Ekonomiczne Problemy Usług nr 1/2017 (126), t. 2

ISSN: 1896-382X | www.wnus.edu.pl/pl/edu
DOI: 10.18276/epu.2017.126/2-19 | strony: 185–194

Renata Jedlińska
Uniwersytet Jana Kochanowskiego w Kielcach
Wydział Prawa, Administracji i Zarządzania
e-mail: rene28@poczta.onet.pl

Problem przestępczości elektronicznej

Kod JEL: K42
Słowa kluczowe: cyberprzestrzeń, hacking, przestępczość komputerowa, craker
Streszczenie. W artykule przedstawiono genezę i specyfikę przestępstw elektronicznych, co wynika przede wszystkim z tego, że miejsca, gdzie są one dokonywane, nie zawsze są „miejscami" w dosłownym tego słowa znaczeniu. Wykorzystywanie internetu jako miejsca popełniania przestępstwa jest szczególnie niebezpieczne, ze względu na bardzo wysoką liczbę potencjalnych ofiar oraz trudności w wykrywaniu sprawców przestępstw. Światowa sieć informatyczna zmniejsza efektywność mechanizmów identyfikacji. Cyberprzestrzeń pozbawiona jest wszelkich fizycznych atrybutów czyjejś obecności, takich jak: odciski palców, głos, wizerunek. Celem artykułu jest pokazanie zasięgu i skali przestępczości elektronicznej na świecie, a także negatywnych skutków, które są jej efektem.

Wprowadzenie

Gwałtowny rozwój techniki w końcu XX wieku spowodował powstanie wielu nowych zjawisk, które z uwagi na swe społeczne niebezpieczeństwo i szkodliwość, są ścigane jako przestępstwa lub wykroczenia. Jednym z takich zjawisk, wynikającym z ogromnego postępu technicznego w przetwarzaniu i przechowywaniu informacji jest przestępczość popełniana za pomocą nowoczesnych technologii teleinformatycznych – przestępstwa komputerowe[1].

Przestępczość komputerowa (cyberprzestępczość) jest nową i jedną z najszybciej rozwijających się form przestępczości transgranicznych. Internet stał się niemal niezbędnym elementem naszego życia, dzięki któremu można przekazywać informacje

[1] www.unic.un.org.pl.

i komunikować się z całym światem, dlatego przestępcy wykorzystują związane z tym możliwości. Obecnie z cyberprzestrzeni korzysta kilka miliardów użytkowników. Jest to idealna przestrzeń dla przestępców, którzy pozostając anonimowi uzyskują dostęp do naszych danych osobowych (Jakubowski, 1996).W artykule w pierwszej kolejności przedstawiłam zagadnienia dotyczące genezy, rodzajów i metod przestępczości elektronicznej. Następnie omówiłam kwestie dotyczące sprawców przestępstw komputerowych i metod ich zwalczania. Celem niniejszego artykułu jest więc pokazanie olbrzymiego, negatywnego wpływu przestępczości elektronicznej na życie współczesnego człowieka we wszystkich sferach jego funkcjonowania.

1. Geneza przestępczości elektronicznej

Przestępstwa komputerowe pojawiły się, gdy komputery przestały być ściśle strzeżonym przedmiotem zamówień rządowych i stały się dostępne dla instytucji gospodarczych.

Komputeryzacja była wykorzystywana do sterowania rutynowymi czynnościami w gospodarce i administracji już na początku lat 50. XX wieku, jednak dopiero w latach 60. ujawniono pierwsze, a w 70. poważniejsze wypadki oszustw, sabotażu, a także szpiegostwa gospodarczego z wykorzystaniem komputerów (Kosiński, 2015, s. 33–35).

W latach 60. XX wieku rozpoczęło się masowe przetwarzanie informacji, danych osobowych przez tworzenie banków danych. Brak ograniczeń związanych z dostępem do tych danych wkrótce odebrano jednak jako zagrożenie praw obywatelskich. Niemal równocześnie z pojawieniem się w latach 70. otwartych systemów sieciowych rozpowszechniły się ich nadużycia określane jako Hawking[2].

Upowszechnienie komputerów osobistych w latach 80. spowodowało masowe zjawisko sporządzania pirackich kopii programów, a rozwinięcie sieci bankomatów, natychmiast skutkowało nadużyciami za pomocą kart magnetycznych. Zorganizowane grupy przestępcze zaczęły wykorzystywać powszechność poczty elektronicznej, a także ścisłe powiązania między systemami przetwarzania danych a telekomunikacją, również do celów przestępczych zarówno kryminalnych, jak i gospodarczych, a nawet do perfekcyjnego zacierania śladów przestępstwa.

W latach 90. komputery stały się integralnym elementem niemal każdej dziedziny życia. Rozwój światowych sieci komputerowych, stała obniżka cen oraz powstanie programów przyjaznych dla użytkownika niewymagających specjalistycznej wiedzy sprzyjały coraz szerszemu używaniu tych urządzeń. W naturalny sposób stały się one przedmiotem działalności sprzecznej z prawem (Siwicki, 2013, s. 162).

[2] http://prawo.vagla.pl.

2. Przestępczość elektroniczna i jej rodzaje

Nie istnieje jedna wyczerpująca definicja tego zjawiska. Każdy z ekspertów ma swoje własne określenie. Według K. Jakubowskiego pojęcie przestępczości elektronicznej jest nieprecyzyjne i wieloznaczne: „W szerokim rozumieniu, przestępczość ta obejmuje wszelkie zachowania przestępne związane z funkcjonowaniem elektronicznego przetwarzania danych, polegające zarówno na naruszaniu uprawnień do programu komputerowego, jak i godzące bezpośrednio w przetwarzaną informację, jej nośnik i obieg w komputerze oraz cały system połączeń komputerowych, a także w sam komputer. Należy tu zaznaczyć, iż będą to zarówno czyny popełniane przy użyciu elektronicznych systemów przetwarzania danych (komputer jako narzędzie do popełnienia przestępstwa), jak i skierowane przeciwko takiemu systemowi" (Kosiński, s. 126). Międzynarodowa Organizacja Policji Kryminalnych Interpol definiuje przestępczość elektroniczną jako przestępczość w zakresie technik komputerowych. Przestępstwami obejmowanymi zbiorczą nazwą komputerowych są zarówno czyny skierowane przeciwko systemowi komputerowemu (gdzie komputer jest celem ataku), jak i czyny dokonane przy użyciu komputera.

Komputery oraz sieci komputerowe mogą uczestniczyć w przestępstwie na kilka sposobów:

- komputer lub sieć mogą być narzędziem przestępstwa (zostaną użyte do jego popełnienia),
- komputer lub sieć mogą być celem przestępstwa (ofiarą),
- komputer lub sieć mogą być użyte do zadań dodatkowych związanych z popełnieniem przestępstwa (np. do przechowywania danych o nielegalnych działaniach) (Grzelak, Liedel, 2014, s. 134).

Przestępczość elektroniczna często nazywana jest przestępczością komputerową bądź też cyberprzestępczością. W polskim prawie zdefiniowane są przestępstwa z użyciem komputerów, nie ma jednak oficjalnej definicji cyberprzestępstwa. Taką definicję wypracował X Kongres ONZ w Sprawie Zapobiegania Przestępczości i Traktowania Przestępców:

- cyberprzestępstwo w wąskim sensie (przestępstwo komputerowe), to wszelkie nielegalne działanie, wykonywane w postaci operacji elektronicznych, wymierzone przeciw bezpieczeństwu systemów komputerowych lub procesowanych przez te systemy danych,
- cyberprzestępstwo w szerokim sensie (przestępstwo dotyczące komputerów), to wszelkie nielegalne działanie, popełnione za pomocą lub dotyczące systemów lub sieci komputerowych, włączając w to między innymi nielegalne posiadanie i udostępnianie lub rozpowszechnianie informacji przy użyciu systemów lub sieci komputerowych (*Wymiana doświadczeń*…, 2008).

Cyberprzestępczość oznacza działalność mającą na celu wyrządzenie szkód za pomocą sieci teleinformatycznych, w szczególności internetu. Z reguły bywa tak, że wspaniałe osiągnięcia umysłu ludzkiego w zakresie elektroniki, informatyki i telekomunikacji, które w ostatnich dekadach gruntownie odmieniły nasze życie i bez których młodsza część społe-

czeństwa nie wyobraża sobie funkcjonowania, nie są wolne od zagrożeń.

To oczywiste, że w jednym kraju pewne działanie uznane za nielegalne w innym może być dozwolone, ma to zwłaszcza ogromne znaczenie w najczęstszej w internecie sytuacji, kiedy sprawcę dzielą tysiące kilometrów od ofiary.

Wraz z rozwojem elektronicznego handlu za pośrednictwem internetu wyłoniły się kolejne rodzaje przestępstw:

1. Kradzież danych o kartach kredytowych – hakerzy wykorzystując luki w zabezpieczeniach, wykradają dane o kartach kredytowych, za pomocą których klienci regulują płatności.
2. Oszustwa w handlu online – bardziej wyrafinowani hakerzy mogą wręcz udawać poważne firmy handlujące określonym towarem. Podszywają się pod znanych sprzedawców wykorzystując to, że przez internet nie można sprawdzić tożsamości. Zagrożeniem dla kupujących w sklepach online są również nieuczciwi sprzedawcy. Ponieważ z reguły trudno jest do nich dotrzeć, pozwalają sobie na niewywiązanie się z umowy łub dostarczenie wybrakowanych towarów i usług.
3. Pranie brudnych pieniędzy – opracowanie metody dokonywania przez internet transakcji przelewu pieniędzy z konta na konto w ciągu sekundy, przez naciśnięcie kilku klawiszy wywołało zjawisko „prania brudnych pieniędzy". Przestępcy, szczególnie handlarze bronią i narkotykami, wykorzystują możliwości jakie daje internet do ukrywania swoich źródeł dochodów oraz dysponowania pieniędzmi i dokonywania przelewów bez obawy wykrycia.
4. Rozpowszechnianie pornografii – łatwość przesyłania danych przez internet sprzyja aktywności osób związanych z produkcją i dystrybucją pornografii. Chociaż w internecie istnieje zakaz zamieszczania treści wulgarnych czy sprzecznych z prawem, to w sieci można znaleźć, skopiować oraz przesłać pornograficzne zdjęcia, filmy, jak też rozmawiać na forach dyskusyjnych na temat dowolnej formy seksu. Groźniejszym przestępstwem jest rozpowszechnianie w sieci pornografii dziecięcej oraz ułatwianie kontaktów pedofilskich. Według danych z 1996 roku strony WWW z takimi materiałami odwiedziło 170 tys. użytkowników miesięcznie, trzeba zwrócić uwagę na to, że było to 13 lat temu (Sucharzewska 2010, s. 123–128).

Polskie prawo karne przewiduje kilka rodzajów przestępczości komputerowej. Przepisy te nie są zebrane w całość lecz rozmieszczone w poszczególnych rozdziałach Kodeksu karnego z 1997 roku, dodatkowo osobno zebrane zostały formy piractwa komputerowego, ich katalog zamieszczono w Ustawie z 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (t.j. Dz.U z 2002 r., nr 80, poz. 904 z późn. zm.). Osobno ujęto również nielegalne kopiowanie układów scalonych. Zajęła się tym zagadnieniem Ustawa z 30 marca 2002 roku Prawo własności przemysłowej (t.j. Dz.U z 2003 r., nr 119, poz. 1117).

3. Metody przestępczości

W literaturze wyróżnia się bardzo wiele metod przestępczego działania bezpośrednio wpływającego na system komputerowy. Do najczęstszych i najbardziej rozpowszechnionych należą:

- niszczenie danych (np. podrabianie lub przerabianie dokumentów, naruszanie oryginalnych zapisów),
- tzw. konie trojańskie i inne wirusy komputerowe,
- metoda „salami", czyli kradzież małych sum z różnych źródeł,
- superzapping, czyli bezprawne wykorzystywanie programów użytkowych przez zmiany, zniszczenie lub ujawnienie danych,
- tzw. podnoszone drzwi (urządzenia sprzyjające dokonaniu przestępstwa),
- przeciek danych,
- asynchroniczne ataki i tzw. bomby logiczne,
- podsłuch,
- używanie komputera jako narzędzia planowania oraz kontroli przestępczości,
- oczyszczanie, czyli przeszukiwanie komputera,
- piggybacking (nieupoważnione wejście do obiektów strzeżonych),
- impersonacja (podszywanie się pod uprawnionego użytkownika) (Sowa, 2001).

Przykładem jak wielkie szkody może wyrządzić atak poprzez internet jest internetowy paraliż Estonii, jednego z najbardziej zinformatyzowanego na świecie kraju. W 2007 roku doszło tam do pierwszego w historii skutecznego ataku na główne instytucje państwa dokonanego spoza jego terytorium środkami elektronicznej komunikacji.

Planowa, perfidna akcja internetowa doprowadziła do paraliżu działalności rządu, partii politycznych, mediów, banków. Zasadnicza strategia ataku była prosta i znana od lat, choć nigdy dotąd nie została wykorzystana na taką skalę. Polega na przesyłaniu do serwerów obsługujących atakowane instytucje olbrzymiej liczby danych i próśb o informacje, co powoduje faktyczne unieruchomienie tych serwerów. Organizacja i koordynacja akcji była nieprawdopodobnie sprawna, w szczytowym momencie, po dwóch tygodniach „wojny", dziesiątki tysięcy komputerów na całym świecie zmuszono przez rozsyłających złośliwy software inicjatorów akcji do atakowania celów w Estonii olbrzymią liczbą danych, tysiące razy przekraczającą normalny ruch internetowy. Sytuacja była dramatyczna, a jej ponure wspomnienie dodatkowo komplikuje, że zakończenie tej pierwszej międzynarodowej wojny sieciowej przypisuje się raczej zaprzestaniu wrogich działań przez agresorów niż udanej akcji obronnej. Dzisiaj po problemie nie ma już śladu, poza doświadczeniem, które jest nauczką dla wszystkich[3].

[3] http://prawo.vagla.pl.

4. Sprawcy komputerowych przestępstw

Sprawców przestępstw komputerowych można podzielić na dwie grupy:

1. Przestępcy, którzy używają zaawansowanych narzędzi informatycznych i swojej wiedzy informatycznej do popełniania przestępstw:
   a) haker – to komputerowy ekspert o ogromnej wiedzy z informatyki, początkowo termin ten miał jedynie negatywne znaczenie: oznaczał sieciowego włamywacza, potrafiącego ominąć zabezpieczenia systemu (nieniszczącego danych); z czasem pojęcie to rozszerzono o pozytywne znaczenie, opisujące hakera jako szczególnie uzdolnionego programistę lub eksperta ds. sieci, wykorzystującego swe umiejętności w dobrej wierze, pomagającego wyszukiwać i zabezpieczać luki w sieciowych aplikacjach; obecnie hakerów dzieli się na trzy grupy: przestępców-włamywaczy, błyskotliwych programistów i ekspertów ds. bezpieczeństwa; ich wspólną cechą jest wysoki poziom wiedzy programistycznej, różnicą jest sposób jej wykorzystania – w dobrym lub złym celu;
   b) cracker – pojęcie ma dwa główne znaczenia: to osoba łamiąca zabezpieczenia serwerów w sieci w celu kradzieży lub zniszczenia danych albo osoba analizująca kod programów pod kątem ich zabezpieczeń przed kopiowaniem, w celu ich usunięcia (lub obejścia); termin ten ma wydźwięk negatywny – działania crackerów mogą powodować duże straty finansowe firm, ale obecnie stosuje się też pojęcie „dobrego crackera", pomagającego w kontroli zabezpieczeń przed nielegalnym kopiowaniem, takie osoby są zatrudniane jako konsultanci, m.in. przez firmy produkujące oprogramowanie, testujący zabezpieczenia nowych produktów; zarówno pozytywni, jak i negatywni crackerzy cechują się wysokimi umiejętnościami programistycznymi.

2. Przestępcy, dla których komputer lub sieć jest jedynie narzędziem dodatkowym. Mogą oni np.:
   - za pomocą sieci szukać ofiar, zarówno do przestępstw dokonanych online, jak i w świecie rzeczywistym,
   - przechowywać dane dotyczące przestępczej działalności,
   - kontaktować się za pomocą np. e-maili ze swoimi wspólnikami (Fischer, 2005).

O tym, jak łatwo jest paść ofiarą hakerów przekonał konkurs hakerski, przeprowadzony 18 marca 2009 roku. Zadaniem uczestników zawodów było włamanie do systemów urządzeń mobilnych oraz komputerów. Co ciekawe, żadnego z pięciu atakowanych smartfonów nie udało się zhakować, natomiast przeglądarki internetowe, przez które włamywano się do komputerów, poległy wszystkie. Okazuje się, ze przeglądarki internetowe, z których korzystamy także w domach, są pełne luk, stanowiących łatwy cel dla hakerów. Na szczęście informacje o błędach w aplikacjach, wykrywanych w czasie trwania konkursu, są skrzętnie gromadzone przez jego organizatora i przekazywane producentom oprogramowania.

Globalny charakter współczesnych systemów informatycznych potęguje skalę zagrożenia. Przestępczość teleinformatyczna jest zjawiskiem stosunkowo mało rozpozna-

walnym z wielu powodów, do najważniejszych należą:

- rozmiary zagrożeń przestępczością komputerową, oraz jej związek z biznesem są wciąż niedoceniane,
- rzeczywiste rozmiary przestępczości teleinformacyjnej są trudne do określenia, gdyż sprawcy działają stosunkowo długo i powodują poważne straty zarówno materialne, jak i niematerialne,
- przestępstwa tego typu ujawniane są przypadkowo, najczęściej z powodu błędów popełnianych przez sprawców,
- organy ścigania odgrywają minimalną rolę w ujawnianiu tych przestępstw, z tego powodu nie występuje prewencyjna rola śledztwa, a także wyroku (Misiuk, Kosiński 2007, s. 32–45).

Czynnikami sprawiającymi że przestępstwa komputerowe są bardziej atrakcyjną formą działalności przestępczej jest to, że:

- dokumentacja informacji, które w klasycznym systemie znajdowałyby się w różnych miejscach, gromadzone są w jednym miejscu – pamięci komputera, przez co łatwiej znaleźć dostęp, bez wzbudzania podejrzeń,
- system zabezpieczenia jest zaniedbywany na korzyść szybkości i sprawności, szczególnie w przypadku dużej konkurencji.

W ogólnie dostępnym internecie można znaleźć tysiące informacji o sposobach nielegalnego wejścia w system komputerowy oraz specjalistycznego oprogramowania służącego do przełamywania wyrafinowanych zabezpieczeń (Kliś, 2016).

5. Zwalczanie przestępstw komputerowych

Przestępczość komputerowa jest obecnie rozwinięta na tak szeroką skalę, że konieczne jest podjęcie wszelkich starań i wykorzystanie wszelkich możliwości, aby ją ograniczyć. Uwzględniając specyfikę przestępstw komputerowych, do ich zwalczania należy wykorzystać zarówno przepisy karnoprawne, jak i techniczne zabezpieczenia systemów informatycznych.

Dotychczasowa praktyka i orzecznictwo sądowe wskazują na ograniczone możliwości ścigania sprawców przestępstw komputerowych. Przyczyny takiego stanu rzeczy wynikają głównie ze specyfiki tych przestępstw, co polega przede wszystkim na: ponadnarodowym charakterze, możliwości zdalnego działania sprawców, krótkim czasie popełnienia przestępstwa, możliwości łatwego kamuflowania czynu, potrzebie wyspecjalizowanej kadry i specjalistycznej techniki wykrywania i zbierania dowodów, charakterystycznym *modus operandi*, minimalnej roli organów ścigania w ich ujawnieniu.

Geograficzne granice nie są w stanie przeszkodzić w dokonaniu przestępstwa. Trudno mówić o jakichkolwiek ograniczeniach terytorialnych czy czasowych, jeśli komputer jest połączony z siecią i działa online. Ogrom i decentralizacja internetu pozwala na dużą swobodę działań przestępczych (Horoszkiewicz, 2008, s. 234–250).

Telefon z terminalem podłączonym w jednej części świata może być użyty do popełnienia przestępstwa w systemie komputerowym online w każdej innej części świata,

a kilkusekundowa transmisja danych może być porównana z błyskawiczną ucieczką z miejsca zdarzenia. W przypadku działań w sieci sprawcy nie ma na miejscu przestępstwa. Powoduje to wiele przeszkód formalnych, utrudniających ściganie. Ponadto sprawca przestępstwa nie będąc na miejscu przestępstwa nie zostawia śladów, zaś czas pojawienia się skutków czynu może się bardzo różnić od momentu ich zainicjowania Przestępstwa komputerowe mogą być łatwo i dobrze zakamuflowane, np. skutki sabotażu komputerowego można przypisać awarii systemu lub błędom oprogramowania. Dowody przestępstwa komputerowego dają się łatwo usuwać z komputera i bardzo często programy przestępcze mają wbudowane procedury automatycznej samolikwidacji po wykonaniu zadania. Możliwość wykrycia takiego programu jest możliwe tylko wtedy, gdy jeszcze działa lub gdy nie został całkowicie wymazany z komputerowego nośnika danych.

Cechy przestępstw komputerowych, na które zwracają uwagę organy ścigania, a które wymagają podjęcia odrębnych działań przez właściwie wyszkoloną kadrę specjalistów to: specyficzne dowody, które dla osób nieznających techniki informatycznej są niewidoczne lub niezrozumiale, brak śladów w tradycyjnym rozumieniu, łatwa usuwalność dowodów, możliwość kodowania danych, których kontrola wymaga specjalistycznych urządzeń (komputerów z odpowiednim oprogramowaniem). Podjęcie działań przez organ ścigania po dokonaniu przestępstwa musi być stosunkowo szybkie i obejmować właściwe zabezpieczenie materiału dowodowego, zarówno rzeczowego, jak i osobowego. Prowadzący postępowanie poza wiedzą własną z zakresu działania sprzętu, powinien dysponować zapleczem w postaci konsultantów i biegłych, którzy nakierunkują jego działania. Ze względu na charakter informatyki, która jest dziedziną podlegającą dynamicznym zmianom, nierzadko występują trudności z uzyskaniem opinii biegłych (Fischer, 2000, s. 321–327).

Przestępstwa komputerowe mają dotychczas niespotykane cechy, w znacznym stopniu utrudniające ich wykrycie oraz udowodnienie. Według FBI organy ścigania ujawniają tylko 15% przestępstw. Właściwie ukształtowane prawo i praktyka mogą zwiększyć ich skuteczność, ale dużej pomocy wymaga się od samych użytkowników komputerów. Jest to o tyle utrudnione, ze poszkodowany w momencie działania sprawcy może nie być świadomy, że zachodzi zdarzenie – przestępstwo. Nierzadkie są też przypadki, gdy np. kierownicy poszkodowanych przedsiębiorstw nie wykazują zainteresowania ściganiem i nie zgłaszają policji nadużycia komputera (Misota, 2003, s. 219–230).

Zapobieganie przestępstwom komputerowym może przybierać najróżniejsze formy. Wciąż podejmuje się działania mające na celu stworzenie spójnego systemu regulacji prawnych, a także wszelkiego rodzaju akcji informacyjnych, szkoleniowych oraz wykrywczych.

Komputery chronione są środkami fizycznymi i technicznymi przed ewentualną ich kradzieżą czy dostępem do danych w nich zawartych. Podstawowe zabezpieczenie informacji zgromadzonych w systemach komputerowych stanowią hasła. Są one indywidualnymi kluczami do naszych prywatnych zasobów i narzędzi elektronicznej wymiany informacji. Warto pamiętać o wymyślaniu oryginalnych haseł i częstym ich zmienianiu. Inną kwestią związaną z przesyłaniem informacji jest ich autoryzacja, dzięki czemu możemy zweryfikować autorstwo przekazu. Weryfikację tożsamości umożli-

wia podpis cyfrowy, jest to przekształcenie kryptograficzne danych dołączone do komunikatu, umożliwiające odbiorcy przekazu sprawdzenie ich autentyczności i zapewniające ochronę nadawcy przed ich sfałszowaniem. Inną powszechniejszą formą obrony zwłaszcza przed hakerami są „zapory ogniowe" – *firewalls*, stawiane między komputerem a siecią zewnętrzną. Informatyczna zapora ogniowa jest punktem kontroli wszystkich informacji, zarówno wychodzących, jak i przychodzących. Zadanie to wykonuje komputer z odpowiednim oprogramowaniem, pośrednicząc w przepływie informacji między np. firmą a resztą świata. W Pentagonie i innych instytucjach rządowych informacje najważniejsze chronione są przez „ścianę powietrzną" – *air wall*, co oznacza przechowywanie ich w komputerach niedostępnych dla sieci.

Zabezpieczenia techniczne mogą także chronić programy przed ich bezprawnym kopiowaniem. W walce z piractwem mogą być wykorzystane takie urządzenia i środki jak: hologramy, karty z mikroprocesorem, systemy magnetyczne, zminiaturyzowane naklejki (Kowalski, 2014).

Podsumowanie

Komputeryzacja, niosąc za sobą postęp techniczny w zakresie przetwarzania i przechowywania informacji, powoduje istotne jak widać zjawiska uboczne w postaci rozwijającej się na szeroką skalę przestępczości komputerowej. Z przedstawionego katalogu przestępstw wynika, że mają one związek nie tylko z zakłócaniem działalności gospodarczej, ale także z zagrożeniami w komunikacji czy łączności, mogą skutkować zagrożeniem życia, zdrowia czy mienia oraz bezpieczeństwa publicznego. Są to z jednej strony przestępstwa, które należą do tradycyjnych, jak kradzież czy oszustwo, z drugiej zaś strony są to nowe typy przestępstw, których nie można popełnić bez użycia komputera. Straty, jakie na skutek przestępstw komputerowych ponoszą producenci, użytkownicy a także Skarb Państwa są bardzo duże, w ich wyniku wszyscy jesteśmy poszkodowani. Na świecie w rękach cyberprzestępców są miliony komputerów, a dotychczasowe doświadczenia nie pozostawiają złudzeń co do intencji ich wykorzystania – od szpiegostwa, zakłócania kontroli ruchu lotniczego, unieruchamiania instalacji energetycznych przez zwalczanie konkurencji gospodarczej do terroryzmu we wszelkich formach. Konieczne jest zatem podjęcie na szeroką skalę działań zarówno prewencyjnych, jak i akcji wykrywawczych. Przed popełnianiem przestępstw komputerowych należy również chronić się przez wykorzystanie wszelkich istniejących zabezpieczeń technicznych.

Bibliografia

Fischer, B. (2000). *Przestępstwa komputerowe i ochrona informacji*. Kraków.

Fischer, B. (2005). *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne*. Zakamycze.

Grzelak, M., Liedel, K. (2014). *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*. Kraków: Wydawnictwo UE.

Horoszkiewicz, J. (2008). *Przestępczość komputerowa*. Szczytno.

http://prawo.vagla.pl/node/905 (11.2015).

http://prawo.vagla.pl/sskrypts/cybercrimel.html (19.10.2026).

http://www.unic.un.org.pl, dostęp (14.12.2016).

Jakubowski, K. (1996). Przestępczość komputerowa, Zarys problematyki. *Prokuratura i Prawo, 12*.

Kliś, M. *Przestępczość w Internecie*. Pobrano z: http://prawo.vagla.pl/node/905 (11.2016).

Kosiński, J. (2015). *Paradygmaty cyberprzestępczości*. Warszawa: Difin.

Kowalski, P. *Skimming w bankomatach. Czy jesteśmy bezpieczni?* Pobrano z: http://wwweuro bank.pl/doradzamy-artykuly,3,skimming-w-bankomatch,47,169.html (12.2014).

Misiuk, A., Kosiński, J. (2007). *Przestępczość teleinformatyczna*. Szczytno.

Misota, J.(2003). *Elektroniczne instrumenty płatnicze*. Bydgoszcz–Poznań: Oficyna Wydawnicza Branta.

Siwicki, M. (2013). *Cyberprzestępczość*. Warszawa: C.H. Beck.

Sowa, M. (2001). Ogólna charakterystyka przestępczości internetowej. *Palestra, 5–6*.

Sucharzewska, A. (2010). *Ochrona prawna systemów informatycznych wobec zagrożenia cyber-terroryzmem*. Warszawa: Wolters Kluwer.

Wymiana doświadczeń w zakresie przestępczości (2008). Warszawa: Komenda Główna Policji. Pobrane z: http://www.katowice.szkolapolicji.gov.pl/pdf/Karty_platnicze.pdf (12.12.2016).

PROBLEM OF ELECTRONIC CRIME

Keywords: cyberspace, hacking, computer crime, craker

Summary. The article introduce a genesis and a specificity of electronic crimes, whete its specificity results among all from the fact, that the place where they are committed, is not always the same "place" in a common sense. Using the Internet, as a places of the committing an offence, is particularly dangerous due to the very high number of potential victims and problems with low detectability of crimes and its offender. The global network is reducing the effectiveness of mechanisms of the identification. The cyberspace is deprived of all physical attributes of someone's presence, so as: fingerprints, voice, image. The aim of the article is showing the range and the scale of electronic crime in the world, as well as its effects.

Translated by Renata Jedlińska

Cytowanie

Jedlińska, R. (2017). Problem przestępczości elektronicznej. *Ekonomiczne Problemy Usług, 1* (126/2), 185–194. DOI: 10.18276/epu.2017.126/2-19