

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Shchapaniak** Jméno: **Andrei** Osobní číslo: **524967**
Fakulta/ústav: **Fakulta informačních technologií**
Zadávající katedra/ústav: **Katedra aplikované matematiky**
Studijní program: **Informatika**
Specializace: **Znalostní inženýrství**

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Automatizované bezpečnostní audity Ethereum smart kontraktů

Název diplomové práce anglicky:

Automated Security Auditing of Ethereum Smart Contracts

Jméno a pracoviště vedoucí(ho) diplomové práce:

Ing. Josef Gattermayer, Ph.D. katedra informační bezpečnosti FIT

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: **14.10.2025**

Termín odevzdání diplomové práce: _____

podpis vedoucí(ho) ústavu/katedry

podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Diplomant bere na vědomí, že je povinen vypracovat diplomovou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v diplomové práci.

Datum převzetí zadání

Shchapaniak Andrei

Podpis studenta

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Shchapaniak** Jméno: **Andrei** Osobní číslo: **524967**
Fakulta/ústav: **Fakulta informačních technologií**
Zadávající katedra/ústav: **Katedra aplikované matematiky**
Studijní program: **Informatika**
Specializace: **Znalostní inženýrství**

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Automatizované bezpečnostní audity Ethereum smart kontraktů

Název diplomové práce anglicky:

Automated Security Auditing of Ethereum Smart Contracts

Pokyny pro vypracování:

Smart contract security audits are critical for preventing vulnerabilities that can lead to significant financial losses. Audits relying on manual code review are time-consuming and may miss still miss vulnerabilities. Recent advances in Large Language Models (LLMs) have demonstrated potential for automated reasoning and code analysis, opening new possibilities for AI-assisted security auditing.

The goal of this thesis is to investigate the application of LLMs for automated security auditing of Ethereum smart contracts and develop a prototype system that enhances the efficiency and coverage of vulnerability detection.

Instructions:

- Study Ethereum smart contract security, common vulnerability patterns, and existing auditing methodologies.
- Conduct a state of the art review on the integration of Large Language Models for automated reasoning and the development of AI-based auditing agents.
- Design a system that integrates an LLM into the security auditing workflow.
- Implement a prototype to perform automated vulnerability detection in smart contract audits.
- Evaluate and compare the implemented system with existing auditing tools and frameworks in terms of accuracy, coverage, and efficiency. Test the system on a dataset of real-world smart contracts with known vulnerabilities.
- Discuss the obtained results, limitations, and potential improvements of LLM-based auditing systems.

Seznam doporučené literatury: