CBKE
e-BIULETYN

Przestępstwa skierowane przeciwko poufności, integralności i dostępności danych oraz systemów komputerowych w polskim kodeksie karnym - z uwzględnieniem aktualnych zmian nowelizacyjnych

Piotr Siemkowicz

- artykuł jest zmodyfikowanym fragmentem rozdziału mojej pracy doktorskiej pisanej pod kierownictwem prof. Dr hab. Marka Bojarskiego o tytule „Przestępstwa popełniane za pośrednictwem sieci Internet"

Z pośród wszystkich przestępstw popełnianych za pośrednictwem sieci Internet, najbardziej uciążliwymi dla użytkowników sieci, jest grupa działań o charakterze przestępczym, których głównym, a często jedynym celem jest spowodowanie uszkodzenia bądź zniszczenia innych systemów informatycznych oraz pokonanie zabezpieczeń innych komputerów. Niebagatelne znaczenie mają zwłaszcza działania nakierowane przeciwko poufności danych i informacji zawartych w systemach informatycznych albowiem informacje i dane przechowywane i chronione w tych systemach mają często z punktu widzenia strategii dysponujących nimi korporacji i podmiotów wartość znacznie większą niż same systemy komputerowe.

Tego rodzaju działania określić możemy w uproszczeniu hackingiem, mając zarazem świadomość, że w grupie tej pomieścić można wiele rodzajów zachowań przestępczych, w zależności od przyjętego przez sprawcę (*hackera*) sposobu działania oraz celu jaki działaniem tym zamierza osiągnąć. W szczególności do czynów takich w polskim kodeksie karnym po zasadniczej nowelizacji dokonanej ustawą z dnia 24 października 2008 r. o zmianie ustawy kodeks karny oraz niektórych innych ustaw (Dz. U. z 2008 r. Nr 214, poz. 1344), zaliczyć możemy czyn z art. 267 § 1 kk (hacking *sensu stricte*), art. 267 § 2 kk (czysty dostęp do systemu informatycznego), podsłuch komputerowy z art. 267 § 3 kk, bezprawną ingerencję w zapis informacji w celu udaremnienia lub znacznego utrudnienia zapoznania się z tą informacją przez uprawnioną osobę – art. 268 § 1 i § 2 kk, sabotaż komputerowy – czyli zamach na dostępność elektronicznie przetwarzanej informacji – art. 268 a § 1 i § 2 kk oraz art. 269 a kk [1]. Polski kodeks karny w art. 269 b § 1 kk przewiduje także kryminalizację wytwa-

[1] A. Adamski, Cyberprzestępczość – aspekty prawne i kryminologiczne, Studia Prawnicze – Kwartalnik, nr 4/2005, s. 54 – 61;

rzania, pozyskiwania, zbywania oraz udostępniania innym osobom urządzeń lub programów komputerowych przystosowanych do popełniania czynów z art. 165 § 1 pkt 4 kk, art. 267 § 3 kk, art. 268 a § 1 lub § 2 kk w zw. z § 1, art. 269 § 2 kk albo z art. 269 a kk, a także haseł komputerowych, kodów dostępu lub innych danych umożliwiających dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej. Tym samym przepis art. 269 b § 1 kk wprowadzony jeszcze przy nowelizacji kodeksu karnego z 18 marca 2004 r. (Dz. U. Nr 69, poz. 626), a zmieniony także w ramach ostatniej nowelizacji z 24 października 2008 r., przewidział w polskim prawie karnym kryminalizację tzw. narzędzi hackerskich [2].

W zakresie możliwości ścigania czynów z art. 267 § 1 – 4 kk, art. 268 § 1 – 3 kk oraz art. 268 a § 1 – 2 kk obowiązuje w Polsce także tryb wnioskowy, co oznacza, że przestępstwa te ścigane są dopiero na wniosek pokrzywdzonego.

W tym miejscu należy podkreślić, iż nowelizacja dokonana ustawą z dnia 24 października 2008 r. – głównie w zakresie dotyczącym przestępstw z art. 267 § 1 i § 2 kk, a także czynu z art. 269 a kk, jest wynikiem dostosowania (implementacji) polskiego prawa karnego w tym zakresie do Decyzji Ramowej Rady Unii Europejskiej z dnia 24 lutego 2005 r., w sprawie ataków na systemy informatyczne (2005/222/WSiSW) [3]. W szczególności wskazana Decyzja Ramowa zobowiązała państwa członkowskie do podjęcia niezbędnych środków w celu kryminalizacji następujących zachowań:

1. nielegalnego dostępu do systemów informatycznych – polegającego na umyślnym, bezprawnym dostępie do całości lub części systemu informatycznego, przy czym zastrzeżono, iż kryminalizacja w tym zakresie powinna obejmować przynajmniej przypadki które nie są wypadkami mniejszej wagi. Dodatkowo wskazano, iż każde państwo może zdecydować, że zachowania dotyczące nielegalnego dostępu do systemów informatycznych będą objęte oskarżeniem jedynie w przypadkach, gdy przestępstwo popełniane jest z naruszeniem zabezpieczenia (art. 2 ust 1 i 2);
2. nielegalnej ingerencji w system – polegającej na umyślnym, poważnym naruszeniu lub przerwaniu funkcjonowania systemu informatycznego poprzez wprowadzanie, przekazywanie, uszkadzanie, usuwanie, niszczenie, zmienianie, zatajanie lub uczynienie niedostępnymi danych komputerowych – kiedy dokonane jest bezprawnie, przynajmniej w wypadkach, które nie są przypadkami mniejszej wagi (art. 3);
3. nielegalnej ingerencji w dane – mającej postać umyślnego, bezprawnego usunięcia, uszkodzenia, pogorszenia, zmiany, zatajania lub uczynienia niedostępnymi danych komputerowych w systemie informatycznym – kiedy dokonywane jest bezprawnie, przynajmniej w przypadkach, które nie są przypadkami mniejszej wagi (art. 4);
4. kierowania, pomagania, podżegania oraz usiłowania w zakresie czynów określonych w art. 2, 3 i 4 Decyzji Ramowej (art. 5), z tym, iż każde państwo członkowskie zostało uprawnione do zadecydowania o ewentualnej niekaralności usiłowania popełniania czynów o których mowa w art. 2 – a więc polegających na uzyskaniu nielegalnego dostępu do systemów informatycznych.

Przedmiotowa Decyzja Ramowa zakreśliła także ramy wysokości sankcji karnych za poszczególne przestępstwa – zobowiązując państwa do zastosowania wskazanych przez siebie granic karalności w tym zakresie. W szczególności więc w zakresie czynów mających postać nielegalnej ingerencji w system oraz nielegalnej ingerencji w dane Decyzja Ramowa przewidziała zastosowanie kar od 1 roku do 3 lat pozbawienia wolności (art. 6 ust 2). W art. 7 ust 1 przewidziano natomiast tzw. okoliczności obciążające, przy czym przepis ten zobowiązał państwa członkowskie do surowszego traktowania czynów określonych w art. 2, 3 i 4 w sytuacji gdy zostały one popełnione w ramach organizacji przestępczej, a w szczególności przyjęcia granic ustawowego zagrożenia w takim wypadku od 2 do 5 lat pozbawienia wolności.

[2] A. Adamski, Cyberprzestępczość – aspekty prawne i kryminologiczne, op. Cit., s. 60 – 61;

[3] Decyzja Ramowa Rady Unii Europejskiej z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne – 2005/222/WSiSW, dostępna na stronie internetowej: http://www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:PL:PDF;

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

Przestępstwa o charakterze *hackingu* uprzednio wyszczególnione zostały także w art. 2 – 6 Konwencji Rady Europy o cyberprzestępczości (Convention on Cybercrime, CETS No.: 185, opening of the treatry 23.11.2001 r., entry into force 01.07.2004 r.) [4] - pod wspólną nazwą zawartą w tytule 1 „przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów". Konwencja o cyberprzestępczości zobowiązała przy tym państwa – strony do podjęcia niezbędnych środków prawnych zmierzających do uznania za przestępstwa w ich prawie wewnętrznym:

1. nielegalnego dostępu – polegającego na umyślnym, bezprawnym dostępie do całości lub części systemu informatycznego, przy czym strony zostały uprawnione do wprowadzenia wymogu, że przestępstwo to musi zostać popełnione poprzez naruszenie zabezpieczeń z zamiarem pozyskania danych informatycznych lub z innym nieuczciwym zamiarem, lub w odniesieniu do systemu informatycznego, który jest połączony z innym systemem informatycznym (art. 2);
2. nielegalnego przechwytywania danych – polegającego na umyślnym, bezprawnym przechwytywaniu za pomocą urządzeń technicznych, niepublicznych transmisji danych informatycznych „do", „z" lub w ramach systemu informatycznego, łącznie z emisjami elektromagnetycznymi pochodzącymi z systemu informatycznego przekazującego takie dane informatyczne. Strony zostały także uprawnione do wprowadzenia wymogu, że przestępstwo to musi zostać popełnione z nieuczciwym zamiarem lub w związku z systemem informatycznym, który jest połączony z innym systemem informatycznym (art. 3);
3. naruszenia integralności danych – polegającego na umyślnym i bezprawnym niszczeniu, wykasowywaniu, uszkadzaniu, dokonywaniu zmian lub usuwaniu danych informatycznych, przy czym strony zostały uprawnione do zastrzeżenia wymogu zaistnienia dodatkowo poważnej szkody na skutek przedmiotowych działań (art. 4);
4. naruszenia integralności systemu – polegającego na umyślnym i bezprawnym poważnym zakłócaniu funkcjonowania systemu informatycznego poprzez wprowadzanie, transmisję, niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie danych informatycznych (art. 5);
5. niewłaściwego użycia urządzeń – polegającego na umyślnym i bezprawnym produkowaniu, sprzedaży, pozyskiwaniu z zamiarem wykorzystania, importowaniu, dystrybucji lub innym udostępnianiu:
   - urządzenia, w tym także programu komputerowego, przeznaczonego lub przystosowanego przede wszystkim dla celów popełnienia któregokolwiek z przestępstw określonych zgodnie z art. 2 – 5;
   - hasła komputerowego, kodu dostępu lub podobnych danych, dzięki którym całość lub część systemu informatycznego jest dostępna, z zamiarem wykorzystania dla celów popełnienia któregokolwiek z przestępstw określonych zgodnie z art. 2 – 5.

W art. 6 pkt b Konwencja o cyberprzestępczości przewidziała przy tym kryminalizację samego posiadania wskazanych powyżej narzędzi hackerskich a więc – programów komputerowych, haseł komputerowych, kodów dostępu lub podobnych danych, z zamiarem ich wykorzystania w celu popełnienia któregokolwiek z przestępstw określonych zgodnie z art. 2 – 5. Dodatkowo zastrzeżono jednak, iż strona może wprowadzić w swoim prawie wewnętrznym wymóg, iż odpowiedzialność karna dotyczyć będzie posiadania jedynie większej ilości takich jednostek (narzędzi hackerskich). Także istotnym jest zastrzeżenie zawarte w art. 6 ust 2, iż niniejszych przepisów nie należy interpretować jako mających na celu pociągnięcia do odpowiedzialności karnej w przypadku, gdy produkcja, sprzedaż, pozyskiwanie z zamiarem wykorzystania, importowanie, dystrybucja lub inne udostępnianie lub posiadanie wskazanych jednostek, nie jest dokonywane w celu popełnienia przestępstw określonych w art. 2 – 5, jak też w przypadku dozwolonego testowania lub ochrony systemu informatycznego.

[4] Konwencja Rady Europy z dnia 23.11.2001 r. o cyberprzestępczości, tekst Konwencji dostępny pod adresem http://www.vagla.pl/skrypts/cybercrime_konwencja.html oraz http://conventions.coe.int;

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

W praktyce mówić możemy przy tym o trzech modelach kryminalizacji działań hackerskich. Zgodnie ze stanowiskiem P. Kardasa [5] w przypadku pierwszego - najszerszego modelu, kryminalizacji podlega samo przełamanie zabezpieczeń oraz wdarcie się przez hackera do systemu komputerowego, przy czym nie jest tutaj istotny faktyczny cel działania sprawcy, a w szczególności czy rzeczywiście wejdzie on w posiadanie informacji zgromadzonych w tym systemie, lecz istotne jest samo narażenie zgromadzonych w systemie informacji i danych na niebezpieczeństwo.

W drugim – węższym zakresowo modelu, zakłada się natomiast karalność wdarcia się do systemu komputerowego bezpośrednio w celu uzyskania zgromadzonych tam informacji. Tym samym sprawca przestępstwa hackingu musi działać w zamiarze bezpośrednim oraz być nastawiony kierunkowo na zdobycie informacji znajdujących się w systemie komputerowym.

Trzeci model – najwęższy zakłada natomiast, iż do przestępstwa dojdzie dopiero w przypadku faktycznego wdarcia się sprawcy do systemu komputerowego poprzez przełamanie szczególnych zabezpieczeń – np. w postaci hasła, a także działaniom sprawcy musi towarzyszyć fakt rzeczywistego uzyskania konkretnych informacji zawartych w systemie. Tym samym zdaniem P. Kardasa (w rozumieniu trzeciego modelu kryminalizacji hackingu) nawet gdyby doszło do włamania do systemu jednakże sprawca nie uzyskałby w jego wyniku informacji w nim zawartych – nie można mówić o przestępstwie o charakterze hackingu [6].

A. Adamski odmiennie od P. Kardasa, wyodrębnia natomiast jedynie dwa główne modele w zakresie kryminalizacji hackingu [7]. W szczególności pierwszy – restrykcyjny model, reprezentatywny dla krajów anglosaskich (USA – Floryda, Australia – Wiktoria, Wielka Brytania), zakłada ochronę samej nienaruszalności systemu komputerowego. W modelu tym karaniu podlega każda forma uzyskania nieuprawnionego dostępu do cudzego systemu komputerowego, niezależnie od tego czy związane to było z pokonaniem przez sprawcę zabezpieczeń dostępu do tego systemu, czy też nie.

Drugi model – mniej restrykcyjny oraz charakterystyczny dla krajów skandynawskich (Dania, Szwecja) a także Niemiec, Finlandii i Grecji zakłada, że przedmiotem ochrony jest wyłączny dostęp do systemu komputerowego osób do tego uprawnionych, z tym, że niezbędnym warunkiem uznania działań hackerskich za przestępstwo jest aby system przed takim nieuprawnionym dostępem chroniony był odpowiednimi zabezpieczeniami [8]. Tym samym w drugim omawianym modelu karalności podlega jedynie nieuprawniony oraz wiążący się z przełamaniem tych zabezpieczeń dostęp do cudzego komputera lub systemu informatycznego [9].

Na gruncie polskiego prawa karnego przestępstwo hackingu *sensu stricte* reguluje treść art. 267 § 1 kk. Zauważyć przy tym należy, iż przepis ten w uprzednim brzemieniu (sprzed nowelizacji z dnia 24 października 2008 r. – a więc „*kto bez uprawnienia uzyskuje informację dla niego nie przeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenia*") zakładał, że naruszenie poufności następowało dopiero z chwilą nieuprawnionego uzyskania informacji, a więc *de facto* z chwilą jej przeczytania [10]. Tym samym polska regulacja art. 267 § 1 kk odpowiadała dotychczas trzeciemu modelowi kryminalizacji hackingu, zaproponowanemu przez P. Kardasa [11]. Podkreślić także należy, iż w literalnym brzmieniu przepis art. 267 § 1 kk sankcjonował dotychczas sam fakt zapoznania się przez hackera z treścią przechowywanej w systemie komputerowym informacji, np. cudzej korespondencji elektronicznej, danych strategicznych rozwoju i planowania konkurencyjnej firmy oraz wszelkich nie przeznaczonych dla niego informacji. Dodatkowo niezbędnym warunkiem odpowiedzialności hackera było także dotarcie do tych informacji na skutek przełama-

[5] P. Kardas, Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle aktualnie obowiązującego stanu prawnego, Czasopismo Prawa Karnego i Nauk Penalnych, Rok IV, 2000 r., z. 1, s. 60;

[6] P. Kardas, Prawnokarna ochrona informacji w polskim prawie karnym…, op. Cit., s. 60;

[7] A. Adamski, Prawo karne komputerowe, Wydawnictwo C. H. BECK, Warszawa 2000 r., s. 45;

[8] A. Adamski, Prawo karne komputerowe, op. Cit., s. 45 – 46;

[9] S. Bukowski, Przestępstwo hackingu, Przegląd Sądowy, nr 4, kwiecień 2005 r., s. 140;

[10] S. Bukowski, Przestępstwo hackingu, op. Cit., s. 141;

[11] P. Kardas, Prawnokarna ochrona informacji w polskim prawie karnym…, op. Cit., s. 60;

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

nia stosownych zabezpieczeń[12]. Tym samym już na wstępie należy stwierdzić, że ujęcie przestępstwa hackingu *sensu stricte* w regulacji kodeksu karnego z 1997 r. sprzed nowelizacji z dnia 24 października 2008 r. nie było wystarczające. W szczególności obejmowało ono bowiem i penalizowało wyłącznie „kradzież" informacji jako takiej [13], natomiast nie obejmowało swoim zakresem innych działań przestępczych hackera – które mógł on przeprowadzać za pośrednictwem sieci komputerowej, w tym zwłaszcza sieci Internet. Działania hackerskie nakierowane mogą być bowiem nie tylko na zdobycie i zapoznanie się z informacją innej osoby bądź podmiotu, ale także mogą polegać na „włamaniu" się do cudzego systemu informatycznego, wyłącznie w celu wykazania braku skutecznych zabezpieczeń w tym systemie, bądź też sprawdzenia własnych umiejętności informatycznych [14], a nawet w celu pozostawienia śladu „swojej bytności" w innym systemie komputerowym poprzez dokonanie w nim zmian lub umieszczenie informacji o „odwiedzinach", w postaci np. zamieszczonego w systemie lub na stronie WWW stosownego tekstu lub adnotacji – często o wulgarnej i nieprzyzwoitej treści. Znane są także przypadki włamań do innych systemów informatycznych jedynie w celu „kradzieży czasu pracy innego komputera" [15]. Tym samym w działaniach hackerskich wcale nie musi chodzić o zdobycie informacji, ale również o inne cele (zabawa, prestiż, doskonalenie własnych umiejętności hackerskich) – jednakże zawsze działania te dokonywane są w obrębie systemu informatycznego konkretnego komputera lub kilku połączonych komputerów, zazwyczaj za pośrednictwem sieci i z wykorzystaniem metod informatycznych.

W uprzednim brzmieniu przepisu art. 267 § 1 kk samo skopiowanie przez sprawcę plików z danymi z innego systemu informatycznego lub komputera, zawierających informację – nie było jeszcze tożsame z popełnieniem tego przestępstwa. Do jego realizacji konieczne było dodatkowo zapoznanie się przez hackera z treścią tej informacji, którą wszak miał on „uzyskać". Jak słusznie podkreślano bowiem w doktrynie, naruszenie poufności informacji następuje z chwilą „uzyskania informacji", a więc bezpośrednio z chwilą zapoznania się z jej treścią [16]. Tym samym art. 267 § 1 kk w dotychczasowym brzmieniu sprzed nowelizacji z dnia 24 października 2008 r., w żadnym razie nie penalizował sytuacji, gdy hacker po uzyskaniu dostępu do cudzego komputera kopiował – czasami ogromne ilości danych informacyjnych na nośnik magnetyczny – np. twardy dysk własnego komputera, jednak nie zapoznawał się z nimi, lecz przekazywał je bezpośrednio innej osobie na której zlecenie działał – np. konkurencyjnemu przedsiębiorcy [17]. Zauważyć przy tym także należy, że tego rodzaju działania hackerskie, gdy faktycznie haker nie zapozna się ze skopiowanymi informacjami z innego komputera są bardzo częste – chociażby ze względu na rozmiar informacji które zazwyczaj podlegają skopiowaniu.

Trafny był w tym zakresie pogląd A. Adamskiego, iż faktycznie działania hackerskie obejmują także szereg technik infiltracji systemów komputerowych nie wiążących się w żadnym zakresie z przełamywaniem zabezpieczeń. Hackerzy mogą stosować w tym celu wobec użytkownika, czy też administratora systemu metody podstępu zwane „inżynierią społeczną" (*social engineering*), czy też technik ataku *IP – spoofing*, polegających na spreparowaniu adresu źródłowego IP w nagłówku danych przesyłanych przez Internet, przechwycić hasło lub inną informację w czasie jej transmisji (*sniffing*) bądź też po prostu wykorzystać lukę w zabezpieczeniach (*bug*). Nadto jak zauważał cytowany autor, nie popełniał przestępstwa z art. 267 § 1 kk (w jego brzmieniu sprzed nowelizacji z 24 października 2008 r.), także ten, kto wykorzystywał błąd programisty i wchodził do systemu przez „dziurę" w konfiguracji lub oprogramowaniu systemowym po to aby uzyskać znajdującą się w tym systemie informację, przy czym „przechodzenie przez dziurę nie wymagało od hackera ingerencji w zapis na komputerowym nośniku informacji lub korzystania ze specjalnego oprogramowania" [18]. Przykładowo można więc wskazać na zachowanie hackera który starał się przedostać do systemu kompute-

[12] A. Adamski, Karalność hakingu na podstawie przepisów kodeksu karnegio z 1997 r., Przegląd Sądowy, nr 11 – 12, listopada – grudzień 1998 r., s. 150;

[13] W. Wróbel, przestępstwa przeciwko ochronie informacji, rzeczpospolita nr 206, 3 września 1993 r.;

[14] A. Fadia, Etyczny hacking. Nieoficjalny przewodnik, Wydawnictwo Mikom, 2003 r., s. 15 – 20;

[15] A. Adamski, Karalność hakingu na podstawie przepisów kodeksu karnego z 1997 r., op. Cit., s.151;

[16] M. Bojarski, Naruszenie tajemnicy korespondencji, System Prawa Karnego, t. IV, cz. 2, Ossolineum 1989 r., s. 72;

[17] A. Adamski, Karalność hakingu na podstawie przepisów kodeksu karnego z 1997 r., op. Cit., s.151;

[18] A. Adamski , Hacking a nowy kodeks karny , Informatyka 9/98 , s. 9;

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

rowego wyłącznie poprzez szukanie luk w oprogramowaniu, będących błędami lub niedopatrzeniami programistów, po czym już bez pokonywania zabezpieczeń, poprzez odnalezioną „furtkę" przedostawał się do systemu komputerowego oraz przejmował nie przeznaczone dla niego informacje [19]. W sytuacji takiej bez wątpienia nie dochodziło do przełamania elektronicznych, magnetycznych lub też innych zabezpieczeń, a tym samym brak było jakichkolwiek podstaw do postawienia sprawcy zarzutu z art. 267 § 1 kk (w dawnym jego brzmieniu), bądź też z innego przepisu kodeksu karnego, chociaż niewątpliwie działania te osiągały ten sam skutek, a więc uzyskanie przez hackera danych bądź też nie przeznaczonych dla niego informacji.

Tym samym czyn taki pozostawał w rzeczywistości bezkarny, a także w takim wypadku nie można było nawet przypisać hackerowi usiłowania popełnienia czynu z art. 267 § 1 kk [20].

Wobec powyższych niedoskonałości legislacyjnych, dotychczasowa redakcja art. 267 § 1 kk spotykała się z ogólną i w pełni uzasadnioną krytyką doktryny prawniczej, a także zmuszała ona do poszukiwania rozwiązań i konstrukcji prawnych „*per analogiam*", które pozwalałyby wyeliminować ewidentnie istniejącą w tym względzie lukę prawną oraz dopasować treść tego przepisu do faktycznych metod działań hackerskich – często wymykających się tak wąskiej regulacji prawnej.

Odnosząc się do treści art. 267 § 1 kk (w jego dawnym brzmieniu), a w szczególności pojęcia „uzyskania informacji", A. Adamski proponował więc aby poprzez zapoznanie się z informacją – nieprzeznaczoną dla hackera, rozumieć także zapoznanie się z treścią hasła, którym zazwyczaj zabezpieczony jest dany system komputerowy [21]. Tym samym na skutek przełamania tego zabezpieczenia – zazwyczaj za pomocą specjalnego programu komputerowego pozwalającego na odgadywanie haseł, sprawca przestępstwa hackingu zapoznawał się z nieprzeznaczonym dla niego hasłem – a więc minimalną treściowo informacją, bez której nie mógłby dotrzeć do pozostałych informacji i danych. Zauważyć przy tym należy, że przy takiej interpretacji art. 267 § 1 kk w dawnym jego brzemieniu, nawet jeżeli po przełamaniu i poznaniu hasła hacker następnie zrezygnowałby z dalszych działań, i w rzeczywistości wcale do cudzego systemu komputerowego nie wszedł, już zrealizowałby on treść dawnego art. 267 § 1 kk – ponieważ zapoznałby się z samym hasłem. Tym samym, jak dalej podkreślał A. Adamski, nie musiało następnie wcale dojść do użycia złamanego hasła i wniknięcia do systemu komputerowego, ponieważ karalna stawała się już czynność przygotowawcza jaką było uzyskanie informacji warunkującej wejście do cudzego systemu komputerowego [22].

Taka szeroka interpretacja przestępstwa z art. 267 § 1 kk w jego dawnym brzmieniu była jak się wydaje w pełni celowa, ponieważ zakładała ona w zasadzie karanie już dorozumianych czynności przygotowawczych (poznanie treści hasła). Nie może bowiem ulegać wątpliwości, że gdyby celem włamania do systemu komputerowego – nawet poprzez przełamanie zabezpieczeń, nie było faktyczne zapoznanie się z treścią przechowywanych w cudzym komputerze informacji (np. z korespondencją lub dokumentami zawartymi na twardym dysku), brak byłoby jakichkolwiek podstaw do uznania, że zaistniało przestępstwo z art. 267 § 1 kk w jego brzemieniu sprzed nowelizacji z dnia 24 października 2008 r. [23].

Zupełnie inną – wąską interpretację art. 267 § 1 kk w jego brzmieniu sprzed przedmiotowej nowelizacji, przedstawiał natomiast W. Wróbel [24] uznając, że do odpowiedzialności za przestępstwo hackingu z art. 267 § 1 kk konieczne jest spełnienie dwóch niezależnych od siebie warunków, a mianowicie, że sprawca uzyskał dostęp do systemu komputerowego przełamując specjalne zabezpieczenie oraz, że następnie uzyskał dodatkowo znajdujące się w tym systemie informacje, które musiały być różne od treści hasła zabezpieczającego dostęp do systemu [25].

---

[19] S. Bukowski, Przestępstwo hackingu, op. Cit., s. 153;

[20] A. Adamski , Hacking a nowy kodeks karny , op. Cit. , s. 10 - 12;

[21] A. Adamski, Karalność hakingu na podstawie przepisów kodeksu karnego z 1997 r., op. Cit., s. 151 – 152;

[22] A. Adamski, ibidem, s. 152;

[23] A. Adamski, ibidem, s.151;

[24] W. Wróbel, Przestępstwa przeciwko ochronie informacji, Rzeczpospolita, nr 206 z 03.09.1993 r.;

[25] W. Wróbel, Uwagi wprowadzające do Rozdziału XXXIII Kodeksu Karnego „Przestępstwa przeciwko ochronie informacji", w G. Bogdan, K. Buchała, Z. Ćwiąkalski, M. Dąbrowska - Kardas, P. Kardas, P. Majewski, M. Rodzynkiewicz, M. Szewczyk, W. Wróbel, A. Zoll, Kodeks Karny. Część szczególna. Komentarz, t. II, Kraków 1999 r., s. 968 – 969;

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

Kodyfikacja karna w zakresie dotyczącym uregulowania przestępstw o charakterze *hackingu* na gruncie kodeksu karnego z 1997 r. sprzed nowelizacji z dnia 24 października 2008 r., jak słusznie zauważał A. Adamski, obejmowała także jedynie najprostsze metody działania hackerów – zmierzające w zasadzie do prostego przełamania zabezpieczeń w celu uzyskania informacji, do których nie byli oni uprawnieni. W tym kontekście A. Adamski wyróżniał co najmniej trzy grupy działań hackerskich w których pomimo oczywistej bezprawności tych działań i wiążącej się z nimi realnej szkody, nie można było na gruncie art. 267 § 1 kk oraz art. 267 § 2 kk w ich brzmieniu sprzed wspomnianej nowelizacji, przypisać sprawcy zrealizowania znamion tych czynów. W szczególności w zależności od sposobu działania sprawców omówienia wymagają więc następujące techniki działań hackerskich: 1. *hacking* z użyciem podstępu, 2. *hacking* z zastosowaniem podsłuchu oraz 3. *hacking* z wykorzystaniem luk bezpieczeństwa [26].

W pierwszej grupie (hackingu z użyciem podstępu) pomieścić można tych hackerów, którzy potrzebne im informacje w celu zdobycia dostępu do konkretnego komputera lub systemu informatycznego, w tym zwłaszcza hasła dostępu, zdobywają poprzez wprowadzenie w błąd osoby dysponującej dostępem do systemu lub system ten nadzorującą co do faktycznej tożsamości osoby rozmawiającej z nią przez telefon lub np. przesyłającej wiadomości e – mail. Tym samym hacker stwarza wrażenie u osoby z którą się kontaktuje, że jest np. rzeczywistym właścicielem konta internetowego, który zapomniał hasła dostępu i prosi o pomoc lub jest przedstawicielem firmy administrującej system oraz naprawiającej jego usterki. Następnie wykorzystując naiwność lub dobroduszność pracowników systemu informatycznego lub nadzorujących pracę serwera, hacker uzyskuje często potrzebne mu informacje w postaci „rzekomo zapomnianego" hasła dostępu lub niezbędnych kodów.

Sprawca *hackingu* posługujący się podstępem może także czasami wykorzystywać bardziej złożone metody infiltracji systemów komputerowych za pomocą tzw. metody ataku IP (*Internet Protocol*) - spoofing [27]. Metoda ta sprowadza się do ataku na system komputerowy, którego zadaniem jest zapewnienie bezpieczeństwa w sieci poprzez blokadę dostępu do tego systemu nieuprawnionych pakietów danych – tych które nie dysponują określonym i zgodnym adresem IP, oraz polega na przerobieniu przez hackera adresów IP na przesyłanych przez niego do systemu pakietach danych za pomocą posiadanego specjalnego oprogramowania, w taki sposób, by system rozpoznał te dane jako pochodzące z własnej sieci informatycznej. System mylnie rozpoznawszy pakiety danych jako własne, nie dokonuje procedury sprawdzenia użytkownika, a w szczególności nie zadaje mu pytania o hasło dostępu uznając, iż uprzednio był już zalogowany w tym systemie. Jest to swoiste obejście zabezpieczeń przez hackera, który tym samym w ogóle nie musi uzyskać informacji o treści hasła dostępowego. Hacker nie dokonuje więc przełamania zabezpieczeń elektronicznych, magnetycznych czy też innych, co powodowało, iż w sytuacji, gdy dodatkowo nie zapoznawał się z nieprzeznaczonymi dla niego informacjami – np. ściągając je w formie cyfrowej, zapisując na płytę CD – R i przekazując takie dane osobie zlecającej, trudno było na gruncie art. 267 § 1 kk w jego poprzednim brzmieniu sprzed nowelizacji z 24 października 2008 r. przypisać mu dokonanie przestępstwa *hackingu*.

A. Adamski wskazywał także na analogiczne metody działania hackerów, które mogły na gruncie art. 267 § 1 kk w jego poprzednim brzmieniu, wykluczyć możliwość pociągnięcia takich sprawców do odpowiedzialności karnej, a polegające na posługiwaniu się takimi technikami uzyskania dostępu do cudzego systemu komputerowego, jak np. przechwycenie sesji legalnego użytkownika (*session hijacking*) bądź też metodą zwaną „fragmentacja – reasemblacja pakietów", ponieważ metody te polegające na podszywaniu się pod uprawnionego użytkownika systemu także mają charakter podstępu [28].

Sytuację tą radykalnie zmieniła dopiero wspomniana nowelizacja dokonana ustawą z dnia 24 października 2008 r. o zmianie ustawy kodeks karny oraz niektórych innych ustaw (Dz. U. z 2008 r., Nr 214, poz. 1344). W szczególności przepis art. 267 § 1 kk w brzmieniu nadanym mu po przedmio-

[26] A. Adamski, Karalność hackingu na podstawie przepisów kodeksu karnego z 1997 r., op. Cit., s 153 – 157;

[27] D. Icove, K. Seger, W. Von Stroch, Computer Crime. A Crimefighter's Handbook, O'Reilly & Associates Inc, Sebastopol, CA 1995, s. 50;

[28] A. Adamski, Karalność hackingu, op. Cit., s. 155;

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

towej nowelizacji stanowi, iż kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenia, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności dla lat 2. Dodatkowo w ramach przedmiotowej nowelizacji do kodeksu karnego wprowadzono także zupełnie nowy art. 267 § 2 kk stanowiący, iż tej samej karze (jak za czyn z art. 267 § 1 kk) podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego. Tym samym w aktualnym brzmieniu art. 267 § 1 kk, w związku z użyciem w treści tego przepisu sformułowania „kto bez uprawnienia uzyskuje dostęp do informacji", a także włączenia do katalogu znamion wypełniających ten czyn także możliwości „obejścia" elektronicznych, magnetycznych, informatycznych lub innych szczególnych zabezpieczeń, zachowania hackerskie opisane powyżej, a polegające na uzyskaniu dostępu do informacji zawartej w systemie informatycznym do którego hacker „wnika" w ramach podstępu bądź też obejścia zabezpieczeń, w pełni podlegają kryminalizacji w ramach art. 267 § 1 kk.

Dużą trudność w ściganiu tego rodzaju zachowań przestępczych może stanowić natomiast fakt, iż pomimo tego, że zazwyczaj serwery internetowe automatycznie rejestrują polecenia wydawane przez aktualnych użytkowników – a wiec i od osób które w sposób bezprawny uzyskały dostęp do takiego serwera, niemniej dla osoby posiadającej minimum wiedzy informatycznej i programistycznej, usunięcie logów które wskazywałyby na uprzednie korzystanie z dostępu do poszczególnych katalogów i plików zawierających konkretne informacje, bądź też po prostu wyłączenie rejestracji tych poleceń, nie stanowi w rzeczywistości żadnej trudności [29].

Jak podkreślał przy tym A. Adamski w wydanej na zlecenie Biura Analiz Sejmowych opinii do projektu ustawy z druku nr 458 – Rządowy projekt ustawy o zmianie ustawy Kodeks karny oraz niektórych innych ustaw [30], przedmiot penalizacji art. 267 § 1 kk w jego aktualnym brzmieniu, dotyczy faktycznie klasycznej formy *hackingu* – czyli polegającego na uzyskaniu nieuprawnionego dostępu do całości lub części systemu komputerowego w wyniku naruszenia jego zabezpieczeń. Uzyskanie dostępu do systemu komputerowego jest już także definiowane przy użyciu zobiektywizowanego kryterium „uzyskania dostępu do informacji" przechowywanej w systemie, który jest zabezpieczony przed nieuprawnionym dostępem np. za pomocą hasła, *firewall* bądź programu antywirusowego, przy czym sprawca aby uzyskać dostęp do systemu musi te zabezpieczenia pokonać lub obejść używając odpowiednich narzędzi i technik hackerskich – co wskazuje na umyślny charakter działania sprawcy.

Oczywiście w przypadku *hackingu* informacją do której hacker uzyskuje bez uprawnienia dostęp podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając stosowane zabezpieczenia elektroniczne, magnetyczne i informatyczne – w rozumieniu właściwych systemów bezpieczeństwa komputerowego oraz programów komputerowych – jest bądź informacja o charakterze zapisu cyfrowego bądź też program komputerowy, w który bezpośrednio ingeruje lub który przenosi na własny nośnik informatyczny. Uzyskanie przy tym przez hackera dostępu do nie przeznaczonej dla niego informacji oznacza możliwość przeglądania, kopiowania, blokowania, usuwania albo też wykorzystywanie w inny sposób przechowywanej w systemie informacji i to niezależnie od celu wniknięcia do systemu [31].

Zgodnie także z opinią R. Koszuta, zmiana legislacyjna w zakresie przepisu art. 267 § 1 kk zasadniczo usunęła dotychczas występujące w tym uregulowaniu luki prawne, przy czym zmieniła ona zasadniczo koncepcję na jakiej uregulowanie to aktualnie jest oparte [32]. W szczególności dotychczasowe brzmienie art. 267 § 1 kk (przed nowelizacją z dnia 24 października 2008 r.) odpowiadało klasycz-

[29] A. Frisch, UNIX, Administracja systemu, Warszawa, 1996 r., s. 193 – 199;

[30] A. Adamski, Opinia do projektu ustawy z druku nr 458 Rządowy projekt ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw, Biuro Analiz Sejmowych – Opinia Zlecona, Toruń 4 lipca 2008 r.,s. 3 – 4, dostępne na stronie internetowej: http://orka.sejm.gov.pl/RexDomk6.nsf/0/8C3096FB8C026D9AC12574720043B40C/$file/i1772_08-.rtf.;

[31] A. Adamski, Opinia do projektu ustawy z druku nr 458 Rządowy projekt ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw, op. Cit., s. 4, dostępne na stronie internetowej: http://orka.sejm.gov.pl/RexDomk6.nsf/0/8C3096FB8C-026D9AC12574720043B40C/$file/i1772_08-.rtf.;

[32] R. Koszut, Cyberpornografia i haking – wybrane aspekty proponowanej nowelizacji prawa karnego, Boston, nr 5, 2008 r., s. 36;

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

nemu przestępstwu naruszenia korespondencji i w żaden sposób nie spełniało swojej funkcji w zakresie możliwości ścigania sprawców naruszeń polegających na uzyskaniu nielegalnego dostępu do systemu teleinformatycznego czy też „włamania" komputerowego. Podstawowym mankamentem tego przepisu w dotychczasowym brzmieniu, był także wymóg udowodnienia hackerowi faktu uzyskania informacji, a więc zapoznania się lub wręcz zrozumienia treści tej informacji, co *de facto* wcale nie musiało oznaczać zawładnięcia nośnikiem informacji czy też skopiowania danych. Przepis art. 267 § 1 kk w aktualnym brzmieniu (po nowelizacji) usuwa te luki, albowiem za karalne uznane zostaje już uzyskanie bezprawnego dostępu do informacji, a więc uzyskanie możliwości jej dysponowania, przy czym zachowanie sprawcy podlegające penalizacji polega obecnie na podłączeniu się do sieci telekomunikacyjnej, a nie jak było dotychczas do przewodu służącego do przekazywania informacji.

Niewątpliwie duże znaczenie ma użycie w art. 267 § 1 kk w jego nowym brzmieniu znamienia „omijania zabezpieczeń", albowiem daje to możliwość penalizacji zachowań polegających na uzyskiwaniu dostępu do systemu informatycznego i zgromadzonych w nim danych nie tylko poprzez pokonanie zabezpieczeń (elektronicznych, magnetycznych, informatycznych lub innych szczególnych zabezpieczeń), ale także poprzez szukanie i wykorzystywanie luk w zabezpieczeniach oraz wad tego systemu. Nie ulega natomiast wątpliwości, iż pomimo faktu powszechnego wykorzystywania przez administratorów systemu zabezpieczeń w postaci np. *firewall*, programów antywirusowych, haseł dostępu, wskazane systemy bezpieczeństwa i zabezpieczenia nie są doskonałe i w pewnych sytuacjach osoba dysponująca określoną wiedzą informatyczną, bądź często nawet na skutek przypadkowych działań, może uzyskać dostęp do systemu i przechowywanych w nim informacji i danych. Dotychczas zachowania takie były zupełnie bezkarne – obecnie po nowelizacji art. 267 § 1 kk, podlegać będą one ściganiu [33].

W przypadku natomiast art. 267 § 2 kk w jego brzmieniu nadanym ustawą z dnia 24 października 2008 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw, tożsamej karze jak za czyn z art. 267 § 1 kk podlega także ten kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego. Unormowanie to dotyczące zachowania mającego postać tzw. „czystego dostępu do systemu informatycznego", wzbudza pewne zastrzeżenia i wątpliwości interpretacyjne. W szczególności jak trafnie zauważa A. Adamski w opisie czynu z art. 267 § 2 kk nie występuje już w odróżnieniu do dyspozycji art. 267 § 1 kk element „przełamania" lub „omijania" zabezpieczeń. Przepis ten w zasadzie w ogóle nie charakteryzuje sposobu działania sprawcy i ma bardzo ogólny charakter, co *de facto* oznacza, że przepis ten kryminalizuje wszelkie możliwe przypadki uzyskania nieuprawnionego (nieautoryzowanego) dostępu do systemu informatycznego oraz przy użyciu jakiejkolwiek metody, a także bez względu na to czy system ten posiada jakieś zabezpieczenia, czy też zabezpieczeń takich wcale nie posiada [34]. Faktycznie pociąga to za sobą niebezpieczeństwo objęcia kryminalizacją wszelkich zachowań które wiążą się z uzyskaniem dostępu do innego systemu informatycznego – nawet przypadkowego, skoro przepis art. 267 § 2 kk nie wymaga umyślności działania sprawcy, a jedynie formułuje znamię „bez uprawnienia uzyskuje dostęp". W tym też kontekście uznać należy art. 267 § 2 kk za nieprecyzyjny oraz stwarzający w praktyce możliwość problemów interpretacyjnych, co prowadzić może do serii postępowań karnych dotyczących sytuacji przypadkowego uzyskania dostępu przez użytkowników sieci Internet do systemu informatycznego – który nawet nie musi być zabezpieczony [35]. Dodatkowo wskazać należy w ślad za A. Adamskim, iż komplementarność przepisu art. 267 § 2 kk w odniesieniu do § 1 art. 267 kk ogranicza praktycznie zakres jego stosowania do takich sytuacji gdy uzyskanie nieuprawnionego dostępu do systemu komputerowego nie wiąże się równocześnie z uzyskaniem dostępu do zawartych w tym systemie informacji. W rzeczywistości natomiast często może dojść do sytuacji gdy dany użytkownik uzyska nieautoryzowany dostęp do bez-

[33] R. Koszut, Cyberpornografia i haking – wybrane aspekty proponowanej nowelizacji prawa karnego, op. Cit., s. 36;

[34] A. Adamski, Opinia do projektu ustawy z druku nr 458 Rządowy projekt ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw, op. Cit., s. 4 – 5, dostępne na stronie internetowej: http://orka.sejm.gov.pl/RexDomk6.nsf/0/8C3096FB8C-026D9AC12574720043B40C/$file/i1772_08-.rtf.;

[35] G. Zawadka, Bicz na hakerów czy pułapka na internautów, Rzeczpospolita, 20.11.2008 r., artykuł dostępny na stronie internetowej: http://www.rp.pl/artykul/222070.html;

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

przewodowej sieci komputerowej Wi – Fi [36]. Oznacza to faktycznie, iż osoba która np. przypadkowo podłączy się do takiej bezprzewodowej sieci Wi – Fi uzyska nie tylko dostęp do wszystkich komputerów oraz urządzeń które pracują w tej sieci – co jest w efekcie tożsame ze *sniffingiem* a więc podsłuchiwaniem całego ruchu w tej sieci, ale także uzyska dostęp do informacji znajdujących się w tych komputerach. Łatwo można sobie także wyobrazić zupełnie przypadkowe podłączenie się do niezabezpieczonej sieci bezprzewodowej Wi – Fi innego użytkownika – np. sąsiada z bloku mieszkalnego, co w efekcie prowadzi do uzyskania dostępu (bez uprawnienia) do cudzego systemu komputerowego, przy czym jeżeli taki użytkownik przewidywał taką możliwość i z nią się godził, poniesie on każdorazowo odpowiedzialność karną z art. 267 § 2 kk [37].

Tym samym mamy na gruncie aktualnie obowiązujących unormowań art. 267 § 1 i § 2 kk do czynienia z faktyczną przewagą przepisu uzupełniającego (art. 267 § 2 kk) nad zasadniczym (art. 267 § 1 kk), ponieważ pierwszy wskazany przepis ma w odniesieniu do art. 267 § 1 kk znacznie szersze granice stosowania, a także nie przewiduje w odniesieniu do sprawcy uzyskującego nieuprawniony dostęp do systemu informatycznego (bądź jego części) żadnych dodatkowych warunków ograniczających zakres jego odpowiedzialności karnej - takich jak przełamywanie bądź też obchodzenie zabezpieczeń[38]. Sytuacja ta stwarza natomiast niebezpieczeństwo niedookreśloności omawianego przepisu z art. 267 § 2 kk, a tym samym zbyt dużej swobody jego interpretacji przez organy ścigania oraz organy procesowe.

Zgodzić należy się także ze spostrzeżeniem R. Koszuta, iż faktycznie przepis art. 267 § 2 kk w jego aktualnym brzmieniu – będąc przykładem kryminalizacji tzw. czystego dostępu do systemu komputerowego (naruszenia miru komputerowego), jest zbliżony do przestępstwa naruszenia miru domowego z art. 193 kk [39].

W aktualnym stanie prawnym, w związku z nowelizacją art. 267 § 1 kk oraz użyciem w redakcji tego przepisu sformułowania „uzyskuje dostęp do informacji", o wypełnieniu znamion tego przestępstwa nie decyduje już więc szczególny sposób działania sprawcy w jaki uzyskuje on zastrzeżone informacje, lecz sam fakt uzyskania dostępu do tych informacji, przy czym nawet w przypadku braku konieczności uprzedniego przełamania zabezpieczeń przez sprawcę *hackingu,* czyn taki także wypełnia znamiona tego przestępstwa. Tym samym sformułowanie użyte w treści art. 267 § 1 kk (po nowelizacji z 24 października 2008 r.) - „uzyskuje dostęp do informacji" rozumieć należy aktualnie już nie jako „poznanie treści informacji", lecz jako wejście w „fizyczne" jej posiadanie [40].

Ogólnie rzecz ujmując, przedmiotem ochrony art. 267 § 1 kk jest więc szeroko rozumiane prawo do poufności, które obejmuje prawo do dysponowania informacją, przy czym pokrzywdzonym przestępstwem *hackingu* może być zarówno osoba fizyczna jak też osoba prawna, instytucja oraz organizacja – pozostające dysponentami informacji do których sprawca uzyskuje bez uprawniania dostęp. Przestępstwo to także w praktyce możliwe jest do popełnienia wyłącznie z zamiarem bezpośrednim, albowiem trudno założyć aby sprawca przestępstwa z art. 267 § 1 kk nie miał pełnej świadomości faktu, że uzyskuje dostęp do informacji dla niego nieprzeznaczonej [41].

Przepis art. 267 § 3 kk po nowelizacji z dnia 24 października 2008 r. - dotyczy natomiast tzw. *hackingu* z zastosowaniem podsłuchu (sankcjonowanego przed omawianą nowelizacją przez art. 267 § 2 kk). Omawiany przepis stanowi, iż odpowiedzialności karnej podlega ten kto w celu uzyskania informacji do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem. Zmiana na gruncie nowelizacji z dnia 24

[36] A. Adamski, Opinia do projektu ustawy z druku nr 458 Rządowy projekt ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw, op. Cit., s. 4 – 5, dostępne na stronie internetowej: http://orka.sejm.gov.pl/RexDomk6.nsf/0/8C3096FB8C-026D9AC12574720043B40C/$file/i1772_08-.rtf.;

[37] R. Koszut, Cyberpornografia i haking – wybrane aspekty proponowanej nowelizacji prawa karnego, op. Cit., s. 37;

[38] A. Adamski, Nowej ujęcie cyberprzestępstw w kodeksie karnym – ale czy lepsze?, Prawo Teleinformatyczne, nr 3/5, 2007 r., s. 8;

[39] R. Koszut, Cyberpornografia i haking – wybrane aspekty proponowanej nowelizacji prawa karnego, op. Cit., s. 36;

[40] M. Bojarski, Naruszenie tajemnicy korespondencji, op. Cit., s. 72 - 73;

[41] R. Koszut, Kwestie sporne na tle wykładni przestępstwa hackingu, (w:) Nowa Kodyfikacja Prawa Karnego, Tom VIII, pod redakcją L. Boguni, Wrocław 2001 r., Acta Universitatis Wratislaviensis, nr 2305, s. 83 – 84;

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

października 2008 r., sprowadzała się przy tym jedynie do zamiany zwrotu „*posługiwania się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym*" na sformułowanie „posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem". Oczywistym jest przy tym, że pomimo tego, iż sam program komputerowy nie jest urządzeniem, to już komputer z zainstalowanym właściwym programem (np. typu *password sniffer*) pozwalającym na monitorowanie ruchu w sieci i przechwytywanie początkowych sekwencji bajtów danej sesji zawierającej identyfikatory i hasła dostępu, będzie urządzeniem o charakterze specjalnym [42]. Tym samym wskazana zmiana legislacyjna miała jak się wydaje charakter jedynie kosmetyczny.

Czyn z art. 267 § 3 kk jest także przestępstwem umyślnym, które można popełnić tylko w zamiarze bezpośrednim, zaś osoba która instaluje urządzenie podsłuchowe np. na cudze zlecenie ponosi odpowiedzialność karną na podstawie art. 267 § 3 kk tylko wówczas jeżeli ma ona świadomość, iż nie jest uprawniona do zakładania tego rodzaju urządzeń. Osoba zlecająca takiego rodzaju działania odpowiadać będzie natomiast za sprawstwo kierownicze w zakresie polecenia popełnienia czynu z art. 267 § 3 kk [43].

Sprawca zrealizuje przy tym normę art. 267 § 3 kk w jego aktualnym brzmieniu, w każdej sytuacji gdy w celu uzyskania informacji do których nie jest uprawniony – posłuży się stosownym urządzeniem lub oprogramowaniem pozwalającymi na uzyskanie takich informacji zawartych w jakimkolwiek systemie informatycznym, i to bez względu na to czy system ten jest chroniony zabezpieczeniami, a sprawca w tym celu je przełamie, czy też w ogóle nie jest on chroniony, a sprawca uzyska dostęp do tego systemu za pomocą opisywanych urządzeń i oprogramowania bez przełamywania jakichkolwiek zabezpieczeń. Warunkiem przypisana mu realizacji tego przestępstwa jest jednak wykazanie, iż faktycznie uzyskał dostęp do tych informacji, gdyż w przeciwnym razie samo posługiwanie się określonym urządzeniem lub oprogramowaniem, a nawet wejście w posiadanie omawianych początkowych sekwencji zawierających identyfikatory czy też kody dostępu, bez ich dalszego wykorzystania w celu zdobywania informacji zawartych w systemie informatycznym, nie zrealizuje znamion czynu z art. 267 § 3 kk, a jedynie może wypełnić znamiona uzyskania tzw. czystego dostępu do całości lub części systemu informatycznego – a więc z art. 267 § 2 kk w jego aktualnym brzmieniu.

Kwalifikowaną ze względu na wyrządzenie znacznej szkody majątkowej formę opisywanego przestępstwa zawiera natomiast art. 268 § 3 kk.

Czyn z art. 268 § 2 kk jest więc przestępstwem umyślnym które można popełnić zarówno w zamiarze bezpośrednim jak i ewentualnym. Jest to także przestępstwo skutkowe, a warunkiem odpowiedzialności za czyn z art. 268 § 2 kk, jest udaremnienie lub znaczne utrudnienie zapoznania się z informacją przez uprawnioną do tego osobę. Podkreślić przy tym należy, że nie będzie podlegał odpowiedzialności za ten czyn użytkownik, który w wyniku błędu w programie, lub awarii sprzętu przypadkowo dokonał uszkodzenia lub usunięcia zapisu informacyjnego, nawet wówczas gdy chodziło o istotną informację [44].

Nie będzie także podlegało odpowiedzialności karnej nieumyślne zawirusowanie cudzego komputera w następstwie nie zachowania należytej ostrożności, nawet jeżeli w skutek tego dojdzie do zniszczenia, uszkodzenia lub usunięcia zapisu istotnej informacji. Oznaczać to będzie, iż pracownik który używa komputera służbowego w zakładzie pracy do celów prywatnych oraz wczytuje weń program komputerowy bądź plik zawarty na zainfekowanej dyskietce, bez uprzedniego sprawdzenia, czy dyskietka ta nie jest zainfekowana, nie poniesie odpowiedzialności karnej za skutki swojego zaniedbania, i to nawet jeżeli doprowadzą one do poważnych następstw [45]. Podobnie zniszczenie lub usunięcie informacji w systemie komputerowym nie będzie podlegało odpowiedzialności karnej na podstawie art. 268 § 2 kk w sytuacji gdy do zniszczenia tej informacji dojdzie po zapoznaniu się już z jej treścią przez osobę uprawnioną lub gdy pokrzywdzony posiada kopię zniszczonego lub usunię-

[42] A. Adamski, Karalność hackingu, op. Cit., s.156;
[43] A. Adamski, Prawo Karne Komputerowe, op. Cit., s.64;
[44] S. Bukowski, Przestępstwo hackingu, op. Cit., s.156;
[45] A. Adamski, Prawo karne Komputerowe, op. Cit., s. 71 – 72;

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

tego pliku z zapisaną informacją która podlegała zniszczeniu lub usunięciu, a więc w sytuacji gdy odtworzenie wskazanej informacji nie nastręczy dla pokrzywdzonego większych trudności [46].

Jeżeli natomiast sprawca uzyskał dostęp do danego systemu informatycznego, jedynie w celu ingerencji w treść publicznej i ogólnie dostępnej strony WWW, bądź też jej usunięcia, to działania takie należy rozpatrywać w kontekście ewentualnego wyczerpania znamion czynu z art. 268 § 2 kk stanowiącego, iż sankcji karnej podlega ten, kto nie będąc do tego uprawnionym niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji, albo też udaremnia w inny sposób lub znacznie utrudnia osobie uprawnionej zapoznanie się z takim zapisem lub informacją, w przypadku gdy czyn ten dotyczy zapisu na informatycznym nośniku danych.

Jak słusznie zauważa przy tym M. Sowa, zmiana treści strony WWW w kontekście wyczerpania tym zachowaniem znamion czynu z art. 268 § 1 i § 2 kk, każdorazowo musi podlegać również ocenie, w zakresie tego czy informacja której zmian, usunięcia lub uszkodzenia na tej stronie dokonano była faktycznie informacją istotną[47]. Oznacza to, że przestępstwem będzie wyłącznie taki atak hackerski który w ostateczności udaremni lub utrudni zapoznanie się z taką istotną informacją. Istotność informacji możemy przy tym określić odnosząc jej wartość do standardów obowiązujących w danej dziedzinie której informacja ta dotyczy, a także oceniając nakład pracy i środków koniecznych do uzyskania danej informacji [48]. Tylko w takim bowiem przypadku gdy zawarta na stronie WWW informacja miała charakter istotny, zmiana zapisu strony WWW oraz jej treści stanowić będzie czyn karalny.

Dodać przy tym również należy, że w praktyce w większości wypadków sama zmiana treści zapisu strony WWW nie będzie równoznaczna z wyczerpaniem znamion czynu z art. 268 § 1 i § 2 kk. W szczególności bowiem większość stron WWW zawiera informacje o charakterze reklamowym bądź też publicystycznym, przy czym nie wydaje się aby zazwyczaj informacje te, aczkolwiek zmienione w następstwie ingerencji hackera, można było uznać za istotne w rozumieniu art. 268 § 1 kk – dotyczącego raczej informacji które z natury rzeczy nie są dostępne dla ogółu użytkowników (strategia firmy, informacje handlowe, bazy danych itp.). Nie zmienia to jednak faktu, że hacker dokonujący zniszczenia lub zmiany informacji zawartych na stronach WWW – zamieszczając np. treści obraźliwe dla autora strony bądź innych osób lub podmiotów prawnych (za M. Sową przytoczyć można tutaj przykłady kilkukrotnych ataków na serwer Telekomunikacji Polskiej S. A., gdzie hackerzy po włamaniach zamieszczali na tej stronie własne witryny z ośmieszającymi tą firmę tekstami, w tym także parodiując nazwę oraz zamieszczone tam rysunki reklamowe), podlegać może odpowiedzialności karnej na zasadzie innych przepisów, w tym w szczególności za ścigane z oskarżenia prywatnego przestępstwo pomówienia z art. 212 § 1 kk bądź zniesławienia z art. 216 § 1 kk. W większości wypadków czyny takie mogłyby być potraktowane także jako postaci kwalifikowane z art. 212 § 2 kk oraz art. 216 § 2 kk – a więc jako dokonane za pośrednictwem środka masowego komunikowania. Nie ulega bowiem wątpliwości, że sieć Internet – dostępna dla nieograniczonego kręgu użytkowników, jest narzędziem masowej komunikacji zwłaszcza, iż strony WWW zazwyczaj dostępne są także dla nieograniczonej ilości osób, będąc w pewnym sensie namiastką publikacji *quasi* prasowych.

Sytuacja będzie nieco bardziej skomplikowana, gdy hacker uzyska dostęp do strony WWW chronionej hasłem – przełamując to zabezpieczenie bądź też je obchodząc – np. znajdując lukę w systemie bezpieczeństwa, gdyż w tym wypadku hacker swoim zachowaniem wyczerpać może kilka czynów karalnych. Przełamując zabezpieczenie systemu w celu dotarcia na wskazaną stronę WWW chronioną hasłem, dokonuje on bowiem czynu z art. 267 § 1 kk (i to zarówno poprzez uzyskanie dostępu do treści strony WWW dla niego nie przeznaczonej jak też przełamanie bądź obejście samego hasła), a także w przypadku gdy na stronie tej dokona przeróbek – wpisując przykładowo obraźliwe treści, wyczerpać może swoim zachowaniem dodatkowo treść art. 212 § 1 lub § 2 kk i art. 216 § 1 lub § 2 kk.

Warto także zauważyć, iż w sytuacji gdy działania hackerskie doprowadzą do umyślnego zniszczenia lub uszkodzenia zapisu na komputerowym nośniku informacji (nośniku danych) – spełniającego bezpośrednio kryteria dokumentu opisanego w art. 115 § 4 kk, czyn taki należałoby kwalifiko-

[46] A. Adamski, ibidem, s. 72;

[47] M. Sowa, Ogólna charakterystyka przestępczości internetowej, Palestra, nr 5 – 6, maj – czerwiec 2001 r., s. 35;

[48] S. Bukowski, Przestępstwo hackingu, op. Cit., s. 156;

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

wać bezpośrednio jako przestępstwo zniszczenia, uszkodzenia lub uczynienia bezużytecznym czy też usunięcia dokumentu, opisane w art. 276 kk [49].

Działania *hackingu* mogą mieć także postać tzw. sabotażu komputerowego lub dywersji informatycznej, opisanej w art. 269 § 1 i § 2 kk. Przepisy te znowelizowane w zakresie czynu z art. 269 § 2 kk ustawą z dnia 4 września 2008 r. o zmianie ustaw w celu ujednolicenia terminologii informatycznej (Dz. U. Nr 171, poz. 1056), ze względu na rodzaj przetwarzanych przez systemy komputerowe informacji, mają głównie na celu zapewnienie prawnej ochrony serwerom związanym bezpośrednio z sektorem administracji publicznej i wojskowości, które zawierają i udostępniają szczególnie istotne i podlegające ochronie rodzaje informacji, doniosłe z punku widzenia obronności oraz funkcjonowania administracji publicznej [50]. Przepis ten w aktualnym brzmieniu stanowi w szczególności, iż odpowiedzialności karnej podlega ten kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych.

Podobnej odpowiedzialności karnej podlega również ten kto dopuszcza się czynu opisanego w treści art. 269 § 1 kk w warunkach kwalifikowanych (art. 269 § 2 kk) - niszcząc albo wymieniając informatyczny nośnik danych lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych.

Tym samym można stwierdzić w uproszczeniu, iż bezpośrednim celem działania sprawcy dywersji informatycznej jest zakłócenie funkcjonowania systemu komputerowego lub telekomunikacyjnego, a także najczęściej sparaliżowanie ich działania. Przedmiotem ochrony jest w tym wypadku integralność i dostępność informacji przetworzonej elektronicznie o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji lub też dla funkcjonowania administracji publicznej [51]. Zauważyć także należy, iż zachowanie wypełniające znamiona z art. 269 § 1 kk polegające na usunięciu z systemu komputerowego danych informatycznych jest sankcjonowane w każdej sytuacji, a więc także niezależnie od tego czy pokrzywdzony podmiot posiada kopię zapasową danych które zostały usunięte lub zmodyfikowane, czy też dane te zostały bezpowrotnie utracone.

Zamach na dostępność informacji może przybierać w przypadku dywersji informatycznej także dwojaką formę. W szczególności atak ten może być atakiem o charakterze destrukcyjnym lub też przeciążeniowym [52]. Pierwszy rodzaj ataku (destrukcyjny) polega przy tym na zniszczeniu lub modyfikacji danych w sposób powodujący zablokowanie działania systemu komputerowego. Atak poprzez przeciążenie ma natomiast na celu sparaliżowanie działania systemu komputerowego poprzez jednoczesne wydawanie mu wielu poleceń, których wykonanie przekracza możliwości operacyjne systemu, i tym samym prowadzi do jego przeciążenia i zablokowania.

Szczególną postać przestępstw hackerskich o specyfice dywersji informatycznej stanowić mogą także działania opisane w treści art. 268 a § 1 i § 2 kk oraz w treści art. 269 a kk.

Zgodnie z treścią art. 268 a § 1 kk odpowiedzialności karnej podlega ten kto nie będąc do tego uprawnionym niszczy, uszkadza, usuwa lub zmienia, a także utrudnia dostęp do danych informatycznych, lub też w istotny sposób zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych. Kwalifikowaną postać wskazanego przestępstwa, które może polegać na niszczeniu, uszkadzaniu lub usuwaniu danych informatycznych – poprzez wyrządzenie tym działaniem znacznej szkody majątkowej, stanowi natomiast czyn z art. 268 a § 2 kk, przy czym znaczną szkodą majątkową zgodnie z treścią art. 115 § 7 kk w zw. z art. 115 § 5 kk będzie szkoda której wartość w chwili popełnienia czynu z art. 268 a kk przekroczy dwustukrotną wysokość najniższego miesięcznego wynagrodzenia.

---

[49] A. Adamski, Prawo Karne Komputerowe, op. Cit., s. 75;

[50] A. Adamski, Cyberprzestępczość – aspekty prawne i kryminologiczne, op. Cit., s. 57;

[51] A. Adamski, Prawo Karne Komputerowe, op. Cit., s. 77;

[52] A. Adamski, ibidem, s. 78;

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

Zgodnie natomiast z treścią art. 269 a kk (zmienionego w ramach nowelizacji z dnia 24 października 2008 r.) odpowiedzialności karnej podlega ten, kto nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej. Zmiana względem poprzedniej redakcji art. 269 a kk – sprzed nowelizacji, polegała przy tym na dodaniu znamienia „utrudnienia dostępu", które uprzednio w przepisie tym nie występowało. Jak zauważa przy tym A. Adamski pojęcie „utrudniania dostępu" jest ekwiwalentem znaczeniowym dwóch bliskoznacznych pojęć (*suppressing or rendering inaccessible*) występujących w art. 3 Decyzji Ramowej w sprawie ataków na systemy informatyczne oraz zastosowanie go w przedmiotowym przepisie art. 269 a kk jest w pełni celowe [53].

Zawarte w treści art. 268 a § 1 kk oraz art. 269 a kk (a także w treści uprzednio omawianych przepisów art. 268 § 2 kk i 269 § 2 kk po nowelizacji z dnia 4 września 2008 r.) pojęcie danych informatycznych jest przy tym zbieżne z treścią art. 1 cytowanej powyżej Konwencji o cyberprzestępczości oraz oznacza dowolne przedstawianie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny. System informatyczny w tym wypadku oznacza przy tym każde urządzenie lub grupę wzajemnie połączonych lub powiązanych ze sobą urządzeń, z których jedno lub więcej zgodnie z programem wykonuje automatyczne przetwarzanie danych [54].

Czyn z art. 268 a § 1 i § 2 kk jest przestępstwem materialnym, znamiennym skutkiem w postaci zniszczenia, uszkodzenia, usunięcia, spowodowania zmiany lub utrudnienia dostępu do danych informatycznych lub też w postaci zakłócenia dostępu do tych danych informatycznych, zakłócenia w istotnym stopniu lub uniemożliwienia automatycznego ich przetwarzania, gromadzenia lub przekazywania. Jest to także bez wątpienia przestępstwo umyślne, które może być popełnione zarówno z zamiarem bezpośrednim jak też ewentualnym [55]. Oznacza to, iż odpowiedzialności z art. 268 a § 1 i § 2 kk podlegać będzie nie tylko hacker który po przedostaniu się do cudzego systemu komputerowego dokonuje w sposób świadomy destrukcyjnych działań opisanych w tym przepisie na danych informatycznych, ale także osoba która po wejściu do systemu komputerowego dokona usunięcia lub uszkodzenia danych informatycznych niejako przy okazji innych podejmowanych oraz docelowych działań hackerskich takich jak np. kopiowanie plików bądź informacji zawartych w zaatakowanym systemie komputerowym.

Odmiennie w przypadku przestępstwa z art. 269 a kk, możemy mówić jedynie o zamiarze bezpośrednim działań hackerskich, gdyż sprawca przedostając się do systemu komputerowego w pełni świadomie podejmuje działania i czynności które w istotnym stopniu mają doprowadzić do zakłócenia pracy systemu komputerowego lub sieci teleinformatycznej. Tym samym przestępstwo to jest przestępstwem materialnym warunkowanym zaistnieniem określonego skutku w postaci zakłócenia pracy systemu komputerowego lub sieci teleinformatycznej, przy czym zanim skutek ten nie nastąpi możemy mówić co najwyżej o usiłowaniu popełnienia tego czynu [56]. Samo pojęcie istotnego stopnia zakłócenia oznacza natomiast jak się wydaje sytuację, gdy w ocenie przeciętnego dysponenta – administratora czy też użytkownika systemu komputerowego, stopień zakłócenia działania systemu jest na tyle znaczny, iż nie da się bez odpowiedniego nakładu czasu oraz pracy naprawić tego systemu oraz doprowadzić do stanu poprzedniego.

Warto także zauważyć, że działania o charakterze hackerskim mogą być wykorzystywane do popełniania innych przestępstw, takich jak w szczególności szpiegostwo komputerowe z art. 130 § 3 kk oraz sprowadzenie stanu powszechnego niebezpieczeństwa z art. 165 § 1 pkt 3 i 4 kk.

---

[53] A. Adamski, Opinia do projektu ustawy z druku nr 458 Rządowy projekt ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw, op. Cit., s. 10, dostępne na stronie internetowej: http://orka.sejm.gov.pl/RexDomk6.nsf/0/8C3096FB8C-026D9AC12574720043B40C/$file/i1772_08-.rtf.;

[54] B. Kunicka – Michalska, w Kodeks Karny część szczególna, tom II pod redakcją A. Wąska, wydawnictwo C. H. BECK, Warszawa 2006 r., s. 627;

[55] B. Kunicka – Michalska, w Kodeks Karny część szczególna, tom II, op. Cit., s. 628 – 630;

[56] B. Kunicka – Michalska, ibidem, s. 640;

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

Zgodnie z treścią art. 130 § 3 kk penalizacji podlega bowiem działanie sprawcy, który w celu udzielenia obcemu wywiadowi wiadomości których przekazanie może wyrządzić szkodę Rzeczpospolitej Polskiej, między innymi wchodzi do systemu informatycznego w celu uzyskania takich danych. Pomimo tego, iż przepis art. 130 § 3 kk nie uzależnia „wejścia do systemu informatycznego" od określonej metody działania sprawcy [57], jest oczywistym, iż do takiego działania może dojść także za pośrednictwem działań hackerskich (z art. 267 § 1 kk), w szczególności bowiem takie wejście do systemu głównie za pośrednictwem sieci Internet, poprzedzone może być przełamaniem bądź ominięciem elektronicznych, magnetycznych, informatycznych lub innych szczególnych zabezpieczeń tego systemu. Warunkiem niezbędnym przy tym do pociągnięcia sprawcy do odpowiedzialności karnej za czyn z art. 130 § 3 kk będzie okoliczność aby przedmiotowe wejście do systemu informatycznego dokonane zostało w celu szpiegowskim, a więc w celu uzyskania wiadomości których przekazanie może wyrządzić szkodę Rzeczpospolitej Polskiej. W sytuacji więc, gdy hacker przedostanie się do takiego systemu informatycznego (np. sieci komputerowej Sztabu Generalnego Wojska Polskiego), ale w innych celach niż uzyskania wiadomości do celów szpiegowskich (np. zniszczenia danych, lub w celu sprawdzenia swoich umiejętności), dojdzie jedynie do zrealizowania czynu z art. 267 § 1 lub § 2 kk, nie zaś z art. 130 § 3 kk [58].

Dodatkowo jeżeli działania hackerskie (określone w treści art. 267 § 1, § 2 lub § 3 kk) doprowadzą do sprowadzenia niebezpieczeństwa dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach – poprzez uszkodzenie lub unieruchomienie urządzenia użyteczności publicznej, w szczególności dostarczającego wodę, światło, ciepło, gaz, energię albo urządzenia zabezpieczającego przed nastąpieniem niebezpieczeństwa powszechnego lub służącego do jego uchylenia, a także gdy sprawca swoimi działaniami zakłóci, uniemożliwi lub w inny sposób wpłynie na automatyczne przetwarzanie, gromadzenie lub przetwarzanie danych informatycznych – wywołując tym stan niebezpieczeństwa dla życia lub zdrowia wielu osób lub mienia w wielkich rozmiarach (np. paraliżując pracę szpitala z licznymi pacjentami w ciężkim stanie zdrowia), sprawca będzie odpowiadał odpowiednio za przestępstwo z art. 165 § 1 kk, bądź z art. 165 § 3 kk – jeżeli następstwem tego czynu będzie śmierć człowieka lub ciężki uszczerbek na zdrowiu. Jeżeli sprawca działać będzie natomiast nieumyślnie, a więc w sytuacji gdy np. realizując poprzez działania hackerskie normę art. 267 § 1 lub § 3 kk, nie będzie zarazem obejmował swoim zamiarem sprowadzenia przez te czynności niebezpieczeństwa dla życia lub zdrowia wielu osób lub mienia w wielkich rozmiarach – odpowie za nieumyślną postać tego czynu z art. 165 § 2 lub § 4 kk.

W polskim kodeksie karnym, zgodnie z treścią art. 269 b § 1 kk sankcji karnej podlega także wytwarzanie, pozyskiwanie, zbywanie lub udostępnianie innym osobom urządzeń lub programów komputerowych przystosowanych do popełniania przestępstw określonych w art. 165 § 1 pkt 4 kk, art. 267 § 3 kk, art. 268 a § 1 lub 2 kk w zw. z § 1, art. 269 § 2 kk albo art. 269 a kk, a także haseł komputerowych, kodów dostępu lub innych danych umożliwiających dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej. Tym samym brak w tym przepisie kryminalizacji samego faktu posiadania i przechowywania narzędzi hackerskich, a zachowanie takie w odróżnieniu od ustawodawstw wielu krajów, w tym USA, Holandii, Włoch, Szwajcarii, Izraela oraz Federacji Rosyjskiej nie podlega ściganiu jako czyn zabroniony [59]. Pomimo jednak braku jednoznacznego sformułowania w tym zakresie, zauważyć należy, iż fakt kryminalizacji „pozyskiwania" takich narzędzi hackerskich także pozwala na skuteczne ściganie sprawców dysponujących takimi narzędziami [60]. Wszak hacker najpierw musi pozyskać takie programy, w taki bądź inny sposób, aby następnie móc je przechowywać i posiadać. W sposób dorozumiany można więc jak się wyda-

[57] A. Adamski, Prawo karne komputerowe, op. Cit., s. 133;

[58] A. Adamski, ibidem, s. 133 – 134;

[59] A. Adamski, ibidem, s. 72 – 74;

[60] K. Gienas, Prawnokarne aspekty „narzędzi hackerskich", Prawo Mediów Elektronicznych – Biuletyn Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej Wydziału Prawa Administracji i Ekonomii Uniwersytetu Wrocławskiego – Bezpłatny dodatek (2) do Monitora Prawniczego nr 3, rok 2005, s. 37;

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

je uznać, iż każdy fakt posiadania i dysponowania narzędziami hackerskimi musiał być poprzedzony ich „pozyskaniem".

Przepis art. 269 b § 1 kk jest następstwem dostosowania polskich przepisów karnych do treści art. 6 Konwencji Rady Europy z dnia 23.11.2001 r. o cyberprzestępczości. Zgodnie bowiem z art. 6 pkt 1 cytowanej Konwencji, każda strona winna podjąć środki ustawodawcze oraz inne, niezbędne do usankcjonowania w jej prawie krajowym przestępstw polegających na umyślnej i bezprawnej produkcji, sprzedaży, dostarczaniu w celu używania, sprowadzaniu, rozpowszechnianiu lub udostępnianiu:

- urządzenia w tym także programu komputerowego przeznaczonego lub przystosowanego głównie w celu popełniania przestępstw hackingu, podsłuchu komputerowego, naruszenia integralności danych oraz sabotażu komputerowego;
- hasła komputerowego, kodu dostępu lub podobnych danych, dzięki którym całość lub część systemu informatycznego jest dostępna z zamiarem wykorzystania w celu popełniania wskazanych powyżej przestępstw.

Faktycznie jednak państwa – strony konwencji nie zostały zobligowane do wprowadzenia pełnego kanonu przepisów karnych w brzmieniu art. 6 omawianej konwencji, za wyjątkiem sprzedaży, rozpowszechniania lub innego udostępniania narzędzi hackerskich. Tym samym na państwach – stronach konwencji nie spoczywa dotychczas obowiązek kryminalizacji samego faktu posiadania narzędzi hackerskich jako takich, a jedynie zachowań związanych z przekazywaniem tych narzędzi innym osobom oraz ich wykorzystywaniem w praktyce [61].

Przedmiotem ochrony art. 269 b kk jest szeroko rozumiane bezpieczeństwo systemów komputerowych oraz przechowywanych w nich danych – a więc poufność, integralność i dostępność wskazanych danych [62].

Jak zauważa K. Gienas, art. 269 b kk kryminalizuje *de facto* stadium przygotowania do popełniania szeregu przestępstw związanych z funkcjonowaniem sieci Internet [63]. W szczególności przechowywanie programów komputerowych o charakterze destrukcyjnym, w tym wirusów komputerowych, można uznać za formę przygotowania do przestępstwa z art. 268 § 2 kk, jeżeli osoba taka zamierza następnie program ten użyć w celu zniszczenia, usunięcia lub zmiany istotnej informacji zapisanej na informatycznym nośniku danych. Podkreślić przy tym należy, że omawiane przygotowanie do czynu z art. 268 § 2 kk na gruncie polskiego kodeksu karnego także nie podlega sankcjonowaniu i jest zachowaniem prawnie dozwolonym [64], co wydaje się błędem lub niedopatrzeniem ustawodawczym.

Przepis art. 269 b § 2 kk nakłada natomiast na sąd w razie skazania za przestępstwo określone w art. 269 b § 1 kk, obowiązek obligatoryjnego orzeczenia przepadku określonych w tym przepisie przedmiotów (wymienionych w § 1 art. 269 b kk) – w przypadku (jak należy się domyślać z redakcji tego przepisu) gdy stanowią one własność sprawcy. W sytuacji zaś gdy narzędzia hackerskie stanowiły własność innej osoby niż sprawca, sąd może orzec ich przepadek na zasadach fakultatywnych, w szczególności gdy uzna to za celowe ze względu na charakter konkretnej sprawy oraz stwierdzonego stanu faktycznego.

Kryminalizacja posiadania (w tym także pozyskiwania) narzędzi hackerskich nieodłącznie wiązać się będzie z określeniem minimalnej liczby narzędzi hackerskich których posiadanie zadecyduje o tym, iż doszło do popełnienia przestępstwa. W przypadku dystrybucji tych narzędzi (w rozumieniu art. 269 b § 1 kk) mówić należy natomiast o aktywnym udostępnianiu omawianych narzędzi hackerskich innym osobom np. za pośrednictwem poczty e – mail, przy czym w przypadku udostępniania narzędzi hackerskich wystarczające będzie już umieszczenie ich np. na serwerze internetowym na użytek innych osób, w sposób pozwalający na ich skopiowanie i ściągnięcie na twardy dysk własnego

---

[61] A. Adamski, Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy, Toruń 2001 r., s. 40 – 41;

[62] K. Gienas, Uwagi do przestępstwa stypizowanego w art. 296 b kodeksu karnego, Prokurator, nr 1, 2005 r., s. 76;

[63] K. Gienas, Uwagi do przestępstwa stypizowanego w art. 296 b kodeksu karnego, op. Cit., s. 75;

[64] A. Adamski, Prawo karne Komputerowe, op. Cit., s. 74;

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

komputera [65]. Tym samym jak słusznie podkreśla A. Adamski art. 269 b kk nie wymaga od sprawcy działania w zamiarze bezpośrednim, lecz wystarczającym jest gdy sprawca działa w zamiarze ewentualnym np. poprzez udostępnienie na stronie WWW „narzędzi hackerskich" lub też samych tylko odsyłaczy do stron na których one się znajdują, jednakże ze świadomością, że narzędzia te mogą posłużyć innej osobie do zaatakowania wybranego przez nią systemu komputerowego [66]. Aktualnie dystrybucja narzędzi hackerskich polega także głównie na udostępnianiu szerokiej gamy oprogramowania w postaci wirusów komputerowych oraz skryptów wykorzystywanych w atakach typu *denial of service*, mających na celu spowolnienie lub przeciążenie pracy systemu komputerowego poprzez przesyłanie zbyt dużych ilości informacji, przy czym odbywa się ona zarówno poprzez strony WWW, jak też listy dyskusyjne, serwery FTP, a także aplikacje typu peer to peer (P2P) [67].

Warto w tym miejscu w ślad za K. Gienasem zauważyć, że wadą art. 269 b § 1 kk, jest brak regulacji wskazującej w sposób wyraźny, iż nie popełnia przestępstwa z tego przepisu osoba wykorzystująca narzędzia hackerskie wyłącznie w celu testowania stabilności systemu informatycznego [68], a więc pośrednio sprawdzająca skuteczność zabezpieczeń tego systemu przed nieuprawnionymi atakami hackerskimi. W praktyce problematyczne może okazać się także rozróżnienie narzędzi hackerskich od w pełni legalnych programów komputerowych – pisanych na potrzeby testowania sprawności systemów komputerowych oraz testowania ich stabilności [69]. Bez wątpienia bowiem analitycy systemów komputerowych mają jedyną możliwość potwierdzenia skuteczności ich zabezpieczeń poprzez symulowanie próby ataku, a więc posługując się programami zbliżonymi w swoim działaniu do programów hackerskich. Istotnym problemem z punktu widzenia prawa karnego będzie również określenie jaki program już jest narzędziem hackerskim, a kiedy jest jeszcze programem użytkowym - bez cech narzędzia hackerskiego. W tym kontekście można mówić o podwójnej naturze niektórych programów komputerowych – stosowanych zarówno przez hackerów do ataku internetowego jak też przez administratorów systemu do analizowania prawidłowości jego działania.

Najtrafniejszym wydaje się tutaj zastosowanie rozróżnienia funkcjonalnego. Program staje się wyłącznie wtedy narzędziem hackerskim gdy zostaje użyty bezpośrednio do ataku hackerskiego z zewnątrz sieci, w celu jakiejkolwiek ingerencji w nienaruszalność innego systemu komputerowego. W sytuacji gdy program o podobnych cechach służy administratorowi systemu do jego testowania od wewnątrz systemu, bez wyrządzania szkody w systemie, jest on programem użytkowym.

Oczywiście rozróżnienie to nie jest do końca ostre i nie obejmuje wszystkich możliwych sytuacji, jak np. działania hackera zatrudnionego w firmie komputerowej za pośrednictwem dostępnych dla niego, firmowych i w pełni legalnych programów komputerowych do testowania sprawności systemu komputerowego, a więc od wewnątrz tego systemu – w celach wybitnie destrukcyjnych, jednakże sytuacje takie należy uznać raczej za wyjątkowe.

Na zakończenie stwierdzić należy, iż ostatnie nowelizacje polskiego kodeksu karnego dostosowujące przepisy art. 267 kk – 269 b kk do wymogów unijnych, zapewniają aktualnie stosunkowo dobry poziom ochrony karno – prawnej przed atakami i działaniami o charakterze hackerskim. Niewątpliwie nie oznacza to, iż ustawodawca nie będzie w przyszłości zmuszony do ewentualnych dalszych zmian nowelizacyjnych odnośnie omawianych czynów karalnych, co jest nieuniknionym następstwem szybkiego postępu technicznego szczególnie dostrzeganego na gruncie technologii informatycznych i telekomunikacyjnych. Rozwój cybertechnologiczny z jednej strony stwarza bowiem nowe możliwości dla ludzkości, z drugiej jednak strony naraża obecne społeczeństwa na nowe, niewyobrażalne jeszcze kilkanaście lat wstecz zagrożenia o charakterze przestępczym. W aspekcie korzystania także przez cyber - przestępców z coraz to doskonalszych narzędzi w postaci nowoczesnego sprzętu komputerowego, oprogramowania, a także coraz szybszej technologii przesyłania danych

[65] K. Gienas, Prawnokarne aspekty „narzędzi hackerskich", op. Cit., s. 35;
[66] A. Adamski, Cyberprzestępczość – aspekty prawne i kryminologiczne, op. Cit., s. 61;
[67] K. Gienas, Uwagi do przestępstwa stypizowanego w art. 296 b kodeksu karnego, op. Cit., s. 76;
[68] K. Gienas, Prawnokarne aspekty „narzędzi hackerskich", op. Cit., s. 37;
[69] K. Gienas, ibidem, s. 35 – 36;

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

i przekazu cyfrowego, zmuszeni jesteśmy do stałego wypatrywania nowych zagrożeń które bez wątpienia stanowić będą nieuniknione następstwa nowych technik i działań hackerskich. Dalszy poziom zagrożeń przynieść mogą także w przyszłości działania hackerskie o charakterze cyberterroryzmu, przeprowadzane przez zorganizowane grupy terrorystyczne, a skierowane głównie na cele o charakterze strategicznym jak np. sieci komputerowe obiektów wojskowych, szpitali, portów lotniczych czy też rejonów energetycznych. Ataki te bez wątpienia nie będą także często ograniczać się do „kradzieży" czy też uszkodzenia danych informatycznych, lecz głównym ich celem może stać się także maksymalizacja strat wynikających ze zniszczenia bądź przeprogramowania systemu informatycznego, mającego bezpośrednie przełożenie na funkcjonowanie określonej społeczności. Już teraz nie trudno sobie bowiem wyobrazić z jakiego rodzaju następstwami bezpośrednio dla ludności mielibyśmy do czynienia w przypadku np. destabilizacji systemu informatycznego zarządzania lotami dużego portu lotniczego, systemu bezpieczeństwa elektrowni atomowej bądź też odpowiedzialnego za niezakłócone dostarczanie energii elektrycznej do dużej aglomeracji miejskiej. W dobie bowiem powierzania często całkowitej kontroli nad istotnymi sferami funkcjonowania społeczeństw „elektronicznym nadzorcom", istnieć musi także stała obawa zakłócenia ich funkii i pracy, w następstwie ataków o charakterze hackerskim. Jest to niewątpliwa cena jaką trzeba zapłacić za możliwość korzystania z tzw. zdobyczy cywilizacyjnych oraz informatycznych ułatwień praktycznie w każdej sferze życia.

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone