RAPORT


# Standardy bezpieczeństwa e-podręczników

Opracował: Marcin Sołodki

# Standardy bezpieczeństwa e-podręczników

Raport dla autorów e-podręczników
oraz twórców platformy do upowszechniania e-podręczników
dotyczący bezpieczeństwa pracy z e-podręcznikami
użytkowników w wieku od 6 do 18 lat

Opracował: Marcin Sołodki

Ośrodek Rozwoju Edukacji
Warszawa 2013

Projekt graficzny

**Studio Kreatywne Małgorzaty Barskiej**

Redakcja i korekta

**Elżbieta Gorazińska**

Redakcja techniczna

**Barbara Jechalska**

**Ośrodek Rozwoju Edukacji**



przygotowany na podstawie umowy zawartej 10 lipca 2013 roku

pomiędzy Ośrodkiem Rozwoju Edukacji a Marcinem Sołodkim.

Ośrodek Rozwoju Edukacji

00-478 Warszawa

Aleje Ujazdowskie 28

www.ore.edu.pl

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

# Spis treści

# Wstęp

Raport został przygotowany na zlecenie Ośrodka Rozwoju Edukacji w celu dostarczenia wytycznych i rekomendacji autorom treści e-podręczników oraz twórcom platformy do upowszechniania e-podręczników.

Wytyczne obejmują tematykę bezpieczeństwa dzieci i młodzieży korzystających z komputera i internetu, ze szczególnym uwzględnieniem pracy z zasobami edukacyjnymi online zawartymi w e-podręcznikach.

Z uwagi na szeroki przekrój wiekowy odbiorców e-podręczników – grupa uczniów od 6 do 18 lat – niezbędne jest zaprezentowanie ich autorom nowych trendów obecnych w szerokiej aktywności internetowej dzieci i młodzieży. Z tego powodu konieczne stało się przygotowanie wykazu zagrożeń, uwzględniającego szczegółowy podział użytkowników internetu na grupy wiekowe: 6–9 lat, 10–12 lat, 13–15 lat, 16–18 lat.

Rodzaje aktywności i wynikające z nich zagrożenia dla dzieci i młodzieży zostały przedstawione przez pryzmat doświadczeń autora, nabytych w pracy w omawianym obszarze tematycznym, a także na podstawie badań przeprowadzonych między innymi przez Fundację Dzieci Niczyje oraz firmy Orange i Kaspersky.

W opracowaniu wykorzystano wyniki badań z ostatnich kilku lat – zarówno polskich, jak i zagranicznych – ukazujących różnice między internautami zamieszkującymi w wielu częściach Europy.

Do opracowania raportu posłużyły wyniki następujących badań:

- „EU NET ADB. Badanie nadużywania internetu przez młodzież w Polsce" – raport szczegółowy z części ilościowej, (2012), Fundacja Dzieci Niczyje (www.fdn.pl/eu-net-adb).
- „EU Kids Online. Polskie dzieci w internecie. Zagrożenia i bezpieczeństwo na tle danych dla UE", (2010), Szkoła Wyższa Psychologii Społecznej (www.swps.pl/warszawa/nauka-i-rozwoj/eu-kids-online).
- „EU Kids Online. Zagrożenia i bezpieczeństwo w internecie z perspektywy dzieci w Europie", (2010), Szkoła Wyższa Psychologii Społecznej (www.swps.pl/warszawa/nauka-i-rozwoj/eu-kids-online).


Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

- „Rodzice wobec zagrożeń dzieci w internecie", (2008) – próba obejmująca 500 rodziców, TNS OBOP dla Fundacji Dzieci Niczyje (www.dzieckowsieci.fdn.pl/badania).
- „Zagrożenia wobec dzieci w internecie", (2008), Geminius dla Fundacji Dzieci Niczyje (www.dzieckowsieci.fdn.pl/badania).
- „Dzieci aktywne online w oczach rodziców", (2008) – wyniki badań dotyczących poglądów rodziców na temat korzystania przez dzieci z internetu oraz świadomości zagrożeń płynących z sieci, Geminius we współpracy z Fundacją Dzieci Niczyje (www.dzieckowsieci.fdn.pl/badania).
- „Dzieci aktywne online", (2007) – raport z badań aktywności online użytkowników internetu w wieku 7–14 lat, dotyczący m.in. czasu spędzanego w sieci i poszukiwanych treści, Geminius dla Fundacji Dzieci Niczyje (www.dzieckowsieci.fdn.pl/badania).
- „Niebezpieczne treści online", (2013) – badanie globalne, Kaspersky (www.kaspersky.pl).

Oprócz klasyfikacji zagrożeń według kryterium wiekowego konieczne było zwrócenie uwagi na zróżnicowanie dzieci i młodzieży pod względem kompetencji medialnych, zwłaszcza wykraczających poza umiejętności grupy rówieśniczej. Warto też pamiętać, że różnice w aktywnościach komputerowo-internetowych związane są z płcią i miejscem zamieszkania. Potrzebne jest więc kompleksowe spojrzenie na zagrożenia internetowe i zadbanie o bezpieczeństwo użytkowników w szerokim spektrum wskazanych w raporcie uwarunkowań.

*Warszawa, wrzesień 2013* *Marcin Sołodki*



Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

# Rozdział I

## Zakres tematyczny raportu

W raporcie zaprezentowane zostały kwestie pedagogiczno-dydaktyczne oraz aktualne trendy w użytkowaniu przez dzieci i młodzież nowych technologii informacyjno-komunikacyjnych. Autorom e-podręczników oraz twórcom platformy do ich upowszechniania rekomenduje się następujące zagadnienia:

1) Bezpieczeństwo pracy z e-podręcznikiem oraz treściami dydaktycznymi online – analizę opartą na dostępnych danych ilościowych i jakościowych z badań przeprowadzonych w Polsce i za granicą, dotyczących grup wiekowych objętych projektem w klasach 1–3, 4–6 szkoły podstawowej, gimnazjum i liceum.
2) Cechy bezpiecznego e-podręcznika.
3) Stosowanie przez autorów treści do e-podręcznika konstrukcyjnych i użytkowych zasad bezpieczeństwa.
4) Bezpieczna praca ucznia korzystającego z e-podręcznika według analizy rekomendowanej w pkt 1., ze szczególnym uwzględnieniem:
   - kontekstu grup wiekowych;
   - kontekstu różnic między pracą ucznia z e-podręcznikiem w klasie a pracą samodzielną w domu;
   - kontekstu rodzica.
5) Bezpieczna praca nauczyciela korzystającego z e-podręcznika, ze szczególnym uwzględnieniem:
   - kontekstu grup wiekowych;
   - kontekstu różnic między pracą z e-podręcznikiem w klasie a samodzielną pracą w domu;
   - kontekstu tworzenia własnych komponentów treści przez nauczycieli i łączenia ich z gotowymi zasobami udostępnionymi w e-podręczniku.
6) Ewaluacja bezpiecznego korzystania z e-podręcznika prowadzona na poziomie szkoły.
7) Rekomendacje dla autorów e-podręczników oraz przykłady najlepszej praktyki.


Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

# Rozdział II

# Aktywności internetowe dzieci i młodzieży

Dzięki szerokiemu dostępowi polskich gospodarstw do internetu znacząco zwiększa się liczba młodych internautów. Z internetu korzystają już nie tylko dzieci ze szkół podstawowych, ale także często w wieku przedszkolnym. Pierwsze kontakty z internetem polegają najczęściej na wykorzystywaniu 1–3 stron www, gdzie zgromadzone są głównie proste gry online, w których dzieci mają za zadanie:

- znaleźć kolory, kształty, liczby;
- trafić do celu;
- przejść przez przeszkody;
- wcielić się w postać i wykonywać zlecone proste zadania;
- ubrać postać.

Kategorie gier popularnych wśród dzieci w wieku przedszkolnym i uczniów szkoły podstawowej mających 6–12 lat to:

- zręcznościówki;
- ubieranki;
- kolorowanki;
- memo;
- wyścigi.

Dzieci w wieku przedszkolnym i szkoły podstawowej wykorzystują internet przede wszystkim do zabawy. Według badań „Dzieci aktywne online", przeprowadzonych przez firmę Gemi-nius, główne kategorie tematyczne, które interesują dzieci w wieku 7–14 lat, dotyczą kultury i rozrywki, nowych technologii, społeczności, informacji, stylu życia, edukacji. Należy jednak wziąć pod uwagę, że badania zostały wykonane kilka lat temu, co w przypadku internetu i nowych technologii ma ogromne znaczenie – oznacza dezaktualizację wyników.

W konsekwencji postępu technologicznego nastąpiła zmiana zainteresowań użytkowników internetu, mających 9–18 lat, w kierunku serwisów społecznościowych**,** które obecnie są bardzo popularne i znajdują się na pierwszym miejscu wśród rodzajów aktywności dzieci i młodzieży.



Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Według statystyk z 2013 roku, sporządzonych na podstawie badań globalnych przeprowadzonych przez firmę Kaspersky (producent oprogramowania zabezpieczającego), strony pornograficzne i erotyczne (16,8%) zostały zdystansowane przez portale społecznościowe (31,3%), którym młodzież poświęca większość czasu. Do pierwszej trójki zakwalifikowały się niespodziewanie sklepy internetowe (16,7%), znacznie wyprzedzając popularne – jak mogłoby się wydawać – kategorie takie jak czaty i fora czy poczta internetowa.

Z danych wynika, że w maju 2013 roku dzieci, których aktywność komputerowa jest regulowana przez moduł kontroli rodzicielskiej oprogramowania firmy Kaspersky, próbowały uzyskać dostęp do różnych portali społecznościowych ponad 52 miliony razy, podczas gdy liczba prób odwiedzenia stron przeznaczonych dla dorosłych przekroczyła 25 milionów.

Zdecydowana większość (90%), według innego projektu badawczego – „EU NET ADB”[1], przeprowadzonego na przełomie 2011 i 2012 roku, deklaruje, że jest użytkownikiem przynajmniej jednego portalu społecznościowego. Swoje profile na tego typu stronach posiada 94% dziewcząt i 85% chłopców. Do najbardziej popularnych serwisów społecznościowych w Polsce należą www.facebook.com i nk.pl (dawniej Nasza Klasa). Należałoby przy tym zaznaczyć, że serwis społecznościowy Facebook zezwala na rejestrację dzieci w wieku powyżej lat 13, jednak z doświadczeń wynika, że korzystają z niego dzieci poniżej tej granicy, i w związku z tym aktywnymi użytkownikami Facebooka są również 9–12-latki i młodsi.

Nowe i szersze funkcje internetu, w tym szczególnie serwisów społecznościowych, dają większe możliwości internautom. Stwarzają jednak niebezpieczeństwo nadużyć i niosą inne zagrożenia. Tematyka zagrożeń zostanie omówiona w dalszej części raportu, jednak nie sposób nie zaakcentować jej już teraz.

Aktywności dzieci i młodzieży w internecie zmieniają się wraz z wiekiem internautów. O ile dzieci ze szkoły podstawowej eksplorują internet głównie w poszukiwaniu gier, ciekawych

[1] Celem projektu badawczego „EU NET ADB” było określenie skali problemu nadużywania internetu wśród młodzieży w Europie oraz wskazanie czynników powodujących takie zachowania. Badanie było prowadzone od października 2011 r. do maja 2012 r. wśród młodzieży w wieku 14–17 lat w siedmiu krajach europejskich: Grecji, Hiszpanii, Islandii, Holandii, Niemczech, Polsce i Rumunii (www.programbadawczy.fdn.pl/eu-net-adb). Badanie składało się z części ilościowej i jakościowej. W części ilościowej przeprowadzono badania ankietowe na reprezentatywnej próbie 13 284 respondentów w siedmiu krajach europejskich, zaś w części jakościowej – 124 wywiady pogłębione z nastolatkami wykazującymi przynajmniej niektóre symptomy nadużywania internetu.



Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

filmów, obrazów, animacji, w późniejszym etapie szkoły podstawowej (klasy IV–VI) – również ciekawych osób, o tyle młodzież gimnazjalna i ponadgimnazjalna angażuje się także w tworzenie zasobów internetowych.

Technologia Web 2.0, która rozwinęła się około 2001 roku, polega na zmianie paradygmatu interakcji między właścicielami serwisów a jego użytkownikami. Oznacza to większą aktywność użytkowników w tworzeniu treści w danym serwisie. Popularne w latach 2001–2010 blogi dały wyraz zainteresowania młodych ludzi współtworzeniem przestrzeni wirtualnej, w której funkcjonują. Od 2010 roku ustąpiły miejsca serwisom społecznościowym.

Jedną z ważniejszych cech technologii Web 2.0 była i jest możliwość nawiązywania kontaktów. Według przywoływanych już wyników badania „EU NET ADB" w grupie wiekowej 14–15 lat liczba znajomych na FB wynosi 204 osoby (mediana), natomiast w grupie 16–17 lat są to już 224 osoby (mediana). Istotne dla autorów treści e-podręczników jest, że więcej znajomych deklarują dziewczęta, wśród których liczba znajomych na FB sięga 240 osób, niż chłopcy deklarujący 200 osób. Przy opracowaniu treści do e-podręczników należałoby więc kierować się oczekiwaniami odbiorcy, biorąc pod uwagę nie tylko jego wiek, ale również płeć.

Możliwość gromadzenia dużej liczby znajomych, zwłaszcza przez dziewczęta, bez wiedzy o zabezpieczeniach prywatności, niesie zagrożenie w postaci niebezpiecznych konsekwencji nawiązywania tych znajomości. Doświadczenia wskazują, że w grupie znajomych mogą znaleźć się osoby o złych zamiarach. Specjaliści ds. bezpieczeństwa zdecydowanie odradzają dzieciom spotykanie się z osobami poznanymi w internecie.

Na pytanie: „Do czego wykorzystujesz internet?", stawiane dzieciom w wieku szkoły podstawowej, najczęściej padają odpowiedzi:

- do zabawy, głównie korzystania z gier;
- do rozmowy z innymi internautami;
- do wyszukiwania informacji potrzebnych w szkole;
- do słuchania muzyki, oglądania filmów i animacji;
- do korzystania z Facebooka, NK i Youtuba.



Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Z raportu sporządzonego na podstawie badania „EU Kids Online”[2], przeprowadzonego w październiku 2010 roku, wynika, że dzieci podejmują w sieci wiele różnorodnych, potencjalnie korzystnych aktywności: 9–16-latki wykorzystują internet do nauki szkolnej (81%), grania w gry komputerowe (74%), oglądania filmów i klipów wideo (83%) oraz kontaktowania się za pomocą komunikatorów (61%). Nieco mniej dzieci publikuje i dzieli się zdjęciami (38%), wiadomościami (31%), używa kamer internetowych (29%), korzysta z serwisów umożliwiających dzielenie się plikami (17%) oraz prowadzi blogi (10%).

Z kolei badanie „EU NET ADB”, przeprowadzone w 2012 roku wśród dzieci w wieku 14–17 lat, ujmuje temat aktywności w internecie poprzez wskazanie ich form i biorąc za podstawę płeć, wiek oraz wykształcenie rodziców.

[2] Badanie „EU Kids Online”, (10.2010) dotyczyło zagrożenia i bezpieczeństwa w internecie z perspektywy dzieci w Europie (wstępne wyniki badań). Badanie „EU Kids Online II” – nadużywania internetu przez dzieci w wieku 9–16 lat.



Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Tabela 1. Formy aktywności podejmowane w internecie (wg płci, wieku oraz wykształcenia rodziców)

| Odsetek młodzieży podejmującej daną aktywność przynajmniej raz w tygodniu | Ogółem | Płeć | | Wiek | | Wykształcenie rodziców | |
|---|---|---|---|---|---|---|---|
| | | Dz. | Ch. | 14-15 | 16-17 | Podst./ Średnie | Wyższe |
| Oglądanie klipów/filmów | 84 | 80 | 88 | 84 | 84 | 81 | 87 |
| Komunikatory | 80 | 81 | 79 | 79 | 84 | 79 | 82 |
| Portale społecznościowe | 79 | 87 | 71 | 78 | 82 | 79 | 79 |
| Odrabianie pracy domowej/ poszukiwanie informacji | 76 | 79 | 74 | 77 | 74 | 77 | 76 |
| Ściąganie muzyki | 66 | 63 | 68 | 66 | 65 | 68 | 63 |
| Cele hobbystyczne | 63 | 58 | 69 | 64 | 62 | 56 | 70 |
| Poczta elektroniczna | 52 | 52 | 53 | 51 | 54 | 48 | 56 |
| Fora internetowe | 34 | 28 | 40 | 33 | 36 | 31 | 38 |
| Ściąganie filmów | 31 | 23 | 39 | 31 | 32 | 32 | 31 |
| Wieloosobowe gry typu FPS – „strzelanki” | 30 | 6 | 54 | 29 | 31 | 28 | 30 |
| Wieloosobowe gry typu MMO RPG | 28 | 8 | 48 | 26 | 30 | 25 | 30 |
| Czaty | 27 | 21 | 34 | 28 | 24 | 23 | 31 |
| Gry dla jednego gracza | 23 | 18 | 28 | 22 | 24 | 23 | 21 |
| Ściąganie gier | 20 | 6 | 34 | 19 | 22 | 20 | 18 |
| Serwisy informacyjne | 17 | 4 | 31 | 16 | 20 | 14 | 20 |
| Serwisy z informacjami o seksie | 17 | 4 | 31 | 16 | 20 | 14 | 20 |
| Prowadzenie własnej strony lub bloga | 16 | 21 | 12 | 17 | 16 | 15 | 17 |
| Ściąganie oprogramowania | 16 | 5 | 26 | 15 | 16 | 16 | 15 |
| Sieciowe gry strategiczne | 15 | 5 | 26 | 14 | 16 | 16 | 14 |
| Zakupy i aukcje internetowe | 11 | 7 | 15 | 11 | 11 | 10 | 14 |
| Poszukiwanie informacji medycznej | 8 | 8 | 9 | 9 | 7 | 7 | 9 |
| Gry online z nagrodami pieniężnymi | 7 | 3 | 11 | 7 | 7 | 7 | 7 |
| Hazard | 2 | 1 | 5 | 3 | 3 | 2 | 3 |

Źródło: Badanie „EU NET ADB”, 2012



Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Ze względu na potrzeby dokumentacji istotne jest rozpoznanie sprzętu, z którego korzystają dzieci, aby łączyć się i surfować w internecie. Z badania „EU Kids Online", przeprowadzonego w październiku 2010 roku wśród dzieci w wieku 9–16 lat i ich rodziców, wynika, że dzieci w Polsce, podobnie jak w Europie, łączą się z internetem przeważnie przez komputer osobisty, posiadany tylko do własnej dyspozycji lub używany wspólnie z innymi domownikami, oraz za pomocą laptopa. Tabela 2., z wynikami badania „EU Kids Online", zawiera porównanie i ukazuje pełny zakres urządzeń, z których dzieci w Polsce i Europie łączą się z internetem. Próba dzieci korzystających w Polsce z internetu liczyła 960 osób w wieku 9–11 lat, wyniki obliczono dla kompletnych danych – 960 dzieci. Cała próba badanych w Europie liczyła 23 420 dzieci w wieku 9–11 lat.

Tabela 2. Jak dzieci w Polsce i Europie łączą się z internetem

| **Urządzenie, za pomocą którego dzieci łączą się z internetem** | **% dzieci w Polsce** | **% dzieci w Europie (średnio)** |
|---|---|---|
| Komputer używany wspólnie z innymi | 57 | 55 |
| Własny komputer osobisty | 52 | 34 |
| Telefon komórkowy | 37 | 28 |
| Zestaw telewizyjny | 35 | 31 |
| Własny laptop | 13 | 23 |
| Laptop używany wspólnie z innymi | 13 | 23 |
| Konsola do gier | 11 | 24 |
| Inne przenośne urządzenie | 5 | 10 |

Źródło: Badanie „EU Kids Online", 2010

Dodatkowo należałoby zwrócić uwagę, iż badanie zostało przeprowadzone ponad 2 lata temu, w następstwie czego w grupie urządzeń nie znalazły się popularne obecnie tablety i smartfony**.** Z globalnych badań przeprowadzonych przez aQooQoo (m.in. dzięki użytkowaniu telefonu aQooQoo LOCO), markę stworzoną dla potrzeb urządzeń i oprogramowania dla dzieci, wynika, że w Polsce 83% dzieci w wieku 10 lat ma własny telefon komórkowy, część – smartfony. Wynik ten umieszcza nasz kraj na 1. miejscu w świecie. Tuż za Polską plasują się dzieci z Wielkiej Brytanii, gdzie 73% spośród nich posiada swój własny telefon. Wyprzedzamy w tej statystyce nie tylko Anglików, ale również Amerykanów, kraje takie jak:


Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Brazylia (73%), Niemcy (69%), Meksyk (68%), Chiny (49%), Hiszpania (37%), a nawet Japonia (20%).

Z kolei wyniki badań MRI, przedstawione w raporcie „American Kids Study", informują o ogromnym wzroście liczby telefonów komórkowych wśród dzieci. Porównując wyniki badań z 5 lat, okazało się, że w grupie wiekowej 10–11 lat liczba ta zwiększyła się o ponad 80%. Co ciekawe, z badań wynika, że częściej posiadaczami własnych telefonów komórkowych są dziewczynki niż chłopcy.

Biorąc pod uwagę wyniki powyższych badań, można zdefiniować kolejne zagrożenia. Po pierwsze programy zabezpieczające przed złośliwym oprogramowaniem, o ile są dobrze opracowane na komputery stacjonarne i laptopy, o tyle na smartfony i tablety wciąż trwa przygotowywanie prawidłowo działających zabezpieczeń. Owszem, na rynku są już dostępne programy napisane z myślą o zabezpieczaniu urządzeń mobilnych, jednak jest ich jeszcze stosunkowo mało i nie są stuprocentowo skuteczne.

Funkcje urządzeń mobilnych, jak również opcje w aplikacjach mobilnych, wymagają od użytkownika m.in. zaakceptowania lokalizacji urządzenia, a tym samym użytkownika. Geolokalizacja określa, w jakim miejscu w danej chwili znajduje się użytkownik mobilnego urządzenia. Opcja ta może powodować zagrożenie szybkiego ustalenia miejsca pobytu dziecka i doprowadzenie do spotkania z nieodpowiednią osobą.

W grupie zagrożeń wynikających z korzystania z urządzeń mobilnych znajdują się też mikropłatności**,** do których użytkownik nakłaniany jest w drodze manipulacji. Dziecko może np. być namawiane do wykupienia kolejnego poziomu w grze, odkrycia za pieniądze kolejnych elementów czy pozyskania dodatkowych artefaktów lub części ubioru postaci z gry, a dzieci nie mają świadomości, że płatne części programu czy gry wymagają od nich pobrania mikropłatności z konta.

Innym rodzajem zagrożenia związanym z korzystaniem urządzeń mobilnych są częste kradzieże cennego sprzętu.

Z przywoływanych już badań, przeprowadzonych przez firmę Kaspersky w maju 2013 roku, wynika, że stałą pozycją w pierwszej piątce najczęściej podejmowanych aktywności są zakupy robione przez dzieci w sklepach internetowych, które mogą stwarzać zagrożenie


Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

utraty finansów w przypadku nienależytego zabezpieczenia kart kredytowych przez rodziców lub kiedy nie wylogują się oni np. z portalu aukcyjnego.

Dorośli użytkownicy internetu rozgraniczają świat wirtualny i realny, w przeciwieństwie do dzieci, które żyją w obydwu światach, łącząc je i korzystając z nich równolegle.

W *Manifeście dzieci sieci* wydanym w 2012 roku czytamy:
*Sieć nie jest dla nas technologią, której musieliśmy się nauczyć i w której udało nam się odnaleźć. Sieć jest procesem, który dzieje się i nieustannie przekształca na naszych oczach; z nami i przez nas*.
*Sieć nie jest dla nas czymś zewnętrznym wobec rzeczywistości, ale jej elementem. My nie korzystamy z sieci, my w niej i z nią żyjemy.*

Ten ciągły proces wprowadza nas w kolejne zagrożenie, jakim jest nadmierne korzystanie z nowych technologii. Z badania „EU NET ADB", przeprowadzonego na przełomie 2011 i 2012 roku wśród 14–17-latków, wynika, że 66% dzieci korzysta z internetu codziennie, najczęściej 1–2 godziny. Częściej korzystają z niego chłopcy i starsze nastolatki, w wieku 16–17 lat.

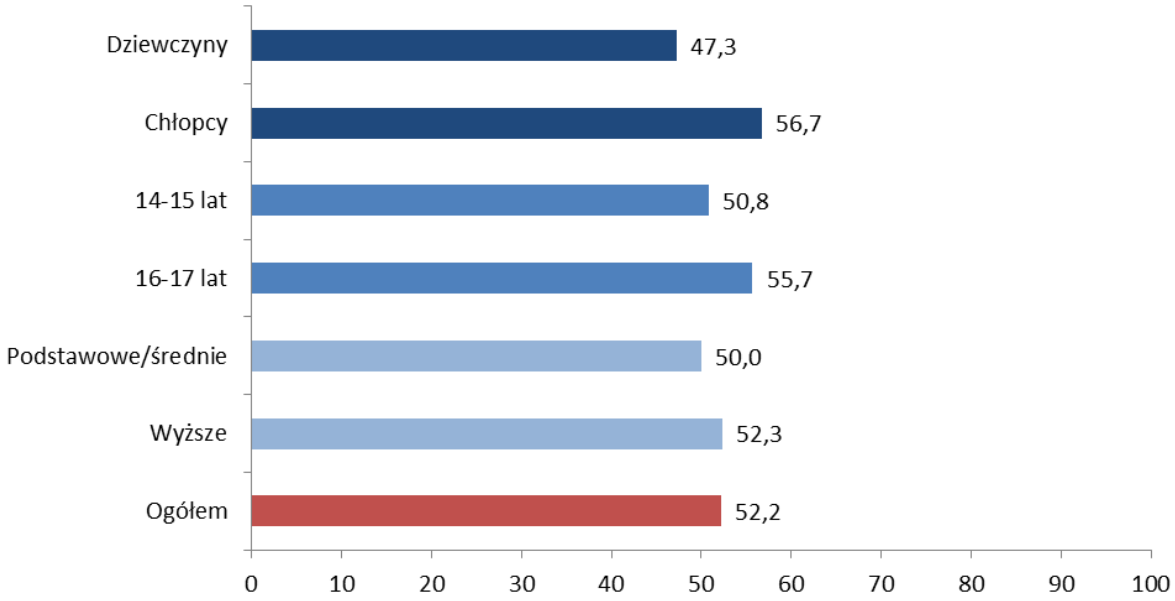
Tabela 3. Średni czas spędzany w internecie

| Średnia (w godzinach) | Dzień, kiedy są lekcje | Dzień, kiedy nie ma lekcji |
|---|---|---|
| Wcale | 3,13 | 1,21 |
| Tylko kilka minut | 6,16 | 2,21 |
| Około pół godziny | 9,34 | 3,69 |
| Około godziny | 16,02 | 6,9 |
| Około 1,5 godziny | 13,19 | 7,79 |
| Około 2 godzin | 14,94 | 14,59 |
| Około 2,5 godziny | 7,7 | 8,16 |
| Około 3 godzin | 10,16 | 11,85 |
| Około 3,5 godziny | 3,8 | 6,48 |
| Około 4 godzin | 7,03 | 13,64 |
| Ponad 4 godziny | 8,52 | 23,49 |

Źródło: Badanie „EU NET ADB", 2012


Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Wykres 1. Osoby korzystające z internetu co najmniej 2 godziny dziennie, w czasie lekcji (według płci, wieku oraz wykształcenia rodziców – procentowo)




Źródło: „EU NET ADB", 2012

Istotnym aspektem e-podręcznika jest takie skonstruowanie jego treści, aby młodzi ludzie korzystający z zawartych w nim materiałów edukacyjnych mieli możliwość mimowolnego oderwania się od treści. Równie ważne jest, aby treści charakteryzowały się sinusoidalnym przekazem emocjonalnym, powodując w danej chwili osłabienie przekazu i dając tym samym czas na obniżenie napięcia u osoby uczącej się. Dzieci w wieku 6–9 lat są w stanie skupić się na jednym zadaniu ok. 30 minut. Ta umiejętność ćwiczona jest w dalszych klasach szkoły podstawowej, co powoduje, że uczniowie z klas IV–VI, tj. dzieci w wieku 10–12 lat, potrafią poświęcić na zadanie ok. 50 minut i wielokrotnie wracać do niego po przerwach. Młodzież gimnazjalna umie skupić uwagę na zadaniu/problemie ponad 50 minut, natomiast 16-latki i starszą młodzież ocenia się wyżej – są w stanie skoncentrować się na problemie podobnie długo jak dorośli.

Trudno o rzetelne informacje, dotyczące kolejnego zagrożenia, których nie sposób podważyć – czyli czasu, jaki dzieci i młodzież mogą spędzać w internecie, aby nie doszło do objawów przedawkowania, tj. bólu i zawrotów głowy, bólu i pieczenia oczu, bólu kręgosłupa, trudności w skupieniu uwagi na innych pozakomputerowych aktywnościach, rezygnacji z życia codziennego w świecie rzeczywistym, zmniejszającej się liczby realnych znajomych.


Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Najczęściej spotykane zalecenia dotyczące czasu przeznaczanego na korzystanie z komputera, w tym internetu, przez dzieci i młodzież mówią, że powinien on wynosić, w zależności od wieku:

- 3–5 lat: 15 minut;
- 6–10 lat: 30 minut;
- 11–13 lat: 60 minut;
- 14–18 lat: 90 minut.

Lekcje prowadzone z wykorzystaniem e-podręcznika powinny mieć wyodrębniony początek i zakończenie, po to by użytkownik wiedział, kiedy kończy się lekcja i kiedy sam może ją zakończyć.



Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

# Rozdział III

# Bezpieczne dzieci w sieci – kontekst rodzica

*Sieć nie jest dla nas czymś zewnętrznym wobec rzeczywistości, ale jej elementem. My nie korzystamy z sieci, my w niej i z nią żyjemy.*

*Manifest dzieci sieci, 2012*

Nie bez powodu przywoływany jest raz jeszcze powyższy istotny cytat. Tym razem w kontekście rodzic – dziecko – internet, w celu ukazania różnic pokoleniowych w odbiorze i korzystaniu z nowych technologii.

Pierwsze w Polsce internetowe łącze analogowe zostało uruchomione 26 września 1990 roku. Prawdziwy rozkwit sieci nastąpił pod koniec lat 90., a współczesny uczeń, obecnie w wieku 6–18 lat, urodził się już w czasie, kiedy internet w Polsce istniał. Jest to więc tylko jeden z powodów, dla których dzieciom łatwiej jest wypowiadać w *Manifeście* słowa: *My nie korzystamy z sieci, my w niej i z nią żyjemy* – łatwiej niż rodzicom, czyli osobom w wieku około 30–42 lat. Kiedy oni uczęszczali do szkoły podstawowej czy średniej, w latach 70., 80., 90., elementy nauczania z wykorzystaniem komputera pojawiały się na lekcjach przedmiotu praca technika i było to raczej rozpoznawanie *zx spectrum*, później *atari* czy *commodore 65* w zakresie prostych gier wgrywanych z kasety.

Z tego powodu warto przytoczyć inne znaczące daty, dotyczące historii internetu w Polsce:

- 1995 – uruchomiono największy polski portal internetowy www.wp.pl;
- 1999 – powstał największy polski portal aukcyjny www.allegro.pl;
- 2005 – w sieci pojawił się serwis www.youtube.com, który umożliwił bezpłatne umieszczanie, oglądanie filmów oraz *live streaming*;
- 11 listopada 2006 – powstał największy polski serwis społecznościowy www.Nasza-Klasa.pl, obecnie www.nk.pl, którego pierwotnym celem było umożliwienie użytkownikom odnalezienia osób ze swoich szkolnych lat i odnowienie z nimi kontaktu;
- Maj 2008 – rozpoczęła działanie polska wersja językowa serwisu www.facebook.com, istniejącego na świecie od 4 lutego 2004.

Jak łatwo zauważyć, większość z tych istotnych dat przypada na ostatnie dziesięciolecie. Obecnie dzieci znają internet znacznie lepiej niż ich rodzice, wiedzą, jak poruszać się w nim,


Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

aby znaleźć to, czego szukają, i wykorzystać w życiu wirtualną przestrzeń. To dorośli oddzielają wirtualny świat od realnego, dzieci łączą je i sprawnie wykorzystują, miksując obie płaszczyzny.

Niezaprzeczalnie kompetencje komputerowo-internetowe dzieci są znacznie większe niż rodziców, jednak mimo to obowiązkiem rodziców jest dostarczenie dzieciom wiedzy dotyczącej zasad bezpiecznego poruszania się po internecie. Bezpieczeństwo w cyber-przestrzeni niewiele różni się od bezpieczeństwa w rzeczywistości. Jedyne różnice powiązane są z funkcjonalnościami sieci, i dlatego warto, aby rodzice zapoznali się z nimi, najlepiej z pomocą dzieci. Rozmowa o internecie między rodzicami a dziećmi stworzy temat do rozmów o zagrożeniach internetowych, które naturalnie łatwiej dostrzeże dorosły, np.: niebezpieczne treści, niebezpieczne kontakty online, ryzykowne transakcje online, uzależnienie od internetu itd.

Warto, aby dzieci i rodzice wspólnie nauczyli się korzystać z e-podręczników i aby to dzieci pokazały rodzicom edukacyjną wirtualną przestrzeń nowego podręcznika. Obawa rodziców o utratę autorytetu w oczach dzieci jest nieuzasadniona. Dzieci chętnie pokażą, jak korzystają z e-podręczników, ułatwiając komunikację rodzic – dziecko (uczeń), również w obszarze zagrożeń online, które mogą zaistnieć podczas korzystania z e-podręczników przy odrabianiu pracy domowej.

Czy rodzice są świadomi zagrożeń, jakie niesie nieprzemyślane korzystanie przez dzieci z internetu? To jedno z pytań postawionych w trakcie badania „Dzieci online w oczach rodziców”[3]. Wyniki badania pokazują, że zdecydowana większość rodziców za niebezpieczne uważa przede wszystkim te formy aktywności online, które wiążą się z przekazywaniem przez najmłodszych internautów danych osobistych – adresu zamieszkania (85%) i numeru telefonu (79%). Nieco mniej rodziców (75%) jako niebezpieczne ocenia spotkanie się dziecka z osobą poznaną przez internet. Udostępnianie adresu e-mail osobie poznanej w internecie oraz umieszczanie tam swoich zdjęć jest traktowane jako niebezpieczne przez odpowiednio 55% i 48% respondentów. Jednocześnie duża grupa rodziców nie jest w stanie ocenić, jakie formy internetowej aktywności najmłodszych internautów mogą stanowić zagrożenie.

[3] Wyniki badań nad przekonaniami rodziców o korzystaniu przez ich dzieci z internetu oraz świadomością zagrożeń płynących z sieci. Badanie przeprowadzone zostało w marcu 2008 r. przez firmę badawczą Geminius we współpracy z Fundacją Dzieci Niczyje.



Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

# Rozdział IV

# Pomoc dzieciom i młodzieży w sytuacjach zagrożenia bezpieczeństwa podczas korzystania z nowych technologii

Rodzice i pedagodzy szkolni powinni interweniować w razie zaistnienia sytuacji zagrażającej dzieciom podczas korzystania z internetu. Jeżeli dzieci nie mogą takiej pomocy otrzymać, ponieważ dorosłe osoby nie są w stanie im pomóc albo dzieci nie chcą zwracać się z tego typu problemami do dorosłych, należałoby poinformować je o innym rozwiązaniu.

Między innymi z tego powodu powołano zespół specjalistów Helpline.org.pl, działający w Fundacji Dzieci Niczyje, którego przedstawiciele pomagają w trudnych sytuacjach, jak:

- ośmieszanie, szantażowanie, wysyłanie dzieciom wulgarnych wiadomości;
- zadawanie na czacie czy komunikatorze krępujących pytań, proszenie o zdjęcie, namawianie dzieci na spotkanie;
- włamanie się na konto w grze czy na portalu społecznościowym;
- wysyłanie lub prezentowanie dzieciom treści zawierających pornografię lub przemoc.

Swoją pomoc Helpline.org.pl kieruje nie tylko do dzieci i młodzieży; ze specjalistami mogą się skontaktować również rodzice i profesjonaliści.

Sytuacje, w których rodzice mogą kontaktować się z Helpline.org.pl:

- nieumiejętność przeprowadzenia rozmowy z dzieckiem o bezpieczeństwie w internecie;
- niepokój związany z tematyką, którą dzieci zajmują się w internecie;
- zaistniały już kontakt z niebezpiecznymi treściami – prezentującymi pornografię, przemoc, propagującymi narkotyki, faszyzm, sekty, inne ryzykowne zachowania;
- niepokój dotyczący znajomości zawieranych w internecie przez dzieci;
- dostrzeżone u dzieci objawy uzależnienia od internetu.

Sytuacje, w których profesjonaliści mogą kontaktować się z Helpline.org.pl:

- prośba dzieci lub rodziców o pomoc w sprawach związanych z zagrożeniami w internecie.

Komunikację ze specjalistami z Helpline.org.pl: umożliwiają:

- bezpłatny numer telefonu: 800 100 100, czynny od poniedziałku do piątku, w godzinach od 12.00 do 18.00;



Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

- wiadomości e-mail (helpline@helpline.org.pl );
- czat z poziomu strony (www.helpline.org.pl);
- formularz kontaktowy na stronie „Zadaj nam pytanie” (www.helpline.org.pl).



Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

# Rozdział V

# Zagrożenia dzieci i młodzieży w internecie – typologia

## 1. Szkodliwe treści

Ten rodzaj zagrożenia szczególnie dotyczy dzieci, które dopiero zaczynają korzystać z komputera i internetu, czyli najmłodszych internautów. Dzieci w wieku 6–10 lat narażone są na niebezpieczne treści, często niezgodne z polskim prawem, wśród których znajdują się pornografia dziecięca, twarda pornografia, rasizm i ksenofobia.

**Pornografia dziecięca**

Polskie prawo zabrania sprowadzania, przechowywania lub posiadania treści pornograficznych z udziałem dziecka poniżej lat 15, także rozpowszechniania i publicznego prezentowania pornografii z udziałem osoby małoletniej poniżej lat 18.

**Twarda pornografia**

Polskie prawo zabrania rozpowszechniania i publicznego prezentowania pornografii z aktami przemocy lub posługiwania się zwierzęciem.

Konsekwencje kontaktu dziecka z treściami prezentującymi pornografię:

- dziecko nie rozumie treści, które ogląda;
- nie wie, że treści to czyjś wytwór, a nie realna sytuacja;
- przeżywa emocje tak, jakby było świadkiem realnej sytuacji;
- uczy się, że świat jest zagrażający – dziecko generalizuje;
- czuje się winne, że ogląda trudne i zakazane treści.

**Rasizm i ksenofobia**

W Polsce zabronione jest propagowanie faszystowskiego lub innego totalitarnego ustroju oraz szerzenie nienawiści wobec jednostki czy grupy społecznej ze względu na jej pochodzenie, kulturę, wyznanie lub z powodu jej bezwyznaniowości.

Powyższe treści są nienależycie zabezpieczane przed dziećmi. Polskie prawo wymaga jedynie umieszczenia przed nimi strony zawierającej klauzulę informującą użytkownika, że jeśli nie ma ukończonych lat 18, powinien opuścić tę stronę. Najczęściej klauzuli towarzyszy migający duży napis „Wejdź" oraz ukryty lub mały napis „Wyjdź". Już na tej stronie często znajdują się



Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

treści pornograficzne. Dzieci trafiają na nie przypadkowo, a ponad 60% z nich deklaruje, że strona uruchomiła się w sposób od nich niezależny.

Oprócz stron zawierających treści niezgodne z prawem istnieje wiele skierowanych wyłącznie do osób dorosłych. Są to np. popularne portale informacyjne, na których wydawca zamieszcza treści, również zdecydowanie nie dla dzieci: porady i zdjęcia erotyczne, brutalne sceny przemocy, zdjęcia czy filmy z katastrof i wypadków itp.

## 2. Kontakty online

Zagrożenie to dotyczy osób, które podejmują kontakty za pośrednictwem internetu, szukając nowych znajomych. Wśród nowo poznanych osób mogą znaleźć się ludzie mający złe zamiary, co oznacza zagrożenie w momencie dojścia do spotkania. Dzieci w wieku 6–12 lat nie powinny spotykać się z osobami poznanymi w internecie. Młodzież w wieku 12–15 lat, kiedy decyduje się na spotkanie, powinna powiadomić o tym rodziców lub opiekunów, dodatkowo wybrać się na to spotkanie w towarzystwie rówieśnika lub osoby dorosłej. Kontakty online umożliwiają portale społecznościowe, czaty, fora, e-maile, aplikacje mobilne, gry społecznościowe.

## 3. Cyberprzemoc

Cyberprzemoc jest rodzajem przemocy, która polega na wykorzystywaniu technologii informacyjnych i komunikacyjnych. Narzędziami używanymi w cyberprzemocy są: poczta elektroniczna, komunikatory, czat, strony i blogi, fora dyskusyjne, serwisy społecznościowe, rozmowy GSM, SMS, MMS.

Formy cyberprzemocy:

- nękanie, straszenie, szantażowanie, rejestrowanie i dystrybucja niechcianych zdjęć i filmów;
- dystrybucja ośmieszających, upokarzających informacji;
- podszywanie się pod kogoś.

Rozwój nowych technologii, szczególnie w dziedzinie telefonii komórkowej, powoduje, że sprzęt daje użytkownikom więcej możliwości rejestrowania filmów, zdjęć i ich natychmiastowej publikacji w internecie. Są to z jednej strony pożyteczne funkcje, ale, niestety, bywają wykorzystywane w złym celu. Często dochodzi do sytuacji rejestrowania osób, które


Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

sobie tego nie życzą, i umieszczania materiału w internecie. Raz zamieszczony film, zdjęcie czy inne nagranie zostaje w sieci na zawsze, generując trudności w dorosłym życiu, na przykład przy rekrutacji do szkoły czy pracy.

## 4. Kradzież tożsamości

Do takiej sytuacji dochodzi w prosty sposób – kiedy dzieci zapominają o wylogowaniu się po zakończonej pracy czy zabawie w internecie. Jeśli z komputera, np. w szkole, korzysta następny uczeń, pojawia się niebezpieczeństwo skorzystania z konta poprzedniej osoby na platformie edukacyjnej czy w serwisie społecznościowym lub aukcyjnym. Konstruktorzy platformy udostępniającej e-podręczniki powinni zadbać o funkcje automatycznego wylogowywania się po zakończonej sesji, a także wtedy, kiedy po upływie ok. 5 minut nie zajdzie żadna interakcja, aktywne użycie treści.

## 5. Kradzież danych osobowych

Powszechnym zjawiskiem w sieci jest bezmyślne pozostawianie przez dzieci swoich danych osobowych oraz wszelkiego typu informacji o sobie i bliskich. Dzieci nie zastanawiają się, dlaczego dany serwis pobiera od nich tak wiele danych, nie czytają regulaminów, w których wszystko jest wytłumaczone, ale najczęściej drobnym drukiem. W konsekwencji nierozważnych działań w różnych miejscach w sieci dochodzi do sytuacji, które stwarzają innym internautom okazję do zestawienia tych danych i skrzywdzenia ich właściciela. Przygotowując platformę udostępniającą e-podręczniki, należałoby szczególnie zadbać o obszar rejestracji. Dzieci powinny mieć możliwość udostępniania swoich danych osobowych wyłącznie za zgodą rodziców lub opiekunów, co musi zostać ujęte w klauzuli.

## 6. Nadmierne korzystanie z komputera i internetu

Zjawisko nadużywania komputera i internetu występuje wtedy, kiedy zachodzą równocześnie dwie okoliczności:

- czas i intensywność korzystania z internetu przebiegają w sposób niekontrolowany;
- korzystanie z internetu prowadzi do zaniedbania innych czynności życiowych.



Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

W pierwszej części opracowania zostały przytoczone wyniki badań, które wskazują na coraz dłuższe korzystanie z komputera i internetu przez dzieci. W grupie 14–17-atków 66% deklaruje, że z internetu korzysta codziennie, najczęściej 1–2 godzin.

## 7. Wirusy komputerowe

Ten rodzaj zagrożenia wymieniany jest przez dzieci i rodziców w pierwszej kolejności, najprawdopodobniej w wyniku wieloletniej edukacji w tym zakresie, bowiem do niedawna jedynie ta wąska tematyka zagrożeń dzieci, płynąca z obszaru online, była ujęta w podstawie programowej. Aby uniknąć ataku wirusów, wystarczy dobre oprogramowanie zabezpieczające. Należałoby jednak zwrócić uwagę na najnowsze zagrożenia tego typu, mianowicie przejmowanie przez hakerów kamerek internetowych, coraz częściej na stałe wbudowanych w laptopy. Zaleca się podczas niekorzystania z kamery zasłonić obiektyw, co jest klasyczną i skuteczną metodą zapobiegawczą.

## 8. Utrata dóbr materialnych

Jest rodzajem zagrożenia, które dotyczy osób dorosłych, dokonujących transakcji za pośrednictwem internetu. Dziecko nie ma swobody wykonywania czynności cywilnoprawnych, w tym zawierania umów, lub ma ją w stopniu ograniczonym. Zgodnie z przepisami Kodeksu cywilnego dziecko, które nie ukończyło lat 13, nie ma zdolności do czynności prawnych, zaś małoletni, którzy ukończyli lat 13, ale nie ukończyli lat 18, mają tę zdolność w zakresie ograniczonym. W konsekwencji wszystkie czynności prawne dokonywane przez osoby do tego nieuprawnione są z mocy prawa nieważne. Wyjątek stanowią umowy dotyczące drobnych spraw życia codziennego, które stają się ważne w momencie wykonania umowy.

## 9. Nowe zjawiska: *fomo, hitting, grooming*

***Fomo*** *(fear of missing out)*, czyli lęk przed ominięciem nas przez coś, określany przez psychologów jako lęk przed przeoczeniem wydarzenia towarzyskiego czy ważnej informacji, które mogą mieć wpływ na nasze plany. Jest to zachowanie polegające na ciągłej chęci bycia podłączonym do internetu, bycia online. Nie dopracowano się jeszcze profesjonalnej metody testowania osób pod kątem tego zjawiska, ale w sieci można znaleźć różne testy zawierające pytania na ten temat, np:


Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

- Kiedy przygotowujesz np. pracę domową, to pierwszą myślą, która przychodzi ci do głowy, jest chęć umieszczenia pracy na Facebooku i oczekiwanie na komentarze?
- Kiedy wybierasz się na wakacje, to pierwszą czynnością, którą wykonujesz, jest sprawdzenie, czy ośrodek ma nieograniczony dostęp do internetu?

Udzielenie odpowiedzi „Tak" na większość pytań wskazuje na występowanie objawów zjawiska *fomo*.

Zjawisko *fomo,* jako jeszcze nie w pełni zbadane, trudne jest do zaprezentowania i co więcej, niełatwo dawać wskazówki, jak mu zaradzić, chociaż mówi się, że ma bardzo długą historię. Można je odnieść do potrzeby porównywania się z innymi i bycia najlepszym – tym, który pierwszy dopisze komentarz pod zdjęciem, filmem, tekstem – czyli obrazami lub informacjami tekstowymi, które zamieszczone zostały na Facebooku czy w innym serwisie społecznościowym, jak Twitter, My Space, Google+, Pinterest. Nie bez powodu zjawisko to kojarzone jest z serwisami społecznościowymi, ponieważ w tych miejscach w internecie trwa bezustanna aktualizacja – znajomi dodają komentarze, filmy, linki, oceniają, „lajkują". Dlatego tzw. społecznościówki mają potencjał uzależniający i są ściśle związane z *fomo*. Konstruktorzy e-podręczników oraz platform, które będą je udostępniać, powinni więc zadbać, aby cały system nie wymuszał na uczniach ciągłego bycia online – nieustannej aktualizacji i śledzenia zmian, sprawdzania nowinek itd., aby nie dochodziło do sytuacji, w których uczeń odczuwa lęk przed przeoczeniem czegoś istotnego.

***Hitting*** to wyśmiewanie, atak na użytkowników sieci, notoryczne zamieszczanie negatywnych komentarzy przy twórczości innych internautów.

Zakładając istnienie w systemie e-podręczników funkcji publikowania twórczości uczniów oraz jej oceniania w grupie przez innych, osobą kontrolującą ten proces będzie nauczyciel lub w domu – rodzic. Jeśli zajdzie potrzeba interwencji, powinna istnieć możliwość zgłoszenia incydentu administratorom platformy w celu zabezpieczenia dowodów, a następnie usunięcia incydentu z publicznej przestrzeni.

***Grooming*** oznacza działania podejmowane w celu zaprzyjaźnienia się i nawiązania więzi emocjonalnej z dzieckiem, aby zmniejszyć jego opory i później doprowadzić do seksualnego wykorzystania, nakłonienia do prostytucji czy udziału w pornografii dziecięcej. Potocznie przez *child grooming* rozumie się uwodzenie dzieci przez internet, co jest procesem


Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

polegającym najczęściej na stopniowym przywiązywaniu dziecka do pedofila. Następstwem tego procesu jest pojawianie się trudności emocjonalnych u dziecka, a jeśli dojdzie do wykorzystania seksualnego – także poczucie winy za to, co się stało.

## 10. Plagiat

Zjawisko potocznie określone zwrotem „kopiuj – wklej" (nazwa pochodzi od funkcji m.in. edytorów tekstu). Jest często spotykane, szczególnie wśród uczniów, którzy przeszukują sieć w celu zminimalizowania czasu i ograniczenia wysiłku, z założenia przeznaczonego na wykonanie np. pracy domowej. W sieci istnieją programy umożliwiające analizę dokumentu tekstowego czy obrazu o cechach plagiatu. Służą one zapobieganiu plagiatowi również wtedy, kiedy praca autorstwa jednego ucznia kopiowana jest przez innego.



Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

# Rozdział VI

# Rola nauczyciela w bezpiecznej edukacji dzieci, wykorzystującej e-podręczniki

Nauczyciel stanowi bardzo istotne ogniwo w edukacji dzieci i młodzieży, wykorzystującej e-podręcznik. Dlatego niezbędne jest, aby szczegółowo poznał to narzędzie – jego pełne możliwości oraz obszary, w których można się nim posłużyć do realizacji celów innych niż przyjęte.

Obszarem, w którym cele te mogą się ujawnić, jest udostępniona uczniom komunikacja tekstowa w grupie (jeśli istnieje na platformie upowszechniającej e-podręczniki). Funkcja komunikacji tekstowej, która np. została udostępniona uczniom na platformie e-learningowej Fundacji Dzieci Niczyje (www.fdn.pl/kursy), w 90% – jak wskazują doświadczenia i monitoring – wykorzystywana jest do pogawędek, nawet szykanowania rówieśników z grupy lub nauczyciela.

Nauczyciel w procesie edukacji wykorzystującej e-podręcznik będzie więc pełnił role:

- koordynatora procesu;
- twórcy dodatkowego kontentu;
- kontrolera wykorzystania narzędzia;
- administratora i opiekuna.

Konieczne jest, aby edukacja z wykorzystaniem e-podręczników została poprzedzona edukacją w zakresie zagrożeń dzieci i młodzieży w internecie, na którą składają się: zapoznanie uczniów z możliwościami rozpoznawania i weryfikacji niebezpiecznych treści podawanych online; identyfikowanie cyberprzemocy, uzależnienia od komputera, groźnych kontaktów online oraz przestrzeganie obowiązku poszanowania własności.

Przydatne jest skorzystanie przez nauczyciela z bezpłatnych materiałów edukacyjnych, opracowanych przez specjalistów ds. edukacji, pracujących w programie „Dziecko w sieci" Fundacji Dzieci Niczyje.



Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

W poniższej tabeli podane zostały pozycje e-learningowe, które w prosty sposób można wykorzystać w szkole.

Tabela 4. Pozycje e-learningowe do wykorzystania w szkole

| Lp. | Nazwa | Adresat | Opis | Czas trwania |
|---|---|---|---|---|
| 1. | **Sieciaki – poznaj bezpieczny internet** | Uczniowie klas I–III szkoły podstawowej | Kurs składa się z 8 modułów, w których dzieci poznają podstawowe zasady bezpieczeństwa. Zadaniem użytkownika kursu jest zdobycie 7 stopni wtajemniczenia i dołączenie do drużyny Sieciaków. | 3 x 45 min |
| 2. | **321 internet** | Uczniowie klas IV–VI szkoły podstawowej | Tematem kursu są przygody piątki uczniów szkoły podstawowej – Kuby, Ani, Sandry, Szymona i Piotrka. Na przykładzie ich losów użytkownik poznaje różne formy zagrożeń związanych z internetem: cyberprzemoc, kontakty online, plagiat, uzależnienie od internetu.<br>Kurs składa się z siedmiu modułów, w których zaprezentowana jest pięcioczęściowa kreskówka. Każda część przedstawia jedno z zagrożeń, na jakie mogą natknąć się najmłodsi użytkownicy sieci. Zadaniem ucznia jest wybór odpowiedniego zakończenia kreskówki. | 2 x 45 min |
| 3. | **Lekcja bezpieczeństwa** | Uczniowie klas IV–VI szkoły podstawowej; klas I–III gimnazjum | Podczas tej lekcji uczniowie jednego z gimnazjów przytaczają krótkie historie na temat prywatności w sieci, które ich dotyczyły albo o których słyszeli. Każde zagadnienie podsumowywane jest przez konsultantkę Helpline.org.pl. | 45 min |
| 4. | **Gdzie jest Mimi?** | Uczniowie klas IV–VI szkoły podstawowej; klas I–III gimnazjum | Podejrzana o prowadzenie obraźliwego bloga Mimi staje się obiektem agresji rówieśniczej – zarówno na terenie szkoły, jak i w sieci. Nie wytrzymuje presji i ucieka z domu. Uczestnicy kursu poznają różne aspekty cyberprzemocy z perspektywy ofiary, świadków oraz sprawcy, dowiadują się też, jak radzić sobie w takich sytuacjach. | 45 min |



Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

| | | | | |
|---|---|---|---|---|
| 5. | **W sieci** | Uczniowie klas I–III gimnazjum; szkoły ponadgimnazjalne | Kurs składa się z 2 modułów, w których młodzież zapoznaje się z historią internetu oraz dwoma powszechnie występującymi zagrożeniami: niebezpiecznymi kontaktami z osobami poznanymi w sieci oraz cyberprzemocą. Uczestnicy kursu dowiedzą się, jak radzić sobie w niektórych trudnych sytuacjach, związanych z korzystaniem z sieci. | 45 min |

Źródło: Opracowanie własne

Nie bez znaczenia jest skorzystanie przez nauczycieli – jako autorów treści do e-podręczników – z kursu adresowanego do profesjonalistów, obejmującego tematykę bezpieczeństwa dzieci online. Kurs „Dziecko w sieci" poświęcony jest bezpieczeństwu dzieci i młodzieży w internecie i został udostępniony bezpłatnie na platformie pod adresem www.fdn.pl/kursy. Materiał przeznaczony jest dla nauczycieli i innych profesjonalistów pracujących z dziećmi. Składa się z 18 modułów i trwa około 80 minut. Zadaniem użytkownika kursu jest przejście wszystkich modułów i poprawne rozwiązanie testu końcowego.

Oprócz powyższych propozycji istnieje możliwość skorzystania z pozostałych materiałów oferowanych przez Fundację Dzieci Niczyje. Ich szczegółowy wykaz dostępny jest pod adresem: www.dzieckowsieci.fdn.pl

## 1. Ocena zasobów internetowych

Nauczyciele, opracowując treści do lekcji z wykorzystaniem e-podręczników, powinni weryfikować każdą stronę, którą polecają uczniom.

Poniższa lista służy autorom treści e-podręczników na etapie dodawania linków – odnośników do zewnętrznych witryn. Zaleca się, aby każdy z autorów kontentu – poczynając od autorów podstawowych po autorów końcowych (nauczycieli) – posługiwał się nią, jeśli poleca zewnętrzną stronę www. Witryny te muszą spełniać wszystkie z niżej wymienionych wymagań.


Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Tabela 5. Kryteria oceny bezpiecznych zasobów internetowych

| | |
|---|---|
| Każdy element treści skierowany jest do dzieci i/lub młodzieży. Wyjątek stanowią serwisy o walorach edukacyjnych, adresowane do dorosłych, których przekaz musi być jednak sprawdzony pod względem zrozumienia przez ucznia z danego poziomu edukacji. | ☐ |
| Wyeliminowanie treści nielegalnych – pornograficznych, propagujących faszyzm, publicznie znieważających z powodu przynależności narodowej, etnicznej, rasowej. | ☐ |
| Wyeliminowanie treści szkodliwych, do których nie powinny mieć dostępu dzieci – erotycznych i pornograficznych, obraźliwych, poniżających oraz zawierających groźby, propagujących przemoc, nienawiść, zażywanie środków odurzających. | ☐ |
| Wyeliminowanie odnośników do witryn, w jakiejkolwiek formie zawierających treści nielegalne lub szkodliwe (częstym procederem jest umieszczanie linków do stron z treściami pornograficznymi czy erotycznymi w dolnych partiach strony czy w stopce). | ☐ |
| Strona nie uczestniczy w systemie wymiany bannerów, które dopuszczają udział witryn, o których mowa powyżej. | ☐ |
| Moderowanie forum, treści, czatu (aby sprawdzić, czy forum jest moderowane, należy wpisać testowo słowa, które powinny zostać usunięte przez moderatora lub nie powinny być dopuszczone). | ☐ |
| Niepublikowanie zdjęć z wizerunkiem dzieci, z wyjątkiem zdjęć zakupionych. | ☐ |
| Wygląd (grafika, estetyka) strony jest interesujący dla dzieci i dostosowany do możliwości młodego odbiorcy. | ☐ |
| Informacje zawarte na stronie są łatwe do odnalezienia i użycia. | ☐ |
| Strona jest łatwa i wygodna w obsłudze, pozbawiona rozpraszających uwagę obrazków, czcionek czy tła. | ☐ |
| Łatwa nawigacja po całej witrynie. | ☐ |
| Formularz rejestracyjny jest opatrzony klauzulą podawania i ochrony danych osobowych, zawierającą zgodę rodzica/opiekuna na podanie danych osobowych/korespondencyjnych. | ☐ |
| Formularz rejestracyjny posiada certyfikat bezpieczeństwa https. | ☐ |
| Tytuł i adres strony odpowiadają jej treści. | ☐ |



KAPITAŁ LUDZKI NARODOWA STRATEGIA SPÓJNOŚCI
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ SPOŁECZNY
Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

| | |
|---|---|
| Teksty na stronie powinny być poprawne językowo. | ☐ |
| Informacje zamieszczane na stronie powinny być aktualne i prawdziwe; jeżeli strona nie jest statyczna, powinny być zamieszczane daty aktualizacji. | ☐ |
| Strona powinna posiadać regulamin zrozumiały dla najmłodszych internautów, przy założeniu, że odbiorcą jest również dziecko w wieku od lat 6. | ☐ |

Źródło: www.sieciaki.pl/best

Kryteria oceny bezpiecznych zasobów edukacyjnych częściowo pochodzą z dokumentacji Fundacji Dzieci Niczyje, opracowanej na potrzeby weryfikacji stron do katalogu bezpiecznych stron.

Mając na uwadze bezpieczeństwo, należy ponadto zwrócić uwagę na dodatkowe elementy strony, a które powinny być dostępne w obrębie witryny:

1) Kontakt – dane podmiotu prowadzącego oraz administratora strony, na wypadek konieczności uzyskania pomocy.
2) Dział dla rodziców – informacje o serwisie, zasadach zabawy, regulaminie, polityce prywatności, zasadach bezpiecznego poruszania się dzieci w internecie.
3) Regulamin, który jest obowiązkowy w serwisie internetowym i dzięki któremu dzieci i opiekunowie dowiadują się:
   - kto prowadzi serwis;
   - na czym polega rejestracja;
   - kto i w jaki sposób administruje danymi osobowymi;
   - gdzie można zgłosić problem;
   - czy korzystanie z serwisu jest płatne.

Jeżeli serwis zakłada konieczność rejestracji, zalecane jest ograniczenie zbierania danych do potrzebnego minimum.

Obowiązkiem administratora strony www jest umieszczenie klauzuli wyrażenia zgody rodzica czy opiekuna na podanie danych osobowych dziecka. *Checkbox* zawarty przy klauzuli nie powinien być automatycznie zaznaczony.


Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Przykład klauzuli dotyczącej podawania i ochrony danych osobowych dziecka:

*Wyrażam zgodę na przetwarzanie danych osobowych mojego dziecka przez (nazwa i adres podmiotu prowadzącego serwis) w celu uzyskania przez dziecko pełnego dostępu do zawartości serwisu oraz otrzymywania informacji związanych z serwisem Sieciaki.pl. Jednocześnie oświadczam, iż wiem o przysługującym mi prawie do wglądu lub modyfikacji danych mojego dziecka*.

Zgoda ta jest dobrowolna (ustawa z dn. 29.08.1997 r. o ochronie danych osobowych, tekst jednolity: Dz.U. z 2002 roku Nr 101, poz. 926, z późn. zm.).



Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

# Rozdział VII

# Bezpieczne korzystanie z e-podręczników – ewaluacja na poziomie szkoły

Przygotowany dzisiaj e-podręcznik, zgodny ze standardami bezpieczeństwa, jutro może przynieść zagrożenie w wyniku dynamicznego rozwoju internetu oraz pojawiania się nowych sposobów wykorzystywania tego narzędzia przez uczniów. Dlatego celem niniejszego opracowania jest dostarczenie wiedzy zarówno autorom treści startowych, jak i nauczycielom, czyli autorom treści kolejnego etapu.

Platforma udostępniająca e-podręczniki powinna zostać wyposażona w komplet dokumentacji regulującej sposób bezpiecznego korzystania z e-podręczników przez uczniów i nauczycieli, na którą składają się:

- regulamin korzystania z e-podręcznika w szkole;
- regulamin korzystania z e-podręcznika w domu;
- umowa między uczniem a nauczycielem dotycząca sposobu korzystania z narzędzia;
- prawa i obowiązki ucznia oraz prawa i obowiązki nauczyciela;
- lista kryteriów bezpieczeństwa strony www (Tabela 5.), którą posługuje się nauczyciel jako autor treści powstających podczas polecania stron www;
- oświadczenie nauczyciela dotyczące zapoznania się z publikacją, stosowania zasad bezpiecznego tworzenia treści oraz poszerzania wiedzy z zakresu tematyki bezpieczeństwa dzieci online.



Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

# Rozdział VIII

# Porady dla autorów treści e-podręczników

Niezbędne jest, aby edukacja z wykorzystaniem e-podręczników została poprzedzona zdobyciem przez dzieci i młodzież wiedzy z zakresu zagrożeń pojawiających się podczas korzystania z internetu. Raport zawiera wykaz sugerowanych narzędzi edukacyjnych, dotyczących omawianego obszaru tematycznego, z podziałem na wszystkie poziomy edukacji (Tabela 4.).

Autorzy treści e-podręczników powinni polecać użytkownikom sprawdzone witryny, korzystając z formularza zawartego w opracowaniu (Tabela 5.), a w konsekwencji uczniowie unikną potencjalnych zagrożeń, jak:

- niebezpieczne treści;
- niemoderowane czaty;
- wirusy komputerowe.

Należy dbać o komfort pracy dzieci, które mają różną zdolność skupiania uwagi i odpowiednio – chętnie lub niechętnie – wracają do zadania po przerwie. Materiał i proces edukacyjny powinny uwzględniać czas na przerwę podczas korzystania przez uczniów z e-podręcznika.

Przygotowując platformę udostępniającą e-podręczniki, należy szczególnie zadbać o obszar rejestracji. Dzieci mogą udostępniać swoje dane osobowe wyłącznie za zgodą rodziców czy opiekunów, co musi zostać ujęte w klauzuli udostępniania i ochrony danych. Zalecane jest, aby zbieranie danych ograniczone było do potrzebnego minimum.

Konstruktorzy platformy udostępniającej e-podręczniki powinni przewidzieć funkcję automatycznego wylogowania się po zakończonej sesji, a także wtedy, kiedy po upływie około 5 minut od jej zakończenia nie zajdzie żadna interakcja, aktywne użycie treści.

Konstruktorzy e-podręczników oraz platform, które będą je udostępniać, powinni zapewnić, komfort niewymuszania na uczniach ciągłego bycia online, nieustannej aktualizacji i śledzenia zmian, sprawdzania nowinek – aby nie dochodziło do sytuacji, w których uczeń odczuwa lęk przed przeoczeniem czegoś istotnego.



Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Zakładając istnienie w systemie e-podręczników funkcji publikowania twórczości uczniów i jej oceny przez innych uczniów z grupy, należy przyjąć, że osobą kontrolującą ten proces będzie nauczyciel lub w domu – rodzic. Jeśli zajdzie potrzeba interwencji, osoby kontrolujące powinny mieć możliwość zgłoszenia incydentu administratorom platformy w celu zabezpieczenia dowodów, a następnie usunięcia incydentu i jego skutków z publicznej przestrzeni.

Rodzice i nauczyciele mogą skorzystać z pomocy Helpline.org.pl – porad specjalistów ds. bezpieczeństwa dzieci i młodzieży w internecie.

Nauczyciel, zlecając pracę domową z wykorzystaniem e-podręcznika, powinien uwzględnić czas, w jakim uczeń wykona zadanie, oraz zsumować go z czasem ogółem spędzonym online przez ucznia w tym dniu. W opracowaniu wyszczególniono czas adekwatny do wieku ucznia.

Nauczyciele będący autorami treści do e-podręczników powinni ukończyć kurs dla profesjonalistów, obejmujący tematykę bezpieczeństwa dzieci online. Przykładem jest „Dziecko w sieci” – bezpłatny kurs dostępny pod adresem www.fdn.pl/kursy

W celu zwiększenia bezpieczeństwa uczniów podczas korzystania z e-podręczników dodatkowo zaleca się:

- opracowanie oprogramowania do weryfikacji zawartości stron www – w zakresie tekstu i obrazu – polecanych uczniom przez nauczycieli;
- udział autorów treści e-podręczników w szkoleniach związanych z nowymi trendami w edukacji dzieci i młodzieży;
- szkolenie autorów treści e-podręczników w zakresie aktywności i bezpieczeństwa online dzieci i młodzieży;
- analizę gotowego e-podręcznika przeprowadzoną przez niezależnego eksperta ds. bezpieczeństwa online dzieci i młodzieży;
- badania focusowe przeprowadzone w grupie uczniów;
- audyt bezpieczeństwa e-podręczników oraz platformy udostępniającej narzędzia.


Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

## Podsumowanie

Powszechność korzystania z edukacyjnych zasobów multimedialnych, w tym zasobów internetowych, powoduje, że bezpieczeństwo dzieci i młodzieży online jest uważane za niezwykle istotne zagadnienie społeczne. Uczniowie i nauczyciele jako uczestnicy procesu edukacyjnego powinni być objęci ochroną i wyposażeni w narzędzia służące jej realizacji w celu efektywnego korzystania z e-podręcznika. Funkcje e-podręcznika – z założenia proste i intuicyjne – muszą zapewnić spokojne i bezpieczne przekazywanie i gromadzenie wiedzy. E-podręczniki nie mogą mimowolnie generować sytuacji zagrażających ich użytkownikom.

Konstruując nowoczesny podręcznik elektroniczny oraz platformę upowszechniającą, na każdym etapie pracy należy zwracać baczną uwagę na aspekt bezpieczeństwa. Wiedza z tej dziedziny musi być aktualizowana wraz z rozwojem nowych technologii i bieżących funkcji internetu. Tylko wtedy uda się przygotować i stale zapewniać bezpieczne środowisko pracy ucznia i nauczyciela.



Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

# Spis tabel i wykresów



# Bibliografia

1. www.dzieckowsieci.fdn.pl/badania
2. www.fdn.pl/eu-net-adb
3. www.programbadawczy.fdn.pl/eu-net-adb
4. www.fdn.pl/kursy
5. www.swps.pl/warszawa/nauka-i-rozwoj/eu-kids-online
6. www.sieciaki.pl/best
7. www.helpline.org.pl



Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

# RAPORT

ORE Ośrodek Rozwoju Edukacji

Aleje Ujazdowskie 28
00-478 Warszawa
tel. 22 345 37 00
fax 22 345 37 70

www.ore.edu.pl

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Publikacja współfinansowana przez Unię Europejską w ramach Europejskiego Funduszu Społecznego