

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	Využití OpenAI analýzy datových toků pro potřeby kybernetické bezpečnosti
Jméno autora:	Pavel Filip
Typ práce:	bakalářská
Fakulta/ústav:	Fakulta elektrotechnická (FEL)
Katedra/ústav:	Katedra telekomunikační techniky
Oponent práce:	Ing. Jaroslav Burčík Ph.D., LL.M.
Pracoviště oponenta práce:	Katedra telekomunikační techniky ČVUT FEL

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání	mimořádně náročné
<i>Hodnocení náročnosti zadání závěrečné práce.</i>	
<p>Práce se zabývá problematikou kybernetické bezpečnosti malé a střední firmy. Cílem práce bylo ujasnit si jaké přístupy jsou pro takovou ochranu vhodné a ekonomicky smysluplné. Ambicí pak bylo nastudovat principy fungování nástrojů NLP (natural language processing), které mediálně reprezentuje např. Chat GPT a vyzkoušet, jakým způsobem by s jejich pomocí, bylo možné usnadnit práci firemních správců bezpečnosti.</p> <p>Téma považuji za mimořádně náročné, neboť od studenta vyžaduje poměrně komplexní znalost problematiky správy podnikových sítí a kybernetické bezpečnosti, která je umocněna novostí NLP. Zadání tedy v oblasti nasazení NLP nesměřovalo ke konkrétní implementaci, ale k prozkoumání silných a slabých stránek této technologie a určení vhodné cesty pro její využití v další práci. Proto obtížnost zadání hodnotím dle výše uvedeného výroku.</p>	

Splnění zadání	splněno s menšími výhradami
<i>Posuďte, zda předložená závěrečná práce splňuje zadání. V komentáři případně uveďte body zadání, které nebyly zcela splněny, nebo zda je práce oproti zadání rozšířena. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.</i>	
<p>Zapsáním tohoto tématu se student přihlásil k velké porci práce. Jak se v průběhu řešení ukázalo, student měl na vstupu jen základní teoretické znalosti administrace sítí a minimální v oblasti problematiky kybernetické bezpečnosti. Žádnou zkušenost pak s metodami strojového učení. A tak i když poctivě studoval doporučenou literaturu a konzultoval poznatky s vedoucím práce či oborovými specialisty, tato nezkušenost, spolu s velmi krátkým časem, který zbýval na odevzdání práce, velmi ovlivnila formu a konečný výsledek zpracování bakalářské práce. Celkově však zadání a jeho jednotlivé části považuji za splněné. Menší výhrady mám pouze k formě, jakou jsou jednotlivé části zpracovány.</p>	

Zvolený postup řešení	správný
<i>Posuďte, zda student zvolil správný postup nebo metody řešení.</i>	
<p>Zvolený postup řešení považuji za správný. Student v přehledové části podchytil základní architektonické pohledy na firemní IT a dále pak technické i netechnické aspekty firemní kybernetické bezpečnosti. Provedl rozbor standardů vhodných pro sběr dat ze síťového provozu a vybral vhodné opensource nástroje pro bezpečnostní monitoring sítí, které tento typ dat dokáží zpracovat. Následně jeden z nástrojů (Suricata) implementoval a začal experimentovat s možnostmi jeho strojového zpracování pomocí NLP. Zde se opět jednalo pro studenta o zcela novou oblast, u které se mu podařilo zvládnout základy a sestavit například základní aplikační rozhraní pro nástroj excel, které umělo NLP Chapt GPT automatizovaně dotazovat. S využitím tohoto rozhraní pak student experimentoval s NLP nad množinou dat, která představovala základní provoz v síti.</p> <p>Ačkoli vlastní postup považuji za správný, student podcenil množství informací, které musí nastudovat, v hlavě si utřídit a vhodnou formou zachytit do výsledného reportu. Pro dosažení lepšího hodnocení pak v práci postrádám hlubší vazbu na problematiku malé a střední firmy, danou zadáním. Zároveň by práci prospělo zkrácení pasáží, které jsou přehledového/encyklopedického charakteru, a naopak větší prostor bych uvítal pro úvahy či kroky a rozhodnutí, které student v průběhu práce učinil a které směřovaly jeho postup při plnění zadání.</p>	

Odborná úroveň

C - dobře

Posudte úroveň odbornosti závěrečné práce, využití znalostí získaných studiem a z odborné literatury, využití podkladů a dat získaných z praxe.

Po stránce odborné práci hodnotím stupněm dobře. Ačkoli se student snaží využívat aktuálních poznatků z této oblasti, je zřejmé, že ani poctivé a intenzivní čtení citovaných zdrojů nedokáže v omezeném čase vyvážit malé praktické zkušenosti s tématy, která nám dnes připadají běžná a téměř základní. Některé formulace a závěry tak ukazují na špatné pochopení toho, co je principem fungování té, které služby/systému/protokolu či doplácení na nevhodně zvolené studijní zdroje a jejich překlad.

Formální a jazyková úroveň, rozsah práce

C - dobře

Posudte správnost používání formálních zápisů obsažených v práci. Posudte typografickou a jazykovou stránku.

Strukturu práce po stránce formální považuji za vhodnou, využívající doporučených vzorů. Výhrady mám k typografii, kde student nesjednotil používané typy písma a v různých částech práce používá rozdílné vzory písem a fontů. Rovněž tabulky, dle mého názoru, je vhodnější sjednotit do stejné grafické úpravy, byť jsou přejaté (a správně citované), z různých zdrojů. Této části mohl student věnovat více pozornosti.

Co mne v práci chybí nejvíce po stránce jazykové úrovně je její „čtivost“ a celková uhlazenost. Student nashromáždil řadu zdrojů a vygeneroval v přehledových kapitolách velké množství textu u kterého pak hrozilo, že by výsledná délka práce přesáhla akceptovatelnou mez. V průběhu konzultací tak student musel několikrát práci krátit a „prořezávat“. A ačkoli došlo k podstatnému zkrácení objemu textu, práci chybí něco, co bych nazval „její duší“. Tedy něco, co vysvětluje myšlenkové pochody autora, uvozuje témata a odstavce v kapitolách a vytváří logické můstky při přechodu mezi tématy. Ačkoli jsme toto konzultovali a student se snažil text vyladit, přesto zůstal velký prostor pro zlepšení.

Výběr zdrojů, korektnost citací

B - velmi dobře

Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení závěrečné práce. Charakterizujte výběr pramenů. Posudte, zda student využil všechny relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.

V práci student pracuje převážně s online zdroji. Citace online zdroje respektuje doporučený formát a obsahuje uvedení data funkčnosti. Zde nemám výhrad. Ačkoli jsou klíčové zdroje podloženy respektovanými autory či institucemi, řada citací směřuje na články, které jsou psané spíše pro uživatele manažera než technika specialistu. Zároveň zde existuje nebezpečí, že obsah a vyznění těchto článků může být ovlivněno obchodním zájmem autora. Zde spatřuji hlavní zdroj chyb, nepřesností a přílišných zjednodušení, které snižují odbornou kvalitu práce. Za mnohem vhodnější bych v přehledových pasážích považoval odkazovat např. na wikipedii.

Další komentáře a hodnocení

Vyjádřete se k úrovni dosažených hlavních výsledků závěrečné práce, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, publikačním výstupům, experimentální zručnosti apod.

Nemám dalších komentářů, vše podstatné jsem popsal výše.

III. CELKOVÉ HODNOCENÍ, OTÁZKY K OBHAJOBĚ, NÁVRH KLASIFIKACE

Shrňte aspekty závěrečné práce, které nejvíce ovlivnily Vaše celkové hodnocení. Uveďte případné otázky, které by měl student zodpovědět při obhajobě závěrečné práce před komisí.

S ohledem na úroveň vstupních znalostí, student zvolil velmi těžké téma. Nicméně, dle jeho vyjádření, ho toto téma zajímá a chce se v něm odborně dále rozvíjet. K vlastnímu průběhu realizace a intenzitě prací nemám výhrad. Student pracoval samostatně a s nadšením. Každý týden jsme konzultovali nové poznatky, zjištění a diskutovali další směřování práce. Student na mne celkově zanechal velmi pozitivní dojem. Pokud bych se měl v hodnocení zaměřit na znalostní progres, který student předvedl mezi počátkem prací a odevzdáním výsledku, tak tento považuji za velmi velký. I z tohoto důvodu a přes výše uvedené výhrady, jsem se rozhodl práci hodnotit klasifikačním stupněm **B - velmi dobře**.

Datum: 11.6.2023

Podpis: