

Umělá inteligence v procesech zajištění kybernetické bezpečnosti subjektu

Bc. Dominik Pulda

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. Dominik Pulda
Osobní číslo:	L22380
Studijní program:	N1032A020002 Bezpečnost společnosti
Specializace:	Ochrana obyvatelstva
Forma studia:	Kombinovaná
Téma práce:	Umělá inteligence v procesech zajištění kybernetické bezpečnosti subjektu

Zásady pro vypracování

- Zpracujte teoretický vstup do dané problematiky.
- Proveďte analýzu možností využití umělé inteligence v oblasti kybernetické bezpečnosti subjektu.
- Na základě výsledků analýzy navrhnete konkrétní opatření v procesech zajištění kybernetické bezpečnosti subjektu.
- Sumarizujte získané výstupy diplomové práce.

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

Seznam doporučené literatury:

1. BROOKS, Charles J.; GROW, Christopher; CRAIG, Philip a SHORT, Donald. *Cybersecurity essentials*. Indianapolis, Indiana: Sybex, John Wiley, 2018. ISBN 978-1-119-36239-5.
2. GÉRON, Aurélien. *Hands-On Machine Learning with Scikit-Learn, Keras and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems*. 2nd edition. Sebastopol, California: O'Reilly Media, 2019. ISBN 978-1-492-03264-9.
3. KAUR, Ramanpreet; GABRIJELČIČ, Dušan a KLOBUČAR, Tomáš. *Artificial intelligence for cybersecurity: Literature review and future research directions*. Information Fusion. (101804), 29. 2023. ISSN 1566-2535.
4. KOLOUCH, Jan a BAŠTA, Pavel. *Cybersecurity*. Praha: CZ.NIC, z.s.p.o. CZ.NIC, 2019. ISBN 978-80-88168-31-7.
5. MUELLER, John Paul a MASSARON, Luca. *Machine Learning For Dummies*. 1st edition. Hoboken, New Jersey: Wiley, 2016. ISBN 978-1119245513.

Další odborná literatura dle doporučení vedoucího diplomové práce.

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

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

L.S.

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

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 mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

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

V Uherském Hradišti, dne 25. 4. 2025

.....
podpis autora

ABSTRAKT

Diplomová práce se zaměřuje na problematiku aplikace umělé inteligence v oblasti kybernetické bezpečnosti, a to s důrazem na detekci phishingu a malwaru v prostředí malého podniku bez interního IT oddělení. Cílem práce bylo navrhnout prakticky realizovatelné řešení ochrany pro modelový subjekt Finakta s.r.o. prostřednictvím výběru vhodného AI nástroje. Práce zahrnuje teoretickou analýzu metod detekce hrozeb, vícekritériální porovnání komerčně dostupných řešení a návrh implementačního postupu. Výsledky potvrdily, že zvolené řešení zvyšuje bezpečnostní úroveň podniku bez nutnosti zásahu do jeho infrastruktury a zároveň ukázaly, že moderní zabezpečení s využitím umělé inteligence nemusí být nutně finančně náročné.

Klíčová slova: kybernetická bezpečnost, malware, malý podnik, phishing, umělá inteligence

ABSTRACT

This Master's thesis focuses on the application of artificial intelligence in the field of cybersecurity, with particular emphasis on the detection of phishing and malware in the context of a small enterprise without an internal IT department. The aim of the thesis was to propose a practically feasible security solution for the model subject Finakta s.r.o. through the selection of an appropriate AI tool. The thesis includes a theoretical analysis of threat detection methods, a multi-criteria comparison of commercially available solutions, and the design of an implementation procedure. The results confirmed that the selected solution enhances the company's cybersecurity level without requiring significant changes to its infrastructure, and also demonstrated that modern AI-based security can be implemented without excessive financial burden.

Keywords: artificial intelligence, cybersecurity, malware, phishing, small business

Tímto bych rád vyjádřil upřímné poděkování vedoucímu diplomové práce, panu Ing. Petru Svobodovi, Ph.D., za jeho odborné vedení a cenné rady, které mi byly oporou při zpracování této práce.

Zvláštní poděkování patří také panu Ing. Tomáši Ráčilovi za jeho podněty a motivaci, které mi dodaly sebedůvěru a odhodlání práci začít i úspěšně dokončit.

„Amatéři hackují systémy, profesionálové hackují lidi.“
— Bruce Schneier

„Trvá 20 let vybudovat reputaci a jen pár minut kybernetického incidentu ji zničit.“
— Stéphane Nappo

OBSAH

ÚVOD.....	12
CÍL PRÁCE A POUŽITÉ METODY.....	13
I TEORETICKÁ ČÁST	15
1 ZÁKLADNÍ TERMINOLOGIE.....	16
1.1 TERMINOLOGIE SOUVISEJÍCÍ S UMĚLOU INTELIGENCÍ	16
1.1.1 Umělá inteligence.....	16
1.1.2 Strojové učení.....	17
1.1.3 Hlubkové učení	17
1.1.4 Federované učení	18
1.1.5 Neuronové sítě	19
1.1.6 Zpracování přirozeného jazyka	20
1.1.7 Generativní umělá inteligence.....	21
1.1.8 Anomální detekce.....	22
1.2 TERMINOLOGIE SOUVISEJÍCÍ S KYBERNETICKOU BEZPEČNOSTÍ	22
1.2.1 Kybernetická bezpečnost	23
1.2.2 Kybernetický útok	23
1.2.3 Malware.....	24
1.2.4 Phishing a sociální inženýrství.....	25
1.2.5 Distributed Denial of Service útoky.....	27
1.2.6 Structured Query Language Injection útoky	29
1.2.7 Zero-Day útoky	29
1.2.8 Advanced Persistent Threats	29
1.2.9 Internet of Things útoky	30
1.2.10 Deepfake	30
2 PRÁVNÍ RÁMEC A MEZINÁRODNÍ NORMY	32
2.1 ČESKÁ LEGISLATIVA A NÁRODNÍ STRATEGIE KYBERNETICKÉ BEZPEČNOSTI	32
2.1.1 Zákon o kybernetické bezpečnosti (č. 181/2014 Sb.)	32
2.1.2 Zákon o zpracování osobních údajů (č. 110/2019 Sb.).....	35
2.1.3 Návrh nového zákon o kybernetické bezpečnosti	35
2.1.4 Trestní zákoník (č. 40/2009 Sb.)	37
2.1.5 Problémy a výzvy spojené s trestní odpovědností v oblasti kyberkriminality	39
2.1.6 Národní strategie kybernetické bezpečnosti ČR 2021-2025	40
2.2 ISO/IEC 27000 FAMILY	42
2.2.1 ISO/IEC 27001	42
2.2.2 ISO/IEC 27002.....	42
2.2.3 ISO/IEC 27005	43
2.3 MEZINÁRODNÍ LEGISLATIVA	43
2.3.1 Nařízení Evropského parlamentu a Rady (EU) 2024/1689.....	43
2.3.2 Směrnice Evropského parlamentu a Rady (EU) 2022/2555	45
2.3.3 Nařízení Evropského parlamentu a Rady (EU) 2016/679.....	46

3	DÍLČÍ ZÁVĚR TEORETICKÝCH VÝCHODISEK DIPLOMOVÉ PRÁCE	47
II	PRAKTICKÁ ČÁST	48
4	ANALÝZA A KOMPARACE PŘÍSTUPŮ K DETEKCI VYBRANÝCH KYBERNETICKÝCH HROZEB	49
4.1	ANALÝZA A POROVNÁNÍ METOD DETEKCE MALWARE	49
4.1.1	Tradiční přístup – signaturní detekce	49
4.1.2	Tradiční přístup – heuristická analýza.....	51
4.1.3	Detekce malwaru pomocí umělé inteligence.....	53
4.1.4	Komparace metod detekce malware.....	56
4.1.5	Zhodnocení přístupů k detekci malwaru	57
4.2	ANALÝZA A POROVNÁNÍ METOD DETEKCE PHISHINGU	58
4.2.1	Tradiční přístup – blacklisting.....	58
4.2.2	Tradiční přístup – filtrování e-mailů	60
4.2.3	Tradiční přístup – vzdělávání a osvěta uživatelů	61
4.2.4	Metoda umělé inteligence – strojové učení	63
4.2.5	Metoda umělé inteligence – hluboké učení	65
4.2.6	Metoda umělé inteligence – jazykové modely	66
4.2.7	Komparace vybraných metod pro detekci phishingu	68
4.2.8	Zhodnocení přístupů k detekci phishingu	70
5	ANALÝZA A NÁVRH NÁSTROJE UMĚLÉ INTELIGENCE PRO ZVÝŠENÍ KYBERNETICKÉ BEZPEČNOSTI SUBJEKTU	71
5.1	CHARAKTERISTIKA MODELOVÉHO SUBJEKTU	71
5.2	PRŮZKUM TRHU: NÁSTROJE S VYUŽITÍM UMĚLÉ INTELIGENCE PRO DETEKCI PHISHINGU A MALWARE.....	72
5.2.1	Microsoft Defender for Business	73
5.2.2	Sophos Intercept X	73
5.2.3	CrowdStrike Falcon Go.....	74
5.2.4	SentinelOne Singularity Control	74
5.2.5	Acronis Cyber Protect	74
5.3	FINANČNÍ ANALÝZA VYBRANÝCH ŘEŠENÍ VYUŽÍVAJÍCÍCH UMĚLOU INTELIGENCI PRO DETEKCI PHISHINGU A MALWARU	75
5.3.1	Normalizace finanční náročnosti.....	76
5.3.2	Zhodnocení finanční náročnosti vybraných AI řešení	77
5.4	POSOUZENÍ VHODNOSTI NAVRHOVANÝCH ŘEŠENÍ PRO SUBJEKT FINAKTA S.R.O.	78
5.4.1	Zhodnocení vhodnosti vybraných řešení.....	80
5.5	VÝBĚR KONKRÉTNÍHO ŘEŠENÍ PRO MODELOVÝ SUBJEKT	81
5.5.1	Vyhodnocení výběru řešení pro modelový subjekt.....	82
5.6	NÁVRH IMPLEMENTACE DOPORUČENÉHO ŘEŠENÍ	83
5.6.1	Předpoklady implementace	83
5.6.2	Postup nasazení řešení.....	83

5.6.3	Časový rámec implementace.....	84
5.6.4	Přínosy pro subjekt Finakta s.r.o.....	84
6	DISKUSE	85
	ZÁVĚR	86
	SEZNAM POUŽITÉ LITERATURY.....	88
	SEZNAM TABULEK.....	102
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	103

ÚVOD

V posledním desetiletí dochází k dynamickému rozvoji technologií, který s sebou přináší nejen nové příležitosti, ale také nové hrozby. Kybernetická bezpečnost se tak stává jedním z klíčových aspektů ochrany kritické infrastruktury, firemních dat i osobních údajů jednotlivců. Zároveň se rychlým tempem rozvíjí i oblast umělé inteligence, která proniká do širokého spektra odvětví a začíná hrát významnou roli také v oblasti zabezpečení informačních systémů.

Téma této diplomové práce je tedy nanejvýš aktuální – jak kybernetická bezpečnost, tak umělá inteligence patří k často diskutovaným fenoménům současnosti, jejichž význam bude s ohledem na vývoj digitální společnosti dále narůstat. Cílem této práce je prozkoumat možnosti využití metod a nástrojů umělé inteligence pro detekci, prevenci a reakci na kybernetické hrozby, přičemž pozornost bude věnována jak teoretickým základům, tak i praktickým aplikacím v modelovém subjektu.

Vzhledem k rostoucímu počtu sofistikovaných kybernetických útoků, které tradiční bezpečnostní nástroje často nedokážou včas zachytit, je nasazení inteligentních systémů založených na strojovém učení či hlubokých neuronových sítích perspektivním směrem, který může významně přispět ke zvýšení úrovně ochrany informačních systémů.

Při zpracování této diplomové práce byl jako podpůrný nástroj využit generativní model umělé inteligence ChatGPT (verze GPT-4o) dostupný prostřednictvím aplikace společnosti OpenAI dostupný na adrese: <https://chat.openai.com>. Tento nástroj byl použit výhradně za účelem revize vlastních textů, konzultace formulace myšlenek a asistence při překladu cizojazyčných odborných zdrojů. Veškerý obsah vytvořený s jeho podporou byl následně pečlivě zkontrolován autorem práce, který za něj přebírá plnou odpovědnost.

CÍL PRÁCE A POUŽITÉ METODY

Hlavním cílem této diplomové práce je navrhnout prakticky realizovatelné řešení pro zvýšení kybernetické bezpečnosti malého podniku v oblasti detekce a reakce na vybrané kybernetické hrozby. Tohoto cíle bude dosaženo prostřednictvím výběru a aplikace nástroje využívajícího umělou inteligenci.

Za účelem dosažení hlavního cíle byly stanoveny následující dílčí cíle:

- Zhodnotit a porovnat tradiční a moderní (AI založené) přístupy k detekci kybernetických hrozeb, a to na základě odborné literatury a analytických metrik.
- Provést vícekritériální komparaci vybraných komerčně dostupných AI nástrojů určených pro detekci phishingu a malwaru.
- Na základě komparativní analýzy vybrat vhodný nástroj pro prostředí malého podniku bez interního IT oddělení.

Na základě stanovených cílů byly formulovány následující pracovní hypotézy, které byly ověřovány v rámci praktické části práce:

H1: AI nástroje pro detekci kybernetických hrozeb dosahují vyšší přesnosti než tradiční přístupy, zejména v případě neznámých variant malwaru.

H2: Existují komerčně dostupné AI nástroje, které jsou technicky i finančně dostupné v podmínkách malého podniku bez interního IT týmu.

H3: Implementace vhodného AI řešení přináší významné zvýšení úrovně kybernetické ochrany subjektu, a to i bez potřeby zásadních změn v IT a datové infrastruktuře.

Použité metody

Při zpracování diplomové práce byly využity následující metody:

- Analýza odborných zdrojů a literární rešerše

Studium české i zahraniční odborné literatury, vědeckých článků a technických zpráv v oblasti umělé inteligence a kybernetické bezpečnosti s cílem vymezit klíčové pojmy, technologické přístupy a rámce právní regulace.

- Komparativní analýza

Porovnání tradičních a moderních (AI založených) metod detekce kybernetických hrozeb na základě dostupných empirických údajů a metrik výkonnosti.

- Vícekriteriální hodnocení

Aplikace vícekriteriálního rozhodování pro posouzení vhodnosti dostupných nástrojů využívajících umělou inteligenci pro modelový subjekt.

- Lineární normalizace

Použita pro převod měřítek hodnocených kritérií do společné numerické škály, aby bylo možné objektivně porovnat alternativy nástrojů.

- Kvalitativní analýza modelového subjektu

Popis a vyhodnocení vnitřního prostředí modelového subjektu se zaměřením na schopnost implementovat nové nástroje a procesy v oblasti kybernetické ochrany.

- Návrhová metoda

Vytvoření prakticky realizovatelného návrhu implementace AI řešení včetně předpokladů a očekávaných přínosů, reflektující technické, ekonomické a organizační možnosti subjektu.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ TERMINOLOGIE

Tato kapitola přibližuje základní pojmy spojené s umělou inteligencí a kybernetickou bezpečností. Nejprve se věnuje klíčovým technologiím AI, jako je strojové učení, neuronové sítě nebo generativní modely, a jejich využití v oblasti bezpečnosti. Druhá část se zaměřuje na kybernetické hrozby, metody útoků a obranné mechanismy. Cílem je vytvořit teoretický rámec pro další části práce a lépe porozumět roli AI v ochraně digitálních systémů.

1.1 Terminologie související s umělou inteligencí

Tato subkapitola se zaměřuje na klíčové pojmy z oblasti umělé inteligence, které jsou relevantní pro kybernetickou bezpečnost. Pro pochopení jejího fungování je nezbytné se seznámit s koncepty, jako je strojové učení, hluboké učení, neuronové sítě nebo zpracování přirozeného jazyka. V této části budou tyto termíny vysvětleny.

1.1.1 Umělá inteligence

Umělá inteligence (AI) je komplexní a dynamicky se rozvíjející oblast, která nemá jednotnou definici. Různé přístupy ji vnímají odlišně v závislosti na tom, jaký aspekt jejího fungování zdůrazňují. Gong (2025) popisuje AI jako technologii napodobující lidské inteligentní chování, včetně vnímání a kognice. Tento přístup klade důraz na schopnost AI simulovat procesy typické pro lidskou mysl, což zahrnuje analýzu informací, rozpoznávání vzorců a rozhodování. Al-Harbi (2025) naopak vnímá AI jako výpočetní modely schopné učení, predikce a rozhodování, přičemž se uplatňuje zejména v oblastech automatizace a analýzy dat. Tato definice reflektuje AI jako nástroj, který nejen zpracovává informace, ale také na jejich základě činí závěry a přizpůsobuje se různým scénářům. Zhao et al. (2025) definují AI jako disciplínu zaměřenou na vývoj algoritmů, které nejen simulují lidskou inteligenci, ale zároveň se dokážou adaptovat na proměnlivé podmínky prostředí. Tento přístup zdůrazňuje flexibilitu AI a její schopnost přizpůsobit se změnám, což je klíčové zejména v oblastech, kde je nutné rychle reagovat na nové situace, například v kybernetické bezpečnosti.

Všechny zmíněné definice se shodují v tom, že AI je systémem umožňujícím simulaci lidské inteligence a rozhodování na základě dat. Rozcházejí se však v důrazu na jednotlivé aspekty – zatímco Gong (2025) zdůrazňuje imitaci lidského chování, Al-Harbi (2025) se zaměřuje na schopnost učení a predikce. Zhao et al. (2025) pak kladou důraz na adaptabilitu AI v proměnlivém prostředí. Každá z těchto definic tak reflektuje jiný klíčový aspekt AI, což

ukazuje, že umělá inteligence není jednotně definovaným pojmem, ale dynamickým oborem s různými přístupy k jeho chápání.

1.1.2 Strojové učení

Strojové učení (Machine Learning, ML) představuje jednu z klíčových oblastí umělé inteligence, která umožňuje systémům učit se z dat a následně na jejich základě činit rozhodnutí. Podle Gérona (2019) je strojové učení definováno jako proces, při kterém algoritmy automaticky objevují vzory v datech a používají je k predikci budoucího chování. Tato schopnost je široce využívána v oblastech, jako je zpracování přirozeného jazyka, rozpoznávání obrazu nebo detekce kybernetických hrozeb. Schlisselberg a Darshan (2025) se zaměřují na roli parametrů v modelech strojového učení a zdůrazňují, že jejich správná alokace výrazně ovlivňuje schopnost modelu generalizovat naučené vzory. Autoři navrhuji heuristické principy, které umožňují optimalizovat výpočetní náročnost a zlepšit přesnost predikce. Mueller a Massaron (2016) pak strojové učení popisují jako disciplínu, která využívá metody jako dozorované a nedozorované učení, posilované, učení a hluboké učení. Tyto metody se liší způsobem, jakým modely zpracovávají data – zatímco dozorované učení se opírá o trénovací sady obsahující vstupy a výstupy, nedozorované učení se snaží najít skryté struktury v neoznačených datech.

Při porovnání těchto definic je patrné, že všechny zdůrazňují schopnost modelů učit se ze zkušeností a přizpůsobovat se novým podmínkám. Géron (2019) klade důraz na aplikace v reálném světě, Schlisselberg a Darshan (2025) se soustředí na technické aspekty optimalizace modelů, zatímco Mueller a Massaron (2016) poskytují širší klasifikaci metod strojového učení. Společným jmenovatelem je však využití velkých datových souborů a algoritmů k automatizaci rozhodovacích procesů, což činí strojové učení nepostradatelným nástrojem v moderní kybernetické bezpečnosti.

1.1.3 Hlubkové učení

Hluboké učení (Deep Learning, DL) je specifická podmnožina strojového učení, která využívá vícevrstvé neuronové sítě k analýze složitých vzorců v datech. Géron (2019) popisuje hluboké učení jako techniku inspirovanou strukturou lidského mozku, kde jednotlivé vrstvy neuronů provádějí hierarchické zpracování informací – od jednoduchých prvků po složité abstrakce. Tento přístup umožňuje efektivní rozpoznávání obrazů, přepis řeči nebo analýzu přirozeného jazyka. Marmoni et al. (2025) dále zdůrazňují, že hluboké učení představuje významný posun oproti tradičním metodám strojového učení, protože

dokáže automaticky extrahovat užitečné vlastnosti z neoznačených dat bez nutnosti ručního zásahu. Autoři zároveň poukazují na vysoké výpočetní nároky, které jsou klíčovým omezením této technologie. Singh a Sharan (2024) se zaměřují na specifickou oblast hlubokého učení – konvoluční neuronové sítě (CNN), které se osvědčily zejména v oblasti počítačového vidění. Podle jejich studie jsou CNN klíčovou součástí moderních bezpečnostních systémů, například při detekci škodlivého softwaru či analýze síťového provozu.

Při porovnání hlubokého učení se strojovým učením lze nalézt několik zásadních rozdílů. Strojové učení obecně zahrnuje různé metody analýzy dat, včetně regresních modelů, rozhodovacích stromů nebo podporovaných vektorových strojů (SVM), zatímco hluboké učení je založeno výhradně na neuronových sítích s mnoha skrytými vrstvami. Géron (2019) uvádí, že strojové učení se obvykle spoléhá na ruční extrakci příznaků, hluboké učení však dokáže tyto příznaky objevit samo. Zatímco klasické strojové učení je často vhodné pro menší datové sady a vyžaduje pečlivou přípravu vstupních parametrů, hluboké učení vyniká při práci s obrovskými objemy dat, ale jeho trénování je výpočetně náročnější. Jak zdůrazňují Marmoni et al. (2025), hluboké učení přináší vyšší přesnost a robustnost modelů, avšak za cenu vyšších požadavků na výpočetní výkon a potřebu velkého množství kvalitních trénovacích dat.

1.1.4 Federované učení

Federované učení (FL) je inovativní metoda trénování modelů strojového učení, která umožňuje zpracování dat přímo na koncových zařízeních, čímž eliminuje potřebu centralizovaného ukládání dat. Tento přístup hraje zásadní roli v oblasti kybernetické bezpečnosti, kde je ochrana soukromí a bezpečnost dat klíčová. Podle studie Ferraga et al. (2021) se federované učení stále více uplatňuje v zabezpečení internetu věcí, kde umožňuje efektivnější detekci kybernetických hrozeb, aniž by docházelo k odhalení citlivých dat koncových uživatelů. Na druhou stranu, podle Zhanga et al. (2021) je využití federovaného učení v kybernetické bezpečnosti spojeno s řadou výzev, včetně rizik spojených s tzv. adversariálními útoky (adversarial attacks), při kterých útočníci manipulují modely FL za účelem jejich zneužití.

Výhody federovaného učení v kybernetické bezpečnosti

Hlavní přínos federovaného učení spočívá v jeho schopnosti decentralizovaného tréninku modelů, což zajišťuje vyšší úroveň soukromí a nižší riziko úniku dat. Tento přístup je

užitečný zejména v sektorech, kde je nutné chránit citlivá data, například v bankovníctví nebo zdravotnictví. (Ferrag et al., 2021)

Zhang et al. (2021) zároveň poukazuje, že federované učení umožňuje rychlejší přizpůsobení modelů novým hrozbám bez nutnosti přenosu dat na centrální servery.

Rizika a výzvy spojené s federovaným učení

Navzdory zmíněným výhodám přináší federované učení řadu bezpečnostních výzev. Jedním z hlavních problémů je tzv. poisoning attack, kdy útočníci infikují jednotlivé uzly škodlivými daty, což může vést k nesprávnému trénování modelu. Zhang et al., 2021.

Ferrag et al. (2021) dále upozorňují na problém tzv. re-identifikace uživatelů, kdy lze z váhových aktualizací modelu zpětně rekonstruovat některé informace o trénovacích datech. Z tohoto důvodu se v poslední době stále více prosazuje diferenciální soukromí a homomorfní šifrování jako způsoby ochrany dat při federovaném učení.

1.1.5 Neuronové sítě

Neuronové sítě (Artificial Neural Networks, ANN) jsou výpočetní modely inspirované strukturou a funkcí lidského mozku. Tyto sítě se skládají z vrstev propojených uzlů (neuronů), které zpracovávají vstupní data a na základě váhových koeficientů generují výstupy. Neuronové sítě lze chápat jako soubor algoritmů, které se učí rozpoznávat vzory v datech pomocí trénovacích procesů. Každý neuron ve vrstvě provádí jednoduché matematické operace a předává výsledek dalším neuronům, čímž vzniká vícevrstvá struktura umožňující zpracování složitých nelineárních vztahů. (Géron, 2019)

Podle Schlisselberga a Darshana (2025) je klíčovým principem neuronových sítí schopnost adaptace prostřednictvím změny váhových parametrů během procesu učení. Autoři zdůrazňují, že výkonnost neuronových sítí je ovlivněna optimalizací těchto parametrů a navrhuje strategie pro zlepšení jejich efektivity při zpracování velkých datových souborů. Stamov et al. (2025) ve své studii uvádějí, že neuronové sítě jsou využívány nejen v klasických aplikacích (například zpracování obrazu nebo rozpoznávání řeči), ale nacházejí uplatnění i v pokročilých oblastech, jako jsou kvantové neuronové sítě, které kombinují principy kvantového výpočtu a hlubokého učení.

Fernandes a Bessy (2025) pak upozorňují na skutečnost, že neuronové sítě poskytují flexibilitu při řešení komplexních problémů, ale čelí výzvám spojeným s interpretací výsledků. Autoři navrhuje hybridní modely kombinující neuronové sítě s expertními

systemy, které umožňují transparentnější rozhodovací procesy, což je zásadní například v kritických aplikacích kybernetické bezpečnosti.

Neuronové sítě se od tradičního strojového učení liší především svou schopností automaticky extrahovat vlastnosti z dat, aniž by bylo nutné je explicitně definovat. Zatímco klasické algoritmy, jako jsou rozhodovací stromy nebo lineární regrese, vyžadují ruční zpracování vstupních příznaků, neuronové sítě se samy učí rozpoznávat skryté vzory a vztahy. Jak uvádí Géron (2019), hlavní výhodou neuronových sítí je jejich schopnost pracovat s nelineárními vztahy a složitými strukturami dat, což je činí ideálními pro úkoly, jako je zpracování obrazu, přirozeného jazyka nebo i detekce kybernetických hrozeb. Na druhou stranu, jak zdůrazňují Schlisselberg a Darshan (2025), neuronové sítě mají vysoké výpočetní nároky a vyžadují velké množství trénovacích dat pro dosažení přesných výsledků, což může být limitující při práci s omezenými zdroji.

1.1.6 Zpracování přirozeného jazyka

Zpracování přirozeného jazyka (Natural Language Processing, NLP) je podoblast umělé inteligence zaměřená na analýzu, porozumění a generování lidského jazyka. Tato technologie kombinuje lingvistické znalosti s algoritmy strojového a hlubokého učení, což umožňuje zpracovávat a interpretovat velké objemy textových dat. Kaur, Gabrijelčič a Klobučar (2023) zdůrazňují roli NLP v kybernetické bezpečnosti, zejména v automatizovaném zpracování hrozeb (například analýza otevřených zdrojů – OSINT) a identifikaci potenciálních útoků z veřejně dostupných dat. NLP je zásadní pro detekci phishingových e-mailů, analýzu sentimentu na dark webu a sledování kybernetických hrozeb ve více jazycích, což je klíčové pro globální monitorování rizik.

Podle Branca, Coga a Medeiros (2024) se NLP uplatňuje v systémech detekce útoků na webové aplikace pomocí klasifikace síťového provozu a logů. Autoři prezentují model, který kombinuje NLP s klasickými metodami kybernetické bezpečnosti a zvyšuje efektivitu detekce útoků skrytých v zašifrovaném provozu, což je zásadní v kontextu moderních bezpečnostních hrozeb. Sayyafzadeh a Weatherspoon (2024) dále upozorňují na využití NLP pro analýzu phishingových e-mailů pomocí sentimentální analýzy a velkých jazykových modelů (LLM). Tento přístup umožňuje přesnější detekci podvodných zpráv a manipulativního obsahu, což zvyšuje schopnost organizací bránit se proti cíleným útokům.

NLP hraje klíčovou roli i v boji proti dezinformacím. Kloo (2024) popisuje využití NLP v kombinaci s modely síťové vědy k identifikaci a kontextualizaci tvrzení, která mohou

obsahovat zavádějící nebo nepravdivé informace. Tento přístup může být využíván v oblasti sociální kybernetické bezpečnosti k potírání šíření nepravdivých informací na sociálních sítích a v digitálních médiích.

Na rozdíl od tradičních metod strojového učení, které se zaměřují na strukturovaná numerická data, NLP pracuje s nestrukturovanými textovými vstupy a je schopno extrahovat sémantický význam a jazykové vzory. Jak upozorňuje Silvestri a Gargiulo (2024), s nástupem velkých jazykových modelů došlo k výraznému pokroku v analýze textu, což umožňuje komplexnější pochopení jazykových nuancí a kontextuální interpretaci. Tyto modely však zároveň vyvolávají obavy o bezpečnost a ochranu osobních údajů v případě, že jsou používány v citlivých aplikacích kybernetické bezpečnosti.

1.1.7 Generativní umělá inteligence

Generativní umělá inteligence představuje pokročilou oblast umělé inteligence, která je schopna vytvářet zcela nové obsahy – od textů, obrázků, zvuku až po simulace a samotný kód. Generativní AI se v oblasti kybernetické bezpečnosti uplatňuje při simulaci sofistikovaných kybernetických útoků, což pomáhá testovat odolnost systémů a zlepšovat obranné strategie. Tento přístup umožňuje bezpečnostním týmům předvídat budoucí hrozby a vyvíjet účinnější detekční mechanismy. (Ferrag et al., 2025)

Nadella et al. (2025) upozorňují na využití generativní AI v oblasti správy datové bezpečnosti. Jejich navržený rámec dokáže generovat scénáře potenciálních úniků dat a testovat účinnost bezpečnostních opatření v reálném čase. Díky tomu mohou organizace lépe identifikovat zranitelnosti a preventivně reagovat na možné hrozby. Autoři zároveň zdůrazňují, že generativní modely nacházejí využití nejen při odhalování rizik, ale také při simulaci komplexních bezpečnostních incidentů, což zvyšuje adaptabilitu obranných mechanismů.

Další významnou oblastí je automatizované penetrační testování (tzv. PenTest++), na které se zaměřují Al-Sinani a Mitchell (2025). Jejich studie ukazuje, jak generativní AI může vytvářet nové typy útoků na digitální infrastrukturu, čímž umožňuje bezpečnostním specialistům odhalit skryté slabiny. Autoři však varují, že stejná technologie může být zneužita kybernetickými zločinci k vytváření realistických phishingových kampaní či podvodného obsahu, což komplikuje jejich detekci a neutralizaci.

Generativní AI poskytuje kybernetické bezpečnosti nové možnosti v oblasti detekce a prevence hrozeb. Její schopnost simulovat reálné útoky, generovat testovací scénáře

a analyzovat slabá místa z ní činí účinný nástroj pro ochranu citlivých dat. Jak však zdůrazňuje Blake (2025), s těmito výhodami přichází i značná rizika – například vytváření realistických deepfake videí, jednoduchá tvorba škodlivého softwaru nebo podvodného obsahu. Blake (2025) pak upozorňuje na nezbytnost vývoje regulačních rámců a zavádění etických zásad pro bezpečné využívání těchto pokročilých technologií.

1.1.8 Anomální detekce

Anomální detekce je zásadním nástrojem v oblasti kybernetické bezpečnosti, který umožňuje identifikovat neobvyklé chování nebo odchylky od běžných vzorců v datech. Tyto odchylky mohou signalizovat potenciální hrozby, jako jsou neoprávněné přístupy, síťové útoky nebo pokusy o manipulaci s daty. (Shah a Best, 2025)

Jiný přístup k definici nabízí Joseph et al. (2025), kteří zdůrazňují nejen samotné rozpoznání anomálií, ale také potřebu jejich správné interpretace a kategorizace. Autoři upozorňují, že pouhá detekce odchylky není dostatečná – důležité je posoudit, zda jde o skutečnou hrozbu, nebo o falešně pozitivní výsledek. Tento přístup klade důraz na přesnost a kontextuální pochopení detekovaných událostí, což je nezbytné pro efektivní rozhodování v reálném čase.

Zajímavou perspektivu přináší Bello (2025), který rozšiřuje pojetí anomální detekce o aspekt behaviorální analýzy. Tvrdí, že kromě statistických odchylek by měly moderní systémy sledovat také změny v chování uživatelů nebo zařízení. Tento přístup se ukazuje jako mimořádně užitečný v prostředích, kde útočníci často napodobují legitimní aktivity, aby se vyhnuli odhalení. Behaviorální analýza umožňuje identifikovat i jemné odchylky, které mohou signalizovat pokročilé a dlouhodobé hrozby.

1.2 Terminologie související s kybernetickou bezpečností

Tato subkapitola se zaměřuje na klíčové pojmy v oblasti kybernetické bezpečnosti, které jsou zásadní pro pochopení mechanismů ochrany digitálních systémů. V době rostoucí digitalizace a narůstajícího počtu kybernetických hrozeb je nezbytné seznámit se s termíny, které charakterizují jak samotné útoky, tak obranné strategie proti nim.

Cílem této subkapitoly je poskytnout přehled o nejdůležitějších termínech souvisejících s kybernetickou bezpečností a vytvořit pevný teoretický základ pro pochopení efektivních metod ochrany digitálního prostředí před stále sofistikovanějšími kybernetickými útoky.

1.2.1 Kybernetická bezpečnost

Morris et al. (2024) definují kybernetickou bezpečnost jako soubor metod a strategií zaměřených na ochranu informačních systémů před neoprávněným přístupem, narušením a zneužitím. Autoři zdůrazňují, že tato oblast zahrnuje nejen technologická opatření, jako jsou šifrování a monitorování sítí, ale také organizační a právní rámce, které určují pravidla pro ochranu dat. Studie také poukazuje na rostoucí roli umělé inteligence a strojového učení v oblasti prevence a detekce kybernetických hrozeb.

Jedním ze základních pilířů kybernetické bezpečnosti je triáda CIA (Confidentiality, Integrity, Availability), která vymezuje tři klíčové aspekty ochrany informačních systémů. Rehberger (2024) popisuje tento model jako rámec zajišťující důvěrnost (ochrana před neoprávněným přístupem), integritu (zachování přesnosti a spolehlivosti dat) a dostupnost (zajištění přístupu oprávněných uživatelů k informacím, kdykoli je potřebují). Zdůrazňuje, že narušení kterékoli z těchto složek může vést k rozsáhlým bezpečnostním incidentům.

Podle Koloucha a Bašty (2019) se kybernetická bezpečnost neomezuje pouze na technická opatření, jako jsou firewally, šifrování nebo antivirové programy, ale zahrnuje také organizační a legislativní strategie, které pomáhají minimalizovat bezpečnostní rizika. Autoři zdůrazňují, že efektivní ochrana vyžaduje nejen preventivní opatření, ale i schopnost rychlé reakce na kybernetické incidenty.

Stejný pohled sdílí Brooks et al. (2018), kteří vnímají kybernetickou bezpečnost jako komplexní strategický proces. Efektivní ochrana digitálních systémů podle nich vyžaduje nejen technologická řešení, ale také průběžné monitorování hrozeb, školení zaměstnanců a implementaci bezpečnostních politik, které snižují riziko kybernetických útoků, jako jsou malware, phishing nebo DDoS útoky.

1.2.2 Kybernetický útok

Kybernetický útok je úmyslná činnost zaměřená na narušení digitálních systémů, kompromitaci jejich integrity, důvěrnosti nebo dostupnosti, často s cílem získat neoprávněný přístup, způsobit škodu nebo narušit provoz kritické infrastruktury. Tento přístup reflektuje široké spektrum kybernetických hrozeb, od jednotlivých hackerských aktivit až po státem sponzorované útoky vedené proti strategickým digitálním infrastrukturám. (Shukla, Johnson a Jones, 2025)

Podle Muurimäkiho (2025) mohou kybernetické útoky cílit na různé oblasti digitální bezpečnosti. Některé jsou zaměřené na získání citlivých dat prostřednictvím phishingu nebo malware, zatímco jiné usilují o vyřazení systémů z provozu, například pomocí DDoS útoků. Autor zdůrazňuje, že s rostoucí digitalizací jsou tyto útoky stále sofistikovanější a jejich prevence se stává klíčovou výzvou kybernetické bezpečnosti.

Jiný přístup nabízí Podgorski (2024), který rozděluje kybernetické útoky podle jejich primárního cíle. Rozlišuje mezi útoky zaměřenými na důvěrnost dat, jako jsou keyloggery nebo spyware, a útoky na dostupnost systémů, kam spadají ransomwarové kampaně a síťové útoky. Tato klasifikace zdůrazňuje důsledky kybernetických útoků nejen na individuální uživatele, ale i na organizace a národní bezpečnost.

Podle Aliyevy (2025) se kybernetické útoky staly nejen nástrojem kyberkriminality, ale také součástí hybridní války, kde jsou využívány jako prostředek geopolitického nátlaku. Rostoucí sofistikovanost těchto útoků vede k vývoji pokročilých obranných mechanismů, včetně strojového učení a behaviorální analýzy, které umožňují rychlou detekci anomálií a minimalizaci potenciálních škod.

1.2.3 Malware

Malware, zkratka pro malicious software, v překladu škodlivý software, který je navržený k narušení, poškození nebo neoprávněné manipulaci s počítačovými systémy. Malware je možno definovat jako jakýkoli software navržený k narušení, poškození nebo neoprávněné manipulaci s počítačovými systémy, často za účelem finančního zisku nebo sabotáže. (Chapple a Nijim, 2024).

Různé typy malwaru mají odlišné metody infekce a různé cíle, od sběru citlivých informací až po blokování přístupu k systémům nebo jejich úplné zničení. Mezi nejběžnější druhy malwaru patří:

- **Viry**

Viry jsou jedním z nejstarších typů malwaru a jejich hlavní charakteristikou je samo replikace – tedy schopnost připojit se k jiným souborům nebo programům a šířit se na další zařízení. Počítačové viry historicky nejčastější formou malwaru, i když moderní kybernetické hrozby je do značné míry nahradily pokročilejšími variantami. (Gritzalis, Choo a Patsakis, 2024)

- **Trojské koně**

Trojský kůň se maskuje jako legitimní software, ale ve skutečnosti obsahuje škodlivý kód. Trojské koně se vydávají za legitimní aplikace, ale ve skutečnosti umožňují útočníkovi vzdálený přístup k napadenému zařízení. Tento typ malwaru se často využívá k instalaci dalšího škodlivého softwaru nebo krádeži přihlašovacích údajů. (Chapple a Nijim, 2024)

- **Spyware**

Spyware je typ malwaru, který sledováním uživatele získává citlivé údaje, jako jsou hesla, údaje o bankovních účtech nebo historie prohlížení internetu. Spyware je jedním z nejrozšířenějších typů malwaru a bývá distribuován prostřednictvím nakažených webových stránek nebo nevyžádaných e-mailů. (Gritzalis, Choo a Patsakis, 2024)

- **Ransomware**

Ransomware je druh malwaru, který zašifruje soubory oběti a požaduje výkupné za jejich zpřístupnění. Tento typ útoku se stal v posledních letech jednou z nejzávažnějších kybernetických hrozeb, přičemž útoky často míří na kritickou infrastrukturu. Ransomware je nejvýnosnější formou kyberkriminality, která útočníkům umožňuje vynucovat platby za dešifrování souborů. (Chapple a Nijim, 2024)

- **Rootkit**

Rootkity jsou pokročilé formy malwaru, které umožňují skrytý přístup k napadenému zařízení. Tento typ malwaru je obzvláště nebezpečný, protože dokáže obejít bezpečnostní opatření a často se maskuje před antivirovými programy. uvádějí, Rootkity se nejčastěji využívají v cílených útocích, kde útočníci potřebují dlouhodobý přístup k napadenému systému bez odhalení. (Chapple a Nijim, 2024)

1.2.4 Phishing a sociální inženýrství

Phishing a další techniky sociálního inženýrství patří mezi nejrozšířenější formy kybernetických útoků, protože zneužívají lidskou psychologii namísto technických zranitelností. Zatímco phishing se zaměřuje na podvodné získání citlivých údajů, sociální inženýrství zahrnuje širší spektrum manipulativních technik, které mohou vést k neoprávněnému přístupu do systémů. Phishing patří k nejběžnějším kybernetickým

hrozbám využívajícím sociální manipulaci k získání citlivých informací, jako jsou hesla nebo finanční údaje. (Mailewa et al., 2025)

Phishingové kampaně se stávají stále sofistikovanějšími a využívají nové technologie, včetně umělé inteligence, k personalizaci podvodných zpráv a zvýšení jejich důvěryhodnosti. Moderní phishingové útoky již nejsou omezeny pouze na e-maily, ale zahrnují také telefonní hovory (vishing) a podvodné SMS zprávy (smishing). (Mandru, 2025)

Rostoucím rizikem je také quishing (QR code phishing), kdy útočníci zneužívají QR kódy k přesměrování obětí na podvodné weby nebo k instalaci škodlivého softwaru. Tento typ útoku je zvláště nebezpečný, protože oběti při skenování kódu nevidí cílovou URL adresu, což usnadňuje maskování škodlivých odkazů. Quishing se často objevuje na důvěryhodně vypadajících fyzických či digitálních materiálech, jako jsou letáky, e-maily nebo webové stránky, a jeho cílem je krádež přihlašovacích údajů, finanční podvody nebo instalace malwaru do zařízení oběti. (Amoah a Hayfron-Acquah, 2022)

Kromě těchto metod se stále větší hrozbou stává deepfake phishing, který využívá generativní umělou inteligenci k vytváření realistických audio a video deepfake podvodů. Útočníci dokážou napodobit hlas nebo vzhled konkrétních osob, například výkonných manažerů, a přesvědčit zaměstnance k převodu peněz či sdílení citlivých informací. Tento typ útoku se stále častěji objevuje v rámci kompromitace firemní e-mailové komunikace (BEC – Business Email Compromise), kdy útočníci falšují e-maily nebo hlasové zprávy vedoucích pracovníků, aby oklamali podřízené a přiměli je k provedení podvodných transakcí. S rostoucí kvalitou deepfake technologií se tento druh útoku stává stále sofistikovanějším a obtížněji odhalitelným, což představuje vážnou hrozbu pro kybernetickou bezpečnost. (Macron, 2025)

Existuje několik variant phishingových útoků:

Spear phishing – cílený phishing, kdy útočník využívá informace o oběti k vytvoření personalizované zprávy.

Whaling – speciální forma spear phishingu zaměřená na vedoucí pracovníky a vysoce postavené osoby.

Clone phishing – útočník znovu odešle legitimní e-mail, ale nahradí původní odkazy nebo přílohy škodlivými verzemi. (Mandru, 2025)

Mezi nejčastější metody sociálního inženýrství patří:

Pretexting – metoda, při níž si útočník vymyslí důvěryhodný scénář (např. falešný pracovník IT podpory nebo bezpečnostní specialista) a pod touto identitou se snaží získat důvěrné informace. Tento typ útoku je často využíván při krádežích identity nebo finančních podvodech. (Gururaj et al., 2024)

Baiting – technika, při které útočník láká oběť na atraktivní návnadu, například zdarma nabízený software nebo falešné aktualizace, které ve skutečnosti obsahují škodlivý software. Tento typ útoku je běžně využíván ke stažení malwaru do systémů. (Gururaj et al., 2024)

Tailgating – metoda fyzického průniku do zabezpečených prostor, kdy útočník využívá lidské důvěřivosti. Například se vydává za zaměstnance bez přístupové karty a přesvědčí nic netušícího pracovníka, aby mu podržel dveře a umožnil vstup do budovy. (Gururaj et al., 2024)

1.2.5 Distributed Denial of Service útoky

DDoS (Distributed Denial of Service) útoky patří rovněž mezi nejrozšířenější kybernetické hrozby, jejichž cílem je přetížit cílový systém nebo síť tak, aby se staly nedostupnými pro legitimní uživatele. K tomuto účelu útočníci často využívají botnety, tedy sítě kompromitovaných zařízení, která hromadně zasílají požadavky na cílovou infrastrukturu. Moderní DDoS útoky navíc často využívají šifrovaný provoz nebo automatizované taktiky, které jim umožňují obejít tradiční obranné mechanismy. (Xu et al., 2025)

Podle Janabi et al. (2024) mají DDoS útoky mnoho podob, ale lze je rozdělit do tří hlavních kategorií: volumetrické útoky, protokolové útoky a aplikační útoky. Každý typ využívá odlišné techniky k narušení fungování cílové infrastruktury.

- **Volumetrické útoky**

Volumetrické DDoS útoky jsou nejčastější formou těchto útoků a jejich principem je zahlcení šířky pásma obrovským množstvím síťového provozu. Tento typ útoku využívá masivní objemy falešných datových paketů, které přetíží síťové linky, což vede k výpadku služeb

- **UDP Flood** – útočník zaplaví cílový server obrovským množstvím UDP paketů zaslaných na náhodné porty. Server je nucen odpovídat „nedostupnými“ zprávami, což vede k jeho vyčerpání.

- **DNS Amplification** – útočník využívá zranitelné DNS servery k zesílení útoku. Odesláním malého DNS dotazu s podvrženou IP adresou oběti získá násobně větší odpověď, čímž efektivně přetíží cílovou síť. (Janabi et al., 2024)

- **Protokolové útoky**

Tento typ DDoS útoků zneužívá slabiny síťových protokolů a způsobuje přetížení serverových nebo síťových zdrojů. Hlavní hrozbou těchto útoků jejich schopnost vyčerpávat omezené zdroje serveru, například tabulky připojení nebo procesorový výkon. Mezi nejznámější protokolové útoky patří:

- **SYN Flood** – útok zneužívá handshake mechanismus protokolu TCP. Útočník opakovaně posílá SYN požadavky na otevření spojení, ale nikdy jej nedokončí. Výsledkem je, že server udržuje neuzavřená připojení, dokud nevyčerpá všechny dostupné zdroje.
- **Ping of Death** – útočník zasílá nadměrně velké ICMP (ping) pakety, které při jejich sestavení na straně cílového systému způsobí přetečení vyrovnávací paměti a následné zhroucení systému. (Xu et al., 2025)

- **Aplikační útoky**

Aplikační útoky se zaměřují na specifické služby nebo aplikace a mají za cíl inaktivovat konkrétní aplikace, aniž by bylo nutné generovat velký objem síťového provozu. Tyto útoky bývají sofistikovanější a obtížněji detekovatelné, protože jejich provoz často napodobuje běžnou uživatelskou aktivitu. Mezi nejznámější aplikační útoky patří:

- **Slowloris** – tento útok otevírá velké množství nekompletních HTTP spojení, která server drží otevřená co nejdéle, dokud nevyčerpá dostupné připojovací sloty a neodmítne nové požadavky. Slowloris je extrémně efektivní proti webovým serverům, které neomezují maximální počet současných připojení.
- **Low Orbit Ion Cannon (LOIC)** – tento nástroj umožňuje útočníkům koordinovat útoky z velkého množství počítačů současně, přičemž vytváří obrovské množství síťových požadavků na cílový server, čímž jej vyřazuje z provozu. (Rakesh a Vasanthakumar, 2024)

1.2.6 Structured Query Language Injection útoky

SQL Injection je typ útoku využívající kritické zranitelnosti webových aplikací, která umožňuje útočníkům manipulovat s databázovými dotazy vložením škodlivého SQL kódu do vstupních polí aplikace. Tento typ útoku může vést k neoprávněnému přístupu k citlivým datům, jejich změně nebo smazání, a v některých případech dokonce k ovládnutí celého serveru. (Al-Araji, 2024)

SQL Injection útoky se obvykle dělí na klasický SQL Injection, Blind SQL Injection a Out-of-Band SQL Injection, přičemž každá metoda využívá jiný způsob interakce s databází. (Manjunatha a Shastry, 2024)

Klasický SQL Injection útok umožňuje přímou manipulaci s databází prostřednictvím nechráněného vstupu, zatímco Blind SQL Injection nevrací přímé chyby, ale útočník postupně zjišťuje strukturu databáze pomocí logických podmínek. Out-of-Band SQL Injection je méně častá technika, která využívá externí kanály, jako jsou DNS nebo HTTP požadavky, k extrakci dat. (Sree et al., 2024)

1.2.7 Zero-Day útoky

Zero-Day útoky patří mezi velmi nebezpečné kybernetické hrozby, protože zneužívají dosud neznámé zranitelnosti v softwaru, které vývojáři ještě nestihli opravit. Útočníci tak mohou získat přístup k systémům, provádět vzdálené exekuce kódů nebo obejít bezpečnostní opatření. Zero-day zranitelnosti jsou často využívány sofistikovanými kyberzločineckými skupinami s cílem ohrožit vládní instituce, korporace, ale i běžné uživatele, přičemž odhalení a mitigace bývají velmi složité. (Gritzalis et al., 2024)

1.2.8 Advanced Persistent Threats

Advanced Persistent Threats (APT) označují dlouhodobé cílené kybernetické útoky, které jsou často financované jednotlivými státy nebo sofistikovanými kybernetickými skupinami. Cílem těchto útoků je proniknout do vybraného systému, zůstat v něm co nejdéle skrytý a systematicky sbírat citlivé informace nebo provádět sabotážní akce. (Aggrey et al., 2025)

Mohamed (2024) uvádí, že APT útoky se vyznačují pečlivým plánováním, využitím zero-day zranitelností a kombinací různých technik, jako je phishing, malware nebo laterální pohyb v síti.

APT útoky obvykle probíhají v několika fázích, od počátečního průniku přes eskalaci oprávnění až po dlouhodobé sledování a vynášení dat. Historicky byly APT útoky spojovány s významnými incidenty, jako byly útoky na vládní infrastrukturu, energetické sítě nebo velké korporace. Obrana proti APT útokům vyžaduje pokročilé bezpečnostní strategie, včetně behaviorální analýzy, aktivního monitorování sítě a segmentace kritických systémů. (Selmanaj, 2024)

1.2.9 Internet of Things útoky

Internet věcí (IoT, Internet of Things) zahrnuje širokou škálu zařízení připojených k internetu, od chytrých domácích spotřebičů po průmyslové senzory a zdravotnické přístroje. Vzhledem k jejich propojení a časté absenci robustních bezpečnostních opatření se IoT zařízení stávají cílem kybernetických útoků (Abbadi, 2025).

Hatamleh et al. (2025) upozorňují, že hlavními hrozbami jsou malware (např. Mirai botnet), útoky typu Man-in-the-Middle (MitM), únosy zařízení (device hijacking) a zneužití zranitelností v nedostatečně aktualizovaném firmwaru.

Vzhledem k neustálému nárůstu IoT zařízení a jejich využití v kritických infrastrukturách, jako jsou zdravotnictví, doprava a energetika, je jejich zabezpečení klíčovým tématem kybernetické bezpečnosti. Jednou z nejefektivnějších obran proti IoT útokům je implementace síťové segmentace, šifrování dat a pravidelná aktualizace softwaru. (Gupta et al., 2025)

1.2.10 Deepfake

Deepfake technologie představují pokročilou formu syntetických médií vytvářených pomocí umělé inteligence, zejména hlubokých neuronových sítí. Podle Wazida et al. (2024) se jedná o metodu, která využívá generativní adversariální sítě k manipulaci s obrazovým nebo zvukovým obsahem tak, že výsledný materiál působí autenticky. Neekhara et al. (2021) definují deepfake jako synteticky generovaný obsah, jehož cílem je napodobit skutečné osoby nebo události s vysokou mírou realističnosti, což ho činí potenciálně nebezpečným v oblasti kybernetické bezpečnosti a šíření dezinformací. Pantserev (2020) upozorňuje na to, že deepfake technologie nejsou využívány pouze k neškodné zábavě, ale mohou být i záměrně zneužity k ovlivňování veřejného mínění nebo k podvodnou útočnou manipulaci identity.

Deepfake technologie se nejčastěji využívají k podvodům, manipulaci s veřejným míněním a narušování osobní a národní bezpečnosti. (Wazid et al., 2024) Podle Pantsereva (2020) mohou deepfake videa posloužit jako nástroj pro psychologickou válku a šíření propagandy, například v politických kampaních nebo ve vojenském konfliktu.

Aby bylo možné deepfake obsah účinně odhalovat, navrhuji odborníci různé obranné strategie. Wazid et al. (2024) doporučují využití strojového učení a umělé inteligence k detekci anomálií ve videích a zvukových záznamech, zatímco Neekhara et al. (2021) upozorňují na potřebu robustnějších modelů odolných vůči adversariálním útokům, kdy útočníci modifikují videa tak, aby zůstala nerozpoznatelná pro detekční algoritmy. V současnosti se využívají technologie jako forenzní analýza metadat, detekce nepřirozeného pohybu rtů a zvýšená kontrola důvěryhodnosti mediálního obsahu. (Neekhara et al., 2021)

2 PRÁVNÍ RÁMEC A MEZINÁRODNÍ NORMY

Tato kapitola se zaměřuje na právní rámec kybernetické bezpečnosti a související legislativní normy. V první části bude rozebrána česká legislativa a národní strategie kybernetické bezpečnosti, včetně klíčových zákonů upravujících oblast kybernetické bezpečnosti, ochrany osobních údajů a trestní odpovědnosti za kybernetickou kriminalitu, následně budou stručně představeny mezinárodní normy ISO/IEC 27000, které definují standardy pro řízení bezpečnosti informací. Závěrečná část se zaměří na mezinárodní legislativu, včetně evropských regulací, jako jsou AI Act, NIS 2 a GDPR v kontextu kybernetické bezpečnosti.

2.1 Česká legislativa a Národní strategie kybernetické bezpečnosti

Tato subkapitola se zabývá legislativním rámcem ve vztahu ke kybernetické bezpečnosti v České republice. Zaměřuje se na české klíčové právní předpisy a dále pak na Národní strategii kybernetické bezpečnosti ČR 2021-2025.

2.1.1 Zákon o kybernetické bezpečnosti (č. 181/2014 Sb.)

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, je základním právním rámcem pro ochranu informačních systémů a kritické infrastruktury v České republice. Hlavním cílem zákona je zajištění bezpečnosti digitální infrastruktury, ochrana veřejných i soukromých subjektů před kybernetickými hrozbami a zajištění kontinuity služeb nezbytných pro fungování státu. (Česko, 2014)

Působnost zákona a vymezení subjektů

Zákon se vztahuje na několik kategorií subjektů, jejichž informační systémy jsou klíčové pro fungování státu a ekonomiky. Mezi ně patří:

- Orgány veřejné moci, zejména ministerstva, úřady a další státní instituce.
- Provozovatelé kritické informační infrastruktury, tedy organizace z oblastí energetiky, zdravotnictví, dopravy nebo finančního sektoru, jejichž systémy jsou nezbytné pro fungování státu.
- Poskytovatelé základních služeb, například vodárny, elektrárny či dopravní systémy, jejichž výpadek by mohl mít závažný dopad na společnost.
- Poskytovatelé digitálních služeb, jako jsou cloud computing, internetové platformy nebo online tržiště, které hrají klíčovou roli v digitální ekonomice (Česko, 2014)

Zákon stanovuje dvě hlavní kategorie bezpečnostních opatření – organizační a technická. (Česko, 2014)

Organizační opatření

Organizační opatření se zaměřují na řízení procesů souvisejících s kybernetickou bezpečností, nastavení pravidel a odpovědností v rámci organizace a školení zaměstnanců. Jedním z klíčových požadavků je zavedení bezpečnostní politiky, která musí jasně definovat pravidla pro ochranu informačních systémů a řízení přístupu k citlivým údajům. Tato politika zahrnuje také řízení rizik, což znamená pravidelné vyhodnocování zranitelností a implementaci opatření k jejich minimalizaci. Organizace musí být schopné dokumentovat a prokazatelně aplikovat procesy zaměřené na kybernetickou ochranu. Dalším důležitým aspektem je řízení přístupových práv, tedy definování toho, kdo může přistupovat k určitým informačním systémům a jakým způsobem. To zahrnuje jak autentizaci uživatelů, tak i omezení přístupů na základě funkčních rolí v organizaci. (Česko, 2014)

Zákon rovněž ukládá povinnost školit zaměstnance v oblasti kybernetické bezpečnosti. To je klíčové zejména proto, že lidský faktor je stále jedním z nejslabších článků v oblasti informační bezpečnosti. Zaměstnanci musí být pravidelně informováni o aktuálních kybernetických hrozbách, metodách sociálního inženýrství a správném nakládání s citlivými daty. (Česko, 2014)

Technická opatření

Technická opatření mají za cíl přímou ochranu systémů a dat před kybernetickými útoky. Patří mezi ně implementace bezpečnostních technologií a pravidelný monitoring infrastruktury. Jedním z klíčových prvků je monitorování síťového provozu a detekce anomálií. Subjekty musí zavést nástroje pro sledování provozu, které dokážou detekovat neobvyklé aktivity a potenciální hrozby. Tato opatření pomáhají včasné identifikovat například pokusy o průnik do systému nebo šíření malwaru. (Česko, 2014)

Dalším zásadním opatřením je řízení přístupu k systémům a datům. To zahrnuje nejen správu uživatelských účtů a přístupových oprávnění, ale také nasazení vícefaktorové autentizace (MFA), která snižuje riziko neoprávněného přístupu. (Česko, 2014)

Zákon rovněž vyžaduje použití šifrování pro ochranu citlivých dat. Šifrování se používá jak pro uchovávaná data, tak pro přenos. Tím je zajištěno, že i v případě úniku informací nejsou tato data snadno čitelná. (Česko, 2014)

Kromě toho je nutné nasazení firewallů a antivirové ochrany, které poskytují první linii obrany proti kybernetickým útokům. Firewally slouží k filtrování síťového provozu a blokování nežádoucí komunikace, zatímco antivirové programy detekují a eliminují škodlivý software. Důležitým technickým opatřením je také zálohování dat a plán obnovy po incidentu. Organizace musí mít zavedené pravidelné zálohování klíčových dat a zároveň vypracovaný plán pro jejich obnovu v případě kybernetického útoku nebo jiného narušení provozu. (Česko, 2014)

Hlášení incidentů a role CSIRT a CERT týmů

Jedním z klíčových bodů zákona je povinnost hlásit kybernetické bezpečnostní incidenty, a to prostřednictvím specializovaných týmů CSIRT (Computer Security Incident Response Team) a CERT (Cyber Emergency Response Team). (Česko, 2014)

CSIRT týmy se zaměřují především na monitorování kybernetických hrozeb, prevenci útoků a poskytování metodické podpory organizacím. Hrají důležitou roli v analýze bezpečnostních incidentů, vydávání doporučení a spolupráci s dalšími bezpečnostními složkami na národní i mezinárodní úrovni. V České republice tuto roli zastává NÚKIB jako hlavní národní CSIRT tým. (Česko, 2014)

Na druhé straně, CERT týmy mají primárně reaktivní roli, tedy se zaměřují na přijímání hlášení o kybernetických incidentech, jejich vyhodnocování a poskytování podpory při jejich řešení. Kromě samotné reakce na incidenty hrají roli i v koordinaci opatření ke zmírnění jejich dopadu. V České republice tuto funkci plní vládní CERT tým (GovCERT.CZ), který je zodpovědný za kybernetickou bezpečnost státních institucí a kritické infrastruktury. (Česko, 2014)

Hlavní rozdíl mezi těmito týmy tedy spočívá v jejich zaměření – CSIRT týmy jsou orientované na prevenci, analýzu a koordinaci, zatímco CERT týmy se specializují na okamžitou reakci a řešení kybernetických incidentů. Přestože mají odlišné úkoly, oba typy týmů spolupracují s cílem zajistit vyšší úroveň kybernetické bezpečnosti a efektivně chránit digitální infrastrukturu České republiky. (Česko, 2014)

Zákon stanovuje, že orgány a osoby spadající pod jeho působnost musí bezodkladně po jejich detekci nahlásit kybernetické bezpečnostní incidenty Národnímu úřadu pro kybernetickou a informační bezpečnost (NÚKIB), který koordinuje řešení incidentů na státní úrovni. (Česko, 2014)

2.1.2 Zákon o zpracování osobních údajů (č. 110/2019 Sb.)

Zákon č. 110/2019 Sb. je zásadním právním rámcem, který upravuje ochranu osobních údajů v České republice a zároveň implementuje evropské nařízení GDPR. Tento zákon stanovuje pravidla pro zpracování osobních údajů, definuje povinnosti správců a zpracovatelů dat, a upravuje pravomoci Úřadu pro ochranu osobních údajů (ÚOOÚ), který zajišťuje dohled nad dodržováním legislativy. (Česko, 2019)

Podle Bočánka et al. (2024) má tento právní rámec zásadní vliv na oblast kybernetické bezpečnosti, protože reguluje využití automatizovaných nástrojů pro detekci a analýzu bezpečnostních incidentů. Zvláštní důraz je kladen na umělou inteligenci, která umožňuje rychlejší a efektivnější identifikaci kybernetických hrozeb, avšak její nasazení je omezeno požadavkem na transparentnost a lidský dohled.

Jedním z klíčových požadavků zákona je zajištění kybernetické bezpečnosti při zpracování osobních údajů. Správci a zpracovatelé dat mají povinnost zavést adekvátní technická a organizační opatření, která zabrání neoprávněnému přístupu, úniku nebo zneužití dat. Podle Vostoupala et al. (2024) se tato pravidla stávají ještě přísnějšími s příchodem směrnice NIS 2, která zpřísňuje požadavky na bezpečnost informačních systémů a zvyšuje odpovědnost organizací za případné narušení ochrany dat. (Vostoupal et al., 2024)

V případě závažného bezpečnostního incidentu mají organizace povinnost hlásit narušení zabezpečení osobních údajů do 72 hodin Úřadu pro ochranu osobních údajů (ÚOOÚ). Jak uvádí Dušek (2023), tato povinnost klade vysoké nároky na podniky a státní instituce, které musejí zajistit kontinuální monitoring a rychlou reakci na bezpečnostní hrozby.

Zákon také stanovuje pravidla pro automatizované zpracování osobních údajů, včetně využití umělé inteligence. AI systémy nesmějí automaticky rozhodovat o subjektech údajů, pokud nedošlo k výslovnému souhlasu nebo pokud to není nutné pro výkon smlouvy či zákonné povinnosti. Tato omezení podle Polčáka et al. (2023) představují výzvu pro nasazení AI v kybernetické bezpečnosti, protože omezený přístup k datům může snížit účinnost bezpečnostních systémů.

2.1.3 Návrh nového zákon o kybernetické bezpečnosti

Nový zákon o kybernetické bezpečnosti, jehož návrh byl schválen dne 17. července 2024 a vstup v platnost se očekává nejdříve v polovině roku 2025, představuje modernizaci oproti původnímu zákonu 181/2014 Sb., o kybernetické bezpečnosti. Reaguje na nové hrozby

v kyberprostoru, rozvoj digitálních služeb a požadavky evropské směrnice NIS2, která zavádí přísnější pravidla pro členské státy EU. Hlavní změnou je rozšíření působnosti zákona na větší počet subjektů, podrobnější pravidla pro dodavatele a přesnější mechanismy hlášení kybernetických incidentů. Původní zákon 181/2014 Sb. se zaměřoval primárně na ochranu informačních systémů státní správy a kritické infrastruktury, zatímco nový zákon se vztahuje také na soukromé subjekty, které poskytují klíčové služby. Definuje pojem regulovaná služba, pod kterou spadají nejen vládní instituce, ale také energetické, finanční, zdravotnické a dopravní podniky, poskytovatelé cloudových a IT služeb, online platformy a další klíčové odvětví. Nová legislativa zavádí přísnější bezpečnostní opatření pro regulované subjekty a detailněji rozlišuje dva režimy povinností – vyšší a nižší. Také zpřísňuje sankce a stanovuje nové požadavky na dodavatele kybernetických služeb. (NÚKIB, 2025)

Tabulka 1 popisuje nejzásadnější změny ve znění stávajícího zákona č. 181/2014 Sb., o kybernetické bezpečnosti, a v návrhu Nového zákona o kybernetické bezpečnosti.

Tabulka 1 Hlavní rozdíly mezi zákonem č. 181/2014 Sb., a návrhem nového zákona o kybernetické bezpečnosti

Oblast	Zákon 181/2014 Sb.	Návrh nového zákona o kybernetické bezpečnosti
Předmět úpravy	Ochrana informačních a komunikačních systémů veřejné správy, kritické infrastruktury a digitálních služeb	Rozšířeno na soukromé subjekty a větší množství regulovaných služeb podle NIS2
Regulované subjekty	Orgány veřejné moci, kritická informační infrastruktura, poskytovatelé digitálních služeb	Střední a velké podniky v sektorech jako energetika, zdravotnictví, doprava, výroba, bankovníctví, poštovní služby, věda a výzkum, online platformy
Pojem „regulovaná služba“	Není definováno, ale existuje pojem „kritická informační infrastruktura“ a „základní služba“	Nově zavádí pojem „regulovaná služba“, kterou určuje NÚKIB a která má významný dopad na ekonomiku a bezpečnost ČR
Bezpečnostní opatření	Organizační a technická opatření pouze pro kritickou infrastrukturu a vybrané digitální služby	Podrobnější opatření včetně povinnosti bezpečnostních auditů, řízení rizik a přísnější kontroly dodavatelů
Hlášení incidentů	Povinnost hlášení pouze pro kritickou infrastrukturu, ale bez přesně daných lhůt	Přesně stanovené lhůty: prvotní hlášení do 24 hodin, podrobnější hlášení do 72 hodin

Dodavatelé IT služeb	Minimální regulace dodavatelů	Přísnější kontrola dodavatelů, nutnost zahrnout bezpečnostní požadavky do smluv
Přizpůsobení evropské legislativě	Částečně vychází ze starších směrnic EU	Implementuje směrnici NIS2 a další předpisy EU
Sankce za nedodržení	Opatření spíše administrativního charakteru, méně přísná vymáhání	Vyšší sankce, možnost pozastavení služeb, přísnější kontrola dodržování zákona
Režimy povinností	Všechny subjekty mají víceméně stejné požadavky	Dva režimy: Vyšší: povinnosti pro strategické subjekty Nižší: povinnosti pro méně významné poskytovatele
Role NÚKIB	Dohled nad kritickou infrastrukturou a bezpečnostní politikou státu	Posílené pravomoci NÚKIB, může určovat regulované subjekty, provádět audity a vyhlášovat bezpečnostní opatření

(zdroj: NÚKIB, 2025, vlastní zpracování)

2.1.4 Trestní zákoník (č. 40/2009 Sb.)

Trestní zákoník č. 40/2009 Sb. je základním právním předpisem určujícím skutkové podstaty trestných činů a jejich sankcionování. Kyberkriminalita představuje specifickou oblast trestního práva, která se zaměřuje na zneužívání informačních technologií k páchání trestné činnosti. Tento typ kriminality zahrnuje široké spektrum jednání, jako je neoprávněný přístup k počítačovým systémům, kybernetické podvody či zneužití osobních údajů. (Česko, 2009)

Klíčová ustanovení trestního zákoníku týkající se kyberkriminality

Český trestní zákoník obsahuje několik ustanovení, která se vztahují ke kybernetické trestné činnosti:

§ 230 – Neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací

Tento paragraf se zaměřuje na neoprávněné získání přístupu k počítačovému systému nebo jeho části překonáním bezpečnostních opatření. Takové jednání je trestáno odnětím svobody až na dva roky, zákazem činnosti nebo propadnutím věci. Dále postihuje neoprávněné užití, vymazání, zničení, změnu nebo padělání dat uložených v počítačovém systému či na nosiči

informací. Rovněž zahrnuje neoprávněné vložení nebo přenos dat do systému nebo jiný zásah do programového a technického vybavení počítačového systému. Za tyto činy hrozí trest odnětí svobody až na tři roky. V případě, že je čin spáchán s úmyslem způsobit škodu, získat neoprávněný prospěch nebo narušit funkčnost systému, může být trest zvýšen na šest měsíců až čtyři roky. Pokud pachatel čin spáchá jako člen organizované skupiny nebo způsobí značnou škodu, trestní sazba se může zvýšit až na osm let. (Česko, 2009)

§ 231 – Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

Tento paragraf postihuje neoprávněné nakládání s nástroji umožňujícími přístup k počítačovým systémům. Trestá se výroba, distribuce, dovoz, vývoz nebo přechovávání zařízení, programů nebo hesel, které mohou být zneužity k neoprávněnému přístupu nebo zásahu do počítačového systému. Trestní sazba činí až dvě léta odnětí svobody, propadnutí věci nebo zákaz činnosti. Pokud je čin spáchán organizovanou skupinou nebo pokud pachatel získá značný prospěch, může být trest zvýšen až na tři léta, případně až na pět let v případě velkého rozsahu prospěchu. (Česko, 2009)

§ 232 – Neoprávněný zásah do počítačového systému nebo nosiče informací z nedbalosti

Tento paragraf upravuje situace, kdy pachatel z hrubé nedbalosti poruší povinnost vyplývající ze svého zaměstnání, povolání, funkce nebo smluvně převzaté odpovědnosti, a tím způsobí škodu na cizím majetku. Pokud například zaměstnanec IT oddělení neúmyslně smaže nebo poškodí důležitá data, čímž způsobí značnou škodu, může mu hrozit trest odnětí svobody až na šest měsíců, zákaz činnosti nebo propadnutí věci. Pokud čin způsobí škodu velkého rozsahu, trestní sazba může vzrůst až na dvě léta. (Česko, 2009)

§ 234 – Neoprávněné opatření, padělání a pozměnění platebního prostředku

Tento paragraf se vztahuje na neoprávněné nakládání s platebními prostředky, což zahrnuje jak fyzické platební karty, tak digitální platební prostředky a virtuální aktiva používaná k převodu peněz. Trestný čin podle tohoto paragrafu zahrnuje neoprávněné opatření, zpřístupnění, přijetí nebo přechovávání cizího platebního prostředku bez souhlasu jeho oprávněného uživatele, přičemž za takové jednání hrozí trest odnětí svobody až na dvě léta, zákaz činnosti nebo propadnutí věci. Pokud pachatel sobě nebo jinému opatří padělaný nebo pozměněný platební prostředek, může být potrestán odnětím svobody na jeden až pět let. Padělání nebo pozměnění platebního prostředku s úmyslem jeho použití jako pravého je považováno za závažnější trestný čin, za který lze uložit trest odnětí svobody od tří do osmi

let. Pokud je tento čin spáchán organizovanou skupinou nebo ve značném rozsahu, trestní sazba se pohybuje mezi pěti až deseti lety odnětí svobody nebo může být uloženo propadnutí majetku. V případech, kdy pachatel působí v organizované skupině ve více státech nebo je rozsah činu velký, se trest pohybuje mezi osmi až dvanácti lety odnětí svobody nebo propadnutím majetku. (Česko, 2009)

2.1.5 Problémy a výzvy spojené s trestní odpovědností v oblasti kyberkriminality

Trestní odpovědnost v oblasti kyberkriminality naráží na několik zásadních problémů, které vyplývají z povahy kybernetického prostředí a jeho globálního dosahu. Níže jsou rozpracovány klíčové výzvy, se kterými se orgány činné v trestním řízení, zákonodárci a soudy potýkají při vyšetřování, stíhání a trestání pachatelů kyberkriminálních činů.

Obtížnost identifikace pachatelů a digitální anonymita

Jedním z největších problémů je anonymita pachatelů, která je v kyberprostoru snadno dosažitelná. Použití anonymizačních nástrojů, jako jsou VPN, Tor, proxy servery nebo darknet, umožňuje zločincům skrýt svou identitu a maskovat skutečné místo působení. Kyberzločinci navíc využívají sofistikované techniky, jako je IP spoofing nebo přesměrování datových toků přes několik jurisdikcí, což ztěžuje jejich vystopování. Výzkumy ukazují, že až 60 % kybernetických trestných činů není nikdy objasněno. Orgány činné v trestním řízení často nemají dostatečné prostředky nebo technologické know-how k prolomení těchto ochranných mechanismů, což vede k nízké míře objasněnosti kybernetických deliktů. (Ajayi, 2016)

Jurisdikční problémy a mezinárodní povaha kyberkriminality

Kyberkriminalita je typická tím, že její pachatelé, oběti i samotná infrastruktura mohou být rozptýleny po celém světě. Například hacker v Rusku může napadnout server ve Spojených státech, přičemž škoda vznikne uživateli v Evropské unii. To způsobuje komplikace při určení právní jurisdikce, která by měla případ řešit. Mezinárodní spolupráce v této oblasti je často pomalá a neefektivní kvůli rozdílným právním rámcům jednotlivých států. Budapešťská úmluva o kyberkriminalitě (2001) sice vytvořila základ pro mezinárodní spolupráci, avšak řada států, včetně Ruska a Číny, k ní nepřistoupila, což brání efektivnímu přeshraničnímu stíhání pachatelů. (Brenner, 2012)

Nedostatek digitálních důkazů a jejich volatilita

Digitální důkazy jsou na rozdíl od fyzických důkazů velmi nestálé – mohou být rychle smazány, změněny nebo zašifrovány. Hackeri často používají techniky jako disk wiping, šifrování dat či samo-destruktivní malware, které eliminují jakékoliv důkazy o jejich činnosti. Navíc sběr digitálních důkazů vyžaduje specializované forenzní technologie a experty, kteří musí zajistit, že důkazy budou soudně uznatelné. Tento proces je časově i finančně náročný, a proto mnoho menších policejních útvarů nemá odpovídající vybavení ani školení pro analýzu kyberzločinců. (Koops, 2012)

Automatizované a umělou inteligencí řízené kyberútoky

S rozvojem umělé inteligence se objevují automatizované kyberútoky, které nevyžadují přímou kontrolu člověka. AI-driven útoky mohou například automaticky hledat zranitelnosti v systémech, generovat sofistikované phishingové zprávy nebo provádět deepfake podvody. V těchto případech může být obtížné přisoudit odpovědnost konkrétní osobě. Například, pokud AI systém autonomně provede útok bez přímého příkazu svého operátora, vzniká otázka, kdo by měl být právně odpovědný – vývojář softwaru, provozovatel serveru, nebo někdo jiný? (Oreku a Mtenzi, 2017)

Technologická propast mezi pachateli a vyšetřovateli

Kyberzločinci často využívají nejnovější technologie, zatímco policejní složky za nimi výrazně zaostávají. Podle výzkumu Hewese (2016) má méně než 40 % vyšetřovatelů odpovídající technické vzdělání, aby mohli efektivně bojovat s kyberkriminalitou. Nedostatek odborně proškolených specialistů vede k tomu, že vyšetřování kybernetických trestných činů trvá výrazně déle než u běžné kriminality. Navíc je nutné, aby orgány činné v trestním řízení spolupracovaly s technologickými firmami a poskytovateli internetových služeb, což však naráží na otázky ochrany soukromí a právní odpovědnosti těchto společností.

2.1.6 Národní strategie kybernetické bezpečnosti ČR 2021-2025

Národní strategie kybernetické bezpečnosti České republiky 2021–2025 je základním koncepčním dokumentem, který vymezuje dlouhodobý přístup státu k zajištění kybernetické bezpečnosti. Strategie vychází ze současných bezpečnostních hrozeb, vývoje informačních a komunikačních technologií a mezinárodních závazků České republiky. Jejím hlavním cílem je zajistit odolnost digitální infrastruktury, zvýšit spolupráci mezi klíčovými subjekty

a vytvořit efektivní mechanismy ochrany proti kybernetickým útokům. Dokument je koncipován na základě tří strategických vizí a jejich implementaci zajišťuje Akční plán pro období 2021–2025, který konkretizuje jednotlivé kroky vedoucí k realizaci strategických cílů. (NÚKIB, 2020)

Hlavní cíle a vize

Strategie je strukturována do tří základních vizí, které vymezují dlouhodobý přístup České republiky ke kybernetické bezpečnosti:

- **Sebevědomě v kyberprostoru**

Hlavním cílem této oblasti je posílit schopnost detekce a reakce na kybernetické hrozby a vytvořit efektivní obranný mechanismus pro digitální infrastrukturu státu. Strategie v tomto směru podporuje rozvoj analytických kapacit a nástrojů, které umožní včasnou identifikaci kybernetických útoků a minimalizaci jejich dopadů. Součástí této vize je také posílení strategické komunikace o kybernetických hrozbách mezi státní správou, soukromým sektorem a občany. (NÚKIB, 2020)

- **Silná a spolehlivá spojení**

Vzhledem k mezinárodní povaze kybernetických hrozeb klade strategie důraz na aktivní zapojení České republiky do globálních bezpečnostních struktur, včetně EU, NATO, OSN a OECD. Strategie zdůrazňuje nutnost mezinárodní spolupráce při sdílení informací o kybernetických incidentech, vytváření společných obranných opatření a zvyšování bezpečnostní spolupráce s technologickými firmami a akademickými institucemi. (NÚKIB, 2020)

- **Odolná společnost 4.0**

Tato oblast se zaměřuje na zvýšení kybernetické gramotnosti obyvatel a odborníků. Strategie podporuje rozvoj vzdělávacích programů a školení, jejichž cílem je posílit bezpečnostní povědomí veřejnosti a odborné kompetence v oblasti kybernetické bezpečnosti. Zahrnuje také podporu výzkumu a inovací, které přispějí k dalšímu rozvoji obranných mechanismů proti kybernetickým útokům. (NÚKIB, 2020)

Způsob implementace Strategie (Akční plán 2021–2025)

Implementace strategie je konkrétně rozpracována v Akčním plánu pro období 2021–2025, který stanovuje praktické kroky k dosažení jednotlivých strategických cílů. Tento dokument rozděluje implementační opatření do několika klíčových oblastí. (NÚKIB, 2021)

Strategie zdůrazňuje potřebu úzké spolupráce mezi klíčovými aktéry kybernetické bezpečnosti. Akční plán proto obsahuje opatření pro vytvoření bezpečné platformy pro sdílení informací o kybernetických hrozbách mezi státní správou, bezpečnostními složkami a soukromým sektorem. V rámci této oblasti se plánuje také zlepšení koordinace mezi orgány státní správy při řešení kybernetických incidentů. (NÚKIB, 2021)

Dalším klíčovým bodem implementace je modernizace technických kapacit pro boj s kybernetickými hrozbami. Akční plán zahrnuje opatření jako pravidelné penetrační testování kritických informačních systémů, posílení detekčních systémů pro monitoring síťového provozu a zavádění automatizovaných obranných mechanismů využívajících umělou inteligenci. (NÚKIB, 2021)

2.2 ISO/IEC 27000 Family

Tato subkapitola stručně pojednává o „rodině“ norem ISO/IEC 27000, která představuje soubor mezinárodních standardů zaměřených na řízení informační bezpečnosti (ISMS – Information Security Management System). Zajišťují systematický přístup k ochraně informací na základě identifikace rizik a zavedení odpovídajících bezpečnostních opatření. (Disterer, 2013)

2.2.1 ISO/IEC 27001

ISO/IEC 27001 je základní norma definující požadavky na zavedení, provoz a neustálé zlepšování systému řízení bezpečnosti informací (ISMS), přičemž jako jediná z rodiny umožňuje oficiální certifikaci. (Gillies, 2011)

Mezi klíčové prvky patří nastavení bezpečnostních politik, ochrana informačních aktiv, řízení přístupu, zvládání bezpečnostních incidentů a průběžné vyhodnocování účinnosti opatření. Certifikace podle této normy přispívá k posílení důvěry zainteresovaných stran. (Disterer, 2013)

2.2.2 ISO/IEC 27002

Norma ISO/IEC 27002 poskytuje praktické pokyny pro výběr a implementaci bezpečnostních opatření v souladu s ISO/IEC 27001. Zaměřuje se na řízení přístupu, šifrování, detekci a reakci na incidenty či bezpečnost cloudových řešení. Ačkoli není certifikovatelná, slouží jako důležitý podpůrný dokument při zavádění ISMS. (Calder, 2024)

2.2.3 ISO/IEC 27005

ISO/IEC 27005 se orientuje na řízení rizik informační bezpečnosti. Nabízí rámec pro identifikaci aktiv, analýzu hrozeb a zranitelností, hodnocení dopadů a návrh opatření ke zmírnění rizik. Norma neukládá konkrétní metodiku, ale poskytuje strukturovaný proces pro tvorbu efektivní strategie řízení rizik. (Faris et al., 2014)

2.3 Mezinárodní legislativa

Tato subkapitola se zabývá mezinárodním legislativním rámcem ve vztahu ke kybernetické bezpečnosti, přičemž se zaměřuje na klíčové právní předpisy regulující digitální prostředí v Evropské unii. Pozornost je věnována AI Act, který stanovuje pravidla pro vývoj a nasazení systémů umělé inteligence s důrazem na bezpečnostní rizika, směrnici NIS 2, která harmonizuje kybernetickou bezpečnost kritických a digitálních infrastruktur v členských státech, a vztahu GDPR k ochraně osobních údajů v kontextu kybernetických hrozeb.

2.3.1 Nařízení Evropského parlamentu a Rady (EU) 2024/1689

Nařízení Evropského parlamentu a Rady (EU) 2024/1689, známé jako „AI Act“ je první komplexní legislativní rámec Evropské unie zaměřený na regulaci systémů umělé inteligence. Jeho hlavním cílem je zajistit bezpečné, etické a odpovědné využívání AI v souladu s hodnotami EU, jako jsou ochrana základních práv, demokracie, právního státu a ochrany životního prostředí (Evropská unie, 2024). Tento akt byl formálně schválen Evropským parlamentem 13. června 2024 a představuje horizontální legislativu, což znamená, že se vztahuje na všechny sektory a odvětví využívající AI. (Butt, 2024)

AI Act stanovuje harmonizovaná pravidla pro vývoj, uvádění na trh a používání systémů AI v EU, přičemž klade důraz na důvěryhodnou umělou inteligenci zaměřenou na člověka. Zavádí rovněž mechanismy dohledu a vymáhání pravidel, včetně přísnějších požadavků na vysoce rizikové AI systémy a odpovědnosti vývojářů a provozovatelů AI. (Myklebust et al., 2025)

AI Act je inspirován definicí AI přijatou Organizací pro hospodářskou spolupráci a rozvoj (OECD). Zahrnuje systémy AI, které pracují s různou mírou autonomie a zpracovávají vstupní data za účelem generování výstupů, jako jsou predikce, obsah, doporučení nebo rozhodnutí, jež mohou ovlivnit fyzické nebo virtuální prostředí. (Butt, 2024)

Klasifikace systémů AI podle rizika

AI Act definuje čtyři úrovně rizika na základě dopadu na bezpečnost, základní práva a veřejný pořádek. Každá kategorie má specifické regulační požadavky:

Nepřijatelné riziko

Nejvyšší úroveň rizika představují AI systémy, které jsou považovány za nepřijatelné, protože ohrožují základní práva a svobody. Mezi zakázané praktiky patří:

- Sociální scoring inspirovaný čínským modelem, kdy je chování občanů sledováno a vyhodnocováno na základě různých kritérií
- Manipulativní AI, která využívá podprahové techniky k ovlivnění rozhodování uživatelů
- Vzdálená biometrická identifikace v reálném čase pro účely vymáhání práva (s výjimkami pro velmi specifické případy, např. teroristické útoky)
- Manipulativní AI systémy, které mohou vést k fyzické nebo psychické újmě jednotlivců
- Systémy, které využívají zranitelnosti lidí (např. děti nebo osoby se zdravotním postižením) k ovlivnění jejich rozhodování (Evropská unie, 2024)

Vysoké riziko

Druhou kategorií jsou vysoce rizikové AI systémy, které mohou mít významný dopad na zdraví, bezpečnost nebo základní práva občanů. Mezi vysoce rizikové systémy patří AI používaná v:

- Kritické infrastruktury (např. doprava, energetika)
- Vzdělávání (např. systémy pro hodnocení studentů)
- Zaměstnání a HR (automatizované rozhodování o náboru nebo propouštění)
- Přístupu k základním službám (např. kreditní scoring, zdravotnictví)
- Prosazování práva (např. prediktivní policejní systémy)
- Migraci a hraniční kontrole (např. detekce lživých výpovědí žadatelů o azyl)
- Spravedlnosti a demokratických procesech (např. automatizované rozhodování soudů) (Evropská unie, 2024)

Omezené riziko

Do této kategorie spadají AI systémy, které nevyžadují striktní regulaci, ale musí být transparentní. Příklady zahrnují:

- Chatboti a generativní AI – uživatelé musí být jasně informováni, že komunikují s AI.
- Automatizované doporučovací systémy – například algoritmy personalizovaného obsahu na sociálních sítích.

Pro tyto systémy AI Act stanovuje hlavně požadavky na transparentnost a ochranu před zneužitím. (Evropská unie, 2024)

Minimální nebo žádné riziko

Sem spadají AI systémy, které nejsou považovány za potenciálně nebezpečné a nepodléhají žádným zvláštním regulacím. Jde například o:

- Spam filtry
- AI v počítačových hrách
- Automatizovaní asistenti v chytrých domácnostech. (Evropská unie, 2024)

2.3.2 Směrnice Evropského parlamentu a Rady (EU) 2022/2555

Směrnice Evropského parlamentu a Rady (EU) 2022/2555, známá jako NIS 2, byla přijata s cílem posílit kybernetickou bezpečnost v Evropské unii. Směrnice nahrazuje původní regulaci NIS (2016/1148) a zavádí jednotný rámec kybernetické bezpečnosti napříč členskými státy EU. Rozšiřuje působnost na širší spektrum subjektů, které nově zahrnují nejen provozovatele základních služeb, ale i digitální poskytovatele, jako jsou cloudové platformy, sociální sítě či online tržiště. Organizace jsou rozděleny na „základní“ a „důležité“ subjekty s odlišnou mírou dohledu a sankcí. Subjekty musí zavést komplexní opatření pro řízení kybernetických rizik, včetně zabezpečení dodavatelského řetězce, vícefaktorové autentizace, detekce incidentů a plánů reakce na ně. Zásadní novinkou je povinnost hlásit významné incidenty ve dvou fázích – do 24 hodin předběžná zpráva a do 72 hodin podrobnější analýza. (Evropská unie, 2022)

Prováděcí nařízení Komise (EU) 2024/2690 specifikuje technické a metodické požadavky, které vycházejí z mezinárodních standardů ISO/IEC 27001 a 27002. Nařízení definuje klíčová bezpečnostní opatření a stanovuje jednotný přístup k posuzování, monitorování a oznamování incidentů v celé EU. Cílem je zajistit, že subjekty splní vysoké požadavky na

kybernetickou odolnost bez ohledu na jejich velikost či sektor působnosti. (Evropská unie, 2024)

2.3.3 Nařízení Evropského parlamentu a Rady (EU) 2016/679

Obecné nařízení o ochraně osobních údajů (GDPR) představuje jednotný rámec ochrany dat napříč EU. Kromě právních zásad zajišťuje i kybernetickou bezpečnost při zpracování osobních údajů prostřednictvím technických a organizačních opatření. Článek 32 ukládá povinnost zavést například šifrování, pseudonymizaci, dostupnost a integritu dat, obnovu po incidentech a pravidelné testování bezpečnostních opatření. (Evropská unie, 2016)

Nařízení rovněž stanovuje oznamovací povinnost: správce musí do 72 hodin nahlásit incident dozorovému úřadu, a v případě ohrožení práv jednotlivců musí informovat i dotčené osoby. (Evropská unie, 2016)

Tyto požadavky jsou komplikovány při přeshraničním přenosu dat a v prostředí digitálních identit, kde rozdílné regulační rámce mezi státy způsobují zpoždění v oznamování a ohrožují jednotnou ochranu dat. (Supangkat et al., 2025)

Významnou výzvou je rovněž interoperabilita a bezpečnost sdílení osobních údajů mimo EU. GDPR povoluje přenos dat pouze do zemí s odpovídající úrovní ochrany – jako jsou Kanada či Japonsko – zatímco jiné, například USA nebo Čína, vyžadují dodatečná opatření. Ta však nemusí být v praxi vždy účinná, což vytváří prostor pro zneužití dat třetími stranami. (Supangkat et al., 2025)

3 DÍLČÍ ZÁVĚR TEORETICKÝCH VÝCHODISEK DIPLOMOVÉ PRÁCE

Teoretická část diplomové práce poskytuje přehled klíčových pojmů souvisejících s umělou inteligencí a kybernetickou bezpečností. Zabývá se technologickými aspekty, jako je strojové učení, federované učení a generativní AI, dále pak pojmy z oblasti kybernetické bezpečnosti, ale také legislativním rámcem, a to jak národním, tak mezinárodním. Důraz je kladen na pochopení aktuálních kybernetických hrozeb a možností jejich prevence prostřednictvím moderních technologií.

V rámci kapitoly Základní terminologie byly definovány základní pojmy z oblasti umělé inteligence, včetně neuronových sítí, generativní AI a zpracování přirozeného jazyka, které umožňují pokročilé analýzy a predikce v bezpečnostních systémech. Rovněž byly popsány klíčové pojmy kybernetické bezpečnosti, jako jsou různé typy kybernetických útoků, obranné mechanismy a nástroje pro detekci hrozeb. Spojení těchto oblastí ukazuje, jak umělá inteligence může výrazným dílem přispívat k efektivnější ochraně před kybernetickými útoky, avšak poukazuje i na existenci nových nástrojů pro útočníky, kteří tak mohou provádět sofistikovanější útoky, což zvyšuje složitost obranných mechanismů a klade větší nároky na bezpečnostní opatření.

Kapitola Právní rámec a mezinárodní normy se opírá o Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, který definuje povinnosti subjektů kritické infrastruktury a organizací zajišťujících digitální služby. Na úrovni EU hraje klíčovou roli směrnice NIS2 (Směrnice EU 2022/2555), která posiluje požadavky na kybernetickou odolnost členských států. Česko na tuto směrnici již zareagovalo, v současné době byl návrh nového zákona o kybernetické bezpečnosti schválen vládou a bude se v další fázi legislativního procesu projednávat v Poslanecké sněmovně.

Celkově lze konstatovat, že propojení umělé inteligence a kybernetické bezpečnosti představuje zásadní výzvu i příležitost. AI umožňuje efektivnější identifikaci a ochranu před hrozbami, avšak zároveň přináší nové bezpečnostní riziko spojené se zneužitím těchto technologií. Proto je nutné nejen rozvíjet pokročilé bezpečnostní strategie, ale také zajistit odpovídající legislativní a etický rámec, který zajistí rovnováhu mezi technologickým pokrokem a ochranou dat i digitální společnosti.

II. PRAKTICKÁ ČÁST

4 ANALÝZA A KOMPARACE PŘÍSTUPŮ K DETEKCI VYBRANÝCH KYBERNETICKÝCH HROZEB

Tato kapitola se věnuje systematické analýze a porovnání metod detekce kybernetických hrozeb, a to jak v oblasti malwaru, tak phishingu. Zohledňuje a porovnává tradiční techniky, a moderní přístupy založené na umělé inteligenci.

Analýza je provedena na základě vybraných hodnoticích kritérií, mezi něž patří přesnost detekce, míra falešně pozitivních výsledků, výpočetní náročnost, provozní náklady, nároky na lidskou obsluhu a schopnost reagovat na nové nebo neznámé hrozby. Jednotlivé metody jsou hodnoceny prostřednictvím komparativního rámce vycházejícího z dostupných odborných studií, technických reportů a empirických analýz. Tento přístup umožňuje provést kvalifikované srovnání efektivity jednotlivých řešení i bez přímého technického testování, přičemž reflektuje interdisciplinární charakter problematiky a dostupnost dat.

Výsledky analýzy jsou prezentovány formou tabulek s komentovanými závěry a dále rozpracovány do komparativní části, která umožňuje identifikovat silné a slabé stránky jednotlivých přístupů.

4.1 Analýza a porovnání metod detekce malware

Tato subkapitola se zaměřuje na analýzu metod detekce malware, přičemž hodnotí jak tradiční přístupy, jako je signaturní a heuristická analýza, tak moderní metody využívající umělou inteligenci. Každá metoda je hodnocena dle klíčových kritérií, jako je přesnost, výpočetní náročnost či schopnost detekovat nové a neznámé hrozby. Výsledky analýzy jsou přehledně zobrazeny v tabulkách s barevně zvýrazněným hodnocením, které umožňují rychlou orientaci v efektivitě jednotlivých metod. Na základě těchto individuálních analýz následuje jejich vzájemné porovnání, které umožňuje posoudit jejich silné a slabé stránky a vyhodnotit, zda moderní metody představují perspektivní přístup k ochraně subjektu před kybernetickými hrozbami.

4.1.1 Tradiční přístup – signaturní detekce

Signaturní detekce je tradiční metoda používaná v antivirovém softwaru, která porovnává soubory s databází známých malwarových signatur. Každý škodlivý kód má svůj unikátní binární otisk, který je v databázi antiviru. Pokud se signatura nalezeného souboru shoduje s existující signaturou v databázi, soubor je označen jako hrozba a zablokován. Tento přístup je široce používán v běžných antivirech. (Beaumarchais et al., 2024)

Výhody metody signaturní detekce

- **Vysoká přesnost pro známý malware**
 - Signaturní detekce poskytuje extrémně přesnou detekci známých škodlivých kódů, protože porovnává soubory s již ověřenými signaturami. Díky tomu má nízký počet falešných poplachů. (van Ovayan et al., 2024)
- **Nízká výpočetní náročnost**
 - Tato metoda nevyžaduje složité algoritmy nebo analýzu chování. Proces skenování je rychlý a nenáročný na výpočetní výkon, což ji činí vhodnou pro nízkonapěťová zařízení a starší hardware. (Beaumarchais et al., 2024)
- **Nízké provozní náklady**
 - Signaturní detekce je finančně méně náročná než pokročilé metody. Nevyžaduje výkonné servery nebo datové analýzy, což ji činí atraktivní volbou pro menší organizace s omezeným rozpočtem na kybernetickou bezpečnost. Je však potřeba vzít v potaz dodatečné náklady spojené se správou signaturních databází. (Cen et al., 2025)
- **Nízké nároky na lidskou obsluhu**
 - Většina operací signaturní detekce je automatizovaná, takže není nutné, aby administrátoři ručně zasahovali do procesu skenování. Zásah člověka je vyžadován pouze při aktualizaci signatur a řešení falešně pozitivních detekcí. (Beaumarchais et al., 2024)

Nevýhody metody signaturní detekce

- **Neúčinnost proti zero-day útokům**
 - Signaturní metoda nemůže detekovat nový malware, pokud jeho signatura ještě není v databázi. To znamená, že nové hrozby mohou obcházet ochranu, dokud antivirové databáze nebudou aktualizovány. (van Ovayan et al., 2024)
- **Neúčinnost vůči polymorfnímu a metamorfnímu malwaru**
 - Pokročilé malware techniky, jako polymorfismus a metamorfismus, umožňují malwaru měnit svůj kód při každém spuštění, čímž se vyhne signaturní detekci. (Beaumarchais et al., 2024)

- **Závislost na pravidelných aktualizacích databáze**
 - Aby byla signaturní detekce účinná, databáze signatur musí být pravidelně aktualizována. Mezi vznikem nového malwaru a přidáním jeho signatury do databáze může být časová mezera, během které je systém zranitelný. (van Ovayan et al., 2024)

Dílčí závěr

Signaturní detekce je osvědčenou a široce používanou metodou antivirové ochrany, která se vyznačuje vysokou přesností při odhalování známého malwaru, nízkou výpočetní náročností a finanční dostupností. Její hlavní nevýhodou je však závislost na pravidelných aktualizacích databáze signatur, což ji činí neefektivní proti novým, dosud neznámým hrozbám, včetně zero-day útoků a polymorfního malwaru. Klíčové vlastnosti této metody jsou přehledně shrnuty v tabulce 2.

Tabulka 2 Klíčové vlastnosti signaturní detekce

Kritérium	Hodnocení
Detekce známého malwaru	Velmi efektivní
Rychlost skenování	Velmi efektivní
Falešně pozitivní detekce	Nízká
Detekce zero-day útoků	Slabá detekce
Odolnost proti mutujícímu malwaru	Slabá odolnost
Potřeba aktualizací	Slabé – silná potřeba aktualizací
Výpočetní náročnost	Nízká náročnost
Provozní náklady	Nízké
Nároky na lidskou obsluhu	Nízké

(zdroj: vlastní zpracování)

4.1.2 Tradiční přístup – heuristická analýza

Heuristická analýza je pokročilejší detekční metoda než signaturní přístup, protože nevyžaduje předem definované vzory (signatury), ale identifikuje hrozby na základě

podezřelých vzorců chování a charakteristik kódu. Funguje na principu statické analýzy kódu a dynamického sledování chování souborů. Tento přístup umožňuje detekci nových nebo variabilních forem malwaru, které nejsou v signaturní databázi. Je často využíván v moderních antivirových řešeních, kde slouží jako doplňková vrstva ochrany vedle signaturní analýzy. (Darwish et al., 2024)

Výhody heuristické analýzy

- **Detekce nových a neznámých hrozeb**
 - Hlavní výhodou heuristické analýzy oproti signaturním metodám je určitá schopnost detekovat i neznámý malware, který nebyl dosud katalogizován. (Darwish et al., 2024)
- **Flexibilita vůči polymorfnímu a metamorfnímu malwaru**
 - Protože heuristická analýza nespohlhá na pevné signatury, může efektivně detekovat malware, který mění svůj kód při každém spuštění. (Darwish et al., 2024)
- **Detekce podezřelých operací**
 - Heuristická analýza sleduje chování aplikací v reálném čase a může zabránit škodlivé aktivitě ještě před jejím dokončením. Například pokud program bez zjevného důvodu šifruje soubory, může být označen jako ransomware.

Nevýhody heuristické analýzy

- **Vysoká míra falešných poplachů**
 - Heuristická analýza může označit legitimní software jako škodlivý, protože detekuje podezřelé vzory, které mohou být součástí běžných programů. (Darwish et al., 2024)
- **Vyšší výpočetní náročnost**
 - Na rozdíl od signaturní detekce, která pouze porovnává kód se známými vzory, heuristická analýza vyžaduje složitější zpracování (např. emulaci kódu, sandbox testování), což může zpomalit výkon systému. (Darwish et al., 2024)

- **Potřeba častých úprav a aktualizací pravidel**
 - Heuristické algoritmy je nutné pravidelně upravovat, aby nebyly příliš restriktivní ani příliš tolerantní vůči novým typům malwaru. To s sebou nese vyšší nároky na lidský zásah, zejména v podobě ověřování a korekcí prováděných bezpečnostními specialisty. (Darwish et al., 2024)

Dílčí závěr

Heuristická analýza představuje pokročilý detekční přístup, který oproti signaturní metodě umožňuje identifikaci nových a neznámých hrozeb na základě podezřelého chování a struktury kódu. Její hlavní výhodou je schopnost detekovat polymorfní a metamorfní malware a reagovat na neznámé útoky v reálném čase. Na druhou stranu však vyžaduje vyšší výpočetní výkon, časté úpravy algoritmů a nese s sebou riziko falešných poplachů. Tabulka 3 přehledně shrnuje klíčové vlastnosti heuristické analýzy.

Tabulka 3 Klíčové vlastnosti heuristické analýzy

Kritérium	Hodnocení
Detekce známého malwaru	Průměrná detekce (metoda k tomu není primárně určena)
Rychlost skenování	Průměrná
Falešně pozitivní detekce	Časté falešně pozitivní detekce
Detekce zero-day útoků	Částečně účinná
Odolnost proti mutujícímu malwaru	Průměrná odolnost
Potřeba aktualizací	Střední potřeba aktualizací
Výpočetní náročnost	Střední náročnost
Provozní náklady	Střední náklady
Nároky na lidskou obsluhu	Střední nároky

(zdroj: vlastní zpracování)

4.1.3 Detekce malwaru pomocí umělé inteligence

Detekce malwaru pomocí umělé inteligence ve využití strojového a hlubokého učení k identifikaci a predikci hrozeb. Tento přístup nevyužívá fixní signatury ani předem

definovaná pravidla, ale analyzuje velké objemy dat a učí se rozpoznávat vzory chování malwaru na základě historických útoků. Hlavním cílem tohoto principu je automatizovat proces rozpoznání hrozeb a minimalizovat závislost na ruční analýze. (Dodiya et al., 2025)

Výhody detekce malwaru pomocí AI

- **Schopnost detekovat neznámé a zero-day útoky**
 - AI dokáže rozpoznat nové a neznámé hrozby na základě anomálií v datových vzorech. (Ali, 2024)
- **Automatizace a minimální lidský zásah**
 - Detekce založená na AI nevyžaduje časté manuální aktualizace databáze, protože se sama učí z nových vzorců útoků a přizpůsobuje se měnícím se hrozbám. (Iqbal a Ranhbi, 2025)
- **Schopnost zpracovávat velké množství dat**
 - Díky AI může systém sledovat a analyzovat obrovské objemy dat v reálném čase, což umožňuje efektivní detekci malwaru ve velkých sítích. (Galli et al., 2024)
- **Nízká potřeba lidského faktoru během provozu**
 - Ve srovnání s jinými metodami nejméně zatěžuje běžnou IT administraci, avšak vyžaduje specializované znalosti pro údržbu a aktualizaci. (Dodiya et al., 2025)

Nevýhody detekce malwaru pomocí AI

- **Náročnost na výpočetní výkon**
 - Systémy využívající AI vyžadují značné výpočetní zdroje, protože musí neustále analyzovat obrovské množství dat a trénovat modely. (Azzam et al., 2024)
- **Zranitelnost vůči adversariálním útokům**
 - Útočníci mohou manipulovat AI modely tím, že jim předloží speciálně upravená data, která je zmatou a obejdou detekční mechanismy. (Alazab et al., 2025)

- **Vysoké náklady na implementaci**
 - Nasazení systémů detekce využívající AI vyžaduje drahou infrastrukturu a odborné znalosti, což může být problémem pro menší organizace. (Ali, 2024)

Dílčí závěr

Detekce malwaru pomocí umělé inteligence využívá strojové a hluboké učení k identifikaci hrozeb bez potřeby fixních signatur. Její hlavní výhodou je schopnost odhalit zero-day útoky, přizpůsobovat se novým hrozbám a automaticky analyzovat velké objemy dat v reálném čase, čímž minimalizuje manuální zásahy.

Na druhou stranu vyžaduje vysoký výpočetní výkon, je zranitelná vůči adversariálním útokům a její implementace je finančně náročná, vyžadující odbornou správu.

Tabulka 4 přehledně shrnuje klíčové vlastnosti detekce malwaru pomocí AI.

Tabulka 4 Klíčové vlastnosti detekce malwaru pomocí AI

Kritérium	Hodnocení
Detekce známého malwaru	Velmi efektivní
Rychlost skenování	Variabilní (rychlá pro běžné analýzy, pomalejší pro hloubkovou analýzu)
Falešně pozitivní detekce	Přesnější než heuristika, menší přesnost než signatury
Detekce zero-day útoků	Velmi efektivní
Odolnost proti mutujícímu malwaru	Velmi efektivní
Potřeba aktualizací	Nízká
Výpočetní náročnost	Vysoká (závisí na implementaci a infrastruktuře)
Provozní náklady	Vysoké (při implementaci, variabilní při provozu)
Nároky na lidskou obsluhu	Nízké pro běžný provoz, vysoké pro správu modelů

(zdroj: vlastní zpracování)

4.1.4 Komparace metod detekce malware

Tato subkapitola se zaměřuje na porovnání tradičních metod detekce malware a přístupů využívajících umělou inteligenci, zejména hlubokého učení. Srovnání je založeno na základě klíčových kritérií, které jsou detailněji vysvětleny níže. Klíčovou referencí pro toto porovnání je studie *Application of Deep Learning Models for Real-Time Automatic Malware Detection* (Gutierrez et al., 2024), která poskytuje podrobnou analýzu efektivity tradičních metod, modelů hlubokého učení a jejich vzájemného porovnání ve stejných podmínkách.

Kritéria hodnocení detekčních metod

- Přesnost – udává procento správně klasifikovaných případů z celkového množství testovaných vzorků.
- Citlivost – odráží schopnost metody správně identifikovat malware (pravdivé pozitivní případy).
- Falešně pozitivní míra (FP Rate) – vyjadřuje, kolik legitimního softwaru bylo chybně označeno jako škodlivé.
- F1-skóre – kombinuje přesnost a citlivost do jedné metriky, čímž poskytuje vyvážený pohled na výkon modelu.
- Výpočetní náročnost – určuje, jak velké výpočetní zdroje metoda potřebuje pro detekci malware.
- Úspěšnost proti polymorfnímu malware – hodnotí schopnost metody detekovat malware, který se dynamicky mění.
- AUC-ROC (Area Under the Receiver Operating Characteristic Curve) – metrika hodnotící schopnost modelu rozlišit mezi malware a legitimním softwarem.

Tabulka 5 shrnuje porovnání tradičních metod detekce malware s přístupy využívajícími umělou inteligenci (AI) na základě různých kritérií.

Tabulka 5 Komparace klasických metod a metod AI v detekci malware

Kritérium	Tradiční přístupy	Přístupy využívající AI
Přesnost	Obecně nižší v porovnání s AI, studie prokázala 85 % procent pro signaturní detekci, 80 % pro heuristickou analýzu	Vysoká, studie prokázala 95 % úspěšnost s využitím DL modelů

Citlivost	Byla prokázána nižší citlivost v porovnání s AI, 80 % pro signatury, 78 % pro heuristiku	Studie prokázala 93 % citlivost DL modelů
Falešně pozitivní (FP Rate)	Vyšší míra v případě heuristické analýzy, nižší v případě signaturní detekce	Obecně mezi heuristikou a signaturami
F1-skóre	82,5 % signaturní detekce 79 % heuristická analýza	94 % pro modely DL
Výpočetní náročnost	Obecně nižší	Obecně vyšší, zejména pro modely DL
Úspěšnost proti polymorfnímu malwaru	Obecně velmi slabá	Velká úspěšnost, zejména pro modely DL
AUC-ROC	82 % signaturní detekce 81 % heuristická analýza	96 % u zkoumaných modelů DL

(zdroj: Gutierrez et al., 2024, vlastní zpracování)

4.1.5 Zhodnocení přístupů k detekci malwaru

Výsledky této analýzy jasně ukazují, že metody hlubokého učení výrazně překonávají tradiční přístupy ve většině sledovaných kategorií, zejména v přesnosti, citlivosti a úspěšnosti proti polymorfnímu malware. Především se však samy učí a přizpůsobují novým typům útoků, čímž poskytují mnohem dynamičtější a spolehlivější ochranu před kybernetickými hrozbami.

Pro organizace a firmy mohou metody umělé inteligence představovat zásadní výhodu – umožňují automatizovanou ochranu s minimální potřebou manuálních zásahů a efektivní detekci i dosud neznámého malware. Díky schopnosti zpracovávat velké objemy dat v reálném čase se tyto systémy stávají ideálním řešením pro firmy, které se chtějí chránit před moderními kybernetickými hrozbami bez nutnosti neustálých aktualizací databází signatur.

Vzhledem k rychlému rozvoji AI lze navíc očekávat, že tyto technologie budou stále dostupnější a optimalizovanější i pro menší podniky. S postupnou optimalizací výpočetní náročnosti a rostoucí efektivitou se tak AI může stát klíčovým pilířem kybernetické bezpečnosti firem, které chtějí proaktivně chránit svá data a systémy před stále sofistikovanějšími útoky.

4.2 Analýza a porovnání metod detekce phishingu

Tato subkapitola se zaměřuje na analýzu metod detekce phishingu, přičemž hodnotí jak tradiční přístupy, tak moderní techniky využívající umělou inteligenci. Jednotlivé metody jsou posuzovány na základě předem stanovených kritérií, mezi něž patří přesnost detekce, výpočetní náročnost, míra falešně pozitivních výsledků, schopnost adaptace na nové hrozby či provozní náklady. Výsledky analýzy jsou přehledně shrnuty v tabulkách, které usnadňují srovnání efektivity jednotlivých přístupů. Závěrečná část subkapitoly pak představuje jejich komparativní vyhodnocení, které poukazuje na výhody a limity jednotlivých metod a hodnotí potenciál moderních řešení při zvyšování úrovně ochrany proti phishingovým útokům.

4.2.1 Tradiční přístup – blacklisting

Metoda blacklisting spočívá v identifikaci a zablokování přístupu k doménám, které jsou známy jako phishingové či jinak škodlivé. Uživatelé při pokusu o otevření takové stránky obdrží varování nebo jim je přístup zablokován (např. prostřednictvím prohlížeče nebo antivirového softwaru). Blacklisting se často provádí pomocí centrálně spravovaných seznamů nebo na úrovni podnikových firewallů. (Alanezi, 2021)

Výhody metody blacklisting

- **Okamžitá ochrana**
 - Metoda je velmi účinná při blokování přístupu ke stránkám, které již byly nahlášeny jako phishingové. (Alanezi, 2021)
- **Jednoduchost**
 - Nízká náročnost na uživatele. (Alanezi, 2021)
- **Vysoká efektivita při opakovaných útocích**
 - Metoda je obzvlášť účinná proti znovu používaným phishingovým URL adresám, které jsou často šířeny prostřednictvím hromadných spamových e-mailů. (Alanezi, 2021)

Nevýhody metody blacklisting

- **Neúčinnost proti novým phishingovým hrozbám**
 - Nově vytvořená phishingová stránka se do seznamu dostane až po určité době, což snižuje účinnost této metody. (Alanezi, 2021)
- **Snadné obejítí blacklistu**
 - Útočníci mohou blacklist obejít častou změnou URL adres nebo IP adres. (Alanezi, 2021)
- **Potřeba časté aktualizace**
 - Účinnost blacklistů silně závisí na pravidelné aktualizaci a spolehlivých zdrojích informací. (Alanezi, 2021)

Dílčí závěr

Blacklisting představuje jednoduchý a často využívaný tradiční přístup k ochraně proti phishingovým útokům, který se opírá o blokování přístupu ke známým škodlivým doménám. Díky své nenáročnosti a schopnosti okamžitě reagovat na již identifikované hrozby je metoda efektivní zejména při opakovaných nebo masově šířených útocích. Tabulka 6 přehledně shrnuje základní charakteristiky této metody. Klíčovou slabinou blacklistingového přístupu zůstává jeho neúčinnost vůči novým hrozbám, které dosud nebyly zařazeny do databází, a potřeba jejich časté a spolehlivé aktualizace.

Tabulka 6 Klíčové vlastnosti blacklistingu

Kritérium	Hodnocení
Přesnost	Efektivní u známých hrozeb, nízká efektivita u nových hrozeb
Falešně pozitivní detekce	Nízká míra
Nároky na lidskou obsluhu	Minimální pro běžné uživatele
Výpočetní náročnost	Nízká
Schopnost adaptace na nové hrozby	Neefektivní vůči novým/neznámým hrozbám
Provozní náklady	Relativně nízké – záleží na poskytovateli

(zdroj: vlastní zpracování)

4.2.2 Tradiční přístup – filtrování e-mailů

Filtrování e-mailů je jednou z nejrozšířenějších obranných metod proti phishingu. Jeho cílem je analyzovat příchozí e-mailovou komunikaci a rozpoznat zprávy, které vykazují znaky podvodného nebo škodlivého obsahu. Tato metoda může být založena na jednoduchých pravidlech (např. seznamy podezřelých domén, klíčová slova), nově se však nabízí moderní implementace pokročilých technik s využitím AI, jako je analýza obsahu pomocí natural language processing. (Birthriya et al., 2024)

Výhody metody filtrování e-mailů

- **Automatizovaná obrana první linie**
 - Filtrování e-mailů je schopné blokovat phishingové zprávy ještě předtím, než se dostanou k uživateli. Využívá vícevrstvou detekci, čímž poskytuje efektivní první linii obrany. (Birthriya et al., 2024)
- **Snadná integrace a nenáročný provoz**
 - Filtry lze snadno integrovat do většiny e-mailových systémů, přičemž běžný provoz probíhá zcela automaticky bez nutnosti zásahu běžného uživatele. (Tally et al., 2004)
- **Možnost implementace pokročilé detekce pomocí AI**
 - Moderní systémy využívající NLP a hluboké učení jsou schopny rozeznat i skrytější phishingové vzorce v textu nebo struktuře zprávy. (Birthriya et al., 2024)

Nevýhody metody filtrování e-mailů

- **Falešné poplachy a ztráta důvěry**
 - Příliš agresivní filtry mohou označit legitimní e-maily jako nebezpečné, což vede ke ztrátě důležitých zpráv nebo důvěry uživatelů v systém. (Birthriya et al., 2024)
- **Nutnost časté aktualizace a trénování**
 - Bez pravidelné aktualizace pravidel a modelů dochází k výraznému poklesu účinnosti detekce nových hrozeb. (Birthriya et al., 2024)

- **Nízká účinnost proti cíleným útokům (spear-phishingu)**
 - Sofistikované spear-phishing útoky často neobsahují tradiční znaky spamu a mohou tak projít filtrem. (Tally et al., 2004)

Dílčí závěr

Filtrování e-mailů patří mezi základní nástroje obrany proti phishingu a v současné praxi představuje jednu z nejpoužívanějších metod. Jeho hlavní předností je schopnost automaticky eliminovat škodlivé zprávy dříve, než dorazí k uživateli, což z něj činí efektivní prvek první linie ochrany. Díky snadné implementaci a možnosti využití pokročilých AI technik, jako je analýza přirozeného jazyka, se jedná o metodu, která je dobře adaptovatelná na současné podmínky. Tabulka 7 zachycuje přehled klíčových vlastností této metody včetně jejích technických možností a provozních aspektů.

Tabulka 7 Klíčové vlastnosti filtrování e-mailů

Kritérium	Hodnocení
Přesnost	Efektivní u známých hrozeb, slabší u cílených útoků
Falešně pozitivní detekce	Střední až nízká míra, záleží na nastavení filtru
Nároky na lidskou obsluhu	Nízké, systém automatizován
Výpočetní náročnost	Nízká
Schopnost adaptace na nové hrozby	Značně omezená bez AI, statický systém
Provozní náklady	Nízké až střední – dle zvoleného řešení

(zdroj: vlastní zpracování)

4.2.3 Tradiční přístup – vzdělávání a osvěta uživatelů

Vzdělávání uživatelů a osvěta v oblasti phishingu představují klíčovou součást obranných strategií, protože většina phishingových útoků cílí právě na lidský faktor. Cílem je zvýšit schopnost uživatelů rozpoznat podvodné e-maily, odkazy a webové stránky. Školení mohou mít různou formu: prezentace, testovací phishingové kampaně, interaktivní moduly nebo gamifikace. Úspěšné programy kombinují praktické simulace a opakované připomínání. (Reinheimer et al., 2020)

Výhody metody vzdělávání a osvěty uživatelů

- **Zvýšení dlouhodobé odolnosti vůči útokům**
 - Uživatelé, kteří absolvují cílené školení, mají větší šanci rozpoznat phishing v reálných situacích a správně na něj reagovat.
- **Flexibilita**
 - Školení může být přizpůsobeno konkrétním skupinám uživatelů, jejich technickým schopnostem a pracovním rolím.
- **Dlouhodobý přínos pro organizační kulturu bezpečnosti**
 - Zvyšuje se nejen odolnost vůči phishingu, ale i obecné bezpečnostní vědomí zaměstnanců.

Nevýhody metody vzdělávání a osvěty uživatelů

- **Neefektivita bez pravidelného opakování**
 - Bez pravidelných připomenutí účinek školení klesá – uživatelé zapomínají a chybují.
- **Vysoké nároky na motivaci a aktivní zapojení**
 - Pasivní nebo nezáživná školení mají malý efekt – uživatelé si informace nezapamatují.
- **Náročnost měření efektivity**
 - Výsledky osvěty se měří obtížně – obvykle až podle počtu incidentů nebo úspěšnosti simulovaných útoků.

Dílčí závěr

Vzdělávání a osvěta uživatelů představují klíčový pilíř obrany proti phishingu, protože umožňují posílit lidský faktor – nejslabší, ale zároveň nejvíce ovlivnitelný článek bezpečnostního řetězce. Správně navržené a opakovaně realizované školení zvyšuje pravděpodobnost, že uživatelé rozpoznají podvodné pokusy a zareagují adekvátně. Úspěšnost osvěty však závisí na pravidelnosti, kvalitě zpracování a míře zapojení účastníků, přičemž její efektivitu bývá obtížné kvantifikovat bez delšího časového horizontu. Klíčové vlastnosti této metody jsou shrnuty v tabulce 8.

Tabulka 8 Klíčové vlastnosti metody vzdělávání a osvěty uživatelů

Kritérium	Hodnocení
Přesnost	Zcela závislá na uživateli, vysoká variabilita
Falešně pozitivní detekce	Nízká – uživatel sám posuzuje riziko
Nároky na lidskou obsluhu	Vysoké – školení, testování, pravidelná osvěta
Výpočetní náročnost	Nízká
Schopnost adaptace na nové hrozby	Relativně vysoká, člověk dokáže reagovat i na nové formy hrozeb
Provozní náklady	Nízké až střední – dle zvoleného řešení

(zdroj: vlastní zpracování)

4.2.4 Metoda umělé inteligence – strojové učení

Využití strojového učení spočívá ve schopnosti algoritmů učit se ze vstupních dat a na jejich základě klasifikovat, zda daný vstup (například e-mail, URL nebo doména) představuje phishingovou hrozbu. Typicky se využívá metod jako jsou Decision Trees, Support Vector Machines a Random Forest. Modely se trénují na datech obsahujících různé charakteristiky (např. struktura URL, délka e-mailu, jazykové znaky, hlavičky), a následně klasifikují nové případy jako phishingové nebo legitimní. V praxi se již nyní tyto modely často nasazují v e-mailových branách, prohlížečích nebo jako součást antivirových nástrojů. (Hassan, 2024)

Výhody metod ML

- **Přesnost i bez obrovských dat**
 - Modely ML dokážou dosahovat velmi dobrých výsledků i při menším množství dat (Alanezi, 2021)
- **Nízká výpočetní náročnost**
 - Vhodné i pro menší organizace – nepotřebuje výkonné servery ani grafické karty, běží rychle a efektivně. (Tang a Mahmoud, 2021)

Nevýhody metod ML

- **Nízká schopnost adaptace na nové hrozby**
 - Modely strojového učení jsou statické – bez nového tréninku nezachytí nové typy útoků, které se výrazně liší od dat použitých při učení. (Tang a Mahmoud, 2021)
- **Závislost na kvalitě dat**
 - Pokud jsou data chybně označená nebo nevyvážená, model nebude fungovat správně. (Alanezi, 2021)

Dílčí závěr

Strojové učení představuje perspektivní a technicky vyspělý přístup k detekci phishingových hrozeb, který využívá algoritmy schopné klasifikace na základě trénovacích dat. Výhodou této metody je vysoká přesnost při identifikaci známých útoků, nízká výpočetní náročnost a provozní efektivita, díky čemuž je vhodná i pro menší organizace. Tabulka 9 shrnuje klíčové parametry využití strojového učení v kontextu boje proti phishingu. Mezi hlavní omezení patří nízká flexibilita vůči novým typům hrozeb a závislost na kvalitě vstupních dat, které významně ovlivňují výstupy modelu.

Tabulka 9 Klíčové vlastnosti metod strojového učení

Kritérium	Hodnocení
Přesnost	Efektivní u známých hrozeb, slabší u cílených útoků
Falešně pozitivní detekce	Středně efektivní – riziko falešných poplachů při slabém tréninku
Nároky na lidskou obsluhu	Nízké
Výpočetní náročnost	Nízká
Schopnost adaptace na nové hrozby	Nízká, nutnost přecvičení modelu pro nové útoky
Provozní náklady	Nízké až střední – podle frekvence trénování a údržby modelu

(zdroj: vlastní zpracování)

4.2.5 Metoda umělé inteligence – hluboké učení

Metody hlubokého učení využívají vícevrstvé neuronové sítě k automatickému učení komplexních vzorců ze vstupních dat – bez nutnosti ručního navrhování znaků. Tyto modely se učí na velkých objemech dat a díky své hloubce dokážou odhalit i skrytější vzory phishingu, které tradiční metody nerozpoznají. (Hassan, 2024)

Výhody metod DL

- **Vysoká přesnost a nízká chybovost**
 - Modely DL dosahují výborných výsledků v přesnosti díky schopnosti pracovat s jazykovými vzory a syntaxí. (Alanezi, 2021)
- **Schopnost detekovat nové a sofistikované hrozby**
 - Díky svému způsobu učení dokážou zachytit i útoky, které se dosud nevyskytly ve výcvikových datech. (Tang a Mahmoud, 2021)
- **Vhodné pro zpracování přirozeného jazyka**
 - Zvládají porozumět kontextu zpráv – nejen klíčovým slovům, ale i záměru autora. (Hassan, 2024)

Nevýhody metod DL

- **Vysoká výpočetní náročnost**
 - Trénink a nasazení modelů vyžaduje moderní a výkonné hardware. (Tang a Mahmoud, 2021)
- **Nízká interpretovatelnost výsledků**
 - Neuronové sítě jsou černé skříňky – obtížně se vysvětluje, proč rozhodly, že daný vstup je phishing. (Tang a Mahmoud, 2021)
- **Náročnost přípravy a tréninku**
 - Potřebují velké množství označených dat, pečlivou přípravu textu, s tím se pojí zvýšené požadavky na lidskou údržbu. (Alanezi, 2021)

Dílčí závěr

Hluboké učení představuje vysoce sofistikovaný přístup k detekci phishingu, který díky využití vícevrstevných neuronových sítí umožňuje zachytit i složité jazykové a kontextové

vzorci, jež běžné techniky často přehlíží. Tento typ umělé inteligence se uplatňuje zejména tam, kde je klíčová vysoká přesnost, schopnost adaptace a práce s přirozeným jazykem. Tabulka 10 poskytuje hodnocení hlavních charakteristik těchto metod při detekci hrozeb phishingu. Nevýhodou zůstává vysoká výpočetní náročnost, složitá interpretovatelnost výsledků a značné nároky na přípravu dat i odbornou údržbu modelu, což může limitovat její praktické nasazení v menších organizacích.

Tabulka 10 Klíčové vlastnosti metod hlubokého učení

Kritérium	Hodnocení
Přesnost	Velmi vysoká
Falešně pozitivní detekce	Nízké
Nároky na lidskou obsluhu	Nízké pro uživatele, zvýšené nároky na údržbu a trénink modelu
Výpočetní náročnost	Vysoká, nutnost velké výpočetní kapacity
Schopnost adaptace na nové hrozby	Vysoká, schopnost detekovat nové hrozby
Provozní náklady	Střední – podle frekvence trénování a údržby modelu

(zdroj: vlastní zpracování)

4.2.6 Metoda umělé inteligence – jazykové modely

Metody z oblasti zpracování přirozeného jazyka (NLP) umožňují analýzu textu na úrovni významu, kontextu a záměru. Moderní jazykové modely, jako jsou BERT (Bidirectional Encoder Representations from Transformers) nebo transformery obecně (např. RoBERTa, GPT-like modely) jsou trénovány na rozsáhlých datech v podobě textu a dokážou rozpoznat klamavé fráze, psychologické vzorce, jazyk manipulace či neobvyklé výrazy, které se často objevují ve phishingových e-mailech. Používají se pro klasifikaci textu (phishing vs. legitimní), detekci podezřelého záměru zprávy či extrakci významových prvků (např. výzva k akci, naléhavost, sociální inženýrství). (Sospeter a Odoyo, 2024)

Výhody metod NLP

- **Porozumění kontextu a významu phishingových zpráv**
 - Na rozdíl od klasických filtrů, které rozpoznávají pouze klíčová slova nebo URL, NLP modely chápou smysl vět a záměr komunikace, včetně manipulativního a psychologicky cíleného jazyka. (Sospeter a Odoyo, 2024)
- **Schopnost generalizace i na nové typy phishingu**
 - Díky porozumění textové struktuře jsou tyto modely schopné detekovat i varianty útoků, které neobsahují tradiční indikátory (např. URL), ale mají podobné jazykové znaky. (Sospeter a Odoyo, 2024)

Nevýhody metod NLP

- **Vysoké nároky na výpočetní zdroje a infrastrukturu**
 - Trénink i nasazení velkých NLP modelů jsou náročné a vyžadují značné výpočetní zdroje. U rozsáhlých datových toků se může výkon stát úzkým hrdlem. (Sospeter a Odoyo, 2024)
- **Obtížná interpretace rozhodnutí modelu**
 - U hlubokých jazykových modelů je velmi těžké pochopit, proč konkrétní zprávu označily jako phishingovou. (Sospeter a Odoyo, 2024)

Dílčí závěr

Jazykové modely založené na technikách zpracování přirozeného jazyka (NLP) přinášejí do oblasti detekce phishingu nový kvalitativní přístup – umožňují analyzovat text z hlediska významu, kontextu a záměru komunikace. Díky této schopnosti dokážou efektivně odhalit i skryté manipulativní vzorce, které tradiční metody často nerozpoznají. Tabulka 11 shrnuje hodnocení hlavních charakteristik těchto metod při detekci hrozeb phishingu. Přestože NLP modely vynikají vysokou účinností, jejich nasazení je spojeno s výraznou výpočetní náročností a složitější interpretací výsledků, což může komplikovat jejich širší implementaci zejména v prostředích s omezenými technickými kapacitami.

Tabulka 11 Klíčové vlastnosti metod NLP

Kritérium	Hodnocení
Přesnost	Velmi vysoká – schopnost porozumět významu a záměru textu
Falešně pozitivní detekce	Nízké
Nároky na lidskou obsluhu	Nízké pro uživatele, zvýšené nároky na trénink a monitoring modelu
Výpočetní náročnost	Vysoká, nutnost velké výpočetní kapacity
Schopnost adaptace na nové hrozby	Vysoká, schopnost detekovat nové hrozby
Provozní náklady	Střední až vysoké – podle frekvence trénování a údržby modelu

(zdroj: vlastní zpracování)

4.2.7 Komparace vybraných metod pro detekci phishingu

Tato subkapitola navazuje na předchozí analytické části, které detailně rozebíraly jednotlivé přístupy k detekci phishingových útoků – od tradičních metod, jako je blacklisting, filtrování e-mailů či školení uživatelů, až po moderní AI techniky využívající umělou inteligenci, zejména strojové a hluboké učení a zpracování přirozeného jazyka (NLP).

Cílem této části je systematické porovnání uvedených metod na základě souboru vybraných hodnotících kritérií. Komparace vychází z empirických dat dostupných ve vědecké literatuře. Klíčovými referencemi pro toto srovnání jsou studie Xiang et al. (2009), kteří analyzovali výkonnost blacklistů, dále Somesha et al. (2020), kteří testovali různé modely hlubokého učení v oblasti phishingu, a také Khan a Rana (2021), jejichž práce se zaměřila na srovnání modelů neuronových sítí pro detekci phishingových webů.

Srovnání metod je provedeno na základě následujících šesti kritérií:

- Přesnost – schopnost metody správně rozlišit mezi phishingem a legitimní komunikací.
- Falešně pozitivní detekce – míra, s jakou metoda chybně označí legitimní zprávu či stránku jako phishingovou.

- Nároky na lidskou obsluhu – vyhodnocuje zejména zatížení koncových uživatelů (např. potřebu školení, zásahů).
- Výpočetní náročnost – technické požadavky na hardware a infrastrukturu ze strany organizace.
- Schopnost adaptace na nové hrozby – jak efektivně se metoda vypořádá s neznámými a zero-day útoky.
- Provozní náklady – celkové náklady na implementaci, údržbu a provoz z pohledu organizace.

Tabulka 12 tyto metody podrobně srovnává, dílčí závěr poskytuje subkapitola Zhodnocení přístupů k detekci phishingu.

Tabulka 12 Komparace klasických metod a metod AI v detekci phishingu

Kritérium	Tradiční přístupy	Přístupy využívající AI
Přesnost	Efektivní při detekci známých hrozeb, studie prokázala přesnost 87,4 %	Dosahují vysoké přesnosti, uvádí se přesnost až 99,5 %
Falešně pozitivní detekce	Velmi nízké, uvádí se přenosť kolem 0,04 %	Zpravidla vyšší oproti tradičním metodám, studie prokázaly míru okolo 0,5 %
Nároky na lidskou obsluhu	Nízké u automatizovaných metod, vyšší u školení uživatelů (uživatel musí aktivně rozpoznat hrozbu)	Nízké pro běžné uživatele; vyšší pro administrátory při tréninku, validaci a update modelů
Výpočetní náročnost	Nízká – jednoduché filtry, seznamy, pravidla	ML: nízká až střední. DL/NLP: vysoká (nutnost výkonného HW i na koncových zařízeních)
Schopnost adaptace na nové hrozby	Nízká – tradiční metody zpravidla nereagují na nové hrozby bez aktualizace	Vysoká – zejména DL/NLP dokážou detekovat i nové typy phishingu díky analýze vzorců a jazykového kontextu
Provozní náklady	Nízké až střední – závisí na zvoleném řešení	ML: nízké až střední (podle dat a update). DL/NLP: střední až vysoké kvůli tréninku modelů a HW nárokům

(zdroj: vlastní zpracování)

4.2.8 Zhodnocení přístupů k detekci phishingu

Komparace tradičních metod detekce phishingu a moderních přístupů využívajících umělou inteligenci ukázala, že obě skupiny metod disponují specifickými výhodami i omezeními. Tradiční techniky, jako jsou blacklisty, heuristická pravidla či školení uživatelů, se vyznačují nízkými provozními náklady, nenáročnou implementací a minimální výpočetní zátěží. Jejich účinnost je však výrazně limitována schopností adaptace na nové a neznámé hrozby.

Naopak metody založené na strojovém a hlubokém učení či zpracování přirozeného jazyka vykazují vyšší přesnost a lepší adaptabilitu, zejména v detekci sofistikovaných a dosud neznámých phishingových útoků. Jejich nasazení je však spojeno s vyššími nároky na výpočetní infrastrukturu, odbornou správu a celkové provozní kapacity.

Z provedené analýzy nevyplyvá, že by některý z přístupů jednoznačně dominoval, nicméně ukazuje se, že jejich vzájemné doplnění by mohlo významně přispět ke zvýšení celkové úrovně kybernetické bezpečnosti. Tuto hypotézu potvrzuje i aktuální studie Sahu et al. (2024), podle níž hybridní model překonává jednotlivé přístupy ve všech sledovaných ukazatelích – přesnosti, preciznosti, míře úspěšné detekce i celkové výkonnosti. Autoři dále uvádějí, že kombinovaný přístup významně snižuje výskyt falešně pozitivních detekcí, a tím zvyšuje celkovou spolehlivost systému pro odhalování phishingu.

Kombinace tradičních metod a pokročilých technik umělé inteligence se tak jeví jako slibný směr dalšího vývoje, který zohledňuje jak technickou účinnost, tak provozní a ekonomické aspekty kybernetické ochrany.

5 ANALÝZA A NÁVRH NÁSTROJE UMĚLÉ INTELIGENCE PRO ZVÝŠENÍ KYBERNETICKÉ BEZPEČNOSTI SUBJEKTU

Tato část diplomové práce se zabývá návrhem a analýzou zavedení nástroje založeného na umělé inteligenci, jehož cílem je zvýšit úroveň kybernetické bezpečnosti modelového podniku. Zvláštní důraz je kladen na detekci phishingových útoků a škodlivého softwaru (malware), které představují nejčastější typy kybernetických hrozeb, jimž čelí jednotlivé subjekty.

Na základě poznatků z předchozích částí práce bude zhodnoceno, jaké konkrétní přínosy může přinést implementace AI řešení v praxi, a to jak z hlediska detekční účinnosti, tak i z pohledu nákladů, provozní zátěže a technické realizovatelnosti.

5.1 Charakteristika modelového subjektu

Pro účely aplikační části byla zvolena modelová firma Finakta s.r.o., která zastupuje typického zástupce malého podnikatelského subjektu v oblasti administrativních služeb. Tento typ organizací je charakteristický nízkou technologickou vybaveností a absencí specializovaného IT oddělení, přičemž zároveň zpracovává velké množství elektronické dokumentace, faktur a důvěrných údajů klientů.

Z pohledu kybernetické bezpečnosti je tento typ subjektu vysoce ohrožen phishingem a malwarem, a to zejména z důvodu:

- častého otevírání příloh od neznámých subjektů,
- absence pokročilých ochranných mechanismů,
- nízké úrovně IT gramotnosti zaměstnanců.

Tato část práce se proto zaměřuje na praktickou analýzu přínosů nasazení AI nástroje, který by zvýšil úroveň ochrany před těmito hrozbami, a to bez nutnosti složitého zásahu do infrastruktury nebo nákladného školení uživatelů.

Základní profil organizace:

- **Název:** Finakta s.r.o. (modelový subjekt)
- **Obor podnikání:** Účetní, daňové a administrativní služby
- **Velikost organizace:** 20 zaměstnanců

- **Typické činnosti:** Vedení účetnictví, zpracování mezd, daňové poradenství, správa dokumentace
- **Používané technologie:** Microsoft 365 (Outlook, OneDrive, Teams), online účetní software, e-mailový provoz přes Exchange Online
- **Technická podpora:** Externí IT servis 1× týdně, ad hoc při problémech
- **Bezpečnostní opatření:** Základní antivirový program (např. AVG Free), standardní e-mailový filtr poskytovatele, žádná behaviorální nebo AI detekce
- **Bezpečnostní školení:** Nepravidelné, naposledy realizováno před více než rokem
- **Citlivá data ve firmě:** Osobní údaje klientů, účetní doklady, smlouvy, přístup do bankovníctví

Na základě uvedených charakteristik lze identifikovat tři hlavní typy kybernetických hrozeb, kterým je organizace Finakta s.r.o. nejvíce vystavena:

- Phishingové e-maily – zaměstnanci pravidelně přijímají velké množství zpráv s přílohami a odkazy, často od neznámých subjektů. Vzhledem k nedostatečné školenosti a absenci pokročilé AI detekce je vysoké riziko otevření podvodného odkazu nebo zadání přihlašovacích údajů na falešné stránce.
- Škodlivé přílohy (malware) – z důvodu časté práce s fakturami a jinými dokumenty (PDF, DOCX, XLSX) je firma zranitelná vůči útokům, které zneužívají důvěru v běžné formáty. Tradiční antivir nemusí detekovat sofistikované útoky, včetně zero-day malware.
- Ransomware – ve spojení s předchozími typy hrozeb hrozí napadení ransomwarem, který může zašifrovat důležitá účetní data.

5.2 Průzkum trhu: Nástroje s využitím umělé inteligence pro detekci phishingu a malware

S ohledem na charakteristiku organizace Finakta s.r.o. a vyhodnocená rizika v oblasti kybernetické bezpečnosti bude proveden průzkum dostupných řešení založených na umělé inteligenci, která se zaměřují na ochranu proti phishingu a malware. Cílem je identifikovat nástroje vhodné pro malé až střední podniky s omezenou technickou kapacitou, které

potřebují jednoduché a efektivní zabezpečení bez nutnosti složitého nastavování nebo vlastního IT týmu.

5.2.1 Microsoft Defender for Business

Microsoft Defender for Business je řešení cílené na malé a střední podniky. Vyznačuje se nativní integrací s ekosystémem Microsoft 365, která zajišťuje bezproblémový provoz a jednotnou správu v rámci uživatelského prostředí, které je firmám často již známé. Produkt je navržen s důrazem na jednoduchost správy, což je klíčové pro organizace, které nemají vlastní IT oddělení. Z hlediska funkčnosti nabízí komplexní ochranu koncových bodů, včetně detekce hrozeb pomocí AI, pokrytí phishingu a správy zranitelností. (Microsoft, 2025)

Licenční poplatek činí 2,8 EUR na uživatele za měsíc. Cena zahrnuje kompletní balík funkcí bez potřeby samostatných doplňků. (Microsoft, 2025)

5.2.2 Sophos Intercept X

Sophos Intercept X je pokročilé řešení, které podporuje integraci s M365, nicméně správa probíhá samostatně přes Sophos Central. Je vhodný pro malé i střední podniky a cloudová konzole Sophos Central je hodnocena jako relativně přehledná. Důležitým aspektem je, že nasazení obvykle probíhá přes partnera a vyžaduje základní orientaci v IT. Z hlediska ochrany nabízí špičkovou ochranu proti malwaru, ransomwaru a exploitům s pokročilými funkcemi. (Sophos, 2025)

Cenová politika společnosti Sophos je individuální a závisí na konkrétním obchodním vztahu s distributorem či partnerem. Pro účely této práce byla společnost Sophos kontaktována s žádostí o orientační cenovou nabídku, avšak žádná odpověď nebyla poskytnuta.

Z tohoto důvodu byly využity veřejně dostupné informace ze stránek autorizovaného přeprodejce EnterpriseAV (2025). Podle těchto údajů činí orientační cena balíčku Sophos Intercept X pro 10–24 uživatelů následující:

- 1 rok: 65,76 USD za zařízení
- 2 roky: 111,80 USD za zařízení (tj. 55,90 USD/rok)
- 3 roky: 144,02 USD za zařízení (tj. 48,01 USD/rok)

5.2.3 CrowdStrike Falcon Go

CrowdStrike Falcon Go se zaměřuje především na ochranu koncových bodů. Integrace s M365 je možná, ale není nativní a integrace s Microsoft bezpečnostními centry je omezená. Produkt je vytvořen explicitně pro menší firmy bez IT oddělení a nabízí jednoduché nasazení, konfiguraci i provoz. Využívá technologii CrowdStrike pro detekci a prevenci hrozeb a poskytuje spolehlivou základní ochranu vhodnou pro malé a střední podniky. (CrowdStrike, 2025)

Cena licence činí 59,99 USD za zařízení ročně. (CrowdStrike, 2025)

5.2.4 SentinelOne Singularity Control

SentinelOne Singularity Control nabízí možnost integrace, ale přímé propojení s M365 není určeno pro menší podniky bez IT. Vyžaduje samostatnou správu mimo M365 platformu. Balíček "Control" je základní, ale plnohodnotná verze SentinelOne. Správa je autonomní, nicméně nasazení a optimalizace může být náročnější pro firmy bez IT podpory. Z hlediska ochrany poskytuje vysokou úroveň behaviorální AI pro detekci a reakci na malware, ransomware a bezsouborové útoky a má výborné funkční pokrytí. (SentinelOne, 2025)

Cena licence balíčku Singularity Control činí 79,99 USD za zařízení ročně. (SentinelOne, 2025)

5.2.5 Acronis Cyber Protect

Acronis Cyber Protect nabízí přímou integraci pro zálohování dat v M365 a úzkou integraci bezpečnostních funkcí s prostředím Microsoft, včetně ochrany OneDrive a e-mailů. Poskytuje kombinaci ochrany proti malwaru, řízení zranitelností, patch management, filtrování URL a integrované zálohování. Řešení je běžně dodáváno formou služby, což usnadňuje správu pro firmy bez IT. Konsoliduje platformu pro bezpečnost a zálohu. (Acronis, 2025)

Cena licenčního balíčku Acronis Cyber Protect Standard činí 56,79 EUR za zařízení ročně při jednoletém předplatném. Při zvolení tříletého období se cena snižuje na 50,40 EUR ročně a při pětiletém závazku na 44,00 EUR ročně za zařízení. (Acronis, 2025)

5.3 Finanční analýza vybraných řešení využívajících umělou inteligenci pro detekci phishingu a malwaru

Cílem této části je porovnat jednotlivá vybraná bezpečnostní řešení z hlediska jejich pořizovacích nákladů, a to v kontextu modelové firmy Finakta s.r.o., která disponuje 20 pracovními zařízeními. Vzhledem k tomu, že všechna uvažovaná řešení jsou navržena jako cloudové služby s minimálními požadavky na správu a technickou infrastrukturu, analýza se zaměřuje výhradně na licenční náklady, které by organizace musela uhradit za roční provoz.

Vzhledem k tomu, že jednotlivé společnosti uvádějí licenční ceny v eurech nebo amerických dolarech, budou náklady přepočítány na české koruny podle devizového kurzu České národní banky ke dni 11. 4. 2025, který činí:

- 1 EUR = 25,160 CZK
- 1 USD = 22,162 CZK

Tabulka 13 uvádí porovnání vybraných AI nástrojů z hlediska licenčního modelu a ročních nákladů. Ceny po přepočtu dle výše uvedeného kurzu byly následně zaokrouhleny na celé koruny.

Tabulka 13 Porovnání nákladů na implementaci AI řešení kybernetické bezpečnosti

Produkt	Licenční model	Roční náklady (měna)	Roční náklady (CZK)
Microsoft Defender for Business	2,8 EUR / uživatel / měsíc	672,00 EUR	16 903 CZK
Sophos Intercept X	65,76 USD / uživatel / roční plán	1 315,20 USD	29 147 CZK
	111,8 USD / uživatel / dvouroční plán	1 118,00 USD	24 777 CZK
	144,02 USD / uživatel / tříroční plán	960,13 USD	21 278 CZK
CrowdStrike Falcon Go	59,99 USD / zařízení / rok	1 999,80 USD	26 589 CZK
SentinelOne Singularity Control	79,99 USD / zařízení / rok	1 599,80 USD	35 442 CZK

Acronis Cyber Protect	56,76 EUR / zařízení / rok (roční plán)	1 135,20 EUR	28 562 CZK
	50,4 EUR / zařízení / rok (tříroční plán)	1 008,00 EUR	25 361 CZK
	44 EUR / zařízení / rok (pětiletý plán)	880,00 EUR	22 141 CZK

(zdroj: vlastní zpracování)

5.3.1 Normalizace finanční náročnosti

Pro potřeby vícekritériálního rozhodování je nezbytné převést vybrané kvantitativní ukazatele (v tomto případě roční finanční náklady na pořízení licencí) do jednotné bodové škály. K tomuto účelu byla zvolena metoda Min-Max normalizace, která umožňuje porovnat různě velké číselné hodnoty v rámci definovaného intervalu. Výsledné bodové hodnoty, získané na základě této metody, jsou uvedeny v tabulce 14 a slouží jako vstup do celkového hodnocení vhodnosti jednotlivých řešení. Výsledné bodové ohodnocení je zaokrouhleno na jedno desetinné místo.

Tabulka 14 Normalizace finanční náročnosti vybraných řešení

Produkt	Roční náklady	Výpočet bodů	Výsledek
Microsoft Defender for Business	16 903 CZK	$10 - \left(\frac{16903 - 16903}{35442 - 16903} \right) \times 9$	10,0
Sophos Intercept X	29 147 CZK	$10 - \left(\frac{29147 - 16903}{35442 - 16903} \right) \times 9$	4,1
	24 777 CZK	$10 - \left(\frac{24777 - 16903}{35442 - 16903} \right) \times 9$	6,2
	21 278 CZK	$10 - \left(\frac{21278 - 16903}{35442 - 16903} \right) \times 9$	7,9
CrowdStrike Falcon Go	26 589 CZK	$10 - \left(\frac{26589 - 16903}{35442 - 16903} \right) \times 9$	5,3
SentinelOne Singularity Control	35 442 CZK	$10 - \left(\frac{35442 - 16903}{35442 - 16903} \right) \times 9$	1,0
Acronis Cyber Protect	28 562 CZK	$10 - \left(\frac{28562 - 16903}{35442 - 16903} \right) \times 9$	4,3
	25 361 CZK	$10 - \left(\frac{25361 - 16903}{35442 - 16903} \right) \times 9$	5,9

	22 141 CZK	$10 - \left(\frac{22141 - 16903}{35442 - 16903} \right) \times 9$	7,5
--	------------	--	-----

(zdroj: vlastní zpracování)

5.3.2 Zhodnocení finanční náročnosti vybraných AI řešení

Finanční analýza pěti vybraných AI nástrojů pro kybernetickou ochranu subjektu Finakta s.r.o. odhalila podstatné rozdíly v ročních nákladech spojených s jejich pořízením a provozem. Srovnání bylo provedeno při jednotném předpokladu nasazení řešení pro 20 uživatelů nebo zařízení, a to na bázi jednoleté licence a při veřejně dostupných cenách. Celkové roční náklady na úrovni celé firmy se pohybují v rozmezí 16 903 až 35 442 Kč.

Z hlediska přímých nákladů vychází jako nejlevnější varianta řešení Microsoft Defender for Business, jehož cena činí přibližně 17 tisíc korun ročně. Ostatní produkty se pohybují v rozmezí 22–35 tisíc korun, přičemž ceny odrážejí rozdílnou hloubku pokrytí, úroveň ochrany i zaměření jednotlivých nástrojů (např. koncové body vs. zálohování).

Za zvláštní pozornost stojí produkty, které nabízejí víceleté licenční plány – konkrétně Sophos Intercept X a Acronis Cyber Protect. Tyto modely snižují jednotkovou cenu, čímž zvyšují cenovou atraktivitu při dlouhodobém nasazení. Například pětiletý plán Acronis Cyber Protect přináší roční náklady nižší než 23 000 Kč, což představuje značnou úsporu oproti roční licenci. Podobně tříletý plán Sophosu snižuje roční náklady na úroveň 21 278 Kč, v tomto případě se však vychází z cenové nabídky dostupné přes autorizované přeprodejce, neboť oficiální ceník výrobce tyto varianty přímo neuvádí.

Je však třeba dodat, že v kontextu rychlého vývoje AI technologií v oblasti kybernetické bezpečnosti může být uzavírání víceletých smluv problematické. Modelový subjekt by tím mohl omezit svou schopnost pružně reagovat na nové hrozby či výhodnější řešení na trhu. Proto lze za rozumnější zvolit roční model licencování, který umožňuje pravidelné přehodnocení účinnosti a relevance daného nástroje.

Celkově tedy platí, že mezi jednotlivými produkty existují výrazné rozdíly v pořizovacích nákladech, které mohou hrát klíčovou roli při rozhodování v prostředí malého podniku s omezeným rozpočtem.

5.4 Posouzení vhodnosti navrhovaných řešení pro subjekt Finakta s.r.o.

Tato kapitola se zaměřuje na hodnocení vhodnosti jednotlivých nástrojů využívajících umělou inteligenci v oblasti kybernetické bezpečnosti pro potřeby konkrétního modelového subjektu – firmy Finakta s.r.o. Cílem je určit, do jaké míry jednotlivá řešení odpovídají provozním, technickým a organizačním charakteristikám malé služby poskytující kancelářské a účetní činnosti.

Hodnocení je založeno na třech konkrétních kritériích:

- Kritérium 1: možnost bezproblémové integrace s prostředím Microsoft 365, které firma již využívá
- Kritérium 2: vhodnost z hlediska velikosti a typu organizace, zejména s ohledem na absenci vlastního IT oddělení
- Kritérium 3: rozsah funkčního pokrytí, tedy schopnost nástroje chránit před phishingem, malware a dalšími běžnými hrozbami

Každé řešení je v tabulce 15 hodnoceno bodově na škále od 1 do 10 pro každé ze tří stanovených kritérií, přičemž 1 představuje zcela nevyhovující stav a 10 maximální vhodnost z hlediska daného kritéria. Výsledné hodnocení každého nástroje je vypočteno jako aritmetický průměr všech tří dílčích známek, přičemž tento průměr slouží jako celková míra vhodnosti daného řešení pro potřeby firmy Finakta s.r.o.

Tato hodnota bude následně zohledněna ve finálním rozhodovacím procesu, kde bude propojena s výstupy finanční analýzy a použita jako vstup do multikritériálního vyhodnocení.

Tabulka 15 Hodnocení vybraných řešení kybernetické ochrany podle klíčových kritérií

Produkt	Kritérium	Hodnocení (stručný popis)	Bodové hodnocení
Microsoft Defender for Business	Kritérium 1	Nativní součást ekosystému Microsoft 365. Zajišťuje zcela bezproblémovou integraci a jednotnou správu v rámci známého uživatelského prostředí.	10
	Kritérium 2	Produkt je přímo navržen pro malé a střední podniky s důrazem na jednoduchost správy bez nutnosti vlastního IT oddělení.	10

	Kritérium 3	Nabízí komplexní ochranu koncových bodů, detekci hrozeb pomocí AI, pokrytí phishingu a správu zranitelností. Pokrývá běžné hrozby velmi dobře.	8
	Výsledné bodové hodnocení:		9,3
Sophos Intercept X	Kritérium 1	Podporuje integraci s M365, nicméně vyžaduje samostatnou správu přes Sophos Central.	8
	Kritérium 2	Vhodný pro malé i střední podniky, cloudová konzole Sophos Central je relativně přehledná. Nicméně nasazení obvykle probíhá přes partnera a vyžaduje základní orientaci v IT.	7
	Kritérium 3	Nabízí špičkovou ochranu proti malwaru, ransomwaru a exploitů s pokročilými funkcemi. Silné pokrytí běžných i pokročilých hrozeb.	10
	Výsledné bodové hodnocení:		8,3
CrowdStrike Falcon Go	Kritérium 1	Zaměřuje se především na ochranu koncových bodů. Integrace s M365 je možná, ale není nativní a integrace s Microsoft bezpečnostními centry je omezená.	7
	Kritérium 2	Vytvořeno explicitně pro menší firmy bez IT oddělení. Nabízí jednoduché nasazení, konfiguraci i provoz.	9
	Kritérium 3	Využívá technologii CrowdStrike pro detekci a prevenci hrozeb, poskytuje spolehlivou základní ochranu vhodnou pro SMB.	8
	Výsledné hodnocení:		8
SentinelOne Singularity Control	Kritérium 1	Nabízí možnost integrace, ale přímé propojení s M365 není určeno pro menší podniky bez IT. Vyžaduje samostatnou správu mimo M365 platformu.	7
	Kritérium 2	Balíček "Control" je základní, ale plnohodnotná verze SentinelOne. Správa je autonomní, nicméně nasazení a optimalizace může být náročnější pro firmy bez IT podpory.	8
	Kritérium 3	Vysoká úroveň behaviorální AI pro detekci a reakci na malware, ransomware a další útoky.	9
	Výsledné hodnocení:		8

Acronis Cyber Protect	Kritérium 1	Nabízí přímou integraci pro zálohování dat v M365. Integrace bezpečnostních funkcí je těsně spojena s prostředím Microsoft, včetně ochrany OneDrive a e-mailů.	9
	Kritérium 2	Řešení je běžně dodáváno formou služby, což usnadňuje správu pro firmy bez IT. Konsoliduje platformu pro bezpečnost a zálohu.	9
	Kritérium 3	Poskytuje kombinaci ochrany proti malwaru, řízení zranitelností, patch management, filtrování URL a integrované zálohování.	9
	Výsledné hodnocení:		9

(zdroj: vlastní zpracování)

5.4.1 Zhodnocení vhodnosti vybraných řešení

Na základě výše uvedené tabulky hodnocení jednotlivých bezpečnostních řešení podle tří definovaných kritérií lze konstatovat, že nejvhodnějším řešením pro potřeby modelové organizace Finakta s.r.o. je Microsoft Defender for Business.

Toto řešení dosáhlo nejvyššího hodnocení (9,3 z 10) díky své plné integraci s Microsoft 365, jednoduchosti nasazení a správy bez nutnosti specializovaného IT personálu a solidnímu rozsahu bezpečnostních funkcí, které dostatečně pokrývají běžné hrozby.

Acronis Cyber Protect, které se umístilo na druhém místě (9,0 bodů), je zajímavé zejména pro firmy, které kromě kybernetické ochrany vyžadují i integrované zálohování dat. Jeho přidanou hodnotou je vysoká úroveň automatizace a služební model vhodný pro firmy bez vlastní IT infrastruktury. Výhodou je také jeho rozšířená integrace s Microsoft 365, zejména v oblasti datové bezpečnosti.

Sophos Intercept X dosahuje velmi dobrých výsledků z hlediska bezpečnostního pokrytí, avšak nižší hodnocení u ostatních kritérií odráží vyšší nároky na správu a potřebu nasazení prostřednictvím partnera.

CrowdStrike Falcon Go a SentinelOne Singularity jsou rovněž kvalitní řešení vhodná pro segment malých a středních podniků. Falcon Go boduje zejména jednoduchostí a vhodností pro firmy bez IT, zatímco SentinelOne vyniká technologickou vyspělostí. Jejich slabší stránkou v tomto srovnání je složitější integrace s Microsoft 365.

5.5 Výběr konkrétního řešení pro modelový subjekt

Na základě výsledků finanční analýzy v části 5.3 a hodnocení vhodnosti řešení pro organizaci Finakta s.r.o. v části 5.4 bude provedeno vícekritériální porovnání všech posuzovaných nástrojů za užití metody váženého součtu. Cílem je určit nejvhodnější AI nástroj pro kybernetickou ochranu modelové firmy s ohledem na cenovou dostupnost i technickou a provozní vhodnost.

Hodnoticí kritéria a váhy:

V rámci hodnocení byla zvolena dvě klíčová kritéria:

A – Finanční náročnost (váha 40 %)

B – Vhodnost řešení pro organizaci Finakta s.r.o. (váha 60 %)

Přestože je cena důležitým faktorem, zejména v kontextu menší organizace s omezeným rozpočtem, hlavní důraz byl kladen na celkovou vhodnost řešení pro konkrétní potřeby firmy. Ta zahrnuje nejen funkční pokrytí a možnosti integrace do stávajícího prostředí, ale i schopnost nástroje efektivně fungovat v podmínkách organizace bez vlastního IT oddělení.

Finanční stránka tedy byla zohledněna výrazně, nikoli však dominantně, protože i cenově dostupné řešení ztrácí na hodnotě, pokud není prakticky využitelné nebo nezajišťuje potřebnou úroveň ochrany. Zvolený poměr 60:40 tak umožňuje zohlednit jak provozní realitu malého podniku, tak technickou a organizační efektivitu daného nástroje.

Kritériální hodnocení jednotlivých řešení zobrazuje tabulka 16.

Tabulka 16 Kritériální hodnocení vybraných řešení pro modelový subjekt

Produkt	Cena (body)	Vhodnost (body)	Výpočet	Výsledek
Microsoft Defender for Business	10	9,3	$(0,4 \times 10) + (0,6 \times 9,3)$	9,58
Sophos Intercept X (roční)	4,1	8,3	$(0,4 \times 4,1) + (0,6 \times 8,3)$	6,62
Sophos Intercept X (dvouroční)	6,2	8,3	$(0,4 \times 6,2) + (0,6 \times 8,3)$	7,46
Sophos Intercept X (tříroční)	7,9	8,3	$(0,4 \times 7,9) + (0,6 \times 8,3)$	8,14
CrowdStrike Falcon Go	5,3	8,0	$(0,4 \times 5,3) + (0,6 \times 8)$	6,92

SentinelOne Singularity Control	1,0	8,0	$(0,4 \times 1) + (0,6 \times 8)$	5,20
Acronis Cyber Protect (roční)	4,3	9,0	$(0,4 \times 4,3) + (0,6 \times 9)$	7,12
Acronis Cyber Protect (tříroční)	5,9	9,0	$(0,4 \times 5,9) + (0,6 \times 9)$	7,76
Acronis Cyber Protect (pětiletý)	7,5	9,0	$(0,4 \times 7,5) + (0,6 \times 9)$	8,40

(zdroj: vlastní zpracování)

Pro větší přehlednost budou tyto výsledky převedeny do tabulky 17 seřazené sestupně (od nejlepšího po nejhorší řešení), a to za účelem poskytnutí uceleného přehledu analýzy vybraných řešení pro modelový subjekt.

Tabulka 17 Výsledné pořadí posuzovaných řešení pro modelový subjekt

Pořadí	Produkt	Cena (body)	Vhodnost (body)	Výsledek
1	Microsoft Defender for Business	10,0	9,3	9,58
2	Acronis Cyber Protect (pětiletý)	7,5	9,0	8,40
3	Sophos Intercept X (tříroční)	7,9	8,3	8,14
4	Acronis Cyber Protect (tříroční)	5,9	9,0	7,76
5	Sophos Intercept X (dvouroční)	6,2	8,3	7,46
6	Acronis Cyber Protect (roční)	4,3	9,0	7,12
7	CrowdStrike Falcon Go	5,3	8,0	6,92
8	Sophos Intercept X (roční)	4,1	8,3	6,62
9	SentinelOne Singularity Control	1,0	8,0	5,20

(zdroj: vlastní zpracování)

5.5.1 Vyhodnocení výběru řešení pro modelový subjekt

Na základě vícekritériálního hodnocení pro potřeby modelové organizace Finakta s.r.o., bylo stanoveno celkové skóre pro každé z posuzovaných AI nástrojů. Nejlépe hodnoceným

řešením se stal Microsoft Defender for Business, který dosáhl nejvyššího souhrnného bodového výsledku a vykazuje optimální rovnováhu mezi cenovou dostupností a technickou vhodností pro malé podniky bez vlastního IT zázemí.

Na dalších místech se umístily nástroje Acronis Cyber Protect a CrowdStrike Falcon Go, které rovněž dosáhly velmi solidních výsledků, avšak s určitými kompromisy ve funkčním pokrytí nebo míře integrace. Ostatní řešení vykázala nižší skóre především z důvodu vyšší ceny nebo technologické komplexnosti, která by mohla být pro daný typ organizace nevhodná.

5.6 Návrh implementace doporučeného řešení

Na základě výsledků byl jako nejvhodnější nástroj pro potřeby modelového subjektu Finakta s.r.o. zvolen Microsoft Defender for Business. Tato kapitola se zaměřuje na návrh jeho nasazení do prostředí firmy tak, aby byla zajištěna maximální míra ochrany při minimálních nárocích na provoz a správu.

5.6.1 Předpoklady implementace

Organizace Finakta s.r.o. je menší firma s přibližně 20 zařízeními (notebooky a stolní počítače), která ke své každodenní práci využívá cloudové nástroje v rámci předplatného Microsoft 365 Business Standard. Firma nedisponuje vlastním IT oddělením, běžná správa je zajišťována prostřednictvím externího dodavatele IT služeb. Tato výchozí situace plně odpovídá předpokladům nástroje Microsoft Defender for Business, který je navržen jako jednoduché, integrované a automatizované řešení pro malé a střední podniky.

5.6.2 Postup nasazení řešení

Zavedení řešení Microsoft Defender for Business do prostředí firmy Finakta s.r.o. by probíhalo v několika navazujících krocích, které lze zvládnout bez výrazné organizační zátěže. Celý proces je možné realizovat buď interně (v případě základních IT znalostí), nebo ve spolupráci s externím správcem informačních technologií.

Prvním krokem by bylo zajištění potřebných licencí a aktivace služby v rámci prostředí Microsoft 365, které již firma využívá. Na to navazuje samotné zavedení ochranných funkcí na jednotlivá zařízení zaměstnanců – tento proces je možné provést hromadně, čímž se výrazně snižuje časová i technická náročnost.

Po úspěšném nasazení by bylo vhodné nastavit základní bezpečnostní pravidla, ale vzhledem k vysoké míře automatizace však není nutné provádět složité manuální nastavení – lze využít doporučené výchozí konfigurace.

Součástí zavedení řešení by mělo být i krátké proškolení uživatelů, které by mohlo mít podobu jednoduché instruktáže zaměřené na ovládací prvky daného softwaru, práci s výstrahami a případně i na rozpoznávání základních kybernetických hrozeb.

Z hlediska provozu by bylo důležité zajistit základní dohled nad výstupy systému – např. pravidelnou kontrolu hlášení o detekovaných hrozbách, a případnou úpravu nastavení podle aktuálního vývoje hrozeb nebo potřeb firmy.

5.6.3 Časový rámec implementace

Celý proces nasazení lze zrealizovat v horizontu 7 až 14 dnů, a to včetně školení uživatelů a testovací fáze. V případě využití externího IT správce může být implementace dokončena i během několika dní, jelikož veškerá konfigurace probíhá v cloudovém prostředí bez nutnosti zásahu do fyzické infrastruktury firmy.

5.6.4 Přínosy pro subjekt Finakta s.r.o

Zavedením Microsoft Defender for Business získá organizace Finakta s.r.o. následující výhody:

- Komplexní ochranu proti phishingovým útokům, malwaru, ransomware a dalším hrozbám v rámci jednoho nástroje.
- Snadnou správu bez nutnosti budování vlastní IT infrastruktury nebo týmu specialistů.
- Úzkou integraci s prostředím Microsoft 365, které je již ve firmě používáno.
- Nízké provozní náklady, díky jednoduchému licencování a absenci potřeby dalšího softwaru či hardwaru.

6 DISKUSE

Praktická část této diplomové práce se zaměřila na analýzu a aplikaci nástrojů umělé inteligence pro detekci kybernetických hrozeb, konkrétně malwaru a phishingu, v prostředí modelového subjektu Finakta s.r.o. Výsledky této aplikace jsou v souladu s teoretickými východisky uvedenými v první části práce, a zároveň poukazují na několik klíčových aspektů, které potvrzují i rozvíjejí aktuální poznatky v oblasti AI a kybernetické bezpečnosti.

V teoretické části byla umělá inteligence prezentována jako adaptivní nástroj schopný rozpoznávat vzory a predikovat chování na základě dat. To se v praxi potvrdilo zejména při analýze pokročilých metod detekce phishingu, jejichž přesnost překonává tradiční přístupy založené na blacklistech či filtraci klíčových slov. Zvláště výrazně se osvědčilo hluboké učení, které je schopné identifikovat sofistikované útoky i při změněném kontextu nebo jazykové formě.

Porovnání tradičních a AI přístupů v oblasti detekce malwaru rovněž ukázalo významný posun. Zatímco signaturní detekce je účinná pouze proti známým hrozbám, AI umožňuje identifikaci tzv. zero-day útoků a variant, které se doposud v systému nevyskytly. Tento fakt potvrzují teoretická východiska o adaptabilitě neuronových sítí a jejich schopnosti rozpoznávat anomálie v reálném čase. Výsledky vícekritériální analýzy rovněž ukázaly, že nástroje s AI jsou nejen technologicky pokročilé, ale v určitých případech i ekonomicky dostupné, pokud se zohlední celkové náklady na riziko a lidský faktor.

Zvláštní pozornost si pak zaslouží otázka implementace AI do prostředí malého podniku, jako je Finakta s.r.o. Praktická část ukázala, že výběr a nasazení AI nástroje je reálně proveditelné a finančně zvládnutelné i bez podpory interního IT oddělení, za předpokladu volby systému s intuitivním rozhraním a kvalitní uživatelskou podporou. Tím se potvrzuje rostoucí trend zpřístupňování těchto technologií širšímu spektru organizací, včetně menších podniků, které dříve neměly kapacity či zdroje pro jejich nasazení.

Závěrem lze konstatovat, že dosažené výsledky jsou v souladu s teoretickými poznatky, a v některých oblastech (např. finanční dostupnost AI řešení pro malé podniky) je dokonce rozvíjejí. AI se ukazuje jako klíčová technologie pro budoucnost kybernetické bezpečnosti, jejíž praktické nasazení je již dnes nejen technologicky, ale i ekonomicky realizovatelné.

ZÁVĚR

Cílem této diplomové práce bylo navrhnout prakticky realizovatelné řešení kybernetické bezpečnosti pro modelový subjekt – malý podnik Finakta s.r.o. – prostřednictvím výběru a aplikace nástroje využívajícího umělou inteligenci (AI), se zaměřením na detekci malwaru a phishingu. V průběhu práce byly rovněž naplněny všechny stanovené dílčí cíle a ověřeny tři pracovní hypotézy.

Hlavní cíl práce byl naplněn prostřednictvím vícekritériální analýzy komerčně dostupných řešení a návrhu konkrétního bezpečnostního systému pro podnik Finakta s.r.o., včetně jeho implementačního rámce. Zvolený nástroj byl posouzen z hlediska efektivity detekce, technických požadavků, nákladovosti a celkové vhodnosti pro menší organizaci bez interního IT oddělení.

Byly ověřeny následující pracovní hypotézy:

- H1: Potvrdilo se, že nástroje založené na AI skutečně dosahují vyšší přesnosti než tradiční přístupy, a to zejména v případě sofistikovaných phishingových kampaní a dosud neznámých variant malwaru.
- H2: Bylo prokázáno, že na trhu existují AI nástroje (např. Microsoft Defender for Business), které jsou technicky i finančně vhodné pro nasazení v malých podnicích bez specializovaného IT týmu.
- H3: Analýza a návrh řešení potvrdily, že implementace doporučeného nástroje vede ke zvýšení bezpečnostní úrovně organizace, aniž by vyžadovala zásadní zásahy do její existující IT a datové infrastruktury.

Umělá inteligence se v oblasti kybernetické bezpečnosti ukazuje jako výrazně účinnější alternativa ke klasickým metodám detekce hrozeb. Z provedené analýzy vyplývá, že nástroje využívající strojové a hluboké učení – zejména v kombinaci s přístupy z oblasti zpracování přirozeného jazyka – vykazují vyšší úspěšnost při odhalování komplexních a adaptivních útoků, u nichž běžné metody často selhávají.

Vícekritériální analýza na základě technických, funkčních a ekonomických parametrů prokázala, že existují dostupná AI řešení vhodná i pro malé podniky bez vlastního IT zázemí. Nejlépe se osvědčily nástroje, které kombinují vysokou detekční schopnost s přívětivým uživatelským rozhraním, přiměřenou cenovou politikou a snadnou implementací do reálného provozu.

Navržené řešení pro podnik Finakta s.r.o. se ukázalo jako technicky proveditelné, finančně únosné a organizačně udržitelné. Návrh reflektoval specifika provozního prostředí, byl doplněn časovým rámcem, popisem vstupních předpokladů i očekávaných přínosů. Významným faktorem je skutečnost, že doporučené řešení nevyžaduje výraznější úpravy stávající infrastruktury – což je v případě malých a středních podniků zásadní.

Významným přínosem této práce je rovněž formulace přenositelného metodického postupu pro výběr AI nástroje kybernetické ochrany. Tento rámec je možné aplikovat na další subjekty obdobného typu, což zvyšuje praktickou využitelnost výsledků nejen v rámci jednoho podniku, ale i na širší úrovni malých a středních organizací.

Umělá inteligence dnes představuje jeden z nejpokročilejších nástrojů v oblasti kybernetické bezpečnosti. Její schopnost adaptivního učení, prediktivní analýzy a autonomního rozhodování jí zajišťuje výsadní postavení nejen při detekci hrozeb, ale i při jejich aktivní prevenci. A vskutku, tato práce potvrdila, že AI je již dnes prakticky využitelná i v menších organizacích a její význam bude v následujících letech dále sílit.

Současně však platí, že čím mocnější nástroj držíme v rukou, tím snáze může být zneužit. Technologie, které dnes chrání firmy před hrozbami, mohou být zároveň nasazeny útočníky – například při generování personalizovaných phishingových útoků, vytváření deepfake podvodů či obcházení detekčních systémů. Tato dvojsečnost vyvolává závažné otázky nejen technického, ale i etického a právního charakteru.

Z těchto důvodů by se další výzkum v oblasti umělé inteligence neměl soustředit výlučně na technologický rozvoj, ale měl by se aktivně zabývat také otázkami etiky, transparentnosti rozhodovacích procesů a odpovědné regulace AI systémů. Právě zde bude nutné v blízké budoucnosti hledat vyvážený přístup mezi technologickým pokrokem, bezpečností a ochranou základních práv v rámci demokratické digitální společnosti.

SEZNAM POUŽITÉ LITERATURY

ABBADI, Dhafer. *Cyber Threats and Risk Mitigation Strategies for Cloud Systems and the Internet of Things*. Preprints [online]. 2025. Dostupné z: https://www.preprints.org/frontend/manuscript/ffb288da910b3abfe715b0464774852e/download_pub. [cit. 2025-02-22].

ACRONIS, 2025. Acronis Cyber Protect. Online. Dostupné z: <https://www.acronis.com/en-eu/#business>. [cit. 2025-04-12].

AGGREY, Richard; ADJEI, Bright Ansah; AFODOU, Karl Osei a DSANE, Nana Adwoa Konadu. *Analysing Recent APT Incidents: Case Studies and Lessons Learned*. ResearchGate [online]. 2025. Dostupné z: https://www.researchgate.net/profile/Richard_Aggrey/publication/387298480_Analysing_Recent_APT_Incidents_Case_Studies_and_Lessons_Learned/links/6766d370e74ca64e1f2412dd/Analysing-Recent-APT-Incidents-Case-Studies-and-Lessons-Learned.pdf. [cit. 2025-02-22].

AJAYI, E. F. G. *Challenges to enforcement of cyber-crimes laws and policy*. Journal of Internet and Information Systems [online]. 2016, roč. 7, č. 1, s. 12–25. Dostupné z: <https://academicjournals.org/journal/JIIS/article-full-text-pdf/930ADF960210/1000>. [cit. 2025-02-28].

ALANEZI, Mafaz. *Phishing Detection Methods: A Review* [online]. 2021, roč. 3, č. 9, s. 19–35. Technium. ISSN 2668-778X. Dostupné z: https://www.researchgate.net/publication/355896081_Phishing_Detection_Methods_A_Review. [cit. 2025-03-24].

ALAZAB, M.; AWAJAN, A; a FARUQUI, N. *AI-based Adversarial Defense in Cybersecurity*. IEEE [online]. 2025. Dostupné z: <https://ieeexplore.ieee.org/abstract/document/10836696>. [cit. 2025-03-15].

ALI, Sajid. *Enhancing Endpoint Security with AI: Machine Learning Approaches to Malware Prevention*. ResearchGate [online]. 2024. Dostupné z: <https://www.researchgate.net/publication/388523706>. [cit. 2025-03-15].

ALIYEVA, Tarlan. *Investigation of Cyberattack and Intrusion: Methods and Tool*. IntechOpen [online]. 2025. Dostupné z: <https://www.intechopen.com/online-first/1209643>. [cit. 2025-02-21].

AL-ARAJI, Zainab H. *A Survey on Bio-Inspired Algorithm for SQL Injection Attacks: Survey on Bio-Inspired Algorithm for SQL Injection Attacks*. Basrah Researches Sciences [online]. 2024. Dostupné z: <https://jou.jobrs.edu.iq/index.php/home/article/view/112>. [cit. 2025-02-22].

AL-HARBI, Ahmad. *The Impact of AI on Financial Professionals*. Online. Journal of Next-Generation Research 5.0. S. 13. ISSN 3075-2868. 2025. Dostupné z: <https://jngr5.com/index.php/journal-of-next-generation-resea/article/download/84/68>. [cit. 2025-02-15].

AL-SINANI, Hassan Said a MITCHELL, Charles J. *PenTest++: Elevating Ethical Hacking with AI and Automation*. arXiv preprint [online]. 2025. Dostupné z: <https://arxiv.org/pdf/2502.09484>. [cit. 2025-02-20].

AMOA, Godwin A. a HAYFRON-ACQUAH, J. B. *QR Code Security: Mitigating the Issue of Quishing (QR Code Phishing)*. International Journal of Computer Science. 2022. Dostupné z: https://www.researchgate.net/profile/Godwin-Awuah-Amoah-2/publication/364593009_QR_Code_Security_Mitigating_the_Issue_of_Quishing_QR_Code_Phishing/links/6356ab206e0d367d91c0a7cb/QR-Code-Security-Mitigating-the-Issue-of-Quishing-QR-Code-Phishing.pdf. [cit. 2025-03-13].

AZZAM, S. M.; EMAM, O. E. a ABOHANY, A. A. *Deep Learning-based Intrusion Detection for Cybersecurity*. Springer [online]. 2024. Dostupné z: <https://link.springer.com/article/10.1186/s40537-024-00957-y>. [cit. 2025-03-15].

BEAUMARCHAIS, J.; WEBER, P.; CALLAGHAN, N. a BAUER, G. *Integrated dynamic behavioral fingerprinting for real-time ransomware detection: A pattern-based classification*. OSF [online]. 2024. Dostupné z: <https://osf.io/9ehbq/download>. [cit. 2025-03-15].

BELLO, Halima Oluwabunmi. *Integrating Behavioral Biometrics and Machine Learning to Combat Evolving Cybercrime Tactics in Financial Systems*. ResearchGate [online]. 2025. Dostupné z: https://www.researchgate.net/publication/388851586_Integrating_Behavioral_Biometrics_and_Machine_Learning_to_Combat_Evolving_Cybercrime_Tactics_in_Financial_Systems. [cit. 2025-02-20].

BLAKE, Harrison. *Comparative Analysis of Traditional AI and Generative AI in Threat Detection and Mitigation*. ResearchGate [online]. 2025. Dostupné z: <https://www.researchgate.net/publication/388930848>. [cit. 2025-02-20].

BOČÁNEK, Petr; NOVOTNÝ, Jakub a VESELÝ, Ondřej. *The impact of AI on cybersecurity and personal data protection in the Czech Republic*. Masaryk University Journal [online]. 2024. Dostupné z: <https://journals.muni.cz/revue/article/download/39865/33637>. [cit. 2025-02-27].

BIRTHRIYA, Santosh Kumar; AHLAWAT, Poonam a JAIN, Ankit Kumar. *An Efficient Spam and Phishing Email Filtering Approach using Deep Learning and Bio-inspired Particle Swarm Optimization*. International Journal of Computing and Digital Systems [online]. 2024. ISSN 2210-142X. Dostupné z: <https://www.researchgate.net/publication/387127632>. [cit. 2025-04-03].

BRANCO, Rodrigo; COGO, Victor a MEDEIROS, Igor. *Towards a Web Application Attack Detection System Based on Network Traffic and Log Classification*. ENASE [online]. 2024. Dostupné z: https://di.fc.ul.pt/~imedeiros/papers/ENASE2024_RodrigoB.pdf. [cit. 2025-02-15].

BRENNER, Susan W. *Cybercrime and the Law: Challenges, Issues, and Outcomes*. Cambridge: Cambridge University Press, 2012. ISBN 978-1-107-00512-9.

BROOKS, Charles J.; GROW, Christopher; CRAIG, Philip a SHORT, Donald. *Cybersecurity essentials*. Indianapolis, Indiana: Sybex, John Wiley, 2018. ISBN 978-1-119-36239-5.

BUTT, Junaid Sattar. *Analytical Study of the World's First EU Artificial Intelligence (AI) Act, 2024*. International Journal of Research Publication and Reviews, 2024, roč. 5, č. 3, s. 7343–7364. ISSN 2582-7421. Dostupné z: <https://www.researchgate.net/publication/384675254>. [cit. 2025-03-09].

CALDER, Alan a WATKINS Steve. *IT Governance – An International Guide to Data Security and ISO 27001/ISO 27002 (8th Edition)*. Eighth. IT Governance Publishing, 2024. ISBN 1787784096

CEN, Mingcan.; JIANG, Frank. a DOSS, Robin. *RansoGuard: A RNN-based framework leveraging pre-attack sensitive APIs for early ransomware detection*. Computers & Security

- [online]. 2025. Dostupné z: <https://www.sciencedirect.com/science/article/pii/S0167404824005996>. [cit. 2025-03-15].
- CHAPPLE, Mike a NIJIM, Samer. *Database Security*. IEEE Xplore [online]. 2024. Dostupné z: <https://ieeexplore.ieee.org/abstract/document/10508518/>. [cit. 2025-02-21].
- CROWDSTRIKE, 2025. CrowdStrike Falcon Go. Online. Dostupné z: <https://www.crowdstrike.com/en-us/products/>. [cit. 2025-04-12].
- ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) - znění od 6. 8. 2022. In: *Zákony pro lidi.cz* [online]. © AION CS 2010–2025. Dostupné z: <https://www.zakonyprolidi.cz/cs/2014-181#f5278850>. [cit. 2025-02-24]
- ČESKO. Zákon č. 110/2019 Sb., o zpracování osobních údajů. In: *Zákony pro lidi.cz* [online]. © AION CS 2010–2025. Dostupné z: <https://www.zakonyprolidi.cz/cs/2019-110>. [cit. 2025-02-27].
- DISTERER, Gerhard. *ISO/IEC 27000, 27001 and 27002 for information security management*. Journal of Information Security [online]. 2013. Dostupné z: https://serwiss.bib.hs_hannover.de/files/938/ISOIEC_27000_27001_and_27002_for_Information_Security_Management.pdf. [cit. 2025-03-02].
- DODIYA, Kiran; KUMAR, K. a SHARMA, P. *CYBERSECURITY'S NEW FRONTIER: AI-Driven Innovations Against Malware Threats*. ResearchGate [online]. 2025. Dostupné z: <https://www.researchgate.net/publication/384232040>. [cit. 2025-03-15].
- DUŠEK, Marek. *GDPR, AI and the challenges of personal data security in the digital age*. Academia.edu [online]. 2023. Dostupné z: https://www.academia.edu/download/104505854/admsci_13_00154.pdf. [cit. 2025-02-27].
- ENTERPRISEAV, 2025. Sophos Central Intercept X Advanced. Online. Dostupné z: <https://www.enterpriseav.com/Intercept-X-Adv.asp?>. [cit. 2025-04-12].
- EVROPSKÁ UNIE. *Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. Úřední věstník Evropské unie, L 119, 4.5.2016. Dostupné z: <https://data.europa.eu/eli/reg/2016/679/oj>. [cit. 2025-03-09].

EVROPSKÁ UNIE. *Nařízení Evropského parlamentu a Rady (EU) 2024/1689 o umělé inteligenci*. Úřední věstník Evropské unie, 2024. Dostupné z: <http://data.europa.eu/eli/reg/2024/1689/oj>. [cit. 2025-03-09].

EVROPSKÁ UNIE. *Prováděcí nařízení Komise (EU) 2024/2690 ze dne 17. října 2024, kterým se stanoví pravidla pro uplatňování směrnice (EU) 2022/2555, pokud jde o technické a metodické požadavky na opatření k řízení kybernetických bezpečnostních rizik a bližší upřesnění případů, v nichž se incident považuje za významný*. Úřední věstník Evropské unie, L 2690, 18.10.2024. Dostupné z: https://data.europa.eu/eli/reg_impl/2024/2690/oj. [cit. 2025-03-09].

EVROPSKÁ UNIE. *Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)*. Úřední věstník Evropské unie, L 333, 27.12.2022. Dostupné z: <https://data.europa.eu/eli/dir/2022/2555/oj>. [cit. 2025-03-09].

FARIS, S.; MEDROMI, H.; EL HASNAOUI, S.; IGUER, H. a SAYOUTI, A. *Toward an Effective Information Security Risk Management of Universities' Information Systems Using Multi Agent Systems, ITIL, ISO 27002, ISO 27005*. International Journal of Advanced Computer Science and Applications, Vol. 5, No. 6, 2014. Dostupné z: <https://www.ijacsa.thesai.org>. [cit. 2025-03-02].

FERNANDES, Filipe S.; BESSA, Ricardo J. *Evolving Symbolic Model for Dynamic Security Assessment in Power Systems*. IEEE Transactions on Modern Power Systems [online]. 2025. Dostupné z: <https://ieeexplore.ieee.org/abstract/document/10858603/>. [cit. 2025-02-15].

FERRAG, Mohamed Amine; FRIHA, Otman; MAGLARAS, Leandros a JANICKE, Helge. *Federated deep learning for cyber security in the internet of things: Concepts, applications, and experimental analysis*. IEEE Access, 2021. Dostupné z: <https://ieeexplore.ieee.org/abstract/document/9562531>. [cit. 2025-03-10].

FERRAG, Mohamed Amine; MAGLIARELLA, Maria; PIASTRELLI, Francesca et al. *Generative AI in Cybersecurity: A Comprehensive Review of LLM Applications and Vulnerabilities*. Internet of Things and Cybersecurity [online]. 2025. Dostupné z: <https://www.sciencedirect.com/science/article/pii/S2667345225000082>. [cit. 2025-02-20].

GALLI, A.; LA GATTA, V.; MOSCATO, V. a POSTIGLIONE, M. *Explainability in AI-based Behavioral Malware Detection Systems*. ScienceDirect [online]. 2024. Dostupné z: <https://www.sciencedirect.com/science/article/pii/S0167404824001433>. [cit. 2025-03-15].

GÉRON, Aurélien. *Hands-On Machine Learning with Scikit-Learn, Keras and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems*. 2nd edition. Sebastopol, California: O'Reilly Media, 2019. ISBN 978-1-492-03264-9.

GILLIES, Alan. *Improving the quality of information security management systems with ISO27000*. The TQM Journal [online]. 2011. Dostupné z: <https://doi.org/10.1108/17542731111139455>. [cit. 2025-03-02].

GONG, Ke, 2025. *On artificial intelligence and how to develop, teach and govern it*. Online. *Cultures of Science*. S. 5. Dostupné z: <https://doi.org/10.1177/20966083251315257>. [cit. 2025-02-15].

GRITZALIS, Dimitris; CHOO, Kim-Kwang Raymond a PATSAKIS, Constantinos. *Malware*. Springer [online]. 2024. Dostupné z: <https://link.springer.com/content/pdf/10.1007/978-3-031-66245-4.pdf>. [cit. 2025-02-21].

GUPTA, Ankur.; SAWHNEY, Sahil. a AHMED, Suhaib. *Secure Internet of Things Device with Single-Channel Communication for Resource-Constrained Applications*. MDPI [online]. 2025. Dostupné z: <https://www.mdpi.com/2673-4591/78/1/9>. [cit. 2025-02-22].

GURURAJ, L.; JANHAVI, V. a AMBIKA, V., 2024. *Social Engineering in Cybersecurity: Threats and Defenses*. CRC Press. ISBN 978-1-032-52440-5.

GUTIERREZ, Rommel; VILLEGAS-CH., William; NARANJO GODOY, Lorena; MERA-NAVARRETE, Aracely a LUJÁN-MORA, Sergio. *Application of Deep Learning Models for Real-Time Automatic Malware Detection*. IEEE Access [online]. 2024. Dostupné z: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10620215>. [cit. 2025-03-16].

HATAMLEH, Hazem; ALNASER, Mahmoud; SALOUM, Said a SHARADQEH, Ahmed. *PictureGuard: Enhancing Software-Defined Networking–Internet of Things Security with Novel Image-Based Authentication and Artificial Intelligence-Powered Systems*. MDPI [online]. 2025. Dostupné z: <https://www.mdpi.com/2227-7080/13/2/55>. [cit. 2025-02-22].

HASSAN, Mohammed. *Evaluation of Deep Learning Algorithms in Comparison for Phishing Email Identification*. Applied Mathematics on Science and Engineering [online].

2024. 1 (1): 21 – 35. Dostupné z: <https://www.furthersci.org/journal-admin/uploads/articles/amse113.pdf>. [cit. 2025-04-03].

HEWES, Charles A. *Threat and challenges of cyber-crime and the response*. SAM Advanced Management Journal [online]. 2016, roč. 81, č. 3, s. 18–29. Dostupné z: <https://search.proquest.com/openview/7716c4878859466d45fa4173f91a2f50/1?pq-origsite=gscholar&cbl=40946>. [cit. 2025-02-28].

IQBAL, J. a RAHBI, F. *The Evolution of Ransomware: AI-Powered Detection and Prevention Strategies*. ResearchGate [online]. 2025. Dostupné z: <https://www.researchgate.net/publication/388103178>. [cit. 2025-03-15].

JANABI, Ahmed Hasan; KANAKIS, Triantafyllos a JONSHON Mark. *Survey: Intrusion Detection System in Software-Defined Networking*. ResearchGate [online]. 2024. Dostupné z: https://www.researchgate.net/profile/Ahmed_Janabi_/publication/385628063_Survey_Intrusion_Detection_System_in_Software_Defined_Networking/links/6735963c4a70511f071e0734/Survey-Intrusion-Detection-System-in_Software-Defined-Networking.pdf. [cit. 2025-02-22].

JOSEPH, Sunday; AJAYI, Adekunbi Justina; METIBEMU, Olofunke Cynthia et al. *The Impact of Artificial Intelligence on Cyber Security in Digital Currency Transactions*. ResearchGate [online]. 2025. Dostupné z: https://www.researchgate.net/publication/388997716_The_Impact_of_Artificial_Intelligence_on_Cyber_Security_in_Digital_Currency_Transactions. [cit. 2025-02-20].

KAUR, Ramanpreet; GABRIJELČIČ, Dušan a KLOBUČAR, Tomaž. *Artificial intelligence for cybersecurity: Literature review and future research directions*. Information Fusion. (101804), 29. 2023. ISSN 1566-2535.

KHAN, M. F. a RANA B. L. *Detection of Phishing Websites Using Deep Learning Techniques*. Turkish Journal of Computer and Mathematics Education [online]. 2021. Dostupné z: <https://www.proquest.com/docview/2628339739?pq-origsite=gscholar&fromopenview=true&sourcetype=Scholarly%20Journals>. [cit. 2025-04-04].

KLOO, Ian, 2024. *Automated Misinformation Detection with Natural Language Processing and Network Science Models*. Pittsburgh: School of Computer Science Carnegie Mellon

University [online]. Dostupné z: https://iankloo.github.io/thesis_proposal.pdf. [cit. 2025-02-20].

KOLOUCH, Jan a BAŠTA, Pavel. *Cybersecurity*. Praha: CZ.NIC, z.s.p.o. CZ.NIC, 2019. ISBN 978-80-88168-31-7.

KOOPS, Bert-Jaap. *Criminal law and cyberspace as a challenge for legal research*. SCRIPTed [online]. 2012, roč. 9, č. 2, s. 115–135. DOI: [10.2966/scrip.090212.115](https://doi.org/10.2966/scrip.090212.115). [cit. 2025-02-28].

LI, Shanxi; ZHOU, Qingguo; ZHOU, Rui a LV, Qingquan. *Intelligent malware detection based on graph convolutional network*. The Journal of Supercomputing [online]. 2022, roč. 78, č. 4182–4198. DOI: [10.1007/s11227-021-04020-y](https://doi.org/10.1007/s11227-021-04020-y). [cit. 2025-03-16].

MACRON, Tolu. *Generative AI and Cybersecurity: Analyzing the Dual Use of Deepfake Technology for Threats and Defensive Measures*. ResearchGate [online]. 2025. Dostupné z: https://www.researchgate.net/profile/Tolu_Macron/publication/388323713_Generative_AI_and_Cybersecurity_Analyzing_the_Dual_Use_of_Deepfake_Technology_for_Threats_and_Defensive_Measures/links/6792cbc94c479b26c9b18872/Generative-AI-and-Cybersecurity-Analyzing-the-Dual-Use-of-Deepfake-Technology-for-Threats-and-Defensive-Measures.pdf. [cit. 2025-03-13].

MAILEWA, Akalanka B.; ALI, A.; OVERBOE, C. a MOHOTTALALAGE, T. *The Human Factor in Cybersecurity: Understanding Psychology, Training Efficacy, and Error Reduction Strategies*. ResearchGate [online]. 2025. Dostupné z: https://www.researchgate.net/profile/Akalanka_Mailewa/publication/387971383_The_Human_Factor_in_Cybersecurity_Understanding_Psychology_Training_Efficacy_and_Error_Reduction_Strategies/links/6785c5642be36743a5d55455/The-Human-Factor-in-Cybersecurity-Understanding-Psychology-Training-Efficacy-and-Error-Reduction-Strategies.pdf. [cit. 2025-02-22].

MANDRU, Sri-Kanth. *Defending Against Social Engineering: Techniques and Best Practices*. ResearchGate [online]. 2025. Dostupné z: https://www.researchgate.net/profile/Sri_Kanth_Mandru/publication/384749931_Defending_Against_Social_Engineering_Techniques_and_Best_Practices/links/67a103d4207c0c20fa7497f9/Defending-Against-Social-Engineering-Techniques-and-Best-Practices.pdf. [cit. 2025-02-21].

MANJUNATHA, B. A. a SHASTRY, K. A. *Intelligent Defense Strategies: Machine Learning-Enhanced SQL Injection Detection and Prevention via Honeypots*. IEEE Xplore [online]. 2024. Dostupné z: <https://ieeexplore.ieee.org/abstract/document/10721851/>. [cit. 2025-02-22].

MARMONI, Giacomo Marco; BLAHŮT, Jan; MARTINO, Salvatore et al. *Environmental processes driving to slope failures: investigations, monitoring, and modelling through natural field laboratories*. Frontiers in Earth Science [online]. 2025 Dostupné z: <https://www.frontiersin.org/journals/earth-science/articles/10.3389/feart.2025.1556839/full>. [cit. 2025-02-15].

MICROSOFT, 2025. Microsoft Defender pro firmy. Online. Dostupné z: <https://www.microsoft.com/cs-cz/security/business/endpoint-security/microsoft-defender-business#>. [cit. 2025-04-10].

MOHAMED, Nasser. *A review of AI approaches in combating advanced persistent threats (APTs) in cybersecurity*. IEEE Xplore [online]. 2024. Dostupné z: <https://ieeexplore.ieee.org/abstract/document/10724580/>. [cit. 2025-02-22].

MORRIS, Michael; HAMMON, James; ANDERSON, Karen a VIKAYANON, Kevin. *Cybersecurity Educators Wanted: A White Paper from the NICE Community Coordinating Council*. NIST [online]. 2024. Dostupné z: <https://www.nist.gov/document/cybersecurity-educators-wanted-white-paper-december-2024>. [cit. 2025-02-20].

MUELLER, John Paul a MASSARON, Luca. *Machine Learning For Dummies*. 1st edition. Hoboken, New Jersey: Wiley, 2016. ISBN 978-1119245513.

MUURIMÄKI, Mikael. *Define Software Bill of Materials (SBOM) as part of software supply chain in a multiplatform IT environment*. Theseus.fi [online]. 2025. Dostupné z: https://www.theseus.fi/bitstream/handle/10024/878189/Muurimaki_Mikael.pdf. [cit. 2025-02-21].

MYKLEBUST, Thor; STÅLHANE, Tor a VATN, Dorthea Mathilde Kristin. *The AI Act and The Agile Safety Plan*. SpringerBriefs in Computer Science. Cham: Springer Nature, 2025. ISBN 978-3-031-80504-2. DOI: 10.1007/978-3-031-80504-2.

NADELLA, Goutham S.; ADDULA, Subba R.; YADULLA, Aslam R. a SAJJA, Gopi S. *Generative AI-Enhanced Cybersecurity Framework for Enterprise Data Privacy*

Management. Computers [online]. 2025. Dostupné z: <https://www.mdpi.com/2073-431X/14/2/55>. [cit. 2025-02-20].

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Akční plán kybernetické bezpečnosti 2021–2025* [online]. Praha: NÚKIB, 2021. Dostupné z: <https://nukib.gov.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/>. [cit. 2025-02-27].

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Národní strategie kybernetické bezpečnosti České republiky 2021–2025* [online]. Praha: NÚKIB, 2021. Dostupné z: <https://nukib.gov.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/>. [cit. 2025-03-01].

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Průvodce novým zákonem o kybernetické bezpečnosti* [online]. Praha: NÚKIB, 2025. Dostupné z: <https://portal.nukib.gov.cz/pruvodce-novym-zakonem-o-kyberneticke-bezpecnosti>. [cit. 2025-03-14].

NEEKHARA, Parth; DOLHANSKY, Brian a BITTON, Jonathan. *Adversarial Threats to Deepfake Detection: A Practical Perspective*. CVPR Workshop, 2021. Dostupné z: https://openaccess.thecvf.com/content/CVPR2021W/WMF/html/Neekhara_Adversarial_Threats_to_DeepFake_Detection_A_Practical_Perspective_CVPRW_2021_paper.html. [cit. 2025-03-10].

OREKU, George S.; MTENZI, Fredrick J. *Cybercrime: Concerns, Challenges, and Opportunities*. Cham: Springer, 2017. ISBN 978-3-319-44257-0.

PANTSEREV, Konstantin. *The Malicious Use of AI-Based Deepfake Technology as the New Threat to Psychological Security and Political Stability*. Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity, 2020. Dostupné z: https://link.springer.com/chapter/10.1007/978-3-030-35746-7_3. [cit. 2025-03-10].

PODGORSKI, Grzegorz. *Analyzing Cyber-Attack Trends on an Educational Institution: A Case Study (2021–2023)*. European Research Studies Journal [online]. 2024. Dostupné z: <https://ersj.eu/journal/3703/download/Analyzing+Cyber-attack+Trends+on+an+Educational+Institution+A+Case+Study+20212023.pdf>. [cit. 2025-02-21].

POLČÁK, Radim; HÁLA, Jan a JURÁŠEK, Lukáš. *Legal aspects of AI in cybersecurity: The Czech Republic perspective*. Torrossa [online]. 2023. Dostupné z: <https://www.torrossa.com/it/resources/an/5629217>. [cit. 2025-02-27].

RAKESH, Venkata S. a VASANTHAKUMAR, Gopalakrishnan U. *Evaluation of supervised classification approach for DDoS threat detection in software-defined networks*. IJITS [online]. 2024. Dostupné z: [https://ijits-bg.com/sites/default/files/archive/2024\(vol.16\)/No4/contents/2024-N4-09.pdf](https://ijits-bg.com/sites/default/files/archive/2024(vol.16)/No4/contents/2024-N4-09.pdf). [cit. 2025-02-22].

REHBERGER, Johann. *Trust No AI: Prompt Injection Along The CIA Security Triad*. arXiv preprint [online]. 2024. Dostupné z: <https://arxiv.org/abs/2412.06090>. [cit. 2025-02-20].

REINHEIMER, Benjamin, et al. *An Investigation of Phishing Awareness and Education Over Time: When and How to Best Remind Users*. USENIX Association [online]. 2020. Dostupné z: https://www.usenix.org/system/files/soups2020-reinheimer_0.pdf. [cit. 2025-04-03].

SAHU, Santosh Kumar; MOHAPATRA, Ranjan Kumar a MOHANTY, Debabrata. *A Hybrid Machine Learning Model for Phishing Website Prediction*. International Journal of Engineering Research and Applications [online]. 2024. roč. 14. č. 12. s. 80–84. ISSN 2248-9622. Dostupné z: <https://www.ijera.com/papers/vol14no12/14128084.pdf>. [cit. 2025-04-04].

SAYYAFZADEH, Saeed a WEATHERSPOON, Megan. *Securing against deception: exploring phishing emails through ChatGPT and sentiment analysis*. IEEE Transactions on Information and Applications [online]. 2024. Dostupné z: <https://ieeexplore.ieee.org/abstract/document/10685564>. [cit. 2025-02-15].

SELMANAJ, Driton. *Adversary Emulation with MITRE ATT&CK: Bridging the Gap Between the Red and Blue Teams*. Cham: Springer, 2024. ISBN 978-3-031-65203-5.

SENTINELONE, 2025. SentinelOne Singularity Control. Online. Dostupné z: <https://www.sentinelone.com/platform-packages/>. [cit. 2025-04-12].

SHAH, Waseem a BEST, Thomas. *Threat Detection and Risk Management: Using AI to Counter Cyber Threats*. ResearchGate [online]. 2025. Dostupné z: https://www.researchgate.net/publication/388847378_Threat_Detection_and_Risk_Management_Using_AI_to_Counter_Cyber_Threats. [cit. 2025-02-20].

SHUKLA, M.; JOHNSON, S. a JONES, P. *Cascading Effects of Cyber-Attacks on Smart Infrastructure in Connected Places*. SSRN [online]. 2025. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5097760. [cit. 2025-02-20].

SCHLISSELBERG, Ofir a DARSHAN, Ran, 2025. *The impact of allocation strategies in subset learning on the expressive power of neural networks*. Online. Cornell University. Dostupné z: <https://arxiv.org/abs/2502.06300>. [cit. 2025-02-15].

SILVESTRI, Stefano a GARGIULO, Francesco. *Special Issue on eHealth Innovative Approaches and Applications*. Applied Sciences 14 [online]. 2024. No. 6: 2571. Dostupné z: <https://doi.org/10.3390/app14062571>. [cit. 2025-02-20].

SINGH, Priti a SHARAN, Om Har. *Deep convolution models: Basic definitions, types, and applications in solar energy, engineering, and finance*. Taylor & Francis [online]. 2024. Dostupné z: <https://www.taylorfrancis.com/chapters/edit/10.1201/9781003564874-5/deep-convolution-models-priti-singh-om-sharan-raghuvanshi>. [cit. 2025-02-15].

SOMESHA, M.; PAIS, A.; RAO, R. a RATHOUR, V. *Efficient deep learning techniques for the detection of phishing websites*. Sādhanā [online]. 2020. 45. Dostupné z: <https://doi.org/10.1007/s12046-020-01392-4>. [cit. 2025-04-04].

SOPHOS, 2025. *Sophos*. Online. Dostupné z: <https://www.sophos.com/en-us>. [cit. 2025-04-12].

SOSPETER, Kipchirchir a ODOYO, Wilfred. *AI-Based Phishing Attack Detection and Prevention Using Natural Language Processing (NLP)*. The 5th International Conference on Information Technology and Security [online]. 2024. Dostupné z: https://www.researchgate.net/publication/388736093_AI_Based_Phishing_Attack_Detection_And_Prevention_Using_Natural_Language_Processing_NLP. [cit. 2025-04-03].

SREE, Usha; REDDY, Harshitha P.; REDDY, Vineel Kumar a SUMANTH, Kumar. *SQL Injection Attacks: Exploiting Vulnerabilities in Database Systems*. Taylor & Francis [online]. 2024. Dostupné z: <https://www.taylorfrancis.com/chapters/edit/10.1201/9781003488682-3/sql-injection-attacks-exploiting-vulnerabilities-database-systems-usha-sree-harshitha-reddy-vineel-kumar-reddy-sumanth>. [cit. 2025-02-22].

STAMOV, Georgi; STAMOV, Todor a STAMOVA, Iskra. *On the Global Practical Exponential Stability of h -Manifolds for Impulsive Reaction–Diffusion Cohen–Grossberg*

Neural Networks with Time-Varying Delays. Entropy [online]. 2025. Dostupné z: <https://www.mdpi.com/1099-4300/27/2/188>. [cit. 2025-02-15].

SUPANGKAT, Suhono Harso; FIRMANSYAH, Hendra Sandhi; RIZKIA, Irma a KINANDA, Rezky. *Challenges in Implementing Cross-Border Digital Identity Systems for Global Public Infrastructure: A Comprehensive Analysis*. IEEE Access [online]. 2025. Dostupné z: <https://ieeexplore.ieee.org/iel8/6287639/6514899/10909091.pdf>. [cit. 2025-03-09].

TANG, Lan a MAHMOUD, Qusay. *A Survey of Machine Learning-Based Solutions for Phishing Website Detection*. Machine Learning and Knowledge Extraction [online]. 2021. 3(3), 672-694. 2021. Dostupné z: <https://doi.org/10.3390/make3030034>. [cit. 2025-04-03].

VAN OVAYAN, M.; CARUTHERS, J.; ENGELHARDT, A. a REDGRAVE, A. *Novel framework for autonomous ransomware detection using hierarchical threat signal profiling*. TechRxiv [online]. 2024. Dostupné z: <https://www.techrxiv.org/doi/pdf/10.36227/techrxiv.173273662.29033096>. [cit. 2025-03-15].

VOSTOUPAL, Michal; KŘÍŽEK, Tomáš a ŠAFRÁNEK, Pavel. *Cybersecurity legislation and personal data protection: The impact of NIS 2 in the Czech Republic*. ScienceDirect [online]. 2024. Dostupné z: <https://www.sciencedirect.com/science/article/pii/S0267364924000554>. [cit. 2025-02-27].

WAZID, Mohammad; MISHRA, Ajay Kumar; MOHD, Naseer a DAS, Abhishek Kumar. *A Secure Deepfake Mitigation Framework: Architecture, Issues, Challenges, and Societal Impact*. Cyber Security and Applications, 2024. Dostupné z: <https://www.sciencedirect.com/science/article/pii/S2772918424000067>. [cit. 2025-03-10].

XIANG, Guanghai; HONG, Jason I.; ROSE, Carolyn P. a CRANOR, Lorrie Faith. *Cantina+: A Feature-Rich Machine Learning Framework for Detecting Phishing Web Sites*. ACM Transactions on Information and System Security. 2009. roč. 14, č. 2, s. 1–28. DOI: 10.1145/2019599.2019606

XU, Hui; BAI, Longtan a HUANG, Wei. *An optimization-inspired intrusion detection model for software-defined networking*. Electronic Research Archive [online]. 2025. Dostupné z: <https://www.aimspress.com/aimspress-data/era/2025/1/PDF/era-33-01-012.pdf>. [cit. 2025-02-22].

ZHANG, Tianyu; HE, Cheng a GAO, Long. Federated learning for Internet of Things. ACM, 2021. Dostupné z: <https://dl.acm.org/doi/abs/10.1145/3485730.3493444>. [cit. 2025-03-10].

ZHAO, Liran; SUN, Quinbo a DANG, Zhaohui. *A learning-based algorithm for turn-based orbital pursuit-evasion problem with reaction-time delay*. Online. *Engineering Applications of Artificial Intelligence*. Roč. 2025, č. 145. ISSN 0952-1976. Dostupné z: <https://www.sciencedirect.com/science/article/pii/S0952197625002313>. [cit. 2025-02-15].

SEZNAM TABULEK

Tabulka 1 Hlavní rozdíly mezi zákonem č. 181/2014 Sb., a návrhem nového zákona o kybernetické bezpečnosti	36
Tabulka 2 Klíčové vlastnosti signaturní detekce	51
Tabulka 3 Klíčové vlastnosti heuristické analýzy	53
Tabulka 4 Klíčové vlastnosti detekce malwaru pomocí AI	55
Tabulka 5 Komparace klasických metod a metod AI v detekci malware	56
Tabulka 6 Klíčové vlastnosti blacklistingu	59
Tabulka 7 Klíčové vlastnosti filtrování e-mailů	61
Tabulka 8 Klíčové vlastnosti metody vzdělávání a osvěty uživatelů	63
Tabulka 9 Klíčové vlastnosti metod strojového učení	64
Tabulka 10 Klíčové vlastnosti metod hlubokého učení	66
Tabulka 11 Klíčové vlastnosti metod NLP	68
Tabulka 12 Komparace klasických metod a metod AI v detekci phishingu	69
Tabulka 13 Porovnání nákladů na implementaci AI řešení kybernetické bezpečnosti	75
Tabulka 14 Normalizace finanční náročnosti vybraných řešení	76
Tabulka 15 Hodnocení vybraných řešení kybernetické ochrany podle klíčových kritérií ..	78
Tabulka 16 Kriteriaální hodnocení vybraných řešení pro modelový subjekt	81
Tabulka 17 Výsledné pořadí posuzovaných řešení pro modelový subjekt	82

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AI	Artificial Intelligence
ANN	Artificial Neuron Networks
APT	Advanced Persistent Threats
CIA	Confidentiality, Integrity, Availability
CNN	Convolutional Neuron Networks
DDoS	Distributed Denial of Service
DL	Deep Learning
FL	Federated Learning
IoT	Internet of Things
ML	Machine Learning
QR	Quick-Response
SQL	Structured Query Language
SVM	Support Vector Machines
URL	Uniform Resource Locator