Analýza legislativních požadavků na kybernetickou bezpečnost ve vazbě na oblast umělé inteligence

Školitel: prof. Mgr. Roman Jašek, Ph.D., DBA

Konzultant: Ing. David Malaník, Ph.D. / Ing. Radek Vala, Ph.D.

Ústav fakulty: Ústav informatiky a umělé inteligence

Studijní program: **Bezpečnostní technologie, systémy a management**

Anotace:

Umělá inteligence (AI) je rychle se rozvíjející technologie mající potenciál významného komplexního dopadu na celou společnost. AI se již nyní dotýká téměř všech oblastí lidské činnosti včetně zdravotnictví, dopravy, financí a bezpečnosti. V oblasti informační bezpečnosti je AI využívána k vývoji nových technologií a metod, které mohou pomoci zlepšit bezpečnost lidí a majetku. Například AI se používá k vývoji pokročilých systémů detekce a prevence kriminality, k zlepšení bezpečnosti v dopravě a k vývoji nových metod pro ochranu před kybernetickým útokem. S rozvojem AI však vyvstávají i nové výzvy a systémy AI mohou být potenciálně zneužity k útokům na bezpečnostní systémy nebo k šíření dezinformací. Evropská unie definuje nové nařízení AI Act, neboli Akt o umělé inteligenci, které má za cíl zajistit, aby systémy umělé inteligence (AI) byly bezpečné, spravedlivé a transparentní. Nařízení bylo přijato Evropským parlamentem a Radou v červnu 2022 a vstoupí v platnost v červenci 2024.

Cílem výzkumu bude analýza dopadů legislativních požadavků na bezpečnost v oblasti AI, budou identifikovány klíčové aplikační oblasti s možnou další legislativní úpravou tak, aby se zajistilo bezpečné používání chytrých nástrojů a systémů AI v průmyslu a společnosti.

Literatura:

[1] Analyzing the European Union AI Act: What Works, What Needs Improvement (Politicians and technologists detail the major areas of negotiation and what's at stake for the U.S.), 2023. Online. Dostupné z: https://hai.stanford.edu/news/analyzing-european-union-ai-act-what-works-what-needs-improvement. [cit. 2023-10-18].

[2] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY, KTERÝM SE STANOVÍ HARMONIZOVANÁ PRAVIDLA PRO UMĚLOU INTELIGENCI (AKT O UMĚLÉ INTELIGENCI) A MĚNÍ URČITÉ LEGISLATIVNÍ AKTY UNIE, 2021. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52021PC0206. [cit. 2023-10-18].

[3] KOLOUCH, Jan, 2016. CyberCrime. CZ.NIC. Praha: CZ.NIC, z.s.p.o. ISBN 978-80-88168-15-7.

[4] KOLOUCH, Jan a BAŠTA, Pavel, 2019. CyberSecurity. CZ.NIC. Praha: CZ.NIC, z.s.p.o. ISBN 978-80-88168-31-7.

[5] PORADA, Viktor; RAIS, Karel a , a kolektiv autorů, 2021. Právní, kriminalistické a kybernetické aspekty kybernetické kriminality a bezpečnosti: pocta Vladimíru Smejkalovi. Brno: Akademické nakladatelství CERM. ISBN 978-80-7623-065-1.

[6] SMEJKAL, Vladimír; SOKOL, Tomáš a KODL, Jindřich, 2019. Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-765-8.

[7] ŠTĚDROŇ, Bohumír, 2020. Právo a umělá inteligence. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-803-7.