

Kibernetinio saugumo reikalavimų užtikrinimas kritinės infrastruktūros sistemose naudojant formalaus verifikavimo ir dirbtinio intelekto metodus

Daniel Daukševič

Matematikos ir Informatikos Fakultetas, Vilniaus Universitetas
daniel.dauksevic@mif.stud.vu.lt

Ataskaitinė Informatikos krypties doktorantų konferencija
2025 m. spalio 2 d.



Doktorantūra

Tema

Kibernetinio saugumo reikalavimų užtikrinimas kritinės infrastruktūros sistemose naudojant formalaus verifikavimo ir dirbtinio intelekto metodus

Mokslo kryptis

Informatika N009

Vadovas

prof. dr. Linas Laibinis

Studijų laikotarpis

2023 m. lapkričio mėn. 1 d. - 2027 m. spalio mėn. 31 d. (I metai)

Turinys

- 1 Tyrimas
- 2 Studijos
- 3 Moksliniai tyrimai
- 4 Mobilumo veiklos
- 5 Kito pusmečio planas

Praėjusio pusmečio darbo planas darbai

- Finalizuoti mokslo literatūros ir publikacijų analizę
- Išlaikyti pasirenkamąjį studijų dalyką “Automatizuoti verifikavimo ir validavimo metodai”
- Pasiectus rezultatus pristatyti tarptautinėje mokslo konferencijoje

- 1 Tyrimas
- 2 Studijos
- 3 Moksliniai tyrimai
- 4 Mobilumo veiklos
- 5 Kito pusmečio planas

Tyrimo objektas

- Kibernetinio saugumo reikalavimai kritinės infrastruktūros sistemose
- Kibernetinio saugumo reikalavimų verifikavimas taikant formalius metodus
- Kibernetinio saugumo reikalavimų užtikrinimo optimizavimas taikant dirbtinį intelektą

Tyrimo tikslas I

- Iširti būdus ir metodus kibernetinio saugumo modeliavimui privalomųjų saugumo reikalavimų užtikrinimui
- Iširti kibernetinio saugumo pažeidžiamų lygmenų įtaką ir sudaryti taksonomijas pažeidžiamumo paviršiui aprašyti
- Iširti formalius verifikavimo metodus tinkamus sukurti modelio formaliajam verifikavimui

Tyrimo tikslas II

- Iširti dirbtinio intelekto metodus taikytinus verifikavimo parametrų identifikavimui ar optimalumo kriterijų derinimui
- Iširti, kiek formalūs verifikavimo metodai išbandyti kritiškai saugių (angl. safety-critical), gedimams atsparių (angl. fault-tolerant, resilient) ar adaptyvių (angl., adaptive) sistemų verifikavimui gali būti pritaikyti verifikuojant kibernetinio saugumo savybes kritinėse infrastruktūrose.

Planuojami rezultatai

- Sukurti metodikas formalizuoti kibernetinio saugumo reikalavimus modeliuojant kritinių infrastruktūrų tinklus;
- Kritinės infrastruktūros sistemų kibernetinio saugumo vertinimo metodikos;
- Kritinės infrastruktūros sistemų kibernetinio saugumo stiprinimo rekomendacijos;

- 1 Tyrimas
- 2 **Studijos**
- 3 Moksliniai tyrimai
- 4 Mobilumo veiklos
- 5 Kito pusmečio planas

Studijų planas

Studijų metai	Egzaminai ¹	
	Planas	Ivykdyta
I (2023/2024)	1	1
II (2024/2025)	2	2
III (2025/2026)	1	
IV (2026/2027)		
Iš viso:	4	3

Lentelė 1. Studijų planas ir jo vykdymo suvestinė

Studijuojami dalykai

Egzaminai		
Planas	Įvykdyta	Būklė
Informatikos ir informatikos inžinerijos tyrimo metodai ir metodika 2024 m. II ketvirtis	Informatikos ir informatikos inžinerijos tyrimo metodai ir metodika, 2024-06-25	Išlaikyta
Fundamentalieji informatikos ir informatikos inžinerijos metodai 2025 m. I ketvirtis	2025 m. I ketvirtis	Išlaikyta
Automatizuoti verifikavimo ir validavimo metodai 2025 m. II ketvirtis	2025 m. II ketvirtis	Išlaikyta
Gilieji neuroniniai tinklai 2026 m. II ketvirtis	2026 m. II ketvirtis	-

Lentelė 3. Mokslinių tyrimų ir disertacijos rengimo etapai

- 1 Tyrimas
- 2 Studijos
- 3 Moksliniai tyrimai
- 4 Mobilumo veiklos
- 5 Kito pusmečio planas

Planuojamas mokslinių tyrimų planas

PLANUOJAMAS MOKSLINIŲ TYRIMŲ PUBLIKAVIMAS

Preliminari mokslinės publikacijos tema, numatomas mokslo leidinys		Data
1.	Tyrimo "Requirements of Cybersecurity of Critical Infrastructure Systems" rezultatų publikavimas tarptautiniame recenzuojamoje mokslo žurnale arba konferencijoje (Pvz. ECCWS, SAFECOMP)	2025 m. II ketvirtis
2.	Tyrimo "Methods for modelling cyber security requirements for critical infrastructure systems" rezultatų publikavimas tarptautiniame recenzuojamoje mokslo žurnale arba konferencijoje (Pvz. ECCWS, SAFECOMP)	2026 m. III ketvirtis
3.	Tyrimo "Formal verification of the requirements ensuring the security of critical infrastructure systems" rezultatų publikavimas žurnaluose su citavimo rodikliu (WoS IF) (Pvz. Journal of cybersecurity, Journal of IEEE, IT IEEE Transactions on Dependable and Secure Computing Professional, IEEE Transactions on Reliability, Formal Aspects of Computing)	2026 m. IV ketvirtis
4.	Tyrimo "Ensuring and improving the cyber security of critical infrastructure systems using formal verification and artificial intelligence" rezultatų publikavimas žurnaluose su citavimo rodikliu (WoS IF) (Pvz. Journal of cybersecurity, Journal of IEEE, IT IEEE Transactions on Dependable and Secure Computing Professional, IEEE Transactions on Reliability, Formal Aspects of Computing)	2027 m. II ketvirtis

Mokslinių tyrimų suvestinė

Studijų metai	Dalyvavimas konferencijose				Publikacijos					
	Tarptautinėse ²		Nacionalinėse ³		Su citav. rodikliu ⁴			Be citav. rodiklio ⁵		
	Planas	Įvykdyta	Planas	Įvykdyta	Planas	Įvykdyta ⁶	Būklė ⁷	Planas	Įvykdyta ⁶	Būklė ⁷
I (2023/2024)										
II (2024/2025)	1	0						1	0	Pateikta
III (2025/2026)	1							1		
IV (2026/2027)					2			1		
Iš viso:	2	0			2	0		2	0	

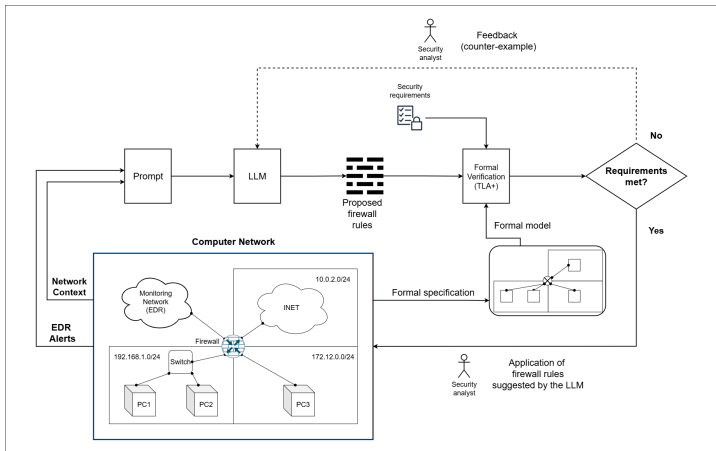
Lentelė 2. Ataskaitinis laikotarpis - studijų metai II: 2024/2025 - II pusmetis

Pateikti straipsniai

Publikacijos			
Planas	Ivykdyta	Būklė	Publikacijos tipas
IEEE ICC 2026 Conference Proceedings	D.Daukševič, L.Laibinis, R.Magan “Formal verification of LLM-based cybersecurity improvements”	Pateikta (2025-09-29)	Be citav. rodiklio

Lentelė 4. Pateikti publikacijai straipsniai

Formal verification of LLM-based cybersecurity improvements



- 1 Tyrimas
- 2 Studijos
- 3 Moksliniai tyrimai
- 4 Mobilumo veiklos**
- 5 Kito pusmečio planas

Bendradarbiavimas su Granados Universitetu



Vasaros stovykla Marktoberdorf 2025



- 1 Tyrimas
- 2 Studijos
- 3 Moksliniai tyrimai
- 4 Mobilumo veiklos
- 5 Kito pusmečio planas

Disertacijos rengimo etapai

MOKSLINIŲ TYRIMŲ IR DISERTACIJOS RENGIMO ETAPAI

Darbo pavadinimas	Atlikimo terminai	
	Nuo	Iki
1. Mokslinių tyrimų disertacijos tema apžvalga ir analizė (Lietuvoje ir užsienyje):		
1.1. Disertacijos tyrimo objekto detalizavimas	2024 m. I ketvirtis	2024 m. I ketvirtis
1.2. Mokslinės literatūros ir publikacijų analizė	2024 m. I ketvirtis	2025 m. IV ketvirtis
1.3. Kitų publikacijų analizė (standartai, reikalavimai ir pan.)	2024 m. I ketvirtis	2025 m. IV ketvirtis
2. Mokslinio tyrimo vykdymas:		
2.1. Tyrimo metodikos sudarymas:		
2.1.1. Tyrimo metodikos iškeltiems uždaviniams spręsti parinkimas	2024 m. I ketvirtis	2024 m. III ketvirtis
2.1.2. Teorinio ir empirinio tyrimų (pagal pasirinktą metodiką) planų sudarymas	2024 m. IV ketvirtis	2025 m. II ketvirtis
2.2. Teorinis tyrimas:		
2.2.1. Kritinės infrastruktūros sistemų saugumo pažeidžiamų lygmenų įtakos tyrimas bei taksonomijos pažeidžiamumo paviršiui aprašyti sudarymas	2024 m. III ketvirtis	2026 m. I ketvirtis
2.2.2. Kritinės infrastruktūros sistemų saugumo užtikrinimo reikalavimų modeliavimo apjungiant formalaus verifikavimo ir dirbtinio intelekto metodų tyrimas	2025 m. III ketvirtis	2026 m. III ketvirtis
2.3. Empirinis tyrimas:		
2.3.1. Kritinės infrastruktūros sistemų saugumo užtikrinimo reikalavimų formalaus verifikavimo tyrimas (parinktų pavyzdžio sistemų pagrindu)	2026 m. I ketvirtis	2027 m. I ketvirtis
2.3.2. Kritinės infrastruktūros sistemų saugumo užtikrinimo sprendimų ir taikomų metodų optimizavimas ir tobulinimas taikant formalaus verifikavimo ir dirbtinio intelekto įrankius (parinktų pavyzdžio sistemų pagrindu)	2026 m. III ketvirtis	2027 m. II ketvirtis
2.4. Gautų duomenų analizė, apibendrinimas, išvadų parengimas:		
2.4.1. Gautų duomenų analizė	2026 m. II ketvirtis	2027 m. I ketvirtis
2.4.2. Rezultatų apibendrinimas ir išvadų parengimas	2027 m. I ketvirtis	2027 m. II ketvirtis
3. Atskirų daktaro disertacijos dalių (tyrimo metodikos, rezultatų, ginamų teiginių, išvadų, ir kt.) parengimas:		
3.1. Tyrimo metodikos sudarymas	2024 m. I ketvirtis	2025 m. II ketvirtis
3.2. Teorinės disertacijos dalies parengimas	2024 m. III ketvirtis	2026 m. III ketvirtis
3.3. Eksperimentinės disertacijos dalies parengimas	2026 m. I ketvirtis	2027 m. II ketvirtis
3.4. Gautų duomenų analizė, apibendrinimas, išvadų parengimas	2026 m. I ketvirtis	2027 m. II ketvirtis
4. Daktaro disertacijos parengimas ir svarstymas padalinyje:	2027 m. I ketvirtis	2027 m. III ketvirtis
5. Daktaro disertacijos gynimas:	2027 m. III ketvirtis	2027 m. IV ketvirtis

Kito pusmečio darbo planas

- Pabaigti mokslinės literatūros ir publikacijų analizę;
- Paruošti sekantį straipsnį tarptautinei mokslo konferencijai;
- Pradėti rezultatų analizę;
- Pradėti studijuoti pasirenkamąjį studijų dalyką "Gilieji neuroniniai tinklai"