



# SÉMANTICKÉ PUBLIKOVANIE SPRAVODAJSKÝCH DÁT O BEZPEČNOSTNÝCH HROZBÁCH

Bc. Matej Rychtárik

# ZÁKLADNÉ ÚDAJE

- **Študent:** Bc. Matej Rychtárik
- **Vedúci:** doc. RNDr. Martin Homola, PhD.
- **Ciel':**

Cieľom je navrhnuť vhodnú ontológiu pre publikovanie spravodajských dát o bezpečnostných hrozbách a vytvorenie repozitára za týmto účelom v sieti prepojených dát.

# AKTUÁLNY STAV

- Tvorba článku v spolupráci s vedúcim práce a p. **Ing. Štefan Balogh, PhD.**
  - Moja úloha: spracovať existujúce ontológie, čo spracúvajú a či sú písané v .owl
  - Z tohto článku budem čerpať svoje spracovania existujúcich ontológií do časti Existujúce riešenia
- Napísaná časť práce prehľadu problematiky
- Rozbehané prostredie na vývoj ontológií – Protégé



# POSTUP DO KONCA LETA

- Dokončiť analýzu existujúcich riešení
- Z začať s tvorbou ontológie na základe zistených poznatkov
- Dokončiť kapitolu prehľad problematiky

# VALIDÁCIA A ROBUSTNOSŤ

- Ontológia – Tbox
  - Kontrola konzistentnosti výslednej ontológie
  - Kontrola splniteľnosti tried
- Ontológia – Abox
  - Kontrola konzistentnosti dát
  - Kontrola splniteľnosti dopytu
- Vytvorenie Test Case, ktoré budú musieť byť splnené

# PREŠTUDOVANÉ MATERIÁLY 1

- Christian Bizer, Tom Heath, and Tim Berners-Lee. **Linked data**: The story so far.
- Tim Berners-Lee, James Hendler, and Ora Lassila. **The semantic web**.
- Nicola Guarino, Daniel Oberle, and Steen Staab. **What is an ontology?**
- Michael Iannacone, Shawn Bohn, Grant Nakamura, John Gerth, Kelly Huer, Robert Bridges, Erik Ferragut, and John Goodall. **Developing an ontology for cyber security knowledge graphs**. – STUCCO
- Vasileios Mavroeidis and Siri Bromander. **Cyber threat intelligence model**: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence.



# PREŠTUDOVANÉ MATERIÁLY 2

- Leo Obrst, Penny Chase, and Richard Markelo. Developing an ontology of the cyber security domain. Zareen Syed, Ankur Padia, Tim Finin, M. Lisa Mathews, and Anupam Joshi. **UCO**: A unie
- A.T. Schreiber and Raimond. Ontotext and, **sparql** overview. <https://www.w3.org/TR/2013/REC-sparql11-overview-20130321/>
- A.T. Schreiber and Raimond. **Rdf framework**. <https://www.w3.org/TR/rdf11-primer/>
- Malek Ben Salem and Chris Wacek. Enabling new technologies for cyber security defense with the **icas** cyber security ontology.

# PREŠTUDOVANÉ MATERIÁLY 3

- Takeshi Takahashi, Bhola Panta, Youki Kadobayashi, and Koji Nakao. Web of cybersecurity: Linking, locating, and discovering structured cybersecurity information.
- Alessandro Oltramari, Lorrie Faith Cranor, Robert J Walls, and Patrick D McDaniel. Building an ontology of cyber security.
- John Pinkston, Jerrey Undercoer, Anupam Joshi, and Timothy Finin. A target-centric ontology for intrusion detection.



# PRESKÚMANÉ ÚLOŽISKÁ

- <https://cwe.mitre.org/index.html>
- <https://cve.mitre.org/index.html>
- <https://capec.mitre.org/>