Interdyscyplinarne Studia Społeczne
Numer 1 (3), 2017

Katarzyna Derlatka
Uczelnia Nauk Społecznych w Łodzi

Cyberzagrożenia w edukacji dla bezpieczeństwa i świadomość uczniów w obszarze bezpieczeństwa Internetu

Streszczenie: Na agendę przedmiotu określanego jako edukacja dla bezpieczeństwa składają się następujące elementy: ogólne zasady bezpieczeństwa państwa, organizacja działań ratowniczych, przygotowanie do kryzysu, edukacja zdrowotna, z wyłączeniem bardzo istotnych elementów – cyberbezpieczeństwa i cyberzagrożeń. Zagrożenia internetowe odnoszące się do trzech głównych obszarów, takich jak: nieodpowiednie kontakty w sieci, negatywne treści oraz niebezpieczne działania podejmowane przez dzieci wymagają naprawy. Po pierwsze, konieczne jest wprowadzenie lekcji poświęconych zagrożeniom i bezpieczeństwu w sieci. Po drugie, ciągła cyfryzacja w procesie nauczania, pojawianie się e-booków oraz wykorzystanie internetu, wymaga od nauczycieli zwracania uwagi na zachowania dzieci w internecie oraz na bezpieczne wykorzystywanie przez nich źródeł. Po trzecie, młodzi ludzie nie znają zasad bezpieczeństwa obowiązujących w sieci. Internet jest źródłem informacji na temat polityki, ekonomii, kultury, zdrowia itd. Wiedza dzieci na temat narzędzi dezinformacji, manipulacji i propagandy jest na satysfakcjonującym poziomie, ale umiejętność poruszania się w warunkach szumu informacyjnego jest mała.

Słowa kluczowe: edukacja, bezpieczeństwo, internet, badania, młodzież.

Internet jest niemal nieograniczonym źródłem informacji – może służyć rozrywce oraz być wykorzystywany do nawiązywania kontaktów. Korzystanie z niego przynosi zyski, niesie pomoc, ale ma on też swoją ciemną, niebezpieczną stronę. To medium jest też pełne zagrożeń. Trudno go kontrolować ze względu na globalny zasięg i dostęp, w związku z czym stał się polem działania również ludzi o złych intencjach oraz źródłem wielu negatywnych zjawisk. Szczególnie niebezpieczny jest dla dzieci, które ze względu na brak doświadczenia życiowego nierzadko poddają się bezkrytycznie cyfrowej rzeczywistości, wnikają w nią i nie zdają sobie sprawy z niebezpieczeństwa, jakie im może grozić, mimo, że przebywają w domu, własnym pokoju w gronie rodzinnym. W związku z tym stale rozwijany jest obszar edukacji dzieci na temat bezpiecznego korzystania z Internetu. Organizowane są dedykowane prelekcje w szkołach, realizowane prewencyjne kampanie medialne o tym, jak unikać zagrożeń w sieci. Od wczesnych lat szkolnych uczy się dzieci korzystania z narzędzi informatycznych. Czy w związku z tym wiedzą one wystarczająco dużo o zagrożeniach w sieci? Jakie są ich umiejętności radzenia sobie w cyberprzestrzeni? Nasuwa się tu także pytanie, czy przedmiot o wdzięcznej nazwie „Edukacja dla bezpieczeństwa" porusza zagadnienia z obszaru cyberbezpieczeństwa? W artykule tym zostaną przedstawione zagrożenia w sieci, wyniki badań

naukowych na temat świadomości zagrożeń i zachowań dzieci w Internecie oraz zagadnienia programu nauczania przedmiotu „Edukacja dla bezpieczeństwa". W celu prezentacji umiejętności korzystania z Internetu i świadomości zagrożeń dla dzieci w wirtualnym świecie w artykule tym zostaną także zaprezentowane wyniki badania własnego, które miało na celu poznanie zakresu korzystania z mediów społecznościowych przez dzieci, a także poznanie ich wiedzy na temat negatywnych zjawisk występujących, szczególnie w portalach społecznościowych (np. prześladowanie, popularnie zwane hejtem, fałszywe treści propagowane przez tzw. trolle, świadomość istnienia przemocy w sieci, niekontrolowanego kontaktu z nieznajomymi etc.).

Prezentowane badania własne uzupełniono także wynikami innych badań przeprowadzonych na młodzieży, które ukazują stan ich wiedzy o zagrożeniach w sieci. Warto tu wspomnieć, że najbardziej wyrazistym obszarem Internetu, przydatnym do zidentyfikowania zagrożeń i reagowania na nie lub nie przez dzieci, są media społecznościowe. W mediach tych dzieci wykazują dużą aktywność ze względu na przyjazne i łatwe z technicznego punktu widzenia (obsługa) środowisko, umożliwiające komentowanie, zamieszczanie zdjęć, bezpośrednią komunikację (tzw. czat). Prezentowane wyniki badania będą także ilustracją zjawisk, zagrożeń występujących w Internecie. Według danych ze stycznia 2017 roku miesięcznie z Facebooka korzystało 15 milionów użytkowników w Polsce, a dzieci w wieku 13-17 lat, mających profile w tym medium było 1,9 miliona (We Are Social. Sg, Digital in 2017 Eastern Europe).

Przedstawione w artykule dane pokazują poziom świadomości bezpieczeństwa dzieci w obszarze Internetu. Można też zauważyć różnice w zakresie wiedzy dzieci na ten temat w zależności od ich wieku oraz odmienne postrzeganie związków przyczynowo skutkowych podczas korzystania z mediów społecznościowych. Badania zostały przeprowadzone metodą sondażową w grupie 33 uczniów z dwóch warszawskich szkół, w tym wśród 19 uczniów 2 klasy gimnazjum (12 piętnastolatków i 7 czternastolatków) oraz 14 uczniów 6 klasy szkoły podstawowej w wieku: 11 lat - 2 uczniów, 12 i 13 lat – po 6 uczniów. Badani uczniowie w obu szkołach pochodzili z jednej klasy. Dzieci anonimowo opowiedziały na 18 pytań. Istnieje prawdopodobieństwo, że stan wiedzy dzieci w prezentowanych badaniach może być związany z poziomem edukacji w szkołach na temat zagrożeń w sieci, czy w związku z tym, można postawić tezę, że system edukacji w polskich szkołach należycie podchodzi do nauczania dzieci o cyberbezpieczeństwie?

Cyberbezpieczeństwo w jako element przedmiotu „Edukacja dla bezpieczeństwa"

Pomimo wprowadzenia tematów dotyczących tzw. bezpieczeństwa online do programów nauczania informatyki i coraz szerszego upowszechniania tej tematyki w szkołach, także przez

organizacje pozarządowe, regularne zajęcia nt. bezpieczeństwa w Internecie nie są jeszcze w polskich szkołach powszechne. Jak pokazują badania prowadzone przez Fundację Orange, z 2013 roku (Bezpieczeństwo dzieci w Internecie - raport z badania dzieci i rodziców zrealizowanego w 2013 r.), tylko 56% młodzieży gimnazjalnej zadeklarowało, że kiedykolwiek miało w szkole takie zajęcia, 29% zadeklarowała, że nigdy nie miała takich zajęć, a pozostali wybrali odpowiedź „nie pamiętam". Z kolei z badań „Dziecko w Sieci" Fundacji Dzieci Niczyje, wynika, że w grupie wiekowej 7-14 lat, z sieci codziennie korzysta niemal co drugie dziecko, a w grupie nastolatków 90 procent przyznało, że korzysta z Internetu codziennie. Spośród tej grupy 70 procent korzysta z możliwości grania online.

Jednym z elementów kształcenia w obszarze bezpieczeństwa jest cyberedukacja. Jest to szczególnie ważne z punktu widzenia przenoszenia do cyberprzestrzeni wielu usług świadczonych przez administrację publiczną oraz usług o charakterze finansowym. Niebezpiecznymi zjawiskami, z którymi stykają się użytkownicy sieci stają się kradzieże danych, kradzieże tożsamości i przejmowanie kontroli nad prywatnymi komputerami (Doktryna cyberbezpieczeństwa RP 2015). Dlatego istotnym stają się bieżące działania informacyjne i edukacyjne skierowane do dzieci i dorosłych w zakresie bezpiecznego korzystania z Internetu oraz informowanie o zidentyfikowanych zagrożeniach. Spośród działań społecznych w sferze bezpieczeństwa opisanych w Strategii Bezpieczeństwa Narodowego RP z 2014 roku, wskazano, że priorytetowe znaczenie ma - podnoszenie świadomości społecznej w kwestii rozumienia zagrożeń dla bezpieczeństwa i kształtowanie kompetencji pozwalających reagować na nie w sposób celowy i racjonalny. Edukacja dla bezpieczeństwa, bowiem, obejmuje działalność służącą zdobywaniu przez obywateli wiedzy i umiejętności z zakresu bezpieczeństwa. Realizowana jest przez szkolnictwo powszechne i wyższe, centralne i lokalne instytucje państwowe oraz stowarzyszenia i organizacje pozarządowe. Zadania w zakresie edukacji dla bezpieczeństwa dotyczą zwiększenia nacisku na jakość kształcenia w obszarach istotnych dla bezpieczeństwa państwa i obywateli w powszechnym systemie edukacji i w szkolnictwie wyższym oraz doskonalenia zawodowego m.in. nauczycieli przedmiotu „Edukacja dla bezpieczeństwa" (Doktryna cyberbezpieczeństwa RP 2015). W dokumencie tym czytamy także, że: „Należy uznać indywidualnych użytkowników, ich umiejętności i świadomość bezpieczeństwa, za jeden z filarów cyberbezpieczeństwa państwa, a co za tym idzie, kształtować mechanizmy przekazywania wiedzy oraz umiejętności w taki sposób, aby służyły zwiększeniu szans na osiągnięcie pożądanego poziomu cyberbezpieczeństwa". Istotnym jest więc pytanie, jak system edukacji, niedawno zreformowany, podchodzi do edukacji dla bezpieczeństwa z punktu widzenia cyberbezpieczeństwa?

W podstawie programowej przedmiotu „Edukacja dla bezpieczeństwa" dla klasy VIII szkoły podstawowej stwierdzono, że: **„**Przedmiot Edukacja dla bezpieczeństwa przygotowuje uczniów teoretycznie i praktycznie do wykształcenia umiejętności właściwego zachowania oraz

odpowiednich reakcji w sytuacjach trudnych i kryzysowych, stwarzających zagrożenie dla zdrowia i życia. Przedmiot obejmuje różnorodne treści kształcenia: z zakresu bezpieczeństwa państwa, w tym powszechnej samoobrony i obrony cywilnej oraz treści dotyczące organizacji działań ratowniczych, edukacji zdrowotnej i pierwszej pomocy" (Podstawa programowa przedmiotu Edukacja dla bezpieczeństwa klasa VIII szkoły podstawowej 2016, Ministerstwo Edukacji Narodowej). Podobne zapisy znajdują się w wytycznych dla klas gimnazjalnych i licealnych. Warto podkreślić, że program nauczania przedmiotu nie dotyczy tematyki cyberbezpieczeństwa, mimo, że w każdym z dokumentów wymienia się elementy obronne państwa i różne zagrożenia. Poniższa tabela zawiera spis celów kształcenia w przedmiocie „Edukacja dla Bezpieczeństwa".

Tabela 1. Cele kształcenia w podstawie programowej nauczania przedmiotu Edukacja dla Bezpieczeństwa (Źródło: Ministerstwo Edukacji Narodowej)

Cele kształcenia w podstawie programowej nauczania przedmiotu Edukacja dla Bezpieczeństwa		
Klasa VIII szkoły podstawowej	Klasa III gminazjum	liceum – zakres podstawowy
1. Bezpieczeństwo państwa. (Zna i charakteryzuje podstawowe pojęcia związane z bezpieczeństwem państwa, rozumie istotę problemu bezpieczeństwa; wymienia składniki bezpieczeństwa państwa. Rozumie i przedstawia historyczną ewolucję bezpieczeństwa Polski. Jest zorientowany w geopolitycznych uwarunkowaniach bezpieczeństwa, wynikających z położenia Polski. Zna i przedstawia rolę organizacji międzynarodowych w zapewnieniu bezpieczeństwa Polski. Wymienia i charakteryzuje współczesne problemy bezpieczeństwa międzynarodowego 2. Przygotowanie do działań ratowniczych w sytuacjach nadzwyczajnych zagrożeń (wypadków masowych i katastrof). 3. Podstawy pierwszej pomocy. 4. Edukacja zdrowotna. Zdrowie w wymiarze indywidualnym i zbiorowym. Zachowania prozdrowotne.	1. Znajomość powszechnej samoobrony i ochrony cywilnej. Uczeń rozumie znaczenie powszechnej samoobrony i ochrony cywilnej. 2. Przygotowanie do działania ratowniczego. Uczeń zna zasady prawidłowego działania w przypadku wystąpienia zagrożenia życia i zdrowia. 3. Nabycie umiejętności udzielania pierwszej pomocy. Uczeń umie udzielać pierwszej pomocy w nagłych wypadkach.	1. Znajomość struktury obronności państwa. Uczeń rozróżnia struktury obronności państwa, rozumie ich rolę oraz zna formy spełniania powinności obronnych przez organy administracji i obywateli. 2. Przygotowanie do sytuacji zagrożeń. Uczeń zna zasady postępowania w przypadku wystąpienia zagrożenia życia, zdrowia lub mienia; zna zasady planowania i organizowania działań. 3. Opanowanie zasad pierwszej pomocy. Uczeń umie udzielać pierwszej pomocy poszkodowanym w różnych stanach zagrażających życiu i zdrowiu.

Źródło: Opracowanie własne według podstawy programowej nauczania przedmiotu „Edukacja dla Bezpieczeństwa" Ministerstwa Edukacji Narodowej

Jeśli program edukacyjny dotyczy reagowania na zagrożenia, przeciwdziałania im i podnoszenia świadomości w obszarze bezpieczeństwa, w tym obronności, nasuwa się pytanie dlaczego brakuje w nim tak ważnej kwestii jak cyberbezpieczeństwo. Zrozumienie struktury obronnej państwa to także przeciwdziałanie cyberzagrożeniom, które mogą mieć wpływ na bezpieczeństwo państwa, społeczeństwa i rodziny.

Działania edukacyjne w zakresie cyberbezpieczeństwa skierowane do dzieci

Wraz z rozwojem Internetu dzieci zostały narażone na wpływ szkodliwych treści, takich, jak materiały prezentujące sceny przemocy, szkodliwe wartości i postawy społeczne czy pornografia. Duży problem stanowi kontakt dzieci z nieznajomymi osobami - zjawisko groomingu (uwodzenie dzieci online), ale również zachęcanie do uczestnictwa w sektach, ekstremistycznych ugrupowaniach politycznych, np. w grupach neonazistowskich, czy terrorystycznych, stosowania używek, wciągania w niebezpieczne gry takie, jak „Niebieski Wieloryb" (zmuszająca graczy do samookaleczania, a nawet odbierania sobie życia). Innymi problemami są różne formy przemocy rówieśniczej, brak ochrony prywatności, czy też generalne uzależnienie dzieci od mediów elektronicznych. W ramach rozpowszechniania wiedzy na temat bezpieczeństwa w sieci, identyfikacji cyberzagrożeń realizowane są liczne społeczne programy edukacyjne i tworzone dedykowane strony internetowe mające na celu wsparcie dzieci i rodziców w korzystaniu z Internetu. Dla ochrony dzieci w sieci działa m.in. Fundacja Dzieci Niczyje, która od 2003 roku zajmuje się problematyką bezpieczeństwa dzieci i młodzieży w Internecie. Działaniem takim zajmuje się także Urząd Komunikacji Elektronicznej, który uruchomił program „Dla ochrony dzieci w Internecie". Na stronie internetowej Fundacji Odkrywców Innowacji i Fundacji Drabina Rozwoju http://wiedza.bezpiecznyinternet.edu.pl/wyszukiwarka/wybor) powstała baza, która zawiera wyselekcjonowane, materiały na temat bezpieczeństwa i zagrożeń w sieci. Ministerstwo Edukacji Narodowej zamieściło informacje na swojej stronie internetowej m.in. „Standardy bezpieczeństwa online placówek oświatowych" oraz inne materiały (dostępne pod adresem: https://bezpiecznaszkola.men.gov.pl/programy/bezpieczna-i-przyjazna-szkola/dzialania-krajowe/). Informacje na temat bezpieczeństwa i zagrożeń w sieci dostępne są również na stronie: http://bezpiecznyinternet.edu.pl/. Dodatkowo w MEN powstał Zespół Kryzysowy, którego zadaniem jest podjęcie szerokorozumianych działań prewencyjnych na rzecz bezpieczeństwa uczniów w Internecie. Na stronie internetowej Fundacji Dla Kultury.pl (www.ambasadorzy.kulturaonline.pl) działa platforma e-learningowa, na której zmieszczone są specjalne szkolenia. O bezpieczeństwie dzieci i młodzieży w Internecie traktują także serwisy: dyżurnet.pl, ore.edu.pl, akademia.nask.pl, kursor.edukator.pl, saferinternet.pl, plikifolder.pl. W ramach edukacji i prewencji można także znaleźć bezpłatne publikacje, takie jak kompendium „Bezpieczeństwo dzieci online"

wydane przez Polskie Centrum Programu Safer Internet (NASK i Fundację Dzieci Niczyje), a także poradnik dla rodziców „Bezpieczne Media" wydany przez Fundację Orange. Zatem działania edukacyjne realizowane przez różne środowiska, fundacje, stowarzyszenia, ministerstwo etc. mają szeroki i dynamiczny zakres publikacji na temat cyberbezpieczeństwa, jednak edukacja ta mimo swojej merytorycznej wartości wymaga ciągłej aktualizacji i powtarzania, gdyż jak pokazują dane w dalszej części artykułu dzieci stale są narażone na zagrożenia w sieci.

Charakterystyka zagrożeń w Internecie dla dzieci i młodzieży

Sieć internetowa to nieograniczony zasób różnorakich treści, w tym niosących zagrożenia, które znajdziemy m.in. w aplikacjach mobilnych, czatach i komunikatorach, grach online, poprzez dostęp do Internetu mobilnego oraz czaty wideo, usługi geolokalizacyjne, a także w portalach społecznościowych. Szczególnie groźne dla dzieci w Internecie są cyberprzemoc, pornografia dziecięca, mowa nienawiści, nierozważne publikowanie wizerunku dziecka przez dorosłych, plagiatowanie, promowanie zachowań autodestrukcyjnych, reklama i marketing online skierowane do dzieci, udostępnianie niemoralnych plików z sieci, uwodzenie dzieci w Internecie, niebezpieczne kontakty. Lista jest długa, ale każde z wymienionych oblicz Internetu może stanowić zagrożenie także dla dorosłych, jeśli brakuje im stosownej wiedzy na temat właściwego i bezpiecznego korzystania z Internetu oraz kontroli i wsparcia. W raporcie – „Safer Children in a Digital World. The Report of the Byron Review" (Byron, 2008), wymieniono potencjalne zagrożenia dla dzieci, które korzystają z Internetu. Są to:

- zagrożenia dla rozwoju fizycznego (wady wzroku, otyłość, zespół urazowy - nadgarstka, wady postawy, m.in. problemy szyjnego odcinka kręgosłupa - ból i zwyrodnienie);
- zagrożenia dla rozwoju poznawczego (treści nasączone emocjami – związane np. z przemocą czy pornografią – silnie oddziaływujące modelująco;
- zagrożenia dla rozwoju emocjonalnego i społecznego, czyli nadmierne korzystanie z Internetu może negatywani wpływać na interakcje społeczne;
- zagrożenia związane z dominującą rolą Internetu w aktywności dziecka na tle innych jego aktywności, uzależniający aspekt korzystania z Internetu.

Wiele z istniejących zagrożeń występuje w mediach społecznościowych, które są popularną formą prezentacji różnych treści i aktywnej komunikacji wśród młodzieży, szczególnie przy użyciu mobilnych technologii, które umożliwiają nieograniczony czasem i miejscem dostęp do sieci. Stopień aktywności i znajomość sieci społecznościowych wśród dzieci pokazują wyniki przeprowadzonego badania własnego.

Tabela2. Popularność mediów społecznościowych wśród nastolatków

	Klasa 2 gimnazjum				Klasa 6 szkoła podstawowa					
Liczba respondentów	12		7		6		6		2	
Wiek respondentów	15		14		13		12		11	
	TAK	NIE	TAK	NIE	TAK	NIE	TAK	NIE	TAK	NIE
Czy masz konta w mediach społecznościowych? Zaznacz właściwą odpowiedź.	12	0	6	1	6	0	5	1	0	2
Czy masz konto na Facebooku?	12	0	6	1	6	0	3	3	0	2
Czy masz konto na Twitterze?	2	10	0	7	1	5	0	6	0	2
Czy masz konto na Instagramie?	8	4	2	5	3	3	3	3	0	2

Źródło: Opracowanie własne.

Według powyższej tabeli najpopularniejszym portalem społecznościowym wśród ankietowanych jest Facebook. Należy tu wspomnieć, że zgodnie z regulaminem Facebooka (Data ostatniej aktualizacji: 30 stycznia 2015 r.) „Zabronione jest korzystanie z Facebooka przez osoby poniżej 13. roku życia." Mimo to ankietowane dzieci w wieku 12, 13 lat deklarują, że mają w nim konta. Największa grupa użytkowników jest wśród 15 i 14-latków oraz 13-latków. Dzieci 11-letnie nie deklarowały posiadania takiego konta, a 12-letnie w 50%.

Kolejnym medium w rankingu popularności jest Instagram – aplikacja używana do zamieszczania i komentowania zdjęć. W tej kategorii najwięcej użytkowników jest wśród najstarszych uczniów, najmłodsi badani nie używali tej aplikacji. Na pytanie dotyczące aplikacji Twitter, większość uczniów odpowiedziała, że nie posiada tam konta. Na 33 ankietowane osoby tylko 3 zadeklarowały posiadanie aktywnego profilu. Twitter to portal społecznościowy oparty o usługę mikroblogowania, umożliwiający użytkownikom wysłanie wiadomości składających się ze maksymalnie ze 140 znaków wiadomości tekstowych. Zamieszczane w nim treści i komentarze mają zdecydowanie charakter polityczno-społeczny, co prawdopodobnie stanowi przyczynę małego zainteresowania wśród dzieci. Według danych „We are social, Digital in 2017 Eastern Europe", w Polsce spośród 15 milionów Polaków korzystających z mediów społecznościowych,

62% użytkowników korzysta z Facebooka, a 24% z Twittera i Instagrama.Wróćmy jednak do zagrożeń dla młodzieży.

Według Raportu „Bezpieczeństwo dzieci korzystających z Internetu" (2008) możemy je podzielić na następujące obszary.

1. Treści - zawartość Internetu, szczególnie niebezpieczne treści, materiały, które mogą mieć szkodliwy wpływ na rozwój i psychikę dziecka. W Polsce do nielegalnych zalicza się materiały pornograficzne z udziałem dzieci, promujące pedofilię, przemoc wobec ludzi i zwierząt oraz treści o charakterze rasistowskim i ksenofobicznycznym, obejmujące także przekazy promujące zachowania autodestrukcyjne (takie jak promocja brania narkotyków, skrajnego odchudzania, czy opisywanie sposobów na samobójstwo). Według badań EU Kids online z 2010 r., odsetek dzieci napotykających na niebezpieczne treści wyraźnie się zmniejszył, choć w dalszym ciągu jest znaczący (Livingstone, Haddon, 2009; Livingstone, Mascheroni, Staksrud, 2015). Międzynarodowe badania EU-NET-ADB z 2012 r. pokazały, że kontakt z pornografią miało ponad dwie trzecie (67%) polskich gimnazjalistów, z pozostałymi niebezpiecznymi treściami wymienionymi powyżej, przynajmniej raz, kontakt miało 54% gimnazjalistów. Wyróżniono tu zagrożenia komercyjne, zagrożenia związane z agresją i przemocą, zagrożenia związane ze sferą seksualną, zagrożenia związane z wartościami (Pyżalski, 2017).

2. Kontakty – z niebezpiecznymi osobami. Internet umożliwia nawiązywanie nowych znajomości i łatwe znajdowanie ludzi o podobnych zainteresowaniach czy poglądach. Daje też użytkownikowi dostęp do ogromnych zasobów treści oraz możliwość aktywnego uczestniczenia w wielu działaniach (między innymi publikowania własnych treści). Niestety kontrola dorosłych nad tym, co dzieci robią w Internecie, jest bardzo ograniczona (Pyżalski, 2017). Przykładem tzw. złego kontaktu jest zjawisko „groomingu", czyli uwodzenia dzieci w Internecie w celu późniejszego wykorzystania seksualnego, niebezpieczne kontakty mogą dotyczyć także zjawisk takich jak werbunek do sekty lub grupy przestępczej. Przywołane powyżej badania pokazują, że aż 69% gimnazjalistów poznało w Internecie kogoś, kogo nie znało wcześniej (EU-NET-ADB z 2012 r.). Co bardziej niepokojące, aż 31% spotkało się z taką osobą na żywo. W procesie uwodzenia pedofile poddają dzieci psychomanipulacji. Według badań EU Kids Online, co czwarty polski internauta w wieku 9–16 lat kontaktuje się w sieci z osobami, których osobiście nigdy nie poznał (średnio w Europie 30%). Spotkania twarzą w twarz z osobami poznanymi w Internecie deklaruje 8% młodych użytkowników sieci (średnio w Europie 9%).

Zawieranie kontaktów w osobami nieznajomymi było także jednym z zagadnień ankiety przeprowadzonej dla potrzeb tego artykułu. W przedstawionej poniżej tabeli na pytanie: Czy kiedykolwiek ktoś próbował zaprosić Cię do sekty, tajemniczej grupy społecznościowej itp.? siedmioro uczniów odpowiedziało tak. Co pozwala na stwierdzenie, że uczniowie są świadomi takiego zagrożenia, ale bardzo niepokojące są pozytywne odpowiedzi na kolejne pytanie: Czy przyjmujesz do grona znajomych w mediach społecznościowych osoby, których nie znasz osobiście? Dziesięcioro spośród 33 badanych przyjmuje nieznane osoby do grona znajomych w mediach społecznościowych. Jeszcze bardziej zastanawiające jest to, że uczniowie, którzy temu zaprzeczyli mają wielu znajomych na Facebooku. Dotyczy to pytania trzeciego w powyższej tabeli: Ilu masz znajomych na Facebooku? Podaj faktyczną lub przybliżoną liczbę. Podane w tabeli wyniki (liczne grupy znajomych, mało prawdopodobne w rzeczywistości) zostały oznaczone przez ankietowanych, którzy na pytanie 2 odpowiadali i tak i nie. Oznacza to, że być może są to tzw. znajomi znajomych, gdzie jakiś kontakt między użytkownikami nastąpił, bądź znają się z widzenia. Jednak niektóre zadeklarowane wartości są tak duże, że, jeśli są prawdziwe, powinny być niepokojące dla rodziców i wychowawców. Należałoby sprawdzić, czy deklarowani znajomi są faktycznie znani badanym dzieciom, czy też są to przypadkowe osoby, być może mające złe zamiary.

Tabela 3. Kontakty w Internecie

	Klasa 2 gimnazjum				Klasa 6 szkoła podstawowa					
Liczba respondentów	12		7		6		6		2	
Wiek respondentów	15		14		13		12		11	
	TAK	NIE	TAK	NIE	TAK	NIE	TAK	NIE	TAK	NIE
1. Czy kiedykolwiek ktoś próbował zaprosić Cię do sekty, tajemniczej grupy społecznościowej itp.?	7	5	1	6	0	6	0	6	0	2
2. Czy przyjmujesz do grona znajomych w mediach społecznościowych osoby, których nie znasz osobiście?	7	5	1	6	1	5	1	5	0	2

3. Ilu masz znajomych na Facebooku? Podaj faktyczną lub przybliżoną liczbę.	2629 45 500 0 1500 69 650	180 111 200 72 68	2	95 0 300 65 103 65	175	300 600 300 500 70	0	50 2 5 - 30 327 0 0	0	0

Źródło: Opracowanie własne.

3. Zachowanie – czyli niebezpieczne działania, jakie dzieci same mogą podejmować. Są to cyberprzemoc, czyli zachowania określane mianem agresji elektronicznej, które mogą przyjmować różne formy takie, jak zamieszczanie kompromitujących materiałów, agresja werbalna, tworzenie specjalnych obraźliwych stron lub profili. Stosunkowo nowym, trendem jest tzw. seksting, czyli przesyłanie własnych intymnych zdjęć lub filmików za pomocą telefonu komórkowego lub komunikatorów internetowych. W niedawnym badaniu Fundacji Dzieci Niczyje do wysyłania takich materiałów przyznało się aż 11% młodych ludzi. Ofiarą różnych form przemocy pada nawet co piąty gimnazjalista (22%).

Poziom możliwego kontaktu z cyberprzemocą pokazują kolejne dane z przeprowadzonego badania.

Tabela 4. Komunikacja i przemoc internetowa

	Klasa 2 gimnazjum				Klasa 6 szkoła podstawowa					
Liczba respondentów	12		7		6		6		2	
Wiek respondentów	15		14		13		12		11	
	TAK	NIE	TAK	NIE	TAK	NIE	TAK	NIE	TAK	NIE
1. Czy komentujesz posty innych użytkowników?	9	3	4	3	5	1	5	1	0	2
2. Czy wiesz, co to jest hejt?	12	0	7	0	6	0	6	0	2	0

3. Czy potrafisz zidentyfikować hejtera?	11	1	7	0	3	3	5	1	1	1
4. Czy byłaś (łeś) świadkiem przemocy w mediach społecznościowych?	8	4	4	3	1	5	2	4	0	2
5. Czy kiedykolwiek byłaś (łeś) ofiarą przemocy w sieci internetowej?	5	7	2	5	0	6	0	6	0	2

Źródło:Opracowanie własne.

Na pytanie: Czy komentujesz posty innych użytkowników? - 23 z 33 respondentów odpowiedziało tak, co oznacza, że świadomie lub nie mogą stać się potencjalnym źródłem przemocy w zależności od formy komentarza i jego subiektywnego odbioru. Nie zawsze, bowiem agresywny tekst musi zawierać wulgaryzmy. Wystarczy żartobliwa wypowiedź, jakikolwiek dwuznaczny, czy negatywny komentarz, by wywołać lawinę innych, niekoniecznie miłych, obraźliwych komentarzy dla autora publikowanego tekstu. Komunikacja w firmie pisemnej nie zawiera dodatkowych elementów, takich jak język ciała (gestów, mimiki), które umożliwiają odbiorcy zrozumienie intencji, np. żartobliwego tonu wypowiedzi. Internet umożliwia określenie emocjonalne wypowiedzi w zasadzie przy pomocy tzw. emotikonów (grafiki „buziek" np. z uśmiechem), ale nie każdy użytkownik rozumie potrzebę uzupełnienia treści o takie dodatkowe „emocjonalne" elementy. Wracając do wyników badań, wszyscy ankietowani uczniowie, bez względu na wiek i stopień zaawansowania w korzystaniu z Internetu deklarują, że wiedzą, czym jest „hejt", czyli obraźliwy lub agresywny komentarz zamieszczony w Internecie (pyt. 2). Niemalże połowa uczniów była świadkami przemocy w mediach społecznościowych (pyt. 4), a siedmioro stało się ofiarą przemocy w Internecie, w tym przypadku byli to uczniowie starsi 14 i 15-letni.

4. Uzależnienie. Kolejnym zagrożeniem, bardzo niebezpiecznym dla zdrowia psychicznego (m.in. izolacja dzieci i młodzieży, zaburzone relacje rówieśnicze, rodzinne, kłopoty szkolne, agresja) jest uzależnienie od Internetu. Sprzyja temu dostępność i atrakcyjność Internetu oraz często ograniczona kontrola rodzicielska. Problem ten stanowi przedmiot licznych analiz, badań i dyskusji. Powagi problemowi dostarczają ostatnie doniesienia Światowej Organizacji Zdrowia, która zwróciła uwagę na to zagrożenie i planuje wpisać uzależnienie m.in. od Internetu i gier na listę chorób psychicznych. Uzależnienie od gier nie jest nowym zjawiskiem, zmaga się z nim coraz więcej osób. Według statystyk, w Polsce jest prawie 16 milionów

graczy, również dzieci. Szacuje się, że z tej grupy około 15 % (czyli około 2,5 miliona osób) jest uzależnionych od gier i Internetu. Uzależnionych od Internetu, wg kryteriów Young[1], jest ok. 15% polskich nastolatków (dane z 2009 roku). Badania EU-Net-ADB (Badanie nadużywania Internetu przez młodzież w Polsce i Europie z 2012 roku), dotyczące młodzieży w wieku 14–17 lat, wskazały, że nadużywanie Internetu dotyczy 1,3% tej populacji, a korzysta z niego 12% młodzieży w tym wieku. Temat uzależnień dzieci od Internetu podjęty został w badaniach EU Kids Online, gdzie wskazno pięć symptomów uzależnienia od Internetu: zagrożenie dla zdrowia fizycznego (zakłócenia snu, zaburzenia odżywania), nauki, zainteresowań, potencjalnych konfiktów w rodzinie i funkcjonowania społecznego oraz trudności w ograniczeniu lub wykluczeniu uzleżniającej aktywności.

5. Zagrożenia informacyjne**.** To kolejny nieco odmienny od pozostałych obszar bezpieczeństwa w Internecie, choć teoretycznie spójny z punktem 1. Treści, to jednak stanowi indywidualną kategorię ze względu na niejednoznaczny charakter. Można tu wymienić niebezpieczne działania takie jak: operacje psychologiczne, które polegają na wpływaniu na emocje, motywacje, obiektywne rozumowanie. Celem jest tu wzmocnienie lub nakłonienie do zachowań korzystnych dla realizacji własnych interesów. Kolejnym sposobem oddziaływania na odbiorcę poprzez Internet jest inżynieria społeczna - zespół metod i środków celowego manipulowania społeczeństwem.

Ważnym zagrożeniem jest dziś trolling, czyli antyspołeczne zachowanie charakterystyczne dla internetowych grup, forów dyskusyjnych, czatów i sieci społecznościowych. To zamierzone wpływanie na innych użytkowników w celu ich ośmieszenia lub obrażenia poprzez wysyłanie napastliwych, kontrowersyjnych, często nieprawdziwych przekazów. Na ten typ zagrożenia dzieci są narażone szczególnie w mediach społecznościowych. Nieprawdziwy, zniekształcony przekaz informacyjny może negatywnie wpływać na poczucie tożsamości młodego człowieka, jego poglądy i wiedzę, której mocne filary zbudowane przez lata nauki mogą zostać zachwiane. Wszechobecna w Internecie propaganda i dezinformacja, czyli rozpowszechnianie zmanipulowanych lub sfabrykowanych informacji (albo kombinacji jednych i drugich) w celu skłonienia odbiorców do określonych zachowań korzystnych dla dezinformującego

[1] Kimberly Young wyróżniła pięć podtypów uzależnienia od internetu: 1. Erotomania internetowa (cybersexual addiction), 2. Socjomania internetowa (cyber-relationship addiction), 3. Uzależnienie od sieci (net compulsions), 4. Przeciążenie informacyjne lub przeladowanie informacjami (information overload), 5. Uzależnienie od komputera (computer addiction). Young w jednym ze swoich opracowań dokonała także systematyki cech odróżniających normalne użytkowanie internetu od patologicznego. Fazy, przez które przechodzą internauci coraz bardziej uzależniając się wyglądają następująco: I faza - zaangażowania - użytkownik zapoznaje się z internetem i jego możliwościami. II faza - zastępowania - intensywne uczucia występujące w poprzedniej fazie zastępowane są przez redukcję dyskomfortu. III faza - ucieczki - uzależnienie pogłębia się prowadząc do silnej i coraz większej potrzeby oraz chęci korzystania z internetu.

oraz odwrócenie ich uwagi od faktycznie zaistniałych wydarzeń, to kolejne zagrożenie, któremu nieświadomie ulegają odbiorcy informacji. Także manipulacja informacją poprzez wykorzystanie prawdziwych informacji, ale w taki sposób, żeby wywołać fałszywe implikacje np. pomijanie niektórych, istotnych, ale niewygodnych informacji, czy dobór informacji, tak, żeby budziły fałszywe skojarzenia, to kolejny sposób wpływania na zachowanie i myślenie, zwłaszcza młodego człowieka. Skutkiem takich zagrożeń informacyjnych polegających na deformowaniu treści oraz wprowadzaniu do systemów informacyjnych nieprawdziwych informacji, może być nieświadome, niezamierzone powielanie przez użytkowników np. mediów społecznościowych sprzecznego przekazu informacyjnego. Oznacza to nieświadomy udział w generowaniu zagrożeń informacyjnych. U odbiorcy takich niebezpiecznych przekazów może wystąpić deficyt informacyjny, skutkujących podatnością na wrogą perswazję. Pojawia się tu dezinformacja będąca wynikiem agresywnych działań propagandowych. Narzucane obce idee niezgodne z interesem społecznym i państwa, może skutkować pojawieniem się i rozwojem postaw aspołecznych i antypaństwowych, agresywnych, defetystycznych (np. islamofobia, szpiegomania).

W prezentowanych badaniach własnych okazuje się, że młodzież jest świadoma zagrożeń informacyjnych, choć samo badanie nie pozwala na twierdzenie, że ankietowani znają definicje tych zagrożeń, niemniej konkretne odpowiedzi świadczą o rozumieniu występowania poszczególnych zjawisk i pojęć. W poniższej tabeli w odpowiedzi na pytanie 6. pojawiają się wartości ułamkowe, gdyż ankietowani zakreślili zarówno odpowiedź twierdzącą i przeczącą, co najprawdopodobniej oznacza niepewność, co do prawdziwości informacji prezentowanych w sieci.

Tabela 5. Znajomość zagrożeń informacyjnych

	Klasa 2 gimnazjum				Klasa 6 szkoła podstawowa					
Ilość respondentów	12		7		6		6		2	
Ile masz lat?	15		14		13		12		11	
	TAK	NIE	TAK	NIE	TAK	NIE	TAK	NIE	TAK	NIE
1. Czy wiesz, kto to jest troll?	11	1	7	0	6	1	5	1	1	1
2. Czy potrafisz zidentyfikować trolla?	11	1	5	2	5	1	3	3	0	2
3. Czy rozumiesz pojęcie propaganda?	10	12	7	0	4	2	6	0	2	0

4. Czy rozumiesz pojęcie dezinformacja?	8	4	5	2	1	5	3	3	0	2
5. Czy wiesz na czym polega manipulacja informacją?	10	2	6	1	5	1	6	0	1	1
6. Czy uważasz za prawdziwe informacje udostępnione w sieci internetowej?	4,5	7,5	1,5	5,5	0	6	0,5	5,5	0	2

Źródło: Opracowanie własne.

Okazuje się, że większość badanych wie, czym są konkretne zagrożenia, twierdzi, że potrafi je zidentyfikować, rozumie ich mechanizmy działania. Pytanie 6: Czy uważasz za prawdziwe informacje udostępnione w sieci internetowej? Większość wybrała opcję „nie", co oznacza, że wiedzą iż nie wszystko, co zostało umieszczone w sieci jest prawdziwe. Potrafią być sceptyczni, mają świadomość potrzeby weryfikacji zastanych informacji, ale niewiadomym jest, czy rzeczywiście sprawdzają treści zamieszczone w Internecie. Niemniej jednak nie ufa wszystkim przekazom, a to skłania do poszukiwania prawdy i poszerzania wiedzy.

Podsumowanie

Z przeprowadzonego badania własnego wynika, że świadomość działania Internetu, w tym umiejętność identyfikacji zagrożeń jest większa wśród starszych uczniów. Uczniowie jedenastoletni na większość pytań odpowiadali „nie", co wskazywałoby na większą ostrożność w korzystaniu z sieci, niepewność w wirtualnym środowisku, brak doświadczenia lub brak dostępu do sieci spowodowany uważniejszą kontrolą rodziców ze względu na wiek dzieci. Wiedza i praktyka związana z użytkowaniem Internetu młodszych dzieci jest mniejsza, mimo potencjalnego wpływu starszych kolegów z klasy (vide: różnica wieku uczniów w badanej klasie w szkole podstawowej). Zaprezentowane w artykule wyniki badań, analiza programu nauczania przedmiotu „Edukacja dla bezpieczeństwa" oraz wskazane zagrożenia, z którymi ma i może mieć do czynienia młodzież wskazują na konieczność następujących działań edukacyjnych i naprawczych.

Po pierwsze, konieczne jest wprowadzenie w programie edukacji dedykowanych zajęć lekcyjnych na temat zagrożeń i bezpieczeństwa w sieci. Ze względów programowych i możliwości czasowych można tego typu zagadnienie wprowadzić jako obowiązkowe na lekcjach „Informatyki"i „Edukacji dla bezpieczeństwa". Tematyka cyberbezpieczeństwa, niestety nie jest wyraźnie sformułowana

w treściach programowych nauczania tych przedmiotów. Można domniemywać, że przekazywana na ten temat wiedza zależy wyłącznie od nauczyciela prowadzącego. Stąd wniosek, że system edukacji w polskich szkołach w zbyt małym stopniu realizuje nauczanie dzieci o cyberbezpieczeństwie. Zadowalająca jest ilość publikacji internetowych i realizowanych pozaszkolnych programów edukacyjnych (spotkań tematycznych, konferencji, warsztatów etc.) na ten temat cyberbezpieczeństwa, jednak ze względu na pozaszkolny charakter (nieobowiązkowe zajęcia) może ona niedostatecznie docierać do odbiorców – tu akurat dzieci. Obowiązkowe lekcje na ten temat w szkole mogłyby znacznie skuteczniej oddziaływać, poprzez kontrolę znajomości zasad bezpieczeństwa.

Po drugie, postępująca cyfryzacja w nauczaniu, e-podręczniki i Internet, wymaga od nauczycieli permanentnego zwracania uwagi na zachowanie dzieci w Internecie, na sposoby bezpiecznego korzystania z tego źródła. Realizacja takiej kontroli wymaga stworzenia sposobu prowadzenia nadzoru dzieci we współpracy z rodzicami oraz wdrożenia większej ilości zajęć edukacyjno-prewencyjnych. Jeśli tego typu przekaz od nauczyciela będzie naturalnym elementem wprowadzenia do zajęć, podczas których wykorzystuje się Internet, nawet do prac domowych, to istnieje nadzieja, że zasady te zostaną zapamiętane przez młodzież i będą naturalnie stosowane. Tu zaznaczyć trzeba, że nie unikniemy tzw. uzależnienia młodych ludzi od Internetu, gdyż korzystanie z nowoczesnych technologii jest elementem postępu i zmiany cywilizacyjnej, jest czymś naturalnym i koniecznym do funkcjonowania w społeczeństwie. Należy jednak kontrolować czas korzystania z tego dobrodziejstwa naszych czasów i wykorzystać go jako nieograniczone źródło wiedzy w procesie edukacji. Traktowanie tzw. uzależnienia od Internetu jako choroby psychicznej może być nadużyciem. Taki stan muszą potwierdzić szczegółowe badania danej jednostki, a przyjmuje się, że codzienne, długie korzystanie z sieci może być symptomem uzależnienia. To błąd. Gdybyśmy cofnęli się o 30 lat, to samo można by powiedzieć o słuchaniu muzyki na kasetach, oglądaniu filmów video, czytaniu książek w niewłaściwej pozycji etc. Nowe czasy i technologie tworzą nowe standardy życia.

Po trzecie, młodzież nie zna zasad bezpieczeństwa w sieci. Wydaje im się, że wiedzą, jak należy postępować w określonych przypadkach, ale są to zazwyczaj informacje cząstkowe. Konieczna jest zatem edukacja na temat zagrożeń, realizowana np. w ramach przedmiotu „Edukacja dla Bezpieczeństwa". W sytuacji, gdy konkretny młody człowiek stanie w obliczu zagrożenia w Internecie, prawdopodobieństwo właściwego postępowania jest niewielkie. Warto pamiętać, że nawet dorośli nie potrafią sobie radzić z prześladowaniem, stresem i strachem, więc nie można takich umiejętności oczekiwać od dziecka czy nastolatka. Internet jest źródłem opinii na temat polityki, gospodarki, kultury, zdrowia etc. Świadomość istnienia narzędzi dezinformacji, manipulacji i propagandy wśród uczniów jest na zadowalającym poziomie, jednak umiejętność poruszania się wśród tzw. szumu informacyjnego jest niewielka.

Bibliografia

Bezpieczeństwo dzieci korzystających z Internetu. Raport. (2008). Telekomunikacja Polska, Fundacja Dzieci Niczyje. [dostęp: 22.12.2017].

Bezpieczeństwo dzieci w Internecie – raport z badania dzieci i rodziców zrealizowanego w 2013 r. (2013). TNS na zlecenie Fundacji Orange. Fundacja Dzieci Niczyje. [dostęp: 22.12.2017].

Byron, T. (2008). *Safer Children in a Digital World. The Report of the Byron Review. Department for Children*, Schools and Families Publications, Sherwood Park, UK.

Doktryna cyberbepieczeństwa. (2015). Biuro Bezpieczeństwa Narodowego. Warszawa.

Eurobarometr (2008). Raport EU Kids Online. http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20I%20(2006-9)/EU%20Kids%20Online%20I%20Reports/EUKidsOnlineFinalReport.pdf. [dostęp: 22.12.2017].

EU NET ADB. (2012). Badanie nadużywania Internetu przez młodzież w Polsce - raport szczegółowy z części ilościowej (informacje na temat badania na stronie: www.fdn.pl/eu-net-adb. [dostęp: 22.12.2017].

EU NET ADB. (2012). Badanie nadużywania Internetu przez młodzież w Polsce i Europie. Fundacja Dzieci Niczyje. Warszawa. [dostęp: 22.12.2017].

Kontakty dzieci z niebezpiecznymi treściami w Internecie - raport. Gemius. (2006, 2007). Fundacja Dzieci Niczyje. [dostęp: 22.12.2017].

Korzystanie z Internetu i zagrożenia online wśród młodzieży gimnazjalnej - przegląd dostępnych wyników badań stworzony przez Fundacją Dzieci Niczyje w ramach projektu Szkoła Bezpieczna w Sieci współfinansowanego ze środków Ministerstwa Edukacji Narodowej. (2013). Fundacja Dzieci Niczyje. [dostęp: 22.12.2017].

Kirwil, L. (2011). *Polskie dzieci w Internecie. Zagrożenia i bezpieczeństwo*, Część 2, Dwuczęściowy raport z badań EU Kids Online II, przeprowadzonych wśród dzieci w wieku 9–16 lat i ich rodziców. Warszawa: SWPS – EU Kids Online - PL.

Livingstone, S, Haddon, L (2009). *EU Kids Online: Final report*. LSE, London: EU Kids Online.

Livingstone, S, Mascheroni, G, Staksrud, E. (2015). *Developing a frame- work for researching children's online risks and opportunities in Europe*, London: EU Kids Online.

Makaruk, K., Wójcik, S. (2012). *EU NET ADB – Badanie nadużywania internetu przez młodzież* w Polsce i Europie, Warszawa, Fundacja Dzieci Niczyje, http://fdn.pl/eu-net-adb.

Melosik, Z. (2014). *Kultura popularna i tożsamość młodzieży. W niewoli władzy i wolności*. Kraków: Oficyna Wydawnicza Impuls.

Podstawa programowa przedmiotu Edukacja dla bezpieczeństwa klasa VIII szkoły podstawowej. (2016). MEN. https://men.gov.pl/wp-content/uploads/2016/11/podstawa-programowa-przedmiotu-edukacja-dla-bezpieczenstwa.pdf. [dostep: 20.12.2017].

Podstawa programowa przedmiotu Edukacja dla bezpieczeństwa III etap edukacyjny: gimnazjum. (2011). https://men.gov.pl/wp-content/uploads/2011/02/8c.pdf. [dostęp. 20.12.2017]

Pyżalski, J. (red.). (2017). *Małe dzieci w świecie technologii informacyjno-komunikacyjnych. Pomiędzy utopijnymi szansami a przesadzonymi zagrożeniami*. Łódź: Wydawnicwo Eter.

Sajkowska M. (2009, 2010). *Wiktymizacja dzieci i młodzieży w Polsce. Doświadczenia* młodych *Polaków*. Fundacja Dzieci Niczyje/Gemius Polska. Dziecko w Sieci, Gemius, Fundacja Dzieci Niczyje, styczeń 2006, badani: dzieci 12–17 lat, N=1 779.

Strategia Bezpieczeństwa Narodowego RP. (2014). Biuro Bezpieczeństwa Narodowego. Warszawa.

We are social (2017). Digital in 2017 Eastern Europe. https://www.slideshare.net/wearesocialsg/digital-in-2017-eastern-europe [dostęp: 22.12.2017].

Wojtasik, Ł. (2009). *Przemoc rówieśnicza a media elektroniczne*, „Dziecko Krzywdzone. Teoria, badania, praktyka", nr 1(26). Warszawa: Fundacja Dzieci Niczyje.

Wojtasik, Ł. (2014). *Seksting wśród dzieci i młodzieży*, „Dziecko krzywdzone. Teoria, badania, praktyka". Nr 13(2).

Wójcik, S. (red.). (2013). *Korzystanie z Internetu i zagrożenia online wśród młodzieży gimnazjalnej*, Fundacja Dzieci Niczyje. Fundacja Orange. Warszawa. [dostęp: 22.12.2017].

Young, K.S. (1996). *Pathological Internet use: A case that breaks the stereotype*, "Psychological Reports", 899–902.

Young, K.S. (1998). *Internet addiction: The emergence of a new clinical disorder*, Cber Psychology and Behavior, No. 1, 237–244.

Summary: The agenda of the school subject called security education concerns following issues: general principles of state security and emergency situations, preparation for crisis, health education, excluding vital items such as cyber security and cyber threats. Internet threats regarding three main areas such as inappropriate contacts in the network, negative content, and dangerous actions undertaken by children, require repairs. First of all, it is necessary to introduce lessons concerning the threats and security in the network. Secondly, constant digitization in teaching, implementation of e-books and the Internet in learning processes, require monitoring and supervising children's activities within these resources. Thirdly, young people do not know the security rules in the network. The Internet is a source of opinion on politics, economy, culture, health etc. Knowledge about the tools of disinformation, manipulation and propaganda among children is at a satisfactory level. However, the ability to navigate among the so-called information overload is still not sufficient enough.

Key words: education, security, internet, research, youth

Katarzyna Ewa Derlatka, doktor nauk wojskowych, specjalista bezpieczeństwa narodowego, absolwentka Wydziału Dziennikarstwa i Nauk Politycznych Uniwersytetu Warszawskiego oraz Wydziału Bezpieczeństwa Narodowego Akademii Obrony Narodowej. Jest wykładowcą Uczelni Nauk Społecznych. Pracowała również w Akademii Sztuki Wojennej, była także prelegentem Rządowych Wyższych Kursów Obronnych. Ma doświadczenie w pracy dziennikarskiej, Public Relations i komunikacji w sprawach bezpieczeństwa. Jest ekspertem w zakresie bezpieczeństwa przemysłowego i biznesu. Posiada m.in. certyfikat BTEC (The British Business and Technology Education Council) Profesional Award Level 4 in Security Management oraz Audytora Wewnętrznego ISO 27001. Tematykę badawczą podjętą w rozprawie doktorskiej poświęconej Funkcji mediów w systemie zarządzania kryzysowego kontynuowała w innych opracowaniach i publikacjach, m.in. w: *Modele zagrożeń* aglomeracji miejskiej wraz z systemem *zarządzania kryzysowego na przykładzie miasta stołecznego Warszawy*, (2009), *Zarządzanie kryzysowe a media i granice państw w erze globalizacji* (2010), *Zarządzanie kryzysowe*, (2014), *Potęga informacji* (2016), *Media społecznościowe w podnoszeniu świadomości bezpieczeństwa i komunikacji w zarządzaniu kryzysowym* (2016).

Kontakt z autorką: kederlatka@gmail.com