

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

Daniel Daukševič

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

Ataskaitinė Informatikos krypties doktorantų konferencija
2024 m. rugsėjo 30 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)

Disertacijos rengimo etapai

MOKSLINIŲ TYRIMŲ IR DISERTACIJOS RENGIMO ETAPAI

Darbo pavadinimas		Atlikimo terminai		Pastabos
		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 išskeltiems 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	

Planuojamas mokslinių tyrimų publikavimas

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

Turinys

- 1 Tyrimas
- 2 Studijuojami dalykai
- 3 Bendrieji gebėjimai
- 4 Mobilumo veiklos
- 5 Kito pusmečio planas

- 1 Tyrimas
- 2 Studijuojami dalykai
- 3 Bendrieji gebėjimai
- 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 sukurto 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;

Rengimo etapai

- Tyrimo metodikos sudarymas
- Teorinis tyrimas
- Empirinis tyrimas
- Gautų duomenų analizė ir apibendrinimas

Tyrimo metodika

- Reikalavimų identifikavimas
- Formalių metodų pasirinkimas
- Dirbtinio intelekto metodų pasirinkimas
- Eksperimentinė analizė
- Tikslų pasiekimo įvertinimas

- 1 Tyrimas
- 2 Studijuojami dalykai
- 3 Bendrieji gebėjimai
- 4 Mobilumo veiklos
- 5 Kito pusmečio planas

Studijų planas

STUDIJŲ PLANAS

	Dalyko pavadinimas	Kreditai (ECTS)	Atsiskaitymo data	Dalyko konsultantas
1.	Informatikos ir informatikos inžinerijos tyrimo metodai ir metodika	8	2024 m. II ketvirtis	A. Lupeikienė
2.	Fundamentalieji informatikos ir informatikos inžinerijos metodai	8	2025 m. I ketvirtis	J. Žilinskas
3.	Gilieji neuroniniai tinklai	7	2025 m. II ketvirtis	P.Treigys
4.	Automatizuoti verifikavimo ir validavimo metodai	7	2026 m. I ketvirtis	L.Laibinis

Dalykai

- ***Informatikos ir informatikos inžinerijos tyrimo metodai ir metodika (Išlaikyta)***
- Fundamentalieji informatikos ir informatikos inžinerijos metodai
- Automatizuoti verifikavimo ir validavimo metodai
- Gilieji neuroniniai tinklai

Studijų planas

Studijos		Studijuojami dalykai		
Metai	Pusmetis	Planas	Vykdoma	Įvykdyta
2024	Pavasaris	1		1
	Ruduo	1	1	
2025	Pavasaris	1		
	Ruduo	1		

- 1 Tyrimas
- 2 Studijuojami dalykai
- 3 Bendrieji gebėjimai**
- 4 Mobilumo veiklos
- 5 Kito pusmečio planas

Mokymų planas

BENDRIEJI GEBĖJIMAI

	Dalyko pavadinimas	Kreditai (ECTS)	Atsiskaitymo data
1.	PEDAGOGINĖS VEIKLOS GEBĖJIMŲ UGDYMO MODULIS	1	2025 m. IV ketvirtis
2.	LATEX	1.25	2025 m. IV ketvirtis
3.	RETORIKA	1	2025 m. IV ketvirtis

Mokymai

- ***Pedagoginės veiklos gebėjimų ugdymo modulis (Išlaikyta)***
- ***LaTeX (Išlaikyta)***
- Retorika

Mokymų planas

Studijos		Bendrieji gebėjimai		
Metai	Pusmetis	Planas	Vykdoma	Įvykdyta
2024	Pavasaris			2
	Ruduo		1	
2025	Pavasaris			
	Ruduo	3		

- 1 Tyrimas
- 2 Studijuojami dalykai
- 3 Bendrieji gebėjimai
- 4 Mobilumo veiklos**
- 5 Kito pusmečio planas

Mobilumo planas

Studijos		Mobilumas		
Metai	Pusmetis	Planas	Vykdoma	Įvykdyta
2024	Pavasaris			1
	Ruduo			
2025	Pavasaris			
	Ruduo	1		

Vasaros mokykla "Cyber in Normandy 2024" (06.24-07.05)



pav. 1: ENSICAEN vasaros mokykla

Vasaros mokykla "Cyber in Normandy 2024" (06.24-07.05)



pav. 2: ENSICAEN vasaros mokyklos dalyviai

Vasaros mokykla "Cyber in Normandy 2024" (06.24-07.05)



pav. 3: ENSICAEN vasaros mokyklos paskaita

- 1 Tyrimas
- 2 Studijuojami dalykai
- 3 Bendrieji gebėjimai
- 4 Mobilumo veiklos
- 5 Kito pusmečio planas

Tikslai

- Išlaikyti studijuojamą privalomąjį dalyką
- Atsiskaityti studijuojamą bendrųjų gebėjimų modulį
- Sudaryti teorinio ir empirinio tyrimų (pagal pasirinktą metodiką) planus