EDUKACJA MEDIALNA

W ŚWIECIE PONOWOCZESNYM

pod redakcją
Bronisława Siemienieckiego

Wydawnictwo
Naukowe
Uniwersytetu
Mikołaja Kopernika

EDUKACJA MEDIALNA
W ŚWIECIE PONOWOCZESNYM

pod redakcją naukową
Bronisława Siemienieckiego

WYDAWNICTWO NAUKOWE
UNIWERSYTETU MIKOŁAJA KOPERNIKA

Toruń 2012

Recenzenci

Maria Kozielska
Marek Sokołowski

Opieka redakcyjna

Wioletta Kwiatkowska

Projekt okładki

Monika Pest

Na okładce wykorzystano pracę
© vladgrin – Fotolia.com

Publikacja dofinansowana przez Urząd Marszałkowski
Województwa Kujawsko-Pomorskiego w Toruniu

Printed in Poland

ISBN 978-83-231-2987-5

WYDAWNICTWO NAUKOWE UMK
ul. Gagarina 5, 87-100 Toruń
REDAKCJA: tel. (56) 611 42 95; fax (56) 611 47 05
e-mail: wydawnictwo@umk.pl
DYSTRYBUCJA: ul. Reja 25, 87-100 Toruń
tel./fax (56) 611 42 38, e-mail: books@umk.pl
www.wydawnictwoumk.pl
DRUK: Wydawnictwo Naukowe UMK

Spis treści

EDUKACJA MEDIALNA
W ŚWIECIE PONOWOCZESNYM
POD REDAKCJĄ
BRONISŁAWA SIEMIENIECKIEGO
TORUŃ 2012

BEATA STACHOWIAK
KATEDRA EUROPY WSCHODNIEJ
WYDZIAŁ POLITOLOGII I STUDIÓW MIĘDZYNARODOWYCH
UNIWERSYTET MIKOŁAJA KOPERNIKA
TORUŃ

PROBLEMATYKA BEZPIECZEŃSTWA I ZAGROŻENIA JEDNOSTKI W SPOŁECZEŃSTWIE INFORMACYJNYM – PODSTAWY PROGRAMOWE I STANDARDY KSZTAŁCENIA A WYMAGANIA RZECZYWISTOŚCI

WSTĘP

Przełom drugiego i trzeciego tysiąclecia oraz, jak na razie, pierwsza dekada XXI wieku to czas globalizacji i rozwoju społeczeństwa informacyjnego. Społeczeństwa, które może być rozpatrywane w wielu kontekstach, w tym także jako nowy, dynamiczny i nieliniowy system. Ten zaś układ może być postrzegany jako system cybernetyczny i jako globalne społeczeństwo ryzyka[1]. W takim układzie szczególnej wartości i znaczenia nabiera dyskusja na temat bezpieczeństwa i zagrożeń w globalnym społeczeństwie informacyjnym.

[1] P. Sienkiewicz, *Bezpieczeństwo i wolność w globalnym społeczeństwie informacyjnym*, dostępny w Internecie: http://www.dobrauczelnia.pl/upload/File/KONFERENCJE/BAZPIECZENSTWO/sienkiewicz.pdf [4.05.2011].

Hasła bezpieczeństwo używa się do określenia stanu pewności, spokoju, braku zagrożenia. Według Abrahama Maslowa potrzeba bezpieczeństwa zajmuje drugie miejsce w hierarchii potrzeb ludzkich, tuż za potrzebami fizjologicznymi – to bardzo wysoka lokata. Należy podkreślić, że bezpieczeństwo jest nie tylko podstawową potrzebą jednostek, ale także grup społecznych i państw. Niezaspokojenie tej potrzeby skutkuje odczuwaniem niepokoju oraz poczuciem zagrożenia. Stany bezpieczeństwa i zagrożenia są zatem ze sobą ściśle związane na zasadzie antonimu. Problematyka bezpieczeństwa oraz zagrożeń zawsze była obecna w działaniach i rozważaniach ludzkości, tylko że wraz z upływem wieków i tysiącleci zmieniały się spojrzenia ludzi na te kwestie. Jest to naturalne, gdyż, podobnie jak ludzkość, również niebezpieczeństwa ewaluowały. Kiedyś zagrożeniem dla człowieka był spadek temperatury poniżej zera, ponieważ dla ludzi niepotrafiących wykrzesać ognia sytuacja taka była groźna. Lęk budziły także takie naturalne zjawiska jak zaćmienie Słońca[2], Księżyca. Przez wiele stuleci poczucie zagrożenia wywoływały również choroby zakaźne[3], dziś wiele z nich dzięki szczepieniom ochronnym oraz antybiotykom i lekom antywirusowym jest dla ludzkości tylko mrocznym wspomnieniem. Jednak należy pamiętać o tym, że pojawiły się nowe schorzenia[4] i nadal część z nich jest nieuleczalna[5]. Obserwacje wskazują na to, że ludzkość oswa-

[2] Wystarczy sobie w tym miejscu przypomnieć scenę zaćmienia Słońca, opisaną przez Bolesława Prusa w powieści pt. *Faraon*.

[3] O lęku ludzi przed chorobami, których dróg rozprzestrzeniania ludzkość długo nie znała, świadczą chociażby słowa hymnu religijnego *Święty Boże*. W pieśni tej, według polskiej tradycji kościelnej, pierwszą strofę sublikacji stanowi inwokacja: hymn *Święty Boże*, po którym następuje właściwa suplikacja zawarta w słowach: „Od powietrza, głodu, ognia i wojny. Wybaw nas Panie! Od nagłej i niespodziewanej śmierci. Zachowaj nas Panie! My grzeszni Ciebie Boga prosimy. Wysłuchaj nas Panie!" dodanych w XVIII wieku, kiedy czarna śmierć, czyli dżuma (morowe powietrze) zbierała obfite żniwo w Europie (w Gdańsku 18 tysięcy, a w Londynie 35 tysięcy ofiar).

[4] Do nowych chorób należą między innymi te, które pojawiają się w wyniku przekraczania przez wirusy barier między gatunkami, oraz te, które stanowią nowe odmiany wirusów i bakterii: SARS (zespół ostrej ciężkiej niewydolności oddechowej), HIV (zespół nabytego braku odporności) i inne.

[5] Należy do nich np. większość chorób genetycznych: achorondroplazja, dystrofia mięśniowa Duchenne'a i inne.

ja zagrożenia wokół siebie, potrafi z nimi walczyć oraz im przeciwdziałać. Jednak, co należy podkreślić, w miejsce ujarzmionych lęków i niebezpieczeństw pojawiają się nowe.

Pojawianie się nowych zagrożeń, które są często związane z rozwojem technologicznym, jest znane ludzkości od jej zarania. I także obecnie to zjawisko ma miejsce, gdyż rozwój między innymi technologii informacyjno-komunikacyjnych generuje wiele nowych potencjalnie niebezpiecznych sytuacji. Dlatego też tak ważnym obszarem dyskusji staje się temat bezpieczeństwa i zagrożeń w społeczeństwie informacyjnym. Problematykę tę można rozważać z punktu widzenia jednostki, grupy społecznej czy też państwa. Obszar dyskusji jest więc bardzo szeroki. W poniższym artykule autorka skupi się jedynie na tematyce bezpieczeństwa i zagrożeń wobec jednostki w społeczeństwie informacyjnym.

Zagrożenia jednostki w społeczeństwie informacyjnym

Stan zagrożenia jednostki w społeczeństwie informacyjnym można rozumieć jako pewien stan psychiczny lub świadomościowy, który jest spowodowany postrzeganiem przez jednostkę pewnych zjawisk charakterystycznych dla społeczeństwa informacyjnego jako niekorzystnych lub niebezpiecznych dla człowieka. Odbiór może mieć charakter subiektywny, aczkolwiek niektóre z czynników wywołujących zagrożenia w społeczeństwie informacyjnym mają charakter obiektywny. Rodzaju i poziomu zagrożeń nie można określić mianem constans, gdyż charakteryzują się swoistą dynamiką uzależnioną od tempa rozwoju technologii informacyjno-komunikacyjnych, od ich zasięgu i popularności, a także od poziomu świadomości użytkowników. Oznacza to, że zagrożenia w społeczeństwie informacyjnym są funkcją wielu zmiennych, w tym także niewspomnianego wcześniej czasu. Z kolei bezpieczeństwo jednostki w społeczeństwie informacyjnym można pojmować jako stan pewności, spokoju, braku zagrożenia ze strony czynników charakterystycznych dla społeczeństwa informacyjnego.

Poniżej zostaną przedstawione zagrożenia dla jednostki w społeczeństwie informacyjnym, dla ułatwienia opis ten zostanie wzbogacony rysunkiem. W obszarze „życie rodzinne i osobiste" mieści się wiele zagrożeń dla jednostki. Wśród nich możemy odnaleźć:

1. Drastyczne powiększenie się dystansu międzypokoleniowego spowodowanego rozwojem technologii.
2. Nowe uzależnienia, w tym między innymi technoholizm[6].
3. Technostres[7].
4. Technofobia[8].
5. Poczucie osamotnienia jednostki w rodzinie, często spowodowane zastąpieniem kontaktów osobistych kontaktami wirtualno-technologicznymi.
6. Brak poczucia stabilizacji spowodowane stałym przemieszczaniem się ludzi w poszukiwaniu pracy bądź lepszej posady.
7. Wypieranie się przez rodziny funkcji wychowawczej na rzecz szkoły i mediów.
8. Zanikanie rodzin wielopokoleniowych z powodu narastania problemów związanych z opiekuńczą funkcją rodziny nad dziećmi, osobami starszymi i chorymi.

W sferze określanej mianem „praca zawodowa" do zagrożeń jednostki wynikających z rozwoju społeczeństwa informacyjnego należy zaliczyć:

1. Dehumanizacja stosunków między pracownikami, a także pracownikami a pracodawcami oraz pracownikami a petentami.
2. Ograniczenie osobistych kontaktów i wzrost poczucia osamotnienia.

---

[6] Technoholizm to rodzaj uzależnienia człowieka od środków technicznych. Osoba uzależniona cierpi między innymi z powodu stanów lękowych, zaburzeń snu i apetytu. Dochodzą do tego też trudności z koncentracją. Najliczniejszą grupę wśród technoholików stanowią osoby uzależnione od Internetu.

[7] Technostres można rozumieć jako fizjologiczną i psychologiczną reakcję człowieka na działanie stresora, w tym przypadku nowoczesnych technologii. Technostres może objawiać się między innymi: niepokojem, drażliwością, psychicznym zmęczeniem, depresją, koszmarami sennymi, paniką, bólami głowy, spadkiem odporności, bólami mięśniowymi, poczuciem ogólnej bezsilności itd.

[8] Technofobia to chorobliwy lęk przed techniką, w tym także przed komputerami i innymi urządzeniami elektronicznymi.

3. Zwiększenie liczby bezrobotnych spowodowanej automatyzacją szczególnie czynności odtwórczych.
4. Zmiana struktury zatrudnienia, narastanie konieczności ciągłego szkolenia i poszerzania kwalifikacji czy nawet przekwalifikowania się.
5. Wydłużenie okresu pracy.
6. Zwiększenie nadzoru pracowników przez pracodawców z użyciem nowych technologii – syndrom „Wielkiego Brata".
7. Zanikanie granic między czasem pracy a czasem wypoczynku, np. w wyniku telepracy[9].

Kolejną sferą jest „edukacja i nauka", w niej także mieszczą się zagrożenia wywołane rozwojem technologicznym:

1. „Przeładowanie" informacyjne.
2. Zmniejszenie się kontroli w zakresie praw autorskich.
3. Wyłonienie się wąskiej elity hamującej dostęp do informacji.
4. Groźba prymatu technologii nad nauczycielami.
5. Ślepa wiara w technologie informacyjno-komunikacyjne, brak zainteresowania czytelnictwem.
6. Niska ocena pewnych dziedzin nauki.
7. Fragmentaryzacja wiedzy.
8. Dehumanizacja stosunków międzyludzkich, szczególnie bolesna w placówkach edukacyjnych.

Interesującym obszarem rozważań nad zagrożeniami jednostki w społeczeństwie informacyjnym jest także płaszczyzna, na której następuje styk jednostki i społeczeństwa, w tym przypadku można zdefiniować takie zagrożenia, jak:

1. Dehumanizacja relacji w społeczeństwie.
2. Kontrola i zmniejszenie zakresu prywatności – liczne zagrożenia i naruszania prywatności.
3. Zwiększenie się zróżnicowania społeczeństwa wskutek poszerzania grup społecznych objętych wykluczeniem cyfrowym[10].

---

[9] Telepraca to forma świadczenia pracy poza siedzibą firmy za pośrednictwem środków technologii informacyjno-komunikacyjnej.

[10] Wykluczenie cyfrowe, zwane także podziałem cyfrowym, to stratyfikacja społeczeństwa, w którym linia podziału jest tworzona przez dostęp lub jego brak do In-

4. Analfabetyzm komputerowy.
5. Pojawienie się nowych form przestępczości godzących w jednostkę.
6. Manipulowanie informacją.
7. Nieprzestrzeganie praw obywateli społeczeństwa informacyjnego[11].

Zagrożenia także tkwią w sferze określonej „opieka zdrowotna":

1. Dehumanizacja opieki medycznej – pacjent często staje się tylko rekordem.
2. Nowe choroby związane z rozwojem technologii.
3. Uzależnienie systemów opieki zdrowotnej od systemów komputerowych.

Jest jeszcze jedna kategoria nazwana „jednostka – administracja publiczna", w niej także można umieścić zagrożenia, które są związane z jednostką oraz administracją publiczną tak bardzo wspieraną przez nowe technologie. Należą do nich:

1. Dehumanizacja stosunków międzyludzkich w sektorze administracji publicznej.

---

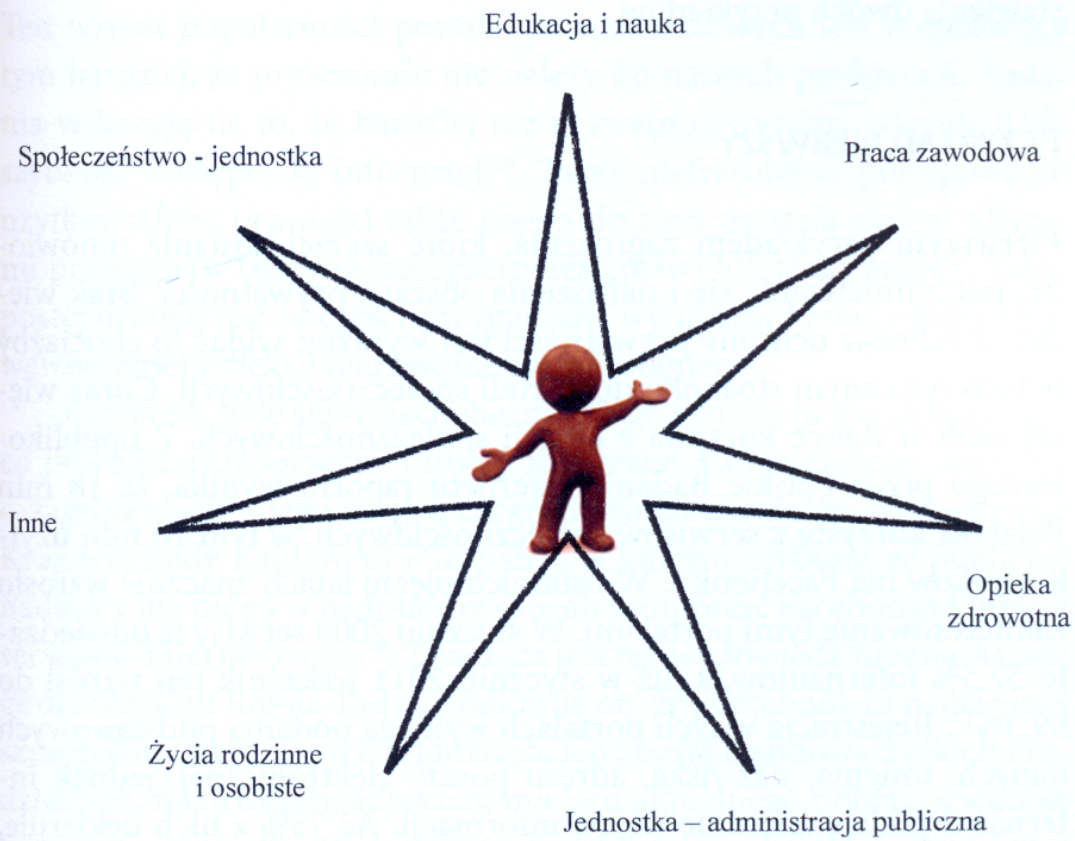
ternetu i innych nowoczesnych form komunikacji. Zjawisko to wynika przede wszystkim z szybkiego rozwoju technologii informacyjno-komunikacyjnych. Należy jednak pamiętać, iż czynnikiem wywołującym ten podział jest nie tylko fizyczny dostęp do Internetu i nowych technologii, ale także brak umiejętności posługiwania się nimi, niska przepustowość sieci, a także brak znajomości języków obcych.

[11] W roku 1999 CEPIS wyszedł z inicjatywą stworzenia Karty Praw Obywateli Społeczeństwa Informacyjnego. Zgodnie z założeniami karta ta miała zagwarantować obywatelom ich tradycyjne prawa oraz dostęp do informacji. Główne założenia Karty zostały ujęte w pięciu punktach.

1. Dostęp do Internetu oraz zasobów informacyjnych powinien być powszechny.
2. Informacja powinna spełniać oczekiwania dotyczące jej zawartości, nie może wprowadzać w błąd.
3. Wszelkie dane o zgodnych z prawem zachowaniach i interesach obywateli społeczeństwa informacyjnego nie mogą być wykorzystywane przeciwko nim.
4. Wszyscy obywatele powinni być pewni, że będą im dostępne środki zadośćuczynienia w przypadku naruszenia autentyczności lub prywatności informacji.
5. Społeczności mają obowiązek umożliwienia obywatelom zdobywania umiejętności potrzebnych do uczestniczenia w społeczeństwie informacyjnym.

Niestety, w dniu dzisiejszym ta inicjatywa jest zapomniana.

2. Zbieranie wielu danych, często wrażliwych, na temat obywateli.
3. Dostęp do danych przez osoby nieupoważnione.
4. Pojawienie się możliwości popełnienia nowych przestępstw, w tym także przeciwko dokumentom.
5. Wycieki danych.



Rys. 1. Człowiek i obszary zagrożeń w społeczeństwie informacyjnym

Źródło: opracowanie własne.

Na rysunku 1. ujęto jeszcze kategorię „inne", w niej mogą mieścić się te zagrożenia, które nie znalazły się w poprzednich obszarach lub jeszcze nie zostały ujawnione i zdefiniowane. Powyższy przegląd zagrożeń dla jednostki w społeczeństwie informacyjnym ukazuje, jak poważne jest to zjawisko oraz jak rozległe. Niektóre z niebezpieczeństw są związane bezpośrednio z nowymi technologiami, inne są pośrednim skutkiem użytkowania nowych wynalazków. Nie ma żadnych wątpliwości, że człowiek powinien być świadomy tych niebezpieczeństw. Po

pierwsze, aby aktywnie funkcjonować w społeczeństwie informacyjnym. Po drugie, aby podejmować w sposób świadomy decyzje związane z profilaktyką zagrożeń lub działaniami dotyczącymi samych sytuacji niebezpiecznych. Niestety, wyniki obserwacji oraz badań wskazują na to, że w Polsce (i nie tylko) poziom wiedzy w tym obszarze jest niewystarczający. Autorka, aby uzasadnić tę tezę, ograniczy się do przedstawienia dwóch przykładów.

PRZYKŁAD PIERWSZY

Pierwszym przykładem zagrożenia, które szerzej zostanie omówione, jest zmniejszanie się i naruszenia obszaru prywatności. Brak wiedzy w zakresie ochrony prywatności jest wyraźny, widać to chociażby w bezkrytycznym stosunku do portali społecznościowych. Coraz więcej osób w Polsce korzysta z portali społecznościowych. Z opublikowanego przez Polskie Badania Internetu raportu wynika, że 18 mln Polaków korzysta z serwisów społecznościowych, w tym 10 mln użytkowników ma Facebook[12]. W ostatnich pięciu latach znacznie wzrosło zainteresowanie tymi portalami. W styczniu 2006 serwisy te odwiedzało 57,5% internautów, a już w styczniu 2011 wskaźnik ten wzrósł do 99,3%[13]. Rejestracja w tych portalach wymaga podania podstawowych danych: imienia, nazwiska, adresu poczty elektronicznej, jednak internauci podają znacznie więcej informacji. Aż 75% z nich deklaruje, że udostępnia swoją datę urodzenia, 68% swoje zdjęcie, a 83% dane o miejscu zamieszkania[14]. Czynią to, w większości przypadków nie zastanawiając się nad tym, że podane przez nich dane będą dostępne dla bardzo wielu osób. Tym samym poziom prywatności osoby korzystającej bezkrytycznie i bezmyślnie z portalu społecznościowego dąży do zera. Problem niedbania o swoją prywatność dotyczy bardzo wielu

[12] Polski Megapanel ocenia użytkowników Facebooka na dziesięć milionów realnych użytkowników, natomiast oficjalne statystyki Facebooka podają sześć milionów realnych kont (Ratuszniak 2011b).

[13] Raport PBI: Prywatność i własny wizerunek w przestrzeni social media.

[14] Ibidem.

osób, gdyż jedynie 7% internautów nie ma konta na portalu społecznościowym, a znaczna ich część ma takie konta w kilku miejscach[15]. Według danych publikowanych przez Polskie Badania Internetu najbardziej popularnym w Polsce portalem społecznościowym jest Nasza Klasa – 78% wskazań, na drugim miejscu znajduje się Facebook – 68%, a na trzecim jest Grono ze wskaźnikiem wynoszącym zaledwie 13%. Ten wzrost popularności portali społecznościowych jest niepokojący tym bardziej, że prywatność nie należy do naszych preferencji. Badania wskazują na to, że bardziej niż prywatność cenimy wygodę bądź szybkość dostępu do informacji[16]. Także niefrasobliwe postępowanie użytkowników prowadzi także często do tego, że stają się oni ofiarami przestępstw (nie zawsze cyberprzestępstw) lub tracą pracę[17]. Takie postępowanie jest w części przypadków wynikiem braku wiedzy oraz wewnętrznej refleksji nad swoim postępowaniem.

Facebook staje się wszechobecny, a jego promocja jest natarczywa, co powoli budzi sprzeciw i uwagi krytyczne. Coraz częściej mówi się o zagrożeniach z jego strony, czego dowodzi chociażby oświadczenie Krajowej Rady Radiofonii i Telewizji, w którym czytamy, że publiczni nadawcy nie mogą w nadmierny sposób promować Facebooka i innych serwisów internetowych[18]. Znacząca jest też wypowiedź Juliana Assange dla telewizji Russia Today, podkreśla on, że „Facebook to najbardziej szczegółowa baza danych o ludziach, ich kontaktach towarzyskich i rodzinnych, nazwiskach, adresach, miejscu aktualnego pobytu, sposobie komunikowania się. Wszystko to znajduje się w USA i dostępne jest amerykańskim organizacjom wywiadowczym"[19]. To wynik domyśl-

[15] Ibidem.

[16] H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life,* Stanford 2009, Stanford University Press, ISBN: 0804752362.

[17] W tym miejscu jako przykłady należy podać: postępowania działów rekrutacyjnych, które styl życia potencjalnych pracowników oceniają na podstawie profili na portalach społecznościowych. Innym przykładem mogą być przypadki utraty pracy po umieszczeniu nieprzychylnych firmie wpisów na Facebooku itp.

[18] B. Ratuszniak, *„Facebookowi" w Polsce stuknęło 6 milionów kont,* Dostępny w Internecie: http://interaktywnie.com/biznes/artykuly/social-media/facebookowi-w-polsce-stuknelo-6-milionow-kont-20110, [dostęp: 4.05.2011].

[19] Onet 2011.

nych ustawień na portalach społecznościowych, które pozwalają na ujawnianie wielu danych o rodzinie, edukacji, przebiegu kariery zawodowej. Ponadto wielu użytkowników akceptuje zaproszenia od nieznajomych, nie zawsze wiedząc, kto proponuje znajomość – prowadzi to do zwiększenia dostępu do informacji. Z psychologicznego punktu widzenia trudno się oprzeć takim zaproszeniom, świadczą one w pewnym stopniu o popularności czy też interpersonalnej atrakcyjności. Innym skutkiem beztroskiego zachowania na portalu społecznościowym jest fakt wykorzystywania przez firmy zdjęć użytkowników portali na banerach reklamowych bez ich zgody. Taka możliwość jest wynikiem jednego kliknięcia na przycisk I like.

Innym negatywnym skutkiem braku troski, a przede wszystkim wiedzy o prywatności w sieci, jest mityczne wręcz przekonanie o rzekomej w niej anonimowości. Wielu osobom wydaje się, że nick gwarantuje pozycję incognito w Internecie. To jednak jest złudne przekonanie. Tropy naszych wirtualnych wędrówek pozostają w wielu miejscach: są to loga odwiedzanych przez nas serwisów internetowych (dane o numerze IP), historia przeglądarek internetowych, archiwa forów dyskusyjnych, grup dyskusyjnych. Stąd chociażby pojawiające się w skrzynkach pocztowych reklamy produktów oraz usług. Nie można także zapominać o programach szpiegujących, spyware zdradza upodobania użytkowników sieci. Sami także instalujemy rozmaite aplikacje, tzw. toolbary, które ułatwiają nam co prawda codzienne życie, ale zapamiętują nasze preferencje i mogą je przekazywać dalej. Oddzielnym tematem jest uszanowanie cudzej prywatności.

PRZYKŁAD DRUGI

Drugim przykładem zagrożeń wobec jednostki w społeczeństwie informacyjnym jest przestępczość komputerowa, która dotyka zarówno sfery życia zawodowego, jak i prywatnego. Człowieka mogą dotykać przestępstwa nie tylko nakierowane na jednostkę, ale także na grupy ludzkie. Jednostka musi być świadoma istniejących przestępstw nie tylko po to, aby nie stać się ofiarą, ale także po to, aby nie stać się mimowolnym

przestępcą. Nieznajomość prawa nie zwalnia od odpowiedzialności za swoje czyny. Przestępczość komputerowa pojawiła się i istnieje równolegle z rozwojem komputeryzacji. Nowe rozwiązania technologiczne pociągają powstawanie nowych przestępstw. Definicji przestępczości komputerowej jest wiele, na ogół rozumie się ją jako wszelkie zachowania przestępne związane z funkcjonowaniem elektronicznego przetwarzania danych. Ważne jest to, że są to czyny przestępcze popełnione za pomocą elektronicznych systemów przetwarzania danych (komputer jako narzędzie przestępstwa), ale także i czyny skierowane przeciwko takiemu systemowi. W obowiązującym w Polsce kodeksie karnym[20] przestępstwa komputerowe są ujęte w kilku rozdziałach. Mimo licznych głosów nie ma w polskim kodeksie karnym oddzielnego rozdziału poświęconego przestępstwom komputerowym. I tak, można wyróżnić:

- przestępstwa przeciwko ochronie informacji[21],
- przestępstwa przeciwko mieniu[22],
- przestępstwa przeciwko bezpieczeństwu powszechnemu[23],
- przestępstwa przeciwko Rzeczypospolitej Polskiej[24],
- przestępstwa przeciwko wiarygodności dokumentów[25].

Do pierwszej grupy przestępstw należy hacking komputerowy (włamanie do komputera oraz kradzież danych), podsłuch komputerowy (nieuprawnione przechwycenie informacji), bezprawne niszczenie informacji, sabotaż komputerowy. W grupie drugiej wymienia się nielegalne uzyskanie programu komputerowego, paserstwo programu komputerowego, oszustwo komputerowe, oszustwo telekomunikacyjne, kradzież karty uprawniającej do podjęcia pieniędzy z automatu bankowego. W trzeciej grupie mieszczą się takie poważne przestępstwa jak: sprowadzanie niebezpieczeństwa dla życia lub zdrowia wielu osób albo mienia w znacznych rozmiarach, nieumyślne zakłócenie automatycznego przetwarzania informacji związane ze sprowadzeniem nie-

---

[20] Kodeks karny – DzU Nr 88, poz. 553 z roku 1997.
[21] Rozdział XXXIII art. 267 § 1 i 2, art. 268 § 2 oraz art. 296 § 1 i 2 kk.
[22] Rozdział XXXV art. 278 § 2 i 5, art. 285 § 1, art. 287 § 1 oraz art. 293 § 1 kk.
[23] Rozdział XX art. 165 § 1 ust. 4, art. 165 § 2 i art. 167 § 2 kk.
[24] Rozdział XVII art. 130 § 2 i 3 oraz art. 138 § 2 kk.
[25] Rozdział XXXIV art. 270 § 1 kk.

bezpieczeństwa powszechnego, zamach terrorystyczny na statek morski lub powietrzny. W grupie przestępstw przeciwko Rzeczypospolitej Polskiej znajduje się szpiegostwo komputerowe albo wywiad komputerowy oraz szpiegostwo albo wywiad komputerowy na szkodę państwa sojuszniczego. W grupie piątej mieszczą się fałszerstwa komputerowe.

Można jeszcze wyróżnić także inne rodzaje przestępstw, których podstawa prawna jest zawarta w innych ustawach. Oto niektóre z nich, np. nielegalne kopiowanie, rozpowszechnianie lub publikowanie prawnie chronionego programu komputerowego[26]. Do tej grupy przestępstw należy również włączyć: przywłaszczenie sobie autorstwa lub wprowadzenie w błąd co do autorstwa programu lub jego części[27], rozpowszechnianie programu komputerowego bez podania nazwiska autora[28], inne naruszenie cudzego prawa autorskiego w celu uzyskania korzyści majątkowej[29], rozpowszechnianie bez upoważnienia lub wbrew warunkom upowszechniania cudzego programu komputerowego[30], utrwalanie lub zwielokrotnianie bez uprawnienia lub wbrew jego warunkom cudzego programu komputerowego[31], paserstwo nośnika programu komputerowego[32], uniemożliwienie lub utrudnianie wykonywania prawa do kontroli korzystania z programu[33]. Natomiast na podstawie ustawy o ochronie topografii układów scalonych przestępstwem komputerowym jest nielegalne kopiowanie układów scalonych[34].

Komputeryzacja może być także wykorzystywana do popełniania innych przestępstw: przekazywania materiałów pornograficznych, w tym pedofilskich, propagowania treści szerzących rasizm, nazizm, antysemityzm, przemoc, pośredniczenia w nawiązywaniu

---

[26] Ustawa o prawie autorskim i prawach pokrewnych, DzU Nr 24 poz. 83 z dnia 4 lutego 1994 roku, art. 1 ust. 2, p. 1.

[27] Ibidem, art. 111 ust. 1.

[28] Ibidem, art. 115 ust. 2.

[29] Ibidem, art. 115 ust. 3.

[30] Ibidem, art. 116 ust. 1.

[31] Ibidem, art. 117 ust. 1.

[32] Ibidem, art. 118.

[33] Ibidem, art. 119.

[34] Ustawa o ochronie topografii układów scalonych, Dz U Nr 100, poz. 498 z 1992 roku, art 42.

kontaktów seksualnych, w tym także o charakterze pedofilskim. Nie można zapominać także o tym, iż grupy przestępcze wykorzystują systemy komputerowe do popełniania przestępstw o charakterze gospodarczym, czyli oszustw, nielegalnych transferów finansowych. Wspominając o innych przestępstwach, nie można także pominąć cybelstalkingu[35] – ofiary często nie wiedzą, jak w takiej sytuacji się zachować.

Obserwacja oraz wyniki niektórych badań wskazują na to, że w Polsce nie jest najlepiej ze znajomością problematyki przestępstw komputerowych. Świadczy o tym chociażby skala piractwa komputerowego w naszym kraju. Według badań, które przeprowadzono za rok 2010 na zlecenie BSA[36] w krajach Unii Europejskiej, skala piractwa komputerowego w Polsce wynosi 54%, a wartość użytkowanego nielegalnego oprogramowania wyniosła 553 milionów dolarów. Wyższe wskaźniki zanotowano jedynie w czterech państwach: na Łotwie – 56%, w Grecji – 59%, w Rumunii – 64% oraz w Bułgarii – 65% (Baranowska-Skimina 2011). Innym przykładem wynikającym z nieznajomości problematyki zagrożeń przestępczością komputerową jest beztroski stosunek pracowników do wykorzystywania środków technologii informacyjno-komunikacyjnych w pracy. Zasoby elektroniczne mogą być rezerwuarem wirusów, trojanów, programów szpiegujących. Również uruchamianie w tle pewnych aplikacji czy też otwieranie stron internetowych może być źródłem przecieku danych. Niestety, większość pracowników nie zdaje sobie sprawy z tych zagrożeń. Pracownicy nie tylko korzystają z aplikacji, które są niezbędne w pracy, ale także wykonują wiele czynności online w celach prywatnych. Według wyników badań Pierwszego Ogólnopolskiego Badania Pracowników przeprowadzone-

[35] Cyberstalking – nękanie osoby z użyciem mediów elektronicznych, takich jak Internet czy telefonia komórkowa. Do cyberstalkingu zalicza się rozsyłanie kompromitujących materiałów w Sieci, włamanie na konta poczty elektronicznej, komunikatorów oraz portali społecznościowych w celu rozsyłania bądź rozmieszczania kompromitujących materiałów i wpisów, tworzenie ośmieszających bądź kompromitujących stron internetowych, wykonywanie komuś zdjęć, filmowanie go bez jego zgody.

[36] BSA, czyli Business Software Alliance, to międzynarodowa organizacja reprezentująca światowy przemysł informatyczny. Adres jej witryny internetowej to http://www.bsa.org [dostęp: 2.05.2012].

go w roku 2010 najbardziej popularne jest korzystanie z poczty – uzyskana punktacja 4,5 (w skali od 1 do 7[37]), przeglądanie stron WWW ze wskaźnikiem 4,4, natomiast korzystanie z serwisów społecznościowych znajduje się na miejscu piątym z wartością 2,4[38]. Te dane wskazują na to, że pracownicy nie widzą niczego zdrożnego w takim zachowaniu. Ale bardziej niebezpieczne jest to, że nie zdają sobie sprawy z tego, iż ich postępowanie może zagrozić między innymi bezpieczeństwu danych w firmie.

Przykłady można mnożyć, ale nawet ograniczenie się tylko do dwóch wskazuje na to, że Polakom brakuje wiedzy na temat zagrożeń, jakie niosą za sobą nowe technologie. Niestety, temat ten nie jest w dostateczny sposób omawiany ani podczas edukacji szkolnej, ani podczas studiów. W następnym podrozdziale zostaną omówione zapisy w podstawach programowych oraz standardach kształcenia, poświęcone bezpieczeństwu w społeczeństwie informacyjnym.

TEMATYKA BEZPIECZEŃSTWA I ZAGROŻEŃ W SPOŁECZEŃSTWIE INFORMACYJNYM A PODSTAWY PROGRAMOWE I STANDARDY KSZTAŁCENIA

Problematyka zagrożeń i działań na rzecz bezpieczeństwa dotyczy wszystkich obywateli społeczeństwa informacyjnego, nikt nie może uciec od tej tematyki bez względu na wiek, wykształcenie, wykonywany zawód, płeć czy też miejsce zamieszkania. Dlatego też konieczne jest ujęcie tej tematyki w podstawach programowych oraz w standardach kształcenia. Zdaniem autorki postulat ten nie jest spełniony, a zapisy w wymienionych dokumentach są niepełne i przestarzałe. Edukacja szkolna w Polsce jest podzielona na cztery etapy. Niezmiernie ważnym dokumentem jest *Podstawa programowa*, w tym przypadku tom obejmujący edukację matematyczną oraz techniczną. Analiza zapisów

[37] W badaniach tych 1 oznaczało nigdy, a 7 zawsze.

[38] Kobiety w badaniach tych deklarowały częstsze korzystanie z serwisów społecznościowych w pracy, wynik dla kobiet wynosił 2,6, a dla mężczyzn tylko 2,1.

wskazuje na to, iż uczeń kończący klasę trzecią, czyli pierwszy etap edukacji szkolnej, powinien znać „zagrożenia wynikające z korzystania z komputera, Internetu i multimediów"[39]. A dokładnie:

- Wiedzieć, że praca przy komputerze męczy wzrok, nadweręża kręgosłup, ogranicza kontakty społeczne.
- Mieć świadomość niebezpieczeństw wynikających z anonimowości kontaktów i podawania swojego adresu.
- Stosować się do ograniczeń dotyczących korzystania z komputera, Internetu i multimediów[40].

Na drugim etapie edukacyjnym, tj. w klasach IV–VI, w celach kształcenia, w ich wymaganiach ogólnych, w punkcie pierwszym zostało ujęte: „bezpieczne posługiwanie się komputerem i oprogramowaniem, świadomość zagrożeń i ograniczeń związanych z korzystaniem z komputera i Internetu"[41]. Natomiast w treściach nauczania, w wymaganiach szczegółowych w zakresie problematyki bezpieczeństwa w społeczeństwie informacyjnym w punkcie pierwszym, a ściślej 1.6, znajduje się zapis „przestrzega podstawowych zasad bezpiecznej i higienicznej pracy przy komputerze, wyjaśnia zagrożenia wynikające z niewłaściwego korzystania z komputera"[42]. Natomiast w punkcie siódmym, a dokładniej w 7.2., czytelnik odnajduje zapis „szanuje prywatność i pracę innych osób", w 7.3. „przestrzega zasad etycznych i prawnych związanych z korzystaniem z komputera i Internetu, ocenia możliwe zagrożenia"[43]. Opisane cele kształcenia dotyczą szkoły podstawowej, w której realizowany jest przedmiot o nazwie zajęcia komputerowe.

Na trzecim etapie edukacyjnym, tj. na poziomie gimnazjum, w celach kształcenia, w ich wymaganiach ogólnych podstawy programowej przedmiotu informatyka wnikliwy czytelnik odnajduje dwa punkty, które mieszczą się w kontekście bezpieczeństwa oraz zagrożeń w spo-

---

[39] *Podstawa programowa z komentarzami*, t. 6: *Edukacja matematyczna i techniczna w szkole podstawowej, gimnazjum i liceum. Matematyka, zajęcia techniczne, zajęcia komputerowe, informatyka*, s. 97.

[40] Ibidem.

[41] Ibidem.

[42] Ibidem.

[43] Ibidem.

łeczeństwie informacyjnym. To punkt pierwszy, który dotyczy „bezpiecznego posługiwania się komputerem i jego oprogramowaniem, wykorzystania sieci komputerowej, komunikowania się za pomocą komputera i technologii informacyjno-komunikacyjnej"[44]. A także punkt piąty, który skupia się na „ocenie zagrożeń i ograniczeń, docenianiu społecznych aspektów rozwoju i zastosowań informatyki"[45]. W treściach kształcenia znajdują się dokładniejsze zapisy, i tak punkt 5.1. wskazuje na to, że uczeń „samodzielnie i bezpiecznie pracuje w sieci lokalnej i globalnej"[46]. A w punkcie 7.2. znajduje się zapis, że uczeń „opisuje korzyści i niebezpieczeństwa wynikające z rozwoju informatyki i powszechnego dostępu do informacji, wyjaśnia zagrożenia związane z uzależnieniem się od komputera". Natomiast punkt 7.3. dotyczy „zagadnień etycznych i prawnych związanych z ochroną własności intelektualnej i ochroną danych oraz przejawami przestępczości komputerowej"[47]. Na czwartym etapie w celach kształcenia powtarza się punkt pierwszy i piąty z etapu trzeciego, czyli gimnazjalnego. W treściach nauczania, w wymaganiach szczegółowych w punkcie 1.3. jest zapis, że uczeń „korzysta z podstawowych usług w sieci komputerowej, lokalnej i rozległej, związanych z dostępem do informacji, wymianą informacji i komunikacją, przestrzega przy tym zasad netykiety i norm prawnych, dotyczących bezpiecznego korzystania i ochrony informacji oraz danych w komputerach w sieciach komputerowych"[48]. Natomiast w punktach 7.1. oraz 7.2. znajdują się noty o tym, że uczeń „opisuje szanse i zagrożenie dla rozwoju społeczeństwa, wynikające z rozwoju technologii informacyjno-komunikacyjnych", a także „omawia normy prawne odnoszące się do stosowania technologii informacyjno-komunikacyjnych, dotyczących rozpowszechniania programów komputerowych, przestępczości komputerowej, poufności, bezpieczeństwa i ochrony danych oraz informacji w komputerze i sieciach komputerowych"[49].

[44] Ibidem, s. 103.
[45] Ibidem, s. 105.
[46] Ibidem.
[47] Ibidem.
[48] Ibidem, s. 107.
[49] Ibidem, s. 109.

Warto dodać, że w szkołach jest przedmiot edukacja dla bezpieczeństwa, jednak w celach kształcenia nie ma mowy o problematyce bezpieczeństwa w społeczeństwie informacyjnym. Jak można zauważyć, zapisy dotyczące bezpieczeństwa i zagrożeń w społeczeństwie informacyjnym w podstawie programowej są bardzo, ale to bardzo symboliczne. Praktyka wskazuje na to, że treści te są traktowane raczej pobieżnie lub są, co gorsza, pomijane. Nauczyciele, jeżeli zwracają uwagę na tę problematykę, to bardziej skupiają się na ergonomii stanowiska komputerowego, profilaktyce antywirusowej (to też ważne tematy) niż na kwestiach związanych z prywatnością czy też przestępczością komputerową.

W przypadku studiów wyższych programy kształcenia muszą spełniać standardy kształcenia, które są zatwierdzone przez Radę Główną Szkolnictwa Wyższego. W dokumencie tym, w punkcie piątym, tj. w innych wymaganiach, w ustępie pierwszym są opisane wskazówki dotyczące przedmiotu technologia informacyjna. Treść tego zapisu brzmi „technologii informacyjnej – w wymiarze trzydziestu godzin, którym należy przypisać dwa punkty ECTS. Treści kształcenia w zakresie technologii informacyjnej: podstawy technik informatycznych, przetwarzanie tekstów, arkusze kalkulacyjne, bazy danych, grafika menedżerska i/lub prezentacyjna, usługi w sieciach informatycznych, pozyskiwanie i przetwarzanie informacji – powinny stanowić co najmniej odpowiednio dobrany podzbiór informacji zawartych w modułach wymaganych do uzyskania Europejskiego Certyfikatu Umiejętności Komputerowych (ECDL – European Computer Driving Licence)"[50]. W zapisie tym nie ma ani jednego słowa o bezpieczeństwie i zagrożeniach w społeczeństwie informacyjnym. To bardzo niepokojące, tym bardziej, że studia stopnia pierwszego przygotowują do podjęcia pracy zawodowej. A propozycja obowiązkowych zajęć dla studentów ogranicza się do obsługi pakietu biurowego i korzystania z programu pocztowego oraz przeglądarki internetowej. A gdzie tematy dotykające problematyki bezpie-

[50] Załącznik nr 81. Standardy kształcenia dla kierunku studiów: Politologia s. 7. Źródło: http://www.bip.nauka.gov.pl/bipmein/redir.jsp?place=galleryStats&id=9831 [01.05.2011].

czeństwa i zagrożeń w społeczeństwie informacyjnym, Biuletynu Informacji Publicznej, usług świadczonych online dla obywateli? To pytanie wydaje się retoryczne.

Autorka zdaje sobie sprawę z tego, że wprowadzenie oddzielnego przedmiotu do programu studiów w wymiarze piętnastu lub trzydziestu godzinnym jest raczej niemożliwe (aczkolwiek wskazane) przede wszystkim z powodów finansowych. Jednak nożna zastosować rozwiązania podobne jak w przypadku szkolenia w zakresie bezpieczeństwa i higieny pracy oraz ergonomii czy też zajęć z zakresu ochrony własności intelektualnej. Taki pięcio- lub sześciogodzinny moduł byłby co prawda rozwiązaniem połowicznym i oszczędnościowym, które jednak można by w przyszłości rozszerzyć do zajęć w wymiarze piętnastogodzinnym. Poniżej zostanie przedstawiony program takich zajęć.

BEZPIECZEŃSTWO W SPOŁECZEŃSTWIE INFORMACYJNYM – PROPOZYCJA ZAJĘĆ

Zajęcia z zakresu bezpieczeństwa w społeczeństwie informacyjnym mogłyby się odbywać w ramach jednego bądź dwóch spotkań kończących się testem na zaliczenie lub zaliczeniem na ocenę. Niewykluczone jest zastosowanie e-learningu. W związku z ograniczonym czasem powinny składać się z czterech modułów. Modułową strukturę zajęć przedstawia rysunek 2. Jak można zauważyć ma on charakter puzzli, co wskazuje na to, że każdy element składowy może być wymieniony bądź układ może zostać rozszerzony o dodatkowe elementy, chociażby w sytuacji, kiedy zaistniałaby możliwość zwiększenia liczby godzin zajęć. Poszczególne elementy zajęć będą przedstawione według następującego schematu: temat, uzasadnienie, tematyka zajęć.

TEMATYKA: ICT W PRACY

Uzasadnienie: Studia stopnia pierwszego są studiami zawodowymi, w swoim założeniu nie tylko przygotowują do kontynuowania nauki na studiach stopnia drugiego, ale także do podjęcia pracy na stanowiskach,

które są opisane w sylwetce absolwenta. Z tego też powodu ujęcie problematyki zastosowania środków ICT w pracy zawodowej jest niezbędne.

Rys. 2. Modułowy schemat zajęć z zakresu bezpieczeństwa w społeczeństwie informacyjnym

Źródło: opracowanie własne.

Tematyka zajęć: Przede wszystkim należy podjąć temat pracowniczego dekalogu w pracy ze środkami ICT, tj. poufność danych, legalność używanego oprogramowania, regularna zmiana haseł, kwestie wykorzystywanie komputera do celów prywatnych, profilaktyka antywirusowa. Tematów związanych z ergonomią stanowiska komputerowego nie trzeba poruszać, gdyż o tym mówi się na szkoleniach BHP, które są obowiązkowe w ramach studiów.

Temat: Prywatność.

Uzasadnienie: Uzasadnienie w tym obszarze zostało podane w przykładzie pierwszym.

Tematyka zajęć: Na płaszczyźnie tej należy zapoznać nie tylko z możliwymi zagrożeniami, ale także z zasadami postępowania, które mają uchronić użytkownika przed utratą własnej lub naruszeniem cudzej prywatności. Należy podjąć tematy związane z trybami pracy przeglądarek internetowych, programów szpiegujących, zasadami postępowania z nieużywanymi kontami w sklepach internetowych, ser-

wisów aukcyjnych, portali społecznościowych, zasadami związanymi z podawaniem informacji o sobie, możliwościami śledzenia osób na podstawie ich aktywności w sieci.

Temat: Cyberprzestępstwa.

Uzasadnienie: Uzasadnienie zostało zawarte w opisanym przez autorkę przykładzie drugim. Najważniejsze jednak jest przesłanie, które można zawrzeć w słowach: nie stać się ofiarą przestępstwa komputerowego ani też nie rozpocząć kariery cyberrzezimieszka.

Tematyka zajęć: Krótka charakterystyka cyberprzestępstw wraz z katalogiem kar, procedura zgłaszania przestępstw komputerowych oraz zasady przeciwdziałania im.

Temat: Inne.

Uzasadnienie i tematyka zajęć: Taki dodatkowy obszar jest niezbędny, chociaż można mu poświęcić niewiele czasu. Powinien zostać spożytkowany przede wszystkim na aktualne problemy albo zagrożenia sytuacyjne charakterystyczne dla danego kierunku studiów.

Autorka zdaje sobie sprawę z tego, że zakres materiału pięcio- bądź sześciogodzinnego modułu jest niewystarczający, ale w ciągu tak krótkiego czasu pewne tematy można jedynie zasygnalizować. Jednak pominięcie tej problematyki w czasie studiów byłoby jeszcze bardziej szkodliwe. Oszczędne rozwiązania nie mogą być stosowane przez dłuższy czas, tym bardziej że rozwój technologiczny przybiera na swojej dynamice. Świadczy o tym chociażby rosnąca liczba nowych wirusów, trojanów itp. Również należy wziąć pod uwagę to, że problem bezpieczeństwa w społeczeństwie informacyjnym rozszerza się wraz ze spektrum form korzystania z aplikacji. Obecnie z Internetu można korzystać nie tylko za pośrednictwem komputera stacjonarnego, ale także i laptopa – dostęp przez Wi-Fi jest coraz bardziej powszechny. Sposoby wykorzystywania mobilnego Internetu są jednak jeszcze rozleglejsze – nie można zapominać o aplikacjach dostępnych w telefonach komórkowych. Producenci oraz dostawcy usług już dawno zauważyli ten nowy trend wśród użytkowników i do swojej oferty wprowadzili nie tylko telefony z coraz większymi wyświetlaczami oraz klawiaturą QWERTY, ale także oferują coraz szybszy mobilny Internet.

Podsumowanie

Mówiąc o konieczności zapoznawania uczniów na wszystkich etapach edukacji oraz studiów z problematyką bezpieczeństwa informacyjnego, nie można zapominać o kilku kwestiach. Po pierwsze, treści te powinny być obowiązkowe na wszystkich kierunkach studiów i wcześniejszych etapach edukacyjnych. Po drugie, program zajęć powinien być modernizowany każdego roku. Po trzecie, należy dążyć do tego, aby wymiar godzinowy zwiększył się co najmniej do piętnastu godzin. Po czwarte, należy także pamiętać o osobach, które znajdują się poza systemem edukacyjnym i zorganizować dla nich, chociażby w ramach akcji społecznej, informacje o bezpieczeństwie i zagrożeniach w społeczeństwie informacyjnym.

Bibliografia

Kodeks karny. DzU Nr 88 poz. 553 z roku 1997. [online]. [dostęp: 4 maja 2011 roku]. dostępny w Internecie: http://karne.pl/karny.html.

Nissenbaum Helen, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford 2009, Stanford University Press, ISBN: 0804752362.

Podstawa programowa z komentarzami, t. 6. *Edukacja matematyczna i techniczna w szkole podstawowej, gimnazjum i liceum. Matematyka, zajęcia techniczne, zajęcia komputerowe, informatyka.*

Sienkiewicz Piotr, *Bezpieczeństwo i wolność w globalnym społeczeństwie informacyjnym*, [online]. [dostęp: 4 maja 2011 roku]. Dostępny w Internecie: http://www.dobrauczelnia.pl/upload/File/KONFERENCJE/BAZPIECZENSTWO/sienkiewicz.pdf.

Stachowiak Beata, *Obywatel społeczeństwa informacyjnego – dzisiaj i jutro*, w: *Zbliżenia cywilizacyjne. Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej we Włocławku*, t. 3, Włocławek 2007.

Wolski Karol: *I Ogólnopolskie Badanie Pracowników. Raport z badania 2010.* [online]. [dostęp 4 maja 2011 roku]. Dostępny w Internecie: http://www.badanie-pracownikow.pl/raport.pdf.

Zasoby internetowe

Baranowska-Skimina Aleksandra, *Piractwo komputerowe na świecie 2010*. [online]. [dostęp: 22 maja 2011 roku]. Dostępny w Internecie: http://www.egospodarka.pl/65664,Piractwo-komputerowe-na-swiecie-2010,1,39,1.html.

Prywatność i własny wizerunek w przestrzeni social media. Raport. Polskie Badania Internetu. [online]. [dostęp 4 maja 2011]. Dostępny w Internecie: http://www.pbi.org.pl/s/p/aktualnosci/prywatno%C5%9B%C4%87%20i%20w%C5%82asny%20wizerunek.pdf.

Ratuszniak Beata, *„Facebookowi" w Polsce stuknęło 6 milionów kont*. [online]. [dostęp: 4 maja 2011 roku]. Dostępny w Internecie: http://interaktywnie.com/biznes/artykuly/social-media/facebookowi-w-polsce-stuknelo-6-milionow-kont-20110.

Ratuszniak Beata, *KRRiT „zakazuje" Facebooka. Będą kary*. [online]. [dostęp: 4 maja 2011 roku]. Dostępny w Internecie: http://interaktywnie.com/biznes/artykuly/social-media/krrit-zakazuje-facebooka-beda-kary-20085.

Twórca WikiLeaks, *Facebook to najbardziej przerażająca machina do szpiegowania*. [online]. [dostęp: 4 maja 2011]. Dostępny w Internecie: http://wiadomosci.onet.pl/swiat/tworca-wikileaks-facebook-to-najbardziej-przerazaj,1,4260642,wiadomosc.html.