

# NÁZEV DIPLOMOVÉ PRÁCE V ČESKÉM JAZYCE

Kriminalizace útoků na informační systémy

## ABSTRAKT

Diplomová práce se zabývá problematikou kriminalizací útoků na informační systémy. Aktuálnost tématu je podřezna rapidním vývojem informačních a komunikačních technologií a přesunem každodenních aktivit do virtuálního prostředí. V současné době kybernetická kriminalita představuje rostoucí nebezpečí nejenom pro jednotlivce, ale také pro stát. Cílem práce je představit kybernetické útoky a trestněprávně je klasifikovat. Dále je pozornost koncentrována na procesněprávní stránku útoků, zejména na jejich odhalování, vyšetřování a postup při mezinárodní spolupráci. Opomenut není ani nadnárodní a mezinárodní rámec v boji proti kybernetické kriminalitě. Snahou práce je zjistit jakým problematickým aspektům čelí tuzemská právní úprava a jaký budoucí vývoj v oblasti kyberzločinu lze očekávat.

Úvodní část objasňuje základní pojmy, se kterými práce hojně pracuje. Následně jsou představeny klíčové mezinárodní instrumenty v boji proti kybernetické kriminalitě. Těžiště je věnováno představení jednotlivých druhů kybernetických útoků a jejich následné trestněprávní klasifikaci. Navazující část přibližuje procesní rovinu problematiky, přičemž vymezená část obsahuje taktéž poznatky z kriminologie, jako je typologie pachatelů a jejich motivů. Zmíněna je taktéž problematika aktuálních trendů v kyberprostoru, jako jsou cloudová úložiště, virtuální měny a virtuální krádeže. Závěrem jsou představeny statistické údaje týkající se nápadu kybernetické trestné činnosti v České republice během posledních let a možného předpokládaného budoucího vývoje. Kapitola současně reflektuje i vývoj kybernetické trestné činnosti v souvislosti s koronavirovým onemocněním COVID-19 a probíhajícím válečným konfliktem na Ukrajině. Mimo to jsou prezentovány vize a cíle České republiky v oblasti kybernetické bezpečnosti.

## KLÍČOVÁ SLOVA

kybernetická kriminalita, kyberútok, kyberprostor