Dr Wojciech Kasprzak[1]
Collegium Balticum w Szczecinie

WYKRYWANIE I ŚCIGANIE SPRAWCÓW KRADZIEŻY DÓBR Z GIER KOMPUTEROWYCH

Streszczenie

W artykule opisana została problematyka kradzieży dóbr z gier komputerowych. Współczesne źródła rozrywki zawierają często wiele elementów wykorzystujących wirtualne środki płatnicze. Wiąże się to z wzrostem kradzieży na tle cyfrowym, także w stosunku do gier internetowych. Głównym celem hakerów stały się loginy, hasła dostępu do kont internetowych, dane personalne, numery kart kredytowych i wirtualne elementy, które mogą zostać sprzedane. Wykrywanie przestępstw podobnego typu jest niezwykle trudne dla współczesnych organów ścigania. Sprawca czynu zabronionego jest często osoba z zagranicy wykorzystującą zaawansowaną technologię, wirusy, robaki komputerowe i innego rodzaju złośliwe oprogramowanie. W artykule omówione zostało również podejście organów ścigania do problematyki kradzieży dóbr z gier komputerowych.

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

[1] Dr Wojciech Andrzej Kasprzak – prawnik, absolwent Wydziału Prawa i Administracji Uniwersytetu Warmińsko-Mazurskiego w Olsztynie. Doktorat *Ślady cyfrowe. Studium prawno-kryminalistyczne* pod kierownictwem dr hab. Denisa Sołodowa na Uniwersytecie Warmińsko-Mazurskim w Olsztynie w 2015 r. W swoich opracowaniach łączy zainteresowania prawem i kryminalistyką z osiągnięciami współczesnej informatyki. W 2014 r. wyróżniony nagrodą im. Prof. Tadeusza Hanauska, ustanowioną przez Polskie Towarzystwo Kryminalistyczne i Uniwersytet Warszawski.

Kontakt z Autorem: kasprzak.wojciech@o2.pl.

DETECTING AND PURSUING THE PERPETRATORS OF THEFT OF GOODS IN COMPUTER GAMES

Abstract

The article discussed is the issue of the theft of goods from computer games. Modern multimedia entertainment is equipped with a number of items associated with electronic payment sytemami. Increasingly, there are cases of theft of digital data contained in the online games. The main target of hackers are logins and passwords for online accounts, personal information, credit card numbers, virtual items that can be sold. Detection of such crimes is a very difficult and a challenge for today's law enforcement agencies. Offender is a foreign person, and often uses technologically advanced digital tools in the form of viruses, worms and other malicious software. The article described the issue of actions taken by law enforcement agencies to report the crime for theft of goods from a computer game.

Keywords: brak słów kluczy w języku angielskim

Postęp technologiczny zawsze oznacza nowe przywileje dla konsumentów, szerszy dostęp do informacji, szybsze i bardziej komfortowe usługi, otwiera też 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 komputera, nie wychodząc nawet z domu lub miejsca pracy, kafejki internetowej. Poza klasycznymi i znanymi policji działaniami hakerów (włamania do prywatnych firm, tworzenie wirusów) istnieje jeszcze wiele innych mało znanych rodzajów przestępstw komputerowych, które stają się coraz większym zagrożeniem.

Źródłem kradzieży dóbr cyfrowych, stały się gry internetowe. Najbardziej podatnymi grami na kradzież są produkcje z gatunku MMO (Massively Multiplayer Online). Gry te pozwalają na wspólną zabawę milionom ludzi jednocześnie w wirtualnie wykreowanym świecie[2] za pośrednictwem Internetu. Gracz – konsument wciela się w takiej grze w wykreowanego przez siebie awatara – protagonistę[3] i wraz z innymi graczami z całego świata dąży do wyznaczonego celu. MMORPG jest obecnie najpopularniejszą

[2] J. Dovey, H. W. Kennedy, *Kultura gier komputerowych*, Warszawa 2011, s. 114.

[3] Ibidem, s. 118.

formą rozrywki wśród miłośników gier komputerowych. Specyfika tego gatunku wynika z paru unikatowych cech, których nie posiadają inne gatunki gier, lub które nie są wystarczająco wyeksponowane przez wirtualną rozrywkę. Cechą dominującą w grach MMORPG jest ścisła współpraca pomiędzy graczami. Osamotniony użytkownik nie jest w stanie osiągnąć postawionych przed nim zadań. Element społecznościowy jest głównym czynnikiem przykuwającym użytkowników do wybranej gry MMO[4].

Program, poza dostarczaniem rozrywki i odczuć czysto estetycznych, pozwala na zawiązywanie znajomości pomiędzy graczami z całego świata. Produkcja ta jest także miejscem spotkań, rozmów, wirtualnego życia, a także sposobem na oderwanie się od rzeczywistości. Mechanikę rozgrywki w grach z gatunku MMORPG trudno zaklasyfikować do jednej dziedziny – jak w przypadku innych rodzajów gier. Produkt ten jest bardzo złożony, ponieważ na całość składa się wiele pomniejszych elementów jak współpraca, rywalizacja, eksploracja. Często jest on mieszaniną wszystkich innych gatunków gier. Są w nim czynniki bardzo mocno oddziałujące na psychikę odbiorcy, jak ciągła chęć polepszania swojej sytuacji w grze i presja rywalizacji z innymi graczami. Gracz gra, bo chce by jego awatar (bohater) był coraz silniejszy, chce utrzymywać kontakty z poznanymi ludźmi, a także z nimi rywalizować. Odbiorca w ostateczności stara się współistnieć razem ze światem gry, tworząc własne wirtualne *alter ego* będące, przykładowo „potężnym czarodziejem i pogromcą smoków", podczas, gdy w codziennym życiu jest np. nauczycielem. Poczucie bycia kimś zupełnie innym i szansa na wcielanie się w pewnego rodzaju aktora biorącego udział w „wielkiej wyprawie przeciw siłom zła" jest właśnie fenomenem, który powoduje olbrzymią popularność gier gatunku MMORPG[5].

Producent gry, udostępniając produkt konsumentom przez Internet, opiera się na dwóch podstawowych metodach płatności. Najpopularniejszą metodą jest Free to Play (F2P – Darmowa Gra). Mechanizm ten polega na mikrotransakcjach. Producent udostępnia swój produkt za darmo, ale dodaje możliwość robienia

[4] D. Urbańska-Galanciak, *Homo players Strategie odbioru gier komputerowych*, Warszawa 2010, s. 77.

[5] Ibidem, s. 75.

zakupów za prawdziwe pieniądze, w elektronicznym sklepie na oficjalnej stronie produkcji. Konsument może za niewielką opłatą dokupić do swojego „bohatera" dodatkowe elementy jak zbroję lub miecz, niedostępny 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 wysokości 30 lub 60 dni. Każdy użytkownik gry MMORPG przed rozpoczęciem rozgrywki musi utworzyć indywidualne konto, na którym będą zapisywane postępy w grze. Konto znajduje się na serwerach właściciela gry i jest zabezpieczone loginem i hasłem, a także systemami bezpieczeństwa, jakie zapewnia dostawca usługi gry komputerowej. Konto to z czasem nabiera pewnej wartości, stając się „dobrem internetowym". Czas, poświęcony na zdobycie określonych rzeczy w grze można przeliczyć na sumę pieniędzy, jaką płaci się za możliwość użytkowania takiej gry. Użytkownik przeznacza własny czas na doskonalenie posiadanej postaci. Staje się to pewnego rodzaju mieniem niematerialnym człowieka, który spędził olbrzymią ilość czasu w wirtualnym świecie[6].

W świetle prawa, Internet sam w sobie nie może być przypisany określonemu podmiotowi jako konkretne dobro prawne z uwagi na jego ogólnoświatowy wymiar. Konkretnym podmiotom mogą być natomiast przypisane określone dobra zawarte w Internecie lub takie, dzięki którym funkcjonują np. technologie i urządzenia. Konsument, który godzi się na korzystanie z Internetu ponosi w tym celu pewne koszty. Nie płaci za sam Internet ponieważ ten sam w sobie nie wiąże się z żadnymi formalnymi kosztami w sensie dobra materialnego, płaci za możliwość użytkowania sieci i jej funkcji. Internet stanowi więc źródło korzyści dla szeregu podmiotów umieszczających swoje usługi w sieci np. innych użytkowników, przedsiębiorców, podmiotów obsługujących poprawne funkcjonowanie i rozwój Internetu. Charakter

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

dóbr związanych z Internetem dzieli się na dwie kategorie: materialne i niematerialne.

Istota funkcjonowania Internetu jest związana z poprawnym działaniem wielu urządzeń, czyli dóbr materialnych takich jak urządzenia przesyłające, odpowiadające za gromadzenie danych i cała infrastruktura związana z techniczną obsługą sieci. Art. 49 k.c. stanowi, że urządzenia służące do doprowadzania lub odprowadzania płynów, pary, gazu, energii elektrycznej oraz inne urządzenia podobne nie należą do części składowych nieruchomości, jeżeli wchodzą w skład przedsiębiorstwa. Natomiast osoba, która poniosła koszty budowy tego rodzaju urządzeń i jest ich właścicielem, może żądać, aby przedsiębiorca, który przyłączył urządzenia do swojej sieci nabył ich własność za odpowiednim wynagrodzeniem chyba, że w umowie strony postanowiły inaczej. Z żądaniem przeniesienia własności tych urządzeń może wystąpić także przedsiębiorca[7]. Nie ma więc przeciwwskazań aby zapisem „innych urządzeń podobnych" nie objąć także urządzeń doprowadzających Internet jak sieci telekomunikacyjne, światłowody, nadajniki dalekiego zasięgu itp.

Do dóbr materialnych w kontekście użytkowania Internetu zalicza się też wszelkie dobra biorące udział w wymianie handlowej za pośrednictwem sieci. Najlepszym przykładem dla takiego obrotu dobrami są sklepy internetowe i aukcje internetowe. Sam sklep w postaci elektronicznej stanowi mienie należące do jego właściciela. Przedstawia on realną wartość (marka, nazwa) mimo, że nie posiada fizycznej placówki jak sieć sklepów TESCO lub Real. Stanowi wiec dobro internetowe.

Dobra Internetowe niematerialne to wszelkiego rodzaju dane przesyłane droga elektroniczną, nie posiadające cech fizycznych np. nośników CD/DVD. Dzielą się one na:

1) dobra niechronione (nieregulowane) w szczególny sposób (z którymi nie wiążą się odrębne prawa wyłączne, czyli przewidziane ustawowo prawa polegające na decydowaniu przez podmiot wyłącznie uprawniony o korzystaniu z danego dobra przez inne podmioty),

[7] R. Golat, *Prawo Internetu dla praktyków*, Gdańsk 2009, s. 14.

2) dobra stanowiące wyodrębniony normatywnie przedmiot ochrony (regulowane ustawowo w sposób szczególny, w tym poprzez ochronę poszczególnych dóbr na zasadzie odrębnych praw wyłącznych).

Wszelkie dobra z gier komputerowych gatunku MMORPG zaliczają się do dóbr niematerialnych. Konsument może uznać za swoje mienie rzeczy niematerialne znajdujące się na używanym koncie gry pod postacią danych cyfrowych. Dobra takie zalicza się do niechronionych (nieregulowanych). Brak jest szczegółowych zapisów ustawowych dotyczących dóbr o takim charakterze. Ustawodawca zalicza je do elektronicznych danych i kradzieży informacji. Czynnikiem, który pozwala na zaliczenie dobra niematerialnego pochodzącego z gry komputerowej jako swoje mienie o wartości realnej jest indywidualne przeżycie psychiczne lub myślowe, długotrwałe doznanie emocjonalne płynące z prowadzenia rozgrywki w grze internetowej. To, co osiąga się w grze komputerowej staje się naszym dobrem niematerialnym. Sama gra stanowi zbiór danych cyfrowych (produkt jest skonstruowany z języka informatycznego), Internet stanowi natomiast jedno z podstawowych źródeł informacji (danych). Informacje są dobrami prawnymi, gdyż mają znaczenie dla korzystających z nich podmiotów, w tym przedsiębiorców, choć informacje jako takie nie są przedmiotem odrębnych praw wyłącznych[8]. Polskie prawo uznaje dobra z gier komputerowych za informacje i dane. Mienie to nie ma fizycznej postaci, występuje jedynie w formie wirtualnej, niematerialnej. Dodatkowo nie jest odrębnie regulowane.

W 99% przypadków kradzież dobra z gier komputerowych dotyczy gier MMORPG. Każdy użytkownik posiadający dostęp do produktu jest zmuszony do przestrzegania rygorystycznych systemów bezpieczeństwa w celach ochrony jego mienia wirtualnego. Konta do gier MMORPG są zabezpieczone loginem i hasłem indywidualnego użytkownika. 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. Już posiadanie konta wymaga nabycia produktu, elementy, które pojawiają się na koncie

[8] R. Golat, op. cit., s. 15.

z upływem czasu, także nabywają realną wartość. 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[9].

Wypuszczenie każdego nowego produktu w dobie Internetu, wymagającego stałego połączenia z siecią naraża nasz komputer na ataki z zewnątrz. Działania hakerów obejmują kilka metod. Pierwszą 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. Trzecią i ostatnią metodą działań przestępców jest łamanie zabezpieczeń i rozpowszechnianie pirackiego oprogramowania. Podstawowym problemem w zabezpieczeniach systemów jest fakt, że nie da się ich w 100% ochronić. 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 dzielą się 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 zarówno u czytelnika jak i autora[10]. Działalność osoby pragnącej dokonać kradzieży dóbr z gier komputerowych to jeden z rodzajów ataków

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

[10] M. Siwicki, *Nielegalna i szkodliwa treść w Internecie*, Warszawa 2011, s. 249, por. M. Brzozowska, *Ochrona danych osobowych w sieci*, Wrocław 2012, s. 28.

hakerskich. Ataki hakerskie dzieli się ze względu na różne kryteria.

Przy uwzględnieniu miejsca ich przeprowadzania:

- zewnętrzne (zdalne) – ataki przeprowadzane są z systemów znajdujących się poza atakowaną siecią, na przykład atak na sieć firmy NARF.Inc odbywa się z sieci firmy Agresory.Inc.
- wewnętrzne (lokalne) – ataki przeprowadzane są z systemów znajdujących się w atakowanej sieci, na przykład atak na główny serwer firmy NARF.Inc odbywa się z serwera działu zaopatrzenia tej samej firmy[11].

Ataki takie mają na celu spowodowanie szkody lub kradzież danych z systemów. Są to powszechne metody stosowane przez konkurencyjne firmy wykradające sobie technologie i informacje. Konsekwencjami mogą być najczęściej przerwy w pracy i działaniu poszczególnych komputerów lub całej sieci. Dodatkowo zdarzają się także uszkodzenia sprzętu, utraty ważnych i poufnych danych.

Ze względu na zamiar wyróżnia się:

- atak umyślny – atakujący zdaje sobie sprawę z tego, co robi i jakie konsekwencje mogą z tego wyniknąć, na przykład atak w celu uzyskania konkretnie wytyczonych informacji,
- atak nieumyślny – atakujący przypadkowo i nieświadomie dokonuje ataku, na przykład jeden z użytkowników serwera przez błąd programu obchodzi system autoryzacji uzyskując prawa administratora.

Biorąc pod uwagę skutek otrzymuje się:

- atak udany – rozpoczęty atak przez atakującego kończy się osiągnięciem zamierzonego celu, na przykład poprzez przeskanowanie sieci wykrywa lukę w zabezpieczeniu, którą wykorzystuje do ataku. Atak kończy się powodzeniem a haker zaciera za sobą ślady i opuszcza atakowany cel. Udany skutek ataku możemy podzielić na:
  - aktywny – w wyniku ataku system komputerowy traci integralność, na przykład atak włamywacza, który

[11] P. Krawaczyński, D. Zelek, *Rodzaje i klasyfikacja włamań oraz ataków internetowych*, s. 2, http://www.hal.trzepak.net/faq/winxp/wlamania.htm, [15.06.2015].

usuwa pewną ilość ważnych danych oraz powoduje zmianę działania programów. Atakiem aktywnym może być także modyfikowanie strumienia danych lub tworzenie danych fałszywych,

- pasywny – atak ten polega na wejściu do systemu bez dokonywania żadnych zmian w treści cyfrowej, na przykład atak włamywacza, który kopiuje pewną ilość ważnych danych nie powodując zmian w działaniu programów. Atakiem pasywnym może być także podsłuchiwanie lub monitorowanie przesyłanych danych. W tym przypadku celem osoby atakującej jest odkrycie zawartości komunikatu. Typowym atakiem pasywnym może być analiza przesyłu danych (traffic analysis). Ataki pasywne są bardzo trudne do wykrycia, ponieważ nie wiążą się z modyfikacjami jakichkolwiek danych,

– atak nieudany – rozpoczęty atak ostatecznie nie osiąga zamierzonego celu.[12]

W przypadku, gdy użytkownik gry internetowej staje się ofiarą przestępstwa kradzieży mienia, nie pozostaje na straconej pozycji. Pokrzywdzony powinien podjąć odpowiednie działania w stosunku do zaistniałej sytuacji. Pierwszym etapem jest zgłoszenie problemu do administratora usługi, w której nastąpiło popełnienie przestępstwa kradzieży. W tym celu pokrzywdzony ma do dyspozycji liczne wewnętrzne odnośniki i narzędzia takie jak maile, formularze zgłoszenia problemu, telefon kontaktowy, a także może napisać do odpowiedniej osoby w samej grze. Firmy dostarczające gry z gatunku MMORPG umieszczają wewnątrz świata gry postacie operowane przez wyznaczonych w tym celu pracowników. Taka osoba ma właśnie na celu zapewnić błyskawiczny kontakt w razie zaistnienia problemu. Administrator usługi po zgłoszeniu problemu przez pokrzywdzonego jest zobowiązany wewnętrznym regulaminem każdej z produkcji do podjęcia działań w celu rozwiązania i usunięcia zaistniałego problemu. Konto pokrzywdzonego zostaje na czas sprawdzania wyłączone z użytku. Administrator usługi sprawdza czy na konto faktycznie nastąpiło włamanie poprzez prześledzenie logów (jest to zapis

[12] P. Krawaczyński, D. Zelek, op. cit., s. 3.

elektroniczny, który stanowi historię operacji przeprowadzonych na danym koncie), a także numerów IP, z jakich łączono się z serwerami. Po wykryciu nieprawidłowości, administrator informuję pokrzywdzonego o wykryciu błędu i udziela dalszych szczegółowych informacji na temat czasu potrzebnego by przywrócić konto do stanu z przed włamania. Celem działań administratora jest przede wszystkim przywrócenie możliwości korzystania z usługi dla pokrzywdzonego, nie jest on za to organem śledczym i nie będzie podejmował działań mających na celu schwytanie i dochodzenie zadośćuczynienia od sprawcy. Całość działań administratora systemu nie powinna przekroczyć miesiąca, po tym czasie pokrzywdzony otrzyma zwrot dostępu do konta, a także zostaną przywrócone wszelkie skradzione dobra, które były celem ataku. W przypadku, gdy przestępca sprzedał dane do konta i samą możliwość jego użytkowania, nowy właściciel traci na rzecz pokrzywdzonego prawo użytkowania danego konta. Warto nadmienić, że opisany wyżej schemat działania administratora jest przykładem dla firm dysponujących znacznym zapleczem pracowników. Bardzo często zdarza się tak, że w przypadku kradzieży mienia będących częścią składową gier dostarczanych przez mniejsze firmy, administratorzy wykazują bierność i nie reagują na skargi pokrzywdzonego. W takim przypadku można wymusić egzekwowanie prawa przez poinformowanie odpowiednich organów ścigania.

Pokrzywdzony zawiadamia organ procesowy[13] o podejrzeniu popełnienia przestępstwa. Aby wszczęcie postępowania było prawnie dopuszczalne, powinien istnieć, co najmniej taki zespół danych, który obiektywnie uprawdopodabnia fakt popełnienia przestępstwa, subiektywnie zaś wywołuje co do tego faktu wysoki

[13] Organy ścigania określane także jako organy procesowe zalicza się do kategorii uczestników postępowania karnego. Organ taki posiada określoną strukturę organizacyjną i działa w oparciu o właściwe przepisy. W ramach postępowania przygotowawczego procesu można wyróżnić organy prowadzące postępowanie (śledztwo, dochodzenie) oraz organ nadzorujący przebieg postępowania, które same podejmują czynności procesowe, w tym także czynności dowodowe. Z. Świda, R. Ponikowski, W. Posnow, *Postępowanie karne część ogólna*, Warszawa 2008, s. 79; J. Grajewski, *Prawo karne procesowe część ogólna*, Warszawa 2007, s. 184; S. Waltoś, *Proces karny zarys systemu*, Warszawa 2009, s. 481; T. Grzegorczyk, J. Tylman, *Polskie postępowanie karne*, Warszawa 2011, s. 219.

stopień podejrzenia[14]. Organ procesowy w momencie wszczęcia postępowania musi określić klasyfikację prawną czynu zgłoszonego przez pokrzywdzonego.

W obecnym systemie polskiego prawa kradzież dobra z gier komputerowych w większości przypadków jest klasyfikowana jako kradzież informacji na mocy art. 267 k.k. Są jednak znane przypadki, gdy takie zgłoszenie jest zaliczane jako kradzież z włamaniem na mocy art. 279 k.k. Przestępstwo jakim jest kradzież mienia z gier internetowych posiada wszelkie przesłanki do tego by zawsze było klasyfikowane jako kradzież z włamaniem[15]. Dla przykładu: Policja z Zielonej Góry w 2011r. wszczęła postępowanie w sprawie zgłoszenia kradzieży „statku kosmicznego" o przybliżonej wartości 1000 zł, ponieważ pokrzywdzona inwestowała w grę prawdziwe pieniądze. Organ zaklasyfikował czyn jako kradzież z włamaniem[16]. Inny przypadek zgłoszenia kradzieży z gry internetowej dotyczył mieszkańca mazurskich Mikołajek. Pokrzywdzony złożył doniesienie o kradzieży dwóch postaci z gry MMORPG o łącznej wartości 5000zł. Poszkodowany przedstawił dowody zakupu wirtualnych przedmiotów, jakie znajdowały się na koncie. Policja podjęła działania mające na celu ustalenie sprawcy czynu zabronionego i zaklasyfikowała czyn jako kradzież z włamaniem[17].

Organ przeprowadzający czynności sprawdzające[18], powinien w pierwszej kolejności przesłuchać pokrzywdzonego, a następnie sprawdzić prawdziwość jego wersji. Ważne jest, aby pokrzywdzony przed zgłoszeniem podejrzenia popełnienia przestępstwa, wykorzystał wszystkie dostępne możliwości mogące pomóc mu w odzyskaniu skradzionego mienia (np. powiadomienie administratora usługi). Jest to ważny czynnik dowodowy w sprawie prowadzonej przez organ ścigania. W momencie przesłuchania,

---

[14] T. Grzegorczyk, J. Tylman, *Polskie postępowanie karne*, Warszawa 2011, s. 669.

[15] R. Zawłocki, *Przestępstwa przeciw mieniu i gospodarcze*, Warszawa 2011, s. 87.

[16] http://www.polskieradio.pl/5/3/Artykul/505045,Policja-szuka-zlodzieja-statku-kosmicznego, [15.06.2015].

[17] http://www.fakt.pl/Ukradli-mi-szamanke-z-komputera-,artykuly,87579,1.html, [15.06.2015].

[18] Z. Świda, R. Ponikowski, W. Posnow, op. cit., s. 229; J. Grajewski, op. cit., s. 318.

pokrzywdzony powinien udzielić szczegółowych informacji na temat zdarzenia, dostarczyć możliwie jak największą liczbę informacji oraz poinformować, że skradzione dobra były niematerialne, ale posiadały wartość materialną w pieniądzach. Organ prowadzący przesłuchanie powinien ustalić:

- tytuł gry, której dotyczy zgłoszenie,
- administratora gry,
- wydawcę gry i ustawowego reprezentanta wydawcy na terenie Polski. Informacja ta jest bardzo ważna, ponieważ 99,9% produkcji gier internetowych to marki zagraniczne, często nie posiadające nawet oddziału na terenie Polski,
- co zostało skradzione. Pokrzywdzony musi wyraźnie zaznaczyć czy zostało mu ukradzione całe konto w grze internetowej, sam dostęp do takiego konta, czy też integralne części powiązane z takim kontem (elementy wyposażenia postaci gracza, same postacie bohaterów).

W czasie przesłuchania trzeba dążyć do ustalenia domniemanej przyczyny kradzieży. Pokrzywdzony może mieć informacje, które pozwolą określić, jakiego rodzaju ataku komputerowego padł ofiarą. Śledztwo może przebiegać inaczej, jeżeli zostanie ustalone, że do kradzieży mogło dojść na komputerze pokrzywdzonego, bez ingerencji zewnętrznej ze strony Internetu.

Największym problemem zarówno dla pokrzywdzonego jak i organu prowadzącego postępowanie jest ustalenie wartości skradzionego mienia. Rzeczy niematerialne o charakterze wirtualnym trudno jest wycenić, ponieważ nie posiadają swoich fizycznych odpowiedników. Wartością będzie subiektywna ocena pokrzywdzonego względem czasu i środków poświęconych na zdobycie danych wartości, które zostały skradzione. Elementy składowe skradzionego mienia mogą się zasadniczo różnić od siebie, gdyż część może pochodzić z wirtualnego sklepu, przypisanego do gry. Posiadają wtedy swoją sztywną cenę i ułatwiają oszacowanie całości poniesionych strat. Reszta elementów skradzionych musi być obiektywnie przeliczona na czas poświęcony w celu zdobycia takich materiałów (chodzi tu zarówno o przedmioty istniejące w grze, ale takie, które można zdobyć dla swojego bohatera jedynie przez czynne uczestniczenie w rozgrywce). Następnym czynnikiem wpływającym na oszacowanie całości po-

niesionych strat są wniesione opłaty abonamentowe, pozwalające pokrzywdzonemu na użytkowanie samej gry. Musi być to wartość wyliczona odpowiednio to skali poniesionych strat. Jeżeli pokrzywdzony utracił całkowicie dostęp do konta to można liczyć ten element jako całość spędzonego w świecie gry czasu od pierwszego logowania, w jednostkach miesięcznych[19]. Dopiero po zsumowaniu wszystkich tych elementów można wstępnie wnioskować o przybliżonej wartości skradzionego mienia. Nie jest możliwe precyzyjne wyliczenie takiej wartości, ponieważ sama specyfika mienia o charakterze wirtualnym jest trudna do oszacowania. Dopiero wtedy organ procesowy może wszcząć postępowanie lub też odmówić jego wszczęcia, gdy zachodzą uzasadnione przesłanki procesowe w oparciu o art. 17 k.p.k.

Informacje w formie elektronicznej są istotnym elementem w systemie dowodów[20]. W sprawie o kradzież mienia z gier komputerowych znaczenie mają właśnie „dowody elektroniczne", które pozwolą ujawnić okoliczności czynu i wysunąć określone wnioski. Narzędziem w rękach organu procesowego mogą być opinie biegłych informatyków i możliwość dokonywania ustaleń faktycznych na podstawie tego rodzaju dowodów i ich prezentacji w postępowaniu sądowym[21]. Organ prowadzący postępowania może zwrócić się do administratora usługi gry internetowej, w której doszło do przestępstwa kradzieży o przekazanie materiału dowodowego na potrzeby śledztwa. Uzyskane w ten sposób dowody elektroniczne dostarczą informacji na temat rodzaju ataku na konto pokrzywdzonego, adresu, z jakiego dokonano nieautoryzowanego logowania i narzędzi, jakimi posłużył się przestępca. Administrator dostarcza również informacje o podjętych czynnościach po zgłoszeniu zaistniałego problemu przez pokrzywdzonego.

---

[19] R. Zawłocki, *Przestępstwa przeciw mieniu i gospodarcze*, Warszawa 2011, s. 68.

[20] T. Grzegorczyk, *Dowody w procesie karnym*, Warszawa 1998, s. 4, R. Kmiecik, *Prawo dowodowe*, Zakamycze 2005, s. 19; Z. Doda, A. Gaberle, *Dowody w procesie karnym*, Warszawa 1995, s. 23, A. Gaberle, *Dowody w sądowym procesie karnym*, Kraków 2007, s. 21, R. Kmiecik, *Prawo dowodowe zarys wykładu*, Warszawa 2008, s. 23, K. J. Pawelec, *Proces dowodzenia w postępowaniu karnym*, Warszawa 2010, s. 15.

[21] K. J. Pawelec, op. cit., s. 25.

Komputer jest urządzeniem teleinformatycznym będącym nośnikiem danych i konieczne jest zabezpieczenie komputera należącego do pokrzywdzonego na potrzeby śledztwa. Maszyna zapisuje w swojej pamięci wszelkie operacje przeprowadzone w systemie. Powołanie biegłego z zakresu informatyki, pozwoli ujawnić działanie programu trzeciego (wirusa) na komputerze należącym do pokrzywdzonego, a także wszelkie inne próby nieautoryzowanego wejścia osoby trzeciej (hakera) do systemu operacyjnego. Biegły sądowy może również sprawdzić legalność posiadanego oprogramowania na komputerze pokrzywdzonego. Może się więc zdarzyć tak, że w przypadku wykrycia pirackiej kopii programu na dysku twardym, pokrzywdzony stanie się również oskarżonym w innym już postępowaniu karnym. Opinia biegłego będzie jednoznacznym dowodem świadczącym o tym czy włamania dokonano poprzez komputer pokrzywdzonego czy wewnętrzne serwery administratora gry internetowej.

Ustalenie źródła incydentu da odpowiedź czy atak nastąpił z komputera znajdującego się na terenie Polski. Bardzo często zdarza się, że hakerami są mieszkańcy państw obcych. Specyficzne systemy prawa, obowiązujące w tych krajach mogą sprawić, iż ustalenie i ukaranie sprawcy będzie trudne, jeśli pochodzi on z np. w Chin, Brazylii, Rosji. Próba ściągnięcia podejrzanego dla potrzeb prowadzonego postępowania karnego musiałaby się wiązać z zastosowaniem ekstradycji obywatela obcego państwa. Sprawa będzie wyglądała inaczej, gdy okaże się, że włamanie nastąpiło w całości na terenie Polski. Sprawdzenie adresu IP da organom ścigania informacje na temat dokładnego położenia komputera, z jakiego dokonano włamania i jego domniemanego właściciela. Metoda taka jest, zatem bardzo skuteczna, ale tylko w przypadkach, gdy sprawca również jest obywatelem Polski. W momencie zatrzymania podejrzanego zabezpiecza się także materiał dowodowy pod postacią komputera, z którego dokonano włamania i wszelkich nośników danych znalezionych w miejscu zamieszkania i zatrzymania sprawcy czynu zabronionego. Analiza skonfiskowanego sprzętu komputerowego na potrzeby śledztwa dostarczy dowodów pod postacią zapisów elektronicznych. Dowody takie pozwolą określić dokładną datę i czas popełnienia przestępstwa, a także, jakimi narzędziami posłużył się podejrza-

ny. Należy mieć także na uwadze, że zabezpieczanie materiału dowodowego w pewnych sytuacjach może być utrudnione lub nawet niemożliwe. Sprawca może umyślnie zatrzeć ślady swojej działalności w pamięci komputera, znacząco utrudnić tym samym pracę organów śledczych. W przypadku zniszczenia fizycznego nośnika danych lub innego uszkodzenia mechanicznego takiego nośnika, odtworzenie historii procesów jakie zaszły w systemie może być niemożliwe.

Przestępstwa komputerowe różnią się w znacznym stopniu od przestępstw klasycznych. Dużym problemem dla współczesnych organów ścigania i współczesnej kryminalistyki jest zatrzymanie sprawcy przestępstwa internetowego, pochodzącego z obcego kraju. Wynika to z faktu, że sprawca przestępstwa nie musi być fizycznie na miejscu zbrodni, co utrudnia wykrycie i ściganie sprawcy. Haker, aby dokonać zaplanowanego czynu może wykorzystać w tym celu dowolne urządzenie teleinformatyczne przystosowane do tego by łączyć się z siecią internetową. Nie istnieją granice przestępstwa komputerowego, przez co powstaje szereg przeszkód formalnych, utrudniających ich ściganie z uwagi na różnorodność systemów prawnych oraz problemy wynikające z właściwości podmiotów uprawnionych do ścigania.

Bibliografia

1. Brzozowska M., *Ochrona danych osobowych w sieci*, Wrocław 2012.
2. Doda Z., Gaberle A., *Dowody w procesie karnym*, Warszawa 1995.
3. Dovey J., Kennedy H. W., *Kultura gier komputerowych*, Warszawa 2011.
4. Gaberle A., *Dowody w sądowym procesie karnym*, Kraków 2007.
5. Golat R., *Prawo Internetu dla praktyków*, Gdańsk 2009.
6. Grajewski J., *Prawo karne procesowe część ogólna*, Warszawa 2007.
7. Grzegorczyk T., *Dowody w procesie karnym*, Warszawa 1998.
8. Grzegorczyk T., Tylman J., *Polskie postępowanie karne*, Warszawa 2011.
9. http://www.fakt.pl/Ukradli-mi-szamanke-z-komputera-,artykuly,87579, 1.html, [15.06.2015].
10. http://www.polskieradio.pl/5/3/Artykul/505045,Policja-szuka-zlodzieja-statku-kosmicznego, [15.06.2015].
11. Kmiecik R., *Prawo dowodowe zarys wykładu*, Warszawa 2008.
12. Kmiecik R., *Prawo dowodowe*, Zakamycze 2005.
13. Krawaczyński P., Zelek D., *Rodzaje i klasyfikacja włamań oraz ataków internetowych*, http://www.hal.trzepak.net/faq/winxp/wlamania.htm, [15.06.2015].

14. Pawelec K. J., *Proces dowodzenia w postępowaniu karnym*, Warszawa 2010.
15. *Rosnąca popularność gier MMORPG*, Praca w biznesie komputerowym, http://praca.komputerowcy.info/2012/02/14/rosnaca-popularnosc-gier-mmorpg/, [14.02.1012].
16. Siwicki M., *Nielegalna i szkodliwa treść w Internecie*, Warszawa 2011.
17. Stefański R. A., *Prawo karne materialne część szczególna*, Warszawa 2009.
18. Świda Z., Ponikowski R., Posnow W., *Postępowanie karne część ogólna*, Warszawa 2008.
19. Urbańska-Galanciak D., *Homo players. Strategie odbioru gier komputerowych*, Warszawa 2010.
20. Waltoś S., *Proces karny zarys systemu*, Warszawa 2009.
21. Zawłocki R., *Przestępstwa przeciw mieniu i gospodarcze*, Warszawa 2011.