EDUKACJA DLA BEZPIECZE ŃSTWA

CYWILIZACYJNE PROBLEMY BEZPIECZEŃSTWA

Pod redakcją
Krzysztofa Augustyniaka
Andrzeja Piotrowskiego

Poznań 2011

Recenzje
prof. dr hab. inż. Piotr Sienkiewicz
dr hab. Bogdan Zalewski

Korekta
Marta Walachowska

Projekt okładki i strony tytułowej
Marta Walachowska
Marta Zduniak

Autorzy zdjęć
PGE Arena Gdańsk
Marta Dziedzic

Skład komputerowy
Marta Walachowska

ISBN: 978-83-61304-37-1

Wydanie publikacji dofinansowane przez Fundację
„EDUKACJA DLA BEZPIECZEŃSTWA”

Wydawnictwo Wyższej Szkoły Bezpieczeństwa
ul. Wyspiańskiego 16/6, 60-750 Poznań
tel. 61 851 05 18
e-mail: wydawnictwo@wsb.net.pl
www.wsb.net.pl

Druk i oprawa
“ESUS” Agencja Reklamowo – Wydawnicza
ul. Wierzbięcice 35, 61-855 Poznań
tel./fax. 61 835 35 36
www.esus.pl

Wydanie pierwsze
Druk ukończono w czerwcu 2011 r.

SPIS TREŚCI

ROZDZIAŁ II

Przedmowa

Przekazana na ręce Czytelnika książka ma charakter pracy zbiorowej podsumowującej wystąpienia z VII Ogólnopolskiego Seminarium Naukowego zatytułowanego: „Cywilizacyjne problemy bezpieczeństwa", odbywającego się w dniach 20-22 kwietnia 2011 roku w Gdańsku i organizowanego przez Wydział Zamiejscowy w Gdańsku Wyższej Szkoły Bezpieczeństwa z siedzibą w Poznaniu. Prezentowane w niej treści stanowią przegląd najnowszych współcześnie prowadzonych badań empirycznych i analiz teoretycznych z zakresu szeroko rozumianej problematyki bezpieczeństwa.

Zachodzące przeobrażenia cywilizacyjne nie mogą pozostać bez wpływu na zmiany zagrożeń a także sposoby przeciwdziałania im. Debaty, które miały miejsce w trakcie trwania seminarium koncentrowały się wokół dwóch obszarów tematycznych: „Bezpieczeństwo imprez masowych w kontekście Euro 2012" oraz „Społeczne aspekty przestępczości teleinformatycznej". Wyzwania, jakie stoją przed naszym krajem w zakresie zapewnienia bezpieczeństwa w trakcie trwania Euro 2012 kazały szczególnie uważnie pochylić się nad tym zagadnieniem. Wystąpienia znakomitych praktyków jak i uznanych autorytetów naukowych wskazały główne możliwe źródła zagrożeń a także najlepsze sposoby ich przeciwdziałania i niwelowania. Przedmiotem dociekań było ustalenie form, zakresu oraz ewentualnych skutków wydarzeń mogących zagrozić bezpieczeństwu uczestników imprez masowych. Wydarzanie, jakim jest Euro 2012 skupia uwagę nie tylko kibiców, ale także i osób, które bezpieczeństwu mogłyby zagrozić. Kwestia ta jest o tyle istotna, że nasz kraj nie ma dotychczas dużego doświadczenia w organizowaniu imprez tego typu oraz że nadal borykamy się z szeroko rozumianymi problemami związanymi z zapewnieniem bezpieczeństwa organizacji sportowych imprez masowych.

Drugi z obszarów tematycznych skupiał się na: „społecznych aspektach przestępczości teleinformatycznej". Nowe media to także nowe problemy, z którymi należy się zmierzyć. Wyzwania, jakie stoją przed nami w tym zakresie, są nadal bardzo aktualne, gdyż ścieżka rozwoju, którą kroczymy ku społeczeństwu wiedzy, niemożliwa jest do realizacji bez bezpiecznego rozwoju teleinformatycznego. Zgromadzone artykuły przestawiają najnowsze trendy związane z przestępczością oraz metody zapewnienia bezpieczeństwa w cyberprzestrzeni.

Mamy nadzieję, że książka ta wychodzi naprzeciw aktualnym problemom cywilizacyjnym związanym z bezpieczeństwem i stanowić będzie użyteczne źródło informacji dla osób zainteresowanych tą problematyką.

Andrzej PIOTROWSKI

SPOŁECZNE ASPEKTY PRZESTĘPCZOŚCI TELEINFORMATYCZNEJ

Krzysztof AUGUSTYNIAK
Wyższa Szkoła Bezpieczeństwa w Poznaniu
Wydział Zamiejscowy w Gdańsku

ZAGROŻENIA ZWIĄZANE Z SEKSUALNYM WYKORZYSTYWANIEM DZIECI I PORNOGRAFIĄ DZIECIĘCĄ W INTERNECIE JAKO WYZWANIA DLA ORGANÓW ŚCIGANIA

Wzrastająca rola Internetu, łączącego w ramach swych możliwości funkcję nośnika informacji oraz taniego multimedialnego komunikatora, sprzyja powszechnemu dostępowi do nowoczesnej wiedzy i najnowszych osiągnięć myśli ludzkiej, ale także niesie ze sobą niebezpieczeństwo transferu treści stanowiących naruszenie zasad moralnych i obowiązujących przepisów prawa. Jednym z najgroźniejszych i szkodliwych zjawisk w tym zakresie jest rozpowszechnianie pornografii dziecięcej. Internet umożliwił także osobom o skłonnościach pedofilskich nie tylko zaspokajanie fantazji seksualnych, ale również nawiązywanie kontaktów z małoletnimi w celu doprowadzenia do fizycznego spotkania i ich seksualnego wykorzystania poprzez udział w społecznościach internetowych, chat -roomach, dyskusjach na forum, itd.

Jak wynika z badań realizowanych wśród polskich dzieci korzystających z Internetu,[1] ok. 80% z nich mimowolnie spotyka się w sieci z materiałami o charakterze pornograficznym. Znaczna część tych treści staje się dostępna podczas poszukiwania innych, ważnych dla użytkownika informacji. Obserwacja serwisów internetowych zawierających treści z omawianego obszaru pozwala stwierdzić, że duża ilość zawartych tam materiałów jest świadomie kierowana do nastoletnich „serferów". Sama zaś pornografia dziecięca stała się aktualnie bardzo rozpowszechnionym, globalnym procederem przestępczym, doskonale funkcjonującym w Internecie. Tysiące młodych ludzi staje się każdego roku ofiarami tego rodzaju działalności przestępczej. Do głównych zagrożeń związanych z omawianymi zjawiskami zalicza się przede wszystkim mimowolny odbiór treści pornograficznych przez nieletnich oraz uprzedmiotowienie dzieci w realizacji filmów i zdjęć pornograficznych.[2] Jednak jak podkreśla P. Jenkins, pośrednim zagrożeniem może być również stymulowanie dorosłych do podjęcia aktywności seksualnej z nieletnimi poprzez oglądanie pornografii dziecięcej.[3]

Badania Fundacji „Dzieci Niczyje" wskazują ponadto, że aż 56% dzieci korzystających z Internetu, wciąganych jest mimowolnie w rozmowy o charakterze seksualnym.[4] W opinii osób obserwujących omawiane zjawisko, o szkodliwości tego typu zachowań sprawców może świadczyć fakt, że wulgarność i agresywność

---

[1] Ł. Wojtasik, *Pedofilia i pornografia w Internecie – zagrożenia dla dzieci. Raport z badań* (w:) „Dziecko krzywdzone", 2003, nr 5
[2] O. Calcetas-Santos, *Child Pornography on the Internet*. (w:) C.A. Arnaldo: *Child Abuse on the Internet. Ending the Silence*. UNESCO Publishing. 2001
[3] P. Jenkins, *Beyond Tolerance. Child Pornography on the Internet. University Press*. New York, 2001
[4] Ł. Wojtasik, op. cit.

prowadzonych rozmów powoduje u około 20-30% uczestniczących w nich dzieci nasilenie stanów lękowych i przeżywanie stresu.[5]

Według badań przeprowadzonych w Stanach Zjednoczonych w latach 1999/2000 metodą ankiety telefonicznej,[6] korzystające z Internetu dzieci i młodzież w wieku 10-17 lat spotykały się z takimi działaniami sprawców wykorzystywania seksualnego, jak na przykład: propozycje o charakterze seksualnym[7] (20%), agresywne propozycje seksualne[8] (3%) oraz niechciane prezentacje materiałów pornograficznych podczas eksplorowania zasobów Internetu lub korzystania z poczty elektronicznej (25%). Skalę zagrożenia przedstawiają również badania przeprowadzone przez S. Livingston i M. Bober,[9] które stwierdziły, że 57% młodych użytkowników Internetu miała kontakt z pornografią za pośrednictwem sieci, a aż 10% uczestników badań deklarowało intencjonalne poszukiwanie i oglądanie pornografii.

Wykorzystywanie dzieci w przedsięwzięciach o charakterze pornograficznym oraz odbiór przez nieletnich takich treści jest niezwykle szkodliwe dla ich rozwoju i przyszłego funkcjonowania w społeczeństwie. Ponadto, wiąże się zwykle z określonymi konsekwencjami prawnymi także dla samych nieletnich.

O powadze sytuacji świadczyć mogą również badania przeprowadzone przez organizację „Kidprotect" we współpracy z portalem Onet.pl.[10] W toku ich trwania stwierdzono bowiem aż 18.000 zapytań dotyczących pornografii dziecięcej w ciągu jednego miesiąca. Wskazuje to jednoznacznie na wysokie zainteresowanie tematem, ale także – w opinii realizatorów badań – na wysokie poczucie bezkarności wpisujących je osób. Według ustaleń dziennikarzy „Gazety wyborczej"[11] w Polsce żyje bez nadzoru 7,6 tys. osób podejrzanych o pedofilię, z których część wyszła na wolność po wyrokach. Według tego samego źródła, w 2006 roku ofiarą pedofilów padło ponad 4 tysięcy dzieci, w 2007 roku ponad 8 tysięcy, a w roku 2008 prawie 6 tysięcy.

Mając powyższe na uwadze, autor także podjął próbę określenia poziomu aktualnie istniejącego zagrożenia, w oparciu o informacje uzyskane z sondażu diagnostycznego przeprowadzonego wśród młodzieży wybranych szkół gimnazjalnych i średnich.[12] Jednym z głównych celów badań było określenie poziomu kontaktu nieletnich z problematyką pornografii dziecięcej występującej w Internecie.

Badaną populację stanowiła 773 osobowa grupa młodzieży w wieku 13-18 lat. Wśród ankietowanych osób reprezentowane były obie płci, przy czym dziewczęta

---

[5] Por.: D. Finkelhor, K.J. Mitchell, J. Wolak: O*nline Victimization. A report on the Nation's Youth. National Center for Missing and Exploited Children*. 2001; Ł. Wojtasik: op. cit.; Ł. Wojtasik: „Dziecko w Sieci" – raport z badań. 2004. (www.dzieckowsieci.pl)

[6] D. Finkelhor, K.J. Mitchell, J. Wolak: *Online Victimization*… op. cit.

[7] Czytaj: proponowanie przez osobę dorosłą kontaktu seksualnego lub rozmowa na tematy związane z seksem

[8] Czytaj: propozycje o charakterze seksualnym z wykorzystaniem Internetu, telefonu i regularnej poczty, mające na celu zaaranżowanie spotkania z nieletnim

[9] S. Livingston, M. Bober, *UK Children Go Online. Final report of key project findings*. 2005 (*http://www.children-go-online.net*)

[10] J. Śpiewak: *Zainteresowanie internetową pedofilią w Polsce*. (*http://www.kidprotect.pl/artykuly*)

[11] *http://wiadomosci.onet.pl/2001236,11,item.html*

[12] w Szczytnie, Toruniu i Sopocie

stanowiły populację liczącą 392 osoby (50,7% ogółu). Najwięcej uczestników badań legitymowało się wiekiem 15-16 lat (62,9% ogółu respondentów).

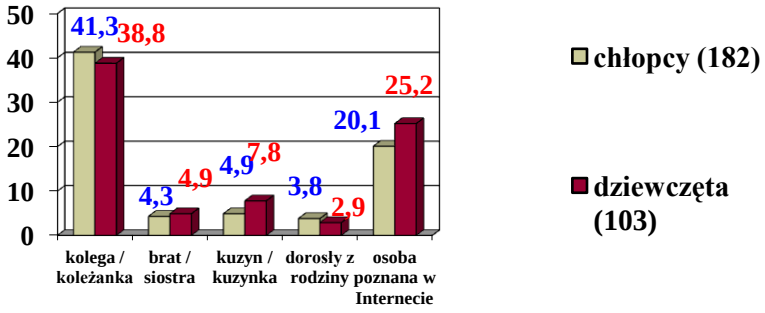
Analiza wyników badań

Udzielone odpowiedzi świadczą o wszechstronnym wykorzystaniu Internetu przez młodzież, zgodnie zresztą z jego podstawowym przeznaczeniem. Nie może jednak budzić wątpliwości fakt, iż ta wszechstronność może być także źródłem oddziaływań negatywnych, takich jak na przykład działalność przestępcza związana z naruszeniem praw autorskich (P2P), praw obywatelskich i godności osobistej (chat'y i grupy dyskusyjne), czy wreszcie wykorzystywaniem seksualnym (zdjęcia, filmy, itp.). Mogą one w sposób zdecydowany wpływać na bezpieczeństwo psychiczne i fizyczne dzieci i młodzieży.

Młodzież potwierdza fakt otrzymywania wulgarnych i/lub agresywnych treści. W naszych badaniach uczyniło to 50,7% ich uczestników. Spośród nich, blisko 46% osób przyznało, że takie sytuacje zdarzają się rzadko, ale jednocześnie, 24,6% określiło odpowiedź na poziomie „czasami", a 12,3% nawet na poziomie „dość często".

Kolejnym, bardzo niepokojącym wątkiem, uwidocznionym podczas analizy wyników naszych badań, jest kontakt młodzieży z treściami o charakterze pornograficznym oraz jej odczucia dotyczące obejrzanych materiałów. Z deklaracji respondentów wynika, że 18,1% dziewcząt i aż 34,3% chłopców przynajmniej jeden raz otrzymało propozycję obejrzenia zdjęć lub filmów pornograficznych. Zdecydowana większość młodzieży z tej grupy otrzymywała je wielokrotnie. Osobami zachęcającymi do wymienionych zachowań były najczęściej koleżanki i koledzy, a ponadto także rodzeństwo i kuzyni. O ile w tych przypadkach można przyjąć, iż wynikało to raczej z ciekawości i „burzy hormonów" okresu dorastania, o tyle szokującym może być fakt wychodzenia z takimi propozycjami przez dorosłych członków rodziny.

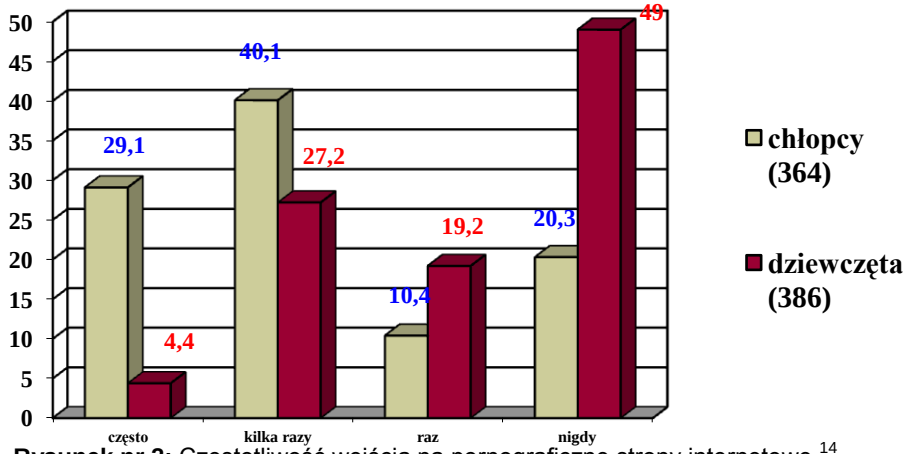
W tym kontekście, dużej wagi nabiera również informacja o liczbie osób poznanych przez respondentów w Internecie, które także proponowały uczestnikom naszych badań oglądanie materiałów zawierających wspomniane treści. Według uzyskanych danych, co piąty chłopiec i co czwarta dziewczyna otrzymała taką propozycję z wymienionego źródła.



Rysunek nr 1: Osoby proponujące obejrzenie zdjęć i filmów pornograficznych[13]
Źródło: opracowanie własne

[13] Wartość procentowa obliczana dla liczby osobników danej płci, którzy odpowiedzieli na pytanie.

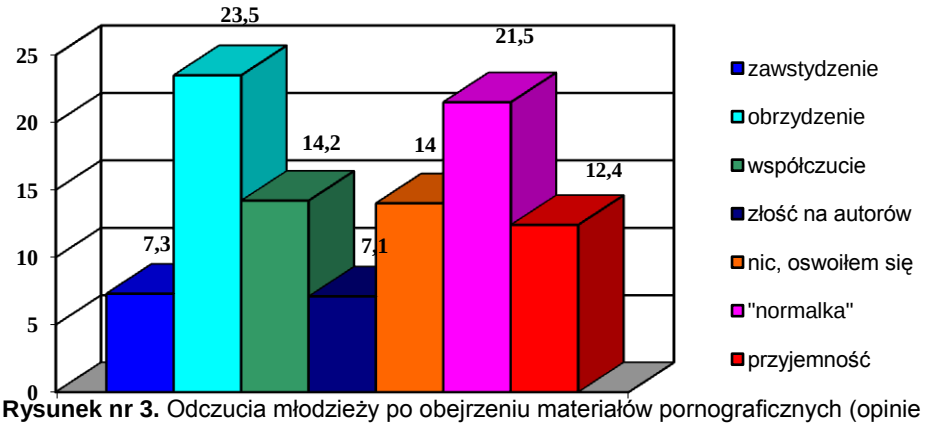
Innym źródłem dostępu młodzieży do omawianych materiałów były strony internetowe specjalizujące się w prezentowaniu pornografii. Niemal 80% chłopców i 51% dziewcząt przynajmniej jeden raz weszło na taką stronę. Niektórzy z nich zrobili to intencjonalnie, a dla pozostałych działanie takie było przypadkowe, związane głównie z uruchomieniem linków zamieszczonych na innych stronach pozostających w zainteresowaniu młodzieży. Nie zmienia to jednak faktu, że łatwość dostępu i pozyskania zdjęć i filmów pornograficznych jest ogromnym wyzwaniem dla administratorów sieci internetowej i osób starających się powstrzymać rozwój tego procederu.



Rysunek nr 2: Częstotliwość wejścia na pornograficzne strony internetowe.[14]
Źródło: opracowanie własne

W kwestionariuszach przeprowadzonej ankiety młodzież miała również okazję podzielenia się swoimi odczuciami związanymi z oglądaniem materiałów zawierających treści o charakterze pornograficznym. Spośród osób, które wyraziły swą opinię w tym zakresie, co czwarta z nich odczuwała obrzydzenie, co siódma – współczucie, a co czternasta – zawstydzenie lub złość na autorów. Pomimo znajomości specyfiki w wieku dojrzewania młodzieży, niemałym zaskoczeniem dla autora była jednak struktura odczuć „pozytywnych". Według deklaracji dużej części respondentów, oglądanie zdjęć i filmów pornograficznych nie robi na nich żadnego wrażenia, ponieważ jest to „normalka" (21,5%) lub są oswojeni z tą problematyką (14%). Natomiast ósma część dziewcząt i chłopców stwierdziła odczuwanie przyjemności z tego faktu. W grupie tej znalazło się 78 chłopców i 14 dziewcząt. Ze względu na deklaratywny charakter badań oraz anonimowość przeprowadzonych badań ankietowych można było spodziewać się pewnej liczby wpisów nie w pełni odpowiadających rzeczywistym odczuciom młodzieży. Jednakże przedstawione powyżej liczby powinny zmusić rodziców, wychowawców i wszystkich zainteresowanych pracą wychowawczą do głębszej zadumy nad tym problemem.

[14] Wartość procentowa obliczana dla liczby osobników danej płci, którzy odpowiedzieli na pytanie.



Rysunek nr 3. Odczucia młodzieży po obejrzeniu materiałów pornograficznych (opinie 744 osób)

Źródło: opracowanie własne

Zagrożeń związanych z korzystaniem z sieci internetowej należy jednak upatrywać także w tym, iż sama młodzież swoim zachowaniem także generuje możliwość ich powstawania. W świecie wirtualnym dzieci i młodzież przybierają nowe tożsamości, a nawiązując nowe kontakty zwykle posługują się pseudonimami. Często eksperymentują z autoprezentacją w sieci. Hamulce narzucone zazwyczaj przez wiek, płeć, wygląd zewnętrzny czy choćby określoną rolę społeczną tutaj przestają działać, a tożsamość internauty staje się płynna.[15] Z tych to m.in. powodów, a także z braku świadomości potencjalnych konsekwencji, młodzi użytkownicy sieci internetowej podejmują wysoce ryzykowne czynności, takie, jak np.: wysyłanie adresów e-mail, zdjęć, numerów telefonów, a nawet adresów zamieszkania nieznanym bliżej osobom.

W przeprowadzonych badaniach, 54,3% chłopców i 43% dziewcząt przyznało się do kilkakrotnego wysłania adresu e-mail osobom znanym sobie tylko z Internetu, swoje zdjęcie przesyłało co najmniej jeden raz aż 41,1% chłopców i niemal 40% dziewcząt, natomiast numer telefonu odpowiednio 40,6% chłopców i 35,5% dziewcząt. Szczególny niepokój budzi jednak to, że do nieznanych sobie osób 12,6% chłopców oraz 9,6% dziewcząt uczestniczących w badaniach przynajmniej jeden raz wysyłało adres swojego miejsca zamieszkania. O ile w trzech pierwszych przypadkach w grę wchodzić mogą zagrożenia o charakterze wirtualnym, takie jak np: wysyłanie niepożądanych treści, wykorzystanie zdjęć i/lub telefonów do działań niezgodnych z prawem, itp., o tyle w odniesieniu do adresu zamieszkania istnieją realne zagrożenia wynikające z bezpośredniego kontaktu ewentualnego sprawcy przestępstwa z jego ofiarą.

W większości przypadków spotkania w świecie rzeczywistym z osobami poznanymi w Internecie to spotkania rówieśników. Na szczególne podkreślenie zasługuje jednak fakt ujawniony w naszych badaniach, iż prawie 11% chłopców i 7,4% dziewcząt, spośród deklarujących uczestniczenie w takich spotkaniach, w rzeczywistości spotkało się z osobami dorosłymi. Są to zdecydowanie

[15] por.: L.J. Gurak, Cyberliteracy: *Navigating the Internet with awareness*, Yale University Press. New Haven, CT, 2001, oraz K.Y.A. McKenna, J.A. Bargh, *Plan 9 from cyberspace: The implications of the Internet for personality and social psychology* (w:) „Personality and Social Psychology Review", 2000, nr 4 (1), s. 57-75

niepokojące dane, ponieważ 25 chłopców i 14 dziewcząt z badanej populacji potencjalnie mogło mieć bezpośredni kontakt z osobami wykazującymi skłonności pedofilskie. Wprawdzie nie posiadamy informacji o przebiegu tych spotkań, ani o treści prowadzonych rozmów, to jednak sam fakt wystąpienia takich sytuacji zmusza do zastanowienia i podjęcia działań uświadamiających młodych ludzi o możliwości wystąpienia określonych zagrożeń.

Biorąc pod uwagę pełną analizę wyników przeprowadzonych badań autor stwierdził, iż w badanej populacji występuje:

- realne zagrożenie nieletnich niekontrolowanym dostępem do treści agresywnych i pornograficznych;
- niski poziom wiedzy na temat zasad bezpiecznego korzystania z usług internetowych;
- niski poziom wiedzy na temat instytucji mogący podjąć interwencję w przypadkach łamania prawa przez użytkowników Internetu;
- brak dostatecznej kontroli użytkowania przez nieletnich komputera osobistego oraz Internetu;
- brak znajomości zasad bezpiecznego korzystania z Internetu ze strony rodziców i opiekunów;
- generowanie potencjalnego zagrożenia związanego z użytkowaniem Internetu przez znaczną część uczestniczącej w badaniach młodzieży;
- zubożenie psychiki znacznej części młodzieży, rozpatrywane w kategoriach moralnych i emocjonalnych, a także więzi społecznych.

Jeżeli nawet nie wszystkie deklaracje respondentów są odzwierciedleniem ich rzeczywistych postaw i potencjalnych zachowań, to i tak uwidocznionych zostało wiele problemów, z którymi muszą się zmierzyć rodzice, szkoły oraz instytucje państwowe i organizacje społeczne mogące wpływać na poziom kształcenia i wychowania młodego pokolenia. Niezbędne są natychmiastowe działania zmierzające do uświadomienia młodzieży i rodzicom (opiekunom) realnych zagrożeń wynikających z korzystania z globalnej sieci informatycznej, wdrożenia umiejętności bezpiecznego korzystania z jej usług oraz przeciwdziałania patologiom w niej występującym.

Łatwość dostępu i pozyskania zdjęć i filmów pornograficznych jest poważnym wyzwaniem dla administratorów sieci internetowej i osób starających się powstrzymać rozwój tego procederu. Ogromną rolę w zwalczaniu przestępczości internetowej, dotyczącej zwłaszcza treści pornograficznych oraz wykorzystania seksualnego dzieci i młodzieży, odgrywa również Policja i organizacje pozarządowe monitorujące Internet.

Oprócz codziennej pracy operacyjnej i dochodzeniowej Policja realizuje szereg projektów zmierzających do pozyskiwania informacji na temat omawianej powyżej działalności przestępczej. Jednym z nich jest realizowany przez Wyższą Szkolę Policji we współpracy z innymi instytucjami podległymi Ministerstwu Spraw Wewnętrznych i Administracji projekt badawczo-rozwojowy,[16] w którego ramach trwają prace nad powołaniem do życia tzw. „Wirtualnego Komisariatu". Celem tego przedsięwzięcia jest m.in. monitorowanie zagrożeń wynikających z rozwoju

[16] Projekt badawczo-rozwojowy nr OR00004007 pt. „*Przeciwdziałanie i zwalczanie przestępczości zorganizowanej i terroryzmu w warunkach bezpiecznego, przyśpieszonego i zrównoważonego rozwoju społeczno-gospodarczego",* WSPol. Szczytno 2009

technologicznego oraz stworzenie możliwości powiadamiania organów ścigania przestępstw o naruszeniu zasad prawnych lub etycznych funkcjonowania społeczeństwa.

Zwalczanie przestępczości związanej z wykorzystywaniem seksualnym dzieci i młodzieży oraz pornografii dziecięcej jest niezwykle trudne i wiąże się z potrzebą podjęcia działań systemowych ukierunkowanych na rozpoznawanie i skuteczne jej zwalczanie. Z punktu widzenia proceduralnego, utrudnienia związane są przede wszystkim z międzynarodowym charakterem tego rodzaju przestępczości, złożoności procesu wykrywczego, sposobu uzyskiwania i gromadzenia materiału dowodowego a także specyficznego postępowania z pokrzywdzonymi i świadkami. Nie ulega wątpliwości, że oprócz konieczności systematycznego doskonalenia bazy legislacyjnej niezbędne jest także zintensyfikowanie współpracy instytucji i organizacji publicznych z organizacjami pozarządowymi i podmiotami prywatnego sektora finansowego. Ze względu na międzynarodowy charakter wymienionego rodzaju przestępczości oraz potrzebę zwiększenia efektywności podejmowanych działań niezbędne jest także współdziałanie służb i instytucji zarówno 27 krajów członkowskich Unii Europejskiej, jak i ścisła współpraca z podobnymi podmiotami państw sąsiadujących z zewnętrznymi granicami Unii od strony wschodniej, tj. z Ukrainą, Mołdawią i Białorusią. Jest to zresztą zgodne z priorytetami Ministerstwa Spraw Wewnętrznych i Administracji zawartymi w Programie Partnerstwa Wschodniego.[17]

Problematykę wykorzystywania seksualnego dzieci oraz pornografii dziecięcej zawiera także Program Sztokholmski,[18] w którym czytamy, iż *ochrona dzieci przed niebezpieczeństwem niegodziwego traktowania w celach seksualnych jest ważnym elementem strategii na rzecz ochrony praw dziecka* (pkt 4.4.3) Ponadto, w Konkluzjach Rady Unii Europejskiej w sprawie europejskiej koalicji finansowej oraz krajowych koalicji finansowych przeciwko pornografii dziecięcej w Internecie[19] sformułowano apel Rady UE do państw członkowskich i Komisji Europejskiej w sprawie podejmowania wysiłków mających na celu zwalczanie dystrybucji treści pedofilskich przy jak najszerszej współpracy z sektorem finansowym i zaangażowaniu podmiotów gospodarczych. W dokumencie tym stwierdzono także, że zwiększenie skuteczności prowadzenia dochodzeń i ścigania wymienionych przestępstw wymaga udostępnienia odpowiednim służbom skutecznych narzędzi dochodzeniowych, przynajmniej w sprawach związanych z wykorzystaniem technologii informatyczno-komunikacyjnych. Zdaniem autorów „Konkluzji" mogą one uzyskać postać np. operacji pod przykryciem, kontrolę komunikacji, niejawną inwigilację (w tym także elektroniczną), monitorowanie rachunków bankowych oraz inne metody dochodzenia finansowego.[20]

Z tego punktu widzenia, jednym z narzędzi do walki z rozpowszechnianiem pornografii dziecięcej może stać się blokowanie dostępu do stron internetowych.

---

[17] *http://www.msz.gov.pl/files/PARTNERSTWO%20WSCHODNIE/Eastern%20Partnership%20Partnerstwo%20Wschodnie%20en%20pl.pdf*

[18] *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:pl:PDF*, s. 22, (pobrano 20.04.2011)

[19] *www.consilium.europa.eu/uedocs/NewsWord/PL/jha/111120.doc*, (pobrano 20.04.2011); *por: http://register.consilium.europa.eu/pdf/pl/09/st11/st11456-re02.pl09.pdf*, (pobrano 20.04.2011)

[20] Ibidem

Rozwiązanie takie wprowadziło już kilka państw członkowskich Unii Europejskiej. Należą do ich m.in. Szwecja, Finlandia, Dania, Norwegia, Szwajcaria, Włochy oraz Malta. Działania te podejmowane są po dokładnym przeanalizowaniu problemu i w ścisłej zgodności z obowiązującym prawem, a także w oparciu o inicjatywę CIRCAMP (*Cospol Internet Related Child Abusive Material Project*)[21] propagującą mechanizm zgłaszania i blokowania stron z pornografią dziecięcą.

Według analiz przeprowadzonych przez KG Policji w oparciu o doświadczenia krajów Unii Europejskiej można wnioskować o *braku centralnego mechanizmu dystrybucji informacji o blokowanych stronach internetowych*.[22] Każdy z krajów realizujących system blokady dostępu wdraża własne rozwiązania i mechanizmy dystrybucji informacji dla dostawców telekomunikacyjnych. Wiąże się z tym jednak brak jednolitego zakresu przetwarzanych danych. Dlatego też Biuro Kryminalne KGP zainicjowało przedsięwzięcie mające na celu stworzenie ujednoliconych mechanizmów i algorytmów postępowania dotyczących blokowania stron internetowych zawierających pornografię dziecięcą.[23] Podstawą inicjatywy jest zebranie kluczowych informacji dotyczących problematyki zwalczania wykorzystywania seksualnego dzieci i pornografii dziecięcej w cyberprzestrzeni w krajach członkowskich UE i wybranych krajach Partnerstwa Wschodniego za pomocą specjalnie przygotowanego kwestionariusza. Wyniki analiz uzyskanych danych zostaną opublikowane w postaci „Konkluzji Rady" i przedstawione na forum grupy roboczej w drugiej połowie bieżącego roku.[24]

Zdaniem autorów inicjatywy, skutkiem podjętych działań powinno być utworzenie centralnego rejestru usług niedozwolonych, którego administratorem będzie EUROPOL, standaryzacja zasad zasilania rejestru danymi z poszczególnych krajów oraz określenie wspólnego formatu zgłaszania blokowania stron internetowych. Ponadto, zakłada się opracowanie optymalnego rozwiązania blokowania dostępu do treści pornograficznych z udziałem dzieci w Internecie w oparciu o istniejące już systemy i doświadczenia, zmniejszenie liczby stron internetowych z pornografią dziecięcą, a także nawiązanie bezpośredniego kontaktu i współpracy pomiędzy funkcjonariuszami zajmującymi się zwalczaniem wymienionej przestępczości w państwach członkowskich Unii Europejskiej oraz wybranych krajach programu Partnerstwa Wschodniego.[25]

Wszystkie wyżej wymienione przedsięwzięcia powinny w znaczącym stopniu przyczynić się do ograniczenia możliwości kontaktu internautów z treściami o charakterze pornografii dziecięcej, zwiększenia efektywności działań prewencyjnych i procesów wykrywczych dotyczących przestępczości związanej z wykorzystywaniem seksualnym dzieci a tym samym zmniejszenia zagrożeń dla nieletnich płynących z Internetu.

---

[21] Por: *www.circamp.eu; http://ec.europa.eu/information_society/apps/projects/factsheet/index.cfm?project_ref=SIP-2007-TN-140701; http://www.terena.org/activities/tf-csirt/meeting24/kripos-circamp.pdf*, (pobrano 20.04.2011)

[22] Projekt BK KGP „Zwalczanie wykorzystywania seksualnego dzieci i pornografii dziecięcej w cyberprzestrzeni – współdziałanie służb i instytucji w krajach członkowskich UE oraz wybranych krajach programu Partnerstwo Wschodnie", 2011

[23] Ibidem

[24] Ibidem

[25] Ibidem

Mirosław BORKOWSKI
Wyższa Szkoła Bezpieczeństwa w Poznaniu
Wydział Zamiejscowy w Gdańsku

BEZPIECZEŃSTWO PRAW AUTORSKICH W INTERNECIE

Rozwój nowoczesnych technologii, w tym niezwykły wręcz rozwój Internetu sprawia, że w konfrontacji techniki z prawem, w wielu wypadkach systemy prawne a przede wszystkim systemy ochrony praw są często bezradne. Ochrona podstawowych praw obywateli w takich przypadkach jest utrudniona. Podobnie jest w przypadku ochrony praw autorskich w Internecie. Przeglądając strony internetowe, śledząc różnego rodzaju wpisy użytkowników komunikatorów społecznych itp., zauważamy, że np. ustalenie autora niektórych wpisów jest wręcz niemożliwe. Można odnieść wrażenie, że cyberprzestrzeń[1] rządzi się swoimi prawami, które nie zawsze zgodne są z „prawem pisanym" funkcjonującym poza tym obszarem.

Wpływ Internetu na coraz większą liczbę dziedzin życia, a przede wszystkim rozwój różnego rodzaju przestępstw elektronicznych dokonywanych za jego pośrednictwem, zmusza do wprowadzania zabezpieczeń, zarówno technologicznych jak i prawnych. Należy też zdawać sobie sprawę, że proces regulacji prawnych, systemowych nigdy nie będzie nadążał za rozwiązaniami technicznymi. Wprowadzenie nowych zabezpieczeń będzie powodowało uruchomienie nowych procesów mających na celu „złamanie zabezpieczeń" lub „obejście prawa".

Od wielu już lat proponuje się wprowadzenie wspólnych zasad dotyczących funkcjonowania Internetu, zapewnienia i zabezpieczenia ochrony praw jego użytkowników. Zwolennikom wprowadzenia tego typu regulacji twierdzących, że ustalenie wspólnych zasad pozwoli między innymi na „zapewnienie praw użytkowników i ukształtowanie odpowiedzialności poszczególnych ich grup w sposób pewny i jednolity"[2] należy przyznać rację. Należy jednak skonstatować, że jest to zadanie niezwykle trudne. Może się również okazać, że przy tak olbrzymiej ilości użytkowników takiej różnorodności kulturowej i rozwarstwieniu społecznym będzie to zadanie awykonalne.

Inną drogą prowadzącą do poprawy bezpieczeństwa użytkowników Internetu, do ochrony praw, w tym praw autorskich w Internecie są wszelkiego rodzaju działania zmierzające do poprawy świadomości i kultury prawnej podmiotów uczestniczących w tym globalnym zjawisku (co również jest zadaniem niezwykle trudnym, być może trudniejszym niż stworzenie „dobrego prawa").

---

[1] Cyberprzestrzeń to pojęcie funkcjonujące w słownictwie od 1984 roku, kiedy to W. Gibson użył go w swojej powieści *„Neuromancer".* Obecnie funkcjonuje kilka definicji tego terminu. Najczęściej pod tym pojęciem kryje się swoista przestrzeń elektroniczna powstała w wyniku połączenia ze sobą komputerów. W literaturze prawniczej można znaleźć definicję cyberprzestrzeni, według której jest to „pojęcie używane do określenia wspólnej płaszczyzny wymiany informacji przez wszystkich użytkowników sieci globalnej. Jej specyficzna cecha jest aterytorializm – nie ma ona żadnego fizycznego desygnatu, w przeciwieństwie do przestrzeni znanych prawu międzynarodowemu w jego dotychczasowym kształcie" (w:) J. Kulesza: *Międzynarodowe prawo Internetu*. Poznań 2010, s. 55

[2] Op. cit., s. 11

Na dzień dzisiejszy należy przyjąć, że Internet, z uwagi na swój międzynarodowy charakter, nie daje się zamykać w ramach krajowych systemów prawnych.

Powszechnie Internet kojarzony jest z możliwością przeglądania różnego rodzaju stron www (*World Wide Web*). Należy przyjąć, że jest to najpopularniejsze zastosowanie Internetu. Nie jest to jednak funkcja, za pomocą której należy definiować to zjawisko. Internet to *ogólnoświatowa sieć komputerowa*,[3] to „*ogólnoświatowy, dynamicznie rozwijający się system powiązanych sieci komputerowych, który oferuje wiele usług takich jak: zdalne logowanie się użytkowników, przesyłanie plików, poczta elektroniczna, World Wide Web (WWW) i grupy dyskusyjne. Opiera się na protokole TCP/IP (…).*[4]

Do dnia dzisiejszego nie istnieje żadna wiążąca, międzynarodowa definicja tego zjawiska. Można więc przyjąć – i tak uczyniono na potrzeby niniejszej pracy – że Internet to *globalny system wymiany danych, funkcjonujący w oparciu o wzajemnie połączone sieci lokalne, rozmieszczone w wielu fizycznych lokalizacjach, umożliwiający jednoczesną, wielopłaszczyznową interakcję użytkowników z całego świata.*[5] Przez „wielopłaszczyznową interakcję" należy rozumieć zarówno możliwość tworzenia stron *www* i ich przeglądania, pozyskiwanie informacji, przesyłanie poczty elektronicznej czy możliwość wymiany obrazów, dźwięków, itp. Nie bez znaczenia jest również możliwość dokonywania zakupów a coraz większą popularność zdobywają wszelkiego rodzaju komunikatory społecznościowe. Czynności te zostały tu podane jedynie przykładowo, trudno jest bowiem dokładnie określić możliwości Internetu, które nieustannie zmieniają się, rozwijają i są ściśle powiązane z postępem technologicznym.

Przy tak obszernym zakresie przedmiotowym, możliwości dokonywania wielu czynności, w tym czynności prawnych, mogą się pojawić i pojawiają się problemy prawne. Wystarczy zasygnalizować problemy związane z wolnością słowa, z regulacjami dotyczącymi tzw. e-handlu, ochroną korespondencji, naruszaniem dóbr osobistych w Internecie czy naruszaniem praw autorskich.

Rozwój Internetu, z jednej strony przyczynił się do wzrostu liczby osób, które umieszczają „w sieci" różnego rodzaju utwory – często będąc nieświadomymi przysługujących im praw; z drugiej strony Internet umożliwia niekontrolowane korzystanie z dóbr intelektualnych. W literaturze przedmiotu mowa jest o co najmniej kilku problemach prawnych związanych z taką sytuacją. W związku z zakresem niniejszego artykułu należy podkreślić przede wszystkim konieczność zmian przepisów dotyczących ochrony praw autorskich i pokrewnych, szeroko rozumianego prawa medialnego, prawa znaków towarowych i własności przemysłowej.

---

[3] S. Dubisz: (red) *Uniwersalny słownik języka polskiego*, t 2. Warszawa 2003, s. 127, hasło: Internet

[4] Jest to fragment definicji podanej przez Bryana Pfaffenberga. Taka definicja znajduje się na stronie internetowej: http://czytelnia.pwn.pl. Jednak na stronie tej nie ma przywołanego źródła tj. tytułu pracy, w której została podana ta definicja. Można dowiedzieć się jedynie, że przytoczona definicja znajduje się w książce *Komunikacja językowa w Internecie.* Na przywołanej stronie znajduje się jedynie nazwisko J. Grzenia, jednak nie ma wyraźnego sygnału, czy jest to nazwisko autora książki czy autora wpisu na stronie internetowej

[5] J. Kulesza: *Międzynarodowe*…, s. 57

Według J. Barta i R. Markiewicza najważniejszymi problemami powstającymi na styku wykorzystywania Internetu i praw autorskich są:

a) wątpliwości towarzyszące oznaczeniu jurysdykcji i prawa właściwego ze względu na czynności faktyczne i prawne dokonywane w Internecie (…);
b) trudności wytyczenia ochrony autorskoprawnej w sieciach komputerowych (…);
c) zasadnicza zmiana dotychczasowych paradygmatów działalności wydawniczej w kontekście rozpowszechniania utworów w sieciach komputerowych (…);
d) wykorzystanie nowoczesnej techniki informacyjnej w zakresie zarządzania (także zbiorowego) prawami autorskimi i pokrewnymi".[6]

Nie wszystkie wyżej wymienione grupy problemów, również z uwagi na ograniczenia edytorskie, będą poddane analizie w dalszej treści artykułu. Szczególna uwaga zostanie skierowana na zagadnienie podmiotu praw autorskich zwłaszcza w przypadku tzw. „autorstwa zbiorowego" oraz na ochronę praw autorskich przy zastosowaniu systemu odesłań (linków). Zasygnalizowany zostanie również problem kopiowania stron internetowych.

Istniejąca już od 10 lat[7] Wikipedia nie jest jedynym produktem[8] tego typu, jednak to na jej przykładzie zobrazowany zostanie problem „autorstwa zbiorowego". Zgodnie z tekstem informacji znajdującej się na stronie: http://pl.wikipedia.org/wiki/Wikipedia[9] wikipedia *to wielojęzyczny projekt internetowej encyklopedii działającej na zasadzie otwartej treści. Funkcjonuje wykorzystując oprogramowanie MediaWiki (…) umożliwiające edycje każdemu użytkownikowi odwiedzającemu stronę i aktualizację jej treści w czasie realnym.* Jej sloganem reklamowym jest hasło „Wolna encyklopedia, którą każdy może redagować".

I właśnie ta, niewątpliwie szczytna idea, jest źródłem wielu problemów, w tym problemów prawnych.

Skoro specyfiką tego „kosmicznego kompendium"[10] uznanego za „wzorową społeczność internetową"[11] jest możliwość tworzenia, edytowania, opracowywania oraz uzupełniania i kasowania haseł czy ich fragmentów przez wszystkich jej użytkowników, rodzi się problem autorstwa wpisu. Sytuację taką coraz częściej w literaturze nieprawniczej określa się mianem „autorstwa zbiorowego", „kolektywnego" czy „autorstwa otwartego".[12] Określenia takie nie mieszczą się jednak w zakresie pojęć prawnych zawartych w ustawie z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (tekst jednolity: Dz. U z 2006 r. Nr 90,

---

[6] J. Barta, R. Markiewicz: *Prawo autorskie*. Warszawa 2010, s.298-299

[7] Wikipedia powstała 15 stycznia 2001 r., strona *http://pl.wikipedia.org/wiki/Wikipedia* (pobrano 20.03.2011 r.)

[8] Op. cit. Na przywołanej stronie w zakładce „Inne encyklopedie internetowe" wymienione są encyklopedie: *Stanford Encyklopedia of Philosophy, h2g2, Everything2* czy nieistniejąca już *Nupedia*. Do projektów podobnych w swym funkcjonowaniu do Wikipedii zalicza się jeszcze: *Susning.nu., Wnciclopedia Libre, WikiZnanie, Wikicytaty, Wikibooks, Wikiźródła, Wikimedia Commons* czy *Wikiversity*

[9] Op. cit. (odczyt: 20.03.2011)

[10] Op. cit.

[11] Op. cit.

[12] M. Jankowska: *Autorstwo „zbiorowe" na przykładzie Wikipedii* (w:) Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z prawa Własności Intelektualnej, z. 4/2010, s.24 i literatura tam przytoczona

poz. 631 z późn. zm. dalej: PrAut.), ani w ustawodawstwie unijnym dotyczącym prawa autorskiego.

Autorzy tekstów nieprawniczych opisujących zasady funkcjonowania Internetu, w tym Wikipedii, dokonują klasyfikacji osób mających wpływ na jej kształt na: użytkowników zarejestrowanych, użytkowników anonimowych, boty[13], autorów zarejestrowanych oraz autorów anonimowych.[14] Należy pamiętać, że na ostateczny wygląd i zawartość hasła w Wikipedii maja wpływ również: administratorzy, biurokraci, checkuserzy i stewardzi.[15] I chociaż podział ten zapewne jest zrozumiały dla osób zainteresowanych funkcjonowaniem internetu, to dla prawa autorskiego nie jest pomocny. Dla prawa autorskiego istotny jest bowiem „przejaw działalności twórczej o indywidualnym charakterze" (art. 1 ust. 1 ustawy o prawie autorskim i prawach pokrewnych), niezależnie od funkcji, uprawnień czy nazwy poszczególnych osób.

Aby móc określić autora Wikipedii należy spróbować określić jej charakter prawny, wybrać prawo właściwe do przeprowadzenia takiej oceny. Z uwagi na dostępność do Internetu, do Wikipedii na całym świecie, nie jest to zadanie proste. Należy bowiem pamiętać, że większość serwerów obsługujących Wikipedię oraz jej zmiany znajduje się na Florydzie, jednak pojedyncze serwery zlokalizowane są we Francji, Holandii a nawet w Korei Południowej.[16] W takiej sytuacji rodzi się więc pytanie o właściwy wybór prawa potrzebnego do oceny sytuacji prawnej osób tworzących Wikipedię, a tym samym należy zastanowić się, według jakiego prawa będzie określane autorstwo oraz ochrona praw autora. Teoretycznych możliwości jest kilka: prawo amerykańskie – z uwagi na największe nagromadzenie serwerów; prawo państwa, w którym znajduje się serwer „obsługujący" wprowadzane czy poprawiane hasło; w końcu – prawo według statusu personalnego osoby tworzącej (celowo nie używam określenia „autor"). Do tej pory problemy te nie zostały rozstrzygnięte. Można jedynie wspomnieć, że w literaturze (głównie nieprawniczej) problem ten jest przedstawiany w sposób zróżnicowany.[17]

Z uwagi na brak jednolitych regulacji prawnych tego zagadnienia w prawie zarówno unijnym jak i w konwencjach międzynarodowych, dalszy ciąg rozważań oparty będzie przede wszystkim na naszej ustawie o prawie autorskim i prawach pokrewnych. Warto więc przypomnieć kilka definicji, które są niezbędne by móc określić charakter prawny tego zjawiska. Należy również poddać analizie zakres niektórych pojęć mogących przyczynić się do lepszego zrozumienia omawianego zagadnienia.

---

[13] Op. cit. s. 24

[14] Op. cit. s. 25

[15] Op. cit. s. 25. Mianem *administratorów*, w cytowanej pracy, określa się „użytkowników mających np. możliwość edycji stron całkowicie zabezpieczonych, zmiany stopnia zabezpieczenia strony, cofania zmian strony dokonanej w trakcie usuwania i przywracania stron oraz nadawania i odbierania uprawnień redaktora". *Biurokraci* to „użytkownicy mający uprawnienie do nadawania statusu administratora lub biurokraty innym użytkownikom „. *Checkuserzy* „mają uprawnienia do sprawdzania adresów IP zalogowanych użytkowników w celu wykrywania działań mających na celu niszczenie stron". Z kolei *stewardzi* to „użytkownicy mający uprawnienia do nadawania i odbierania statusu administratora, biurokraty oraz checkusera"

[16] Informacje ze strony internetowej*: http://pl.wikipedia.org/wiki/Wikipedia* (pobrano: 20.03.2011 r.)

[17] M. Jankowska: *Autorstwo…,* s.29-30 i literatura tam przytoczona

I tak, zgodnie z brzmieniem art. 1 ust. 1 ustawy o prawie autorskim i prawach pokrewnych, utworem jest *każdy przejaw działalności twórczej o indywidualnym charakterze, ustalonym w jakiejkolwiek postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia*.

Analizując formę i zakres Wikipedii można odnieść wrażenie, że jej charakter prawny zbliżony jest do: zbioru, bazy danych, utworu połączonego czy w ostateczności do utworu zbiorowego. Niestety, dokładna analiza definicji powyższych określeń skłania do konstatacji, że Wikipedii nie da się podporządkować żadnemu z nich.

Cechy utworu spełniają jedynie zbiory i bazy danych, o ile przyjęty w nich dobór, układ lub zestawienie ma twórczy charakter (art. 3 *PrAut*). Trudno jest znaleźć w Wikipedii cechy „mające twórczy charakter". Jest to, ogólnie rzecz ujmując, alfabetyczny wykaz pojęć wraz z objaśnieniami, wyjaśnieniami jakich wiele znajduje się w zarówno w wersji elektronicznej jak i drukowanej. Skoro więc Wikipedia nie jest zbiorem (w rozumieniu prawa autorskiego), nie spełnia cech utworu, to można pokusić się o stwierdzenie, że wpisy dokonywane przez jej „twórców" nie są chronione prawem autorskim.

Jeśli chodzi o „bazę danych" – jest to forma, która według wielu autorów jest formą najbardziej adekwatną.[18] Ustawa o prawie autorskim i prawach pokrewnych nie definiuje tego pojęcia dlatego też omawiając to zagadnienie bardzo często sięga się do dyrektywy 96/9/WE Parlamentu Europejskiego i Rady z dnia 11 marca 1996 roku w sprawie ochrony prawnej baz danych (Dz. Urz. UEL.1996.77.20), w której to, w art. 1 ust 2, zdefiniowano bazy danych jako *zbiór niezależnych utworów, danych lub innych materiałów uporządkowanych w sposób systematyczny lub metodyczny, indywidualnie dostępnych środkami elektronicznymi lub innymi sposobami.* Podobnie jak przy próbach określania Wikipedii jako „zbiór", również przypadek porównywania jej z „bazą danych" budzi wiele zastrzeżeń. Baza danych ma składać się między innymi z „niezależnych utworów", a cechy tej nie posiadają dokonywane tam wpisy. W literaturze przedmiotu[19] przyjmuje się, że przesłankami „twórczości" w przypadku baz danych są: systematyka i metoda zgromadzenia danych, twórczy wybór zawartości baz, twórcza forma jej przedstawiania. Żadnej z tych przesłanek nie spełnia Wikipedia.

Wiele utworów powstaje w wyniku połączenia kilku dzieł stworzonych odrębnie (najpopularniejszym przykładem takiego dzieła połączonego jest „poezja śpiewana"). Przesłankami powstania dzieła połączonego są: istnienie co najmniej dwóch odrębnych utworów; połączenie tych utworów; cel – jakim jest wspólne rozpowszechnianie (art. 10 *PrAut*). Warunkiem koniecznym powstania takiego utworu jest umowa zawarta przez twórców określająca zasady rozpowszechniania. Również w tym wypadku (podobnie jak przy analizie „zbioru" i „bazy danych") należy stwierdzić, że Wikipedia nie spełnia warunków uznania jej za „dzieło

[18] M. Jankowska: *Autorstwo…,* s. 31 i literatura tam przytoczona

[19] S. Stanisławska-Kloc: *Ochrona baz danych*, (w:) Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Wynalazczości i Ochrony Własności Intelektualnej, z. 82/2002, s. 66

połączone". Dodatkowo, nie spełnia pozostałych przesłanek tzn. brakuje zarówno zezwolenia jak i umowy zawartej przez wszystkich „twórców" określającej warunki rozpowszechniania. Warto też odnotować zdanie przedstawicieli nauki, zgodnie z którym połączenie utworów nie jest nową formą utworu, lecz jedynie rodzajem jego wykonania.[20]

Jak już zostało wcześniej przytoczone, Wikipedia określa się jako *wielojęzyczny projekt internetowej encyklopedii*, może więc należałoby ją traktować, w myśl regulacji zawartej w art. 11 *PrAut*, jako utwór zbiorowy. W ustawie stwierdzono bowiem, że rodzajem utworu zbiorowego jest encyklopedia. Jednak sama ustawa nie definiuje pojęcia „utwór zbiorowy". Zarówno w doktrynie, jak i w orzecznictwie można znaleźć definicje tego pojęcia. Według D. Sokołowskiej, „utworem zbiorowym" jest *utwór, na który składają się wybrane przez wydawcę (producenta) nie mniej niż dwa utwory pochodzące od różnych twórców oraz nietwórcze wkłady, połączone na zasadzie twórczego układu przez redaktora albo inną wskazaną przez wydawcę (producenta)*[21]. Z kolei, zgodnie z wyrokiem Sądu Apelacyjnego w Krakowie z 10 lutego 1995 roku (I ACr 722/94), wydanym w oparciu o art. 10 ustawy o prawie autorskim z roku 1952, utwór zbiorowy w rozumieniu powołanego przepisu *składa się z szeregu odrębnych części, które łączy w jedną całość działalność redaktorska, polegająca przede wszystkim na odpowiednim wyborze oraz układzie tych elementów. Założeniem utworu zbiorowego jest to, że poszczególne jego części są utworami poszczególnych autorów. Takimi utworami są np. encyklopedie, słowniki, księgi pamiątkowe, kalendarze*.

W obu przypadkach podkreśla się, że utwór zbiorowy ma być złożony z „utworów". Wybór utworów tworzących taki utwór uzależniony jest od decyzji wydawcy, bądź producenta a na ich układ ma wpływ *redaktor lub inna osoba wskazana przez wydawcę/producenta*. Specyfiką tworzenia stron Wikipedii jest możliwość ich tworzenia uzależniona głównie od aktywności i inwencji twórców. Z analizy informacji znajdujących się na internetowej stronie Wikipedii wynika, że większą wagę przykłada się do zabezpieczeń strony przed tzw. „wandalizmem" niż do kwestii związanych z szeroko rozumianą jakością, poprawnością edytorską itp. Brakuje również wyraźnie wyodrębnionego „zespołu redakcyjnego", koordynatora działań, który „scalałby" poczynania dokonujących wpisów bądź ich zmian w jedną, określoną formę. Owa otwartość Wikipedii, będąca niewątpliwą jej zaletą, działa jednak przeciwko uznaniu jej za utwór zbiorowy w rozumieniu prawa autorskiego.

Kolejnego argumentu przemawiającego przeciwko uznaniu Wikipedii za utwór zbiorowy dostarcza niepublikowany wyrok SN z dnia 7.05.1968 roku, zgodnie z którym *wydawnictwo jest zobowiązane do zorganizowania fachowego zespołu osób dokonujących zarówno oceny całości jak i prac redakcyjnych i adjustacyjnych*.[22] Z cytowanego wyroku jednoznacznie wynika, że podstawą stworzenia utworu zbiorowego jako całości jest praca „fachowego zespołu", a w przypadku Wikipedii – *tworzą ją użytkownicy odwiedzający stronę i aktualizujący jej treść w czasie realnym*. Nawet przy założeniu, że takimi

[20] M. Jankowska: *Autorstwo…,* s. 31 i literatura tam przytoczona
[21] D. Sokołowska: *Utwory zbiorowe w prawie autorskim* (w:) Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Wynalazczości i Ochrony Własności Intelektualnej", z. 76/2001 r., s. 142
[22] M. Janowska: *Autorstwo…,* s. 30 i literatura tam przytoczona

„tworzącymi użytkownikami" są osoby posiadające ogromną wiedzę na dany temat, eksperci, to i tak nie można uznać ich za zespół tworzący „utwór zbiorowy".

Podsumowując, rozważania dotyczące charakteru prawnego Wikipedii należy przytoczyć jeszcze jeden wyrok Sądu Apelacyjnego w Warszawie z dnia 11 stycznia 2005 roku (sygn. akt I ACa 154/2004), zgodnie z którym: *znamion intelektualnej twórczości nie można się dopatrywać w doborze materiałów, informacji, danych, gdy taki dobór jest całkowicie zdeterminowany celem zbioru lub gdy ma charakter oczywisty. Dzieło będące wynikiem pracy rutynowej bądź rezultatem możliwym do osiągnięcia przez osoby podejmujące się tego samego zadania, nie ma charakteru twórczego*.[23]

Kształt Wikipedii i jej struktura pozwalają na rozpatrywanie zagadnień autorstwa na dwóch płaszczyznach. Autorstwa Wikipedii jako całości oraz autorstwa poszczególnych haseł. Sposób tworzenia haseł, ich ciągłe zmiany i modyfikacje, nie tylko rodzi problem należytego określenia twórców ale dodatkowo – w świetle regulacji prawa autorskiego – uniemożliwia właściwe zakwalifikowanie tych czynności.

Należy stwierdzić, że taka forma tworzenia haseł nie spełnia wymogów współautorstwa przynajmniej z dwóch powodów. Po pierwsze, zgodnie z brzmieniem art. 9 *PrAut* – o współautorstwie można mówić w przypadku „utworu", a za taki nie można uznać ani Wikipedii ani poszczególnych jej haseł; po drugie – z uwagi na brak wyraźnego porozumienia i współpracy pomiędzy osobami dokonującymi kolejnych wpisów. Ustawa nie wymaga zachowania jakiejś szczególnej formy konsensusu, wystarczy, że owo porozumienie będzie miało charakter faktyczny, dorozumiany. Współtwórczość, przy tworzeniu haseł, należy jednak rozpatrywać w kontekście uzasadnienia wyroku SN z dnia 5 lipca 2002 roku (III CKN 1096/00), w którym to między innymi stwierdzono, że *techniczny i pomocniczy udział w powstawaniu dzieła (…) nie daje podstaw do uznania ich za współtwórców*, i dalej *jedynie przejawy działalności twórczej o indywidualnym charakterze mogą być uznane za dzieła i podlegają ochronie prawa. Chodzi zatem o kreacyjny, subiektywnie nowy, oryginalny wytwór intelektu, wywołany niepowtarzalną osobowością twórcy, który – wykonany przez kogoś innego – wyglądałby inaczej*. W dalszej części przywoływanego uzasadnienia stwierdzono, że *współtwórczość w rozumieniu Prawa autorskiego nie zachodzi, gdy współpraca określonej osoby nie ma charakteru twórczego, lecz pomocniczy, chociażby umiejętność wykonywania czynności pomocniczych wymagała stopnia wiedzy fachowej, zręczności i inicjatywy osobistej*.

Od 15 czerwca 2009 roku tj. od dnia obowiązywania licencji CC-BY-SA 3,0[24] nie istnieje problem kopiowania, rozpowszechniania czy modyfikowania treści artykułów zamieszczonych w Wikipedii. Umożliwia ona bowiem dokonywanie wszystkich tych czynności przy zachowaniu prawa autorskiego do tekstu pierwotnego. Problemem może być jednak rozróżnienie pomiędzy „autorem pierwszym" i „autorem drugim", który uzupełnia utwór lub jego fragment stworzony wcześniej.[25] Można wyobrazić sobie sytuację, w której jeden z uzupełniających hasło podaje informacje bądź cytuje inną osobę „A" bez podawania źródła.

[23] LexPolonica Maxima nr dok. 376270
[24] Tekst licencji znajduje się m.in. na stronie *www.wikipedia.org/wiki/Wikipedia* (pobrano 20.03.2011 r.)
[25] Porównaj J. Barta (w:) M. Jankowska: *Autorstwo…,* s. 33

Sytuację komplikuje fakt, iż osoba „A" zamieszczając dowolny tekst również popełniła plagiat, podając jak swój tekst osoby „Z". Rodzi się pytanie o zakres odpowiedzialności osoby „A" jak i osoby dokonującej wpisu na stronie Wikipedii. Z technicznego punku widzenia sprawa może okazać się bardzo prosta, bowiem system identyfikacji użytkowników umożliwi dokładne określenie kiedy, z którego komputera i np. z jakiego miejsca na Ziemi, wprowadzane były zmiany, dokonywano modyfikacji tekstu.

Nie zmieni to jednak sytuacji, w której bardzo często nieświadomie, zostaną naruszone czyjeś prawa autorskie. Nie sprawi też, że zniknie problem odpowiedzialności za naruszenie tych praw.

Kwestia naruszenia praw autorskich, a tym samym ich bezpieczeństwa w Internecie wiąże się z zagadnieniem odesłań tzw. linków. Problem ten był i jest dostrzegany zarówno przez praktyków jak i teoretyków prawa.[26] Należy stwierdzić, że co do zasady sam system odesłań do innych zbiorów znajdujących się w Internecie nie stanowi naruszenia prawa, w tym prawa autorskiego. Nie wdając się w techniczne szczegóły funkcjonowania i identyfikacji zasobów w Internecie należy wspomnieć jedynie o zasadzie działania i typologii odesłań.

O tym jak funkcjonuje system odesłań zapewne wie każdy kto choć raz zetknął się z Internetem i próbował znaleźć interesujące go informacje. Każdy użytkownik intuicyjne potrafi wyjaśnić zasady funkcjonowania tego zjawiska, bez którego Internet nie nabrałby takiego znaczenia i nie zaistniał w obecnym kształcie. W literaturze przedmiotu[27] odesłanie internetowe określa się *jako połączenie pochodzące z jednego zasobu dostępnego w ramach WWW do innego zasobu. Składa się z dwóch punktów zaczepienia – „kotwic" (ang. anchor) oraz kierunku. Kierunek wskazuje „drogę" od wyjściowego punktu zaczepienia, czyli zasobu, z którego użytkownik jest odsyłany do docelowego punktu zaczepienia, czyli zasobu, do którego odesłanie ma doprowadzić użytkownika".*

W zakresie typologii powszechnie[28] przyjmuje się istnienie: odesłań zwykłych (ang. *surface links*), odesłań głębokich (ang. *deep links*), odesłań wbudowanych (ang. *hotlinks*). Z systemem odesłań bezpośrednio związane jest stosowanie ramek (ang. *framing*).

Najmniej wątpliwości budzi kwestia odesłań zwykłych które polegają na bezpośrednim odesłaniu do innej strony głównej. Na zasadzie przeciwstawienia do odesłań zwykłych funkcjonuje instytucja odesłań głębokich. Każdy korzystający z Internetu zapewne spotkał się z sytuacją, w której aby móc odszukać interesującą go stronę czy informację, musiał nawet kilkakrotnie aktywować inne strony, z których to dopiero następowało odesłanie do tej strony właściwej. Taka sytuacja w literaturze określana jest w sposób niejednorodny, może to być nazwane odesłaniem: *do strony zależnej*, *>>stron wewnętrznych<< adresata*, *do stron położonych głębiej* czy wreszcie *do stron z cudzą ofertą.*[29]

---

[26] Duży wykaz literatury prawniczej zajmującej się tym zagadnieniem znajduje się w artykule autorstwa B. Widła, *Odpowiedzialność za naruszenie majątkowych praw autorskich przez stosowanie odesłań (linków) internetowych,* (w:) Zeszyty Naukowe Uniwersytetu Jagiellonskiego. Prace z Prawa Własności Intelektualnej, z. 4/2010, s. 51

[27] Op. cit. s. 52-53

[28] Porównaj: B. Widła: *Odpowiedzialność…,* s. 53; J. Kulesza, *Międzynarodowe…,* s. 81; J. Barta, R. Markiewicz, *Prawo* …, s. 307

[29] Wszystkie przywołane określenia pochodzą z: B. Widła, *Odpowiedzialność…,* s. 54 i literatura tam przytoczona

Ciekawą kategorię odesłań stanowią odesłania wbudowane tzw. *hotlinki.* Stanowią one „swoiste hiperłączenie", które polega na udostępnieniu rysunku lub tekstu bez opuszczenia strony pierwotnej, przy czym te „obce dokumenty" zostają „zintegrowane" ze stroną, z której użytkownik korzysta.[30] Na stronie Wikipedii – hasło „hotlink"[31] znajduje się definicja w brzmieniu: *to technika budowania serwisu internetowego w oparciu o zasoby należące do innych serwisów. Mowa tutaj o zajmujących przepustowość i miejsce na serwerze plikach multimedialnych, plikach graficznych, plikach archiwalnych lub programach komputerowych*.

Odmianą odesłań jest „ramkowanie" (*ang. framing*), które polega na łączeniu się jednej strony internetowej (podstawowej, oryginalnej) za pomocą *hiperlinka* z inną stroną internetową w taki sposób, że na oryginalnej stronie pojawia się ona w środku ramki. Taka sytuacja może wywołać przekonanie, że materiał zawarty w ramkach jest elementem oryginalnej strony. W rezultacie może to prowadzić zarówno do naruszenia prawa ochronnego na znak, do czynów nieuczciwej konkurencji oraz do naruszenia praw autorskich, poprzez podawanie nieprawidłowych danych autora lub wręcz sugerowanie autorstwa konkretnego materiału.

Kopiowanie zawartości stron internetowych a następnie wykorzystywanie ich w całości lub we fragmentach na innej stronie jest jednym z najpowszechniejszych naruszeń autorskich praw majątkowych. Wiele firm – często nieświadomie – narusza prawa autorskie. Wystarczy przejrzeć strony internetowe firm, by przekonać się, w jaki sposób dochodzi do naruszenia prawa autorskiego. Prawie każda firma na swej stronie posiada „zakładkę", w której „gromadzi" informacje o sobie. Bardzo często są to „skopiowane" całe artykuły pojawiające się w prasie lub na innych stronach internetowych. Zazwyczaj tego typu proceder odbywa się bez zgody autora, właściciela autorskich praw, bez umowy licencyjnej.

Podobnie funkcjonuje tzw. *press cliping* czyli monitorowanie mediów. Co do zasady zbieranie informacji, poddawanie ich różnym analizom nie jest działaniem sprzecznym z prawem. Z naruszeniem praw autorskich w tym zakresie mamy do czynienia w momencie, gdy taka czynność jest dokonywana przez osobę trzecią na zlecenie np. konkretnego przedsiębiorcy. Należy bowiem pamiętać, że zgodnie z treścią art. 23 ust. 1 *PrAut*. *bez zezwolenia twórcy wolno nieodpłatnie korzystać z już rozpowszechnionego utworu w zakresie własnego użytku osobistego.* Z kolei „własny użytek osobisty" *obejmuje korzystanie z pojedynczych egzemplarzy utworów przez krąg osób pozostających w związku osobistym, w szczególności pokrewieństwa, powinowactwa lub stosunku towarzyskiego* (art. 23 ust. 2 PrAut). Co więcej, na dozwolony użytek może powoływać się jedynie osoba fizyczna.

Można więc stwierdzić, że podczas kopiowania zawartości stron internetowych, ich części oraz tzw. monitoringu prasy może dochodzić do naruszenia prawa autorskiego. Aby było on zgodne z prawem konieczne jest spełnienie kilku warunków a przede wszystkim podpisanie stosownych umów z wydawcami.

---

[30] J. Barta, R. Markiewicz: *Odpowiedzialność za odesłania w Internecie* (w:) M. Pyziak-Szafnicka (red.) *Odpowiedzialność cywilna. Księga pamiątkowa ku czci Profesora A. Szpunara*. Kraków 2004, s. 627

[31] *http://pl.wikipedia.org/wiki/Hotlink* (pobrano 20.03.2011 r.)

Naruszenie praw autorskich powinno być rozpatrywane wraz z zagadnieniem odpowiedzialności. Warto więc zasygnalizować ten problem na przykładach z ostatnich miesięcy. W Australii wielkie wytwórnie muzyczne i filmowe przegrały sprawę o „blokowanie" pirackich stron. Sąd Federalny w Sydney (informacja za Reuters'em), stwierdził, że *samo dostarczanie Internetu nie oznacza naruszenia, a iiNet w rzeczywistości nie miał władzy pozwalającej na powstrzymanie nielegalnych pobrań.*[32] W tej samej sprawie Sąd stwierdził ponadto, że *prawdą jest, że za pomocą Internetu dochodzi do naruszeń praw autorskich, ale nie można pociągać operatorów do odpowiedzialności za to, że „coś powinno być zrobione"*.[33]

Inaczej problem naruszenia prawa własności intelektualnej w Internecie ocenia Rzecznik Generalny w sprawie C-324/09 (*L'Oreal SA vs eBay International AG*), który uważa, że *powtarzające się akty naruszeń prawa do znaku towarowego mogą prowadzić do nałożenia odpowiedzialności za naruszenie podmiotu organizującego sprzedaż*.[34]

Kwestia odpowiedzialności za naruszenie praw autorskich w Internecie dostrzegana jest w wielu państwach Unii Europejskiej. Bardzo często wiązana jest jednak z ingerencją w prywatność. Nie ulega wątpliwości, że ochrona praw autorskich powinna mieć miejsce. Należy jednak czynić to bardzo ostrożnie i w sposób niezwykle wyważony. Nie wolno akceptować restrykcyjnych propozycji zmian dyrektywy IPRED *(Intellectual Property Rights Enforcement Directive)* polegających między innymi na kontrolowaniu dostawców treści Internetu. Nie do zaakceptowania jest, tym bardziej prawo Hadopi.[35]

Przy wprowadzaniu wszelkiego rodzaju regulacji prawnych, mających służyć ochronie własności intelektualnej w Internecie, warto kierować się opinią Rzecznika Generalnego Trybunału Sprawiedliwości Pedra Cruza Villalona, który stwierdził: *środek, który nakazuje dostawcy dostępu do Internetu, wdrożenie systemu filtrowania i blokowania połączeń elektronicznych w celu ochrony prawa własności intelektualnej, narusza co do zasady prawa podstawowe.*[36] Rzecznik generalny – w tej samej opinii – dochodzi do wniosku, że aby taki nakaz był skuteczny *musiałby doprowadzić do filtrowania wszystkich treści – zarówno wysyłanych, jak i odbieranych przez klientów tego dostawcy Internetu (…) system musiałby tez umożliwić blokowanie transferu plików, który naruszałby prawa autorskie*. Najistotniejszą uwagą rzecznika jest stwierdzenie, z którym należy się zgodzić, że *środek ten byłby stosowany prewencyjnie, nawet bez wcześniejszego stwierdzenia naruszenia praw autorskich przez użytkowników*.[37]

---

[32] *www.di.com.pl* (pobrano: 12.04.2011 r.)

[33] Op. cit.

[34] Opinia Rzecznika Generalnego Jaaskinena z 9 grudnia 2010 r. sprawa C-324/09, *www.eur-lex.europa.eu* (pobrano14.04.2011 r.)

[35] To skrót od „Wysoki Urząd ds. rozpowszechniania utworów i ochrony praw w Internecie), powszechnie używane określenie na francuską ustawę mającą na celu walkę z piractwem w Internecie, pozwalającej na blokowanie dostępu do Internetu osobom podejrzanym o łamanie praw autorskich (blokowanie po trzecim ostrzeżeniu) oraz wprowadzającej odpowiedzialność zbiorową.

[36] Opinia Rzecznika Generalnego Trybunału Sprawiedliwości w sprawie C-70/10, komunikat prasowy Trybunału Sprawiedliwości Unii Europejskiej nr 37/11, *www.curia.eu* (pobrano: 14.04.2011 r.)

[37] Op. cit.

Taka sytuacja byłaby sprzeczna nie tylko z Kartą praw podstawowych ale również z pozostałymi dokumentami określającymi podstawowe prawa i wolności człowieka i obywatela.

Na podstawie powyższych – z konieczności edytorskich – bardzo ograniczonych rozważań, można pokusić się o stwierdzenie, że bezpieczeństwo praw autorskich w Internecie nie jest należycie chronione. Niepokojące jest to, że mimo funkcjonowania tego „zjawiska" od wielu już lat, w dalszym ciągu jest duża różnorodność przyczyn takiego stanu rzeczy. W przypadku Wikipedii, problemem jest sama jej kwalifikacja – utwór czy nie, a jeżeli tak to jaki. Jak należy oceniać osoby tworzące ją – twórcy, współautorzy czy może wprowadzić do ustawodawstwa odrębną kategorię takich podmiotów.

Zagadnienie odesłań też nie jest wolne od problemów naruszeń praw autorskich. Niezależnie od rodzaju odesłania, a należy podkreślić, że podana powyżej klasyfikacja ich, jest irrelewantna z punktu widzenia prawa autorskiego, bowiem ocena wszystkich odesłań dokonywana jest na podstawie takich samych kryteriów, można w pewnych sytuacjach zostać posądzonym o bezprawne rozpowszechnianie utworu. Największe zagrożenie takiego zarzutu niesie za sobą instytucja odesłań głębokich oraz tzw. *framingu*.

Najmniej problemów związanych z zapewnieniem bezpieczeństwa praw autorskich w Internecie związanych jest ze zjawiskiem kopiowania zawartości stron internetowych oraz tzw. monitorowaniem mediów. W tym zakresie sytuacja prawna jest zdecydowanie najlepsza. Prawo autorskie w sposób wyczerpujący reguluje to zagadnienie i jedynie celowe lub nieświadome działania są przyczyną naruszania praw autorskich. Należy mieć nadzieję, że wzrastająca świadomość społeczeństwa i znajomość prawa autorskiego z biegiem czasu doprowadzą do ewolucyjnego wyeliminowania tego problemu.

Iwona ISKIERKA, Janusz KRZEMIŃSKI, Zbigniew WEŻGOWIEC
Politechnika Częstochowska

BEZPIECZEŃSTWO BANKOWOŚCI ELEKTRONICZNEJ W ODBIORZE SPOŁECZNYM

Wstęp

Konieczność wykorzystywania technologii informacyjno-komunikacyjnych (TIK) przez współczesne społeczeństwa jest traktowana jako jeden z istotnych czynników ich rozwoju. O randze tego zagadnienia świadczą wielostronne działania, jakie podejmuje Unia Europejska oraz rządy poszczególnych krajów członkowskich, zmierzające do zintensyfikowania wykorzystania tych technologii we wszystkich dziedzinach życia gospodarczego, społecznego i kulturalnego. Szczegółowo zostały one wyartykułowane w licznych dokumentach unijnych, jak i w dokumentach poszczególnych krajów członkowskich. Jednym z najważniejszych i najnowszych z nich to dokument Unii Europejskiej – *Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Europejska Agenda Cyfrowa* z 2010 roku.[1] W dokumencie tym zwrócono szczególną uwagę na zagadnienia związane z ujednoliceniem rynku cyfrowego w Unii Europejskiej, a w konsekwencji ujednoliceniu usług na platformie cyfrowej, w tym usług związanych z bankowością elektroniczną.

W Polsce dokumentem, który kompleksowo omawia problemy wykorzystania technologii informacyjno-komunikacyjnych we wszystkich aspektach funkcjonowania państwa i społeczeństwa jest dokument pod nazwą *Strategia rozwoju społeczeństwa informacyjnego w Polsce do roku 2013* z grudnia 2008 roku.[2]

W ramach Funduszy Europejskich na lata 2007-2013 i wynikającej z nich Narodowej Strategii Spójności na lata 2007-2013 zdefiniowano osiem kluczowych kompetencji, które są niezbędne do jak stwierdzono „*samorealizacji i rozwoju osobistego, bycia aktywnym obywatelem, integracji społecznej i zatrudnienia*". Jedną z tych kluczowych kompetencji są kompetencje informatyczne, w ramach których na potrzeby niniejszego opracowania, autorzy postanowili skoncentrować się na umiejętności korzystania przez obywateli z usług dostępnych w sieci Internet, a w szczególności z usług związanych z bankowością elektroniczną. Przy czym umiejętności te potraktowano jako pewien zbiór kompetencji, w skład którego wchodzi nie tylko umiejętność operowania kontem bankowym i płatnościami on-line, czy też korzystanie ze sklepów internetowych, ale również umiejętność reagowania na zagrożenia występujące w sieci i aktywna współpraca z bankiem w celu zapewniania maksymalnego bezpieczeństwa transakcji przeprowadzanych poprzez sieć, zwłaszcza w przypadku, gdy użytkownik korzysta z urządzeń mobilnych na przykład telefonu komórkowego.

---

[1] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Europejska Agenda Cyfrowa. *http://www.mswia.gov.pl.* (pobrano 5.09.2010 r.)

[2] Strategia rozwoju społeczeństwa informacyjnego w Polsce do roku 2013, grudzień 2008. *http://www.mswia.gov.pl/strategia/*. (pobrano 2.09.2010 r.)

Bankowość elektroniczna w Unii Europejskiej

Unia Europejska przywiązuje dużą wagę do rozwoju technologii informacyjno –komunikacyjnych, a w szczególności zwraca uwagę na konieczność maksymalnego wykorzystania możliwości ekonomicznych i społecznych tych technologii. Podstawowym dokumentem Unii Europejskiej, stanowiącym zbiór wytycznych dotyczących wdrożenia TIK do gospodarki unijnej jest *Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Europejska Agenda Cyfrowa* z 2010 roku.[3] Głównym założeniem Agendy Cyfrowej „*jest uzyskanie trwałych korzyści ekonomicznych i społecznych z jednolitego rynku cyfrowego w oparciu o szybki i bardzo szybki Internet i interoperacyjne aplikacje.*"

Realizacji tego zadania upatruje się między innymi w ułatwieniach transakcji internetowych i transgranicznych. Polegać mają one między innymi na ograniczeniu technicznych i prawnych przeszkód w transgranicznej płatności kartami kredytowymi, ujednoliceniu płatności elektronicznych i elektronicznego fakturowania. Dokument zwraca również uwagę na pilną konieczność zakończenia prac nad Jednolitym Europejskim Obszarem Płatniczym (SEPA) i wdrożeniem w trybie pilnym dyrektywy w sprawie pieniądza elektronicznego. Agenda Cyfrowa zwraca również uwagę na bardzo istotne kwestie związane z bezpieczeństwem transakcji finansowych dokonywanych w sieci Internet. W punkcie *2.3 Zaufanie i bezpieczeństwo* tego dokumentu wyraźnie stwierdzono, że bez w pełni wiarygodnych nowych technologii nie będzie możliwości rozwoju najbardziej zaawansowanych usług internetowych takich jak miedzy innymi bankowość elektroniczna. Z tego też względu w Agendzie Cyfrowej dużo miejsca poświęcono problemom bezpieczeństwa w sieci i walki z cyberprzestępczością, które to zadanie winno spoczywać na wszystkich krajach Unii Europejskiej.

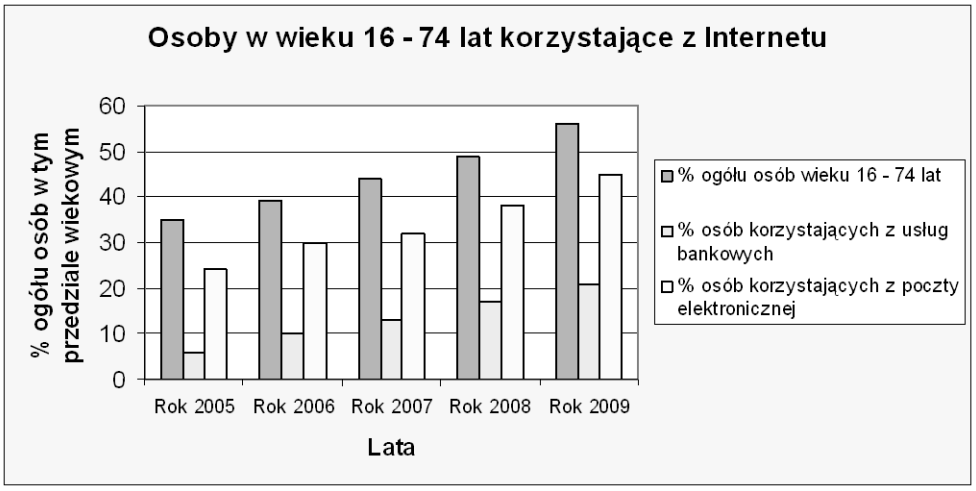
Rozwój zaawansowanych usług takich jak bankowość elektroniczna jest możliwa tylko pod warunkiem szerokiego ich zaakceptowania przez użytkowników. Stanie się to możliwe tylko wówczas, gdy użytkownicy będą posiadać odpowiednie umiejętności, oraz usługi te w odczuciu społecznym będą bezpieczne tak ze względu na ochronę prywatności danych użytkownika jak i bezpieczeństwo jego „elektronicznego" portfela. Kwestie te wyraźnie artykułuje, jak wspomniano wyżej, Europejska Agenda Cyfrowa w punkcie *2.3 Zaufanie i bezpieczeństwo*.

Korzystanie z usług bankowości elektronicznej jest możliwe oczywiście tylko przy zapewnieniu obywatelom dostępu do sieci Internet. Na rysunku nr 1 przedstawiono dane, wykorzystując informacje z Roczników Statystycznych GUS, obrazujące stopień korzystania z Internetu przez obywateli polskich z przedziału wiekowego 16-74 lat.

Analizowane dane obejmują okres od 2005 do 2009 roku. Na wykresie przestawiono trzy parametry. Pierwszy dotyczy ogólnej liczby osób (w % w stosunku do całej populacji w tej grupie wiekowej), która korzysta z Internetu. Drugi wskazuje na % osób w tej grupie wiekowej korzystającej z usług

[3] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno -Społecznego i Komitetu Regionów. Europejska Agenda Cyfrowa. *http://www.mswia.gov.pl.* (pobrano 5.09.2010 r.)

bankowości elektronicznej. Trzeci parametr, traktowany jako porównawczy, dotyczy % osób w tej grupie wiekowej korzystającej z poczty elektronicznej. Usługa ta jest, bowiem najpopularniejszą usługą wykorzystywaną przez użytkowników Internetu.



Rysunek nr 1: Osoby w wieku 16-74 lat korzystające z Internetu
Źródło: Opracowanie własne na podstawie Roczników Statystycznych GUS

Przedstawione dane jednoznacznie wskazują na stały wzrost, w badanym okresie, wszystkich trzech parametrów. Interesujący nas wskaźnik, mówiący o procencie osób korzystających z bankowości elektronicznej, w analizowanym okresie wzrósł trzy i półkrotnie i wyniósł w 2009 roku 21%. Jest on jednak, pomimo to, ponad dwukrotnie mniejszy niż odpowiedni wskaźnik dotyczący poczty elektronicznej. Należy przy tym zaznaczyć, że usługi bankowe znalazły się w 2009 roku na piątym miejscu w hierarchii celów, jakie powodowały korzystanie przez Polaków z Internetu.[4] Wyprzedziły je takie cele jak: komunikowanie się, uzupełnianie wiedzy, wyszukiwanie informacji o produktach i wyszukiwanie informacji o zdrowiu. Dodatkowo w raporcie[5] zamieszczono również interesującą informację mówiącą o tym, że z bankowości elektronicznej korzysta 33% osób posiadających szerokopasmowy dostęp do Internetu i tylko 19% osób posiadających dostęp podstawowy. Świadczy to wyraźnie o wpływie rozwoju technologii na poziom absorpcji nowoczesnych usług oferowanych w sieci Internet, w tym usług bankowości elektronicznej. Pozostaje jednak faktem, że tylko co piąty obywatel w Polsce (a co trzeci w Unii Europejskiej) korzysta z usług bankowości elektronicznej.[6] Wskaźnik ten należy uznać za wysoce niewystarczający, zwłaszcza biorąc pod uwagę fakt, że 59% gospodarstw domowych w Polsce miało w 2009 roku dostęp do Internetu, podczas gdy średnia dla Unii Europejskiej była

[4] *Społeczeństwo informacyjne w liczbach 2010*. Departament Społeczeństwa Informacyjnego. Ministerstwo Spraw Wewnętrznych i Administracji. Warszawa 2010 *http://www.mswia.gov.pl.* (pobrano 7.04.2011 r.)
[5] Ibidem
[6] Ibidem

tylko o sześć procent większa i wynosiła 65%.[7] Dane te wskazują na jeszcze stosunkowo małą kreatywność Polaków w sferze wykorzystania zaawansowanych usług oferowanych przez sieć internetową takich jak bankowość elektroniczna.

Współczesne zagrożenia związane z korzystaniem z bankowości elektronicznej

W raz z rozwojem zaawansowanych usług dostępnych w sieci Internet i coraz powszechniejszym ich wykorzystywaniem przez użytkowników, wzrasta stopień zagrożenia związany z bezpieczeństwem przesyłania poufnych danych, które są niezbędne do realizacji większości z nich. Jedną z najbardziej wrażliwych z tych usług, ze względu na konieczność zapewnienia bezwzględnego bezpieczeństwa transakcji, jest bankowość elektroniczna. A ponieważ jest ona bezpośrednio związana z obrotem środkami finansowymi w sieci, to stała centrum zainteresowania licznych grup przestępczych, stara się różnymi sposobami i z różnym skutkiem wpływać na jej działanie. W praktyce sprowadza się to najczęściej do przechwytywania przez cyberprzestępców transakcji dokonywanych w sieci przez klientów banków i zagarniania zasobów ich kont.

Współcześnie cyberprzestępcy do ataków wykorzystują najczęściej złośliwe oprogramowanie połączone z technikami znanymi jako socjotechnika lub inżynieria społeczna. Ideą tego typu ataku, zwanego *phishingiem*, jest skłonienie użytkownika, na przykład poprzez wysłanie e-maila, do odwiedzenia odpowiednio spreparowanej strony, najczęściej banku, na której nieświadomy niczego użytkownik podaje swoje dane takie jak login i hasło czy numer karty kredytowej. Dane te służą później napastnikowi do ataku na właściwe konto klienta. Odmianą tego typu ataku jest *pharming*, w którym przekierowanie na odpowiednią stronę dokonuje się niejako automatycznie poprzez podmianę adresu DNS na zainfekowanym komputerze klienta.

Inżynieria społeczna jest na tyle skuteczną techniką pozyskiwania danych przez cyberprzestępców, że stosują ją również do pozyskiwania poufnych danych od pracowników znanych firm którzy, wydawałoby się, powinni być wyczuleni i odporni na tego typu działania.[8] Fakt ten potwierdza znaną tezę głoszoną od dawna przez specjalistów od spraw bezpieczeństwa komputerowego, że najsłabszym ogniwem bezpieczeństwa systemu komputerowego jest tak zwany „czynnik ludzki".

Na początku roku 2011 zaobserwowano w Polsce, właśnie tego typu ataki na konta bankowe dokonywane za pomocą trojana Zeus. Trojan ten wśród specjalistów od bezpieczeństwa komputerowego znany jest również pod nazwami: Zboot, PRG, Wsnpoem, Gorhax, Kneber. Został on szczegółowo opisany w raporcie: *Botnet Zeus – analiza w laboratorium CERT*.[9] Atakom z użyciem tego złośliwego oprogramowania najczęściej podlegały strony bankowości elektronicznej ipko.pl oraz bsk.com.pl.[10] Przed atakami wykorzystującymi trojana

[7] Ibidem
[8] A. Nowak :*Wielkie korporacje nieodporne na inżynierię społeczną*, *http://di.com.pl/news/32914.html*. (pobrano 8.04.2011 r., 31.07.2010, 13:50)
[9] *Botnet Zeus – analiza w laboratorium CERT*. CERT Polska / NASK 11 stycznia 2011 r.
[10] Raport 2010. CERT Polska. Zawiera raport z systemu ARAKIS. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne. *http://www.cert.pl* (pobrano 8.04.2011 r.)

Zeus ostrzegała, na początku roku 2011, między innymi użytkowników Neostrady Telekomunikacja Polska [11] oraz bank BNP Paribas Fortis.[12]

O nowym zagrożeniu, które pojawiło się 3 kwietnia 2011 roku, poinformował na swojej stronie CERT Polska.[13] Związane jest ono z wykradaniem poufnych informacji ze stron internetowych poprzez ściągnięcie w e-mailu na swój komputer, zainfekowanego złośliwym oprogramowaniem o nazwie SpyEye, pliku PDF. Portal CERT Polska przestrzega przed otwieraniem tego typu załączników i zaleca bezzwłoczne ich kasowanie.

Podstawowe zagrożenia, na jakie narażone są współczesne systemy komputerowe przedstawiono w *Raporcie 2010 CERT Polska*.[14] W raporcie tym zwrócono uwagę, że od kilku lat nasila się tendencja do uzyskiwania danych dostępowych za pomocą *snifferów* i koni trojańskich, czego przykładem jest właśnie trojan Zeus. Ciągle najczęstszą metodą ataku na system komputerowy pozostaje tak zwana technika *drive-by download*, która polega na umieszczeniu w kodzie strony skryptu, który wykorzystuje lukę w oprogramowaniu i przekierowuje użytkownika do serwera, z którego instalowane jest złośliwe oprogramowanie.

Przekaz medialny dotyczący anomalii występujących w bankowości elektronicznej

Obywatel korzystający z usług bankowości elektronicznej jest, jak pokazują dane statystyczne,[15] najczęściej zaawansowanym użytkownikiem Internetu i technologii informacyjno-komunikacyjnych. Z tego też względu należy założyć, że większość informacji, z których korzysta w życiu codziennym dociera do niego poprzez sieć. Również wiadomości dotyczące bankowości elektronicznej, w tym występujących ewentualnych awarii w systemach bankowych, czerpie z sieci Internet. Autorzy postanowili prześledzić te informacje i ocenić, jaki one mogły mieć wpływ na zachowania, reakcje i zaufanie użytkowników do systemów bankowych, a w szczególności do bankowości elektronicznej. Dokonano tego w okresie od 30 września 2010 roku do 15 marca 2011 roku, przeglądając portale Wyborcza.biz i onet.pl, jako jedne z popularniejszych stron podających aktualne wiadomości ekonomiczne.

Analizę rozpoczyna wiadomość, jaka ukazała się w dniu 30 września 2010 roku na portalu onet.pl informująca o rozbiciu przez Scotland Yard gangu cyberprzestępców, którzy wykorzystując konia trojańskiego Zeus okradali konta

---

[11] *Masz Neostrady? TP ostrzega przed phishingiem*, *http://technologie.gazeta.pl/internet/ 1,104530,9167456, Masz_Neostrade__TP_ostrzega_przed_phisingiem.html*

[12] *Bezpieczeństwo w systemie bankowości internetowej*, (pobrano 2.04.2011 r.) *http://www.bnpparibasfortis.pl/news/komunikaty -10520.htm,*

[13] *UWAGA! SpyEye w PDF atakuje polskich internautów*, *http://www.cert.pl/news/3480/ langswitch_lang/ en*, (pobrano 4.04.2011 r.)

[14] Raport 2010. CERT Polska. Zawiera raport z systemu ARAKIS. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne. *http://www.cert.pl* (pobrano 8.04.2011 r.)

[15] *Strategia rozwoju społeczeństwa informacyjnego w Polsce do roku 2013*, grudzień 2008. *http://www.mswia.gov.pl/strategia/*. (pobrano 2.09.2010 r.) Społeczeństwo informacyjne w liczbach 2010. Departament Społeczeństwa Informacyjnego. Ministerstwo Spraw Wewnętrznych i Administracji, Warszawa 2010, *http://www.mswia.gov.pl.* (pobrano 7.04.2011 r.) *http://www.ingbank.pl/indywidualni/bankowosc-elektroniczna/ing-bankonline#tab=1.* (pobrano 8.04.2011 r.)

bankowe klientów wielu instytucji bankowych w Wielkiej Brytanii i USA.[16] W informacji podano, że grupa przestępców jest najprawdopodobniej częścią wschodnioeuropejskiego gangu, co niedwuznacznie sugeruje, że gang może działać również na terenie Polski.

Po południu dnia 11 października 2010 roku portal Finanse *Wyborcza.biz* poinformował o awarii sieci bankowości elektronicznej ING Banku.[17] Wystąpiły trudności z dostępem do internetowej strony głównej banku i brak możliwości logowania do systemu. Informację tę potwierdził bank wyjaśniając, że trwają intensywne prace związane z usunięciem awarii.

W poniedziałkowe południe, 29 listopada 2010 roku nastąpiła najprawdopodobniej jedna z największych awarii w historii mBanku, należącego do grupy BRE, informował o godzinie 15.58 portal Finanse *Wyborcza.biz*.[18] Awaria polegała na błędnym księgowaniu przelewów, na przypadkowym wysyłaniu przelewów do nieuprawnionych odbiorców, błędnych kwot przelewów jak i nieprawidłowych danych adresowych tak nadawcy jak i odbiorcy. Rzecznik mBanku potwierdził wystąpienie awarii, nie był jednak w stanie określić jej skali i przyczyn. Jak podawał portal *Wyborcza.biz* po dwóch godzinach od wystąpienia awarii nastąpiło zablokowanie mLinii i dodatkowo wyłączony został serwis internetowy Multibanku, instytucji finansowej z grupy BRE. Poważnym problemem w przypadku tej awarii był fakt, że bank udostępnił dane osobowe jednych klientów drugim, co oznacza naruszenie ochrony danych osobowych. Awaria okazała się na tyle poważna, że w wieczornej aktualizacji tej wiadomości z godziny 19.01,[19] portal *Wyborcza.biz* informuje o ciągłych kłopotach banku z przywróceniem normalnego funkcjonowania wszystkich usług bankowości elektronicznej i próbach przywrócenia normalnego funkcjonowania infolinii. Nie była ciągle znana, przynajmniej oficjalnie, przyczyna awarii, jej skutki i zasięg.

Tymczasem informacja jest propagowana przez sieć Internet. Liczne głosy internautów, klientów mBanku, opisujące indywidualne przypadki dotyczące tej awarii, przedstawia portal kontakt24.tvn.pl w informacji z godziny 14.12.[20]

Awaria, a właściwie jak ocenili to przedstawiciele banku krótkotrwałe przeciążenie systemu, występuje w piątek 3 grudnia 2010 roku w serwisie Pekao24 i funkcjonalności brokerskiej Banku Pekao SA. Informuje o tym portal *Wyborcza.biz*.[21]

W niedzielę 5 grudnia 2010 roku, portal *Wyborcza.biz* podsumowuje miniony tydzień działalności bankowości elektronicznej artykułem pod znamiennym tytułem:

---

[16] M. Gajewski: *Scotland Yard rozbija duży gang hakerów wczoraj*, *http://technowinki.onet.pl/wiadomosci/scotland-yard-rozbija-duzy-gang-hakerow,1,3707250, artykul.html* CHIP.PL wiadomość z dnia 30.09.2010 godz. 14:14. (dodano 1.10.2010 r.)

[17] *Padł system bankowości elektronicznej ING Banku*, *http://wyborcza.biz/finanse/1,105684,8494776,Padl_system_bankowosci_elektronicznej_ING_Banku.html*, ostatnia aktualizacja 2010-10-11 14:35 (dodano 11.10.2010 r.)

[18] M. Samcik: *Wielka awaria w mBanku! Klienci dostali cudze przelewy*, *http://wyborcza.biz/finanse/1,105684,8737731,Wielka_awaria_w_mBanku__Klienci_dostali_cudze_przelewy.html* ostatnia aktualizacja 2010-11-29, 15:58. (dodano 29.11.2010 r.)

[19] Ibidem

[20] *Klienci mBanku dostają nie swoje pieniądze*, *http://kontakt24.tvn.pl/temat,klienci-mbanku-dostaja-nie-swoje-pieniadze,43685.html?token=c8b7b9ce042f0c28df65d81f16fcbd91*, (pobrano 29.11.2010 r.)

[21] *Czwarta wpadka banków w tym tygodniu. Dziś było Pekao*, *http://wyborcza.biz/finanse/1,105684,8760523,Czwarta_awaria_w_tym_tygodniu__dzis_Pekao.html* ostatnia aktualizacja 2010-12-03 14:06, (pobrano 4.12.2010 r.)

„*Czarna seria bankowych awarii to nie przypadek. Zawiniły…*"[22] Wymienia w nim kolejno awarie w bankach i tak: poniedziałek – mBank i opisywana powyżej awaria; wtorek – ING Bank Śląski: brak możliwości logowania i płacenia kartami debetowymi, niedziałające bankomaty; środa – Kredyt Bank: awaria systemu dokonującego przelewy; czwartek – awaria w Volkswagen Banku; piątek – opisywana powyżej awaria w Banku Pekao SA.

Dla czytelnika śledzącego informacje dotyczące bankowości elektronicznej nie była to z pewnością lektura napawająca optymizmem. Reputacja i profesjonalność działających w naszym kraju banków zostały wystawione na poważną próbę. Pocieszeniem dla klientów banków czytających te wiadomości, był z pewności fakt, że żadna z omawianych awarii nie trwała dłużej niż kilka godzin a spowodowane były one, jak twierdzą niektórzy specjaliści, niezbyt fortunnym testowaniem nowości wprowadzanych w usługach bankowości elektronicznej, co ma zwykle miejsce w miesiącu grudniu.

Koniec roku nie był pomyślny ponownie dla mBanku. W Sylwestra nie działał przez pewien czas system przelewów zewnętrznych.[23] Awarię zgodnie z oświadczeniem rzecznika banku usunięto o godzinie 14.30 31 grudnia 2010 roku.

Na początku nowego 2011 roku pojawiło się kolejne zagrożenie – trojan Zeus/Zbot, który atakuje systemy komputerowe i telefony komórkowe poprzez przechwycenie danych dotyczących kont bankowych, a w efekcie umożliwia cyberprzestępcy przejęcie konta i opróżnienie go. Informacje o zagrożeniu tym trojanem i zalecenia banków, między innymi ING Banku, mBanku, Multibanku, dotyczące ochrony przed tym niebezpieczeństwem można znaleźć w informacjach portalu *Wyborcza.biz* z dnia 17 i 22 lutego 2011 roku.[24] A już 25 lutego portal gazeta.pl, za Dziennikiem Gazeta Prawna, donosi o śledztwach prowadzonych przez policję i ABW związanych z zaatakowaniem tym wirusem banków: ING Bank Śląski, Pekao S.A., mBank i Millennium.[25] 15 marca 2011 roku portal di.com.pl informuje o mobilnej wersji tego wirusa zwanego Zeus-in-the-Mobile (ZitMo).[26] Wersja ta, potrafiąca przechwycić autoryzowaną transakcję z wykorzystaniem SMS-ów zawierająca unikalne hasła dostępowe, jest szczególnie niebezpieczna dla użytkowników bankowości internetowej, wykorzystujących do komunikacji z bankiem telefony komórkowe.

---

[22] *Czarna seria bankowych awarii to nie przypadek. Zawiniły*. *http://wyborcza.biz/finanse/1,105684,8768338,Czarna_seria_bankowych_awarii_to_nie_przypadek__Zawinily___.html* ostatnia aktualizacja 2010-12-05 11:17, (pobrano 6.12.2010 r.)

[23] *Sylwestrowa awaria mBanku. Nie można było zrobić przelewu*, *http://wyborcza.biz/finanse/1,105684,8889811,Sylwestrowa_awaria_mBanku__Nie_mozna_zrobic_przelewu.html,* ostatnia aktualizacja 2010-12-31 14:4, (pobrano 1.01.2011 r.)

[24] M. .Loda: *Kolejne banki ostrzegają przed wirusem Zeus*, *http://wyborcza.biz/finanse/1,105684,9124393,Kolejne_banki_ostrzegaja_przed_wirusem_Zeus.html,* aktualizacja: 2011-02-17 14:58, Dostęp: 17.02.2011; Loda M., Nowa wersja Trojana atakuje klientów banków *http://wyborcza.biz/biznes/1,01562,9117424,Nowa_wersja_Trojana_atakuje_klientow_bankow.html,* aktualizacja: 2011-02-21 08:24, (pobrano 22.02.2011 r.)

[25] *Polskie banki łupem hakerów z W. Brytanii i Rosji*, *http://wiadomosci.gazeta.pl/Wiadomosci/1,80273,9163990,Hakerzy_napisali_wirusa_atakujacego_banki__Nie_ma.html,* ostatnia aktualizacja 2011-02-25 07:06, (pobrano 25.02.2011 r.)

[26] A. Wasilewska-Śpioch: *Zeus ciska piorunami w klientów polskich banków*, *http://di.com.pl/news/36593,0,Zeus_ciska_piorunami_w_klientow_polskich_bankow.html*, aktualizacja 15-03-2011, 15:22, (dodano 8.04.2011 r.)

Zaufanie klienta do bankowości elektronicznej priorytetem dla instytucji bankowych

Na stronach internetowych banków, użytkownik ma możliwość zapoznania się z podstawowymi zasadami bezpieczeństwa, jakie powinien zachować korzystając z bankowości elektronicznej. Szczegółowe informacje na ten temat zawiera również strona internetowa Związku Banków Polskich.[27] W zakładce *Bankowość elektroniczna* > *Bezpieczny Bank* > *Bankowość internetowa* można znaleźć poradnik Związku Banków Polskich dotyczący bezpieczeństwa transakcji bankowych w Internecie. W Poradniku przedstawiono podstawowe metody, jakie wykorzystują banki w celu zapewnienia bezpieczeństwa transakcji realizowanych przez klientów drogą elektroniczną. Zostały one przedstawione w następującej postaci:

- *„podstawowa identyfikacja klienta: – identyfikator + PIN, tonek, token + PIN;*
- *protokół szyfrowania transmisji danych w Internecie – SSL;*
- *dostęp w oparciu o certyfikaty;*
- *kody wysyłane SMS'em;*
- *jednorazowe kody autoryzujące transakcje;*
- *podpis elektroniczny, funkcja skrótu i jej zastosowanie;*
- *karty mikroprocesorowe z zapisanym certyfikatem;*
- *limity transakcji;*
- *automatyczne wygasanie sesji po okresie nieaktywności użytkownika".*

Wydaje się, że część tych informacji na przykład związanych z protokołem SSL dla wielu użytkowników, przede wszystkim indywidualnych, nie będzie zrozumiała. A jest to o tyle istotne, że użytkownik banku łączy się z jego systemem poprzez Internet wykorzystując komputer albo telefon komórkowy i jego niewiedza dotycząca niektórych aspektów połączenia może mieć decydujące znaczenia dla bezpieczeństwa przeprowadzanej przez niego transakcji, a dokładniej bezpieczeństwa jego konta.

Poradnik, w części dotyczącej zachowań użytkownika banku, stanowią: zasady ogólne, zasady dotyczące płatności z internetowego konta bankowego, zasady dotyczące płatności kartami płatniczymi przez Internet. Zasady ogólne dotyczą podstawowych zagadnień, na jakie musi zwrócić uwagę użytkownik bankowości elektronicznej. Mówią one między innymi o formach komunikowania się banku z klientem, zalecają klientowi sprawdzanie zabezpieczeń stosowanych przez bank na stronie internetowej i używanie legalnego oprogramowania aplikacyjnego oraz aktualnego oprogramowania antywirusowego, przestrzegają przed otwieraniem załączników otrzymywanych z pocztą e-mail od nieznanych nadawców i odwiedzaniem nieznanych stron internetowych.

Zasady dotyczące płatności z internetowego konta bankowego stanowią zbiór zaleceń, do których powinien stosować się użytkownik wykonujący wszelkie operacje związane z korzystaniem z tego konta. Do najważniejszych z nich zaliczono procedury związane z poprawnym zalogowaniem się i wylogowywaniem z systemu, ochronę hasła i PIN-u oraz systematyczne śledzenie wszystkich informacji dotyczących spraw bezpieczeństwa udostępnianych przez bank.

[27] *http://www.zbp.pl/bezpieczny_bank Związek Banków Polskich*

Zasady dotyczące płatności kartami płatniczymi przez Internet odnoszą się do bezpiecznego posługiwania się tymi kartami przy korzystaniu ze stron sklepów internetowych oraz ochrony samej karty przed nieuprawnionym przekazaniem jej danych osobom postronnym.

Przedstawione w poradniku zasady, a w sumie poradnik zawiera ich dwadzieścia siedem, stanowią kanon postępowania klienta bankowości elektronicznej, którego bezwzględnie powinien przestrzegać każdy użytkownik banku korzystający z tej formy usługi bankowej. Niestety praktyka życia codziennego pokazuje, że większość użytkowników nie stosuje się do tych zasad. Wnioski takie można wyciągnąć analizując informacje przekazane, za TNS OBOP, przez portal *Wyborcza.biz*.[28] Według badań TNS OBOP 67% polskich internatów odwiedza potencjalnie niebezpieczne strony, 62% otwiera pocztę od nieznanych osób, a 36% z nich otwiera załączniki w tej poczcie. Powszechnymi uchybieniami, których dopuszczają się polscy internauci są ponadto: nie stosowanie firewali, używanie zbyt prostych haseł, umieszczanie kodów PIN na kartach bankomatowych, nie chronienie wpisywanych numerów PIN w trakcie operacji bankomatowych czy też korzystanie z serwisów bankowych z wykorzystaniem komputerów ogólnodostępnych na przykład w kawiarenkach internetowych.

Podsumowanie

Internetowe usługi bankowe stają się coraz popularniejsze wśród klientów banków. Bezsprzeczne zalety związane z możliwością dysponowania swoim rachunkiem dwadzieścia cztery godziny na dobę przez siedem dni w tygodniu powodują stały wzrost liczby klientów bankowości elektronicznej. Związek Banków Polskich ocenia, że pod koniec 2011 roku w Polsce będzie około 10 milionów tego typu aktywnych użytkowników banków.

Dynamiczny rozwój bankowości elektronicznej stawia przed bankami niezwykle ważne zadania związane z zapewnieniem bezpieczeństwa transakcji dokonywanych poprzez sieć. Z zadań tych banki wywiązują się, w porównaniu z innymi krajami, bardzo dobrze, na co zwraca uwagę między innymi Raport.[29]

Zdecydowanie gorzej sytuacja związana z bezpieczeństwem transakcji wygląda po stronie klienta, który bardzo często nie stosuje się do zaleceń banków dotyczących kwestii bezpieczeństwa, nie dba o zabezpieczenie swojego komputera programami antywirusowymi i nie dokonuje systematycznego uaktualniania oprogramowania.

Koniecznym jest więc prowadzenie tak przez banki jak i organizacje pozarządowe, ale również i szkoły systematycznej akcji uświadamiającej dotyczącej uwrażliwienia użytkowników Internetu na kwestie związane

[28] P. Poznański: *Polak zagrożony w sieci. Głównie z własnej winy*, *http://wyborcza.biz/biznes/1,100896,8556551,Polak_zagrozony_w_sieci_Glownie_z_wlasnej_winy.html*

[29] *Bezpieczeństwo bankowości internetowej. Raport Bankier.pl*, październik 2009, *http://www.bankier.pl,* (dodano 10.10.2010 r.)

z bezpiecznym korzystaniem z usług oferowanych przez sieć, a zwłaszcza usług związanych z bankowością elektroniczną. Dobrym przykładem może być tutaj, uruchomiony 21 października 2010 roku, portal BezpieczniejwSieci.org.[30] Portal ten zawiera kompleksowy zbiór informacji dotyczący bezpiecznego korzystania z sieci. Znajdują się tam porady zarówno dla użytkowników początkujących, jak i zaawansowanych. Tego typu działania należy przyjąć z wyjątkową aprobatą, gdyż problem bezpieczeństwa w sieci jest i będzie stanowił w najbliższej przyszłości najważniejsze wyzwanie, przed jakim staną zarówno instytucje finansowe operujące w Internecie, jak i zwykli użytkownicy bankowości elektronicznej. Bezpieczne transakcje to usatysfakcjonowany klient, który mając zaufanie do systemu bankowego, będzie coraz częściej korzystał z usług bankowości elektronicznej.

[30] *http://bezpieczniejwsieci.org*, (dodano 12.04.2011 r.)

Iwona ISKIERKA, Sławomir ISKIERKA
Politechnika Częstochowska

PROGRAMOWANIE GIER EDUKACYJNYCH W PROGRAMIE *EXPRESSION BLEND*

Wstęp

W 1962 roku Steve Russell i jego zespół utworzył pierwszą grę komputerową na komputerze typu mainframe PDP-1, który był własnością uczelni *Massachusetts Institute of Technology*. Była to pierwsza gra pod nazwą *Spacewar!,* funkcjonująca wyłącznie na komputerach. Została ona darmowo udostępniona użytkownikom przez jej twórców. W roku 1958 powstała gra *Tennis for Two*, a jeszcze wcześniej, w roku 1952 gra pod nazwą *Noughts and Crosses*. Obie gry wyświetlano nie na monitorach, lecz na oscyloskopach podłączonych do ówczesnych komputerów.[1] W kolejnych latach gry komputerowe przechodziły ewolucję. Należy zauważyć, że wśród tworzonych gier były i takie, które nie zawierały żadnej grafiki, ale mogły być używane na komputerach, które nie miały ekranów. Warto uświadomić sobie, że gra na najniższym poziomie abstrakcji jest niczym innym jak programem komputerowym. Współcześnie zdecydowana większość programów jest efektem pracy zespołów programistów, z których każdy może pracować nad pewnym fragmentem projektu. Na etapie finalnym fragmenty te łączone są w spójną całość. Dotyczy to również procesu tworzenia gier.[2] Do programowania gier można wykorzystać wiele środowisk, wśród nich *XNA Game Studio, Visual Studio, Microsoft Expression Blend.* Zestaw bibliotek *XNA Game Studio* wspomaga tworzenie gier i aplikacji przeznaczonych na systemy *Windows* oraz *Windows Phone 7* i platformę *Xbox 360*. Pakiet jest dodatkiem do programu *Visual Studio* i został oparty o *.NET Compact Framework*. Dzięki niemu tworzenie i edytowanie gier oraz aplikacji staje się znacznie prostsze. W pakiecie *Expression Studio* udostępniono projektantom profesjonalne narzędzia projektowe i programistyczne, potrzebne do tworzenia aplikacji nowej generacji dla systemu *Microsoft Windows* i aplikacji internetowych.[3]

1. Historia gier

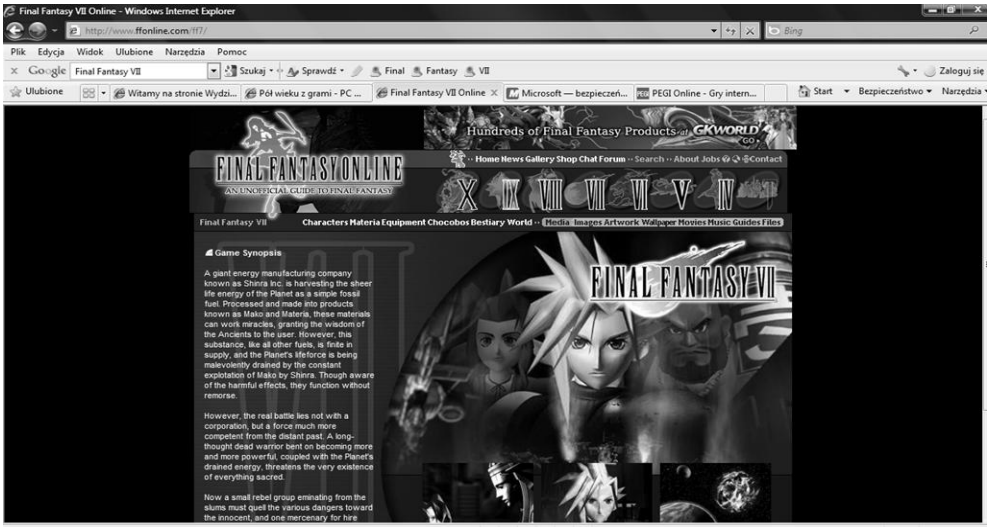
Pierwsze gry planszowe były grami wyścigowymi. Jedna z najstarszych istniejących plansz służyła do gry Sonet, która była popularna w Egipcie ponad 2000 lat temu. Gra rozgrywana była pomiędzy dwoma graczami, którzy posiadają po kilka pionków. Ponieważ nie znano jeszcze kostek do gry, gracze rzucali pałeczkami i poruszali swoimi pionkami po planszy. Celem było doprowadzenie swoich pionków do końca, który reprezentował niebo.[4] Oprócz gier wyścigowych, kolejnym wczesnym typem były odmiany gry *Nine Men's Morris*. Gra używała planszy z połączonymi punktami. Gry tego typu ewoluowały do takich gier jak warcaby i szachy. Celem było usunięcie pionków przeciwnika i jednoczesna

[1] P. Brągoszewski, *Pół wieku z grami*, PC World Computer 05, 2006
[2] K. Hawkins, D. Astle, *OpenGl programowanie gier*. Gliwice-Helion 2003
[3] *http://www.microsoft.com/poland//developer/expression/studio/przewodnik.mspx*
[4] G. Rosenzweig, *Flash 5 ActionScript. Gry i zabawy*, Translator. Warszawa 2002

ochrona własnych. Tego typu gry symulowały stały element w historii ludzkości czyli wojnę.

Świat gier planszowych przyjął znaną obecnie postać pod koniec XIX i na początku XX wieku. Gry zaczęły być wymyślane, masowo produkowane i rozpowszechniane przez takie firmy jak Milton Bradley i Parker Brothers. Na podstawie starych pomysłów powstały nowe standardy, takie jak *Scrabble* i *Monopoly*. Wśród wielu rodzajów gier szczególne zainteresowanie wzbudzały zawsze gry wojenne. Za twórcę pierwszej rozrywkowej gry wojennej uznawany jest zazwyczaj pisarz H.G. Wells. Ze świata gier wojennych wyłonił się świat gier fabularnych, z grą *Dungeons & Dragons*. Wywodzi się ona z miniaturowych gier figurkowych, jako wariant gry *Chainmail* zawierającej zbliżony system gry. Publikacja *D&D* jest szeroko uznawana za początek nowoczesnych gier RPG i, co więcej, całego przemysłu *role-playing*. Gracze *D&D* tworzą swoje postaci biorące udział w wyimaginowanych przygodach w scenerii fantasy.

Gry fabularne zmieniły definicję gier i czasu ich trwania. Stworzyły nowy rynek firm i graczy i stworzyły podwaliny do rozwoju gier komputerowych.



Rysunek nr 1: Strona Final Fantasy VII
Źródło: *http://www.ffonline.com/ff7/*

W 1962 roku utworzono pierwszą grę komputerową. Później pojawiła się klasyczna gra *Adventure*, która uważana jest za prekursora wszystkich gier komputerowych i RPG. Gra komunikowała się z użytkownikiem tylko za pomocą tekstu. Opisywała otoczenie gracza, a on wydawał polecenia. Gry komputerowe pojawiły się na rynku najpierw w postaci automatów na monety. Pierwszą grą wideo działającą na monety była gra *Computer Space Nolana Bushnella*. W roku 1979 japońska firma Taito opracowała grę *Space Invaders* – pierwszy prawdziwy hit na rynku gier wideo. W późnych latach sześćdziesiątych Ralph Baer rozpoczął tworzenie pierwszego domowego systemu gier wideo. Gotowy system został nazwany *Odyssey*. Wkrótce potem takie firmy jak Fairchild, RCA, Atari i Mattel wprowadziły nowe systemy, które można było programować.

W momencie pojawienia się na rynku komputerów osobistych, pojawiły się możliwości tworzenia bardziej rozbudowanych gier. Programiści mogli tworzyć gry w łatwy sposób, przy minimalnych inwestycjach, w odróżnieniu od kosztownego procesu tworzenia gier dla konsol wideo. Komputery pozwoliły twórcom gier eksperymentować z nowymi technikami. Takie gry jak *Doom* rozpoczęły gatunek gier trójwymiarowych, pokazywanych z perspektywy pierwszej osoby. Lata 70-te ubiegłego wieku to prawdziwy początek gier komputerowych, rozumianych jako masowa rozrywka. W 1972 roku powstała gra *Pong*, przebój pierwszych domowych komputerów osobistych i popularnych jeszcze niedawno salonów gier. W tym samym roku pojawiła się pierwsza domowa konsola do gier – *Odyssey*. Rozpoczyna się rozwój gier sieciowych. W roku 1996 pojawia się *Meridian 59*, jeden z pierwszych MMORPG z graficznym interfejsem (*massively-multiplayer online role-playing game*), fabularny, rozgrywany wyłącznie przez Internet. Następnie w 1997 roku pojawia się *Ultima Online*, a w 1999 roku do dyspozycji graczy zostaje oddany *Counter-Strike*. W roku 2001 pojawia się nowa generacja konsoli do gier: *Microsoft Xbox, Sony Playstation 2* i *Nintendo GameCube*. Jest to także czas pojawienia się nowej rodziny gier – gier przeznaczonych do telefonów komórkowych.

2. Bezpieczne korzystanie z różnego rodzaju gier i wykorzystywanie zasobów sieci Internet

Firma *Microsoft* przygotowała zestaw porad dotyczących oprogramowania, bezpieczeństwa w domu, bezpieczeństwa i zabawy dzieci w grach internetowych, wskazówek dotyczących zabezpieczania sprzętu, quizy dla rodziców, filmy o nauczaniu dzieci zasad bezpieczeństwa w sieci, ochrony danych osobowych, umiejętnego i bezpiecznego korzystania z poczty elektronicznej, aktualizacji i konserwacji komputera, quizy na temat wirusów komputerowych. Pakiet zasobów użytkownik może znaleźć na stronie:

http://www.microsoft.com/poland/protect/default.mspx

Wiele miejsca, wśród materiałów poświęconym zasadom bezpieczeństwa w sieci, zajmuje problematyka gier komputerowych i możliwości stworzenia bezpieczniejszego środowiska korzystania z gier. Zagadnienia dotyczące gier zawarto w dziale: Dzieci i gry: Porady dla rodziców dotyczące bezpiecznej gry. Przedstawiając i rozszerzając wiedzę na temat społeczności graczy, klasyfikacji gier i sposobów wykorzystania wbudowanych w gry narzędzi służących zachowaniu bezpieczeństwa i prywatności, można sprawić, że dziecko będzie grać w bezpieczniejszym środowisku. Przedstawiono kilka podstawowych porad dotyczących zapewnienia ochrony dziecku, które uczestniczy w grach i współzawodnictwie *online*. Rodzic i dziecko mogą, korzystając z przedstawionych materiałów, uzupełnić wiedzę dotyczącą klasyfikacji gier i zasad zachowania poufności informacji. Mogą również zapoznać się z zasadami użytkowania każdej z witryn gier *online*. Rodzic powinien obserwować i sprawdzać, w co i z kim grają dzieci. Należy również wprowadzić odpowiednie zasady obejmujące ograniczenie czasu gry, możliwość grania tylko z kolegami i koleżankami, których dziecko zna spoza Internetu, oraz zakaz rozmów internetowych z obcymi i ujawniania jakichkolwiek danych osobowych, takich jak prawdziwe imię dziecka i jego miejsce zamieszkania.

Dużą rolę w poszerzaniu wiedzy dotyczącej gier oraz ochrony młodzieży w Europie przed nieodpowiednią treścią gier odgrywa system PEGI.[5] System PEGI (*Pan European Games Information*) stanowi klasyfikację gier interaktywnych, której zadaniem jest pomóc w określeniu, czy dana gra jest odpowiednia dla dziecka. Celem systemu PEGI jest zagwarantowanie tego, by nieletni nie mieli styczności z grami, które są nieodpowiednie dla danej grupy wiekowej. PEGI jest wspierany przez głównych producentów konsol, a także wydawców i twórców gier interaktywnych oraz dostarcza rodzicom ujednolicony system klasyfikacji wiekowej dla wszystkich gier w większości państw europejskich. W ostatnich kilku latach system *Pan European Game Information* (PEGI) oferował rodzicom szczegółowe zalecenia, co do tego, czy treść danej gry jest odpowiednia dla młodzieży. Cechą systemu PEGI jest podawanie wiarygodnych, łatwych do zrozumienia informacji w postaci etykiet z oznaczeniem wieku i opisem treści na opakowaniach gier, dzięki którym można świadomie podejmować decyzje o ich zakupie. Zgodnie z informacjami na witrynie *http://www.xbox.com/pl-PL/Marketplace/gameratings*, gry zawierające pewne drażliwe treści w Wielkiej Brytanii mogą też być klasyfikowane przez BBFC (tak jak filmy na DVD lub kasetach VHS). Jedynym większym państwem europejskim, które nie stosuje systemu PEGI, są Niemcy, gdzie obowiązuje odrębny obowiązkowy system o nazwie USK. Rodzice oraz dzieci mogą także korzystać z PEGI *Online*. PEGI *Online* to nowy element systemu PEGI. Jego celem jest lepsza ochrona młodzieży w Europie przed nieodpowiednią treścią gier i pomoc rodzicom w poznaniu ryzyka i potencjalnych szkód, które te gry mogą nieść ze sobą. PEGI *Online* opiera się na czterech filarach:

- Kodeksie bezpieczeństwa PEGI *Online* (PEGI *Online Safety Code*) i Umowie ramowej podpisywanej przez wszystkich uczestników;
- logo PEGI *Online* eksponowanym przez licencjobiorców;
- specjalnej witrynie internetowej dla wnioskodawców i wszystkich użytkowników;
- procesie niezależnej administracji, poradnictwa i rozstrzygania sporów.

Na stronie systemu PEGI *Online* użytkownik znajdzie dokładną definicję oraz klasyfikację gier internetowych. Ponieważ trudno jest opisać precyzyjnie style i rodzaje gier, przyjmuje się, że obecnie istnieją cztery główne rodzaje gier internetowych. Są to: minigry / Gry przez przeglądarkę (*browser games*), gry promocyjne (*advergames*), gry sieciowe oraz gry typu *Massively Multiplayer*. Szczególną uwagę ze względu na bezpieczeństwo dziecka należy zwrócić na gry typu *Massively Multiplayer*. Gry te różnią się od innych gier internetowych pod dwoma względami: w rozgrywce uczestniczy jednocześnie wielu graczy oraz gra jest ciągła (tzn. jest kontynuowana niezależnie od tego, czy konkretny gracz w niej uczestniczy, czy nie).

Gry tego typu przedstawiają bogaty, trójwymiarowy świat zaludniony tysiącami graczy. Na stronie *http://www.pegionline.eu/pl/index/id/171/* można znaleźć informację, że gra *World of Warcraft* firmy Blizzard Entertainment/Vivendi Game ma ponad 6 milionów abonentów (1 milion w Europie i ponad 1,5 miliona

[5] *http://www.xbox.com/pl-PL/Marketplace/gameratings*

w Chinach). *Everquest* uważany niegdyś za lidera rynku ma około 500 000 abonentów, a Ultima Online 250 000. Są to przeważnie gry fabularne (*role-playing games*), w których uczestnicy grają role fikcyjnych postaci i wspólnie tworzą lub kontynuują akcję. Gry te są powszechnie znane pod nazwą MMORPG (*Massively Multiplayer Online Role-Playing Games* – internetowe gry fabularne dla wielu graczy). Wiele gier MMORPG prowadzi do powstania wirtualnych społeczności. Może to narazić graczy na ryzyko związane z interakcjami w czasie rzeczywistym z nieznanymi partnerami w grze. Należy zwrócić uwagę na zagrożenia w tym zakresie: tworzone w wyniku prowadzenia gry treści, mogą być nieodpowiednie dla młodzieży i niezgodne z oceną nadaną danej grze, niektórzy gracze zachowują się w sposób nieodpowiedni dla młodzieży, na przykład używają nieodpowiedniego lub obelżywego języka, są napastliwi, uczestnicząc w grach umożliwiających komunikację tekstową, głosową lub wzrokową, dopuszczają się nieuczciwych zachowań, takich jak oszukiwanie i podsłuchiwanie lub podglądanie, albo zachowują się agresywnie, może dojść do naruszenia prywatności. Udział w tego typu grach internetowych czasem zachęca dzieci do nawiązywania kontaktów, podawania informacji o sobie, a nawet spotykania się z nieznanymi osobami poza grą. Na stronie systemu PEGI *Online* zarówno rodzic jak i dziecko znajdzie dokładne wskazówki jak zachować się w takiej sytuacji.

Rysunek nr 2: Strona systemu PEGI Online
Źródło: *http://www.pegionline.eu/pl/index/id/171/*

3. *Expression Blend,* język C# i *Visual Studio* w procesie tworzenia gier

Firma Microsoft od połowy 2006 roku publikuje wersje trial swoich najnowszych produktów dla osób zajmujących się interaktywnym tworzeniem stron WWW i aplikacji webowych. Zestaw proponowanych narzędzi nosi nazwę *Expression Studio*. W procesie tworzenia interaktywnych stron WWW istotnymi czynnikami wpływającymi na końcowy efekt pracy są: wybór odpowiedniej technologii, skomplikowanie narzędzi, możliwości współpracy grafika i programisty, możliwości współpracy wielu narzędzi i sposób wymiany danych między nimi. W pakiecie *Expression Studio* uwzględniono najistotniejsze elementy wpływające na proces budowy i strukturę tworzonych aplikacji. W skład pakietu wchodzą następujące produkty: *Expression Web, Expression Blend, Expression Design, Expression Encoder [http://www.idg.pl/news/342397/Expression.Studio.3.0. pierwsze.bety.za.plotem.html* Dawid Długosz]. Microsoft wydał także czwartą wersję swojej platformy Silverlight. Technologia ta działa jako *plugin* do przeglądarek i umożliwia programowanie aplikacji. Technologię *Silverlight* stworzono do wyświetlania treści multimedialnych z wykorzystaniem zasobów sprzętowych użytkownika. *Silverlight* powstał z myślą o bogatych aplikacjach internetowych (RIA). W *Silverlight* można wykorzystać całe środowisko .NET i znane programistom języki: C# czy VB.NET. Pozwala to na łatwe przejście ze standardowych aplikacji (również wielowątkowych) do świata *Silverlight*. Zintegrowane środowisko programistyczne wykorzystywane do pracy z *Silverlightem* to najczęściej *Visual Studio Microsoftu*. Darmową wersję *Visual Studio 2008*, również do zastosowań komercyjnych, można pobierać ze strony *Microsoftu.*[6] Do pracy potrzebne jest jeszcze środowisko uruchomieniowe *Silverlighta* i SDK.[7]

Visual Studio ze środowiskiem uruchomieniowym *Silverlight* oraz *Expression Blend + SketchFlow* to dwa najczęściej wykorzystywane programy do tworzenia i edycji aplikacji wykorzystujących technologię *Silverlight*. C# jest językiem programowania przeznaczonym dla platformy NET. W założeniach twórców miał on być prosty w użyciu, nowoczesny, wszechstronny i w pełni obiektowy. Popularność oraz uznanie profesjonalistów świadczą o tym, że cel ten został osiągnięty. Język programowania C# został zaprojektowany specjalnie dla firmy *Microsoft*. C# czerpie najlepsze wzorce z języka Java oraz C++. Język C# zawiera bogatą bibliotekę klas pozwalających na tworzenie i rozwijanie aplikacji okienkowych, bazodanowych, a także dynamicznych aplikacji internetowych.

[6] *http://www.microsoft.com/expre...*
[7] *http://www.internetmaker.pl/artykul/6593,1,silverlight_-_pierwsze_kroki.html*
http://silverlight.net/getstar...