NÁZEV DIPLOMOVÉ PRÁCE V ČESKÉM JAZYCE

Kriminalizace útoků na informační systémy

ABSTRAKT

Kyberkriminalita představuje stále větší nebezpečí pro lidskou společnost. Hlavním cílem této práce je zjistit, jaké útoky na informační systémy představují hrozbu pro stát a zda představují nové technologické trendy v oblasti útoků na informační systémy výzvu pro současnou českou právní úpravu v oblasti trestního práva. Metodologie se napříč touto prací různí. K naplnění cíle práce je použita především analytická metoda spolu se syntézou. V některých částech je pak užíván přístup empirický.

V úvodní části práce jsou vysvětleny klíčové instituty v oblasti kyberkriminality a mezinárodní instrumenty pro boj proti kyberkriminalitě. Nejvýznamnějším dokumentem je Úmluva Rady Evropy o počítačové kriminalitě. Stěžejní část práce je věnována úskalím současné české právní úpravy v souvislosti s kyberútoky. Závěrečná část práce se zabývá aktuálními technologickými trendy, jako je umělá inteligence, cloudová úložiště, virtuální měny a internet věcí, které hrají významnou roli v oblasti útoků na informační systémy.

Současná česká právní úprava zareagovala na stoupající tendence kyberkriminality, a proto byly zavedeny nové druhy trestných činů. Umělá inteligence představuje především problém z hlediska odpovědnosti za způsobený trestný čin. Cloudová úložiště vytvářejí výzvu v oblasti vyšetřování trestných činů, konkrétně zajišťování důkazů. Kryptoměny mohou velmi dobře posloužit k ukrytí peněz získaných z trestné činnosti. Propojení všech věcí v rámci internetu věcí vytváří zranitelné struktury, které se mohou stát terčem útoku. Přestože současná právní úprava dostačuje, je rozvoj technologií tak turbulentní, že bude v blízké době nutné přijmout nový právní rámec. Zároveň je na místě zvýšit zabezpečení počítačových systému, a to jak na úrovni státu, tak na úrovni samotných uživatelů.

KLÍČOVÁ SLOVA

kyberkriminalita, kyberprostor, kyberútok