Vilniaus universitetas
Duomenų mokslo ir skaitmeninių Technologijų institutas

Informatikos krypties doktorantų konferencija

Veiklos ataskaita už 2021 m. kovo 26 d. – 2021 m. spalio 1 d.

Arnoldas BUDŽYS – Informatikos N 009 doktorantas

Darbo vadovas – dr. Viktor Medvedev

Doktorantūros pradžios ir pabaigos metai: 2020 - 2024

2020–2021m.

- **STUDIJŲ PLANAS IR JO VYKDYMO SUVESTINĖ**

Studijų metai	Egzaminai [1]		Dalyvavimas konferencijose [2]		Publikacijos [3]		
	Planas	Įvykdyta	Planas	Įvykdyta	Planas	Įvykdyta	Būklė [4]
I (2020/2021)	**1**	**1**					
II (2021/2022)	2		1		1		
III (2022/2023)	1		1		1		
IV (2023/2024)			1		1		
Iš viso:	4	1	3		3		

2020–2021 m.

- **ATASKAITINIŲ METŲ DARBO PLANAS IR JO SUVESTINĖ**

Egzaminai		Dalyvavimas konferencijose		Publikacijos	
Planas	Įvykdyta	Planas	Įvykdyta	Planas	Įvykdyta
Informatikos ir informatikos inžinerijos tyrimo metodai ir metodika	Išlaikyta				
Tarptautinė vasaros/žiemos stovykla; Dalyvavimas bendruosius gebėjimus stiprinančiose veiklose.	Dalyvauta vasaros mokykloje: „DeepLearn 2021 Summer” Las Palmas Gran Kanarija, Ispanija Liepos 26-30, 2021 m.				

Mokslinių tyrimų ir disertacijos rengimo planas:

2020–2021 m.

Mokslinių tyrimų disertacijos tema apžvalga ir analizė (Lietuvoje ir užsienyje):

- **Disertacijos tyrimo objekto detalizavimas.**
- **Atlikti mašininio mokymosi metodų taikymo kompiuterių tinkluose analitinę apžvalgą**
- **Nustatyti (identifikuoti) mokslines problemas, kylančias uždaviniuose, susijusiuose su įsilaužimų prevencija kompiuterių tinkluose taikant mašininio mokymosi metodus.**
- **Tyrimo tikslo suformavimas.**

2021–2022 m.

Mokslinio tyrimo vykdymas:

- **2.1. Tyrimo metodikos sudarymas:**
- 2.1.1. Tyrimo metodikos iškeltiems uždaviniams spręsti parinkimas;
- 2.1.2. Teorinio ir empirinio tyrimų suplanavimas pagal pasirinktą metodiką.
- **2.2. Teorinis tyrimas:**
- 2.2.1. Mašininio mokymosi metodų, naudojamų kompiuterių tinkluose įsilaužimų prevencijai, tyrimas.
- 2.2.2. Įsilaužimų prevencijos atpažinimo mašininio mokymosi metodo sukūrimas ir/ar testavimas.

2022–2023 m.

- **2.3. Empirinis tyrimas:**
- 2.3.1. Sudarytų metodų pritaikymas praktinių uždavinių sprendimui.
- 2.3.2. Gautų duomenų analizė, rezultatų apibendrinimas, išvadų parengimas.

2023–2024 m.

Atskirų daktaro disertacijos dalių (tyrimo metodikos, rezultatų, ginamų teiginių, išvadų, ir kt.) parengimas:

- 3.1. Tikslų, uždavinių, tyrimo metodikos, ginamųjų teiginių patikslinimas;
- 3.2. Analitinės disertacijos dalies parengimas;
- 3.3. Teorinės disertacijos dalies parengimas;
- 3.4. Eksperimentinės disertacijos dalies parengimas;
- 3.5. Bendrųjų išvadų formulavimas.

2024 m. birželio mėnesį

- Daktaro disertacijos parengimas ir svarstymas padalinyje

2024 m. rugsėjo mėnesį

- Daktaro disertacijos gynimas

Disertacijos tema, tyrimo objektai ir tikslas

Preliminari disertacijos tema:

- Anomalinių įvykių identifikavimas ir jų užkardymas kompiuterių tinkluose taikant mašininio mokymosi metodus

Tyrimo objektai:

- vartotojo sugeneruoti klaviatūros, pelės biometriniai duomenys, bei mašininio mokymosi metodų taikymas anomalinių įvykių identifikavimui.

Tikslas

- sukurti arba patobulinti mašininiu mokymusi grįstą metodą, skirtą anomalinių įvykių identifikavimui ir jų užkardymui kompiuterių tinkluose (pasiūlyti efektyvią metodiką anomalinių įvykių identifikavimui ir jų užkardymui kompiuterių tinkluose).

Tyrimo uždaviniai

- Identifikuoti tinkamus metodus anomalinių įvykių identifikavimui ir jų užkardymui kompiuterių tinkluose;
- Atlikti skirtingų mašininio mokymosi metodų, skirtų anomalinių įvykių identifikavimui ir jų užkardymui kompiuterių tinkluose, analizę ir tyrimą;
- Identifikuoti aktualias mokslines problemas, kylančias uždaviniuose, susijusiose su anomalinių įvykių identifikavimu ir jų užkardymu kompiuterių tinkluose;
- Sukurti arba patobulinti mašininiu mokymosi grįstą metodą anomalinių įvykių užkardymui;
- Pritaikyti sukurtą arba patobulintą metodą realaus laiko duomenims ir atlikti gautų duomenų analizę, rezultatų apibendrinimą, išvadų parengimą

LITERATŪROS ANALIZĖS APIBENDRINIMAS

- Klaviatūros bei pelės biometriniai duomenys yra naujas autentifikavimosi būdas. Jo išskirtinumas nuo kitų biometrinio autentifikavimosi būdų yra tas, jog tokiam autentifikavimuisi nereikia papildomos įrangos.
- Remiantis straipsnių apžvalga, galima teigti, jog kiekvieno vartotojo sudarytas klaviatūros bei pelės biometrinių duomenų profilis yra autentiškas ir negali būti atkartojamas.

Pagrindinės klaviatūros dinamikos išskiriamos savybės yra šios:

- Išlaikymo trukmė (angl. *Dwell time (DT)*) – paspausto klavišo laikymo laikas;
- Flight time (FT) – laikas tarp vieno klavišo atleidimo ir kito klavišo paspaudimo;
- Dviejų, trijų ar daugiau iš eilės paspaustų klavišų naudojimas (angl. *2-graph, 3-graph*);
- Rašymo dažnumas, klaidų dažnis ir spausdinimo greitis.

- Svarbiausias KD sistemos etapas yra klasifikavimo etapas, kuriame išgauti požymiai naudojami autentiškumo nustatymo sprendimui priimti. Populiariausias klasifikavimo metodas – atraminių vektorių klasifikatorius (angl. *support vector machine (SVM)*) dėl didesnio tikslumo ir mažesnio skaičiavimo intensyvumo.
- Iš mašininio mokymosi algoritmų vienos klasės naivusis Bajeso algoritmas (angl. *one-class naïve Bayes (ONENB)*) yra veiksmingas, kai taikomas anomalijų testams; tačiau ONENB algoritmo taikymo klavišų paspaudimo dinamika pagrįstam autentiškumo nustatymui, tyrimų atlikta nedaug.
- Dažniausiai straipsniuose sutinkami duomenų rinkiniai kurie buvo pasirinkti tinklo apsimokymui yra viešai prieinami tinklalapyje https://vmonaco.com/datasets/

KITO PUSMEČIO DARBO PLANAS

- Išlaikyti egzaminą: „*Fundamentalieji informatikos ir informatikos inžinerijos metodai*“;
- Apžvalginio straipsnio rašymas (periodiniame recenzuojame mokslo žurnale arba konferencijų medžiagoje);
- Dalyvauti „*Data Analysis Methods for Software Systems*“ konferencijoje kuri vyks Druskininkuose š. m. gruodžio 2–4 dienomis;
- Literatūros apžvalgos rašymas;
- Tinkamų metodų identifikavimas ir mokslinio naujumo formulavimas.

KLAUSIMAI?

Ačiū už dėmesį.