ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 797 STUDIA INFORMATICA NR 33 2013

Agnieszka Szewczyk*
Uniwersytet Szczeciński

PIRACTWO KOMPUTEROWE. ANALIZA ZJAWISKA W ŚWIETLE BADAŃ ANKIETOWYCH

Streszczenie

W artykule omówiono podstawowe problemy piractwa komputerowego, podając jego rodzaje, przykłady, występowanie oraz strategie antypirackie. Zawarto w nim również prezentację wyników badań ankietowych tego problemu.

Słowa kluczowe: piractwo komputerowe, przestępczość komputerowa

Wprowadzenie

Tematem niniejszego artykułu jest piractwo komputerowe, jako jedno z bardziej powszechnych przestępstw komputerowych, a w szczególności aspekty ekonomiczne tego procederu. Wraz z szybkim rozwojem techniki przestępstwa komputerowe rozpowszechniły się na ogromną skalę, stwarzając duże zagrożenie dla wielu dziedzin życia codziennego. W krajach wysoko rozwiniętych wraz z rozwojem informatyzacji dość szybko zaczęto zauważać zagrożenia dla społeczeństwa informacyjnego, jakie niesie ze sobą wzrost przestępczości komputerowej. Jednak wciąż jest na świecie wiele krajów, gdzie tego typu przestępczość traktowana jest marginalnie i nie są prowadzone żadne akcje, kampanie czy ustanawiane odpowiednie przepisy prawne mające na celu jej likwidację bądź przynajmniej ograniczenie. W ochronie systemów informatycznych ważną rolę odgrywają, oprócz odpowiednich przepisów prawnych, specjalne kampanie i działania techniczno-organizacyjne. Właściwe zabezpieczenie przestrzegania praw do własności intelektualnej stanowi jeden z priorytetowych celów rządów wielu krajów, jednak obecnie jego realizacja napotyka nadal na poważne przeszkody.

* aszew@wneiz.pl

Przestępstwa komputerowe definiowane są w literaturze przedmiotu w bardzo niejednoznaczny sposób. Wynika to z ich dużej różnorodności i złożoności, a także z faktu, że w polskim prawie nie ma odrębnej gałęzi dotyczącej wyłącznie informatyki.

Przestępstwa komputerowe stanowią dziś ogromne zagrożenie dla społeczeństwa informacyjnego, choć świadomość społeczna jest w tym temacie nadal niewielka, a temat – choć bardzo rozległy – przedstawia się zwykle w literaturze w sposób mało usystematyzowany. Stąd próba przedstawienia najważniejszych aspektów związanych z jednym z powszechniejszych przestępstw komputerowych – piractwem komputerowym.

Celem niniejszego artykułu jest znalezienie odpowiedzi na pytanie, w jaki sposób polscy producenci i dystrybutorzy oprogramowania radzą sobie z narastającą przestępczością komputerową, jaka jest ich świadomość i zainteresowanie tym tematem, jakie stosują zabezpieczenia przeciwko piractwu komputerowemu.

W celu uzyskania odpowiedzi między innymi na te pytania przeprowadzona została ankieta wśród producentów i dystrybutorów oprogramowania. Należy zwrócić uwagę, że jakkolwiek można przyjąć, że wykorzystana próba badawcza nie jest może reprezentatywna dla ogólnej liczby firm software'owych, to niewątpliwe pozwala na określenie i definicję pewnych prawidłowości związanych z piractwem komputerowym w naszym kraju.

1. Piractwo komputerowe i jego formy

Piractwo to kopiowanie, reprodukowanie, używanie i wytwarzanie bez zezwolenia produktu chronionego przez prawo autorskie. Często ma wiele wspólnego z crackerstwem, które w tym ujęciu oznacza wszelkie czynności dokonywane w celu złamania zabezpieczeń programów bądź ich usunięcia, tworzenie programów generujących kody seryjne, usuwanie zabezpieczeń wyłączających pewne opcje lub ograniczające czasowo funkcjonalność programu itp. Znaczna część programów komputerowych posiada zabezpieczenia uniemożliwiające ich kopiowanie. Dopiero złamanie takiego zabezpieczenia umożliwia wykonywanie kolejnych kopii programu. Piractwo komputerowe jest charakterystycznym rodzajem kradzieży. Odpowiedzialność za tego typu czyn przewiduje art. 278 § l Kodeksu karnego, który mówi, że: „Kto zabiera w celu przywłaszczenia cudzą rzecz ruchomą, podlega karze pozbawienia wolności od 3 miesięcy do 5 lat". A w odniesieniu do programu komputerowego w § 2 tegoż artykułu Stwierdza się, że: „Tej samej

karze podlega, kto bez zgody osoby uprawnionej uzyskuje cudzy program komputerowy w celu osiągnięcia korzyści majątkowej". Wyjaśnienia wymaga pojęcie programu komputerowego. Zgodnie z definicją podaną przez K. Golat i R. Golat jest to: „logicznie uporządkowany ciąg instrukcji, przeznaczony do uzyskania za pośrednictwem sprzętu komputerowego pożądanego przez użytkownika systemu informatycznego wyniku, który w wielu wypadkach sprowadza się do otrzymania poszukiwanej informacji" (Golat i Golat, 2010, s. 20–30). Ochronie podlega każdy program komputerowy bez względu na wartość, przeznaczenie i formę wyrażenia. Uzyskanie programu komputerowego oznacza skopiowanie programu. Nie ma znaczenia, z jakiego źródła jest kopiowany i na jaki nośnik. Skopiowanie do pamięci RAM również jest uzyskaniem w rozumieniu tego przepisu.

Istotne jest jednak uzyskanie korzyści majątkowej. Korzyścią majątkową w przypadku kopiowania i sprzedaży „pirackiego" oprogramowania jest uzyskanie zysku z jego zbycia. W niektórych interpretacjach tego przepisu można spotkać stwierdzenie, że korzyścią majątkową jest także to, że osoba kopiująca program w nielegalny sposób nie płaci za niego. Warto jednak wspomnieć, że również nabywca nielegalnego oprogramowania ponosi odpowiedzialność karną jako nabywca kradzionej rzeczy na mocy art. 293 kk., w którym określone zostało, iż przepisy dotyczące umyślnego i nieumyślnego paserstwa stosuje się odpowiednio do programów komputerowych. Należy wspomnieć, że muzyka zapisana w formacie .wav lub .mp3 nie jest programem komputerowym i nie stosuje się do niej przepisów wymienionych powyżej. Utwory te pozostają jednak pod ochroną cytowanej ustawy, bowiem art. 117 ust. 1 Ustawy o prawie autorskim, mówi: „Kto bez uprawnienia albo wbrew jego warunkom, w celu rozpowszechnienia, utrwala lub zwielokrotnia cudzy utwór w wersji oryginalnej lub w postaci opracowania, artystyczne wykonanie, fonogram, wideogram lub nadanie". Wydaje się, że artykuł 278 k.k. uchyla stosowanie art. 117 w stosunku do programów komputerowych, natomiast art. 117 stosuje się w wypadku bezprawnego zwielokrotniania utworów muzycznych i filmowych (.wav, .mp3, .ayi).

Przeciętnie szacuje się, że z każdej używanej legalnej kopii oprogramowania dla komputerów PC wykonywana jest przynajmniej jedna kopia nielegalna. W niektórych krajach z każdej używanej legalnej kopii oprogramowania wykonywanych jest do 99 nielegalnych kopii. Piractwo komputerowe uderza w przemysł komputerowy, a w efekcie w końcowego użytkownika. Dotyka boleśnie wszystkich producentów i dystrybutorów oprogramowania, ale wpływa też na zwiększenie cen programów, niższy poziom wsparcia i opóźnienia w powstawaniu nowych

produktów, co wpływa na obniżenie ogólnego wyboru i jakości oprogramowania. Producenci oprogramowania przeznaczają całe lata na tworzenie oprogramowania przeznaczonego do publicznego użytku. Kupując pirackie oprogramowanie, powoduje się, że pieniądze zamiast do twórców, trafiają do przestępców, w związku z tym nie mogą być przeznaczone na prace rozwojowo-badawcze i tworzenie nowych, lepszych wersji oprogramowania. Piractwo komputerowe powoduje również straty ekonomiczne na skalę lokalną i globalną. Zmniejszenie z powodu piractwa sprzedaży legalnej wpływa na zmniejszenie zatrudnienia i straty finansowe nie tylko producentów czy dystrybutorów oprogramowania, ale także budżetu państwa, ponieważ powoduje utratę dochodu z podatków. Piractwo komputerowe niejednokrotnie uniemożliwia rozwój lokalnych firm produkujących oprogramowanie, ponieważ część z nich nie będzie w stanie zrekompensować kosztów wytworzenia oprogramowania, gdy wskaźnik piractwa i straty własne są zbyt wysokie, w związku z tym niemożliwe jest kontynuowanie prac rozwojowych i firma wycofuje się z rynku, co wiąże się także ze stratą dla użytkowników (Wójcik, 2008).

Według firmy Uplook: „Piractwo komputerowe przyjmuje najróżniejsze formy. Może polegać na instalowaniu w sieci lub na komputerze nielicencjonowanej kopii programu, instalowaniu danego programu na większej liczbie komputerów, niż przewiduje to licencja na program, kopiowanie programu z nośnika na nośnik, kopiowanie programu z internetu i wiele innych. Zabronione jest kopiowanie programu bez zgody producenta, dystrybucja nielegalnych kopii, jak również używanie nielegalnych kopii" (www.aplusc-systems.com/).

Istnieje pięć podstawowych form piractwa komputerowego (Golat, 2010, s. 20–30):

1. Wykonywanie dodatkowych kopii – ta forma piractwa występuje, gdy w obrębie firmy wykonywane są dodatkowe kopie programu do użytku na innych stanowiskach komputerowych. Do tej kategorii zalicza się również wymianę nośników z oprogramowaniem pomiędzy pracownikami firmy.
2. Instalacja na twardym dysku – niektóre firmy komputerowe, sprzedając zestawy komputerowe, instalują na dysku system operacyjny i inne nielegalne kopie oprogramowania, aby być bardziej atrakcyjnymi dla klientów.
3. Fałszowanie – powielanie i sprzedaż nielegalnych kopii oprogramowania chronionego przez prawo autorskie, czasami stwarzającego pozory legalnego, a czasem widocznie nielegalnego, np. zapakowanego w folię z ręcznie opisana etykietą.
4. Piractwo przez BBS – jest to wczytywanie oprogramowania chronionego prawami autorskimi przez użytkowników dołączonego poprzez modem do BBS-u.

Piractwa komputerowego dokonywanego poprzez BBS nie należy mylić z wykorzystywaniem oprogramowania *public domain* lub *shareware*. *Shareware* jest oprogramowaniem, które może być chronione prawami autorskimi lub nie, dostrzegalna jest jednak wyraźna chęć właściciela praw autorskich – twórcy, aby oprogramowanie było ogólnie dostępne, powielane i kopiowane i aby masowo z niego korzystano. Firma Microsoft nie produkuje żadnego oprogramowania typu *shareware* przeznaczonego do dystrybucji lub używania przez BBS. Wszelkie oprogramowanie Microsoftu oferowane bez zezwolenia przez BBS należy uważać za nielegalne.

5. Wypożyczenie oprogramowania – ma miejsce wówczas, gdy program znajdujący się na legalnym nośniku zostaje udostępniony użytkownikom, którzy kopiują go na swój twardy dysk, a następnie zwracają udostępniony nośnik z legalną kopią wypożyczającemu. Można wyróżnić trzy rodzaje piractwa polegającego na „wypożyczaniu" oprogramowania: produkt zostaje „wypożyczony" ze sklepu komputerowego w celu zainstalowania na domowym lub biurowym komputerze wypożyczającego; produkt zostaje wypożyczony za pośrednictwem „klubu" wysyłkowego; produkt zostaje zainstalowany na komputerach, które zostają wypożyczone kolejnemu użytkownikowi. W niektórych przypadkach Microsoft zezwala danej firmie na wypożyczanie lub wynajmowanie komputerów, na których są zainstalowane produkty firmy Microsoft. W takich przypadkach wymaga się, aby firma ta, w ramach umowy wynajmu lub dzierżawy, uzyskała zgodę „wypożyczającego" na przestrzeganie warunków umowy licencyjnej dla użytkownika ostatecznego na używanie oprogramowania firmy Microsoft. Szczególny przypadek użytkowania niezgodnego z przeznaczeniem zachodzi w sprzedaży detalicznej – w sklepach komputerowych prowadzona jest dystrybucja produktów będących jedynie uaktualnieniami pełnych wersji programów lub produktów rozprowadzanych w sieci hurtowej po cenach promocyjnych.

Microsoft nie uznaje żadnej formy naruszenia opracowanej umowy licencyjnej, niezależnie od sposobu naruszenia, i podejmuje różne środki, aby uniemożliwić jej naruszanie. Firma ta zazwyczaj udziela licencji większości OEM (Original Equipment Manufacturer) na fabryczne instalowanie swoich produktów systemowych bezpośrednio na dyskach twardych sprzedawanych komputerów. W niektórych przypadkach OEM otrzymuje licencję na fabryczne instalowanie na dysku twardym pewnych programów użytkowych. Jeśli chodzi o produkty systemowe, OEM musi dołączyć do produktu umowę licencyjną Microsoftu, kar-

tę rejestracyjną Microsoftu i certyfikat autentyczności, często także podręcznik użytkownika i zestaw dyskietek, natomiast do programów użytkowych musi być dołączona umowa licencyjna i karta rejestracyjna Microsoftu. Istnieją przesłanki sugerujące nielegalność produktów dostępnych w sprzedaży sklepowej lub zainstalowanych na dysku twardym w chwili zakupu zestawu komputerowego. Taką przesłanką może być sytuacja, kiedy Microsoft udziela licencji na sprzedaż swoich produktów wraz z zestawem komputerowym, jednak często zdarza się, że takie produkty są sprzedawane bez komputera, co jest niezgodne z licencją i prawem. Produkty Microsoftu sprzedawane w sklepach komputerowych są produkowane wyłącznie przez firmę Microsoft, w związku z tym nie mogą nosić oznaczeń handlowych żadnych innych firm, nie powinny też umieszczać na przedniej okładce podręcznika użytkownika napisu „Tylko do sprzedaży z nowym komputerem" lub „Tylko do dystrybucji z nowym komputerem" (Jakubowski, 2011).

Ważnymi przesłankami świadczącymi o nielegalności sprzedawanego produktu mogą być:

– brak umowy licencyjnej,
– brak karty rejestracyjnej produktu,
– brak certyfikatu autentyczności dla odpowiednich produktów systemowych towarzyszących nowemu komputerowi,
– brak podręcznika użytkownika, zapasowych dyskietek, karty rejestracyjnej, certyfikatu autentyczności zawierającego antypiracki hologram dla produktów systemowych zainstalowanych w komputerze, które są dostarczane w opakowanej postaci razem z komputerem. Produkty systemowe dostarczane w opakowaniu muszą zawierać wszystkie te elementy,
– wszelkie inne przesłanki świadczące o nielegalności dyskietek, np. ręcznie opisane etykiety dyskietek,
– niemożność uzyskania od sprzedawcy podręcznika użytkownika do programów zainstalowanych w komputerze bądź propozycja nabycia tego podręcznika z innego źródła,
– uzyskanie od sprzedającego kserokopii podręcznika użytkownika lub podręcznika niezapakowanego w folię – często podręcznika o obniżonej jakości,
– brak nośników z oprogramowaniem w sytuacji, kiedy oprogramowanie jest zainstalowane w komputerze bądź propozycja zainstalowania takiego oprogramowania za darmo lub po niższym koszcie,
– brak wyraźnych zabezpieczeń, takich jak hologram na uaktualnieniach (*upgrade*) systemów operacyjnych dostępnych w sprzedaży detalicznej, napis „tyl-

ko do sprzedaży z nowym komputerem" lub „tylko do dystrybucji z nowym komputerem" umieszczony na przedniej okładce podręcznika użytkownika produktu systemowego nabytego w sprzedaży detalicznej bez nabycia nowego komputera (http://spkif.w.interia.pl/1prawo.html).

2. Strategie ochrony przed piractwem komputerowym

W ostatnich miesiącach obserwuje się znaczący wzrost zainteresowania sprawą legalności oprogramowania komputerowego. Świadczy o tym wiele publikacji prasowych, relacje radiowe i telewizyjne oraz ogromna liczba pytań adresowanych do producentów oprogramowania oraz do Business Software Aliance (BSA). Pytania w dużym stopniu dotyczą kwestii weryfikacji legalności oprogramowania w firmach. W przypadku firm dysponujących niewielką liczbą zestawów komputerowych nie stanowi to wielkiego problemu, jednak w firmach o rozbudowanej sieci komputerowej rzędu kilkudziesięciu i więcej komputerów rozmieszczonych często w różnych budynkach taka weryfikacja nastręcza poważnych trudności, z którymi firmy często nie są w stanie poradzić sobie o własnych siłach. W Internecie można znaleźć specjalne oprogramowanie wspomagające ten proces, jednak nie zawsze jest ono wystarczające i niekiedy nie spełnia pokładanych w nim nadziei. W takiej sytuacji rozwiązaniem jest zwrócenie się do jednej z firm zajmujących się audytem sprzętu i oprogramowania komputerowego. Ich usługi przyniosą wymierne efekty w postaci kompleksowej inwentaryzacji sprzętu i oprogramowania. Oprócz weryfikacji i wskazania najkorzystniejszych sposobów osiągnięcia pełnej legalności oprogramowania firma zlecająca uzyskuje:

– kompletny spis wszystkich aplikacji zainstalowanych zarówno na serwerze, jak i końcówkach klienckich uwzględniający numery wersji, kompletność instalacji, zmienione nazwy plików i pliki skompresowane,
– dokładne określenie konfiguracji sprzętowej wszystkich komputerów PC,
– wykrycie i usunięcie wirusów,
– wykrycie i usunięcie niepożądanych plików, aplikacji *etc*.

Korzyści płynące z takiego raportu są ogromne, umożliwia on bowiem efektywne zarządzanie posiadanymi zasobami. Pomaga zaplanować wydatki na informatykę w firmie, ponieważ wskazuje na realne potrzeby w zakresie sprzętu i oprogramowania. Efektem jest optymalizacja niezbędnych inwestycji związana z redukcją kosztów (Znierzchowski, 2010).

Raport jest przydatny także w przypadku kontroli ze strony organów podatkowych – środki trwałe, jakimi są sprzęt i oprogramowanie, zestawione są wówczas zgodnie ze stanem faktycznym. Istotny jest także fakt, iż w przypadku wykrycia nielegalnego oprogramowania przez firmę audytującą firma zlecająca wykonanie audytu nie ponosi natychmiastowych konsekwencji – zleceniodawca może liczyć na 60-dniowy okres na legalizację oprogramowania (dotyczy wyłącznie oprogramowania Microsoft) przy równoczesnym zobowiązaniu firmy audytującej do zachowania pełnej tajemnicy (dotyczy wyłącznie audytów prowadzonych przez firmy posiadające certyfikat Microsoft Audit Partner).

Jak już wspomniano powyżej, audyt oprogramowania dostarcza informacji na temat wszystkich aplikacji obecnych na każdym z komputerów znajdujących się w firmie. Dzięki temu można dowiedzieć się:
– ile aplikacji pracuje na stacjach roboczych,
– jakie aplikacje są obecne na stacjach roboczych,
– czy komputery służą pracownikom jedynie do pracy,
– czy są obecne programy niepotrzebne, niepożądane (tzn. stare i nieużywane wersje programów, wirusy).

Dodatkowym efektem audytu jest zwolnienie miejsca na dyskach i zwiększenie szybkości działania komputerów poprzez usunięcie niepotrzebnych danych i aplikacji. Przeprowadzenie audytu polega na uruchomieniu na każdym komputerze specjalnej aplikacji skanującej, która zbiera informacje o plikach przechowywanych na dyskach twardych. Wynikiem takiego skanowania jest lista wszystkich aplikacji zainstalowanych na jednostkach roboczych. Firmy audytujące proponują:
– ograniczenie audytu do zeskanowania jednostek w poszukiwaniu zainstalowanych aplikacji,
– rozszerzenie audytu o aspekt legalności, czyli przeprowadzenie dla całego oprogramowania audytu legalności.

W każdej firmie może zdarzyć się, że w komputerach będą pojawiać się aplikacje instalowane przez pracowników, o których nie wiedzą przełożeni. Osoby odpowiedzialne za oprogramowanie w firmie powinny mieć pełną kontrolę nad danymi przechowanymi w sieci firmy. Przydatne jest więc regularne przeprowadzanie audytu oprogramowania. Podsumowując – audyt oprogramowania jest nieocenioną pomocą dla firm, które chcą mieć pełną kontrolę nad zainstalowanym oprogramowaniem. Dostarcza on nie tylko informacji na temat zgromadzonych przez firmę programów, ale również pozwala na usprawnienie działania kompute-

rów, przyspieszenie ich pracy, a także wykrycie i usunięcie wszelkich niepożądanych danych, aplikacji czy wirusów.

Audyt legalności dostarcza także informacji na temat zainstalowanego oprogramowania, na które firma nie posiada licencji, ma ich zbyt mało lub też za dużo. Firmy audytujące doradzają dodatkowo w zakresie optymalnego technologicznie i kosztowo uzupełnienia brakujących licencji. Audyt legalności polega na dokładnym sprawdzeniu, czy firma jest uprawniona do korzystania z zainstalowanego oprogramowania pod względem prawnym. W celu przeprowadzenia audytu legalności, oprócz skanowania powierzchni dysków twardych za pomocą specjalnych programów, niezbędne jest też zgromadzenie wszystkich licencji na oprogramowanie znajdujących się w firmie. Zestawienie posiadanych licencji z liczbą i rodzajem zainstalowanych programów pozwala na określenie stanu legalnego oprogramowania w firmie oraz na wykrycie braków w licencjach. W praktyce żadna firma nie może być pewna tego, że korzysta jedynie z licencjonowanego oprogramowania. Wynika to z faktu, iż wielu pracowników samowolnie instaluje nielicencjonowane aplikacje, często nawet w sytuacjach, kiedy firma stosuje zabezpieczenia w celu uniknięcia instalacji aplikacji przez pracowników. Audyt legalności jest praktycznie jedynym sposobem na uzyskanie tej pewności i doskonałym sposobem zapewnienia firmie statusu legalności. Firmy, w których nastąpi pozytywna weryfikacja posiadanego oprogramowania, a także te, które uzupełnią braki w licencjach w ciągu wskazanego czasu, otrzymają wystawiony przez Microsoft Certyfikat License Management Program. Ponadto analiza informacji audytowych umożliwia przygotowanie optymalnych planów zakupów oprogramowania w przyszłości i lepsze zarządzanie oprogramowaniem.

Już 10 lat temu stowarzyszenia producentów fonograficznych w Australii, Kanadzie, Danii oraz w Niemczech rozpoczęły stosowanie nowej inicjatywy przemysłu fonograficznego w walce z nielegalną wymianą plików: kampanię informacyjną skierowaną do użytkowników sieci *peer-to-peer* (P2P) rozpowszechniających muzykę bez zgody posiadaczy praw do poszczególnych utworów.

Listy rozsyłane są bezpośrednio do osób korzystających z programów P2P za pomocą funkcji *Instant Messaging*, dostępnej w systemach wymiany plików, takich jak Kazaa, Grokster, Direct Connect i wielu innych. Wiadomości zawierają informację, iż rozpowszechnianie muzyki w Internecie bez zgody uprawnionych podmiotów stanowi naruszenie prawa. Podkreślają również, że nieautoryzowana wymiana plików to działanie na szkodę nie tylko wykonawców, autorów tekstów

i wytwórni fonograficznych, ale również wszystkich innych osób związanych z tworzeniem muzyki.

Ta inicjatywa jest najnowszym projektem kampanii informującej o zagrożeniach wynikających z rozpowszechniania nieautoryzowanych plików muzycznych w sieciach komputerowych – w ramach tej kampanii w ponad 20 krajach wysłano broszury do tysięcy firm, instytucji państwowych i ośrodków akademickich. International Federation of the Phonographic Industry (IFPI) wraz z organizacjami reprezentującymi autorów, sprzedawców i muzyków utworzyło stronę www.pro-muzic.org, pierwsze i najbardziej wyczerpujące źródło informacji na temat legalnej muzyki na świecie.

Kampanie polegające na walce z piractwem w Internecie przeprowadza też od lat amerykańskie stowarzyszenie Recording Industry Association of America (RIAA). Zamierza ono zlikwidować albo przynajmniej w dużym stopniu ograniczyć ten proceder, w tym celu przeprowadziło już szereg działań o różnym stopniu skuteczności, z których najbardziej znaczące były liczne procesy sądowe wytaczane serwisom bezpośredniej wymiany plików. Sposób ten był jednak mało skuteczny – na miejscu jednego zlikwidowanego serwisu P2P pojawiały się trzy nowe. Jednym z pomysłów RIAA było wprowadzanie do sieci P2P m.in. podróbek piosenek, plików niekompletnych, zmieszanych z innymi, szybko jednak zaczęto sobie radzić z tego typu plikami, a sam pomysł również nie przyniósł oczekiwanych rezultatów. Kolejnym sposobem miały być indywidualne pozwy sądowe przeciw użytkownikom, którzy kopiują lub udostępniają szczególnie dużo plików. Ograniczyło to w dużym stopniu liczbę użytkowników sieci P2P, jednak tylko w Stanach Zjednoczonych. Inny pomysł RIAA może okazać się jednak bardziej skuteczny. Z danych przedstawionych przez stowarzyszenie wynika, że zdecydowana większość najaktywniejszych piratów kopiuje pliki w pracy, korzystając z firmowego sprzętu. Dlatego też nowa kampania RIAA ma polegać na uświadamianiu właścicieli firm w tym temacie. Kilka miesięcy temu odbył się nawet proces pokazowy – niewielka amerykańska firma, której pracownicy kopiowali nielegalne pliki, zmuszona została do wypłacenia RIAA miliona dolarów odszkodowania. Sposobem na ograniczenie tego typu działań mogą być specjalne filtry, uniemożliwiające pracownikom korzystanie z sieci P2P – koszt ich zainstalowania nieporównywalnie niższy w stosunku do kary, jaka może grozić firmie w procesie o odszkodowanie. Apel o zastosowanie takiego rozwiązania RIAA rozesłało do tysiąca największych amerykańskich firm (www.winter.pl/internet/w0830.html).

Amerykańskie Federalne Biuro Śledcze poinformowało o swojej gotowości do włączenia się w walkę z nielegalnym kopiowaniem muzyki, filmów i oprogramowania. Jednym z przejawów i elementów owej walki ma być umieszczenie na sprzedawanych w USA płytach CD i DVD specjalnych etykiet ostrzegających przed konsekwencjami nielegalnego kopiowania zapisanych na nośnikach materiałów. Federalne Biuro Śledcze zamierza współpracować z licznymi organizacjami czynnie zaangażowanymi w walkę z piractwem na świecie, takimi jak Motion Picture Association of America (MPAA), RIAA oraz Entertainment Software Association (ESA (). W ramach kampanii informacyjnej na sprzedawanych w USA płytach DVD i CD z muzyką, filmami, grami i oprogramowaniem umieszczony zostanie tekst, informujący, że nielegalne kopiowanie i dystrybuowanie zapisanych na nośnikach materiałów jest przestępstwem zagrożonym karą do 5 lat więzienia lub 250 tys. USD grzywny – nawet, jeżeli użytkownik nie czerpie korzyści majątkowej z tego procederu. FBI planuje również intensywniejsze niż do tej pory ściganie piratów, a także opracowanie nowej technologii zabezpieczania płyt (www.intemetstandard.com.pl/news/63974.html).

Podczas targów Consumer Electronics Show (CES) w styczniu 2003 roku odbywały się cykliczne spotkania poświęcone problemowi piractwa. Do walki z internetowym piractwem filmowym i muzycznym przyłączyli się też najbardziej zainteresowani, czyli artyści tacy jak: Sheryl Crow, The Edge, Ben Affleck, Alicia Keys oraz Dr. Dre. Podczas spotkania odbyła się także prezentacja projektu nowego odtwarzacza audio firmy HP, zbudowanego w oparciu o iPoda Apple'a. Artyści pojawili się podczas wystąpienia Carly Fioriny, szefowej koncernu Hewlett-Packard (HP), który, jak mieliśmy okazję się dowiedzieć, zamierza instalować w swoich produktach zabezpieczenia antypirackie. HP zamierza również instalować w swoich komputerach oprogramowanie iTunes Musie Storę Apple'a (umożliwiające korzystanie z internetowego serwisu muzycznego o tej samej nazwie). Muzyka oferowana przez iTunes jest w odpowiedni sposób zabezpieczona przed nielegalnym kopiowaniem. Odtwarzacze, które wprowadzi na rynek HP, podobnie jak iPod posiadać będą wbudowane twarde dyski – w najprostszym modelu dysk będzie miał 20 GB pojemności. Cenę takiego urządzenia ustalono na 399 USD. Podczas pokazu artyści tłumaczyli zgromadzonym, jakie są skutki piractwa i jak wpływa ono na rynek muzyczny. Zdaniem Jimmy'ego Iovine'a, prezesa wytwórni Interscope, największym problemem, związanym z piractwem jest niska świadomość społeczna w tym temacie i fakt, że większość użytkowników nie widzi nic złego w nielegalnym kopiowaniu muzyki czy filmów. Koalicja MUSIC (*Musie United for Strong Internet Copy-*

right), do której przystąpili tacy artyści, jak Madonna, Elton John, Eminem, Sting i Britney Spears, rozpoczęła szeroką kampanię edukacyjną mającą na celu głównie zwalczanie masowej kradzieży muzyki w Internecie. Kampanię tę rozpoczęto już stosunkowo dawno. W dwóch najważniejszych dziennikach amerykańskich „The New York Times" i „The Los Angeles Times" pojawiły się całostronicowe ogłoszenia, w których zadaje się pytanie: „Kogo naprawdę obchodzi nielegalne ściąganie muzyki z „Internetu?" Kolejnym krokiem kampanii mają być spoty telewizyjne i radiowe, w których najpopularniejsi artyści będą uświadamiać fanów, że nielegalne pobieranie plików jest porównywalne do kradzieży płyty ze sklepu. Podobne treści znaleźć będzie można na stronie www.musicunited.org. Szacuje się, że dziennie ściąganych jest nielegalnie z Internetu ponad 2,6 mld plików z muzyką – głównie poprzez serwisy P2P, takie jak KaZaA, Morpheus czy Gnutella. Do koalicji MUSIC przystąpiły liczne organizacje, takie jak: Alliance of Artists and Recording Companies, Association For Independent Musie, American Federation of Musicians, American Federation of Television and Radio Artists, ASCAP, BMI, Country Musie Association, Christian Musie Trade Association, Gospel Musie Association, Hip Hop Summit Action Network, Jazz Alliance International, Musie Managers Forum-USA, Nashville Songwriters Association International, National Academy of Recording Arts and Sciences, Recording Industry Association of America, Recording Industries Musie Performance Trust Funds, SESAC, SoundExchange, Tennessee Songwriters Association International, and The Songwriters Guild of America.

3. Prezentacja wyników badań ankietowych dotyczących zjawiska piractwa komputerowego

Zaprezentowane poniżej badanie ankietowe jest badaniem fakultatywnym. Charakteryzuje się dobrowolnością udzielania odpowiedzi na pytania, za pomocą których prowadzi się rozpoznanie interesującej nas dziedziny. W trakcie tego badania skierowano do wybranej kategorii firm odpowiedni zestaw pytań, przy czym nie narzucono im obowiązku odpowiedzi. Wobec tego uzyskano odpowiedzi tylko od tych firm, które zechciały i były w stanie ich udzielić w sposób dostatecznie precyzyjny.

W trakcie ustalania badanej zbiorowości stwierdzono również, że większość firm odmawia wypełnienia ankiety, a firmy, które ostatecznie zgodziły się wziąć udział w badaniu, zrobiły to pod warunkiem zachowania anonimowości zgodnie z Ustawą o ochronie danych osobowych.

Kontakt z firmami wytypowanymi drogą losowania został nawiązany drogą elektroniczną. Na 150 firm wytypowanych drogą losowania w badaniu zgodziło się wziąć udział 45. Zastrzegły sobie one jednak całkowitą anonimowość.

Ankieta została przeprowadzona w elektronicznej formie pisemnej (przeprowadziła ją studentka Uniwersytetu Szczecińskiego Magdalena Roesler). Zastosowano w niej różne możliwości odpowiedzi na postawione pytania:
– system odpowiedzi: „tak" bądź „nie",
– uzupełnienie brakujących odpowiedzi,
– wariantowy zbiór odpowiedzi.

Pytania do ankiety zostały przedstawione w załączniku 1.

W badaniu wzięły udział firmy różnej wielkości, zarówno małe firmy jednoosobowe, jak i duże przedsiębiorstwa, zatrudniające wielu pracowników. Większość firm, które zgodziły się na udział w badaniu, ma swoją siedzibę w województwie mazowieckim (18 firm) i małopolskim (13 firm). W badaniu wzięły udział także firmy z województwa zachodniopomorskiego (8 firm), śląskiego (4 firmy) oraz pomorskiego (2 firmy). Zostało to przedstawione w tabeli 1.

Tabela 1

Terytorialny rozkład respondentów badania ankietowego

Województwo	Liczba firm, które wzięły udział w badaniu ankietowym
Mazowieckie	18
Małopolskie	13
Zachodniopomorskie	8
Śląskie	4
Pomorskie	2
Razem	45

Źródło: opracowanie własne.

Znakomita większość firm, które zgodziły się wziąć udział w badaniu, to firmy jednoosobowe (60%) lub zatrudniające niewielu pracowników: od 2 do 5 – 13%, i od 5 do 10 – 15,5% ogólnej liczby firm biorących udział w badaniu. Właściciele dużych przedsiębiorstw monitowani o wzięcie udziału w badaniu najczęściej odmawiali, niewiele z nich zgodziło się na wypełnienie ankiety, najczęściej dopiero po wielokrotnym zapewnianiu o anonimowości. Może to świadczyć o tym, że duże firmy, ponosząc ogromne straty spowodowane piractwem kompute-

rowym, mogą niechętnie ujawniać związane z tym dane. Jednym z powodów, który nasuwa się w tej sytuacji, jest obawa producentów i dystrybutorów oprogramowania przed zwróceniem uwagi piratów na łatwość pokonania zabezpieczeń stosowanych przez firmę, o czym pośrednio mogą świadczyć duże straty poniesione przez te firmy. W tabeli 2 zawarto rozkład odpowiedzi na pierwsze pytanie ankiety.

Tabela 2

Liczba pracowników zatrudnionych przez firmę

Ilu pracowników zatrudnia Państwa firma	Liczba udzielonych odpowiedzi	Procent ogólnej liczby odpowiedzi
Firma jednoosobowa	27	60,0
2–5	6	13,0
5–10	7	15,5
1 –20	3	7,0
Powyżej 20	2	4,5

Źródło: opracowanie własne.

Drugie pytanie ankiety dotyczyło rocznych obrotów generowanych przez firmę. Chodziło o to, aby uzyskać obraz, jakiego rodzaju firmy zgodziły się na wzięcie udziału w badaniu. Odpowiedzi, które przeważały, potwierdzają informacje uzyskane na podstawie pytania pierwszego – znakomita część firm biorących udział w badaniu to firmy małe. Obrót poniżej 50 tys. PLN deklaruje 50% firm biorących udział w badaniu. Dużą część stanowią także firmy generujące rocznie obrót w granicach 50–100 tys. PLN (26,5%) oraz w granicach 100–500 tys. PLN (24,5%). W tabeli 3 przedstawiono rozkład odpowiedzi na drugie pytanie ankiety.

Tabela 3

Wielkość obrotów generowanych przez firmę

Jakiego rzędu obroty generuje firma rocznie (PLN)	Liczba udzielonych odpowiedzi	Procent ogólnej liczby odpowiedzi
Poniżej 50 tys.	18	40,0
50–100 tys.	12	26,5
100–500 tys.	11	24,5
500 tys.–1 mln	4	9,0
Powyżej 1 mln	0	0,0

Źródło: opracowanie własne.

Kolejne pytanie ankiety dotyczyło obszaru działalności firmy. Na rynku lokalnym działa 67% firm biorących udział w badaniu. Mniej, bo tylko 27% firm, jako obszar działalności wskazuje całą Polskę, natomiast tylko trzy firmy (6%) biorące udział w ankiecie, to firmy międzynarodowe. W tabeli 4 zestawiono odpowiedzi na trzecie pytanie ankiety.

Tabela 4

Obszar działalności firmy

Obszar działalności firmy	Liczba udzielonych odpowiedzi	Procent ogólnej liczby odpowiedzi
Rynek lokalny	30	67
Rynek ogólnopolski	12	27
Rynek międzynarodowy	3	6

Źródło: opracowanie własne.

Większość firm biorących udział w badaniu jest zarówno producentami, jak i dystrybutorami oprogramowania (58%). Firmy będące tylko producentami stanowią 18% wszystkich badanych firm, natomiast te, które są tylko dystrybutorami – 24%. W tabeli 5 zawarto rozkład odpowiedzi na czwarte pytanie ankiety.

Tabela 5

Profil działalności firmy

Firma jest	Liczba udzielonych odpowiedzi	Procent ogólnej liczby odpowiedzi
Tylko producentem	8	18
Tylko dystrybutorem	11	24
Producentem i dystrybutorem	26	58

Źródło: opracowanie własne.

Firmy biorące udział w badaniu w większości są producentami/dystrybutorami oprogramowania specjalistycznego, ściśle dedykowanego określonej grupie odbiorców. Ten wariant odpowiedzi zaznaczyło aż 60% respondentów. Spora część firm (22%) produkuje/dystrybuuje także oprogramowanie użytkowe, przeznaczone dla szerokiego grona odbiorców. Wśród respondentów znalazły się także 3 firmy (7%) zajmujące się oprogramowaniem użytkowym, 4 takie (9%),

które deklarują produkcję/dystrybucję kilku z wymienionych powyżej rodzajów oprogramowania, a także jedna firma, zajmująca się produkcją bądź dystrybucją wyłącznie oprogramowania dodatkowego (wspomagającego). W tabeli 6 przedstawiono odpowiedzi na piąte pytanie ankiety.

Tabela 6

Rodzaje oprogramowania produkowanego/dystrybuowanego przez firmę

Jakiego rodzaju oprogramowanie produkuje/dystrybuuje firma	Liczba udzielonych odpowiedzi	Procent ogólnej liczby odpowiedzi
Specjalistyczne, ściśle dedykowane określonej grupie odbiorców	27	60
Użytkowe, dla szerokiego grona odbiorców (powszechnego użytku)	10	22
Rozrywkowe	3	7
Dodatkowe (wspomagające, np. wtyczki, plug-iny do innych programów)	1	2
Kilka z wymienionych powyżej	4	9
Inne	0	0

Źródło: opracowanie własne.

Znaczna większość firm, biorących udział w badaniu, deklaruje prowadzenie wielu form sprzedaży produktów. Stanowią one 67% wszystkich respondentów. Tylko 6 firm (13%) zadeklarowało sprzedaż wyłącznie przez sieć dystrybutorów, a 4 (9%) jedynie drogą pocztową. Dwie firmy (4.5%) prowadzą sprzedaż tylko przez Internet, także dwie prowadzą sprzedaż wiązaną, dołączając swój produkt do innych sprzedawanych produktów, np. czasopism. Tylko jedna z badanych firm prowadzi wyłącznie sprzedaż osobistą w siedzibie firmy. W tabeli 7 zawarto rozkład odpowiedzi na szóste pytanie ankiety.

Podobnie jak powyżej sytuacja przedstawia się, jeśli chodzi o formy płatności akceptowalne przez firmę – tu również większość firm (60%) dopuszcza wiele form płatności. Spora część firm (24%) zadeklarowała też, że jedyną dopuszczalną formą płatności za ich produkt, jest gotówka. Trzy firmy (7%) dopuszczają tylko przelew na konto, tyleż samo firm stosuje wyłącznie płatność kartą. Płatności jedynie przez Internet interesują tylko jedną firmę z biorących udział w badaniu. W tabeli 8 zaprezentowano rozkład odpowiedzi na siódme pytanie ankiety.

Tabela 7

Formy sprzedaży prowadzonej przez firmę

Jakie formy sprzedaży prowadzi firma	Liczba udzielonych odpowiedzi	Procent ogólnej liczby odpowiedzi
Osobista w siedzibie firmy	1	2,0
Drogą pocztową (wysyłkowo)	4	9,0
Przez sieć przedstawicieli handlowych	0	0,0
Przez sieć dystrybutorów	6	13,0
Przez Internet	2	4,5
Jako produkt dodatkowy (dołączany do zestawów komputerowych, czasopism)	2	4,5
Kilka z wymienionych powyżej	30	67,0
Inne	0	0,0

Źródło: opracowanie własne.

Tabela 8

Formy rozliczeń stosowane przez firmę

Jakie formy płatności/rozliczeń stosuje firma	Liczba udzielonych odpowiedzi	Procent ogólnej liczby odpowiedzi
Gotówka	11	24
Przelew na konto	3	7
Płatność kartą	3	7
Płatności przez Internet	1	2
Kilka z wymienionych powyżej	27	60
Inne	0	0

Źródło: opracowanie własne.

Pytanie ósme dotyczyło szczegółowych informacji na temat rodzajów zabezpieczeń oprogramowania przed piractwem komputerowym stosowanych przez respondentów badania. Połowa badanych firm deklaruje stosowanie kilku z wymienionych sposobów zabezpieczeń. 18% firm stosuje wyłącznie fizyczne zabezpieczenie płyty z oprogramowaniem, także 18% firm dedykuje oprogramowanie dla konkretnej konfiguracji sprzętowej (np. konkretnego modelu podzespołu). Jedynie programowe zabezpieczenie stosuje tylko 7% badanych firm. Za-

skakujące natomiast jest stwierdzenie 3 spośród badanych firm, które deklarują, że nie stosują żadnych form zabezpieczenia antypirackiego. W tabeli 9 zawarto rozkład odpowiedzi na ósme pytanie ankiety.

Tabela 9

Formy zabezpieczeń antypirackich stosowane przez firmę

Czy i jakie formy zabezpieczenia oprogramowania przed piractwem stosuje firma	Liczba udzielonych odpowiedzi	Procent ogólnej liczby odpowiedzi
Zabezpieczenie sprzętowe (sprzętowe klucze kodowe)	0	0
Oprogramowanie dedykowane jest dla konkretnej konfiguracji sprzętowej (konkretnego modelu podzespołu)	8	18
Fizyczne zabezpieczenie płyty z oprogramowaniem	8	18
Zabezpieczenie programowe	3	7
Kilka z wymienionych powyżej	23	50
Inne	0	0
Firma nie stosuje żadnych zabezpieczeń	3	7

Źródło: opracowanie własne.

Na pytanie dziewiąte, dotyczące rodzajów stosowanego zabezpieczenia programowego, odpowiedziało 25 firm biorących udział w badaniu. Było ono skierowane do tych firm, które w poprzednim pytaniu zaznaczyły odpowiedź czwartą, czyli zadeklarowały stosowanie zabezpieczenia programowego lub odpowiedź piątą – stosowanie różnych form zabezpieczenia (a więc również zabezpieczenia programowego). Pozostałe firmy poproszone zostały o przejście do kolejnego pytania. Wśród firm, które udzieliły odpowiedzi na to pytanie, aż 44% zadeklarowało stosowanie systemu rejestracji telefonicznej lub *on-line* jako programowej formy zabezpieczenia antypirackiego. Nieco mniej, bo 32% firm stosuje system kodów programowych. 12% respondentów odpowiedziało, że ich firma wprowadziła system sprawdzający istnienie w środowisku niższej wersji oprogramowania jako warunku koniecznego do instalacji i użytkowania oprogramowania firmy, także 12% firm stosuje kilka z wymienionych powyżej sposobów. W tabeli 10 przedstawiono rozkład odpowiedzi na dziewiąte pytanie ankiety.

Tabela 10

Rodzaje zabezpieczeń programowych stosowanych przez firmę

Jaki rodzaj zabezpieczeń programowych stosuje firma	Liczba udzielonych odpowiedzi	Procent ogólnej liczby odpowiedzi
System kodów programowych	8	32
Zabezpieczenie programowe przed kopiowaniem płyty (np. wykrycie obecności programów kopiujących uniemożliwia instalacje oprogramowania)	0	0
System rejestracji telefonicznej lub *on-line*	11	44
System sprawdzający istnienie w systemie niższej wersji oprogramowania	3	12
Kilka z wymienionych powyżej	3	12
Inne	0	0

Źródło: opracowanie własne.

Pytanie dziesiąte dotyczyło kosztów stosowania zabezpieczeń antypirackich. Konkretnie chodziło o wskazanie, jaką część kosztów wytworzenia produktu firma przeznacza na zabezpieczenie przed nielegalnym kopiowaniem programu. Zdecydowana większość firm, bo aż 63%, szacuje, że koszty zastosowania zabezpieczenia antypirackiego stanowią 10%–30% kosztów wytworzenia produktu. 24% firm przeznacza na to 0–10% poniesionych kosztów, 11% firm natomiast deklaruje, że koszty te stanowią aż 30%–50% kosztów wytworzenia programu. Żadna z badanych firm nie przeznacza na ten cel powyżej 50% kosztów, natomiast jedna z firm nie potrafiła wskazać właściwego przedziału. Wynika z tego, że firma ta w małym stopniu interesuje się zabezpieczeniami antypirackimi albo nie stosuje ich wcale. W tabeli 11 zaprezentowano rozkład odpowiedzi na dziesiąte pytanie ankiety.

Tabela 11

Koszty ponoszone przez firmę na zastosowanie zabezpieczenia antypirackiego

Jaką część kosztów wytworzenia produktu jednostkowego stanowi zastosowanie sposobu zabezpieczenia produktu przed piractwem	Liczba udzielonych odpowiedzi	Procent ogólnej liczby odpowiedzi
0–10%	11	24
10%–30%	28	63
30%–50%	5	11
Powyżej 50%	0	0
Trudno powiedzieć	1	2

Źródło: opracowanie własne.

Jedenaste pytanie ankiety dotyczyło zainteresowania firmy obecnością jej nielegalnie powielonych produktów na lokalnym rynku. Znaczna większość (91%) respondentów nie wykazuje zainteresowania tego typu statystykami i nie prowadzi związanych z tym badań. Dwie firmy (4,5%) prowadzą kontrolę miejsc podejrzanych o rozprowadzanie i sprzedaż tychże kopii, także dwie firmy deklarują, ze kontrolują sieci P2P w tym zakresie. W tabeli 12 zawarto rozkład odpowiedzi na jedenaste pytanie ankiety.

Tabela 12

Zainteresowanie firmy obecnością na rynku nielegalnych kopii jej produktów

W jaki sposób firma interesuje się obecnością nielegalnych kopii własnych produktów na lokalnym rynku (szara strefa)	Liczba udzielonych odpowiedzi	Procent ogólnej liczby odpowiedzi
Kontrola miejsc podejrzanych o rozprowadzanie i sprzedaż tychże kopii (giełdy, targowiska)	2	4,5
Kontrola sieci P2P	2	4,5
Inne (jakie)	0	0,0
Firma nie prowadzi tego typu badań	41	91,0

Źródło: opracowanie własne.

Kolejne pytanie dotyczyło podstaw, na jakich firma prowadzi (jeśli prowadzi) szacowanie strat własnych spowodowanych obecnością na rynku nielegalnych kopii jej produktu. Aż 67% firm prowadzi weryfikacje na podstawie liczby prób rejestracji produktu przy użyciu tego samego klucza. Niestety, rozkład odpowiedzi udzielonych na to pytanie wskazuje na to, że firmy wypełniły ankietę nie do końca rzetelnie, bowiem w jednym z wcześniejszych pytań tylko 11 firm zadeklarowało, że stosuje system rejestracji produktu *on-line* bądź telefoniczny, a jedynie w ten sposób firmy mogłyby dokonywać zadeklarowanego w tym pytaniu rodzaju weryfikacji. Trzy z badanych firm (7%) zadeklarowały również, że współpracują z prokuraturą, a jedna, że swoje straty szacuje na podstawie upublicznionych efektów użytkowania oprogramowania. Jest to dość rzadko stosowany sposób szacowania strat własnych, bowiem można stosować go jedynie w przypadku oprogramowania generującego pliki o charakterystycznych rozszerzeniach, niebędących w powszechnym użytku. Zaskakujące jest też, że aż 24% firm nie prowadzi tego typu szacunków. W tabeli 13 zawarto rozkład odpowiedzi na dwunaste pytanie ankiety.

Tabela 13

Podstawy prowadzonych przez firmę statystyk na temat strat własnych spowodowanych piractwem

Na jakiej podstawie firma prowadzi statystyki/ szacowanie strat własnych spowodowanych nielegalnym kopiowaniem jej produktów	Liczba udzielonych odpowiedzi	Procent ogólnej liczby odpowiedzi
Współpraca z prokuraturą	3	7
Weryfikacja na podstawie liczby prób rejestracji produktu przy użyciu tego samego klucza	30	67
Szacowanie na podstawie upublicznionych efektów użycia oprogramowania	1	2
Inne	0	0
Firma nie prowadzi tego rodzaju statystyk	11	24

Źródło: opracowanie własne.

Pytanie trzynaste dotyczyło szacunkowych wysokości strat ponoszonych przez firmy z powodu piractwa komputerowego. Należy tu podkreślić, że firmy podając te wartości, często nie kierowały się prowadzonymi statystykami czy badaniami, a straty szacowały orientacyjnie. Ponad połowa firm (56%) ocenia straty z powodu piractwa na 20%–50%. 13% deklaruje, że straty te z pewnością przekraczają 50%, tyleż samo widzi je na poziomie znacznie niższym bo 5%–20%. Tylko jedna firma (2%) nie stwierdziła strat z powodu piractwa, natomiast aż 4 (9%) nie umiały sprecyzować poziomu, na jakim piractwo komputerowe wpływa na obniżenie zysków firmy. W tym miejscu należałoby zaznaczyć, że straty na poziomie np. 50% oznaczają, że 50% nabywców nielegalnej kopii oprogramowania kupiłaby legalną kopię, gdyby na rynku nie było nielegalnej wersji produktu. W tabeli 14 przedstawiono rozkład odpowiedzi na trzynaste pytanie ankiety.

Tabela 14

Szacunkowa wysokość strat ponoszonych przez firmy z powodu piractwa

Na jaką wysokość firma ocenia straty spowodowane nielegalnym kopiowaniem jej produktów	Liczba udzielonych odpowiedzi	Procent ogólnej liczby odpowiedzi
Firma nie stwierdziła strat z powodu piractwa	1	2
Do 5%	3	7
5%–20%	6	13
20%–5%	26	56
Powyżej 50%	6	13
Trudno powiedzieć	4	9

Źródło: opracowanie własne.

W pytaniu czternastym spytano firmy o stosowanie w ostatnim czasie nowych zabezpieczeń czy strategii antypirackich. Żadna z firm nie podniosła w tym celu ceny produktu, natomiast aż 29% firm obniżyła cenę produktu, mając nadzieję, że w ten sposób zmniejszy się skala piractwa komputerowego. 18% firm nie zastosowało żadnych nowych strategii, jednak aż 53% zastosowało inne sposoby, niewymienione w pytaniu. Firmy poproszone w ankiecie o ich wskazanie, mówiły o wprowadzeniu zabezpieczeń, których do tej pory nie stosowały, np. wprowadzenie konieczności rejestracji *on-line*, znaczna część firm rozszerzyła w ten sposób liczbę stosowanych zabezpieczeń. W tabeli 15 zawarto rozkład odpowiedzi na czternaste pytanie ankiety.

Tabela 15

Nowe strategie ochrony przed piractwem stosowane przez firmę

Czy firma w ostatnim czasie zastosowała nowe (jakie?) strategie zabezpieczenia antypirackiego	Liczba udzielonych odpowiedzi	Procent ogólnej liczby odpowiedzi
Podniesiono cenę produktu jednostkowego	0	0
Obniżono cenę produktu jednostkowego	13	29
Inne strategie	24	53
Nie zastosowano żadnych nowych strategii	8	18

Źródło: opracowanie własne.

Pytanie piętnaste miało na celu sprawdzenie świadomości firm na temat organów zajmujących się ściganiem przestępstw komputerowych. Aż 67% respondentów zadeklarowało, że wiedzą, do kogo należy się zwrócić w przypadku wykrycia przestępstwa komputerowego. Na 30 firm, które zaznaczyły tą odpowiedź, aż 20 jako organ, do którego należy się w takim wypadku zwrócić wskazało policję. 5 firm podało policyjny telefon zaufania, który okazuje się być coraz popularniejszy, świadczy to o coraz lepszej świadomości społeczeństwa na temat pracy policji i dobrze wróży na przyszłość kolejnym policyjnym akcjom tego typu. 5 firm zapytanych do kogo należy się w takim wypadku zwrócić, jako odpowiedź podało ZAiKS, co świadczy o tym, że brane zostało tutaj pod uwagę również piractwo fonograficzne. W poniższej tabeli zawarto rozkład odpowiedzi na piętnaste pytanie ankiety.

Tabela 16

Do kogo należy się zwrócić w sprawie odkrytego przestępstwa komputerowego

Czy wie Pani/Pan do kogo należy się zwrócić w sprawie odkrytego przestępstwa komputerowego	Liczba udzielonych odpowiedzi	Procent ogólnej liczby odpowiedzi
Tak	30	67
Nie	15	33

Źródło: opracowanie własne.

Kolejne pytanie dotyczyło znajomości przepisów i uregulowań związanych z przestępczością komputerową, najwięcej, bo aż 53% wskazało w tym temacie na ustawę o ochronie danych osobowych, być może związane jest to z faktem, że jest ona ostatnio bardzo popularna i szeroko omawiana w mediach. 29% respondentów wskazało na ustawę o prawie autorskim i prawach pokrewnych, a aż 18% odpowiedziało, że nie zna żadnych regulacji prawnych dotyczących przestępczości komputerowej. W poniższej tabeli zawarto rozkład odpowiedzi na szesnaste pytanie ankiety. Rozkład procentowy poszczególnych wariantów zaprezentowano również na wykresie.

Tabela 17

Znajomość uregulowań prawnych związanych z informatyką

Czy zna Pani/Pan jakąś regulację prawną związaną z informatyką	Liczba udzielonych odpowiedzi	Procent ogólnej liczby odpowiedzi
Kodeks karny	0	0
Ustawa o prawie autorskim i prawach pokrewnych	13	29
Ustawa o ochronie danych osobowych	24	53
Inne	0	0
Nie znam	8	18

Źródło: opracowanie własne.

Ustawa o prawie autorskim jest znana większości respondentów, ale mała ich część, bo zaledwie 18% wskazała na właściwą datę jej uchwalenia. Również 18% nie umiało podać daty uchwalenia tej ustawy, a aż 53% podało tok 1997. Być może jest to związane z faktem coraz większego nagłaśniania przez media

sprawy ochrony tych danych. W poniższej tabeli zawarto rozkład odpowiedzi na siedemnaste pytanie ankiety.

Tabela 18

Znajomość ustawy o ochronie praw autorskich

Od którego roku obowiązuje w Polsce ustawa o ochronie praw autorskich	Liczba udzielonych odpowiedzi	Procent ogólnej liczby odpowiedzi
1942	0	0
1985	3	7
1994	8	18
1997	23	50
Żadna z odpowiedzi nie jest poprawna	3	7
Nie wiem	8	18

Źródło: opracowanie własne.

Znakomita większość (82%) respondentów nigdy nie interweniowała w sprawie własnych praw autorskich. Tylko 8 respondentów potwierdziło, że taka interwencja miała miejsce. We wszystkich przypadkach były to właśnie sprawy przypadków piractwa komputerowego. W poniższej tabeli zawarto rozkład odpowiedzi na osiemnaste pytanie ankiety.

Tabela 19

Interwencja w sprawie własnych praw autorskich

Czy kiedykolwiek interesowała się Pani/Pan sprawą własnych praw autorskich	Liczba udzielonych odpowiedzi	Procent ogólnej liczby odpowiedzi
Tak	8	18
Nie	37	82

Źródło: opracowanie własne.

Aż 56% respondentów zaznaczyło, że wie, jaki organ jest odpowiedzialny za ochronę praw autorskich i wskazało na Ministra Kultury i Sztuki, 2 na Ministra Sprawiedliwości, 5 osób napisało, że odpowiedzialne za ochronę praw autorskich są organizacje zrzeszające twórców. W tabeli 20 zawarto rozkład odpowiedzi na dziewiętnaste pytanie ankiety.

Tabela 20

Jaki organ odpowiedzialny jest za ochronę praw autorskich

Czy wie Pani/Pan, jaki organ jest odpowiedzialny za zgodną z prawem ochronę praw autorskich	Liczba udzielonych odpowiedzi	Procent ogólnej liczby odpowiedzi
Tak	25	56
Nie	20	44

Źródło: opracowanie własne.

Aż 53% respondentów uważa, że w Polsce prawa autorskie nie są odpowiednio chronione. Przeciwnego zdania jest zaledwie 9% respondentów, natomiast opinii w tym temacie nie wyraziło 31%. Zaproponowano również 3 rozwiązania własne, przy czym dotyczyły one we wszystkich wypadkach zwiększenia kar nakładanych na przestępców komputerowych i zintensyfikowania kontroli prowadzonej przez policję i prokuraturę.

Tabela 21

Czy prawa autorskie w Polsce są odpowiednio chronione

Czy uważa Pani/Pan, że w Polsce prawa autorskie są odpowiednio chronione	Liczba udzielonych odpowiedzi	Procent ogólnej liczby odpowiedzi
Tak	4	9
Nie	24	53
Nie mam zdania na ten temat	14	31
Inne proponowane rozwiązania	3	7

Źródło: opracowanie własne.

Na podstawie przeprowadzonych badań trzeba z przykrością stwierdzić, że zainteresowanie firm zajmujących się produkcją/dystrybucja oprogramowania problemami ochrony własnych praw autorskich, strat związanych z łamaniem tych praw i innych kwestii związanych z przestępczością komputerową jest niewielkie. Firmy nie prowadzą statystyk, nie interesują się obecnością na rynku pirackich kopii własnych produktów, nie potrafią wskazać proponowanych sposobów rozwiązania tej kwestii.

Mimo że znaczna część ankietowanych miała styczność z przestępstwami komputerowym, nie chronią oni swoich praw autorskich w jakiś szczególnie bez-

pieczny sposób. Stosuje się zwykłe, najprostsze zabezpieczenia, które nie są żadną przeszkodą nawet dla przeciętnego użytkownika oprogramowania. Dostępność na rynku zarówno sprzętu, jak i oprogramowania do powielania nośników z oprogramowaniem sprawiła, że zabezpieczenia stosowane przez firmy nie są żadną przeszkodą lub stanowią niewielkie utrudnienie. W dzisiejszych czasach należałoby jednak pomyśleć o bardziej skomplikowanych i przemyślanych sposobach zabezpieczenia oprogramowania i tym samym ochrony praw autorskich. Firmy szacują swoje straty związane z piractwem komputerowym na dość wysokim poziomie, jednak są to dane orientacyjne, nieoparte w większości na żadnych statystykach.

Regulacje prawne związane z informatyką także nie są znane przeciętnym obywatelom, tak jak i Ustawa o prawie autorskim i prawach pokrewnych (która dotyczy ich bezpośrednio) czy Kodeks karny. Większość respondentów nie wie nawet o najważniejszych artykułach tych ustaw, które powinny ich zainteresować choćby z tego względu, że dotyczą ich własnych praw. Wielu z nich potrafiło tylko stwierdzić, że nie są zadowoleni z istniejącej ochrony, ale nikt nie zaproponował innych ciekawych rozwiązań tego problemu.

Podsumowanie

Przestępczość komputerowa jest tematem bardzo złożonym i niejednorodnym, dlatego nie sposób przedstawić wszystkich jej aspektów. Z jednej strony są to przestępstwa tradycyjne, jak kradzież czy oszustwa, jednak z drugiej strony, ze względu na swoje cechy charakterystyczne, muszą być rozpatrywane również w innych aspektach, nieznanych do tej pory systemowi prawnemu.

W poszczególnych rozdziałach zostały omówione najważniejsze – zdaniem autorki – i najbardziej typowe zagadnienia związane z tym tematem. Z przedstawionego przeglądu przestępstw komputerowych wynika, że mogą one mieć wpływ nie tylko na straty związane z prowadzeniem działalności gospodarczej, ale mogą również skutkować zakłóceniami komunikacji czy łączności, a nawet powodować zagrożenie bezpieczeństwa czy wręcz życia. Szybkiemu rozwojowi informatyzacji powinny towarzyszyć odpowiednie regulacje prawne. Jednak można zauważyć, że, komputeryzacja rozwija się w znacznie szybszym tempie i przepisy prawne nie nadążają za tak szybkim rozwojem. Straty, jakie ponoszą przedsiębiorcy, użytkownicy, a także Skarb Państwa powodują, że wszyscy jesteśmy poszkodowani z powodu przestępczości komputerowej. Konieczne jest więc podejmowanie wszelkiego rodzaju działań zarówno prewencyjnych, jak

i wykrywczych akcji przeciwko popełnianiu przestępstw komputerowych. Należy chronić się również, stosując nowoczesne zabezpieczenia techniczne, nadążające technologicznie za rozwojem przestępczości komputerowej. Jak wynika z ankiety, która dla potrzeb niniejszej pracy została przeprowadzona wśród producentów i dystrybutorów oprogramowania komputerowego, świadomość zagrożeń i sposoby uchronienia się przed piractwem komputerowym nie osiągają wystarczającego poziomu i nadal możemy mówić o niewystarczającej ochronie na tym szczeblu.

Przestępczość komputerowa jest tematem bardzo obszernym, głównie ze względu na swoją specyfikę i szybki rozwój. Temat nie został w niniejszej pracy wyczerpany w całości (również ze względu na reprezentatywność próby badawczej). Jednak można stwierdzić, że w skomputeryzowanym świecie, w którym technika rozwija się z niespotykaną dotąd prędkością, informacje najbardziej aktualne w czasie gromadzenia materiałów w chwili składania jej do druku mogą wydawać się już przestarzałe. Niemniej starano się przedstawić najbardziej uniwersalne aspekty przestępczości komputerowej w taki sposób, aby zawarte w pracy zagadnienia były maksymalnie ponadczasowe.

Bibliografia

Golat K., Golat R. (2010), *Prawo komputerowe. Zagadnienia podstawowe*, IBIS, Warszawa.

http://www.aplusc-systems.com/ (dostęp 15.02.2013).

http://www.spkif.w.interia.pl/1prawo.html (dostęp 15.02.2013).

http://www.winter.pl/internet/w0830.html (dostęp 15.02.2013).

Jakubowski K.J. (2011), *Przestępczość komputerowa. Zarys problematyki*, „Prokuratura i Prawo", nr 12.

Wójcik W.J. (2008), *Hacking!*, „Prawo i Życie", nr 36.

Znierzchowski Z. (2010), *Rozkradana informatyka*, Wydawnictwo Rzeczpospolita, Warszawa.

Załącznik 1

1. Ilu pracowników zatrudnia Państwa firma?

□ Firma jednoosobowa □ 2–5 □ 5–10 □ 10–20 □ powyżej 20

2. Jakiego rzędu obroty generuje firma rocznie [PLN]?

□ poniżej 50 tys. □ 50–100 tys. □ 100–500 tys. □ 500 tys.–1 mln □ powyżej 1 mln

3. Obszar działalności firmy

□ rynek lokalny □ rynek ogólnopolski □ rynek międzynarodowy

4. Firma jest:

□ tylko producentem oprogramowania □ tylko dystrybutorem oprogramowania
□ producentem i dystrybutorem oprogramowania

5. Jakiego rodzaju oprogramowanie produkuje/dystrybuuje firma?

□ specjalistyczne, ściśle dedykowane określonej grupie odbiorców
□ oprogramowanie użytkowe dla szerokiego grona odbiorców (powszechnego użytku)
□ oprogramowanie rozrywkowe
□ oprogramowanie dodatkowe (wspomagające, np. wtyczki, plug-iny do innych programów)
□ kilka z wymienionych powyżej
□ inne (jakie) .....

6. Jakie formy sprzedaży stosuje firma?

□ osobista w siedzibie firmy
□ drogą pocztową (wysyłkowo)
□ przez sieć przedstawicieli handlowych
□ przez sieć dystrybutorów
□ przez Internet
□ jako produkt dodatkowy (dołączany do zestawów komputerowych, czasopism)
□ kilka z wymienionych powyżej
□ inne (jakie) .....

7. Jakie formy płatności/rozliczeń stosuje firma?

□ gotówka
□ przelew na konto
□ płatność kartą
□ płatności przez Internet (w tym np. płatność za pomocą sms)
□ kilka z wymienionych powyżej
□ inne (jakie) .....

8. Czy i jakie formy zabezpieczenia oprogramowania przed piractwem stosuje firma?

□ zabezpieczenie sprzętowe (np. sprzętowe klucze kodowe)
□ oprogramowanie dedykowane jest dla konkretnej konfiguracji sprzętowej (konkretnego modelu podzespołu)
□ fizyczne zabezpieczenie płyty z oprogramowaniem
□ zabezpieczenie programowe
□ kilka z wymienionych powyżej
□ inne (jakie?) .....
□ firma nie stosuje żadnych zabezpieczeń

Jeżeli firma nie stosuje zabezpieczeń programowych, proszę przejść do pytania nr 10.

9. Jaki rodzaj zabezpieczeń programowych stosuje firma?

□ system kodów programowych
□ zabezpieczenie programowe przed kopiowaniem płyty (np. wykrycie obecności programów kopiujących uniemożliwia instalacje oprogramowania)
□ system rejestracji telefonicznej lub *on-line*
□ system sprawdzający istnienie w systemie niższej wersji oprogramowania
□ kilka z wymienionych powyżej
□ inne (jakie?) .....

10. Jaką część kosztów wytworzenia produktu jednostkowego stanowi zastosowanie sposobu zabezpieczenia produktu przed piractwem?

□ 0–10% □ 10%–30% □ 30%–50% □ powyżej 50% □ trudno powiedzieć

11. W jaki sposób firma interesuje się obecnością nielegalnych kopii własnych produktów na lokalnym rynku (szara strefa)?

□ kontrola miejsc podejrzanych o rozprowadzanie i sprzedaż tychże kopii (giełdy, targowiska)
□ kontrola sieci P2P
□ inne (jakie) .....
□ firma nie prowadzi tego typu badań

12. Na jakiej podstawie firma prowadzi statystyki/szacowanie strat własnych spowodowanych nielegalnym kopiowaniem jej produktów?

□ współpraca z prokuraturą
□ weryfikacja na podstawie ilości prób rejestracji produktu przy użyciu tego samego klucza
□ szacowanie na podstawie upublicznionych efektów użycia oprogramowania
□ inne (jakie?) .....
□ firma nie prowadzi tego rodzaju statystyk

13. Na jaką wysokość (%) firma ocenia straty spowodowane nielegalnym kopiowaniem jej produktów?

□ firma nie stwierdziła strat z tytułu piractwa □ do 5% □ 5%–20%
□ 20%–50% □ powyżej 50% □ trudno powiedzieć

14. Czy firma w ostatnim czasie zastosowała nowe (jakie) strategie zabezpieczenia antypirackiego?

□ podniesiono cenę produktu jednostkowego
□ obniżono cenę produktu jednostkowego
□ inne strategie (jakie) .....
□ nie zastosowano żadnych nowych strategii

15. Czy wie Pani/Pan do kogo należy się zwrócić w sprawie odkrytego przestępstwa komputerowego?

□ tak (do kogo?) .....
□ nie

16. Czy zna Pani/Pan jakąś regulację prawną związaną z informatyką?

□ Kodeks karny
□ Ustawa o prawie autorskim i prawach pokrewnych
□ Ustawa o ochronie danych osobowych
□ inne (jakie) .....
□ nie znam

17. Od którego roku obowiązuje w Polsce ustawa o ochronie praw autorskich?

□ 1942 □ 1985 □ 1994 □ 1997
□ inna data (jaka?) ..... □ nie wiem

18. Czy kiedykolwiek interesowała się Pani/Pan sprawą własnych praw autorskich?

□ tak (w jakiej sprawie?) .....
□ nie

19. Czy wie Pani/Pan, jaki organ jest odpowiedzialny za zgodną z prawem ochronę praw autorskich?

□ tak (jaki?).....
□ nie

20. Czy uważa Pani/Pan, że w Polsce prawa autorskie są odpowiednio chronione?

□ tak □ nie
□ nie mam zdania na ten temat □ inne proponowane rozwiązania .....

SOFTWARE PIRACY. ANALYSIS OF THE PHENOMENON ACCORDING TO THE POLL SURVEY RESULTS

Summary

This article discusses the basic problems of software piracy by its types, examples, and the presence of anti-piracy strategies. It includes also a presentation of survey results for this problem.

Translated by Agnieszka Szewczyk

Keywords: software piracy, cyber-crime