CYRIS Cyber Research and Inovations in Security

leden/2026

NEWSLETTER

AKTUALITY VE VÝZKUMU A VÝVOJI V KYBERNETICKÉ BEZPEČNOSTI

Národní úřad pro kybernetickou a informační bezpečnost
NÚKIB

Staňte se členy národního výzkumného a inovačního ekosystému!

Benefity z členství v CYRIS:

Buďte v kontaktu

Komunikujte napřímo s dalšími členy národního ekosystému v oblasti výzkumu a vývoje v kybernetické bezpečnosti, předávejte si klíčové informace a hledejte partnery pro Vaše projekty!

Přehled o aktuálním dění

Mějte přehled o tom, co se děje v oblasti výzkumu, vývoji a inovací v kybernetické bezpečnosti! Získejte tipy na zajímavé akce, publikace a zjistěte bližší informace o novinkách v oblasti podpory, aktuálních projektů a nových technologií.

Ovlivňujte budoucnost výzkumu

Získejte možnost udávat směr vývoje českému výzkumnému ekosystému v oblasti kybernetické bezpečnosti! Poskytujte vstupy a připomínkujte klíčové dokumenty na národní i evropské úrovni.

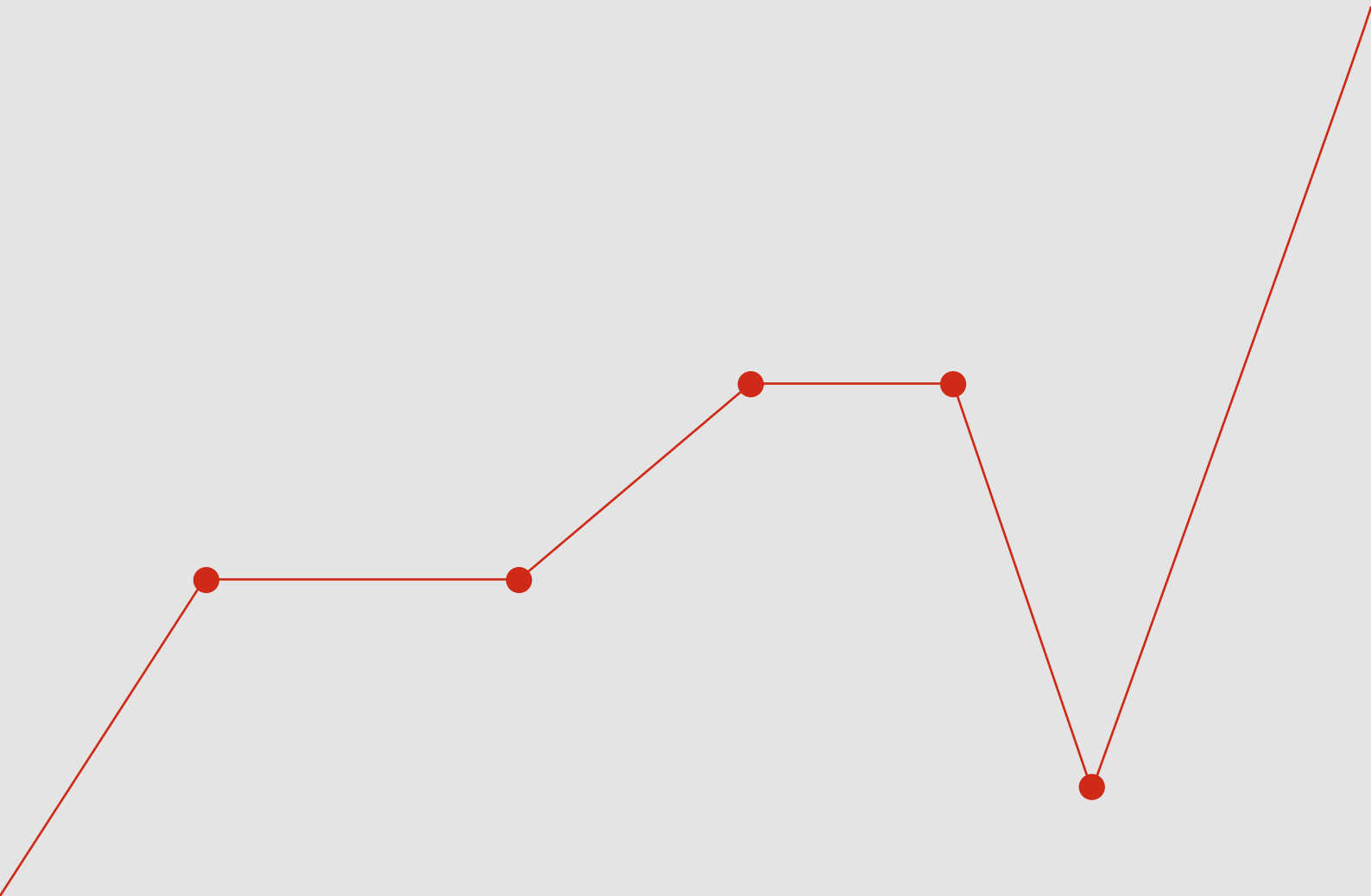
Aktuality, události a financování

4 Otevřený přístup k publikacím v programu Horizont Evropa

5 Evropské investice do výzkumu rostou, ale české výdaje klesají

6 Vyhlášení 4. Výzvy k podávání projektů „Cyber Resilience Boost: Podpora budování kapacit pro kybernetickou odolnost produktů II.

Online matchmaking a infoden k výzvě DEPLOYO9



Otevřený přístup k publikacím v programu Horizont Evropa

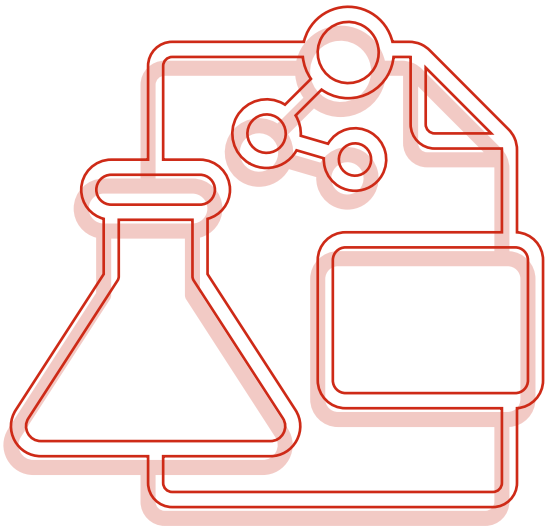
Otevřený přístup k vědeckým publikacím je **povinnou součástí projektů financovaných z programu Horizont Evropa** a představuje významnou změnu v tom, jak jsou výsledky výzkumu sdíleny a využívány napříč Evropou.

Cílem Evropské komise je zajistit, aby recenzované vědecké články vzniklé z veřejných prostředků byly **okamžitě a bezplatně dostupné odborné komunitě i veřejnosti**. To podporuje rychlejší šíření znalostí, vyšší transparentnost a lepší návaznost dalšího výzkumu.

Pro příjemce grantů to však znamená nutnost pečlivě plánovat publikační strategii, orientovat se v licenčních podmínkách a správně pracovat s autorskými právy. Důležitou roli hraje také správné plánování nákladů na publikování, které může být zahrnuto do rozpočtu projektu.

Přehled pravidel otevřeného přístupu proto pomáhá výzkumným organizacím snížit administrativní rizika, zvýšit viditelnost výsledků a sladit publikační strategii s požadavky evropského financování.

vedavyzkum.cz



Evropské investice do výzkumu rostou, ale české výdaje klesají

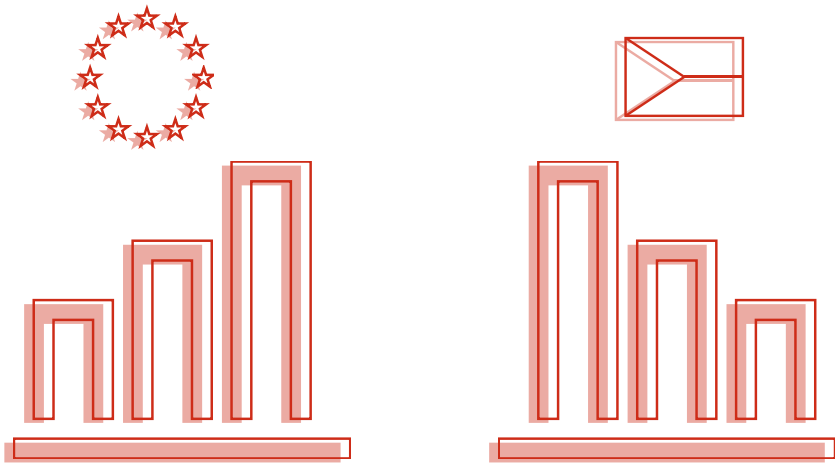
Výdaje na výzkum a vývoj v Evropské unii dlouhodobě rostou a potvrzují snahu posilovat inovace a konkurenceschopnost evropské ekonomiky, což je považováno za klíčový nástroj konkurenceschopnosti, technologické suverenity a ekonomického růstu.

Nejnovější data však ukazují, že tento pozitivní trend se neprojevuje ve všech členských státech stejně. Zatímco řada zemí zvyšuje veřejné i soukromé výdaje na výzkum, **v České republice dochází k jejich poklesu, zejména ve veřejném sektoru**.

Tento vývoj může mít dopad na schopnost země udržet krok s rychle se rozvíjejícími technologiemi a zapojovat se do mezinárodních výzkumných iniciativ.

Nižší investice se mohou projevit také v omezené účasti v evropských programech a menší atraktivitě pro špičkové výzkumníky. Jedná se o důležitou debatu o strategickém směřování národního financování a o potřebě stabilního a dlouhodobého plánování, která bude vyžadovat aktivní spolupráci ze strany celé národní výzkumné komunity.

vedavyzkum.cz



Investice *Výdaje*

Vyhlášení 4. Výzvy k podávání projektů „Cyber Resilience Boost: Podpora budování kapacit pro kybernetickou odolnost produktů II.“

NÚKIB v roli NKC vyhlásil 4. Výzvu k podávání projektů „Cyber Resilience Boost: Podpora budování kapacit pro kybernetickou odolnost produktů II.“. Příjem žádostí o podporu projektu byl zahájen dne **2. února 2026 a bude ukončen 2. dubna 2026 v 19:00 hodin**.

Výzva alokuje prostředky na **podporu budování kapacit** subjektů působících v oblasti kybernetické bezpečnosti v souvislosti s implementací Nařízení Evropského parlamentu a Rady (EU) 2024/2847 ze dne 23. října 2024 o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky (akt o kybernetické odolnosti, Cyber Resilience Act – CRA).

Podporovány budou aktivity zaměřené na **vývoj podpůrných nástrojů a dokumentace pro sebehodnocení dle požadavků CRA, realizaci vzdělávacích aktivit primárně pro malé a střední podniky a posilování spolupráce, standardizace a sdílení osvědčených postupů** napříč odbornou komunitou a relevantními aktéry. Více informací je zveřejněno na webu NÚKIB v sekci Aktuální výzvy.

Online matchmaking a infoden k výzvě DEPLOYO9

NKC České republiky, Slovenska, Portugalska a Španělska pořádají **online matchmaking a infoden k aktuálně otevřeným tématům výzvy DEPLOY09 v rámci programu Digitální Evropa**.

Akce se uskuteční online dne 12. února 2026 od 14:30 a nabídne prostor pro pitch prezentace, představení projektových záměrů i navazování nových partnerství.

Účastníci se seznámí s otevřenými výzvami v oblasti kybernetické bezpečnosti a budou mít možnost prezentovat své organizace či projektové nápady v tematických pitching sekcích. Akce je určena zejména zástupcům firem, výzkumných a akademických institucí, zájemcům o zapojení do konsorcií a dalším relevantním stakeholderům. Registraci na akci je možné provést zde, bližší informace naleznete na webu události.

NCC-CZ
CZECHIA CYBERSECURITY COORDINATION CENTRE

Spolufinancováno Evropskou unií

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Podpořeno z programu Digitální Evropa v rámci projektu National Coordination Centre 2.0 – The Czech Republic (zkr. NCC-CZ 2.0, č. 101227749). Názory a stanoviska uvedené vyjadřují pouze názory autora(ů) a nemusí nutně odrážet názory Evropské unie ani Evropského centra kompetencí pro kybernetickou bezpečnost. Evropská unie ani poskytovatel dotace nenesou za tyto názory odpovědnost.

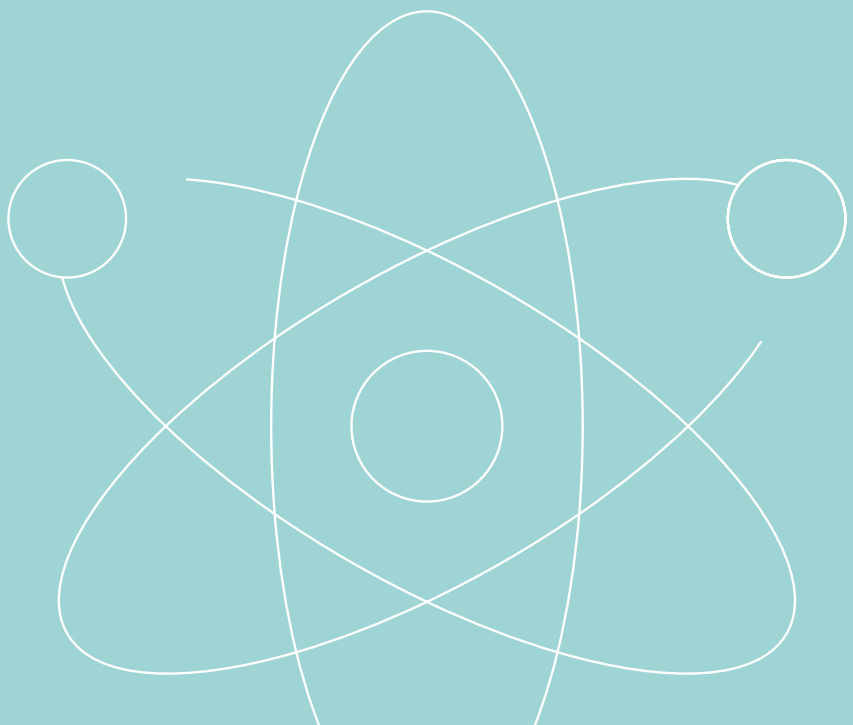
Technologické novinky, objevy a zprávy

8 Space-based QKD:Komerční budoucnost kvantové bezpečnosti

9 Nový systém distribuce klíčů pro ochranu biometrických dat v postkvantové éře

10 NIST posouvá bezpečný hardware nové generace do standardů

11 BPFDoor výzva ke spolupráci v oblasti detekce v české infrastruktuře



Space-based QKD: Komerční budoucnost kvantové bezpečnosti

Satelitní kvantová komunikace se velmi rychle stává strategickým pilířem kybernetické bezpečnosti.

Podle analýzy Space Insider dosahuje trh kosmické QKD v roce 2025 hodnoty přibližně 500 milionů USD a do roku 2030 má vzrůst na 1,1, miliardy USD.

Tento růst táhnou zejména **Čína**, která již provozuje vlastní QKD satelity, evropské iniciativy **Euro QCI** a **EAGLE-1** a severoamerické firmy jako **Honeywell** nebo **Boeing**. Technologie slibuje extrémně bezpečný přenos dat odolný vůči kvantovým útokům, ale její masové nasazení zatím brzdí vysoké náklady, citlivost na atmosférické podmínky a nízká úroveň technologické připravenosti.

Odborníci odhadují, že komerční využití ve velkém měřítku přijde až po roce 2035, přesto už dnes probíhají pilotní projekty a testy na orbitálních platformách. Space-based QKD tak představuje nejen technologický trend, ale i geopolitickou výzvu, protože státy i firmy, které investují nyní, budou mít náskok v éře kvantových hrozeb.

spaceinsider.tech

Nový systém distribuce klíčů pro ochranu biometrických dat v postkvantové éře

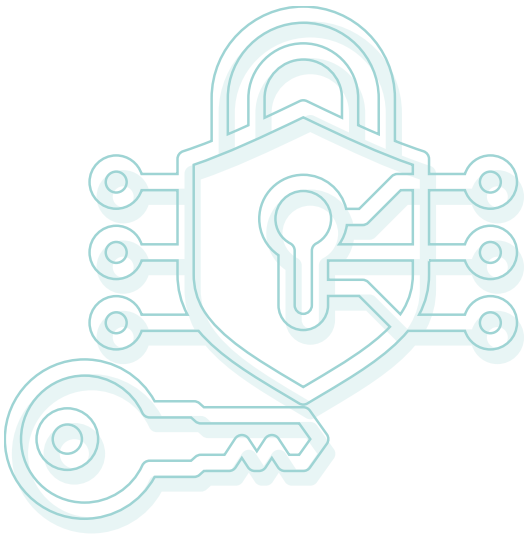
Výzkumníci představili **nový systém distribuce kryptografických klíčů, který posiluje ochranu biometrických dat vůči hrozbám budoucích kvantových klíčů**.

Řešení reaguje na rostoucí riziko, kdy současné šifrovací metody nebudou dlouhodobě schopny zajistit bezpečnost citlivých údajů, jako jsou otisky prstů, rozpoznávání obličeje či další biometrické charakteristiky.

Klíčovým prvkem návrhu je využití post kvantové kryptografie, která je odolná vůči kvantovým útokům, a bezpečné správy klíčů během jejich přenosu i ukládání. Systém je navržen s ohledem na praktické nasazení v reálných informačních systémech, například v digitálních identitách, přístupových kontrolách nebo ověřování uživatelů ve veřejném a soukromém sektoru.

Navrhovaný přístup představuje důležitý krok k dlouhodobé ochraně biometrických dat a ke zvýšení důvěry v jejich bezpečné využívání v kritických aplikacích, kde by případné selhání ochrany mohlo mít závažné technologické i společenské dopady do budoucna.

biometricupdate.com



NIST posouvá bezpečný hardware nové generace do standardů

Americký národní institut pro standardy a technologie (NIST) prostřednictvím iniciativy **Standards for Unified Secure Hardware Interfaces (SUSHI) posouvá bezpečný hardware nové generace blíže k mezinárodním standardům a praktickému nasazení**.

> Cílem projektu je usnadnit integraci hardwarových bezpečnostních prvků, které zvyšují odolnost systémů vůči sofistikovaných kybernetickým útokům, včetně hrozeb spojených s dodavatelským řetězcem.

SUSHI se zaměřuje na standardizaci komponent, jako jsou bezpečné procesory, moduly pro ochranu paměti nebo mechanismy důvěryhodného spuštění. Důležitým přínosem je snaha propojit výzkum, průmysl a standardizační procesy, aby nové technologie nebyly pouze laboratorním řešením, ale součástí běžných IT a OT systémů.

Zavádění bezpečného hardwaru na úrovni standardů může výrazně snížit náklady na implementaci a zvýšit interoperabilitu napříč platformami. Pro organizace to znamená lepší připravenost na budoucí regulační požadavky a vyšší úroveň ochrany kritických systémů, kde software samotný již nestačí. Projekt zároveň reaguje na rostoucí tlak na hardwarovou důvěru v oblasti cloudu, edge zařízen a kritické infrastruktury napříč veřejným a soukromým sektorem.

nist.gov

BPFDoor výzva ke spolupráci v oblasti detekce v české infrastruktuře

Bezpečnostní komunita v České republice čelí v posledních letech **rizikům spojených s výskytem malware BPFDoor**, jakožto vysoce sofistikovaného backdooru určeného pro linuxové servery. Na tento problém upozorňuje jeden z členů komunity CYRIS **bezpečnostní výzkumník Jindřich Karásek**, který působí jako Lead Security Researcher ve společnosti Rapid7 a zároveň na Akademii věd ČR.

V rámci průběžného výzkumu jeho tým identifikoval několik kompromitovaných serverů v české infrastruktuře a existující indicie, že skutečný rozsah zasažení může být výrazně širší.

BDFDoor je dlouhodobě **spojován s čínskými APT skupinami a určen především pro kyberšpionáž**. Jeho nebezpečnost spočívá ve zneužití *Berkeley Packet Filter, díky němuž malware pasivně „naslouchá“ síťovému provozu a zůstává zcela neaktivní, dokud nezachytí speciální síťový **magic packet. Novější varianty navíc lépe maskují svou přítomnost, vydávají se za běžné systémové služby, falšují časová razítka souborů a umožňují laterální šíření v napadené síti.

S cílem lépe porozumět této hrozbě a podchytit její skutečný rozsah byla zahájena nekomerční výzkumná iniciativa zaměřena na sběr vzorků BDFDoor, analýzu aktivačních mechanismů a tvorbu detekčních pravidel pro síťovou ochranu (zejména IDS/IPS, firewally a Suricata. Projekt probíhá ve spolupráci s institucemi jako TF-SCIRT a Europol.

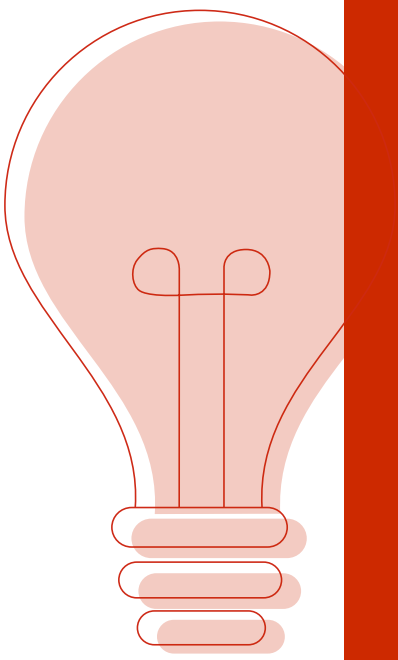
Výzkumný **tým zároveň vyzývá organizace ze státní správy, akademické a výzkumné sféry, neziskového sektoru a oblasti kritické infrastruktury ke spolupráci**. Zapojení partnerů, kteří mohou detekční pravidla nasadit a sdílet anonymizované informace o nálezech, je klíčové pro zvýšení odolnosti celé české infrastruktury. Zájemci o spolupráci nebo další informace se mohou obrátit na pana Karáska prostřednictvím e-mailové adresy **karasek@psu.cas.cz**.

Příspěvek od člena komunity Jindřicha Karáska

*Technologie pro nízkoúrovňové filtrování a zpracovávání síťových paketů bez velké zátěže na výkon.

**Speciální síťový paket, který slouží jako spouštěč pro malware.

Tip na akci



Masters of Digital 2026

Konference Masters of Digital 2026 se uskuteční 25. února 2026 v Bruselu v hotelu Steinberger Wiltcher's s možností online účasti pro všechny zájemce. Akce propojí špičky digitálního průmyslu, politiky a inovátorů a nabídne diskuse o klíčových tématech, která oblivní směřování Evropy v nadcházejících letech. Letošní ročník se zaměří na strategii umělé inteligence pro posílení průmyslové konkurence-schopnosti, na zajištění kybernetické bezpečnosti v globálně rozděleném prostředí a na zjednodušení regulací, které podpoří hospodářský růst a inovace.

Registrace je otevřená, kapacita pro osobní účast je však omezena, proto doporučujeme se přihlásit co nejdříve. Více informací o konferenci a registraci naleznete na stránkách akce Masters of Digital 2026.

mastersofdigital.org

Věděli jste, že

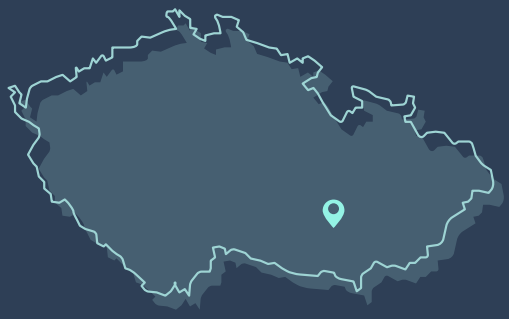
nedávný výzkum mezi českými vysokoškoláky ukazuje, že umělá inteligence se rychle stala běžnou součástí studia, avšak orientace v pravidlech jejího používání zůstává nízká. Téměř polovina studentů neví, zda jejich univerzita disponuje oficiálními směrnicemi k AI, a jen menšina zná jejich konkrétní obsah. Zároveň se ale jasně projevuje zájem o srozumitelná, jednotná a férová pravidla, která by podpořila akademickou integritu a zároveň umožnila smysluplné využití technologií. Studenti AI využívají především pragmaticky nejčastěji nástroje jako Google Translate, DeepL, ChatGPT nebo Grammarly, a to zejména k překladům a jazykové korektuře a většina z nich nepočítá s placenými nástroji. Pro výzkumné vzdělávací instituce je to důležitý signál, protože AI už není okrajovým tématem, ale systémovou otázkou řízení kvality, etiky a financování vzdělávání i výzkumu. Bez jasných pravidel se potenciál AI mění z příležitostí v riziko.

vedavyzkum.cz

Kontaktní informace

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

Národní úřad pro kybernetickou a informační bezpečnost
NÚKIB

Celkově studující využívali umělou inteligenci spíše ke zvýšení efektivity práce a opravě chyb než k hlubšímu výzkumu

shrnuje způsob využívaní AI výzkumnice z Fakulty sociálních věd Univerzity Karlovy, Kateřina Turková.