Cyberbezpieczeństwo Polski

Wstęp

3.3. Zapewnienie bezpieczeństwa transakcjom w Internecie

Zakończenie
Bibliografia

Opis zawartości pracy:

Celem niniejszej pracy jest rozpoznanie zagrożeń dotyczących funkcjonowania głównie państwa, jak i obywateli w sieci, a także zapewnienie im bezpieczeństwa przed zagrożeniami w cyberprzestrzeni.

W pierwszym rozdziale scharakteryzowano podstawowe zagrożenia w cyberprzestrzeni między innymi cyberprzestępczość i cyberterroryzm, w celu odróżnienia tych zagrożeń. Przedstawiano przykłady jak dotąd przeprowadzonych ataków w cyberprzestrzeni. Zwrócono również uwagę na przestępstwa komputerowe, które są najmłodszym rodzajem przestępczości. Ponadto scharakteryzowano zjawisko cyberwojny.

Drugi rozdział w całości został poświęcony Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej. Przedstawiono zagadnienia zawarte
w „Rządowym Programie Ochrony Cyberprzestrzeni na lata 2011-2016”.
W kolejnym podrozdziale ukazano podstawowe organy odpowiedzialne za nadzorowanie i ochronę w cyberprzestrzeni – czyli omówione zostały zasady działania „Rządowego Zespołu Reagowania na Incydenty Komputerowe”, również CERT-u Polska, policji, prokuratury i sądów powszechnych. Rozdział kończy charakterystyka współpracy państwa polskiego z organizacjami międzynarodowymi w walce z cyberprzestępczością, ze szczególnym uwzględnieniem roli Unii Europejskiej w oparciu o „Konwencje Rady Europy o cyberprzestępczości” i „Decyzje ramową Rady w sprawie ataków na systemy informatyczne”, oraz rola instytucji takich jak NATO czy ONZ.

Trzeci rozdział przedstawia działania podejmowane w ramach

bezpieczeństwa w Internecie między innymi głownie w kwestii edukacji dzieci i młodzieży, ochrony prywatności, a także zapewnienia bezpieczeństwa transakcjom w Internecie.
Wszystkie opracowania zastosowane w niniejszej pracy znajdują się w bibliografii umieszczonej na końcu pracy.