Henryk Fedewicz,
Violetta Paleolog-Demetraki

CYBERPRZESTĘPCZOŚĆ – NOWYM RODZAJEM ZAGROŻEŃ DLA BEZPIECZEŃSTWA PAŃSTWA

Współczesny świat stoi wobec nowych wyzwań i zagrożeń dla bezpieczeństwa międzynarodowego, wśród których kluczową rolę odgrywają cyberzagrożenia. Ich charakter oraz zakres jest zróżnicowany, od zwykłych ataków hackerskich po akcje, za którymi stoją państwa. Rozwijane scenariusze ataków skłaniają poszczególne państwa oraz organizacje międzynarodowe jak Unia Europejska czy NATO, do zdefiniowania zagrożeń oraz podjęcia odpowiednich działań celem ich neutralizacji.

Współczesne czasy charakteryzują gwałtowne przemiany wszystkich dziedzin życia. Następuje szybki rozwój najnowszych technologii, wkraczających w każdą sferę życia ludzi. Komputer, Internet oraz telefon komórkowy są powszechnie używane i stanowią narzędzia powszechnego komunikowania się na całym świecie. Internet ma ogromny wpływ na każdą dziedzinę ludzkiej aktywności. Wielu użytkowników wykorzystuje go do zdobywania wiedzy, rozwijania umiejętności czy pracy zawodowej. Niestety wraz z rozwojem Internetu jego integralną częścią stały się przestępstwa komputerowe. Istnieje ogromna ilość osób, wykorzystujących sieć internetową do łamania prawa. Ofiarami działań cyberprzestępców mogą stać się jednostki rządowe, urzędy, banki, przedsiębiorcy oraz zwykli użytkownicy. Skutki takich działań mogą być odczuwalne przez społeczeństwo a konsekwencje dla gospodarki i infrastruktury mogą obejmować straty ekonomiczne, utratę konkurencyjności gospodarki lub zagrożenia dla obronności państwa.

Termin «cyberprzestrzeń» po raz pierwszy został użyty w 1984 roku przez Wiliama Gibsona, który był twórcą cyberpunkowego nurtu «science fiction». W swoich powieściach *Neuromancer* i *Burnig Chrome* przedstawił świat wirtualnej, immersyjnej rzeczywistości wygenerowany przez komputer, określany matrycą. Termin ten wszedł do użytku publicznego na początku lat 90-tych. Na przełomie XX/XXI wieku nastąpił wzrost popularyzacji tego terminu spowodowany eksplozją rozwoju sieci Internet. Obecnie «cyberprzestrzeń» określa globalną infrastrukturę informacyjną (teleinformatyczną) i jest przestrzenią cybernetyczną. Przestrzeń cybernetyczna w tzw. modelu Wardena traktowana jest jako piąty «wymiar» walki (obok lądu, morza, powietrza i przestrzeni kosmicznej).

Cyberprzestrzeń jest światem informacji tworzonych za pomocą Internetu lub przestrzenią komunikacyjną tworzoną przez system internetowych powiązań.

Pojęcie cyberprzestrzeni zostało wprowadzone również w polskim porządku prawnym. Definicję tego pojęcia zawarto w nowelizacji ustawy o stanie wojennym oraz w ustawie o stanie klęski żywiołowej. Według tej nowelizacji cyberprzestrzeń to przestrzeń przetwarzania oraz wymiany informacji tworzonej przez systemy teleinformatyczne.

Definicję cyberprzestrzeni państwa zawarto także w Rządowym programie ochrony cyberprzestrzeni RP opracowanym na lata 2011–2016. Wg tego programu cyberprzestrzeń jest cyfrową przestrzenią przetwarzania oraz wymiany informacji tworzoną przez sieci i systemy teleinformatyczne, które są powiązane pomiędzy sobą oraz z użytkownikami. Cyberprzestrzeń RP obejmuje terytorium państwa Polskiego i miejsca poza jego terytorium, gdzie funkcjonują placówki dyplomatyczne RP i kontyngenty wojskowe RP.

Pojmowanie cyberprzestrzeni jako powiązań działalności ludzkiej z technologią informacyjno-komunikacyjną powoduje, że charakteryzuje się ona szczególnymi właściwościami. Znamiennymi cechami cyberprzestrzeni są jej płynność, plastyczność, powtarzalność w czasie rzeczywistym oraz obliczalność z dużą dokładnością. Cyberprzestrzeń ma charakter wirtualny pozbawiony parametru geograficznego, jest więc bytem nieograniczonym i niemierzalnym. Jej granice wyznacza stopień internetyzacji świata. Cyberświat nie posiada granic ani końca. Jest to przestrzeń bez miejsca, w której różne płaszczyzny i sfery nakładają się na siebie, przecinają i przenikają – przekraczając kategorie terytorialności.

Cyberzagrożenia stanowią nowy rodzaj wyzwań i zagrożeń dla bezpieczeństwa współczesnego państwa i wskazują na konieczność traktowania tej sfery jako strategicznej.

Do najpopularniejszych zagrożeń w cyberprzestrzeni należą:

– kradzieże tożsamości;

– ataki z użyciem oprogramowania złośliwego (wirusy, *malware*, robaki itp.);

– spam (niepotrzebne lub niechciane wiadomości elektroniczne);

– blokowanie dostępu do usług (DoS oraz DDoS, *mail bomb*)

– ataki socjotechniczne (*phishing* – wyłudzanie informacji poufnych przez podszywanie się pod osobę lub instytucję godną zaufania).

Wyzwaniem stają się współcześnie ataki typu APT (*advanced persistent thereat).* Ataki te łączą różnego typu narzędzia, a ich przygotowania trwają wiele tygodni. Przeprowadzają je zorganizowane grupy, które dysponują odpowiednim budżetem oraz czasem niezbędnym

do zinfiltrowania celu i przeprowadzenia precyzyjnego ataku w celu kradzieży wrażliwych danych lub zniszczenia/ uszkodzenia systemu komputerowego.

Cyberprzestrzeń stanowi zagrożenie dla infrastruktury teleinformatycznej. Zagrożenia klasyfikowane przez CERT Polska dzielą się na następujące grupy:

– złośliwe oprogramowanie (wirus, koń trojański, robak sieciowy, dialer, oprogramowanie szpiegowskie),

– gromadzenie informacji (skanowanie, podsłuch, inżyniera społeczna),

– próby włamań (próby nielegalnego logowania, wykorzystanie znanych i nieznanych luk systemowych),

– włamania (na konto zwykłe, uprzywilejowane, do aplikacji),

– atak na dostępność zasobów (DoS, DDoS, sabotaż komputerowy),

– oszustwa komputerowe (kradzież tożsamości, podszycie się, naruszenie praw autorskich, nieuprawnione wykorzystanie zasobów),

– atak na bezpieczeństwo informacji (nieuprawniony dostęp, nieuprawniona zmiana).

Źródłem ataków mogą być hakerzy, rządy państw oraz organizacje terrorystyczne. Kradzież informacji umożliwia uzyskanie informacji o działalności spółek skarbu państwa, ich projektach inwestycyjnych czy wykorzystywanych technologiach.

Umożliwia również uzyskanie informacji potencjalnie potrzebnych do przeprowadzenia ataku cyberterrorystycznego. Zagrożenia te dotyczą również serwerów i portali instytucji, urzędów i innych podmiotów. Ataki mogą zostać wykorzystane do penetracji systemu oraz spowodować paraliż sieci wewnętrznej.

Do głównych wyzwań i zagrożeń bezpieczeństwa w cyberprzestrzeni XXI wieku należą: wojna informacyjna, cyberterroryzm, cyberszpiegostwo i cyberprzestępczość.

Obecnie wojna informacyjna to zorganizowana zewnętrzna militarna aktywność państwa, skierowana na niszczenie systemu informacyjnego przeciwnika oraz ochrona własnych systemów informacyjnych przed działaniem przeciwnika.

Według niektórych definicji wojna informacyjna to użycie udoskonalonych środków elektronicznych podczas wojny, natomiast według innych to wszelkie działania, które zmierzają do zniszczenia systemów informacyjnych przeciwnika zarówno w czasie wojny jak i pokoju. Głównym celem wojny informacyjnej są systemy infrastruktury krytycznej państw i organizacji międzynarodowych.

Cyberterroryzm to cyberprzestępstwo o charakterze terrorystycznym. Cyberterroryzm jest jednym z głównych zagrożeń bezpieczeństwa narodowego i międzynarodowego. Jest zjawiskiem o charakterystyce dynamicznie narastającej i oscylującym na pograniczu różnych obszarów, do których zalicza się: bezpieczeństwo teleinformatyczne, technologie teleinformacyjne i informatyczne, bezpieczeństwo fizyczne, bezpieczeństwo osobowe, dane osobowe, regulacje prawne narodowe oraz międzynarodowe.

Do reprezentatywnych definicji cyberterroryzmu i najczęściej spotykanych należy definicja Dorothy Denning: «(…) Cyberterroryzm to połączenie pojęcia cyberprzestrzeni i terroryzmu. To groźba lub bezprawny atak wymierzony w system informatyczny lub zgromadzone dane, w celu zastraszenia czy wymuszenia na władzach państwowych lub jej przedstawicielach ustępstw lub oczekiwanych zachowań, w celu wsparcia określonych celów (np. politycznych). Aby działania takie zostały zakwalifikowane jako terroryzm informacyjny, atak powinien powodować znaczne straty lub takie skutki, które wywołują powszechne poczucie strachu».

Działania wywiadowcze w cyberprzestrzeni umożliwiają dostęp do wielu informacji, które mogą być istotne dla bezpieczeństwa narodowego i międzynarodowego.

Cyberszpiegostwo jest wykorzystaniem przestrzeni teleinformatycznej w celu zdobywania informacji niejawnych. Jest to tańszy, prostszy i bezpieczniejszy proceder niż tradycyjne formy szpiegostwa. Ułatwia ono zdobywanie tajnych informacji, które współcześnie traktowane są jako wartościowy towar. Powodem zdobywania zastrzeżonych informacji są zamiary uzyskania nowoczesnych technologii. Głównym celem tych operacji są instytucje rządowe, instytucje badawcze oraz korporacje. Coraz częściej cyberprzestrzeń wykorzystywana jest przez służby państwowe, świadczy o tym poziom zaawansowania i skomplikowania wielu operacji wywiadowczych.

Cyberprzestępstwo jest czynem zabronionym popełnionym w obszarze cyberprzestrzeni. Cyberprzestępczość to bardzo szybo rozwijający się obszar przestępczości. Jego szybkość, wygodę oraz anonimowość a także rozwijające się technologie wykorzystuje coraz więcej przestępców. Dokonują oni ataków na systemy i dane komputerowe oraz m.in. rozpowszechniania wirusów, botnerów, kradzieży tożsamości, wykorzystywania seksualnego dzieci, dystrybucji pornografii, oszustw na aukcjach internetowych i w usługach finansowych.

Cyberprzestępczość coraz szybciej rozszerza obszary ataku oraz dysponuje coraz nowocześniejszymi technikami działania. Istotną jej cechą jest występująca pomiędzy cyberprzestępcami globalna wymiana informacji dotyczących technik i metod działania oraz zabezpieczeń. Stanowi to

utrudnienie w walce z cyberprzestępczością. Manipulowanie informacjami w cyberprzestrzeni uzyskanymi w sposób legalny i nielegalny skutkuje przestępstwami o charakterze ekonomicznym, w szczególności oszustwami finansowymi, które najbardziej zagrażają instytucjom finansowym a szczególnie bankom. Prowadzenie nielegalnych operacji finansowych jest głównym obszarem zainteresowania cyberprzestępczości zorganizowanej, prowadzonej na obszarze wytypowanych państw. Wraz z rozwojem technologii cyberprzestępczość przekształca się w ogromny biznes, na którym przestępcy szybko zarabiają ponosząc minimalne ryzyko. Rośnie liczba przestępców, dla których nie ma barier językowych i ograniczenia zasięgu geograficznego a liczba okazji do przestępstwa ma globalny charakter.

Podstawowe przestępstwa popełniane w ostatnich latach w cyberprzestrzeni najczęściej dotyczą:

– oszustw dokonywanych za pośrednictwem Internetu,
– wykorzystania elektronicznych instrumentów płatniczych, najczęściej jest to phishing,
– pedofilii i pornografii dziecięcej,
– handlu towarami licencjonowanymi bez posiadania uprawnień,
– nielegalnego handlu towarami akcyzowymi,
– nieuprawnionego uzyskiwania informacji (hacking),
– podsłuchu komputerowego (sniffing),
– udaremniania dostępu do informacji,
– przełamywania zabezpieczeń komputerowych
– złośliwych oprogramowań.

Struktura fizyczna sieci Internet w Polsce składa się z setek tysięcy komputerów i innych urządzeń elektronicznych, przesyłających dane w wielu kierunkach, a od ich właściwego działania, na które składa się wiele czynników, takich jak konfiguracja, administracja, aktualizacja oprogramowania, czynnik ludzki itp. zależy poprawne funkcjonowanie usług dostarczanych za pomocą Internetu. Efektywne bezpieczeństwo oznacza ochronę danych. Wszystkie strategie i procedury powinny odzwierciedlać potrzeby ochrony danych niezależnie od przyjmowanie przez nie formy: dokumenty na dysku, wydrukowane, przekazywane faksem czy telefonicznie. Dane powinny być chronione niezależnie od nośnika, na którym występują.

W polskim ustawodawstwie brak jest jednolitej regulacji prawnej dotyczącej odpowiedzialności za nadużycia w sieci. Przepisy rozproszono w kilku aktach prawnych: w kodeksie karnym, ustawie o ochronie danych osobowych, ustawie o prawie autorskim i prawach pokrewnych, ustawie o świadczeniu usług drogą elektroniczną. Zgodnie z obowiązującymi

zasadami ustawodawstwo polskie musi uwzględniać rozwiązania aktów prawa europejskiego przede wszystkim Konwencji o Cyberprzestępczości i ramowej decyzji Rady w sprawie ataków na systemy informatyczne.

W celu skutecznego zapobiegania i zwalczania cyberzagrożeń konieczne okazało się współdziałanie rządów na arenie międzynarodowej oraz ujednolicenie i dostosowanie się do zewnętrznych wymogów środków prawnych w poszczególnych krajach oraz współpraca dotycząca prewencji. Wypracowano modelowe rozwiązania na poziomie międzynarodowym, które stały się punktem odniesienia do regulacji krajowych.

W zakresie zwalczania przestępczości komputerowej pod nadzorem Rady Europy przyjęto w Budapeszcie i otwarto do podpisu 23 listopada 2001 roku Konwencję o cyberprzestępczości, która weszła w życie w dniu 1 lipca 2004 roku (po ratyfikacji w pięciu państwach, z czego trzech należących do RE – zgodnie z warunkami nadania jej obowiązującej mocy).

Polska podpisała porozumienie 23 listopada 2003 roku i ratyfikowała 28 października 2014 roku. W polskim systemie prawnym przepisy prawne nawiązujące do Konwencji pojawiły się po jej podpisaniu i doprowadziły w większości do zgodności jej przepisów z prawem krajowym. Nie jest ona jednak adekwatnym narzędziem w przeciwdziałaniu przestępczości związanej z systemami teleinformatycznymi, których technologia rozwija się w błyskawicznym tempie.

W dobie globalizacji ochrona cyberprzestrzeni jest bardzo ważnym i zarazem trudnym przedsięwzięciem. Wymaga ona zaangażowania państw, organizacji krajowych i międzynarodowych oraz stosowania nowych rozwiązań technologicznych i technicznych skutecznie przeciwdziałających cyberzagrożeniom.

Proces ten oprócz działań specjalistycznych powinien być wspierany metodami administracyjno-organizacyjnymi, technicznymi, fizycznymi oraz specjalnymi. Ochrona cyberprzestrzeni to podstawowe zadania administracji państwowej oraz podmiotów odpowiedzialnych za tego rodzaju zadania.

Rząd RP w ramach krajowych zadań mających na celu poprawę bezpieczeństwa w cyberprzestrzeni stworzył «Rządowy program ochrony cyberprzestrzeni na lata 2011–2016» a Ministerstwo Administracji i Cyfryzacji stworzyło dokument pt. «Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej», obowiązujący od 25 czerwca 2013 roku.

«Rządowy program ochrony cyberprzestrzeni na lata 2011–2016» (RPOC) zawiera propozycje działań mających charakter prawno-organizacyjny, edukacyjny i techniczny. Celem przedstawionych działań jest zwiększenie zdolności do zwalczania i zapobiegania zagrożeniom występującym w cyberprzestrzeni. RPOC nie obejmuje niejawnych sieci

oraz systemów teleinformatycznych. Strategicznym celem Programu jest zagwarantowanie ciągłego bezpieczeństwa cyberprzestrzeni Państwa.

Polityką ochrony objęto systemy teleinformatyczne administracji rządowej, władzy ustawodawczej i sądowniczej, samorządów terytorialnych oraz systemy strategiczne. Polityka nie obejmuje obszarem zadaniowym niejawnych systemów teleinformatycznych. Strategicznym celem dokumentu jest osiągnięcie dopuszczalnego poziomu bezpieczeństwa w cyberprzestrzeni Państwa, który realizowany będzie poprzez następujące działania: szacowanie ryzyka, bezpieczeństwo portali administracji rządowej, założenia działań legislacyjnych, proceduralno-organizacyjnych, naukowych oraz technicznych.

Poważnym problemem gwarantującym bezpieczeństwo cyberprzestrzeni jest brak jednoznacznych norm prawnych, pozwalających na skuteczne działanie państwa oraz jego instytucji. Konieczne są prawne uregulowania zasad ochrony i ustalenie obszarów odpowiedzialności ochrony polskiej cyberprzestrzeni a także odpowiedzialności za ochronę krytycznej infrastruktury teleinformatycznej. Poszczególne elementy infrastruktury krytycznej są własnością wielu jednostek administracji publicznej a znaczna ich część jest w rękach podmiotów prywatnych. Niezbędne jest zapewnienie spójnej polityki bezpieczeństwa oraz ustalenie metod i zakresu współpracy wszystkich elementów. Państwo polskie powinno wypracować mechanizmy kooperacji w zakresie ochrony CRP przy współdziałaniu z innymi krajami oraz organizacjami międzynarodowymi. Kwestie techniczne są również obszarem wymagającym działania.

Dla zapewnienia bezpieczeństwa cyberprzestrzeni niezbędna jest rozbudowa systemów ostrzegania przed atakami oraz wdrożenie dodatkowych rozwiązań prewencyjnych oraz szczególnej ochrony najważniejszych systemów teleinformatycznych połączonej z ćwiczenia, które pozwolą ocenić jej odporność na ataki cybernetyczne. W celu przeciwdziałania skutkom potencjalnych incydentów niezbędne jest opracowanie planu wykorzystania w sytuacji kryzysowej systemu powszechnej komunikacji oraz stworzenie zapasowych rozwiązań, które pozwolą na przejęcie zadań krytycznej infrastruktury w przypadku jej niedostępności.

W obliczu globalizacji bezpieczeństwo cyberprzestrzeni jest jednym z podstawowych celów strategicznych każdego państwa. Zadaniem systemu odpowiedzialnego za bezpieczeństwo cyberprzestrzeni RP jest niedopuszczenie do ataków elektronicznych poprzez reagowanie na bieżące zagrożenia i wykrywanie sprawców. Ochroną przed zagrożeniami przestępczością o charakterze elektronicznym oraz dokumentami

strategicznymi przygotowanymi przez centralne instytucje rządowe zajmują się wyspecjalizowane państwowe instytucje.

Bezpieczeństwo sieci oraz systemów komputerowych dotyczy ochrony systemów teleinformatycznych przed złośliwymi programami, przed szpiegostwem komputerowym, przed oszustwami, przed niszczeniem programów i danych, ochrony poufności i integralności transmitowanych danych, uwierzytelniania i autoryzacji użytkowników, usług i hostów oraz paraliżowania pracy systemów komputerowych.

Zabezpieczenia oznaczają wszystkie możliwe elementy osobowe, techniczne, programowe lub organizacyjne wykorzystywane w procesach ochronnych do działań, których celem jest zapewnienie odpowiedniego poziomu ochrony logicznej i fizycznej informacji oraz elementów systemu teleinformatycznego. Zabezpieczenie danych wrażliwych poprzez kodowanie ma przede wszystkim zapobiec nieuprawnionemu dostępowi do nich przez osoby postronne.

Podstawowym sposobem ochrony zasobów jest ochrona fizyczna wrażliwych elementów systemu komputerowego jak: pomieszczenie gdzie pracuje serwer, stacja robocza administratora sieci. Kolejnym poziomem zabezpieczeń jest bezpieczeństwo systemu operacyjnego. Systemy wyposażone są w mechanizmy kontroli dostępu, zapis kartotek oraz plików gwarantowania zezwoleń na czytanie przez określonych użytkowników oraz notowanie dostępów i autoryzacji. System bezpieczeństwa teleinformatycznego powinien być skuteczny, co oznacza, że przełamanie nawet części środków ochronnych nie powinno prowadzić do naruszenia tajności, integralności lub dostępności chronionej informacji; każda próba penetracji systemu powinna być rozpoznana i sygnalizowana. Podstawowa ochrona przed włamaniami sieciowymi jest w gestii administratora. Jego zadaniem jest zarządzanie kontami użytkowników, zmiana haseł, dodawanie nowych użytkowników oraz usuwanie nieaktualnych lub zmiana uprawnień zależnie od potrzeb.

W celu ochrony oprogramowania niezbędne jest stosowanie oprogramowań przeciwdziałającym nieuprawnionym działaniom w sieciach jak:

– oprogramowanie antywirusowe przeciwdziałające oprogramowaniu złośliwemu;

– systemy wykrywania intruzów polegające na identyfikacji czy zdarzenie jest działaniem typowym czy zagrożeniem w sieci;

– zapory sieciowe analizujące ruch sieciowy wchodzący zgodnie z określonymi przez administratora sieci zasadami;

– skanery sieciowe poszukujące w istniejącym systemie bezpieczeństwa słabych punktów.

W obecnych zinformatyzowanych realiach niezbędna jest ochrona różnych zasobów od strony technicznej. Funkcję taką pełnią zespoły typu CERT. Ze względu na zmieniające się zagrożenia w cyberprzestrzeni z roku na rok zwiększa się potrzeba ich istnienia. Rozwinięcie akronimu CERT to Compuer Emergency Response Team, co oznacza zespół do reagowania na incydenty komputerowe. Incydentem komputerowym jest każde zdarzenie, które w jakikolwiek sposób narusza lub zagraża infrastrukturze, za którą jest odpowiedzialny dany CERT. Może to być przypadek phishingu, działalność złośliwego oprogramowania lub inne zdarzenie będące zagrożeniem dla funkcjonowania danej sieci i bezpieczeństwa jej zasobów. Istnieją Cert-y rządowe, wojskowe, akademickie i w dużych komercyjnych firmach (przeważnie z branży IT). Wszystkie mają do czynienia z włamaniami, oszustami komputerowymi, atakami, a ich celem jest zagwarantowanie bezpieczeństwa zarządzanemu obszarowi infrastruktury. Gdy dochodzi do incydentu zespoły uruchamiają procedury, które usuwają lub ograniczają niebezpieczeństwo.

Często jest to możliwe w wyniku wieloletniej współpracy i rozwiniętych kontaktów pomiędzy zespołami, jak: instytucje rządowe i finansowe, policja oraz operatorzy telekomunikacyjni. Współpraca pomiędzy zespołami jest niezbędna ponieważ Internet nie uznaje granic. Większość państw europejskich posiada przynajmniej jeden zespół narodowy CERT, stanowiący punkt kontaktowy dla danego kraju.

Ochrona cyberprzestrzeni RP z każdym rokiem wymaga opracowywania oraz wdrażania coraz nowszych rozwiązań technicznych i jest to konieczne ze względu na zwiększającą się liczbę użytkowników sieci Internet, korzystającą z zaawansowanych technologii. Ponadto atakujący wykorzystują nowe metody w celu przeprowadzenia ataków oraz ciągle zmieniają profil prowadzonych działań, dlatego prowadzone działania organizacyjne oraz techniczne muszą być zintensyfikowane.

Szczególnej uwagi wymaga poziom bezpieczeństwa systemów informatycznych w sektorze publicznym. Atak hakerski na infrastrukturę krytyczną państwa może spowodować wielomilionowe straty w gospodarce oraz zdestabilizować państwo. Funkcjonowanie najważniejszych obiektów infrastruktury krytycznej państwa uzależnione jest od rozwiązań teleinformatycznych, dlatego cyberataki stanowią coraz poważniejsze zagrożenie.

W naszym kraju nie odnotowano dotychczas incydentu, który stanowiłby zagrożenie dla bezpieczeństwa publicznego. Należy jednak pamiętać, że we współczesnym świecie granice państw nie są żadną barierą dla przestępców w cyberprzestrzeni, dlatego możliwość wystąpienia takiego incydentu jest bardzo prawdopodobna. Nie można ignorować potencjalnych

zagrożeń ze względu na możliwości przeciwników oraz rozwój technologiczny. W celu zagwarantowania bezpieczeństwa cyberprzestrzeni ważne jest wspólne działanie państw celem wypracowania najskuteczniejszych regulacji prawnych oraz technicznych, które będą zabezpieczeniem przed ewentualnymi atakami.

Zapewnienie bezpieczeństwa cyberprzestrzeni wymaga zaangażowania szerokiego grona użytkowników globalnej sieci. Podnoszenie świadomości użytkowników na niebezpieczeństwa czyhające w cyberprzestrzeni – przyczyni się do ochrony tego środowiska.

Literatura

1. Sienkiewicz P., Wizje i modele wojny informacyjnej, http://winntbg. bg.agh.edu. pl/skrypty2/0095/373-378.pdf,

2. Ustawa z dnia 29 sierpnia 2002 roku o stanie wojennym oraz kompetencjach Naczelnego Dowództwa Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom RP (Dz. U. z 2002 r. nr 156, poz. 1301 ze zm.) oraz ustawa z dnia 30 sierpnia 2011 roku o zmianie ustawy o stanie wojennym oraz kompetencjach Naczelnego Dowództwa Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom RP (Dz. U. z 2011 r. nr 222, poz. 1323),

3. Ustawa z dnia 18 kwietnia 2002 roku o stanie klęski żywiołowej (Dz. U. z 2002 r. nr 62, poz. 558 ze zm.),

4. Rządowy program ochrony cyberprzestrzeni RP na lata 2011-2016, Warszawa 2011 http://bip.msw.gov.pl/bip/programy/19057,Rządowy-Program-Ochrony-Cyberprzestrzeni-RP-na-lata-2011-2016.html,

5. Białoskórski R., Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku, WSCiL, Warszawa 2011,

6. Grzelak M., Liedel K., Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski, «Bezpieczeństwo Narodowe» nr 22, 2/2012,

7. Lichocki E., Cyberterrorystyczne zagrożenie dla bezpieczeństwa teleinformatycznego państwa polskiego, http://oapuw.pl/wp-content/uploads/ 2013/11/M.Lakomy-zagrozenia-dla-bezpieczenstwa-teleinformatyczne-go. pdf,

8. Lichocki E., Cyberterroryzm jako nowa forma zagrożeń dla bezpieczeństwa, [w:] K. Liedel (red.) Transnarodowe obszary bezpieczeństwa narodowego, Difin, Warszawa 2011,

9. Lakomy M., Zagrożenia dla bezpieczeństwa teleinformatycznego, http://oapuw.pl/wp-content/uploads/2013/11/M.Lakomy-zagrozenia-dla-bezpieczenstwa-teleinformatycznego.pdf,

10. http://bip.msw.gov.pl/bip/raport-o-stanie-bezpie/18405,Raport-o-stanie-bezpieczenstwa.html,

11. Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. nr 133, poz., 8

12. Ustawa z dnia 12 września 2014 r. o ratyfikacji konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie 23 listopada 2001 r. (Dz. U. z 4 listopada 2014, poz., 1514).

Федевіч Генрик. Кіберзлочинність – новий вид загрози для національної безпеки

Резюме. *Метою даної статті є ознайомлення читача з інформацією про безпеку інформаційних систем, передусім, інтернет-мережі, що охоплює багато аспектів, а її класичний елемент – це боротьба з кіберзлочинністю. Глобальний характер інформаційних мереж, через комплексне управління засобами в мультимедійній комунікації в реальному часі між європейськими та міжнародними установами дозволить підвищити ефективність системи та вплине на рівень безпеки та правопорядку держав.*

Представлені концепції і методи штучного інтелекту повинні стати джерелом натхнення при проектуванні інформаційних систем, а також питань зі сфери отримання та застосування знань про злочинні методи, сформульовані висновки надають можливість здійснювати синтетичні оборонні і наступальні операції в поточному контексті міжнародного тероризму.

Fedevich G. Cybercrime – a new type of danger for the security of the country (state)

Abstract. *The aim of this paper is closing the reader with information concerning the security of information systems, including primarily the Internet, the importance of which covers many aspects, and its classical element is the fight against cybercrime.*

The global nature of information networks, through comprehensive management of multimedia communication in real time between the European and international institutions, will increase the efficiency of the system and will affect the level of security and the legal order of states. The concepts and methods of artificial intelligence, should be an inspiration for the design of information systems, and issues in the area of acquisition and extraction of knowledge about criminal methods and the conclusions being drawn allow for synthetic defensive and offensive operations in the current context of international terrorism.

The author of publications specializing in topics related to information security and protection, and scientific achievements includes work in the field of legal and forensic issues interests of the state, as well as negative developments in process management with their numerous social-economical implications.

Стаття надійшла 22 вересня 2015 р.