Anna Zalesińska, Przemysław Pęcherzewski, Piotr Rodziewicz

Rozdział 5. Zagrożenia związane z rozwojem nowych technologii

Większość technologii ma swój świetlisty awers,
ale życie dało im rewers – czarną rzeczywistość.

Stanisław Lem

1. Przestępstwa komputerowe (Anna Zalesińska, Przemysław Pęcherzewski)

1.1. Pojęcie przestępstwa komputerowego w ujęciu materialnoprawnym i procesowym (Anna Zalesińska)

Dynamiczny rozwój Internetu sprawił, że świat wkroczył w nową erę, a przed użytkownikami sieci otworzyły się zupełnie nowe możliwości. Jednakże, rozwój nowoczesnych technologii ma też swoją „ciemną stronę", czego przejawem jest rozwój przestępczości w nowej wirtualnej rzeczywistości na niespotykaną dotąd skalę. W literaturze przedmiotu na określenie nowego zjawiska używa się takich pojęć jak „przestępstwo komputerowe", „przestępstwo związane z wykorzystaniem komputera", „przestępstwo internetowe", „cyberprzestępstwo", „przestępstwa związane z technologią cyfrową". Już sam problem znalezienia adekwatnej nazwy dla omawianego zagadnienia budzi kontrowersje. Zgodnie z terminologią zawartą w *Konwencji Rady Europy o cyberprzestępczości* właściwym terminem powinno być „cyberprzestępstwo"[1].Częstokroć jednak używa się nazwy przestępstwo komputerowe, co jest zgodne z określeniami występującymi w językach innych państw, jako przykład można wskazać „*computer criminality*" czy „*Komputerkriminalität*"[2].

Według K. J. Jakubskiego przestępstwo komputerowe jest to zjawisko kryminologiczne, obejmujące wszelkie zachowania przestępne związane z funkcjonowaniem elektronicznego przetwarzania danych, godzące bezpośrednio w przetwarzaną informację, jej nośnik i obieg w komputerze oraz w całym systemie połączeń komputerowych, a także w sam sprzęt komputerowy oraz prawo do programu komputerowego[3].

---

1 http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=25/06/04&CL=ENG

2 Por. T. Tomaszewski, *Kryminalistyczna problematyka przestępczości komputerowej, „*Problemy kryminalistyki", nr 143, 1980, s. 69.

3 Por. K. J. Jakubski, *Przestępczość komputerowa – podział i definicja, „*Przegląd Kryminalistyki", nr 2/7, 1997, s. 31

Według A. Adamskiego[4] problematyka przestępstw komputerowych może być rozpatrywana zarówno w ujęciu materialnoprawnym, jak i karnoprocesowym. Na gruncie prawa karnego materialnego przestępstwa komputerowe oznaczają z reguły dwa rodzaje zamachów:

a) w pierwszym przypadku przedmiotem zamachu są systemy, dane oraz programy komputerowe. System komputerowy może także stanowić środowisko zamachu, gdy dochodzi do naruszenia jego integralności i modyfikacji znajdujących się w nim danych, przy wykorzystaniu złośliwego oprogramowania komputerowego (tzw. przestępstwa *stricte* komputerowe);

b) druga grupa to czyny, których celem jest naruszenie dóbr prawnych tradycyjnie chronionych przez prawo karne przy wykorzystaniu elektronicznych systemów przetwarzania informacji. Do takich przestępstw będzie należeć m.in. oszustwo (oszustwo komputerowe oraz oszustwo telekomunikacyjne), fałszerstwo dokumentów, paserstwo programu komputerowego, zniesławienie lub zniewaga przy wykorzystaniu środków komunikacji elektronicznej, czy też tzw. pranie brudnych pieniędzy.

Natomiast w ocenie A. Adamskiego przestępstwo komputerowe w aspekcie karnoprocesowym wiąże się z faktem, iż system komputerowy może zawierać dowody działalności przestępnej[5]. Inaczej rzecz ujmując do kategorii przestępstw komputerowych można zaliczyć, wszelkie czyny zabronione przez prawo karne, gdzie ściganie następuje przy wykorzystaniu systemów teleinformatycznych jako takich.

W wyniku ostatnich nowelizacji polskie prawo karne materialne oraz procedura karna odpowiadają w dużej mierze standardom wyznaczonym przez ustawodawstwo unijne oraz *Konwencję o cyberprzestępczości*. Celem wprowadzonych zmian było zapewnienie wysokiego poziomu bezpieczeństwa teleinformatycznego. Zbudowanie bezpiecznego systemu i aplikacji jest warunkiem koniecznym efektywnego funkcjonowania elektronicznego rządu w Polsce. Aczkolwiek, mimo podejmowanych inicjatyw i trwających prac naukowo–badawczych z uwagi na złożoność i czasochłonność wielu spośród proponowanych procesów, luki zabezpieczeń stanowią jednak poważny i wymierny problem dla użytkowników sieci informatycznych.

---

4 Por. A. Adamski, *Nowa kodyfikacja karna. Kodeks karny. Krótkie komentarze. Zeszyt 17. Przestępstwa komputerowe w nowym kodeksie karnym,* Ministerstwo Sprawiedliwości. Departament Kadr i Szkolenia, Warszawa, 1998 r. s. 15 – 24 oraz A. Adamski, *Prawo karne komputerowe,* Warszawa, 2000 r., s. 30–34.

5 *Ibidem.*

1.2. Systematyka przestępstw komputerowych (Anna Zalesińska)

Międzynarodowa Organizacja Policji Kryminalnych „Interpol" przestępczość komputerową definiuje jako przestępczość w zakresie technologii komputerowych i dzieli ją na sześć obszarów[6], tj.

a) naruszanie praw dostępu do zasobów (w szczególności *hacking*, czyli nieupoważnione wejście do systemu informatycznego);

b) przechwytywanie danych; kradzież czasu, czyli korzystanie z systemu poza uprawnionymi godzinami; modyfikację zasobów przy pomocy bomby logicznej, konia trojańskiego, wirusa i robaka komputerowego,

c) oszustwa przy użyciu komputera (w szczególności oszustwa bankomatowe; fałszowanie urządzeń wejścia lub wyjścia, np. kart magnetycznych lub mikroprocesorowych; oszustwa na maszynach do gier; oszustwa poprzez podanie fałszywych danych identyfikacyjnych; oszustwa w systemach telekomunikacyjnych),

d) powielanie programów (w tym gier we wszelkich postaciach, innych programów komputerowych oraz topografii układów scalonych),

e) sabotaż zarówno sprzętu, jak i oprogramowania,

f) przechowywanie zabronionych prawem zbiorów.

Szczególne znaczenie dla omawianego zagadnienia ma *Konwencja o cyberprzestępczości*, w której zostały zdefiniowane minimalne standardy karalności opisanych w niej czynów. Przyjęta w niej systematyka bazuje na podziale na następujące kategorie:

a) przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów (nielegalny dostęp, nielegalne przechwytywanie danych, naruszenie integralności danych, naruszenie integralności systemu, niewłaściwe użycie urządzeń);

b) przestępstwa komputerowe (fałszerstwo komputerowe, oszustwo komputerowe);

c) przestępstwa ze względu na charakter zawartych informacji (przestępstwa związane z pornografią dziecięcą);

d) przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych.

Na potrzeby niniejszego opracowania została przyjęta systematyka za A. Adamskim[7]. W ramach kolejnych działów zostały scharakteryzowane poszczególne typy przestępstw komputerowych na tle regulacji polskiego kodeksu karnego.

---

6 Por. www.interpol.int

7 Por. A. Adamski, *Nowa kodyfikacja karna… Op. cit.* s. 25 – 167 oraz A. Adamski, *Prawo karne… Op. cit.* s. 35 – 136.

1.2.1. Przestępstwa komputerowe przeciwko ochronie informacji, w tym ingerencja w dane za pomocą nielegalnego oprogramowania (Przemysław Pęcherzewski)

1.2.1.1. *Hacking* (art. 267 § 1 k.k.)

W artykule 267 kodeksu karnego zostało stypizowane przestępstwo *hackingu*, nazywane „kradzieżą informacji". Przedmiotem ochrony jest prawo do swobodnego dysponowania informacją i jej poufność[8]. Wyróżnia się dwa typy tego czynu zabronionego.

Pierwszy polega na nieuprawnionym uzyskaniu dostępu do informacji nieprzeznaczonej dla sprawcy poprzez podłączenie się do sieci telekomunikacyjnej. Znamiona tego czynu są jasno określone i nie wymagają szerszego omówienia. W praktyce najczęściej czyn ten polega na fizycznym podłączeniu się do kabla sieci komputerowej lub innej, a także do sieci bezprzewodowej i uzyskaniu dostępu do odczytu lub zapisu danych przesyłanych w tej sieci.

Przykład 1: Jan Kowalski używając programu komputerowego uzyskuje dostęp do systemu operacyjnego lub pliku zabezpieczonego hasłem.

Drugi typ czynu polega na nieuprawnionym uzyskaniu dostępu do informacji nieprzeznaczonej dla sprawcy poprzez ominięcie albo przełamanie elektronicznych, magnetycznych, informatycznych lub innych szczególnych zabezpieczeń. Znamiona tego przestępstwa w najlepszy sposób odzwierciedlają zachowanie, które nazywa się w języku potocznym *hackingiem*.

Do ustawowych znamion należy uzyskanie bez uprawnień dostępu do zabezpieczonej informacji nieprzeznaczonej dla danej osoby. Wszelkie te znamiona muszą zostać spełnione łącznie.

Poprzez brak uprawnień należy rozumieć sytuację, kiedy sprawca uzyskuje dostęp do informacji wbrew woli osoby dysponującej tą informacją[9].

Jest to przestępstwo skutkowe. Skutkiem czynu nie jest sam fakt zapoznania się sprawcy z informacją, lecz do przypisania sprawstwa wystarczające jest uzyskanie przez sprawcę jedynie dostępu do tych informacji, czyli potencjalna możliwość zapoznania się z nią.

Dla bytu przestępstwa konieczne jest, aby informacja była zabezpieczona w sposób elektroniczny, magnetyczny lub informatyczny. Takim zabezpieczeniem będzie np. za-

---

8 Por. P. Kardas, *Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych,* „Czasopisma Prawa Karnego i Nauk Penalnych", Nr 1 z 2001 r., s. 61

9 *Op. cit*., s. 68, Definicję taką można odnaleźć w uchwale Sądu Najwyższego z dnia 22.01.2003 r., sygn. I KZP 43/02: istotą występku, o jakim mowa w art. 267 § 1 k.k., jest uzyskanie informacji dyskrecjonalnej, nie- przeznaczonej dla sprawcy (…). Dysponent informacji jest władny mniej lub bardziej szeroko określić krąg podmiotów dla których informacja jest przeznaczona. Każdy, kto spoza tego kręgu, uzyskałby takową informację, działaniem swoim wyczerpuje znamiona przestępstwa określonego w art. 267 § 1 k.k.

bezpieczenie hasłem dostępu do pliku, komputera, systemu operacyjnego czy też dysku twardego. Zabezpieczeniem będzie również kryptograficzne zaszyfrowanie pliku lub całości dysku.

Przykład 2: Jan Kowalski, wykorzystując program do łamania haseł, łamie hasło i uzyskuje dostęp do zabezpieczonej sieci bezprzewodowej. Poprzez podłączenie się kablem do sieci firmowej uzyskuje się dostęp do znajdujących się tam plików.

Nie będzie natomiast wyczerpywało znamion czynu zabronionego posłużenie się hasłem zdobytym w inny sposób niż wskutek przełamania zabezpieczeń, czyli np. odgadniętym, znalezionym w śmieciach, podpatrzonym w trakcie wpisywania przez inną osobę.

1.2.1.2. Nielegalny podsłuch i inwigilacja przy użyciu urządzeń technicznych (art. 267 § 2 i § 3 k.k.)

Istota czynu zabronionego stypizowanego w art. 267 § 1 k.k. sprowadza się do uzyskania przez sprawcę dostępu do informacji dla niego nieprzeznaczonej poprzez podłączenie się do sieci telekomunikacyjnej lub poprzez przełamanie albo ominięcie elektronicznych, magnetycznych, informatycznych lub innych szczególnych zabezpieczeń.

W § 2 stypizowany został czyn zabroniony polegający na nieuprawnionym uzyskaniu dostępu do całości lub części systemu teleinformatycznego.

Paragraf 3 art. 267 penalizuje zachowanie polegające na posłużeniu się przez sprawcę urządzeniem lub oprogramowaniem podsłuchowym w celu uzyskania informacji, do której sprawca nie jest uprawniony. Czyn karalny polega na założeniu lub posłużeniu się fizycznym lub programowym urządzeniem podsłuchowym. Czynność ta może polegać np. na podłączeniu urządzenia typu „*key-logger*" do klawiatury lub zainstalowaniu programu, który będzie logował aktywność użytkownika i zapisywał znaki wprowadzane za pomocą klawiatury lub rejestrował wszystkie lub tylko niektóre z wysyłanych danych. Odmiennie od czynów stypizowanych w § 1 i § 2, przestępstwo stypizowane w § 3 nie jest przestępstwem skutkowym[10].

1.2.1.3. Naruszenie integralności zapisu informacji (art. 268 § 1 k.k.)

W artykule 268 § 1 k.k. stypizowany został czyn zabroniony polegający na zniszczeniu, uszkodzeniu, usunięciu lub zmianie zapisu istotnej informacji.

Przedmiotem ochrony niniejszego przepisu jest integralność i bezpieczeństwo informacji przed ich naruszeniem ze strony osób trzecich. Jako szeroko pojmowany przedmiot ochrony wskazywana jest także dostępność informacji, rozumiana jako swoboda

---

[10] Maciej Szwarczyk, Aneta Michalska-Warias, Joanna Piórkowska-Flieger, Tadeusz Bojarski (red.) *Kodeks karny. Komentarz*, LexisNexis, Warszawa 2010 (wydanie IV).

dostępu do niej przez osoby uprawnione[11]. Zakresem § 1 objęte są informacje zapisane czy też utrwalone w każdy sposób, na dowolnym nośniku informacji.

W § 2 art. 286 stypizowany został typ zmodyfikowany czynu z § 1. Przepis § 2 przewiduje surowszą odpowiedzialność ze względu na rodzaj nośnika informacji, na którym zapisana jest informacja. Chodzi o informację zapisaną na **informatycznym nośniku danych**.

W kodeksie karnym brak jest ustawowej definicji tego pojęcia, a pierwotne brzmienie przepisu posługiwało się określeniem „komputerowego nośnika informacji". Definicję tego pojęcia odnaleźć można w art. 3 pkt 1 i 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[12], zgodnie z którym informatyczny nośnik danych to „*materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej lub analogowej"*. Urządzeniami takimi będą wszelkie optyczne i magnetyczne nośniki danych (np. płyty cd/dvd/Blue Ray/HDDVD, taśmy), magnetyczne i elektroniczne urządzenia zapisujące dane – dyski HDD, SDD, pen drive, karty pamięci.

Przykład: Grupa hakerów włamuje się na komercyjny serwer świadczący usługi multimedialne online i kradnie hasła oraz dane użytkowników, np. numery kart kredytowych. Po dokonaniu kradzieży kasowane są niektóre informacje, a inne zmieniane (zacieranie śladów poprzez kasowanie logów), w celu utrudnienia wykrycia sprawcy.

Z uwagi na brzmienie § 1 w doktrynie podnosi się, że zakresem penalizacji objęte będzie także posłużenie się przez sprawcę wirusem, robakiem czy bombą czasową, czyli programami, które mogą usuwać dane, modyfikować je lub utrudniać dostęp do informacji.

Przykład: Zwolniony z pracy pracownik, chcąc zemścić się na pracodawcy, wprowadza do jego komputera wirus, który kasuje dane.

1.2.1.4. Niszczenie lub utrudnianie dostępu do danych informatycznych (art. 268a k.k.)

Artykuł 268a został dodany do kodeksu karnego przez art 1 pkt 8 ustawy z dnia 14 marca 2004 r. zmieniającej kodeks karny z dniem 1 maja 2004 r.

Dokonując interpretacji przepisu, można wyróżnić dwa typy karalnych zachowań. Istota pierwszego z nich sprowadza się do nieuprawnionego zniszczenia, uszkodzenia, usunięcia, zmiany lub utrudniania dostępu do danych informatycznych, czyli sposób realizacji czynu jest niemalże identyczny jak w przypadku przepisu art. 268 § 1 k.k.,

---

11 A. Adamski, *Nowa kodyfikacja karna…*, *op. cit.*, s. 64.

12 Dz.U. z 2005 r. Nr 64, poz. 565.

przy czym przepis ten chroni każde dane, także te nie posiadające równie istotnego znaczenia co dane określone w poprzedzającym artykule.

Drugim rodzajem zachowania jest zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych.

1.2.1.5. Sabotaż komputerowy (art. 269 § 1 i k.k.)

Przepis art. 269 § 1 k.k. wprowadził kwalifikowany typ czynu zabronionego stypizowanego w art. 268 § 2 k.k.[13]

Od chwili wejścia w życie kodeksu karnego z 1997 r. artykuł ten był dwukrotnie zmieniany. Pierwsza zmiana dotyczyła poprawienia zakresu penalizacji, druga nastąpiła wskutek „uporządkowania" pojęć informatycznych w polskich ustawach w 2008 r.

Przedmiotem ochrony są szczególnego rodzaju informacje, mające istotne znaczenie dla funkcjonowania państwa, a w szczególności ich nienaruszalność, integralność i poufność.

Przedmiotem ochrony tego przepisu są dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego.

Jest to przestępstwo materialne, skutkowe, może zostać popełnione jedynie umyślnie. Stąd nie będzie możliwe przypisanie odpowiedzialności karnej osobom posiadającym komputery-zombi.

Przestępstwo można popełnić na dwa sposoby. Pierwszym z nich jest niszczenie, uszkodzenie, usunięcie lub zmiana danych informatycznych. Drugim sposobem działania sprawcy jest zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania takich danych, np. za pomocą ataku DDoS.

Kodeks karny nie zawiera definicji pojęcia „**dane informatyczne**". Zostało ono zdefiniowane w artykule 1 *Konwencji o cyberprzestępczości*. Poprzez dane informatyczne należy rozumieć „*dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny"*[14]. Słusznie podnosi się, że tłumaczenie to nie jest do końca trafne, a jego wykładnia może być problematyczna[15].

---

[13] P. Kardas, *Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych,* „Czasopisma Prawa Karnego i Nauk Penalnych", nr 1 z 2001 r., s. 95

[14] Tłumaczenie tekstu Konwencji dostępne pod adresem http://prawo.vagla.pl/skrypts/cybercrime_konwencja.htm

[15] Por. S. Bukowski, *Projekt zmian Kodeksu karnego – Dostosowanie do Konwencji o cyberprzestępczości, „*Gazeta Sądowa", nr 4/2004, s. 54–55

Dane informatyczne objęte zakresem przepisu muszą obiektywnie mieć szczególne znaczenie dla obronności, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego[16].

§ 2 penalizuje zachowanie polegające na dopuszczeniu się czynu określonego w § 1, poprzez niszczenie albo wymianę informatycznego nośnika danych lub niszczenie albo uszkodzenie urządzenia służącego do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych.

1.2.1.6. Zakłócanie pracy systemu komputerowego lub sieci teleinformatycznej (269a k.k.)

Przepis ten penalizuje zachowanie polegające na istotnym zakłóceniu pracy systemu komputerowego lub sieci teleinformatycznej poprzez nieuprawnioną transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych.

Przykładem takich czynów są ataki na komercyjne serwisy internetowe, które paraliżują lub spowalniają ich działanie lub uniemożliwiają wejście na daną stronę internetową.

Do wyczerpania znamion czynu konieczne jest zakłócenie funkcjonowania systemu albo sieci w stopniu istotnym.

1.2.1.7. Wytwarzanie lub udostępnianie urządzeń lub programów przystosowanych do popełnienia przestępstwa (269b k.k.)

Zakresem przepisu art. 269b zostały objęte zachowania polegające na wytwarzaniu, pozyskiwaniu, zbywaniu lub udostępnianiu innym osobom urządzeń lub programów komputerowych przystosowanych do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a, a także haseł komputerowych, kodów dostępu lub innych danych umożliwiających dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej.

Problemy interpretacyjne może stwarzać interpretacja pojęcia programu przystosowanego do popełnienia określonych przestępstw. Często bowiem przestępstwa te dokonywane są za pomocą „zwykłych" programów wykorzystywanych w codziennej pracy informatyków lub programistów.

---

[16] P. Kardas, *Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych,* „Czasopisma Prawa Karnego i Nauk Penalnych", nr 1 z 2001r., s. 95

1.2.2. Przestępstwa komputerowe przeciwko wiarygodności dokumentów, obrotowi gospodarczemu i pieniężnemu (Anna Zalesińska)

1.2.2.1. Pojęcie dokumentu elektronicznego na gruncie kodeksu karnego

Na gruncie doktryny i orzecznictwa ukształtowały się liczne koncepcje dotyczące potencjalnych możliwości zdefiniowania tego terminu, jednakże wciąż brak jest jednej powszechnie uznawanej i akceptowanej definicji. **Powszechnie jednak przyjmuje się bardzo szeroką definicję tego terminu, uwypuklając najważniejsze elementy tworzące „dokument", tj. materiał, na którym został sporządzony** (papier, drewno, elektroniczny nośnik informatyczny, itp.), **treść oświadczenia woli ujęta w postaci słownej** (tego wymogu nie spełniają pisma zakodowane, zaszyfrowane, z którymi druga strona nie może się zapoznać) **oraz podpis**, choć jest to kwestia sporna w literaturze[17]. Z uwagi na funkcjonalność, najbardziej adekwatną wydaje się być koncepcja przyjęta przez K. Piaseckiego[18]. Mianowicie pod pojęciem dokument, rozumie on każdy nośnik, na którym została utrwalona myśl człowieka, gdyż ta definicja pozostaje aktualna również w zdygitalizowanym świecie.

Z punktu widzenia prawa karnego materialnego, najważniejszym elementem dokumentu jest jego treść, a celem ochrony jest zapewnienie bezpieczeństwa obrotu prawnego poprzez dbałość o jego wiarygodność, stąd też wąski zakres definicji przyjętej w art. 115 § 14 k.k.

Dokumentem w rozumieniu kodeksu karnego jest każdy przedmiot lub inny zapisany nośnik informacji, z którym jest związane określone prawo albo który ze względu na zawartą w nim treść stanowi dowód prawa, stosunku prawnego lub okoliczności mającej znaczenie prawne.

1.2.2.2 Fałszerstwo komputerowe (art. 270 § 1 k.k.)

Istotą przestępstwa określonego w art. 270 k.k. jest karalne fałszowanie dokumentu lub używanie sfałszowanego dokumentu jako autentycznego. Celem ochrony jest zapewnienie zaufania do instytucji dokumentu, stąd też ustawodawca za karalne zachowania uznał zarówno jego podrabianie i przerabianie, jak i posługiwanie się tak sfałszowanym dokumentem, tj. zapewnienie ochrony przed fizycznym zamachem na jego autentyczność. Przedmiotem ochrony jest wiarygodność instytucji dokumentu, celem

---

17 Por. D. Szostek, *Czynność prawna a środki komunikacji elektronicznej,* Kraków, 2004 r., s. 231

18 Por. K. Piasecki, *Kodeks Postępowania Cywilnego. Komentarz.,* pod red. K. Piaseckiego, t. 1, Warszawa, 2001, s. 1023 – 1024.

zapewnienia ochrony obrotowi prawnemu i gospodarczemu[19]. Indywidualnym przedmiotem ochrony są interesy (dobra) konkretnego pokrzywdzonego, określone przez rodzaj i treść prawa, wyrażonego w dokumencie stanowiącym przedmiot określonego przestępstwa. Dobrem tym może być np. informacja, mienie, a nawet życie lub zdrowie.[20] Czyn zabroniony można popełnić na trzy sposoby, tj. podrabiając albo przerabiając dokument, bądź też używając tak sfałszowanego dokumentu, z tym, że dla karalności tego czynu nie jest istotne, czy taki dokument zawiera prawdziwe, czy fałszywe informacje[21]. Czyn zabroniony w zakresie fałszerstwa (podrabianie lub przerabianie) może popełnić każdy, ale wyłącznie z zamiarem bezpośrednim – kierunkowym, natomiast w zakresie używania sfałszowanego dokumentu jako autentycznego można popełnić umyślnie, z zamiarem bezpośrednim albo ewentualnym.

Regulacje to pozostają aktualne, także gdy przedmiotem omawianego czynu zabronionego jest dokument wytworzony w postaci elektronicznej, gdyż jak już wskazano na gruncie prawa karnego ochronie prawnej podlega dokument w szerokim tego słowa znaczeniu.

1.2.2.3. Zniszczenie lub pozbawienie mocy dowodowej dokumentu elektronicznego (art. 276 k.k.)

W rozumieniu art. 276 k.k. czynem zabronionym jest niszczenie, uszkadzania, czynienie bezużytecznym, ukrywanie lub usuwanie dokumentu przez osobę, która nie ma prawa wyłącznie nim rozporządzać (strona przedmiotowa). Analogicznie jak w przypadku art. 271 k.k. przedmiotem ochrony jest wiarygodność dokumentów, rozumiana jako dowodowa wartość dokumentów. Pod pojęciem dokumentu, którym „nie można wyłącznie rozporządzać" należy rozumieć nie tylko taki, który jest wyłącznie cudzy, ale również dokument urzędowy oraz dokument stwierdzający czyjeś uprawnienia i obowiązki (np. testament, weksel, czek, etc.), które istnieją jedynie w jednym egzemplarzu. Jest to przestępstwo powszechne, które można popełnić umyślnie, z zamiarem bezpośrednim albo ewentualnym.

W przypadku dokumentu utrwalonego w postaci elektronicznej przedmiotem ochrony jest nośnik danych, na którym został on utrwalony. Wskazać należy, że „dokument elektroniczny", w przeciwieństwie do „dokumentu tradycyjnego", może z łatwością zostać zwielokrotniony i zmodyfikowany, stąd też koniecznym jest zapewnienie

---

19 Wyroku Sądu Najwyższego z dnia 3 czerwca 1996 r., sygn. akt II KKN 24/96, „Prokuratura i Prawo", 1997 r., Nr 2, poz. 5.

20 Por. A. Wąsek, R. Zawłocki, *Kodeks karny. Część szczególna. Komentarz do art. 222–316. Tom II,* Warszawa, 2010 r.

21 Wyrok Sądu Najwyższego z dnia 26 października 1938 r., sygn. akt 1 K 2813/37, Zb. Orz. SN 1939, Nr 6, poz. 135.

jego wartości dowodowej przez wykorzystanie różnych metod kryptograficznych. W pozostałym zakresie regulacje zawarte w art. 276 k.k. stosuje się analogicznie.

1.2.2.4. Nierzetelne prowadzenie dokumentacji działalności gospodarczej (art. 303 k.k.)

Przepis ten określa przestępstwo, którego istotą jest wyrządzenie szkody przedsiębiorcy wskutek nieprawidłowego prowadzenia dokumentacji gospodarczej. Przedmiotem ochrony jest rzetelność i uczciwość informacji gospodarczych poprzez ochronę wiarygodności dokumentacji gospodarczej oraz majątkowych interesów przedsiębiorców, kontrahentów i pozostałych uczestników obrotu. Zachowanie sprawcy polega na wyrządzeniu szkody wskutek braku prowadzenia dokumentacji działalności gospodarczej bądź prowadzenie jej w sposób nierzetelny lub niezgodny z prawem. Pod pojęciem „dokumentacji" należy rozumieć każdą formę zapisu dokumentującą działalność gospodarczą prowadzoną w celach podatkowych, statystycznych, ewidencyjnych i informacyjnych (np. księgi rachunkowe, księgi przychodów i rozchodów, rejestry, ewidencje, faktury, w tym faktury elektroniczne). Podmiotem może być każda osoba fizyczna, która zobowiązała się do prowadzenia dokumentacji działalności gospodarczej na rzecz przedsiębiorcy. Rozważany czyn zabroniony może zostać popełniony tylko umyślnie, z zamiarem bezpośrednim albo ewentualnym.

1.2.2.5. Fałszerstwo kart płatniczych (art. 310 k.k.)

Przedmiotem ochrony art. 310 k.k. jest system gospodarczy, a dokładniej jego najistotniejszy element, tj. środki płatnicze. Tym samym jego celem jest zapewnienie zaufania do autentyczności wszelkich znajdujących się w obrocie środków płatniczych. Jako działania przestępne rozumie się podrabianie, przerabianie lub usuwanie oznaki umorzenia, bez względu na to, czy dany środek płatniczy został użyty jako autentyczny bądź też, czy z tego tytułu sprawca osiągnął jakiekolwiek korzyści materialne. Jest to przestępstwo powszechne umyślne.

Pod pojęciem karty płatniczej należy rozumieć kartę identyfikującą wydawcę i upoważnionego posiadacza, uprawniającą do wypłaty gotówki lub dokonywania zapłaty, a w przypadku karty wydanej przez bank lub instytucję ustawowo upoważnioną do udzielania kredytu – także do dokonywania wypłaty gotówki lub zapłaty z wykorzystaniem kredytu[22].

Fałszerstwo kart płatniczych może polegać z jednej strony na zeskrobaniu danych (numeru karty, daty ważności itp.) z oryginalnej karty i naklejeniu ich na falsyfikat karty,

---

[22] Art. 4 pk3 Ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2002 r., nr 72, poz. 665 t. j.).

na sprasowaniu karty i ponownym wytłoczeniu numeru karty, daty ważności i innych danych ograniczających ważność karty[23], ale także na manipulowaniu zapisem na ścieżce magnetycznej. J. Jakubski wyróżnia cztery postaci fałszerstwa kart płatniczych, tj. podrobienie, przerobienie, całkowite sfałszowanie oraz fałszerstwo elektroniczne[24].

1.2.3. Przestępstwa komputerowe przeciwko mieniu (Przemysław Pęcherzewski)

1.2.3.1. Nieuprawnione uzyskanie programu komputerowego (art.278 § 2 k.k.)

W § 2 art. 278 k.k. penalizującego kradzież stypizowany został czyn zabroniony o innych znamionach, polegający na uzyskaniu cudzego programu komputerowego. Podobnie jak przestępstwo kradzieży jest to przestępstwo kierunkowe, materialne. Nie polega ono jednak na fizycznym pozbawieniu władztwa nad rzeczą drugiej osoby, ze względu na okoliczność, że przedmiotem ochrony przepisu są majątkowe prawa autorskie[25] osoby uprawnionej. W prawie polskim programy komputerowe podlegają ochronie jak utwory.

Do ustawowych znamion przepisu należy uzyskanie cudzego programu komputerowego bez zgody osoby uprawnionej w celu osiągnięcia korzyści majątkowej.

Chwilą dokonania czynu jest „*moment nieuprawnionego zdobycia – zapisania na nośniku danych*[26]" programu komputerowego.

Duże problemy interpretacyjne sprawia znamię „uzyskania" programu. Według M. Skwarzyńskiego uzyskanie programu może polegać także na „*zastosowaniu programu crack i uzyskaniu dostępu do pełnej wersji programu*". Taka interpretacja, mimo iż może wynikać z dyrektyw wykładni celowościowej, wydaje się być słuszna, jednakże wychodzi ona poza ustawowe znamiona czynu, poszerzając jego zakres o znamiona „uzyskania dostępu do programu".

1.2.3.2. Paserstwo programu komputerowego (art. 293 § 1 k.k.)

Przestępstwo paserstwa programu komputerowego zostało określone w art. 293 § 1 k.k., który stanowi, że przepisy art. 291 i 292 (czyli dotyczące umyślnego i nieumyślnego paserstwa) stosuje się odpowiednio do programu komputerowego. Oznacza to, że paserstwo programu komputerowego będzie polegało na nabyciu, pomocy do

---

23 J. Jakubski, *Przestępstwa związane z użyciem kart,* „Prawo bankowe", 1994 r., nr 2, s. 83 – 92.

24 *Ibidem.*

25 M. Skwarzyński, *Przestępstwo uzyskania programu komputerowego- art. 278§2 k.k.,* Palestra 3/2010, s. 36

26 *Op. cit.* s. 41

zbycia, przyjęciu lub pomocy w ukryciu programu komputerowego uzyskanego za pomocą czynu zabronionego, czyli czynu stypizowanego w art. 278 § 2 k.k[27]. *„Przypisanie indywidualnej odpowiedzialności wymaga wykazania osobie podejrzanej, że cechy programu lub okoliczności, w jakich doszło do jego uzyskania, powinny były wywołać w niej wątpliwość co do trafności przekonania o legalnym pochodzeniu tego programu”*[28].

1.2.3.3. Oszustwo komputerowe (art. 287 k.k.)

Istotą oszustwa komputerowego jest działanie polegające na nieuprawnionym wpływaniu na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmianie, usunięciu albo wprowadzeniu nowego zapisu danych informatycznych. Zachowanie to musi zostać podjęte w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody. Cechą odróżniającą standardowe oszustwo od oszustwa komputerowego jest przedmiot wykonawczy czynu. Sprawca oszustwa komputerowego nie wprowadza w błąd („nie oszukuje”) innej osoby, ale w celu uzyskania korzyści majątkowej lub wyrządzenia szkody wpływa na sposób działania oprogramowania lub systemu komputerowego, czyli, używając języka potocznego, „oszukuje” system komputerowy[29].

Jest to przestępstwo kierunkowe, formalne i nie wymaga, aby działaniem swoim sprawca wyrządził innej osobie szkodę lub uzyskał korzyść majątkową[30]. Może być popełnione jedynie w zamiarze bezpośrednim, zabarwionym.

Przykład: Sprawca, wykorzystując luki w systemie zabezpieczeń, uzyskuje dostęp do płatnych zasobów danego serwisu.

1.2.3.4. Oszustwo telekomunikacyjne (art. 285 k.k.)

Przepis artykułu 285 k.k. penalizuje zachowanie polegające na włączeniu się do urządzenia telekomunikacyjnego i uruchomieniu na cudzy rachunek impulsów telefonicznych. Czynność ta nazywana jest *phreaking.* Obecnie przepis ten stracił na znaczeniu, gdyż do jego znamion należy „uruchomienie impulsów telefonicznych”, które to pojęcie dotyczyło jedynie funkcjonowania analogowych systemów telefonicznych, przewidujących impulsowy sposób wybierania numeru. Obecnie dominuje tonowy lub cyfrowy system wybierania numerów telefonicznych, a zasady naliczania opłat za połą-

---

27 Por. A. Adamski, *Nowa kodyfikacja karna…*, *op. cit*,. s. 111

28 A. Adamski, *Nowa kodyfikacja karna…*, *op. cit.* s., 114

29 Por. A. Adamski, *Nowa kodyfikacja karna…*, *op. cit*,. s. 115.

30 A. Marek, *Prawo karne*, 4 wydanie, CH Beck, Warszawa 2003, s. 552.

czenie telefoniczne nie przewidują naliczania opłat na zasadzie impulsów, lecz są uzależnione od czasu połączenia i wybranego numeru[31].

Obecnie „oszustwo telekomunikacyjne" może polegać np. na klonowaniu kart sim w celu wykorzystania telefonu na koszt innej osoby[32].

1.2.4. Inne typy przestępstw (Anna Zalesińska)

1.2.4.1. Szpiegostwo komputerowe (art. 130 § 3 k.k.)

Przedmiotem ochrony jest bezpieczeństwo zewnętrzne (niepodległość, integralność terytorialna, ustrój konstytucyjny, podstawy bezpieczeństwa, etc.). Popełnić ten czyn może każdy, zarówno Polak, jak i cudzoziemiec oraz apatryda, jeżeli jest współpracownikiem obcego wywiadu bądź też przekazuje mu wiadomości, które mogą wyrządzić szkodę Rzeczypospolitej Polskiej. Kwalifikowaną postacią tego przestępstwa jest prowadzenie lub kierowanie działalnością obcego wywiadu.

Zgodnie z art. 130 § 3 k.k. karalnym jest również udzielenia obcemu wywiadowi wiadomości, których przekazanie może wyrządzić szkodę Rzeczypospolitej Polskiej, gromadzenie ich lub przechowywanie, a także wchodzenie do systemu informatycznego w celu ich uzyskania albo zgłaszanie gotowości działania na rzecz obcego wywiadu przeciwko Rzeczypospolitej Polskiej. Przestępstwo takie może być popełnione w dwojaki sposób, tj. poprzez uzyskanie programu komputerowego przez skopiowanie go na nośnik należący do sprawcy lub przez zabór nośnika, na którym został utrwalony. Po skopiowaniu programu komputerowego przez sprawcę program ten nadal pozostaje we władztwie pokrzywdzonego i właśnie ten charakterystyczny element dla tej odmiany przestępstwa nie pozwala na traktowanie go jako „zwykłej kradzieży"[33].

1.2.4.2. Sprowadzenie niebezpieczeństwa powszechnego (art. 165 k.k.)

Przedmiotem ochrony jest bezpieczeństwo powszechne. Zachowanie sprawcy musi wywołać określone, konkretne i dające się udowodnić niebezpieczeństwo dla chronionego dobra prawnego (przestępstwo skutkowe)[34]. Jest to przestępstwo powszechne, które może być popełnione umyślnie, jak i nieumyślnie. Regulacja ta, w szczególności art. 165 § 1 pkt 4, została sformułowana w bardzo elastyczny sposób, stąd też penalizacji podle-

---

31 *Op. cit,.* s. 128-129.

32 „Wprost", Nr 34/2008 (1339), artykuł dostępny pod adresem http://www.wprost.pl/ar/136520/Podsluch-totalny/

33 Por. A. Adamski, *Nowa kodyfikacja karna… op. cit.,* s. 157-162.

34 Wyrok Sądu Najwyższego z dnia 12 czerwca 1987 r., sygn. akt III KR 205/87, OSNPG 1988, Nr 8, poz. 79.

ga jakakolwiek działalność, której celem jest sprowadzenie niebezpieczeństwa powszechnego, również przy wykorzystaniu sieci informatycznych.

1.2.4.3. Pornografia dziecięca (art. 202 k.k.)

Uzasadnieniem wprowadzenia zakazu z art. 202 § 1 k.k. jest ochrona wolności indywidualnej człowieka. Prezentacja treści pornograficznych w Internecie bez wątpienia odbywa się publicznie, o czym mówi art. 202 § 1 k.k., a umieszczanie takich treści na stronach internetowych lub w innych miejscach, a nawet wszelkie inne wprowadzenie takich treści do ogólnie dostępnej sieci, wyczerpuje znamiona rozpowszechniania i udostępniania. Penalizowana jest jedynie taka działalność, która narzuca odbiór treści z góry, stąd też na twórcach witryn internetowych spoczywa obowiązek zabezpieczania ich poprzez stosowanie odpowiednich komunikatów, takich jak prośba o potwierdzenie pełnoletniości bądź informacja, że dana strona zawiera treści o charakterze pornograficznym. Natomiast celem regulacji przewidzianej w art. 202 § 2 k.k. jest zapewnienie ochrony małoletnim poniżej 15 roku życia przed treściami o charakterze pornograficznym poprzez stosowanie odpowiednich mechanizmów zabezpieczających. W przypadku Internetu może to być wymóg podania numeru karty kredytowej. Kolejne paragrafy penalizują zachowanie polegające na produkcji, utrwalaniu lub sprowadzaniu, przechowywaniu lub posiadaniu, rozpowszechnianiu lub publicznym prezentowaniu treści pornograficznych z udziałem małoletniego (lub zawierające wytworzony lub przetworzony wizerunek małoletniego) albo treści pornograficznych związanych z prezentowaniem przemocy lub posługiwaniem się zwierzęciem.

W kontekście omawianej regulacji pojawia się dość istotne zagadnienie odpowiedzialności administratorów serwerów oraz osób prowadzących katalogi stron internetowych. W takiej sytuacji odpowiedzialność właściciela jest ograniczona jedynie do przypadków, kiedy świadomie udostępnia on usługę do takich właśnie celów. Podobnie nie odpowiadają sieci telekomunikacyjne, a także osoby, które umożliwiają dostęp do nich.

2. Cyberterroryzm (Piotr Rodziewicz)

Jednym z zagrożeń związanych z funkcjonowaniem cyberprzestrzeni jest cyberterroryzm. Jak wskazuje się cyberterroryzm, czyli terroryzm wymierzony przeciwko newralgicznym dla państwa systemom, sieciom i usługom teleinformatycznym jest zagrożeniem o coraz większym znaczeniu[35]. W istocie brak jest jednej powszechnie

[35] Zob. Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011. Założenia, Warszawa, marzec 2009, str. 4 – http://www.cert.gov.pl/portal/cer/30/Rzadowy_program_ochrony_cyberprzestrzeni.html.

przyjmowanej definicji cyberterroryzmu[36]. Zgodnie z jedną z definicji cyberterroryzm jest 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"*[37]. Przedmiotem wyżej wymienionego ataku może być m.in. krajowa infrastruktura krytyczna[38], a atak ten, jak już zostało wskazane, nie ma charakteru konwencjonalnego, ale pochodzi z cyberprzestrzeni. Infrastruktura krytyczna może stać się celem potencjalnego ataku z uwagi na jej kluczowe znaczenie dla państwa, m.in. dla jego gospodarki, bezpieczeństwa itp. Definicję legalną infrastruktury krytycznej można odnaleźć w ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2007 r. Nr 89, poz. 590 z późn. zm.)[39]. Zgodnie z postanowieniami art. 3 pkt 2 powyższej ustawy przez infrastrukturę krytyczną należy rozumieć systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców.Infrastruktura krytyczna obejmuje systemy:

a) zaopatrzenia w energię i paliwa,
b) łączności i sieci teleinformatycznych,
c) finansowe,
d) zaopatrzenia w żywność i wodę,
e) ochrony zdrowia,
f) transportowe i komunikacyjne,
g) ratownicze,
h) zapewniające ciągłość działania administracji publicznej,
i) produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Znaczna część powyższej infrastruktury w ramach działalności korzysta ze środków komunikacji elektronicznej. Jako przykład można wskazać instytucje rynku finansowego, takie jak banki, giełda, czy też infrastruktura transportowa, np. lotniska, też jak również organy administracji publicznej świadczące usługi dla obywateli drogą elektro-

---

36 Zob. T. Szubrycht, „*Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*", Zeszyty Naukowe Akademii Marynarki Wojennej, Rok XLVI, nr 1 (160), 2005, str. 175 i n.www.amw.gdynia.pl/library/File/ZeszytyNaukowe/2005/Szubrycht_T.pdf; Zob. J. E. Mehan, „*Cyberwar, Cyberterror, Cybercrime*", 2008, str. 32.

37 T. Szubrycht, *op. cit.*, str. 175.

38 W.K. Clark, P.L. Levin, "*Securing the Information Highway. How to Enhance the United States' Electronic Defenses*" [w:] Foreign Affairs, November/December 2009, str. 4.

39 Dalej zwana w niniejszym opracowaniu ustawą o zarządzaniu kryzysowym.

niczną. W związku z powyższym narażona jest ona na niebezpieczeństwo ataków pochodzących z cyberprzestrzeni. Jak wskazuje się, ataki pochodzące z cyberprzestrzeni stanowią szczególnego rodzaju zagrożenia ze względu na potencjalne szkody, jakie mogą za sobą nieść[40]. Zgodnie z definicją zawartą w założeniach *Rządowego programu ochrony cyberprzestrzeni RP na lata 2009-2011* przez cyberprzestrzeń państwa należy rozumieć „*przestrzeń komunikacyjną tworzoną przez system wszystkich powiązań internetowych znajdujących się w obrębie państwa*"[41]. O tym, że cyberterroryzm nie stanowi problemu tylko i wyłącznie teoretycznego, ale jest realnym zagrożeniem, świadczą liczne ataki hakerów na infrastrukturę krytyczną. Jakoprzykład można wskazaćatak przeprowadzony w dniach od 27 kwietnia do 11 maja 2007 r. w Estonii, gdzie zaatakowane zostały strony internetowe rządu, kancelarii prezydenta, głównych gazet, banków, a także wewnętrzna sieć estońskiej policji[42], czy też atak z lutego 2000 r., kiedy to unieruchomione zostały m.in. serwery CNN, eBay, Yahoo[43]. Incydenty w sieci również dotknęły witryny internetowe działające w polskiej cyberprzestrzeni, niemniej jednak nie miały one charakteru tak zmasowanego, jak wymienione powyżej[44].

W celu ochrony jednostek administracji publicznej przed atakami w cyberprzetrzeni został z dniem 1 lutego 2008 r. powołany do życia Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL[45]. Zespół CERT.GOV.PL funkcjonuje w ramach Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego (ABW)[46]. Ponadto w dniu 9 marca 2009 r. Komitet Stały Rady Ministrów przyjął dokument *Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011 – założenia*[47]. Co do zasady zadaniem programu jest zwiększenie poziomu bezpieczeństwa w cyberprzestrzeni państwa. Założenie to ma być realizowane za pomocą szeregu zadań szczegółowych[48].

---

40 W.K. Clark, P.L. Levin, *op. cit.*, str. 4.

41 Rządowy… *op. cit.*, str. 4.

42 Biuro Bezpieczeństwa Narodowego, oprac. S. Moćkun, „*Terroryzm cybernetyczny – zagrożenia dla bezpieczeństwa narodowego i działania amerykańskiej administracji*", Warszawa, lipiec 2009, str. 4, http://www.bbn.gov.pl/download.php?s=1&id=2359.

43 *Ibidem*, str. 3.

44 Zob. Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2010, Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, str. 35 i n.,http://www.cert.gov.pl/portal/cer/57/Raporty_o_stanie_bezpieczenstwa_cyberprzestrzeni_RP.html.

45 Zob. http://www.cert.gov.pl/portal/cer/27/15/O_nas.html.

46 *Ibidem*.

47 http://www.mswia.gov.pl/portal/pl/2/6966/Zalozenia_do_Rzadowego_programu_ochrony_cyberprzestrzeni_RP_na_lata_20092011.html.

48 Zob. zadania szczegółowe: Rządowy… *op. cit.*, str. 5 i n.

Podsumowując, cyberterroryzm jest jednym z zagrożeń związanych z funkcjonowaniem Internetu. Z uwagi na dotkliwe konsekwencje, jakie mogą spowodować ataki w cyberprzestrzeni wydaje się, że w celu przeciwdziałania tej negatywnej aktywności powinny zostać podjęte prace nad stworzeniem odpowiednich ram prawnych umożliwiające skuteczną walkę z tym zjawiskiem, ale także, co najważniejsze, umożliwiające podejmowanie działań prewencyjnych chroniących przed atakami w cyberprzestrzeni. Prace takie już się toczą w ramach wyżej wskazanego programu rządowego, którego jednym z zadań jest m. in. zdefiniowanie z prawnego punktu widzenia zjawiska cyberterroryzmu oraz prawne uregulowanie zasad ochrony krytycznej infrastruktury teleinformatycznej[49].

[49] Zob. *Ibidem*, str. 8.