NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

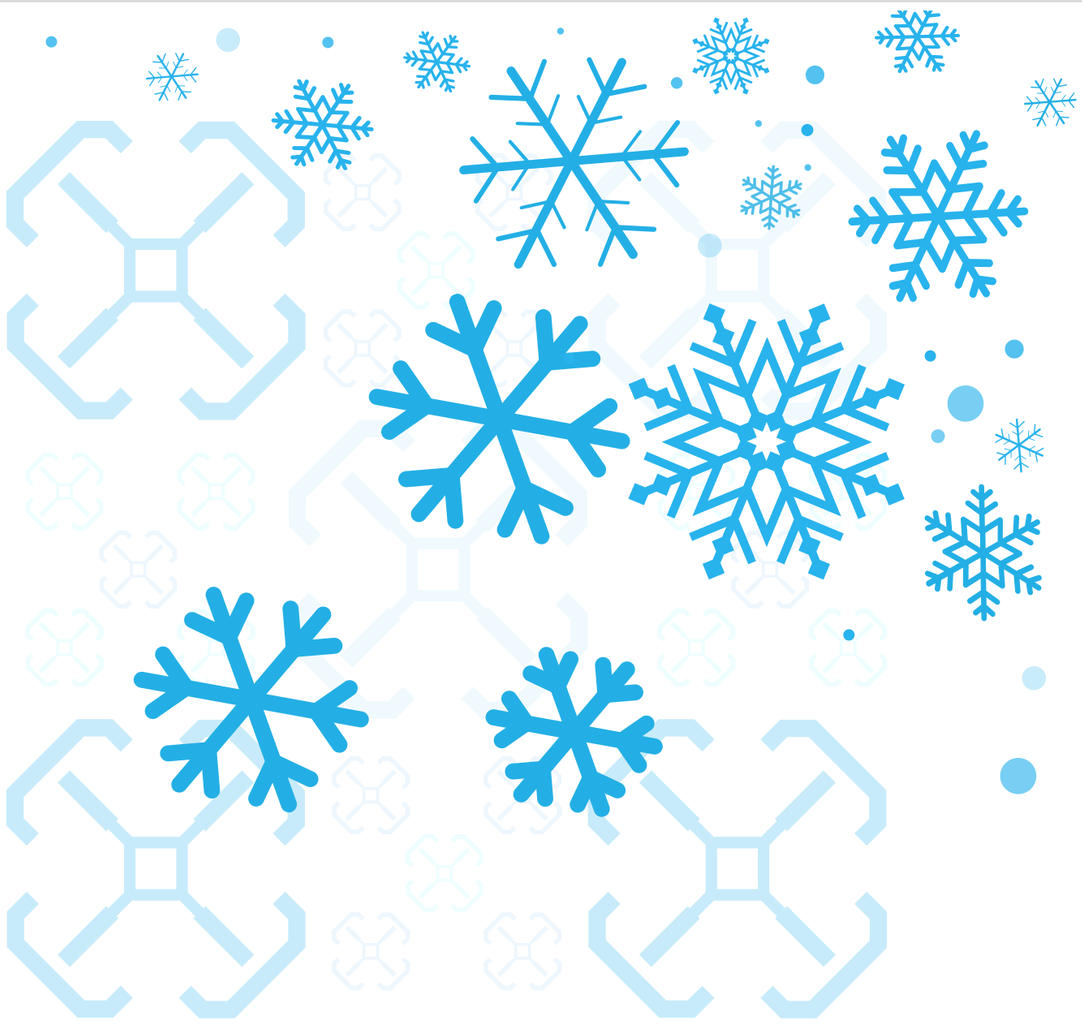
Aktuality ve výzkumu a vývoji v kybernetické bezpečnosti

11/2023

LISTOPAD

Listopad plný novinek pro národní komunitu v oblasti výzkumu a vývoje v kybernetické bezpečnosti

Dne 15. listopadu 2023 se v brněnském CyberCampusCZ již po sedmé sešli členové Platformy pro výzkum a vývoj v oblasti kybernetické a informační bezpečnosti. Kromě prezentací o aktuálním dění a trendech na poli výzkumu a vývoje měli účastníci možnost poslechnout si panelové diskuze na téma role státu v oblasti podpory výzkumu a vývoje, přechodu ke kvantově odolné kryptografii či vzdělávání a cvičení na poli kybernetické bezpečnosti. NÚKIB zároveň oficiálně odstartoval projekt českého Národního koordinačního centra výzkumu a vývoje v oblasti kybernetické bezpečnosti (NKC). Projekt zaměřený na vybudování hlavního kontaktního bodu pro komunikaci s EU a koordinaci spolupráce na národní úrovni při příležitosti svého startu rovněž spustil webové stránky, prostřednictvím kterých bude národní komunitu informovat o aktuálním dění na poli EU, finančních příležitostech či možnostech spolupráce se zahraničními partnery.



Program SECTECH vyhlásil výsledky druhé veřejné soutěže

Ministerstvo vnitra, pod které spadá Program bezpečnostního výzkumu ČR 2021–2026: vývoj, testování a evaluace nových bezpečnostních technologií (SECTECH), vyhlásilo 10. listopadu 2023 výsledky druhé veřejné soutěže tohoto programu. Soutěž byla vyhlášena 15. března 2023, přičemž Rada programu podpořila 19 projektů s celkovou finanční alokací 297 mil. CZK. Mezi podpořenými projekty nechybí vývoj technologií v oblastech boje proti DeepFakes, analýzy logů či vysokorychlostní filtrace síťového provozu. Kompletní seznam podpořených projektů je zveřejněn na stránkách Ministerstva vnitra.

Evropská komise uspořádala první setkání s tzv. pledgers v rámci Akademie kybernetických dovedností

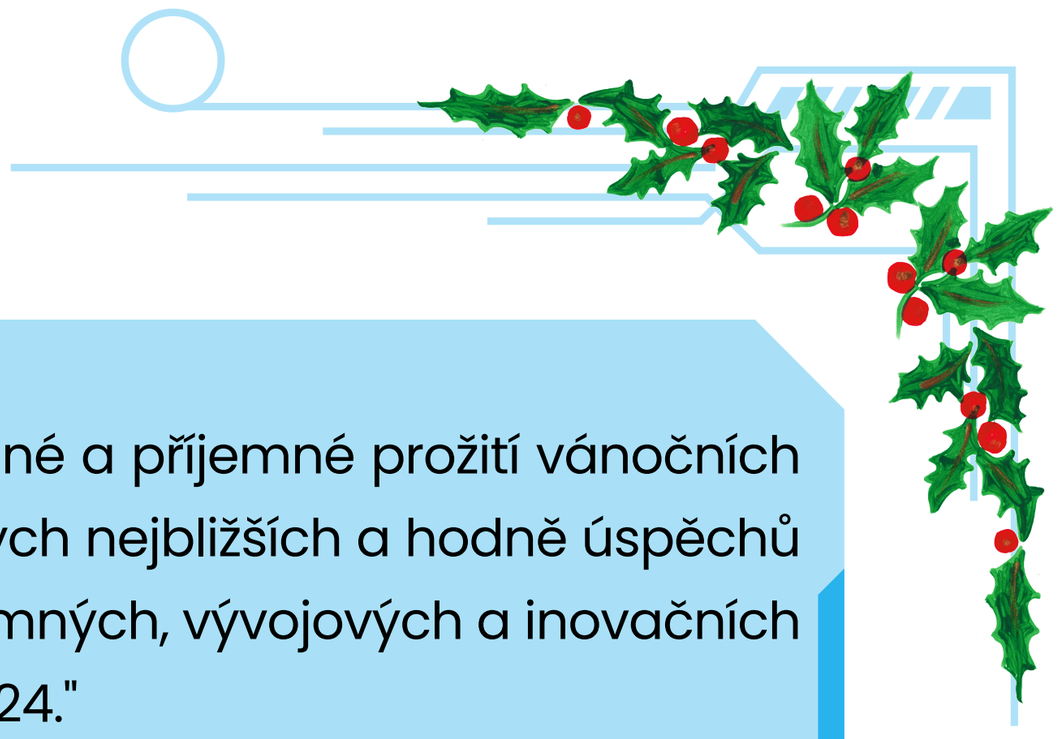
Cybersecurity Skills Academy představuje unijní iniciativu pro zajištění koordinovaného přístupu k posílení evropského pracovního trhu na poli kybernetické bezpečnosti a reaguje na potřebu zvyšovat počet odborníků na prevenci, odhalování a obranu EU před kybernetickými útoky. Pledgers jsou zástupci firem, kteří se zavázali přispět k naplnění cílů Akademie, například skrze poskytování bezplatných školení. Jednání s Evropským kompetenčním centrem (ECCC) a Agenturou EU pro kybernetickou bezpečnost (ENISA) se zúčastnili také zástupci společností Cisco, CompTIA, Leonardo, Workday, SANS | GIAC, ISACA, NVIDIA Deep Learning Institute, Microsoft a ISC2.

Evropské rámcové programy otevírají sadu nových výzev

V rámci pracovního programu Horizon Europe byly ohlášeny výzvy v celkové hodnotě 290 mil. EUR na období 2023-2024. Až 85 mil. EUR bude směřováno na podporu výzkumu v oblasti datových a výpočetních technologií, souvisejících především s inovacemi v oblasti umělé inteligence. Významnými jsou rovněž pilotní projekty zaměřené na rozvoj průmyslové platformy internetu věcí. Dalších 205 mil. EUR je určeno projektům z oblasti podpory digitální a technologické konkurenceschopnosti Evropy a dosažení cílů evropské zelené dohody. Příjem žádostí byl také zahájen v programu Digital Europe, v rámci kterého byly zveřejněny výzvy s celkovou alokací 42 mil. EUR. Výzvy jsou zaměřeny na tři klíčové oblasti – Specializované vzdělávací programy v klíčových kapacitních oblastech, Analýza pokročilých digitálních dovedností a Akademie kyberbezpečnostních dovedností. Žádosti v rámci programu Digitální Evropa je možné podávat do 21. března 2024.

Americká kvantová síť Quantum Corridor se chlubí téměř okamžitým přenosem dat

Technologická společnost Quantum Corridor se sídlem v americkém Chicagu vydala prohlášení, ve kterém uvedla, že se jí v rámci vlastní testovací kvantové komunikační sítě podařilo dosáhnout rychlosti přenosu informací tisíckrát vyšší než u tradičních sítí. Její první přenos dat na vzdálenost 19 kilometrů dosáhl zpoždění pouhých 0,266 milisekundy, což je pětset-krát rychlejší než mrknutí lidského oka. Během následujících devíti měsíců se navíc Quantum Corridor rozšíří na celkových 263 mil (423 kilometrů), čímž se stane největší kvantovou výpočetní sítí ve Spojených státech. Dle současného nastavení by měla být tato síť po svém dokončení schopna přenést objem dat o velikosti veškerého obsahu současného internetu v jediném přenosu. Quantum Corridor zdůrazňuje význam využití sítě především v oblasti národní obrany, kybernetické bezpečnosti a strojového učení. Mohla by ji také využívat autonomní vozidla, kterým umožní dosáhnout rychlejších reakcí, a tím zajistit jejich efektivnější a bezpečnější provoz. Quantum Corridor je zároveň první severoamerickou sítí, která dosáhla kapacity 40 terabitů za sekundu. V celosvětovém měřítku však není zdaleka nejrychlejší. Prvenství drží japonští inženýři, kterým se podařilo dosáhnout nejvyšší rekordní rychlosti internetu 319 terabitů za sekundu.



„Přejeme vám klidné a příjemné prožití vánočních svátků v kruhu svých nejbližších a hodně úspěchů při realizaci výzkumných, vývojových a inovačních projektů v roce 2024."

Oddělení vědy, výzkumu a inovací

Čeští vědci součástí evropského projektu zaměřeného na vývoj AI pro řešení celospolečenských problémů

Evropa již v současné době zaostává ve vývoji umělé inteligence za významnými zahraničními producenty, zejména USA a asijskými zeměmi. Zvrátit tento trend se ovšem aktivně snaží skrze podpůrné programy pro rozvoj AI, jako je projekt ELIAS (European Lighthouse of Artificial Intelligence for Sustainability), na který Evropská komise vyčlenila 11 mil. EUR (přibližně 268 mil. CZK). Cílem projektu je rozvoj umělé inteligence v oblasti hospodářského rozvoje, sociálních konotací AI a environmentální udržitelnosti. Projektu se účastní 34 partnerů ze 17 členských států, včetně České republiky, kterou v projektu reprezentuje Český institut informatiky, robotiky a kybernetiky ČVUT v Praze. Výzkumníci budou v následujících čtyřech letech pracovat na vývoji nových výpočetních systémů s potenciálem pro využití v širokém spektru oblastí dopadajících na kvalitu života od zvýšení bezpečnosti každodenního využívaní AI až po modelování a analýzu klimatických změn. Projekt je podpořen ze strany průmyslu a partnery projektu jsou také soukromé společnosti jako například IBM, Bosch či Bitdefender. Hlavním koordinátorem projektu je univerzita v Trentu a českému zástupci bylo přiděleno půl mil. EUR (přibližně 12 mil. CZK).

Vědeli jste, ŽE...

...obchodní asociace DIGITAL-EUROPE vydala aktualizovaný manifest nesoucí název Europe 2030: A Digital Powerhouse? Publikace dokumentuje vliv turbu-lentního období posledních let na úrovni celé EU a popisuje až 20 konkrétních řešení a cílů, díky kterým se EU transformuje do role digitální velmoci. Naplněním těchto kroků založených především na aktivní integraci technologií jako je umělá inteligence nebo 5G sítě do praktického fungování, povedou k zisku vedoucího postavení v oblasti inovací v rámci inkluzivní a bezpečné digitální demokracie.

Kvantové technologie jsou využitelné také za účelem zabezpečení cloudu

Technologie cloudu jako taková již sama o sobě zvyšuje kybernetickou bezpečnost díky škálovatelné infrastruktuře, centralizovanému zabezpečení a rychlé reakci na hrozby. Výzkumníci z American Institute of Physics v současné době pracují na dalším prohloubení zabezpečení cloudu, a to pomocí kvantových technologií a post-kvantové kryptografie. Ve svém inovativním návrhu zabezpečení použili šifrovací klíče založené na kvantových náhodných číslech distribuovaných pomocí Shamirova algoritmu sdíleného „tajemství“. Shamirův algoritmus sám o sobě funguje na principu distribuce utajené informace skupině tak, aby daná informace, neboli „tajemství“, mohlo být dešifrováno pouze tehdy, když jsou dešifrovací klíče ověřeny u vícero příjemců zároveň. Takovéto řešení, i když s velmi vysokou úrovní zabezpečení, má výraznou nevýhodu v podobě požadavku na úložný prostor v cloudu, na kterém je nasazen. Tento nedostatek se ovšem vědcům podařilo limitovat právě díky kombinaci s kvantovými šifrovacími klíči, které umožňují bezpečný přenos dat prostřednictvím sítě do distribuovaných cloudů. Samotný Shamirův algoritmus tedy nemusí být uložen přímo na cloudu, čímž je eliminován největší nedostatek tohoto řešení. Tento přístup zvyšuje bezpečnost, zrychluje ukládání dat a nesnižuje odolnost proti chybám. Vzhledem k tomu, že řešení splňuje současné kvantové a kryptografické standardy, plánují výzkumníci podpořit také jeho komerční implementaci. V budoucnu se chtějí zaměřit také na výzkum integrace dalších kvantových technologií do cloudového úložiště.

Nástroj AntiFake ochrání váš hlas před zneužitím skrze deepfake

Syntéza podvodné řeči je v současnosti jedním z nejaktuálnějších typů zranitelností, díky které může útočník nejen vylákat citlivé informace z oběti, ale také třeba autorizovat různé datově citlivé úkony. Výzkumníci z Washington University in St. Louis ovšem vyvinuli nástroj s názvem AntiFake na ochranu před tímto typem deepfaku. Na rozdíl od tradičních metod detekce deepfaků, které se používají k vyhodnocení a odhalení syntetického zvuku jako nástroj pro zmírnění následků útoku, zaujímá AntiFake proaktivní postoj. Nástroj se totiž snaží aktivně předcházet samotné syntéze podvodné řeči skrze znemožnění útočníkovi vyčíst z hlasových záznamů potřebné charakteristiky. V zásadě se jedná o reverzi samotného procesu vytváření deepfaku za použití stejného typu umělé inteligence, který deepfaky vytváří. Zjednodušeně řečeno je nahraný zvukový signál „zkreslen“ umělou inteligenci natolik, aby ho AI nebyla schopna syntetizovat, ale aby lidským posluchačům zněl pořád téměř identicky. AntiFake byl testován na pěti nejpokročilejších syntetizátorech řeči s 24 účastníky a dosáhl více než 95% míry úspěšnosti v ochraně potenciální oběti. Aktivní nasazení a využívání nástrojů jako jsou AntiFake umožní využívat technologii se širokým potenciálem použití např. v personalizovaných hlasových asistentech či jiných komunikačních nástrojích bezpečně a bez výrazných rizik.

Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Kontaktní informace

11/2023

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