Mgr Wojciech Kasprzak
Collegium Balticum w Szczecinie

WYBRANE PRAWNO-KRYMINALISTYCZNE PROBLEMY KRADZIEŻY DÓBR Z GIER KOMPUTEROWYCH

Streszczenie

Internet jest centralną bazą danych i źródłem wymiany informacji między usługodawcami a konsumentami. Technologia ta dała również początek fali nowych rodzajów przestępstw na tle cyfrowym. W ostatnich latach obserwujemy rosnące zjawisko kradzieży towarów z gier komputerowych. Najbardziej dochodowym gatunkiem gier przynoszącym miliony dolarów zysku w skali miesięcznej są gry MMO (Massively Multiplayer Online). Produkcje takie łącząc miliony graczy do wspólnej rozrywki w wirtualnym świecie. Dostawca usługi wymaga od potencjalnych odbiorców opłaty abonamentowej związanej z możliwością dalszego użytkowania produktu. To, co przyciąga przestępców szukających nowych form pozyskiwania pieniędzy to możliwość wykradzenia i sprzedania cennych danych i zawartości konta w grze. Autor opisuje metody działania przestępców, charakteryzuje gry w świetle dóbr materialnych, przedstawiona zostaje kwalifikacja prawna kradzieży i procedury zgłaszania przestępstwa kradzieży w grach komputerowych.

Słowa kluczowe: gry, cyberprzestępczość, MMO, kradzież, Internet, cyberprzestrzeń.

SELECTED LEGAL AND CRIMINAL ASPECTS OF THEFT IN COMPUTER GAMES

Abstract

Internet as a central database and information exchange between consumers gave beginning to a wave of new types of crime. In recent years we have seen an increasing phenomenon of theft of goods from computer games. The most profitable games yielding millions of dollars profits are MMO (Massively Multiplayer Online). Productions such bringing together millions of gamers to the common entertainment enforce payment for additional fees associated with

the possibility of further use of the product: subscription fees, re-buy additional accessories to better performance in the game. It attracted offenders seeking new forms of raising money. The author gives the article the method of action of criminals, gives the concept a computer goods from game, the legal classification of theft and procedures for reporting an offense of theft in computer games.

Keywords: games, cybercrime, MMO, theft, Internet, cyberspace.

Uwagi ogólne

Postęp technologiczny zawsze oznacza nowe przywileje dla konsumentów, większe możliwości, szerszy dostęp do informacji, szybsze i bardziej komfortowe usługi. Jednak zawsze z nowymi możliwościami otwierają się także drogi dla nowych patologii. Powstanie Internetu jako centralnej bazy danych i wymiany informacji pomiędzy konsumentami dało początek całej fali nowych rodzajów przestępstw. Sprawca jest w stanie osiągnąć korzyści w sposób sprzeczny z prawem za pomocą domowego komputera, nie wychodząc z domu, miejsca pracy lub kafejki internetowej. Poza klasycznymi i znanymi organom ścigania działaniami hakerów (np. włamania do prywatnych firm, tworzenie wirusów) istnieje jeszcze wiele innych mało znanych rodzajów przestępstw komputerowych, które stają się coraz większym zagrożeniem.

W ostatnich latach obserwuje się zwiększające się zjawisko kradzieży dóbr z gier komputerowych. Najbardziej dochodowymi grami przynoszącymi milionowe zyski są te z gatunku MMO (Massively Multiplayer Online). Produkcje takie, zrzeszając miliony graczy do wspólnej rozrywki, wymuszają wnoszenie dodatkowych opłat związanych z możliwością dalszego użytkowania produktu – jak opłaty abonamentowe lub dokupienie dodatkowych akcesoriów umożliwiających lepsze wyniki w grze. Zainteresowało to wirtualnych przestępców szukających nowych możliwości pozyskiwania pieniędzy. Okazało się, że formy przestępstw związanych z grami internetowymi nie ograniczają się tylko do piractwa i łamania praw autorskich. Hakerzy rozwinęli swoją działalność na obszar gier internetowych w celu kradzieży dobra znajdującego w się w takich grach i będącego mieniem wirtualnym, niematerialnym ale o wartości realnej w pieniądzu. Rozpoczął się niele-

galny handel kradzionymi danymi użytkowników gier. Wartościowymi informacjami dla hakerów stały się dane personalne użytkowników, ich adresy, numery kart kredytowych. Wszystkie te elementy przypisane do kont gier internetowych stały się nowym celem cyberprzestępców. Straty szacowane na setki milionów dolarów, stawiają problem w innym świetle. Kradzieże takie w skali jednostki mogą nie robić zbyt dużego wrażenia na organach ścigania, ponieważ straty wynoszę najczęściej mniej niż 1000 zł, jednak w skali globalnej rosną do kwot sięgających milionów złotych.

Badania statystyczne potwierdzają, że istnieje znaczący wzrost aktywności hakerów za każdym razem, gdy następuje premiera gry z gatunku MMO. Liczba dostępnych metod i narzędzi wykorzystywanych przez hakerów jest olbrzymia. Sama działalność takich osób jest trudna w wykryciu i zapobieganiu przyszłym atakom. Z uwagi na specyficzny charakter, jakim jest sieć komputerowa – Internet – uważana za ponad graniczną i niezwykle trudną w kontroli, zacierają się w niej klasycznie rozumiane obszary jurysdykcji. W tej sytuacji największym problemem współczesnych organów ścigania, na tle obecnej technologii, jest doprowadzenie sprawcy czynu zabronionego przed oblicze sprawiedliwości oraz bagatelizowanie groźnego problemu kradzieży dóbr z gier komputerowych. Pokrzywdzony często nawet nie wie, że z problemem kradzieży z gry internetowej może się udać do organów ścigania.

Ważnym zagadnieniem jest sposób klasyfikowania czynu przestępczego, ponieważ budzi on problemy interpretacyjne na tle kodeksu karnego. Obecnie kradzież z gry internetowej jest zwykle klasyfikowana jako kradzież informacji, podczas gdy czyn ten posiada wszelkie przesłanki do tego by zostać uznanym za kradzież z włamaniem.

Pojęcie dobra komputerowego w grze i prawna klasyfikacja jego kradzieży

Gatunek MMORPG jest najbardziej rozbudowanym rodzajem gier komputerowych. Twórca, udostępniając swój produkt do gry

przez Internet, wykorzystuje dwie podstawowe metody płatności. Najpopularniejsza jest metoda „Free to Play" (F2P – Darmowa Gra). Producent udostępnia swój produkt za darmo, ale dodaje także możliwość robienia zakupów za prawdziwe pieniądze, w elektronicznym sklepie na oficjalnej stronie produkcji. Konsument może w tym momencie za niewielką opłatą dokupić do swojego „bohatera" dodatkowe elementy jak np. zbroję lub miecz, niedostępne w inny sposób. Gracz zyskuje tym samym przewagę nad użytkownikiem nie wykorzystującym takiego sklepu. Drugim rodzajem płatności jest metoda „Pay to Play" (P2P – Płać by Grać). Właściciel takiej gry wymaga od konsumenta uiszczania miesięcznych opłat abonamentowych w określonej wysokości, w zamian za dostęp do gry. Najczęściej abonament taki obejmuje czas gry w liczbie 30 lub 60 dni, po skończeniu, którego konsument, by kontynuować rozgrywkę, musi dokupić nowy abonament.

Każdy użytkownik gry MMORPG przed rozpoczęciem rozgrywki musi utworzyć swoje indywidualne konto, na którym będą zapisywane postępy w grze. Konto takie znajduje się na serwerach właściciela gry i jest zabezpieczone loginem i hasłem, a także systemami bezpieczeństwa, jakie zapewnia dostawca usługi gry komputerowej. Warto w tym momencie zaznaczyć, że konto to z czasem nabiera pewnej wartości, staje się „dobrem internetowym". Czas, jaki użytkownik poświęca na zdobycie określonych rzeczy w grze można przeliczyć na sumę pieniędzy, jaką płaci się za możliwość użytkowania gry. Użytkownik poświęca czas na doskonalenie własnej postaci. Staje się to pewnego rodzaju mieniem osoby, która spędziła olbrzymią ilość czasu w wirtualnym świecie[1]. Sam proces płatności odbywa się najczęściej za pośrednictwem kart kredytowych. Czasem właściciel danej marki udostępnia też inne metody płatności jak przelew. Jedną z bardziej innowacyjnych metod płatności dla osób nie posiadających dostępu do kart kredytowych lub kont internetowych jest możliwość opłacenia wymaganej kwoty za pośrednictwem specjalnej karty PrePaid. Metoda płatności kartą PrePaid wywodzi się z sieci telefonii komputerowej polegającej na zakupie określonych ilości

[1] *Rosnąca popularność gier MMORPG*, Praca w biznesie komputerowym, http://praca.komputerowcy.info/2012/02/14/rosnaca-popularnosc-gier-mmorpg/, [14.02.2012].

jednostek taryfikacyjnych[2]. W przypadku gier MMORPG płatność taka polega na zakupie specjalnej karty, która posiada indywidualny kod seryjny, po wprowadzeniu, którego konsument uzyskuje przedłużenie abonamentu. Wiele firm, które są właścicielami gier z gatunku MMORPG wymaga wręcz uiszczania opłat abonamentowych tylko za pomocą karty kredytowej. W momencie tworzenia kont i akceptacji regulaminu konsument jest proszony o zdefiniowanie metody płatności. Przypisując swoje dane personalne, adres zamieszkania, numer telefonu i numer swojej kary kredytowej do konta, powierza te dane do ochrony właścicielowi usługi. Płatność jest wówczas ściągana automatycznie z rachunku bankowego w comiesięcznych odstępach. Jednym z głównych niebezpieczeństw takiego rozwiązania jest bezpośrednie narażenie wrażliwych danych personalnych na szkodliwe działanie osób trzecich np. hakerów. Systemy bezpieczeństwa stosowane przez właścicieli usług komputerowych nie zapewniają należytej ochrony. Bardzo często zdarzają się kradzieże kont internetowych, w skrajnych przypadkach nawet wyczyszczenie kart kredytowych pojedynczych konsumentów.

Historia notuje poważne ataki hakerów na branżę gier. W 2011 r. firma Sony zapewniła dostęp do sieciowej usługi PlayStation Network (PSN), która umożliwia m.in. granie „online" (przez Internet), jak również kupowanie przez sieć gier, muzyki i filmów. Sony podało, że na świecie ma już 70 milionów aktywnych kont PSN. Oszacowano też, że z usługi korzysta około 50% posiadaczy PS3 w Polsce (a więc prawie 150 tysięcy osób)[3]. W pewnym momencie nastąpił jednak problem z działaniem usługi, który trwał blisko tydzień. Firma Sony w oficjalnym oświadczeniu przyznała, że na przełomie 17-18 kwietnia 2011 r. nastąpił atak na usługę PSN ze strony hakerów. Sprawcom udało się wykraść hasła, dane personalne i numery kart kredytowych blisko połowy użytkowników PSN. To co wywołało jednak największy skandal, to opieszałość firmy Sony z oficjalnym opu-

[2] *Co to jest karta typu PrePaid*, wp.pl polonia, http://polonia.wp.pl/country,1,title,Co-to-jest-karta-typu-PrePaid,wid,10478181,faq.html?ticaid=1f4d5, [03.01.2012].

[3] *PlayStation Network: Sony wydaje oświadczenie. Gorzej być nie mogło...*, http://www.cdaction.pl/news-18922/playstation-network-sony-wydaje-oswiadczenie-gorzej-byc-nie-moglo.html, [26.04.2011].

blikowaniem tych informacji, zostały one podane dopiero około siedem dni po ataku hackerskim. Sprawcom udało się w tym czasie sprzedać dane użytkowników osobom trzecim. Nie są znane prawdziwe statystyki dotyczące poniesionych strat na skutek przestępczej działalności i opieszałości firmy Sony. Wszyscy klienci usługi PSN zostali zmuszeni do zmiany haseł w samej usłudze jak i swoich zabezpieczeń odpowiedzialnych za karty kredytowe i rachunki bankowe.

Firma Blizzard właściciel największej gry MMORPG stosuje też ciekawą metodę na przedłużenie czasu gry w swojej usłudze, która to zasługuje na odrębne omówienie. Pracownicy Blizzard Entertainment dali swoim konsumentom możliwość zapraszania innych osób, potencjalnych odbiorców ich produktu. Usługa ta nazywa się Recruiting a Friend (RaF – zwerbuj przyjaciela) polega ona na wysłaniu zaproszenia do osoby trzeciej na dołączenie do rozgrywki w grze World of WarCraft za darmo na okres kilku dni. W momencie, gdy zwerbowany użytkownik wykupi abonament na stałe by dalej grać, osoba zapraszająca otrzyma nagrodę od firmy Blizzard pod postacią darmowego przedłużenia czasu gry na okres 30 dni. Mechanizm w swojej prostocie jest bardzo przystępny i chętnie wykorzystywany przez odbiorców firmy Blizzard. Konsument za swoje starania otrzymuje nagrodę a Firma nowego klienta. Zabieg taki niestety powoduje też pewną patologię. RaF stał się wartościową metodą na zarobek poprzez sprzedanie tej usługi za mniejsze pieniądze niż wykupienie klasycznego abonamentu. Sprzedaż jest prowadzona za pośrednictwem aukcji internetowych na portalach takich jak Allegro. Osoby sprzedające zrzeszają się często w duże grupy, by bardziej efektywnie wykorzystywać możliwości RaF, co staje się dla nich źródłem zarobku. Działanie na taką skalę jest zabronione przez właściciela gry. RaF jest bezpłatną usługą, którą można wykorzystać by pozyskać nowych graczy. Natomiast jej sprzedaż jest zabroniona przez wewnętrzny regulamin produktu.

Sklep twórców gry nie jest jedynym miejscem dokonania transakcji i wymiany waluty, bardzo często odbywa się to za pośrednictwem Internetu na aukcjach. Przykładowo, po wpisaniu określonych słów „kluczy" służących do precyzyjnego wyszukiwania określonego rodzaju aukcji, konsument może znaleźć inte-

resujące go dobro sprzedawane hurtowo. Handlem takim zajmują się często osoby prywatne skupujące wybrane elementy wykorzystywane w sklepie gry. Metoda działania takich osób polega na wynajdywaniu najtańszej z ofert a następnie sprzedaniu jej za większą sumę na aukcjach. Ceny poszczególnych elementów w wewnętrznym sklepie gry komputerowej z gatunku MMO mogą się od siebie różnić. Firma będąca właścicielem gry stara się ustalać ceny tak by były one odpowiednie dla danego kraju. W praktyce działa to tak, że różne kraje mają inne ceny i ich obywatele mogą kupić wybrane elementy taniej niż obywatele innego kraju. W Polsce tacy handlarze nagminnie skupują dobra z gier przeznaczone na rynek rosyjski, gdzie marża jest dużo niższa niż cena tych samych przedmiotów na rynku polskim. Przedmioty te są następnie wystawiane za większą kwotę i odsprzedawane na polskich aukcjach. Problem ten nie dotyczy tylko samych dóbr ze sklepów MMO. Bardzo łatwo i szybko można kupić też egzemplarze gier, pod postacią kluczy elektronicznych. Klucz taki jest indywidualny dla każdej kopii gry i stanowi pewne zabezpieczenie przed złodziejami i pirackimi kopiami danej produkcji. Ceny takich gier są często nawet o 80% niższe niż odpowiedniki w oryginalnych sklepach. Przyczyną niskich cen jest kupowanie takich kluczy za pomocą kradzionych kart kredytowych. Cały proceder jest bardzo prosty w swojej konstrukcji. Zaczyna się od zdobycia hasła i danych do konta internetowego lub karty kredytowej, przez złodzieja lub hakera za pomocą dostępu do Internetu. Sprawca sprzedaje te dane pośrednikowi, który przenosi je w inne miejsce i udostępnia handlarzowi kupującemu hurtowe ilości danych kluczy elektronicznych. Najczęściej klucze te pochodzą z Chin lub Rosji. Ostatnim etapem jest kupno kluczy przez prywatnych handlarzy i wystawienie ich po zaniżonej cenie na portalach aukcyjnych. Klucze takie są często blokowane po pewnym czasie od aktywacji przez firmę będącą właścicielem marki. Konsument jednak traci w tej sytuacji pieniądze a próba ich odzyskania jest bardzo utrudniona z powodu długiego okresu od nabycia klucza do momentu zablokowania konta. Sprzedawca broni się natomiast zrzucając winę na kupującego, że złamał pewnie warunki regulaminu korzystając z danej gry a teraz próbuje wyłudzić pieniądze. Serwisy aukcyjne często same zamykają

konta takich sprzedawców i kasują aukcje. Jednak handlarze wracają za parę dni z nowym kontem i nowymi aukcjami.

W art. 278 Kodeksu karnego zostały zamieszczone przestępstwa: kradzieży zwykłej § 1, kradzieży programu komputerowego § 2, kradzieży energii lub karty kredytowej § 5 oraz wypadek mniejszej wagi każdego z tych przestępstw w § 3. Samym dobrem chronionym w rozumieniu art. 278 k.k. są prawa majątkowe do rzeczy ruchomej i faktyczne władztwo nad rzeczą ruchomą, nośnikiem, na którym zapisany jest program komputerowy, kartą bankomatową. Kradzież należy zaklasyfikować jako zabór rzeczy ruchomej będącej nie tylko w posiadaniu właściciela, ale także każdej inne osoby, która w danej chwili jest w posiadaniu rzeczy i nią aktualnie włada[4]. Istotnym zagadnieniem jest charakter pewnych elementów art. 278 i ich klasyfikacji. Kradzież programu komputerowego nie można zaklasyfikować wprost jako kradzieży, bo program komputerowy nie spełnia podstawowych warunków kradzieży. Czyn nie polega na zaborze rzeczy, ponieważ w rozumieniu obecnego prawa informacja nie jest rzeczą. Ważnym aspektem jest także fakt, że zabór nie pozbawia osoby uprawnionej dalszego dysponowania programem, ponieważ ten w wersji elektronicznej jest dobrem niematerialnym i znajduje się pod postacią kodu komputerowego na dysku właściciela. Stąd też uznając, że chodzi tu nie tylko o uzyskanie programu (jego kopii a nie samego nośnika danych – płyty CD/DVD) od jego autora, wprowadza się odpowiedni typ przestępstwa zbliżony do kradzieży art. 278 § 2 k.k. pkt. 2[5].

Art. 278 Kodeksu karnego przewiduje jako podmiot przestępstwa każdą osobę zdolną do odpowiedzialności karnej. Przedmiotem wykonawczym kradzieży w rozumieniu art. 278 k.k. jest natomiast cudza rzecz ruchoma. Samo pojęcie rzeczy ruchomej należy tutaj rozumieć w ujęciu art. 115 § 9 k.k. Wymogiem zaklasyfikowania czynu jako kradzież musi być fakt, że rzecz jest cudza, czyli nie stanowi własności sprawcy w chwili popełnienia

[4] Uchwała SN z 19.4.1977r., VII KZP 3/77, OSNKW 1977, Nr 6, poz. 54; Wyrok SN z 30.12.1970r., IV KR 211/70, biuletyn SN 1971, nr 4, poz. 69.

[5] A. Grześkowiak, K. Wiak (red.), *Kodeks karny Komentarz*, Warszawa 2012, s. 1174.

czynu zabronionego[6]. Kradzież w ujęciu art. 278 kodeksu karnego jest więc przestępstwem z winy umyślnej o charakterze kierunkowym, znamiennym celem. Treścią celu w przypadku kradzieży rzeczy, energii lub karty bankomatowej jest przywłaszczenie. Sprawca w takim przypadku działa z chęcią i w celu przywłaszczenia, jeżeli zamierza traktować cudzą rzecz, energię lub kartę bankomatową jako swoją własność przez włączenie jej do swojego majątku. Samą czynnością sprawczą kradzieży jest zabór, czyli wyjęcie spod władztwa innej osoby i objęcie skradzionej rzeczy władaniem przez sprawcę, wbrew woli osoby dysponującej rzeczą[7]. Inaczej została określona czynność sprawcza kradzieży z art. 278 § 2 k.k. dotycząca programu komputerowego. Ustawodawca określił czynność jako „uzyskanie" programu komputerowego i wskazał, że określenie to ma szersze konotacje niż termin „zabór", ponieważ obejmuje wszelkie postaci przejęcia programu komputerowego, bez zgody jego dysponenta w taki sposób, który umożliwia użytkowanie tego programu przez osobę nieuprawnioną, równocześnie z osobą pokrzywdzoną (dwie osoby używają programu w tym samym czasie o tej samej licencji i kodach indywidualnych)[8]. Oznacza to, że zabór nośnika programu komputerowego jak i skopiowanie samego programu i uzyskanie do niego dostępu, wskazuje na materialny charakter tego przestępstwa. Sprawstwo dokonuje się w momencie umożliwienia sobie lub innej nieupoważnionej osobie trzeciej korzystanie z programu.

Kodeks karny na mocy art. 279 k.k. wyróżnia kradzież z włamaniem, polegającą na złamaniu zabezpieczeń chroniących dane dobro. Przepis art. 279 k.k. chroni dokładnie te same dobra prawne co art. 278, a także chroni systemy bezpieczeństwa mienia np. (drzwi, zamki, sejf, hasło, systemy bezpieczeństwa), polegające na zamknięciu wartościowej rzeczy w pomieszczeniu lub innych bezpiecznym miejscu służącym jego ochronie. Zakres podmiotu, strony przedmiotowej i podmiotowej kradzieży z włamaniem należy interpretować tak samo jak kradzież a art. 278,

[6] A. Marek, T. Oczkowski, *Kradzież i przywłaszczenie*, [w:] R. Zawłocki (red. tomu), *System prawa karnego*, Warszawa 2011, tom 9, s. 74.

[7] A. Grześkowiak, K. Wiak (red.), *Kodeks karny...*, op. cit., s. 1176.

[8] Wyrok SA w Krakowie z 8.7.2009 r., II AKa 98/09, KZS 2009, Nr 7-8, poz. 58.

z tą różnicą, że art. 279 charakteryzuje się szczególnym sposobem popełnienia i stanowi przestępstwo niezależnie od wartości przedmiotu wykonawczego. Ustawodawca wyraźnie określił czynniki, jakie muszą być spełnione by sprawstwo zaklasyfikować jako kradzież z włamaniem. Przyjmuje się, że włamanie możliwe jest tylko wówczas, gdy rzecz znajduje się w pomieszczeniu zamkniętym. Sama definicja pomieszczenia zamkniętego rozumiana jest w szeroki sposób i obejmuje nie tylko budynki lub lokale, ale także sejfy, zamknięte na klucz szuflady, zaplombowany pojemnik. Drugim czynnikiem obok „zamkniętego pomieszczenia" określonego przez ustawodawcę w art. 279 k.k. jest „przełamanie zabezpieczenia", które nie musi wiązać się z wtargnięciem do pomieszczenia. Samo zabezpieczenie musi być „wyraźną manifestacją woli właściciela czy posiadacza mienia, woli właśnie zabezpieczenia go przed innymi osobami"[9]. Poza zabezpieczeniami o charakterze materialnym jak (drzwi, zamki, sejfy), występują także różne rodzaje zabezpieczeń niematerialnych jak kody dostępu, hasła i loginy systemów komputerowych. Sprawca czynu zabronionego z art. 279 k.k., mimo że nie używa siły fizycznej, by zdobyć określone informacje musi przełamać zabezpieczenia elektroniczne. Stosowanie art. 279 § k.k. do kradzieży programu komputerowego i karty uprawniającej do podjęcia pieniędzy z bankomatu wymaga pewnych modyfikacji w utrwalonej wykładni znamienia „włamanie" ukształtowanej w kontekście kradzieży rzeczy[10]. Uzyskanie dóbr w ten sposób nie polega na zaborze a na uzyskaniu do nich dostępu. Sąd Najwyższy orzekł, że samo zabezpieczenie w takim przypadku jest ekwiwalentem pomieszczenia zamkniętego[11].

Polskie prawo uznaje dobra z gier komputerowych za informacje i dane. Mienie takie nie posiada fizycznej postaci, występuje jedynie w formie wirtualnej, niematerialnej. Dodatkowo nie

---

[9] Wyrok SN z 24.6.2010 r., V KK 388/09, OSNKW 2010, Nr 9, poz. 82.

[10] A. Grześkowiak, K. Wiak (red.), *Kodeks karny...*, op. cit., s. 1181; M. Bojarski, J. Giezek, Z. Sienkiewicz, *Prawo karne materialne. Część ogólna i szczególna*, Warszawa 2004; A. Barczak-Oplustil, G. Bogdan, Z. Ćwiąkalski, M. Dąbrowska-Kardas, P. Kardas, J. Majewski, J. Ralewski, M. Rodzynkiewicz, M. Szewczyk, W. Wróbel, [w:] A. Zoll (red.), *Kodeks karny. Część szczególna komentarz*, Kraków 2006.

[11] Wyrok SN z 9.9.2004 r., V KK 1444/04, OSNwSK 2004, Nr 1, poz. 1533.

jest odrębnie regulowane. W 99% przypadków kradzież dobra z gier komputerowych dotyczy gatunku gier internetowych czyli MMORPG. Każdy użytkownik posiadający dostęp do produktu jest zmuszony do przestrzegania rygorystycznych systemów bezpieczeństwa w celach ochrony swojego mienia wirtualnego. Konta do gier MMORPG są zabezpieczone systemem logowania posiadającym login i hasło dla indywidualnego użytkownika. Jest to zatem dobro chronione, kradzież wymaga przełamania zabezpieczenia i dostania się do wnętrza systemu. Wszystko, co znajduje się na koncie gry posiada wartość realną mimo, że jest to mienie niematerialne i wirtualne. Samo posiadanie konta wymaga nabycia produktu, elementy, które pojawiają się na koncie z upływem czasu, także posiadają realną wartość, ponieważ konsument poświęca swój czas na doskonalenie elementów gry. System, na jakim opiera się wartość konta gry internetowej jest dość skomplikowany. Takie konto jest zabezpieczone, a właściciel marki zapewnia bezpieczne użytkowanie swojego produktu. W momencie włamania, utraty danych, właściciel gry jest zobowiązany do przywrócenia konta do stanu sprzed włamania. Realna wartość zawartości konta może być indywidualnie przeliczana przez jego użytkownika, nie ma sztywnych ram cenowych. Konsument na podstawie poświęconego czasu, opłaconego abonamentu i opłat dodatkowych może wyliczyć szacowaną wartość swojego mienia pod postacią konta w grze internetowej i jest to przeliczane na realne pieniądze, stanowi zatem realne mienie, chociaż postać tego mienia jest wirtualna[12].

Kradzież konta w grze internetowej powinna być klasyfikowana jako kradzież z włamaniem. Proceder taki posiada wszystkie przesłanki kodeksowe włamania. Wymogiem dostania się na konto przez złodzieja jest przełamanie systemu zabezpieczeń elektronicznych. Wszystkie konta posiadają takie zabezpieczenia. Dodatkowo niektóre firmy dostarczające usługę, jaką są gry internetowe MMO zapewniają swoim konsumentom dodatkowe metody ochrony ich kont przez nieautoryzowanym wejściem. Dodatkowe zabezpieczenia polegają najczęściej na dodatkowych systemach kodowania z wykorzystaniem urządzeń zewnętrznych.

[12] R. A. Stefański, *Prawo karne materialne część szczególna*, Warszawa 2009, s. 571.

Kolejnym elementem przemawiającym za kradzieżą z włamaniem jest chęć przestępcy do zagarnięcia mienia w celach majątkowych. Skradzione konta są sprzedawane na portalach aukcyjnych, jako sprzedaż „czasu poświeconego na grę", zabieg taki pozwala ominąć wewnętrzne regulaminy portali aukcyjnych. Poza osobą poszkodowaną w postaci pierwotnego użytkownika konta, dochodzi jeszcze nowy nabywca, który zakupił konto na aukcji. Firma odpowiedzialna za bezpieczeństwo konta, odda je pierwszemu właścicielowi razem z całą jego zawartością do momentu włamania, osoba, która nabyła konto na aukcji utraci je ze względu na nabycie rzeczy pochodzącej z kradzieży, dodatkowo będzie też dochodziła roszczeń względem nieuczciwego sprzedawcy.

Metody kradzieży dóbr z gier komputerowych

Wypuszczenie każdego nowego produktu w dobie Internetu, wymagającego stałego połączenia z siecią naraża każdy komputer na ataki z zewnątrz. Działania hakerów można podzielić na różne kategorie. Pierwszą metodą jest bezprawna i nieautoryzowana próba włamania się do sieci komputerowej, systemu lub pojedynczego PC. Drugą metodą jest tworzenie złośliwego oprogramowania, służącemu destrukcji danych, szpiegowaniu lub ułatwianiu zdalnego dostępu do komputera ofiary. Trzecia metoda działania przestępców to łamanie zabezpieczeń i rozpowszechnianie pirackiego oprogramowania.

Podstawowy problem w zabezpieczeniach systemów sprowadza się do braku możliwości ich 100% ochrony. Internet pozwala stworzyć to, co nie istnieje i zmienić to, co już zostało stworzone. Hakerzy zawsze znajdą lukę w systemach bezpieczeństwo, jest to tylko kwestia czasu. Rodzaje ataków można podzielić na kilkanaście odmian. Niżej wymienione sposoby działań hakerów są jedynie najczęściej stosowanymi przykładami, gdyż szczegółowe opisanie wszystkich metod wymagałoby posiadania specjalistycznej

wiedzy z zakresu informatyki i kodowania[13]. Działalność osoby pragnącej dokonać kradzieży dóbr z gier komputerowych to jeden z rodzajów ataków hakerskich.

Haker do ataku i włamania jak każdy przestępca posługuje się odpowiednimi narzędziami. Najczęściej mianem złośliwego oprogramowania wykorzystywanego przez przestępców określa się programy komputerowe służące do zdobywania informacji, łamania zabezpieczeń i szpiegowania. Programy takie dzielimy na wiele kategorii. Do najpopularniejszych wirusów wykorzystywanych przy włamywaniu się do gier komputerowych i sieci należą:

– Ping of Death (PoD) – do komputera ofiary jest wysyłany pakiet składający się z pociętych fragmentów IP. Większość komputerów pracuje na stosach pakietów TCP/IP o określonej długości. Wysyłany pakiet po odebraniu przez komputer jest składany w całość i przekracza dozwoloną długość IP. Powoduje to zacięcie się lub restart komputera. Metoda jest czasem używana przez hakerów by sprawdzić czy wybrany komputer jest podatny na atak od strony portów i usług.

– Email bombing – do ofiary są wysyłane setki maili zawierających złośliwe oprogramowanie, otwarcie takiego maila powoduje załadowanie się wirusa do systemu komputerowego. Atak uniemożliwia też normalne korzystanie z poczty mailowej i wymaga ingerencji obsługi serwisu, na którym znajduje się skrzynka pocztowa. Maile takie nie są rozsyłane ręcznie przez hakera a najczęściej za pomocą programu komputerowego. Wykrycie agresora jest bardzo trudne, ponieważ często posługuje się on innym zainfekowanym komputerem w celu rozpowszechniania takich maili bez wiedzy prawowitego właściciela. Użytkownik nawet nie jest świadomy tego, że w ostatniej godzinie jego komputer wysłał 1000 maili.

– Email spamming – jest to odmiana email bombing, atak jest skierowany jednak do wielu adresatów w tym samym czasie.

– SPIT – rodzaj spamu (niechcianych wiadomości, reklam itp) atakujących głównie poczty głosowe.

[13] M. Siwicki, *Nielegalna i szkodliwa treść w Internecie. Aspekty prawno-karne*, Warszawa 2011, s. 249; M. Brzozowska, *Ochrona danych osobowych w sieci*, Wrocław 2012, s. 28.

– Hijacking – polega na przechwytywaniu pakietów wysyłanych przez adresata do odbiorcy. Przykładowo komputer (adresat), z którego logujemy się na internetowe konto bankowe (odbiorca) przesyła pakiet informacji zawierający nasz login i hasło. Metoda hijacking-u umożliwia teraz przejęcie tego pakietu i jego skopiowanie na komputer hakera. Większość sieci bankowych ma kodowane połączenia, jednak metoda taka jest skuteczna w przypadku niezabezpieczonego połączenia.

– ActivSynchro – bardziej zaawansowana metoda od hijacking, działa bardzo podobnie, ale polega na podesłaniu na komputer odbiorcy programu, który podszyje się pod oryginalnego odbiorcę i przechwyci wysłane pakiety informacji. Dodatkowo rozsynchronizuje połączenie TCP. Atak ten jest wykorzystywany głównie przy komunikacji pomiędzy dwoma maszynami, pozwala także podsłuchiwać komunikacje i uniemożliwić łączenie się w przyszłości.

– Root compromise – program podsyłany na komputer ofiary służący do zdobycia przez hakera statusu administratora systemu. Haker jako administrator posiada szereg uprawnień pozwalających mu ingerować w wewnętrzny system atakowanego komputera i przechwycenie każdego rodzaju danych, jakie są przechowywane na dysku. Wirus może być podesłany w zainfekowanym mailu lub programie. Atak ten wykorzystuje także luki w systemie operacyjnym i może dostać się do komputera przez np odwiedzenie zainfekowanej strony internetowej.

– Exploit – jest zautomatyzowaną metodą prowadzącą do opanowania systemu (także do zwiększenia uprawnień itp). Przeważnie jest to sekwencja czynności mających na celu wykorzystanie błędów w oprogramowaniu systemów operacyjnych, usług sieciowych lub aplikacji użytkownika do uzyskania dostępu do powłoki systemowej z podwyższonymi uprawnieniami lub uzyskania danych, do których dostęp jest ograniczony lub zabroniony. Istnieją dwa rodzaje exploitów: „local" (lokalne) uruchamiane na atakowanym systemie i „remote" (zdalne) uruchamiane na systemie atakującym (bądź na systemie specjalnie do tego wcześniej przygotowanym). Ich konstrukcja oraz sposób działania bezpośrednio zależy od: atakowanej aplikacji; systemu operacyjnego, na którym aplikacja jest uruchamiana (także jego konfigu-

racji); architektury sprzętowej; rodzaju popełnionego błędu, który będzie wykorzystany do ataku[14]. Exploit jest jednym z najgroźniejszych rodzajów narzędzi hakerskich. Program ten umożliwił kradzież danych z sieci firmy SONY.

– Password attack – jest ogólnym terminem opisującym różne czynności, których celem jest ominięcie mechanizmów ochrony systemu komputerowego opartych na systemie haseł, a więc wszelkie próby złamania, odszyfrowania lub skasowania haseł. Ataki na hasło należą do najprymitywniejszych metod włamań do systemów komputerowych. Umiejętność łamania haseł to w gruncie rzeczy pierwsze czynności, których uczą się początkujący agresorzy – głównie ze względu na to, iż nie wymaga ona specjalnego wykształcenia. Obecnie każdy może łamać hasła Linuksa przy pomocy gotowych programów. Głównie wyróżnia się trzy sposoby łamania:

1) frequency analysis – metoda wykorzystująca częstość występowania liter.
2) ciphertext relative length analysis – metoda wykorzystująca długość zakodowanego tekstu.
3) similar plaintext analysis – metoda badająca zaszyfrowane podobne informacje.

Okazuje się, że wiele aplikacji stosuje proste sposoby szyfrowania danych. W wielu przypadkach zaszyfrowane hasło może zostać odtworzone dosłownie za pomocą kliku operacji matematycznych. W przypadku dużej grupy programów dobre algorytmy kryptograficzne zostały z kolei błędnie użyte przez autorów. W rezultacie liczba obliczeń potrzebnych do złamania hasła spada drastycznie w porównaniu z teoretyczną siłą algorytmu. Czas potrzebny na odtworzenie hasła jest wtedy często niezależny od jego długości i stopnia skomplikowania[15].

– Brute force – metoda stosowana w sytuacjach, gdy wszystkie inne zawodzą. Haker podstawia w miejsce hasła różne kombinację znaków w celu odszyfrowania danych. Użycie tej metody może być niezwykle czasochłonne, często jest stosowane przez

[14] P. Krawaczyński, D. Zelek, *Rodzaje i klasyfikacja włamań oraz ataków internetowych*, s. 28, http://faqxp.cba.pl/faq/winxp/wlamania.htm, [11.02.2012].

[15] P. Krawaczyński, D. Zelek, *Rodzaje...*, op. cit., s. 32.

początkujących i niedoświadczonych przestępców. Hasło jest ciągiem znaków, algorytmem. Istnieją jednak programy pozwalające na automatyczne szukanie właściwego algorytmu.

– Dictionary attack – rozbudowana wersja brute force, agresor przypuszcza, że hasło jako algorytm jest odwzorowaniem jakiegoś słowa słownikowego. Program następnie sprawdza kolejne warianty słownikowe do momentu wyczerpania źródła. Przykładem haseł łamanych w ten sposób są słowa: miłość, bóg, ziemia. Administratorzy systemów często zalecają w celach zwiększenia ochrony, wybieranie haseł połączonych literami i cyframi np.: ziemia375. Zbieg taki znacząco zmniejsza ryzyko udanego odszyfrowania tą metodą.

– Kret – sposób wykorzystywany przez hakera w celu uzyskania pewnych informacji o atakowanym komputerze i systemie. Nadawca (agresor) wysyła maila od odbiorcy (ofiary) np. z ofertą sklepową, promocją, oferta pracy itp. Wykorzystując podstęp zmusza odbiorcę do odesłania odpowiedzi na wiadomość mailową. Pierwotnie wysyłany mail ma w sobie ukryty kod mający na celu zapisanie określonych danych w tej wiadomości. Po odesłaniu przez ofiarę takiego maila np. z podziękowaniem lub odmowa na zaproponowane usługi, haker uzyskuje informację o adresie IP, systemie i innych podstawowych danych o komputerze. Zabieg taki jest pewnego rodzaju nadaniem czy komputer będzie podatny na ataki.

– Web-hacking – haker za pomocą odpowiedniego manipulowanie adresem strony internetowej (URL) jest w stanie dokonać określonych zmian pozwalających podobnie jak przy metodzie kreta na zdobycie podstawowych informacji o komputerze. Fałszywy link jest np. zamieszczany na forum publicznym, rozsyłany w wiadomościach typu spam itp.

– XSS – są to ataki z rodziny HTML Injection odnoszące się do danych zapisywanych / tworzonych poprzez przeglądarkę internetową, a połączonych z przeglądaną stroną WWW. Mowa tu głównie o plikach cookie oraz treściach tworzonych dynamicznie. Jeżeli włamywaczowi uda się wykonać wstrzyknięty przez niego kod z prawami aplikacji web, może spowodować to m.in. kompromitacje DOM (Document Object Mode). Z kolei to może prowadzić do kradzieży plików cookie, przejęcia internetowego kon-

ta, zmianę ustawień konta, itp. W atakach typu XSS wyróżnia się trzy główne gałęzie rozwoju oraz działania, które tworzą swoiste typy ataków XSS:[16]

- *Dom-based XSS – (znany także jako Local XSS bądź po prostu Type 0 XSS) – w tym przypadku błąd istnieje na stronie www, znajdującej się po stronie samego klienta (ma to miejsce wtedy, gdy np. strona oczekuje wpisania określonych danych w aktyw-nym polu bądź pasku URL a następnie dane te są wykorzysty-wane do dokonania zmian w tym samym dokumencie HTML). Je-żeli dane, które wprowadzimy w takim polu będą inne od oczekiwanych (np. kod JavaScript) i strona go wykona, można tu mówić o ataku XSS. Bardziej skomplikowane zastosowanie tego typu ataku może polegać m.in. na podaniu przez włamywacza na spreparowanej stronie specjalnego odnośnika (link), który to po kliknięciu przez ofiarę będzie się odwoływał do podatnej strony www znajdującej się w lokalnym systemie po stronie klienta. Tak, więc jeżeli użytkownik posiada na swoim dysku twardym zapi-saną stronę www, która to jest podatna na Type 0 XSS, stanowi to także duże zagrożenie.*
- *Non-persistent XSS – (zwany także Reflected XSS bądź po prostu Type 1 XSS) – najbardziej znany i rozpowszechniony typ ataków XSS. Ma on miejsce wtedy, kiedy to dane wprowadzane przez użytkownika są impulsem do generowania przez skrypty po stronie serwera strony www z odpowiednim wynikiem – r ezultatem. Najczęstszym polem podatnym na ten atak jest np. pole „szukaj" na stronach internetowych. Atakujący podsyła ofierze odnośnik wyszukany opcją "szukaj" URL, który to poprzez odpowiednie wstrzyknięcie kodu zwróci wynikową stronę www w kierunku atakującego, a nie w stronę zwyczajnego użytkownika (innymi słowy, atakujący zobaczy treść, którą normalnie zobaczyłaby ofiara). Może to być wykorzystane do zdobycia poufnych danych, prywatnych korespondencji itp.*

[16] P. Krawaczyński, D. Zelek, *Rodzaje...*, op. cit., s. 35.

- *Referes XSS – (opcjonalnie znany jako Persistent XSS, Second-order XSS bądź po prostu Type 2 XSS) – najniebezpieczniejsza oraz najbardziej potężna technika XSS (bardzo często używana). Atak ten ma miejsce wtedy, kiedy to dane podawane przez użytkownika do okna aplikacji internetowej są przetrzymywane w „jakiś" sposób na serwerze (np. baza danych) a następnie są wyświetlane na stronie www. Najczęstsze miejsce tego typu ataku to wszelakiego rodzaju fora dyskusyjne, systemy komentarzy bądź też księgi gości. Metoda bardzo wygodna dla atakującego, ponieważ dokonuje on jednego wstrzyknięcia, które to oddziałuje na duża liczbę odbiorców (np. każdy otwierający internetową księgę gości, którą to wcześniej odwiedził atakujący, pozostawiając po sobie ślad w postaci złośliwego kodu JavaScript). Dodatkowo na ten rodzaj ataku są podatne także takie aplikacje jak systemy kont pocztowych, logi systemowe, itp.*[17]

– Socjotechnika to jedna z najczęstszych metod ataku na konta graczy. Haker stara się wpłynąć na umysł odbiorcy w taki sposób by uzyskać od samej ofiary potrzebne dane. Socjotechnika jest to psychologiczna metoda zdobywania informacji. Takim atakiem może być np. mail, telefon lub inna forma zawiadomienia użytkownika danej usługi o pewnym wyimaginowanym problemie, jaki zaistniał. Haker podszywa się wówczas najczęściej pod administratora lub pracownika firmy, w której konsument posiada swoje konto. Wysyłane maile najczęściej odnoszą się do faktu zaistniałego zagrożenia w stosunku do istniejącego konta gracza – użytkownika i wymagane jest natychmiastowe potwierdzenie danych poufnych. Haker najczęściej zamieszcza link do podrobionej strony, bliźniaczo podobnej do oryginalnej, na której użytkownik musi zalogować się na swoje konto. Dane oczywiście zostają przesłane na komputer hakera.

– Koń Trojański (znany także jako Trojan) jest programem, który poniekąd podszywając się pod przydatną i użyteczną aplikację dla potencjalnego użytkownika, posiada tak naprawdę ukryte funkcje, które to pozwalają z kolei jego autorowi na prze-

[17] P. Krawaczyński, D. Zelek, *Rodzaje...*, op. cit., s. 36.

prowadzanie nieautoryzowanych oraz niepożądanych czynności na maszynie swojej ofiary. Dla zachowania pozorów, niektóre konie trojańskie rzeczywiście oferują swojej ofierze przydatne funkcje, jednak użytkownik nie ma pojęcia, iż oprócz tych funkcji istnieje cały szereg innych postronnych procedur, dzięki to, którym na pierwszy rzut oka „przyjazny" program jest niebezpiecznym narzędziem w rękach włamywacza (atakujący jest w stanie kierować działaniem trojana bez wiedzy użytkownika). Trojany mogą także nie oferować żadnych przydatnych funkcji dla swojej ofiary, ponieważ ofiara może nawet nie zdawać sobie sprawy z tego, iż w jej systemie w ogóle znajduje się trojan (kolokwialnie mówiąc jest on „głęboko ukryty"). Chociaż Koń trojański to określenie całej gamy niebezpiecznych aplikacji, to bardzo często słowo to występuje także w konkretnym znaczeniu, tj. może ono opisywać postronną aplikację, która pozwala włamywaczowi na zdalne administrowanie systemem ofiary[18].

– Backdoor – program umożliwiający przestępcy nieautoryzowane wejście do systemu poprzez lukę w systemach bezpieczeństwa. Program o cechach ukrytych, bardzo trudno wykrywalny gdyż najczęściej podczepia się jak element kody pod już istniejącą aplikację zainstalowaną na dysku. Haker używający „tylnych drzwi" uzyskuje prawa administratora i jest w stanie uzyskać wszelkie dane obecne na zainfekowanym komputerze, a także wykorzystać takiego PC do dalszych ataków na inne maszyny. Metoda taka działa na zasadzie pajęczyny gdzie wewnątrz znajduje się zainfekowany komputer służący za źródło sygnału przekazywanego innym jednostkom w systemie. Backdoor jest potencjalnie najniebezpieczniejszą bronią w rekach hakera, ponieważ nie da się przed nim całkowicie zabezpieczyć. Nawet najlepiej zabezpieczony komputer i system może posiadać setki małych luk w ochronie, takie luki są właśnie wykorzystywane przez oprogramowanie Backdoor. Sam program ma także inne zastosowanie, jest używany często przez administratora sieci np w fabrykach do zdalnego nadzoru nad setkami komputerów. Podczas awarii jednej z jednostek, administrator jest w stanie zdalnie wejść ze swojego komputera na maszynę i naprawić problem nie

[18] P. Krawaczyński, D. Zelek, *Rodzaje...*, op. cit., s. 47.

wstając z krzesła. Hakerzy uczynili jednak z Backdoor jedną z najgroźniejszych broni.

– Rootkit – program implementowany często do innego złośliwego oprogramowania jak „strażnik". Jego celem jest ukrycie działalności hakera i niepożądanego programu.

– Spyware – program szpiegowski, mający za zadanie zapisywanie w swojej pamięci wszelkiej aktywności na zainfekowanym komputerze. Do jego zadań należy np zapisywanie kolejności wciskanych klawiszy na klawiaturze w celu późniejszego odsortowania z nich loginów i haseł. Spywere jest często uważany za pochodne Koni Trojańskich, ale zaliczany jest do grupy złośliwego oprogramowania pod nazwą „malware". Bardzo często program tego typu w odróżnienia od Trojana, ma ściśle sprecyzowane zadanie do wykonania.

– Keylogger – program z rodziny koni trojańskich (spyware), służący do przechwytywania i zapisywania do pliku znaków wpisywanych przez użytkownika za pośrednictwem klawiatury. W połączeniu z innym programem typu backdoor (działającym w oparciu o model klient-serwer) pozwala uzyskać hasła oraz inne istotne informacje o użytkowniku komputera. Keylogger jest najczęściej wykorzystywanym narzędziem złodziei w grach komputerowych. Użytkownik korzystający z usług gier internetowych często poszukuje różnego rodzaju dodatków i materiałów do gry, w którą aktualnie gra. Takie strony i dodatki padają najczęściej ofiarą hakerów w celu późniejszego dostania się na dysk komputera. Gracz przeglądający zainfekowane pliki/strony nieświadomie pobiera Keylogger na swój komputer, co skutkuję w 90% przypadkach utratą konta w grze komputerowej.

– Scumware – program instalujący się na dysku komputera i umieszczający na witrynach internetowych linków do stron lub plików. Takie linki są widoczne jedynie dla użytkownika korzystającego z komputera zainfekowanego Scumware. Oprogramowanie jest używane głównie w celach reklamowych, ale ma także zastosowanie w rozpowszechnianiu keyloggerów i innych programów szpiegujących.

– Stealware – bardzo niebezpieczny program szpiegujący, ponieważ ujawnia się tylko w jednym momencie. Aktywuje go płatność dokonywana za pomocą Internetu na zainfekowanym

komputerze np. kartą płatniczą, przelewem internetowy. Program w chwili wysłania żądania przelania pieniędzy natychmiast kopiuje dane personalne, klucze i kody karty kredytowej. Dodatkowo ma także funkcję podmiany danych. Program jest w stanie przekierować płatność podmieniając dane adresata na te podane przez hakera. Często bywa wykorzystywany przy opłatach abonamentowych za korzystanie z gier internetowych MMORPG.

Przedstawione metody włamań to tylko niewielka część tych, jakim dysponują hakerzy. Działalność przestępcza na tle komputerów i kradzieży danych przy użyciu Internetu ulega ciągłym zmianom i ewolucji[19].

Bibliografia

1. Barczak-Oplustil A., Bogdan G., Ćwiąkalski Z., Dąbrowska-Kardas M., Kardas P., Majewski J., Ralewski J., Rodzynkiewicz M., Szewczyk M., Wróbel W., [w:] Zoll A. (red.), *Kodeks karny. Część szczególna komentarz*, Kraków 2006.
2. Bojarski M., Giezek J., Sienkiewicz Z., *Prawo karne materialne. Część ogólna i szczególna*, red. M. Bojarski, Warszawa 2004.
3. Brzozowska M., *Ochrona danych osobowych w sieci*, Wrocław 2012.
4. *Co to jest karta typu PrePaid*, wp.pl polonia, http://polonia.wp.pl/country,1,title,Co-to-jest-karta-typu-PrePaid,wid,10478181,faq.html?ticaid=1f4d5, [03.01.2012].
5. Dziak P., Figat P., Kaczanowska K., Sarna M., Wownysz J., *Bezpieczne korzystanie z Internetu*, Warszawa 2012.
6. Grześkowiak A., Wiak K. (red.), *Kodeks karny. Komentarz*, Warszawa 2012.
7. Jordan T., *Hakerstwo*, Warszawa 2011.
8. Klander L., *Hacker proof – czyli jak sie bronić przed intruzami*, Warszawa 1998.
9. Korusiewicz A., *Zagrożenia w sieci Internet*, Warszawa 2007.
10. Krawaczyński P., Zelek D., *Rodzaje i klasyfikacja włamań oraz ataków internetowych*, http://faqxp.cba.pl/faq/winxp/wlamania.htm, [11.02.2012].
11. Marek A., Oczkowski T., *Kradzież i przywłaszczenie*, [w:] Zawłocki R. (red. tomu), *System prawa karnego*, Warszawa 2011, tom 9.
12. *PlayStation Network: Sony wydaje oświadczenie. Gorzej być nie mogło ...*,

[19] L. Klander, *Hacker proof – czyli jak sie bronić przed intruzami*, Warszawa 1998, s. 304; P. Dziak, P. Figat, K. Kaczanowska, M. Sarna, J. Wownysz, *Bezpieczne korzystanie z Internetu*, Warszawa 2012, s. 5; A. Korusiewicz, *Zagrożenia w sieci Internet*, Warszawa 2007, s. 32; T. Jordan, *Hakerstwo*, Warszawa 2011, s. 85.

http://www.cdaction.pl/news-18922/playstation-network-sony-wydaje-oswiadczenie-gorzej-byc-nie-moglo.html, [26.04.2011].
13. Post. SN z 24.6.2010r., V KK 388/09, OSNKW 2010, Nr 9, poz. 82.
14. *Rosnąca popularność gier MMORPG*, Praca w biznesie komputerowym, http://praca.komputerowcy.info/2012/02/14/rosnaca-popularnosc-gier-mmorpg/, [14.02.1012].
15. Siwicki M., *Nielegalna i szkodliwa treść w Internecie. Aspekty prawno karne*, Warszawa 2011.
16. Stefański R. A., *Prawo karne materialne. Część szczególna*, Warszawa 2009.
17. Uchwała SN z 19.4.1977 r., VII KZP 3/77, OSNKW 1977, Nr 6, poz.54.
18. Wyrok SA w Krakowie z 8.7.2009 r., II AKa 98/09, KZS 2009, Nr 7-8, poz. 58.
19. Wyrok SN z 9.9.2004 r., V KK 1444/04, OSNwSK 2004, Nr 1, poz. 1533.
20. Wyrok SN z 30.12.1970 r., IV KR 211/70.