



NEMZETI
KÖZZSZOLGÁLATI
EGYETEM
LUDOVIKA

A PROMPTOLÁSTÓL A NAPRAKÉSZ TUDATOSÍTÁSIG

Avagy mire is lehet jó még egy promptverseny?

Magyar Sándor
2025. április 10.

Agenda



Bevezetés

A prezentáció
céljának áttekintése.



Verseny

Beszélgetés a
versenyképesség
aspektusairól.



Feladatok

A teljesítendő
feladatok vázlata.



Tudatosítás

A tudatosság
fontosságának
hangsúlyozása.



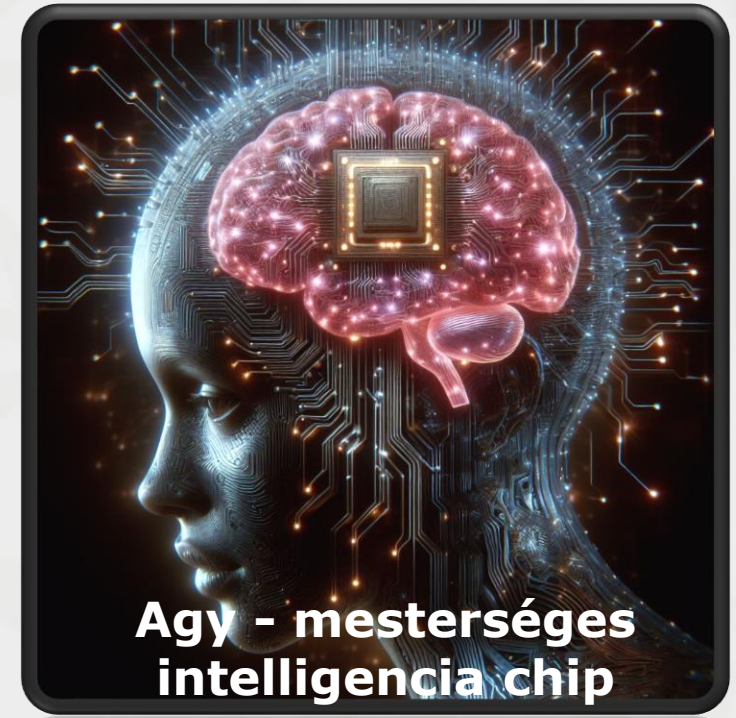
Összegzés

A megvitatott
kulcspontok
összefoglalása.

Mesterséges Intelligencia

- Azon módszerek és elméletek összessége, amelyek célja az emberi kognitív képességek (például tanulás, érvelés, problémamegoldás) számítógépes modellezése és reprodukálása. Ez magában foglalja olyan algoritmusok és rendszerek kidolgozását, amelyek képesek autonóm döntéshozatalra, mintázatfelismerésre, valamint komplex adatok értelmezésére.

Mesterséges intelligencia



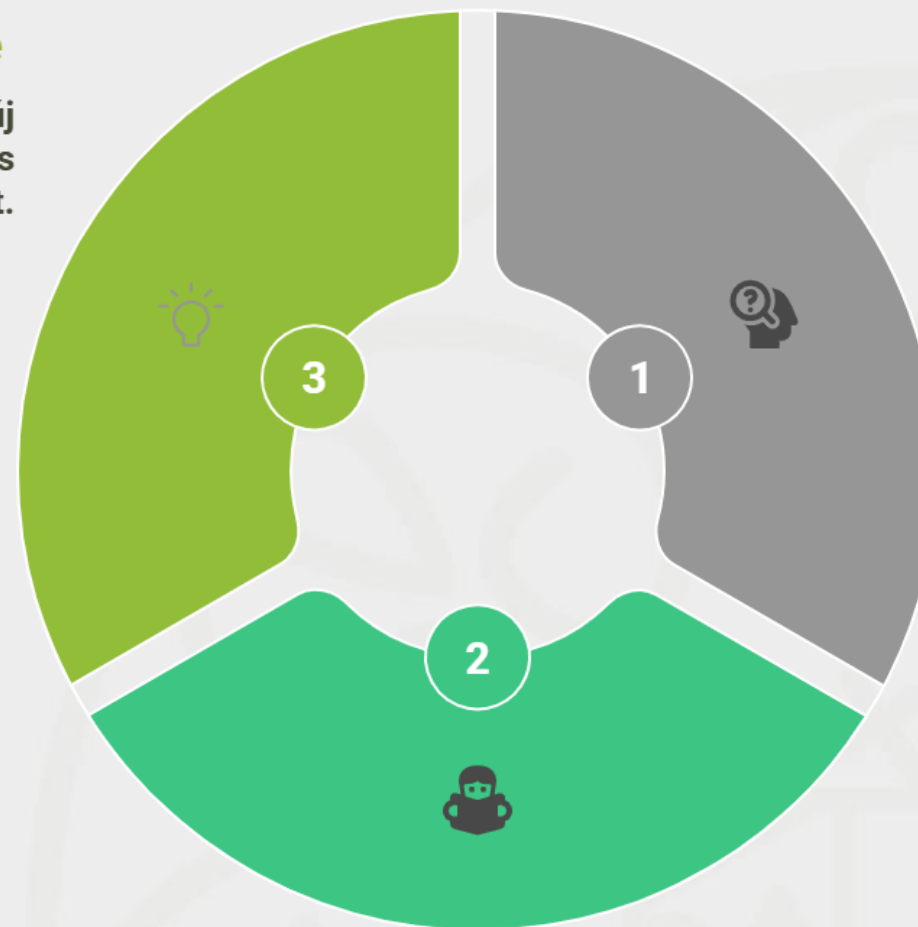
Eredmény elérése régi módi tanulási folyamattal

Tudás megszerzése

Megszerzünk új
ismereteket és
készségeket.

Nemtudás elismerése

Felismerjük, hogy
hiányzik a tudás.



Tanulás

Aktívan keresünk információt
és megértést.

Promptolás

- A promptolás olyan eljárás vagy módszertan, amelynek során a felhasználó célzott utasításokkal látja el a mesterséges intelligenciát annak érdekében, hogy a kívánt választ vagy tartalmat generáltassa vele.
- A promptolás lényege, hogy strukturált, egyértelmű és célszerű bemenetet adjunk az MI-rendszernek, így befolyásolva annak kimenetét és növelve a válasz minőségét.

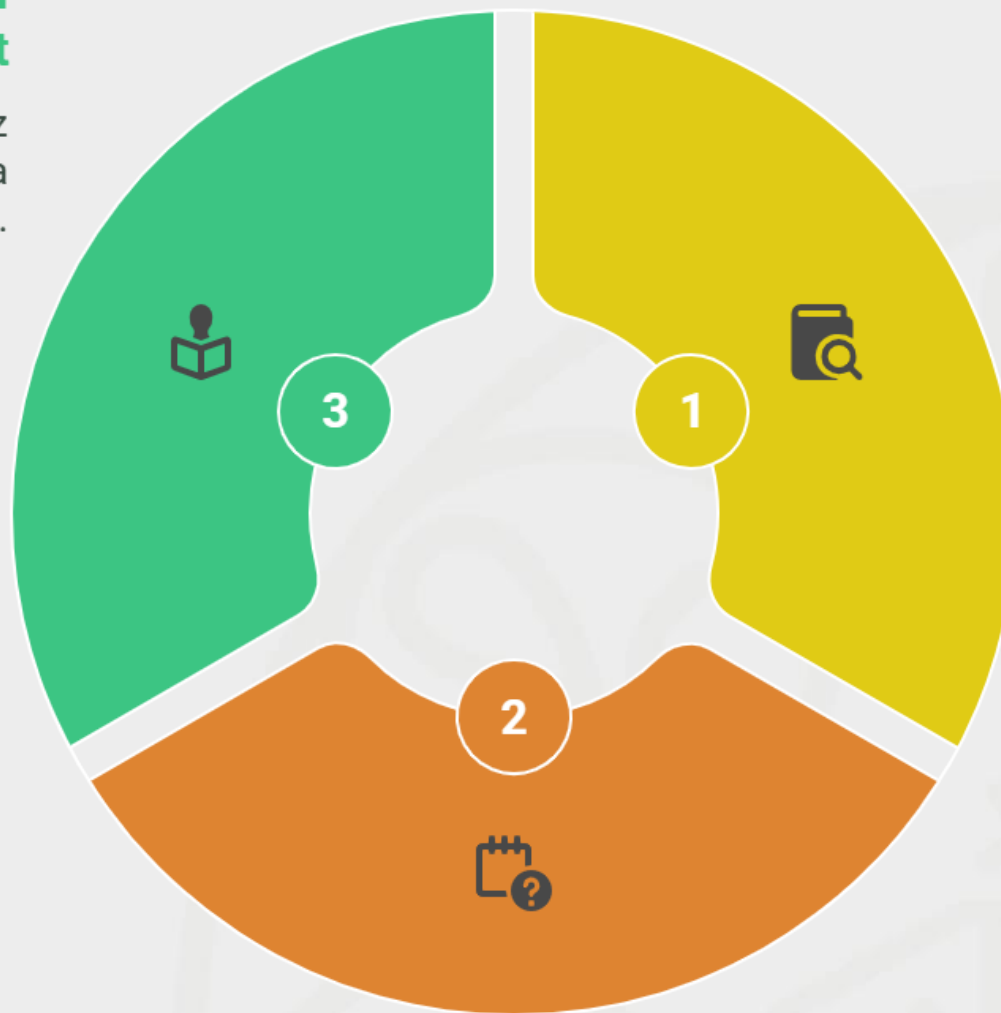
Eredmény elérése az módszerrel

Megszerezni a Tudást

Gyűjteni az
információt és a
megértést.

Felismerni a Tudásrészeket

Azonosítani,
hogymit nem
tudunk.

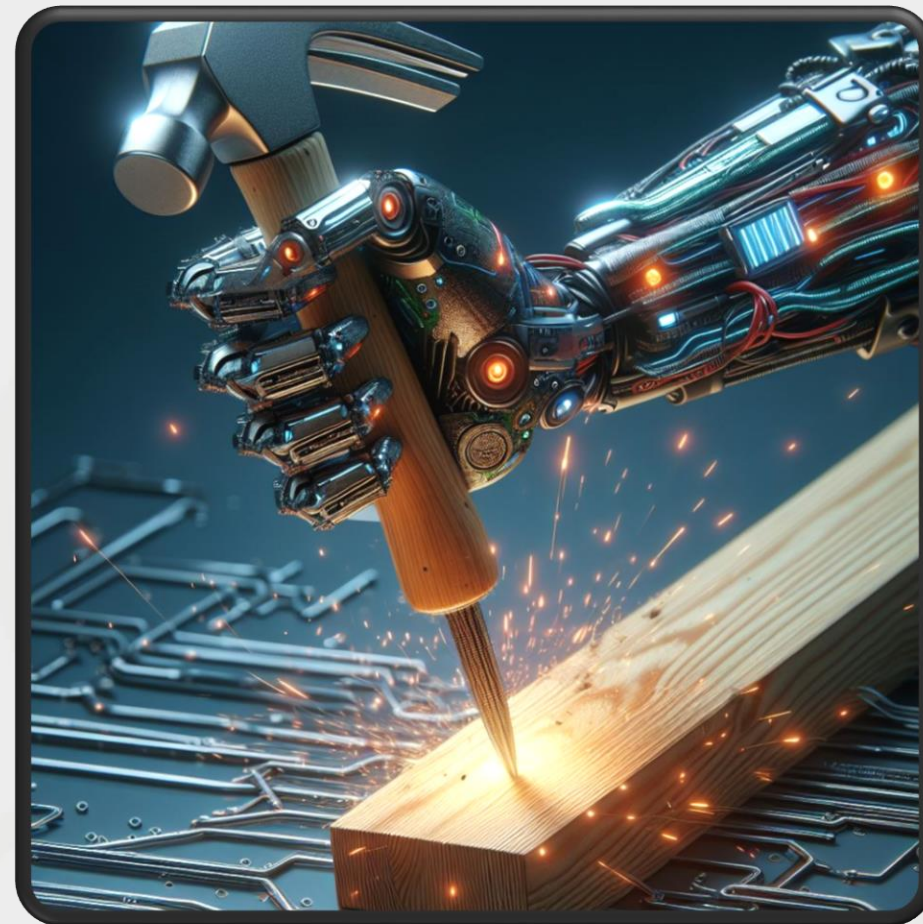


Megfogalmazni a Kérdéseket

Fejleszteni a pontos kérdéseket.

Arany kalapács

„Akinak kalapács van a kezében,
az mindenhol szöget lát!”



Biztonság

Promptok:

- Mik a generatív mesterséges intelligencia használatának veszélyei egy vállalatnál?
- Mik a mesterséges intelligencia használatának veszélyei a shadow IT szempontjából?

Verseny

Kiberbiztonsági promptoló verseny célja

- A hallgatók együttműködését ösztönző, problémamegoldó gondolkodásra épülő promptoló verseny, amely során egy adott védelmi fókuszú kiberbiztonsági problémára dolgoznak ki megoldásokat. A versenyben két fős csapatok a mesterséges intelligencia (MI) promptolásával adnak átfogó megoldást egy adott kiberbiztonsági eseményre. A promptoló verseny nemcsak a kiberbiztonsági gondolkodásmódot és a prompt mérnöki készségeket fejleszti, hanem az együttműködés és a kommunikáció fontosságára is ráirányítja a figyelmet.

Verseny kiírása

- **Célközönség:** Nemzeti Közzolgálati Egyetemmel jogviszonyban álló hallgatók.
- **Csapatok létszáma:** Két fő.
- **Időtartam:** 3 óra
- **Elvárt ismeretek:** Generatív MI használata, alapszintű kiberbiztonsági ismeretek.
- **Platform:** a résztvevők által szabadon választott ingyenes és előfizetéses MI platformokon hajtják végre feladataikat.
- **Erőforrások és eszközök:** A résztvevők saját eszközeiken dolgozhatnak. NKE WIFI hálózat a rendezvényen elérhető.

Ajánlott szerepkörök



Prompt mérnök

MI promptok
megtervezése és
optimalizálása.



Megoldás elemző

A generált válaszok
értékelése és végső
dokumentáció
elkészítése.

Etikai irányelvek

- Kizárólag védelmi megoldások kidolgozása megengedett.
- Támadási technikák gyakorlati tesztelése tilos!
- A kidolgozott megoldásoknak meg kell felelniük a hatályos jogszabályoknak!
- Fair play szellem betartása kötelező.

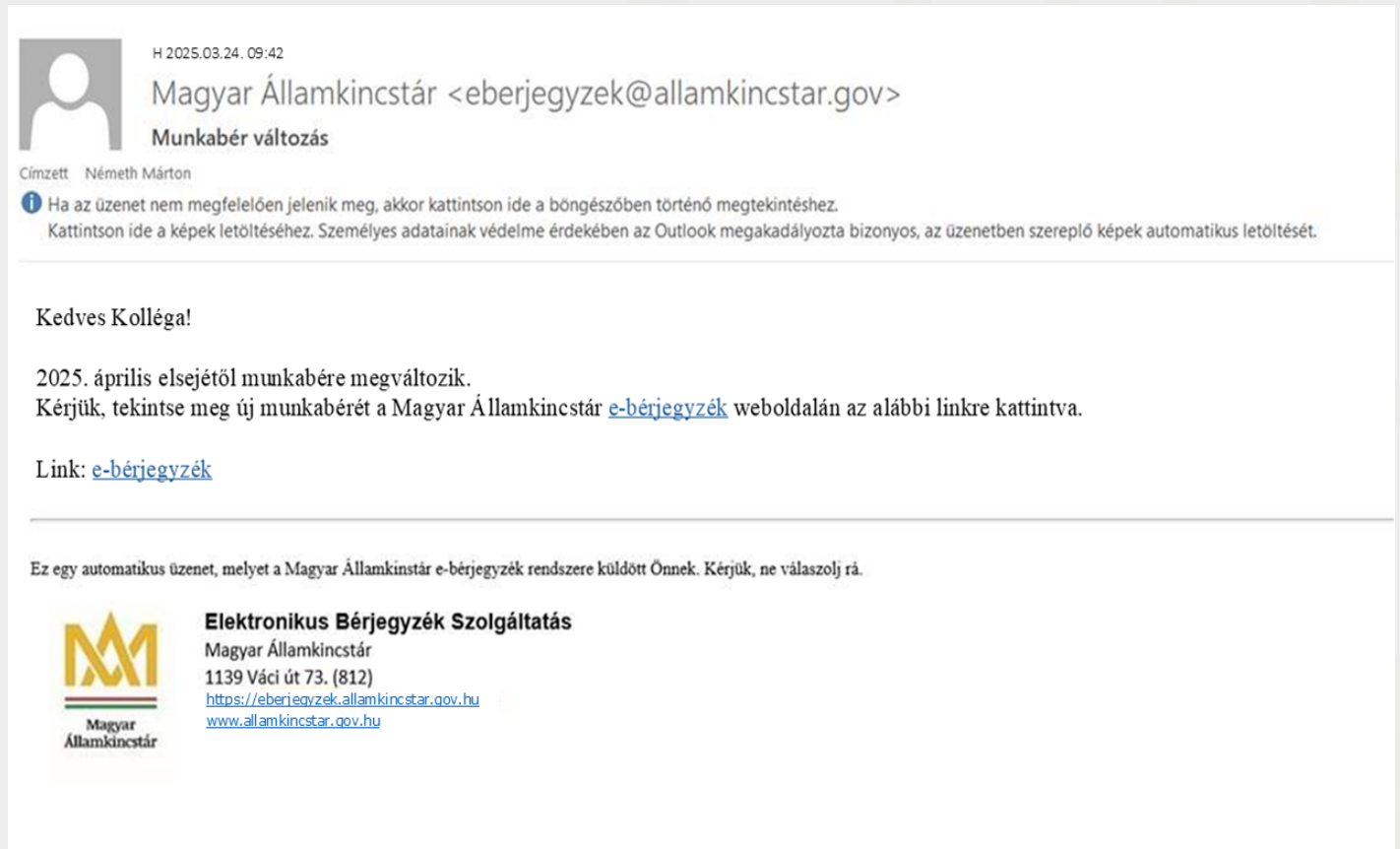
Verseny felépítése

- 1. szabályok és feladatok ismertetése (15 perc).
- 2. első feladat megoldása (45 perc).
- 3. első feladat dokumentálásának megküldése (5 perc).
- 4. második feladat megoldása (50 perc).
- 5. második feladat dokumentálásának megküldése (5 perc).
- 6. rövid prezentációk tartása (5-7 perc) az általuk kidolgozott megoldásokról és promptok bemutatásáról.
- 7. értékelés (10 perc).
- 8. eredményhirdetés (10 perc).

FELADATOK

Szerepbe helyezés

Ön a Nemzeti Közsolgálati Egyetem (NKE) **IT biztonsági vezetője**. Az imént értesült róla, hogy adathalász levelek érkeztek az NKE-re az alábbi tartalommal.



1.1 Tájékoztató értesítés promptolása

- Promptok segítségével hozzon létre egy azonnali tájékoztató értesítést, amelyet a NKE elektronikus postafiókjaiba ki lehet küldeni annak érdekében, hogy megelőzhetőek legyenek az NKE postafiókkal rendelkezők adatszolgáltatásai.
- Tájékoztató levél paraméterei:
 - a könnyebb átláthatóság érdekében legfeljebb egy A4-es oldal terjedelmű legyen;
 - tartalmazzon olyan vizuális elemet (pl. fotó, illusztráció vagy piktogram), amely felhívja a figyelmet és kapcsolódik a tartalomhoz;
 - röviden magyarázza el a teendőket a legrosszabb forgatókönyvre is kitérve;
 - legyen vizuálisan átgondolt, figyelemfelkeltő, és könnyen értelmezhető formátumú. A dokumentum célja, hogy egy kiberbiztonsági incidensről hatékonyan tájékoztassa a megcélzott célcsoportot, ezért a tartalom és a megjelenés támogassa a gyors megértést és a cselekvésre ösztönzést (pl. figyelmeztető jelzések, jól strukturált szöveg, ikonok, színek, kiemelések használata).

1.2 Rövid leírások promptolása

- Promptoljon négy különböző (egyenként max. 10 sor) rövid leírást egy e-mailes kiértékelés formájában arról, hogyan tájékoztatná az Egyetem munkatársait alábbi szerepkörök alapján a bekövetkezett adathalász esetről:
 - adminisztratív munkakörben dolgozó;
 - oktató;
 - hallgató;
 - üzemeltetésen dolgozó munkatárs (takarító, biztonsági szolgálat stb.).

1.3 válaszlevél promptolása

Egy hallgató írt Önnek aggódva, mert rákattintott egy gyanús linkre. Promptoljon neki válaszlevélként egy rövid, megnyugtató üzenetet, ami tartalmazza:

- egy bekezdésben (max. 5 sor) az eseményt;
- a további teendőit (max. 5-10 sor).

2.1 E-learning tananyag létrehozása

Az előző feladattal összhangban hozzon létre az NKE felhasználóknak szóló e-learning tananyagot adathalász támadásokról, 3-5 oldal terjedelemben. A feladat esetében szükséges képekkel, esettanulmányokkal (2-3 valós életben bekövetkezett adathalász támadás) stb. is színesíteni a tartalmat.

A tananyaghoz emellett szükséges 10 önellenőrző kérdés promptolása.

Az e-learning tananyaghoz az 10 feleletválasztós teszt promptolását az alábbiak alapján végezzék el:

- 4 lehetséges válasz kérdésenként.
- Akár több jó megoldás is lehetséges.
- Jó válaszok megjelölése.
- jó válaszok sorrendje véletlenszerű.

2.2 Vezetői jelentés promptolása

Rektor részére vezetői jelentés promptolása, amely tartalmazza a megtett intézkedéseket és a jövőbeni adathalász elleni események elkerülésének a javaslatait.

- A vezetői jelentés rövid, tömör és lényegre törő dokumentum, amely egy hosszabb jelentés, tanulmány vagy projekt főbb pontjait foglalja össze. Célja, hogy a vezetők, döntéshozók gyorsan megértsék a legfontosabb információkat, anélkül hogy az egész anyagot el kellene olvasniuk. A szöveg elején célszerű röviden bemutatni a dokumentum témáját és célját, majd ismertetni a legfontosabb megállapításokat, problémákat és következtetéseket. Ezt követően érdemes konkrét javaslatokat megfogalmazni a továbblépésre vagy döntéshozatalra vonatkozóan, végül pedig egy rövid záró gondolatban összefoglalni, miért releváns a dokumentum, és milyen további lépések javasoltak. Az írás során fontos a tömörség, a világos és közérthető nyelvezet, a logikus szerkezet, valamint az, hogy kerüljük a szakzsargont és a túlzott részletezést. Az összefoglaló ideális esetben legfeljebb 1-2 oldal hosszú, és jól tagolt, könnyen áttekinthető formában készült.

2.3 stílus keverés

- Az Egyetem Adatvédelmi tisztségviselője a segítségét kéri a fenti incidenssel kapcsolatban. Feladata, hogy az egyetem belső e-learning tananyagát kiegészítse egy olyan figyelemfelkeltő rövid anyaggal, amely jogi és személyes szempontokat ötvözve mutatja be, milyen következményei lehetnek egy adathalász incidensnek. A dokumentum az alábbiak alapján készüljön el:
 - első lépésként promptolja a modellt, hogy írjon egy rövid, jogi szempontú adatvédelmi szabályzatot adathalász támadásra való reagálásról, száraz, paragrafus-szerű stílusban, hivatkozva bizonyos paragrafusokra (pl. GDPR, Infotv.).
 - Ezt követően kérje meg, hogy ugyanebbe a szövegbe fűzze bele egy fiktív hallgató személyes történetét, aki véletlenül megadta az adatait. Ebben legyen érzelmi narratíva (például félelem, megbánás), de a jogi szakaszok maradjanak változatlanok, azokat ne módosítsa.
 - Az elkészült anyag hossza: max. 300 szó, vegye figyelembe mind a jogi, mind a személyes narratív szempontokat.

A promptolás dokumentációjának szempontjai

- A verseny célja nem csupán a végtermékek létrehozása, hanem a promptolási folyamat átlátható és reflektív dokumentálása is. Ennek érdekében minden csapat köteles az alábbiakat teljesíteni:
- Minden egyes elkészített feladathoz mellékelni kell:
 - az összes használt promptot (beleértve a kísérletező változatokat is),
 - a promptolás során tapasztalt kihívásokat és megfigyeléseket (pl. miért módosították a promptot, milyen válaszokat kaptak, mire kellett különösen figyelniük),
 - a választott promptstratégia rövid leírását (pl. szerepkijelölés, stílusinstrukciók, kimeneti formátumra vonatkozó elvárások).

GPT-4.5 passed a Turing test, according to a new study

Turing teszt



Összegzés

- A versennyel kapcsolatban nagy volt az érdeklődés.
- Bevált, mint motiváció.
- Számos tapasztalat született a hallgatók és a zsűri részéről is.
- Jó megoldások születtek.
- Tananyagfejlesztésre ad lehetőséget a jövőben.
- Hasonlítható egy TTX-hez.
- A promptolás jövő/jelen elvárt kompetenciája.



KÖSZÖNÖM A FIGYELMET!

uni-nke.hu