Spis treści

Drodzy Czytelnicy,

w odpowiedzi na różne niepokojące zjawiska, jakie miały miejsce w polskiej szkole, uchwałą Rady Ministrów nr 172/2008 z dnia 19 sierpnia 2008 roku został przyjęty i wdrożony rządowy program „Bezpieczna i przyjazna szkoła”.

Istotą programu jest budowanie szkoły wspierającej uczniów i jednocześnie wymagającej, poprzez stwarzanie klimatu współpracy, porozumienia, wzajemnego szacunku i dialogu, stanowiących podstawę bezpieczeństwa zarówno dla uczniów, jak i dla nauczycieli.

Rozpatrując kwestie bezpieczeństwa we współczesnej szkole, nie można pominąć tak ważnego obszaru, jaki stanowi technologia informacyjno-komunikacyjna. Stąd temat numeru „Cyfrowe (nie)bezpieczeństwo”.

W treści programu rządowego wielokrotnie występują odwołania do korzyści, jakie dla poprawy relacji interpersonalnych i klimatu społecznego w szkole mogą przynieść nowoczesne technologie. Autorzy programu zachęcają do prowadzenia z uczniami zajęć pogłębiających ich umiejętności korzystania z nowoczesnych technologii i wykorzystanie ich w nauce, kulturze, sztuce, zabawie, warsztatach kształtujących umiejętność korzystania z informacji jako źródła budowania wspólnot (np. hobbystycznych, etnicznych, specjalistycznych), do podnoszenia umiejętności komunikowania się za pomocą narzędzi technologii informacyjno-komunikacyjnych tak, aby szanować prawa rówieśników, nauczycieli i innych użytkowników nowoczesnych mediów.

Technologia informacyjna znalazła zastosowanie na wielu obszarach działalności szkoły: zarówno w szeroko rozumianej dydaktyce, jak i w administracji, w zarządzaniu pracą szkoły. Stąd kwestie związane z cyfrowym bezpieczeństwem dotyczą bardzo rozległej tematyki. Wpisuje się do niej, między innymi, zarówno bezpieczna praca z komputerem jako narzędziem pracy, niebezpieczeństwa związane z dostępem dzieci i młodzieży do Internetu, uzależnienia, jak również zewnętrzne ataki na komputery szkolne w celu ich wykorzystania do działalności przestępczej czy zagrożenia ze strony złośliwego oprogramowania.

W tym numerze „Meritum” znajdą Państwo wiele wartościowych materiałów, poruszających zagadnienia cyfrowych zagrożeń. Artykuły, przygotowane przez ekspertów i praktyków zajmujących się zagadnieniami zagrożeń generowanych przez nowe technologie, przedstawiają bogatą ofertę działań podejmowanych przez fundacje, stowarzyszenia i organizacje pozarządowe, mających na celu zapewnienie bezpieczeństwa dzieci w cyberprzestrzeni.

Znajdą Państwo także informacje dotyczące zapewnienia bezpieczeństwa danych (np. z elektronicznych dzienników czy programów bibliotecznych) oraz wnikliwie omówioną problematykę prawną dotyczącą tego tematu.

Chciałabym zwrócić Państwa uwagę na dwa artykuły.

W pierwszym autorka, Małgorzata Rostkowska, wybrała z podstawy programowej kształcenia ogólnego zapisy dotyczące bezpieczeństwa pracy przy komputerze i opatrzyła je własnym komentarzem. Bardzo ważne jest, aby każdy nauczyciel, nie tylko nauczyciel przedmiotów informatycznych, znał cele i treści podstawy programowej, związane z bezpieczną pracą ucznia przy komputerze podłączonym do sieci Internet.

Drugi artykuł, to tekst „Stop cyberprzemocy!” autorstwa Małgorzaty Nowak, dyrektora Zespołu Szkół im. Ziemi Lubelskiej w Niemcach. Jest to przykład konkretnych działań wychowawczych, jakie może podjąć nauczyciel czy dyrektor szkoły w celu przeciwdziałania agresji elektronicznej wśród młodzieży.

Zapraszam do lektury!

G. Gregorczyk

Edyta Sabicka
Kamila Knol
Agata Matuszewska

Agresja elektroniczna wśród młodzieży – rodzaje, skutki, profilaktyka

Zagadnienia definicyjne

Z uwagi na fakt, iż agresja elektroniczna jest stosunkowo nowym zjawiskiem, terminologia dotycząca tej tematyki nie jest jeszcze ujednolicona. Według nomenklatury zaproponowanej przez Jacka Pyżalskiego, najszerszy zakres pojęciowy posiada termin „agresja elektroniczna", tłumaczony wprost z angielskiego *electronic aggression*. Zamiennie proponowany jest termin „cyberprzemoc". Pyżalski definiuje te wyrażenia bardzo ogólnie jako agresję z użyciem technologii komunikacyjnych[1].

Z kolei Łukasz Wojtasik posługuje się następującą definicją cyberprzemocy: *Cyberprzemoc* (*cyberbullying*) *to wykorzystywanie technik informacyjnych i komunikacyjnych do świadomego, wielokrotnego i wrogiego zachowania się osoby lub grupy osób, mającego na celu krzywdzenie innych*[2].

Wracając do terminologii Pyżalskiego, pojęciem węższym znaczeniowo od agresji elektronicznej jest nękanie internetowe (*online harrassment*, *Internet harrassment*). Są to działania występujące *online*, skierowane przeciwko innej osobie, mające na celu jej skrzywdzenie. Warto zwrócić uwagę, iż w przypadku tego zjawiska zachowania ograniczone są jedynie do tych występujących w Internecie. Z kolei pojęcie agresji elektronicznej odnosiło się ogólnie do technologii komunikacyjnych, obejmujących tym samym również np. akty agresji przy użyciu telefonów komórkowych.

Najwęższy zakres znaczeniowy według terminologii Pyżalskiego ma pojęcie *mobbing* elektroniczny, tłumaczone z angielskich *cyberbullying*, *Internet bullying*. Pojęcie to odnosi się do zachowań agresywnych występujących w danej grupie społecznej, do której należą zarówno sprawca, jak i ofiara. Ponadto *cyberbullying* cechuje się celowością działań, ich powtarzalnością i nierównowagą sił. Cechy te zostaną szerzej umówione w dalszej części artykułu.

Charakterystyka cyberbullyingu

Z uwagi na specyfikę komunikacji za pomocą nowoczesnych technologii, również akty agresji w wirtualnym świecie posiadają pewne charakterystyczne cechy. Jacek Pyżalski[3] zwraca uwagę na cztery z nich: powtarzalność, intencja skrzywdzenia drugiej osoby, nierównomierność sił, realizowanie aktów agresji w obrębie znanej grupy społecznej.

Powtarzalność w kontekście *cyberbullyingu* związana jest z właściwościami samych nowoczesnych technologii. Pyżalski przytacza za Boyd cztery kluczowe właściwości materiałów umieszczonych w sieci. Pierwszą z nich jest trwałość, bowiem treści umieszczone w sieci mogą pozostać tam praktycznie nieskończenie długi czas. Ponadto Internet umożliwia wyszukiwanie danych treści, co znacznie ułatwia dostęp do nich. Co więcej, treści te

[1] Pyżalski J. *Agresja elektroniczna dzieci i młodzieży – różne wymiary zjawiska*, Dziecko krzywdzone nr 1(26)/2009, s. 12-26.
[2] Wojtasik Ł. *Przemoc rówieśnicza z użyciem mediów elektronicznych – wprowadzenie do problematyki*, Dziecko krzywdzone nr 1(26)/2009, s. 7-11.
[3] Pyżalski J. *Agresja elektroniczna dzieci i młodzieży – różne wymiary zjawiska*, ibidem.

z łatwością mogą być kopiowane przez kolejnych użytkowników. Wreszcie ostatnią poruszaną kwestią jest obecność tzw. „niewidzialnej publiczności", czyli bardzo dużej grupy internautów, trudnej do identyfikacji.

Drugą cechą *cyberbullyingu* jest intencja skrzywdzenia innej osoby, czyli celowość działań sprawcy. Według Jacka Pyżalskiego jest to cecha dość dyskusyjna, ponieważ niejednokrotnie występują sytuacje, w których sprawca daleki jest od chęci skrzywdzenia drugiej osoby, a swoje zachowanie tłumaczy żartem bądź specyficznym sposobem komunikacji w danej grupie społecznej. Ofiara jednak ma poczucie krzywdy w związku z daną sytuacją. Co więcej, z uwagi na charakter komunikacji internetowej sprawca najczęściej nie dostrzega bezpośrednio niewerbalnych sygnałów ofiary, które świadczą o jej poczuciu krzywdy. To utwierdza go w przekonaniu o braku negatywnych konsekwencji swojego działania.

Kolejną cechą *cyberbullyingu* jest nierównomierność sił, czyli przewaga sprawcy nad ofiarą. W tradycyjnym *bullyingu* przewaga ta wynika najczęściej z siły fizycznej bądź psychicznej, natomiast w świecie wirtualnym przewaga ta związana jest m.in. z faktem anonimowości sprawców świadków aktu agresji, a także z samymi cechami treści publikowanych w Internecie, które wyszczególniła Boyd: *trwałość, możliwość wyszukiwania, kopiowalność, występowanie „niewidzialnej publiczności"*.

Ostatnia wymieniana przez Jacka Pyżalskiego cecha *cyberbullyingu* dotyczy relacji pomiędzy sprawcą a ofiarą. Niektórzy badacze uważają, iż termin „cyberbullying" powinien charakteryzować jedynie sytuacje, gdy sprawca i ofiara należą do tej samej grupy społecznej. Takie przypadki aktów agresji mają miejsce np. w klasie szkolnej, gdy ofiara doświadcza przemocy ze strony tych samych sprawców zarówno w realnym świecie, jak i za pomocą nowoczesnych technologii[4].

Typy agresji elektronicznej

Agresja elektroniczna może przejawiać się w różnorodny sposób i często budzić kontrowersje zarówno wśród ofiar, jak i sprawców, ponieważ niejednokrotnie mogą być uznane za nieszkodliwe żarty czy wygłupy. Należy jednak pamiętać, że jeśli dochodzi do poczucia krzywdy, zranienia drugiej osoby, pojawienia się lęku czy wstydu, to mamy do czynienia z agresją.

Jacek Pyżalski na podstawie przeprowadzonych wśród studentów badań jakościowych (wywiadów i obserwacji) dokonał analizy agresji elektronicznej. W oparciu o kryteria takie jak: relacje między sprawcą a ofiarą, długotrwałość oddziaływania, relacje zachodzące między uczestnikami agresji oraz kontekst oddziaływań, opracował wstępną typologię, do której zaliczyć można agresję elektroniczną:

- wobec nauczycieli – sprawcą w tym przypadku może być jeden uczeń lub cała ich grupa,
- wobec celebrytów, czyli osób znanych z mediów – sprawcy nie łączy z ofiarą relacja osobista, a agresja ma charakter pośredni,
- ze strony lub w stosunku do osób nieznajomych w realnym świecie – agresja często jest spontaniczna, a sprawca nie poznał nigdy ofiary w realnym świecie,
- związana z relacją osobistą – uczestników agresji łączyła bliska relacja, a niemożność jej wznowienia prowadzi do zastosowania aktów agresji,
- w kontekście dowcipu – traktowanie agresji jako żartu,

a także:

- *mobbing* elektroniczny wobec rówieśników – sprawcy należą do jednej grupy społecznej w realnym świecie, choć mogą pozostać anonimowi z uwagi na wykorzystywanie nowoczesnych technologii komunikacyjnych; akty agresji mają charakter powtarzalny,
- groźby karalne – stosowanie konkretnych gróźb pod adresem ofiary,
- oszustwo elektroniczne – uczestnicy agresji mogą, ale nie muszą znać się w realnym świecie; polega na oszukiwaniu ofiary lub podszywaniu się pod nią, by ją ośmieszyć lub wykorzystać[5].

Możemy się zastanawiać nad tym, czy komentowanie zamieszczonych w sieci wypowiedzi użytkowników Internetu lub zdjęć celebrytów jest czymś nagannym. Oczywiście nie, pod warunkiem że komentarze te mają charakter konstruktywnej, merytorycznej krytyki, a nie są wulgarnymi wypowiedziami i wyzwiskami skierowanymi do autorów wypowiedzi czy bohaterów zdjęć.

Może się także wydawać, że SMS o treści „Nie pokazuj się jutro w szkole, bo tak ci wkopiemy,

[4] Ibidem.
[5] Pyżalski J. *Agresja elektroniczna wirtualne ciosy, realne rany* – cz. I, Remedium, wrzesień 2008, s. 26-27.

że przez miesiąc z domu nie wyjdziesz!!" jest czymś niegroźnym, bo od słów do czynów jeszcze daleko. Jednak taka wiadomość budzi w człowieku poczucie zagrożenia i obawy. Aktów agresji elektronicznej jest znacznie więcej. Zalicza się do nich również rozpowszechnianie danych osobowych bez zgody i wiedzy ich właściciela czy wysyłanie użytkownikom Internetu niechcianych linków prowadzących do stron z pornografią lub zdjęciami powszechnie wywołującymi obrzydzenie i niesmak. Ponadto dość powszechne, szczególnie wśród użytkowników forów internetowych, staje się intencjonalne publikowanie w sieci wrogich, obraźliwych lub kontrowersyjnych wiadomości, wywołujących gwałtowną reakcję użytkowników, czyli tzw. *trolling*[6].

Kolejnymi przejawami agresji w cyberprzestrzeni są czynności wymagające już większego zaangażowania sprawcy i posiadania pewnych kompetencji w zakresie nowoczesnych technologii komunikacyjnych. Można przypuszczać, że te akty agresji dokonywane są z premedytacją właśnie ze względu na konieczność zaangażowania pewnych środków technicznych i czasu. Wymienić tu można tworzenie ośmieszających filmów i fotomontaży, a następnie umieszczanie ich na stronach internetowych lub wysyłanie innym na telefon komórkowy bez zgody uczestników tego „dzieła"; tworzenie stron internetowych mających na celu ośmieszenie (choć w tym przypadku zdarza się, że zachowanie takie postrzegane jest jako niegroźne i traktowane jest jako głupi żart, bo czymże jest strona internetowa zmierzająca do wyłonienia najbrzydszej osoby w szkole?), jak również prowokowanie ofiary do zachowań ośmieszających czy agresywnych, a następnie filmowanie całego zajścia w celu zamieszczenia filmu w Internecie, czyli tzw. *happy slapping*. Przykładem takiego działania może być prowokowanie bijatyki poprzez splunięcie przypadkowej osobie w twarz, a następnie filmowanie jej reakcji, by film ten zamieścić w sieci. Niektórzy sprawcy agresji elektronicznej posuwają się nawet do tego, by nakłaniać bezdomnych lub biednych ludzi do zachowań uwłaczających godności i filmują ich w celu udostępnienia tego nagrania innym użytkownikom Internetu. Sprawcy tej formy agresji zachęcają swe ofiary do „wygłupów", tańczenia czy innych ośmieszających zachowań, oferując im w zamian papierosy lub alkohol. Jest to bardzo kontrowersyjny przykład agresji elektronicznej, ponieważ żadna ze stron nie uważa, by była sprawcą lub ofiarą. Obiektywnie jednak można uznać, iż ma tu miejsce celowe kompromitowanie człowieka.

Konsekwencje agresji elektronicznej

Agresja elektroniczna to zjawisko stosunkowo nowe i dlatego nasza wiedza na temat jej konsekwencji jest uboższa niż w przypadku agresji tradycyjnej, jednak już teraz wiadomo, że niesie ona za sobą negatywne konsekwencje. Wydaje się, że agresja dokonywana za pomocą nowoczesnych technologii komunikacyjnych nie jest groźna, bo nie prowadzi do uszczerbku na zdrowiu, nie widać fizycznych skutków agresji, a jednak w sferze psychicznej ofiary pozostawia skutki w postaci lęku, utraty wiary w siebie, obniżenia poczucia własnej wartości, wstydu, a niekiedy nawet izolacji społecznej, depresji czy, w skrajnych przypadkach, prób samobójczych. Badania przeprowadzone przez Fundację Dzieci Niczyje w styczniu 2007 roku pokazują, że prawie połowa osób zastraszanych w sieci lub poprzez SMS-y odczuwała zdenerwowanie, strach budziło to wśród 20% respondentów, a wstyd odczuwało 11% badanych. W przypadku osób, których kompromitujące zdjęcia zostały umieszczone w sieci, najczęściej spotykano się ze zdenerwowaniem (66%), poczuciem wstydu (33%) oraz strachem (12%)[7]. Dlatego też bez wątpienia możemy mówić o tym, że agresja elektroniczna może nieść za sobą negatywne skutki.

Z relacji ofiar można dowiedzieć się, że spotkanie się z agresją elektroniczną nie pozostaje bez wpływu na ich funkcjonowanie w środowisku społecznym czy kondycję psychiczną. Marta Wojtas, która jest psychologiem i pracownikiem Helpline.org, stwierdziła nawet, że *cyberprzemoc wpływa na psychikę dziecka o wiele mocniej niż przemoc twarzą w twarz. Dziecko czuje się osaczone, zdane tylko na siebie i bezsilne. Ofiara cyberprzemocy ze strony szkolnych rówieśników jest przekonana, że z jej sytuacją już nic się nie da zrobić. Nie liczy na interwencję dorosłych*[8]. Autorka zwraca uwagę na to, że agresja elektroniczna jest długotrwała – kompromitujące zdjęcia czy obraźliwe komentarze zamieszczone w sieci pozostają tam na długo i każdy użytkownik Internetu może mieć do nich dostęp.

[6] Kamińska M. *Flaming i trolling – kulturotwórcza rola konfliktu we wspólnocie wirtualnej* [w:] Wawrzak-Chodaczek M. *Komunikacja społeczna w świecie wirtualnym*, Wydawnictwo Adam Marszałek, Toruń 2008, s. 287.

[7] Wojtasik Ł. Badanie *Przemoc rówieśnicza a media elektroniczne*, styczeń 2007, Fundacja Dzieci Niczyje, Gemius SA, próba: N=891 internautów w wieku 12-17 lat.

[8] Świerczyńska K. *Ofiary cyberprzemocy* (www.dziennik.pl/wydarzenia/article235719/Ofiary_cyberprzemocy.html).

Liczba świadków, czyli „niewidzialna publiczność" jest nieograniczona, co może potęgować w ofierze poczucie poniżenia.

Wspomnienia osób mających takie doświadczenia są dla nich bardzo bolesne.

Dwunastoletnia dziewczynka z Virginii mówi, że: *Bycie ofiarą cyberbullyingu naprawdę sprawiło, że czułam się okropnie zdołowana. Myślałam czasem o zemście albo powiedzeniu osobie, która mnie krzywdziła, co o tym myślę, ale pewnie to i tak by nie pomogło. Zwykle nie mówię nikomu o tym, co się stało, by nie donosić. Jednak to nie jest donoszenie, bo to się działo naprawdę*[9].

Warto zauważyć, jak silne reakcje emocjonalne towarzyszą ofiarom *cyberbullyingu* i jak przekłada się to na ich funkcjonowanie w życiu społecznym. Z badań Fundacji Dzieci Niczyje wynika, że aż 54% nastoletnich internautów, których niechciane zdjęcia lub filmy pojawiły się w sieci, nie dzieli z nikim informacji o zdarzeniu[10]. Oznacza to, że młodzi ludzie są często pozostawieni sami sobie z problemem i samotnie muszą toczyć walkę o swoją godność i poczucie bezpieczeństwa. Brak informacji o tego typu aktach agresji może wynikać z poczucia wstydu, a także przekonania, że i tak nic nie da się zrobić.

Kolejna osoba, która stała się ofiarą *cyberbullyingu*, mówi o swoich przeżyciach w następujący sposób: *Byłam ofiarą mobbingu elektronicznego. To obniżyło moją samoocenę. To sprawiło, że czułam się gorsza. Czasem potrafiłam chodzić cały dzień, czując się bezwartościowa, czując że nikogo nie obchodzę. To sprawiło, że czułam się bardzo, bardzo zdołowana*[11].

Michel Walrave i Wannes Heirman, przytaczając rożne wyniki badań zauważają, że ofiary *cyberbullyingu* trzy raz częściej cierpią na depresję[12].

Niekiedy skutki agresji elektronicznej mogą być tragiczne. Głośna w ostatnim czasie stała się sprawa 15-letniej Megan Gillan, która na jednym z portali społecznościowych była ośmieszana i borykała się z obraźliwymi komentarzami pod swoim adresem. Działania te wywarły na niej tak silne wrażenie, że popełniła samobójstwo. Przypadek ten nie jest niestety odosobniony, stąd tak ważne jest uzmysłowienie sobie, że *cyberbullying* to nie jedynie niemądre żarty złośliwych dzieciaków, ale istotny problem rodzący niekiedy bardzo poważne konsekwencje. Dlatego tak ważne jest podejmowanie działań profilaktycznych.

Zapobieganie agresji elektronicznej

Zapobieganie agresji elektronicznej to jeden z trudniejszych tematów. W związku z tym, że mamy do czynienia ze stosunkowo nowym zjawiskiem, w bardzo wielu szkołach brakuje odpowiednich procedur postępowania, brakuje też samych programów profilaktycznych... Często brakuje również pomysłów na to, jak sobie radzić z narastającym problemem, jakim jest nieodpowiednie wykorzystywanie nowoczesnych technologii przez młodzież.

W tym miejscu trzeba dodać, że aby jakiekolwiek działania profilaktyczne były rzeczywiście skuteczne, nie mogą być adresowane tylko do ucznia, który doświadczył już na własnej skórze skutków agresji elektronicznej, czy to jako sprawca, czy też ofiara. Powinny one przebiegać równocześnie w wielu różnych środowiskach, m.in. w szkole (klasie szkolnej), rodzinie, ale też bliższym i dalszym środowisku naszego podopiecznego. Nie wystarczy powiedzieć uczniowi, by w razie kłopotów zgłosił się do swojego wychowawcy albo rodzica, bo co się stanie, jeśli okaże się, że ani jeden, ani drugi nie ma pojęcia o nowoczesnych technologiach i nie będzie potrafił pomóc? Albo – jeszcze gorzej – zamiast pomóc, zaszkodzi? Znany był przypadek, kiedy to rodzic w porozumieniu z wychowawcą klasy zabronił dziecku (ofierze *cyberbullyingu*) korzystania z Internetu, uzasadniając swoją decyzję tym, że *jak dziecko nie będzie widziało, co wypisują na jego temat, to się nie będzie denerwować*... W konsekwencji dziewczyna uciekła z domu.

Warto dodać, co podkreślają także Anna Słysz i Beata Arcimowicz, że często dzieje się tak, iż dorośli stawiają dopiero pierwsze kroki w obsłudze Internetu i nie mają możliwości kontrolowania poczynań swojej pociechy. Jednak zarówno rodzice, jak i nauczyciele powinni pamiętać, że to nie Internet jest zagrożeniem samym w sobie, a ludzie, którzy z niego korzystają w nieodpowiedni sposób[13]. Dlatego zabranianie dziecku korzystania z dobrodziejstw rozwoju technologii nie ma większego

9 http://www.cyberbullying.us/shareyourstory.php
10 Wojtasik Ł. Badanie *Przemoc rówieśnicza a media elektroniczne*, ibidem.
11 http://www.cyberbullying.us/shareyourstory.php
12 Walrave M., Heirman W. *Skutki cyberbullying – oskarżenie czy obrona technologii?*, Dziecko krzywdzone – Cyberprzemoc nr 1(26)/2009.
13 Słysz A., Arcimowicz B. *Przyjaciele w internecie*, GWP, Gdańsk 2009.

sensu i nie może być traktowane jako jeden ze sposobów profilaktyki.

W odniesieniu do *cyberbullyingu*, podobnie jak w przypadku uzależnienia od alkoholu czy narkotyków również możemy wyróżnić trzy poziomy profilaktyki: pierwszo-, drugo- i trzeciorzędową i każda z nich adresowana będzie do innego rodzaju odbiorców.

Profilaktyka pierwszorzędowa

Pierwszorzędowe oddziaływania profilaktyczne skierowane są zazwyczaj do ogółu społeczeństwa. Mają one za zadanie zapobieganie pojawieniu się problemów. Dostarczają rzetelnej informacji dostosowanej do potrzeb odbiorców (informacja ta nie może być jednak zbyt szczegółowa). Tak więc w ramach zajęć poświęconych tej tematyce możemy np. pokazać młodzieży różnicę pomiędzy komunikacją werbalną a pośredniczoną przez Internet, wskazywać na jej specyficzne cechy, mechanizmy, pułapki. Doskonałym przykładem takiej profilaktyki jest kampania społeczna zrealizowana przez Fundację Dzieci Niczyje „Dziecko w sieci", która obejmowała kilka akcji: „Nigdy nie wiadomo, kto jest po drugiej stronie" (zwracała uwagę na problem pedofilii i uwodzenia nieletnich), „Internet to okno na świat. Cały świat" (pokazywała, że w Internecie dzieci mogą spotkać się z nieodpowiednimi, niedostosowanymi do ich wieku treściami, takimi jak pornografia, przemoc czy rasizm) oraz ostatnia akcja „Stop cyberprzemocy"[18].

Profilaktyka drugorzędowa

Profilaktyka drugorzędowa, to już tzw. wczesna interwencja. Jest adresowana do osób, u których pojawiają się pierwsze przejawy zaburzeń w zachowaniu, co do których istnieje poważne podejrzenie, że w nieprawidłowy sposób korzystają np. z zasobów sieci czy też możliwości, jakie stwarza Internet. Mogą to być dzieci lub młodzież z tzw. grup ryzyka, np. jeśli wiemy, że nasi podopieczni mają przyjaciół, którzy są uzależnieni od komputera i sami zaczynają spędzać coraz więcej czasu, traktując komputer jako formę rozrywki i zaniedbując obowiązki, szkołę, dom. Zadaniem tego poziomu profilaktyki jest powstrzymanie procesu patologizacji, zakłada on również kształtowanie umiejętności psychospołecznych, interpersonalnych. Przykładem takiej profilaktyki mogą być zajęcia z bibliotekarapii podejmujące tematykę *cyberbullyingu*, podczas których proponuje się młodym ludziom różne lektury, m.in. książkę pt. „Błysk Flesza" Christiana Linkera, która w bardzo przystępny sposób ukazuje zjawisko *happy slappingu*[19].

Oczywiście, zgodnie z założeniem, że lepiej zapobiegać niż leczyć, należy kłaść szczególny nacisk na rozwój profilaktyki pierwszo- i drugorzędowej, czasem jednak konieczne jest zastosowanie profilaktyki trzeciorzędowej.

Profilaktyka trzeciorzędowa

Profilaktyka na tym poziomie jest adresowana do osób, u których już występuje zdiagnozowana patologia. Profilaktyka trzeciorzędowa ma na celu przywrócenie osoby po terapii do społecznie użytecznego stylu życia. Przykładem takiej profilaktyki może być sytuacja, kiedy np. prosimy osobę, która była sprawcą agresji elektronicznej i doświadczyła z tego powodu przykrych konsekwencji, by jako ekspert podzieliła się swoim doświadczeniem ze środowiskiem osób zagrożonych *cyberbullyingiem* (osób z tzw. grupy ryzyka). Aby opowiedziała im (ku przestrodze) o swoich przeżyciach na podstawie własnych doświadczeń. Innym przykładem mogą też być specjalistyczne zajęcia z psychoterapii lub terapii przez sztukę, np. z arteterapii, pomagające odreagować ofiarom *cyberbullyingu* negatywne emocje i doznania.

Warto pamiętać, że niezależnie od złożoności problemu, wsparcia, porady i konsultacji udziela linia Helpline 0-800-100-100 i może tu dzwonić zarówno młodzież potrzebująca pomocy, jak i rodzice czy nauczyciele poszukujący informacji[20].

Podsumowując, *cyberbullying* to nie tylko niemądre żarty dzieciaków, to rzeczywisty problem niosący ze sobą niekiedy bardzo poważne konsekwencje, z którym jako nauczyciele, rodzice, opiekunowie dzieci i młodzieży musimy nauczyć się sobie radzić. Oczywiście mamy świadomość, że nie wyczerpałyśmy do końca tematu profilaktyki, a jedynie wskazałyśmy pewien kierunek i zachęciłyśmy do śledzenia prac naszego zespołu badawczego „Cyberbullying – projekt badawczy", kierowanego przez dr. Jacka Pyżalskiego[21], gdzie już niedługo powinny ukazać się nasze autorskie materiały traktujące szerzej tę tematykę.

[18] http://www.dzieckowsieci.pl
[19] Linker Ch. *Błysk flesza*, Nasza Księgarnia, Warszawa 2009.
[20] http://www.helpline.org.pl
[21] http://www.wsp.lodz.pl/Cyberbullying-344-0.html

Bibliografia i webgrafia

1. Kamińska M. *Flaming i trolling – kulturotwórcza rola konfliktu we wspólnocie wirtualnej* [w:] Wawrzak-Chodaczek M. *Komunikacja społeczna w świecie wirtualnym*, Wydawnictwo Adam Marszałek, Toruń 2008.
2. Linker Ch. *Błysk flesza*, Nasza Księgarnia, Warszawa 2009.
3. Pyżalski J. *Agresja elektroniczna dzieci i młodzieży – różne wymiary zjawiska*, Dziecko krzywdzone nr 1(26)/2009.
4. Pyżalski J. *Agresja elektroniczna wirtualne ciosy, realne rany* – cz. I, Remedium, wrzesień 2008.
5. Słysz A., Arcimowicz B. *Przyjaciele w internecie*, GWP, Gdańsk 2009.
6. Świerczyńska K. *Ofiary cyberprzemocy* (www.dziennik.pl/wydarzenia/article235719/Ofiary_cyberprzemocy.html).
7. Walrave M., Heirman W. *Skutki cyberbullying – oskarżenie czy obrona technologii*?, Dziecko krzywdzone – Cyberprzemoc nr 1(26)/2009.
8. Wojtasik Ł. Badanie *Przemoc rówieśnicza a media elektroniczne*, styczeń 2007, Fundacja Dzieci Niczyje, Gemius SA, próba: N=891 internautów w wieku 12-17 lat.
9. Wojtasik Ł. *Przemoc rówieśnicza z użyciem mediów elektronicznych – wprowadzenie do problematyki*, Dziecko krzywdzone nr 26/2009.

http://www.cyberbullying.us/shareyourstory.php

http://www.dzieckowsieci.pl

http://www.helpline.org.pl

http://www.wsp.lodz.pl/Cyberbullying-344-0.html

Edyta Sabicka jest pedagogiem specjalnym, arteterapeutą, członkiem zespołu „Cyberbullying – projekt badawczy", członkiem zarządu Łódzkiego Towarzystwa Pedagogicznego, pedagogiem specjalnym w Przedszkolu Miejskim nr 214 z Oddziałami Integracyjnymi w Łodzi

Kamila Knol i Agata Matuszewska są członkami zespołu „Cyberbullying – projekt badawczy", studentkami V roku pedagogiki w zakresie profilaktyki i animacji społeczno-kulturalnej na Uniwersytecie Łódzkim

PEGI – ogólnoeuropejski system oceniania gier (*Pan European Game Information*) powstał w 2003 roku w celu udzielenia rodzicom pomocy w podejmowaniu świadomych decyzji o zakupie gier komputerowych.

Struktura systemu PEGI została przygotowana na bazie wcześniej istniejących europejskich systemów klasyfikacji przez Europejską Federację Oprogramowania Interaktywnego ISFE (*Interactive Software Federation of Europe*) we współpracy z największymi producentami konsoli komputerowych, wydawcami i dystrybutorami gier oraz przy aktywnym udziale partnerów społecznych, takich jak konsumenci, rodzice i grupy religijne.

PEGI jest stosowany w 32 krajach, między innymi w Austrii, Belgii, Bułgarii, Czechach, Danii, Estonii, Francji, Grecji, Irlandii, Holandii, Hiszpanii, Norwegii, Niemczech, Polsce.

We wrześniu 2009 oznaczenia PEGI zostały uznane za oficjalnie obowiązujące w Polsce i każda gra jest w odpowiedni sposób oznakowana.

Dr Jerzy Zygmunt Szeja

Gry i młodzi gracze

Czy granie w gry komputerowe jest niebezpieczne?

Na początku odpowiem na pytanie postawione w podtytule, ponieważ zapewne to ono zainteresowało osobę, która czyta ten artykuł. Tak, gry komputerowe mogą być niebezpieczne. Ale nie dlatego, że taka jest ich natura, ale z tego powodu, że prawie nie ma dziedzin działalności człowieka, które nie niosłyby ze sobą zagrożeń. Tak publicznie chwalone zajęcia sportowe, niewątpliwie bardzo pożyteczne dla każdego człowieka, a szczególnie młodego, mogą prowadzić nie tylko do wzrostu tężyzny fizycznej, sprawności, koordynacji ruchowej itd., ale też do wielu kontuzji. Większość dyscyplin sportowych, i to nie tylko uprawianych wyczynowo, ale też okazjonalnie, grozi zarówno urazami, jak i trwałym kalectwem. Są sporty, w których corocznie giną sportowcy: himalaiści, szybownicy, uczestnicy wyścigów. W dodatku społeczną akceptację zdobyły sporty, w których zaangażowanie wymaga stałego pobudzania w sobie agresji, jak boks, rugby, zapasy oraz liczne gry zespołowe z piłką nożną na czele.

Z drugiej strony każde hobby, w które dostatecznie mocno się zaangażujemy, może rodzić stany oceniane negatywnie przez osoby postronne. Zapewne wszyscy znamy jakichś zapalonych hobbystów, którzy by nic innego nie robili, tylko poświęcali się ulubionej dziedzinie. A jeśli akurat nie mogą się jej oddawać, z niechęcią myślą i mówią o czymś innym. I to dotyczy zarówno sportów tak statycznych, jak szachy, jak i zajęć tak podobno relaksujących, jak wędkarstwo. Kilka lat temu media doniosły o morderstwie, jakiego dopuścił się łowiący na warszawskim brzegu Wisły emeryt, rozdrażniony płoszącym mu ryby kajakarzem, dwukrotnie młodszym od siebie. Zaczął od bardzo obraźliwych określeń, a skończył pchnięciem noża.

W takim kontekście gry komputerowe nie cechują się niczym osobliwym. Część graczy to pasjonaci, którzy spędzają przed ekranem dużo czasu, często kosztem innych zajęć, w tym nauki, jeśli są uczniami lub studentami. Większość gra z umiarem. To trochę tak, jak z oglądaniem telewizji: są tacy, którzy spędzają przed ekranem większość życia, inni racjonalnie dawkują tę rozrywkę. Niemniej jednak statystyczny Polak ogląda TV przeszło cztery godziny dziennie. Grająca młodzież podobnie dużo czasu poświęca zabawom z komputerami i konsolami.

Tak więc poprawne pytanie nie brzmi, „Czy gry komputerowe są niebezpieczne?", bo w specyficznych okolicznościach mogą być groźne, jak wszystko, tylko „Dlaczego gry komputerowe postrzega się jako niebezpieczne?". Aby na tak postawione pytanie odpowiedzieć, warto przywołać prace antropologa Richarda Schechnera, który bardzo interesował się grami i zabawami jako źródłami kultury. Stwierdza on, analizując prace innego badacza: *W krajach Zachodu zabawa jest kategorią podejrzaną: to działanie skażone nierzeczywistością, nieautentycznością, podwójnością (…). Schutz na pierwszy plan wysuwał „świat powszechnej pracy" jako archetyp naszego doświadczenia rzeczywistości. (…) Jakkolwiek inne spostrzeżenia Schutza są użyteczne, nie mogę się zgodzić na tego typu hierarchię. To właśnie zabawa, a nie świat powszechnej pracy stanowi podstawę, wzorzec, matecznik wszelkich doświadczeń i oddzielających się od zabawy, łuszczących się sfer rzeczywistości*[1] .

Podobną postawę przyjmuje znakomity mediewista i antropolog Johan Huizinga, w grach dostrzegając czynnik kulturo- i społecznotwórczy. Autor „Homo ludens" nazywa *zabawę (…) czynnością powołującą do życia związki społeczne, które ze swej strony chętnie otaczają się tajemnicą*[2].

W grach widzą zagrożenie osoby kierujące się mentalnością purytańską, które we wszystkim, co nie jest pracą zarobkową lub działalnością w inny

1 Schechner R. *Zabawa* [w:] idem, *Przyszłość rytuału*, Warszawa 2000, s. 34.
2 Huizinga J. *Homo ludens*, Warszawa 1998, s. 31.

sposób utylitarną, dopatrują się znamion dzieła szatana, czemu sprzyja owa aura tajemnicy (niegrający zwykle nie mogą zrozumieć, o co chodzi w tych rozrywkach, zwłaszcza że sami często nie potrafią użytkować nawet najprostszych programów komputerowych). Doskonale ten trend obrazuje okładka książki „Oddziaływanie „agresywnych" gier komputerowych na psychikę dzieci"[3], na której tytuł wpisany jest w płomienie. Swoją drogą książka powołuje się na błędne metodologicznie badania przeprowadzone na niereprezentatywnej próbce, mylące skutek z przyczyną. Jest to zresztą błąd często spotykany. Bo o ile nie daje się udowodnić teza miła autorom badań, że gry komputerowe niszczą psychikę dziecka, to bardzo łatwo wykazać, że w gry o podwyższonym poziomie agresji chętniej grają osoby agresywne, a w zabawy spokojniejsze: dzieci grzeczne. Agresywni chłopcy z chęcią wybierają słynną brutalną GTA, a spokojniejsze dziewczynki częściej np. The Sims. I choć nikt rozsądny nie twierdzi, że ciemne zakamarki podwórzowych studni Pragi źle działają na umysły przebywających tam i nudzących się, krótko ostrzyżonych młodych ludzi, tylko że to dresiarze z różnych powodów upodobali sobie takie miejsca, to jednak podobne sądy dotyczące gier komputerowych są powszechne. Nikt poważny nie twierdzi, że ktoś polubił bicie innych pięściami, ponieważ zaczął trenować boks, bo przecież jest zupełnie odwrotnie. Tyle że boks i niebezpieczne miejsca niektórych miast to kwestie proste i oswojone. A gry komputerowe zagościły w naszej cywilizacji stosunkowo niedawno i w świadomości osób poszukujących prostych odpowiedzi na temat powodów tak licznych dewiacji społecznych zastąpiły miejsce przedtem zajmowane m.in. przez telewizję. Tak zresztą jest z każdym medium, które pojawia się w naszej szybko zmieniającej się cywilizacji: niecałe sto lat temu to kino ściągało na siebie gromy ludzi książki. Oskarżane było o sianie zepsucia i tandetną, żerującą na najniższych instynktach, rozrywkę. I jeżeli spojrzymy na produkcję filmową pierwszych lat kina, trudno tam znaleźć dzieła wybitne. Królowały nieskomplikowane komedie oparte na prostackim humorze. I jakże szybko pojawiły się produkcje o podejrzanym charakterze, w tym niedwuznacznie pornograficzne.

Jeżeli więc gry komputerowe będą się rozwijały tak jak film, za pewien czas doczekamy się nie tylko upowszechnienia społecznej aprobaty dla nich, ale też gier wykazujących wybitne wartości artystyczne. Już dziś można wskazać wiele tytułów, które mają niebanalną problematykę i stawiają swym uczestnikom wymagania nie niższe niż najlepsze dzieła kultury popularnej. Dobrym przykładem jest polska produkcja pt. „Wiedźmin"[4], oparta na znanych książkach Andrzeja Sapkowskiego. Można mieć nadzieję, że za kilka lat pojawią się gry, dla których właściwym kontekstem będą książki wysokoartystyczne.

Badacze kultury dawno zauważyli wybitne wartości gier oraz ambiwalentny do nich stosunek części dorosłych. Zygmunt Freud na długo przed Huizingą i Caillois[5] dostrzegł kulturotwórczą wartość gry/zabawy (*Spiele*) dziecięcej. Znajduje dla niej powody identyczne z motywacją działalności artystycznej: *Czy pierwszych śladów działań poetyckich nie powinniśmy szukać już u dziecka? Ulubionym i najintensywniejszym zajęciem dziecka jest zabawa. (…) każde bawiące się dziecko zachowuje się jak poeta, tworząc swój własny świat*[6]. Gra/zabawa dostarcza dziecku przyjemności. Jej źródło tkwi w fantazjowaniu. Tej samej przyjemności pożąda człowiek dorosły, ale tylko artysta może fantazjować na jawie bez narażania się na potępienie społeczne. *Fantazjowanie człowieka jest trudniejsze do obserwacji niż zabawa dzieci. Dziecko bawi się wprawdzie również, samo lub wraz z innymi dziećmi stwarza w tym celu zamknięty system psychiczny, ale jeśli nawet nie odgrywa czegoś przed dorosłymi, to nie kryje przed nimi swojej zabawy. Dorosły natomiast wstydzi się swoich fantazji i ukrywa je przed innymi*[7].

Gry komputerowe a szkoła

Istotnym składnikiem kultury współczesnej, a zwłaszcza projektowanego jej kierunku określanego jako Web 2.0 mają być gry komputerowe i to one są – moim zdaniem – nadzieją pedagogów, choć prawie żaden z nich nie zdaje sobie z tego sprawy. Większość gier komputerowych ma fabułę i inne składniki świata przedstawionego, co zbliża je do literatury pięknej i filmu fabularnego. Najwięcej podobieństw łączy gry i fantastykę, szczególnie z takimi jej pododmianami, jak *fantasy*, *science fiction* i horror[8]. Fabuła gier bardzo często ma wyraźne korzenie mityczne, a bohaterowie są wcieleniami najważniejszych archetypów osobowych: Sieroty, Męczennika, Wędrowca, Wojownika,

3 Gala A., Ulfik-Jaworska I. [red.] *Oddziaływanie „agresywnych" gier komputerowych na psychikę dzieci*, Marki 2004.
4 Gra wydana przez CD Projekt w 2008 r.
5 Caillois R. *Ludzie a gry i zabawy* [w:] idem, *Żywioł i ład*, Warszawa 1973, s. 295-467.
6 Freud Z. *Poeta i fantazjowanie* [w:] Pospiszyl K. *Zygmunt Freud – człowiek i dzieło*, Wrocław 1991, s. 249.
7 Ibidem, s. 250.
8 Por. Szeja J. *Przyczyny popularności fantastyki i gier fabularnych w kulturze współczesnej* [w:] Surdyk A. [red.] *Kulturotwórcza funkcja gier, Gra jako medium, tekst i rytuał*, Poznań 2007, t. 1, s. 189-195.

Maga-Czarodzieja, Starego Mędrca, Dziewicy, Czarownicy, Królowej. Szczególnie często są spotykane postaci uosabiające archetyp Cienia, co powierzchownym obserwatorom gier dostarcza motywów do oskarżeń o ich demoralizujący wpływ. Tymczasem w takim kształcie zabaw z komputerem tkwi wielki potencjał kulturotwórczy, bo jak pisze znakomity polski znawca Junga Zenon Waldemar Dudek: *Archetypy wprowadzają porządek w życie osoby, społeczeństwa i kultury. Mogą uczynić człowieka mądrym, nawet mimo jego ograniczonej wiedzy*[9]. Mądrość jest synonimem życiowej skuteczności i etyczności zarazem, więc jej wykształcenie jest celem nauczania. Zauważmy też, że podmiot takiego procesu wpajania archetypów zdobywa mądrość, choć nie zdobywa wiedzy. Niemniej jednak nie jest to naszym problemem: obecna cywilizacja wiedzy ma wprost w nadmiarze, a sztuką jest jej odnalezienie – np. wyszukanie w Internecie wiarygodnej, pożądanej informacji wśród innych, tymczasowo nieprzydatnych lub o wątpliwej jakości.

Istotne są pytania praktyka: Jak konkretnie miałoby wyglądać nauczanie we współczesnej kulturze multimedialnej i interaktywnej? Co robić z masowym odejściem młodzieży od czytania literatury należącej do kanonu? Na pewno już niedługo większość systemów oświatowych krajów zaawansowanych technologicznie będzie musiała na te pytania odpowiedzieć. Na dziś można rzec tylko tyle: należy promować skuteczne i bezpieczne korzystanie z Internetu i nie powinno się zabraniać zabaw z grami komputerowymi, a instytucje oświatowe powinny być zainteresowane promowaniem szczególnie wartościowych tytułów dostosowanych do odpowiedniego wieku ucznia oraz upowszechnianiem wiedzy na temat ratingu gier i zasad obowiązującego w Europie systemu PEGI[10]. Za szczególnie szkodliwe powinno się uznać postawy negujące gry z przyczyn ideologicznych, na podstawie wątpliwych przesłanek i niepoprawnych merytorycznie, tendencyjnych badań.

Wśród licznych typów gier komputerowych najwartościowsze dla realizowania celów formacyjnych są cRPG (komputerowe odpowiedniki narracyjnych gier fabularnych), ale z roku na rok wzrasta potencjał gier typu MMORPG (internetowe RPG rozgrywane z innymi ludźmi), które wydają się szczególnie przeznaczone dla osób stale obecnych w sieci[11]. Gry te są znakomitą platformą socjalizacyjną i powołują do istnienia masowe społeczności sieciowe nowego typu.

Niedostrzeganie w grach wyżej zarysowanych możliwości pedagogicznych ma źródło m.in. w niedostatkach zrozumienia, w jaki sposób literatura działa formacyjnie. Wiele osób nie rozumie istoty kształcenia polonistycznego w tym zakresie, a dowodów na to dostarczyły m.in. publiczne dyskusje na temat ministerialnej listy lektur obowiązkowych. Szczególnie przykre jest, że właściwie żadna ze stron tej dyskusji nie wykazała się odpowiednią wiedzą. Np. wbrew mniemaniom ministra Romana Giertycha i większości jego adwersarzy literatura piękna nie działa przez swoją wymowę ani przez przykład. Cóż bowiem pozytywnego łączy dzieje Konrada, Kordiana, hrabiego Henryka, Wokulskiego, Raskolnikowa, Judyma, Baryki, Ziembiewicza? Błądzi ten, kto myśli, że Soplica i Kmicic mogą być wzorotwórczy dla współczesnej młodzieży. Nie bardziej niż Józio z „Ferdydurke", czyli tak naprawdę wcale. Jak stwierdza Jerzy Kaniewski: *znaczenie kanonu zasadza się nie na potencjalnie zamkniętych w nim sensach, a na wartości samej lektury, rozumianej nie tylko jako proces odczytywania wpisanych w dzieło znaczeń, ale i jako umiejętność stawiania utworowi pytań i poszukiwania na nie odpowiedzi*[12]. Polonista właściwie realizuje swoje powołanie, gdy wyposaża uczniów w umiejętność odbioru dzieła, zachęca do lektury i budzi refleksję. Formacyjny charakter ma sam akt czytania kompetentnego odbiorcy, który w ten sposób staje się uczestnikiem kultury. Podobnie do refleksji może zapraszać film i gra komputerowa. Zresztą w bardzo wielu grach ich uczestnik musi przeczytać wiele tekstów o charakterze literackim. Celują w tym zwłaszcza gry z podgatunku cRPG.

Gry komputerowe są ważnym składnikiem naszej zaawansowanej technologicznie cywilizacji. Jak i inne zjawiska mogą być też niebezpieczne, jednak już dziś, mimo niewielu lat swego rozwoju, wykazują cechy, których wykorzystanie może mieć bardzo pozytywne konsekwencje. Na pewno powinny być uważnie badane przez naukowców i instytucje do tego powołane, jak na Zachodzie DiGRA (*Digital Games Research Association*[13]), a w Polsce PTBG (Polskie Towarzystwo Badania Gier[14]).

9 Dudek Z.W. *Cień, Anima, Wielka Matka*, Charaktery nr 7/2005.
10 Zob. http://www.pegi.info/pl/index
11 Por. Szeja J. *Gry fabularne. Nowe zjawisko kultury współczesnej*, Kraków 2004.
12 Kaniewski J. *Jaki kanon?,* Polonistyka nr 5(445)/2007, s. 11.
13 Istnieje od 2003 r. Pierwszym przewodniczącym DiGRA był prof. Frans Mäyrä, następnym prof. Tanya Krzywinska (od 2006 r.). DiGRA jest stowarzyszeniem skupiającym naukowców i praktyków zajmujących się badaniem gier i powiązanych z nimi zagadnień.
14 Założone w 2004, zarejestrowane w 2005 r.

Bibliografia

1. Caillois R. *Ludzie a gry i zabawy* [w:] idem, *Żywioł i ład*, Warszawa 1973.
2. Dudek Z.W. *Cień, Anima, Wielka Matka*, Charaktery nr 7/2005.
3. Freud Z. *Poeta i fantazjowanie* [w:] Pospiszyl K. *Zygmunt Freud – człowiek i dzieło*, Wrocław 1991.
4. Gala A., Ulfik-Jaworska I. [red.] *Oddziaływanie „agresywnych" gier komputerowych na psychikę dzieci*, Marki 2004.
5. Huizinga J. *Homo ludens*, Warszawa 1998.
6. Kaniewski J. *Jaki kanon?,* Polonistyka nr 5(445)/2007.
7. Schechner R. *Zabawa* [w:] idem: *Przyszłość rytuału*, Warszawa 2000.
8. Szeja J. *Przyczyny popularności fantastyki i gier fabularnych w kulturze współczesnej* [w:] Surdyk A. [red.] *Kulturotwórcza funkcja gier, Gra jako medium, tekst i rytuał*, t. 1, Poznań 2007.
9. Szeja J.Z. *Cywilizacja zabawy? Próba spojrzenia w przyszłość* [w:] Surdyk A., Szeja J.Z. [red.] *Kulturotwórcza funkcja gier. Cywilizacja zabawy czy zabawy cywilizacji? Rola gier we współczesności*, Homo Communicativus nr 3(5), Poznań 2008.
10. Szeja J.Z. *Fabuła na żywo*, Perspektywy nr 11/2001.
11. Szeja J.Z. *Gry fabularne – nowe zjawisko kultury współczesnej*, Kraków 2004.
12. Szeja J.Z. *Jakie są przyczyny popularności gier komputerowych?*, Nowa Polszczyzna nr 4/2005.
13. Szeja J.Z. *Nowe formy kształcenia: narracyjne gry fabularne*, Polonistyka nr 7/2000.
14. Szeja J.Z. *Świat graczy* [w:] Surdyk A., Szeja J.Z. [red.] *Kulturotwórcza funkcja gier. Gra w kontekście edukacyjnym, społecznym i medialnym*, Homo Communicativus nr 2(4), Poznań 2008.

Autor jest kulturoznawcą, polonistą, nauczycielem licealnym i akademickim, prezesem Polskiego Towarzystwa Badania Gier

Klasyfikacja PEGI dzielona jest na dwie części: klasyfikacji wiekowej i opisu treści.

Oznaczenia klasyfikacji wiekowej znajdują się w lewym dolnym rogu na froncie opakowania zawierającego grę.

Oznaczenia dotyczące treści zawartych w grze (jeśli występują) znajdują się z tyłu opakowania wraz z powtórzonym oznaczeniem wiekowym. W zależności od rodzaju gry, na okładce mogą znajdować się obrazki wskazujące na występowanie w grze następujących elementów: przemoc, wulgaryzmy, lęk, narkotyki, seks, dyskryminacja, hazard i gra w Internecie z innymi ludźmi.

Należy pamiętać, że *rating* wiekowy nie uwzględnia poziomu trudności ani umiejętności niezbędnych do danej gry, natomiast dostarcza wiarygodnych informacji o stosowności gry z punktu widzenia ochrony dzieci. Przykładowo klasyfikacja 12 oznacza, że gra nie zawiera treści nieodpowiednich dla dzieci w wieku 12 lat i powyżej.

Więcej informacji na stronie www.pegi.info

Jaromir Bogacz

Ciemna strona Internetu

To był jeden z internetowych hitów 2006 roku. Na amatorskim nagraniu widać jak Ghyslain Raza, pulchny 15-latek, z wielkim zaangażowaniem wymachuje drągiem udając, że jest jednym z rycerzy Jedi. Kiedyś taki film skończyłby pewnie jako niewinny dowcip, przypominany przez krewnych, ku zażenowaniu głównego bohatera. Pech chciał, że jeden z kolegów postanowił skorzystać z możliwości oferowanych przez nowe technologie i umieścił film w Internecie. Autor znany od teraz jako „Star Wars Kid" niemal od razu stał się obiektem kpin milionów ludzi na całym świecie. Wyśmiewany przez kolegów przestał chodzić do szkoły i znalazł się pod opieką psychologa. Rzeczywiście trudno sobie nawet wyobrazić wstyd dziecka, które przez głupi żart staje się pośmiewiskiem – dosłownie – całego świata.

Ta historia bardzo dobrze pokazuje nowe problemy, jakie pojawiły się wraz z rozwojem Internetu, i nowe wyzwania, jakie stoją przed pedagogami. Pytani o zagrożenia w sieci, niektórzy natychmiast wyobrażają sobie wirusy błyskawicznie przeskakujące z komputera na komputer i niszczące nasze dane. Inni przede wszystkim dostrzegają jakieś ciemne zakamarki Internetu – strony pełne przemocy lub pornografii dziecięcej. I dobrze, bo to wciąż są aktualne problemy. Ale ich rozwiązanie należy w dużej mierze do policji i informatyków, a nauczyciel może przed nimi co najwyżej ostrzegać.

Natomiast przygotowanie uczniów do życia w wirtualnym społeczeństwie, to przede wszystkim rola pedagogów. Internet już dawno przestał być tylko źródłem pożytecznych informacji, a stał się zupełnie nowym środowiskiem, w którym możemy robić zakupy, wymieniać plotki i zawierać znajomości. Tylko że ten drugi świat rządzi się swoimi prawami, a to co nam (albo naszym uczniom) wydaje się bezpieczne w świecie rzeczywistym, nie musi być takie w jego wirtualnym odpowiedniku. W powyższym przykładzie zachowanie kolegów miało być zapewne głupim żartem, a jednak już na zawsze naznaczyło kanadyjskiego nastolatka.

Żyjemy w świecie, w którym dane w tempie błyskawicy okrążają świat. Coraz rzadziej mamy pewność, jak naprawdę wygląda i reaguje osoba, z którą rozmawiamy, a każda przypadkowo ujawniona informacja może zostać w Internecie już na zawsze. Często nie zdajemy sobie sprawy zarówno z możliwości, jak i zagrożeń, jakie to stwarza. Tym bardziej nie są ich świadomi (lub o nich nie myślą) uczniowie. W Wielkiej Brytanii rząd zdecydował się wprowadzić do obowiązkowego programu szkoły podstawowej kurs uczący dzieci bezpiecznego zachowania w sieci. Program brytyjski, prowadzony pod hasłem „Zip it, Block it, Flag it"[1] uczy dzieci:

- ochrony prywatności (*zip it* – tu w znaczeniu: trzymaj buzię zamkniętą na kłódkę),
- radzenia sobie z agresją innych użytkowników sieci (*block it* – blokuj tych, którzy sprawiają, że czujesz się nieswojo),
- radzenia sobie z niechcianymi treściami (*flag it* – oznacz i poinformuj opiekuna, gdy się na takie natkniesz).

W swoim krótkim opisie podstawowych zagrożeń, jakie stoją przed uczniami, do tej listy dodałem wciąż jeszcze aktualny problem złośliwego oprogramowania.

Prywatność

Większość z nas pewnie pamięta billboardy i spoty reklamowe z opasłym panem w przykrótkiej koszulce, przedstawiającym się na czacie jako „Wojtek, lat 12". Niewątpliwie kampanii prowadzonej pod hasłem „Nigdy nie wiadomo, kto jest po drugiej stronie" udało się wzbudzić społeczne zainteresowanie. I bardzo dobrze, bo ta wcale nieoczywista dla małego dziecka prawda, stanowi dobry początek do rozmowy o bezpiecznym przeglądaniu Internetu.

[1] Na stronie programu (http://clickcleverclicksafe.direct.gov.uk/index.html) można uzyskać informacje, czego brytyjskie dzieci będą się uczyły w ramach zajęć z bezpieczeństwa w Internecie.

Właśnie dlatego, że nigdy nie wiadomo, kto jest po drugiej stronie, dziecko nie powinno ujawniać żadnych wiadomości prywatnych (adresu, numeru telefonu czy nawet imienia i nazwiska – lepiej, żeby surfując, korzystało z jakiegoś *nicka*). Kolejnymi zasadami, jakie Perry Aftab wymienia w książce „Internet a dzieci. Uzależnienie i inne niebezpieczeństwa[2]", są niespotykanie się bez zgody rodziców z osobami poznanymi przez Internet oraz informowanie rodziców o osobach poznanych w sieci. Te reguły powinny być dla dziecka jasne, gdy zaczyna swoją przygodę z Internetem.

Ujawnianie poufnych informacji, to nie tylko problem małych dzieci. Starsi użytkownicy okazują się równie podatni na podobne zagrożenia, jeśli tylko prośba o ich dane zostanie sformułowana trochę bardziej formalnie. Jedna z najpopularniejszych obecnie metod stosowanych przez *hackerów*, zwana *phishingiem* (co po polsku znaczy mniej więcej tyle co łowienie haseł), polega na masowym wysyłaniu formalnie wyglądających wiadomości z prośbą o podanie numeru i hasła do naszego konta bankowego, np. z powodu rzekomej weryfikacji. Zwykle podany jest link, który prowadzi na przygotowaną wcześniej przez *hackera* stronę, łudząco podobną do oryginalnej witryny banku. Ta prosta metoda niestety okazuje się bardzo skuteczna – na tyle, że dał się na nią nabrać nawet sam dyrektor FBI Robert Mueller.

W przypadku starszych uczniów nie mają sensu tak mocne ograniczenia, jak te proponowane przez Perry'ego Afaba. Ważniejsze jest, aby uświadamiać im, jak ważna jest umiejętność decydowania, które informacje powinny być dostępne publicznie. W badaniach amerykańskiej firmy Career Builder okazało się, że 45% pracodawców sprawdza informacje o kandydatach w sieci, a 35% odrzuca podania pod wpływem informacji tam znalezionych. W dodatku te liczby podwoiły się w porównaniu z rokiem ubiegłym[3].

Nawet kiedy nasz profil jest dostępny tylko dla znajomych, nic to nie zmieni, jeśli nie będziemy zachowywali innych środków ostrożności. W grudniu 2009 roku reporterzy „Dziennika" w ramach prowokacji założyli fikcyjne konta na Naszej Klasie i Facebooku i wysyłali zaproszenia losowo wybranym użytkownikom[4]. Okazało się, że prawie co trzeci z nich potwierdził swoją znajomość z zupełnie obcą sobie osobą i dał jej dostęp do wszystkich swoich danych. Zadziałał tu prosty mechanizm wzajemności – skoro ty mnie uważasz za znajomego, to choć cię nie pamiętam, zaprzeczenie znajomości byłoby nieuprzejme.

Na koniec warto też pomyśleć o jakimś dobrym haśle, czymś bardziej kreatywnym niż „abc123" lub *password* (hasło) – te dwa należą do najczęściej używanych w sieci. Bywa, że *hackerzy* szukają słabo zabezpieczonych kont na portalach społecznościowych, korzystając z listy najpopularniejszych haseł. Później wykorzystują te konta np. do rozsyłania spamu wśród znajomych ofiary.

Agresja

Na lekcjach bezpieczeństwa internetowego brytyjskie dzieci, poza poznaniem zasad zachowania prywatności, dowiadują się, jak reagować na agresywne zaczepki i niechciane treści. Nawet w zwykłych dyskusjach prowadzonych w Internecie poziom agresji jest dużo wyższy niż poza nim. Naukowcy próbowali to zjawisko wytłumaczyć na różne dziwne sposoby, np. frustracją z powodu wolnego przepływu danych, który jakoby uniemożliwiał płynną rozmowę.

Patricia Wallace[5] próbuje tłumaczyć takie zachowania poczuciem bezkarności, jakie daje anonimowość, oraz brakiem komunikacji niewerbalnej. Gdy nie widzimy reakcji wywołanej przez nasze słowa, dużo trudniej o empatię.

Czy agresja „sieciowa" może przenieść się do realnego świata? Odpowiedź wcale nie jest oczywista – duża część internautów traktuje te wirtualne „pyskówki" (*flame war*) niezupełnie serio, jako pewną konwencję, charakterystyczną dla nowego medium. Bardzo często któryś z nich celowo umieszcza prowokacyjny wpis (takie działanie nazywane jest *trollingiem*), aby wywołać „pyskówkę". Niektóre portale są nawet podejrzewane o zatrudnianie zawodowych *trolli*, aby pobudzić dyskusję na swoim forum (jak choćby w przypadku Jasia Śmietany na forum Onetu).

Problemy zaczynają się, gdy internauci zjednoczą się przeciw pewnej grupie (zwłaszcza na polskich forach bardzo dużo jest wątków rasistowskich, homofobicznych itd.) lub, co gorsza, przeciw konkretnej osobie. To ostatnie zjawisko nazwane zostało *cyberbullyingiem* (czyli „nękaniem w sieci"). W polskim Internecie gwałtowna dyskusja na ten temat przetoczyła się po opublikowaniu

[2] Aftab P. *Internet a dzieci. Uzależnienia i inne niebezpieczeństwa*, Prószyński i S-ka, Warszawa 2003.
[3] www.careerbuilder.com
[4] Czubkowska S. *Tak Polacy obnażają się w sieci* (http://www.dziennik.pl/wydarzenia/article513430/Tak_Polacy_obnazaja_sie_w_sieci.html).
[5] Wallace P. *Psychologia Internetu*, Rebis, Poznań 2001.

w „Dużym Formacie" reportażu Magdaleny Grzebałkowskiej[6] o gdańskiej licealistce, która naraziła się klasowej elicie, a w konsekwencji była przez nią wyśmiewana i obrażana na jednym z portali internetowych. Łatwo można przytoczyć przypadki dużo bardziej drastyczne, ale ten wydaje się szczególnie interesujący właśnie ze względu na ową dyskusję. Okazało się, że bardzo duża część internautów zbagatelizowała problem, zresztą podobnie jak rodzice napastliwych nastolatków. Pojawiły się głosy, że gazeta rozdmuchała niewinny w sumie incydent – obmawianie jednych uczniów przez innych nie jest oczywiście niczym chwalebnym, ale też niczym nowym – nowe jest tylko medium.

A jednak zmiana medium tylko pozornie jest zupełnie nieznacząca. W opisanym przypadku u ofiary oprócz poczucia odtrącenia i winy (co sprawiło, że właśnie na mnie się uwzięli?), dołącza się wstyd z publicznego charakteru poniżenia. Sytuacja, w której każdy człowiek może bez żadnych kosztów opublikować informację na całym świecie, jest czymś absolutnie bezprecedensowym. Wszelkie analogie z wcześniejszymi mediami zawodzą – umieszczenie czegoś na blogu nie jest tym samym co opisanie zdarzenia w pamiętniku, a obmowa w dyskusji na forum to nie to samo co w telefonicznej rozmowie. Przynajmniej częścią odpowiedzialności, która kiedyś spoczywała tylko na dziennikarzach i osobach publicznych, zostają teraz obarczone dzieci. I dlatego właśnie niezbędna jest edukacja medialna. O wadze problemu niech świadczą dane pochodzące z badań firmy Gemius dla Fundacji Dzieci Niczyje przeprowadzonych wśród kilkuset osób w wieku 12-17 lat i przytoczone przez „Gazetę Wyborczą"[7]. Co drugi z respondentów (52%) miał do czynienia z jakimś rodzajem agresji w Internecie lub poprzez komórkę. Co piąty badany (21%) był w Internecie ośmieszany, poniżany lub upokarzany. Straszenia i szantażu doświadczyło 16% badanych.

Pornografia

Strony pornograficzne nieodmiennie zajmują pierwsze miejsce pośród zagrożeń wymienianych przez rodziców, których dzieci korzystają z Internetu[8]. Z danych przytaczanych przez Aleksandrę Jaszczak w artykule „Cyberedukacja seksualna i cyberseks młodzieży"[9] wynika, że spośród badanych, których średnia wieku wynosiła 19 lat, zaledwie 22% nigdy nie przeglądało stron pornograficznych w celu osiągnięcia satysfakcji seksualnej, a aż 67% przyznało, że wiedzę na tematy związane ze sferą seksualną czerpało m.in. właśnie z oglądania pornografii. Gdy naukowcy z Montrealu chcieli przeprowadzić badania nad wpływem pornografii na młodych mężczyzn, musieli się wycofać, ponieważ… nie znaleźli żadnego mężczyzn, który by takich materiałów nie oglądał.

Dostęp do pornografii powoli staje się więc czymś powszechnym. Jakie to będzie miało skutki? Naukowcy raczej nie wieszczą katastrofy, choć przyznają, że w różnych badaniach widać pewną zależność pomiędzy oglądaniem przez nastolatków pornografii a oddzielaniem seksu od uczuć i traktowaniem go jako zwykłej fizjologicznej potrzeby. Dużo większym problemem pozostaje dostępność tzw. twardej pornografii (z użyciem przemocy). Patricia Wallace przytacza eksperymenty potwierdzające jej wpływ na poziom agresji, zwłaszcza względem kobiet, a to tylko wierzchołek góry lodowej. Internet jest pełen materiałów pedofilskich, wzywających do przemocy czy nawet uczących, jak skonstruować bombę. Niestety na takie strony można się natknąć zupełnie przypadkowo, wpisując całkiem niewinne hasła do wyszukiwarki. Dlatego, aby małe dzieci mogły bezpiecznie przeglądać Internet, niezbędne są programy blokujące niepożądane strony – a i tak warto ostrzec dzieci przed możliwym zagrożeniem i nauczyć je, co powinny w takim wypadku zrobić (rozłączyć się i porozmawiać z opiekunem). Starszym uczniom warto podać adres strony, gdzie mogą zgłaszać treści niezgodne z prawem – np. dyzurnet.pl. Trzeba też pamiętać, że jeśli uczniowie będą chcieli wejść na zakazaną stronę, programy filtrujące mogą nie wystarczyć. Często można je w prosty sposób obejść przy pomocy serwerów Proxy, łączących się z żądaną stroną i przesyłających jej treść na dany komputer.

Niestety próba zwalczania ciemnej strony Internetu przypomina czasem wysiłki Syzyfa. W 2006 roku, po dużej kampanii medialnej udało się doprowadzić do zamknięcia strony RedWatch, na której faszyści nawoływali do ataków na „zdrajców białej rasy", prezentując zdjęcia i adresy znienawidzonych przez siebie działaczy społecznych i dziennikarzy. Niedługo później witryna wróciła do sieci – została przeniesiona na inny serwer. Sprawę utrudnia fakt, że strona funkcjonuje na serwerach amerykańskich i do jej każdorazowego zamknięcia potrzebna jest koordynacja działań z FBI. To oczy-

6 Grzebałkowska M. *Żal mi dziewczyny z mojej klasy*, Duży Format, 25.06.2008.
7 Domaszewicz Z. *Czy cyberbullying zniszczy anonimowość w internecie*? (http://wyborcza.pl/1,86669,4299345.html).
8 Por. np. badanie „Mądry Internet".
9 Jaszczak A. *Cyberedukacja seksualna i cyberseks młodzieży* [w:] Szmigielska B. [red.] *Całe życie w Sieci*, WUJ, Kraków 2008, s. 95-136.

wiście nie oznacza, że niewielki wysiłek podjęty w celu przeciwdziałania faszystom, pedofilom itp. nie jest wart zachodu. Specyfika Internetu polega jednak na tym, że dużo łatwiej w nim coś umieścić, niż później stamtąd usunąć.

Złośliwe oprogramowanie

Kto tworzy wirusy? Wciąż panuje wyobrażenie, że jest to sprawka genialnych nastolatków, którzy z nudów, chęci sprawdzenia się czy też czystej złośliwości bawią się *hackingiem*. Jak w wywiadzie dla „Computerworld" tłumaczy znany amerykański ekspert do spraw bezpieczeństwa Bruce Schneider[10], czasy samozwańczych naśladowców Neo z „Matrixa" mamy już dawno za sobą. Teraz atakami na komputery zajmują się głównie zorganizowane grupy przestępcze. Jakie znaczenie ma dla przeciętnego internauty wiadomość, kto go atakuje? Wbrew pozorom spore, bo równocześnie zmienił się charakter zagrożeń. Coraz rzadsze są wirusy, które np. niszczą dane. Współczesne wirusy wyszukują w sieci słabiej zabezpieczone komputery, włamują się do nich i… początkowo nie robią nic. Takie przejęcie kontroli nad komputerem ma zazwyczaj jeden z dwóch celów: może chodzić o zdobycie poufnych danych, przede wszystkim numerów kart kredytowych, np. poprzez zainstalowanie programów odczytujących każdy naciśnięty klawisz. Drugim motywem może być chęć uczynienia z naszego komputera *zombie*, czekającego na rozkaz swojego pana. Takie komputery łączone są w sieci zwane botnetami i mogą zostać wykorzystane do masowego rozsyłania spamu bądź ataków na wybrane strony.

Niewątpliwie kluczem do sukcesu dla *hackera* jest ukrycie włamania. W badaniu przeprowadzonym przez American Online okazało się, że ponad 66% posiadaczy zawirusowanych komputerów nie jest świadomych obecności wirusa. Dlatego nie ma sensu zabezpieczanie komputera dopiero, gdy zauważymy jakieś nieprawidłowości – wtedy będzie już na to za późno. Specjaliści od bezpieczeństwa komputerowego ze złością mówią o użytkownikach, którzy lekceważąc podstawowe zasady bezpieczeństwa, nie tylko zagrażają sobie, ale mimowolnie pomagają cybergangsterom. A zasady te są rzeczywiście proste: wgrywanie dostępnych aktualizacji i zaopatrzenie się w dobry, koniecznie regularnie uaktualniany program antywirusowy z *firewallem*. Warto też unikać podejrzanych stron (zwłaszcza z pirackim oprogramowaniem) i w żadnym wypadku nie instalować programów niewiadomego pochodzenia. Częstym trickiem *hackerów* jest przedstawianie wirusa jako... antywirusa. Po wejściu na stronę pojawia się informacja o wykrytym robaku i propozycja instalacji programu, który zagrożenie usunie.

Na zakończenie

Nie ma sensu spierać się o wady i zalety Internetu – i tak stał się medium, do którego przenosi się coraz większa część naszego życia. A jeśli nawet nie naszego, to na pewno naszych uczniów. I niewątpliwie to się już nie zmieni. Dlatego warto wiedzieć, co powinno nam się wydawać podejrzane i jakie działania mogą być niebezpieczne – bo tu, tak jak w rzeczywistym życiu, zagrożenia czekają przede wszystkim na tych, którzy są ich nieświadomi. Przed nauczycielami i rodzicami stoi niemałe wyzwanie – uczyć dzieci i młodzież podstawowych zasad korzystania z nowego medium, aby Internet, mimo ciemnych stron, stawał się coraz szerzej otwartym oknem na świat informacji.

Autor jest absolwentem informatyki UJ, studentem filmoznawstwa

Gry oznaczone tym znakiem uznaje się za odpowiednie dla wszystkich grup wiekowych. Dopuszczalna jest pewna ilość przemocy w komicznym kontekście. W grze nie występują dźwięki i obrazy, które mogą przestraszyć dziecko oraz wulgaryzmy, nagość ani odwołania do czynności seksualnych.

Przykładowe gry z tej grupy: Super Mario Galaxy, Catz, SingStar.

[10] Schneier B. *Bezpieczeństwo nie jest sexi* (http://www.pcworld.pl/news/144463/Bruce.Schneier.Bezpieczenstwo.nie.jest.sexi.html).

Michał Feldman

Internet dojrzał, a my... chorzy?

„Sto lat, sto lat" życzyły temu niecodziennemu jubilatowi miliony ludzi w całej Polsce. 17 sierpnia 2009 roku Internet w Polsce skończył 18 lat. Dzięki niezliczonej liczbie jego zastosowań w codziennym życiu – od rozrywki, przez prowadzenie własnych finansów, uzyskiwanie ważnych informacji, wreszcie po nieskrępowaną komunikację z innymi ludźmi – wiele osób nie wyobraża sobie życia bez codziennego dostępu do Internetu. Czy to zwyczajne wykorzystanie możliwości nowoczesnych technologii, czy już uzależnienie?

Mała dziewczynka stoi na plaży i płacze. Ludzie ją pytają:

– Dlaczego płaczesz?

– Bo się zgubiłam.

– Jak się nazywasz?

– Nie wiem.

– A jak się nazywa twoja mama?

– Nie wiem.

– A swój adres znasz?

– wu-wu-wu-kropka-basia-kropka-pl

Czy podobne historie to wciąż tylko powód do żartów, czy już zwykła codzienność? Czy coś z nich dla nas wynika?

Uzależnienie od Internetu (netoholizm) zostanie wpisane do najnowszej wersji Międzynarodowej Klasyfikacji Chorób i Problemów Zdrowotnych (*International Classification of Diseases*, ICD) jako choroba psychiczna – od połowy 2009 roku huczą wszystkie lekarskie media. Żeby zrozumieć, jak ważna to decyzja, trzeba wiedzieć, że ICD to biblia dla współczesnego lekarza.

Jeżeli jakiejś choroby nie ma w ICD – to w dzisiejszym medycznym świecie oznacza, że taka choroba nie istnieje lub po prostu... nie jest chorobą. Tak jak homoseksualizm, który został wykreślony z klasyfikacji ICD przez Światową Organizację Zdrowia (WHO) w 1990 roku i od tamtej pory nie widnieje na żadnych listach chorób.

Bardzo rzadko zdarza się jednak, że jakiejś choroby lub problemu zdrowotnego nie można znaleźć w ICD. Wystarczy wspomnieć, że oprócz tysięcy takich poważnych dolegliwości, jak cukrzyca, schizofrenia czy grypa, można w ICD znaleźć tak rzadkie problemy, jak „przedłużone przebywanie w stanie nieważkości" czy „kontakt z jadowitymi zwierzętami i roślinami morskimi". To dlatego wielu lekarzy i naukowców naciska, aby uzależnienie od Internetu jako problem masowy, dotyczący według różnych badaczy od 1 nawet do 18% nastolatków, zostało uznane za pełnoprawną chorobę posiadającą swój kod w klasyfikacji ICD.

Trzeba jednak wyraźnie zaznaczyć – uzależnienie od Internetu to z lekarskiego punktu widzenia jednak nie to samo co uzależnienie od alkoholu czy narkotyków. Prof. Wojciech Kostowski (przewodniczący Wydziału Nauk Medycznych PAN w Warszawie) twierdzi, że można je zaliczyć do uzależnień behawioralnych, czyli tzw. zachowań przymusowych. Działa tu typowy układ nagrody: określona czynność czy zachowanie kojarzy się z przyjemnością i działa na odpowiedni ośrodek w mózgu. Do tego typu uzależnień zalicza się również m.in. szopoholizm (uzależnienie od zakupów) czy uzależnienie od hazardu.

W odróżnieniu od uzależnień biologicznych (czyli takich jak alkoholizm, nikotynizm), uzależnienie od Internetu nie wpływa w patologiczny sposób na fizjologię ludzkiego organizmu. Nie powoduje zespołów abstynencyjnych, chociaż w mechanizmie frustracji, po przymusowym odłączeniu od internetowej sieci, często prowadzi do agresywnych zachowań. Może natomiast znacznie zaburzać funkcjonowanie i rozwój młodego człowieka. Utrudnia dojrzewanie emocjonalne i budowanie prawdziwych relacji z rówieśnikami, które są niezbędne w procesie kształtowania młodej osobowości.

Nie należy jednak dać się zwariować – podkreślają specjaliści zajmujący się na co dzień uzależnieniami. Od pewnego czasu modne jest bowiem wyszukiwanie różnych problemów w zachowaniach, w zależności od kontekstu danej chwili.

Lekarze przypominają, że na przykład gloryfikowaną dawniej pracowitość coraz częściej interpretuje się w kategoriach pracoholizmu. Budzące kiedyś niepokój nałogowe czytanie książek (rzekomo powodujące utratę wzroku, zapadniętą klatkę piersiową, anemię, astmę i charłactwo) dziś jest marzeniem rodziców podobnie zaniepokojonych długością czasu, jaką ich dzieci spędzają przed komputerem.

Kiedy zatem martwić się o dziecko, które podejrzanie dużo czasu spędza w Internecie?

Dr Kimberly Young (amerykańska psycholog, jedna z pierwszych osób prowadzących badania nad uzależnieniem internetowym) w 1996 roku przedstawiła kryteria uzależnienia od Internetu. Według testu dr Young wystarczy odpowiedzieć „tak" na pięć z poniższych pytań, aby rozpoznać problemy z uzależnieniem od Internetu u swojego dziecka:

1. Czy czujesz, że Twoje dziecko jest zaabsorbowane Internetem (często myśli o poprzednich bądź następnych pobytach w sieci)?

2. Czy czuje potrzebę coraz dłuższego korzystania z Internetu?

3. Czy pozostaje w sieci dłużej niż pierwotnie planowało?

4. Czy wielokrotnie miało nieudane próby kontroli, ograniczenia czasu lub zaprzestania korzystania z Internetu?

5. Czy dziecko czuje się niespokojne, markotne, zirytowane, przygnębione, gdy nie może korzystać z Internetu?

6. Czy ryzykuje utratę znajomości z przyjaciółmi, zaniedbuje naukę z powodu Internetu?

7. Czy oszukuje Cię, aby ukryć narastający problem Internetu?

8. Czy używa Internetu jako sposobu na ucieczkę od problemów lub sposobu na poprawę pogorszonego nastroju (uczucia bezradności, winy, lęku, depresji)?

Testy, takie jak powyższy, ze względu na konieczne uproszczenia, mają jednak wiele ograniczeń, a ich wyniki często wprowadzają w błąd.

Rodzic może mieć czasem spore trudności z rozpoznaniem uzależnienia, jeśli dziecko stosuje przekonujące wymówki, np. „nie spędzam czasu w Internecie, tylko zbieram materiały do lekcji", „nie mogę inaczej skontaktować się z kolegą/koleżanką, bo mieszka daleko" itp. Rodzice powinni także pamiętać, że sam nastolatek może nie dostrzegać problemu i nie mieć motywacji do zmiany, dopóki nie znajdzie się w poważnym kryzysie. Jeżeli rodzic podejrzewa, że dziecko za dużo czasu spędza w Internecie, powinien skonsultować się ze specjalistą (psychologiem, lekarzem psychiatrą) od uzależnień.

W wielu przypadkach uzależnienie od Internetu mija samoistnie, w czym pomocne może być wsparcie bliskich osób. W poważniejszych przypadkach związanych z silną izolacją społeczną lub znaczącym zaawansowaniem objawów, jedyną metodą jest psychoterapia. Za najskuteczniejszą w walce z tym zaburzeniem uznaje się terapię poznawczo-behawioralną. Nie jest rozwiązaniem abstynencja, jaką zaleca się w leczeniu alkoholizmu lub narkomanii, gdyż Internet dla coraz większej liczby osób jest niezbędnym narzędziem pracy, a konieczność korzystania z niego na różnych obszarach będzie rosła. Głównym celem terapii jest odzyskanie kontroli nad używaniem Internetu, ale paradoksalnie może się okazać, że to nie dziecko spędza za dużo czasu w Internecie, tylko jego rodzic... nieadekwatnie mało.

Adresy, które warto znać:
www.bezpytan.pl – specjalna internetowa poradnia dla uzależnionych (również od Internetu)
Test *online* sprawdzający uzależnienie do Internetu: http://www.psychologia.net.pl/testy.php?test=infoholizm

Autor jest lekarzem psychiatrą w Instytucie Psychiatrii i Neurologii w Warszawie
michal.feldman@konsylium24.pl

Poczucie bezpieczeństwa,
nawet najbardziej usprawiedliwione,
jest złym doradcą.

Joseph Conrad

Dr Elżbieta Gajek

Bezpieczeństwo w sieci tematem lekcji językowej

Uczniowie coraz częściej korzystają z obcojęzycznych stron internetowych, dlatego powinni być świadomi, że podobnie jak na stronach w języku ojczystym, nie wszystkie materiały tam dostępne są dla nich odpowiednie. Umiejętność oceny zawartości strony internetowej ze względu na jej przydatność oraz formę staje się jedną z podstawowych sprawności korzystania z sieci. Powinna być ćwiczona także w językach obcych. Serwisy społecznościowe Web 2.0 zapewniają warunki do publikacji różnorodnych treści, np. filmowych lub graficznych. Uczniowie coraz częściej korzystają z tych serwisów. Powinni mieć świadomość odpowiedzialności za własne publikacje. Ponadto uczniowie nawiązują kontakty w językach obcych w piśmie i w mowie. Powinni więc wiedzieć, jak zachowywać się w interakcjach sieciowych, jak odróżniać zachowania zagrażające od neutralnych.

W zależności od wieku zmienia się podatność dzieci na różne rodzaje zagrożeń, więc zarówno ten temat, jak i sposoby przeciwdziałania niebezpieczeństwom powinny być regularnie omawiane. Bezpieczne zachowanie w cyberprzestrzeni może być w sposób interesujący rozważane na lekcji językowej w ramach szerszego tematu bezpieczeństwa we współczesnym świecie, np. na drogach, w wodzie, w sklepach czy w sytuacji pożaru. W podręcznikach do nauki języka sytuacje ryzykowne, w których istotne są sposoby zachowania spokoju i właściwe reakcje językowe, pojawiają się zdecydowanie rzadziej niż np. zakupy. Typowe ćwiczenia językowe (czytanie tekstu, przygotowanie ankiet, rozwiązywanie quizów w sieci), które zawierają opisy niewłaściwych działań użytkowników sieci, z jednej strony pozwalają uczniom na powtórzenie zasad bezpieczeństwa, rozpoznanie trudnych sytuacji oraz właściwe reagowanie w przypadku ich zauważenia, z drugiej zaś strony stwarzają warunki do przyswojenia użytecznego słownictwa i nabycia sprawności mówienia i pisania w językach obcych o sytuacjach trudnych. Świadomość zagrożeń oraz nabycie umiejętności przeciwdziałania im podnosi kompetencje uczniów w zakresie korzystania z sieci i jednocześnie kieruje ich uwagę na wartości etyczne i edukacyjne sieci. Jednak większość zasobów Internetu jest dostępna w językach dla Polaka obcych.

W sieci znajduje się ogromna liczba różnojęzycznych stron internetowych poświęconych ewaluacji stron internetowych i bezpieczeństwu w cyberprzestrzeni. Dlatego poniższy artykuł będzie dotyczył raczej technik pracy nad bezpiecznym korzystaniem z Internetu niezależnie od nauczanego języka. Podane będą przykładowe, nieliczne adresy stron internetowych (głównie anglojęzycznych) w celu zachęcenia nauczyciela do własnych poszukiwań materiałów odpowiednich do wieku i potrzeb uczniów oraz nauczanego języka. Niestety coraz więcej znakomitych materiałów edukacyjnych jest dostępnych na warunkach komercyjnych.

Praca z tekstem – informacje o bezpieczeństwie w sieci

Do pracy nad tekstem o zagrożeniach stosuje się te same techniki, które zwykle używane są na lekcji językowej do nauczania rozumienia tekstu czytanego.

Przykładowe pytania wprowadzające w temat:

- Co złego może spotkać użytkownika sieci?
- Jakie cechy lub treści strony wskazują, że powinnaś/powinieneś zrezygnować z jej czytania?
- Jakich informacji nie wolno podawać w komunikacji internetowej?
- Jakich informacji o sobie i o bliskich nie wolno publikować w sieci?

Przykładowe pytania do tekstu:

- Do kogo skierowany jest tekst? Podaj wyrażenia uzasadniające Twoją decyzję.
- Jakie zagrożenia zostały opisane?
- Jakie zachowania bohaterów zostały przedstawione?

- Na co należy zwracać uwagę, korzystając ze strony internetowej?
- Jakie wnioski wynikają z przedstawionej sytuacji?

Przed pierwszym czytaniem tekstu czasami warto podać i wyjaśnić uczniom nowe słownictwo. Po przeczytaniu tekstu i wykonaniu ćwiczeń sprawdzających jego zrozumienie, uczniowie mogą rozpocząć dyskusję o swoich doświadczeniach odnoszących się do bezpieczeństwa w sieci. Prace można zakończyć zapisaniem kilku najważniejszych zasad bezpiecznego korzystania z Internetu lub opisaniem własnych doświadczeń.

Dobrym materiałem rozpoczynającym lekcję językową o bezpieczeństwie w sieci lub uzupełniającym tekst może być też krótki film z YouTube'a. Wówczas pracujemy według zasad pracy z filmem. Przykładowo pytamy: Gdzie miała miejsce przedstawiona sytuacja? Kim byli uczestnicy akcji? Jakie były cele ich działania? Jakie były skutki ich działania? Jakie wnioski wynikają z przedstawionej sytuacji?

Wiele interesujących tekstów oraz pomysłów, które można wykorzystać na lekcji z gimnazjalistami i licealistami, znajduje się na stronie SafeKids.com, na przykład kontrakt rodzinny z dziesięcioma zasadami, których należy przestrzegać w sieci (załącznik). Anglojęzyczny kontrakt można, w sposób innowacyjny zastosować na lekcjach różnych języków do ćwiczenia kompetencji mediacji międzyjęzykowej oraz kompetencji różnojęzycznej z wykorzystaniem tłumacza maszynowego Google tłumacz (http://translate.google.pl). Ćwiczenie polega na tym, że uczniowie wklejają tekst kontraktu w okno języka źródłowego. Po uzyskaniu tłumaczenia poprawiają tekst w języku docelowym – ojczystym lub innym znanym, np. niemieckim lub francuskim – zgodnie z jego regułami.

Nastolatki zainteresują się z pewnością kształtowaniem tożsamości cyberobywateli i cyberetyką (*Cyberethics for kids*) w związku z korzystaniem z sieci. Bardzo atrakcyjna dla ich rówieśników może być strona BSA Cyber Tree House (www.cybertreehouse.com), na której umieszczono filmy o bezpieczeństwie w Internecie przygotowane z udziałem młodzieży.

Grupa uczniów bardzo zaawansowana językowo i komputerowo może zainteresować się „Konwencją o cyberprzestępstwach" (*Convention on cybercrime*) lub raportami prasowymi o poważnych przestępstwach w sieci.

Zebrane materiały tekstowe mogą posłużyć do dyskusji. Ponadto mogą być podstawą prezentacji, np. PowerPoint lub plakatu, czy też eseju fotograficznego, zawierającego zdjęcia lub ilustracje wykonane przez uczniów.

Quizy i zabawy

Do problemu bezpieczeństwa w sieci można podejść w formie zabawy językowej. Przykładem przyjaznego quizu w języku angielskim jest materiał na stronie SafeKids Quiz (http://www.safekids.com/quiz). Po udzieleniu odpowiedzi na pytanie opisujące zachowanie w sytuacji, która może być niebezpieczna, uczniowie uzyskują natychmiast ocenę, czy zachowali się właściwie.

Dla najmłodszych dzieci przygotowywane są środowiska uczenia się, które zgodnie z wymogami rozwojowymi bawią, jednocześnie ucząc. Są one szczególnie popularne w Australii i Nowej Zelandii. Przykładem może być Hectors World (http://www.hectorsworld.com), skierowany do najmłodszych użytkowników w sieci. Na wspomnianej już stronie BSA Cyber Tree House można także zagrać w gry online o bezpieczeństwie.

Projekt międzynarodowy o bezpieczeństwie w sieci

Bezpieczeństwo w sieci może być też tematem ciekawych projektów międzynarodowych, np. podjętych w ramach programu eTwinning. Nawet podczas realizacji krótkoterminowego projektu uczniowie mogą rozmawiać z zagranicznymi partnerami o znaczeniu zasad bezpieczeństwa, przygotowywać materiały papierowe lub elektroniczne, zawierające wybrane, najważniejsze zasady korzystania z sieci. Mogą też wspólnie zająć się netykietą w sieci. Ponadto portal Safer Internet Day (http://www.saferinternet.org) zachęca do współpracy międzynarodowej, dzielenia się doświadczeniami i materiałami edukacyjnymi o bezpieczeństwie w sieci. Liczne projekty dotyczące bezpieczeństwa w sieci i Dnia Bezpiecznego Internetu uzyskały w ostatnich latach Narodową Odznakę Jakości eTwinning. Jako przykład można podać polsko-bułgarski projekt Safer Internet Day zrealizowany w Publicznym Gimnazjum nr 2 im. Jana Heweliusza w Żukowie woj. pomorskie lub polsko-portugalski projekt A Safe e-Journey wykonany w Szkole Podstawowej nr 9 im. Mikołaja Kopernika w Dzierżoniowie (opis projektu dostępny na stronie http://www.sp9interklasa.yoyo.pl/bezpieczenstwo.html). Polsko-słowacki projekt Surfing the Net – an illustrated code of conduct zrealizowany w Zespole Szkół Samochodowo-Budowlanych z Częstochowy uzyskał także Europejską Odznakę Jakości eTwinning. Wyniki wypracowane w tym projekcie

można obejrzeć na stronie http://zssb.ids. czest.pl/etwinning1/Surfing/twining%5B1%5D.html.

Podczas pracy nad projektami uczniowie uczą się języka, porozumiewając się z partnerami, oraz poznają zasady bezpiecznego korzystania z sieci. W ten sposób współtworzą społeczność odpowiedzialnych internautów.

Materiały dla nauczycieli

Pomimo że zagrożenia i zasady bezpieczeństwa w sieci są takie same niezależnie od kultury i języka, to jednak traktowanie tych zagadnień w różnych systemach edukacyjnych jest różne. Dlatego warto zapoznać się także z materiałami obcojęzycznymi przeznaczonymi dla nauczycieli. Rozwiązania zagraniczne mogą stać się tematem szkolenia rady pedagogicznej na temat bezpieczeństwa. Przykładowy materiał dla nauczycieli jest zawarty w broszurach brytyjskiej organizacji BECTA zatytułowanej „Signposts to safety. Teaching e-safety at Key Stages 1 and 2" oraz „Signposts to safety. Teaching e-safety at Key Stages 3 and 4a" lub na niemieckojęzycznej stronie kindersicherheit.de (http://www. kindersicherheit.de).

Dla nauczycieli technologii informacyjnej może to być interesująca profesjonalna lektura w obcym języku, zaś dla nauczycieli języków ciekawy materiał z zakresu techniki cyfrowej w edukacji. Gotowe plany lekcji na temat przestępstw sieciowych i sposobów ochrony przed nimi można znaleźć na stronie Cyberethics for teachers (http://www.justice.gov/criminal/cybercrime/rules/lessonplan1.htm).

Podsumowanie

Zajęcia są tematem bezpieczeństwa w sieci na lekcji językowej pozwala łączyć sprawności techniczne, językowe i kulturowe. Uczniowie uświadamiają sobie podobieństwa doświadczeń w korzystaniu z sieci ponad barierami językowymi i geograficznymi. Właściwie przygotowanie uczniów do korzystania z sieci w aspekcie społecznym i etycznym jest równie ważne, jak nauczenie ich sprawności technicznych i językowych. Warto uświadomić sobie, że sprawności techniczne zmieniają się wraz z rozwojem technologii informacyjnych i komunikacyjnych, natomiast wrażliwość moralna oraz dbanie o bezpieczeństwo własne i innych użytkowników sieci są wartościami trwałymi i stanowią warunek konieczny korzystania z sieci, niezależnie od języka komunikacji. Wrażliwość ukształtowana w młodym wieku może trwale wpływać na relacje społeczne w sieci w skali globalnej, niezależnie od języków komunikacji.

Webgrafia

1. BSA Cyber Tree House
http://www.cybertreehouse.com
2. Computer Crime & Intellectual Property Section
http://www.cybercrime.gov
3. Convention on cybercrime CETS No.: 185, 2001
http://conventions.coe.int/Treaty/en/Treaties/Html/185. htm
4. Cyberethics for kids
http:// www.cybercrime.gov/rules/kidinternet.htm
5. Cyberethics for teachers
http://www.cybercrime.gov/rules/lessonplan1.htm.
6. Hectors World
http:// www.hectorsworld.com/#HOMEPAGE.
7. Kindersicherheit
http://www.kindersicherheit.de
8. Safekids Quiz
http:// www.safekids.com/quiz
9. Safekids worldwide
http://www.safekidsworldwide.org
10. Signposts to safety, Teaching e-safety at Key Stages 1 and 2
http://publications.becta.org.uk/download.cfm?resID=32422
11. Signposts to safety; Teaching e-safety at Key Stages 3 and 4a
http://publications.becta.org.uk/download.cfm?resID=32424

Załącznik

Kontrakt w języku angielskim
(źródło: http://www.safekids.com/contract_kid.htm)

Family Contract for Online Safety

Kids' Pledge

1. I will not give out personal information such as my address, telephone number, parents' work address/telephone number, or the name and location of my school without my parents' permission.

2. I will tell my parents right away if I come across any information that makes me feel uncomfortable.

3. I will never agree to get together with someone I "meet" online without first checking with my parents. If my parents agree to the meeting, I will be sure that it is in a public place and bring my mother or father along.

4. I will never send a person my picture or anything else without first checking with my parents.

5. I will not respond to any messages that are mean or in any way make me feel uncomfortable. It is not my fault if I get a message like that. If I do I will tell my parents right away so that they can contact the service provider.

6. I will talk with my parents so that we can set up rules for going online. We will decide upon the time of day that I can be online, the length of time I can be online, and appropriate areas for me to visit. I will not access other areas or break these rules without their permission.

7. I will not give out my Internet password to anyone (even my best friends) other than my parents.

8. I will check with my parents before downloading or installing software or doing anything that could possibly hurt our computer or jeopardize my family's privacy.

9. I will be a good online citizen and not do anything that hurts other people or is against the law.

10. I will help my parents understand how to have fun and learn things online and teach them things about the Internet, computers and other technology.

I agree to the above

Child sign here

I will help my child follow this agreement and will allow reasonable use of the Internet as long as these rules and other family rules are followed.

Parent(s) sign here

Items one through six are adapted from the brochure Child Safety on the Information Highway by Lawrence J. Magid. Copyright 1994 and 1998 by the National Center for Missing and Exploited Children. Printed copies are available free by calling 800 843-5678. (© 1997, 2005 Larry Magid).

Autorka jest adiunktem w Instytucie Lingwistyki Stosowanej na Uniwersytecie Warszawskim i nauczycielem konsultantem w Ośrodku Edukacji Informatycznej i Zastosowań Komputerów w Warszawie

Dr Augustyn Surdyk

Gry, które uczą

Już w czasach starożytnych wykorzystywano gry i inne techniki, dziś do celów dydaktycznych określane mianem ludycznych[1], w myśl zasady „bawiąc, uczyć". Szereg gier, choć służących z pozoru tylko rozrywce, posiada walory edukacyjne. Inne były i są specjalnie konstruowane do celów edukacyjnych, takich jak nauczanie przedmiotów ścisłych, a także przyrodniczych oraz humanistycznych, w tym języków obcych. Znakiem czasów już stało się, iż wyraz „gra" rodzi niemal automatyczne skojarzenie – „gra komputerowa"[2]. Nie byłoby w tym nic złego, gdyż nie da się zaprzeczyć, iż ta branża rozwija się najdynamiczniej, gdyby przy tym nie zapominano o grach planszowych i innych o nieporównywalnie dłuższej historii. Jeszcze gorzej, jeśli gra komputerowa budzi jedynie negatywne konotacje i uprzedzenia. Media raz po raz dostarczają sensacyjnych doniesień o wypadkach, których przyczyną były rzekomo gry komputerowe, jednak przy tym nie wspomina się prawie w ogóle o znacznie liczniejszych przypadkach zastosowań gier w edukacji. Niestety dla mediów częściej ważniejsza jest sensacja, nawet jeśli wyssana z palca, która odejdzie w zapomnienie tak szybko, jak się pojawi. Temat edukacyjnej gry bowiem „nie sprzeda się" tak dobrze, wszak nie jest tak atrakcyjny medialnie, jak kontrowersyjna gra lub tragiczne wydarzenie, którego przyczynę jej się przypisuje.

Skoro nie można zbytnio liczyć na pomoc mediów, nauczycielom pozostaje poszukiwać gier edukacyjnych na własną rękę, choćby poprzez lekturę czasopism naukowych[3] lub popularnonaukowych przeznaczonych dla nauczycieli[4]. Mogą też sięgać po gotowe do zastosowania zbiory gier i innych pokrewnych technik[5]. Jednak w książkach i artykułach naukowych najczęściej można znaleźć jedynie relacje z badań z ich wykorzystaniem (chyba że dotrze się do pełnych monografii, prac doktorskich itp.), rzadziej same przykładowe gry czy ich opisy, a już technicznie niemożliwe jest zawarcie w nich gier wykorzystujących nowe technologie[6]. Jeśli chodzi o gry edukacyjne z wykorzystaniem komputera i Internetu, sprawa jest prosta. Przy skromnym budżecie szkół publicznych prawdopodobnie mało która placówka może pozwolić sobie na zakup często drogich multimedialnych programów edukacyjnych i wyposażenie w nie pracowni komputerowych. Jeszcze skromniejszymi możliwościami dysponują sami nauczyciele, którzy mimo szczerych chęci nie byliby w stanie wyposażyć w oryginalne edukacyjne oprogramowanie multimedialne nawet jednej klasy. Z pomocą przychodzi sam Internet, w którym można znaleźć szereg portali edukacyjnych oferujących darmowe gry dydaktyczne *online* i *offline*, które mogą wspomagać nauczanie różnych przedmiotów (lista przykładowych adresów na końcu artykułu). Dla „odważniej-

1 Termin „technika ludyczna", wprowadzony przez prof. T. Siek-Piskozub (1995), obejmuje gry, symulacje i zabawy (w tym muzykę i piosenkę) posiadające walory edukacyjne i wykorzystywane w dydaktyce. Autorka w obszerny sposób opisuje w swych publikacjach historię zastosowań gier i innych pokrewnych technik w edukacji. O ludologii – młodej dyscyplinie naukowej zajmującej się szeroko pojętymi grami (w tym edukacyjnymi) można przeczytać w: Surdyk A. *Status naukowy ludologii. Przyczynek do dyskusji* [w:] Homo Ludens nr 1/2009, Polskie Towarzystwo Badania, Poznań, s. 223-243.

2 Przy obecnej mnogości różnego typu nośników i odtwarzaczy (poza komputerami konsole różnego rodzaju i inne urządzenia elektroniczne łącznie z telefonami komórkowymi) odpowiedniejszym określeniem obejmującym wszystkie typy tych gier byłoby „gra cyfrowa" (*digital game*).

3 Np. publikacje Polskiego Towarzystwa Neofilologicznego – czasopismo „Neofilolog" i publikacje pokonferencyjne z corocznych konferencji PTN (więcej informacji na stronie www.poltowneo.org.); publikacje Polskiego Towarzystwa Badania Gier – czasopismo „Homo Ludens" i wcześniejsze publikacje pokonferencyjne (więcej informacji oraz publikacje do pobrania w wersji elektronicznej na stronie www.PTBG.org.pl).

4 Np. czasopismo „Języki obce w szkole" (więcej informacji o czasopiśmie i poszczególne numery do pobrania w wersji elektronicznej na stronie www.jows.codn.edu.pl).

5 Np. Alex S., Vopel K.W. *Nie ucz mnie, ale pozwól i pomóż mi się uczyć!* cz. 1-4, Wydawnictwo „Jedność", Kielce 2004; Siek-Piskozub T. *Gry i zabawy w nauczaniu języków obcych*, WSiP, Warszawa, 1994; Vopel K.W., *Gry i zabawy interakcyjne,* cz. 1-6, Wydawnictwo „Jedność", Kielce 1999; Watcyn-Jones P. *Fun class activities Part 1-2. Games and activities for teachers*, Pearson Education Ltd., Harlow 2000.

6 Jest to możliwe jedynie wtedy, gdy do publikacji dołączona jest płyta z grą.

szych" nauczycieli, którzy są gotowi podjąć większe wyzwanie, dostępne są darmowe „silniki"[10] typu *freeware*, na bazie których, bez konieczności posiadania wiedzy i umiejętności informatyka, można stworzyć własną grę komputerową o dowolnej tematyce.

Techniki ludyczne stosowane w edukacji (zarówno tradycyjne, jak i nowoczesne – oparte na multimediach) mają na celu aktywizację osoby uczącej się, czynne włączenie ucznia w proces dydaktyczny. Jego osobiste i emocjonalne zaangażowanie powoduje zaktywizowanie obu półkul mózgowych, wzmocnienie i często tym samym rozwój afektywnych, kognitywnych i duchowych sfer działalności w zakresie (również auto-) dydaktyki danego przedmiotu. Ma to przyczynić się do podniesienia skuteczności samego procesu uczenia się/nauczania. W wielu opracowaniach dowiedziono również autonomizujących walorów tych technik. Odpowiednio dobrane lub opracowane przez samego nauczyciela, zastosowane umiejętnie i w odpowiednim momencie lekcji lub poza nią oraz dostosowane do potrzeb i warunków danej grupy (przede wszystkim poziomu wiedzy i wieku osób uczących się, liczebności grupy, charakteru lekcji oraz wymiaru dostępnych godzin dydaktycznych) – mogą przyczynić się do rozwoju wszelkich sprawności, a także strategii, procesów i mechanizmów związanych z samym uczeniem się, jak np. w nauce języków obcych rozwój zdolności do autokontroli i autokorekty[11]. Tak więc wbrew stereotypom, które nie oszczędzają również gier edukacyjnych, a wynikają jedynie z braku wiedzy na ten temat, zastosowanie gier na lekcji wcale nie musi być jedynie „wypełniaczem czasu".

Poza grami edukacyjnymi większość gier oczywiście służy głównie rozrywce. Nie wszystkie jednak są przeznaczone dla graczy w każdym wieku. Błędne jest stale pokutujące w świadomości społecznej przekonanie, że wszystkie gry przeznaczone są dla dzieci. W uniknięciu zakupu niewłaściwej gry komputerowej dla naszych dzieci lub wychowanków pomagają oznaczenia zamieszczone na opakowaniach (tzw. *rating*), mówiące o wieku odbiorcy, dla którego są przeznaczone, oraz treściach, jakie mogą zawierać. Najpopularniejszym systemem oznakowania gier w Europie jest system PEGI (*Pan European Game Information*). Dlatego warto zapoznać się z symbolami oznakowań na stronie www.pegi.info.pl.

Na zakończenie poniżej prezentuję za Hofman[12] kilka tabelarycznych zestawień przykładowych adresów stron, wyszukiwarek i portali internetowych, oferujących lub pozwalających wyszukać darmowe edukacyjne gry *online* i *offline* oraz inne materiały przeznaczone dla uczniów w różnym wieku i służące nie tylko do nauki języka angielskiego, lecz również przedmiotów przyrodniczych i ścisłych. Życzę miłego eksperymentowania z nowymi mediami!

Tabela 1.
Zagadnienia gramatyczne, edukacyjne gry leksykalne i inne[13]

OPIS	STRONA
Multilanguage dictionary	http://www.net-language.com
Real Audio listening exercises	http://englishlistening.com
Interactive exercises, grammar and listening – online course in English	http://www.bbc.co.uk/polish/learningenglish/
Grammar rules and explanations	http://www.grammarnow.com/
English language listening lab online	http://www.elllo.org/
Online news in English	http://news.bbc.co.uk/

[10] Np. program „Adventure Maker" dostępny do pobrania na stronie www.adventuremaker.com. Przykładem gry dla nastolatków i dorosłych opracowanej na tym silniku jest „Magritte" Marcina Drewsa (2008), osadzona we wciągającej fabule thrillera i prezentująca zabytkowe zakątki Wrocławia oraz zapoznająca gracza z twórczością tytułowego belgijskiego malarza-surrealisty. Gra wraz z pracą dyplomową, której jest częścią dostępne są na stronie internetowej autora pod adresem www.trh.art.pl/magritte/index.html

[11] Glinka M., Surdyk A. *Autokontrola w procesie kształtowania się strategii komunikacyjnych* [w:] Wilczyńska W. [red.] *Autonomizacja w dydaktyce języków obcych. Doskonalenie się w komunikacji ustnej*, Wydawnictwo Naukowe UAM, Poznań 2002.

[12] Autorka jest anglistką, dlatego większość adresów prowadzi do anglojęzycznych stron, jednak zrozumienie i skorzystanie z wielu z nich przy podstawowej znajomości języka angielskiego nie powinno sprawiać problemów.

[13] Hofman A. *Edukacyjne gry off-line i online oraz inne elementy IT w przygotowaniu studentów UG do nauczania L2* [w:] Surdyk A., Szeja J.Z. [red.] *Kulturotwórcza funkcja gier. Cywilizacja zabawy czy zabawy cywilizacji*, Homo Communicativus nr 3(5) /2008, Zakład Teorii i Filozofii Komunikacji IF UAM, Poznań, s. 52.

OPIS	STRONA
Polish site for learners of English	http://republika.pl/b_slawek/main.htm
Polish site for learners of English	http://www.angielski.host.sk/
Polish site for learners of English	http://filo.pl/angielski/
Polish site with grammar activities	http://www3.sympatico.ca/jacek_s/magdak/grammar.htm
Grammar games and activities	http://deil.lang.uiuc.edu/web.pages/grammarsafari.html
Internet Browser	www.clusty.com
Online library	www.books.google.com

Tabela 2.
Edukacyjne gry oraz materiały online i offline dla dzieci od 18 miesięcy[11]

OPIS	STRONA
Printable materials for young learners	http://www.abcteach.com
Educational online games for young learners	http://www.funbrain.com
Easy educational online games for young learners, esp. boys	http://www.hitentertainment.com/bobthebuilde/
Online games and films for young learners, esp. girls	http://myscene.everythinggirl.com/home.aspx
Online games for very young learners	http://pbskids.org/kids
Online games, news and films for young learners, especially about health	http://www.kidshealth.org
Online interactive films about how your body works	http://www.kidshealth.org/kid/closet/how_the_body_works_interim.html
Games and materials for youngest learners	http://www.bbc.co.uk/schools/preschool

Tabela 3.
Edukacyjne gry i eksperymenty do nauki fizyki, chemii, matematyki w L2[12]

OPIS	STRONA
NASA education	http://education.nasa.gov/home/index.html
An interesting NASA project	http://futureflight.arc.nasa.gov/
NASA films for kids	http://ksnn.larc.nasa.gov/k2newsbreaks.cfm
NASA games for kids	http://www.nasa.gov/audience/forkids/games/index.html
Science Clips	http://www.bbc.co.uk/schools/scienceclips/
BBC science & nature	http://www.bbc.co.uk/sn/
DIGGER for 3-14 year-olds	http://www.bbc.co.uk/schools/digger
SPHEROX games – teens and adults	http://www.bbc.co.uk/schools/gcsebitesize/games/
Mathematics for kids 4-11	http://www.bbc.co.uk/schools/numbertime/
LITTLE ANIMAL CENTRE – kids 4-9	http://www.bbc.co.uk/schools/laac/numbers/chi.shtml
STARSHIP – for older kids	http://www.bbc.co.uk/schools/starship/maths/index.shtml
PRINTABLES FOR KIDS	http://www.dltk-teach.com/numbers/index.html
KIDZONE	http://www.kidzone.ws/math/index.htm
PRINTABLES MATHS	http://tlsbooks.com/mathworksheets.htm

[11] Hofman A., ibidem, s. 52-53.
[12] Ibidem, s. 53.

Bibliografia

1. Alex S., Vopel K.W. *Nie ucz mnie, ale pozwól i pomóż mi się uczyć!* cz. 1-4, Wydawnictwo „Jedność", Kielce 2004.
2. Drews M. *Gry komputerowe a analfabetyzm funkcjonalny i informacyjny* [w:] Surdyk A., Szeja J.Z. [red.] *Kulturotwórcza funkcja gier. Gra w kontekście edukacyjnym, społecznym i medialnym,* Homo Communicativus nr 2(4)/2008, Zakład Teorii i Filozofii Komunikacji IF UAM, Poznań.
3. Glinka M., Surdyk A. *Autokontrola w procesie kształtowania się strategii komunikacyjnych* [w:] Wilczyńska W. [red.] *Autonomizacja w dydaktyce języków obcych. Doskonalenie się w komunikacji ustnej*, Wydawnictwo Naukowe UAM, Poznań 2002.
4. Hofman A. *Edukacyjne gry off-line i online oraz inne elementy IT w przygotowaniu studentów UG do nauczania L2* [w:] Surdyk A., Szeja J.Z. [red.] *Kulturotwórcza funkcja gier. Cywilizacja zabawy czy zabawy cywilizacji,* Homo Communicativus nr 3(5) /2008, Zakład Teorii i Filozofii Komunikacji IF UAM, Poznań.
5. Siek-Piskozub T. *Gry i zabawy w nauczaniu języków obcych*, WSiP, Warszawa 1994.
6. Siek-Piskozub T. *Gry, zabawy i symulacje w procesie glottodydaktycznym*, Wydawnictwo Naukowe UAM, Poznań 1995.
7. Surdyk A. *Status naukowy ludologii. Przyczynek do dyskusji* [w:] Homo Ludens nr 1/2009, Polskie Towarzystwo Badania Gier, Poznań.
8. Vopel K.W. *Gry i zabawy interakcyjne,* cz. 1-6, Wydawnictwo „Jedność", Kielce 1999.
9. Watcyn-Jones P. *Fun class activities Part 1-2. Games and activities for teachers*, Pearson Education Ltd., Harlow 2000.

Autor jest adiunktem w Instytucie Lingwistyki Stosowanej UAM w Poznaniu, członkiem założycielem i członkiem Zarządu Głównego – Skarbnikiem Polskiego Towarzystwa Badania Gier

Agnieszka Borowiecka

Uczymy dzieci, jak być bezpiecznym w Internecie

Coraz częściej słyszymy określenia „społeczeństwo informacyjne", „społeczeństwo informatyczne", „społeczeństwo doby Internetu". Powszechny dostęp do Internetu dotyczy nie tylko osób dorosłych, ale także dzieci i młodzieży. Jednak Internet i jego zasoby mają nie tylko same dobre strony, coraz więcej mówi się i pisze o cyberprzemocy, cyberprzestępcach, kradzieży tożsamości itp. Z tego względu zadaniem nauczyciela jest obecnie nie tylko zachęcanie dzieci i młodzieży do korzystania z sieci, ale także nauczenie ich, jak to robić w bezpieczny sposób.

Zagrożenia związane z używaniem komputerów czy korzystaniem z sieci Internet są tematem licznych opracowań, zarówno w wersji papierowej, jak i elektronicznej.

W roku 2009 odbyło się wiele konferencji i zebrań metodycznych dotyczących bezpieczeństwa i ochrony prywatności dzieci i młodzieży. Czy nauczyciele mogą korzystać z istniejących materiałów? Czy powinni samodzielnie przygotowywać opracowania i ćwiczenia dla uczniów? A może wystarczy, by uczniowie poczytali na ten temat w podręcznikach do informatyki? Bardzo trudne i jednocześnie niezwykle istotne wydaje się przekazanie tej wiedzy uczniom szkół podstawowych, szczególnie tym najmłodszym. Od 2009 roku podstawa programowa wprowadza przedmiot o nazwie „Zajęcia komputerowe". Czy w ramach tego przedmiotu powinniśmy mówić o bezpieczeństwie w sieci? I jak to robić?

Odpowiedzią na te pytania mogą się okazać liczne bezpłatne materiały znajdujące się w Internecie lub przekazywane na płytach DVD w ramach konferencji dla nauczycieli informatyki i innych przedmiotów. Spróbuję teraz krótko przedstawić część z nich.

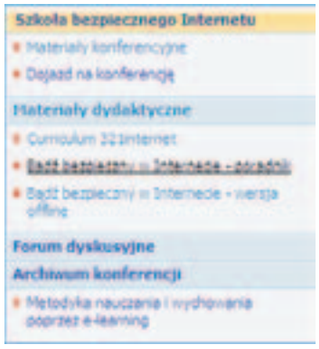
Portal „Partnerstwo dla Przyszłości"

Jedną z inicjatyw portalu „Partnerstwo dla Przyszłości" (http://www.pdp.edu.pl) jest prowadzona pod patronatem Ministerstwa Edukacji Narodowej kampania promująca bezpieczeństwo i prywatność w Internecie wśród dzieci i młodzieży przy wykorzystaniu materiału e-learningowego. Dostęp do tych zasobów umożliwia link znajdujący się na pierwszej stronie portalu: „Bezpieczeństwo i ochrona prywatności dzieci i młodzieży w Internecie".

Rys. 1. Portal „Partnerstwo dla Przyszłości" – strona główna

Po przejściu do części dotyczącej bezpieczeństwa w Internecie mamy dostęp do informacji o organizowanych konferencjach i konkursach związanych z tą tematyką, forum dyskusyjnego oraz poradnika „Bądź bezpieczny w Internecie" w wersji *online* i *offline*. Można stąd również pobrać materiały związane z projektem „3...2...1.. Internet".

Materiały zawarte w poradniku powstały w oparciu o witrynę internetową „Bezpieczeństwo informacji dla szkół" założoną w roku 2005 w związku z obchodami fińskiego Dnia Bezpieczeństwa Informacji (http://www.tietoturvakoulu.fi).



Rys. 2. Menu działu „Bezpieczeństwo w Internecie"

(Poradnik składa się z czterech części: materiałów dla uczniów (historyjki dla uczniów w wieku 7-12 lat, historyjki dla uczniów w wieku 13-16 lat), quizów, wskazówek dla nauczyciela oraz informacji dla rodziców i opiekunów.

Rys. 3. Poradnik „Bądź bezpieczny w Internecie"

Materiały dla uczniów zostały przygotowane w postaci czterech interaktywnych historyjek obrazkowych przedstawiających sytuacje, w jakich mogą się oni znaleźć, zwracających uwagę na zagadnienia związane z bezpieczeństwem i sprawdzających wiedzę uczniów związaną z prezentowaną tematyką:

1. Uczniowie w wieku 7-12 lat

Bezkresny las – czym jest Internet i co można w nim robić, konieczność obrony przed złymi aspektami sieci;

Nowi przyjaciele Ani – netykieta, publikowanie w sieci i prawa autorskie;

2. Uczniowie w wieku 13-16 lat

Rzymska grupa – ochrona praw autorskich, ochrona komputera i znaczenie haseł;

Kłopoty i incydenty – poprawność informacji publikowanych w Internecie, odpowiedzialność za publikowane zdjęcia i tekst, poznawanie ludzi w sieci, sieci *peer-to-peer*.

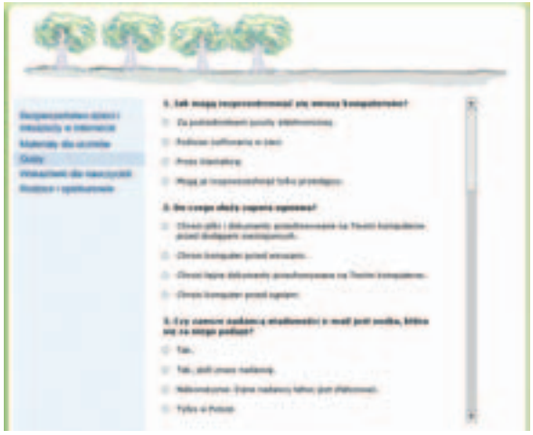
Do obejrzenia historii niezbędne jest zainstalowanie oprogramowania Flash.

Rys. 4. Przykładowy slajd opowieści „Bezkresny las"

Uczniowie mogą zapoznawać się z materiałami samodzielnie, w małych grupach lub wspólnie, pod okiem nauczyciela. Podczas oglądania prezentacji pojawiają się formularze, w których należy wskazać prawidłowe odpowiedzi. Każda odpowiedź jest komentowana.

Rys. 5. Przykładowy slajd opowieści „Rzymska grupa"

Quizy, podobnie jak historyjki obrazkowe, dostępne są w dwóch kategoriach wiekowych: pytania dla uczniów w wieku 7-10 lat lub w wieku 11-14 lat. Po wypełnieniu i zatwierdzeniu quizu do każdego z pytań pojawia się komentarz uzasadniający poprawność udzielonej odpowiedzi. Quizy również wymagają zainstalowania oprogramowania Flash.



Rys. 6. Fragment quizu dla uczniów w wieku 7-10 lat

Kolejną grupę materiałów stanowią wskazówki dla nauczycieli. Pomagają one przypomnieć sobie podstawowe zagadnienia związane z bezpieczeństwem w sieci, prawem autorskim, terminologią związaną z usługami sieciowymi. Dostępne są także krótkie wskazówki dotyczące przeprowadzenia lekcji w oparciu o materiały udostępniane przez portal.

Rys. 7. Wskazówki dla nauczycieli

Autorzy portalu nie zapomnieli także o rodzicach i opiekunach i zamieścili szereg informacji i wskazówek dotyczących bezpieczeństwa w Internecie. W tej części również dostępne są animowane prezentacje (Flash) – przewodnik opracowany z wykorzystaniem materiałów dotyczących bezpiecznego korzystania z Internetu organizacji Childnet International.

Rys. 8. Informacje dla rodziców i opiekunów

Kampania społeczna „Dziecko w Sieci"

Istniejąca od 1991 roku Fundacja Dzieci Niczyje jest organizacją pozarządową, której celem jest ochrona dzieci oraz pomoc dzieciom krzywdzonym, ich rodzinom i opiekunom. Od 2003 roku fundacja zajmuje się problematyką bezpieczeństwa dzieci i młodzieży w Internecie, realizując w ramach programu Akademia Bezpiecznego Internetu następujące przedsięwzięcia:

- ogólnopolską kampanię „Dziecko w Sieci",
- akcję „Stop cyberprzemocy",
- projekt „Sieciaki.pl",
- projekt „Helpline.org.pl".

W ramach kampanii społecznej „Dziecko w Sieci" realizowany jest projekt e-learning (http://elearning.dzieckowsieci.pl), udostępniający na specjalnej platformie kursy dla uczniów szkół podstawowych, gimnazjalnych i ponadgimnazjalnych oraz dla rodziców i nauczycieli.

Rys. 9. Platforma e-learningowa „Dziecko w Sieci"

Zanim zaczniemy korzystać z kursów na platformie, należy zarejestrować się na stronie projektu. Nauczyciele, którzy chcą ze swoimi uczniami korzystać z kursów na platformie, powinni wybrać rejestrację profesjonalisty, podać wymagane dane i nacisnąć „Rejestruj". Po chwili otrzymujemy e-mail zawierający link konieczny do zakończenia rejestracji oraz kod aktywacyjny, który należy przekazać uczniom uczestniczącym w kursie.

Rys. 10. Rejestracja nauczyciela w portalu

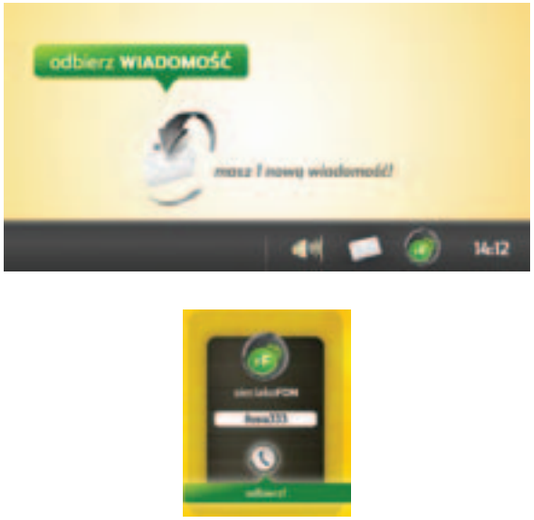
Po zalogowaniu nauczyciel może wybrać z menu po lewej stronie interesującą go czynność, np. zapoznanie się z dostępnymi na platformie szkoleniami, obejrzenie listy swoich uczniów, przesłanie do nich wiadomości lub zmiana ustawień konta.

Rys. 11. Informacje o uczniach uczestniczących w kursie

Kolejnym krokiem jest rejestracja uczniów, podczas której podają kod aktywacyjny otrzymany od nauczyciela lub wpisują kod „ZASADY”, gdy będą samodzielnie zapoznawać się z materiałami publikowanymi w portalu. Po zarejestrowaniu i zalogowaniu uczniowie mają dostęp do pierwszego modułu kursu. Jest to prezentacja w technologii Flash, wymagająca podłączenia do komputera słuchawek bądź głośników.

Kolejne moduły zawierają animowane interaktywne prezentacje przedstawiające różne zagadnienia dotyczące zasad bezpiecznego korzystania z Internetu. Uczestnicy kursu rozwiązują krótkie testy, zapoznają się z przykładowymi konsekwencjami konkretnych zachowań. Przez cały czas dostępny jest słownik zawierający listę omawianych terminów.

Rys. 12. Kurs dla ucznia IV klasy



Rys. 13. Kurs dla ucznia gimnazjum

Rys. 14. Rejestracja rodzica w portalu

Obecnie dostępne są dwa kursy dla uczniów szkół podstawowych (z klas I-III oraz IV-VI) i jeden dla uczniów gimnazjum. Udostępniony kurs dla uczniów klas I-III składa się z następujących modułów: „Wstęp", „Internet", „Udostępnianie danych osobowych", „Znajomości w Sieci", „Niebezpieczne treści", „Zasady kulturalnego korzystania z usług dostępnych w Internecie", „Uzależnienie od Internetu", „Wirusy". Kurs kończy się testem, po którym można otrzymać dyplom ukończenia szkolenia.

Kurs dla uczniów klas IV-VI składa się z modułów: „Wstęp. Historia Internetu", „Podawanie danych osobowych", „Znajomi w Sieci", „Niebezpieczne treści", „Przemoc w Sieci", „Uzależnienie", „Zakupy".

Uczniowie gimnazjum mogą zapoznać się z interaktywnym kursem, podczas którego zostają administratorem portalu społecznościowego Znajomi-Nieznajomi.pl i ćwiczą bezpieczne zachowania związane z zarządzaniem portalem. Kurs również kończy się testem.

Platforma dostępna jest także dla zainteresowanych rodziców. Po zarejestrowaniu się mogą oni ukończyć szkolenia, w których uczestniczą ich dzieci (rys. 14).

Projekt „3... 2... 1... Internet"

Projekt „3... 2... 1... Internet" jest wspólnym przedsięwzięciem Fundacji Dzieci Niczyje oraz firmy Microsoft. W ramach projektu powstały materiały dydaktyczne dla uczniów klas IV-VI, dotyczące bezpieczeństwa internetowego.

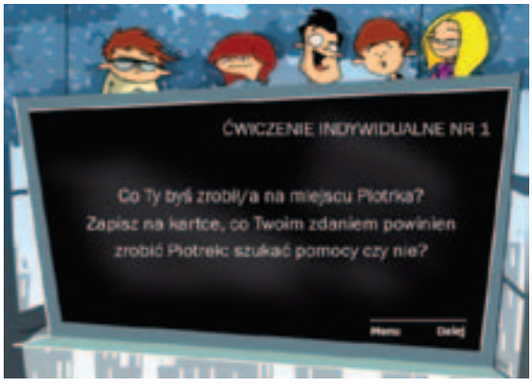
Rysunek 15. Aplikacja „3... 2... 1... Internet"

Ambasadorem projektu w Polsce i narratorem prezentacji multimedialnej stanowiącej fragment opracowanych materiałów jest Krzysztof Hołowczyc. Do poprowadzenia zajęć z wykorzystaniem pakietu wystarczy podstawowa znajomość Internetu i materiały pobrane z sieci lub zapisane na płycie DVD.

Zasadniczym elementem projektu jest 5 interaktywnych kreskówek poświęconych różnym formom internetowych zagrożeń:

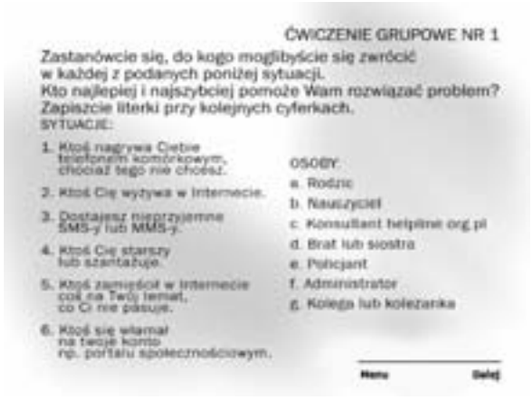
- Dobry żart
- Znajomi-nieznajomi
- Małe zdjęcie DUŻY PROBLEM
- Moja praca domowa
- Komputeromania

Każda z pięciu historii ma dwa zakończenia. Uczniowie wybierają bardziej prawdopodobne (właściwe) ich zdaniem rozwiązanie i oglądają film prezentujący skutki dokonanego wyboru.



Rys. 16. Kadry z kreskówki

Do materiałów dołączone są scenariusze zajęć dla nauczycieli. Zajęcia w ramach projektu przewidziane są na dwie godziny lekcyjne. Przewidziana jest w nich praca grupowa i indywidualna uczniów przeplatana projekcją.


ĆWICZENIE GRUPOWE NR 1

Zastanówcie się, do kogo moglibyście się zwrócić w każdej z podanych poniżej sytuacji. Kto najlepiej i najszybciej pomoże Wam rozwiązać problem? Zapiszcie literki przy kolejnych cyferkach.

SYTUACJE:

1. Ktoś nagrywa Cię telefonem komórkowym, chociaż tego nie chcesz.
2. Ktoś Cię wyzywa w Internecie.
3. Dostajesz nieprzyjemne SMS-y lub MMS-y.
4. Ktoś Cię straszy lub szantażuje.
5. Ktoś zamieścił w Internecie coś na Twój temat, co Ci nie pasuje.
6. Ktoś się włamał na twoje konto np. portalu społecznościowym.

OSOBY:

a. Rodzic
b. Nauczyciel
c. Konsultant helpline org.pl
d. Brat lub siostra
e. Policjant
f. Administrator
g. Koleżanka lub kolezanka

Menu Dalej

Rys. 17. Przykładowe ćwiczenie grupowe

W ramach projektu przygotowano także komiks, który można wykorzystać zamiast kreskówek lub jako element uzupełniający zajęcia.

Rys. 18. Fragment komiksu

Materiały, scenariusz oraz prezentację multimedialną (kreskówki z komentarzem) można pobrać ze stron:

- www.dzieckowsieci.pl
- www.pdp.edu.pl
- www.321internet.pl

Rys. 19. Strona projektu

Projekt „Sieciaki.pl"

Fundacja Dzieci Niczyje w ramach programu „Dziecko w Sieci" wdrożyła projekt „Sieciaki.pl". Jego premiera odbyła się 8 lutego 2005 roku w Dniu Bezpiecznego Internetu. Na stronach serwisu „Sieciaki.pl" dzieci i młodzież może zapoznać się z informacjami dotyczącymi bezpiecznej pracy w Internecie. Informacje te są przekazywane przez czterech bohaterów: AjPi, Spociaka, Netkę i Kompela.

Rys. 20. Strona projektu „Sieciaki"

Postaci Sieciaków zostały wykorzystane w różnych materiałach dostępnych w sieci, między innymi na stronie projektu e-learning (http://elearning.dzieckowsieci.pl) oraz w pakiecie edukacyjnym dla klas I-IV szkoły podstawowej, przygotowanym w ramach programu „Edukacja z Internetem TP" Fundacji Grupy Telekomunikacji Polskiej. W ramach tego programu szkoły mogą korzystać z płyty DVD zawierającej kreskówkę na temat bezpieczeństwa dzieci w Internecie, scenariuszy lekcji oraz usług stałego dostępu do Internetu TP na preferencyjnych warunkach.

Rys. 21. Pakiet „Edukacja z Internetem TP"

Płyta „Edukacja z Internetem TP – materiały dla nauczyciela" zawiera film video, składający się z następujących części:

- „Nie podawaj swoich danych" (8:22)
- „Zabezpiecz swój komputer" (7:54)
- „Mów, jeśli coś jest nie tak" (10:26)

Możliwe jest także odtworzenie całego filmu (22:17) oraz zapoznanie się z prezentacją helpline.org.pl (0:39).

Istotnym elementem pakietu są scenariusze zajęć (1 lub 2 godziny lekcyjne). Do przeprowadzenia zajęć niezbędna jest płyta DVD z filmem i sprzęt do jej odtworzenia oraz materiały drukowane, pobrane ze strony www.dzieckowsieci.pl (sekcja dla profesjonalistów). Podczas zajęć uczniowie przeprowadzają burzę mózgów na temat używania komputerów i Internetu i zapoznają się z filmem. Można także przeprowadzić szereg konkursów i dodatkowych ćwiczeń utrwalających przekazywane informacje.

Rys. 22. Klatka filmu „Nie podawaj swoich danych"

Podsumowanie

Korzystanie z Internetu stało się czynnością naturalną i powszechną, szczególnie dla dzieci i młodzieży. Naszym zadaniem jest zadbanie o to, by robili to w sposób rozsądny i bezpieczny dla siebie. Możemy w tym celu wykorzystać wiele gotowych materiałów. Pamiętajmy jednak, że przede wszystkim należy uczyć na własnym przykładzie – nauczyciel powinien być wzorem do naśladowania dla swoich uczniów.

Autorka jest nauczycielem konsultantem w Ośrodku Edukacji Informatycznej i Zastosowań Komputerów w Warszawie

◄

Gry, które w innym przypadku zostałyby zakwalifikowane do grupy 3, lecz zawierają treści (dźwięki lub sceny) potencjalnie przerażające najmłodszych odbiorców, mogą być uznane za odpowiednie dla tej grupy wiekowej. Dopuszczalne są sceny obejmujące częściową nagość, ale nigdy w kontekście seksualnym.

Przykładowe gry z tej grupy: LEGO Indiana Jones, Shrek Trzeci, The Sims 2.

Robert Makowski

Oferta edukacyjna programu „Dziecko w Sieci”

Nowoczesne technologie to zazwyczaj domena młodych ludzi. To nastolatki, ale i dzieci, często występują w roli domowych ekspertów od Internetu, komputera lub rozbudowanych funkcji telefonu komórkowego. Swoją biegłością w posługiwaniu się nowoczesnymi technologiami zaimponować mogą zarówno rodzicom, jak i nauczycielom. Jak rozmawiać o zagrożeniach niesionych przez Internet z pokoleniem, które już wychowało się w sieci?

1. Zagrożenia dzieci w Internecie

Zacznijmy od faktów. Praktycznie wszystkie dzieci w wieku szkolnym mają dostęp do Internetu. Dla najmłodszego pokolenia korzystanie z sieci jest czynnością zupełnie naturalną, a opinia na internetowym forum jest częstokroć bardziej istotna niż poważanie u kolegów z podwórka. Spędzając dużo czasu w sieci, dzieci i młodzież padają ofiarami nadużyć w Internecie lub mają kontakt z materiałami nieadekwatnymi do ich wieku. Dla jasności warto skategoryzować internetowe zagrożenia, z jakimi dzieci najczęściej mają kontakt.

Kontakt z niebezpiecznymi treściami

Materiały nielegalne to: pornografia dziecięca, pornografia z udziałem zwierząt, prezentująca przemoc, materiały promujące rasizm i ksenofobię. Prawo nie ogranicza publikacji treści prezentujących przemoc, postawy i zachowania zagrażające życiu i zdrowiu (hazard, używki, anoreksja, zaangażowanie w działalność sekt, samouszkodzenia, samobójstwa, itp.), nikt jednak nie ma chyba wątpliwości, że przypadkowy czy świadomy kontakt z nimi odbija się na dziecięcej psychice i zaburza na przykład sposób widzenia relacji międzyludzkich lub postrzeganie własnej seksualności. Niebezpieczne treści są w Internecie bardzo rozpowszechnione. Materiały pornograficzne (traktowane jako legalne, prawo ogranicza jedynie dostęp do nich nieletnim), to najczęstsza kategoria treści publikowanych w sieci. Młodzi internauci trafiają na nie zazwyczaj zupełnie przypadkowo.

Niebezpieczne treści – skala zagrożenia (badania firmy Gemius i Fundacji Dzieci Niczyje grupa 2559 dzieci w wieku 12-17 lat, 2006)

- 71% dzieci trafiło w Internecie na materiały pornograficzne. 63% przypadkowo.
- 51% dzieci trafiło na materiały z brutalnymi scenami przemocy. 61% przypadkowo.
- 28% dzieci trafiło na materiały propagujące przemoc i nietolerancję. 74% przypadkowo.
- Co czwarte dziecko deklaruje, że jego rodzice nie interesują się tym, w jaki sposób korzysta z Internetu.
- Jedynie 10% dzieci stwierdza, że podczas korzystania z sieci jest pod systematyczną opieką rodziców.

Niebezpieczne kontakty

Komunikatory, czaty i portale społecznościowe to jedne z najczęściej wykorzystywanych przez najmłodszych użytkowników usług internetowych. Dzieci zawierają w ten sposób nowe znajomości, a to oznacza ryzyko kontaktu z niebezpiecznymi osobami. Ze względu na niewiedzę i łatwowierność młodzi internauci niejednokrotnie stają się ofiarami przestępstw z użyciem sieci, m.in. oszustw, wyłudzeń lub włamań komputerowych. Często podają obcym osobom poznanym w sieci prywatne informacje (dane osobowe) lub umawiają się z osobami poznanymi w Internecie na spotkania w realnym świecie. O znajomościach z Internetu dzieci zazwyczaj nie mówią rodzicom, na spotkanie idą samodzielnie lub z rówieśnikiem, podczas gdy powinna im towarzyszyć zaufana osoba dorosła, zwłaszcza małym dzieciom. To szczególne zagrożenie, w związku z coraz powszechniejszym zjawiskiem uwodzenia dzieci w Internecie.

Niebezpieczne kontakty – skala zagrożenia (badania firmy Gemius i Fundacji Dzieci Niczyje, grupa 1779 dzieci w wieku 12-17 lat i 687 rodziców, 2006)

- Ponad 90% dzieci korzysta z serwisów komunikacyjnych.
- 68%. otrzymało propozycję spotkania od osób poznanych w sieci.
- 45% bierze w nich udział.
- Jedynie co czwarte dziecko informuje rodziców o spotkaniach z osobami poznanymi w sieci.
- Połowa dzieci idzie na takie spotkanie samodzielnie.
- 28% rodziców nie dostrzega żadnych zagrożeń dla dzieci związanych z korzystaniem z Internetu.

Cyberprzemoc (cyberbullying)

Cyberprzemoc to z kolei nowe oblicze przemocy rówieśniczej. W odróżnieniu od tradycyjnych form nękania, zastraszania lub szantażowania przemoc w sieci wykorzystuje nowoczesne narzędzia komunikacyjne, a co za tym idzie – nabiera nieporównanie szerszej skali. Ośmieszające lub znieważające filmy, kompromitujące zdjęcia raz udostępnione w Internecie są powielane i dystrybuowane za pomocą poczty elektronicznej, blogów, stron internetowych lub forów społecznościowych. Do tej kategorii zagrożeń należy również włączyć podszywanie się pod kogoś, na przykład w celu publikowania wulgarnych komentarzy (by zniszczyć cudzą reputację).

Skala zagrożenia (badania firmy Gemius i Fundacji Dzieci Niczyje, grupa 891 dzieci w wieku 12-17 lat, 2007)

- 57% stała się przynajmniej raz obiektem zdjęć lub filmów wykonanych wbrew ich woli.
- 52% dzieci miało do czynienia z przemocą werbalną w Internecie lub przez telefon komórkowy.
- 47% dzieci doświadczyło wulgarnego wyzywania.
- 29% badanych deklaruje, że ktoś w sieci podawał się za nie wbrew ich woli.
- 21% dzieci doznało poniżania, ośmieszania lub upokarzania.
- 16% doświadczyło próby zastraszenia i szantażowania.
- 14% zgłasza przypadki rozpowszechniania za pośrednictwem Internetu lub telefonii komórkowej kompromitujących je materiałów.

Uzależnienie od Internetu

Problem uzależnienia od sieci jest szczególnie istotny w przypadku dzieci, u których proces ten jest znacznie szybszy niż u dorosłych. Różnorodność usług oferowanych przez Internet i ich atrakcyjność sprawia, że młodzi ludzie spędzają w sieci coraz więcej czasu. Brak samokontroli, a przede wszystkim brak kontroli rodzicielskiej może powodować, że dziecko rezygnuje z innych form aktywności na rzecz czasu spędzanego przed ekranem komputera. To z kolei może się odbić na jego rozwoju psychospołecznym (ograniczenie kontaktów z rówieśnikami, rezygnacja z innych form aktywności pozaszkolnej), a nawet (m.in. ze względu na niewłaściwą pozycję ciała) na jego zdrowiu.

2. „Dziecko w Sieci"

W jaki sposób rozmawiać z dziećmi i młodzieżą o zagrożeniach w Internecie, nie demonizując ich ani nie uciekając w moralizatorstwo? Jak wytłumaczyć dziecku, że nieprzemyślana publikacja jego danych osobowych lub zdjęć w sieci może oznaczać poważne problemy w świecie realnym?

Program „Dziecko w Sieci"

Fundacja Dzieci Niczyje zajmuje się bezpieczeństwem dzieci i młodzieży w Internecie od 2004 roku. Wtedy ruszył program „Dziecko w Sieci" obejmujący kampanię społeczną, której zadaniem było zwrócenie uwagi na zagrożenia najmłodszych internatów oraz kampanię edukacyjną, poświęconą ich bezpieczeństwu. To wówczas powstał spot telewizyjny „Nigdy nie wiadomo, kto jest po drugiej stronie". 30-sekundowy film, którego bohaterem jest 12-letnia Ania i podszywający się pod jej rówieśnika Wojtek, miał za zadanie zwrócić uwagę społeczeństwa na problem, jakim są kontakty dzieci z nieznajomymi osobami w sieci.

W ramach programu działa również Helpline.org.pl. Zadaniem tej komórki FDN jest niesienie pomocy psychologicznej (a jeśli zajdzie taka potrzeba – również prawnej) w sytuacji niebezpiecznych zdarzeń w Internecie. Oferta Helpline.org.pl skierowana jest zarówno do dzieci i młodzieży, jak i do profesjonalistów (nauczycieli, psychologów, pedagogów szkolnych) oraz rodziców.

Najskuteczniejszą metodą ograniczenia skali zagrożeń wobec dzieci w Internecie jest jednak edukacja najmłodszych internautów – tak, by sami potrafili uniknąć kłopotliwych sytuacji. W ramach programu „Dziecko w Sieci" powstają materiały dla nauczycieli, umożliwiające prowadzenie atrakcyjnych zajęć, które bez zbędnego dydaktyzmu za-

poznają najmłodszych internautów z zasadami bezpieczeństwa w Internecie. Fundacja oddaje do dyspozycji nauczycieli kompletne materiały, obejmujące zarówno scenariusze, jak i wykorzystywane podczas zajęć np. materiały multimedialne lub zeszyty ćwiczeń. Zajęcia przygotowano merytorycznie dla wszystkich klas szkół podstawowych i gimnazjum. Do ich przeprowadzenia nie jest wymagana specjalistyczna wiedza – wystarczy typowo użytkowa umiejętność poruszania się po Internecie. Co ważne dla szkół niedysponujących pracownią komputerową – część zajęć można przeprowadzić, posługując się wyłącznie odtwarzaczem DVD i telewizorem.

Serwis internetowy „Dziecko w Sieci"

Wszystkie scenariusze zajęć i materiały niezbędne do ich prowadzenia można znaleźć w serwisie dzieckowsieci.pl. Powstał on również po to, by dostarczać najbardziej aktualnych informacji o działalności edukacyjnej, wciąż prowadzonych kampaniach społecznych i nowościach związanych z programem „Dziecko w Sieci".

Materiały przygotowane przez Fundację Dzieci Niczyje w ramach programu Dziecko w Sieci udostępniane są nieodpłatnie, jedynym ograniczeniem przy ich powielaniu jest konieczność powołania się na źródło. Po przeprowadzeniu zajęć nauczyciel wypełnia sprawozdanie i otrzymuje zaświadczenie, ważne na przykład w dokumentowaniu działalności zawodowej. Głębiej zainteresowani problemem znajdą w serwisie wyniki badań i analiz dotyczących bezpieczeństwa dzieci w Internecie.

Zajęcia szkolne

Oferta edukacyjna Fundacji Dzieci Niczyje została przygotowana z myślą o możliwościach i zainteresowaniach każdej z grup wiekowych. W ramach projektu przyjęliśmy podział:
- klasy I-III szkół podstawowych
- klasy IV-VI szkół podstawowych
- klasy gimnazjalne

Oferta edukacyjna dla klas I-III szkół podstawowych. Zajęcia „Sieciaki"

Umiejętności techniczno-informatyczne nawet najmłodszych dzieci niejednokrotnie zaskakują ich rodziców. Nie zawsze jednak idą z nimi w parze umiejętności społeczne.

W trakcie zajęć poruszane są m.in. takie tematy, jak:
- komunikowanie się z innymi osobami,
- zdobywanie informacji,
- poznawanie nowych ludzi,
- pobieranie plików.

Zajęcia można zrealizować w wersji pełnej (2×45 minut) lub w wersji skróconej (45 minut). W tym czasie dzieci dowiadują się, jak bezpiecznie i efektywnie korzystać z sieci, poznają internetowe zagrożenia, zasady bezpiecznego używania Internetu oraz metody reagowania na internetowe niebezpieczeństwa. Dzięki burzy mózgów, kreskówkom, konkursom i ćwiczeniom dzieci przyswajają wiedzę pozbawioną nadmiernego dydaktyzmu.

Zagrożenia internetowe prezentowane są przez pryzmat przygód drużyny Sieciaków zwalczających złe Sieciuchy (będące uosobieniem zagrożeń, na które dziecko może trafić w sieci). Atrakcyjne dla dzieci postaci Sieciaków doskonale sprawdzają się jako przewodnicy prezentujący podstawowe zasady bezpiecznego korzystania z Internetu.

Kurs e-learning „Poznaj bezpieczny Internet"

Dzieci kolejny raz mogą spotkać się z postaciami Sieciaków w trakcie zajęć e-learningowych przeznaczonych dla najmłodszych internautów. Po zalogowaniu się na platformę edukacyjną kursy.dzieckowsieci.pl nauczyciel lub inna osoba prowadząca zajęcia otrzymuje w mailu link do kodu aktywacyjnego, który powinien zostać przekazany uczniom. Dzięki niemu uczniowie biorący udział w zajęciach zostają przypisani do konkretnego nauczyciela, który może wysyłać do nich wiadomości i śledzić ich postępy w realizacji kursu. Realizacja ośmiu modułów kursu zajmuje trzy jednostki lekcyjne i obejmuje m.in. takie zagadnienia, jak udostępnianie danych osobowych w sieci, internetowe znajomości, niebezpieczne treści, wirusy oraz netykietę.

Oferta edukacyjna dla klas IV-VI szkół podstawowych. Zajęcia „3… 2… 1… Internet!"

Dla starszych uczniów, z klas IV-VI szkół podstawowych, przeznaczony jest kurs „3… 2… 1… Internet!" Poświęcony jest on przede wszystkim prezentacji efektywnego wykorzystywania Internetu jako alternatywy wobec ryzykownych zachowań: cyberprzemocy, spotkań z osobami znanymi wyłącznie z Internetu, upubliczniania swoich danych, piractwa w sieci oraz uzależnień. Niewątpliwą atrakcją zajęć jest osoba prowadzącego – Krzysztofa Hołowczyca, który jako narrator wprowadza uczniów w poszczególne zagadnienia, zapowiada i podsumowuje kreskówki wykorzystywane w trakcie lekcji. By zwiększyć aktywność i zaangażowanie uczniów w zajęcia, każda kreskówka ma alternatywne rozwiązanie dylematu, przed którym staje jej bohater. O tym, jak powinien się za-

chować, decydują uczniowie, mają jednak możliwość poznania również drugiego zakończenia.

Kurs e-learning „Bezpieczna przygoda z Internetem"

Również dla uczniów IV-VI przewidziano zajęcia e-learningowe. Składają się one z 7 modułów, zadaniem użytkownika jest przejście 7 komnat i zdobycie 7 dysków wiedzy. Kurs przewidziano na trzy jednostki lekcyjne. Dzięki platformie e-learningowej nauczyciel ma możliwość komunikacji ze swoją grupą uczniów oraz śledzenia ich postępów.

Oferta edukacyjna dla klas I-III szkół gimnazjalnych. Zajęcia „Stop cyberprzemocy"

Dla uczniów gimnazjum, ze względu na rosnącą skalę przemocy rówieśniczej, powstały zajęcia „Stop cyberprzemocy". Ich celem jest przedstawienie przede wszystkim konsekwencji tego zjawiska – zarówno z perspektywy ofiary, sprawcy, jak świadka zdarzeń. Podstawą do poprowadzenia zajęć jest dwuminutowy film przedstawiający przypadek przemocy rówieśniczej z wykorzystaniem nowoczesnych mediów. Nakręcony w szkolnej szatni przed lekcją WF-u film trafia do Internetu. Jego bohaterka staje się przedmiotem żartów, przestaje przychodzić do szkoły, nie radzi sobie z sytuacją. W trakcie zajęć młodzież dowiaduje się, jakie formy może przyjmować cyberprzemoc, co mogą czuć jej ofiary, jak powinny się zachować, gdzie mogą szukać pomocy, co powinni zrobić świadkowie takich sytuacji. Na realizację zajęć trzeba poświęcić dwie godziny lekcyjne.

Kurs e-learning „Znajomi-nieznajomi.pl"

Uzupełnieniem zajęć lub alternatywą dla nich może być kurs e-learningowy „Znajomi-Nieznajomi". Jego treść odwołuje się do zasad funkcjonowania serwisów społecznościowych. Użytkownik kursu wciela się w rolę administratora zarządzającego takim serwisem. Jego zadaniem jest rozwiązywanie problemów użytkowników, dotyczących np. włamania na konto, kradzieży własności intelektualnej, bezpieczeństwa zakupów w Internecie lub nadużyć w sieci.

Sieciaki

Dodatkowym narzędziem edukacyjnym, którego zadaniem jest utrwalenie i poszerzenie wiedzy dzieci, jest ogólnodostępny serwis edukacyjny www.sieciaki.pl. Został zaprojektowany z myślą o 7-12 latkach, ale korzystają z niego dzieci zarówno młodsze, jak i starsze, można go wykorzystywać również w celach edukacyjnych. Serwis jest bezpieczny – można udostępnić go dziecku bez obaw, że trafi na niewłaściwe treści albo padnie ofiarą werbalnej przemocy.

W części informacyjnej młodzi internauci znajdą wiadomości o Sieciakach i Sieciuchach, jak również Katalog Bezpiecznych Stron BeSt, sprawdzonych i polecanych przez Sieciaki. W serwisie społecznościowym użytkownicy mogą porozumiewać się pomiędzy sobą, wcześniej jednak nauczą się jak powinien wyglądać *nick*, który nie będzie prowokował agresji lub innych nadużyć. Dowiedzą się również, jak stworzyć bezpieczne hasło, które niełatwo będzie złamać. Na SiecioPlanecie użytkownicy serwisu mają okazję sprawdzić się w zadaniach specjalnych i misjach, a równocześnie zdobyć wiedzę o zasadach bezpiecznego korzystania z sieci.

3. Edukacja dla profesjonalistów i rodziców

Wszystkie zajęcia przygotowane w ramach programu „Dziecko w Sieci" wpisują się w ideę edukacji medialnej najmłodszych. Jednocześnie wiemy – m.in. z informacji, które docierają do fundacji – jak często to dorośli są bezradni wobec cyberprzemocy lub internetowych przestępstw. Często również ignorują je, ponieważ sam problem jest mało widowiskowy (cyberprzemoc nie powoduje przecież sińców), a dostrzegalne są dopiero jego konsekwencje. Z myślą o dorosłych powstały więc zajęcia e-learningowe dotyczące zagrożeń dzieci w Internecie. Przygotowano je w wersji dla profesjonalistów (trzy moduły) i rodziców (dwa moduły). W ich tworzeniu brali udział psycholodzy, prawnicy, pedagodzy, wykorzystano również doświadczenia pracowników Helpline.org.pl. Kurs w formie prezentacji multimedialnej przedstawia zagrożenia z jakimi najmłodsi internauci mogą mieć do czynienia w Internecie, informuje również, jak można im zapobiegać lub ograniczać ich skutki. Założeniem była możliwość zarówno samodzielnego oglądania materiału, jak i prezentacja go w trakcie rady pedagogicznej lub spotkania rodziców. Można go traktować zarówno jako integralne zajęcia (oglądając od początku do końca), jak również jako kompendium wiedzy, wybierając jedynie konkretne zagadnienia. Dla nauczycieli przewidziano również prezentację oferty edukacyjnej programu „Dziecko w Sieci". Kurs jest dostępny w serwisie dzieckowsieci.pl (do obejrzenia *online* lub ściągnięcia na dysk komputera), przewidujemy również jego edycję na płytach DVD.

4. Edukacja społeczna

Niedawno (w czerwcu 2009 roku) powrócili bohaterowie spotu „Nigdy nie wiadomo, kto jest po drugiej stronie", czyli Ania i Wojtek. Ponad 5 lat temu kampania ta zwróciła uwagę społeczeństwa na problem ryzykownych kontaktów dzieci w Internecie. Problem nie zniknął – dopiero teraz pojawiają się jednak regulacje prawne dotyczące uwodzenia dzieci w Internecie. Kampania będzie się toczyła pod hasłem „Każdy ruch w Internecie zostawia ślad". Organizatorzy chcą w ten sposób przypomnieć, że – wbrew pozorom – nikt w Internecie nie jest anonimowy, a uwagę społeczeństwa ponownie zwrócić na problem kontaktów dzieci z nieznanymi osobami *online*. Dodatkowo, a może przede wszystkim, kampania ma trafić do potencjalnych sprawców – by nie mogli tłumaczyć się nieznajomością prawa, jak również – by zdali sobie sprawę, że za relacje z dzieckiem w Internecie odpowiedzialność zawsze ponosi dorosły.

Autor jest redaktorem serwisu „Dziecko w Sieci", członkiem zespołu Fundacja Dzieci Niczyje

„Każdy ruch w Internecie zostawia ślad"

8 czerwca 2010 roku weszła w życie nowelizacja kodeksu karnego, dotycząca uwodzenia dzieci w Internecie, dająca szansę na skuteczną walkę z pedofilią w sieci. Tego samego dnia ruszyła nowa odsłona kampanii „Dziecko w Sieci" pod hasłem „Każdy ruch w Internecie zostawia ślad", prowadzona przez Fundację Dzieci Niczyje, Naukową i Akademicką Sieć Komputerową oraz Rzecznika Praw Dziecka.

Kampania ma na celu uświadomienie potencjalnym sprawcom, że nie są ani anonimowi, ani bezkarni, zaś ofiarom krzywdzenia, że prawo jest po ich stronie i że w sytuacji zagrożenia mogą oczekiwać pomocy.

Działaniom medialnym kampanii towarzyszą propozycje edukacyjne – na stronie www.dzieckowsieci.pl dostępny będzie kurs e-learning poświęcony problematyce bezpieczeństwa sieciowego. Kurs, przygotowany przez FDN i Fundację Orange, jest przeznaczony dla rodziców i profesjonalistów pracujących z dziećmi.

Więcej informacji na stronie www.dzieckowsieci.pl/kazdy_ruch

Agnieszka Borowiecka

Kim jestem, czyli tożsamość w sieci

Babcia spojrzała na niego z wyraźną naganą.

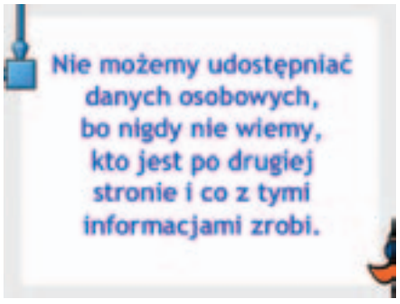
– Zdaje się, że uczycie mnie kłamać? – oburzyła się.

– W tym wieku powinnaś już sama umieć – stwierdziła zimno Janeczka. – Poza tym to nie jest żadne kłamstwo, tylko sama święta prawda. Tyle że opuszczasz trochę po drodze. (...)

– No proszę! – przyświadczył gorąco Pawełek. – I gdzie tu kłamstwo? Uczciwie byłaś przy furtce przez przypadek!

Babcia spojrzała na dzieci prawie z przerażeniem. Przyszła jej do głowy okropna i dość krępująca myśl, że przecież to coś, co jej proponują, w świecie dorosłych nosi nazwę dyplomacji. Właściwie wcale się nie kłamie, mówi się prawdę, tylko coś tam omija się po drodze[1].

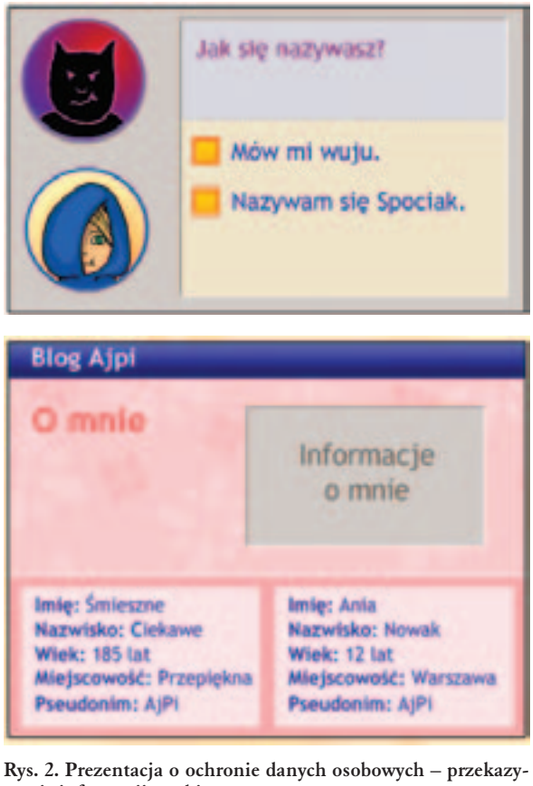
Ostatnio uczestniczyłam w kilku konferencjach dla nauczycieli informatyki, dotyczących bezpieczeństwa i ochrony prywatności dzieci i młodzieży. Przeglądałam także różne opracowania, mające ułatwić zapoznanie uczniów z metodami bezpiecznej pracy w sieci. Moją uwagę zwróciły szczególnie materiały, dotyczące podawania danych osobowych i poznawania nowych osób w sieci.



Rys. 1. Slajd prezentacji o ochronie danych osobowych

Tekst na powyższym zdjęciu nie budzi wątpliwości – prawdą jest, że nigdy nie możemy być w 100% pewni, z kim kontaktujemy się w sieci. Codziennie słyszymy i czytamy o niewłaściwym wykorzystywaniu informacji znalezionych w Internecie, różnego typu cyberprzestępstwach i prześladowaniu. Zachęcanie do ostrożności wydaje się jak najbardziej słuszne. Jednak inne elementy tego samego pokazu wzbudziły we mnie poważne wątpliwości.

Jakie informacje powinien wybrać uczeń? Jako jedynie słuszne jest wskazane, co najwyżej udostępnienie swojego pseudonimu. Wszystkie pozostałe dane są uznawane za niebezpieczne.



Rys. 2. Prezentacja o ochronie danych osobowych – przekazywanie informacji o sobie

[1] Chmielewska J. *Nawiedzony dom*, Młodzieżowa Agencja Wydawnicza, Warszawa 1987.

Rys. 3. Prezentacja o ochronie danych osobowych – prawidłowe odpowiedzi

I to wzbudziło we mnie mieszane uczucia. Rozumiem, że Internet jest wykorzystywany przez różnych przestępców, dziecko może nieświadomie narazić siebie i swoich bliskich na niebezpieczeństwo (włamania, pedofilia, prześladowania itp.). Jeżeli jednak wszyscy mamy ukrywać informacje o sobie, to skąd ktoś inny ma wiedzieć, z kim kontaktuje się w sieci. Oznacza to, że żadna osoba w sieci nie jest tym, za kogo się podaje! Poza tym, tak jak Babcia z książki Joanny Chmielewskiej, mam pewne wątpliwości natury moralnej – czy my przypadkiem nie uczymy dzieci, że kłamstwo nie tylko nie jest naganne, ale wręcz jest zalecane? Czy to, o czym je przekonujemy, dotyczy tylko Internetu, czy powinno również być wykorzystywane w innych kontaktach, w tzw. realu? „Nie rozmawiaj z obcymi", „nie przyjmuj od nieznajomych żadnych przedmiotów" – te zalecenia pamiętamy z własnego dzieciństwa. Ale moja mama nigdy mi nie mówiła: „Jak ktoś cię zapyta gdzie mieszkasz, to powiedz, że w Pałacu Kultury". No tak, pewnie to były inne czasy...

W wielu poważnych opracowaniach czytamy o wyizolowaniu jednostki we współczesnym świecie, ludzie przestają się ze sobą spotykać, jedyny kontakt ze sobą utrzymują za pomocą komórek i Internetu. Dzieci zamiast bawić się z kolegami na świeżym powietrzu, spędzają większość czasu przy komputerze. Uświadomiłam sobie, że ja także z własnymi rodzicami więcej rozmawiam przez telefon niż osobiście. Odnoszę jednak wrażenie, że działania proponowane dzieciom w celu zwiększenia ich bezpieczeństwa prowadzą do dalszego wyobcowania i ograniczenia kontaktów międzyludzkich. Skoro nikt nie jest tym, za kogo się podaje, to może tak naprawdę chyba nie ma po co kontaktować się z kimkolwiek w sieci?

Pamiętajmy równocześnie o tym, że ukrycie danych osobowych nie zapewni nam pełnej anonimowości. Każda nasza aktywność w Internecie zostawia ślad. Niekoniecznie też musimy takie informacje zostawiać sami. Pamiętajmy, że nie jesteśmy zupełnie samotni i nie odpowiadamy za dane, jakie publikują o nas inni.

Co zatem powinniśmy zaproponować naszym uczniom? Jak dalece powinni oni ukrywać informacje o sobie? Te i wiele podobnych pytań pozostaje na razie bez jednoznacznej odpowiedzi. Powinniśmy jednak kierować się zdrowym rozsądkiem i dbając o bezpieczeństwo dzieci, pozwolić im na odrobinę samodzielności i odpowiedzialności.

Pamiętajmy, bardzo ważne jest nie tylko kształtowanie u uczniów umiejętności ostrożnego zachowania w cyberprzestrzeni, ale także rozpoznawanie, które sytuacje są bezpieczne, a kiedy ostrożność jest bardzo wskazana, np. przy posługiwaniu się komunikatorami czy podczas udziału

Rys. 4. Slajd prezentacji „Kłopoty i incydenty" (poradnik „Bądź bezpieczny w Internecie")

w forach i czatach. Dzieci i młodzież mogą się zetknąć także z sytuacją, gdy nie powinny ukrywać swoich danych. W jaki sposób mogłyby ze sobą współpracować przy tworzeniu różnego rodzaju projektów, brać udział w grupach zainteresowań? Jak mogłyby być przeprowadzane różnego typu projekty międzyszkolne i międzynarodowe, gdyby uczniowie nie podawali swoich prawdziwych danych?

Łączenie zasad bezpieczeństwa i zdrowego rozsądku przy udostępnianiu informacji o sobie w Internecie może okazać się dla dzieci i młodzieży bardzo trudne. Doświadczenie i mądrość życiowa rodziców i nauczycieli mogą być tutaj bardzo pomocne.

Wykorzystane slajdy pochodzą z poradnika „Bądź bezpieczny w Internecie" (http://www.partnerstwodlaprzyszlosci.edu.pl/bezpieczenstwo/default.aspx) oraz kursów dla uczniów szkoły podstawowej na platformie e-learningowej „Dziecko w Sieci" (https://kursy.dzieckowsieci.pl).

Autorka jest nauczycielem konsultantem w Ośrodku Edukacji Informatycznej i Zastosowań Komputerów w Warszawie

Dzień Bezpiecznego Internetu

W lutym każdego roku, począwszy od roku 2004, z inicjatywy Komisji Europejskiej obchodzony jest w ramach programu „Safer Internet" międzynarodowy Dzień Bezpiecznego Internetu (*Safer Internet Day*).

Przedsięwzięcie ma na celu przede wszystkim inicjowanie i propagowanie działań na rzecz bezpiecznego dostępu dzieci i młodzieży do zasobów internetowych, zaznajomienie rodziców, nauczycieli i wychowawców z problematyką bezpieczeństwa dzieci w Internecie oraz nagłośnienie tematu bezpieczeństwa *online*.

Od 2005 roku organizatorami Dnia Bezpiecznego Internetu w Polsce są Naukowa i Akademicka Sieć Komputerowa (NASK) oraz Fundacja Dzieci Niczyje (FDN), tworzące Polskie Centrum Programu „Safer Internet", od lat prowadzące szereg kompleksowych działań na rzecz bezpieczeństwa dzieci *online*.

Co roku organizatorzy DBI zachęcają szkoły, organizacje pozarządowe, firmy i prywatne osoby do organizowania przez cały luty lokalnych inicjatyw na rzecz bezpieczeństwa młodych internautów (m.in. zajęć edukacyjnych, happeningów, gazetek szkolnych, audycji w radiowęzłach szkolnych, kampanii informacyjnych, konkursów).

Ponadto 9 lutego we wszystkich krajach Unii Europejskiej ruszyła kampania medialna poświęcona problematyce ochrony prywatności w Internecie – „Think B4 U post!", w Polsce realizowana pod hasłem „Pomyśl zanim wyślesz".

Małgorzata Nowak

Stop cyberprzemocy!

Majowa sobota. Na dworze chłodno, działka musi poczekać. Poranna kawa. Siadam do komputera. Sprawdzam pocztę, odpowiadam na maile, lektura forum, zaglądam na Naszą Klasę. Czas na zaplanowany artykuł. Dzwoni telefon – to SMS od męża. Za chwilę znów sygnał komórki – syn przysyła zdjęcia znad jeziora. Mam swój realny świat pod wirtualną kontrolą. Mogę spokojnie pisać. Jeszcze raz czytam mail od pani dyrektor OEIiZK:

…bardzo ważne są dla nas kwestie zagrożeń generowanych przez nowoczesne technologie, bezpieczeństwo i higiena pracy z komputerem, kwestie wychowawcze (…) chciałabym ogłosić konkurs na napisanie opowiadania lub eseju zawierającego opis problemu związanego z obecnością technologii informacyjnej w naszych szkołach i naszym życiu i sposób jego rozwiązania, a następnie wydać je w postaci publikacji. Pani artykuł jest mi potrzebny jako wzór tego typu materiałów…

Jestem uzależniona od komputera – trudno wyobrazić mi sobie życie bez elektronicznej poczty, rozmów na forum, bez potrzebnych informacji na kliknięcie myszką. Doceniając siłę nowoczesnych technologii informatycznych, jasno zdaję sobie sprawę z płynących z tego samego źródła zagrożeń. Jako pedagog czuję się odpowiedzialna za właściwe kształtowanie umiejętności korzystania ze współczesnych mediów. Buntuję się przeciwko postawie: *a co ja mogę zrobić, nad Internetem się nie zapanuje, nie mam na to wpływu*. To nieprawda – wirtualny świat nie musi być bezkarny. W „realu" można wiele zrobić w celu przeciwdziałania medialnej przemocy. Trzeba tylko chcieć!

Czym jest cyberprzemoc[1]?

Cyberprzemoc to inaczej przemoc z użyciem mediów elektronicznych – przede wszystkim Internetu i telefonów komórkowych. Problem ten dotyczy przede wszystkim dzieci i młodzieży. W Polsce doświadcza go ponad połowa młodych internautów!!! Do działań określanych jako cyberprzemoc zalicza się m.in.:

- wyzywanie, straszenie, poniżanie kogoś w Internecie lub przy użyciu telefonu,
- robienie komuś zdjęć lub rejestrowanie filmów bez jego zgody,
- publikowanie w Internecie lub rozsyłanie telefonem zdjęć, filmów lub tekstów, które kogoś obrażają lub ośmieszają,
- podszywane się pod kogoś w sieci.

Pomimo że akty cyberprzemocy mogą wyglądać niewinnie, potrafią wyrządzać bardzo dużą krzywdę.

Sięgam do swojego elektronicznego archiwum. Czytam artykuły, notatki. Przypominam sobie zdarzenia, sytuacje, reakcje. Może warto je przedstawić?

Wirtualny lincz[2]

O problemie dowiedziałam się przypadkiem. Zaintrygowała mnie luźna uwaga syna: – *Mama, zajrzyj na forum swojego gimnazjum…*

Zajrzałam. Poczytałam. Kilka neutralnych wątków – o grach komputerowych i imprezach. Ze dwa mające funkcję fatyczną: *hej, jest tu ktoś?* I kilka założonych przez Andżelikę. Gimnazjalistka – zbyt puszysta jak na standardy wyznaczane przez nastolatkowe czasopisma, zbyt ufna, niełapiąca dowcipów, na internetowym forum rozpaczliwie szukała towarzystwa, zakładając kolejne wątki. Najpierw pytała: *co tam uwas słychac*, potem uśmiechała się zachęcająco: : -)))))))))))))))))), zapraszała*: tu możecie sie wpisywac.* Posty pozostawały bez odpowiedzi, jednak ich autorka nie poddawała się i z uporem godnym lepszej sprawy szukała przyjaznej duszy w wirtualnym świecie. Najnowszy wątek opatrzony tytułem: *tu można ze mną porozmawiać* trafił na okres świątecznej nudy, czasu siedzenia godzinami w Internecie jako odskoczni od oficjalnoświątecznej sztampy rodzinnych spotkań.

[1] Polecam bardzo: http: //www.cyberprzemoc.pl

[2] Wykorzystano fragmenty: Nowak M. *Konto usunięte*, „Dyrektor Szkoły" nr 3/2009.

I zaczęło się… Grono rozmówców nie było liczne, jednak szybkość pojawiających się postów świadczyła o tym, że w czasie *świąt dzieci się nudzą*… Przekonane o bezkarności często nudzą się wulgarnie i okrutnie. Wątek Andżeliki szukającej towarzystwa zamienił się w słowny lincz pewnych siebie (?), inteligentnych (?), dowcipnych (?) nastolatków. W końcu coś się działo. Dziewczyny przerzucały się skojarzeniami, wyśmiewały tuszę dziewczyny, kpiły z widocznych oznak sympatii do rówieśników. Andżelika próbowała się bronić, była jednak bez szans. Jej spokojny komunikat: *obraziłaś mnie* wywołał kolejne komentarze. Dziecinna prośba: *ty nie pisz na tym wątku bo tylko kumple mogą gadac ale ty nie możesz wiec papapa* pogorszyła tylko sytuację. Sprowokowana, napisała ostro*: sp*… Wzrastająca agresja dziewczyny wywoływała lawinę dalszych wypowiedzi.

Wątek liczył kilkadziesiąt postów. Poraził mnie ich poziom, wulgaryzmy, obsceniczne skojarzenia i seksualne teksty. Jednak nie to było największym zaskoczeniem. Rozmowa nie była anonimowa. Z fotek obok postów uśmiechały się znajome gimnazjalistki: Kasia z wolontariatu, Ada pisząca wiersze, Agnieszka działająca w samorządzie. Dziewczyny, które w szkole znałam jako sympatyczne, fajne nastolatki. Z dobrych domów, żadna patologia, nawet jeśli rodzinne problemy, to w normie współczesnego społeczeństwa: drugi tata, mama za granicą. Na forum pokazywały inną twarz, inny system wartości, były wulgarne, okrutne.

Przeczytałam cały wątek. Była sobota. Myślałam, jak zareagować. Szukałam skutecznego i wychowawczego sposobu reakcji. Wiedziałam, że zachowanie młodzieży brało się z poczucia bezkarności wirtualnego świata. Postanowiłam zaburzyć to przekonanie. Jestem dyrektorem. Forum gimnazjum jest także moim forum. Kliknęłam i włączyłam się do dyskusji: *Dobry wieczór. Mam wrażenie, że tocząca się rozmowa znacznie przekroczyła granice przyzwoitości i kultury, sprawiła przykrość Andżelice i naruszyła jej godność. Poziom zamieszczonych tu wypowiedzi źle świadczy o uczniach naszej szkoły. Jest mi z tego powodu przykro. Zapraszam na rozmowę w realnym świecie w celu wyjaśnienia zasad korzystania z internetowych możliwości komunikowania się i szanowania uczuć innych.* Moja wypowiedź opatrzona imieniem, nazwiskiem i zdjęciem skończyła wymianę postów i niewybrednych komentarzy. Późnym wieczorem w niedzielę pojawił się tylko krótki wpis: *Lol!*

W poniedziałek rano, wchodząc do szkoły, obserwowałam twarze i reakcje uczniów. Wieść o internetowej reakcji dyrektorki musiała się już rozejść. Tak naprawdę zależało mi na nagłośnieniu sprawy – uczniowie powinni się przekonać, że odpowiadają za swoje zachowanie, że wirtualna wersja życia może łatwo zamienić się w realną.

Zapraszam do gabinetu dziewczyny biorące udział w rozmowie na forum. Bez Andżeliki – chcę jej oszczędzić powtórnego przeżywania upokorzeń. Zamiast dziewczyny – zapraszam jej wychowawczynię. Panuje cisza. Nie wyjaśniam problemu, o nic nie pytam. Włączam komputer, loguję się na Naszej Klasie, wchodzę na forum gimnazjum, odnajduję wątek. Proszę gimnazjalistki o głośne czytanie swoich wypowiedzi, sama wcielam się w rolę Andżeliki. Zaczynam: *Tu można ze mną porozmawiać.* Konsternacja. Dziewczyny nie podnoszą wzroku. Zdecydowanie powtarzam prośbę o głośne czytanie swoich wypowiedzi. Ciężko to idzie. Czytane w gabinecie dyrektora, w obecności lubianej nauczycielki, posty przestają być dowcipne. Czytane półgłosem, prawie szeptem, załamującym się głosem, nie przestają być wulgarne, stają się ciężkie, wiszą w powietrzu. Uparcie kontynuuję lekturę – strona po stronie. Pierwsza nie wytrzymuje Ada – zaczyna płakać: – *Przepraszam, nie wiedziałam, że to tak wyjdzie... Nie chciałam dokuczyć Andżelice*… Do wyjaśnień dołącza Kaśka: – *Naprawdę, ja też nie chciałam, nie pomyślałam*… Nie podejmuję dialogu, proszę o doczytanie wątku dokońca. Wreszcie zapada cisza, dziewczyny nie potrafią zapanować nad emocjami, wyciągam chusteczki higieniczne.

– Zrozumiałyście, jak bardzo można kogoś skrzywdzić słowami? Wasze wypowiedzi na forum może przeczytać każdy. Internet to wspaniałe narzędzie, daje możliwość rozmowy i kontaktu z drugim człowiekiem. Od nas zależy, czy te możliwości wykorzystamy, żeby komuś pomoc, czy dokopać.

Prowadzę rozmowę jeszcze przez jakiś czas. Nie muszę dziewczynom specjalnie tłumaczyć problemu. Są inteligentne. Rozumieją. Nie pomyślały, nie zastanowiły się, zrobiły źle. Poniosą konsekwencje. Udzielam im nagany dyrektora szkoły. Informuję o wniosku do wychowawcy o obniżenie oceny z zachowania. Zobowiązuję do spowodowania usunięcia wulgarnych wypowiedzi z forum. Na koniec pytam: – *Powiecie same rodzicom o wydarzeniu, czy mam zadzwonić? – A musimy?? – Tak, rodzice muszą wiedzieć, do czego służy wam Internet.* Nie mają wyjścia. Wiedzą, że nie odpuszczę. Proszę, żeby rodzice zadzwonili do mnie i potwierdzili, że znają sprawę. Wyznaczam termin zniknięcia postów. To musi potrwać. Moderator Naszej Klasy ma określone procedury reagowania w takiej sytuacji. Wszyscy rodzice oddzwonili. Byli zszokowani. Nie spodziewali się. Przepraszali za swoje córki. Wychowawczyni porozmawiała z Andżeliką. Na-

mówiła ją do skorzystania z zajęć socjoterapeutycznych. Może tam znajdzie kogoś, *kto zechce z nią pogadać?* Kilka dni później zaglądam na forum. Wulgarny wątek zniknął. Forum zmieniło wygląd. Zamiast zdjęć gimnazjalistów w wielu miejscach widnieją puste ramki z napisem: Konto usunięte. Reakcja rodziców? Decyzja gimnazjalistów? Nieważne. Wiem, że moje działanie było skuteczne i odniosło wychowawczy skutek.

Fotka (nie)prawdziwa[3]

Młoda germanistka zgłasza problem: na portalu Fotka ktoś założył jej profil. Zdjęcia zrobione podczas lekcji, prawdopodobnie telefonem komórkowym. Zmyślone dane, wulgarny opis. Nie mogłam się tym od razu zająć – jako przewodnicząca szkolnego zespołu nadzorującego egzamin gimnazjalny musiałam dopilnować wszystkich procedur. Poprosiłam wicedyrektora o obejrzenie zamieszczonych zdjęć i próbę ustalenia z nauczycielką miejsca i czasu ich zrobienia. Do sprawy chciałam wrócić po egzaminie. Telefon pani Asi uświadamia mi, że sytuacja się rozwija:

– Pani dyrektor, przepraszam, że dzwonię do domu, ale naprawdę nie mogę sobie z tym poradzić, pojawiły się nowe komentarze. Boję się, że jutro będzie o tym mówić pół szkoły. Poza tym – nie chciałabym, żeby zobaczyli to znajomi, rodzina. Proszę o pomoc…

Nie mogę czekać. Trzeba działać natychmiast. Siadam do komputera i z pomocą syna szybko odnajduję założone fałszywe konto. Oglądam zdjęcia – na szczęście (?) to tylko (?) twarz nauczycielki. Robię powiększenie, analizuję szczegóły. Poznaję paprotkę wiszącą w jednej z klas, kojarzę, gdzie wisi obraz, którego fragment znalazł się w kadrze. Porównuję z planem lekcji. Szybko ustalam klasę, w której prawdopodobnie znajdują się autorzy zdjęć. Jeszcze raz przeglądam założone konto, otwieram kolejne zakładki: „Zdjęcia", „O mnie", „Komentarze", „Znajomi", „Klany", „Imprezy", „Kontakt".

Najbardziej bulwersujące są komentarze: opis preferencji i oczekiwań damsko-męskich, niewybredne słownictwo z błędami ortograficznymi. Klikam w kolejną zakładkę: wśród znajomych rozpoznaję twarze z naszej szkoły. Porównuję z listą uczniów klasy pani Asi. Dwa nazwiska się zgadzają. Kopiuję cały profil wraz ze zdjęciami „Znajomych" – w rozmowach z rodzicami (i policją) warto mieć dowody. Nagrywam na płytę. Jest wieczór, jutro drugi dzień egzaminu, załatwienie sprawy musi poczekać.

Nazajutrz, godzina 9.30. Egzamin w toku. Wszystko zgodnie z procedurami, panuje spokój. Wracam do problemu. Postanawiam pójść na całość – zaskoczenie i pewność informacji są często gwarancją powodzenia. Dzwonię do uczniów, potencjalnych autorów zdjęć, komentarzy i umieszczenia ich w Internecie. Odbiera mama, proszę o zgłoszenie się z synem do szkoły – najlepiej natychmiast. Drugi telefon odbiera uczeń – proszę o to samo. Na pytanie: *– O co chodzi?* – mówię krótko, że sprawa jest poważna i porozmawiamy w szkole. Pół godziny później do gabinetu wchodzi zdenerwowana kobieta z Maćkiem, uczniem szóstej klasy.

– Pani dyrektor, ale on naprawdę nie wie, o co chodzi. – Nic nie zrobiłem! – dodaje chłopak.

– A Fotka? – pytam bez wyjaśnień. Błyskawiczny rumieniec na twarz Maćka jest jednoznaczny. *– A… Fotka…* – powtarza z zaskoczeniem. Matka zdezorientowana patrzy na syna. Wiem, że trafiłam. Zaczynam rozmowę. Informuję, że mam skopiowane i utrwalone zdjęcia, komentarze. Że nauczyciel jest osobą podlegającą ochronie jak funkcjonariusz publiczny. Uprzedzam, że mówienie prawdy będzie okolicznością łagodzącą. Po takim wstępie ustalanie faktów nie wymaga nadzwyczajnych zabiegów: chłopak zaskoczony wiedzą, dowodami i przestraszony konsekwencjami wyjaśnia, że zdjęcia zrobił kolega, założył konto, ale on wiedział o wszystkim. Zakładam, że uczeń mówi prawdę, proszę o pisemny i podpisany opis zdarzeń w celu porównania z wersją kolegi, który czeka w sekretariacie.

Druga rozmowa przebiega podobnie. Co ważne – sprawca przyznaje się do winy, nawet próbuje zmniejszyć rolę kolegi: *– Maciek nic nie zrobił, to ja wszystko…* Sytuacja wyraźnie przerosła chłopaka. Dwunastolatek mimo 1,70 m wzrostu jest tak naprawdę jeszcze dzieckiem. Zacytowane w obecności matki obsceniczne wyrażenia na temat nauczycielki, wulgarne sformułowania przeczytane w gabinecie dyrektora przestają być *dobrym numerem*. Patryk zaczyna płakać, prosi, *żeby nie informować policji, żebym wstawiła się za nim u pani,* powtarza, *że jest mu przykro, że nie chciał…* W swojej reakcji jest szczery – wieloletnia praktyka nauczyła mnie rozpoznawać skruchę pozorowaną.

Mam niewiele czasu, zaraz pojawią się przewodniczący komisji egzaminacyjnych z pracami. Chwila rozmowy z obu chłopakami – informuję o oczekiwaniach: natychmiastowe usunięcia założonego konta, przeproszenie nauczycielki i nienaganne zachowanie do końca roku szkolnego, zgłoszenie się

[3] Wykorzystano fragmenty: Nowak M. *Znajomi z Fotki*, „Dyrektor Szkoły" nr 7/2008.

na rozmowę do szkolnego psychologa. Konsekwencje: obniżenie oceny z zachowania, być może zawiadomienie o sprawie policji – to ostatnie uzależniam od decyzji nauczycielki. Podoba mi się postawa matek: z jednej strony nie bronią bezkrytycznie synów, z drugiej próbują im pomoc w rozwiązaniu sytuacji.

Godzina 13.00. Prace egzaminacyjne spakowane, elektroniczny arkusz wysłany do OKE. Zanim pojadę oddać prace, zamknę sprawę Fotki.

Zapraszam do siebie szkolnego psychologa i panią Asię. Wchodzą mamy i chłopcy – obaj z wiązankami kwiatów. Zapada cisza. Krótko przypominam przebieg zdarzenia. Uświadamiam uczniom jeszcze raz, że głupi żart (?) może stać się powodem czyjegoś cierpienia, a konsekwencje dla sprawcy mogą być bardzo poważne. Podkreślam fakt, że Maciek i Patryk przyznali się od razu do winy i okazali skruchę. Oddaję im głos. Przepraszają, ze spuszczonymi głowami proszą, żeby pani im wybaczyła. Za swoich synów przepraszają ze łzami w oczach matki. Sytuacja ich przerosła – nie jest proste uświadomienie sobie, że syn, takie *dobre i grzeczne dziecko,* umieszcza w Internecie zdjęcia swojej pani od niemieckiego i posługuje się słownictwem rodem z filmu porno. Nauczycielka jest poruszona. Kwiaty i postawa chłopaków, łzy matek – to działa na emocje. Mówi, że *było jej przykro, że się nie spodziewała po nich, że wybacza.* Zobowiązuję uczniów do kontaktu z psychologiem, zależy mi na zrozumieniu groźby pozornej anonimowości Internetu i płynących stąd zagrożeń dla relacji między ludźmi. Kończę spotkanie, tym razem problem udało się szybko rozwiązać. Wieczorem konta nauczycielki na portalu Fotka już nie ma.

***

Dlaczego opisuję te historie? Portale Nasza Klasa, Fotka – to nie jedyne miejsca, gdzie coraz częściej ocenia się szkołę, gdzie można „dokopać" nauczycielowi, dać upust niekontrolowanym emocjom i niewybrednemu słownictwu. Pozorna anonimowość Internetu nie może oznaczać bezradności szkoły, niemocy nauczyciela, obojętności dyrektora. Od nas zależy, czy pozwolimy na swobodny rozwój sytuacji i poczucie bezkarności tylko pozornie wirtualnych a w rzeczywistości jakże realnych sprawców cyberprzemocy. Internet nie jest anonimowy. Elektroniczne media powinny być sprzymierzeńcem człowieka, nie jego wrogiem. Zadaniem rodziców, nauczycieli jest uświadamiać to dzieciom. Zadaniem pedagoga jest skuteczna reakcja na niewłaściwe zachowanie uczniów. Obowiązkiem każdego jest szybka i zdecydowana reakcja na krzywdę wyrządzaną drugiemu człowiekowi. I nie ma to znaczenia, czy agresja ma formę kopniaka, wyzwiska czy obscenicznego zdjęcia. Musisz zareagować. Zanim będzie za późno.

Autorka jest dyrektorem Zespołu Szkół im. Ziemi Lubelskiej w Niemcach

Bezsensowny gniew i wulgarne rozrywki stanowią wentyl bezpieczeństwa dla ludzkiego niepokoju.

Che Guevara (Ernesto Guevara de la Serna)

Jerzy Piskor

Bezpieczeństwo szkolnej infrastruktury informatycznej

Ważnym elementem komputeryzacji pracy szkoły jest szacowanie i kontrola ryzyka związanego z wykorzystaniem komputerów w zakresie zachowania przez nie poufności, łatwości dostępu i integralności.

W 1994 roku utworzyłem w szkole podstawowej informacyjny system wspierania edukacji i zarządzania, który jest ciągle modyfikowany i doskonalony, a doświadczenia z jego funkcjonowania stały się podstawą niniejszego artykułu.

Celem moich działań było zbudowanie bezpiecznego systemu, ale ze względu na złożoność i czasochłonność wielu jego elementów i procesów, poważnym problemem stały się istniejące i pojawiające się nowe luki w zabezpieczeniach.

Prawdziwie bezpieczny system, zgodnie z powszechną definicją, jest idealnym urządzeniem, które poprawnie i w całości realizuje tylko i wyłącznie cele zgodne z intencjami właściciela. W rzeczywistości, w związku z ryzykiem powstania prozaicznych błędów i usterek oraz w wyniku sprzecznych oczekiwań użytkowników, właściciela czy projektanta, tak naprawdę zapewnienie bezpieczeństwa skupia się na zarządzaniu ryzykiem mogących wystąpić zagrożeń i powstających ewentualnie w związku z tym strat. Trzeba zatem podejmować racjonalne kroki zapobiegawcze, mając na uwadze możliwości techniczne i finansowe. Dotychczasowe wsparcie szkół poprzez fundowanie im pracowni komputerowych nie uwzględniało wystarczająco tego problemu. W miarę rozbudowy infrastruktury (sieci rozległe, Internet) coraz większym problemem stają się osoby trzecie mogące wchodzić w interakcje z systemem w sposób niezamierzony ani oczekiwany przez właściciela. Ważnym aspektem tego zagadnienia są błędy i pomyłki (np. techniczne) popełniane najpierw przez programistów, potem przez administratorów (wynikające z niezrozumienia dokumentacji, niestaranności czy niepełnych kwalifikacji) czy wreszcie operatorów (użytkowników nierozumiejących zagadnień prawidłowej i bezpiecznej obsługi – np. uruchamianie załączników od niepewnych nadawców, ignorowanie komunikatów ostrzegawczych czy przypadkowa zmiana np. opcji programów). Innym aspektem tego zagadnienia są kłopoty ze spamem, wynikające historycznie z budowy protokołu SMTP.

Choć wyeliminowanie błędów zabezpieczeń praktycznie nie jest możliwe (nieekonomiczne), można starać się je zminimalizować. Ważne jest, aby budować struktury w sposób ograniczający ewentualne skutki naruszenia zabezpieczeń czy niepożądanej aktywności uprawnionego użytkownika. W efekcie będzie możliwe zminimalizowanie ewentualnych strat i szybka identyfikacja problemów. Kluczem do sukcesu może być ograniczenie do niezbędnego minimum uprawnień użytkowników, wyłączanie zbędnych usług sieciowych na platformach czy stosowanie zapór sieciowych.

Zapewnienie bezpieczeństwa wymaga ciągłych nakładów pracy i nakładów finansowych oraz edukacji użytkowników, aby np. rezygnowali z oglądania niebezpiecznych stron WWW. Konieczna jest więc permanentna aktualizacja oprogramowania oraz zachowanie ostrożności przy korzystaniu z Internetu. Ogromną rolę spełnia też odpowiedni tryb informowania użytkowników o nieprawidłowościach i zagrożeniach, żeby mogli im w porę zapobiec. Należy zatem najpierw budować możliwie najbezpieczniejszą infrastrukturę, a potem ustawicznie pracować nad edukacją jej użytkowników dla bezpieczeństwa.

Początkowo, 20 lat temu, zaczynałem od budowy prostych sieci P2P na skrętce pomiędzy komputerami stosowanymi w zarządzaniu szkołą. Ograniczenia tego rozwiązania i potrzeba połączenia ze sobą grup komputerów w sieć LAN oraz postęp technologiczny wpłynęły na decyzję budowy sieci o topologii pierścieniowo-gwiaździstej (kabel koncentryczny – skrętka). Do tak połączonych stacji w sieci zostały podpięte dwa serwery plików Novell NetWare 3.12 – osobno dla zarządzania i dla edukacji – wraz z aktywnymi urządzeniami sieci (hubami). To rozwiązanie zaspokoiło początkowe potrzeby zbudowanego wówczas informacyjnego

systemu wspierania edukacji i zarządzania. Uruchomienie w Lublinie akademickiej sieci komputerowej stworzyło możliwość podłączenia struktury szkolnej do globalnego systemu sieciowego, jakim stawał się Internet. Szkolna sieć komputerowa oparta o 25-stanowiskowy Novell NetWare została zbudowana w 1995 roku, a następnie rozbudowana o następny 50-stanowiskowy NetWare. W tym samym roku sieć szkolna została podłączona dzierżawionym łączem stałym do sieci Internet Lubmana. Głównym pretekstem do podłączenia się do światowej pajęczyny była możliwość ściągania z Biblioteki Narodowej w Warszawie informacji o pozycjach książkowych w reorganizującej się bibliotece szkolnej. Ówczesne połączenia modemami z providerem za pomocą stałych linii dzierżawionych o bardzo małej przepustowości zostały z czasem zastąpione szybszymi modemami, by w końcu uzyskać dostęp światłowodowy.

W początkowym okresie, ze względu na niszowy w tym czasie charakter rozwiązań technicznych, sprawy bezpieczeństwa sieci były drugoplanowe. Jednak wraz z upowszechnieniem Internetu wzrastała liczba zagrożeń. Wymagało to ciągłej modernizacji parku sprzętowego nie tylko ze względu na zużycie, ale i nowoczesność oraz pewność rozwiązań. Serwer Uniksowy Novella był drogi, więc do sieci zewnętrznej został podłączony za pomocą komputera działającego w systemie Linuks. Były tam uruchomione m.in. usługi typu router, firewall, serwer DNS, Proxy itd., które obecnie wykonywane są za pomocą dedykowanych rozwiązań sprzętowych. Na serwerze Novell NetWare uruchomiony został również serwer WWW.

Oczywiście, przy braku środków finansowych, rozważana była koncepcja wdrożenia w szkole Linuksa. Podjęte próby z czasem zaniechano, gdyż wymagało to dodatkowych umiejętności od posługujących się sprzętem pracowników i nauczycieli. Trudno im było uczyć się obsługi oprogramowania innego od tego, które mieli w domu. Rotacje kadrowe w szkole i hobbystyczna (*non profit*) działalność pracowników w zakresie pracy z Linuksem samoistnie ograniczyły liczbę urządzeń działających w tym systemie do wybranych rozwiązań w niektórych kategoriach. Pomimo że rozwiązania linuksowe są, jak się wydaje, najtańsze, to biorąc pod uwagę określone możliwości kadry szkoły oraz brak odpowiednio dużego i taniego wsparcia technicznego, szkoła wycofała się z Linuksa na rzecz systemów droższych, ale sprawdzonych i posiadających pełne i łatwo dostępne wsparcie techniczne.

Teza, aby w świetlicy zapoznawać uczniów z Linuksem, w kształceniu zintegrowanym z komputerami Macintosh, a dopiero potem z systemem Windows na razie nie może doczekać się realizacji, choć dzięki temu uczniowie nie mieliby w przyszłości żadnych kłopotów i obaw związanych z posługiwaniem się jakimikolwiek komputerami.

Mając na uwadze również wyżej wymienione względy, szkoła starała się o pracownie MEN z wyposażeniem w system Windows, gdyż Linuks jako darmowy system zawsze można było dodatkowo w komputerach doinstalować.

Od momentu otrzymania pierwszej pracowni w 2002 roku z programu MEN w szkole zaprzestano rozwoju systemów oferowanych przez firmę Novell, przechodząc na systemy firmy Microsoft. Zgodnie z programami ministerialnymi nauczyciele zostali objęci szkoleniami w zakresie użytkowania i administracji otrzymanych SBS-ów (*Small Business Server*).

Oferowane szkolenia pomagały w początkowej fazie użytkowania. Aby jednak w pełni wykorzystywać posiadane możliwości sprzętowe, administrator musiał poświęcić wiele czasu i pracy, która nie była dodatkowo opłacana.

Wzrastająca liczba komputerów i pracowni SBS wymagała dostosowania eksploatacji do zwiększającego się zapotrzebowania na rozwiązania szybkie, łatwe i nieskomplikowane w korzystaniu z nowych możliwości, jakie dawały coraz nowsze wersje pracowni.

Dużo więcej uwagi należało poświęcić zarówno zagrożeniom zewnętrznym, jak i wewnętrznym w szkolnej sieci. Już w 2004 roku podczas wystąpienia/warsztatów na III Ogólnopolskim Zjeździe Opiekunów Szkolnych Pracowni Internetowych w Mrozach na temat „Bezpieczeństwa dzieci w sieci" zwróciłem uwagę na wiele aspektów bezpieczeństwa wewnętrznego sieci – poczynając od wychowania uczniów dla bezpieczeństwa, na zabezpieczeniach sprzętu przed nieuprawnionym korzystaniem z treści internetowych kończąc.

Bezpieczeństwo szkolnej infrastruktury obejmuje zatem zarówno bezpieczeństwo informacji krążących w sieci, jak i tych zgromadzonych w bazach danych dostępnych za jej pośrednictwem. Zagrożenia związane z włamaniami do systemów wewnątrzszkolnych są tak znaczące, że środki ochrony poprzez ograniczenie dostępu do zasobów zgodnie z ustaloną polityką ochronną w szkole oraz utajnianie informacji za pomocą kryptografii są niezbędne i konieczne.

Zanim jednak poniesiemy duże nakłady finansowe na zabezpieczenia sprzętowe, musimy pamiętać, że sama technologia nie może zapewnić

pełnego bezpieczeństwa. Ochrona to przede wszystkim właściwe zarządzanie i organizacja.

Właściwa organizacja systemu ochrony obejmuje rozpoznanie jego obszaru oraz określenie (uświadomienie sobie), jak wygląda schemat sieci, punkty dostępowe, kto oraz jak z nich korzysta oraz jakie zasoby są na tyle ważne, aby je chronić, i gdzie są zlokalizowane?

Szkolenia wszystkich użytkowników sieci w szkole w zakresie takiej ochrony jest sprawą bezdyskusyjną, choć często nieuświadomioną (przez co zaniedbaną). Niezbędna jest zarówno stała współpraca agend szkolnych, jak również wspomaganie, zrozumienie i elastyczność wobec użytkowników końcowych – ucznia i nauczyciela. Proces edukacyjny powinien być dostosowany do oczekiwań i potrzeb każdej grupy w szkole, w przeciwnym razie ochrona będzie pomijana, ignorowana lub wyłączana.

Idealny system ochrony szkolnej sieci powinien być zdolny do wykrywania niektórych działań i zachowań pochodzących z zewnątrz i z wewnątrz, które mogą być uznane za podejrzane. Wykrywanie intruzów jest szczególnie ważne, gdy korzystamy z Internetu, choć, jak wynika z badań, prawdopodobnie połowa ataków jest powodowana przez osoby kiedyś związane z daną siecią od wewnątrz. Dlatego zawsze należy pamiętać o nadawaniu uprawnień użytkownikom stosownie do ich pozycji w szkole. Poza dyskusją powinno być włączanie beneficjentów systemu do ochrony, a nie czynienie z nich potencjalnych przeciwników. Przykładem może być tutaj sytuacja, w której dane księgowe i kadrowe są odłączone od sieci dla edukacji i Internetu. Pracownicy mają dodatkowy dostęp do tych zasobów z innych komputerów lub sieci. Koszty zapewnienia bezpieczeństwa są wtedy ułamkiem ewentualnych kosztów wynikłych ze strat powstałych przez brak zapewnienia pełnej ochrony. Jest to kolejny przykład, że technologia nie stanowi o wszystkim, a problem często można rozwiązać prostym działaniem organizacyjnym.

W sieciach rozległych jest wiele miejsc, z których hakerzy mogą penetrować sieć podsłuchem, rozprzestrzeniać wirusy, wykradać informacje, czy zakłócać ich pracę. Nie istnieją metody pełnej ochrony, a utrzymywanie całego arsenału środków nie jest rozsądne i przysparza kłopotów mających swe źródło w zmienności technologii i standardów. Dlatego należy ograniczyć się do ochrony ich granic.

Wraz z rozwojem Internetu i wzrostem liczby użytkowników uzyskujących dostęp do jego zasobów szczególnego znaczenia nabiera ochrona danych metodą kryptograficzną. Oprócz stosowania kart identyfikacyjnych, zamków elektronicznych czy zapór ogniowych, niezbędne staje się szyfrowanie znaczących informacji. Dostęp przez Internet do szkolnych zasobów edukacyjnych powoduje konieczność wprowadzania coraz lepszych zabezpieczeń (nie tylko poprzez odpowiednio spreparowane hasło do zasobów).

Oto aktualne elementy szkolnej infrastruktury informatycznej:

1. Serce infrastruktury – **serwer z Hyper-V 2008 R2 do wirtualizacji serwerów** (zdalnie zarządzany) znajduje się w klimatyzowanej serwerowni zabezpieczonej przed postronnymi osobami kontrolą dostępu i monitoringiem wejść. Umieszczone są w niej dwie szafy 42U 19". Zastosowany został UPS 5kVA do zasilania awaryjnego serwerowni i komputerów. Z każdego pomieszczenia doprowadzono bezpośrednio skrętkę komputerową. W szkole położono łączenie ponad 10 km skrętki. W całej szkole jest ponad 320 gniazd RJ45 umożliwiających dostęp do Internetu. Do połączenia światłowodowego wykorzystano 6-włóknowy kabel światłowodowy o łącznej długości 120 m. Pracownie komputerowe zostały połączone z serwerownią kablem światłowodowym (3 tory dwuwłóknowe).
   Wirtualizacja umożliwia oddzielenie wykorzystywanych zasobów sprzętowych od systemów i aplikacji, które z tych zasobów korzystają. Uruchomienie kilku wirtualnych maszyn na jednym serwerze fizycznym pozwala na zaoszczędzenie miejsca w serwerowni, ograniczenie kosztów zakupu nowych serwerów, redukcję kosztów zasilania i chłodzenia oraz lepsze wykorzystanie mocy obliczeniowej serwerów. W najbliższym czasie wszystkie serwery szkolne będą działał jako maszyny wirtualne.
2. **SBS 2003 i ISA Server**
3. **Router DUAL-WAN ETHERNET Draytek 2930 Vn**
4. **Routery bezprzewodowe: Draytek 2910 VG, Linksys WRT54GL**
5. **Zarządzalne switche**
6. **Pakiet przejścia (Transition Pack) Microsoft**
   Obecnie w szkole działa 5 serwerów SBS. Integracja pracowni jest tak przeprowadzana, aby wszystkie komputery uczniowskie były podłączone do jednego serwera. W tym celu został zakupiony pakiet przejścia dla systemu MS Windows SBS 2003 R2 Premium Edition z licencjami dostępowymi, który umożliwia zamianę

zainstalowanego (skonfigurowanego i działającego) serwera SBS na pełną wersję systemu serwerowego Windows Server 2003 R2 Standard Edition. Tym samym znosi wbudowane do systemu SBS ograniczenia, czyniąc go pełnoprawnym systemem serwerowym, dającym znaczne możliwości skalowalności w zależności od potrzeb. W szkolnych warunkach główną zaletą zastosowania pakietu przejścia jest zniesienie ograniczenia licencyjnego, niepozwalającego podłączyć do jednego serwera więcej niż 75 stacji roboczych.

7. **PCinfo MagicEYE 5.5**
Szkoła podsiada licencje na 120 stanowisk PCinfo® MagicEYE. W wersji STANDARD zawiera moduły:
audyt i ewidencja oprogramowania,
audyt i ewidencja sprzętu,
zarządzanie licencjami,
zdalne instalacje,
zdalne sterowanie.
Jest to rozbudowany system do audytu oprogramowania i zarządzania zasobami IT. PCinfo® MagicEYE umożliwia przeprowadzanie bardzo szczegółowej ewidencji posiadanych komputerów, podzespołów komputerowych i innych urządzeń informatycznych, a także precyzyjne wykrywanie zainstalowanego w komputerach oprogramowania (opcjonalnie także plików graficznych, muzycznych czy filmów). Wszelkie dane pobierane są z instalowanych zdalnie agentów rezydujących na poszczególnych końcówkach sieci i wyświetlane na stanowisku administratora. Możliwe jest także sprawdzanie komputerów pracujących pod kontrolą systemu Linuks. Program umożliwia wprowadzenie liczby posiadanych licencji na oprogramowanie, dzięki czemu można w łatwy sposób wychwycić ewentualne różnice, a także sprawdzić, w których konkretnie komputerach zainstalowane jest dane oprogramowanie.

MagicMONITOR umożliwia:
• monitoring wykorzystania aplikacji
– które uruchomił konkretny użytkownik,
jak długo były one uruchomione,
jak długo użytkownik z nich korzystał (były „on top"),
z jakimi plikami pracował,
liczba uderzeń w klawiaturę i kliknięć myszką w każdej aplikacji,
z kim czatowano przez komunikatory internetowe,
• monitoring WWW:
jakie serwery i strony odwiedzał użytkownik PC,
ile czasu z nich korzystał,
z jakiej przeglądarki internetowej korzystał.

8. **Program antywirusowy – wersja sieciowa**
Moduły wchodzące w skład aplikacji:
serwer,
moduł zarządzający ochroną antywirusową sieci,
administrator,
aplikacja zarządzająca modułem serwera,
WebAdministrator,
aplikacja do zarządzania ochroną sieci przez WWW,
klient AntiVirus,
moduł chroniący komputery końcowe.
Antywirus oferuje w pełni automatyczną ochronę sieci przed wirusami i złośliwym oprogramowaniem. Umożliwia zdalną instalację, automatyczną aktualizację, a także zdalną modyfikację ustawień ochrony antywirusowej. Antywirus rozpoznaje i blokuje wirusy, rootkity, robaki, spyware, trojany, backdoory. Chroni prywatność podczas wykonywania płatności online, blokując wszelkie próby wyłudzenia danych. Uniemożliwia zainfekowanie systemu, dzięki czemu komputer zawsze działa szybko i stabilnie.

9. **Technologia iPAT 3.1**
Technologia iPAT chroni, po włączeniu, zawartość dysku twardego (wybranych partycji) przed nieupoważnionymi trwałymi zmianami. W czasie użytkowania komputera działanie zabezpieczenia jest niewidoczne (transparentne) – po każdym restarcie komputera oryginalna chroniona zawartość jest automatycznie przywracana. Niestety iPAT 3.1 działa tylko z płytą główną INTEL D946GZAB (pracownia EFS z roku 2008 – 10 komputerów).

10. **Karta przywracania**
Karta ta, to urządzenie montowane w slocie PCI, zabezpieczające twardy dysk przed niekontrolowanymi zmianami. Posiada kilka elastycznych trybów przywracania: automatyczny, manualny, cykliczny, rezerwowania danych. Może chronić wiele partycji.
Posiada funkcję modernizacji/uaktualniania danych – w każdej chwili można dodawać nowe programy komputerowe, które muszą być koniecznie chronione. Posiada funkcję zabezpieczania przed zmianami konfiguracji BIOS – tutaj również działa funkcja przywracania.
Niestety, karta nie była jeszcze dopracowana – testy zakończyły się utratą systemu i koniecznością jego ponownej instalacji. Nie z każdą płytą główną działa poprawnie.

11. Uczniowie są chronieni przed niepożądanymi treściami z Internetu następującymi programami zabezpieczającymi:
Beniamin,
Opiekun ucznia,
NetSupport School NSS 10".
Beniamin oraz Opiekun Ucznia blokują, dzięki zaawansowanym filtrom, dostęp do niepożądanych stron. Programy te wymagają szczególnego nadzoru i mogą wprowadzać problemy w codziennym korzystaniu z komputerów, które chronią. NetSupport School został zainstalowany na 27 stanowiskach komputerowych i pozwala na zdalny podgląd komputerów, z których korzystają uczniowie, kontrolę użytkowanych aplikacji i stron internetowych. Dzięki temu nauczyciel, nie wstając od biurka, ma kontrolę nad pracą uczniów. NetSupport School jest programem do wspomagania nauczania w skomputeryzowanej klasie, zapewniającym nauczycielowi możliwość nauczania, nadzorowania oraz współpracy z uczniami, zarówno indywidualnie, jak i grupowo.

Infrastruktura informatyczna powinna nadążać za wzrastającymi potrzebami społeczności szkolnej, która świadomie rozszerza krąg swoich zainteresowań o coraz to nowe możliwości zastosowania komputera w edukacji. Szkoła już od ponad roku dostosowuje do własnych potrzeb platformę edukacyjną Fronter, badamy funkcjonalność Microsoft Live@edu, wykorzystujemy Moodle. A więc poprzeczka bezpieczeństwa musi być zawieszona bardzo wysoko.

Autor jest dyrektorem Szkoły Podstawowej nr 21 im. Królowej Jadwigi w Lublinie
http://piskor.pl

Przemoc występująca w grze ma bardziej dosadny charakter, skierowana jest jednak na postaci fantastyczne lub w nierealistyczny sposób przedstawia przemoc skierowaną na postaci ludzkie, jak np. w grach RPG (komputerowa gra fabularna), osadzonych w fantastycznych światach. Ewentualne wulgaryzmy muszą mieć łagodny charakter i nie mogą zawierać odwołań do seksu.

Przykładowe gry z tej grupy: Cywilizacja IV, Guitar Hero III, World of Warcraft.

Przedstawione w grze przemoc i aktywność seksualna bohaterów wyglądają jak w prawdziwym życiu. Pojawia się bardziej dosadny język, sceny spożywania alkoholu i tytoniu, zażywania narkotyków oraz popełniania przestępstw.

Przykładowe gry z tej grupy: Star Wars: TFU, Final Fantasy XII, Far Cry 2.

Janusz Wierzbicki

Bezpieczeństwo dziecka w pracy przy komputerze i w sieci Internet – monitoring i ograniczanie dostępu do treści niepożądanych

Jednym z najważniejszych zadań stojących dzisiaj przed opiekunami małego ucznia, zarówno w domu, jak i w szkole, jest zapewnienie bezpiecznego korzystania z komputera oraz sieci Internet. Zagadnienia związane z bezpieczeństwem mają oczywiście bardzo szeroki zakres. W niniejszym artykule skupiłem się na bardzo konkretnych kwestiach dotyczących ograniczenia dostępu do treści niepożądanych oraz monitoringu dostępu do sieci Internet przez najmłodszych uczniów. Omówione w artykule bezpłatne Bezpieczeństwo Rodzinne usługi Windows Live może zainstalować i skonfigurować każdy nauczyciel i/lub rodzic w komputerach pozostających pod jego opieką a wykorzystywanych przez dzieci i młodzież. Jest to jedna z wielu usług sieci społecznościowej Windows Live, oferującej między innymi takie funkcje, jak: prowadzenie blogów, przechowywanie do 25 GB danych na dysku sieciowym, obsługę darmowych kont pocztowych o pojemności do 10 GB danych, galerie fotografii, kalendarze internetowe, tworzenie grup użytkowników, korzystanie z komunikatora internetowego z rozbudowanymi możliwościami komunikacji audio/wideo oraz gier online. Z usługami skojarzony jest zestaw aplikacji instalowanych w komputerze a dostępnych do pobrania za darmo w sieci. Bezpieczeństwo Rodzinne może stanowić, wraz z wbudowanymi w Windows Vista/Windows 7 mechanizmami kontroli rodzicielskiej, kompletne narzędzie ochrony i monitoringu naszych podopiecznych.

Wskazówka: Warto zwrócić uwagę, że także inne współczesne systemy operacyjne coraz częściej posiadają wbudowane różnego rodzaju mechanizmy ochrony rodzicielskiej. W niniejszym artykule skupiam się na systemie Windows, gdyż około 93% pracowni szkolnych działa obecnie pod jego kontrolą.

Bezpieczeństwo Rodzinne usługi Windows Live

Bezpieczeństwo Rodzinne usługi Windows Live składa się właściwie z dwóch części: aplikacji, którą instalujemy w chronionych komputerach, oraz serwisu działającego w sieci na serwerach firmy Microsoft. Aplikacja jest darmowa, pobiera się ją i instaluje w każdym komputerze, na którym pracować będą chronieni podopieczni.

W celu instalacji i konfiguracji oprogramowania należy założyć swoje konto – identyfikator w usłudze Windows Live (tzw. Windows Live ID). Identyfikator ten pozwoli nam skonfigurować usługę i kontrolować, co nasi podopieczni robią na komputerach.

Wskazówka: Istnieje specjalna wersja usługi Windows Live@edu przeznaczona dla szkół i uczelni wyższych. Jest całkowicie darmowa i pozwala korzystać z usług Windows Live w domenie szkoły, oferując jednocześnie dla każdego ucznia 10 GB miejsca na profesjonalnym koncie pocztowym w systemie Exchange. Z punktu widzenia szkoły jest to bardzo ciekawa oferta, gdyż likwiduje koszty utrzymania własnych serwerów lub kont pocztowych u płatnych dostawców, oferując jednocześnie możliwość zarządzania kontami uczniów i pracowników szkoły oraz mnóstwo usług dodatkowych, standardowo stanowiących część Windows Live. Gdy szkoła korzysta z tej wersji usługi, wówczas do zarządzania usługą bezpieczeństwa nauczyciele mogą wykorzystać konta założone w domenie szkolnej, gdyż są one pełnoprawnym identyfikatorem we wszystkich usługach Windows Live oraz usługach powiązanych. Więcej informacji na temat usługi Windows Live@edu znajduje się na stronie: http://microsoft.pl/edukacja.

Zarówno instalacja oprogramowania, jak również jego konfiguracja i posługiwanie się nim w celu kontrolowania podopiecznych są bardzo proste i nie jest wymagają od użytkownika żadnej „tajemnej" wiedzy informatycznej.

Jakie funkcje udostępnia Bezpieczeństwo Rodzinne usługi Windows Live?

Bezpieczeństwo Rodzinne usługi Windows Live pozwala decydować o tym, z jakich zasobów Internetu skorzystają uczniowie. Można ograniczyć możliwości wyszukiwania, monitorować i blokować witryny sieci Web lub zezwalać na ich wyświetlanie. Dodatkowo istnieje możliwość decydowania, z kim nasi podopieczni mogą się kontaktować za pomocą programu Messenger.

Jeśli uczniowie są zalogowani za pomocą własnych ustawień konta systemu Windows, to każdy z nich ma inne ustawienia, a my uzyskujemy różne raporty i filtry dotyczące poszczególnych dzieci.

Filtrowanie sieci Web pomaga chronić uczniów przed zawartością, której nie powinni oglądać. Dla każdego podopiecznego można zastosować inne ustawienia, jak również powielać ustawienia wcześniej zdefiniowane.

W szczegółowych raportach aktywności są wyświetlone wszystkie witryny sieci Web, które odwiedziły (lub próbowały odwiedzić) poszczególne dzieci, programy, których używały, oraz czas, jaki spędziły przy komputerze.

Sterowanie odbywa się przez stronę internetową Bezpieczeństwa Rodzinnego usług i Windows, gdzie można dostosować ustawienia bezpieczeństwa każdego dziecka oraz monitorować jego aktywność.

Jakie kroki należy wykonać, by zainstalować i skonfigurować Bezpieczeństwo Rodzinne usługi Windows Live?

Procedura może wydać się skomplikowana, ale nie należy się tym zniechęcać. W razie potrzeby dodatkowe informacje dotyczące zakładania kont, instalacji i konfiguracji Bezpieczeństwa Rodzinnego usługi Windows Live można uzyskać na prowadzonym przeze mnie blogu (http://www.pdp.edu.pl/pdp/k12) na stronach „Partnerstwa dla Przyszłości".

Czytelnicy znajdą tam pomoc w postaci filmów instruktażowych oraz dodatkowych materiałów pisemnych, omawiających wspomnianą powyżej procedurę punkt po punkcie.

Krok pierwszy

Zanim rozpoczniemy inne działania, musimy założyć konto (identyfikator) w usłudze Windows Live. W tym celu należy przejść na stronę http://home.live.com, następnie odszukać i wybrać przycisk „Zapisz mnie". Dalej należy postępować zgodnie ze wskazówkami zawartymi w formularzu rejestracyjnym.

Wskazówka: Identyfikatorem w usłudze Windows Live jest zawsze adres e-mail. Podczas rejestracji jako identyfikator można wykorzystać posiadany adres e-mail lub założyć nowy adres (w domenie hotmail.com lub live.com). Jeżeli założymy nowy adres, wówczas będziemy mogli skorzystać ze wszystkich usług oferowanych w ramach Windows Live – zdecydowanie polecam tę wersję. Jeśli posiadamy już identyfikator Windows Live lub szkoła założyła dla nas konto w ramach usług Windows Live@edu, ten krok pomijamy.

Krok drugi

W każdym z komputerów, w których zabezpieczenie ma działać, dla uczniów objętych kontrolą należy założyć zwykłe konta (bez uprawnień administracyjnych). Dodatkowo w każdym z komputerów konta z uprawnieniami administracyjnymi powinny zostać zabezpieczone hasłem, którego podopieczni nie znają i nie będą mieli szansy zgadnąć.

Uwaga: Jeżeli konta uczniów będą posiadały uprawnienia administratorskie lub będą mieli oni dostęp do konta posiadającego takie uprawnianie, wówczas będą mogli wyłączyć wszelkie zabezpieczenia i monitoring.

Wskazówka: Jeżeli chcemy kontrolować każdego ucznia oddzielnie, ustawiać indywidualne pozwolenia i śledzić, co robił na komputerze, jakie strony przeglądał, z jakich programów korzystał, należy założyć oddzielne indywidualne konto dla każdego użytkownika z indywidualnie ustawionym hasłem. Jest to sposób zalecany i najwłaściwszy. Jednak w przypadku komputerów funkcjonujących w szkole na zasadzie wypożyczania na poszczególne lekcje, komputerów, z których korzysta bardzo wielu uczniów, a które nie mają zarządzania centralnego ze strony serwera, założenie indywidualnego konta z oddzielnym hasłem może być bardzo trudne lub praktycznie niemożliwe. Wówczas należy założyć konto ucznia dostępne dla wszystkich uczniów w danej szkole (lub np. oddzielne konta dla każdej klasy) i nałożyć odpowiednie, wspólne dla uczniów ograniczenia. Należy jednak pamiętać, że mamy ograniczoną możliwość monitorowania

poczynań poszczególnych uczniów, jeżeli nie śledzimy na bieżąco, który z nich używa konkretnego komputera w danej chwili.

Krok trzeci

W każdym komputerze pobieramy i instalujemy program Bezpieczeństwo Rodzinne usługi Windows Live. Program dostępny jest pod adresem http://get.live.com lub http://download.live.com.

Wskazówka: Program jest jedną z kilku dostępnych do pobrania aplikacji. Wyboru, które aplikacje chcemy zainstalować, można dokonać dopiero po rozpoczęciu procesu instalacji.

Krok czwarty

Po instalacji oprogramowania musimy je skonfigurować, co polega zasadniczo na dwóch czynnościach. Pierwsza z nich, to podanie identyfikatora, którego właściciel będzie zarządzał Bezpieczeństwem Rodzinnym usługi Windows Live przez dany komputer. Zazwyczaj jest to identyfikator nauczyciela lub rodzica. Druga czynność polega na wskazaniu kont dzieci, które mają zastać objęte zabezpieczeniami.

W przypadku gdy wcześniej już instalowaliśmy i konfigurowaliśmy oprogramowanie w innym komputerze, gdzie wskazaliśmy konta dzieci, system spróbuje je dopasować do kont założonych w komputerze obecnie używanym. Konfiguracja kont jest znacznie łatwiejsza, gdy te same osoby (uczniowie) używają kilku komputerów na zmianę. Jeżeli nazwy kont będą się zgadzały we wszystkich komputerach, wówczas wystarczy potwierdzić automatyczne dopasowanie nazw przez usługę.

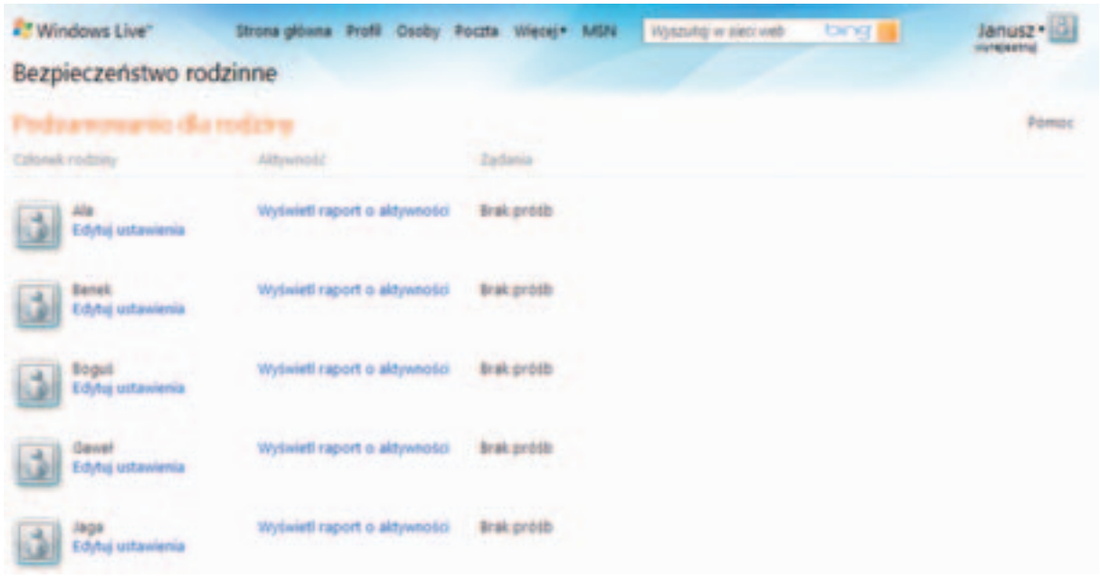
Krok piąty

Konfiguracja działania usługi odbywa się poprzez serwis internetowy, do którego możemy się dostać bezpośrednio z adresu: http://fss.live.com. Jeśli wcześniej nie logowaliśmy się do usług Windows Live, podczas łączenia z serwisem zostaniemy zapytani o nasz identyfikator oraz hasło. Należy użyć tego samego identyfikatora co w kroku czwartym.

Zarządzanie usługami

Po zalogowaniu się w serwisie Bezpieczeństwa Rodzinnego usługi Windows Live uzyskujemy dostęp do ustawień oraz informacji na temat kont naszych uczniów objętych ochroną.

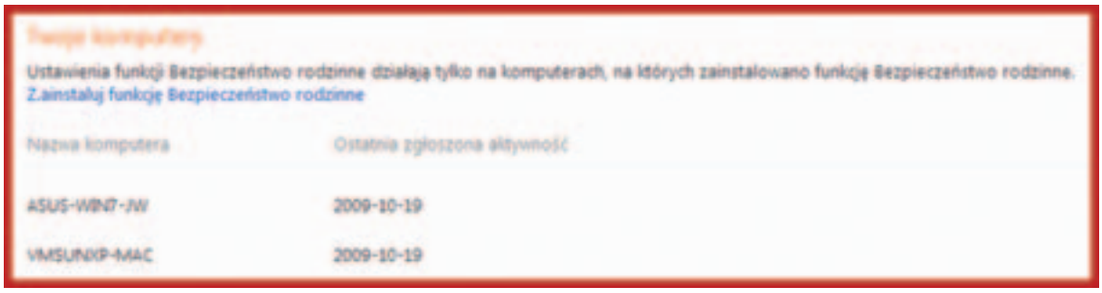
Na głównej stronie znajdują się dwie główne sekcje. Pierwsza zawiera listę kont objętych ochroną (tzw. podsumowanie dla rodziny).



Rys. 1. Lista dzieci

Przy każdym członku rodziny mamy hiperłącze zatytułowane „Edytuj ustawienia" oraz „Wyświetl raport aktywności" oraz w dalszej kolejności ewentualne żądania dostępu do zabronionych stron.

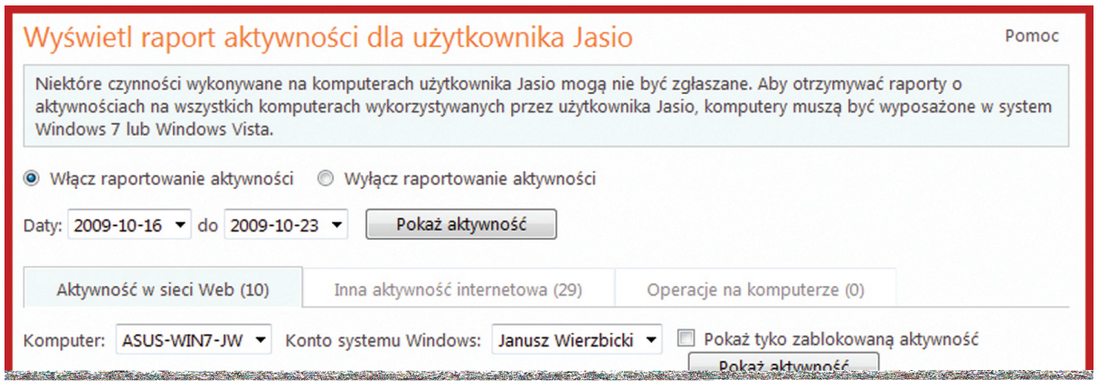
Druga sekcja zawiera listę komputerów, w których zostało zainstalowane Bezpieczeństwo Rodzinne wraz z podaniem ich ostatniej aktywności.



Rys. 2. Lista komputerów

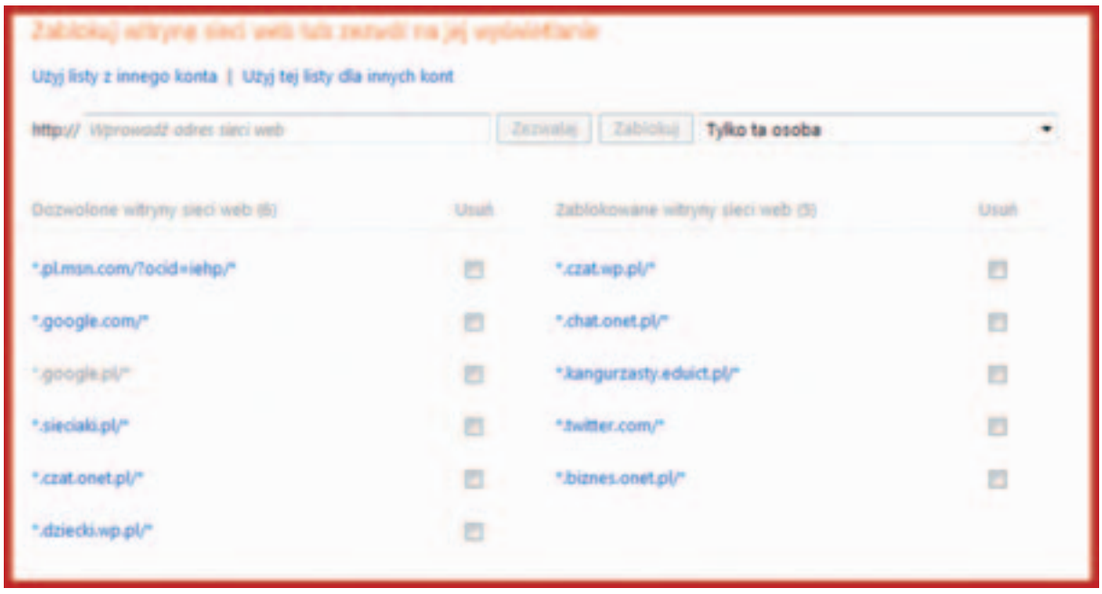
Po kliknięciu „Wyświetl raport aktywności" przejdziemy do szczegółowego raportu dotyczącego danej osoby. W zależności od systemu operacyjnego raport będzie bardziej lub mniej szczegółowy (pełna funkcjonalność dostępna jest dla systemu Windows Vista oraz Windows 7). Jednakże podstawowe dane zawsze będą dostępne, pod warunkiem że raportowanie nie zostało wyłączone (domyślnie jest ono włączone). Na stronie możemy wybrać przedział czasu, dla którego chcemy przeglądać aktywności danego użytkownika (nie dłuższy niż 30 dni wstecz), typ aktywności (zawsze dostępna jest „Aktywność w sieci Web") oraz komputer i/lub konto systemowe, na którym pracowała interesująca nas osoba.

Po zatwierdzeniu naszego wyboru widzimy listę aktywności danej osoby, zgodnie z wybranymi warunkami. W „Aktywności w sieci Web" domyślnie widzimy wszystkie odwiedzane adresy internetowe, grupowane do głównego adresu danego serwisu. Zawsze możemy obejrzeć szczegóły, po wybraniu strzałki znajdującej się po lewej stronie adresu głównego, powodującej rozwinięcie zgrupowanych informacji, gdzie widzimy, o której godzinie nasz podopieczny próbował się z danym adresem połączyć. Wyświetlona jest również informacja, czy połączenie zostało zaakceptowane lub zablokowane oraz ile prób łączności było podejmowanych. Ostatnią opcją jest możliwość zmiany danego ustawienia. Mianowicie wybrany adres internetowy możemy udostępnić lub zablokować dla danego podopiecznego lub dla wszystkich kont objętych ochroną. W zdecydowany sposób ułatwia to tworzenie list adresów dozwolonych lub zablokowanych dla naszych uczniów.



Rys. 3. Lista aktywności blokowanych i dozwolonych

Jeżeli na stronie głównej wybierzemy „Edytuj ustawienia" przy nazwie któregoś podopiecznego, przejdziemy do strony zawierającej zestawienie wszystkich możliwości administracyjnych go dotyczących. Najczęściej używana będzie jednak opcja „Filtrowanie zawartości sieci Web", gdzie możemy wybrać rodzaje (kategorie) serwisów, do których dany uczeń będzie miał dostęp, włączyć odpowiednie tryby filtrowania lub szczegółowo określić listę stron dozwolonych lub zablokowanych. Szczególnie ostatnia opcja może być bardzo przydatna wobec najmłodszych użytkowników Internetu, gdyż możemy szczegółowo określić, z jakich serwisów będą mogli korzystać.



Rys. 4. Lista blokowanych i dozwolonych stron internetowych

Obie listy możemy definiować ręcznie, wpisując adres serwisu w polu http://, a następnie wybierając, dla kogo definiujemy dany adres (dla konkretnego ucznia, dla wszystkich dzieci objętych ochroną lub dla wszystkich bez wyjątku) oraz klikając „Zezwalaj" lub „Zablokuj", wybrać, na której liście adres powinien się znaleźć.

Na tych listach będą również zamieszczane adresy zablokowane lub dozwolone w czasie aktywności naszych podopiecznych.

Dla każdego z użytkowników możemy również wybrać listę zgłoszonych przez niego żądań dostępu do określonych adresów.

Po wybraniu żądań danego użytkownika widzimy, o dostęp do jakich adresów prosi i możemy podjąć decyzję, czy chcemy udostępnić dany adres (tylko jemu lub wszystkim uczniom) lub nadal go blokować.

Rys. 5. Lista żądań użytkownika

Zakończenie

Opisane w niniejszym artykule funkcje Bezpieczeństwa Rodzinnego usługi Windows Live to tylko część dostępnych opcji. W połączeniu z mechanizmami ochrony i monitoringu wbudowanymi w systemy Windows Vista oraz Windows 7 oraz oprogramowaniem antywirusowym mogą stanowić wystarczająco dobre zabezpieczenie naszych uczniów przed dostępem do niewłaściwych materiałów i treści zarówno w domu, jak również na samodzielnych szkolnych stanowiskach komputerowych. Dzięki prostocie instalacji, konfiguracji i użytkowania stanowią warte rozważenia rozwiązanie ochronne.

Więcej informacji na temat usług Windows Live oraz w szczególności Windows Live@edu, Bezpieczeństwa Rodzinnego usługi Windows Live można uzyskać na stronach: http://microsoft.pl/edukacja oraz http://www.pdp.edu.pl/pdp/k12.

Autor jest pracownikiem firmy Microsoft

UWAGA! Dlaczego automatyczna ochrona jest konieczna, ale niewystarczająca?

Warto pamiętać, że aplikacje blokujące dostęp do treści nigdy nie będą zapewniały pełnej ochrony. Dzieje się tak z dwóch powodów – w zależności od sposobu ich działania.

- Pierwszy z nich polega na korzystaniu ze specjalnie przygotowanych czarnych list (*BlackLists*) stron zakazanych. Jednak każdego dnia powstaje wiele nowych adresów internetowych, wiele przestaje istnieć, dlatego możemy mieć praktycznie pewność, że nawet bardzo często aktualizowane listy nie obejmą wszystkich zakazanych serwisów internetowych.
- Drugi sposób działania, to określenie kategorii stron zabronionych na podstawie wyrazów-kluczy znajdujących się w słownikach.

Metody te, mimo iż coraz lepsze, nadal są niedoskonałe i mogą blokować całkowicie bezpieczne, a nawet rekomendowane do użytku przez dzieci strony. Mogą także zdarzać się pomyłki w drugą stronę, co oznacza dostęp do stron niepożądanych.

- Trzeci sposób, to poleganie na kategoriach określanych przez samych twórców stron – jednak ze względu na to, że autorom stron zawierających treści zakazane niekoniecznie zależy na blokowaniu komukolwiek dostępu do nich, jest to nadal bardzo zawodna metoda.

Wniosek jest bardzo prosty – oprócz stosowania automatycznych mechanizmów ochrony przed dostępem do treści niepożądanych i szkodliwych, bardzo ważne jest zapewnienie stałego nadzoru dziecku/uczniowi pracującemu z komputerem i siecią Internet. Mechanizmy automatyczne mają na celu zminimalizowanie szans przypadkowego wejścia przez dziecko na strony niepożądane. Jednakże tylko w połączeniu ze stałą opieką mogą stanowić jeden ze środków zapobiegawczych. Zawsze najważniejsze jest kontrolowanie bezpieczeństwa uczniów oraz uświadamianie im zagrożeń w sposób dostosowany do ich wieku.

Artur Rudnicki

BlackLists – sposób na darmowy filtr treści niepożądanych w polskich szkołach

W dobie wszechobecnego dostępu do Internetu konieczna jest ochrona najmłodszych użytkowników przed treściami niepożądanymi. W domu możemy zrealizować to za pomocą oprogramowania bezpłatnego dla użytkowników prywatnych, ale jak zapewnić taką ochronę w szkołach? Jest oczywiście wiele rozwiązań tego problemu.

Pierwszym możliwym sposobem jest przeniesienie rozwiązania domowego, czyli, uogólniając, zainstalowanie oprogramowania w każdym komputerze w szkole. Gdzie jest haczyk? Po pierwsze musimy to zrobić w każdym komputerze w szkole oddzielnie. Wiąże się to z taką sytuacją: opiekun pracowni, przy często zmienianym oprogramowaniu, co miesiąc instaluje oprogramowanie w każdym komputerze w szkole. Po drugie, za takie rozwiązanie trzeba zapłacić, bowiem szkoła nie jest użytkownikiem prywatnym, który może z takiego oprogramowania korzystać za darmo.

Druga możliwością jest uruchomienie tzw. strażnika całej sieci komputerowej szkoły. Opiekun pracowni nie musi instalować oprogramowania w każdym z komputerów w szkole, ale zarządza strażnikiem z jednego miejsca. Czy takie rozwiązanie jest darmowe? Raczej nie, więc znów jest to wydatek dla szkoły, której często na to po prostu nie stać.

Na kolejną ewentualność w szczególności chciałbym zwrócić uwagę Czytelników, ale zanim przejdę do konkretów, parę informacji ogólnych. Polskie szkoły w latach 2005-2008 zostały wyposażone w sprzęt oraz oprogramowanie wysokiej klasy. Wśród całej masy oprogramowania i sprzętu jest takie, które swobodnie możemy zastosować do opisywanych celów. Jest to Windows Small Bussines Server 2003 Premium Edition, a właściwie jego składnik, czyli Internet Security Administration 2004 (w skrócie ISA 2004). Jest to *firewall*, który stoi na straży całej szkolnej pracowni komputerowej. To dzięki niemu możemy dawać i odbierać uprawnienia dostępu do zasobów w sieci Internet użytkownikom naszej sieci, więc możemy blokować dostęp także do stron, których treści są niepożądane. I tu kolejne pytanie: jak blokować kilkaset tysięcy adresów internetowych i skąd je brać, jak je aktualizować? Znów stajemy przed problemem, jak wprowadzać dane do naszego ISA 2004, ręcznie? Przez pewien czas, niestety, tak to się odbywało – administrator ręcznie wprowadzał adresy stron, aż powstał program BlackLists.

Program BlackLists jest programem ułatwiającym wprowadzanie reguł blokujących dostęp do stron niepożądanych na podstawie tzw. BlackLists, czyli publikowanych plików tekstowych, zawierających adresy serwisów oferujących dostęp do treści takich jak pornografia.

Dzięki programowi administrator w prosty sposób może importować pliki z adresami do swojego serwera ISA i za ich pomocą blokować dostęp do nich wybranym przez siebie użytkownikom.

Autorem programu jest Maciej Rusinek, który udostępnił go dla polskich szkół na podstawie niżej zamieszczonej licencji.

1. Autor nie ponosi odpowiedzialności za jakiekolwiek koszty, szkody lub straty wynikłe z użytkowania programu.
2. Jeśli użytkownik decyduje się użytkować program, zakłada się, że wypróbował wcześniej działanie programu i upewnił się, że jest on dostosowany do wymagań posiadanego sprzętu i oprogramowania.
3. Program jest tylko narzędziem, importującym listy domen oraz adresów URL do ISA Server 2004 oraz tworzącym reguły powodujące blokowanie dostępu do zaimportowanych adresów. Nie stanowi kompletnego rozwiązania i nie może być z takim utożsamiany.

4. Autor programu nie ponosi odpowiedzialności za wybór blokowanych adresów – ich dobór oraz import leży całkowicie po stronie użytkownika.
5. Autor nie zgadza się na rozpowszechnianie programu w połączeniu z już zaimportowanym konkretnym zestawem blokowanych adresów.
6. Ta wersja programu przeznaczona jest tylko dla szkolnych serwerów SBS 2003 zainstalowanych z następujących DVD Kolekcji:
   - DVD Kolekcja Jesień 2005
   - DVD Kolekcja Wiosna 2007
   - DVD Kolekcja Lato 2007
   - DVD Kolekcja Jesień 2007

Należy tu zaznaczyć, że program jest narzędziem ułatwiającym wprowadzanie BlackLists, ale nie jest dostarczany z żadnym plikiem zawierającym adresy do blokowania. Takie pliki należy pobrać z ogólnie dostępnych serwisów internetowych.

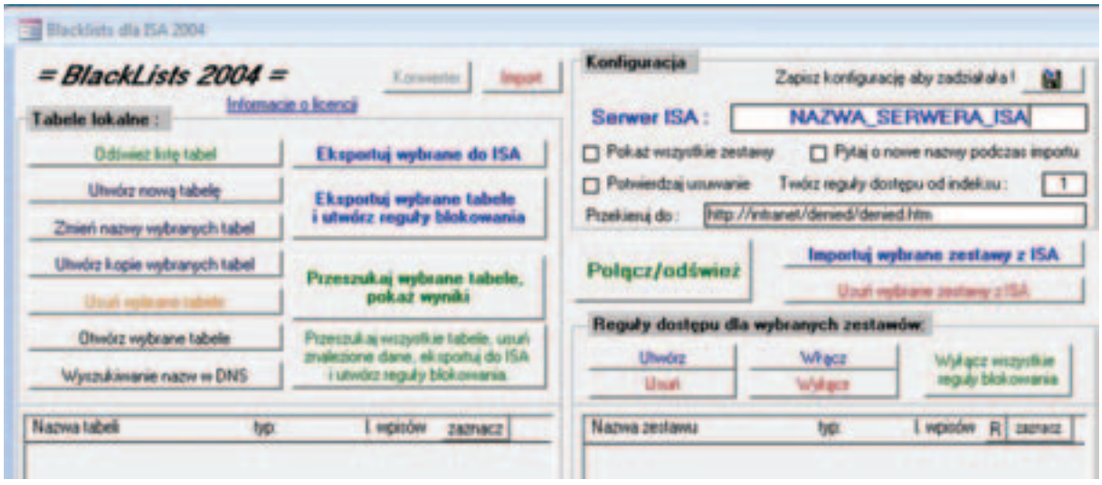
Biorąc pod uwagę powyższe, przedstawię w skrócie, jak wdrożyć ww. program w szkole.

Pierwszą czynnością administratora po zalogowaniu do serwera SBS 2003 powinno być pobranie programu BlackLists ze strony autora, czyli: http://blacklists.w.interia.pl/index_b2004.htm.

Po pobraniu i zapisaniu (pobieramy plik zip) musimy go rozpakować do postaci blacklists2004-1.3PL.mde. Jest to aplikacja uruchamiana dzięki MS Access, więc musimy mieć zainstalowany ten program.

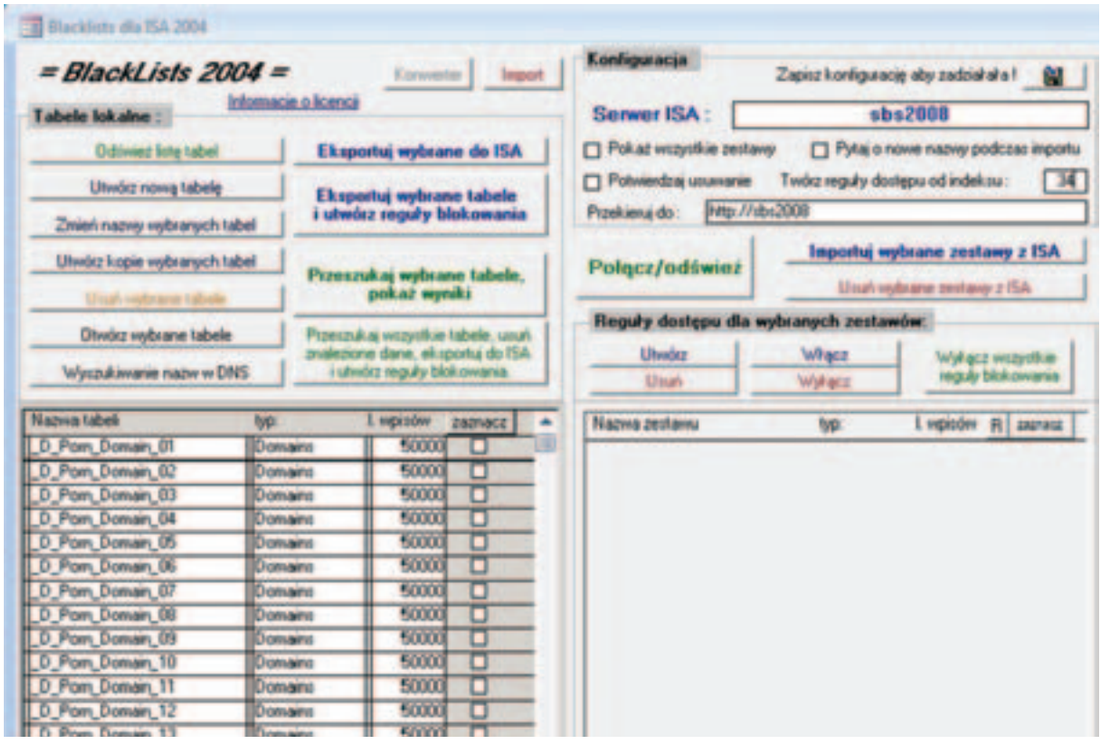
Kolejna czynność, to pobranie listy stron zakazanych z sieci Internet. Możemy to zrobić ze strony http://www.shallalist.de.

Kolejną stroną, z której pobierzemy listę stron zakazanych może być http://www.squidguard.org/blacklists.html. Po pobraniu listy stron zakazanych musimy rozpakować archiwum i znaleźć interesujące nas strony. W naszym przypadku będzie to folder porn. Aby program BlackLists mógł zaimportować zapisane w plikach adresy, musimy zmienić rozszerzenia na txt. W wyniku zmiany rozszerzeń dostaniemy dwa pliki, o nazwach odpowiednio domains.txt i urls.txt. Tak przygotowani możemy uruchomić blacklists2004-1.3PL.mde.

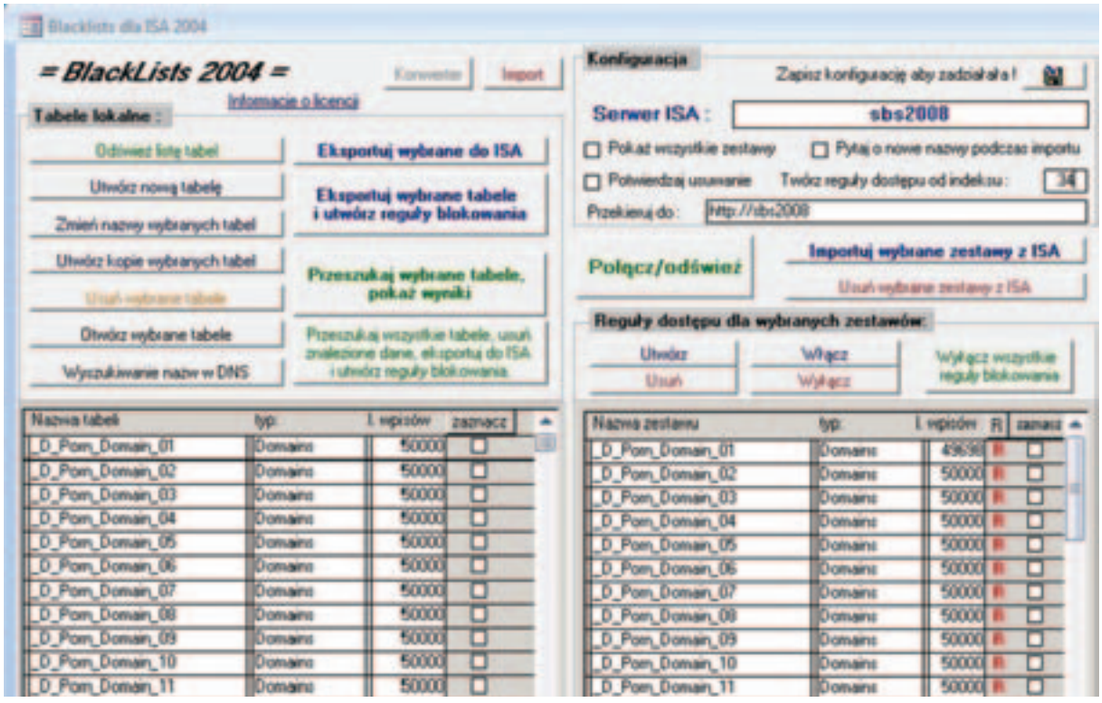


Jak widzimy po lewej stronie, nie posiadamy jeszcze w bazie danych żadnych adresów stron. Należy teraz w sekcji Serwer ISA podać nazwę swojego serwera, np. SBS2008, a następnie zapisać konfigurację, klikając ikonę dyskietki.

Kolejnym krokiem jest import listy stron niepożądanych. Wciskamy „Import", a następnie wskazujemy wcześniej przygotowane pliki z rozszerzeniem txt. Po zaimportowaniu listy stron widok powinien być następujący:



Teraz wystarczy tylko wyeksportować wybrane tabele, utworzyć reguły blokowania i już powinniśmy mieć zablokowanych około 800 000 niechcianych stron. Należy pamiętać przed eksportowaniem tabel do ISA o tym, aby wprowadzić przedostatni nr naszych reguł w sekcji: „Twórz reguły dostępu od indeksu", kliknąć „Połącz/Odśwież", no i oczywiście zaznaczyć tabele, które chcemy eksportować. Po kliknięciu w „Eksportuj wybrane tabele i twórz reguły blokowania" widok naszej bazy powinien być następujący:



Jak widzimy, strony niechciane zostały poprawnie wyeksportowane do naszego serwera ISA, a czerwona litera R oznacza, że reguła jest aktywna. Teraz około 800 000 stron, których nie chcemy w naszej sieci, jest zablokowanych. Pełna instrukcja oraz wsparcie dla programu BlackLists znajdują się na stronie internetowej http://sbs.oeiizk.edu.pl/blacklists.

Nasuwa się pytanie: czy tak skonfigurowanego systemu nie da się oszukać? Oczywiście, że się da. W sieci istnieje wiele możliwości, a jedną z nich jest maskowanie otwieranego adresu internetowego poprzez tzw. anonimowe Proxy. Rozwiązanie problemu jest jednak bardzo proste. Stosując program BlackLists, należy zblokować także i anonimowe Proxy.

Autor jest wicedyrektorem Zespołu Szkół Technicznych im. Tadeusza Kościuszki w Radomiu, nauczycielem przedmiotów informatycznych

W programie przedstawiona jest daleko posunięta przemoc (przez PEGI określana jako „sceny przemocy powodujące u widza uczucie odrazy".

Przykładowe gry z tej grupy: Gears of War, Wiedźmin, Ojciec chrzestny.

Dariusz Stachecki

Dziennik elektroniczny w szkole

Prawne i organizacyjne aspekty bezpiecznego wdrażania i funkcjonowania elektronicznej dokumentacji szkolnej

Rozporządzenie Ministra Edukacji Narodowej z dnia 16 lipca 2009 roku zmieniające rozporządzenie w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej (...) dało możliwość prowadzenia przez szkoły dzienników w postaci elektronicznej. Co ważniejsze, nie trzeba wreszcie wykonywać podwójnej pracy, przepisując dokumenty w tradycyjnej postaci do jej formy elektronicznej, i odwrotnie. Dziennik elektroniczny może być wreszcie jedynym sposobem dokumentowania przebiegu nauczania. Zalet takiego rozwiązania jest wiele. Co jednak zrobić i jakie kroki podjąć, aby wdrożenie e-dziennika i jego późniejsze funkcjonowanie było bezpieczne?

Dla kogo dziennik?

Wiele szkół prowadziło i prowadzi dokumentację elektroniczną jako dodatek do istniejącego tradycyjnego dziennika. Najczęściej decyzja o wdrożeniu elektronicznej formy służyła ułatwieniu rodzicom dostępu do ocen ich dzieci, zapewniała szkole dostęp do różnorodnych statystyk i zestawień, a także była próbą zapobiegania niepożądanych zachowań, jak na przykład wagary.

Wejście w życie cytowanego rozporządzenia umożliwiło prowadzenie dokumentacji w sposób całościowy. Niekwestionowane i najbardziej istotne korzyści płynące z elektronicznego systemu czerpią szkoły, z punktu widzenia prowadzenia przez nie działalności dydaktyczno-wychowawczej. Na elektronicznej formie udostępniania danych korzystają również uczniowie i ich rodzice, co w sposób niezwykle istotny wprowadza współpracę szkoła – dom na jakościowo wyższy poziom.

Jaki system wybrać? Gdzie przechowywać bazę danych?

Dziennik elektroniczny jest systemem informatycznym, który przetwarza dane osobowe. Przy wyborze tego systemu szkoła powinna kierować się nie tylko informacją o zgodności dziennika z rozporządzeniem MEN, ale również tym, czy jest on zgodny z ustawą o ochronie danych osobowych z dnia 29 sierpnia 1997 roku z późniejszymi zmianami oraz rozporządzeniem MSWiA z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (...). W związku z tym zapewnienie właściwego poziomu bezpieczeństwa leży po stronie dyrekcji szkoły. Z doświadczenia wynika, że niewiele szkół w kraju jest w stanie zapewnić właściwy poziom bezpieczeństwa przechowywanych danych, lokalizując bazy informatyczne w swojej placówce. Wymaga to olbrzymich nakładów finansowych, zapewnienia wysokiej klasy profesjonalnego sprzętu oraz wysoko kwalifikowanej kadry administracyjnej. Dlatego decyzja o tym, gdzie przechowywać dane, jest niezwykle istotna.

Jednym z rozwiązań jest podpisanie specjalnej umowy z dostawcą dziennika elektronicznego lub dostawcą usług internetowych, obejmującej i zapewniającej właściwą politykę bezpiecznego dostępu do danych. Standardem jest zapewnienie szkole niezawodnego dostępu do danych poprzez odpowiednie procedury archiwizacji danych, które często odbywają się kilka razy dziennie i są przeprowadzane na kilku niezależnych macierzach serwerowych. Ważna jest również deklaracja o zapewnieniu ochrony danych zgodnie z cytowaną ustawą i rozporządzeniem.

Przy wyborze dziennika elektronicznego trzeba również pamiętać, że musi on zapewniać selektyw-

ność dostępu do danych, zabezpieczenie ich przed dostępem osób nieuprawnionych, przed zniszczeniem, uszkodzeniem lub ich utratą oraz rejestrować historię zmian i ich autorów.

Jak zapewnić i zorganizować dostęp do dziennika?

Selektywność dostępu do danych powinna być realizowana w taki sposób, by każdy z użytkowników miał dostęp tylko do wybranych danych. Przykładowo rodzic może obejrzeć tylko informacje na temat swojego dziecka i informacje ogólne, dotyczące klasy, na przykład terminarz prac klasowych, terminów przeczytania lektur, harmonogram konsultacji i wywiadówek. Podobnie jak w dzienniku tradycyjnym, nauczyciel powinien mieć pełen dostęp do swoich danych (wpisuje dane, edytuje) oraz możliwość przeglądania danych uczniów lub ocen z innych przedmiotów. Powinien mieć również dostęp do ocen z zachowania na poziomie całej szkoły, zgodnie z dokumentem Wewnątrzszkolnego Systemu Oceniania Zachowania. Dziennik elektroniczny powinien również umożliwić poprowadzenie zastępstwa, natomiast dyrektor powinien dysponować również informacjami na temat całej szkoły oraz aktywności użytkowników. Profesjonalne systemy zapewniają możliwość definiowania poziomu uprawnień i ważne jest to, aby wybierając dziennik, taki właśnie system wybrać.

Użytkownik, logując się do systemu DE, musi posiadać unikatowy login i hasło. Zgodnie z rozporządzeniem należy bezwzględnie przestrzegać następujących kryteriów: w przypadku gdy do uwierzytelniania użytkowników używa się hasła, musi się ono składać z co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Administrator stosuje środki ochrony kryptograficznej wobec danych wykorzystywanych do uwierzytelniania (np. SSL/https) natomiast zmiana hasła musi następować nie rzadziej niż co 30 dni. Zgodnie z rozporządzeniem są to tzw. środki bezpieczeństwa na poziomie wysokim.

Ponadto istnieją jeszcze inne wspomagające środki, zapewniające bezpieczne logowanie do systemu, które polecane są użytkownikom o większych uprawnieniach – administratorom, dyrektorom, nauczycielom. Są to na przykład metody biometryczne, do których należy moduł KEYSTROKE. Działanie modułu polega na tym, że system rejestruje indywidualne tempo i tembr wprowadzania hasła, indywidualnego jak odcisk palca. Nawet jeżeli hasło zostanie złamane, to aby zalogować się do systemu, musi być wprowadzone w specjalny sposób, określany jako indywidualna melodia wybierania przycisków klawiatury. Innym niewykluczającym się sposobem jest używanie kwalifikowanych podpisów elektronicznych.

Kolejnym elementem jest blokowanie kont, na które dokonano kilku nieudanych logowań, oraz przechowywanie maksymalnie dużej ilości informacji o tym zdarzeniu, pozwalających zidentyfikować intruza. Zapewnia to stosunkowo wysoki poziom bezpieczeństwa przed hackerskimi metodami łamania haseł.

Aby uniknąć nieautoryzowanego dostępu do systemu, „zalogowane" konto powinno mieć swoją „żywotność", to znaczy po pewnym określonym czasie następuje automatyczne wylogowanie z systemu. Eliminuje to wykorzystanie dostępu zalogowanego użytkownika przez osobę postronną.

Wybierając system, powinniśmy być przekonani, że spełni on wszystkie te, wręcz obowiązkowe postulaty bezpieczeństwa.

Jak wprowadzać dane do dziennika?

Żeby dziennik elektroniczny spełniał swoje zadanie, każdy nauczyciel powinien mieć zapewniony swobodny dostęp do komputera. Większość dobrych systemów oferuje dostęp do dziennika za pomocą Internetu. Jest to powszechna tendencja realizująca koncepcję usług odmiejscowionych, tzw. Cloud Computing, która zapewnia dostęp do danych z każdego miejsca i dowolnego urządzenia potrafiącego skorzystać z sieci Internet. Dzięki temu nauczyciel ma możliwość wprowadzenia ocen np. w domu, bezpośrednio po sprawdzeniu kartkówki.

Idealnym rozwiązaniem jest umieszczenie komputera nauczycielskiego w każdej sali lekcyjnej. Zapewni to bieżące i efektywne wykorzystanie dziennika. Przestrzegać tu należy kilku istotnych zasad. Najważniejsza – komputer nauczycielski to taki, przy którym pracują wyłącznie nauczyciele. Od tej reguły nie może być najmniejszych odstępstw. Trzeba to wyraźnie sprecyzować w szkolnych regulaminach i konsekwentnie egzekwować. Dobrze jest, aby lokalna sieć administracyjna była całkowicie odseparowana od sieci dydaktycznej, czyli takiej, do której mają dostęp uczniowie. Uczeń nie może mieć dostępu do dokumentów tworzonych przez dyrekcję, wychowawców, pedagoga i psychologa, które najczęściej mają charakter poufny. Innym czynnikiem jest wykorzystanie przez szkołę łączy Wi-Fi. Należy je tak przygotować i zabezpieczyć, żeby mogły z nich korzystać wyłącznie określone osoby na określonych komputerach. Unikniemy w ten sposób prób sieciowych podsłuchów i nieautoryzowanego dostępu.

Dane do dziennika powinny być wprowadzane systematycznie. Z doświadczeń wynika, że system najlepiej funkcjonuje wtedy, gdy dziennik elektroniczny traktowany jest jak dziennik tradycyjny – nauczyciel rozpoczyna lekcję od sprawdzenia obecności i wpisania tematu.

Jak zapewnić niezawodny dostęp do systemu?

Jednym z najważniejszych zagadnień mających wpływ na jakość funkcjonowania dokumentacji elektronicznej jest zapewnienie niezawodności. Przygotowując odpowiednią infrastrukturę, powinniśmy zabezpieczyć ją przed awarią sieci energetycznej oraz łączy internetowych. W szkole, w której pracuję, dostęp do dziennika realizowany jest poprzez Internet. W związku z tym łącza internetowe pochodzą od dwóch niezależnych operatorów. Odpowiednia konfiguracja routera zapewnia automatyczny dostęp do Internetu nawet w przypadku awarii u jednego z dostawców. Każde urządzenie dostępowe ma zasilanie awaryjne, umożliwiające pracę z akumulatorów nawet przez kilka godzin. Ponadto wyposażenie nauczycieli w 25 laptopów i 11 netbooków zapewnia stabilną pracę systemu bez istotnych przerw.

Każda szkoła korzystająca z dziennika elektronicznego powinna być również wyposażona w zestaw procedur określających, w jaki sposób postępować w przypadku dłuższych awarii.

Bezpieczeństwo a czynnik ludzki

Nawet przy najlepiej zorganizowanym systemie i zapewnieniu wszelkich dostępnych zabezpieczeń nadal olbrzymie znaczenie ma tzw. czynnik ludzki. Jesteśmy na tyle bezpieczni, na ile przestrzegamy zasad bezpieczeństwa. Każdy powinien pamiętać, że swoich danych dostępowych nie należy ujawniać nikomu, że nie wolno odchodzić od komputera, będąc zalogowanym, nie zapisywać haseł w łatwo dostępnym miejscu itd. Z punktu widzenia współpracy rodziców ze szkołą niezwykle istotne jest, by uczniowie nie znali haseł rodziców. System, w którym uczniowie mają własne loginy i hasła może skutecznie eliminować takie ryzyko.

Czy dziennik elektroniczny jest bezpieczny?

Wprowadzenie rozporządzenia MEN z dnia 16 lipca 2009 roku uruchomiło podaż. Na oświatowym rynku mamy wręcz eksplozję rozmaitych propozycji elektronicznych dzienników. Omawiając kwestię bezpieczeństwa dziennika elektronicznego, nie koncentrowałem się na konkretnym produkcie, lecz omówiłem czynniki, które mają wpływ na bezpieczne wdrażanie i stosowanie elektronicznego systemu w szkole. Starałem się zwrócić uwagę na te aspekty, które pozwolą dyrektorom szkół wybrać produkt najlepszy i jednocześnie zapewniający komfort pracy, stabilność, niezawodność i bezpieczeństwo.

Moje własne kilkuletnie doświadczenie z pracy nad DE pozwala stwierdzić, że jest on znacznie bezpieczniejszy niż tradycyjny dziennik, który łatwiej może zaginąć, ulec zniszczeniu lub dostać się w niepowołane ręce. Ponadto DE staje się łatwiej dostępny dla nauczycieli pracujących w grupach lub realizujących zajęcia międzyklasowe. Wdrożony w naszej szkole system zapewnia najwyższy poziom informacji, błyskawiczny dostęp do rozmaitych statystyk i zestawień. Wygodna i bezpieczna obsługa systemu sprawia, że nikt już nie wyobraża sobie powrotu do tradycyjnych metod.

Autor jest wicedyrektorem Gimnazjum im. F. Szołdrskiego w Nowym Tomyślu, nauczycielem informatyki

Przemoc

Gra zawiera elementy przemocy.

Paweł Górski

Bezpieczeństwo programu zarządzającego biblioteką

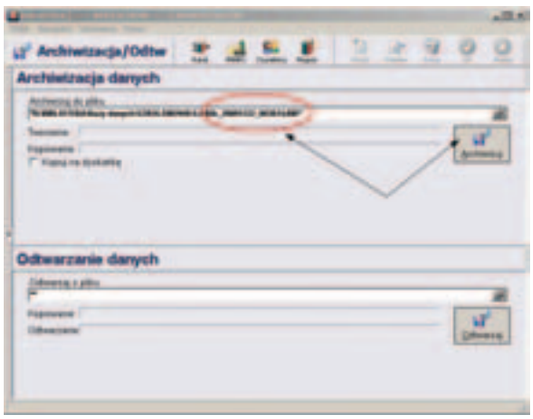
Rozwój technologii cyfrowych i szybko postępująca informatyzacja społeczeństwa polskiego mają duży wpływ na działalność nowoczesnych bibliotek. Komputer, drukarka, czytnik kodów kresowych oraz inny sprzęt elektroniczny stają się podstawowymi narzędziami wykorzystywanymi w codziennej pracy bibliotekarza.

Gdy nauczyciel bibliotekarz otrzyma już taki sprzęt komputerowy, do jego pełnego wykorzystania niezbędny staje się system biblioteczny. Od tego momentu zaczyna się ciężka praca związana z tworzeniem elektronicznego katalogu skomputeryzowanej biblioteki. Do wielkiego finału, jakim będzie udostępnienie w Internecie lub Intranecie (sieć wewnętrzna) pełnego katalogu dla czytelników, może upłynąć nawet kilka lat pracy. Jeżeli elektroniczny katalog będzie źle zabezpieczony, to może zdarzyć się, że pewnego dnia wszystkie bezcenne dane, które z takim trudem tworzone były przez pewien czas, zostaną utracone. Aby tego uniknąć, chciałbym udzielić Państwu kilku rad, z których mogą skorzystać nawet komputerowi laicy.

Uwagi dotyczące bezpieczeństwa odnoszą się do programu „Biblioteka" firmy ProgMan S.A., jednakże większość z nich z powodzeniem może dotyczyć innych systemów bibliotecznych. Zanim do tego przejdziemy, musimy uświadomić sobie, w jaki sposób może dojść do utraty bazy danych. Najczęstsze przypadki, to:

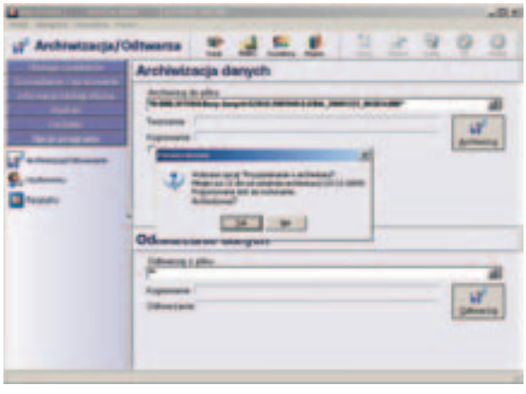
- szeroko pojęty aspekt ludzki,
- awaria sprzętu komputerowego,
- problem z aplikacją, z której korzystamy.

Jak mamy się mamy zabezpieczyć na wypadek takich okoliczności? Najprostszą metodą jest profilaktyka, czyli dbanie o to, aby codziennie archiwizować całą pracę. Użytkownik programu, kończąc pracę, musi otworzyć moduł „Archiwizacja danych" oraz kliknąć ikonę „Archiwizuj".



Rys. 1. Okno archiwizacji danych

W tym momencie program tworzy w jednym pliku pełną kopię bezpieczeństwa. Plik taki jest skompresowaną i zabezpieczoną bazą danych, a w jego nazwie zawarta jest dokładna data wykonania kopii. Osobom, które będą zapominały o wykonaniu takiej ważnej czynności, program oferuje ułatwienie w postaci przypomnienia, które będzie się pojawiać każdorazowo podczas próby zamknięcia programu.



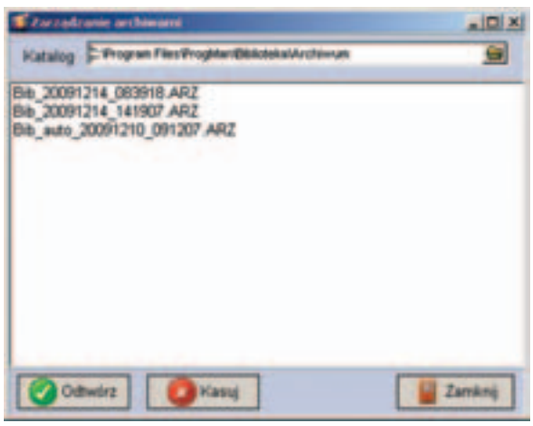
Rys. 2. Okno przypominania o archiwizacji danych

Trzeba jednak pamiętać, że archiwizacja nie rozwiązuje całkowicie sprawy. Oto prosty przykład: załóżmy, że wyrobiliśmy w sobie nawyk codziennej archiwizacji, a pliki znajdują się na dysku systemowym (archiwum domyślnie tworzone jest w katalogu „\Program Files\ProgMan\Biblioteka\…") lub dysk naszego komputera nie jest podzielony na partycje. W praktyce efekt może być tylko jeden. W chwili gdy wymagane będzie formatowanie dysku twardego (wirus lub problem z systemem operacyjnym Windows), ewentualnie urządzenie to po prostu się zepsuje, utracimy wszystkie nasze pliki. Co prawda istnieje wiele specjalistycznych firm, które zajmują się odzyskiwaniem utraconych danych, jednakże skorzystanie z ich oferty jest przede wszystkim bardzo kosztowne i nie zawsze szkoła będzie sobie mogła na to pozwolić.

Co w takim razie robić z archiwizowanymi plikami? Rozwiązania są bardzo proste, ale nie zawsze stosowane. Cenne pliki należy przechowywać na dodatkowych nośnikach danych, takich jak płyta CD/DVD, pamięć przenośna, karta pamięci w osobistym telefonie lub, gdy mamy dostęp do Internetu, można wysłać je w formie załącznika do własnej skrzynki pocztowej.

Jeżeli zastosujemy się do powyższych rad, to w sytuacji kryzysowej mamy pewność, że nie utracimy efektów naszej pracy. W takim przypadku możemy ponownie zainstalować „czystą" wersję programu, a następnie wgrać plik z kopią bezpieczeństwa. Eliminuje to także konieczność ponownego zarejestrowania programu.

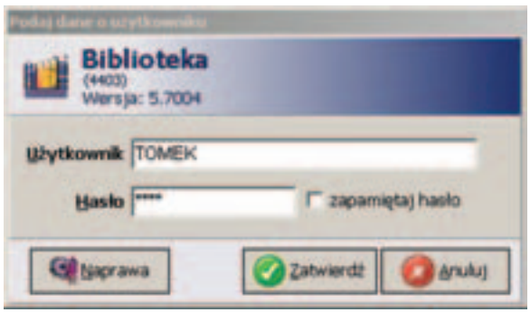
Dla osób, które nie korzystały z funkcji archiwizacji zbiorów, program posiada koło ratunkowe w postaci automatycznego tworzenia archiwum. Taka wymuszona kopia bezpieczeństwa powstaje w chwili przeprowadzania aktualizacji sytemu bibliotecznego (przejście na nowszą wersję programu) lub gdy użytkownik programu „Biblioteka" nie przeprowadzał świadomej archiwizacji zbiorów w okresie dłuższym niż miesiąc.



Rys. 3. Okno zarządzania plikami automatycznej archiwizacji

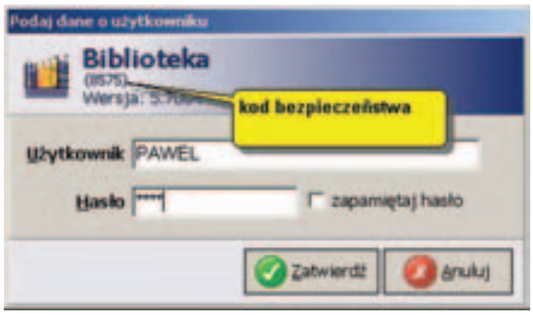
Archiwizacja to nie jedyny element bezpieczeństwa, jaki można stosować w codziennej pracy. Bardziej zaawansowane opcje związane są z procedurami automatycznej naprawy zbiorów czy ochrony programu przed osobami postronnymi.

Systemy biblioteczne posiadają wbudowane mechanizmy naprawy bazy danych, które uaktywniają się automatycznie lub są wywoływane ręcznie. Włączenie tej procedury następuje po nieprawidłowym zamknięciu aplikacji i jest ono możliwe w przypadku zawieszenia systemu lub awarii zasilania.



Rys. 4. Okno naprawy bazy danych

Kolejnym ważnym aspektem jest kwestia ochrony danych przed osobami postronnymi. Podczas pierwszego kontaktu z programem użytkownik uruchamia go jako administrator i dopiero tu tworzy loginy i hasła dostępu do aplikacji. Tak stworzone konta przechowywane są w bazie danych w postaci zaszyfrowywanej. Dodatkowo użytkownikom można przydzielić uprawnienia na różnym poziomie dostępu do programu (czytelnik/bibliotekarz/administrator). Nawet w przypadkach skrajnych, gdy użytkownik zapomni swojego hasła lub loginu, istnieje możliwość bezproblemowego i bezpiecznego wejścia do systemu. Aby to zrobić, użytkownik powinien skontaktować się telefonicznie z pracownikami firmy ProgMan S.A. w celu wygenerowania jednorazowego hasła umożliwiającego wejście do programu z prawami administratora. Hasło takie tworzone jest na podstawie kodu bezpieczeństwa (rys. 5) oraz danych licencyjnych klienta. Dzięki temu nauczycieli bibliotekarz po zalogowaniu się do programu możne ponownie ustawić nowe hasło dostępu do systemu bibliotecznego.



Rys. 5. Okno logowania oraz kodu bezpieczeństwa

Powyższe porady mogą być śmiało wykorzystane przez nowych użytkowników programów bibliotecznych, i nie tylko. Najważniejszą sprawą powinno być uświadomienie sobie, jak ważna jest kwestia bezpieczeństwa zgromadzonych danych, a najprostsze metody, to czysta profilaktyka. Jednakże bardzo często trudno w środowisku bibliotekarzy pokonać barierę psychologiczną związaną ze strachem i niechęcią w stosunku do nowych rozwiązań informatycznych. Miejmy jednak nadzieje, że dzięki powszechnej informatyzacji społeczeństwa bariery te staną się jedynie elementami marginalnymi, stojącymi na drodze do sprawnego zarządzania nowoczesną, skomputeryzowaną biblioteką.

Autor jest zastępcą kierownika Działu Rozwoju Rynku w firmie ProgMan S.A.

◀

Wulgarny język

W grze jest używany wulgarny język.

◀

Strach

Gra może przestraszyć młodsze dzieci.

Łukasz Boguszewski

Odzyskiwanie danych i latające talerze, czyli jak uchronić się przed utratą ważnych informacji

Postęp technologiczny jest nieustanny. Powszechnie używane kiedyś dyskietki dziś są już prawie zapomniane, a płyty CD coraz częściej wypierane przez przenośne pamięci flash. W dzisiejszym skomputeryzowanym świecie na użytkowników różnego typu pamięci elektronicznych czyhają rozmaite awarie. Podczas codziennego eksploatowania naszych „sprzętów", począwszy od kart pamięci, poprzez pendrive'y, po dyski twarde, zarówno te osobiste, jak i macierze dyskowe stosowane w serwerach wielkich organizacji czy firm, mogą zdarzyć się przypadki utraty danych. Problem ten może więc dotknąć każdego, kto choć sporadycznie styka się z tego typu urządzeniami.

Skupimy się dzisiaj na nietypowym uszkodzeniu, do jakiego dochodzi w zaciszu domowym albo w pracy, kiedy coś trzeba zrobić „na wczoraj", a pośpiech jest niestety złym doradcą. W takich wypadkach może dojść do przypadkowego upuszczenia dysku. O uszkodzeniu tym można nawet trafnie powiedzieć „latające talerze", w końcu bądź co bądź dane na dysku są zapisane właśnie na talerzach. Nie będziemy obliczać skomplikowanych wzorów matematycznych, jaką drogę przebył dysk, jaki miał ciężar, w co po drodze uderzył oraz gdzie wylądował. Zastanowimy się natomiast, co mogło się z nim stać, kiedy oddał podłodze swoją energię, skrupulatnie zebraną w drodze na ziemię. Zdesperowany użytkownik często wpada w popłoch, jak to zostało opisane poniżej, i stara się samodzielnie rozwiązać problem.

Co ja tam miałem? Prawie wszystko – odpowiada strach. Muszę jeszcze raz podłączyć dysk, przecież nie było tak wysoko, a gdzieś czytałem, że taki twardziel wszystko wytrzyma. Podłączam dysk. Dźwięki, jakie wydaje, przypominają buczenie. Chyba za wysoko było, więc lądowanie mogło mu zaszkodzić. No nic, trzeba pewnie go otworzyć, może się zaciął, może jakiś trybik się popchnie i po kłopocie. No to do dzieła. Gdzie jest ten śrubokręt? A to co znowu? Co za dziwne śrubki? Pewnie ktoś nie miał innych, ale co to dla mnie, zawsze sobie radziłem, to i teraz sobie poradzę. Wreszcie go rozkręciłem, więc można spokojnie zajrzeć. O jak tu ładnie i czysto, co tu się mogło stać? Dziwne, talerze nie chcą się kręcić, może dlatego, że ten pałąk je trzyma. O już udało mi się go zrzucić do brzegu talerzy, ale dalej nie idzie. Już wiem, to nie w tę stronę, pewnie powinien być przy osi dysku. Strasznie ostry ten śrubokręt. A niech to, zarysowałem talerz. Na szczęście kawałek tylko. Ale talerze dalej nie chcą się kręcić. Dziwne. Może trzeba poluzować te śrubki z wierzchu, co je trzymają? I znowu te dziwne śrubki... wykończą mnie. No nareszcie, teraz talerze się jakoś ruszają. Może warto spróbować podłączyć dysk? I znowu nic... to już ponad moje siły, trzeba zapytać się kogoś, kto to robi na co dzień, przecież muszę koniecznie mieć te dane. Jak tu znaleźć specjalistę? Wiem, wpiszę w Google „odzyskiwanie danych"... Ale dużo tych firm, do której zadzwonić? Najlepiej do pierwszej z góry. To chyba jacyś wariaci... chcą zrobić analizę i pobrać opłatę za to, że dysk był otwierany, a przecież ja im mówiłem, co robiłem. Trzeba gdzie indziej spróbować. No nie, wszyscy się uwzięli na te opłaty za otwieranie dysku. No cóż, muszę chyba wyjąć gotówkę ze skarpety. Oj drogo, wzięli tę opłatę wstępną, mam nadzieję, że dopłata nie będzie za wysoka. Szkoda tylko, że trzeba kilka dni poczekać na tę „całą" analizę, a co ja w pracy powiem? Nareszcie zrobili mi tę analizę, ale wymienili tyle uszkodzeń, że aż dech mi zaparło. Pierwsze, najcięższe, to zatarcie silnika, drugie – uszkodzenie głowic, a trzecie – rozkalibrowanie talerzy.

I tak drodzy Czytelnicy kończy się jeden z wielu epizodów, jakie mają miejsce w trakcie podobnych awarii dysków. Co trzeba zrobić w takiej sytuacji, jakie problemy mogą nas spotkać, gdybyśmy chcieli we własnym zakresie próbować uruchomić taki dysk? Podczas użytkowania pamięci nie jesteśmy w stanie uniknąć wszystkich nieoczekiwanych zdarzeń.

Możemy jednak podjąć odpowiednie środki, by zabezpieczyć się przed utratą danych lub, w przypadku awarii, oddać nasz sprzęt w ręce profesjonalistów.

Metody zapobiegawcze

Wykonuj kopie zapasowe

Aby zmniejszyć do minimum ryzyko utraty dużej partii informacji, należy pamiętać o metodach profilaktycznych. Jedną z najprostszych i najskuteczniejszych jest wykonywanie kopii zapasowych dysku, potocznie nazywanych backupami. Przy tworzeniu kopii należy pamiętać o tym, aby różne obszary na dysku były kopiowane w różnych odstępach czasu. Działy informatyczne wielkich organizacji na całym świecie coraz większą uwagę przywiązują do tego, by tworzone kopie były skuteczne, a ich przywrócenie możliwie szybkie i dokładne. Badania i testy prewencyjne pochłaniają duże środki finansowe, jednak porządny system ochronny zapewnia płynność działania w razie usterki. Dobrze zabezpieczona firma podczas awarii nie traci cennego czasu na przywracanie niezbędnych danych, a co za tym idzie, nie naraża się na ogromne straty finansowe spowodowane wymuszonym postojem w pracy.

Korzystaj z oprogramowania antywirusowego

Każdego dnia użytkownicy komputerów narażeni są na ataki wirusów. Ataki te są częstą i groźną przyczyną utraty danych. Aby uniknąć zarażenia komputera wirusem i jednocześnie ochronić dane, należy korzystać z dobrego oprogramowania antywirusowego. Ważne, by program antywirusowy był dobrze skonfigurowany oraz zaktualizowany, ponieważ, jak powszechnie wiadomo, każdego dnia do sieci trafia cała masa nowych wirusów.

Zmniejsz prawdopodobieństwo zainfekowania wirusem

W dobie wszechobecnego eksploatowania dobrodziejstw sieci, coraz częściej wirusy docierają do nas właśnie tą drogą, ukryte w mailach bądź też na odwiedzanych przez nas stronach WWW.

Internet nie jest jedynym środkiem transportu dla wirusów. Należy zwrócić szczególną uwagę na wszelkiego rodzaju nośniki danych podłączane do komputera. Wiele wirusów przenosi się za pomocą przenośnych dysków USB czy też kart pamięci flash. Dzieje się tak za pośrednictwem pliku uruchamianego automatycznie przez system operacyjny po dostępie do danych nośnika. Podłączanie nośników niewiadomego pochodzenia często kończy się zainfekowaniem systemu operacyjnego.

Postępuj delikatnie z urządzeniem przechowującym dane

Należy pamiętać, że dyski twarde są urządzeniami delikatnymi i nawet najmniejszy wstrząs może spowodować ich uszkodzenie mechaniczne. Porządek w otoczeniu komputera ma pośredni wpływ na zabezpieczenie zawartych w nim danych. Wielu klientów naszej firmy przychodzi z dyskami uszkodzonymi podczas upadku komputera. Upadek ten często spowodowany jest plątaniną kabli do niego podłączonych. Należy wystrzegać się także stawiania wszelkiego rodzaju napojów w pobliżu komputera. Nawet niewielka ilość płynu może spowodować zwarcie, którego skutkiem będzie spalona elektronika dysku lub też, w najgorszym przypadku, jego komutator (tego typu uszkodzenie zalicza się już do grupy uszkodzeń mechanicznych).

Rodzaje uszkodzeń

Błędy użytkowników

Jak wynika z przeprowadzonych badań, aż 30% przypadków utraty danych spowodowanych jest nieumiejętnym użytkowaniem programów w procesie ochrony danych bądź ich przetwarzania przez pracowników. Błędy, które mogą pojawić się podczas pracy, to m.in. przypadkowe usunięcie pliku czy sformatowanie dysku twardego. Pracownik bez odpowiedniej wiedzy na temat przetwarzania danych lub obsługi oprogramowania może uszkodzić dane bądź doprowadzić do ich utraty. Innym rodzajem błędów użytkownika są te, które powodują pogorszenie sytuacji. Oto lista najczęstszych i najbardziej powszechnych błędów użytkownika:

- przypadkowe usunięcie plików przy pominięciu kosza systemowego,
- usunięcie plików z kosza,
- sformatowanie dysku twardego,
- wybór niewłaściwej partycji podczas instalowania systemu operacyjnego (skutkuje nadpisaniem części danych na partycji),
- instalowanie systemu operacyjnego na nośniku z danymi, o których użytkownik zapomniał (skutkuje nadpisaniem części danych),
- praca na nośniku uszkodzonym mechanicznie (skutkuje pogorszeniem stanu nośnika lub rysowaniem talerzy),
- praca na komputerze z usuniętymi plikami (powoduje nadpisanie usuniętych danych),
- pozwolenie na skanowanie dysku za pośrednictwem programu Scandisk (program ten często bezpowrotnie niszczy informacje o uszkodzonych plikach).

Błędy w oprogramowaniu

Drugą ważną przyczyną uszkodzeń są błędy w oprogramowaniu. Firmy produkujące oprogramowanie poświęcają coraz więcej czasu na usunięcie ze swoich produktów jak największej liczby błędów. Jednak pomimo że oprogramowanie jest opracowywane z właściwą troską, zawarte w nim błędy są dzisiaj drugim co do częstotliwości występowania powodem utraty danych.

Awaria sprzętowa

Awaria sprzętu komputerowego związana jest z fizycznym uszkodzeniem nośników danych w komputerach. Utrata danych następuje np. w momencie błędnego ustawienia głowic zapisu/odczytu lub problemów z powierzchnią talerzy. Dane z fizycznie uszkodzonego dysku jest wyjątkowo trudno odzyskać. Wymaga to znacznie większych nakładów pracy i środków. Naprawa takiego sprzętu wymaga również cierpliwości, precyzji oraz dokładności. Zwykle proces odzyskiwania danych z fizycznie uszkodzonych nośników trwa znacznie dłużej, ale w większości przypadków kończy się sukcesem.

Odzyskiwanie danych (data recovery)

Typy utraty danych

Poprzez nieumiejętne użytkowanie komputera można doprowadzić do różnego typu utraty danych. Jednym z częstych przypadków jest przypadkowe skasowanie plików, utrata partycji z danymi przy nieumiejętnej instalacji systemu lub awaria zasilania podczas formatowania. Tego typu wypadki mogą przytrafić się każdemu. Nie należy wówczas wpadać w panikę, gdyż możliwość odzyskania danych jest stuprocentowa, jeśli „misja ratunkowa" przybędzie na miejsce zaraz po ich skasowaniu. Należy pamiętać, że każda próba odzyskiwania danych przez laika może skończyć się ich utratą. Nawet próby ponownego uruchamiania komputera mogą być przyczyną nadpisania przez system operacyjny, co prowadzi do częściowej lub całkowitej utraty danych. Odzyskiwanie danych ze sformatowanego dysku w zdecydowanej większości przypadków kończy się sukcesem. Jedynym minusem jest utrata oryginalnych nazw plików oraz folderów. Mimo ciągłych prób nie udało się stworzyć odpowiedniego oprogramowania, które zachowywałoby właściwe nazwy.

Dobór odpowiedniej firmy data recovery

Aby odzyskanie danych zakończyło się sukcesem, musimy wiedzieć, jak dobrać odpowiednią firmę, której powierzymy nasze cenne dane. Obecnie na rynku jest kilka firm, które trudnią się odzyskiwaniem danych i jednocześnie są do tego odpowiednio przygotowane. Ważne jest, by sprawdzić, w jakich warunkach będzie odbywało się „ratowanie" naszych danych. Profesjonalne firmy posiadają wyposażone laboratoria, odpowiednie narzędzia. Praca na otwartych nośnikach odbywa się w sterylnych komorach laminarnych, gdzie nie ma miejsca na najmniejsze zanieczyszczenie powietrza. Każdy najdrobniejszy pyłek może uszkodzić sektor na dysku, a co za tym idzie, przyczynić się do utraty danych. Zdarzają się na rynku tzw. chałupnicy, którzy po zainstalowaniu oprogramowania dostępnego w sieci, kusząc klienta niskimi cenami, zamiast pomóc, doprowadzają do jeszcze większych komplikacji, a co za tym idzie do zwiększenia kosztów odzyskania danych. Dlatego pamiętajmy, żeby nasze dane powierzyć profesjonalistom z długoletnim doświadczeniem oraz odpowiednim zapleczem.

Opis użytkownika

Bardzo istotnym elementem odzyskiwania danych są informacje od zgłaszającego problem użytkownika. Po krótkiej rozmowie można dowiedzieć się, jaka jest przyczyna awarii, zdiagnozować usterkę oraz skonstatować, jakie komplikacje mogły się pojawić na skutek wcześniejszych prób naprawy przez klienta. Informacje te są bardzo istotne na dalszym etapie odzyskiwania danych. Dlatego tak ważne jest, by w przypadku awarii nie tracić głowy i nie podejmować niepotrzebnych kroków. W krytycznej sytuacji najlepiej od razu udać się do profesjonalnej firmy trudniącej się odzyskiwaniem danych. Ważne też, by nie doprowadzić do kolejnych uszkodzeń fizycznych poprzez nieodpowiedni transport. W przypadku odzyskiwania danych potwierdza się reguła, że pośpiech jest złym doradcą. Cały proces odzyskiwania danych wymaga bardzo dużej precyzji, jest to żmudna, czasochłonna praca, ale efekty, które można uzyskać, są tego warte.

Koszty naprawy uszkodzonego sprzętu bardzo często zależą od rodzaju awarii. Uszkodzenia dzielimy najczęściej na logiczne lub fizyczne. Profesjonalne firmy trudniące się od lat tematyką *data recovery* aktualnie są w stanie naprawić i przywrócić niezbędne informacje praktycznie z każdego rodzaju i modelu pamięci. Pod czujne oko fachowca trafiają więc zarówno karty pamięci aparatów cyfrowych, jak i napędy magnetooptyczne.

Autor jest pracownikiem firmy Streamdata.pl Sp. z o.o.

Marzena Jarocka

Bezpieczeństwo i higiena pracy z komputerem oraz zabezpieczenie komputera (systemów operacyjnych, programów i danych). Zestawienie bibliograficzne w wyborze za lata 2000-2009

Wydawnictwa zwarte

1. Angart Leo: Komputer a zdrowie: jak zapobiegać bólom pleców i stawów oraz ćwiczyć wzrok. – Warszawa: Klub dla Ciebie – Bauer – Weltbild Media, 2008.
2. Bezpieczeństwo i higiena pracy na stanowiskach komputerowych: lista kontrolna bhp. – Warszawa: CIOP, 2000.
3. Bilski Tomasz: Wprowadzenie do ochrony danych. – Poznań: Wydawnictwo Wyższej Szkoły Komunikacji i Zarządzania: Wągrowiec: M-Druk, 2005.
4. Jóźwiak Zbigniew: Stanowiska pracy z monitorami ekranowymi – wymagania ergonomiczne. – Łódź: IMPiPJN, 2001
5. Kamieńska-Żyła Maria: Struktura i ergonomia stanowiska komputerowego. – Tarnobrzeg: Tarbonus, 2002.
6. Kaspersky Kris: Dezasemblowanie kodu: zaawansowane techniki zabezpieczania programów. – Warszawa: RM, 2004.
7. Kiss Bogumił Antoni: Komputery dla rozsądnych. – Wrocław: Wydawnictwo Continuo, 2008.
8. Komputerowe stanowisko pracy: aspekty zdrowotne i ergonomiczne. – Warszawa: Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy, 2003.
9. Konarska Maria, Gedliczka Adam: Sprawdź, czy twoje stanowisko pracy z komputerem jest ergonomiczne. – Warszawa: CIOP, 2001.
10. Lehtinen Rick, Russell Deborah, Gangemi G.T.: Podstawy ochrony komputerów. – Gliwice: Wydawnictwo Helion, 2007.
11. Luber Alan D.: Bezpieczny komputer: czy stać cię na utratę danych? – Warszawa: Wydawnictwo Translator, 2003.
12. Lukatsky Alex: Wykrywanie włamań i aktywna ochrona danych. – Gliwice: Wydawnictwo Helion, 2005.
13. Mendrala Danuta, Szeliga Marcin: Bezpieczeństwo twojego komputera: zadbaj o bezpieczeństwo swojego komputera: poznaj rodzaje zagrożeń, zabezpiecz system operacyjny, programy i dane, usuń skutki ataków. – Gliwice: Wydawnictwo Helion, 2004.
14. Ochrona danych i zabezpieczenia w systemach teleinformatycznych / pod red. Janusza Stokłosy. – Poznań: Wydawnictwo Politechniki Poznańskiej, 2005.
15. Pakuła Jakub: Bezpieczny komputer czyli jak chronić się przed hakerami, wirusami, spywarem, spamem itd. – Michałowice: Komputerowa Oficyna Wydawnicza „Help" Piotr Gomoliński, 2005.
16. Wang Wallace: Tajemnice Internetu, hackingu i bezpieczeństwa: poznaj sposób myślenia i zasady działania hakerów. – Gliwice: Wydawnictwo Helion, 2005.

Artykuły z wydawnictw ciągłych

17. Arnold Arne, Daszkiewicz Krzysztof: Bezpieczeństwo – prosto i skutecznie // PC World Komputer. – 2006, nr 10, s. 98-101.
18. Awaria bez straty danych // PC Format. – 2009, nr 10, s. 62-63.
19. Bądź bezpieczny // Komputer Świat. – 2009, nr 17, s. 20-27.

20. Bezpieczeństwo i optymalizacja // Komputer Świat. Twój Niezbędnik Extra – 2008, nr 4, s. 18-25.
21. Bezpieczne dane // Next. – 2008, nr 9, s. 35-37.
22. Bezpiecznie jak w sejfie // Komputer Świat. – 2009, nr 18, s. 38-44.
23. Bęczkowski Stanisław: Komputer w szkolnej pracowni. Wymogi BHP // Gazeta Szkolna. 2000, nr 31, s. 8.
24. Bragoszewski Paweł: Mój komputer, moja twierdza // PC World Komputer. – 2006, nr 10, s. 102-114.
25. Chojnacki Paweł: Bezpieczeństwo danych w komputerze // Sekretariat. – 2009, nr 10, s. 24-25.
26. Ciesielski Tomasz: XP & Vista: pełna ochrona bez stresu // Chip. – 2007, nr 10, s. 104-109.
27. Daszkiewicz Krzysztof, Apfelböck Hermann: Jak długo przetrwają twoje dane? // PC World Komputer. – 2008, nr 6, s. 112-114.
28. Daszkiewicz Krzysztof, Metzger Christoph: Sejf na dane // PC World Komputer. – 2006, nr 4, s. 72-76.
29. Dbajmy o bezpieczeństwo // Gazeta Szkolna. – 2009, nr 11/12, s. 6.
30. Dębek Piotr, Mańk Bartłomiej: Elektroniczny morderca // Chip. – 2000, nr 6, s. 54-56.
31. Dramczyk Bartłomiej: Spyware, phishing, spam – co nas ochroni? // Chip. – 2008, nr 2, s. 56-61.
32. Dramczyk Bartłomiej: Turbo dla Windows XP: jeden klik i gotowe // Chip. – 2007, nr 8, s. 26-31.
33. Dramczyk Bartłomiej: Zaopiekuj się swoim dyskiem // Chip. – 2009, nr 3, s. 50-53.
34. Dren Marek: Życie na podsłuchu // Chip. – 2008, nr 9, s. 32-36.
35. Drużycki Jakub: Pliki jak w sejfie // Komputer Świat Ekspert. – 2008, nr 6, s. 36-39.
36. Dysk dobrze chroniony // Next. – 2009, nr 3, s. 128-129.
37. Gogołek Włodzimierz: Bezpieczeństwo danych Cz. 1 // Przegląd Techniczny. – 2002, nr 44, s. 23.
38. Gogołek Włodzimierz: Bezpieczeństwo danych Cz. 2 // Przegląd Techniczny. – 2002, nr 45, s. 36.
39. Górski Sebastian: Codzienna higiena systemowa // PC World Komputer. – 2007, nr 2, s. 58-59.
40. Gryz Krzysztof, Karpowicz Jolanta: Źródła pól elektromagnetycznych – monitory ekranowe // Bezpieczeństwo Pracy. – 2002, nr 4, s. 13-17.
41. Grzenkowicz Krystian: Ochrona prawie idealna // PC World. – 2009, nr 10, s. 76-79.
42. Halsen Emma: Ergonomia w Twoim biurze // Sekretariat. – 2009, nr 11, s. 14-17.
43. Haworth Rosemary, Janus Rafał: Biblia bezpieczeństwa // PC World Komputer. – 2008, nr 9, s. 99-103.
44. Hofman-Wiśniewska Justyna: Nasze zdrowie a komputer // Prawo Pracy. – 2001, nr 7/8, s. 45-49.
45. Janus Rafał: Backup od podszewki // PC World Komputer. – 2006, nr 2, s. 80-86.
46. Jóźwiak Zbigniew: Ewolucja stanowiska komputerowego // Atest. – 2007, nr 12, s. 4-5.
47. Już Cezar to robił // PC Format. – 2008, nr 2, s. 108-109.
48. Kamieńska-Żyła Maria, Prync-Skotniczny Krystyna: Ergonomiczna ocena stanowiska komputerowego // Mechanika. – 2001, z. 2, s. 177-185.
49. Kamieńska-Żyła Maria: Obciążenie układu ruchu na stanowiskach komputerowych // Zastosowania Ergonomii. – 2001, nr 3/4, s. 69-72.
50. Kamińska Joanna: Jak prawidłowo siedzieć // Bezpieczeństwo Pracy. – 2005, nr 5, s. 26-28.
51. Kosedowski Marcin: Ukryj swoje dane // PC World. – 2009, nr 4, s. 112-115.
52. Kowal Edward, Miedziarek Sławomir: Wybrane elementy organizacji stanowiska komputerowego i jej wpływ na efektywność pracy // Zastosowania Ergonomii. – 2007, nr 1/2, s. 161-173.
53. Kubacki Adrian: Czy mój komputer jest bezpieczny? // Chip. – 2009, nr 3, s. 112-115.
54. Kubacki Adrian: Dane w pełni bezpieczne // Chip. – 2009, nr 8, s. 42-45.
55. Kubacki Adrian: Niebezpiecznie gorące notebooki // Chip. – 2009, nr 1, s. 126-129.
56. Kubacki Adrian: Niewidzialne zagrożenie // Chip. – 2008, nr 8, s. 120-123.
57. Kwiatkowska Anna Beata, Korpal Andrzej: Szyfrowanie w praktyce // Komputer w Szkole. – 2003, nr 5, s. 56-64.
58. Lepszy komputer // Komputer Świat. – 2009, nr 15, s. 40-43.
59. Leszczyński Wiktor: Przepisy BHP obowiązujące na stanowiskach wyposażonych w monitory ekranowe // Wydawca. – 2001, [nr] 1, s. 44-46.
60. Lisowski Piotr: Menedżery haseł // Chip. – 2008, nr 10, s. 90-91.
61. Lisowski Piotr: Test zabezpieczeń // Chip. – 2009, nr 4, s. 94-97.
62. Majdaniec Jerzy: Jak skutecznie zabezpieczyć peceta // Chip. – 2009, nr 6, s. 32-35.
63. Majdaniec Jerzy: Komputer, który sam się leczy // Chip. – 2009, nr 2, s. 40-44.
64. Majdaniec Jerzy: Te programy zrujnują każdy system // Chip. – 2008, nr 5, s. 32-36.
65. Majdaniec Jerzy: Teren prywatny, wstęp wzbroniony! // Chip. – 2009, nr 2, s. 102-105.
66. Majdaniec Jerzy: Windows na 100% bezpieczny // Chip. – 2008, nr 5, s. 88-92.
67. Majdaniec Jerzy: Witamina C ochroni twój komputer // Chip. – 2008, nr 10, s. 120-123.

68. Migus Michał: Bezpieczeństwo w systemach intranetowych – zapory ogniowe // Zeszyty Naukowe Wyższej Szkoły Biznesu im. bp. Jana Chrapka w Radomiu. – 2005, nr 1, s. 147-168.
69. Mincewicz Krzysztof: BHP w pracowni techniki i informatyki // Wychowanie Techniczne w Szkole. 2002, nr 3, s. 48-52.
70. Młynarczyk Konstanty: Jakiej ochrony faktycznie potrzebujesz? // Chip. – 2007, nr 8, s. 72-76.
71. Na straży bezpieczeństwa // Next. – 2009, nr 3, s. 28-31.
72. Onysyk Wit: Najlepszy przepis na zabezpieczenie danych // Chip. – 2009, nr 7, s. 102-105.
73. Onysyk Wit: Nigdy więcej nie trać danych // Chip. – 2009, nr 9, s. 28-31.
74. Ostapowicz Marcin: Drugi pecet w twoim pececie // Chip. – 2007, nr 7, s. 64-67.
75. Ożarek Grażyna: BHP w pracy z komputrem // Komputer w Szkole. 2001, nr 2, s. 51-56.
76. Pełna ochrona danych // Next. – 2008, nr 9, s. 27-29.
77. Pełzowski Piotr Artur: NoDelete – program zabezpieczający dane komputerowe przed przypadkowym skasowaniem lub przeniesieniem // Wychowanie Techniczne w Szkole. – 2001, nr 4, s. 53-55.
78. Petras Rafał, Koterski Sławomir: Dobre narzędzia, złe narzędzia // Chip. – 2008, nr 3, s. 90-95.
79. Pleban Bartosz: Zarys problematyki ochrony zasobów komputerowych w organizacji // Zeszyt Naukowy. Śląska Wyższa Szkoła Zarządzania im. gen. Jerzego Ziętka w Katowicach. – 2004, nr 8, s. 77-100.
80. Praca, zabawa i… zdrowie // Mama, Tata, Komputer i Ja. – 2009, nr 2, s. 9.
81. Przerwa Jacek: Kryptograficzne systemy plików // Prace Naukowe. Ekonomika. Politechnika Radomska im. Kazimierza Pułaskiego. – 2005, nr 1, s. 167-173.
82. Romanowska-Słomka Iwona: Ocena ryzyka zawodowego: pracujący przy monitorze ekranowym // Atest. – 2005, nr 1, s. 24-25.
83. Rossielewicz Włodzimierz: Czy stanowisko komputerowe odpowiada podstawowym warunkom ergonomii i bhp? // Wychowanie Techniczne w Szkole. – 2003, nr 1, s. 56-58.
84. Rostkowska Małgorzata: Zagrożenia generowane przez nowe technologie // Meritum. – 2008, nr 1, s. 69-73.
85. Rotkiewicz Marek: Praca przy monitorze // Nowe Ubezpieczenia. – 2003, nr 13/14, s. 89-93.
86. Skrzyński Dariusz: BHP i aktualności prawne // Meritum. – 2007, nr 4, s. 125-130.
87. Sobczak Roman: Komputer a zdrowie // Zeszyty Naukowe Wałbrzyskiej Wyższej Szkoły Zarządzania i Przedsiębiorczości. – 2004, nr 2, s. 126-137.
88. Sobota Marcin: Bezpieczeństwo danych w systemach komputerowych oparte na rozwiązaniach kryptograficznych // Zeszyty Naukowe. Organizacja i Zarządzanie. Politechnika Śląska. – 2004, z. 18, s. 25-32.
89. Sterylnie pod palcami // Komputer Świat. – 2009, nr 17, s. 30-33.
90. Susłow Walery, Statkiewicz Michał: Szkolenie informatyków w zakresie projektowania stanowisk pracy z komputerem // Bezpieczeństwo Pracy. – 2004, nr 12, s. 22-24.
91. Śnieżek Henryk: I ty możesz żyć bezpiecznie: bezpieczeństwo i higiena pracy na stanowiskach wyposażonych w monitory ekranowe // Edukacja dla Bezpieczeństwa. – 2006, nr 4, s. 65-69.
92. Taboł Sebastian: Wpływ komputera na zdrowie ucznia // Edukacja i Dialog. 2003, nr 2, s. 21-26.
93. Tajne przez poufne // PC Format. – 2007, nr 9, s. 54-56.
94. Tomaszczyk Jacek: Czy na pewno bezpieczne? // Bibliotekarz. – 2001, [nr] 7/8, s. 28-29.
95. Utracki Dariusz: Oszukać zagrożenie // PC World Komputer. – 2006, nr 10, s. 116-119.
96. Vista – bezpiecznie jak nigdy // Chip. – 2007, nr 9, s. 162-169.
97. W szyku obronnym // Komputer Świat Ekspert. – 2008, nr 6, s. 32-35.
98. Wantoła Leszek: Zagrożenia płynące z komputera // Edukacja dla Bezpieczeństwa. – 2002, nr 3, s. 25-29.
99. Wolska Agnieszka: Wybór systemu oświetleniowego na stanowiskach z komputerami a cechy użytkowników // Bezpieczeństwo Pracy. – 2001, nr 7/8, s. 6-8, 38.
100. Zabezpieczanie danych na dysku // PC Format Krok po Kroku. – 2008, nr 1, s. 61-102.
101. Zabezpieczenie danych // Komputer Świat. Twój Niezbędnik Extra. – 2007, nr 3, s. 5.
102. Zawodowa ochrona // Komputer Świat. – 2007, nr 7, s. 44-45.
103. Zdanowski Sylwester: Ochrona danych // Haking. – 2009, nr 9, s. 14-19.

Autorka jest nauczycielem bibliotekarzem Wydziału Informacyjno-Bibliograficznego Biblioteki Pedagogicznej w Toruniu

Marcin Kozłowski

Przed czym i jak chronić komputer?

„Jeśli czegoś nie ma w Google, to znaczy, że nie istnieje" mówi popularny slogan i sporo w nim prawdy. Według szacunkowych danych Google posiada ponad milion serwerów, tak więc ilość danych na nich zgromadzonych jest imponująca. W sieci możemy znaleźć niemal wszystko, np. teksty, grafikę, pliki dźwiękowe, ogromną liczbę stron edukacyjnych oraz różnych programów. Dzięki usługom oferowanym w Internecie dokonujemy przelewów i płatności (bankowość elektroniczna), robimy zakupy w sklepach internetowych i na aukcjach, rezerwujemy bilety lotnicze, zamawiamy bilety do kina czy teatru, rozmawiamy ze znajomymi i nieznajomymi itd. Niestety Internet posiada swoją ciemną stronę z powodu wielu zagrożeń i każdy użytkownik powinien mieć świadomość, jak i przed czym powinien się ochronić.

Złośliwe oprogramowanie (*malware*, *malicious software*) to wszelkie aplikacje, skrypty itp. mające szkodliwe, przestępcze lub złośliwe działanie w stosunku do użytkownika komputera. Do złośliwego oprogramowania możemy zaliczyć:

- **wirusy komputerowe** – programy bądź fragmenty wrogiego wykonalnego kodu, który dołącza się, nadpisuje lub zamienia inny program w celu reprodukcji samego siebie bez zgody użytkownika,
- **robaki** – złośliwe oprogramowanie podobne do wirusów, rozmnażające się poprzez sieć bądź pamięci przenośne; w przeciwieństwie do wirusów robaki są samodzielnymi programami,
- **trojany** – programy udające przydatne oprogramowanie (często posiadające takie funkcje), jednak wykonujące także inne, ukryte przed użytkownikiem działanie; często umożliwiają dostęp do komputera osobom trzecim,
- **rootkity** – bardzo niebezpieczne narzędzie; zasada ich działania polega na ukrywaniu pewnych procesów bądź programów systemowych i pozwalaniu na włamanie do systemu; rootkity są trudne do wykrycia i mogą ukrywać swoją działalność także przed oprogramowaniem antywirusowym,
- **exploity** – kod umieszczany zazwyczaj na stronach internetowych i w aplikacjach (między innymi pliki typu PDF, doc), umożliwiający poprzez luki w oprogramowaniu bezpośrednie włamanie się do komputera ofiary bądź uruchomienie w nim niebezpiecznego programu,
- **keyloggery** – programy służące do odczytywania i zapisania wszystkich naciśnięć klawiszy, przez co cenne informacje mogą dostać się w niepowołane ręce; warto zwrócić uwagę, że *keyloggery* występują także w postaci sprzętowej – zazwyczaj jest to urządzenie podpinane pomiędzy klawiaturą a komputerem,
- **dialery** – programy, których zadaniem jest łączenie się poprzez modem telefoniczny analogowy lub cyfrowy ISDN z płatnymi numerami 0-700 lub z zagranicą; występują głównie na stronach o treściach pornograficznych.

Jak widać klasyfikacja zagrożeń jest bogata. Trzeba mieć także świadomość, że przedstawiony wykaz nie wyczerpuje tematu, a oprócz tego wiele zagrożeń tego typu może posiadać kilka cech – np. koń trojański może być jednocześnie *keyloggerem*. Z tego powodu niezwykle ważna jest profilaktyka antywirusowa. Przede wszystkim ważne jest posiadanie aktualnego oprogramowania antywirusowego z włączoną ochroną w czasie rzeczywistym. Na polskim rynku mamy dość duży wybór oprogramowania antywirusowego, zawsze też może skorzystać z **oprogramowania darmowego, przeznaczonego do użytku osobistego**. Do takich programów należą między innymi:

Avast free antywirus (http://www.avast.com) poza standardowym antywirusem posiada również antyspyware, antyrootkit oraz antymalware. Jest doskonałym zabezpieczeniem antywirusowym zarówno dla typowych komputerów, jak i dużych serwerów. Program posiada polską wersję językową.

AVG Anti-Virus 9.0 Free Edition (http://free.avg.com) zabezpiecza przed wszelakiego rodzaju szkodliwym oprogramowaniem przy zachowaniu niskich wymagań systemowych i częstych aktualizacjach sygnatur wirusów. W jego skład wchodzi skaner główny oraz skaner rezydentny, monitorujący każdy uruchamiany plik, skaner poczty e-mail (współpracujący m.in. z MS Outlook, Outlook

Express), filtr antyspyware, ograniczający dostęp do informacji dla programów szpiegujących i komponentów reklamowych, a także moduł LinkScanner, którego zadaniem jest ochrona przed niebezpiecznym stronami internetowymi, jeszcze przed ich wyświetleniem. Ocenia on również pod kątem bezpieczeństwa wyniki wyszukiwania Google, MSN i Yahoo.

Avira AntiVir Personal (http://www.free-av.com) to program antywirusowy zaprojektowany z myślą o użytku domowym. Zapewnia rozpoznawanie i ochronę przed wirusami, trojanami, programami typu *backdoor*, robakami internetowymi oraz *keyloggerami*, a także ochronę przed nieznanymi wirusami bootsektorowymi, blokując do nich dostęp, gdy tylko pojawi się w nich plik o podejrzanym formacie.

Microsoft Security Essential (http://www.microsoft. com/security_essentials) to bezpłatne narzędzie służące do zabezpieczania systemu Windows przez różnego rodzaju złośliwym oprogramowaniem, takim jak: wirusy, rootkity, trojany i spyware. Program oferuje bardzo przyjazny i prosty w użyciu interfejs graficzny, trzy tryby skanowania (pełne, skrócone i użytkownika, w którym możemy wybrać dyski, a nawet poszczególne foldery), harmonogram skanowania, automatyczne lub definiowane przez użytkownika aktualizacje baz sygnatur, a także historię wykrytych zagrożeń. Ponadto aplikacja ma małe zapotrzebowanie na zasoby systemowe i umożliwia tworzenie list wykluczeń, pozwalających definiować pliki, lokalizacje, rozszerzenia i procesy pomijane podczas skanowania.

Jeśli chodzi o **oprogramowanie przeznaczone do użytku komercyjnego**, a niewątpliwie szkoły do takich użytkowników należą, to sprawa nie jest już taka prosta. Większość oprogramowania antywirusowego tego rodzaju jest płatna. Wersje dla szkół (lub innych instytucji edukacyjnych) są tańsze niż te przeznaczonych dla typowych firm komercyjnych. Często producenci oprogramowania antywirusowego przedstawiają szkołom specjalne oferty i sprzedają swoje produkty po bardzo niskich cenach. Do tego rodzaju oprogramowania należą:

Arcavir 2010 bezpieczna szkoła z ArcaVir Rescue-Drive (http://www.arcabit.pl) to program antywirusowy polskiego producenta, przeznaczony dla wszystkich komputerów w szkole, posiadający monitor systemu, skaner poczty, *firewall*, skaner stron WWW oraz Bezpieczeństwo rodzinne, dostarczany wraz z pamięcią pendrive, umożliwiającą uruchomienie systemu operacyjnego bezpośrednio z pamięci przenośnej oraz przeskanowanie komputera.

Kaspersky Workspace Security (http://www.kaspersky.pl) to pakiet przeznaczony dla szkół mających do 100 stacji roboczych (za licencję pakietu przeznaczonego do ochrony serwerów plików trzeba dodatkowo zapłacić). Chroni stacje robocze i serwery plików przed wszelkimi rodzajami zagrożeń internetowych, łącznie z wirusami, oprogramowaniem *spyware*, atakami *hackerów* oraz spamem.

MKS_VIR 9.0 Bezpieczna Szkoła (http://www.mks.com.pl) to program antywirusowy przeznaczony dla szkół posiadających do 100 komputerów. Zapewnia pełną ochronę komputera (monitor systemu, skaner dyskowo-plikowy, zaporę sieciową – *firewall*, skaner poczty, filtr spamu oraz monitor rejestru), a także darmową profesjonalną pomoc techniczną w języku polskim. Oprogramowanie dostarczane jest w wersji elektronicznej.

F-secure bezpieczna szkoła (http://www.szkolabezpiecznegointernetu.pl/f-secure) to wielokrotnie nagradzane rozwiązanie zabezpieczające, które zapewnia bezpieczeństwo komputerów podłączonych do Internetu oraz ich pełną wydajność. Dzięki innowacyjnej technologii DeepGuard 2.0., każdy komputer zyskuje kompletną ochronę już w 60 sekund po pojawieniu się nowego zagrożenia. Oprogramowanie ma polską wersję językową, pełne wsparcie techniczne oraz infolinię. Przeznaczony jest dla szkół posiadających do 40 komputerów.

Panda Security Bezpieczn@Szkoła (http://www.pspolska.pl/produkty/oferta_specjalna) – program „Bezpieczn@Szkoła z Panda Security" rozpoczął się 1 października 2008 roku i skierowany jest do dyrektorów szkół publicznych, którzy poszukują kompleksowej ochrony stacji roboczych, serwerów plików i serwerów MS Exchange z centralną konsolą administracyjną. W ramach programu szkoły mogą zakupić w specjalnej cenie roczną licencję bez limitu stanowisk.

Szkoły mogą także skorzystać z darmowego oprogramowania do użytku komercyjnego. W tej grupie programów warto zwrócić uwagę na:

Clam Antywirus (http://clamwin.com) to całkowicie darmowy program antywirusowy, przeznaczony zarówno do użytku osobistego, jak i dla firm. Jego największą wadą jest brak modułu ochrony w czasie rzeczywistym.

Comodo Internet Security (http://www.comodo.com) to pakiet zawierający program antywirusowy i zaporę sieciową, posiadający ochronę w czasie rzeczywistym, całkowicie darmowy, zarówno do użytku domowego, jak i dla firm.

Pisząc o zabezpieczeniu komputerów, nie można pominąć bardzo ważnego oprogramowania, jakim jest zapora sieciowa – tzw. *firewall*. Programy tego typu blokują niepowołany dostęp do komputera poprzez sieć, a także chronią przed wypływaniem danych z komputera do Internetu. W systemach Windows XP wraz z pojawieniem się poprawki ServicePack 2, zapora sieciowa została dodana do systemu, gdzie blokuje nieuprawnione połączenia przychodzące. W systemach Vista oraz Windows 7 zapora potrafi już kontrolować także połączenia wychodzące z komputera. Należy pamiętać, że systemy operacyjne wcześniejsze niż Windows XP SP2 nie posiadają wbudowanej zapory, więc nie należy takich systemów podłączać do Internetu bez zewnętrznej zapory sieciowej.

Na rynku oprogramowania istnieje wiele zapór sieciowych. Są one także wbudowane w pakiety zabezpieczające wraz z antywirusem, tzw. Internet Security. Przykładowo zaporę sieciową posiadają programy Avast czy Comodo Internet Security.

Do popularnych zapór sieciowych, przeznaczonych do użytku domowego, należą:

- Ashampoo FireWall (http://www.ashampoo. com)
- Outpost Firewall Free (http://www.agnitum.com)
- Sunbelt Personal Firewall (http://www.sunbeltsoftware.com)
- Sygate Personal Firewall (http://www.sygate.com)
- ZoneAlarm (http://www.zonelabs.com)

Przy braku zainstalowanego oprogramowania antywirusowego warto skorzystać z możliwości sprawdzenia komputera pod kątem złośliwego oprogramowania przez skaner *online*. Jest to moduł programu antywirusowego, za pomocą którego komputer sprawdza określony przez użytkownika plik lub obszar na dysku twardym, dyskietce czy płycie. Po zakończeniu pracy skaner informuje o liczbie znalezionych wirusów i o tym, ile z nich udało mu się skutecznie usunąć. Aby zastosować skaner, trzeba posłużyć się przeglądarką.

Popularne skanery umożliwiające sprawdzenie komputera znajdują się na stronach:

- http://housecall.trendmicro.com
- http://www.bitdefender.com/scanner/online/free.html
- http://www.pandasecurity.com/homeusers/solutions/activescan
- http://cainternetsecurity.net/entscanner
- http://mks.com.pl/skaner
- http://www.bitdefender.com/scanner/online/free.html
- http://www.arcabit.pl/skaner_on_line

Powyższe skanery potrafią wykryć wirusy, należy pamiętać jednak, że złośliwe oprogramowanie uruchamia się wraz z systemem, dlatego bardzo często skanery online nie są w stanie go usunąć. W takim wypadku pomocne mogą okazać się płyty typu Rescue CD, czyli bootowalne płyty CD (umożliwiające uruchomienie systemu operacyjnego z płyty), zawierające oprogramowanie antywirusowe. Bazują one na różnych dystrybucjach Linuksa i występują w postaci obrazów ISO, które należy wypalić na płycie CD programem do nagrywania płyt (np. darmowy Active@ ISO Burner – http://www.ntfs.com/iso_burner_free.htm).

Należą do nich:

- G-Data Boot CD (http://www.gdata.pl/portal/PL/content/view/116/145)
- Dr. Web LiveCD (ftp://ftp.drweb.com/pub/drweb/livecd)
- ArcaNix (http://bugtraq.arcabit.com/arcanix)
- BitDefender Rescue CD (http://download.bitdefender.com/rescue_cd)
- F-Secure Rescue CD (http://www.f-secure.com/linux-weblog/2009/09/22/rescue-cd-311)
- Vba32 Rescue CD (ftp://anti-virus.by/pub/vbarescue.iso)
- Avira AntiVir Rescue System (http://www.avira.com/en/support/support_downloads.html)
- AVG Rescue CD (http://www.avg.com/us-en/download-file-cd-arl-iso)

Poza wirusami, w Internecie istnieją także programy szpiegujące, tzw. *spyware*, których zadaniem jest gromadzenie informacji o użytkowniku komputera oraz korzystanie z nich bez jego wiedzy. Pomimo że spyware należy do złośliwego oprogramowania, umieszczony został w tym miejscu z dwóch powodów. Po pierwsze, nie wszystkie programy szpiegujące ze względu na swoją „mniej szkodliwą" działalność są wykrywane przez programy antywirusowe, np. potrafią śledzić odwiedzane przez użytkownika strony internetowe i na podstawie ich historii wyświetlać odpowiednie reklamy. Po drugie istnieje specjalistyczne oprogramowanie przeznaczone do wykrywania i usuwania tego typu programów. Do takich aplikacji należą:

- Ad-aware (http://www.lavasoft.com) – program przeznaczony do użytku domowego
- IOBit Security (http://www.iobit.com) – przeznaczony do użytku domowego
- Spybot Search & Destroy (http://www.safer- networking.org) – darmowy, także do użytku komercyjnego

- SUPERAntiSpyware Free Edition (http://www.superantispyware.com) – przeznaczony do użytku domowego
- SpywareBlaster (http://www.javacoolsoftware.com) – przeznaczony do użytku domowego
- Windows Defender (http://www.microsoft.com/poland) – także do użytku komercyjnego, dostępny do pobrania ze strony producenta, jak również poprzez usługę Microsoft Update

Pomimo że powyższe oprogramowanie przeznaczone jest do usuwania oprogramowania typu spyware, potrafi ono także usuwać programy typu Adware czy dialery.

W celu zachowania bezpieczeństwa komputera bardzo istotne i ważne jest systematyczne aktualizowanie systemu operacyjnego i oprogramowania. Działanie takie ma na celu ochronę użytkownika przed oprogramowaniem typu exploit. Ataki ze strony tych programów skierowane są najczęściej na przeglądarki internetowe, jednak zdarzają się także exploity znajdujące się w plikach PDF czy nawet doc. Dlatego, aby uchronić komputer przed tego typu zagrożeniami, należy zawsze na bieżąco aktualizować system i oprogramowanie. Można do tego użyć gotowych programów, których zadaniem jest sprawdzenie aktualnego oprogramowania oraz wyświetlenie dostępnych aktualizacji. Należą do nich:

- Appupdater (http://www.nabber.org/projects/appupdater)
- UpdateStar (http://updatestar.updatestar.com)
- Update Notifier (http://cleansofts.org)

Dbając o bezpieczeństwo komputera, należy zwrócić uwagę także na ochronę prywatności w Internecie. Wszelkie działania (odwiedzane strony, pobrane pliki, zapisane hasła do witryn) wykonywane przy pomocy przeglądarek internetowych umożliwiają ich odtworzenie przez osobę trzecią. Oczywiście każda z przeglądarek internetowych posiada wbudowane mechanizmy do usuwania tych informacji, jednakże warto skorzystać z wyspecjalizowanych pod tym kątem bezpłatnych aplikacji, do których można zaliczyć:

- ATF Cleaner (http://www.atribune.org)
- CCleaner (http://www.piriform.com)
- MRU-Blaster (http://www.javacoolsoftware.com)

Na zakończenie warto dodać, że nie są to wszystkie zagrożenia, z którymi możemy się spotkać w Internecie. Należy zawsze pamiętać, że posiadanie antywirusa, firewalla czy innych programów zabezpieczających nie zapewni 100% bezpieczeństwa, dlatego najważniejsze podczas korzystania z Internetu są profilaktyka i zdrowy rozsądek.

Autor jest starszym specjalistą Działu Technicznego w Ośrodku Edukacji Informatycznej i Zastosowań Komputerów w Warszawie

Seks

W grze pojawiają się nagość i/lub zachowania seksualne lub nawiązania do zachowań o charakterze seksualnym.

Hazard

Gry, które zachęcają do uprawiania hazardu lub go uczą.

Małgorzata Rostkowska

„Prawo autorskie w szkole”

Szanowni Czytelnicy, Koledzy nauczyciele.

Gorąco polecam Państwa uwadze książkę **„Prawo autorskie w szkole”**, wydaną w bieżącym roku przez Ośrodek Edukacji Informatycznej i Zastosowań Komputerów w Warszawie.

Jest to publikacja przeznaczona dla każdego współczesnego nauczyciela. Składa się ze zbioru artykułów, w których można znaleźć informacje, rady i odpowiedzi na większość wątpliwości, związanych z praktycznym stosowaniem prawa autorskiego.

Każdy z nas w swojej pracy stara się wykorzystywać nowe technologie, w tym Internet, aby nauczanie przynosiło coraz lepsze efekty. Często, nawet nieświadomie, wykorzystujemy utwory, które być może chronione są prawem autorskim. Poza tym nierzadko sami jesteśmy twórcami i powinniśmy wiedzieć, na jakich zasadach możemy dysponować naszymi dziełami.

W rekomendowanej książce znajdziemy omówienie aktualnego stanu prawnego dotyczącego prawa autorskiego w aspekcie działalności dydaktycznej nauczyciela, a także treść ustawy o prawie autorskim i prawach pokrewnych. W publikacji zamieszczony został krótki przewodnik dla nauczycieli, dotyczący prawa autorskiego w powiązaniu z technologią informacyjną oraz bardzo interesujące artykuły o wolnej kulturze i nauce w dobie Internetu. Znajdziemy tu także pomoc do sprawdzenia własnej wiedzy na temat prawa autorskiego (a także do sprawdzenia wiedzy swoich uczniów) w postaci testu z prawa autorskiego i praw pokrewnych (na stronie 92), a także informacje na temat publikowania i korzystania z utworów na licencjach *Creative Commons*.

W książce opisane zostały również typy licencji, na których podstawie wykorzystujemy programy komputerowe w edukacji. Godnym polecenia jest też ostatni z zamieszczonych artykułów. Są to refleksje autorki po przeczytaniu książki Lawrence Lessiga „Wolna kultura”, udostępnionej w Internecie na warunkach pozwalających na niekomercyjne rozpowszechnianie i modyfikację. Warto zapoznać się z tym materiałem!

Koniecznie powinniśmy mieć pod ręką tę pozycję, aby w różnych sytuacjach móc do niej zajrzeć, wyjaśnić swoje wątpliwości (co mówi ustawa i jakie są jej interpretacje), poznać dokładnie terminologię (np. nazwy licencji) i dowiedzieć się, jakie są obecnie możliwości radzenia sobie w globalnej sieci (np. kopiowanie grafiki na określonej licencji CC).

Książka „Prawo autorskie w szkole”, której przyświeca idea „Każdy nauczyciel świadomym i prawym twórcą i odbiorcą nauki i kultury w XXI wieku”, dostępna jest w sklepiku Ośrodka Edukacji Informatycznej i Zastosowań Komputerów w Warszawie (ul. Raszyńska 8/10). Pozycja zawiera 128 stron i kosztuje 14 zł. Kontakt ze sklepikiem poprzez stronę OEIiZK http://www.oeiizk.waw.pl.

Autorka jest nauczycielką informatyki w XIV LO im. S. Staszica w Warszawie, doradcą metodycznym w zakresie informatyki dla nauczycieli szkół średnich m. st. Warszawy

Małgorzata Rostkowska

Komentarz do podstawy programowej przedmiotu informatyka

Wstęp

Wymagania opisane w podstawie programowej na każdym etapie edukacyjnym zgrupowane są wokół siedmiu głównych tematów, których brzmienie na poszczególnych etapach niewiele się od siebie różni. Oczywiście pod takimi samymi ogólnymi sformułowaniami kryją się wymagania na różnym poziomie trudności, a często nawet zupełnie inne umiejętności. Na przykład pod hasłem „bezpieczne posługiwanie się komputerem i jego oprogramowaniem w szkole podstawowej", kryją się zupełnie inne umiejętności niż w gimnazjum, a w gimnazjum inne niż w liceum.

Zapisy w nowej podstawie programowej kształcenia ogólnego dotyczącego bezpieczeństwa pracy przy komputerze

Podstawa programowa edukacji wczesnoszkolnej:

Treści nauczania

Zajęcia komputerowe. Uczeń kończący klasę I:

2) wie, jak trzeba korzystać z komputera, żeby nie narażać własnego zdrowia.

Zajęcia komputerowe. Uczeń kończący klasę III:

5) zna zagrożenia wynikające z korzystania z komputera, Internetu i multimediów:

a) wie, że praca przy komputerze męczy wzrok, nadwereża kręgosłup, ogranicza kontakty społeczne,

b) ma świadomość niebezpieczeństw wynikających z anonimowości kontaktów i podawania swojego adresu.

II etap edukacyjny: klasy IV-VI

Cele kształcenia – wymagania ogólne

I. Bezpieczne posługiwanie się komputerem i jego oprogramowaniem; świadomość zagrożeń i ograniczeń związanych z korzystaniem z komputera i Internetu.

Treści nauczania – wymagania szczegółowe

1. Bezpieczne posługiwanie się komputerem i jego oprogramowaniem.

Uczeń:

6) przestrzega podstawowych zasad bezpiecznej i higienicznej pracy przy komputerze, wyjaśnia zagrożenia wynikające z niewłaściwego korzystania z komputera.

7. Wykorzystywanie komputera i technologii informacyjno-komunikacyjnych do rozwijania swoich zainteresowań, zastosowanie komputera w życiu codziennym, opisywanie zagrożeń i ograniczeń związanych z korzystaniem z komputera i Internetu.

Uczeń:

1) opisuje przykłady wykorzystania komputera i sieci Internet w życiu codziennym;

2) szanuje prywatność i pracę innych osób;

3) przestrzega zasad etycznych i prawnych związanych z korzystaniem z komputera i Internetu, ocenia możliwe zagrożenia.

III etap edukacyjny – przedmiot Informatyka

Cele kształcenia – wymagania ogólne

I. Bezpieczne posługiwanie się komputerem i jego oprogramowaniem, wykorzystanie sieci komputerowej; komunikowanie się za pomocą komputera i technologii informacyjno-komunikacyjnych.

V. Ocena zagrożeń i ograniczeń, docenianie społecznych aspektów rozwoju i zastosowań informatyki.

Treści nauczania – wymagania szczegółowe

1. Bezpieczne posługiwanie się komputerem i jego oprogramowaniem, korzystanie z sieci komputerowej.

Uczeń:

5) samodzielnie i bezpiecznie pracuje w sieci lokalnej i globalnej.

3. Komunikowanie się za pomocą komputera i technologii informacyjno-komunikacyjnych

Uczeń:

4) stosuje zasady netykiety w komunikacji w sieci.

7. Wykorzystywanie komputera i technologii informacyjno-komunikacyjnych do rozwijania zainteresowań; opisywanie innych zastosowań informatyki; ocena zagrożeń i ograniczeń, aspekty społeczne rozwoju i zastosowań informatyki.

Uczeń:

2) opisuje korzyści i niebezpieczeństwa wynikające z rozwoju informatyki i powszechnego dostępu do informacji, wyjaśnia zagrożenia związane z uzależnieniem się od komputera;

3) wymienia zagadnienia etyczne i prawne, związane z ochroną własności intelektualnej i ochroną danych oraz przejawy przestępczości komputerowej.

IV etap edukacyjny – zakres podstawowy

Cele kształcenia – wymagania ogólne

I. Bezpieczne posługiwanie się komputerem i jego oprogramowaniem, wykorzystanie sieci komputerowej; komunikowanie się za pomocą komputera i technologii informacyjno-komunikacyjnych.

V. Ocena zagrożeń i ograniczeń, docenianie społecznych aspektów rozwoju i zastosowań informatyki.

Treści nauczania – wymagania szczegółowe

1. Bezpieczne posługiwanie się komputerem, jego oprogramowaniem i korzystanie z sieci komputerowej.

Uczeń:

3) 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.

7. Wykorzystywanie komputera i technologii informacyjno-komunikacyjnych do rozwijania zainteresowań, opisywanie zastosowań informatyki, ocena zagrożeń i ograniczeń, aspekty społeczne rozwoju i zastosowań informatyki.

Uczeń:

1) opisuje szanse i zagrożenia dla rozwoju społeczeństwa, wynikające z rozwoju technologii informacyjno-komunikacyjnych;

2) omawia normy prawne odnoszące się do stosowania technologii informacyjno-komunikacyjnych, dotyczące m.in. rozpowszechniania programów komputerowych, przestępczości komputerowej, poufności, bezpieczeństwa i ochrony danych oraz informacji w komputerze i w sieciach komputerowych.

IV etap edukacyjny – zakres rozszerzony

Cele kształcenia – wymagania ogólne

I. Bezpieczne posługiwanie się komputerem i jego oprogramowaniem, wykorzystanie sieci komputerowej; komunikowanie się za pomocą komputera i technologii informacyjno-komunikacyjnych.

V. Ocena zagrożeń i ograniczeń, docenianie społecznych aspektów rozwoju i zastosowań informatyki.

Treści nauczania – wymagania szczegółowe

7. Uczeń wykorzystuje komputer i technologie informacyjno-komunikacyjne do rozwijania swoich zainteresowań, opisuje zastosowania informatyki, ocenia zagrożenia i ograniczenia, docenia aspekty społeczne rozwoju i zastosowań informatyki:

2) wyjaśnia szanse i zagrożenia dla rozwoju społecznego i gospodarczego oraz dla obywateli, związane z rozwojem informatyki i technologii informacyjno-komunikacyjnych;

3) stosuje normy etyczne i prawne związane z rozpowszechnianiem programów komputerowych, bezpieczeństwem i ochroną danych oraz informacji w komputerze i w sieciach komputerowych;

4) omawia zagadnienia przestępczości komputerowej, w tym piractwo.

Komentarz

Nauczyciel każdego przedmiotu powinien znać przedstawione powyżej cele i treści zawarte w podstawie programowej, dotyczące bezpiecznej pracy ucznia przy komputerze podłączonym do sieci Internet.

Uczeń, w czasie nauki w szkole, będzie poszerzać swoją wiedzę na temat bezpiecznej pracy z komputerem podczas wyodrębnionych wykładów, pokazów i dyskusji. Należy także zadbać o to, aby stosował zdobytą wiedzę w różnych sytuacjach: podczas lekcji informatyki, innych lekcji, kiedy wykorzystuje komputer podczas zajęć dodatkowych i domowych.

Mogą to być drobne sprawy, np. zwrócenie uwagi uczniowi, aby się wyprostował, czy tak ustawił monitor, aby ostre światło nie padało na ekran komputera i nie męczyło oczu.

Innym razem może to być monitorowanie, które strony uczeń przegląda, zainteresowanie się, czy uczniowie nie gromadzą się wokół komputera, aby dokuczać koledze, zwrócenie uwagi na to, czy uczeń napisał temat w liście wysłanym do nauczyciela, sprawdzenie, czy nie kopiuje treści z sieci i nie oddaje jako swoich prac itd.

Ważne jest również, aby nauczyciel własną postawą i przykładem świadczył o prawdziwości i powadze zasad, które wpaja uczniom. Nauczyciel, prezentując własne materiały dydaktyczne, czy to w postaci kart pracy, czy strony WWW lub prezentacji komputerowej, powinien zawsze zwracać uwagę i podkreślać fakt przestrzegania praw autorskich. W prowadzonej z uczniami i rodzicami korespondencji powinien przestrzegać etykiety, nie uczestniczyć w rozsyłaniu spamu i dbać, aby komputer zawsze był dobrze zabezpieczony przed atakami wirusów i *hackerów*.

Ponieważ technologie informacyjno-komunikacyjne coraz głębiej wnikają w codzienne życie uczniów, do starań o bezpieczeństwo dzieci i młodzieży należy także włączyć rodziców uczniów. To oni przede wszystkim muszą poznać zagadnienia, które wiążą się z bezpieczeństwem ich dzieci pracujących lub bawiących się za pomocą komputera, zrozumieć, jakie zagrożenia generują nowoczesne technologie. Jak praca dzieci przy komputerze wpływa na ich zdrowie, jak uchronić dzieci przed przestępcami, którzy przenieśli swoją aktywność do Internetu. A może również zwrócić uwagę, czy ich dziecko samo nie staje się cyberagresorem?

Wśród wielu rodziców nadal panuje przekonanie, że gdy dziecko spędza czas przed komputerem, nic mu nie grozi. W rzeczywistości rodzice mają święty spokój, ale dalekie konsekwencje braku kontroli są często przykre. Rodzice powinni baczniej przyjrzeć się temu, co robią ich dzieci i jaki to ma wpływ na ich rozwój.

Im wcześniej, zarówno w szkole, jak i w domu, rozpoczniemy edukację dotyczącą bezpieczeństwa pracy przy komputerze, tym większa jest szansa na wyrobienie w dziecku właściwych przyzwyczajeń, na jego właściwą postawę i wzbudzenie refleksji.

Źródło

http://www.reformaprogramowa.men.gov.pl/dla-nauczycieli/edukacja-matematyczna-i-techniczna

Autorka jest nauczycielką informatyki w XIV LO im. S. Staszica w Warszawie, doradcą metodycznym w zakresie informatyki dla nauczycieli szkół średnich m. st. Warszawy

Dyskryminacja

Gra pokazuje przypadki dyskryminacji lub zawiera materiały, które mogą do niej zachęcać.

Narkotyki

W grze pojawiają się nawiązania do narkotyków lub jest pokazane zażywanie narkotyków.

Dariusz Skrzyński

Cyberprzestępczość szkolna – zasady odpowiedzialności

Cyberprzestępczość to zbiór wielu różnych przestępstw związanych z funkcjonowaniem systemów i sieci teleinformatycznych, w tym Internetu. W doktrynie prawa, literaturze fachowej i języku potocznym określane są jako „cyberprzestępstwa", „przestępstwa komputerowe" lub „przestępstwa internetowe". Cyberprzestępczość szkolna to nic innego, jak zbiór przestępstw uczniów związanych z ich działalnością komputerową i internetową.

1. Rodzaje cyberprzestępstw

Do najważniejszych cyberprzestępstw szkolnych zaliczamy: *hacking*, *cracking* i *cyberbullying*. Większość z nich nie istnieje samodzielnie, przenikają się nawzajem i uzupełniają. Dlatego, w praktyce, w przypadku odpowiedzialności karnej, sprawcy podlegają kilkunastu zarzutom.

1.1 Hacking

Komputer może być nie tylko narzędziem przestępstwa, ale również stanowić przedmiot ataku. *Hacking*, czyli włamanie do systemów komputerowych, m.in. do serwerów szkoły, jest jednym z najpowszechniejszych przestępstw komputerowych. Stanowi element konieczny do zaistnienia innych cyberprzestępstw, np. oszustw czy kradzieży. Polega na zainfekowaniu komputera ofiary np. koniem trojańskim lub innym programem typu *backdoor* w celu przechwycenia określonych informacji czy ominięcia zabezpieczeń.

1.2 Cracking

Niejednokrotnie działalność sieciowa uczniów dotyczy łamania praw autorskich. Związana jest nie tylko z nielegalnym pozyskiwaniem materiałów z sieci i ich późniejszym wykorzystywaniem (np. tekstów, muzyki, filmów, zdjęć), ale przede wszystkim z łamaniem zabezpieczeń programów komputerowych. Za łamanie zabezpieczeń, oprócz np. kary umownej za naruszenie postanowień umowy lub odpowiedzialności za wyrządzoną szkodę, kodeks karny oraz ustawa o prawie autorskim i prawach pokrewnych przewiduje sankcje karne. Producenci komercyjnego oprogramowania stosują wiele technik zabezpieczających je przed nieuprawnionym użyciem. Sprawca, w celu usunięcia zabezpieczeń, najczęściej tworzy mały program automatyzujący to zadanie, tzw. *crack*. Może być on umieszczony w Internecie lub na nośniku obok programu. Innym rozwiązaniem jest stworzenie generatora kluczy licencyjnych – *keygena*. *Cracker* oraz osoby korzystające z rezultatów jego pracy mają możliwość używania programu nielegalnie lub w sposób niedozwolony przez producenta.

1.3 Cyberbullying

Działaniem bezprawnym uczniów jest w dużej mierze przemoc internetowa, czyli tzw. *cyberbullying*. Jest to prześladowanie, szykanowanie, zastraszanie lub dręczenie innych osób (najczęściej z najbliższego otoczenia sprawcy) z wykorzystaniem Internetu i narzędzi elektronicznych (e-maila, komunikatorów tekstowych typu Gadu-Gadu czy SMS lub głosowych typu Skype, forów internetowych, blogów, a nawet całych stron WWW). Mimo że jest to przede wszystkim poważny problem psychologiczno-społeczny, to dotyczy on również szeregu działań, które są przestępstwami. Oznacza to, że choć cyberprzemoc nie jest zabroniona wprost przepisami prawa, to karalne jest takie zachowanie, które wypełnia znamiona tradycyjnego czynu zabronionego (np. zniewagi, oszustwa, pomówienia, kradzieży, niszczenia danych informatycznych). Przykładowo, jeżeli sprawca wysyła złośliwe SMS-y czy e-maile, takie działania mogą być uznane za przestępstwo gróźb karalnych. Do najczęstszych form *cyberbullyingu* zaliczamy:

- zamieszczanie w sieci filmów nagrywanych np. telefonami komórkowymi, gdzie bohaterami są zarówno koledzy, jak i nauczyciele,
- włamania na konta pocztowe lub konta komunikatorów w celu rozsyłania kompromitujących wiadomości,

- włamania do kont znajomych w portalach internetowych,
- włamania na szkolne serwery w celu skopiowania materiałów egzaminacyjnych,
- kradzież tożsamości z kont społecznościowych,
- tworzenie kompromitujących i ośmieszających stron internetowych.

2. Identyfikacja sprawcy

Złudzenie anonimowości nieletnich sprawców utrwala poczucie bezkarności. Nie oznacza to jednak, że sprawcy nie można zidentyfikować. Ofiary cyberprzemocy często potrafią wskazać sprawcę, którym najczęściej okazuje się kolega ze szkoły, bądź przynajmniej mają przypuszczenie, kto może nim być. Jeżeli jednak nie znają danych sprawcy, powinni skorzystać z uprawnienia do wniesienia skargi na policję, która na tej podstawie zabezpiecza niezbędne dowody oraz kieruje skargę do właściwego sądu. W ramach tych czynności policja jest uprawniona m.in. do ustalenia adresu IP komputera. Może także w toku dalszych czynności służących zabezpieczeniu dowodów próbować ustalić, kto w danym czasie korzystał z danego komputera. W tym celu może zwracać się do dostawców usług internetowych, kawiarenek internetowych, administratorów serwerów, a nawet do administratorów stron czy forów internetowych o udostępnienie takich danych, wyręczając w tym pokrzywdzonego. Dane te są objęte ustawą o ochronie danych osobowych oraz tajemnicą telekomunikacyjną.

Komputer z dostępem do Internetu, co do zasady, posiada własny niezmienny adres IP, na podstawie którego policja w przypadku złamania prawa może ustalić właściciela. Adres IP w połączeniu z dokładnym określeniem czasu jednoznacznie identyfikuje urządzenie w sieci Internet. A to pozwala zidentyfikować użytkownika. W przypadku użytkowników, którzy nie są na stałe włączeni do sieci, lecz korzystają z modemu i linii telefonicznej, z chwilą nawiązania połączenia domenowego z dostawcą Internetu otrzymują oni adres IP. W takiej sytuacji, aby określić, który komputer korzystał z danego adresu IP, należy przyporządkować datę i godzinę korzystającemu z takiego adresu IP. Korzystanie z mechanizmów dynamicznego przydzielania adresu IP może utrudniać zidentyfikowanie konkretnego komputera z danym adresem IP. Pomocne są w tym przypadku dane billingowe, które zawierają informacje m.in. o adresie abonenta, liczbie jednostek taryfowych połączenia, numerach, z którymi uzyskał połączenie, dacie i czasie trwania połączenia. Operator jest obowiązany do rejestracji danych wykonywanych usług telekomunikacyjnych w zakresie umożliwiającym ustalenie należności za wykonanie tych usług. Informacje te są tajemnicą komunikacyjną na podstawie ustawy o prawie telekomunikacyjnym. Ujawnienie tych informacji może nastąpić mocą postanowienia sądu, prokuratora lub na podstawie odrębnych przepisów, np. ustawy o policji.

3. Odpowiedzialność karna a cywilna

W polskim prawie wyróżniamy odpowiedzialność karną i cywilną. Odpowiedzialność karna wynika z przepisów kodeksu karnego oraz innych ustaw, które zawierają przepisy karne (np. ustawy o prawie autorskim). Natomiast odpowiedzialność cywilna wynika z przepisów kodeksu cywilnego. Pomiędzy nimi istnieją istotne różnice. Odpowiedzialność cywilna ma postać wyłącznie majątkową i powstaje dopiero wtedy, gdy zostanie wyrządzona szkoda. Odpowiedzialność karna ma postać osobistą i majątkową. Te dwa rodzaje odpowiedzialności mogą być dochodzone równolegle. Jedna nie wyklucza drugiej.

4. Odpowiedzialność karna nieletnich

Odpowiedzialność karna uczniów z uwagi na ich wiek jest ograniczona. Prawo karne w stosunku do uczniów posługuje się pojęciem nieletniego, czyli osoby, która w momencie popełnienia czynu zabronionego nie ukończyła 17 lat. Dzieci do lat 13 nie mogą być ukarane za popełnione czyny będące przestępstwami. Jeżeli sprawca znajduje się między 13 a 17 rokiem życia, ma wobec niego zastosowanie ustawa o postępowaniu w sprawach nieletnich. W tym przypadku orzeka sąd rodzinny, a najdotkliwszą sankcją z możliwych do zastosowania jest umieszczenie w zakładzie poprawczym. Kodeks karny dotyczy uczniów, którzy ukończyli lat 17. W wyjątkowych sytuacjach możliwe jest pociągnięcie do odpowiedzialności sprawców, którzy ukończyli lat 15. Oznacza to, że uczeń szkoły ponadgimnazjalnej za popełnienie czynów będących przestępstwami będzie odpowiadać na takich samych zasadach, jak każda osoba dorosła. Natomiast uczeń gimnazjum będzie odpowiadał na podstawie ustawy o postępowaniu w sprawie nieletnich (np. w sytuacji włamania do kont pocztowych, komunikatorów lub portali internetowych). Większość nielegalnych działań uczniów to sprawy podlegające powództwu cywilnemu. Oznacza to, że poszkodowany może wystąpić z prywatnym aktem oskarżenia (np. w przypadku zniewagi lub pomówienia). Może jednak zwrócić się do policji, by pomogła ustalić sprawcę. Jeżeli następstwem działań uczniów jest ujawnienie danych osobowych, to wystarczy tylko złożyć zawiadomienie o podejrzeniu

popełnienia przestępstwa, bowiem tego typu przestępstwo jest ścigane z urzędu. Ofiarami przemocy internetowej uczniów są przede wszystkim inni uczniowie. Poszkodowanymi mogą być również osoby dorosłe, w tym nauczyciele. W przypadku nielegalnych działań tego typu w stosunku do nauczycieli zastosowanie ma również przepis art. 63 Karty Nauczyciela. Zgodnie z tym przepisem nauczyciel, podczas lub w związku z pełnieniem obowiązków służbowych, korzysta z ochrony przewidzianej dla funkcjonariuszy publicznych na zasadach określonych w kodeksie karnym. Ochrona ta zapewnia surowsze kary za znieważenie, naruszenie nietykalności cielesnej oraz czynną napaść na ich osobę. Czyny te stają się przestępstwami w momencie, gdy są wymierzone w nauczyciela wykonującego swoje obowiązki. Organ prowadzący szkołę i dyrektor szkoły są obowiązani z urzędu występować w obronie nauczyciela, gdy ustalone dla nauczyciela uprawnienia zostaną naruszone.

5. Odpowiedzialność cywilna małoletnich

Prawo cywilne w stosunku do uczniów posługuje się pojęciem małoletniego, czyli osoby, która nie ukończyła lat 18. Inaczej jednak kształtuje się odpowiedzialność małoletniego, który nie ukończył lat 13, a inaczej małoletniego w wieku od 13 do 18 roku życia. Małoletni, który nie ukończył lat 13, nie posiada zdolności do czynności prawnych oraz nie ponosi odpowiedzialności za wyrządzoną szkodę (nie można mu przypisać winy). Związane jest to z tym, iż osoby takie ze względu na swój stopień rozwoju psychofizycznego nie są w stanie właściwie kierować swym postępowaniem czy też ocenić skutków swoich czynów. Takiej oceny dokonał ustawodawca, tworząc kodeks cywilny. Nie oznacza to jednak, że małoletni poniżej 13 roku życia są całkowicie bezkarni. Odpowiedzialność ta jest przeniesiona na osoby sprawujące opiekę nad nim (rodziców, prawnych opiekunów, nauczycieli, instruktorów). Ich odpowiedzialność wynika ze sprawowanego nadzoru. Nadzorujący może uwolnić się od odpowiedzialności, gdy udowodni, że nadzór był sprawowany należycie. W sytuacjach wyjątkowych, gdy nie da się dowieść winy nadzoru, gdy ściągnięcie odszkodowania od osoby winnej z tytułu nadzoru jest niemożliwe lub utrudnione, jeżeli brak jest osób zobowiązanych do nadzoru, można dochodzić odszkodowania bezpośrednio od dziecka.

Małoletni, który ukończył lat 13, a nie ukończył 18 roku życia, z uwagi na ograniczoną zdolność do czynności prawnych może, ale nie musi, odpowiadać za wyrządzoną szkodę na zasadzie winy. O tym decyduje każdorazowo ocena sądu, czy z uwagi na wiek osiągnął on dostateczną dojrzałość, by w pełni przypisać mu winę. Małoletni musi mieć rozeznanie własnego działania i jego skutków oraz zdawać sobie sprawę z naganności swojego zachowania. W przypadku uznania winy, problemem jest brak własnego majątku małoletniego – najczęściej ciężar naprawienia szkody ponoszą rodzice.

Z *cyberbullyingiem* związany jest temat ochrony wizerunku. Obraz człowieka może być na różne sposoby utrwalany, np. na fotografii, plakacie, rzeźbie, filmie, co rozszerza także możliwość jego bezprawnego wykorzystania. Takie zdarzenia niejednokrotnie powodują naruszenie praw osobistych i majątkowych osoby portretowanej. W praktyce szkolnej takiego rodzaju sytuacje mają miejsce w przypadku zamieszczania na stronach internetowych wizerunku osoby sfotografowanej lub sfilmowanej. Zarówno postanowienia kodeksu cywilnego, jak i ustawy o prawie autorskim zakazują rozpowszechniania wizerunku bez zgody osoby przedstawianej. W praktyce zatem wymagana jest zgoda na rozpowszechnianie wizerunku na stronie internetowej, np. utrwalonego zdjęciem lub nagraniem filmowym (również telefonem komórkowym). Należy pamiętać, że nawet „zamazanie" twarzy lub ukrycie jej za czarnym paskiem nie zwalnia nas z odpowiedzialności. W takiej sytuacji może również dojść do ujawnienia danych osobowych, co jest już przestępstwem.

Autor jest prawnikiem, specjalistą z zakresu prawa oświatowego, prawa pracy i prawa autorskiego

Doskonałe bezpieczeństwo i nietykalność własności oraz osoby: oto prawdziwa wolność społeczna.

Antoine de Rivarol

Nagabywanie dzieci dla celów seksualnych, tzw. grooming

Z dniem 8 czerwca 2010 roku weszła w życie nowelizacja kodeksu karnego. Wprowadziła nowy typ przestępstwa seksualnego wobec małoletnich poniżej lat 15.

Nowelizacja wynika z konieczności dostosowania polskiego prawa do postanowień Konwencji Rady Europy z Lanzarote o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych, podpisanej przez Polskę w dniu 25 października 2007 roku. Jest również próbą reakcji na wzmagające się zjawisko wykorzystywania seksualnego dzieci przez osoby dorosłe, możliwe dzięki nawiązywaniu za pomocą technologii komunikacyjnych kontaktu z dziećmi i doprowadzaniu do spotkania z nimi. Zjawisko to, znane jako *grooming*, wiąże się z zachęcaniem dziecka do udziału w czynności seksualnej, np. poprzez obietnicę nagrody, dyskutowanie na temat intymnych zachowań, prezentowanie treści o charakterze pornograficznym w celu przełamania oporu czy też zahamowań dotyczących sfery seksualnej.

Wykorzystanie seksualne dziecka w kontekście *groomingu* może przybierać różne formy, obejmujące również wykorzystanie w celach związanych z pornografią. Stąd wprowadzenie karalności czynu polegającego na nawiązywaniu kontaktu z małoletnim poniżej 15 lat za pośrednictwem Internetu lub telefonu i podejmowaniu czynności zmierzających do spotkania z nim w celu popełnienia przestępstwa gwałtu, obcowania płciowego lub produkowania bądź utrwalania treści pornograficznych z jego udziałem.

Karane jest również samo złożenie propozycji obcowania płciowego lub udziału w produkowaniu lub utrwalaniu treści pornograficznych dziecku poniżej 15 roku życia.

Przestępstwa te zagrożone są karą do 3 lat pozbawienia wolności.

Aneta Kwiecień i Dariusz Kwiecień

Kilka uwag na temat bezpieczeństwa (prawnego) w kontekście nauczania online

Problem bezpieczeństwa w kontekście organizacji procesu dydaktycznego wspieranego technikami nauczania online jest wielopoziomowy. Począwszy od ochrony dostępu do materiałów, czym zainteresowani będą ich autorzy, poprzez szeroko rozumiane bezpieczeństwo w sieci w odniesieniu szczególnie do osób niepełnoletnich, po ochronę danych osobowych.

Artykuł nie ma charakteru wykładni prawnej, jego zadaniem jest spopularyzowanie świadomości istnienia pewnych wymogów.

Zamierzeniem autorów artykułu jest zakreślenie kilku zagadnień bliskich tematyce bezpieczeństwa i zgodności z obowiązującym prawem w kontekście organizacji i prowadzenia szkoleń *online*, jako instytucjonalnych, zorganizowanych projektów lub elementów wspomagających tradycyjne metody kształcenia. Kierowany jest do osób, które są zaangażowane w organizację i prowadzenie nauczania *online* lub nauczania wspieranego elementami na odległość, a także do osób, które uczestniczą w tego rodzaju formach kształcenia.

Ochrona danych osobowych

Jest to jedno z kluczowych zagadnień towarzyszących organizacji form kształcenia na odległość. Korzystając z wybranej platformy, umożliwiającej publikowanie materiałów i opracowywanie ćwiczeń *online*, użytkownicy muszą posiadać indywidualne konta, przez które są identyfikowani w systemie. Należy ograniczyć się do zbierania minimum informacji o użytkowniku, które są niezbędne w procesie dydaktycznym. Nigdy nie powinno się zbierać danych wrażliwych[1], nawet gdyby takie informacje nie były zapisywane w bazie w sposób jawny[2]. Niektórych jednak nie sposób pominąć. Zwykle jest to imię i nazwisko, adres e-mail oraz klasa czy grupa słuchaczy. Są to więc dane, za pomocą których możliwe jest w łatwy sposób[3] zidentyfikowanie konkretnej osoby[4], a przez to podlegają one ustawowej ochronie. Ochrona ta dotyczy uniemożliwienia dostępu do danych przez osoby nieuprawnione[5]. Wykroczeniem jest nie tylko bezpośrednie udostępnienie zasobów zawierających dane osobowe, ale także umożliwienie (także niecelowe) dostępu do nich[6].

Zgodnie z ustawą przetwarzanie danych osobowych w kontekście nauczania na odległość możliwe jest tylko wtedy, gdy jest wyraźna (nie domniemana) zgoda osoby, której te dane dotyczą[7]. Zgoda może być wyrażona jednokrotnie, pod warunkiem

1 Zabrania się przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym (Dz. U. z 1997 r. Nr 133 poz. 883, ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, rozdz. 1, art. 27, ust. 1).

2 Zabronione jest nadawanie ukrytych znaczeń elementom numerów porządkowych w systemach ewidencjonujących osoby fizyczne, ibidem, rozdz. 1, art. 28, ust. 3.

3 Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań, ibidem.

4 W rozumieniu ustawy, za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (Dz. U. z 1997 r. Nr 133 poz. 883, ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, rozdz. 1, art. 6, ust. 1).

5 Zabezpieczenie danych w systemie informatycznym – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych, zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem, ibidem, art. 7, ust. 2b.

6 Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych, udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2, ibidem, rozdz. 8, art. 51, ust. 1. Kto administrując danymi, narusza, choćby nieumyślnie, obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku, ibidem, art. 52.

7 Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy: osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych, ibidem, rozdz. 1, art. 23, ust. 1, pkt. 1.

iż nie zmienia się cel przetwarzania danych[8]. System musi zapisywać w bazie informacje, kiedy i przez kogo dane zostały wprowadzone oraz komu zostały przekazywane[9].

Tworząc bazę i przetwarzając dane osobowe słuchaczy, należy określić administratora, przejmującego odpowiedzialność za ochronę zbioru danych. Osoby umieszczające swoje dane w bazie muszą być poinformowane o tym, kto jest ich administratorem (wraz z jego siedzibą), w jakim celu jest tworzona baza oraz muszą mieć możliwość dostępu do tych danych i ich zmiany[10]. Na wniosek osoby, której dane dotyczą, należy udzielić również informacji, gdzie dane i w jakim zakresie zostały przekazane[11].

Znaczenie ma także miejsce przechowywania bazy danych. Coraz częściej korzysta się z usług hostingowych. Oznacza to, że serwer, na którym przechowywane są dane osobowe, fizycznie znajduje się poza siedzibą instytucji, która jest ich administratorem. W takim przypadku należ podpisać umowę dotyczącą udostępnienia i przetwarzania danych, określającą zakres dostępu i przetwarzania[12].

Jak już zostało wspomniane, administrator danych osobowych zobowiązany jest do ich zabezpieczenia[13]. Zabezpieczenia i czynności prewencyjne zostały podzielone dla wygody na dwie grupy: organizacyjne i informatyczne. Do organizacyjnych czynności należą: posiadanie przez instytucję polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych[14]. Obowiązkiem administratora danych jest również zgłoszenie zasobu do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych[15]. Szkoły są jednak zwolnione z tego obowiązku, gdy celem prowadzonej przez nie bazy jest wystawienie odpowiedniego dokumentu[16].

Z uwagi na to, iż w omawianym procesie kształcenia na odległość wykorzystana jest globalna sieć Internet, ochrona danych od strony informatycznej klasowana jest na poziomie wysokim[17]. Tak więc system musi spełniać następujące warunki:

- zapisana jest w nim informacja dotycząca daty wprowadzenia danych,
- każdy użytkownik musi posiadać niepowtarzalny identyfikator (często jest to login),
- jeżeli do systemu zostają wprowadzone dane przez osoby, których one nie dotyczą, musi być zapisana informacja o źródle tych danych oraz zapisana informacja, komu dane zostały udostępnione,
- system musi zapewniać zabezpieczenie dostępu do danych na czas nieobecności przy komputerze osoby uprawnionej (np. wygaszacz ekranu wymuszający podanie hasła, wygaśnięcie sesji połączeniowej),
- system musi kontrolować dostęp do danych oraz zapisywać informacje dotyczące czasu dokonanych zmian w bazie, jak również informacje, kto jest autorem tych zmian,
- system musi zapewniać możliwość archiwizowania danych na wypadek ich uszkodzenia lub utraty,
- osoby posiadające dostęp do danych muszą posługiwać się tzw. mocnym hasłem, czyli takim, które składa się z co najmniej ośmiu znaków, w których skład wchodzą małe i wielkie litery oraz przynajmniej jedna cyfra lub znak specjalny. Hasło powinno być zmieniane przynajmniej jeden raz w ciągu 30 dni.

Autorzy artykułu zdają sobie sprawę, że po chociażby pobieżnym przeczytaniu powyższej części artykułu można powątpiewać w sens działań zmierzających do wdrożenia elementów nauczania na odległość w warunkach szkolnych. Wiele jest bowiem wymagań i obowiązków obłożonych sankcjami karnymi. Jednak zachowanie wymogów obowiązującego prawa jest przede wszystkim warunkiem bezpieczeństwa dla osób organizu-

8 Osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych, ibidem, ust. 2.
9 Ibidem, rozdz. 5, art. 38.
10 Ibidem, rozdz. 1, art. 24 oraz art. 32.
11 Ibidem, art. 33, ust. 1, pkt 4.
12 Administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych, ibidem, art. 31, ust. 1.
13 Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne, zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, ibidem, rozdz. 5, art. 36, ust. 1.
14 Dz. U. z 2004 r. Nr 100, poz. 1024, rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, § 3.
15 Dz. U. z 1997 r. Nr 133 poz. 883, ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, rozdz. 6, art. 40.
16 Ibidem, art. 43.
17 Dz. U. z 2004 r. Nr 100 poz. 1024, rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, § 6, ust. 4.

jących tego typu formy kształcenia. Zastosowanie się do wymogów, które zostały zakreślone, jest gwarantem nietykalności dla organizatorów w sytuacji dostania się przechowywanych danych w niepowołane ręce.

Ochrona zasobów

Tym zagadnieniem zajmuje się prawo autorskie. Na wstępie należy zauważyć, iż prawo autorskie nie jest skierowane przeciwko odbiorcom i twórcom materiałów dydaktycznych (w kontekście nauczania *online*). Prawo autorskie stoi na straży nierozerwalnej więzi autora z jego dziełem. W rozumieniu prawa każdy przejaw działalności twórczej o indywidualnym charakterze jest utworem i podlega ochronie prawnej[18]. Nie jest więc ważne, czy utwór ma jakąkolwiek wartość i przeznaczenie, nie jest też wymagane, aby autor utworu poczynił jakiekolwiek kroki celem jego ochrony[19]. Nie jest też ważne, czy autor utworu jest znany[20].

Istnieją jednak utwory, które nie podlegają ochronie. Ochronie podlega sposób wyrażenia, nie są objęte ochroną odkrycia, idee, procedury, metody i zasady działania oraz koncepcje matematyczne[21]. Ponadto przedmiotem prawa autorskiego nie są akty normatywne i urzędowe projekty, urzędowe dokumenty, materiały, znaki i symbole, opublikowane opisy patentowe lub ochronne oraz proste informacje prasowe[22].

Na czym więc polega prawna ochrona utworów w kontekście organizacji elementów nauczania na odległość? Przede wszystkim dotyczy publikowania materiałów dydaktycznych. Jeżeli my sami jesteśmy autorami tych materiałów, możemy (z pewnymi zastrzeżeniami) robić z nimi co chcemy, także publikować. Niejednokrotnie jednak korzysta się z cudzych materiałów, które zostały wcześniej opublikowane. Warto więc zapoznać się przynajmniej z podstawowymi zasadami, którymi powinno się kierować, korzystając z czyjegoś dorobku.

Prawo autorskie nie jest tak restrykcyjne, jak mogłoby się to wydawać. Nie wszystko jest zakazane, nie wszystko jest obłożone obowiązkiem uzyskania zgody autora na wykorzystanie jego dzieła. Najwięcej możliwości istnieje w zakresie tzw. własnego użytku osobistego. Jedynym warunkiem jest wykorzystanie utworu bez uzyskania korzyści materialnych oraz ograniczenie się do kręgu rodziny i bliskich znajomych[23]. Niestety, z tego prawa nie można skorzystać w kontekście organizacji nauczania na odległość, jednak warto mieć jego świadomość. Przygotowując materiały dydaktyczne, z pewnością można skorzystać z tzw. prawa cytatu. W myśl ustawy można przytaczać urywki rozpowszechnionych utworów lub drobne utwory w całości w utworach stanowiących samoistną całość. Ustawa jednak określa okoliczności, którymi są: potrzeba wyjaśnienia, analizy krytycznej, nauczanie lub prawa gatunku[24]. Ustawa nie definiuje pojęcia „urywki", jak również określenia „drobne utwory". Wydaje się, iż pozostawione jest to rozsądkowi i uczciwości osób korzystających z prawa cytatu. Są jednak takie utwory, które można dowolnie wykorzystywać, także w celach majątkowych, bez uzyskania na to zgody autora (autorów) lub jego spadkobiercy. Autorskie prawa majątkowe gasną bowiem z upływem siedemdziesięciu lat od śmierci autora lub najstarszego współautora. Bez obawy można więc zamieścić w sieci Internet wszystkie dzieła Mickiewicza bez uzyskania jakiejkolwiek zgody[25].

Należy jednak pamiętać o pewnym ważnym szczególe. Powyżej zostało powiedziane, iż ochronie prawnej nie podlegają akty normatywne, czyli np. teksty ustaw czy też dzieła wieszcza narodowego. Jednak niezgodne z prawem będzie skanowanie ich z opublikowanych źródeł drukowanych i zamieszczanie w sieci Internet. Zgodnie z ustawą ochronie podlega bowiem sposób wyrażania, czyli w tym wypadku np. skład tekstu. W tym przypadku rozwiązaniem będzie samodzielne przepisanie tekstu (sama treść tych utworów nie jest chroniona) lub podanie linku do odpowiednich zasobów internetowych. Nawiasem mówiąc, link można zamieszczać w każdej sytuacji bez uzyskania na to zgody autora, gdyż w tym przypadku nie my publikujemy jego utwór, a jedynie wskazujemy miejsce publikacji. O skanowaniu, czyli digitalizacji zbiorów oraz ich udostępnieniu ustawa mówi w innym miejscu. Daje takie prawo bibliotekom, archiwom i szkołom, jednakże tylko za pomocą terminali (komputerów) znajdujących się na terenie tych jednostek[26]. Prawo to nie dotyczy więc udostępnia-

18 Dz. U. z 1994 r. Nr 24 poz. 83, ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, rozdz. 1, art. 1, ust. 1.
19 Ibidem, ust. 4.
20 Dopóki twórca nie ujawnił swojego autorstwa, w wykonywaniu prawa autorskiego zastępuje go producent lub wydawca, a w razie ich braku – właściwa organizacja zbiorowego zarządzania prawami autorskimi, ibidem, rozdz. 2, art. 8, ust. 3.
21 Ibidem, rozdz. 1, art. 1, ust. 2, pkt. 1.
22 Ibidem, art. 4.
23 Ibidem, rozdz. 3, art. 23
24 Ibidem, art. 29, ust. 1.
25 Ibidem, rozdz. 4, art. 36, ust. 1.
26 Ibidem, rozdz. 3, art. 28.

nia tychże materiałów w sieci Internet. Wszelkie opublikowane materiały można jednak nieodpłatnie odtwarzać w warunkach szkolnych, jednakże z zachowaniem wymogu braku korzyści materialnych z tego tytułu. Nie można zapomnieć jeszcze o jednym warunku korzystania z cudzych utworów. Za każdym razem trzeba wymienić imię i nazwisko twórcy (w miarę możliwości) oraz źródło pochodzenia materiału[27].

Istnieje nietypowa grupa utworów, które, aby mogły zostać opublikowane, wymagają zgody nie tylko samego autora. Są to fotografie przedstawiające ludzi. Zgoda na opublikowanie tego typu utworu wymagana jest od jego autora, ale także, w pewnych okolicznościach, od osoby przedstawionej na zdjęciu[28]. Ograniczeniom publikowania, nie tylko z uwagi na potrzebę uzyskania zgody autora, podlega również korespondencja[29].

Przygotowując materiały dydaktyczne, sami przejmujemy rolę autorów. W tym kontekście ważne mogą być zasady dotyczące autorskich praw majątkowych. Zachodzi bowiem pytanie, kto jest właścicielem materiałów wykonanych w ramach pracy (np. jako wykładowca, nauczyciel), czyli kto ma do nich prawa majątkowe – autor czy instytucja, w której autor w danym czasie pracował, ewentualnie która z instytucji zatrudniających autora w czasie, gdy materiały zostały wykorzystane (opublikowane). Ustawa zajmuje w tym kontekście dosyć jasne stanowisko – jeżeli utwór powstał w wyniku umowy z pracodawcą, prawa majątkowe pozostają po stronie pracodawcy[30].

Ochrona słuchaczy

Należy zwrócić uwagę na jeszcze jeden aspekt związany z bezpieczeństwem w kontekście nauczania zdalnego. Opracowując materiały dydaktyczne, należy przekazać odbiorcom, najczęściej poprzez linki, źródła opublikowane w sieci Internet. Są one doskonałym uzupełnieniem materiałów autora oraz wskazują odbiorcom bogactwo zasobów globalnej sieci, którą sami mogą wykorzystać w procesie samokształcenia. Częstym błędem, którego dopuszczają się autorzy materiałów, jest pobieżne przeglądanie polecanych źródeł. Z powodu braku czasu czytamy niejednokrotnie tylko nagłówki, nie zagłębiając się w treść polecanych materiałów. Jest to oczywisty błąd, gdyż nie wszystkie zasoby w sieci Internet są godne rekomendowania. Globalna sieć stwarza możliwości łatwej publikacji bez cenzury, ale także bez potwierdzenia merytorycznej poprawności. Zdarza się również, że na znanych stronach pojawiają się odnośniki (linki) do wątpliwych merytorycznie i moralnie zasobów sieci. Należy na to zwrócić tym większą uwagę, czym młodsi są adresaci naszych materiałów. Z pewnością żaden nauczyciel nie chciałby stać się, choćby w pośredni sposób, źródłem treści pornograficznych, rasistowskich czy w inny sposób niezgodnych z prawem. Jedyną więc radą jest dokładne zapoznanie się z witrynami, do których kierowani są słuchacze. Należy tworzyć odnośniki do konkretnych artykułów i zasobów, nie do całej witryny, na której uczeń musiałby dopiero poszukiwać polecanego materiału.

Autorzy są świadomi, iż artykuł ten nie wyczerpuje tematyki bezpieczeństwa w kontekście organizacji kształcenia na odległość, a porusza jedynie wybrane zagadnienia. Z tego powodu zachęcają do czytania ustaw i rozporządzeń. Są one pisane zaskakująco prostym językiem, dalekim od czysto prawnych, niejednokrotnie niezrozumiałych określeń. Poznając obowiązujące prawo, dajemy sobie sami poczucie bezpieczeństwa, jesteśmy również świadomi tego, iż sami stajemy się podmiotem prawa, a co za tym idzie, mamy nie tylko względem jego obowiązki, ale również prawa.

Aneta Kwiecień jest pracownikiem działu szkoleń i kadr w Państwowym Funduszu Rehabilitacji Osób Niepełnosprawnych
Dariusz Kwiecień jest nauczycielem konsultantem w Ośrodku Edukacji Informatycznej i Zastosowań Komputerów w Warszawie

[27] Można korzystać z utworów w granicach dozwolonego użytku pod warunkiem wymienienia imienia i nazwiska twórcy oraz źródła. Podanie twórcy i źródła powinno uwzględniać istniejące możliwości, ibidem, art. 34.

[28] Rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej. W braku wyraźnego zastrzeżenia zezwolenie nie jest wymagane, jeżeli osoba ta otrzymała umówioną zapłatę za pozowanie.

Zezwolenia nie wymaga rozpowszechnianie wizerunku:

1) osoby powszechnie znanej, jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych;

2) osoby stanowiącej jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza, ibidem, rozdz. 10, art. 81.

[29] Jeżeli osoba, do której korespondencja jest skierowana, nie wyraziła innej woli, rozpowszechnianie korespondencji, w okresie dwudziestu lat od jej śmierci, wymaga zezwolenia małżonka, a w jego braku, kolejno zstępnych, rodziców lub rodzeństwa, ibidem, art. 82.

[30] Jeżeli ustawa lub umowa o pracę nie stanowią inaczej, pracodawca, którego pracownik stworzył utwór w wyniku wykonywania obowiązków ze stosunku pracy, nabywa z chwilą przyjęcia utworu autorskie prawa majątkowe w granicach wynikających z celu umowy o pracę i zgodnego zamiaru stron, ibidem, rozdz. 2, art. 12, ust. 1.