ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

POSUDEK VEDOUCÍHO ZÁVĚREČNÉ PRÁCE

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	**Detekce operačního systému zařízení z dat síťového provozu**
Jméno autora:	**Bc. Anastasiia Kuznetsova**
Typ práce:	diplomová práce
Fakulta:	Fakulta jaderná a fyzikálně inženýrská (FJFI)
Katedra:	Katedra softwarového inženýrství
Vedoucí práce:	RNDr. Tomáš Jirsík Ph.D.
Pracoviště vedoucího práce:	Cisco Systems (Czech Republic), s.r.o.

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání a motivace k jeho vypsání — **náročnější**

Hodnocení náročnosti zadání závěrečné práce a krátké průvodní slovo k motivaci pro zadání práce.

Možnost určit operační systém zařízení na základě jeho síťového provozu představuje klíčovou výhodu v oblasti kybernetické bezpečnosti. Znalost operačního systému umožnuje využít tuto informaci v dalších částech systému pro detekci kybernetických útoků a anomálií, jako například při poskytovat přesnější výsledky detekcí, či efektivnější bezpečnostní správě zařízení. Motivací k vypsání práce bylo prozkoumat možnosti využití navštívených domén a strojového učení k určení operačního systému zařízení. Na základě výsledků bude možné navrhnout a implementovat efektivní detekci operačního systému v produktech Cisco.

Zadání diplomové práce patří k náročnějším, protože autorka musela oblast monitorování síťového provozu k tomu, aby mohla správně provést experimenty. Autorka také musela pracovat s velkými objemy dat, což přidávalo na technické komplexitě zadání. V neposlední řadě, zadání diplomové práce bylo spíše výzkumného charakteru, takže autorka při řešení práce musela projít i nemalé množství slepých uliček.

Splnění zadání — **splněno**

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.

Práce splňuje všechny body zadání. Autorka nastudovala danou oblast. Na zvolené datové sadě provedla explorativní analýzu a v rámci experimentů navrhla různé možnosti reprezentace navštívených domén pro strojové učení a pro přípravu trénovacího vzorku dat. Zvolené metody strojového učení jsou v práci dostatečně popsány. Modely jsou vzájemně porovnány vzhledem k dané úloze a vzhledem k parametrům definující trénovací sadu.

Aktivita a samostatnost při zpracování práce — **výborná**

Posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven. Posuďte schopnost studenta samostatné tvůrčí práce.

Autorka byla během vypracování práce nadstandardně aktivní. Práci se mnou konzultovala na týdenní bázi. Veškeré termíny dodržovala a na konzultace chodila připravena. Sama také přicházela s návrhy na nové možnosti přístupu k tvorbě datové sady a vyhodnocení provedených experimentů. Autorka se také snažila pochopit širší souvislosti své práce a neomezovala se pouze na zadanou úlohu. Samotný text práce také konzultovala průběžně a obratem zapracovávala připomínky.

Odborná úroveň — **výborná**

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

Autorka získala rozšířené znalosti z oblasti monitorování síťového provozu. U zvolených algoritmů pro strojové učení získala hluboké znalosti a ověřila si nabyté znalosti na případech z praxe. Odborností práce odpovídá

experimentu, který by bylo možné, v případě zkrácení, publikovat v rámci aplikované konference/workshopu z oblasti kyberbezpečnosti.

Formální a jazyková úroveň **výborná**

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

Práce je psaná v anglickém jazyce, srozumitelnou formou. Místy práce uvažuje příliš široké souvislosti, nicméně tento fakt nenarušuje tok sdělovaných informací. Typografická stránka práce je na velmi dobré úrovni, výsledky jsou srozumitelně prezentovány formou grafů a tabulek zvýrazňující důležitá fakta. Práce je vhodně členěná vzhledem k svému zaměření. Autorka také vhodně provází autora jednotlivými kapitolami pomocí společného schématu reprezentující jednotlivé částí práce.

Výběr zdrojů, korektnost citací **výborné**

Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení závěrečné práce. Charakterizujte výběr pramenů. Posuďte, 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.

Studentka aktivně zpracovala studijní materiály, které jí byly poskytnuty, a to včetně cizojazyčné odborné literatury a článků. Zároveň byla schopna sama dohledat i další relevantní zdroje k danému tématu. Práce čerpá informace jak z odborných článku, tak z online zdrojů, což je dáno typem vypracované práce a zadáním. Citace jsou v souladu s citačními zvyklostmi a normami a informace v práci jsou dostatečně citovány.

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.

Autorka společně s prací odevzdala zdrojový kód pro provedené experimenty, což umožňuje případné ověření experimentů třetími osobami. Kód je dokumentovaný a doprovázen návodem na použití. Jak bylo výše uvedeno, výsledky daných experimentů umožní navrhnout nástroj pro detekci operačních systémů v rámci technického řešení ve společnosti Cisco.

III. CELKOVÉ HODNOCENÍ A NÁVRH KLASIFIKACE

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

Práce splnila všechny body zadání. Rozsah provedených experimentů a množství zkoumaných přístupů k detekci operačních systému je nadstandardní. Práce více než naplňuje všechny formální požadavky kladené diplomovou práci daného typu.

Předloženou závěrečnou práci hodnotím klasifikačním stupněm **A - výborně.**

Datum: 24.5.2023 Podpis: