Diana BRZEZIŃSKA[1]

Uniwersytet Szczeciński[2]

Wydział Prawa i Administracji

brzezinskadiana@gmail.com

PROBLEMATYKA REGULACJI „NARZĘDZI HACKERSKICH" W POLSKIM KODEKSIE KARNYM

ABSTRAKT: „Narzędzia hackerskie" są programami, które stanowią realne zagrożenie dla cyberprzestrzeni. Umożliwiają one osobom, które nie posiadają specjalistycznej wiedzy z dziedziny programowania popełniać przestępstwa, które do tej pory zarezerwowane były dla węższej grupy osób. W artykule przedstawiono problematykę regulacji „narzędzi hackerskich" w polskim kodeksie karnym z 1997 roku. Wskazano wątpliwości interpretacyjne związane z tym pojęciem oraz omówiono obowiązujące w Polsce regulacje.

SŁOWA KLUCZOWE: „narzędzia hackerskie", cyberprzestępczość, cyberbroń, hacker, hacking

THE ISSUE OF „HACKING TOOLS" IN POLISH CRIMINAL LAW

ABSTRACT: The „hacking tools" are the programs which constitute a real threat for the cyberspace. They allow the people without specialistic programming knowledge to commit crimes that previously were reserved only for a small group of people. This article presents the issue of regulation of the „hacker tools" in the Polish Penal Code of 1997. It points the question of interpretation of the term "the hacker tools" and discusses about the existing Polish legislation.

KEYWORDS: hacking tools, cybercrime, cyberweapon, hacker, hacking

WPROWADZENIE

„Narzędzia hackerskie" to urządzenia i programy komputerowe, które zaprojektowano lub przystosowano do celów popełnienia przestępstwa komputerowego, takiego jak przestępstwo hackingu, czy sabotażu komputerowego. Za „narzędzia hackerskie" uważa się m.in. programy i skrypty zaliczane do grupy złośliwego oprogramowania. Jednym z tego typu programów jest koń trojański, który ma na celu obejście zabezpieczeń systemu. W wyniku jego działania, hacker uzyskuje dostęp do danych, które może następnie usuwać, modyfikować, a

[1] Diana Brzezińska – studentka IV roku prawa na Wydziale Prawa i Administracji Uniwersytetu Szczecińskiego.
[2] University of Szczecin.

także przesyłać na inny komputer3. Konia trojańskiego użytkownik zazwyczaj pobiera nieświadomie wraz z nieszkodliwym oprogramowaniem. Napisanie tego typu programu jest trudne i wymaga specjalistycznej wiedzy. Z tego względu hackerem jest zazwyczaj osoba, która posiada umiejętności techniczne i wiedzę informatyczną, a szczególnie wykazuje się dużą znajomością wielu języków programowania. Sytuacja zmienia się w momencie kiedy „narzędzia hackerskie" zostają udostępnione do użytku osobom trzecim. Do korzystania z nich, nie jest potrzebna specjalistyczna wiedza z dziedziny programowania, w zasadzie każda osoba, posiadająca elementarną wiedzę techniczną, za pomocą „narzędzi hackerskich", jest w stanie uzyskać nieuprawniony dostęp do systemu informatycznego. Z tego względu narzędzia te uważa się za programy stanowiące realne zagrożenie dla cyberprzestrzeni4.

Zagrożenie to zostało dostrzeżone przez społeczność międzynarodową i uregulowane w art. 6 Konwencji Rady Europy o cyberprzestępczości. W polskim kodeksie karnym problematyka ta została umiejscowiona w art. 269b. ustawy z 18 marca 2004 r. o zmianie ustawy Kodeks Karny, ustawy - Kodeks postępowania karnego oraz ustawy - Kodeks wykroczeń. Przepis ten już wówczas spotkał się ze sporą krytyką, ze względu na zbyt szeroką penalizację, jak również błędy w katalogu przestępstw, zawartych w tym przepisie. Jednak ustawodawca nie zdecydował się na jego nowelizację.

Celem artykułu jest omówienie problematyki „narzędzi hackerskich" w polskim prawie karnym oraz wykazanie potrzeby nowelizacji art. 269b k.k. W artykule wskazano, iż użytkowanie „narzędzi hackerskich" prowadzi do powstania nowej grupy hackerów, którzy nie muszą cechować się specjalistyczną wiedzą z dziedziny programowania. W wyniku czego dochodzi do rozszerzenia grupy osób, które są w stanie dopuścić się przestępstw komputerowych. W celu, zapewnienia skutecznej, ochrony przed zagrożeniem płynącym z użytkowania narzędzi hackerskich, należy odpowiednio dostosować polską regulację zawartą w art. 269b k.k.

POJĘCIE „NARZĘDZI HACKERSKICH" W KONWENCJI O CYBERPRZESTĘPCZOŚCI

Pod pojęciem „narzędzi hackerskich", należy rozumieć, m.in. skrypty, programy zaliczane do grupy złośliwego oprogramowania, programy służące do przeprowadzania ataków odmowy usługi, wirusy, robaki, konie trojańskie, rootkity, skanery portów, czy programy służące do łamania haseł i kodów[5]. Tego typu programy określa się jako cyberbroń (*cyberweapons*), definiowaną jako narzędzia służące do walki w sieci. Dzielimy je na te o:

[3] F. Randoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016, s. 182-183.

[4] Cyberprzestrzeń rozumie się jako przestrzeń wirtualną, która umożliwia komunikację między komputerami lub innymi mediami cyfrowymi połączonymi siecią; http://sjp.pwn.pl/sjp/cyberprzestrzeń;2553915 (10.04.2016).

[5] F. Randoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016, s. 182.

- charakterze ofensywnym – programy służące działaniom destrukcyjnym, które zostały utworzone przez hackerów[6]. Do tej grupy zaliczyć możemy właśnie „narzędzia hackerskie", np. Cain&Abel.
- charakterze defensywnym – programy, których zadaniem jest zapewnienie bezpieczeństwa systemom komputerowym, sieci oraz przetwarzanych w nich danych[7], np. firewalle[8].

W praktyce jednak rozróżnienie tych programów nastręcza sporych trudności. Granice pomiędzy programami o charakterze defensywnym i ofensywnym są nieostre. Prowadzi to do powstania programów o tzw. dwoistej naturze, które stosowane są zarówno przez hackerów do ataku internetowego, jak i przez administratorów systemu do sprawdzenia prawidłowości zapór systemowych[9].

Cain&Abel może być przykładem programu o dwoistej naturze. Jest to darmowe narzędzie służące do odzyskiwania haseł w systemie Windows. Program łamie zaszyfrowane hasła stosując słowniki, podsłuchuje sieci, dekoduje zakodowane hasła, odzyskuje klucze sieci bezprzewodowych, wykrywa ukryte hasła oraz analizuje protokoły[10]. Program jest udostępniany na licencji freeware[11]. Można pobrać go w wielu serwisach, a więc dostępność do niego jest względnie łatwa. Dedykowany jest dla administratorów sieci, nauczycieli, konsultantów zajmujących się bezpieczeństwem, śledczych, itp.[12]. Zatem jest to program użytkowy. Bez trudu jednak można go wykorzystać jako „narzędzie hackerskie".

POJĘCIE „NARZĘDZI HACKERSKICH" W POLSKIM PRAWIE KARNYM

Choć polskie prawodawstwo nie definiuje wprost pojęcia „narzędzi hackerskich", na podstawie art. 269b k.k. można je uznać za „programy komputerowe przystosowane do popełnienia przestępstwa" określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268 § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a. Uznaje się za nie również hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub w sieci teleinformatycznej.

Zwrot „programy komputerowe przystosowane do popełnienia przestępstwa" powoduje trudności interpretacyjne. Jak słusznie wskazuje P. Siemkowicz, rozróżnienie „narzędzi hackerskich" od legalnych programów komputerowych w praktyce może okazać się problema-

[6] *Ibidem*, s. 183.
[7] *Ibidem.*
[8] Firewalle to tzw. ściana przeciwogniowa. Najprościej mówiąc jest to program zabezpieczający sieć przed nieuprawnionym dostępem z zewnątrz.
[9] P. Siemkowicz, *Przestępstwa skierowane przeciwko poufności, integralności i dostępności danych oraz systemów komputerowych w polskim kodeksie karnym - z uwzględnieniem aktualnych zmian nowelizacyjnych,* CBKE e-biuletyn, s. 17.
[10] http://download.komputerswiat.pl/bezpieczenstwo/odzyskiwanie-danych/cain-abel (10.04.2016).
[11] Freeware to licencja oprogramowania, która pozwala na bezpłatne użytkowanie i rozpowszechnianie programów. Licencja nie zezwala na sprzedaż programów, dokonywanie w nich zmian; http://zsp.szubin.pl /zadania/Pomoce/Licencje/rodzaje_licencji.html (10.04.2016).
[12] *Ibidem.*

tyczne[13]. Administratorzy systemów korzystają z legalnych programów komputerowych, które zostały napisane w celu testowania sprawności systemów komputerowych oraz ich stabilności. Analitycy systemów komputerowych potwierdzają skuteczność zabezpieczeń poprzez symulowanie prób ataków[14]. Z tego względu programy, z których korzystają administratorzy systemów, zbliżone są w swoim działaniu do programów hackerskich. Kwestia ta staje się problematyczna przy próbie rozróżnienia programu hackerskiego od programu użytkowego[15]. Przede wszystkim ze względu na programy o dwoistej naturze, o których już wspomniałam.

P. Siemkowicz, w celu rozwiązania problemu interpretacyjnego, proponuje zastosowanie rozróżnienia funkcjonalnego. Według niego program staje się „narzędziem hackerskim" wyłącznie wtedy, gdy zostanie użyty bezpośrednio do ataku hackerskiego spoza sieci, w celu jakiejkolwiek ingerencji w nienaruszalność innego systemu komputerowego. Natomiast w sytuacji gdy program o podobnych cechach służy administratorowi systemu do jego testowania wewnątrz systemu, bez wyrządzania szkody w systemie, jest on wówczas programem użytkowym[16]. Jednakże ten tok myślenia może być zawodny, bowiem nie obejmuje on wszystkich możliwych sytuacji wykorzystania tego typu programów.

Natomiast jeśli chodzi o hasła komputerowe i kody dostępu, definicja zaproponowana przez W. Wróbla, wydaje się dostatecznie jednoznaczna:

> *pojęcie haseł komputerowych i kodów dostępu stanowi egzemplifikacje danych, umożliwiających dostęp do informacji przechowywanych w systemach informatycznych i sieciach teleinformatycznych. Z reguły jest to ciąg znaków w postaci elektronicznej, których wprowadzenie do systemu umożliwia dokonywanie w nim określonych operacji*[17].

Na chwilę obecną nie dysponujemy definicją, która pozwoliłaby jednoznacznie oddzielić programy nielegalne, od programów legalnych. Problem polega na tym, że każdy z programów legalnie wytworzonych może zostać wykorzystany w celach przestępczych, wbrew woli ich producenta. Podobnie wygląda sytuacja z hasłami komputerowymi i kodami dostępów. Hackerzy potrafią je wykraść, a to już stanowi potencjalne zagrożenie dla danych, które zostały za ich pomocą zabezpieczone.

[13] P. Siemkowicz, *op. cit.*, s. 17.
[14] *Ibidem.*
[15] Oprogramowanie użytkowe oferuje bezpośredni kontakt z człowiekiem, realizuje więc interakcję z użytkownikiem komputera. Przeznaczone jest do wykonywania czynności oraz rozwiązywania problemów zadanych przez użytkownika, np. arkusz kalkulacyjny; https://pl.wikipedia.org/wiki/Oprogramowanie_użytkowe (10.04.2016).
[16] P. Siemkowicz, *op. cit.*, s. 17.
[17] A. Zoll (red.), *Kodeks karny. Część szczególna tom II, komentarz art. 117-277 K.K.*, Warszawa 2013, s. 1529.

REGULACJA ART. 269 B K.K.

B. Kunicka-Michalska wskazuje, że bezpośrednim przedmiotem ochrony art. 269b k.k. „jest poufność, integralność, i dostępność danych informatycznych i systemów, a zarazem bezpieczeństwo informacji przetwarzanych elektronicznie”[18]. Ten przedmiot ochrony właściwy jest również dla przestępstw wymienionych w art. 269b k.k.

Ustawodawca kryminalizuje następujące sposoby działania sprawcy:

- wytwarzanie[19] takich urządzeń/programów/haseł komputerowych/kodów dostępu;
- pozyskiwanie[20] takich urządzeń/programów/haseł komputerowych/kodów dostępu;
- zbywanie[21] takich urządzeń/programów/haseł komputerowych/kodów dostępu;
- udostępnianie innym osobom[22] takich urządzeń/ programów/ haseł komputerowych/ kodów dostępu.

Zatem przepis ten penalizuje czynności przygotowawcze (wytwarzanie/ pozyskiwanie/ zbywanie/ udostępnianie innym osobom) podejmowane w celu dokonania jednego z wymienionych w tym artykule przestępstw, a więc art. 165 § 1 pkt 4 (sprowadzenie niebezpieczeństwa dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach poprzez zakłócanie, uniemożliwianie lub wywarcie w inny sposób wpływu na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych), art. 267 § 3 (nielegalny podsłuch i inwigilacja za pomocą urządzeń technicznych i programów komputerowych), art. 268a § 1 albo § 2 w związku z § 1 (naruszenie integralności danych, utrudnianie dostępu do danych oraz zakłócanie ich przetwarzania), art. 269 § 2 (sabotaż komputerowy) albo art. 269a (zakłócenie pracy systemu komputerowego lub sieci teleinformatycznej), a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej.

KRYTYKA REGULACJI ART. 269 B K.K.

W katalogu przestępstw w art. 269b k.k. ustawodawca nie uwzględnił art. 267 § 1 k.k. (uzyskanie dostępu bez uprawnienia do informacji dla niego nieprzeznaczonej przez podłączenie się do sieci telekomunikacyjnej lub przez przełamanie albo ominięcie elektronicznego, magnetycznego, informatycznego lub innego szczególnego zabezpieczenia), art. 267 § 2 k.k.

[18] B. Kunicka-Michalska *Przestępstwo z art. 269b KK* [w:] L. Gardocki (red.), *System prawa karnego t. 8*, Warszawa 2013, s. 969.

[19] Przez „wytwarzanie” rozumiemy uczestnictwo w procesie zmierzającym do stworzenia urządzenia lub programu; M. Królikowski (red.), *Kodeks Karny. Część szczególna. Tom II*, Warszawa 2013, s. 455.

[20] Przez „pozyskiwanie” należy rozumieć wejście w posiadanie oraz możliwość korzystania, np. przez nabycie haseł komputerowych lub kodów dostępu; M. Królikowski (red.), *op. cit.*, s. 455.

[21] Znamię „zbycia” utożsamiać należy z przeniesieniem własności na inną osobę; M. Królikowski (red.), *op. cit.*, s. 455.

[22] „Udostępnianie” oznacza uczynienie urządzeń, programów komputerowych lub danych dostępnymi dla innej osoby. „W doktrynie podkreśla się, że nie stanowi realizacji znamion komentowanego przestępstwa samo poinformowanie innych osób o sposobie, w jaki można pozyskać określone dane czy program, np. poprzez zamieszczenie ścieżki dostępu do innej witryny internetowej. Zachowanie takie może natomiast stanowić karalne pomocnictwo do pozyskania danych lub programów, o których mowa w art. 269b k.k.”; A. Zoll (red.), *op. cit.*, s. 1317.

(uzyskanie dostępu bez uprawnienia do całości lub części systemu informatycznego), art. 268 § 2 k.k. (zniszczenie, uszkodzenie, usunięcie lub zmienienie zapisu istotnej informacji, znajdującej się na informatycznym nośniku danych albo w inny sposób udaremnienie lub znaczne utrudnienie osobie uprawnionej zapoznania się z nią przez osobę nieuprawnioną), art. 269 § 1 k.k. (zniszczenie, uszkodzenie, usunięcie, zmienienie danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłócenie lub uniemożliwienie automatycznego przetwarzania, gromadzenia lub przekazywani takich danych).

Wydaje się, że ze względu na pominięcie tych przestępstw konstrukcja tego artykułu jest wadliwa. Ustawodawca nie zdecydował się wskazać w jego treści hackingu *sensu stricto* (nieuprawnionego uzyskania informacji z art. 267 § 1 k.k. oraz nieuprawnionego dostępu do systemu informatycznego z art. 267 § 2 k.k.)[23]. Biorąc więc pod uwagę, to że „narzędzia hackerskie" służą m.in. do nieuprawnionego uzyskania informacji, a przede wszystkim do nieuprawnionego uzyskania dostępu do systemu informatycznego, to nieumieszczenie w tym katalogu, art. 267 § 1 k.k. jest przeoczeniem ustawodawcy.

W art. 269b k.k. nie uwzględniono również art. 269 § 1, który penalizuje zniszczenie, uszkodzenie, usunięcie, zmienienie danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego, zakłócenie lub uniemożliwienie automatycznego przetwarzania, gromadzenia lub przekazywani takich danych. Za to zdecydowano się uwzględnić art. 269 § 2 k.k., w którym stypizowano zachowanie polegające na zniszczeniu albo wymienieniu informatycznego nośnika danych lub zniszczeniu albo uszkodzeniu urządzenia służącego do automatycznego przetwarza, gromadzenia lub przekazywania danych informatycznych. Niezwykle trudno pojąć takie działanie ustawodawcy. Nie sposób bowiem znaleźć program komputerowy, hasło komputerowe albo kod dostępu, który byłby w stanie zniszczyć lub wymienić informatyczny nośnik danych albo w jakikolwiek inny sposób dokonać jego fizycznego uszkodzenia. Wydaje się również, że fizyczne uszkodzenie informatycznego nośnika danych nie leży w kręgu zainteresowań hackerów, jak wskazuje B. Hołyst:

> *Hakerzy dążą do zdobycia dostępu do informacji wybranej sieci przez Internet, wykorzystując zarówno luki bezpieczeństwa w systemach, w których pracują serwery Internetu, błędy w protokołach transmisji danych i konfiguracji serwerów WWW, jak i destabilizując systemy zabezpieczeń*[24].

[23] F. Randoniewicz, *Odpowiedzialność karna za hacking…*, *op. cit.*, s. 335.
[24] B. Hołyst, *Kryminologia*, Warszawa 2009, s. 403.

Możliwym jest, że w tej kwestii doszło do błędu ustawodawcy. Zamiast art. 269 § 1 k.k, znalazł się w nim art. 269 § 2 kk. Jeżeli tak jest, to niestety ustawodawca do tej pory nie zdecydował się naprawić tego błędu.

Przepis nie zawiera również żadnych wyłączeń. Zdaniem B. Kunickiej-Michalskiej, wobec administratorów sieci, czy osób zajmujących się bezpieczeństwem systemów informatycznych, „jako działających w ramach praw i obowiązków, ma miejsce wyłączenie odpowiedzialności karnej”[25]. Za taką interpretacją przemawia art. 6 ust. 2 Konwencji o cyberprzestępczości:

> *Art. 6 ust. 2. Niniejszego artykułu nie należy interpretować jako mającego na celu pociągnięcie do odpowiedzialności karnej w przypadku, kiedy produkcja, sprzedaż, pozyskiwanie z zamiarem wykorzystania, importowanie, dystrybucja lub inne udostępnianie lub posiadanie, o którym mowa w ustępie 1 niniejszego artykułu, nie jest dokonywane w celu popełnienia przestępstwa określonego zgodnie z artykułami 2-5 niniejszej konwencji, jak w przypadku dozwolonego testowania lub ochrony systemu informatycznego.*

Jednak za F. Randoniewiczem należy podkreślić, iż „dla bytu tego przestępstwa, zgodnie z Konwencją o cyberprzestępczości, musi być spełniony – po pierwsze – wymóg, by sprawca miał zamiar, by narzędzie zostało użyte do popełnienia przestępstwa określonego w art. 2-5, a więc by działał w zamiarze kierunkowym”[26]. Nietrudno zauważyć, iż nasza regulacja nie do końca odpowiada temu kryterium.

Część znamion przestępstwa, z art. 269b k.k., wymaga by sprawca działał w zamiarze bezpośrednim, np. powzięcie decyzji o wytworzeniu, zbyciu programu. Jednak pozostałe znamiona sprawca może wypełnić w zamiarze ewentualnym, np. przystosowanie programu komputerowego lub urządzenia do popełnienia przestępstwa, udostępnienie programu innym osobom. W art. 269b k.k. nie umieszczono wymogu popełnienia czynu zabronionego w określonym celu, nie możemy więc uznać go za przepis kierunkowy. Nie wymaga się, bowiem od sprawcy działania w zamiarze kierunkowym[27], co bez wątpienia ułatwiłoby interpretację tego przepisu. Pozwalałoby bowiem na wyłączenie odpowiedzialności administratorów sieci, czy osób zajmujących się bezpieczeństwem systemów informatycznych, gdyż wytwarzając tego typu programy lub udostępniając je innym osobom nie działałyby w zamiarze kierunkowym, a więc w celu popełnienia przestępstwa z art. 269 k.k. Nie zostało to jednak sformułowane w przepisie.

Niestety na krytykę zasługuje również nieostra definicja programu przystosowanego do popełnienia przestępstwa. „Po drugie, urządzenia i programy komputerowe muszą być zaprojektowane lub przystosowane głównie do popełnienia któregoś z przestępstw określonych w Konwencji o cyberprzestępczości”[28]. Zdaniem F. Randoniewicza, „po pierwsze, w przepisie

[25] Cyt za F. Randoniewicz, *Odpowiedzialność karna za hacking…*, *op. cit.*, s. 336.
[26] *Ibidem.*
[27] Ł. Pohl, *Prawo karne. Wykład części ogólnej,* Warszawa 2013, s. 136.
[28] F. Randoniewicz, *Odpowiedzialność karna za hacking…*, *op. cit.*, s. 336.

tym mowa jest o programach „przystosowanych" do określonych działań. Istnieje zatem problem, jak ocenić działanie twórcy programu spełniającego kilka funkcji (tzw. programy o podwójnej naturze), użytego następnie przez osobę trzecią w celach przestępczych, których autor by sobie nie życzył"[29]. W pełni podzielam zdanie F. Randoniewicza, w tej kwestii. Jak już wskazywałam, przykładowym programem o podwójnej naturze jest Cain&Abel. Twórca programu stworzył go co prawda do łamania zaszyfrowania haseł, podsłuchiwania sieci, dekodowania haseł, itp., ale z założenia program ten przeznaczony jest dla administratorów sieci, nauczycieli, czy śledczych. Życzeniem autora zdecydowanie nie było jego wykorzystywanie przez hackerów. Nie zmienia to jednak faktu, że program ten możemy uznać za „narzędzie hackerskie". Istnienie programów o podwójnej naturze uwidacznia zbyt szeroką kryminalizację tego przepisu.

HACKER, KTÓRY NIE PROGRAMUJE

Szybki rozwój „narzędzi hackerskich" spowodował, że liczba potencjalnych sprawców przestępstwa hackingu znacznie wzrosła. Zmieniły się również cechy, które charakteryzują sprawców. W wyniku czego grupa tzw. hackerów wciąż ulega powiększeniu.

Według statystyk z 2012 roku, przestępstwa hackingu dopuszczają się głównie osoby w wieku 17-20 lat (około 40 proc.). Kolejne dwie grupy również zasługują na uwagę: osoby w przedziale 21-25 lat popełniają 25 proc. przestępstw, zaś te w wieku 26-30 lat 26 proc[30]. Jak widać sprawcami tego typu czynu są ludzie młodzi. Dla porównania osoby w wieku 51-60 lat stanowią zaledwie 1 proc. Aż 51 proc.[31] z tych osób posiadało wykształcenie średnie, a 20 proc. wyższe[32]. Każdy z tych sprawców musiał posiadać podstawową wiedzę na temat programowania. Niekoniecznie musiało to oznaczać wykształcenie w tym kierunku. Wystarczyły predyspozycje i umiejętności.

Bardziej aktualne statystyki odpowiadają tym poprzednim. Nadal głównymi sprawcami hackingu są ludzie młodzi w wieku 17-30 lat [17-20 lat (30 proc.); 21-25 lat (25 proc.); 26-30 lat (19 proc.)][33]. Statystyki dotyczące ich wykształcenia nie uległy zmianie. Najczęstszymi sprawcami hackingu ponownie okazują się osoby z wykształceniem średnim – 51 proc. oraz wyższym – 20 proc.[34]. Co nie oznacza, że niebawem ta sytuacja nie ulegnie zmianie.

Dzisiaj przestępstwa hackingu na mniejszą skalę może dopuścić się w zasadzie każdy. „Narzędzia hackerskie" zdecydowanie nam to ułatwiają. Umożliwiają bowiem osobom z elementarną wiedzą z dziedziny informatyki popełnić przestępstwo. Sprawia to, że grupa potencjalnych sprawców ulega powiększeniu. Dla przykładu program Cain&Abel, o którym już wspomniałam, jest bardzo łatwo dostępny. Jego obsługa może wydać się skomplikowana,

[29] *Ibidem,* s. 335.
[30] F. Randoniewicz, *Odpowiedzialność karna za przestępstwo hacking…, op. cit.,* s. 58.
[31] *Ibidem.*
[32] *Ibidem.*
[33] F. Randoniewicz,, *Odpowiedzialność karna za hacking…, op. cit.,* s. 440-441.
[34] *Ibidem.*

ale w Internecie dostępnych jest mnóstwo instrukcji, oraz tutoriali na temat jego funkcji i zastosowań. Nie trzeba mieć ogromnej wiedzy z dziedziny informatyki żeby z niego korzystać. Ktoś wytworzy tego typu program, sprzeda go, a osoba która go kupi staje się potencjalnym sprawcą przestępstwa hackingu.

Liczba postępowań wszczynanych na podstawie art. 269b k.k. z roku na rok wzrasta. W 2005 roku było ich zaledwie 6 (stwierdzono 6 przestępstw)[35], w 2014 roku już 47 (stwierdzono 43 przestępstwa)[36]. Z roku na rok rośnie również liczba postępowań wszczynanych na podstawie art. 267 k.k. W 1999 roku wszczęto 182 postępowania (stwierdzono 113 przestępstw), w 2005 roku wszczęto 430 postępowań (stwierdzono 260 przestępstw), a w 2014 roku aż 2868 postępowań (stwierdzono 1901 przestępstw)[37]. „Narzędzia hackerskie" już od lat mają wpływ na tę sytuację. Przestępstwo hackingu przestało być zarezerwowane dla osób, które posiadają specjalistyczną wiedzę z dziedziny programowania oraz specjalistyczny sprzęt. Dzięki możliwości wykorzystania „narzędzi hackerskich", przestępstwa tego może dopuścić się osoba, która posiada standardowy komputer oraz potrafi poprawnie pobrać program z Internetu i go zainstalować. Samo korzystanie z tego typu programów również nie nastręcza większych trudności, gdyż w Internecie istnieje mnóstwo witryn, które zawierają praktyczne instrukcje.

PODSUMOWANIE

Przepis art. 269b k.k. miał stanowić swego rodzaju panaceum na problem łatwo dostępnych „narzędzi hackerskich". Z założenia miał wskazać czym są tego rodzaju narzędzia oraz w jakich przypadkach lub w jakim celu zabronione jest ich wytwarzanie, pozyskiwanie, zbywanie lub udostępnianie osobom trzecim. Niestety ustawodawca dokonał zbyt szerokiej kryminalizacji tego przepisu.

Obecnie nie reguluje on sytuacji osób, które zawodowo zajmują się wytwarzaniem, zbywaniem, przystosowaniem lub udostępnianiem innym osobom upoważnionym programów komputerowych lub urządzeń, które mogłyby zostać wykorzystane do popełnienia przestępstwa, pomimo tego, że wcale nie zostały w tym celu utworzone. Wydaje się, że znacznie lepszym rozwiązaniem, byłoby nadanie przepisowi art. 269b k.k. kierunkowości. Dzięki temu już na poziomie tego artykułu można byłoby wyłączyć działalność osób, które posiadają upoważnienie do tworzenia programów, które mogłyby zostać użyte jako „narzędzia hackerskie".

Ustawodawca, w katalogu przestępstw z art. 269b k.k., nie umieścił również hackingu *sensu stricto* (art. 269 § 1 k.k.). Ponadto zamiast art. 269 § 2 k.k. w katalogu umieszczono prawdopodobnie art. 269 § 1 k.k. Dodanie przepisu art. 269b do kodeksu karnego zdecydo-

[35] *Statystyka Policji*, http://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-14/63633, Wytwarzanie - programu - komputerowego-do-popelnienia-przestepstwa-art-269b.html (10.04.2016).
[36] *Ibidem*.
[37] *Ibidem*.

wanie było zabiegiem słusznym, jednak przepis wymaga nowelizacji, ze względu na wyżej wymienione uchybienia.

Podsumowując, masowa dostępność „narzędzi hackerskich" spowodowała rozszerzenie grupy potencjalnych sprawców hackingu. Korzystanie z tego typu programów nie jest skomplikowane i nie wymaga specjalistycznej wiedzy z zakresu programowania, co sprawia, że nawet osoba z elementarną wiedzą z dziedziny informatyki może dopuścić się tego przestępstwa na mniejszą skalę.

BIBLIOGRAFIA

Definicja W https://pl.wikipedia.org/wiki/Oprogramowanie_użytkowe.

Gardocki Lech (red.). 2013. System prawa karnego. Tom VIII. Warszawa: C.H. Beck.

Hołyst Brunon. 2009. Kryminologia. Warszawa: Lexis Nexis.

Królikowski Michał (red.). 2015. Kodeks Karny - część szczególna. Tom II. Warszawa: C.H. Beck.

Kruzerowski Marek. 2003. W http://zsp.szubin.pl/zadania/Pomoce/Licencje/rodzaje_licencji.html.

Opis programu W http://download.komputerswiat.pl/bezpieczenstwo/odzyskiwanie-danych/cain-abel.

Pohl Łukasz. 2013. Prawo karne. Wykład części ogólnej. Warszawa: Lexis Nexis.

Randoniewicz Filip. 2012. Odpowiedzialność karna za przestępstwo hackingu. Warszawa: Instytut Wymiaru Sprawiedliwości.

Randoniewicz Filip. 2016 rok. Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym. Warszawa: Wolters Kluwer.

Siemkowicz Piotr. 2009. Przestępstwa skierowane przeciwko poufności, integralności i dostępności danych oraz systemów komputerowych w polskim kodeksie karnym – z uwzględnieniem aktualnych zmian nowelizacyjnych. CBKE e-biuletyn nr 2/2009. W http://www.bibliotekacyfrowa.pl/Content/34363/Przestepstwa_skierowane.pdf.

Słownik języka polskiego PWN. W http://sjp.pwn.pl/sjp/cyberprzestrzeń;2553915.

Statystyka Policji W http://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-14/63633,Wytwarzanie-programu-komputerowego-do-popelnienia-przestepstwa-art-269b.html.

Zoll Andrzej (red.). 2013. Kodeks karny. Część szczególna. Tom II. Warszawa: Wolters Kluwer.

AKTY PRAWNE

Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r., ratyfikowana dnia 28 października 2014 roku. Dz.U. 2014 poz. 1514.

Ustawa z dnia 6 czerwca 1997 roku kodeks karny. Dz.U. 1997 nr 88 poz. 553.