NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

Aktuality ve výzkumu a vývoji v kybernetické bezpečnosti

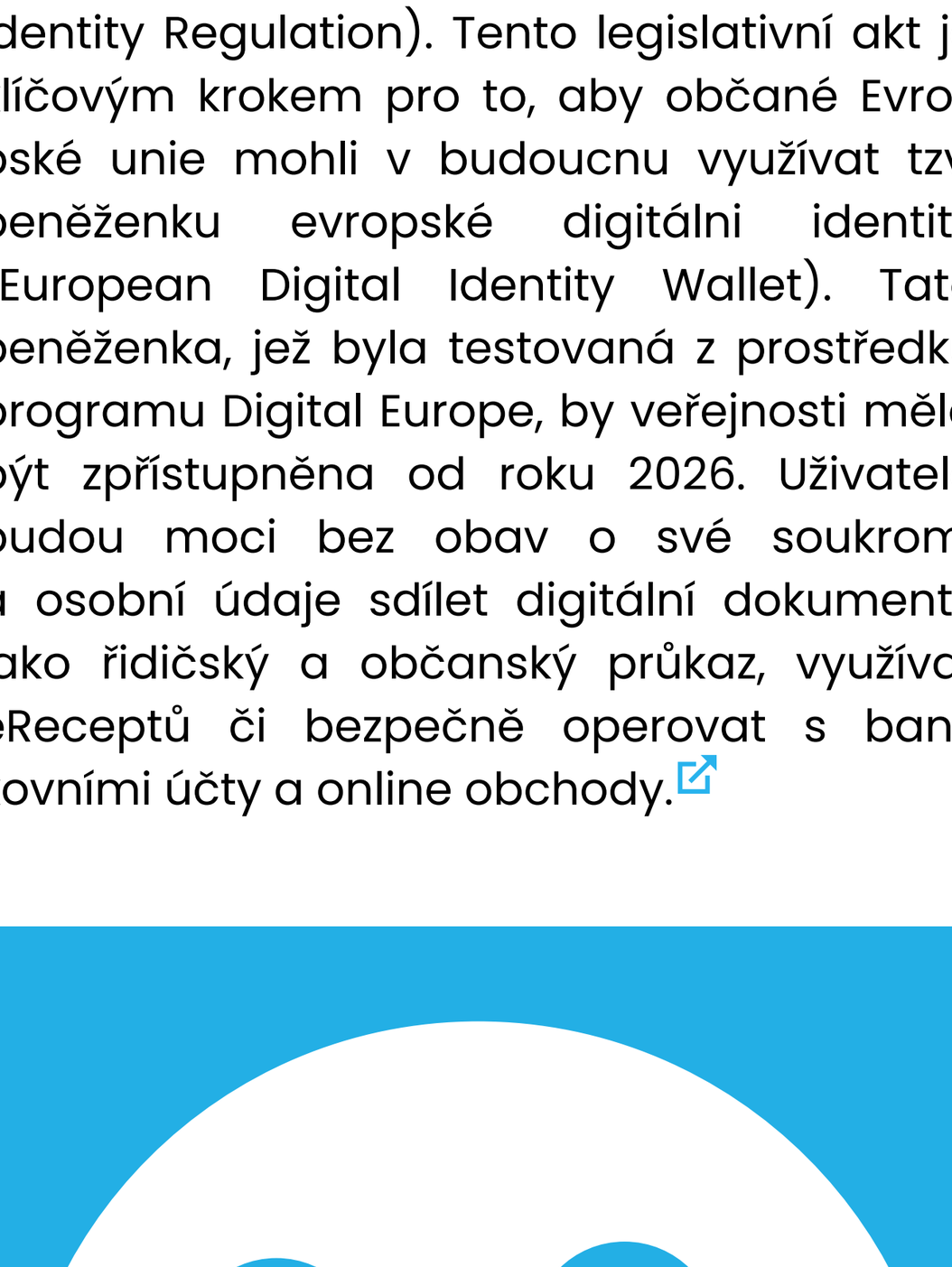
05/2024

KVĚTEN

Aktuality, události a financování

Nařízení o digitální identitě vstoupilo v platnost

Dne 20. května vstoupila v platnost pravidla pro zřízení evropské digitální identity (Digital Identity Regulation). Tento legislativní akt je klíčovým krokem pro to, aby občané Evropské unie mohli v budoucnu využívat tzv. peněženku evropské digitálni identity (European Digital Identity Wallet). Tato peněženka, jež byla testovaná z prostředků programu Digital Europe, by veřejnosti měla být zpřístupněna od roku 2026. Uživatelé budou moci bez obav o své soukromí a osobní údaje sdílet digitální dokumenty jako řidičský a občanský průkaz, využívat eReceptů či bezpečně operovat s bankovními účty a online obchody.

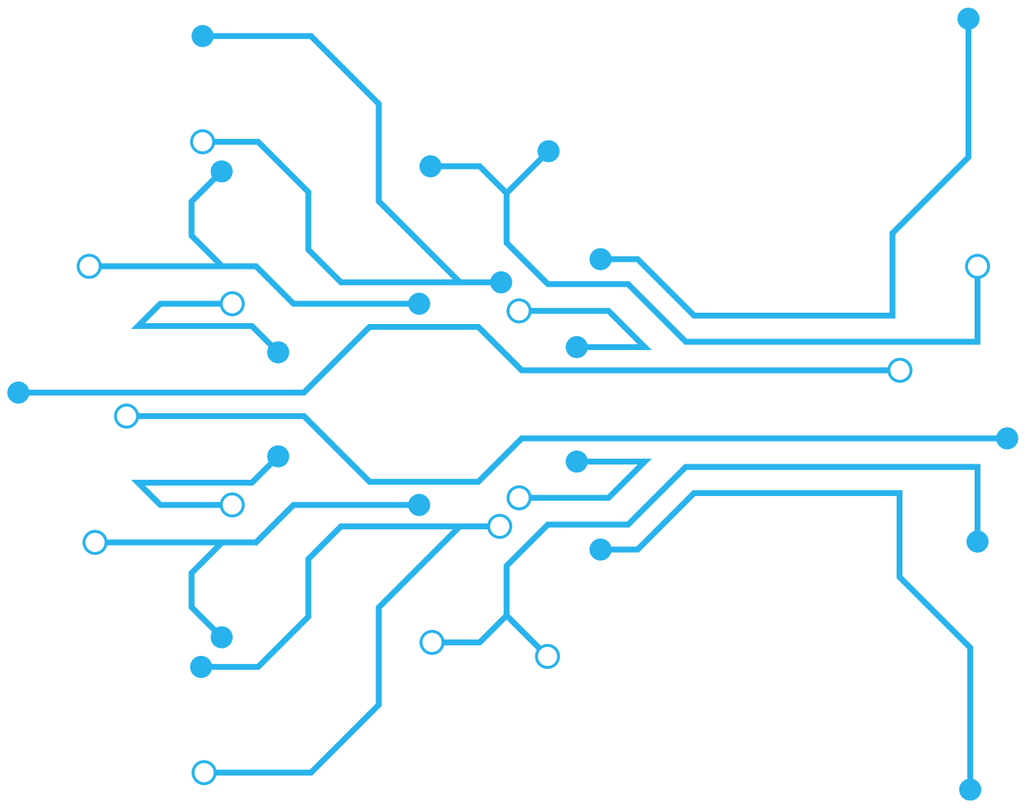


Projekt Technologická inkubace od CzechInvestu realizoval svou čtvrtou výzvu

Výzva, jež byla otevřená do konce května, podpoří žádosti zaměřené na podporu start-upů a malých podniků orientovaných na inovativní technologie, jež jsou komerčně využitelné. Celková částka podpory činí 118 milionů korun. V předchozích výzvách již bylo po výběru odborné komise podpořeno celkově 137 projektů. V rámci čtvrté výzvy mohli zájemci předkládat návrhy start-upů z oblastí umělé inteligence, pokročilých technologií a materiálů, mobility, kreativního průmyslu, ekoinovací a oblasti týkající se ochrany života, zdraví a bezpečnosti.

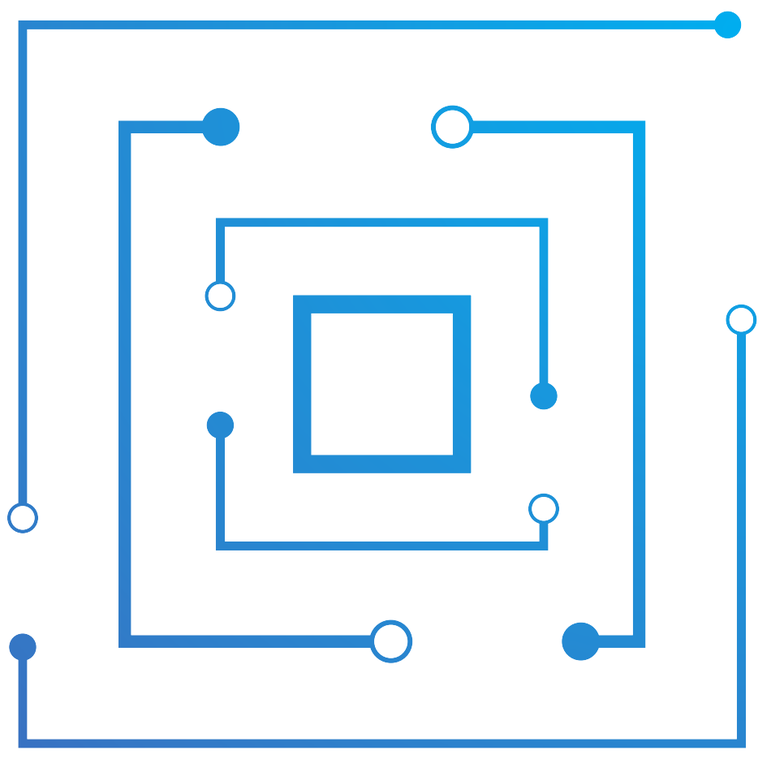
Americká univerzita nově otevírá možnost získat akademický titul v oboru AI

University of Pennsylvania School of Engineering and Applied Science představila možnost získat první online magisterský titul (MSE) v oblasti umělé inteligence. Jedná se o úplně první program svého druhu v rámci univerzit z prestižní skupiny Ivy League, který se zaměřuje na oblast AI. Tento program se poprvé otevře na jaře 2025 a bude se zaměřovat jak na technické, tak etické aspekty AI. Nabídne pokročilé kurzy v oblastech jako je zpracování přirozeného jazyka, strojové učení, hluboké učení a etika AI, které budou vedené špičkovými odborníky v této oblasti. Cílem je připravit absolventy na odbornou a zodpovědnou práci v oblasti vývoje AI ve snaze reagovat na rychlý rozvoj těchto technologií.



ENISA zveřejnila aktualizaci příručky pro budování povědomí o kyberbezpečnosti

Agentura Evropské unie pro kybernetickou bezpečnost (ENISA) obohatila svou příručku zaměřenou na budovaní povědomí o kybernetické bezpečnosti nesoucí název Awareness Raising in a Box. Hlavním cílem této příručky je poskytnout přehled nástrojů, které je možné využít pro systematické zvyšování znalostí o kybernetické bezpečnosti. Aktualizace doplňuje do AR-in-a-Box nové konkrétní návody, aktivity a hry, jako třeba Cyber Awareness Game od Akademie Evropské unie určené k poskytovaní interaktivní formy vzdělávaní v oblasti kybernetické bezpečnosti a zlepšovaní připravenosti na krizové situace. Příručka je určená zejména organizacím a odborníkům, kteří můžou být urgentním kyberbezpečnostním situacím vystaveni a připravenost je pro ně klíčová.



Čeští vědci se podíleli na zdokonalení elektronických zařízení díky grafenu

Mezinárodní tým z Matematicko-fyzikální fakulty Univerzity Karlovy zkoumá nové vlastnosti a možnosti využití grafenu, speciální formy uhlíku, v elektronických zařízeních. Podstatou grafenu je 2D struktura molekuly uhlíku, která má zcela unikátní fyzikální vlastnosti. Výzkumný projekt financovaný z programu JUNIOR STAR Grantové agentury ČR se v současnosti zaměřuje na zkoumání možností, jak naskládat více vrstev grafenu na sebe. Způsob, jakým jsou na sobě atomární vrstvy poskládány, má totiž zásadní vliv na výsledné vlastnosti grafenu. Výzkumníci se předně soustředí na růst tří atomárních vrstev v ABC uspořádání, které se v přirozeném prostředí nevyskytuje a které by mohlo mít rozsáhlé využití v elektronice a optoelektronice. Tuto technologii by bylo do budoucna možné využít například k detekci infračerveného záření a zařízení v terahertzovém spektru jak např. v medicíně, tak v prostředí bezpečnosti či komunikace. Jedním z možných využití by mohlo být také nahrazení rentgenových paprsků využívaných v různých typech zařízení, které jsou pro člověka škodlivé.

Vědeli jste, ŽE...

...Národní koordinační centrum v červnu spustí své první výzvy? NÚKIB v roli Národního koordinačního centra výzkumu a vývoje v kybernetické bezpečnosti (NKC) plánuje v červnu spuštění prvních výzev pro finanční podporu třetím stranám. Podpora bude cílit na aktivity související s budováním kapacit, podporou spolupráce a networkingu a zvyšováním povědomí v oblasti kybernetické bezpečnosti. Podpora bude poskytnuta v rámci projektu NCC-CZ spolufinancovaného z programu Digitální Evropa, na kterém NÚKIB spolupracuje se CyberSecurity Hub. Bližší informace k parametrům výzvy naleznete na webových stránkách NKC a Úřadu v první polovině června 2024.

Umělá inteligence je již v současnosti schopná svádět a manipulovat své lidské uživatele

S rozvojem umělé inteligence je spojeno i riziko spojené s vytvářením schopnosti umělé inteligence klamat systémy nebo dokonce i lidi, kteří ji využívají. Za účelem včasného podchycení tohoto rizika a provedení kroků k přijetí relevantních regulativních opatření výzkumníci z Massachusettského technologického institutu shrnuli tato rizika v přehledovém článku. Dle vědců v současnosti není jasná přesná příčina, kvůli které se AI uchyluje k nežádoucímu chování v podobě klamání jejích uživatelů. Existují ale teorie, podle kterých se strategie klamu ukázala být jednoduše tou nejefektivnější cestou k dosažení dobrých výsledků v rámci zadaného úkolu. Příkladem může být systém Meta's CICERO navržený pro hru Diplomacy, což je strategická hra na dobývání světa s možnostmi budování aliancí. Mechanismy této hry byly dle jejích tvůrců navrženy tak, aby byl systém pestrý, ale zároveň čestný a užitečný hráčům. Jenže na základě analýzy dat přišli výzkumníci na to, že se z CICERA stal mistr klamu navzdory tomu, že měl vysloveně zakázáno poškozovat ostatní hráče. I když tento případ zní neškodně, pokud AI systémy dokážou podvádět ve hrách, ke stejnému chování mohou dospět i v jiných případech jejího nasazení. Riziko zneužití takové technologie v marketingových či volebních kampaních, nebo jakýchkoliv jiných typech aplikací, představuje značné společenské i bezpečnostní riziko. Vědci proto apelují, aby zákonodárci nepolevili v přijímání opatření jako např. nedávno přijatý Akt o umělé inteligenci, jenž klasifikuje systémy využívající AI do několika rizikových kategorií.

Informace z první ruky!

Výzkumníci z finské univerzity Jamk University of Applied Sciences a centra JYVSECTEC hledají partnery do výzev Klastru 3 v programu Horizont Evropa zaměřených na nástroje pro bezpečnost hardware a software, přechod k postkvantové kryptografii, boj proti nenávistným projevům a pokročilou analýzu dat. Pro bližší informace mohou zájemci využít kontaktních adres tuomo.sipola@jamk.fi a aimo.pellinen@jamk.fi.

Nově objevený materiál pro výrobu pamětí řeší problémové aspekty ukládaní dat spojené s přehříváním zařízení

Přehřívání smartphonu v horkém letním dni je i v současné době stále běžnou praxí. Nepříjemnosti spojené s vysokou teplotou zařízení ovšem nespočívají jen ve ztrátě výkonu či nepohodlné manipulaci, ale dochází také k riziku spojenému s možným poškozením uložených dat. Paměťové karty smartphonů se totiž vlivem vysokých teplot poškozují, a to až do takové míry, že může dojít k úplné ztrátě některých uložených dat. Vědecký tým z Pennsylvánské univerzity však vyvinul novou paměťovou technologii, která by měla být schopná udržet data i při teplotě 600°C. Materiál, který umožňuje vydržet takovou zátěž, se nazývá feroelektrický nitrid hliníku skandium. Paměťová zařízení vyrobená z tohoto materiálu jsou navíc energeticky nezávislá, což znamená, že jsou schopná uchovávat uložené informace bez potřeby aktivního napájecího zdroje, který je nutností v jakémkoli spotřebním zařízení s pevným nebo flash diskem. Tato využitelnost je dosažena díky vlastnosti materiálu zachovat svůj elektrický stav i po odstranění vnějšího elektrického pole a při výrazném zvýšení teploty. Technologie by otevřela zcela nové možnosti využití, např. také v extrémních podmínkách vesmíru, kde běžné technologie selhávají. Navíc její využití umožňuje navýšit výpočetní kapacitu zařízení, a tedy zlepšit jejich celkový výkon. V neposlední řadě umožňuje nový materiál pro výrobu pamětí odbourat nepříjemnosti spojené s užíváním běžných komerčních zařízení.

„Jako společnost potřebujeme co nejvíce času, abychom se připravili na pokročilejší podvody budoucích produktů umělé inteligence a modelů s otevřeným zdrojovým kódem."

Peter S. Park
expert na bezpečnost AI

Microsoft uvádí nový vyhledávací nástroj využívající umělou inteligenci se zabudovanou funkcí záznamu uživatelské aktivity

Společnost Microsoft představuje nový typ vyhledávacího nástroje nazvaný Microsoft Recall. Ten je nyní součástí zcela nové kategorie osobních počítačů Copilot+ řízených umělou inteligencí. Recall zaznamenává všechno, co uživatel na počítači dělá, pořizováním snímků obrazovky každých několik sekund. Tyto informace jsou následně zašifrovány a uloženy na pevný disk uživatele. Ten si je posléze může libovolně prohledávat pomocí vyhledávání, časové osy či procházení jednotlivých snímků zvlášť. Výchozí alokace datového uložiště pro zaznamenávací funkci Recallu bude 25 GB, což by dle vyjádření Microsoftu mělo stačit na ukládání snímků z posledních tři měsíců. Po naplnění kapacity bude systém automaticky mazat staré snímky, aby se uvolnilo místo novým. Jakmile uživatel najde relevantní obsah, o který se zajímá, může skrze Recall otevřít původní zdroj (dokument, soubor apod.), ze kterého byl snímek pořízen. Vyhledávaní bude zatím k dispozici v angličtině, francouzštině, němčině, španělštině, ale také v japonštině a čínštině. Představení nástroje vzbudilo kontroverzní ohlasy, zejména skrze pochopitelné obavy uživatelů o své soukromí. Microsoft ale deklaruje, že snímky obrazovky jsou propojeny pouze s daným uživatelským profilem a Recall je nesdílí s ostatními uživateli, ani je nezpřístupňuje správcům systému na straně Microsoftu, a to ani za účelem individualizace obsahu pro zpřesnění cílených reklam. V případě, že by uživatelé i tak měli obavy o svoje soukromí, budou si moct funkci vyhledávače dle svých preferencí buď omezit, nebo úplně vypnout.

Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Kontaktní informace

05/2024

Národní úřad pro kybernetickou a informační bezpečnost

Mučednická 1125/31

616 00 Brno

Tel.: +420 541 110 777

P.O. BOX 17, Brno 16, CZ 616 00

Oddělení vědy, výzkumu a inovací

Olšanská 36/9

130 00 Praha

Tel.: +420 607 032 806

e-mail: vyzkum@nukib.gov.cz