

Posudek diplomové práce

Matematicko-fyzikální fakulta Univerzity Karlovy

Autor práce Bc. Viktor Vašátko
Název práce Applications of Artificial Intelligence in IT Security
Rok odevzdání 2020
Studijní program Computer Science **Studijní obor** Artificial Intelligence

Autor posudku Mgr. Marta Vomlelová Ph.D. **Role** vedoucí
Pracoviště Department of Theoretical Computer Science and Mathematical Logic

Text posudku:

Práce se zabývá užitím technik strojového učení v počítačové bezpečnosti.

Původní idea napojit se na reálné datové toky partnerské organizace se ukázala jako časově nereálná, proto se student orientoval na volně dostupnou databázi.

V úvodní kapitole autor popisuje databázi, ve druhé použité metody strojového učení. Třetí kapitola představuje naučené modely a čtvrtá tvoří množiny pravidel, které je možné srovnat s pravidly tvořenými expertem.

Práce používá pouze základní metody strojového učení. I těmi autor dosahuje výsledků srovnatelných s publikovanými výsledky[6]. Přesto zůstává prostor pro zlepšení pomocí pokročilejších technik.

Základní cíl práce, vytvoření množiny pravidel, byl splněn. Množina těchto pravidel jakožto celek dosahuje srovnatelné přesnosti jako modely v předchozí kapitole. Autor identifikuje těžko rozpoznatelné druhy útoků, které se pravidly identifikovat nepodařilo.

Práce je psaná srozumitelně. Rozbor 13+1 možných typů útoků a příslušných seznamů pravidel je strukturován pravidly zobrazenými v tabulkách a výsledky modelů jsou uvedeny v přehledných maticích záměn.

Student prokázal schopnost samostatné odborné práce.

Práci doporučuji k obhajobě.

Práci nenavrhuji na zvláštní ocenění.

V Praze dne 27. 6. 2020

Podpis