POSUDEK VEDOUCÍHO ZÁVĚREČNÉ PRÁCE

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	**Creating classifiers robust to adversarial attacks**
Jméno autora:	**Bc. Petr Všetečka**
Typ práce:	diplomová
Fakulta/ústav:	Fakulta elektrotechnická (FEL)
Katedra/ústav:	Katedra počítačů
Vedoucí práce:	Mgr. Viliam Lisý, PhD.
Pracoviště vedoucího práce:	Katedra počítačů

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání **náročnější**

Hodnocení náročnosti zadání závěrečné práce.

Úplné splnenie zadania vyžadovalo naštudovanie väčšieho množstvá materiálov z rôznych oblastí nad rámec štúdia. Tieto materiály bolo treba pochopiť dostatočne na to, aby oblasti bolo možné prepojiť.

Splnění zadání **splněno s většími výhradami**

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.

Zadanie považujem za splnené v takmer minimálnej možnej miere. Keďže práca prepoužíva prakticky hotové implementácie klasifikátorov a generátorov adversariálnych príkladov, ťažisko práce malo byť v algoritmoch na zrobustnenie učenia inšpirovaných teóriou hier. V práci je jediná vyhodnotené zmena algoritmu na zrobustnenie pridanie cache do existujúceho algoritmu. Táto modifikácia je ale nová a dostatočne dobre experimentálne vyhodnotená. Preto stále považujem zadanie za splnené.

Aktivita a samostatnost při zpracování práce **D - uspokojivě**

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.

Študent zo začiatku semestra chodil na pravidelné konzultácie aj s pol hodinovým meškaním a často s minimálnym pokrokom od predošlého týždňa s tým, že sa k tomu dostatočne nedostával. Toto sa v druhej polovici semestra výrazne zlepšilo, ale to už neostávalo moc času na vypracovanie skutočne kvalitnej práce. Na záver študent ale preukázal schopnosť samostatne navrhnúť a spracovať vhodné experimenty.

Odborná úroveň **C - dobře**

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

Študent sa dobre zorientoval v problematike vytvárania adversariálnych príkladov a preukázal schopnosť samostatne navrhnúť vhodnú experimentálnu evaluáciu. Práca mu ale aspoň zo začiatku išla veľmi pomaly, čo bolo pravdepodobne spôsobené tým, že sa jej nevenoval dostatočne intenzívne.

Formální a jazyková úroveň, rozsah práce **C - dobře**

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

Práca je písaná pútavo, vo výbornej a zrozumiteľnej angličtine, s minimom typografických chýb. Rozsah práce je ale na spodnej hranici, napriek tomu, že práca obsahuje veľa obrázkov a tabuliek.

Výběr zdrojů, korektnost citací **C - dobře**

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.

Práca s literatúrou je nevyvážená. V oblasti nachádzania a praktických rizík adversariálnych príkladov študent veľmi pekne naštudoval a spracoval existujúcu literatúru a samostatne našiel veľké množstvo relevantných zdrojov. V oblasti obrany proti týmto príkladom to je slabšie, ale literatúry je objektívne málo. Herne teoretickú inšpiráciu zo zadania a články s ňou súvisiace študent prakticky nediskutuje.

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.

Vložte komentář (nepovinné hodnocení).

III. CELKOVÉ HODNOCENÍ A NÁVRH KLASIFIKACE

Shrňte aspekty závěrečné práce, které nejvíce ovlivnily Vaše celkové hodnocení.

Študent splnil zadanie v minimálnej miere a podľa môjho názoru aj s minimálnou časovou investíciou. Napriek tomu ale preukázal schopnosť samostatne pracovať na výskumnom probléme, študovať odbornú literatúru, navrhovať a spracovávať experimenty, a napísať pochopiteľnú a prehľadnú prácu bez väčších chýb.

Předloženou závěrečnou práci hodnotím klasifikačním stupněm **C - dobře.**

Datum: 6.6.2018 Podpis: