Éves jelentés

2025

Számítástechnikai Szakosztály beszámolója

Tartalom

Kapcsolattartási adatok

Vezetőség

Elnök
Dr. Johanyák Zsolt Csaba
Telefon
+36-76-516-413
e-mail
johanyak.csaba@nje.hu

Titkár
Limbay Róbert
Telefon
+36 70 306 1492
e-mail
robert.limbay@gmail.com

Vezetőségi tagok

Név
Szabados Györgyné Andor Éva
Telefon
+36 20 212 0280
e-mail
gyorgyneszabados16@gmail.com

Név
Kamenszky László
Telefon
+36-70-389-6712
e-mail
laszlo.kamenszky@bsis.hu

Név
Dr. Cserny László
Telefon
+36-88-794-973
e-mail
csy.laszlo@gmail.com

Név
Sipos Győző

e-mail
gyozo.sipos@gmail.com

2025. évi rendezvényeink

A Számítástechnikai Szakosztály az EOQ MNB Informatikai Szakbizottságával együttműködve tartotta meg rendezvényeit.

NIS2 a gyakorlatban – Hogyan tudja a megfelelést egy célszoftver támogatni, és miben könnyíti meg a résztvevők munkáját?

Időpont: 2025.03.06.
Előadó: **Dr. Váczi Dániel**, a Brind kiberbiztonsági startup alapítója, ügyvezetője
Helyszín: NJE GAMF

A Brind egy új NIS2 alapú Információbiztonsági Irányítási Platform és Piactér. A startup küldetése, hogy segítsen a megfelelésben, az irányításban és az audit során. Az előadásban ezek mentén mutatja be a platform megálmodója az elmúlt bő egy év tapasztalatai mentén a legnagyobb nehézségeket és osztja meg a tapasztalatait. Az előadást ajánljuk minden a téma iránt érdeklődő hallgatónak és minden érintett szervezet információbiztonsági, informatikai munkatársának, vezetőjének.

A kibervédelem helyzete napjainkban

Időpont: 2025.03.12.
Előadó: **Dr. Göcs László,** Neumann János Egyetem, informatikai igazságügyi szakértő
Helyszín: NJE GAMF

A modern digitális világban a kibervédelem kiemelt jelentőséggel bír mind a vállalatok, mind az egyéni felhasználók számára. Az előadás során áttekintjük a jelenlegi kiberbiztonsági kihívásokat, a leggyakoribb fenyegetéseket, valamint a legújabb védelmi megoldásokat és stratégiákat. Szó lesz az adatvédelem fontosságáról, a zsarolóvírusok, adathalász támadások és más kibertámadási módszerek terjedéséről, valamint az ezek elleni hatékony védekezés lehetőségeiről. Az előadás célja, hogy a résztvevők naprakész információkat kapjanak a kiberbiztonsági trendekről, és gyakorlati útmutatást kapjanak saját védelmi stratégiáik fejlesztéséhez.

AI in Cybersecurity

Időpont: 2025.03.19.
Előadó: **Prof.Dr. Ferdi Sönmez**, İstanbul Aydin University
Helyszín: NJE GAMF

This lecture focuses on how AI can be used to enhance cybersecurity and the challenges and risks involved. It covers the fundamentals, algorithms, and learning modes of AI and how they can be applied to various security technologies and processes. There are many different AI models, stand out as proven applications to cybersecurity, such as machine learning (ML), deep learning (DL), generative AI (GenAI), natural language processing (NLP), and knowledge graph (KG). They can work together to create powerful technologies, including virtual assistants for cybersecurity. The impact of AI on cybersecurity is quite significant in that it helps fill the skill gap, accelerate threat detection, automate processes, and improve security posture. On the other hand, threat actors can misuse and exploit AI to create more sophisticated and evasive cyberattacks. Lastly, we examine the factors that influence the adoption of AI and its future.

Microsoft 365 Copilot – Biztonságos MI használat vállalati környezetben

Időpont: 2026.03.27.
Előadó: **Kozák János**, Crayon Magyarország Kft.
Helyszín: NJE GAMF

A Microsoft 365 Copilot egy rendkívül hasznos MI-alapú eszköz, amely segíti a hatékonyabb munkavégzést dokumentumok létrehozásában, e-mailek kezelésében és információk gyors felfedezésében. Nagyvállalati környezetben azonban kiemelten fontos az adatok védelme, hogy az MI kizárólag az adott felhasználó számára elérhető vállalati tartalmakból dolgozzon.
A biztonságos használat érdekében kulcsfontosságú:

- Adatvédelmi és hozzáférési szabályok beállítása (DLP, Purview)
- Auditálás és naplózás aktiválása (Microsoft 365 Compliance Center)
- Felhasználói engedélyek és szerepkörök pontos meghatározása (RBAC, Conditional Access)
- A Copilot hozzáférésének szabályozása vállalati tartalmakhoz

Mesterséges intelligencia eszközök a szoftverfejlesztésben

Időpont: 2025.09.15.
Előadó: **Dr. Bodon Ferenc**, KX
Helyszín: ÓE BGK

Az AI alapjaiban változtatja meg a szoftverfejlesztők világát. Különböző generációk különböző módon reagálnak a változásra. Az előadásomban egy jellemző folyamatot mutatok be, a tagadást, amely öt fázisból áll. Kitérek majd az AI hatásaira a fejlesztői munkaerőpiacon és praktikus példákon keresztül bemutatom, hogy ma az AI mire használható es mire nem.

AI támogatott programozás - eszközök és technikák

Időpont: 2025.10.02.
Előadó: **Cserkó József**, Neumann János Egyetem
Helyszín: NJE GAMF

Nagyon sokan használják az AI Coding asszisztenseket, és napról-napra jelennek meg új megoldások ezen a területen. Az előadás során áttekintjük a jelenlegi helyzetet, megnézzük melyek azok az asszisztensek amelyek a legjobb teljesítményt nyújták. Beszélni fogunk a hatékonyságról, a Prompt Engineering, Context Engineering, Agentic Coding különböző szintjeiről. Végül arról is szó lesz, hogyan tudjuk ezt beépíteni az oktatásba, akár tanári, akár hallgatói oldalon.

Challenge-Based Learning in Web Security: Real-World Vulnerabilities in the Classroom

Időpont: 2025.10.09.
Előadó: **Prof. Dr. Zlatko Čović**, Subotica Tech-College of Applied Sciences
Helyszín: NJE GAMF

This lecture introduces Challenge-Based Learning (CBL) as an active learning approach in web security education. At Subotica Tech, CBL has been applied through hands-on challenges where students individually solve tasks, submit their code and explanatory reports, and later reflect on solutions in joint discussions.

Through these challenges, students explore and mitigate real-world vulnerabilities such as SQL Injection, XSS, and CSRF in a controlled PHP environment, while practicing secure coding techniques.

Hogyan tartsuk kordában az AI megoldásainkat?

Időpont: 2025.10.30.
Előadó: **Kozák János**, Crayon Magyarország és SoftwareOne Hungary Kft.
Helyszín: NJE GAMF

Az AI – és különösen a generatív AI – hatalmas lehetőségeket nyújt, ugyanakkor új security és megfelelőségi kihívásokat is hoz. Az előadás során bemutatjuk, hogyan tudják a vállalatok felelősen, biztonságosan és szabályozottan bevezetni és működtetni az AI alapú megoldásokat Microsoft technológiák segítségével.

Főbb témáink:

- Microsoft 365 Copilot és Copilot Studio security kontrollok – hogyan biztosítsuk a hatékony, de biztonságos felhasználást.
- M365 biztonsági és megfelelőségi eszközök – hogyan tudjuk tiltani, szabályozni és riportálni a Copilot használatát.
- Microsoft Sentinel integráció – valós idejű monitorozás és fenyegetésészlelés az AI használatban.
- Más generatív AI szolgáltatások tiltása és felügyelete – hogyan akadályozhatjuk meg a nem engedélyezett AI megoldások használatát a szervezetben.

programok segítségével.

Gyere el május másodikán, és ismerd meg, hogy hogyan tudod az üzleti folyamatokat vizualizálni anélkül, hogy bármit is manuálisan kellene elkészítened, valamint, hogy hogyan deríthetsz fényt azokra a folyamatokra, amelyek létezéséről eddig nem is tudtál.

Automatizáció és AI Agentek – mi van a promptoláson túl?

Időpont: 2025.11.13.
Előadó: **Kovach Anton**, Active Vision
Helyszín: NJE GAMF

A mesterséges intelligencia kora új szintre lépett: már nemcsak válaszol a kérdéseidre – hanem dolgozik helyetted. De mit jelent ez a gyakorlatban? Hogyan építhetsz olyan automatizált folyamatokat és AI Agenteket, amelyek valódi értéket teremtenek – akár egyetemistaként, akár vezetőként?

Ipari rendszerek kiberbiztonsága

Időpont: 2025.11.27.
Előadó: **Dr. Répás József**, Alverad Technology Focus Kft.
Helyszín: NJE GAMF

A digitalizáció és az Ipar 4.0 korszakában a gyártás, az energetika, a közlekedés és más kritikus ágazatok egyre inkább támaszkodnak az ipari irányító rendszerekre (ICS) és az ipari technológiákra (OT). Ezek a rendszerek közvetlen kapcsolatban állnak a fizikai környezettel, így működésük biztonsága nem csupán informatikai, hanem gazdasági és társadalmi kérdés is. Az előadás betekintést nyújt az ICS/OT biztonság kihívásaiba és megoldásaiba, különös tekintettel:

- az OT és IT rendszerek eltérő működésére és biztonsági szemléletére,
- a kockázatos ágazatok (pl. energetika, közlekedés, egészségügy, ivóvíz-szolgáltatás) sajátos veszélyeire,
- a kockázatkezelési és védekezési stratégiákra, beleértve a defense-in-depth megközelítést.
- Az előadás választ ad arra, hogy:
- hogyan védhetők az ipari rendszerek a jogosulatlan beavatkozásokkal és kártékony kódokkal szemben,
- milyen különbségek vannak az IT és OT biztonsági prioritások között,
- hogyan lehet összehangolni a technológiai megbízhatóságot és a kiberbiztonsági megfelelést.

A résztvevők átfogó képet kapnak a nemzeti és nemzetközi szabványok (pl. NIST 800-82, 2024. évi LXIX. törvény) szerepéről, valamint gyakorlati példákon keresztül ismerhetik meg, milyen tényezők biztosítják a kritikus rendszerek ellenálló képességét.

Ez az előadás azoknak szól, akik meg akarják érteni, hogyan lehet az ipari rendszerek biztonságát a jövő kihívásaihoz igazítani, és miért elengedhetetlen az OT kiberbiztonság a modern társadalmak működésében.