**UNIVERZITA OBRANY**

**Fakulta vojenských technologií**

Akademický rok: 2022/2023

Studijní program: Kybernetická bezpečnost

Forma studia: prezenční

Studijní obor/modul/specializace:

Katedra: K209

Garant studijního programu: plk. gšt. doc. Ing. Petr Františ, Ph.D.

**ZADÁNÍ DIPLOMOVÉ PRÁCE**

Hodnost, jméno a příjmení studenta: rtn. Vojtěch Bžatek

Téma (česky): Využití postkvantových algoritmů pro zabezpečení informačního systému

Téma (anglicky):

1

|  |  |
| --- | --- |
| Vedoucí závěrečné práce: | Prof. Dr. Ing. Alexandr Štefek |
| Konzultanti: |  |
|  |  |
| Datum zadání: | 1. 6. 2023 |
| Termín odevzdání: | 31. 5. 2024 |
| Podpis studenta: | ……………………………………………………….. |

**I. Upřesnění podmínek zpracování závěrečné práce**

V souvislosti se zpracováním závěrečné práce NEBUDE studentem nakládáno s utajovanými informacemi.

V souvislosti se zpracováním závěrečné práce NEBUDE studentem nakládáno s informacemi pro služební potřebu.

Závěrečná práce NEBUDE obsahovat utajené informace.

Závěrečná práce NEBUDE obsahovat informace pro služební potřebu.

Při zpracování závěrečné práce NEBUDOU zpracovávány osobní údaje.

**II. Cíl závěrečné práce**

Navrhnout možnosti využití nejnovějších poznatků z oblasti kvantového šifrování a využití blockchain pro potřeby ochrany dat v informačních systémech.

Nezbytné součásti diplomové práce:

* Přehled algoritmů a jejich open source implementací z kategorie tzv. postkvantového šifrování.
* Přehled ochranných mechanismů pro zabezpečení dat v informačním systému s ohledem na možnost odhalení manipulace s daty.
* Implementace mikroslužby zabezpečující operace typu šifrování a podepisování nad datovými bloky.
* Implementace mikroslužby zabezpečující technologii blockchain nad logovými soubory informačního systému.

**III. Pokyny pro zpracování závěrečné práce**

1. Zpracujte přehled dostupných opensource implementací šifrování (tzv. postkvantové algoritmy), specificky výstupy ze soutěží nist.gov.
2. Zpracujte přehled možných útoků na standardně implementované informační systémy (datové úložiště).
3. Zpracujte přehled možných protiopatření (ochranných mechanismů).
4. Implementujte mikroslužbu využívající tzv. postkvantových algoritmů pro šifrování pro zabezpečení dat proti specifickým modifikacím dat.

Průběžně udržujte aktualizovaný přehled použité literatury a ke každé dílčí etapě zpracujte cca 7 stran shrnutí.

**IV. Doporučená literatura**

V Brně dne ……………………………… ………………………………………………………….……

Vedoucí závěrečné práce

V Brně dne ……………………………… ………………………………………………………….……

Vedoucí odborné katedry

V Brně dne ……………………………… ………………………………………………………….……

Garant studijního programu

2