být zajímavá. Umožníme-li technologii strojového učení analyzovat satelitní snímky a další relevantní údaje, můžeme získat přehled o fázi obnovy. Použitím technik AI na satelitní snímky a jejich kombinací se stávajícími znalostmi může být možné získat jasnější představu o situaci na místě, což by mohlo pomoci včas odhalit problémy a zefektivnit činnosti při obnově (Poorani et al., 2024).

Je zřejmé, že řešení této datové mezery je v této oblasti jednou z hlavních výzev pro efektivní nasazení řešení AI. Významným aspektem tohoto procesu bude zavedení standardů, pokud jde o sběr dat a sdílení informací mezi různými institucemi a organizacemi, neboť to bude mít zásadní význam pro začlenění AI do procesů obnovy. Je důležité poznamenat, že tyto kroky zahrnují jak technické, tak etické aspekty, jako je ochrana soukromí osob a transparentnost rozhodování. Je nezbytné si uvědomit význam těchto faktorů pro posílení důvěry v systémy založené na dané technologii (Comes, 2024).

Navrhuje se, aby plánování obnovy po havárii ukázalo, jak by technologie AI mohly významně přispět k urychlení a zlepšení procesů obnovy. Je však důležité postupovat obezřetně a zajistit, aby integrace těchto technologií probíhala způsobem, který je v souladu s etickými a právními hledisky. To by pomohlo zajistit jejich účinnost a spravedlivé využívání v krizových situacích (Poorani et al., 2024).

2.3 Bezpečnost obyvatelstva a veřejný dohled s využitím umělé inteligence

Je fér konstatovat, že AI se rychle rozvíjí a v důsledku toho se přizpůsobují i způsoby, jakými se chrání populace. AI nabízí řadu nástrojů pro monitorování, analýzu a predikci chování, které mají potenciál zvýšit efektivitu procesů řízení rizik a zmírňování hrozeb. Již se používá v různých sektorech, jako je hlídka na veřejných místech, stejně jako analýza dat v reálném čase a reakce na bezpečnostní operace. AI se již používá v inteligentních monitorovacích systémech, které dokážou identifikovat abnormální chování, předvídat možná rizika a proaktivně řešit krize (Fang et al., 2023).

Předpokládá se, že jednou z největších výhod AI je její schopnost rychle analyzovat obrovské množství dat. Tato schopnost může pomoci při odhalování podezřelých aktivit, dohledu nad vývojem situací a doporučování vhodných opatření na ochranu veřejnosti. Takový přístup může pomoci zachovat akceschopnost tváří v tvář krizové události, což by mohlo přispět ke komplexnějšímu obrazu bezpečnosti. Ačkoli je to nepochybně přínosné, je důležité si uvědomit výzvy, které s tím souvisejí, včetně ochrany soukromí, transparentnosti a etických aspektů. Doporučuje se proto vytvořit a vyjasnit etický a právní rámec pro AI, který by byl vodítkem pro všechny zúčastněné strany při zavádění a využívání této technologie a garantoval, že AI bude jednat v souladu s právními zásadami a zaměří se především na její využití ve prospěch celé společnosti (Kochupillai et al., 2022).

Rozmanitost typů počítačového vidění pro detekci hrozeb a algoritmů zpracování přirozeného jazyka pro analýzu by v zásadě mohla vést k rozšíření systémů AI ve službách ochrany obyvatelstva. To zahrnuje využití AI k vytváření prediktivních modelů, které pomáhají předvídat trestnou činnost a další rizika. Pro účinnou ochranu obyvatelstva je nezbytně nutná rychlá reakce v krizových situacích a AI automatizující bezpečnostní procesy může v těchto situacích ušetřit člověka chyb (N, Athave, 2019).

Jedním z aspektů, které by bylo možné zvážit, jsou legislativní a etické otázky související s využíváním AI v bezpečnostním sektoru. Při práci na problematice AI pro veřejný dohled by bylo přínosné zvážit potenciální výhody a nevýhody těchto technologií, zejména pokud jde o jejich možný dopad na soukromí. Je nezbytné zajistit, aby se informace kontrolující všudy přítomnými systémy řídily morálními zásadami a zákony, jejichž dodržování by pomohlo zajistit, že tyto systémy budou využívány rozumně a transparentně a zároveň budou zachována základní práva občanů (Fang et al., 2023).

2.3.1 Monitorování veřejných prostor

AI se stává základním nástrojem pro dohled nad veřejným prostorem. Lze ji využít k analýze bezpečnostních hrozeb, odhalování podezřelého chování a zajištění rychlé reakce v krizových situacích. Nejmodernější bezpečnostní systémy integrují špičkové algoritmy strojového učení, rozpoznávání obrazu a analýzu velkých dat, které mají potenciál učinit městský dohled nad městskými centry, dopravními uzly a veřejnými institucemi mnohem efektivnějším než kdykoli předtím. Předpokládá se, že tyto technologie zvyšují míru efektivity dohledu a že také snižují závislost na lidském faktoru a v důsledku toho možnost zanedbání nebezpečného okolí (Zhang et al., 2023).

Systémy rozpoznávání obličejů jsou jednou z nejvýznamnějších aplikací AI využívaných při monitorování veřejných prostor. Využívá se ke sledování, pátrání po pohřešovaných osobách a identifikaci podezřelých osob. Předpokládá se, že pokročilá kombinace hlubokého učení a biometrických údajů umožňuje bezpečnostním složkám snadněji analyzovat záznamy z kamer a porovnávat je s databázemi hledaných osob. Je povzbudivé, že tato technologie se již osvědčila na letištích, nádražních halách a velkých veřejných shromážděních, kde byla použita ke zvýšení bezpečnosti (Ali et al., 2023).

Předpokládá se, že AI má potenciál poskytnout možnost sofistikované analýzy chování v reálném čase, což může hrát významnou roli při identifikaci podezřelého chování, například zavazadel bez dozoru, náhlého shromáždění většího počtu osob a agresivního chování. Algoritmy strojového učení mají potenciál identifikovat běžné vzorce chování, což jim umožňuje rozpoznat anomálie, které mohou operátory v bezpečnostním centru rychle upozornit na možné hrozby. Vzniká tak prostor pro prevenci a zásah, který může pomoci zmírnit riziko výtržností na veřejnosti (Zhang et al., 2023).

Další oblastí, v níž AI hraje důležitou roli, je analýza dopravního proudu a prevence nehod, monitorování veřejných prostranství. Inteligentní dopravní systémy využívají kanály z kamerových systémů, snímačů ve vozidlech a prediktivních algoritmů ke sledování hustoty provozu, odhalování nebezpečí a optimalizaci řízení dopravy. Automatická detekce nehod a překážek na silnicích by například mohla potenciálně pomoci urychlit záchranné služby a usnadnit efektivnější řízení dopravy (Sayed et al., 2023).

Technologie AI má potenciál přinést významné výhody při monitorování veřejných prostor, ale je důležité zvážit soukromí a etické důsledky používání těchto technologií. Z hlediska sledování shromažďuje národní program identifikace rozsáhlé biometrické údaje,

které by podle některých názorů mohly být potenciálně zneužity ke sledování občanů bez jejich souhlasu. Proto je nezbytné mít jasné legislativní rámce a mechanismy dohledu, které chrání lidi a zajišťují transparentnost při používání těchto technologií, aby bylo zajištěno odpovědné používání AI v této oblasti (Uddin, 2023).

2.3.2 Prediktivní modely pro prevenci kriminality

Podle nových informací tyto pokročilé prediktivní modely analyzují vzorce kriminality a pomocí AI určují rizikové oblasti, které se stávají nedílnou součástí prevence kriminality. Pomocí velkých dat, strojového učení a různých dalších statistických metod mohou bezpečnostní složky předpovídat, kde a kdy se trestná činnost s největší pravděpodobností stane. Očekává se, že tento přístup přispěje k zefektivnění policejních hlídek a posílení preventivních opatření. Tento nový přístup má potenciál přispět nejen ke snížení kriminality, ale také k optimalizaci využívání zdrojů veřejné bezpečnosti (Raji, 2024).

Analýza historických údajů o trestné činnosti je jedním ze segmentů prediktivního modelování. Tato analýza může pomoci odhalit základní vzorce a korelace mezi časem, místem a socioekonomickým statusem, které jsou příčinou těchto událostí. Algoritmy mohou ukázat, že některé lokality jsou obzvláště náchylné k vloupáním v určitou denní dobu. Taková zjištění by mohla připravit půdu pro lepší preventivní strategie, jako je počet hlídek a instalace kamer průmyslového sledování. Je také třeba poznamenat, že takové analýzy reagují na aktuální trendy a vyvíjející se vzorce protiprávního jednání (Kaur et al., 2023).

Počítá se s tím, že analýza sociálních médií a dalších otevřených zdrojů dat pomocí AI by mohla bezpečnostním složkám pomoci včas odhalit potenciální nebezpečí. Algoritmy strojového učení mají potenciál monitorovat extremistické projevy, nezákonné plány nebo koordinaci násilí. Tato analýza by mohla potenciálně přispět k odhalování trestné činnosti na jedné straně a k identifikaci klíčových aktérů a prevenci organizovaného zločinu na straně druhé (Raji, 2024).

Prediktivní modely se používají také ke studiu recidivního chování a k zachycení pravděpodobnostního stavu recidivy. Prediktivní modely jsou schopny využít údaje o minulých trestných činech, demografické údaje a další proměnné k výpočtu pravděpodobnosti, že se jedinec dopustí trestné činnosti znovu. Některé země již tento přístup využívají k informování o rozhodnutích souvisejících s podmíněným propuštěním vězňů nebo k vytváření programů zaměřených na prevenci recidivy (Lim et al., 2023).

S prediktivními modely jsou však spojeny určité etické problémy, a to i přes jejich velký přínos v oblasti prevence kriminality. Někteří kritici naznačují, že trénink těchto modelů na nevyvážených nebo historicky zkreslených datech by mohl potenciálně vést k diskriminačním výsledkům. K řešení těchto obav se doporučuje, aby byla zajištěna větší transparentnost používaných algoritmů a aby byly zavedeny nezávislé audity a kontrolní mechanismy, které pomohou minimalizovat riziko nespravedlivého zacházení (Lim et al., 2023).

2.3.3 Umělá inteligence v boji proti terorismu a extremismu

AI má potenciál hrát cennou roli v boji proti terorismu a násilnému extremismu. Je schopna zpracovávat rozsáhlé soubory dat, identifikovat potenciální hrozby v reálném čase a pomáhat bezpečnostním složkám odvrátit násilné činy dříve, než mohou být provedeny. Pomocí pokročilých algoritmů strojového učení je možné identifikovat vzorce chování potenciálních útočníků, monitorovat podezřelé aktivity a předem předvídat možné útoky. Tyto technologie se staly zásadními pro národní bezpečnost i pro mezinárodní ofenzivu proti terorismu (Mbiva et al., 2024).

Technologie AI má například potenciál pomáhat při monitorování online obsahu s cílem identifikovat extremistickou propagandu. I když je důležité pochopit, jak fundamentalisté využívají internet k šíření svých myšlenek, je také zásadní zvážit, proč teroristické skupiny stále více využívají web. Je však důležité si uvědomit potenciál AI při identifikaci podezřelého obsahu, monitorování šíření radikálních myšlenek a rychlé reakci na nezákonné činy. Využívá také technologie zpracování NLP k identifikaci nenávistných projevů a odhalování skrytých sdělení ve vybraných jazycích (Tomasev et al., 2024).

Jednou z nejvýznamnějších výhod celého zavádění AI je, že usnadňuje sledování toku finančních prostředků souvisejících s terorismem. Je známo, že teroristické organizace využívají k financování svých operací složité procesy, včetně kryptoměn a využívání stínových bankovních převodů. Strojové učení má potenciál analyzovat miliony peněžních transakcí s cílem odhalit jakékoli podezřelé chování, které by mohlo naznačovat praní špinavých peněz nebo financování terorismu. Tato potenciální schopnost by mohla finančním institucím a vládám pomoci zvýšit jejich schopnost blokovat převody nezákonných finančních prostředků a narušit teroristické sítě (Mbiva et al., 2024).

AI se také běžně používá k analýze zpravodajských informací a sledování rizikových osob. Bezpečnostní agentury čelí výzvě zpracovávat značné množství dat z různých zdrojů,

včetně záznamů z kamerových systémů, telefonické komunikace a satelitních snímků. Pomocí pokročilých systémů AI lze tyto informace rychle analyzovat a získat tak cenné informace o podezřelých osobách a potenciálních hrozbách. Využití technologie rozpoznávání obličejů a biometrické analýzy navíc usnadnilo identifikaci hledaných osob a sledování jejich pohybu, a to jak v rámci země, tak přes hranice (Robbins, 2021).

Je zřejmé, že AI má v boji proti terorismu mnoho výhod, i když se mohou vyskytnout určité problémy, jako je ochrana soukromí a etické využívání těchto technologií. Otázka hromadného sledování a obsahové analýzy osobních údajů vyvolává obavy ohledně možného zneužívání a porušování lidských práv. Je proto nezbytné, aby tyto nástroje byly používány transparentně a v souladu se zákonem a s náležitým ohledem na ochranu občanských svobod (Mbiva et al., 2024).

2.3.4 Ochrana soukromí a etické výzvy veřejného dohledu

Využití technologií AI při veřejném dohledu je třeba pečlivě zvážit, protože vyvolává značné obavy o soukromí a etické otázky. Výhodou takových pokročilých systémů dohledu, které analyzují lidské chování a předvídají jednání, je bezpečnost. Je však důležité si uvědomit, že tyto technologie představují také riziko pro základní lidská práva. Strojové učení a metody rozpoznávání obličejů, které umožňují identifikaci osob v reálném čase, by mohly potenciálně zesílit rizika masového sledování a neoprávněného shromažďování osobních údajů. Je proto nezbytné, aby se při jejich zavádění dodržovaly nejpřísnější etické a právní normy, které chrání soukromí každého jednotlivce (Burri, 2021).

Klíčovým bodem diskuse bylo, jak vyvážit bezpečnost a právo na soukromí. Jednou z oblastí, kde existuje potenciál pro významný pokrok, je oblast prevence kriminality a terorismu, kde mohou mít technologie AI pro monitorování veřejného prostoru významný dopad. Je však důležité poznamenat, že tyto systémy moci mohou být zneužity státními institucemi a soukromými subjekty, pokud nejsou dostatečně regulovány. Takové technologie by mohly být náchylné ke zneužití, včetně potenciálního nechtěného sledování občanů, jakož i k nechtěné diskriminaci na základě faktorů, jako je rasa, náboženství nebo politické názory. Doporučuje se proto stanovit jasná pravidla týkající se shromažďování a zpracování údajů, aby se zabránilo možnosti jejich zneužití (Veale et al., 2023).

Další významnou etickou výzvou, nad kterou by se měli všichni zamyslet, je transparentnost rozhodování v systémech AI. Algoritmy veřejného dohledu jsou obvykle sestaveny ze složitých modelů strojového učení, jejichž logika nemusí být nutně

transparentní. To vyvolává několik otázek: Jak může být zajištěna spravedlnost a odpovědnost v situacích, kdy dojde k nesprávnému rozhodnutí, včetně identifikace podezřelého? Řešení proto nespočívá pouze v technickém zdokonalení těchto systémů, ale také v zavedení samostatných kontrolních a auditních kanálů, které zajistí jejich spravedlivé a odpovědné používání (Zuboff, 2019).

Jedním z hlavních právních rámců upravujících používání AI při veřejném dohledu je obecné nařízení o ochraně osobních údajů (GDPR), které platí na území Evropské unie. Nařízení zavádí přísné požadavky na transparentnost a souhlas, pokud jde o zpracování osobních údajů, a má proto zásadní vliv na využívání AI v této oblasti (Evropská komise 2025).

Ačkoli má AI v oblasti veřejného dohledu mnoho výhod, etika a ochrana soukromí zůstávají hlavními problémy. Je nezbytné uznat potřebu legislativy a zároveň podporovat odpovědné postupy vývojářů a institucí, které je využívají. Rozumné využívání právních rámců, etických pokynů a technologií chránících soukromí, jako je anonymizace dat nebo sdružené učení, pomůže zajistit, aby byla AI využívána spravedlivě a odpovědně (Veale et al., 2023).

3 VÝZVY A OMEZENÍ UMĚLÉ INTELIGENCE V OCHRANĚ OBYVATELSTVA

Technologie AI nabízí významné příležitosti pro využití v civilní ochraně, ale také čelí několika vážným výzvám, které je třeba řešit, aby bylo možné plně využít její potenciál pro zvládání krizí a katastrof a prevenci. Tři hlavní výzvy, jako jsou technologická, etická a praktická omezení, mohou bránit účinnosti a bezpečnosti těchto technologií v prostředí reálného času. V současnosti dostupné techniky AI, jako jsou neuronové sítě nebo metody strojového učení, jsou svou povahou složité, vyžadují velké množství meziodvětvových dat, která v konkrétní chvíli nejsou k dispozici v dostatečné kvalitě pro přesné předpovědi rizik, což vede k tomu, že v současné době působí jako odrazující prostředek od plného využití AI v oblasti krizového řízení a veřejné bezpečnosti (Neuman, 2023).

Kvalita a dostupnost dat je jednou z hlavních technologických bariér. Provoz těchto systémů AI vyžaduje velké a vysoce kvalitní soubory dat pro efektivní analýzu a předvídání informací o kritických situacích, jako jsou přírodní katastrofy nebo epidemiologické hrozby. Tato data jsou často nedokonalá, neúplná a chybná, což má negativní dopad na kvalitu předpovědí a rozhodnutí. Navíc v případě domácích a mezinárodních krizí mohou být klíčové informace, které mohou mít okamžitou hodnotu pro reakci, špatně dostupné nebo zpožděné, což komplikuje situaci (Binns, 2017).

Etické výzvy jsou důležitým rozměrem AI při ochraně veřejnosti. Klíčovými otázkami je, jak zajistit spravedlivost a transparentnost při rozhodování ze strany AI. V době krize, při záchraně životů nebo koordinaci evakuací, nesmí být dovoleno, aby algoritmy byly utvářeny něčí diskriminací určité části populace nebo aby fungovaly s neúplnými či neobjektivními údaji. Důvěra občanů v tyto systémy je rovněž kritickou proměnnou, občané musí mít pocit, že jejich práva a svobody nejsou ohroženy. Otázka spravedlnosti a transparentnosti rozhodovacího procesu v AI je v obecném smyslu klíčová, zejména v oblasti krizového řízení, kde jediné přesné a včasné rozhodnutí může změnit běh lidského života (Russell, 2021).

Dalším důvodem je spolehlivost systémů AI před hrozbou kybernetických útoků, zvláště když tato technologie hraje větší roli ve veřejné bezpečnosti. Proto je také důležité zabezpečit způsob jejich použití, aby se zabránilo jakémukoli zneužití z hlediska kybernetických útoků, protože ty mohou mít katastrofální následky, zejména pokud dojde k manipulaci s citlivými daty nebo k chybě v rozhodovacím procesu. Ke kybernetické

bezpečnosti těchto technologií jistě patří ochrana obyvatelstva a reakce na krizové situace (Sharma et al, 2022).

Lidé jsou dalším prvkem, který umožňuje AI působit v oblasti ochrany obyvatelstva. Citlivost AI na lidský dohled: Navzdory rychlým změnám je lidský dohled nad rozhodovacími systémy AI zásadní. Z tohoto důvodu je důležité, aby lidé byli schopni zasáhnout během krize a zajistit, aby rozhodnutí učiněná AI měla skutečně smysl. To vyžaduje nejen důvěru v technologii, ale také základní pochopení toho, jak funguje. Mělo by se proto o AI uvažovat jako o zdroji na podporu lidských dovedností a znalostí, nikoli jako o náhražce lidského rozhodování (Russell, 2021).

Souhrnně lze konstatovat, že bariéry aplikace AI v oblasti ochrany obyvatelstva jsou kategorické a mnohostranné. Zatímco daná technologie je velkým příslibem pro zlepšení reakce na krize a zajištění větší bezpečnosti, je nezbytné řešit technologická omezení, etické výzvy, bezpečnostní hrozby a lidské faktory. A to jsou pilíře zodpovědného a bezpečného vývoje a nasazení AI. Významnou roli může hrát kombinace všeho řečeného, což je také zásadní pro úspěch těchto technologií v průběhu času, pokud jde o zajištění komplexních kontrol ochrany soukromí při jejich nasazení v krizovém řízení a při vyšetřování toho, kdo je odpovědný (Neumann, 2023).

3.1 Technologické limity a spolehlivost umělé inteligence systémů

Technologie AI se stala nezbytným nástrojem krizového řízení a ochrany lidského života. V těchto oblastech je nenahraditelná, zejména díky své schopnosti analyzovat velké množství dat a rychle předvídat krizové scénáře. Existují však určitá technologická omezení, která mohou spolehlivost těchto technologií AI podkopat. Mezi hlavní omezení patří vysoké výpočetní nároky, nízká spolehlivost modelů, nízká vysvětlitelnost rozhodnutí, problémy s generalizací a aspekty kybernetické bezpečnosti (Goodfellow et al., 2016).

Jedním z hlavních technických problémů je propastná výpočetní povaha modelů AI. To znamená, že vyžadují především výpočetní výkon, což může být problematické zejména v krizových situacích, kdy je třeba činit okamžitá rozhodnutí a výpočetní zdroje mohou být velmi omezené. Spuštění AI v reálném čase proto vyžaduje optimalizace modelu a také efektivní využití hardwarových akceleratorů, jako jsou GPU, TPU atd. (LeCun et al., 2015).

Budoucí pokračování v další aktualizaci, bude důležitou podmínkou, aby byla zajištěna spolehlivost modelů. Všechny příbuzné systémy AI mohou mít inherentní problémy, pokud

je kapacita trénovacích dat nedostačující a nezobrazující se správně na nový scénář. Například v predikci přírodních katastrof, pokud model detekuje extrémní klimatické podmínky, se kterými se během tréninkové fáze nesetkal, může dojít k mírné odchylce v predikci (Zhang et al., 2022).

Vysvětlitelnost a použitelnost modelů AI je dalším velkým problémem. Je to proto, že hluboké neuronové sítě fungují jako takzvané systémy „černé skříňky“, což ztěžuje analýzu a pravidelnost ověřování toho, jak dané procesy fungují, které stojí za jejich rozhodnutími. To může být rozhodujícím problémem v krizovém managementu, kde je důležité nejen dělat správné předpovědi, ale také vědět, jak a proč byla učiněna určitá rozhodnutí (Wojciech et al., 2017).

Technologie AI může řešit další významné omezení, jako je přizpůsobování se neznámým situacím. Modely jsou trénovány pouze na historických datech, což znamená, že nemusí správně reagovat ve scénáři, který je pro ně zcela nový a neznámý. Například během kybernetických útoků na kritickou infrastrukturu se mohou objevit zcela nové hrozby, které model AI ještě neviděl, a proto na ně nedokáže dostatečně reagovat (Papernot et al., 2017).

Posledním kritickým inflexním bodem je kybernetická bezpečnost systémů AI. Tyto systémy mohou být cílem kybernetických útoků, například takzvané adversarialní útoky, kdy jsou vstupní data manipulována tak, že AI generuje špatné výstupy. Důsledky mohou být hrozné, když systémy navržené k detekci hrozeb nesprávně označují neškodné objekty jako nebezpečné, nebo naopak (Carlini a Wagner, 2017).

Protože většina AI zůstává v rámci svých technologických limitů, je to velká příležitost pro její uplatnění v oblasti civilní ochrany. Přestože má AI mnoho výhod, je stále potřeba se soustředit na výpočetní složitost, přesnost, vysvětlitelnost, robustnost a bezpečnost. Pokračující výzkum a vývoj v těchto oblastech by mohl pomoci vyřešit tato omezení a spolehlivost systémů AI v důležitých aplikacích (Marcus et al., 2020).

3.2 Nedostatek dat a jejich kvalita

Absence problémů s kvalitou je jedním z největších problémů v návrhu AI, který má chránit obyvatelstvo. Algoritmy závisí na velkých souborech dat, které musí být nejen dostatečně široké, ale také reprezentativní a aktuální. Nízká kvalita dat může mít za následek nepřesné předpovědi a nesprávná rozhodnutí, která mohou mít za následek při řešení krizových situací nebezpečné následky (Velev a Zlateva, 2023).

První výzvou, často objevující se je zkreslení dat. Modely AI mohou tyto chyby nejen replikovat, ale co je ještě důležitější, modely s danou technologií je mohou také zvětšit. V bezpečnostních aplikacích je tento problém obzvláště znepokojivý, protože chybná identifikace hrozeb může vést k chybnému profilování nebo k diskriminaci konkrétních populací (Mehrabi et al., 2022).

Pak je tu otázka dostupnosti dat. V krizových situacích, jako jsou přírodní katastrofy nebo kybernetické útoky, mohou být data zastaralá nebo nedostupná v reálném čase. Bez těchto informací je skutečně implementace AI neuvěřitelně složitější, protože modely nemají dostatek dat, aby je mohly správně interpretovat (Velev a Zlateva, 2023).

Jednou z nevýhod je nedostatečná standardizace dat a interoperabilita. Různé organizace a státy také používají různé formáty a metody sběru dat, což může vést k potížím při jejich analýzách. Protože neexistují jednotné standardy, systémy AI mají problémy s výměnou a zpracováním informací (Schneider et al., 2023).

Na tento problém je třeba zaměřit se zavedením efektivnějších přístupů ke shromažďování a ověřování takových údajů spolu s algoritmy odolnými vůči zkreslení. Jedním z nejdůležitějších kroků je otevření a sdílení relevantních datových sad, které umožňují trénovat lepší modely AI. To také vyžaduje spolupráci mezi akademickou sférou, průmyslem a vládními institucemi, aby byla zajištěna dostupnost dobře zpracovaných a vysoce kvalitních údajů, které doplní toto úsilí pro efektivní krizové řízení (Velev a Zlateva, 2023).

3.3 Odolnost umělé inteligence vůči kybernetickým hrozbám

Odolnost AI proti kybernetickým hrozbám je zásadním prvkem pro její efektivní využití při ochraně obyvatelstva. Roste trend kybernetických útoků na systémy AI, které by mohly vést ke zneužití, manipulaci nebo dokonce vyřazení takových systémů z provozu. Klíčovými bezpečnostními hrozbami jsou velmi významné, od nepřátelských útoků, přes potenciální manipulaci s tréninkovými daty až po zranitelnosti v rámci samotné infrastruktury AI a problémy s ochranou soukromí (Akhtar et al., 2021).

Jedno specifické kybernetické riziko je známé jako adversarialní útok, kdy útočníci manipulují se vstupními daty, aby vytvořili nesprávné nebo neočekávané výstupy. V kritických oblastech, jako je detekce hrozeb, autonomní systémy a zdravotnictví, mohou být účinky těchto útoků tak závažné, že jejich zmírnění začíná být naprostou prioritou.

Výzkum také zjistil, že i malé změny v datech mohou způsobit katastrofické chyby v modelech AI, což podkopává jejich celkovou spolehlivost (Akhtar et al., 2021).

Dalším významným rizikem je manipulace s trénovacími daty, známá jako data poisoning. Jestliže jsou trénovací data cíleně pozměněna, může se AI model naučit nesprávné vzorce a vytvářet zkreslené výsledky. Tento problém je obzvláště závažný v oblasti bezpečnostních aplikací, kde může chybná klasifikace mít za následek selhání krizového řízení nebo narušení veřejného pořádku (Lu et al., 2022).

Zranitelnosti v oblasti AI infrastruktury zahrnují bezpečnostní nedostatky v softwaru, hardwaru i samotných algoritmech. Modely se často spoléhají na cloudové platformy, které mohou být terčem útoků, jako jsou denial-of-service, dále jen (DoS) či ransomwarové útoky. Ochrana těchto systémů si žádá nejen robustní šifrovací protokoly a autentizační mechanismy, ale také systémy pro detekci anomálií v chování (Singh et al., 2022).

Jednou z klíčových výzev je rovněž ochrana soukromí a etická rizika spojená s využíváním AI. Sběr, uchovávání a analýza obrovského množství dat přináší značné riziko úniku citlivých informací. Zavedení metod, jako je federované učení nebo diferencované soukromí, může pomoci snížit nebezpečí zneužití osobních údajů a posílit důvěru v systémy (Abadi et al., 2016).

Zvyšování odolnosti AI vůči kybernetickým hrozbám vyžaduje neustálý výzkum v modelové bezpečnosti, vývoj silnějších algoritmů a implementaci standardizovaných bezpečnostních protokolů. Ochrana systémů AI je hlavním klíčem k jejich efektivnímu využití při ochraně veřejnosti a krizovém řízení (Singh et al., 2022).

Technologická omezení, nedostatek kvalitních dat a problémy s kybernetickou bezpečností patří mezi klíčové výzvy vyskytující se při implementaci AI do ochrany veřejnosti. I když AI nabízí mnoho výhod, je nezbytné neustále zlepšovat její spolehlivost a celkovou odolnost vůči kybernetickým hrozbám, s cílem zajištění transparentnosti v rozhodovacích procesech. Budoucí vývoj v této oblasti by měl směřovat k vytvoření bezpečnějších, transparentnějších a odolnějších systémů, které mohou účinně reagovat na krizové situace (Lu et al., 2022).

4 DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI

AI je dnes jedním z nejdůležitějších nástrojů na podporu veřejné bezpečnosti a krizového řízení. Její schopnost zpracovávat velké množství dat, učit se ze zkušeností a dynamicky reagovat na nové podněty otevírá nové možnosti pro systémy ochrany obyvatelstva, ať už jde o včasné varování před hrozbami, optimalizaci zásahů nebo rychlejší obnovu po mimořádných událostech. AI se tak stává klíčovým prvkem při budování odolnosti společnosti vůči krizím, a to jak přírodním, tak způsobeným člověkem.

Teoretická analýza naznačuje, že přínosy AI jsou nejvýraznější v oblastech, kde se kombinuje prediktivní modelování, analýza v reálném čase a personalizované výsledky. Tato technologie umožňuje nejen lépe porozumět dynamice krizových událostí, ale také navrhovat účinnější strategie reakce přizpůsobené konkrétním podmínkám nebo lokalitě a dostupné infrastruktuře i specifickým potřebám obyvatelstva. Klíčovou roli hraje kvalita vstupních dat a spolehlivost samotných modelů, což je jedna z hlavních výzev pro jejich využití v praxi.

Kromě technických aspektů ovšem nelze opomenout ani etický, právní a bezpečnostní rozměr. Využití AI k ochraně obyvatelstva přináší zásadní otázky týkající se soukromí, transparentnosti procesu rozhodování a možné diskriminace určitých skupin. Zvláštní pozornost je proto třeba zaměřit na právní zakotvení těchto technologií, pravidla jejich použití a odpovědnost za jejich výsledky. Zároveň je třeba se zabývat hrozbami, které představuje kybernetický útok, jenž může v kritických okamžicích zásadně narušit fungování systémů AI.

Důležitým aspektem se rovněž stává přímá komunikace mezi jednotlivými systémy AI a obyčejnými uživateli. Aplikace pro první pomoc a připravenost na mimořádné události mohou sehrávat zásadní roli v tom, jak jsou lidé o situaci informováni, jak reagují a jaká rozhodnutí činí v mimořádných situacích. Důraz je kladen na adaptivní a personalizovaný přístup, který by zohledňoval zdravotní stav, polohu a digitální gramotnost uživatele. To otevírá možnost využívat AI nejen jako nástroj pro profesionály, ale také jako prostředek ke zlepšení informovanosti široké veřejnosti o bezpečnosti.

Na základě těchto teoretických východisek se praktická část práce zaměří na podrobnou analýzu vybraných mobilních aplikací v oblasti první pomoci a ochrany zdraví a života. Cílem bude zjistit, do jaké míry využívají principy AI, jaká jsou jejich technická a funkční omezení a kde existuje potenciál pro zlepšení. Výsledkem bude koncepční návrh ideální

aplikace „True Life Guardian“, která bude stavět na silných stránkách stávajících platforem a zároveň řešit problémy spojené s efektivní a eticky odpovědnou implementací AI v oblasti ochrany obyvatelstva.

II. PRAKTICKÁ ČÁST

5 APLIKACE PRO POSKYTOVÁNÍ PRVNÍ POMOCI

Budoucnost se mění díky digitální technologii AI, zejména v oblasti zdravotnictví. V kontextu první pomoci se očekává, že AI umožní, aby se záchranné zásahy staly jednoduššími, rychlejšími a efektivnějšími. Dokáže automaticky přivolat pomoc pomocí mobilních telefonů a detekce dopravních nehod má velký vliv na krátkou dobu krizové reakce. Využití AI při výcviku záchranářů navíc umožňuje efektivnější učení prostřednictvím realistických scénářů a relevantních doporučení pro zlepšení záchranářských dovedností (American CPR Care Association, © 2025).

AI a automatizační techniky, jako je ML a zpracování NLP, umožnily vytvořit interaktivní výcvikové zkušenosti. Metody strojového učení umožňují systému rozvíjet a stavět na vlastních znalostech, zatímco zpracování přirozeného jazyka mu umožňuje interpretovat zadané vstupy (ať už mluvené, nebo psané) a vhodně na ně reagovat. Aplikace první pomoci řízená za pomoci AI by tak například mohla někomu pomoci při resuscitaci nebo rozpoznat příznaky mrtvice a na základě zpětné vazby v reálném čase modelovat instrukce, které uživateli dává na základě získaných odpovědí (American CPR Care Association, © 2025).

Analýza stávajících aplikací, jako je například Záchranka, zahraniční PulsePoint Respond a další, umožňuje hledat silné a slabé stránky těchto existujících aplikací, které pomohou k návrhu lepších řešení. Zkoumání těchto technologií napomůže pochopení potenciálu AI pro optimalizaci zásahů záchranných služeb a také zvýšení informovanosti veřejnosti, stejně jako reakce na zdravotní problémy přítomné v prostředí, včetně první pomoci postiženému jedinci. Proto je cílem této části práce zhodnotit současné aplikace a předložit návrhy na jejich potenciální vylepšení tak, aby AI ještě více sloužila potřebám při prevenci společenských hrozeb a ochrany obyvatelstva (Brooks et al., 2016).

Důvod výběru analyzovaných aplikací

Pro účely analýzy v této kapitole, byly vybrány aplikace Záchranka, PulsePoint Respond, EchoSOS, GoodSAM a Life360 z důvodu jejich různorodosti, mezinárodního dopadu a specifického zaměření na různé aspekty krizové pomoci a první reakce. Každá z těchto aplikací přináší unikátní funkcionality, které přispívají ke komplexnímu pochopení toho, jak mohou digitální nástroje pomáhat při záchranně životů a ochraně obyvatelstva.

Záchranka - Reprezentuje české prostředí a ukazuje, jak lze systém efektivně integrovat do národní infrastruktury záchranné služby. Nabízí přímé napojení na tísňové linky a lokalizační funkce přizpůsobené místním podmínkám.

PulsePoint Respond - Představuje komunitní přístup k první pomoci. Aplikace umožňuje zapojení vyškolených laiků do poskytování pomoci ještě před příjezdem záchranářů. Je tak ukázkou, jak lze využít veřejnost pro záchranu životů.

EchoSOS - Byla vybrána jako příklad mezinárodní krizové aplikace pro cestovatele. Zajišťuje automatické připojení k místní tísňové lince po celém světě a podporuje lokalizaci, což je zásadní pro mimořádné události v zahraničí.

GoodSAM - Je příkladem platformy pro profesionální a dobrovolnické záchranáře, kteří jsou okamžitě informováni o blízké krizové situaci. Ukazuje potenciál rychlého přesměrování pomoci k nejbližší kvalifikované osobě, a to i v městském prostředí.

Life360 - Aplikace zaměřená na sledování polohy a bezpečnost rodiny, rozšiřuje pohled na ochranu obyvatelstva nejen při akutních krizích, ale i z hlediska dlouhodobé prevence a zabezpečení blízkých v každodenním životě.

Tato škála aplikací byla zvolena záměrně, protože společně tvoří komplexní obraz toho, jak různé přístupy - národní, komunitní, cestovní, profesionální i rodinné - přispívají k ochraně zdraví a života prostřednictvím digitálních technologií, s využitím AI.

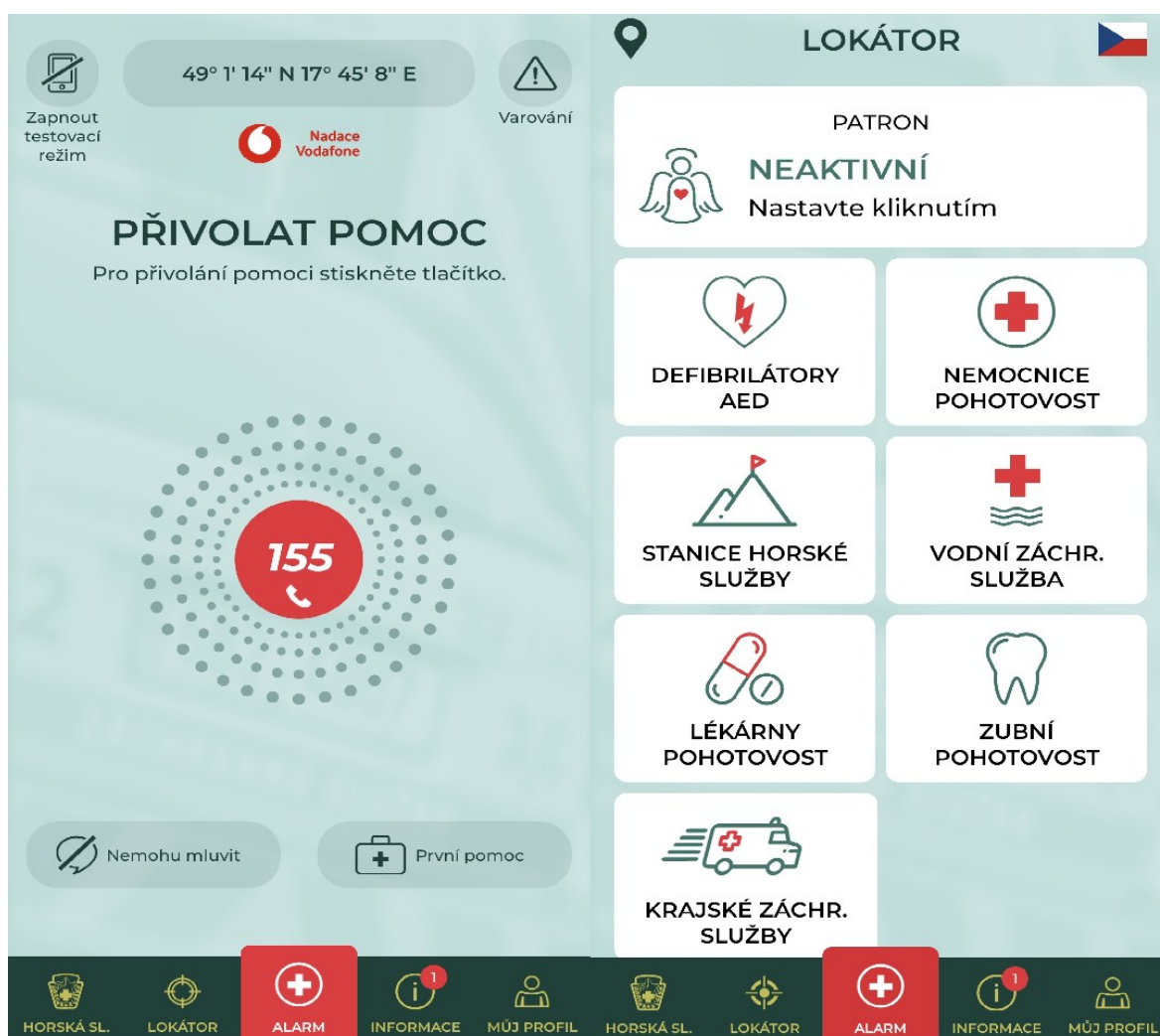
5.1 Aplikace Záchranka

Aplikace Záchranka je český mobilní nástroj, který usnadňuje přivolání pomoci v naléhavých situacích. Jejím hlavním posláním je co nejrychleji zprostředkovat uživatelům kontakt s IZS a nasadit záchranné složky. Díky integraci s dispečinkou záchranných služeb umožňuje okamžité poskytnutí informací o poloze a zdravotním stavu uživatele, čímž se výrazně zvyšuje efektivita zásahu a může pomoci při rozhodování o záchranně života (Záchranka, © 2025).

Aplikace byla spuštěna v roce 2016 a jedná se o malý startupový projekt Jana Šebka ve spolupráci se Zdravotnickou záchrannou službou ČR. Od té doby prošla řadou aktualizací, které vylepšily její funkčnost a rozšířily její využitelnost v nejrůznějších krizových situacích. K prosinci 2024 měla aplikace více než 3 miliony uživatelů. Začínala se zdravotnickou pomocí, ale časem se rozšířila i na ostatní složky IZS, Horskou službu, Vodní záchrannou službu a další odborné složky. V roce 2020 byla aplikace nasazena také v dalších zemích,

jako jsou Slovensko a Rakousko, čímž se stala cenným nástrojem při přeshraničních záchranných akcích (Záchranka, © 2025).

Další z klíčových služeb tohoto systému je automatické odesílání souřadnic GPS při volání na policii na číslo 155. To je důležité zejména za okolností, kdy volající není schopen určit svou polohu, například při nehodě v terénu nebo při lékařské pohotovosti. Dále aplikace umožňuje uživatelům ukládat ve svém profilu zdravotní údaje, jako jsou alergie, chronická onemocnění nebo kontakty na blízké osoby, díky čemuž mohou záchranáři získat cenné informace ještě předtím, než se dostanou na místo události (Záchranka, © 2025).



Obrázek 1: Aplikace Záchranka (Zdroj: Záchranka, © 2025)

Obrázek zobrazuje úvodní stránku aplikace Záchranka, kde je prominentně zobrazeno tlačítko pro přivolání tísňové linky 155, umožňující rychlou reakci v případě nouzové situace. Pod tímto tlačítkem je umístěn lokátor, který umožňuje uživateli snadno přistupovat k informacím o defibrilátorech v okolí, pohotovostech, a speciálních záchranných službách jako jsou vodní a horská služba. Tento nástroj poskytuje uživateli přehled o dostupnosti

těchto důležitých zařízení a služeb v jeho blízkosti, což může výrazně zrychlit a zefektivnit pomoc v kritických momentech.

Další významnou funkcí aplikace je přivolání horské služby, což je užitečné pro horské turisty a sportovce v horách. Uživatelé mohou také využít off-line režim, který odešle nouzovou zprávu, i když je signál slabý. Aplikace obsahuje také mapu automatických externích defibrilátorů (AED), dále poskytuje upozornění na mimořádné události, jako je nepříznivé počasí nebo potenciální záplavy (Záchranka, © 2025).

Aplikace Záchranka se stala klíčovým nástrojem krizové komunikace a její využití neustále roste. Díky inovacím a rozšířeným funkcím se stala nejen prostředkem pro přivolání pomoci, ale také důležitým prvkem prevence a informovanosti veřejnosti v oblasti krizového řízení. Do budoucna se plánuje další vývoj, včetně využití AI pro analýzu mimořádných událostí, což by mohlo jeho využití při ochraně obyvatelstva ještě zefektivnit. Analýza se zaměřuje na silné a slabé stránky aplikace Ambulance s významnými návrhy na zlepšení, což je zásadní pro vyhodnocení jejího využití v krizovém řízení a ochraně obyvatelstva (Záchranka, © 2025).

Silné stránky aplikace Záchranka

- Automatické odeslání polohy a zdravotních údajů: Při aktivaci tísňového volání aplikace automaticky odesílá GPS souřadnice volajícího, což usnadňuje jeho lokalizaci i v případě, že není schopen mluvit. Uživatel může do aplikace předem uložit své zdravotní údaje (např. alergie, chronická onemocnění), které jsou při volání automaticky sdíleny s operátory záchranné služby.
- Přímá integrace s linkou 155 a horskou službou: Záchranka je plně propojena s dispečinkou zdravotnické záchranné služby v České republice, na Slovensku a Rakousku. Umožňuje speciální režim volání Horské služby, který pomáhá při záchrane osob v těžko dostupném terénu.
- Offline funkce a nouzové SMS: V případě nedostupnosti mobilní sítě umožňuje odeslání tísňového volání prostřednictvím SMS, což zvyšuje šanci na přivolání pomoci v oblastech s nízkým pokrytím signálem. Obsahuje interaktivní návody první pomoci, které jsou dostupné i bez internetového připojení.
- Funkce varovných zpráv a upozornění: Aplikace dokáže uživatele informovat o mimořádných událostech, jako jsou přírodní katastrofy, epidemie nebo

nehody v jejich okolí. Obsahuje také informace o nejbližších pohotovostech a lékařských zařízeních.

- Jednoduché a intuitivní uživatelské rozhraní: Aplikace je navržena tak, aby ji mohli snadno používat i senioři nebo lidé s minimálními technickými dovednostmi. Aktivace tísňového volání je možná jedním stiskem tlačítka, což minimalizuje zdržení v krizových situacích.
- Podpora pro sluchově postižené: Uživatelé se sluchovým postižením mohou využít textovou komunikaci s operátory záchranné služby, což zajišťuje dostupnost pomoci i pro osoby s touto specifickou potřebou.

Slabé stránky aplikace Záchranka

- Omezená geografická dostupnost: Aplikace je primárně určena pro Českou republiku, Slovensko a Rakousko, což omezuje její využití v jiných zemích. Uživatelé cestující do zahraničí se musí spoléhat na jiné aplikace nebo místní záchranné systémy. V budoucnu se plánuje rozšíření o mezinárodní expanzi a spolupráci s evropskými záchrannými systémy.
- Závislost na funkčnosti GPS a mobilního připojení: Přesnost lokalizace závisí na kvalitě GPS signálu, což může být problém v husté městské zástavbě, uvnitř budov nebo v horském terénu. Pokud není dostupné žádné připojení k mobilní síti, odeslání informací může být opožděné nebo nemožné.
- Chybějící napojení na dobrovolnické záchranáře: Na rozdíl od některých mezinárodních aplikací (např. GoodSAM) neumožňuje přímou aktivaci vyškolených dobrovolníků v okolí, kteří by mohli poskytnout první pomoc před příjezdem záchranné služby.
- Nedostatečná interakce s jinými krizovými složkami: Aplikace je primárně zaměřena na zdravotnickou záchrannou službu, ale neposkytuje přímou možnost kontaktování hasičů nebo policie (na rozdíl od aplikací jako EchoSOS, které nabízejí široké spektrum krizových kontaktů).
- Vyšší spotřeba baterie při aktivním používání: Neustálé sledování polohy a možnost odesílání varovných zpráv mohou zvyšovat spotřebu baterie, což může být problém zejména při delším pobytu v terénu bez možnosti nabíjení.

- **Chybějící funkce videopřenosu:** Na rozdíl od některých konkurenčních aplikací nenabízí možnost živého videopřenosu, což by mohlo pomoci operátorům lépe vyhodnotit situaci volajícího a poskytnout přesnější pokyny k první pomoci.

Návrhy na zlepšení

Na základě analýzy lze identifikovat několik oblastí pro zlepšení, které by mohly zvýšit efektivitu aplikace Záchranka:

- **Rozšíření dostupnosti aplikace na další země:** Umožnění využití aplikace v dalších státech, případně spolupráce s mezinárodními záchrannými systémy.

Co je potřeba k realizaci: Vyjednání spolupráce s národními záchrannými službami daných států. Lokalizace aplikace (jazyková mutace, mapy, specifika nouzových volání v dané zemi). Integrace s místními systémy tísňového volání (včetně legislativního rámce).

- **Integrace s dobrovolnickými záchrannými sítěmi:** Možnost propojení s vyškolenými dobrovolníky v okolí uživatele, kteří by mohli poskytnout první pomoc před příjezdem profesionálního zdravotnického týmu.

Co je potřeba k realizaci: Vytvoření registru a databáze vyškolených dobrovolníků (např. certifikovaní první pomocníci, hasiči, zdravotníci). Geolokační systém pro přiřazení dobrovolníků v blízkosti události. Právní vymezení odpovědnosti dobrovolníků a pojištění.

- **Zavedení pokročilého určování polohy v interiérech:** Návrh na doplnění stávajícího lokalizačního systému o technologii vnitřního určování polohy, jako jsou majáky Bluetooth Low Energy (BLE), ultrazvuková triangulace nebo přesnější Wi-Fi otisky prstů. To by zlepšilo přesnost v místech, kde jsou signály GPS slabé nebo nedostupné (např. nákupní centra, stanice metra, velké kancelářské budovy).

Co je potřeba k realizaci: Implementace technologií jako BLE majáky v klíčových veřejných budovách (letišť, nádraží, nákupní centra). Spolupráce s provozovateli budov na zpřístupnění signálových map. Vytvoření algoritmů, které kombinují tyto technologie se stávající GPS/Wi-Fi lokalizací.

- **Přidání podpory videopřenosu:** Možnost živého streamování videa by umožnila operátorům lépe analyzovat situaci a poskytnout přesnější pokyny volajícímu.

Co je potřeba k realizaci: Vývoj bezpečného, šifrovaného video kanálu s nízkou latencí. Navýšení kapacity serverů a šířky přenosového pásma. Školení operátorů na práci s videoobsahem v reálném čase.

- **Integrace s dalšími krizovými složkami:** Přidání možnosti kontaktovat nejen zdravotnickou záchrannou službu, ale i hasiče nebo policii, čímž by se aplikace stala univerzálním krizovým nástrojem.

Co je potřeba k realizaci: Vyjednání spolupráce s jednotlivými složkami IZS (hasiči, policie). Úprava systému směřování výzev podle typu události (např. požár → hasiči). Vývoj rozhraní pro různé typy zásahových jednotek a jejich potřeby.

Závěr – hodnocení

Aplikace Záchranka se od svého vzniku stala klíčovým nástrojem pro rychlé a efektivní přivolání pomoci v nouzových situacích. Díky automatickému odesílání polohy a zdravotních údajů výrazně zvyšuje šance na rychlou a adekvátní reakci záchranných složek. Integrace s linkou 155, Horskou službou a dalšími záchrannými složkami umožňuje široké využití v různých krizových situacích, včetně těžko dostupného terénu. Další výhodou je off-line funkčnost, nouzové SMS a varovné zprávy, které poskytují uživatelům důležité informace o aktuálních hrozbách v jejich okolí. Intuitivní uživatelské rozhraní a podpora pro sluchově postižené činí aplikaci přístupnou pro širokou veřejnost.

Aplikace má však některá omezení, jako je geografická dostupnost pouze v několika zemích, závislost na mobilním signálu, GPS a žádné spojení s dobrovolnickými záchrannými sítěmi, které mohou zvýšit šance na rychlé získání pomoci. Mezi další nevýhody patří vyšší spotřeba baterie při aktivním používání a nemožnost odesílat video, které by operátorům pomohlo lépe pochopit situaci volajícího.

Na základě analýzy byla identifikována řada možností pro zlepšení aplikace. Mezi hlavní doporučení patří lepší dostupnost pro další země, lepší propojení s dobrovolníky a dalšími pracovníky záchranných složek, lepší lokalizace GPS pro přesnější určení polohy i v oblastech se slabým signálem a možnost živého přenosu videa pro lepší vyhodnocení situace. Tyto vylepšení by mohly aplikaci Záchranka přiblížit k tomu, aby se z ní stal ještě

účinnější a komplexnější nástroj krizové komunikace, který má potenciál zachránit ještě více životů.

5.2 PulsePoint Respond

Aplikace PulsePoint Respond je revoluční mobilní aplikace, která zvyšuje šance na přežití osob s náhlou srdeční zástavou (NSS) tím, že spojuje vyškolené pracovníky první pomoci s místem, kde se oběť NSS nachází. Hlavním cílem je zkrátit dobu potřebnou k poskytnutí pomoci, a zvýšit tak pravděpodobnost záchrany života před příjezdem záchranné služby (PulsePoint Respond, © 2025).

Poprvé byla aplikace spuštěna v roce 2011 a byla navržena nejen nadací PulsePoint, ale i ve spolupráci s americkými záchrannými službami. Tato aplikace má síť s více než 3 miliony odběratelů. Jejím účelem je automaticky upozornit vyškolené dobrovolníky v okolí, kteří mohou provádět kardiopulmonální resuscitaci (KPR), dokud nedorazí záchranná pomoc. Aplikace je propojena s místními dispečinkami záchranné služby, díky čemuž je zajištěno rychlé nasazení sítě laických záchranářů, pokud někdo utrpí srdeční kolaps na veřejném místě (PulsePoint Respond, © 2025).

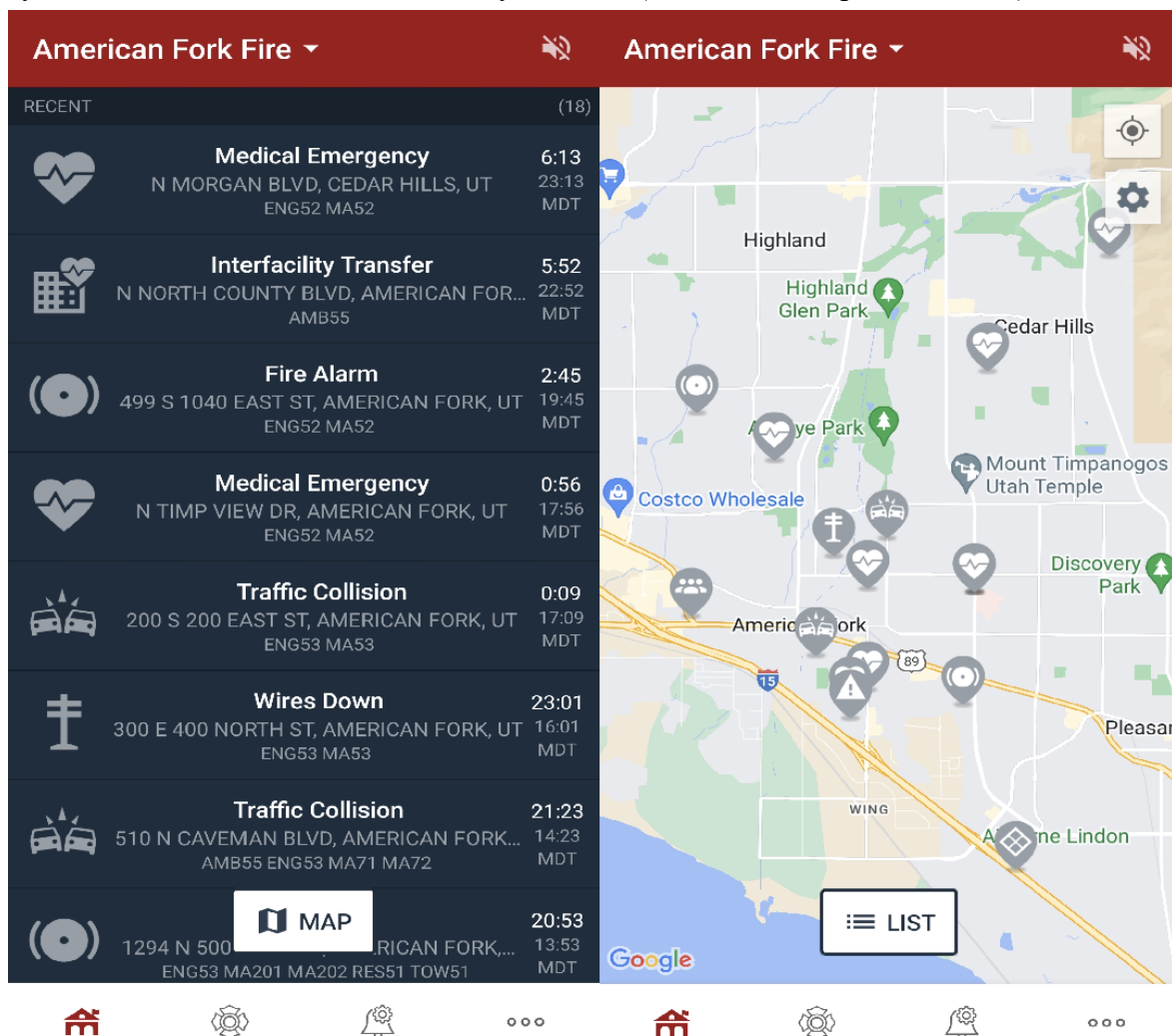
Jednou z jeho hlavních funkcí je interaktivní mapa AED, která dobrovolníkům umožňuje rychle vyhledat nejbližší zařízení, které jim poskytne elektrický výboj. K dispozici je také možnost nahlásit nové AED, čímž se rozšíří databáze a zvýší se dostupnost tohoto život zachraňujícího zařízení (PulsePoint Respond, © 2025).

Kromě poskytování pomoci v případech srdeční zástavy aplikace zahrnuje i živé sledování volání záchranných služeb, takže široká veřejnost může vidět, kde se v danou chvíli nacházejí místní hasiči a lékařské týmy. Tato funkce zvyšuje informovanost o záchranných operacích a může být užitečná i pro profesionální záchranáře. (PulsePoint Respond, © 2025).

PulsePoint Respond vybízí obyčejné lidi, aby se zapojili do komunity poskytovatelů první pomoci a dostali své blízké bezpečně pod kontrolu, než dorazí profesionálové. Vytvořením spojení s vyškolenými dobrovolníky a IZS může podstatně zvýšit míru přežití obětí srdeční zástavy, vzhledem k tomu, že při zajištění úspěšné resuscitace obětí srdeční zástavy hraje zásadní roli čas (PulsePoint Respond, © 2025).

Aplikace se aktivně používá hlavně v USA a Kanadě, ale její koncept je přenositelný i do jiných zemí. V budoucnu se očekává její další rozšíření a případné zapojení AI pro

efektivnější analýzu událostí a lepší koordinaci dobrovolníků. Aplikace je tak skvělým příkladem technologie, která spojuje inovace, komunitní spolupráci a moderní krizové řízení ve prospěch záchrany životů. Tato analýza přezkoumává silné a slabé stránky PulsePoint Respond s významnými návrhy na její vylepšení, které jsou zásadní pro vyhodnocení jejího využití v krizovém řízení a ochraně obyvatelstva (PulsePoint Respond, © 2025).



Obrázek 2: Aplikace PulsePoint Respond (Zdroj: PulsePoint Respond, © 2025)

Na obrázku lze vidět přehled mimořádných událostí a krizových situací vyskytujících se v části Amerického pobřeží, kde jsou právě v danou chvíli řešené tyto problémy. Přehled taky zahrnuje, kdy daný problém byl zaregistrován a v jakou chvíli bude příslušnými jednotkami vyřešen.

Silné stránky aplikace PulsePoint Respond

- **Aktivace vyškolených dobrovolníků v reálném čase:** Aplikace upozorňuje vyškolené dobrovolníky v bezprostřední blízkosti osoby se srdeční zástavou a umožňuje jim okamžitě zasáhnout před příjezdem záchranářů. Zvyšuje

pravděpodobnost zahájení včasné kardiopulmonální resuscitace (KPR), což výrazně zlepšuje šance na přežití pacienta.

- **Napojení na tísňová volání a zdravotnické záchranné služby:** Systém je propojen s dispečinkou tísňových služeb a automaticky informuje dobrovolníky v okamžiku přijetí nouzového volání. Umožňuje efektivnější koordinaci mezi záchranáři, veřejností a zdravotnickými složkami.
- **Interaktivní mapa dostupných AED (automatizovaných externích defibrilátorů):** PulsePoint Respond zobrazuje seznam a polohu nejbližších defibrilátorů, což pomáhá dobrovolníkům rychle zajistit přístup k potřebnému vybavení. Uživatelé mohou do databáze přidávat nové AED a pomáhat tak zlepšovat pokrytí oblasti.
- **Školení a vzdělávání uživatelů:** Aplikace nabízí instruktážní videa a návody na provádění první pomoci a KPR, čímž pomáhá zvyšovat připravenost veřejnosti na krizové situace. Uživatelé mohou absolvovat online tréninky a zlepšovat své dovednosti.
- **Upozornění na mimořádné události:** PulsePoint Respond dokáže uživatele informovat o požárech, dopravních nehodách a dalších mimořádných situacích v jejich okolí. Podporuje komunitní zapojení a umožňuje občanům lépe reagovat na krizové situace.
- **Podpora pro širokou škálu záchranných organizací:** Aplikace je využívána ve spolupráci s hasiči, záchranáři i dalšími krizovými složkami, což z ní činí flexibilní nástroj využívaný pro různé typy nouzových a mimořádných situací.

Slabé stránky aplikace PulsePoint Respond

- **Závislost na dostupnosti vyškolených dobrovolníků:** Efektivita aplikace závisí na dostatečném počtu registrovaných dobrovolníků v dané oblasti. V méně osídlených regionech může být dostupnost pomoci omezená. Nedostatek aktivních uživatelů může vést k situacím, kdy není nikdo k dispozici pro rychlou reakci.
- **Omezená geografická dostupnost:** Aplikace je primárně využívána v USA a některých dalších zemích, ale její dostupnost je omezena na oblasti, kde ji

oficiálně podporují místní záchranné složky. V mnoha zemích zatím neexistuje oficiální integrace s místními nouzovými službami.

- **Absence pokročilých funkcí pro další typy nouzových situací:** PulsePoint Respond se zaměřuje primárně na srdeční zástavu, což omezuje její využití při jiných typech zdravotních krizí, jako jsou epileptické záchvaty, hypoglykemické stavy nebo alergické reakce. Chybí možnost upozornit dobrovolníky na potřebu jiných forem první pomoci.
- **Závislost na mobilním připojení a přesnosti GPS:** Přesnost lokalizace závisí na kvalitě GPS signálu, což může být problém v městské zástavbě, v budovách nebo v oblastech se slabým signálem. Pokud uživatel ztratí mobilní připojení, nemusí obdržet upozornění na nouzovou situaci.
- **Nutnost aktivního zapojení uživatelů:** Aplikace vyžaduje, aby byli dobrovolníci aktivní a ochotní okamžitě reagovat na výzvy, což nemusí být vždy zaručeno. Někteří uživatelé mohou aplikaci nainstalovat, ale nepodílet se na pomoci, což snižuje její efektivitu.
- **Chybějící funkce videopřenosu:** Na rozdíl od některých konkurenčních aplikací (např. GoodSAM) PulsePoint Respond nenabízí možnost videohovoru s operátory nebo dobrovolníky, což by mohlo pomoci při lepším vyhodnocení situace.

Návrhy na zlepšení

- **Rozšíření pokrytí a podpory aplikace v dalších zemích:** Spolupráce s místními zdravotnickými složkami a úřady by mohla pomoci rozšířit dostupnost aplikace do dalších regionů.

Co je potřeba k realizaci: Navázání partnerství s národními nebo regionálními integrovanými záchrannými systémy. Překlad a lokalizace aplikace do jazyků cílových zemí. Právní a regulatorní analýza včetně souladu s ochranou osobních údajů (např. GDPR v EU).

- **Rozšíření zaměření na další typy zdravotních nouzových situací:** Přidání podpory pro další zdravotní stavy, jako jsou alergické reakce, cukrovka nebo epileptické záchvaty, by mohlo zvýšit využitelnost aplikace.

Co je potřeba k realizaci: Konzultace s lékaři a odborníky na urgentní medicínu. Úprava algoritmů pro rozpoznání a kategorizaci různých nouzových stavů. Vyškolení dobrovolníků v poskytování různých forem první pomoci.

- **Integrace s funkcí videopřenosu:** Možnost živého videopřenosu mezi dobrovolníkem a operátorem by mohla pomoci při rychlejší a přesnější vyhodnocení situace.

Co je potřeba k realizaci: Nasazení bezpečné platformy pro videohovory v reálném čase. Vyřešení právních aspektů přenosu obrazu a zvuku (ochrana osobních údajů, souhlas). Optimalizace přenosu videa pro nízkou šířku pásma (např. ve 4G/5G síti).

- **Lepší motivace pro dobrovolníky:** Zavedení systému odměn nebo gamifikace by mohlo podpořit aktivnější zapojení uživatelů.

Co je potřeba k realizaci: Vytvoření systému hodnocení a odměn (např. body, úrovně, odznaky). Možnost získání certifikátů či výhod (např. slevy, ocenění, dobrovolnické hodiny). Přehledné uživatelské statistiky a osobní profil s historií zásahů.

- **Podpora pro offline režim:** Možnost fungování aplikace i v oblastech se slabým signálem by zvýšila její dostupnost a efektivitu.

Co je potřeba k realizaci: Ukládání kritických informací (např. poloha, zdravotní stav) do cache s automatickým odesláním po obnovení signálu. Možnost předvyplnění profilu a nouzových informací uživatelem. Použití SMS fallback (záložní SMS) řešení v místech bez datového připojení.

Závěr – hodnocení

PulsePoint Respond je aplikace pro chytré telefony, která umožňuje lidem rychle reagovat a poskytnout život zachraňující opatření v případě náhlé srdeční zástavy a dalších mimořádných událostí. Mezi hlavní přednosti patří aktivace vyškolených dobrovolníků v reálném čase, propojení se záchrannými službami, interaktivní mapa AED, vzdělávací obsah pro uživatele a podpora široké škály záchranných organizací. Tyto funkce hrají zásadní roli při zvyšování pravděpodobnosti přežití pacienta a usnadňují lepší koordinaci mezi zdravotnickými službami a veřejností.

Aplikace má však svá omezení. Funguje dobře pouze v případě, že je najednou aktivní dostatečný počet dobrovolníků, což v řídké osídlených oblastech nemusí být vždy pravda. Kromě toho je její geografická dostupnost omezená, protože funguje pouze v USA a omezeném počtu dalších zemí. Mezi další nedostatky patří důraz na srdeční zástavu, který zastíňuje ostatní lékařské pohotovosti, což snižuje ostružinovou použitelnost aplikace pro pohotovosti nesouvisející se srdeční zástavou, závislost na přístupu k mobilní síti a přesnosti GPS nebo potřeba pokročilých funkcí, jako je například video streaming, který by mimo jiné usnadnil komunikaci mezi dobrovolníky a dispečinkem.

Aby byla aplikace efektivnější, je třeba provést vylepšení, jako je pokrytí lidí v jiných zemích, umožnění podpory jiných typů zdravotních problémů, zavedení videopřenosu nebo systému odměn, který by povzbudil více dobrovolníků. Další možností by byla podpora off-line, aby aplikace mohla lépe fungovat v oblastech se slabým signálem.

Závěrem lze konstatovat, že PulsePoint Respond nabízí slibný způsob záchrany životů, ale je spojen s určitými technickými a organizačními problémy, jejichž vyřešení může přinést další výhody pro veřejnost a první respondenty v krizovém řízení.

5.3 EchoSOS

EchoSOS je mobilní aplikace, která umožňuje rychle přivolat pomoc v nouzi, a to nejen doma, ale i na cestách v zahraničí. Její největší výhodou je automatické spojení s místními záchrannými službami, díky němuž se uživatelé dostanou do kontaktu s nejbližším záchranným centrem bez ohledu na to, kde na světě se nacházejí (Echo SOS, © 2025).

Aplikace byla vyvinuta ve Švýcarsku s cílem zjednodušit a urychlit komunikaci mezi občany a IZS. Přesný počet uživatelů této aplikace není veřejně dostupný, ale její celosvětový dosah poukazuje na velké množství aktivních uživatelů. Jako systém první pomoci se stala oblíbenou zejména u cestovatelů, turistů a záchranářů jako spolehlivý způsob, jak přivolat pomoc v krizové situaci (EchoSOS, © 2025).

Automatická lokalizace volajícího – funkce, která určuje souřadnice GPS volajícího a odesílá je operátorům tísňového volání je jednou z hlavních funkcí systému EchoSOS. To umožňuje záchranným službám rychleji reagovat na tísňovou situaci, i když si uživatel není jistý konkrétní adresou nebo se nenachází na známém území (EchoSOS, © 2025).

Aplikace je také propojena s lékařskými údaji uživatele, což znamená, že může operátorům předat důležité zdravotní informace, například o chronických onemocněních,

alergiích nebo užívaných lécích. Tento prvek může výrazně zvýšit efektivitu zásahu a přizpůsobit první pomoc konkrétním potřebám pacienta (EchoSOS, © 2025).

Kromě přímého volání záchranné služby EchoSOS nabízí i rychlý přístup k nejbližším zdravotnickým zařízením, lékárnám a automatizovaným externím defibrilátorům (AED). Uživatelé tak mohou rychle najít nejbližší pomoc, aniž by museli složitě vyhledávat dostupné možnosti (EchoSOS, © 2025).

Díky své jednoduchosti, mezinárodní dostupnosti a spolehlivosti získala EchoSOS oblibu zejména mezi častými cestovateli a horskými záchranáři a poskytovateli záchranné služby. S vývojem aplikace a integrací AI pro analýzu krizových stavů se stává EchoSOS stále důležitějším nástrojem digitálního managementu v krizových situacích. V této analýze jsou popsány silné a slabé stránky aplikace EchoSOS se zásadními doporučeními na zlepšení, což je klíčové pro zhodnocení jejího využití v krizovém řízení a ochraně obyvatelstva (EchoSOS, © 2025).



Obrázek 3: Aplikace EchoSOS (Zdroj: EchoSOS, © 2025)

Na obrázku je zobrazená úvodní stránka aplikace EchoSOS, která poskytuje rychlý přístup k důležitým tísňovým kontaktům. Uživatel má možnost ihned kontaktovat složky IZS, jako jsou policie, zdravotnická záchranná služba a hasiči, prostřednictvím jednoho kliknutí. Dále je zde zobrazená nouzová karta, která obsahuje klíčové zdravotní informace uživatele (např. alergie, chronická onemocnění a léky), které mohou být okamžitě přístupné pro záchranné týmy při krizové situaci. Tato funkcionality usnadňuje komunikaci a poskytování informací v případě nouze.

Silné stránky aplikace EchoSOS

- **Automatické přesměrování na lokální tísňovou linku:** Aplikace automaticky rozpozná, ve které zemi se uživatel nachází, a přesměruje volání na správnou tísňovou linku. Uživatel nemusí znát místní číslo pro záchranné služby, což je obzvláště užitečné při cestování.
- **Přesné sdílení polohy:** EchoSOS odešle tísňovým službám přesnou GPS polohu volajícího, což zrychluje a usnadňuje zásah záchranářů. Užitečné v přírodě, horách nebo jiných obtížně dostupných místech.
- **Off-line režim pro situace bez internetu:** Aplikace dokáže zobrazit důležitá nouzová čísla i bez připojení k internetu. Přestože přenos polohy vyžaduje síť, základní informace o tísňových službách jsou stále dostupné.
- **Možnost sdílení zdravotních informací:** Uživatelé mohou uložit své zdravotní údaje (např. alergie, chronická onemocnění, krevní skupinu) pro rychlý přístup v případě nouze. Tísňové služby mohou díky tomu lépe přizpůsobit svou reakci.
- **Integrace s některými záchrannými složkami:** V některých zemích jsou tísňové služby plně integrovány s aplikací, což znamená, že informace o poloze a zdravotním stavu jsou ihned dostupné dispečerům.
- **Uživatelsky přívětivé rozhraní:** Jednoduché a intuitivní ovládání umožňuje rychlou aktivaci nouzového volání i v krizových situacích.

Slabé stránky aplikace EchoSOS

- **Omezená podpora v některých zemích:** Přímá integrace s tísňovými službami není dostupná ve všech státech, což omezuje efektivitu aplikace v některých regionech. Ve státech bez integrace musí operátor údaje o poloze zadávat ručně.

- **Závislost na GPS signálu a mobilním připojení:** Přesnost polohy závisí na kvalitě GPS signálu, což může být problém v husté městské zástavbě nebo v budovách. Odesílání informací o poloze a zdravotním stavu vyžaduje mobilní data nebo Wi-Fi.
- **Absence komunitní pomoci:** Na rozdíl od aplikací jako GoodSAM nebo PulsePoint Respond neumožňuje EchoSOS aktivaci vyškolených dobrovolníků v okolí. Zaměřuje se výhradně na oficiální tísňové služby, což může prodloužit dobu odezvy v některých případech.
- **Omezené funkce pro vzdělávání uživatelů:** Aplikace neobsahuje interaktivní výukové moduly pro první pomoc, což by mohlo zvýšit připravenost uživatelů na krizové situace.
- **Nemožnost přímé komunikace s dispečerem:** Chybí funkce videohovoru nebo textového chatu s operátorem, což by mohlo být užitečné například pro neslyšící nebo osoby ve stresu.

Návrhy na zlepšení

Na základě této analýzy lze navrhnout několik vylepšení, která by mohla zvýšit efektivitu aplikace EchoSOS.

- **Rozšíření přímé integrace s tísňovými službami do dalších zemí:** Spolupráce s více záchrannými složkami by mohla zvýšit efektivitu přenosu polohy a zdravotních údajů.

Co je potřeba k realizaci: Navázání oficiální spolupráce s národními centry tísňového volání a záchrannými složkami. Zajištění právní kompatibility se zákony o ochraně osobních údajů (GDPR). Technická integrace s existujícími systémy nouzové infrastruktury (např. CAD systémy).

- **Možnost aktivace vyškolených dobrovolníků:** Přidání funkce pro upozorňování dobrovolníků v blízkosti pacienta by mohlo zkrátit čas do poskytnutí první pomoci. Co je potřeba k realizaci: Zavedení systému registrace a ověření kvalifikace dobrovolníků (např. školení první pomoci). Geolokační algoritmy pro lokalizaci a upozornění nejbližších dobrovolníků. Nastavení bezpečnostních a etických pravidel pro zapojení laiků do zásahu.

- Integrace videohovoru nebo textového chatu s operátorem: Možnost živé komunikace by mohla pomoci v situacích, kdy není možné telefonovat.

Co je potřeba k realizaci: Nasazení šifrované a bezpečné komunikační platformy pro video/text v reálném čase. Přizpůsobení rozhraní pro nouzovou komunikaci pro různé typy uživatelů (např. neslyšící). Optimalizace provozu pro různé rychlosti připojení a síťové podmínky.

- **Přidání výukových modulů pro první pomoc:** Interaktivní návody a instruktážní videa by mohly pomoci uživatelům lépe reagovat na krizové situace.

Co je potřeba k realizaci: Tvorba nebo licencování certifikovaných vzdělávacích materiálů (video, infografiky, testy). Interaktivní design modulů - například s krokovými návody nebo simulacemi. Lokalizace obsahu podle jazyka a kulturních specifik uživatelů.

- **Podpora pro lepší off-line funkce:** Rozšíření možností aplikace v případě výpadku mobilní sítě by zvýšilo její využitelnost v odlehlých oblastech.

Co je potřeba k realizaci: Implementace možnosti uložit nouzové informace (např. zdravotní profil, adresy) do zařízení. Funkce odeslání nouzové SMS s polohou, pokud není dostupné datové připojení. Upozornění na výpadek signálu s pokyny, jak postupovat (např. manuální volání tísňové linky).

Závěr – hodnocení

Aplikace EchoSOS představuje užitečný nástroj pro rychlé spojení s tísňovými službami, zejména v situacích, kdy uživatel nezná místní nouzové číslo nebo se nachází v obtížně přístupném terénu. Mezi její hlavní přínosy patří automatické přesměrování na správnou linku, přesné sdílení polohy a možnost uložení zdravotních informací, které mohou záchranným složkám pomoci lépe reagovat. Důležitým aspektem je také off-line režim umožňující přístup k tísňovým číslům i bez internetového připojení.

Na druhou stranu aplikace čelí určitým omezením. Přímá integrace s tísňovými službami není dostupná ve všech zemích, což může zpomalit přenos klíčových údajů. Další nevýhodou je závislost na kvalitě GPS signálu a mobilního připojení, absence komunitní pomoci a nedostatečná podpora vzdělávacích funkcí pro první pomoc. Chybějící možnost

přímé komunikace s dispečerem skrze videohovor nebo chat může rovněž představovat překážku v některých situacích.

Pro zlepšení efektivity aplikace by bylo vhodné rozšířit integraci s tísňovými službami do dalších zemí, umožnit aktivaci vyškolených dobrovolníků a přidat funkce jako videohovor nebo textový chat s operátorem. Dále by bylo užitečné implementovat interaktivní výukové moduly pro první pomoc a posílit off-line funkce, aby aplikace mohla lépe fungovat i v oblastech s omezeným signálem. Tato vylepšení by mohla zásadně zvýšit praktičnost a užitečnost EchoSOS v krizových situacích.

5.4 GoodSAM

GoodSAM je mobilní aplikace, která mění pravidla hry a v případě lékařské pohotovosti, automaticky upozorňuje vyškolené záchranáře v případě potřeby. Jejím hlavním účelem je spojit osoby, kterým hrozí nebezpečí ohrožení života, s nejbližšími záchranáři, vyškolenými laiky nebo zdravotníky, kteří jsou nablízku a mohou poskytnout první pomoc do příjezdu sanitky (GoodSAM, © 2025).

Aplikace byla vytvořena ve Velké Británii a její název vychází ze zásady dobrého samaritána, tedy rychlé a nezištné pomoci. Od svého zavedení se osvědčila po celém světě, kde se k ní přihlásily všechny hlavní záchranné služby, nemocnice a mnoho jednotlivých obcí v mnoha zemích. Počet aktivních uživatelů není veřejně dostupný, ale vzhledem k jejímu využívání záchrannými službami po celém světě, se bude jednat o velmi velkou uživatelskou základnu (GoodSAM, © 2025).

Hlavní výhodou GoodSAM je její schopnost automaticky lokalizovat a aktivovat nejbližší kvalifikované osoby, které mohou pomoci při srdeční zástavě, těžkých úrazech nebo jiných život ohrožujících stavech. Jakmile je aktivováno tísňové volání, aplikace odešle upozornění registrovaným dobrovolníkům, kteří se mohou k pacientovi dostat ještě před příjezdem sanitky a zahájit resuscitaci či jinou první pomoc (GoodSAM, © 2025).

Jednou z klíčových funkcí je integrace s tísňovými službami. V některých regionech je GoodSAM napojena přímo na zdravotnické operační středisko, což umožňuje operátorům identifikovat nejbližšího dostupného dobrovolníka a navigovat jej k místu události. Tato technologie výrazně zkracuje dobu do zahájení resuscitace, což je v případě srdeční zástavy zásadní pro přežití pacienta (GoodSAM, © 2025).

Aplikace také obsahuje interaktivní mapu dostupných automatizovaných externích defibrilátorů (AED). Díky této funkci mohou jak dobrovolníci, tak kolemjdoucí rychle najít nejbližší AED a zvýšit tak šanci na úspěšnou resuscitaci (GoodSAM, © 2025).

Další významnou součástí GoodSAM je funkce živého videopřenosu, která umožňuje operátorům tísňové linky vidět situaci přímo na místě události a poskytnout volajícímu či dobrovolníkům okamžité instrukce pro první pomoc. Tento prvek byl úspěšně použit například během pandemie COVID-19 pro vzdálené zdravotní konzultace a diagnostiku (GoodSAM, © 2025).

GoodSAM je využívána nejen zdravotnickými složkami, ale také hasiči, policií a dalšími krizovými službami. V některých regionech slouží k aktivaci dobrovolných záchranářů během velkých mimořádných událostí, jako jsou dopravní nehody, teroristické útoky nebo přírodní katastrofy (GoodSAM, © 2025).

Díky kombinaci geolokace, dobrovolnické sítě a integrace s krizovými službami se GoodSAM stala jedním z nejefektivnějších digitálních nástrojů pro záchranu životů. S rozvojem technologií a rostoucím zapojením AI do analýzy tísňových situací se očekává, že aplikace bude hrát ještě větší roli v moderním systému krizového řízení a první pomoci. Tato analýza se zaměřuje na silné a slabé stránky aplikace GoodSAM s důležitými návrhy na zlepšení, což je klíčové pro zhodnocení jejího využití v krizovém řízení a ochraně obyvatelstva (GoodSAM, © 2025).

Silné stránky aplikace GoodSAM

- **Okamžitá aktivace vyškolených dobrovolníků:** Aplikace propojuje lidi v nouzi s nejbližšími dobrovolníky vyškolenými v první pomoci. Systém umožňuje reakci ještě před příjezdem profesionálních záchranářů, čímž se zvyšuje šance na přežití.
- **Automatická detekce srdeční zástavy:** GoodSAM se často používá ve spojení s tísňovými linkami, které aplikaci aktivují v případě podezření na srdeční zástavu. Umožňuje rychlé nasměrování nejbližšího vyškoleného dobrovolníka k pacientovi.
- **Sdílení polohy a navigace k pacientovi:** Dobrovolníci jsou navigováni přímo k místu události pomocí GPS. Uživatelé mohou také nahlásit nouzovou situaci a sdílet svou polohu s tísňovými službami.

- **Integrace s defibrilátory (AED):** Aplikace ukazuje polohu nejbližších automatizovaných externích defibrilátorů (AED). Dobrovolníci mohou rychle najít a použít AED při zástavě srdce.
- **Podpora videohovorů pro okamžitou konzultaci:** GoodSAM umožňuje živé video připojení mezi volajícím a dispečerem, což může pomoci s poskytnutím první pomoci i v případech, kdy není přítomen vyškolený dobrovolník. Tato funkce je užitečná pro instruktáž laiků v krizových situacích.
- **Spolupráce s tísňovými službami:** GoodSAM je integrovaná s některými záchrannými systémy, což umožňuje lepší koordinaci mezi dobrovolníky a profesionálními složkami.
- **Možnost registrace profesionálů i vyškolených laiků:** Aplikace umožňuje zapojení jak profesionálních zdravotníků, tak vyškolených dobrovolníků, čímž se zvyšuje pokrytí a efektivita reakce na krizové situace.

Slabé stránky aplikace GoodSAM

- **Závislost na počtu aktivních dobrovolníků:** Efektivita aplikace závisí na dostupnosti dobrovolníků v dané oblasti. V méně obydlených lokalitách může být jejich počet omezený. Chybějící dostatečné síť vyškolených osob může znamenat větší reakční dobu.
- **Závislost na připojení k internetu a GPS:** Přesnost lokalizace dobrovolníků i pacientů závisí na síle GPS signálu a mobilního připojení. V oblastech se slabým pokrytím může být problematické, jak lokalizovat pacienta, tak odeslat informace tísňovým složkám.
- **Bezpečnostní a právní otázky:** Aktivace dobrovolníků k zásahům v terénu vyvolává otázky odpovědnosti a bezpečnosti. Některé státy mohou mít legislativní omezení týkající se poskytování první pomoci dobrovolníky mimo profesionální zdravotnické složky.
- **Možné zneužití systému:** Aplikace spoléhá na dobrovolníky, což znamená, že neexistuje 100% záruka jejich odborné způsobilosti v terénu. Mohou se vyskytnout falešné poplachy nebo situace, kdy dobrovolník nesplní očekávání.

- **Omezená dostupnost v některých regionech:** Ne ve všech zemích je GoodSAM plně podporován, což může omezit jeho využitelnost mimo specifické oblasti.

Návrhy na zlepšení

- **Rozšíření dobrovolnické sítě:** Větší propagace a nábor vyškolených dobrovolníků by mohly zlepšit dostupnost služby i v méně obydlených oblastech.

Co je potřeba k realizaci: Spuštění cílených náborových kampaní ve spolupráci se zdravotnickými organizacemi, školami, univerzitami nebo neziskovkami. Vytvoření motivačních programů, jako jsou odměny, certifikáty či veřejné uznání. Propagace na sociálních sítích, v mobilních aplikacích, na zdravotních portálech.

- **Integrace s dalšími krizovými systémy:** Možnost napojení na další aplikace krizového řízení by mohla zlepšit efektivitu spolupráce s profesionálními složkami.

Co je potřeba k realizaci: Napojení na systémy jako jsou CAD dispečerská centra, aplikace národní zdravotní péče (např. Záchranka, EchoSOS). Vytvoření standardizovaných protokolů pro předávání dat (např. lokalizace, stav pacienta, profil dobrovolníka). Právní a technické dohody mezi vývojáři aplikací a složkami IZS.

- **Vylepšená verifikace dobrovolníků:** Zavedení lepšího systému ověřování odborné způsobilosti by mohlo minimalizovat bezpečnostní rizika.

Co je potřeba k realizaci: Spolupráce s certifikačními autoritami (např. ČČK, zdravotní školy, profesní komory) pro potvrzení kvalifikace. Elektronický systém pro nahrání a ověření dokumentů (certifikátů, osvědčení) s možností pravidelné obnovy. Víceúrovňový systém ověření (např. laici / zdravotníci / profesionálové) s různými úrovněmi přístupu k výzvám.

- **Větší důraz na vzdělávání uživatelů:** Přidání interaktivních výukových modulů by mohlo zvýšit obecnou připravenost veřejnosti na poskytnutí první pomoci.

Co je potřeba k realizaci: Vývoj e-learningových kurzů s interaktivními prvky (kvízy, simulace, AR/VR tréninkové prvky). Možnost získání digitálních odznaků nebo certifikátů po úspěšném absolvování. Off-line dostupnost výukových materiálů pro okamžitou pomoc v terénu.

- **Off-line podpora pro nouzové situace:** Umožnění základních funkcí i v režimu off-line by mohlo pomoci v situacích bez dostupného mobilního připojení.

Co je potřeba k realizaci: Možnost uložení základních protokolů první pomoci a instrukcí přímo do aplikace. SMS fallback systém pro odesílání polohy nebo nouzové zprávy bez datového připojení. Upozornění na výpadek signálu a instrukce pro manuální kontaktování tísňové linky.

Závěr – hodnocení

Aplikace GoodSAM představuje inovativní nástroj pro rychlou aktivaci vyškolených dobrovolníků v případě zdravotní nouze, především při srdeční zástavě. Mezi její hlavní výhody patří schopnost propojit osoby v nouzi s nejbližšími dobrovolníky, kteří mohou poskytnout první pomoc ještě před příjezdem záchranných složek. Klíčové funkce, jako je automatická detekce srdeční zástavy, GPS navigace k pacientovi, integrace s AED a možnost videokonzultace s dispečerem, činí z aplikace cenný nástroj pro záchranu životů.

Na druhé straně však efektivita GoodSAM závisí na dostupnosti dobrovolníků v konkrétní oblasti, kvalitě GPS signálu a připojení k internetu. Další výzvou jsou bezpečnostní a právní otázky související s aktivací dobrovolníků, které se mohou lišit v jednotlivých zemích. Potenciální zneužití systému nebo nedostatečná odborná způsobilost některých dobrovolníků představují další rizika.

Na druhou stranu účinnost GoodSAM závisí na dostupnosti dobrovolníků v dané oblasti, kvalitě signálu GPS a připojení k internetu. Další výzvou jsou bezpečnostní a právní otázky spojené s aktivací dobrovolníků, které se mohou v jednotlivých zemích lišit. Další rizika představuje potenciální zneužití systému nebo nedostatečná kompetence některých dobrovolníků.

Pro zlepšení aplikace by bylo vhodné rozšířit síť dobrovolníků, posílit integraci s dalšími krizovými systémy a zlepšit proces ověřování dobrovolníků. Přidání školicích modulů a rozšíření off-line podpory by mohlo dále zvýšit její využitelnost v krizových

situacích. GoodSAM tak zůstává cenným nástrojem pro zdravotnickou pomoc v nouzi, jejíž potenciál lze ještě více rozvíjet implementací navrhovaných zlepšení.

5.5 Life360

Life360 je plnohodnotná aplikace pro zajištění bezpečnosti rodiny a určení polohy, která uživateli umožňuje zjistit, kde se členové jeho rodiny nacházejí, mít jistotu, že jsou v bezpečí, a poskytuje mu možnost komunikovat s nimi v reálném čase. Aplikace Life360, která obsahuje vše od sledování GPS přes detekci nehod a nouzová upozornění až po ochranu před kybernetickými hrozbami, se stala jednou z nejoblíbenějších platforem na trhu pro digitální dohled a ochranu přátel a rodiny (Life360 © 2025).

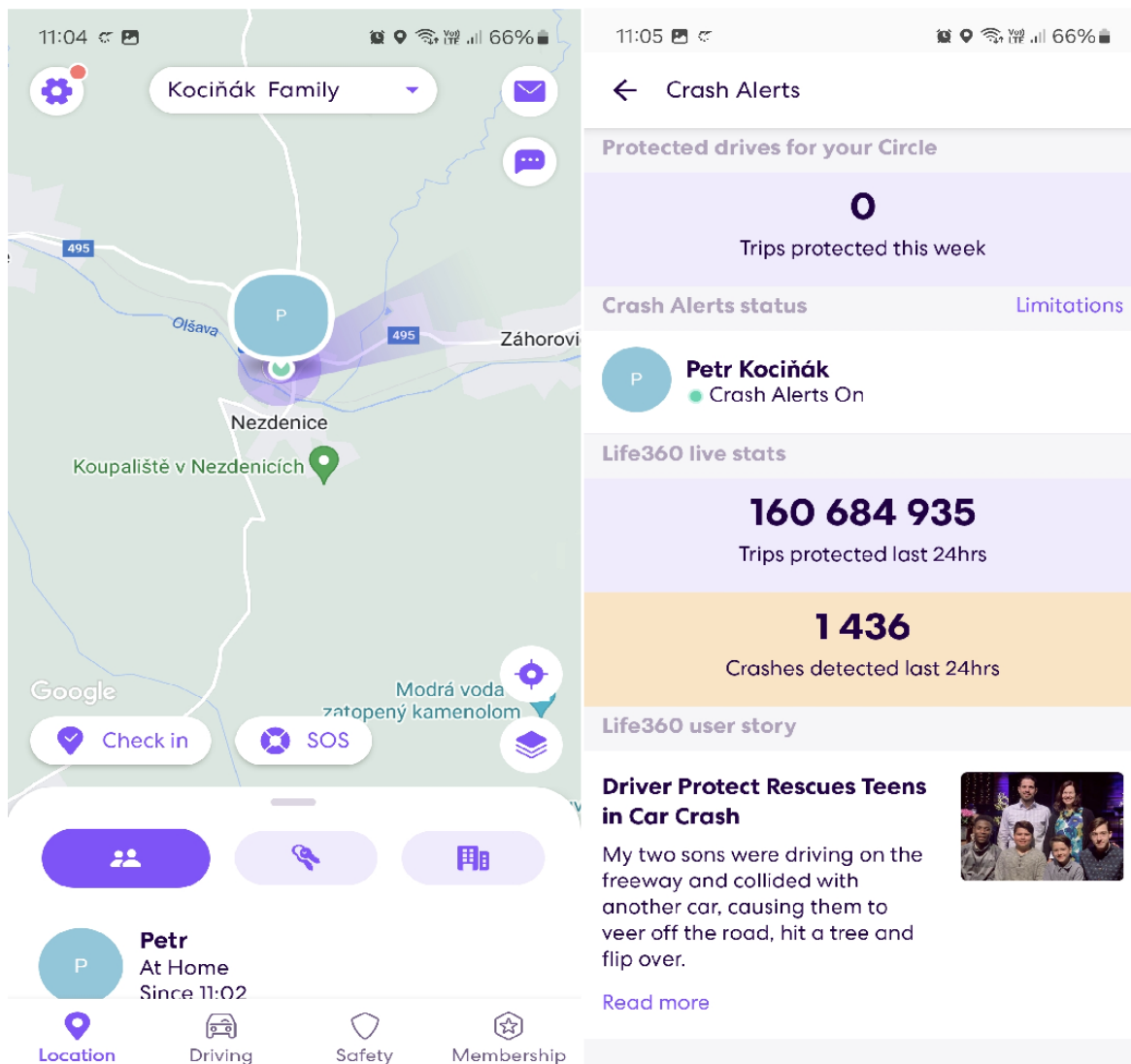
Od svého uvedení na trh v USA v roce 2008 se aplikace rychle rozvíjela. Nyní má desítky milionů uživatelů po celém světě a zaměřuje se na rodiny, které chtějí sledovat zejména své děti nebo starší příbuzné. Aplikaci Life360 využívají také skupiny přátel, cestovatelé nebo společnosti, jejichž cílem je zvýšit bezpečnost svých zaměstnanců v terénu (Life360 © 2025).

Jednou z klíčových funkcí aplikace je sledování polohy členů skupiny v reálném čase. Uživatelé mohou nastavit bezpečné zóny (např. domov, škola, práce) a obdržet oznámení, když někdo dorazí na místo nebo ho opustí. To je užitečné například pro rodiče, kteří chtějí vědět, kdy jejich dítě dorazilo ze školy domů (Life360 © 2025).

Další důležitou funkcí je detekce dopravních nehod. Life360 dokáže pomocí akcelerometru a GPS údajů rozpoznat prudké brzdění, nárazy a jiné krizové situace, a pokud dojde k nehodě, aplikace automaticky upozorní nouzové kontakty nebo dokonce může přivolat pomoc. Tato funkce je užitečná zejména pro mladé řidiče nebo osoby cestující na dlouhé vzdálenosti (Life360 © 2025).

S rostoucím důrazem na digitální bezpečnost a chytré technologie se očekává, že Life360 bude dále rozšiřovat své funkce, zejména v oblasti AI, prediktivní analýzy bezpečnostních rizik a pokročilé ochrany osobních údajů. Díky kombinaci lokalizačních služeb, krizového řízení a kybernetické ochrany zůstává Life360 jedním z nejkompaktnějších nástrojů pro rodinnou a osobní bezpečnost na světě.

Tato analýza se zaměřuje na silné a slabé stránky aplikace Life360 s důležitými návrhy na zlepšení, což je klíčové pro zhodnocení jejího využití v krizovém řízení a ochraně obyvatelstva (Life360 © 2025).



Obrázek 4: Prostředí aplikace Life360 (Zdroj: Life360, © 2025)

Obrázek zobrazuje úvodní stránku aplikace Life360, kde je zobrazená aktuální pozice členů rodiny v Nezdenicích na interaktivní mapě. Uživatel má přehled o pohybu jednotlivých členů rodiny v reálném čase. Dále je vidět sekce upozornění na nehody, která informuje o dopravních nehodách nebo neobvyklých událostech, které se staly členům rodiny v průběhu posledního týdne. Tyto varování pomáhají uživatelům okamžitě zjistit, zda došlo k nějaké krizové situaci v okruhu rodiny nebo kolem jejich aktuální polohy, a umožňují rychlou reakci v případě potřeby.

Silné stránky aplikace Life360

- **Sdílení polohy v reálném čase:** Uživatelé mohou sledovat aktuální polohu členů své skupiny (tzv. "kruh"), což je užitečné zejména pro rodiče monitorující své děti nebo pro krizové situace, kdy je důležité vědět, kde se kdo nachází.
- **Detekce dopravních nehod:** Aplikace automaticky rozpozná náraz při autonehodě a odešle upozornění rodinným příslušníkům. V některých verzích podporuje i přímé propojení s tísňovými službami.
- **Nouzové tlačítko (SOS funkce):** Life360 nabízí SOS režim, který v případě nouze odešle okamžité upozornění členům skupiny s přesnou polohou. Některé verze aplikace také umožňují automatické kontaktování nouzových služeb.
- **Historie pohybu a geofencing:** Uživatelé mohou zpětně prohlížet, kde se členové jejich skupiny nacházeli během určitého období. Geofencing umožňuje nastavit bezpečné zóny - například domov nebo školu – a odesílá upozornění, když někdo oblast opustí nebo do ní vstoupí.
- **Široká dostupnost a jednoduché použití:** Aplikace je k dispozici pro Android i iOS a je navržena tak, aby byla intuitivní i pro méně technicky zdatné uživatele.

Slabé stránky aplikace Life360

- **Obavy o soukromí a nepřetržité sledování:** Neustálé sdílení polohy může být vnímáno jako narušení soukromí, zejména mezi dospívajícími nebo lidmi, kteří nechťejí být nepřetržitě monitorováni. Někteří uživatelé označují aplikaci jako „invazivní“ a omezující svobodu pohybu.
- **Závislost na GPS a mobilních datech:** Přesnost sledování polohy závisí na kvalitě GPS signálu a dostupnosti mobilních dat. V oblastech se slabým pokrytím může aplikace zobrazovat nepřesné údaje nebo úplně přestat fungovat.
- **Placené funkce a omezení bezplatné verze:** Ačkoli základní funkce jsou zdarma, pokročilé funkce (např. detekce nehod, neomezená historie polohy, nouzová pomoc 24/7) jsou k dispozici pouze v placené verzi Life360 Premium.
- **Omezená integrace s oficiálními krizovými službami:** Na rozdíl od aplikací jako Záchranka nebo GoodSAM není Life360 primárně určena pro spolupráci s profesionálními záchrannými složkami, což snižuje její využitelnost v naléhavých krizových situacích.

- **Možnost zneužití a falešných poplachů:** Vzhledem k tomu, že aplikace umožňuje sledování polohy, existuje potenciální riziko jejího zneužití ke kontrole a manipulaci, například v toxických vztazích. Také se mohou vyskytovat falešné poplachy, které mohou vyvolat zbytečné obavy.

Návrhy na zlepšení

- **Větší důraz na ochranu soukromí:** Přidání pokročilejších nastavení ochrany osobních údajů by mohlo pomoci uživatelům lépe kontrolovat, kdy a komu sdílejí svou polohu.

Co je potřeba k realizaci: Vytvoření podrobnějších nastavení pro sdílení polohy (např. časové okno pro sdílení, možnost dočasného vypnutí sledování pro určité kontakty). Implementace transparentních zásad ochrany soukromí a možností uživatelům snadno spravovat jejich data (např. historická data o poloze). Umožnění anonymizace polohy pro určité skupiny (např. rodinné členy, přátelé) nebo pro specifické události.

- **Integrace s krizovými systémy:** Propojení s oficiálními záchrannými službami by mohlo zvýšit efektivitu aplikace v nouzových situacích.

Co je potřeba k realizaci: Vytvoření rozhraní pro programování aplikací, dále jen (API) pro napojení na místní tísňové linky a záchranné systémy (např. 112, 155). Zavedení automatického odesílání informací o poloze a zdravotních údajích do těchto krizových systémů při vyvolání poplachu.

- **Vylepšená off-line podpora:** Možnost nouzového režimu i bez internetu by byla přínosem pro krizové situace v odlehlých oblastech.

Co je potřeba k realizaci: Zavedení off-line režimu pro základní funkce, jako je sdílení polohy, tísňové volání a textové zprávy. Umožnění uchování kritických informací v aplikaci, jako jsou kontakty na tísňové osoby nebo mapy s určenými bezpečnými zónami. Použití technologie pro nouzovou komunikaci bez mobilních dat (např. SMS, satelitní komunikace).

- **Lepší detekce falešných poplachů:** Implementace AI pro rozpoznání falešných poplachů by mohla pomoci snížit zbytečné alarmy.

Co je potřeba k realizaci: Vývoj a implementace algoritmů strojového učení pro analýzu chování uživatele a predikci pravděpodobnosti skutečného

poplachu. Integrace s přístroji, které by mohly detekovat neobvyklé situace (např. senzor pohybu, GPS změny) a vyhodnotit, zda je poplach oprávněný. Možnost zpětné vazby od uživatelů a vyhodnocování výkonnosti AI pro postupné zlepšení přesnosti.

Závěr – Hodnocení

Aplikace Life360 poskytuje vynikající a efektivní sledování uživatelů a zároveň zachovává bezpečnost uživatele, zejména v rámci rodiny a osob v blízkém okolí. Sdílení polohy v reálném čase, detekce dopravních nehod, nouzové SOS tlačítko a geofencing jsou jejími největšími přednostmi. Tyto funkce pomáhají uživatelům získat jistotu a umožňují rychlou reakci při mimořádných událostech. Aplikace je intuitivní a s velmi širokým dosahem, takže se v ní bez problémů zorientují i technicky méně zdatní uživatelé.

Systém Life360 však může být napaden z důvodu nedostatečné ochrany soukromí, protože neustálé sledování může být považováno za obtěžující. Další slabinou je citlivost na měření vzdálenosti prostřednictvím signálu GPS a mobilních dat. Její účinnost v nouzových situacích dále snižuje omezená bezplatná verze a chybějící přímé propojení s oficiálními záchrannými službami.

Některé návrhy se týkaly zlepšení ochrany soukromí uživatelů, integrace s oficiálními krizovými systémy a rozsáhlejšího používání off-line systému. Pomohlo by také zavést sofistikovanější detekci falešných poplachů pomocí AI, aby se snížil počet nesprávných výstrah. Závěrem lze říct, že Life360 může pokračovat ve zvyšování bezpečnosti rodiny, nicméně jeho přítomnost nejen v rodinném životě, ale i v kvalifikovaném světě ukazuje, jakým směrem by měl postupovat, jak se integrovat, aby se vyrovnal s tím, když dojde k nouzovým situacím, a jak se jeho společnosti postarají o ochranu vašeho soukromí.

6 NÁVRH IDEÁLNÍ APLIKACE TRUE LIFE GUARDIAN APP

V současné době čelíme stále častějším krizovým situacím, ať už se jedná o přírodní katastrofy, zdravotní nouzové stavy, nebo bezpečnostní hrozby. Rychlá a efektivní reakce na tyto situace může znamenat rozdíl mezi životem a smrtí. True Life Guardian je revoluční aplikace, která kombinuje to nejlepší ze současných krizových a bezpečnostních aplikací, jako jsou Záchranka, PulsePoint Respond, EchoSOS, GoodSAM a Life360, aby poskytla ucelené řešení pro ochranu obyvatelstva.

Aplikace je navržena tak, aby nejen usnadnila přivolání pomoci v kritických situacích, ale také aby aktivně monitorovala a predikovala rizika pomocí AI. Díky široké paletě funkcí, včetně detekce nehod, sdílení polohy v reálném čase, prediktivní analýzy krizových situací a přímé integrace se záchrannými složkami, poskytuje True Life Guardian komplexní bezpečnostní síť, se zaměřením se na rozlišitelnost a architekturu systému. Tento systém nejenže pomůže jednotlivcům v nouzi, ale také podpoří efektivnější zásahy složek a IZS.

Součástí návrhu je i využití AI pro predikci krizových situací, což zahrnuje výběr a trénování vhodných modelů, práci s historickými a reálnými daty a zajištění spolehlivosti predikčních výstupů. Kombinace těchto aspektů činí z projektu nejen praktický nástroj pro ochranu obyvatelstva, ale i technologicky náročný systém, jehož vývoj a implementace vyžadují spolupráci odborníků z oblastí informatiky, krizového řízení, bezpečnosti a veřejné správy.



Obrázek 5: Logo aplikace True Life Guardian APP (Zdroj: Vlastní)

Název: True Life Guardian (v překladu „Pravý ochránce života“) odráží hlavní poslání aplikace – chránit životy občanů pomocí moderních technologií a AI.

"True" symbolizuje spolehlivost a důvěryhodnost – aplikace poskytuje přesné informace a eliminuje falešné poplachy.

"Life" zdůrazňuje primární cíl – ochranu života v krizových situacích.

"Guardian" vystihuje aktivní roli aplikace jako ochránce, který nejen reaguje na nouzové situace, ale také jim předchází díky AI predikcím.

V čem je aplikace revoluční:

True Life Guardian přináší zcela nový přístup k ochraně obyvatelstva díky kombinaci několika klíčových funkcí:

- **Proaktivní přístup k ochraně:** Na rozdíl od běžných aplikací nečeká na zavolání o pomoc, ale aktivně monitoruje a predikuje hrozby (např. přírodní katastrofy, dopravní nehody, zdravotní rizika).
- **Integrace AI do krizového řízení:** Systém analyzuje data v reálném čase, vyhodnocuje nebezpečí a automaticky navrhuje nejrychlejší řešení.
- **Automatické nouzové hlášení:** Pokud AI detekuje rizikovou situaci (např. pád, nehybnost, zvýšený srdeční tep), aplikace sama kontaktuje záchranné složky s přesnými informacemi.
- **Síťová bezpečnostní spolupráce:** Možnost propojení s ostatními uživateli, blízkými osobami nebo dokonce záchrannými týmy.
- **Minimalizace falešných poplachů:** AI analyzuje více faktorů, čímž omezuje zbytečná varování, která jsou častým problémem u současných aplikací.

Cílová skupina – Kdo bude aplikaci využívat:

True Life Guardian je navržena pro širokou škálu uživatelů - její flexibilita umožňuje přizpůsobení různým potřebám.

- **Jednotlivci** - Občané, kteří chtějí zvýšit svou bezpečnost v každodenním životě.
- **Senioři a lidé s chronickými onemocněními** - Automatická detekce pádů, monitorování vitálních funkcí.

- **Sportovci a cestovatelé** - Horská turistika, cyklistika nebo extrémní sporty s možností rychlé pomoci.
- **Obce a města** - Možnost hromadného varování obyvatel v případě krizové situace (povodně, požáry, blackouty).
- **Složky IZS** - Hasiči, záchranáři, policie mohou využívat sdílená krizová data a optimalizovat zásahy.

6.1 Klíčové vlastnosti aplikace

Efektivní reakce na krizové situace vyžaduje rychlou a přesnou komunikaci, spolehlivé sdílení informací a dostupnost nástrojů, které umožní koordinovanou pomoc. Moderní technologie, zejména AI a mobilní aplikace, dnes hrají klíčovou roli v zajištění bezpečnosti obyvatelstva a umožňují lidem lépe reagovat na nečekané události.

Cílem této kapitoly je představit hlavní funkce aplikace a vysvětlit, jak mohou přispět ke zvýšení bezpečnosti jednotlivců i celých komunit. Tato inovativní řešení nejen zlepšují připravenost na krizové situace, ale také pomáhají minimalizovat jejich dopady prostřednictvím rychlé a efektivní reakce.

Sdílení polohy v reálném čase:

- Možnost sledování polohy členů skupiny (rodiny, přátel, kolegů) v reálném čase.
- Dočasné sdílení polohy s bezpečnostními složkami v případě krizové situace.
- Integrace s chytrými hodinkami a nositelnými zařízeními.

Automatická detekce krizových situací:

- AI rozpoznávání nehod (dopravní nehody, pády, náhlé zdravotní potíže).
- Analýza zvukových signálů – detekce výstřelů, křiku, poplachu.
- Monitorování environmentálních rizik (zemětřesení, požáry, povodně) na základě senzorů a dat z externích zdrojů.
- Integrace s meteorologickými službami pro varování před extrémním počasím.

Nouzová tlačítka a okamžitá pomoc:

- SOS tlačítko: okamžité přivolání pomoci se sdílením polohy a zdravotních údajů.
- Tísňové zprávy se šifrováním pro rychlé informování blízkých nebo záchranných složek.
- AI chatbot pro rychlé vyhodnocení situace a doporučení nejlepších kroků.
- Integrace s defibrilátory v okolí (AED) a informace o jejich dostupnosti.

Integrace s krizovými službami:

- Přímá komunikace s tísňovými linkami a možnost připojení video/audio přenosu.
- Automatická identifikace prioritních případů pomocí AI.
- Možnost dohledání nejbližší pomoci (jednotky IZS).
- Digitální zdravotní karta s přístupem pro záchranáře.

Off-line režim a nízká spotřeba dat:

- Možnost nouzové komunikace i bez internetu pomocí SMS/GPS signálu.
- Optimalizace spotřeby baterie a datové náročnosti.
- Lokální ukládání kritických informací pro krizové situace.

Ochrana soukromí a bezpečnost dat:

- Šifrování dat a anonymizace polohy při běžném používání.
- Možnost časově omezeného sdílení polohy jen v případě nouze.
- AI rozpoznání zneužívání (např. sledování bez souhlasu uživatele).
- Dvoufázové ověřování identity a biometrické přihlášení.

Komunitní spolupráce a dobrovolníci:

- Možnost zapojení vyškolených dobrovolníků (první pomoc, evakuace).
- Sdílení informací o rizicích a varováních mezi uživateli.
- Systém hodnocení pro ověřování spolehlivosti dobrovolníků a uživatelů.
- Vzdělávací platforma s návody na poskytování první pomoci.

6.2 Umělá inteligence v aplikaci

Technologie AI představuje zásadní inovaci v oblasti krizového řízení a ochrany obyvatelstva. Její schopnost analyzovat obrovské množství dat v reálném čase, identifikovat vzorce a predikovat rizikové situace umožňuje záchranným složkám i běžným uživatelům lépe se připravit na mimořádné události a efektivněji na ně reagovat.

Cílem této kapitoly je představit inovativní způsoby, jak AI zvyšuje efektivitu krizového managementu a posiluje bezpečnost obyvatelstva. Díky těmto technologiím se zvyšuje nejen rychlost reakce na nebezpečné situace, ale také schopnost jednotlivců lépe se připravit a chránit sebe i své okolí.

Prediktivní modely krizových situací:

- AI analyzuje historická data o nehodách a vytváří modely rizikových oblastí.

Příklad: Modely mohou indikovat, že v určité oblasti (např. kvůli nepřehlednosti silnic, vysoké frekvenci dopravy nebo špatným povětrnostním podmínkám) je pravděpodobnost nehody výrazně vyšší než v jiných lokalitách.

- Predikce chování přírodních katastrof na základě meteorologických a geologických dat.

Příklad: Model by mohl predikovat, že v důsledku silného deště a zvyšujících se teplot v určitých oblastech dojde k riziku povodní, nebo že v případě seizmické aktivity v regionu dojde k vysoké pravděpodobnosti zemětřesení. Tyto modely mohou včas varovat záchranné složky a umožnit efektivní evakuaci obyvatel.

- Dynamická analýza dopravní situace pro optimalizaci přístupu záchranných složek.

Příklad: Pokud dojde k nehodě na hlavní silnici a záchranné složky se nemohou dostat na místo kvůli hustému provozu, AI může na základě aktuálních dat o dopravní situaci nabídnout alternativní trasu s nižšími zácpami nebo navrhnout cestu přes vedlejší silnice, čímž se zkrátí doba příjezdu.

Závěr: Prediktivní modely krizových situací využívají pokročilé analýzy dat k tomu, aby nejen zlepšily reakční dobu záchranných složek, ale také umožnily proaktivní přístup

k prevenci a mitigaci rizik. Použití těchto modelů může výrazně zlepšit účinnost krizového řízení, snížit počet obětí a minimalizovat materiální škody.

Automatická klasifikace a prioritizace událostí:

- Rozpoznání závažnosti incidentu a doporučení optimální reakce.

Příklad: Pokud dojde k autonehodě na dálničním úseku, AI může analyzovat, zda jsou zranění závažná, a na základě toho rozhodnout, zda je potřeba okamžitá zdravotnická pomoc, nebo zda jde o menší nehodu bez vážných následků. Na základě tohoto hodnocení doporučí optimální záchranné složky.

- Identifikace falešných poplachů a jejich filtrování.

Příklad: Pokud alarm signalizuje požár, ale na základě analýzy historických dat, chování senzorů a dalších indikátorů se ukáže, že se jedná o falešný poplach (např. špatně fungující senzor), AI filtruje tento poplach a neinformuje záchranné složky. Tento proces zabraňuje zbytečným výjezdům a šetří čas a prostředky.

- Využití AI pro real-time analýzu obrazu a videa ze sledovacích kamer.

Příklad: Pokud kamery na dálnici zachytí obraz požáru v autě, AI rozpozná kouř a plameny na základě analýzy obrazu, automaticky identifikuje závažnost situace a upozorní příslušné složky (hasiče a zdravotníky) s informacemi o poloze a rozsahu incidentu. Taková analýza může být užitečná také při sledování veřejných prostor nebo v kritických infrastrukturních zónách, kde je důležité okamžitě reagovat na potenciální krizové situace.

Závěr: Automatická klasifikace a prioritizace událostí pomocí AI může výrazně zefektivnit krizové řízení tím, že urychlí rozhodovací procesy, minimalizuje lidské chyby a optimalizuje využívání záchranných prostředků. Díky tomu, že AI dokáže nejen identifikovat incidenty podle jejich závažnosti, ale i filtrovat falešné poplachy a analyzovat video v reálném čase, může značně zlepšit efektivitu a rychlost reakce v krizových situacích.

Asistenční AI chatbot

- Rychlá diagnostika situace pomocí otázkového algoritmu.

Příklad: Pokud osoba zavolá chatbot pro pomoc při nehodě, chatbot může začít otázkami jako: "Jaké jsou příznaky?" nebo "Byl někdo zraněn?". Na základě

odpovědí může chatbot diagnostikovat, zda se jedná o zdravotní pohotovost (např. krvácení, mdloby) nebo nehodu, která vyžaduje jiný druh pomoci. Chatbot následně doporučí, co dělat dál (např. volání záchranné služby nebo poskytování první pomoci).

- Poskytování návodů na první pomoc nebo evakuaci v krizových situacích.

Příklad: Pokud chatbot detekuje, že uživatel hlásí osobu, která je v bezvědomí a nejeví známky dýchání, může začít poskytovat krok za krokem instrukce k zahájení kardiopulmonální resuscitace (KPR). Pokud by došlo k požáru, chatbot by poskytl instrukce k evakuaci, určení bezpečné cesty a správnému chování během evakuace.

- Interaktivní simulace krizových scénářů pro zvýšení připravenosti uživatelů.

Příklad: Uživatel by mohl projít simulací, kde se dozví, jak reagovat při požáru v budově. Během simulace by chatbot nabízel různé volby (např. evakuace, hledání hasicího přístroje, kontrola zdravotního stavu ostatních), a uživatel by musel zvolit nejlepší postup v dané situaci. Po dokončení simulace chatbot poskytne zpětnou vazbu o správnosti zvolených kroků, což pomůže uživatelům zlepšit jejich připravenost na skutečné krizové situace.

Závěr: Asistenční AI chatbot představuje významnou podporu v krizových situacích, kde jeho schopnost rychlé diagnostiky, poskytování návodů na první pomoc a evakuaci, a nabízení interaktivních simulací krizových scénářů výrazně zlepšuje schopnost uživatelů efektivně reagovat na nebezpečné situace. Chatbot je navržen tak, aby nejen asistoval v reálném čase, ale i pomáhal uživatelům zlepšovat jejich připravenost prostřednictvím tréninkových simulací, což přispívá k větší bezpečnosti a efektivitě v krizovém řízení.

Personalizace a adaptivní nastavení

- AI se učí chování uživatele a doporučuje relevantní bezpečnostní opatření.

Příklad: Pokud uživatel pravidelně používá aplikaci pro sledování své polohy v okolí a pravidelně vyhledává informace o blízkých krizových centrech (např. nemocnice, hasičské stanice), AI by mohla automaticky doporučit bezpečnostní opatření pro určité oblasti nebo nabídnout možnosti varování o blízkých nebezpečných událostech (např. hurikán nebo zemětřesení).

- Možnost přizpůsobení notifikací podle individuálních preferencí.

Příklad: Pokud má uživatel nastavený režim, který ho upozorní na nebezpečí související s jeho specifickým zdravotním stavem (např. alergie nebo epilepsie), AI by dokázala přizpůsobit frekvenci notifikací a informovat pouze o těch událostech, které mohou ovlivnit jeho zdraví.

- Integrace s chytrými zařízeními v domácnosti pro automatizaci varování.

Příklad: V případě požáru může aplikace zaslat varování na chytrý termostat a spustit požární alarmy, které jsou propojeny s aplikací. Pokud uživatel není doma, může aplikace automaticky informovat místní hasičský sbor a zároveň zaslat pokyny ostatním členům domácnosti pro evakuaci.

- Doporučení pro krizovou situaci na základě zdravotního stavu uživatele.

Příklad: Pokud uživatel trpí diabetem a zaznamená pokles hladiny cukru v krvi, aplikace by mu mohla automaticky doporučit, aby si vzal potřebné sladkosti nebo inzulín, případně přivolala pomoc, pokud se stav nezlepší. Aplikace by také mohla doporučit speciální krizové plány přizpůsobené zdravotnímu stavu uživatele, které by zahrnovaly opatření pro konkrétní typy zdravotních problémů.

- Personalizované krizové plány: Aplikace navrhuje krizové plány přizpůsobené zdravotním, lokalizačním a osobním potřebám uživatele.

Příklad: Pokud uživatel žije v oblasti náchylné k záplavám, aplikace by mu mohla nabídnout krizový plán, který zahrnuje varování o povodňových nebezpečích, specifické evakuační trasy, a doporučení pro připravení osobních věcí a zdravotních potřeb v případě nutnosti evakuace. Plán by byl personalizovaný podle konkrétních potřeb a zvyklostí uživatele, například s ohledem na jeho zdravotní stav (např. potřeba léků).

Závěr: Personalizace a adaptivní nastavení pomocí AI umožňuje aplikacím pro krizové řízení, bezpečnostní aplikace nebo zdravotní monitoring poskytnout uživatelům přizpůsobenou a efektivní pomoc. AI, která se učí chování uživatele a přizpůsobuje doporučení na základě individuálních preferencí a zdravotních potřeb, zajišťuje, že každý uživatel dostane přesně to, co potřebuje, a to včas. Tento přístup nejen zvyšuje připravenost na krizové situace, ale také poskytuje uživatelům větší kontrolu nad svou bezpečností a zdravím.

6.3 SWOT analýza aplikace True Life guardian

Aplikace True Life Guardian představuje inovativní nástroj pro krizové řízení a ochranu obyvatelstva, který využívá pokročilé technologie a AI k optimalizaci nouzové reakce. Tento systém kombinuje silné stránky existujících aplikací jako Záchranka, PulsePoint Respond, EchoSOS, GoodSAM a Life360, přičemž rozšiřuje jejich funkcionalitu o prvky prediktivní analýzy, automatické detekce krizových situací a efektivní koordinace záchranných složek.

Tabulka 1: Identifikované faktory SWOT analýzy aplikace True Life Guardian, její silné a slabé stránky

SILNÉ STRÁNKY (STRENGTHS)	SLABÉ STRÁNKY (WEAKNESSES)
Pokročilé AI algoritmy – využití strojového učení k analýze krizových situací v reálném čase.	Možné falešné poplachy – AI nemusí vždy správně vyhodnotit situaci, což může vést k nežádoucím varováním.
Off-line režim – aplikace funguje i bez připojení k internetu, což je klíčové v případě blackoutu.	Závislost na dostupnosti senzorických dat – v případě selhání senzorů nemusí aplikace fungovat správně.
Rychlá a přesná detekce nebezpečí – schopnost identifikovat požáry, povodně nebo jiné hrozby na základě senzorických dat.	Omezené pokrytí v odlehlých oblastech – některé oblasti nemusí mít dostatečná data pro efektivní fungování AI modelů.
Upozornění na míru – aplikace personalizuje varování na základě polohy uživatele a jeho nastavení.	Regulační omezení – právní překážky týkající se sběru dat a jejich ochrany.
Intuitivní uživatelské rozhraní – snadná použitelnost i pro technicky méně zdatné uživatele.	Vysoké nároky na hardware – některé starší mobilní zařízení nemusí zvládnout náročné AI výpočty.
Možnost integrace s krizovými složkami – přímé propojení s hasiči, policií a záchrannými složkami.	Závislost na internetovém připojení – v případě výpadku mobilních dat nebo Wi-Fi může být omezená funkčnost aplikace.

(zdroj: vlastní)

Z výše uvedené tabulky vyplývá, že navržená aplikace pro krizové situace disponuje řadou výrazných silných stránek, které přispívají k její praktičnosti a efektivitě v oblasti ochrany obyvatelstva. Mezi klíčové přínosy patří zejména pokročilé algoritmy AI, schopnost fungovat i v off-line režimu, stejně jako rychlá detekce hrozeb na základě senzorických dat. Dále je výhodou personalizace upozornění pro jednotlivé uživatele, přehledné uživatelské rozhraní a možnost propojení s integrovaným záchranným systémem (IZS). Na druhou stranu byly identifikovány i slabé stránky, které mohou mít vliv na spolehlivost nebo nasazení systému v praxi.

Z této analýzy vyplývá, že ačkoliv aplikace nabízí inovativní řešení s vysokým potenciálem využití v krizovém řízení, je nezbytné věnovat pozornost zejména technickým omezením, legislativním aspektům a zajištění kvality vstupních dat.

Tabulka 2: Identifikované faktory SWOT analýzy aplikace True Life Guardian, její příležitosti a hrozby

PŘÍLEŽITOSTI (OPPORTUNITIES)	HROZBY (THREATS)
Integrace s chytrými domácnostmi – propojení s IoT zařízeními (chytré senzory, kamery, alarmy).	Kybernetické útoky – aplikace pracuje s citlivými daty, což ji činí cílem hackerů.
Rozšíření na další krizové situace – např. predikce dopravních nehod, teroristických útoků nebo šíření nemocí.	Konkurenční tlak – existují jiné AI-based krizové aplikace, které mohou nabídnout lepší služby.
Spolupráce s vládními agenturami – získání státní podpory a oficiální certifikace pro krizové řízení.	Odmítání veřejností – obavy z narušení soukromí mohou vést k nízké adopci aplikace.
Mezinárodní expanze – přizpůsobení aplikace pro různé geografické oblasti a specifické hrozby.	Změny legislativy – přísnější regulace AI a ochrany dat mohou omezit funkčnost aplikace.
Pokroky v AI – využití nejnovějších metod hlubokého učení pro přesnější detekci rizik.	Závislost na infrastruktuře – výpadky mobilních sítí nebo GPS mohou ovlivnit přesnost varování.
Větší povědomí o krizovém řízení – rostoucí zájem veřejnosti o osobní	Možná neochota krizových složek k integraci – státní záchranné složky nemusí

bezpečnost může zvýšit poptávku po aplikaci.	být ochotné se zapojit do ekosystému aplikace.
--	--

(zdroj: vlastní)

Analýza příležitostí ukazuje, že aplikace pro mimořádné události má značný potenciál pro další rozvoj a rozšíření funkcí. Mezi největší příležitosti patří propojení s chytrými domácnostmi pomocí zařízení internetu věcí, rozšíření detekčních schopností na nové typy hrozeb (např. terorismus nebo šíření infekčních chorob) a možnost spolupráce se státními institucemi, což by mohlo aplikaci dodat důvěryhodnost a otevřít cestu k oficiálnímu využití. Existuje také potenciál pro mezinárodní rozšíření a využití nových technologií umělé inteligence, které mohou zvýšit přesnost a spolehlivost předpovědí. V neposlední řadě hraje důležitou roli rostoucí povědomí veřejnosti o krizovém řízení, které může zvýšit poptávku po těchto digitálních nástrojích.

Na druhé straně existují reálné hrozby, které mohou negativně ovlivnit úspěch a praktické využití. Jedním z hlavních rizik jsou kybernetické útoky, neboť aplikace pracuje s citlivými údaji. Dále je třeba vzít v úvahu konkurenční prostředí, pokud jsou na trhu již jiné aplikace AI zaměřené na krizové situace. Kromě toho může být aplikace odmítnuta veřejností kvůli obavám ze sledování nebo zneužití osobních údajů. Hrozbou jsou také legislativní změny, zejména pokud budou přijata přísnější pravidla pro používání AI a ochranu údajů. Závislost na infrastruktuře (mobilní síť, GPS) a případná neochota záchranných složek spolupracovat pak může omezit její skutečné využití v terénu.

Určení vah jednotlivých faktorů podle metody vícekritériálního rozhodování (MCDM):

Ke každému faktoru ve SWOT analýze se přiřadí váha (0–1), která vyjadřuje jeho význam (důležitost) v daném kontextu. Součet vah v každé kategorii (S, W, O, T), který by z ní měl vycházet, by se měl rovnat 1.

- Váha (W) vyjadřuje důležitost dané položky pro úspěch projektu (1 = zanedbatelné, 5 = klíčové).
- Hodnocení (H) vyjadřuje míru naplnění či závažnosti (1 = málo příznivé/závažné, 5 = velmi příznivé/závažné).
- Vážené skóre/Výsledek = $W \times H$.

Váhy a hodnocení byly nastaveny tak, aby odrážely strategickou důležitost každého prvku z hlediska úspěšnosti aplikace a zároveň reálnou možnost jejího ovlivnění skrze dostupné příležitosti. Největší důraz je kladen na technické a datové slabiny, které lze efektivně řešit pomocí technologických inovací AI.

Tabulka 3: SWOT analýza – Silné stránky aplikace True Life Guardian

Faktor	Váha	Hodnocení	Výsledek
Pokročilé AI algoritmy	0,25	4	1,00
Off-line režim	0,20	3	0,60
Rychlá detekce nebezpečí	0,20	4	0,80
Upozornění na míru	0,15	3	0,45
Intuitivní uživatelské rozhraní	0,10	3	0,30
Možnost integrace s krizovými složkami	0,10	3	0,30
Celkem	1	-	3,45

(zdroj: vlastní)

Následující přehled hodnotí klíčové silné stránky aplikace využívající AI pro krizové řízení a ochranu obyvatelstva. Tyto faktory pozitivně ovlivňují efektivitu, využitelnost a přínos navrhovaného systému v praxi:

Pokročilé AI algoritmy

- **Váha:** 0,25 - AI je jádrem celé aplikace, umožňuje automatické vyhodnocení hrozeb, učení z historických dat a rychlou adaptaci na měnící se krizové situace.
- **Hodnocení:** 4 - Algoritmy jsou velmi pokročilé, ale stále existuje prostor pro zlepšení, například v oblasti predikce v méně datově pokrytých oblastech. I tak ale představují klíčovou konkurenční výhodu a zásadní technologický pilíř.

Off-line režim

- **Váha:** 0,20 - Zajištění provozu bez internetového připojení je klíčové v krizových situacích (např. při blackoutu nebo výpadku sítě).

- Hodnocení: 3 - Off-line funkce jsou implementovány, ale ne všechny komponenty systému jsou v tomto režimu plně funkční. To snižuje jejich potenciál a otevírá prostor pro další vývoj.

Rychlá detekce nebezpečí

- Váha: 0,20 - Čas hraje v krizovém řízení zásadní roli – včasná detekce může znamenat rozdíl mezi zvládnutou situací a katastrofou.
- Hodnocení: 4 - Systém již disponuje schopností detekovat ohrožení ve velmi krátkém čase, ale přesnost v kombinovaných scénářích (např. kombinace více typů ohrožení) ještě není ideální.

Upozornění na míru

- Váha: 0,15 - Personalizace notifikací je důležitá pro efektivní komunikaci s uživateli. Pomáhá zabránit zahlcení informacemi a zvyšuje šanci, že si uživatelé včas všimnou relevantních varování.
- Hodnocení: 3 - Aplikace již nabízí určitý stupeň personalizace, ale vázne na přesnosti lokalizačních dat nebo dostupnosti uživatelských preferencí.

Intuitivní uživatelské rozhraní

- Váha: 0,10 - Přístupnost a jednoduchost použití jsou důležité pro masové využití aplikace, zejména u starší populace nebo v panických situacích.
- Hodnocení: 3 - Rozhraní je srozumitelné, ale stále existují příležitosti ke zjednodušení některých funkcí a vizuální optimalizaci pro různé typy zařízení.

Možnost integrace s krizovými složkami

- Váha: 0,10 - Propojení s IZS je důležité pro efektivní reakci a zvýšení důvěryhodnosti systému.
- Hodnocení: 3 - Systém je technicky připraven na integraci, ale chybí zatím institucionální napojení v praxi. To představuje příležitost k dalšímu posílení.

Závěrečné hodnocení: 3,45 / 5

Celkové skóre ukazuje, že aplikace má již nyní solidní technické základy a funkční jádro. Zároveň je ale patrné, že mnoho silných stránek je zatím pouze částečně rozvinutých, což vytváří ideální podmínky pro uplatnění WO strategie: tedy využití externích příležitostí

(např. technologických pokroků, rozšiřujícího se povědomí o krizovém řízení nebo dostupných financí z grantových programů) k tomu, aby se tyto silné stránky staly plně funkčními pilíři systému.

Tabulka 4: SWOT analýza – Slabé stránky aplikace True Life Guardian

Faktor	Váha	Hodnocení	Výsledek
Možné falešné poplachy	0,20	4	0,80
Závislost na dostupnosti senzorických dat	0,25	5	1,25
Omezené pokrytí v odlehlých oblastech	0,20	5	1,00
Regulační omezení	0,15	3	0,45
Vysoké nároky na hardware	0,10	3	0,30
Závislost na internetovém připojení	0,10	4	0,40
Celkem	1	-	4,20

(zdroj: vlastní)

Tato část identifikuje vnitřní nedostatky a omezení systému, které mohou negativně ovlivnit jeho vývoj, implementaci nebo dlouhodobé využití. Hodnocení zohledňuje technologické i organizační limity:

Možné falešné poplachy

- **Váha:** 0,20 - Falešná varování oslabují důvěru veřejnosti, což může vést k ignoraci i skutečně nebezpečných událostí.
- **Hodnocení:** 4 - Významná slabina, zejména pokud algoritmy nejsou dostatečně přesné nebo pokud dochází ke zkreslení dat. Riziko je možné snížit, ale vyžaduje to systematické zlepšování detekčních modelů.

Závislost na dostupnosti senzorických dat

- **Váha:** 0,25 - Klíčová slabina v technickém fungování aplikace. Bez dat z fyzických senzorů (např. čidla teploty, kouře, vibrací) není AI schopna vyhodnocovat situaci ani upozornit na krizový stav.

- Hodnocení: 5 - Kritická závažnost. V oblastech bez nasazené infrastruktury je aplikace zcela nefunkční. Tato slabina má největší dopad na celkovou spolehlivost systému.

Omezené pokrytí v odlehlých oblastech

- Váha: 0,20 - Problém zejména ve venkovských nebo horských oblastech, kde může chybět jak připojení, tak senzory nebo krizová infrastruktura.
- Hodnocení: 5 - Závažný limit, který znemožňuje použití systému tam, kde by mohl být paradoxně nejvíce potřebný – například při povodních, lesních požárech nebo lavínách.

Regulační omezení

- Váha: 0,15 - Právní rámce a normy (např. ochrana osobních údajů, bezpečnostní certifikace) mohou zpomalovat vývoj i nasazení systému.
- Hodnocení: 3 - Střední závažnost. Přestože se tyto překážky netýkají přímé funkčnosti, mohou zásadně ovlivnit možnosti aplikace být oficiálně využívána krizovými složkami nebo obcemi.

Vysoké nároky na hardware

- Váha: 0,10 - I když většina moderních zařízení zvládne aplikaci provozovat, starší telefony nebo levnější zařízení mohou mít problém s výpočetní náročností nebo kapacitou baterie.
- Hodnocení: 3 - Střední závažnost – omezuje některé uživatele, ale většinové rozšíření aplikace tím není zásadně ohroženo.

Závislost na internetovém připojení

- Váha: 0,10 - Stabilní konektivita je důležitá zejména pro přenos dat mezi senzory, serverem a koncovým uživatelem.
- Hodnocení: 4 - Poměrně závažný faktor, protože v krizových situacích může dojít k výpadku internetu, což ohrozí přenos informací a aktualizace systému.

Závěrečné hodnocení: 4,20 / 5

Celkové skóre znamená, že slabiny systému nejsou marginální, ale naopak představují zásadní výzvy pro jeho spolehlivost, dostupnost a důvěryhodnost. Vysoká váha i hodnocení

některých technických faktorů (zejména závislost na datech a omezené pokrytí) naznačují, že úspěšnost aplikace bude silně záviset na přesném cílení příležitostí.

To vytváří prostor pro WO strategii, která by měla aktivně hledat technologické i institucionální způsoby, jak tyto slabiny kompenzovat – například formou grantů na senzorovou infrastrukturu, vývoje off-line režimu nebo spolupráce s mobilními operátory.

Tabulka 5: SWOT analýza – Příležitosti aplikace True Life Guardian

Faktor	Váha	Hodnocení	Výsledek
Integrace s chytrými domácnostmi	0,20	5	1,00
Rozšíření na další krizové situace	0,20	4	0,80
Spolupráce s vládními agenturami	0,20	5	1,00
Mezinárodní expanze	0,15	4	0,60
Pokroky v AI	0,15	4	0,60
Větší povědomí o krizovém řízení	0,10	3	0,30
Celkem	1	-	4,30

(zdroj: vlastní)

Níže uvedené příležitosti představují externí faktory, které mohou přispět k rozvoji a úspěšnému prosazení AI systému v oblasti krizového řízení. Zahrnují zejména technologické, společenské a institucionální trendy:

Integrace s chytrými domácnostmi a IoT

- **Váha: 0,20** - Tato příležitost byla hodnocena jako velmi významná. IoT zařízení (např. detektory kouře, senzory pohybu, kamery) se mohou stát důležitým datovým vstupem pro AI systém aplikace. Díky propojení s domácí infrastrukturou se zvyšuje schopnost včasné detekovat mimořádné události.
- **Hodnocení: 5** - Možnost integrace do chytrých domácností výrazně zvyšuje uživatelskou hodnotu aplikace. Jde o trend, který je technologicky reálný a již se v některých oblastech uplatňuje.

Rozšíření na další krizové situace

- Váha: 0,20 - Tato příležitost má vysokou strategickou hodnotu, protože rozšířením na další typy krizí (např. průmyslové havárie, pandemie) se výrazně zvýší relevance a využitelnost aplikace.
- Hodnocení: 4 - Realizace vyžaduje komplexní modely a více trénovacích dat, ale technologicky je tento cíl v budoucnosti dosažitelným a velice žádoucím u krizových situací.

Spolupráce se státními institucemi

- Váha: 0,20 - Spolupráce s veřejným sektorem je klíčová pro důvěryhodnost, masové nasazení a dlouhodobé financování. Navázání partnerství s IZS, státní správou nebo obcemi může zásadně ovlivnit implementaci.
- Hodnocení: 5 - Velmi silný faktor pro úspěch projektu. Spolupráce může zároveň otevřít nové datové zdroje a podpořit marketing a důvěru veřejnosti.

Mezinárodní expanze

- Váha: 0,15 - Příležitost pro růst mimo domácí trh. Aplikace může být přizpůsobena jazykově i kulturně pro další státy.
- Hodnocení: 4 - Přesto že existují právní a jazykové bariéry, potenciál expanze je značný. Vhodné pro pozdější fázi projektu.

Pokroky v AI

- Váha: 0,15 - Vývoj v oblasti umělé inteligence, jako je edge AI nebo federované učení, může zefektivnit provoz, snížit nároky na připojení a zvýšit přesnost detekcí.
- Hodnocení: 4 - Zlepšení AI technologií je kontinuální a otevírá nové možnosti, ale závisí na dostupnosti výzkumu a implementačních schopnostech vývojářů.

Větší povědomí o krizovém řízení

- Váha: 0,10 - S rostoucí četností krizových událostí roste i zájem veřejnosti o řešení, která zvyšují bezpečnost.
- Hodnocení: 3 - Společenský trend, který sice přímo neovlivňuje technologii, ale hraje důležitou roli v přijetí a šíření aplikace mezi uživateli.

Závěrečné hodnocení: 4,30 / 5

Celkové skóre ukazuje, že aplikace má velmi dobrý potenciál pro další rozvoj, zejména pokud bude schopna využít technologické inovace, vytvořit strategická partnerství a reagovat na rostoucí zájem veřejnosti o krizové řízení. Tento výsledek podporuje zaměření strategie na rozvoj, inovaci a budování důvěry skrze spolupráci se státními institucemi.

Tabulka 6: SWOT analýza – Hrozby aplikace True Life Guardian

Faktor	Váha	Hodnocení	Výsledek
Kybernetické útoky	0,25	4	1,00
Konkurenční tlak	0,20	3	0,60
Odmítání veřejnosti	0,15	3	0,45
Změny legislativy	0,15	3	0,45
Závislost na infrastruktuře	0,15	3	0,45
Možná neochota krizových složek k integraci	0,10	2	0,20
Celkem	1	-	3.15

(zdroj: vlastní)

V této části jsou popsány vnější hrozby, které mohou ohrozit efektivní nasazení a dlouhodobé fungování systému. Hodnocení se zaměřuje na bezpečnost, legislativní prostředí, důvěru veřejnosti i technologickou závislost.

Kybernetické útoky

- **Váha:** 0,25 - Toto riziko je vysoce relevantní, protože aplikace pracuje s citlivými daty, a její zabezpečení je klíčové pro ochranu obyvatelstva. Kybernetické útoky mohou ohrozit její funkčnost i důvěru veřejnosti.
- **Hodnocení:** 4 - Riziko kybernetických útoků je vysoké, ale existují obranné mechanismy (šifrování, redundance, bezpečnostní standardy), které dokážou tento problém částečně zmírnit.

Konkurenční tlak

- Váha: 0,20 - Růst konkurence na poli AI nástrojů zaměřených na bezpečnost může ztížit komerční uplatnění a spolupráci se státními institucemi.
- Hodnocení: 3 - Konkurence může přinést inovace, ale pro méně etablované projekty to stále představuje výzvu.

Odmítání veřejnosti

- Váha: 0,15 - Publicita a přijetí technologie jsou zásadní. Lidé mohou mít obavy z toho, že technologie zasahují do jejich soukromí (monitoring, detekce, varování).
- Hodnocení: 3 - Riziko je střední. Důvěra veřejnosti závisí na transparentnosti aplikace, etickém přístupu a komunikaci.

Změny legislativy

- Váha: 0,15 - Legislativa v oblasti ochrany údajů a regulace AI se vyvíjí rychle, což může ovlivnit provoz aplikace. Právní změny mohou omezit některé její funkce.
- Hodnocení: 3 - Riziko právních změn je střední. Nepředvídatelné změny mohou ovlivnit distribuci nebo používání aplikace.

Závislost na infrastruktuře

- Váha: 0,15 - Aplikace je závislá na technologické infrastruktuře, což představuje problém v krizových situacích, jako je blackout nebo výpadek sítě.
- Hodnocení: 3 - Riziko je střední až vysoké, zejména v krizových scénářích, kdy infrastruktura může selhat.

Možná neochota krizových složek k integraci

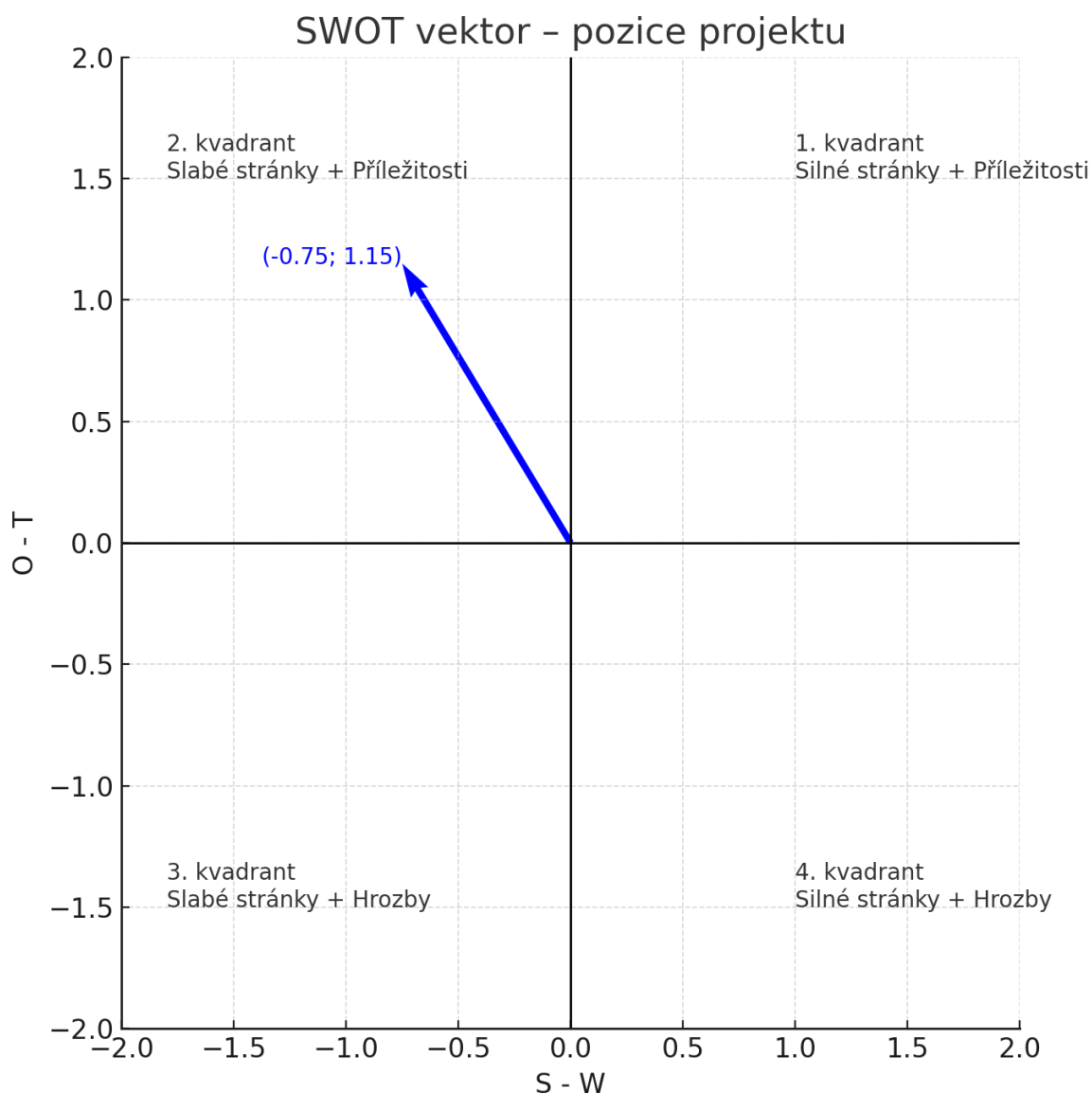
- Váha: 0,10 - Některé složky IZS mohou být skeptické vůči novým technologiím nebo mají vlastní uzavřené systémy.
- Hodnocení: 2 - Riziko je relativně vyšší, protože může být obtížné přesvědčit složky o výhodách technologie.

Celkové hodnocení: 3,15 / 5

Výsledek naznačuje, že hrozby jsou reálné, ale zvládnutelné. Největší rizika se týkají kybernetických útoků, konkurence, veřejné nedůvěry a právních změn.

Interpretace výsledku SWOT vektorové analýzy

Na základě výsledků čtyř SWOT tabulek (Silné stránky - Strengths, Slabé stránky - Weaknesses, Příležitosti - Opportunities, Hrozby - Threats) byl vypočten tzv. SWOT vektor, který určuje celkovou strategickou pozici analyzované AI aplikace v kontextu krizového řízení.



Obrázek 6: Výpočet SWOT vektoru (Zdroj Vlastní)

Z obrázku vychází výpočet SWOT vektoru, ke kterému byly použité tyto vzorce:

Souřadnice osy X: rozdíl mezi silnými a slabými stránkami

$$X = S - W = 3,45 - 4,20 = -0,75$$

Souřadnice osy Y: rozdíl mezi příležitostmi a hrozbami

$$Y = O - T = 4,30 - 3,15 = 1,15$$

Tímto způsobem je pozice projektu reprezentována ve dvourozměrném prostoru pomocí bodu s hodnotou $(-0,75; 1,15)$.

Co tyto hodnoty znamenají:

X souřadnice (S - W) vyjadřuje, zda převažují silné (kladné hodnoty) nebo slabé stránky (záporné hodnoty).

Y souřadnice (O - T) ukazuje, zda projekt nabízí více příležitostí (kladné hodnoty) nebo čelí výraznějším hrozbám (záporné hodnoty).

Výsledek: $(-0,75; 1,15)$ leží ve druhém kvadrantu SWOT matice, který reprezentuje kombinaci:

Slabé stránky (Weaknesses) – tedy projekt má jistá omezení, která je nutno řešit. Příležitosti (Opportunities) – ale zároveň existuje značný potenciál pro další rozvoj a využití.

Z výpočtů vyplývá, že aplikace disponuje silnými technologickými vlastnostmi, a zároveň čelí několika slabinám, které by však bylo možné účinně eliminovat využitím aktuálních příležitostí.

Na základě provedené SWOT vektorové analýzy, jejíž výsledkem je bod $(-0,75; 1,15)$, byla zvolena WO strategie (slabé stránky - příležitosti). Tato pozice odpovídá druhému kvadrantu SWOT matice, který signalizuje, že navzdory převažujícím slabým stránkám existuje významný potenciál pro rozvoj prostřednictvím aktuálních příležitostí. Volba WO strategie je tedy logickým krokem, jak oslabit interní nedostatky využitím externího prostředí.

Výběr WO strategie tedy není pouze teoretickým rámcem, ale reflektuje reálnou možnost překonání slabin pomocí konkrétních a dosažitelných kroků. Aplikace True Life Guardian by tak měla potenciál růstu a posílení své pozice na trhu zejména díky technologickému vývoji, spolupráci s institucemi a schopnosti přizpůsobit se potřebám uživatelů i státu.

Na základě provedené analýzy byla zvolena WO strategie z následujících důvodů:

Klíčové slabé stránky identifikované v analýze:

- Závislost na senzorických datech (např. jednorozměrné vstupy z IoT zařízení).
- Regulační omezení v oblasti sběru dat a ochrany soukromí.
- Technické nároky na hardware a konektivitu.

- Riziko falešných poplachů a nízké robustnosti v krizových scénářích.

Identifikované příležitosti, které mohou slabiny kompenzovat:

- Integrace s chytrými domácnostmi, která umožní diverzifikaci vstupních dat.
- Spolupráce s veřejnými institucemi a krizovými orgány, čímž lze podpořit legislativní rámec a usnadnit adopci.
- Pokrok v AI technologiích, včetně robustnějších modelů a nižších nároků na výpočetní výkon.
- Zvyšující se povědomí veřejnosti o krizovém řízení, což může podpořit důvěru a širší využití aplikace.

Cíl strategie:

Zvýšit spolehlivost, dostupnost a efektivitu AI aplikace při krizovém řízení prostřednictvím eliminace slabin s využitím technologických a společenských příležitostí.

Opatření k odstranění slabých stránek

Snížení falešných poplachů:

- Vylepšení modelů strojového učení přesnějšími datovými sadami.
- Kombinace AI s ručním potvrzením uživatelem.
- Konzultace s krizovými experty pro optimalizaci modelů predikce.

Řešení závislosti na senzorických datech:

- Integrace více datových zdrojů – např. družicových snímků, senzory z chytrých domácností.
- Vývoj off-line režimu, který zachová základní funkcionalitu i bez připojení.

Zajištění dostupnosti v odlehlých oblastech:

- Nasazení alternativních sítí (např. satelitní internet, P2P, mesh networking).
- Vývoj odlehčené verze aplikace pro méně výkonná zařízení a slabé připojení.

Překonání právních a regulačních omezení:

- Transparentní sběr a zpracování dat v souladu s GDPR.
- Lokální zpracování dat přímo v zařízení bez nutnosti cloudu.

- Spolupráce s legislativními orgány a možnost anonymního použití.

Snížení technických nároků:

- Optimalizace AI modelů pro běh na starších zařízeních.
- Delegování náročných operací do cloudu.
- Vývoj modulární aplikace umožňující přizpůsobení podle hardwaru.

Očekávané přínosy této strategie:

- Zvýšení přesnosti predikcí a snížení počtu falešných poplachů.
- Možnost využití aplikace i v odlehlých oblastech bez stabilního připojení.
- Zvýšení důvěry veřejnosti a legislativních institucí díky transparentním mechanismům.
- Širší uživatelská dostupnost aplikace díky optimalizaci pro méně výkonný hardware.
- Větší odolnost vůči krizovým situacím, kde není dostupná plná síťová infrastruktura.

Zavedením této strategie může aplikace True Life Guardian dosáhnout většího přijetí a spolehlivosti v náročných prostředích. Odstranění klíčových nedostatků zajistí, že aplikace bude účinnější a použitelnější pro širokou škálu uživatelů, včetně záchranářů a běžných občanů. Tím se dosáhne maximálního využití potenciálu AI při ochraně veřejnosti a přispěje se ke zvýšení bezpečnosti v mimořádných situacích.

Tento systém představuje revoluční řešení pro moderní krizové řízení, které nejen zvyšuje bezpečnost osob, ale také podporuje efektivnější fungování záchranných služeb. True Life Guardian je krokem vpřed v oblasti ochrany.

Subjekty vhodné pro vývoj a rozvoj aplikace:

Státní instituce - Klíčovou roli by mohly sehrát instituce státní správy, zejména Ministerstvo vnitra a Ministerstvo zdravotnictví ČR, které by mohly být garanty celého projektu. Jejich úkolem by bylo vytvořit právní, bezpečnostní a etický rámec, který by zajistil odpovědné využití AI při řešení krizových situací a ochraně obyvatelstva.

Složky IZS - Praktickými uživateli aplikace by byli především příslušníci Hasičského záchranného sboru ČR, Zdravotnické záchranné služby ČR a Policie ČR. Tyto subjekty by

mohly poskytnout praktické zkušenosti při vývoji funkcionalit, které by odrážely reálné potřeby v terénu a zajistily přímou integraci s operačními systémy krizového řízení.

Technologičtí partneři a vývojáři - Na vývoji samotné technologie se mohou podílet softwarové společnosti a technologické start-upy se zaměřením na AI, mobilní aplikace a kybernetickou bezpečnost. Mezi relevantní hráče patří společnosti jako Unicorn, Avast (nyní Gen Digital) nebo inovativní zdravotnické technologie a startupy v oblasti bezpečnostního softwaru.

Evropské fondy a grantové programy - Financování vývoje a nasazení aplikace by mohly podpořit evropské fondy nebo grantové programy Evropské unie zaměřené na digitalizaci, inovace a posílení odolnosti veřejného sektoru, zejména v oblasti bezpečnosti a zdravotnictví.

Kdo by mohl aplikaci převzít do užívání:

Veřejnost - Aplikace by měla být k dispozici široké veřejnosti zdarma, ideálně jako součást základního softwaru mobilních zařízení nebo prostřednictvím celostátní informační kampaně. Cílem je zvýšit její využívání a účinnost v případě mimořádných událostí.

Složky IZS - Aplikace by mohla být propojena se stávajícími dispečerskými systémy složek IZS a být kompatibilní s již používanými nástroji, jako je platforma GINA nebo aplikace Záchranka. Takové propojení by umožnilo rychlejší reakci a lepší koordinaci mezi jednotlivými složkami záchranného systému.

Místní orgány krizového řízení - By mohly aplikaci využívat k varování obyvatelstva, řízení evakuace a koordinaci pomoci, zejména na úrovni obcí s rozšířenou působností. Integrace se systémem krizového řízení by zvýšila efektivitu při řešení mimořádných událostí.

Zdravotnická zařízení a poskytovatelé domácí péče - V oblasti zdravotnictví by bylo možné aplikaci rozšířit o funkce monitorovacího systému pro osoby s chronickými onemocněními nebo jinými rizikovými faktory. Propojení se systémem domácí péče by umožnilo včasnou reakci na ohrožení zdraví a života při mimořádných událostech.

Možnosti implementace aplikace True Life Guardian do současných systémů:

Integrace jako rozšíření stávající záchranné aplikace Efektivním způsobem implementace by bylo rozšíření funkcí stávající a hojně využívané mobilní aplikace Záchranka. Tato aplikace má v České republice vysokou důvěru veřejnosti, je technicky

stabilní a provozně dobře zavedená, takže je ideálním kandidátem pro integraci nových funkcí založených na AI.

Navrhovaná vylepšení by mohla zahrnovat:

AI predikce krizových situací na základě analýzy dat z více zdrojů (meteorologických, seismologických, sociálních atd.), sdílení polohy v reálném čase mezi uživateli, např. v případě evakuace nebo pomoci v terénu, varovné zprávy na základě dat ze senzorů, např. ze systémů detekujících výpadky elektřiny, znečištění ovzduší nebo zvýšenou pohybovou aktivitu v rizikových oblastech.

Taková implementace by minimalizovala potřebu budování nové infrastruktury, snížila náklady na vývoj a zároveň využila stávající uživatelskou základnu a funkční propojení s IZS.

Vývoj samostatné aplikace s napojením na složky IZS:

Alternativním přístupem by bylo vytvoření zcela nové samostatné aplikace True Life Guardian, která by byla od počátku navržena s důrazem na modularitu, škálovatelnost a interoperabilitu se stávajícími systémy.

Klíčové otázky implementace v tomto případě zahrnují:

Zajištění kompatibility s technickými prostředky IZS, jako jsou krizové mapování, operační a informační systémy KOPIS nebo platforma pro řízení zásahů v terénu GINA.

Integrace datových toků z více zdrojů, zejména meteorologických dat, dopravních informací, dat ze senzorů zařízení internetu věcí nebo dat z městských kamerových systémů.

Vývoj otevřeného rozhraní API umožňujícího propojení s dalšími existujícími aplikacemi, jako jsou Záchranka, PulsePoint Respond, EchoSOS, GoodSAM nebo Life360 aby se zabránilo duplikaci systémů a podpořila se interoperabilita na národní i mezinárodní úrovni.

Tento přístup by umožnil větší flexibilitu a přizpůsobení funkcí specifickým potřebám jednotlivých regionů nebo záchranných služeb.

Navržená aplikace True Life Guardian představuje moderní nástroj, který reaguje na potřebu efektivní ochrany obyvatelstva v krizových situacích. Kombinuje pokročilé funkce, jako je detekce nehod, predikce rizik pomocí AI, lokalizace v reálném čase nebo integrace

se složkami IZS. Inspirací se staly nejlépe fungující světové a domácí aplikace, jejichž silné stránky byly analyzovány a promyšleně integrovány do jednotného systému.

Realizace aplikace True Life Guardian bude vyžadovat spolupráci mezi technologickými firmami, státní správou, bezpečnostními složkami a výzkumnými institucemi. Možnou cestou je buď rozšíření stávající platformy (např. aplikace Záchranka), nebo vytvoření nové aplikace, která bude otevřená dalším integračním řešením. Důraz je třeba klást nejen na funkčnost a spolehlivost, ale i na ochranu osobních údajů, jednoduché uživatelské rozhraní a dostupnost pro všechny skupiny obyvatelstva.

ZÁVĚR

Cílem této práce bylo analyzovat současný stav využití AI v oblasti ochrany obyvatelstva a na základě této analýzy navrhnout ideální mobilní aplikaci pro krizové řízení a první pomoc. Práce se zaměřila na vybrané aplikace, jako jsou Záchranka, PulsePoint Respond, EchoSOS, GoodSAM a Life360, a jejich silné a slabé stránky, přínosy a omezení v oblasti krizového řízení a veřejné bezpečnosti.

První část práce představila teoretické pozadí vývoje AI, včetně její historie, současných technologií a etických problémů spojených s jejím používáním. Druhá část práce se zaměřila na konkrétní aplikace AI v oblasti ochrany obyvatelstva a ukázala, jak AI přispívá ke zlepšení krizového řízení a veřejné bezpečnosti. Byly analyzovány prediktivní modely pro prevenci přírodních katastrof, systémy krizového řízení a technologie pro veřejný dohled a prevenci kriminality.

V praktické části byla provedena analýza stávajících mobilních aplikací první pomoci využívajících AI a navržen koncept aplikace „True Life Guardian App“. Tento návrh odráží současné trendy a potřeby v oblasti rychlé a účinné reakce na krizové situace a poskytuje doporučení pro zlepšení stávajících řešení.

Výsledky analýzy ukázaly, že ačkoli tyto aplikace mají v oblasti první pomoci a krizové komunikace nezastupitelné místo, stále je co zlepšovat, zejména v oblasti prediktivní analýzy a integrace s AI. Na základě těchto zjištění byl navržen koncept aplikace True Life Guardian, která by kombinovala klíčové funkce stávajících nástrojů a zároveň přidávala nové funkce, jako je predikce krizí a automatizované rozhodování na základě analýzy velkých dat.

Analýza SWOT ukázala silné stránky aplikace, zejména schopnost integrovat AI pro zefektivnění krizového řízení, ale také slabé stránky, jako je potřeba kvalitních dat a technologických inovací. Jako nejvhodnější strategie pro další rozvoj byla zvolena strategie WO (využití příležitostí k překonání slabých stránek) za pomoci vícekritériálního rozhodování s cílem maximalizovat účinnost a přesnost v krizových situacích.

Zavedení takového nástroje do praxe by vyžadovalo nejen technologické inovace, ale také širší spolupráci mezi vývojáři, záchrannými službami a vládními institucemi. True Life Guardian by mohl významně přispět k optimalizaci reakčních časů v krizových situacích, a tím snížit počet obětí a minimalizovat škody způsobené přírodními katastrofami, nehodami a jinými mimořádnými událostmi.

Závěrem lze konstatovat, že využití AI v oblasti ochrany obyvatelstva nabízí velký potenciál pro budoucí rozvoj a zefektivnění krizového řízení. Navrhovaná aplikace True Life Guardian je jen jedním z možných směrů, jimiž mohou moderní technologie přispět k lepší ochraně obyvatelstva. Další výzkum a vývoj v této oblasti bude mít zásadní význam pro praktickou implementaci těchto technologií a jejich širší přijetí.

SEZNAM POUŽITÉ LITERATURY

ABADI, Martin; CHU, Andy; GOODFELLOW, Ian; MCMAHAN, H. Brendan; MIRONOV, Ilya et al. Deep Learning with Differential Privacy. Online. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. New York, NY, USA: ACM, 2016, s. 308-318. ISBN 9781450341394. Dostupné z: <https://doi.org/10.1145/2976749.2978318>. [cit. 2025-03-05].

AKHTAR, Naveed; MIAN, Ajmal; KARDAN, Navid a SHAH, Mubarak. Advances in Adversarial Attacks and Defenses in Computer Vision: A Survey. Online. *IEEE Access*. 2021, roč. 9, s. 155161-155196. ISSN 2169-3536. Dostupné z: <https://doi.org/10.1109/ACCESS.2021.3127960>. [cit. 2025-03-05].

ALI, Waqar; TIAN, Wenhong; DIN, Salah Ud; IRADUKUNDA, Desire a KHAN, Abdullah Aman. Classical and modern face recognition approaches: a complete review. Online. *Multimedia Tools and Applications*. 2021, roč. 80, č. 3, s. 4825-4880. ISSN 1380-7501. Dostupné z: <https://doi.org/10.1007/s11042-020-09850-1>. [cit. 2025-02-02].

ALIABADI, Rooz. Medium: New Era of AI-Generated Content and Its Impact on Society. Online. In: © 2024. Dostupné z: <https://medium.com/readyai-org/new-era-of-ai-generated-content-and-its-impact-on-society-5785c1d9b981>. [cit. 2025-02-05].

AMERICAN CPR CARE ASSOCIATION. AI in First Aid Training: Transforming Emergency Preparedness. Online. © 2025. Dostupné z: <https://cprcare.com/blog/use-of-ai-in-first-aid-training/>. [cit. 2025-03-12].

BAROCAS, Solon; HARDT, Moritz a NARAYANAN, Arvind. *Fairness and Machine Learning: Limitations and Opportunities*. The MIT Press, [2023]. ISBN 978-0262048613.

BENDER, Emily M.; GEBRU, Timnit; MCMILLAN-MAJOR, Angelina a SHMITCHELL, Shmargaret. On the Dangers of Stochastic Parrots. Online. In: *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*. New York, NY, USA: ACM, 2021, s. 610-623. ISBN 9781450383097. Dostupné z: <https://doi.org/10.1145/3442188.3445922>. [cit. 2025-03-04].

Binns, Reuben. *Fairness in Machine Learning: Lessons from Political Philosophy* (December 8, 2017). Conference on Fairness, Accountability, and. Transparency, New York, Forthcoming, Proceedings of Machine Learning Research, Vol. 81, p. 1–11, Forthcoming, Online. Dostupné z: <https://ssrn.com/abstract=3086546>. [cit. 2025-01-26].

BIRRER, Alena a JUST, Natascha. What we know and don't know about deepfakes: An investigation into the state of the research and regulatory landscape. Online. *New Media & Society*. ISSN 1461-4448. Dostupné z: <https://doi.org/10.1177/14614448241253138>. [cit. 2025-02-05].

BROOKS, Steven C.; SIMMONS, Graydon; WORTHINGTON, Heather; BOBROW, Bentley J. a MORRISON, Laurie J. The PulsePoint Respond mobile device application to crowdsource basic life support for patients with out-of-hospital cardiac arrest: Challenges for optimal implementation. Online. *Resuscitation*. 2016, roč. 98, s. 20-26. ISSN 03009572. Dostupné z: <https://doi.org/10.1016/j.resuscitation.2015.09.392>. [cit. 2025-03-09].

BURRI, Mira (ed.). *Big Data and Global Trade Law*. Online. Cambridge University Press, 2021. ISBN 9781108919234. Dostupné z: <https://doi.org/10.1017/9781108919234>. [cit. 2025-02-05].

CARLINI, Nicholas a WAGNER, David. Towards Evaluating the Robustness of Neural Networks. Online. In: *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2017, s. 39-57. ISBN 978-1-5090-5533-3. Dostupné z: <https://doi.org/10.1109/SP.2017.49>. [cit. 2025-03-05].

COMES, Tina. AI for crisis decisions. Online. *Ethics and Information Technology*. 2024, roč. 26, č. 1. ISSN 1388-1957. Dostupné z: <https://doi.org/10.1007/s10676-024-09750-0>. [cit. 2025-01-27].

DEVLIN, Jacob; CHANG, Ming-Wei; LEE, Kenton a TOUTANOVA, Kristina. Online. In: *Proceedings of the 2019 Conference of the North*. Stroudsburg, PA, USA: Association for Computational Linguistics, 2019, s. 4171-4186. Dostupné z: <https://doi.org/10.18653/v1/N19-1423>. [cit. 2025-01-26].

ECHOSOS. *EchoSOS – the emergency app*. Online. © 2025. Dostupné z: <https://echosos.com/en/>. [cit. 2025-03-12].

EUROPEAN COMMISSION. *AI Act*. Online. © 2025. Dostupné z: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>. [cit. 2025-02-03].

FANG, Bingbing; YU, Jiacheng; CHEN, Zhonghao; OSMAN, Ahmed I.; FARGHALI, Mohamed et al. Artificial intelligence for waste management in smart cities: a review. Online. *Environmental Chemistry Letters*. 2023, roč. 21, č. 4, s. 1959-1989. ISSN 1610-3653. Dostupné z: <https://doi.org/10.1007/s10311-023-01604-3>. [cit. 2025-01-27].

FLORIDI, Luciano a TADDEO, Mariarosaria. What is data ethics? Online. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*. 2016, roč. 374, č. 2083. ISSN 1364503X. Dostupné z: <https://doi.org/10.1098/rsta.2016.0360>. [cit. 2025-01-27].

FLORIDI, Luciano. *The ethics of artificial intelligence: principles, challenges, and opportunities*. New York: Oxford University Press, [2023]. ISBN 978-0-19-888309-8.

GOODFELLOW, Ian; BENGIO, Yoshua a COURVILLE, Aaron. *Deep learning*. Adaptive computation and machine learning series. Cambridge, Massachusetts: The MIT Press, [2016]. ISBN 978-0-262-03561-3.

GOODSAM PLATFORM. *GoodSAM Instant.Help*. Online. © 2025. Dostupné z: <https://www.goodsamapp.org/>. [cit. 2025-03-12].

GORDON, Faith. Virginia Eubanks (2018) Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. New York: Picador, St Martin's Press. Online. *Law, Technology and Humans*. 2019, s. 162-164. ISSN 2652-4074. Dostupné z: <https://doi.org/10.5204/lthj.v1i0.1386>. [cit. 2025-02-05].

KAUR, Ramanpreet; GABRIJELČIČ, Dušan a KLOBUČAR, Tomaž. Artificial intelligence for cybersecurity: Literature review and future research directions. Online. *Information Fusion*. 2023, roč. 97. ISSN 15662535. Dostupné z: <https://doi.org/10.1016/j.inffus.2023.101804>. [cit. 2025-02-02].

KNIHOVÁ, Ladislava. *AI marketing playbook: jak ChatGPT a umělá inteligence mění svět marketingu*. Praha: Grada, 2024. ISBN 978-802-7152-261.

KOCHUPILLAI, Mrinalini; KAHL, Matthias; SCHMITT, Michael; TAUBENBOCK, Hannes a ZHU, Xiao Xiang. Earth Observation and Artificial Intelligence: Understanding emerging ethical issues and opportunities. Online. *IEEE Geoscience and Remote Sensing Magazine*. 2022, roč. 10, č. 4, s. 90-124. ISSN 2168-6831. Dostupné z: <https://doi.org/10.1109/MGRS.2022.3208357>. [cit. 2025-01-27].

LeCun, Y., Bengio, Y. and Hinton, G. (2015) *Deep Learning*. Nature, 521, 436-444. Online. *Liability for artificial intelligence and other emerging digital technologies*. Online. Directorate-General for Justice and Consumers (European Commission). ISBN 978-92-76-12959-2. Dostupné z: <https://doi.org/10.2838/573689>. [cit. 2025-02-03].

LIFE360. INC. *Life360*. Online. © 2025. Dostupné z: <https://intl.life360.com/>. [cit. 2025-03-12].

LIM, Tristan; GOTTIPATI, Swapna a CHEONG, Michelle L. F. Ethical Considerations for Artificial Intelligence in Educational Assessments. Online. In: KEENGWE, Jared (ed.). *Creative AI Tools and Ethical Implications in Teaching and Learning*. Advances in Educational Technologies and Instructional Design. IGI Global, 2023, s. 32-79. ISBN 9798369302057. Dostupné z: <https://doi.org/10.4018/979-8-3693-0205-7.ch003>. [cit. 2025-02-02].

LU, Yiwei; KAMATH, Gautam a YU, Yaoliang. Indiscriminate Data Poisoning Attacks on Neural Networks. Online. 2022. Dostupné z: <https://doi.org/10.48550/arXiv.2004.07213>. [cit. 2025-03-05].

MARCINKEVIČS, Ričards a VOGT, Julia E. Interpretable and explainable machine learning: A methods-centric overview with concrete examples. Online. *WIREs Data Mining and Knowledge Discovery*. 2023, roč. 13, č. 3. ISSN 1942-4787. Dostupné z: <https://doi.org/10.1002/widm.1493>. [cit. 2025-03-04].

MARCUS, Gary F. a DAVIS, Ernest. *Rebooting AI: building artificial intelligence we can trust*. New York: Vintage Books, a division of Penguin Random House, 2020. ISBN 978-0-525-56604-5.

MAŘÍK, Vladimír; TRČKA, Michal a ČERNÝ, David. *Proč se nebát umělé inteligence? AI pohledem nejen českých odborníků*. Brno: Jota, 2024. ISBN 978-80-7689-459-4.

MBIVA, Stanley Munamoto a CORREA, Fabio Mathias. Machine Learning to Enhance the Detection of Terrorist Financing and Suspicious Transactions in Migrant Remittances. Online. *Journal of Risk and Financial Management*. 2024, roč. 17, č. 5. ISSN 1911-8074. Dostupné z: <https://doi.org/10.3390/jrfm17050181>. [cit. 2025-02-02].

MEHRABI, Ninareh; MORSTATTER, Fred; SAXENA, Nripsuta; LERMAN, Kristina a GALSTYAN, Aram. A Survey on Bias and Fairness in Machine Learning. Online. *ACM Computing Surveys*. 2022, roč. 54, č. 6, s. 1-35. ISSN 0360-0300. Dostupné z: <https://doi.org/10.1145/3457607>. [cit. 2025-03-05].

N., Ilag a ATHAVE, Yogesh. Artificial Intelligence: Risk Assessment and Considerations for the Future. Online. *International Journal of Computer Applications*. 2019, roč. 181, č.

43, s. 47-49. ISSN 09758887. Dostupné z: <https://doi.org/10.5120/ijca2019918529>. [cit. 2025-01-27].

NEUMAN, W. Russell. *Evolutionary intelligence: How Technology Will Make us Smarter*. Cambridge, Massachusetts: The MIT Press, 2023. ISBN 978-0-262-04848-4.

O'NEIL, Cathy. *Weapons of math destruction: how big data increases inequality and threatens democracy*. New York: Crown, [2016]. ISBN 978-0-553-41881-1.

PAPAIIOANNOU, Savvas; KOLIOS, Panayiotis; PANAYIOTOU, Christos G. a POLYCARPOU, Marios M. Synergising Human-like Responses and Machine Intelligence for Planning in Disaster Response. Online. In: *2024 International Joint Conference on Neural Networks (IJCNN)*. IEEE, 2024, s. 1-8. ISBN 979-8-3503-5931-2. Dostupné z: <https://doi.org/10.1109/IJCNN60899.2024.10651466>. [cit. 2025-03-04].

PAPERNOT, Nicolas; MCDANIEL, Patrick; GOODFELLOW, Ian; JHA, Somesh; CELIK, Z. Berkay et al. Practical Black-Box Attacks against Machine Learning. Online. In: *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*. New York, NY, USA: ACM, 2017, s. 506-519. ISBN 9781450349444. Dostupné z: <https://doi.org/10.1145/3052973.3053009>. [cit. 2025-03-05].

Poorani, Lakshmi & Malik, Abdul & Rani, Jeya & Varsha, Madhu & Ramaraj, R. Ravi. (2024). Online. AI for Disaster Response: Enhancing Early Warning Systems and Recovery Efforts. *International Journal of Engineering Technology and Sciences*. XI. 74-83. Dostupné z: https://www.researchgate.net/publication/386478374_AI_for_Disaster_Response_Enhancing_Early_Warning_Systems_and_Recovery_Efforts.

PUGACHEV, Andrei A.; KHARCHENKO, Alina V. a SLEPTSOV, Nikolai A. Transforming the future: a review of artificial intelligence models. Online. *RUDN Journal of Studies in Literature and Journalism*. 2023, roč. 28, č. 2, s. 355-367. ISSN 2312-9247. Dostupné z: <https://doi.org/10.22363/2312-9220-2023-28-2-355-367>. [cit. 2025-03-04].

PULSEPOINT FOUNDATION. *PulsePoint*. Online. © 2025. Dostupné z: <https://www.pulsepoint.org/pulsepoint-respond>. [cit. 2025-03-12].

RAJI, Ibrahim. Predictive Policing: The Role of AI in Crime Prevention. Online. *International Journal of Computer Applications Technology and Research*. ISSN 23198656. Dostupné z: <https://doi.org/10.7753/IJCATR1310.1006>. [cit. 2025-02-02].

ROBBINS, Scott. Facial Recognition for Counter-Terrorism: Neither a Ban Nor a Free-for-All. Online. In: HENSCHKE, Adam; REED, Alastair; ROBBINS, Scott a MILLER, Seumas (ed.). *Counter-Terrorism, Ethics and Technology*. Advanced Sciences and Technologies for Security Applications. Cham: Springer International Publishing, 2021, s. 89-104. ISBN 978-3-030-90220-9. Dostupné z: https://doi.org/10.1007/978-3-030-90221-6_6. [cit. 2025-02-02].

RUSSELL, Stuart J. a NORVIG, Peter. *Artificial intelligence: a modern approach*. Fourth edition. Pearson series in artificial intelligence. Hoboken: Pearson, 2021. ISBN 978-0-13-461099-3.

RUSSELL, Stuart J. *Jako člověk: umělá inteligence a problém jejího ovládní*. Zip. Praha: Argo, 2021. ISBN 978-80-7363-810-8.

SAYED, Sayed A.; ABDEL-HAMID, Yasser a HEFNY, Hesham Ahmed. Artificial intelligence-based traffic flow prediction: a comprehensive review. Online. *Journal of Electrical Systems and Information Technology*. 2023, roč. 10, č. 1. ISSN 2314-7172. Dostupné z: <https://doi.org/10.1186/s43067-023-00081-6>. [cit. 2025-02-02].

SHARMA, Abhinav; JAIN, Arpit; ARYA, Ashwini Kumar a RAM, Mangey (ed.). *Artificial Intelligence for Signal Processing and Wireless Communication*. De Gruyter Series on the Applications of Mathematics in Engineering and Information Sciences. Berlin: De Gruyter, 2022. ISBN 978-3-11-073882-7.

SHU, Kai; SLIVA, Amy; WANG, Suhan; TANG, Jiliang a LIU, Huan. Fake News Detection on Social Media. Online. *ACM SIGKDD Explorations Newsletter*. 2017, roč. 19, č. 1, s. 22-36. ISSN 1931-0145. Dostupné z: <https://doi.org/10.1145/3137597.3137600>. [cit. 2025-02-05].

SCHNEIDER, Johannes; ABRAHAM, Rene; MESKE, Christian a VOM BROCKE, Jan. Artificial Intelligence Governance For Businesses. Online. *Information Systems Management*. 2023, roč. 40, č. 3, s. 229-249. ISSN 1058-0530. Dostupné z: <https://doi.org/10.1080/10580530.2022.2085825>. [cit. 2025-03-05].

Silver, D., Huang, A., Maddison, C. et al. *Mastering the game of Go with deep neural networks and tree search*. Nature 529, 484–489 (2016). Online. Dostupné z: <https://doi.org/10.1038/nature16961>. [cit. 2025-01-26].

SINGH, Anshuman a GUPTA, Brij B. Distributed Denial-of-Service (DDoS) Attacks and Defense Mechanisms in Various Web-Enabled Computing Platforms. Online. *International Journal on Semantic Web and Information Systems*. 2022, roč. 18, č. 1, s. 1-43. ISSN 1552-6283. Dostupné z: <https://doi.org/10.4018/IJSWIS.297143>. [cit. 2025-03-05].

STAHL, Bernd Carsten; BROOKS, Laurence; HATZAKIS, Tally; SANTIAGO, Nicole a WRIGHT, David. Exploring ethics and human rights in artificial intelligence – A Delphi study. Online. *Technological Forecasting and Social Change*. 2023, roč. 191. ISSN 00401625. Dostupné z: <https://doi.org/10.1016/j.techfore.2023.122502>. [cit. 2025-02-05].

SUN, Wenjuan; BOCCHINI, Paolo a DAVISON, Brian D. Applications of artificial intelligence for disaster management. Online. *Natural Hazards*. 2020, roč. 103, č. 3, s. 2631-2689. ISSN 0921030X. Dostupné z: <https://doi.org/10.1007/s11069-020-04124-3>. [cit. 2025-01-27].

SUTTON, Richard S. a BARTO, Andrew G. *Reinforcement learning: an introduction*. Second edition 2018. Adaptive computation and machine learning. Cambridge: A Bradford Book, 1998. ISBN 978-0-262-19398-6.

TOMASEV, Nenad; MAYNARD, Jonathan Leader a GABRIEL, Iason. Manifestations of xenophobia in AI systems. Online. *AI & SOCIETY*. ISSN 0951-5666. Dostupné z: <https://doi.org/10.1007/s00146-024-01893-4>. [cit. 2025-02-02].

TOPAL, Reyhan. The rise of digital repression: How technology is reshaping power, politics, and resistance. Online. *The Information Society*. 2022, roč. 38, č. 1, s. 77-78. ISSN 0197-2243. Dostupné z: <https://doi.org/10.1080/01972243.2022.2014222>. [cit. 2025-02-05].

UDDIN, A S M Ahsan. The Era of AI: Upholding Ethical Leadership. Online. *Open Journal of Leadership*. 2023, roč. 12, č. 04, s. 400-417. ISSN 2167-7743. Dostupné z: <https://doi.org/10.4236/ojl.2023.124019>. [cit. 2025-02-02].

Úřad pro publikace Evropské unie: *BÍLÁ KNIHA o umělé inteligenci – evropský přístup k excelenci a důvěře*. Online. © 2020. Dostupné z: <https://op.europa.eu/cs/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1>. [cit. 2025-03-04].

ÚŘAD VLÁDY ČR. *Akt o umělé inteligenci*. Online. Digitální Česko. © 2025. Dostupné z: <https://digitalnicesko.gov.cz/ai-akt/>. [cit. 2025-02-03].

VAISHYA, Raju; JAVAID, Mohd; KHAN, Ibrahim Haleem a HALEEM, Abid. Artificial Intelligence (AI) applications for COVID-19 pandemic. Online. *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*. 2020, roč. 14, č. 4, s. 337-339. ISSN 18714021. Dostupné z: <https://doi.org/10.1016/j.dsx.2020.04.012>. [cit. 2025-01-27].

VEALE, Michael; MATUS, Kira a GORWA, Robert. AI and Global Governance: Modalities, Rationales, Tensions. Online. *Annual Review of Law and Social Science*. 2023, roč. 19, č. 1, s. 255-275. ISSN 1550-3585. Dostupné z: <https://doi.org/10.1146/annurev-lawsocsci-020223-040749>. [cit. 2025-02-05].

VELEV, D. a ZLATEVA, P. CHALLENGES OF ARTIFICIAL INTELLIGENCE APPLICATION FOR DISASTER RISK MANAGEMENT. Online. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*. 2023, roč. XLVIII-M-1-2023, s. 387-394. ISSN 2194-9034. Dostupné z: <https://doi.org/10.5194/isprs-archives-XLVIII-M-1-2023-387-2023>. [cit. 2025-03-05].

WOJCIECH, Samek; MÜLLER, Klasu-Robert a WIEGAND, Thomas. Explainable Artificial Intelligence: Understanding, Visualizing and Interpreting Deep Learning Models. Online. *ITU Journal: ICT Discoveries - Special Issue 1 - The Impact of Artificial Intelligence (AI) on Communication Networks and Services*. Roč. 2017. Dostupné z: <https://doi.org/10.48550/arXiv.1708.08296>. [cit. 2025-03-05].

YAO, Kan; ZHENG, Yuebing; YAO, Kan a ZHENG, Yuebing. *Fundamentals of Machine Learning*. Online. In: *Nanophotonics and Machine Learning*. Springer Series in Optical Sciences. Cham: Springer International Publishing, 2023, s. 77-112. ISBN 978-3-031-20472-2. Dostupné z: https://doi.org/10.1007/978-3-031-20473-9_3. [cit. 2025-01-26].

ZÁCHRANKA, Z.S. *ZÁCHRANKA Mobilní aplikace pro tísňové volání*. Online. © 2025. Dostupné z: <https://www.zachrankaapp.cz/>. [cit. 2025-03-12].

ZHANG, Zixuan; WANG, Luwei a LEE, Chengkuo. Recent Advances in Artificial Intelligence Sensors. Online. *Advanced Sensor Research*. 2023, roč. 2, č. 8. ISSN 2751-1219. Dostupné z: <https://doi.org/10.1002/adsr.202200072>. [cit. 2025-02-02].

ZUBOFF, Shoshana. *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. London: Profile Books, 2019. ISBN 978-1-78125-685-5.

SEZNAM OBRÁZKŮ

Obrázek 1: Aplikace Záchranka (Zdroj: Záchranka, © 2025).....	54
Obrázek 2: Aplikace PulsePoint Respond (Zdroj: PulsePoint Respond, © 2025)	60
Obrázek 3: Aplikace EchoSOS (Zdroj: EchoSOS, © 2025).....	65
Obrázek 4: Prostředí aplikace Life360 (Zdroj: Life360, © 2025).....	75
Obrázek 5: Logo aplikace True Life Guardian APP (Zdroj: Vlastní)	79
Obrázek 6: Výpočet SWOT vektoru (Zdroj Vlastní).....	98

SEZNAM TABULEK

Tabulka 1: Identifikované faktory SWOT analýzy aplikace True Life Guardian, její silné a slabé stránky.....	87
Tabulka 2: Identifikované faktory SWOT analýzy aplikace True Life Guardian, její příležitosti a hrozby	88
Tabulka 3: SWOT analýza – Silné stránky aplikace True Life Guardian	90
Tabulka 4: SWOT analýza – Slabé stránky aplikace True Life Guardian.....	92
Tabulka 5: SWOT analýza – Příležitosti aplikace True Life Guardian	94
Tabulka 6: SWOT analýza – Hrozby aplikace True Life Guardian	96

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AI	Umělá inteligence - Artificial intelligence
API	Aplikační programovací rozhraní - Application programming interface
BLE	Nízkoenergetická technologie Bluetooth - Bluetooth Low Energy
CAD	Počítačem podporovaný design - Computer aided design
CNN	Konvoluční neuronové sítě - Convolutional neural networks
ČČK	Český červený kříž
DL	Hluboké učení - Deep learning
DNN	Hluboké neuronové sítě - Deep neural networks
GDPR	Obecné nařízení o ochraně osobních údajů - General Data Protection Regulation
GPS	Globální polohovací systém - Global positioning system
GPT	Generativní před trénovaný transformátor - Generative pre-trained transformer
GPU	Grafická procesorová jednotka - Graphics processing unit
IoT	Internet věcí - Internet of Things
IZS	Integrovaný záchranný systém
KPR	Kardiopulmonální resuscitace
ML	Strojové učení - Machine learning
NLP	Zpracování přirozeného jazyka - Natural language processing
RNN	Rekurentní neuronové sítě - Recurrent neural networks
WO	Překonejte slabé stránky využíváním příležitostí