

Cyberbezpieczeństwo Polski

Wstęp

Rozdział I

Zagrożenia w cyberprzestrzeni

1.1. Cyberprzestępczość a cyberterroryzm

1.2. Ataki w cyberprzestrzeni

1.3. Przestępstwa komputerowe

1.4. Cyberwojna

Rozdział II

Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej

2.1. Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016

2.2. Państwowe organy nadzoru i ochrony w cyberprzestrzeni

2.2.1. Rządowy Zespół Reagowania na Incydenty Komputerowe

2.2.2. CERT Polska

2.2.3. Policja

2.2.4. Prokuratura i sądy powszechne

2.3. Współpraca państwa polskiego z organizacjami międzynarodowymi w walce z cyberprzestępczością

2.3.1. Unia Europejska

2.3.1.1. Konwencja Rady Europy o cyberprzestępczości

2.3.1.2. Decyzja ramowa Rady w sprawie ataków na systemy informatyczne

2.3.2. ONZ

2.3.3. NATO

2.3.4. Inne organizacje międzynarodowe

Rozdział III

Obywatele w trosce o bezpieczeństwo informacyjne Polski

3.1. Działania podejmowane w ramach bezpieczeństwa dzieci i młodzieży w Internecie

3.2. Sposoby zapewniania ochrony prywatności

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 najmłodszy 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 głównie 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.