

NÚKIB



Národní úřad
pro kybernetickou
a informační
bezpečnost

Aktuality ve výzkumu a vývoji v kybernetické bezpečnosti

04/2023

DUBEN

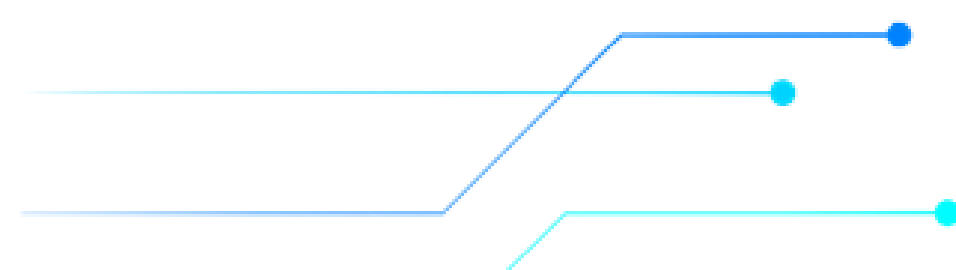
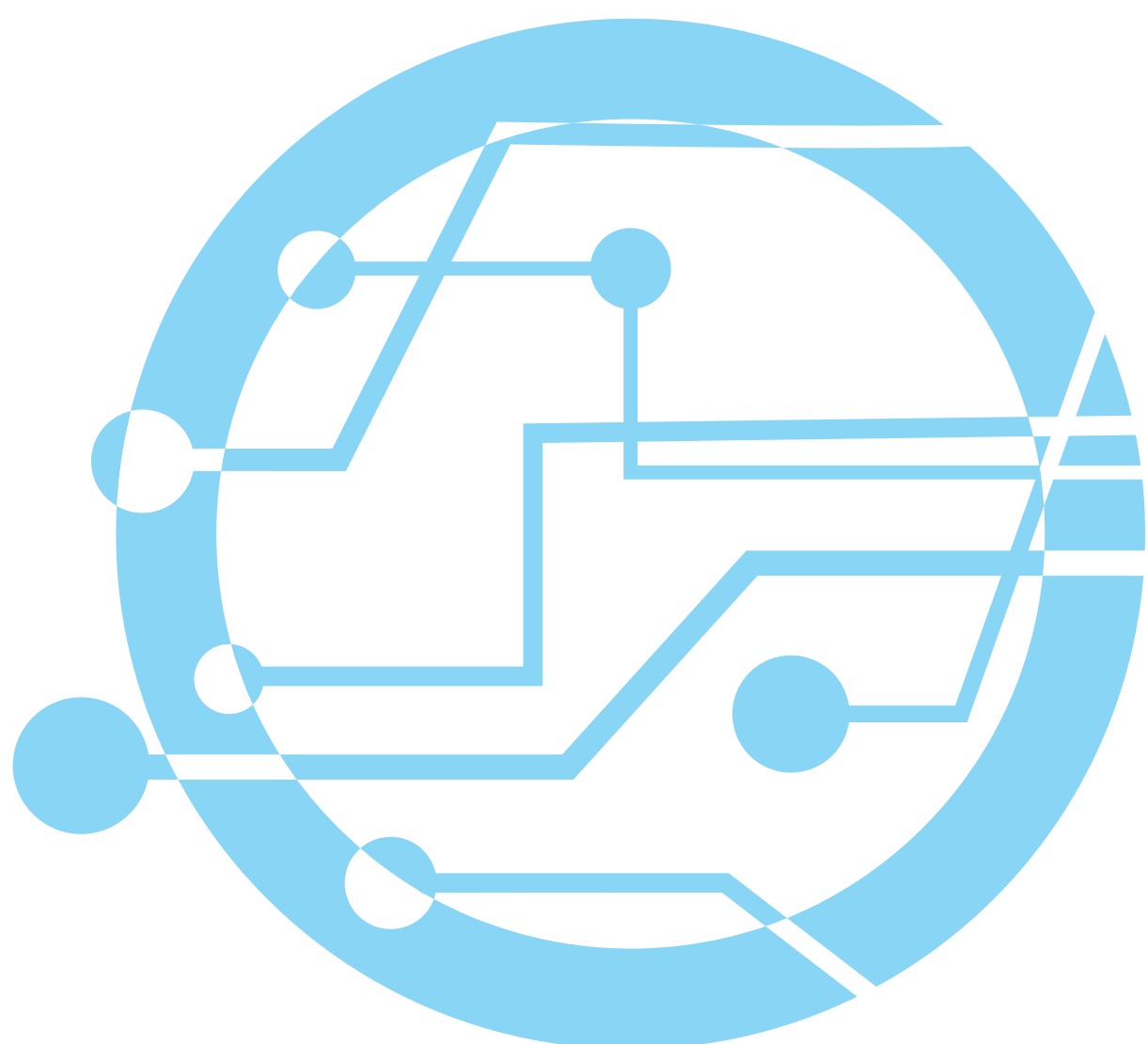
Rozvoj kvantových technologií v Evropě podpoří dva nové projekty s českou účastí

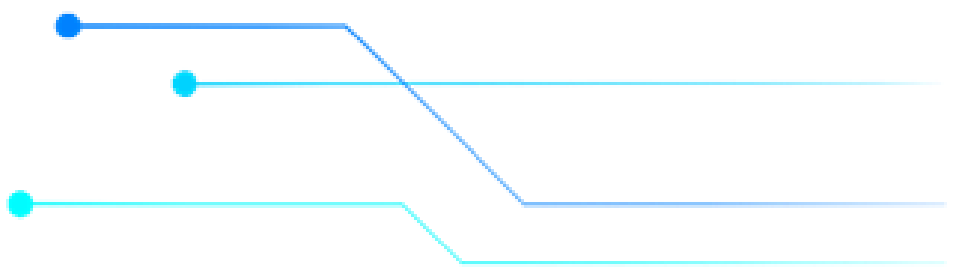
Výzkumná iniciativa Evropské unie Quantum Flagship financovaná programem Horizon Europe umožní realizaci dvou českých projektů z oblasti kvantových technologií: Qu-Test a Qu-Pilot. Evropská iniciativa skrze celkový rozpočet ve výši jedné miliardy eur cílí na rozvoj konkurenceschopného evropského průmyslu kvantových technologií v horizontu nadcházejících deseti let. Finanční prostředky by měly přispět k propojení aktivit výzkumných institucí, akademické obce a také průmyslu v této rychle rostoucí technologické oblasti. Realizaci projektu ohlásila česká poradenská společnost pro výzkum, vývoj a inovační projekty AMIRES, která se podílela na přípravě projektových žádostí a je plnohodnotným partnerem obou projektů.



Evropská komise aktualizovala pracovní programy Horizon Europe

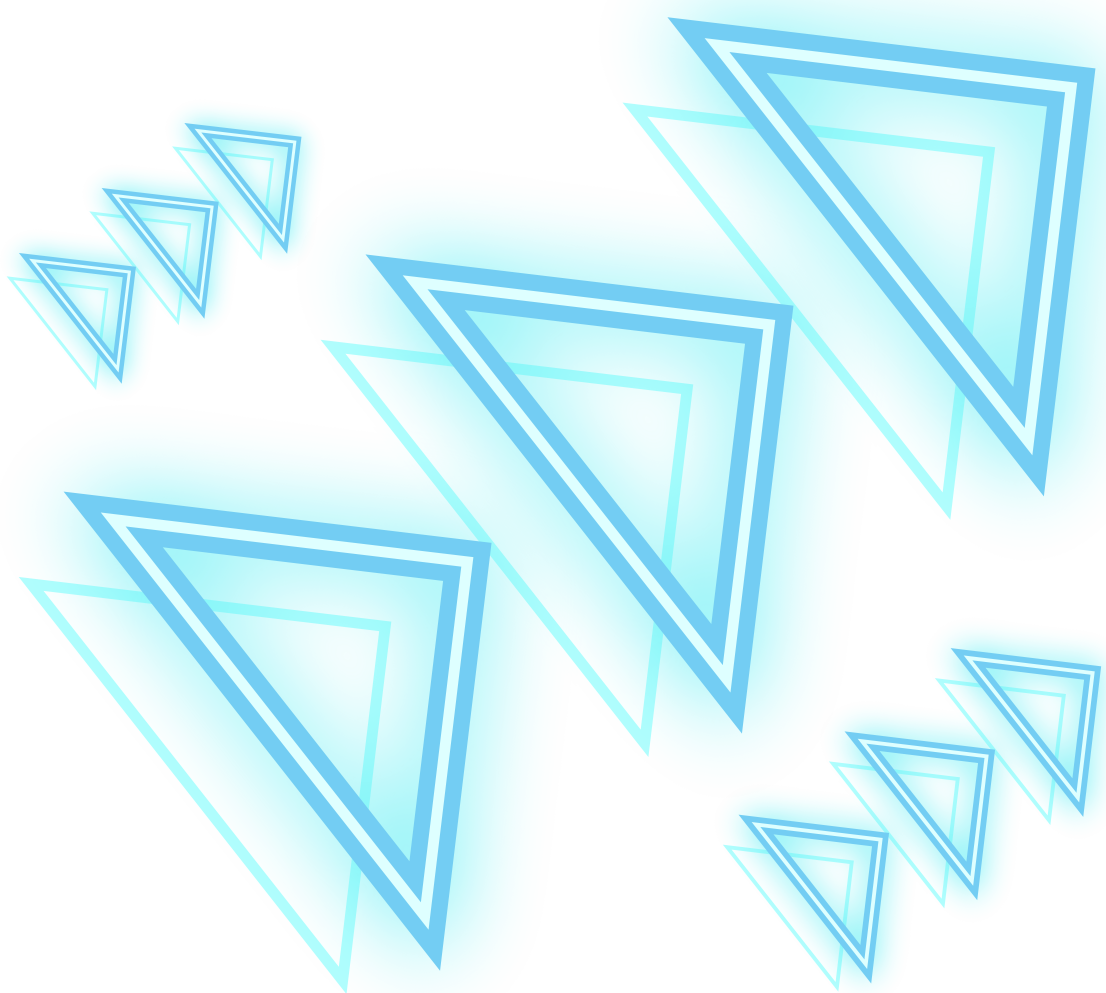
Aktualizace pracovních programů finančního programu Horizon Europe se týká období let 2023–2024. Příležitost pro zajištění financování mají také výzkumné, vývojové a inovační projekty zaměřené na kybernetickou bezpečnost. Na oblast kybernetické bezpečnosti se zaměřuje zejména Klastř 3, Civil Security for Society, kde je k dispozici oblast Increased Cybersecurity, a také Klastř 4, Digital Industry and Space. Kompletní seznam pracovních programů s detailním popisem jejich zaměření je k dispozici ke stažení na stránkách [Evropské komise](#). Ve dnech 27. a 28. června zároveň Evropská komise pořádá pro Klastř 3 [informační dny](#).





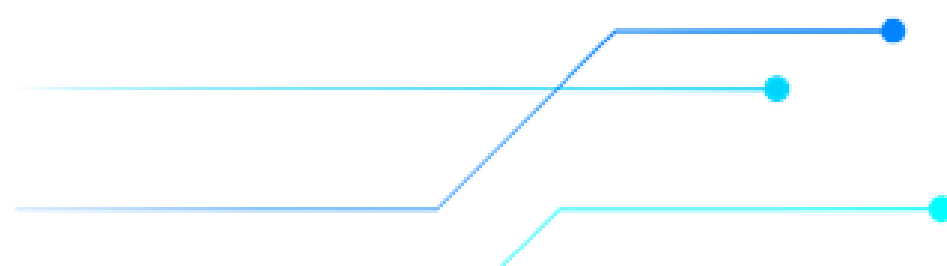
ENISA připravuje konferenci na téma umělé inteligence

Evropská agentura pro kybernetickou bezpečnost (ENISA) uspořádá 7. června konferenci zaměřenou na bezpečnostní aspekty umělé inteligence (UI). Hlavními tématy konference budou kromě klíčových aspektů kybernetické bezpečnosti v systémech UI také diskuze ohledně výzev spojených s implementací a dohledem nad bezpečnou a důvěryhodnou UI. Akce by měla přispět ke sdílení předchozích zkušeností a sjednocení přístupu odborné komunity. Neméně důležitým rozměrem je také potřeba zvyšování povědomí o nutnosti prohlubování odborné spolupráce v zájmu zajištění bezpečné UI. Konference se uskuteční v hybridním formátu, přičemž [online registrace](#) je stále otevřená.



NÚKIB uskutečnil svou první fyzickou misi PROPED směřovanou do Německa

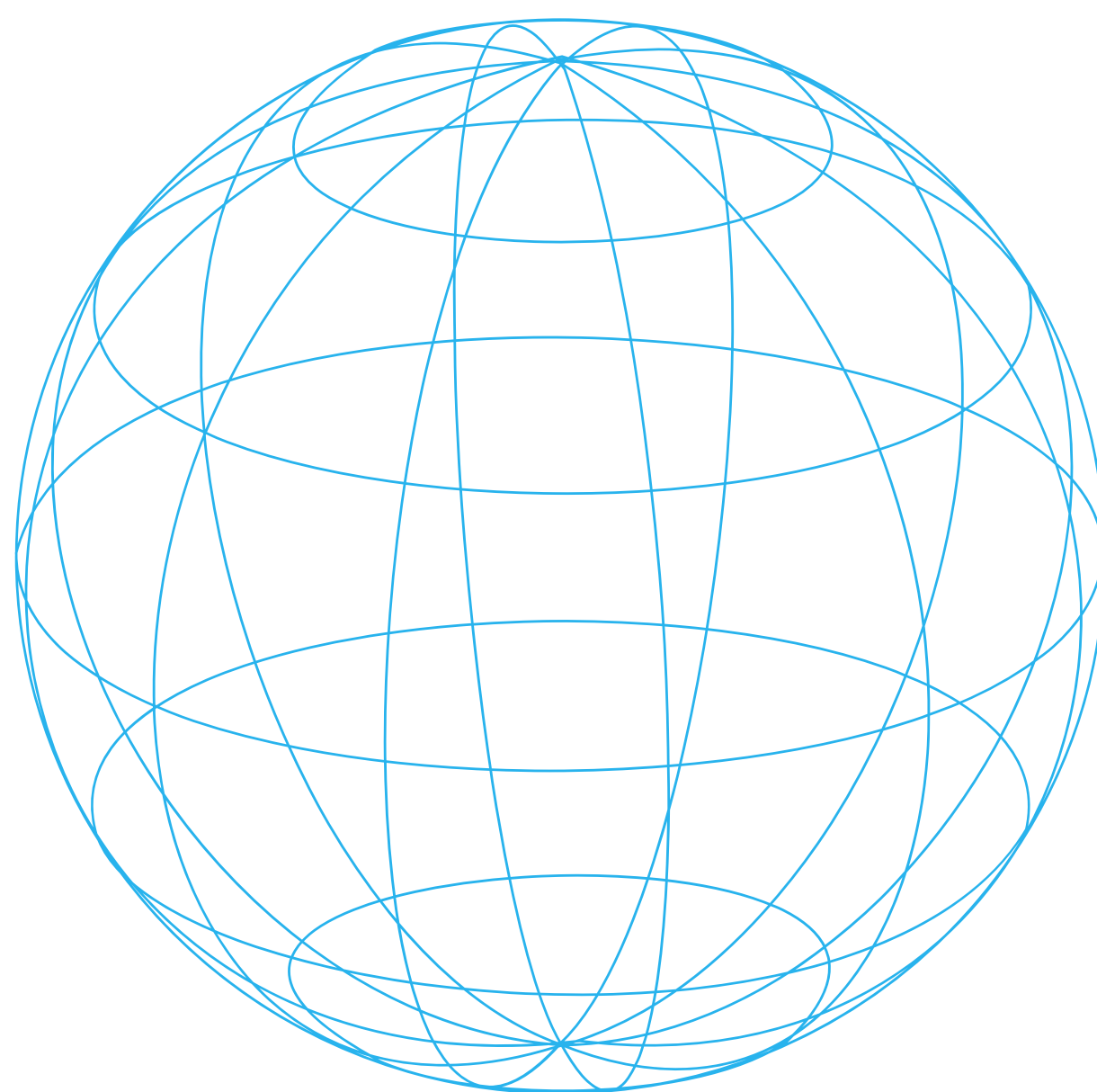
Ve dnech 18.-20. dubna se v německých městech Bonn a Jena sešli odborníci z České republiky a Německa zaměřující se na oblast bezpečnosti komunikačních sítí. Česká delegace složená ze zástupců NÚKIB a univerzit Vysokého učení technického, a Českého vysokého učení technického, navštívila odborná pracoviště Státního úřadu pro bezpečnost informační techniky (BSI) v Bonnu a firmu Quantum Optics v Jeně. Cílem mise bylo prohloubit stávající spolupráci mezi českou a německou výzkumnou komunitou a přispět k nalezení nových možností vzájemné participace v oblasti výzkumu bezpečnosti a zranitelnosti optických komunikačních sítí a systémů.



Technologie 3D hologramu zaznamenala výrazný posun

Nový způsob vytváření dynamických 3D holografických projekcí umožňuje díky jejich ultravysoké hustotě mnohem lepší rozpoznatelnost a rozlišení. Skupina čínských vědců, jež nazývá svůj přelomový přístup trojrozměrná dynamická holografie s asistencí rozptylu (three-dimensional scattering-assisted dynamic holography – 3D-SDH), ukazuje schopnost dosáhnout více než trojnásobně vyššího hloubkového rozlišení, než byly schopny předchozí moderní metody víceplošné holografické projekce. Díky tomu, že tento typ hologramu zobrazuje svoje výstupy ve vysokém rozlišení pixelů a na velkém množství po sobě jdoucích vrstev, jež jsou vedle sebe uloženy velmi těsně, vtěsná do ob-

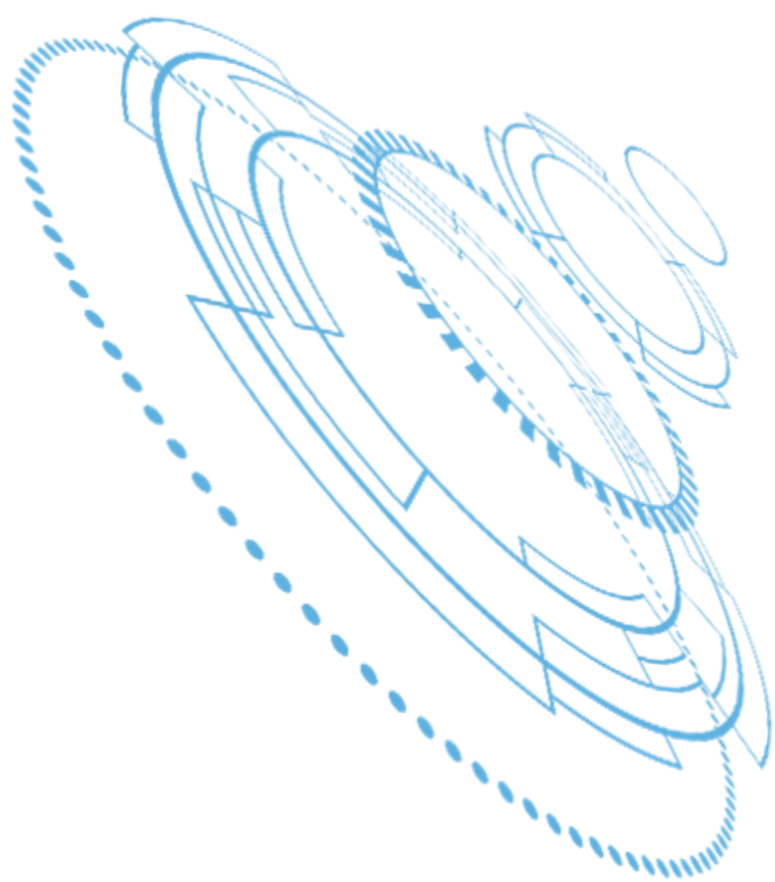
razu mnohem více detailů, což je dále důležité pro zobrazení hloubky, díky které hologram vypadá trojrozměrně. Technologie překonává dva dlouhodobě nejproblematictější aspekty současných digitálních holografických technik, kterými jsou nízké axiální rozlišení a vysoké přeslechy mezi rovinami bránící kontrole hloubky hologramu, a tím omezující kvalitu 3D zobrazení. Takový typ hologramu je možno využít například pro realistické vykreslování světa ve virtuální realitě nebo také pro zlepšení optického šifrování založeného na holografii skrze zašifrování většího množství dat do hologramu.



Výzkumníci pracují na vývoji operačního systému schopného plně eliminovat ransomwarové útoky

Konsorcium amerických univerzit tvořené primárně Massachusetts Institute of Technology a Stanford University pracuje na vývoji operačního systému, který by měl být schopen eliminovat hrozbu v podobě ransomware, schopnou zablokovat systém nebo zašifrovat data v něm uložená. Systém s názvem DBOS (Database-oriented Operating System) je strukturován kolem databází, které sledují a zaznamenávají všechny změny, ke kterým v operačním systému dochází. Tím se DBOS výrazně liší od běžných operačních systémů, jako je např. Linux, který je strukturován kolem souborů. Zjednodušeně řečeno, Linux vnímá každou složku v počítači jako soubor. DBOS místo toho pracuje s myšlenkou, kdy každou složku považuje za tabulku, která je ve své aktuální podobě uchovávána v databázi.

V případě, že dojde k napadení DBOS ransomwarem, struktura tohoto operačního systému mu umožní jednoduchý návrat k předchozí zaznamenané verzi uložené v databázi, a tím se vrátit do stavu před útokem, kdy byl počítač zabezpečený. Narozdíl od běžného souborového systému uživatelé nemusí provádět neustálé zálohy dat v počítači a navíc soubory samotné nejsou ohroženy infikováním škodlivým malwarem. Nově vyvíjený operační systém taktéž výrazně urychlí proces obnovy dat, který bude možno provést během několika minut. Finální verze DBOS ještě není kompletní, jeho tvůrci ho ovšem plánují sdílet ve formě open-source.



„Pokud budou technologie UI používány s odpovědností a v souladu s etickými zásadami, mohou výrazně přispět ke zlepšení kvality vzdělávání i výzkumu.“

**prorektor Univerzity Karlovy
Tomáš Skopal**

Chytré brýle umí číst tichou řeč

Výzkumníci z Cornell University vyvinuli elektronické brýle schopné rozpoznávat řeč bez vydávání zvuku za použití umělé inteligence. Vyvinuté digitální rozhraní kombinuje umělou inteligenci s akustickým snímáním napětí k nepřetržitému rozpoznávání až 31 nevokalizovaných slov na základě pohybů rtů a úst. Nízkoenergetické brýle nazvané EchoSpeech dokážou plnohodnotně fungovat už po několika minutách zpracování tréninkových dat, po kterých algoritmus hloubkového učení analyzuje další vstupy v reálném čase s přesností až 95 %. Následně jsou schopny automaticky rozpoznávat nevokalizovaná slova nebo slovní příkazy, které se uživateli přenášejí do aplikace spuštěné na chytrém telefonu, kde se ukládají ve formě textu, nebo je možné je přehrát do zvukové podoby. Tato technologie by se tak mohla stát obdobou v současnosti využívaného hlasového syntezátoru, který je určený lidem bez schopnosti rozeznít jejich hlasivky. Zásazením mikrofonu a reproduktoru do brýlí je z nich možné učinit jakýsi sonar, který vysílá a přijímá zvukové vlny snímáním obličeje a pohybů úst. EchoSpeech by tedy mohl sloužit také ke komunikaci na místech, kde je klasická řeč nepříjemná nebo nevhodná, například v hlučné restauraci nebo tiché knihovně.

Věděli jste, ŽE...

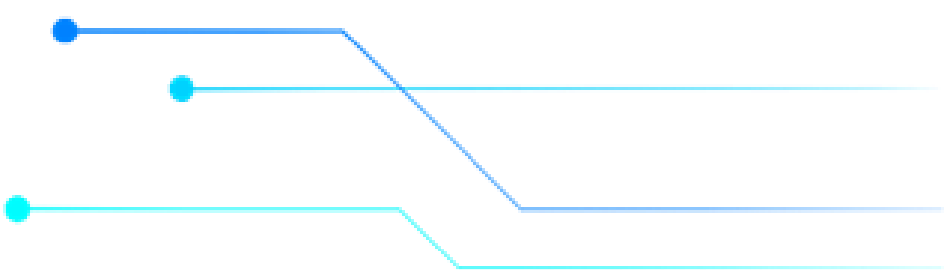
Český vzdělávací systém se aktivně připravuje na přítomnost a využití umělé inteligence ve výuce. Univerzita Karlova a organizace prg.ai jsou zakladateli skupiny určené k diskutování změn ve vzdělávání nevyhnutných pro řešení výzev souvisejících s UI jako např. ChatGPT. Mezi členy této neformální skupiny se řadí kromě zakladatelů také Masarykova univerzita, České vysoké učení technické, Západočeská univerzita v Plzni, Univerzita Jana Evangelisty Purkyně v Ústí nad Labem, Národní pedagogický institut a Smíchovská průmyslová střední škola.

K vyhodnocování vyspělosti kybernetické bezpečnosti podniků přispěje nový nástroj

Nástroj pro hodnocení vyspělosti kybernetické bezpečnosti ve formě online aplikace, vyvinutý Evropskou agenturou pro kybernetickou bezpečnost (ENISA), je určen primárně malým a středním podnikům (SMEs) snažícím se o zhodnocení své úrovně vyspělosti kybernetické bezpečnosti. Díky tomuto nástroji budou podniky moci definovat konkrétní rizika, kterým čelí, a obdržet individuální akční plán zaměřený na jejich eliminaci prostřednictvím konkrétních opatření. Hodnocení kybernetické bezpečnosti proběhne prostřednictvím evaluace několika otázek týkajících se zaměření podniku, jeho velikosti, dostupného rozpočtu apod. Aspekty kybernetické bezpečnosti, které jsou klíčové pro určení úrovně vyspělosti daného podniku, jsou rozděleny do tří oblastí. První oblast tvoří personál, přičemž v rámci ní dochází k posouzení, zda a případně do jaké míry jsou zaměstnanci daného podniku připraveni čelit kybernetickým hrozbám. Druhou oblastí jsou technologie neboli schopnost porozumět používaným technologiím a schopnost výběru adekvátních postupů pro zajištění kybernetické bezpečnosti.

Poslední posuzovanou oblastí jsou samotné procesy, které podnik zavádí pro management bezpečnostních rizik a zajištění kybernetické bezpečnosti. Nástroj by měl také přispět k implementaci nové směrnice o kybernetické bezpečnosti NIS2, a to konkrétně posílením kybernetické odolnosti SMEs.





Národní úřad pro kybernetickou a informační bezpečnost

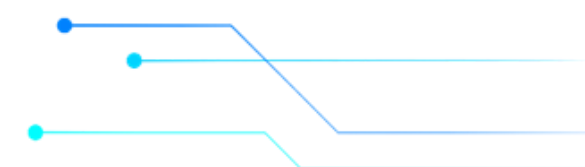
Mučednická 1125/31

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.cz

