**1.Milyen címet adna a ma átbeszélt szakdolgozati témájának?**

Előrejelzési modellek fejlesztése

**2. Mi lenne az alcím?**

Felhő-alapú kiberbiztonsági döntésekhez kapcsolódó, előrejelzési modellek fejlesztése

**3. Hogyan nézzen ki a cím angolul?**

Developing forecasting modells

**4. Mi legyen az alcím fordítása angolra?**

Developing forecasting models, related to cloud-based cybersecurity decisions

**5. Miként írná le kb. 1000 karakterben a dolgozat lényegét (vö. kivonat) = célok, célcsoportok, hasznosság, feladatok, motiváció**

**Célok**: Olyan felhő-alapú rendszer modellezése, ami az adatok elemzése alapján képes azonosítani a szokatlan viselkedéseket és potenciálisan veszélyes mintákat, még mielőtt azok komoly károkat okoznának egy szervezetben.

**Célcsoport**: Kormányzati szervek, Vállalatok, Általános felhasználók.

**Hasznosság:** Egy kibertámadás vagy adatszivárgás nem csak anyagi veszteségeket okozhat, hanem a szervezet reputációját is károsíthatja. Továbbá jelentős bírságokkal is járhat. Az előrejelző programok segíthetnek a jogi problémák elkerülésében. Valamint a biztonságosan működő vállalatok vonzóbbak lehetnek a partnerek és a befektetők számára.

**Feladatok**: Adatgyűjtés, sérülékenységek azonosítása, kockázatértékelés, Riportok készítése, Automatizált intézkedések végrehajtása.

**Motiváció:** A kiberbiztonsági előrejelzési szoftverek fejlesztése komoly kihívást jelent.

**6. Hogyan néz ki angolul (abstract) a magyar kivonat?**

My goal is modeling a cloud-based system that can identify unusual behaviors and potentially harmful patterns based on data analysis before they cause significant damage to an organization.

 It can be beneficial for government agencies, businesses, and general users as well.

A cyberattack or data breach can not only result in financial losses but also damage the reputation of an organization. Furthermore, it can lead to significant fines. Predictive programs can help in avoiding legal issues. Additionally, securely operating companies may appear more attractive to partners and investors.

The tasks of the program include data collection, identifying vulnerabilities, risk assessment, generating reports, executing automated actions, tracking and forecasting cyberattacks and threats on both national and international levels.