cyfrowo bezpieczni.pl

BEZPIECZNA SZKOŁA CYFROWA

Kompetencje w zakresie bezpieczeństwa cyfrowego w polskiej szkole

Raport z badań

Badanie zostało wykonane w ramach projektu Cyfrowobezpieczni.pl – Bezpieczna Szkoła Cyfrowa, realizowanego przez Stowarzyszenie „Miasta w Internecie" ze środków pochodzących z Ministerstwa Edukacji Narodowej w ramach rządowego programu wspomagania w latach 2015-2018 organów prowadzących szkoły w zapewnieniu bezpiecznych warunków nauki, wychowania i opieki w szkołach – „Bezpieczna+"

MINISTERSTWO
EDUKACJI
NARODOWEJ

Autorzy

PhD, inż. Łukasz Tomczyk, Uniwersytet Pedagogiczny w Krakowie

Dr Łukasz Srokowski, Fundacja „Skuteczna Edukacja"

Konsultacja metodologiczna

Dr Arkadiusz Wąsiński (Uniwersytet Łódzki)

Redakcja

Krzysztof Głomb, Stowarzyszenie „Miasta w Internecie"

Tarnów, listopad 2016r.

SPIS TREŚCI

STRESZCZENIE RAPORTU 4
1. WPROWADZENIE 6
2. TEORETYCZNE KONCEPTY I WYNIKI BADAŃ 9
2.1 Zagadnienia techniczno-społeczne 9
2.1.1 Ochrona przed wirusami 9
2.1.2 Hasła, loginy, zasady bezpiecznego użytkowania sieci 10
2.1.3 Wykonywanie operacji finansowych 12
2.1.4 Ergonomia korzystania z urządzeń cyfrowych 13
2.2 Zagadnienia społeczne 14
2.2.1 Wiarygodność informacji dostępnych w Internecie 14
2.2.2 Reklamy w Internecie 15
2.2.3 Naruszenia praw autorskich 16
2.2.4 Cyberprzemoc 18
2.2.5 Kontakty z innymi użytkownikami sieci 20
2.2.6 Kreowanie wizerunku w sieci 21
2.2.7 Seksting i naruszenie prywatności 25
2.2.8 Postawy nauczycieli wobec nowych mediów 26
2.2.9 Postawy rodziców wobec nowych mediów 29
3. METODOLOGIA BADANIA 31
3.1 Dobór próby badawczej oraz konstrukcja narzędzia 31
3.2 Test kompetencyjny oraz moduł mierzący zmienne niezależne 33
3.3 Problemy badawcze 34
4. WYNIKI BADANIA POZIOMU KOMPETENCJI CYFROWYCH W ZAKRESIE BEZPIECZEŃSTWA CYFROWEGO 44
4.1 Szkoła podstawowa 1 – 3 46
4.1.1 Uczniowie 47
4.1.2 Rodzice 49
4.1.3 Nauczyciele 51
4.1.4 Wnioski i rekomendacje - szkoła podstawowa: klasy 1-3 55

4.2 Szkoła podstawowa – klasy 4-6 57
4.2.1 Uczniowie 58
4.2.2 Rodzice 60
4.2.3 Nauczyciele 64
4.2.4 Wnioski i rekomendacje - szkoła podstawowa: klasy 4-6 67
4.3 Gimnazja 68
4.3.1 Uczniowie 69
4.3.2 Rodzice 74
4.3.3 Nauczyciele 78
4.3.4 Wnioski i rekomendacje – gimnazjum 83
4.4 Szkoła ponadgimnazjalna 85
4.4.1 Uczniowie 86
4.4.2 Rodzice 92
4.4.3 Nauczyciele 96
4.4.4 Wnioski i rekomendacje – szkoła ponadgimnazjalna 101
5. WNIOSKI I REKOMENDACJE SYSTEMOWE: JAK PODNIEŚĆ POZIOM KOMPETENCJI BADANYCH GRUP W ZAKRESIE BEZPIECZEŃSTWA CYFROWEGO? 103
5.1 Zmiany w ramach podstawy programowej 103
5.2 Ukierunkowanie działania na najsłabsze obszary 105
5.3 Koncentracja na najmniejszych miejscowościach 106
5.4 Wsparcie najmłodszych nauczycieli 106
6. BIBLIOGRAFIA 108

STRESZCZENIE RAPORTU

W raporcie podjęto analizę teoretycznych aspektów kompetencji związanych z bezpieczeństwem cyfrowym w polskich szkołach i zaprezentowano pogłębioną prezentację wyników badań przeprowadzonych w ramach projektu Cyfrowobezpieczni.pl wraz z wnioskami i rekomendacjami. W badaniach tych – w drugiej połowie 2015 r. - udział wzięła reprezentatywna próba uczniów, nauczycieli i rodziców, uczestniczących w projekcie. Ich celem było określenie poziomu kompetencji tych grup w zakresie przeciwdziałania zagrożeniom, które wiążą się z uczestnictwem uczniów w cyfrowym wymiarze rzeczywistości.

Badania wykazały, że wszystkie grupy badanych wykazują niewystarczający poziom kompetencji do radzenia sobie z zagrożeniami cyfrowymi. Na skali od 0 do 100%, najniższy wynik uzyskali rodzice (55%), podobny stopień i zakres deficytów kompetencyjnych w tym zakresie ujawnił się wśród nauczycieli (57%), najwyższy poziom kompetencji prezentują uczniowie (60%). Należy podkreślić, że różnice między wynikami poszczególnych grup badanych są niewielkie, i wszystkie należy uznać – w najlepszym wypadku – za średnie.

Największe wyzwanie dla badanych stanowił obszar tematyczny prawa autorskiego (średni wynik – 36%), a także bezpieczeństwa transakcji finansowych w Internecie (53%) oraz szerzej – tematyka bezpiecznego logowania i tworzenia bezpiecznych loginów i haseł (56%). Najwyższe kompetencje wykazują badani w zakresie ochrony przeciwwirusowej (75%) oraz ergonomii korzystania z narzędzi cyfrowych przez uczniów (74%).

Grupą najbardziej zagrożoną z powodu niskich kompetencji są w świetle badań mieszkańcy wsi. Średnie wyniki w grupie rodziców z terenów wiejskich są nawet o 12 punktów procentowych niższe, niż w miastach.

Wraz ze wzrostem wieku uczniów pojawiają się także nowe zagrożenia (np. seksting lub cyberprzemoc). Oznacza to, że im starsi są uczniowie, z tym poważniejszymi egzystencjalnie zagadnieniami muszą sobie radzić.

Trend ten został odzwierciedlony w badaniu, w którym uczniowie różnych poziomów nauczania odpowiadali na pytania dotyczące najważniejszych zagrożeń dla ich grupy wiekowej. Wyniki testów wskazują niestety, że tempo wzrostu zagrożeń jest większe, niż tempo rozwoju kompetencji uczniów – im starsi byli badani, tym osiągali niższy wynik. Uczniowie klas 1-3 korzystających z sieci, dla których zagrożeniem jest głównie nadmierna podatność na reklamy, uzyskali w badaniu średni wynik 78%.

Jednak już ich trochę starsi koledzy, z klas 4-6 szkoły podstawowej, stają przed o wiele poważniejszym problemem nawiązywania kontaktów z ludźmi obcymi w sieci oraz podawania swoich danych do publicznej wiadomości, ujawniają dużo niższe kompetencje związane z zachowaniem bezpieczeństwa w tym zakresie (57%). W gimnazjum pojawiły się dodatkowo zagadnienia związane ze świadomością zagrożeń dotyczących zjawisk utożsamianych z sekstingiem i cyberprzemocą. Uczniowie z tych typów szkół wykazali niskie kompetencje - średnio 56% z nich ma świadomość zagrożeń w tym zakresie. Najniższe kompetencje wykazali uczniowie szkół ponadgimnazjalnych, którzy dodatkowo odpowiadali na pytania dotyczące np. bezpieczeństwa operacji finansowych w sieci. Świadomość bezpieczeństwa w odniesieniu do wymienionych zagadnień wykazuje średnio 53% uczniów.

W grupie badanych nauczycieli paradoksalnie najmniejszą świadomość i praktyczne przygotowanie w obszarze bezpieczeństwa cyfrowego ujawnili najmłodsi nauczyciele. Może wydawać się to zaskoczeniem, jednak wniosek ten potwierdzają także inne badania i literatura przedmiotu. Istotniejsze bowiem dla ochrony przed zagrożeniami cyfrowymi nie są kompetencje techniczne (mocniejsze u młodszych nauczycieli, często wychowanych wśród komputerów), ale kompetencje społeczne – jako, że większość najpoważniejszych zagrożeń w sieci ma charakter społeczny.

Badania wskazują na konieczność zdecydowanego rozwijania kompetencji we wszystkich badanych grupach. Poziom wiedzy i umiejętności wykazanych przez respondentów dowodzi, że projekty takie jak Cyfrowobezpieczni.pl, skierowane na uświadamianie i edukowanie nauczycieli, uczniów i rodziców są niezbędne. Skala zagrożeń, płynących ze świata cyfrowego stale zwiększa się. Uczniowie, rodzice, a nawet nauczyciele najwyraźniej nie są w stanie wystarczająco szybko samodzielnie poszerzać kompetencje w ramach indywidualnie realizowanego samokształcenia, które są konieczne do efektywnego radzenia sobie z wieloaspektowo ujmowanymi e-zagrożeniami.

1. WPROWADZENIE

Korzystanie z Internetu przez młode pokolenie stało się powszechne. Niemalże cała populacja młodzieży korzysta z sieci codziennie, w tym ponad połowa wykazuje tendencję do całodziennego bycia online. Urządzenia mobilne stały się jednym z elementarnych narzędzi pozwalających na szybką komunikację, przesyłanie pakietu informacji, pobieranie danych, tworzenie przestrzeni społecznych i rozrywkowych oraz wspomaganie uczenia się (Lange, Osiecki, 2014). Wielu badaczy zachowań w przestrzeni mediów podkreśla odmienność funkcjonowania młodego pokolenia w Internecie w porównaniu ze starszymi generacjami. Częściowe przeniesienie aktywności do mediów sieciowych nie jest już obecnie zjawiskiem nowym. Jednakże pomimo zmiany stylu życia młodych osób, jaka nastąpiła w ciągu ostatnich kilkunastu lat oraz wzrostu kompetencji instrumentalnych w zakresie obsługi nowych mediów, można zauważyć dysonans pomiędzy rozwojem poziomu wybranych składowych kompetencji cyfrowych (por. Siuda et. al., 2013) a świadomością faktycznych zagrożeń związanych z poziomem ryzyka zachowań podejmowanych w mediach cyfrowych.

Minimalizowanie szkodliwych następstw zwiększania częstotliwości i intensywności przebywania w sieci przez cyfrowych autochtonów jest jednym z istotnych obszarów badawczych współczesnej pedagogiki mediów. Rola szkoły i rodziców oraz edukacji równoległej w grupach rówieśniczych jest w tym zakresie znacząca. W szczególności ma ona znaczenie w młodszym wieku szkolnym oraz na etapie zwiększania intensywności korzystania z usług elektronicznych ingerujących w obszary wrażliwe (np. dane osobowe, wizerunek oraz szereg innych z założenia poufnych danych). Kształtowanie pożądanych nawyków bezpiecznego użytkowania ICT (technologie informacyjno-komunikacyjne) oraz kształcenie umiejętności dopasowania rozwiązań aplikacyjnych i sprzętowych w celu zapewnienia odpowiedniego poziomu bezpieczeństwa staje się jednym z kluczowych zadań w dobie społeczeństwa informacyjnego.

W trakcie analizy wyników badań realizowanych w Polsce pojawia się jednak dylemat związany z programami kształcenia oraz poziomem kompetencji bezpiecznego użytkowania mediów elektronicznych przez osoby znaczące w procesie edukacyjno-wychowawczym. Z badań przeprowadzonych w 2014 roku wynika, że polskie placówki edukacyjne nie są w pełni przygotowane informacyjnie i metodycznie do realizowania działań profilaktycznych w obszarze e-zagrożeń. Jednym z rozwiązań sprzyjających podnoszeniu poziomu bezpieczeństwa są kompleksowe strategie wychowawcze, budowane również w ramach akcji edukacyjnych, takich jak projekt Cyfrowobezpieczni.pl. Ich kluczowym celem jest kształtowanie pożądanych wychowawczo postaw i nawyków związanych z użytkowaniem mediów cyfrowych. Zasadność podejmowanych tego typu

działań jest związana również z niezadowalającym wskaźnikiem obecności zagadnień profilaktyki medialnej w procesie edukacji szkolnej. Świadczą o tym wyniki badań polskich i zagranicznych.

Czy na lekcjach informatyki lub podczas innych zajęć w szkole poznawałeś poniższe zagadnienia?

Odpowiedzi	N	%
Jak chronić swój komputer	695	59,9%
Jakie zasady (netykieta) obowiązują podczas komunikowania się poprzez internet	788	67,9%
Jak chronić swoją prywatność w sieci	783	67,4%
Jak bezpiecznie korzystać z serwisów społecznościowych	656	56,5%
Jak działają prawa autorskie w sieci	669	57,6%
Jak wykorzystać Internet w życiu codziennym	345	29,7%
Jak można wykorzystać Internet do nauki (pracy)	919	85,4%

Źródło: (Lange, Osiecki, 2014). Badacze skupieni wokół międzynarodowego projektu

EU KIDS ONLINE podkreślają, że dzieci i młodzież korzystające z nowych mediów są szczególnie zagrożeni łatwym dostępem do deprawujących treści zamieszczanych w Internecie. Chodzi o takie treści, jak: przemoc, okrucieństwo, sceny drastyczne, pornografia, rasizm, nienawiść, agresywny marketing (Kirwil, 2011). Ogólnodostępne treści są jednym z wymiarów zagrożeń elektronicznych. Wśród innych zjawisk należy wymienić również zagrożenia: zdrowia psychicznego i fizycznego (dolegliwości i zmiany fizyczne, zaburzenia psychiczne); społeczno-wychowawcze związane z zachowaniami ryzykownymi wywołanymi przez materiały pornograficzne, seksting oraz cyberprzemoc; zagrożenia związane z uzależnieniami od Internetu, gier, telefonu komórkowego. A także szereg innych cyberprzestępstw i nadużyć w sieci (Lizut, 2014).

Do wymienionych negatywnych czynników wpływu Internetu oraz nowych technologii na codzienne życie młodych osób dochodzi szereg nowych zagrożeń pojawiających się wraz z upowszechnianiem się w życiu codziennym popularnych e-usług. Analiza zagrożeń cyfrowych oraz ich uwarunkowań jest jednym z głównych wyzwań wychowawczych i edukacyjnych przypisanych nie tylko współczesnej szkole, ale i rodzinie.

W polskiej i zagranicznej literaturze przedmiotu (w obrębie pedagogiki mediów) pojawiło się szereg analiz dotyczących: dostępu i sposobu używania nowych mediów przez dzieci i młodzież oraz aktywności podejmowanych w sieci i poza siecią, które generują szereg zjawisk ryzykownego użytkowania sieciowych mediów cyfrowych. W opracowaniach z tego zakresu badacze w mniejszym stopniu koncentrują swoje poszukiwania na korzyściach wynikających z użytkowania komputerów,

tabletów, telefonów komórkowych czy też roli rodziców w socjalizacji i wychowaniu medialnym (Ólafsson, 2013), najczęściej podejmując badania w obszarach już wielokrotnie eksplorowanych i opisywanych. Dlatego też analizy badające poziom kompetencji informatyczno-medialnych, w tym dotyczących e-zagrożeń wykraczają poza dominujące narracje w dyskursie naukowym pedagogiki mediów. W wielu opracowaniach można również zauważyć szereg artykułów i raportów badawczych ukazujących relacje pomiędzy używaniem sieci a zachowaniami młodych osób oraz procesem socjalizacji lub wychowania. Jednakże ciągle słabo rozpoznane są zagadnienia dotyczące pomiaru poziomu kompetencji bezpiecznego użytkowania sieciowych mediów cyfrowych.

Niniejszy raport jest jedną z pierwszych prób w Polsce zdiagnozowania poziomu bezpieczeństwa cyfrowego grup współtworzących przestrzeń cyfrową w środowisku szkolnym oraz domowym. Stworzenie tego typu podejścia było możliwe dzięki skonstruowaniu narzędzi mierzących poziom wiedzy, umiejętności oraz diagnozujących postawy wobec poszczególnych zagrożeń cyfrowych, których znaczenie zmienia się wraz z okresem rozwojowym młodego człowieka.

Oddając w ręce czytelników niniejszy raport, autorzy mają świadomość możliwości różnorodnego rozumienia, a zatem klasyfikowania i pomiaru e-zagrożeń. Całość tematyki wymaga szeroko zakrojonych prac badawczych. Niniejsze badania są głosem w dyskusji prowadzącym do głębszego zrozumienia mechanizmów i procesów warunkujących różne zachowania ryzykowne w sieci, a także zachowania podejmowane poza siecią, które są wywołane uprzednią aktywnością w przestrzeni cyfrowej. Badania te są także jedną z propozycji metodologicznych, służących wypracowaniu ujednoliconej formuły mierzenia zakresu i skali kompetencji i umiejętności efektywnego uczestnictwa w świecie cyfrowym oraz postaw wobec tego świata, rzutujących na ramy procesu projektowania działań edukacyjnych.

2. TEORETYCZNE KONCEPTY I WYNIKI BADAŃ

2.1 ZAGADNIENIA TECHNICZNO-SPOŁECZNE

2.1.1 Ochrona przed wirusami

Szacuje się, że niespełna 90% złośliwego oprogramowania[1] trafia do komputerów użytkowników pocztą elektroniczną. Do infekcji zazwyczaj dochodzi po uruchomieniu załącznika znajdującego się w e-mailu od nieznanej osoby. Po otwarciu załącznika lub otrzymanego hiperłącza może dojść do wgrania wirusów, koni trojańskich, robaków, czy też innego oprogramowania klasyfikowanego jako tzw. *malware* (złośliwe oprogramowanie) (Bochenek, Bisialski, Różycka, Rywczyńska, Silicki, Wrońska, 2014b, s. 251). Inny rodzaj zagrożeń klasyfikowanych jako *malware* wiąże się z wejściem na strony www, które - w sytuacji braku odpowiedniego oprogramowania chroniącego komputer - automatycznie przekazują użytkownikowi złośliwe aplikacje. Największym zagrożeniem w tym zakresie są strony internetowe będące repozytoriami nielegalnego oprogramowania oraz materiałów audiowizualnych. Warezowe serwisy[2] pozwalają swym użytkownikom preparować oprogramowanie w taki sposób, aby przy jego wgraniu na komputer automatycznie instalowane były programy zaliczane do grupy *malware*.

Równie duże zagrożenie w cyberprzestrzeni stanowią serwisy społecznościowe, które służą jako niejawny nośnik do rozprzestrzeniania się wszelkiego rodzaju wirusów lub malware (Fan, Yeung, 2011). Popularność platform skupiających użytkowników na skalę globalną sprzyja podejmowaniu zachowań ryzykownych w postaci udostępniania linków do aplikacji zawierających *malware* oraz uruchamiania skryptów infekujących komputer lub urządzenie mobilne.

W ciągu ostatnich lat wzrosło również zagrożenie atakami na smartfony lub tablety. Szczególnie narażone są urządzenia posiadające system operacyjny Android. Ze zgromadzonych danych wynika, że telefony komórkowe są narażone na atak ponad 9 milionów wirusów, z czego większość z nich dedykowana jest urządzeniom z systemem operacyjnym firmy Google. Wirusy przeznaczone do ataku

[1] Oprogramowanie będące wirusami komputerowymi lub malware, mające na celu przejęcie kontroli nad sprzętem informatycznym bez świadomej zgody użytkownika.
[2] Serwisy będące repozytorium linków do oprogramowania, materiałów audiowizualnych umieszczanych w większości przypadków bez zgody właściciela praw autorskich oraz majątkowych.

na systemy operacyjne urządzeń mobilnych coraz częściej wykorzystują nie tylko luki techniczne w oprogramowaniu systemowym, lecz bazują na niewiedzy użytkowników na temat zasad ich replikacji, czy też właściwych sposobów zabezpieczenia urządzenia (Fastyn, 2016).

Ze zgromadzonych danych wynika, że od momentu, w którym rozpoczęto mierzenie w sieci liczby złośliwego oprogramowania *malware* do momentu badań realizowanych w 2014 r. zanotowano około 200 milionów różnego rodzaju tego typu oprogramowania (Fanning, 2015, s. 9). Jego celem jest: przejęcie kontroli nad zainfekowanym komputerem, spowolnienie go lub uszkodzenie, kradzież danych poufnych, wyświetlanie reklam, wykonywanie ataków na inne komputery oraz wykorzystanie mocy obliczeniowych komputerów do działań poza kontrolą właściciela. Wszystkie negatywne następstwa wgrania *malware* narażają użytkowników na straty związane z utratą danych, na techniczne uszkodzenie sprzętu, a także ewentualną utratę pełnej kontroli nad komputerem stacjonarnym lub urządzeniem mobilnym.

Istnienie tego typu oprogramowania skutkuje podejmowaniem działań edukacyjnych podwyższających świadomość, wiedzę i umiejętności związane z efektywnym zabezpieczaniem komputera lub urządzenia mobilnego typu tablet lub telefon. Rezultatem takich działań jest coraz powszechniej przejawiana wiedza właściwego zabezpieczania się przed *malware*, zgodnie z którą należy: aktualizować system operacyjny, program antywirusowy oraz inne aplikacje zainstalowane w komputerze. Nie należy natomiast instalować oprogramowania nieznanego pochodzenia, wyłączać *firewalla* systemowego, wchodzić na strony z nielegalnymi materiałami, ignorować zasad bezpiecznego użytkowania konta mailowego. Należy także zwracać szczególną uwagę na pliki pakietu MS Office lub pakietu aplikacji pobieranych ze skryptami VBA.

2.1.2 Hasła, loginy, zasady bezpiecznego użytkowania sieci

Tworzenie rozbudowanych haseł stanowi podstawę zachowań podnoszących poziom bezpieczeństwa dostępu do aplikacji komputerowych lub zasobów zawierających dane poufne. Wiedza na temat konstrukcji odpowiednich haseł oraz zasad ich używania jest szczególnie przydatna w sytuacji korzystania z bankowości internetowej, serwisów społecznościowych, czy też sklepów internetowych lub serwisów aukcyjnych. Hasło oraz nazwa użytkownika jest jedną z najpopularniejszych metod weryfikacji autentyczności użytkownika. Użytkownicy często nie doceniają roli, jaką odgrywa dobrze skonstruowane hasło. Zbyt krótkie hasło jest niebezpieczne, podobnie jak generowanie haseł bazujących na popularnych słowach kluczowych (Bochenek, Bisialski, Różycka, Rywczyńska, Silicki, Wrońska, 2014b, s.251).

Przyjmuje się, że silne hasło jest hasłem długim, a więc składa się z odpowiedniej liczby znaków (nawet przekraczających 12 znaków), zawierających również cyfry, duże i małe litery oraz znaki specjalne. Tak przygotowane hasła zwiększają skuteczność ochrony dostępu do usług i programów zawierających dane poufne. Należy jednak podkreślić, że nawet najsilniejsze hasło może zostać przejęte przez szkodliwe oprogramowanie, a także podsłuchane, czy też podpatrzone przez hakera. Dlatego też istnieje konieczność regularnego, profilaktycznego dokonywania zmian haseł we wszystkich kluczowych e-usługach (Bochenek, Bisialski, Różycka, Rywczyńska, Silicki, Wrońska, 2014b, s.251).

Pomimo olbrzymiego postępu technologicznego w minimalizacji zagrożeń cyfrowych, ludzie pozostają najsłabszym ogniwem systemu bezpieczeństwa w Internecie. Zmiana haseł determinowana jest najczęściej wiedzą techniczną na temat negatywnych następstw związanych z włamaniem do konta lub procedurami obowiązującymi w miejscu pracy. Ponadto użytkownicy nowych mediów coraz częściej potrafią zdefiniować optymalny sposób poprawnego konstruowania tzw. mocnego hasła. Jednakże w dalszym ciągu można zaobserwować szereg negatywnych nawyków rzutujących na bezpieczeństwo danych, a związanych z tzw. wygodą użytkownika - np. jedno hasło do wielu kont. (Tam, Glassman, Vandenwauver, 2010).

W instytucjach cechujących się rozbudowaną polityką bezpieczeństwa danych problematyka haseł stanowi priorytetowy cel działań, za które zwykle odpowiadają specjalnie powołane do tego osoby (Ferrillo, Singer, 2015). Duże firmy zarządzające szeregiem danych poufnych stosują systemowo algorytmy do generowania i zmiany haseł. Wiele z tych mechanizmów można stosować również indywidualnie, podczas codziennego korzystania z usług typowych dla współczesnych uczestników rzeczywistości cyfrowej.

Z danych zgromadzonych przez zespół Centrum Ryzykownych Zachowań Komunikacyjnych działający przy Uniwersytecie Palackiego (Republika Czeska) wynika, że:

- ponad 44% użytkowników ma stworzone tzw. uniwersalne hasło, które wykorzystuje do wszystkich usług i serwisów internetowych,
- niespełna 48% użytkowników stosuje hasła składające się z cyfr i liter,
- średnio hasło dostępowe do konta mailowego ma 8,71 znaków,
- jedynie 6,92% haseł można znaleźć w słowniku,
- najbardziej popularne hasła związane są z otaczającymi elementami środowiska życia oraz powiązane są z ważnymi datami oraz istotnym dla użytkownika zespołem cyfr,
- badani użytkownicy unikają stosowania tzw. haseł uniwersalnych jak (12345, 123456, słowo "password").

Stworzenie mocnego hasła jest podstawą do zachowania poufności zgromadzonych danych dostępnych w różnych, rozproszonych zasobach sieci. Należyte zabezpieczenia komputera, aplikacji oraz urządzeń mobilnych minimalizuje potencjalne straty oraz jest jednym ze wskaźników wysokiego poziomu kompetencji cyfrowych (Cipresoo et. al., 2016).

2.1.3 Wykonywanie operacji finansowych

W wielu opracowaniach dotyczących bezpieczeństwa cyfrowego podkreśla się znaczenie zagadnień związanych z szyfrowaniem danych, loginami, hasłami i aktualnymi certyfikatami danych. Oscylują one wokół techniczno-społecznych aspektów zabezpieczenia danych, które są równie istotne, co kompetencje w zakresie korzystania z e-usług. Wiedza na temat technik stosowanych przez oszustów próbujących uzyskać dane poufne jest równie ważna, co techniczna obsługa programów oraz e-usług.

Jednym z najbardziej rozbudowanych i najczęściej występujących zagrożeń jest *phising*, polegający na wyłudzaniu (bez świadomości użytkownika) danych poufnych w celu dokonania transakcji online lub podczas realizowania transferu pieniędzy. Zjawisko to związane jest z otrzymywaniem spreparowanych informacji zachęcających do odwiedzania konkretnej strony przechwytującej dane poufne poprzez podszywanie się pod zaufaną instytucję. Wśród technik związanych z atakiem phisingowym można wyróżnić działania polegające na: podmianie numeru konta docelowego przy kopiowaniu numeru bankowego, podmianie aktualnego numeru konta, modyfikacji danych na liście wykonanych operacji, żądaniu podania jednorazowych kodów przelewu, rozsyłaniu monitów związanych ze zwrotem błędnie przetransferowanych kwot, czy też prośbie o wykonanie testowego przelewu z podaniem loginu i hasła (Bochenek, Bisialski, Różycka, Rywczyńska, Silicki, Wrońska, 2014, s.239-240).

Zjawisko *phisingu* jest jednym z typowych zagrożeń elektronicznych sfery finansowej e-usług. Szacuje się, że tylko w Stanach Zjednoczonych z powodu tego rodzaju zaniedbań użytkowników odnotowano w okresie maj 2004 – maj 2005 r. straty rzędu 900 milionów dolarów. Zazwyczaj były one spowodowane atakami polegającymi na przechwyceniu kodów do kart kredytowych, wejściu przez osoby niepożądane na konta bankowe, zmianie w systemie płatności online oraz kradzieży haseł w systemie eBay (Goldsborough, 2006, s. 20).

Szacuje się, że na świecie istnieje około 150 000 stron internetowych wykonanych w celu *phisingu* (Fanning, 2015, s. 9). Najpopularniejsze formy ataku związane są z wirusami komputerowymi oraz oprogramowaniem szpiegującym (51% przypadków przyczyn włamań na konto), a także z oszustwami w sieci (np. sprzedaż nieistniejących towarów w serwisach internetowych dotyczył 11% wszystkich przypadków). Podszywanie się pod instytucję typu bank związane było z 10% przestępstw. Z kolei w

Polsce łączna wartość szkód wyrządzonych w 2011 roku związanych z kradzieżą środków finansowych oraz naprawą szkód powstałych w ten sposób wynosi ponad trzy miliardy złotych (Mosorov, Niedźwiedziński, 2014, s. 129-130).

W profilaktyce związanej z zabezpieczeniem komputerów przed włamaniem na bankowe konto internetowe główną rolę odgrywają systemy antywirusowe chroniące użytkowników przed złośliwym oprogramowaniem typu Backdoor Trojans, Keylogger Trojans, BotTrojans and worms, spyware oraz stronami internetowymi łudząco podobnymi do oryginalnych stron źródłowych (Communications News, 2006, s. 10).

Oprócz *phisingu*, szpiegującego oprogramowania oraz *pharmingu*[3] należy zwrócić uwagę na inne rodzaje zagrożeń cyfrowych dotyczących transferów pieniężnych realizowanych w trybie online. Równie niebezpieczne dla internauty, cechującego się niższym poziomem biegłości informatyczno-informacyjnej, są zakupy przez internet oraz korzystanie z serwisów aukcyjnych i ogłoszeniowych. W tej kwestii mniejsze znacznie ma techniczna ochrona komputera, zaś o wiele istotniejsze stają się umiejętności krytycznej oceny informacji, umiejętność oceny rzetelności sprzedawcy, a także typowo komunikacyjne kompetencje adekwatne do czynności podejmowanych w świecie realnym.

2.1.4 Ergonomia korzystania z urządzeń cyfrowych

Zbyt długa praca z wykorzystaniem nowych technologii, czyli nadmiarowe użytkowanie mobilnych urządzeń cyfrowych (komputera stacjonarnego, laptopa, tabletu, smartfona itp.) lub nieprawidłowe przygotowanie stanowiska komputerowego do jego użytkowania prowadzi do szeregu dolegliwości fizycznych.

Istnieje szereg praktyk prawidłowym użytkowaniem urządzeń cyfrowych, wśród których można wyróżnić: dostosowanie wielkości biurka i odległości do klawiatury i ekranu w stosunku do wzrostu użytkownika oraz zakup odpowiednio wyprofilowanego, wygodnego i obrotowego krzesła z podłokietnikami. Dobrą praktyką jest również stosowanie przerw w pracy, które umożliwiają zmianę pozycji oraz odpoczynek dla wzroku. Równie istotną kwestią jest zachowanie zasad bezpieczeństwa związanego z ustawieniem oświetlenia. Dobrą praktyką zapewniającą należyty poziom bezpieczeństwa fizycznego są regularne konsultacje z lekarzem okulistą przez osoby pracujące długotrwale z nowymi mediami lub używające intensywnie tychże urządzeń w celach rozrywkowych (Duranowski, 2014, s.66-68). Niestosowanie się do powyższych zasad grozi przemęczeniem i

[3] Mechanizm służący przekierowaniu użytkownika usługi internetowej na serwer zbierający informacje o loginach i hasłach. Bardziej zaawansowana forma phisingu.

utrwaleniem się negatywnych zachowań prowadzących w konsekwencji do deficytów w rozwoju fizycznym, a także do trwałych wad postaw i chorób.

Ergonomia jest dyscypliną, która skupia się na wpływie ludzkich potrzeb i możliwości na sposób projektowania systemów technologicznych w celu optymalizowania warunków pracy człowieka w środowisku nowych technologii. Ergonomia użytkowania nowych mediów określa standardy bezpieczeństwa pracy z użyciem technologii cyfrowych. Stosowanie się do zasad prawidłowego fizjologicznie użytkowania urządzeń cyfrowych sprzyja podniesieniu komfortu pracy oraz minimalizuje negatywne skutki zdrowotne. Ponadto upowszechnianie pośród ludzi młodych zasad ergonomii użytkowania komputerów, tabletów, telefonów sprzyja kształtowaniu prawidłowych nawyków. Zadaniem współczesnych rodziców, jak i szkoły, jest wypracowanie standardów zapewniających wysoki poziom bezpieczeństwa w zakresie ergonomii użytkowania nowych mediów (Slabbert et al., 2014).

Wiele badań (m.in. Hatfield et. al., 2016; Woo et. al., 2016) potwierdziło, że działania profilaktyczne powinny być ukierunkowane na rozbudzanie wrażliwości związanej z: odpowiednim ulokowaniem sprzętu informatycznego, przyjmowaniem należytej postawy ciała, zapewnianiem prawidłowego oświetlenia stanowiska, wietrzeniem pomieszczeń oraz wielu innych czynników minimalizujących skutki negatywnego użytkowania mediów.

Jednocześnie należy zwrócić uwagę nowe media, które mogą stanowić jedno z narzędzi promujących zachowania prozdrowotne (Hamel et. al., 2013). Działania edukacyjne w tym zakresie są zawarte w podstawie programowej i realizowane w ramach zajęć komputerowych (klasy młodsze) oraz informatyki (szkoła gimnazjalna i ponadgimnazjalna). Równolegle do szkolnych działań edukacyjnych działania wychowawcze powinni podejmować w tym zakresie rodzice. Chodzi o kształtowaniu postaw respektowania zasad ergonomii przez młodych użytkowników cyberprzestrzeni w ich naturalnym środowisku życia codziennego.

2.2 Zagadnienia społeczne

2.2.1 Wiarygodność informacji dostępnych w Internecie

Obok treści wartościowych można w sieci znaleźć informacje nierzetelne, przekłamania lub nieścisłości historyczne, błędnie prezentowane założenia oraz wyniki badań oraz teksty promujące np.: niezdrowy tryb życia, zażywanie substancji psychoaktywnych przedstawianych jako nieszkodliwe dla zdrowia, zachowania nietolerancyjne, czy treści wychwalające totalitarne ustroje polityczne.

Dlatego konieczne jest kształtowanie przez rodziców i nauczycieli u dzieci i młodzieży myślenia krytycznego, a także kompetencji związanych z zaawansowanymi technikami wyszukiwania i weryfikowania danych.

Młody człowiek powinien również posiadać utrwalone przekonanie, że kreatorem informacji w sieci może być niemalże każda osoba. Z tego powodu pożądane jest podwyższanie jego świadomości, że wiele zasobów sieci prezentuje subiektywne odczucia i informacje zaprezentowane przez ich twórców, które mogą cechować się nierzetelnością. Dodatkowo młodzi użytkownicy sieci powinni posiadać umiejętność korzystania z różnych źródeł informacji w celu weryfikowania ich wiarygodności, a także umiejętność odróżniania materiałów marketingowych (promujących jakąś ideę) od materiałów informacyjnych (prezentujących istotę danej idei) (Orange, 2015).

Z badań przeprowadzonych w Polsce oraz Republice Czeskiej wynika, że młodzież z obu krajów dość krytycznie podchodzi do informacji zawartych w Internecie. Śladowa liczba respondentów uważa, że należy mieć pełne przekonanie o prawdziwości informacji zawartych w sieci. Większość badanych Czechów i Polaków (powyżej 70%) twierdzi, iż prawdziwość informacji zależy od kontekstu. Dane te burzą stereotyp jakoby polska i czeska młodzież podchodziła bezkrytycznie do informacji zamieszczonych w Internecie (Tomczyk, Kopecky, 2015).

Wierzysz w to, co ludzie piszą o sobie w Internecie?

Odpowiedź	Polska	Czechy
TAK	6,72%	2,42%
NIE	21,43%	21,63%
Czasami TAK, czasami NIE	71,85%	75,84%

Źródło: (Tomczyk, Kopecky, 2015)

Wspomniane badania wskazują również na wysoki odsetek odpowiedzi potwierdzających pozytywną samoocenę respondentów w zakresie poziomu własnych kompetencji cyfrowych.

2.2.2 Reklamy w Internecie

Internet jest przestrzenią, w której obok ogromu treści i aplikacji cyfrowych oraz e-usług pojawia się równocześnie wiele reklam adresowanych do najmłodszych użytkowników. Kanały internetowej dystrybucji reklam są w Internecie ściśle profilowane pod konkretną grupę odbiorców. Decyzje zakupowe są „wymuszane" na często nieświadomych użytkownikach portali społecznościowych, gier sieciowych, ogólnodostępnych stron internetowych poprzez odbiór komunikatów kierowanych do grup docelowych. W Internecie działa wiele firm, których głównym celem jest tworzenie reklam

wyświetlanych razem z innymi treściami informacyjnymi i rozrywkowymi. W niektórych miejscach dedykowanych dzieciom i młodzieży można spotkać się również z reklamami przeznaczonymi dla starszych internautów. Język reklamy online jest specyficzny ze względu na manipulacyjny charakter przekazów medialnych, które utożsamiają posiadanie produktu z odczuciem wygranej, przewagi nad innymi, sukcesu (Wrzesień-Gandolfo, 2015).

Liczba i zakres badań na temat roli rodziców w procesie przygotowania dzieci do konstruktywno-krytycznego odbioru reklam internetowych są ciągle niewystarczające. Dostrzeżono wszakże, że rodzice rozpoznają techniki perswazyjne w Internecie tylko wtedy, gdy sami zostali narażeni na nie (np. poprzez ekspozycję banerów, reklam pop-up). Często jednak nie mają świadomości mechanizmów psychospołecznego oddziaływania w ramach bardziej subtelnych technik marketingowych (na przykład *advergames*). Ponadto istnieje grupa dorosłych błędnie zakładających, że dzieci będą reagować w podobny sposób na techniki perswazyjne jak ich rodzice (Cornish, 2014). Istotne pod względem siły oddziaływania są reklamy produktów i usług, publikowane niejako przy okazji innego wydarzenia (np. w czasie przerw reklamowych w trakcie gry lub materiału audiowizualnego). Uważa się, że prezentowane wówczas walory produktów lub usług skuteczniej utrwalają złe postawy i nawyki np. żywnościowe, relaksacyjno-rekreacyjne, czy komunikacyjne (Soontae, Kang, 2014). Wzorce zachowań związanych z odbiorem i interpretacją przekazów medialnych są w znaczącym stopniu powielane przez dzieci zgodnie z utrwalonymi nawykami posiadanymi przez rodziców (Kowalczyk, Royne, 2016).

Ochrona przed perswazyjnością reklam internetowych stanowi kolejne wyzwanie dla działań pedagogicznych w przestrzeni mediów sieciowych. Szczególnie istotne jest kształtowanie świadomości rodziców w zakresie bezpieczeństwa cyfrowego ich dzieci, a także kreowanie nowych rozwiązań metodycznych w ramach szkolnych programów kształcenia, których celem jest rozwijanie umiejętności krytycznej analizy komunikatów medialnych. Szkodliwy wpływ tych komunikatów na rozwój dziecka jest zjawiskiem niedocenianym przez rodziców i nauczycieli, którzy utożsamiają zagrożenia internetowe z innymi – „cięższymi gatunkowo" zachowaniami, materiałami i sytuacjami (Wrzesień-Gandolfo, 2015).

2.2.3 Naruszenia praw autorskich

Zjawisko dzielenia się plikami komputerowymi jest dobrze znane od początku rozwoju technologii informatycznych. Wzrost szybkości przesyłania danych oraz pojawienie się nowych możliwości transferu i archiwizowania danych w sieci jedynie usprawnił przekazywanie różnego rodzaju treści. Tym samym regułom wymiany i przechowywania podlegają pliki zaliczane do kategorii warezowych, a więc pochodzące z nielegalnej dystrybucji. Obecnie pobieranie plików mp3, filmów, e-booków, programów komputerowych nie jest zjawiskiem technicznie zaawansowanym. Łatwość

techniczna wymiany plików sprzyja niestety nielegalnemu gromadzeniu oprogramowania lub innego rodzaju plików chronionych prawem autorskim (Urbanowicz, 2015). Piractwo komputerowe wzmacniane jest obecnie przez ogólnodostępne i znane strony internetowe zajmujące się komercyjnym udostępnianiem miejsca do wymiany plików na własnych serwerach. Wielu użytkowników nie posiada wystarczającej świadomości prawnej odnośnie konsekwencji pobierania i udostępniania materiałów przez serwisy i usługi typu Catshare, Chomikuj.pl, czy też protokół P2P. Wynika to z braku znajomości prawa, niezapoznania się z regulaminami serwisów oraz ciągle niewystarczającej wiedzy na temat mechanizmów związanych z udostępnianiem i pobieraniem plików z sieci.

Według danych Pricewaterhouse Coopers 7,5 mln Polaków korzysta z nielegalnych serwisów internetowych oferujących treści video. Aż 29-49% ankietowanych płaci za dostęp do treści wideo w serwisach oferujących nielegalny dostęp. Całkowite roczne straty polskiej gospodarki z tytułu piractwa komputerowego wynoszą ok. 500-700 mln zł (PwC, 2014). Badania przeprowadzone przez PwC potwierdzają, że skala i uwarunkowania piractwa komputerowego przynoszą nie tylko poważne następstwa prawne dla użytkowników łamiących prawo, lecz są również zjawiskiem powszechnym oraz szkodliwym dla budżetu państwa oraz przede wszystkim dla twórców i dystrybutorów cyfrowych treści oraz aplikacji.

Zdaniem Janusza Urbanowicza, według polskiego prawa autorskiego każdy użytkownik Internetu ma możliwość korzystania z już rozpowszechnionych materiałów oraz dzielenia się nimi w ramach tzw. dozwolonego użytku. Może korzystać z tej możliwości pomimo faktu, iż są one w polskich realiach chronione prawami autorskimi i pokrewnymi. Warto jednak podkreślić, że ustalenia te nie dotyczą oprogramowania komputerowego (Urbanowicz, 2015).

Inną kategorią działań niezgodnych z prawem jest rozpowszechnianie plików utworów bez zezwolenia właściciela autorskich praw majątkowych. Rozpowszechnianie bez zezwolenia utworu objętego prawami autorskimi jest bowiem przestępstwem. Wielu użytkowników serwisów internetowych nie zdaje sobie sprawy z faktu, iż pobierając film lub inny materiał w postaci pliku z sieci (np. poprzez popularne rozwiązanie służące współdzieleniu zasobów sieciowych w momencie pobierania) udostępnia równocześnie własne pliki (np. pobrane wcześniej filmy lub pliki mp3), co jest równoznaczne z popełnieniem przestępstwa (Urbanowicz, 2015).

Stosunek do piractwa komputerowego należy zestawić z rolą osób znaczących w procesie wychowania. Wśród czynników wzmacniających lub ograniczających zachowania ryzykowne w sieci kluczowe znaczenie odgrywa postawa rodziców. (Wąsiński, Tomczyk, 2015). Rodzice będący autorytetem wychowawczym, stawiający swojemu dziecku granice związane z moralnym wymiarem zachowań ryzykownych oraz posiadający należyty zestaw kompetencji cyfrowych minimalizują negatywne następstwa związane również ze zjawiskiem piractwa. To właśnie w środowisku rodzinnym

kształtowane oraz utrwalane są postawy i nawyki związane z bezpiecznym lub ryzykownym wykorzystywaniem mediów cyfrowych. Środowisko rodzinne jest bardzo ważnym środowiskiem wzmacniającym ogólny poziom bezpieczeństwa cyfrowego oraz minimalizującym zachowania ryzykowne.

Redukowanie zjawiska piractwa komputerowego jedynie do wymiaru prawnego spłaszcza analizę tego typu zachowań ryzykownych. Istotne jest w trakcie działań wychowawczych podkreślanie moralnego wymiaru tego typu działań ryzykownych podejmowanych przez młodych e-użytkowników (Wyrostkiewicz, 2009).

2.2.4 Cyberprzemoc

Istnieje wiele zróżnicowanych podejść w definiowaniu cyberprzemocy. Jednak większość z nich traktuje to zjawisko jako zachowanie ryzykowne, podejmowane za pośrednictwem nowych mediów, mające na celu wywołanie negatywnych uczuć u podmiotu atakowanego. W wielu analizach cyberprzemoc łączona jest z tradycyjnymi mechanizmami przemocy, jednakże z uwzględnieniem komponentu mediów cyfrowych. Liczne badania w tym obszarze są prezentowane w publikacjach analizujących szczegółowo specyfikę i mechanizmy cyberprzemocy oraz różne formy profilaktyki edukacyjnej (Del Rey et. al., 2015). Zjawisko cyberprzemocy stało się w ostatnich czasach, za sprawą upowszechniania ICT, zagadnieniem poddawanym wieloaspektowym analizom.

Jacek Pyżalski podkreśla, że zjawisko cyberprzemocy nie jest oficjalnie zdefiniowane przez polski system prawny. Jednak posiada wiele wspólnego z tradycyjną agresją, między innymi za sprawą: częstotliwości zjawiska, wytworzonej relacji pomiędzy sprawcą a napastnikiem oraz związanych z tym negatywnych intencji. Wspomniane kryteria nie wyczerpują w pełni charakterystyki tego typu zachowań ryzykownych w sieci (Pyżalski, 2016). Trudno jednoznacznie określić skalę zjawiska cyberprzemocy, chociaż szacuje się, że niemalże 13% uczniów doświadczyło jej zaledwie w ciągu jednego roku, w którym realizowano badania (Pyżalski, 2012). W wielu innych badaniach, realizowanych w ostatnich latach wskazuje, że wartość tego wskaźnika jest jeszcze większa.

W sposób szczególny problem zjawisk ryzykownych w sieci dostrzegła Najwyższa Izba Kontroli podkreślając, że *trudności wychowawcze w grupie dzieci i młodzieży występują w dużym nasileniu we wszystkich typach szkół. Szczególnie w gimnazjach wielu uczniów prezentuje nieprawidłowe wzorce zachowań powstałe we wczesnym dzieciństwie i utrwalone na wcześniejszych etapach edukacji. W ostatnich latach pojawiły się nowe zjawiska patologiczne, takie jak: mobbing i bullying (rozumiane najczęściej jako tyranizowanie oraz przemoc rówieśnicza z użyciem mediów elektronicznych). Ocenia się, że przemocy w tzw. sieci doświadcza ponad połowa dzieci w Polsce* (NIK, 2014, s.6). Z podobnymi danymi można spotkać się w badaniach Jacka Pyżalskiego, który podkreśla, że zjawisko agresji elektronicznej (również

wariantów 20 rodzajów wirtualnej przemocy) jest masowe w szczególności na etapie szkoły gimnazjalnej (zob. Pyżalski, 2011; Pyżalski, 2012; Hinduja Patchin, 2011; Hinduja Patchin, 2009; Teen Online & Wireless Safety Survey 2009; Kopecky, 2010). Zjawisko agresji cyfrowej jest o tyle niebezpieczne, o ile sieć sprzyja szybkiemu i nieodwracalnemu multiplikowaniu istniejących w niej danych. Różni się ono od mechanizmu powielania informacji w świecie realnym.

Jacek Pyżalski na potrzeby charakterystyki polskiej cyberagresji wśród młodych użytkowników sieci stworzył następującą typologię zachowań wobec (Pyżalski, 2012, s.157):

- rówieśników – najczęściej osób ze środowiska szkolnego lub najbliższego otoczenia,
- pokrzywdzonych, którymi są najczęściej osoby „słabsze" od sprawcy przykładowo: alkoholicy, osoby upośledzone,
- celebrytów, a zatem osób medialnych, często prezentowanych w portalach plotkarskich, czy też piosenkarzy, sportowców, aktorów,
- danych grup – typ uprzedzeniowy, ukierunkowany nie na konkretne jednostki, lecz na grupy osób np. określonej narodowości (np. fani jakiegoś zespołu sportowego),
- nieznajomych– osoba przypadkowo wybrana, często podczas swobodnego przeglądania zasobów internetowych.

Cyberprzemoc jest zjawiskiem dostrzegalnym zazwyczaj w sytuacji pojawiających się problemów w środowisku szkolnym lub rówieśniczym. W Polsce kilku badaczy prowadzi nad nią w ostatnich latach dogłębne badania. Jednakże problematyka ta wymaga dalszej analizy, szczególnie w kontekście opracowania adekwatnych programów nauczania i profilaktycznych I i II stopnia[4].

Zjawisko cyberagresji w większości swoich odmian cechuje się podobnymi mechanizmami powstawania, lecz jego skutki są o wiele bardziej złożone, niż w przypadku agresji występującej w świecie realnym. Dlatego też konieczne staje się wypracowanie odpowiednich sposobów skutecznej edukacji dzieci i młodzieży w celu ograniczenia jej występowania. Konieczne jest ponadto wypracowanie wystandaryzowanych algorytmów reagowania nauczycieli, pedagogów i kadry zarządzającej w sytuacji wystąpienia cyberprzemocy w środowisku szkolnym (Tomczyk, 2015).

W analizach cyberprzemocy pojawił się także w ostatnich latach wątek cyberprzemocy ukierunkowanej na pedagogów, wychowawców i nauczycieli. Zjawisko to w Polsce nie jest dokładnie rozpoznane, jednakże w krajach o zbliżonych uwarunkowaniach społecznych szacuje się, że co piąty nauczyciel był ofiarą cyberataku, najczęściej ze strony uczniów (Kopecky, Szotkowski, 2017). Wątek ten wymaga dokładniejszej diagnozy w kolejnych badaniach i działaniach związanych z podnoszeniem poziomu bezpieczeństwa w przestrzeni szkolnej.

[4] Pogramy profilaktyczne obejmują działania wyprzedzające zaistnienie danego zjawiska (I stopień profilaktyki) lub są realizowane w sytuacji gdy dane zjawisko już wystąpiło (II stopień profilaktyki). Oba rodzaje działań posiadają odmienne założenia metodyczne.

2.2.5 Kontakty z innymi użytkownikami sieci

Dzieci samodzielnie korzystające z Internetu narażone są na kontakty z innymi użytkownikami sieci. Nie wszyscy z nich mają uczciwe zamiary wobec młodych internautów. Za pośrednictwem portali społecznościowych, czatów, komunikatorów, poczty elektronicznej młody internauta może paść ofiarą wyłudzeń danych osobowych, czy stać się nieświadomie źródłem informacji o bliskich osobach. Wśród zagrożeń pojawiających się w trakcie kontaktu z innymi nieznanymi użytkownikami podejmowane są próby uwodzenia i inicjowania spotkań z przypadkowymi osobami w świecie realnym. Wielu z tych działań można uniknąć poprzez stosowanie zasady ograniczonego zaufania do wszystkich osób poznanych w sieci. Pośród czynników minimalizujących potencjalne zagrożenia związane z ryzykownymi kontaktami można wyróżnić działania związane z (Orange, 2015):

- ograniczaniem dostępu do serwisów komunikacyjnych lub korzystaniem z nich przez dzieci w towarzystwie osób dorosłych,
- uświadamianiem dziecku możliwości manipulacji, do których może dojść poprzez cyfrowe źródła komunikacji,
- ustalaniem zasad zawierania nowych znajomości z ludźmi poznanymi w sieci,
- zwróceniem szczególnej uwagi na nieprzyjmowanie zaproszeń od osób nieznanych,
- ugruntowaniem zasady nieprzesyłania prywatnych informacji do osób nieznanych osobiście,
- ustaleniem kategorycznego zakazu przesyłania w sieci materiałów o charakterze intymnym,
- budowaniem relacji opartej o poszukiwanie pomocy w sytuacjach problemowych zaistniałych w sieci wśród rodziców.

W szczególności na niebezpieczne kontakty narażone są ci młodzi e-użytkownicy, którzy korzystają z portali społecznościowych oraz komunikują się z wykorzystaniem czatów i komunikatorów. Właśnie te formy komunikacji sprawiają najwięcej możliwości do nawiązywania kontaktów pomiędzy młodymi użytkownikami a nieznajomymi, których tożsamości nie można zweryfikować w prosty, łatwy i szybki sposób.

Przestrzeń internetowa sama w sobie skłania do zachowań ryzykownych w aspekcie nawiązania relacji z osobami mającymi różnego rodzaju motywacje do kontaktu z dziećmi (Wojtas, 2015). Z cytowanych wcześniej badań (Tomczyk, Kopecky, 2016) na temat diagnozy zachowań ryzykownych podejmowanych w sieci przez młodzież wyłania się zależność mówiąca o tym, iż wraz z wiekiem maleje odsetek niepełnoletnich osób informujących o spotkaniu z osobą poznaną przez sieć. 15% ankietowanych uczniów w hipotetycznej sytuacji spotkania z osobą poznaną za pomocą mediów sieciowych nie poinformowałaby o tym fakcie nikogo. Z kolei wyniki kilkuletniego badania EU KIDS ONLINE potwierdzają, że na ryzykowne kontakty związane z otrzymywaniem zdjęć intymnych od osób nieznanych narażone jest co ósme dziecko korzystające z sieci bez nadzoru rodziców (Ólafsson et. al.,2013). Pełna ochrona młodych użytkowników sieci wymaga szczególnego ich uwrażliwienia na

następstwa ryzykownych kontaktów online. Istotne jest wypracowanie mechanizmów sprzyjających samokontroli własnych zachowań w kontakcie z innymi użytkownikami, a także samoocenie w tym właśnie kontekście sytuacyjnym.

2.2.6 Kreowanie wizerunku w sieci

Nowe media umożliwiają przesyłanie zdjęć i materiałów audiowizualnych kreujących lub udostępniających wizerunek danego użytkownika. Ten typ aktywności wzmacniany jest przez usługi internetowe sprzyjające gromadzeniu danych w sposób ogólnodostępny np. w portalach społecznościowych. Wielu internautów wykorzystuje mechanizm łatwego rozprzestrzeniania się danych w sposób celowy. Można również zauważyć wzrost miejsc w sieci pozwalających na łatwe kreowanie własnego wizerunku w oparciu o strony rozrywkowe i usługi oraz aplikacje typu Snapchat, Facebook, Twitter, jak również profesjonalne strony internetowe budujące „markę" danej osoby (np. LinkedIn). Tematyka ochrony i świadomego udostępniania danych osobowych staje się zatem jednym z wyzwań dla współczesnych działań pedagogicznych realizowanych w środowisku rodzinnym, jak i szkolnym.

Ochrona własnego wizerunku w sieci wymaga przede wszystkim wyposażenia uczniów w szczególnego rodzaju kompetencje intelektualne, które są trudne do osiągnięcia w toku tradycyjnie realizowanej edukacji informatycznej w szkole. W polskiej podstawie programowej nauczania informatyki na etapie gimnazjalnym dosyć wyraźnie podkreślono znaczenie edukacji w zakresie bezpiecznego użytkowania mediów cyfrowych, wskazując, iż uczeń oprócz tradycyjnych kompetencji technicznych powinien również posiadać umiejętności związane z: klasyfikowaniem korzyści i niebezpieczeństw wynikających z rozwoju informatyki i powszechnego dostępu do informacji, wyjaśnianiem zagrożeń związanych z uzależnieniem się od komputera, wymienianiem zagadnień etycznych i prawnych z zakresu ochrony własności intelektualnej i ochrony danych, a także rozróżnianiem przejawów przestępczości komputerowej (Tomczyk, 2014).

Z wyników badań zrealizowanych w Polsce oraz Republice Czeskiej można wnioskować, że polscy i czescy internauci cechują się podobnym sposobem udostępniania danych w sieci. Zdecydowanie najczęściej prezentowane są dane związane z imieniem i nazwiskiem, adresem e-mailowym, czy też zdjęciem twarzy. Są to dane poufne wymagające podnoszenia poziomu kompetencji związanych z bezpiecznym użytkowaniem nowych mediów.

Które z poniższych danych masz udostępnione w Internecie?

Odpowiedź	Polska	Czechy
Imię i Nazwisko	87,82%	75,64%
Numer telefonu	21,43%	16,78%
Adres zamieszkania	17,65%	12,76%
Adres szkoły	33,61%	16,02%
E-mail	64,71%	58,67%
Namiar na konto w komunikatorze typu Skype	19,75%	16,06%
Hasło do e-maila lub innego konta internetowego	4,20%	2,58%
PESEL (birth certificate numer)	4,62%	2,92%
Zdjęcie twarzy	62,61%	55,19%
Żadnego z nich nie udostępniam	8,82%	10,42%

Źródło: (Tomczyk, Kopecky, 2016)

Wyniki przywołanych badań w projekcie polsko-czeskim są zbliżone do wyników badań zrealizowanych przez warszawski zespół badaczy z Uczelni Pedagogium oraz NASK (Lange, Osiecki, 2014). Ze zgromadzonych danych wynika, że około połowa użytkowników Internetu publikuje swoje zdjęcia, najczęściej w serwisach społecznościowych. Kreowanie wizerunku odbywa się na wiele sposobów. Może następować również poprzez aktywne komentowanie wpisów w portalach społecznościowych, umieszczanie linków do wydarzeń lub artykułów, oznaczanie innych osób na zdjęciach oraz „lajkowanie" postów. Można więc stwierdzić, że każdy pozostawiony po sobie ślad w sieci jest pewną formą nie w pełni uświadamianego tworzenia własnego wizerunku w sieci.

Co najczęściej publikujesz na swoim profilu w portalu społecznościowym

	Wszyscy	Gimnazja	Ponadgimnazjalne	Chłopcy	Dziewczęta
Linki do filmów/zdjęć w innych serwisach	54,1%	51,3%	56,3%	55,0%	53,8%
Linki do artykułów w innych serwisach	19,8%	17,7%	21,5%	21,0%	18,4%
Swoje zdjęcia	47,5%	42,5%	51,6%	32,8%	65,8%
Zdjęcia innych osób (znajomych)	14,5%	14,6%	14,3%	11,1%	18,8%
Zdjęcia innych osób (nieznajomych)	2,6%	3,1%	2,2%	1,8%	3,6%
Własne komentarze/historie	24,0%	27,4%	21,1%	24,0%	23,3%
Inne	16,2%	19,9%	13,3%	21,4%	9,9%

Źródło: (Lange, Osiecki, 2014)

Do grupy zachowań o wysokim stopniu ryzyka należy zaliczyć sytuacje, w których młodzi użytkownicy sieci uznają osoby poznane w trakcie kilkudniowej korespondencji w portalach internetowych za dobrych znajomych. Wówczas obdarzają ich zaufaniem. Aż 40,76% młodych internautów w Polsce przejawia gotowość do podania innym internautom numer telefonu komórkowego. Ponadto dla ponad 43% respondentów w Polsce oraz 26,76% w Czechach wysłanie własnego zdjęcia twarzy nie stanowi kwestii problematycznej (Tomczyk, Kopecky, 2016). Zdjęcie twarzy jest elementem najczęściej udostępnianym w portalach społecznościowych lub innych pokrewnych serwisach.

Które z poniższych danych udostępniłbyś swojemu koledze lub koleżance, którego/ą poznałeś przez Internet. Wyobraź sobie, że się dobrze rozumiecie

Odpowiedź	Poland	Czechy
Imię i Nazwisko	65,97%	51,96%
Numer telefonu	40,76%	26,32%
Adres zamieszkania	15,13%	9,42%
Adres szkoły	19,33%	16,98%
E-mail	41,18%	31,47%
Namiar na konto w komunikatorze typu skype	27,73%	26,36%
Hasło do e-maila lub innego konta internetowego	5,04%	1,11%
PIN do karty płatniczej	3,36%	0,89%
PESEL (birth certificate numer)	5,04%	2,05%
Zdjęcie twarzy	43,70%	26,76%
Żadnego z nich nie udostępniam	21,01%	8,12%

Źródło: (Tomczyk, Kopecky, 2016)

Innym nieco rzadziej występującym sposobem kreowania wizerunku są wyspecjalizowane strony internetowe przyjmujące postać blogów, wideoblogów, kanałów w serwisie Youtube. Dla wielu młodych internautów pozyskanie odbiorców w tym obszarze stanowi jedną z ważniejszych aktywności w sieci. Profesjonalne tworzenie blogów jest przypisane szczególnej grupie internautów wykorzystujących Internet w sposób twórczy, autokreacyjny, odbiegający od typowych form aktywności podejmowanych na co dzień przez użytkowników sieci.

Z blogów i wideoblogów regularnie korzysta w Polsce już około jedna trzecia internautów. Odsetek ten systematycznie wzrasta w każdym roku. Tego typu forma komunikacji jest w stanie kreować upodobania i gusta użytkowników i wpływać na styl życia. Blogi pozwalają być na bieżąco, śledzić trendy pojawiające się w przestrzeni wirtualnej, bądź realnej lub przenikające oba sprzężone ze sobą światy. Najczęściej ten model komunikacji jest związany z aktywnością wolnoczasową. Wielu właścicieli

blogów lub pokrewnych serwisów ujmuje tą formę komunikacji jako działanie opiniotwórcze (Hatalska, 2016, s. 7-9)

Konstruktywno-krytyczne spojrzenie na zjawisko kreowania wizerunku w sieci przyjmuje Magdalena Szpunar, która zauważa, że szansę na zaistnienie w wirtualnej przestrzeni mają osoby o narcystycznej naturze lub traktujące narzędzia cyfrowe w skrajnie instrumentalny sposób. Społeczna istotność jednostek definiowana jest przez permanentną i krzykliwą obecność w kanałach internetowych typu Twitter, Facebook i Instagram. Nieobecność online staje się deklaracją wyróżniania się - specyficzną formą wykluczającą ze społeczności (Szpunar, 2016).

Kreowanie wizerunku w portalach społecznościowych wśród młodych użytkowników wielokrotnie przebiega poza kontrolą rodziców, opiekunów, babć i dziadków dzieci. Znane jest zjawisko podwójnych kont lub ustawianie opcji publikacji informacji w postaci tekstowej lub audiowizualnej, która wyklucza z grona odbiorców rodziców oraz inne osoby z bliskiego środowiska życia. Mechanizm uczestnictwa w sieci umożliwia „podwójne życie", w szczególności osób publikujących materiały kontrowersyjne lub kreujące swój wizerunek w sposób wykraczający poza oficjalnie przyjęte normy zachowań.

Wymienione zjawiska dają podstawę do podejmowania inicjatyw edukacyjnych dotyczących rozbudowywania programów kształcenia w zakresie edukacji medialnej i informatycznej o moduł podejmujący zagadnienie bezpieczeństwa prywatności w sieci. Młodzi użytkownicy Internetu powinni mieć świadomość mechanizmów działania nowych mediów, szybkości rozprzestrzeniania się informacji, prawnych następstw użytkowania sieci w sposób niezgodny z netykietą oraz prawem. Edukacja medialna powinna być obowiązkowym składnikiem programów nauczania na wszystkich poziomach szkoły.

Działania takie znajdują wiele uzasadnień, gdyż wizerunek młodej osoby jest elementem jej tożsamości, niezwykle wrażliwym na negatywne informacje z otoczenia w szczególności w wieku adolescencji. Własne, czasami nieuświadomione działania „public relations" w portalach społecznościowych stają się dla sporej grupy młodych osób ważnym, specyficznie rozumianym, „miarodajnym" odbiciem pozycji społecznej w środowisku rówieśniczym.

Pozytywny wizerunek w sieci jest budowany przez młodych internautów przez wiele lat, z kolei jego osłabienie może odbyć się w bardzo krótkim czasie. Ochrona wizerunku w sieci wymaga przede wszystkim wykształcenia wśród najmłodszej grupy internautów odpowiedniego poziomu kompetencji w myśl zasady „raz wprowadzona do sieci informacja, zdjęcie, plik wideo pozostanie w niej na zawsze".

2.2.7 Seksting i naruszenie prywatności

Portale społecznościowe sprzyjają aktywności zorientowanej na kreowanie własnego wizerunku. W sytuacji dużej ich popularności coraz ciężej jest wytworzyć wizerunek, który byłby oryginalny i atrakcyjny. Na tym tle wielu użytkowników, zwłaszcza młode osoby, podejmuje próby kreowania wizerunku, które z punktu widzenia bezpieczeństwa oraz norm społeczno-moralnych mogą być postrzegane jako kontrowersyjne. Rozwój ICT prowadzi do tzw. usieciowienia użytkowników w jednym miejscu cyberprzestrzeni. Z jednej strony, umożliwia łatwy i szybki transfer danych, a z drugiej, sprzyja poszukiwaniu sposób na zaistnienie w perspektywie pozostałych użytkowników. Jedną ze strategii zwrócenia na siebie uwagi są zachowania utożsamiane z internetowym ekshibicjonizmem. Wiele młodych osób pragnie wejść w rolę celebrytów internetowych, udostępniając, w zasadzie bez ograniczeń, różnego rodzaju informacje na swój temat. Internauci dokonujący autokreacji poprzez umieszczanie prywatnych fotografii lub filmów nie myślą o trudnościach związanych z usunięciem informacji z sieci. Gdy autor udostępnionych materiałów audiowizualnych dochodzi do wniosku, że są ona dla niego kompromitujące, najczęściej nie ma możliwości ingerencji w to, kto je przechowuje i w jaki sposób posługuje się nimi (Andrzejewska, Bednarek, 2014).

Z danych zgromadzonych przez NASK i Pedagogium wyłania się następujący obraz zachowań ryzykownych (Lange, Osiecki, 2014):

- niespełna 8% uczniów wysłało swojemu chłopakowi lub dziewczynie własne intymne zdjęcie,
- 30% młodych osób zna wśród swoich rówieśników osoby przesyłające swoje intymne zdjęcia innym osobom poznanym w sieci,
- 4,4% wysłało swoje intymne zdjęcie innym osobom.

Seksting jest ujmowany jako jedna z form podtrzymywania kontaktu poprzez przesyłanie intymnych zdjęć. Młodym osobom zjawisko to jawi się jako dobra zabawa, czy możliwość uzyskania popularności wśród rówieśników. Jest również jednym z elementów odkrywania własnej seksualności, wzbudzenia zainteresowania płcią przeciwną oraz przeżywania pierwszych fascynacji i doświadczeń seksualnych (Andrzejewska, Bednarek, 2014). Jednakże warto podkreślić, że seksting w skrajnych przypadkach prowadzi do sytuacji, w których osoba umieszczająca zdjęcia w sieci jest narażona na atak cyberprzestępców wykorzystujących zgromadzone fotografie do uzyskania kolejnych zdjęć lub materiałów audiowizualnych o charakterze intymnym (Kopecky, 2017).

Seksualizacja przestrzeni publicznej jest zjawiskiem, którego „twarzą" są bardzo często celebryci będący zazwyczaj idolami nastoletniej młodzieży w wieku szkolnym. Potęguje to u młodych ludzi wrażenie małej szkodliwości umieszczania zdjęć o charakterze seksualnym w sieci (Curnutt, 2012).

Z badań przeprowadzonych w Polsce oraz Republice Czeskiej wynika, że młodzi użytkownicy sieci mają podobny stosunek do upubliczniania własnego wizerunku. Niemalże tyle samo osób uważa, że przesłanie fotografii internetowemu znajomemu może być niebezpieczne (ponad 70%). Wśród młodzieży można wyodrębnić grupę szczególnego ryzyka, gdyż 20% osób udostępnia własne zdjęcia mające charakter seksualny (Tomczyk, Kopecky, 2016).

Zjawisko sekstingu jest istotnie statystycznie powiązane z problemami emocjonalnymi oraz używaniem substancji psychoaktywnych. Wśród starszych grup wiekowych adolescentów seksting powiązany jest z występowaniem inicjacji seksualnej. Można zatem wyodrębnić mechanizm podwójnej zależności, gdzie jedno zachowanie ryzykowne wyzwala drugie i odwrotnie (Ševčíková, 2016).

Udostępnianie własnych intymnych fotografii jest skorelowane z różnego rodzaju zachowaniami ryzykownymi oraz impulsywnością, jednakże nie ma ustalonych współzależności ze zdrowiem psychicznym (Temple et. al., 2014). Zatem zjawisko sekstingu można ujmować jako znak ubocznych skutków rozwoju społeczeństwa informacyjnego, determinowany kulturowymi następstwami przeobrażeń, cechami związanymi z rozwojem seksualności w aspekcie patologicznym oraz społecznymi mechanizmami powielania zachowań ryzykownych.

Stosowanie sekstingu w wielu krajach wiąże się z konsekwencjami prawnymi. Jednak świadomość przekraczania norm prawnych nie prowadzi do rozwiązania problemów generowanych przez zachowania utożsamiane z sekstingiem. Co więcej, kontekst prawny sekstingu przyczynia się w wielu aspektach do niepożądanych następstw (Lampe, 2013).

2.2.8 Postawy nauczycieli wobec nowych mediów

Nowe media stanowią źródło wyzwań dla osób je użytkujących. W niniejszym opracowaniu przyjęto, że uczniowie, nauczyciele oraz rodzice powinni posiadać odpowiedni poziom kompetencji cyfrowych (informatyczno-medialnych) związanych ze sferą techniczno-instrumentalną użytkowania ICT oraz poziom wiedzy dotyczącej funkcjonowania nowych technologii (Frania, 2014a; Frania 2014b). Ważnymi komponentami wymienionych kompetencji są umiejętności krytycznego odbioru informacji zawartych w przekazach mediów (Kubiatko, 2013). Uproszczony model kompetencji informatyczno-medialnych nauczyciela zaprezentowano w schemacie 1.

Schemat 1 Kompetencje informatyczno-medialne współczesnego nauczyciela

Źródło: (Por. Peryt-Poręba, 2011, s.2)

Barbara Kędzierska stoi na stanowisku, że kształtowanie kompetencji informatyczno-medialnych jest możliwe do osiągnięcia poprzez:

- podnoszenie świadomości nauczycieli w zakresie powodów, dla których powinni uaktualniać wiedzę o nowych mediach;
- ukazanie wielostronnych możliwości związanych z użytkowaniem nowych mediów w rożnych kontekstach dydaktycznych i wychowawczych (obejmującej również tematykę zagrożeń cyfrowych);
- rozbudzanie wśród nauczycieli potrzeby rozwijanie praktycznych umiejętności wykorzystywania narzędzi cyfrowych i aplikacji w swojej pracy dydaktycznej (Kędzierska, 2005).

Z badań przeprowadzonych w ramach projektu "*Externalities of use of modern technical teaching resources and applications in learning as an important part of the undergraduate training of teachers in the Czech Republic and Poland - their differences, risk limits and threats*", realizowanego na terenie polskich i czeskich uczelni wyższych kształcących przyszłych pedagogów, wyodrębniono cztery rodzaje postaw wobec nowych mediów (Tomczyk et. al., 2015):

1. technooptymisty – postawy przejawiającej się w entuzjastycznym stosunku do mediów, pojmowanych jako źródła pozytywnie wartościowanych przeobrażeń realiów życia współczesnego człowieka. Media są w tym kontekście postrzegane jako czynnik wywołujący jednoznacznie pozytywne przemiany społeczne, mające korzystny wpływ na warunki aktywności edukacyjnej i jakość życia człowieka. Postawa ta wiąże się z przekonaniem o konieczności dążenia do twórczego wykorzystywania technologii ICT w edukacji formalnej, pozaformalnej i nieformalnej. Nauczyciele przejawiający taką postawę prezentują wysoki poziom kompetencji informatyczno-medialnych, znają aplikacje oraz strony internetowe będące nowoczesnymi i atrakcyjnymi środkami dydaktycznymi, eksperymentują z programami komputerowymi, a także nie obawiają się nieznanych im rozwiązań technologicznych. Deklarują również gotowość stałego aktualizowania i rozwijania umiejętności praktycznego posługiwania się nowymi mediami w celu ich edukacyjnego

zastosowania. Ponadto posiadają o wiele bardziej rozbudowany zakres wiedzy na temat zagrożeń elektronicznych, niż inne grupy pedagogów.

2. technorealisty – postawy charakteryzującej się pewnym dystansem do nowych technologii, który jednak nie oznacza niechęci do modyfikowania własnego stylu funkcjonowania ze względu na postęp technologiczny, lecz raczej ostrożne, roztropne otwieranie się na nowe możliwości edukacyjne. Tak rozumiana roztropność jest w opozycji do pochopnego przyjmowania wszystkiego, co nowe i jeszcze nieznane, ale też w opozycji do „automatycznego" odrzucania wszystkiego, co nowe ze względu na przywiązanie się do tradycyjnych form postępowania. Technorealista potrzebuje sprawdzenia wartości nowych propozycji medialnych, przetestowania ich w kontekście własnych kryteriów i oczekiwań, po to by je na kanwie tego doświadczenia przyjąć bądź odrzucić. Nauczyciele przejawiający taką postawę często nie potrafią ocenić poziomu własnych kompetencji informatyczno-medialnych, jeśli nie mają możliwości ich zweryfikowania w praktycznym działaniu.

3. technopesymisty – postawy związanej z jednoznacznie negatywnym stosunkiem do nowych technologii. W wariancie umiarkowanym odnosi się ona do technologii, jako zbędnych dla rozwoju człowieka zaś w wariancie radykalnym jako wręcz niekorzystnych dla jego rozwoju i funkcjonowania. Technopesymista niekoniecznie jest ignorantem w kwestii znajomości i praktycznych umiejętności korzystania z mediów, lecz negatywnie wartościuje zmiany społeczno-kulturowe determinowane przez postęp technologiczny. Może zatem prezentować niski poziom kompetencji informatyczno-medialnych - wówczas ignoruje nowe technologie w różnych sferach życia społecznego i prywatnego) lub wysoki poziom kompetencji - wówczas odczuwa potrzebę uświadamiania innych przed różnego rodzaju e-zagrożeniami.

4. technoignoranta – postawy charakteryzującej się brakiem zaangażowania w poznawanie nowych mediów, która przejawia się głównie w dystansowaniu się od najnowszych technologii informacyjno-komunikacyjnych oraz odrzucaniu możliwości ich poznawania w celu wyrobienia sobie rzetelnej opinii na ich temat. Nauczycielom takim trudno jest zrozumieć entuzjazm zwolenników nowych mediów, głównie za przyczyną ich niewiedzy o najnowszych technologiach i możliwości ich wykorzystania w procesie dydaktycznym. Brak użytkowania mediów elektronicznych w procesie edukacji budzi wobec osób zaliczanych do tej kategorii ostracyzm ze strony innych pedagogów. Technoignorant niewiele wie również o tematyce zagrożeń elektronicznych, profilaktyce oraz działaniach edukacyjnych w tym zakresie.

2.2.9 Postawy rodziców wobec nowych mediów

Projektując proces badawczy założono, iż kontrola rodziców, jako osób znaczących dla swych dzieci jest jednym z istotnych wyznaczników skali ryzyka zagrożeń cyfrowych. Założenie to wiąże się ze znaczeniem kontroli społecznej dla eliminowania zachowań nieakceptowanych w grupie oraz dla zapewnienia skuteczności promowania zachowań pożądanych wychowawczo. Wiedza rodziców o aktywności dzieci w mediach sieciowych jest jednym z podstawowych kryteriów określających stopień zagrożeń cyfrowych.

Brak kontroli rodziców nad tym, jak często oraz w jaki sposób ich dzieci korzystają z zasobów sieciowych zwiększa ryzyko nabywania przez i utrwalania te ostatnie negatywnych zachowań związanych z użytkowaniem mediów cyfrowych. Z kolei brak wiedzy rodziców o różnych formach aktywności sieciowej ich dzieci utrudnia kształtowanie wspólnego języka pozwalającego na konstruktywny dialog wychowawczy. Mentalnie oddala to obie strony od gotowości nawiązywania dialogu w zakresie codziennych zdarzeń i przeżyć. Z drugiej zaś strony - utrwala w świadomości dzieci przeświadczenie o braku negatywnych konsekwencji własnej aktywności w przestrzeni wirtualnej, a nawet wzmacnia poczucie bezkarności.

W zdecydowanej większości publikacji analizujących różne aspekty zagrożeń cyfrowych podkreślana jest kluczowa rola wychowawcza rodziców i opiekunów prawnych nieletnich podopiecznych w minimalizowaniu szkodliwego oddziaływania nowych mediów. Brak kontroli rodziców i deficyt podstawowej ich wiedzy na temat wspólnego kontaktowania się i obcowania z dziećmi w trybie online rodzi ryzyko braku odpowiedniej opieki wychowawczej. Wówczas pragnienie poszukiwania nowych doznań w cyberprzestrzeni przez dzieci może być rozwijane w kierunkach i formach stanowiących zagrożenie dla prawidłowego rozwoju osobowości. Może też prowadzić do eksperymentowania i utrwalania zachowań dewiacyjnych w przestrzeni Internetu (Wąsiński, Tomczyk, 2011).

Wraz z wiekiem dzieci maleje zainteresowanie rodziców kontrolą w obszarze mediów cyfrowych. Ponad jedna czwarta ankietowanych młodych osób podkreśla, że w przestrzeni mediów sieciowych pozbawieni są całkowitej kontroli rodziców lub opiekunów.

Czy rodzice interesują się tym jak korzystasz z komputera i Internetu?

	Wszyscy	Gimnazjalne	Ponadgimnazjalne	Chłopcy	Dziewczęta
tak, sprawdzają wszystko, co robię w Internecie	5,1%	8,1%	2,7%	4,4%	5,4%
tak, sprawdzają, ale nie wiedzą o wszystkim co robię w Internecie	14,8%	20,1%	10,3%	15,3%	14,4%
tak, starają się sprawdzać, ale tak naprawdę mogę robić, co chcę	24,5%	28,8%	20,9%	22,1%	26,6%
Nie, nie interesują się tym	55,6%	43,0%	66,1%	58,2%	53,6%

Źródło: (Lange, Osiecki, 2014)

Niemalże co piąty nastolatek uczący się w gimnazjum spotyka się z rodzicielską kontrolą zasobów sprzętowych oraz zgromadzonych danych cyfrowych. Nieco częściej ta forma profilaktyki jest realizowana w grupie chłopców. Jedynie 2% uczniów posiada zainstalowany specjalny program kontroli rodzicielskiej zasobów komputera, co może świadczyć o braku popularności tychże rozwiązań lub/i niewiedzy rodziców w tym zakresie. Co dziesiąty nastolatek jest kontrolowany przez rodziców bez jego zgody.

Poza formami kontroli perswazyjno-monitorującej aktywności sieciowej ich dzieci, rodzice mają możliwość sprawować kontrolę w formie współuczestniczenia w przestrzeni sieciowej. Działanie takie dotyczy niemalże co piątego nastolatka i cechuje się o wiele większą skutecznością w perspektywie realnej i skutecznej profilaktyki medialnej w porównaniu do aplikacji wspomagających tzw. „kontrolę rodzicielską".

W jaki sposób rodzice interesują się tym co robisz w sieci?

	Wszyscy	Gimnazjalne	Ponadgimnazjalne	Chłopcy	Dziewczęta
Rozmawiamy o tym	62,3%	58,5%	67,6%	56,1%	67,8%
Monitorują, za moją zgodą urządzenia, którymi łączę się z Internetem	13,2%	16,1%	9,1%	15,9%	11,0%
Zainstalowali filtr rodzicielski	2,3%	2,6%	1,8%	4,2%	0,7%
Są moimi znajomymi na Facebooku (lub innych portalach społecznościowych)	17,0%	16,1%	18,3%	11,3%	21,2%
Sprawdzają i kontrolują bez mojej wiedzy i zgody komputer lub inne urządzenia	10,6%	10,9%	10,0%	13,8%	8,1%
Inne	9,4%	11,6%	6,4%	13,0%	6,4%

Źródło: (Lange, Osiecki, 2014)

Styl wychowawczy przyjęty przez rodziców determinuje zachowania podejmowane przez dzieci w przestrzeni sieciowej. Styl demokratycznego wychowania minimalizuje radykalne przejawy zachowań ryzykownych, z kolei styl wychowania liberalnego lub autokratycznego zwiększają prawdopodobieństwo występowania zachowań ryzykownych wśród dzieci i młodzieży (Valcke, Bonte, Wever, Rots 2010).

Minimalizowanie prawdopodobieństwa utrwalania się zachowań ryzykownych może być efektem świadomej aktywności rodziców, którzy w relacji partnerskiej z dziećmi wspólnie odkrywają realia przestrzeni wirtualnej. Zwiększone prawdopodobieństwo zachowań ryzykownych występuje w sytuacji braku zainteresowania rodziców aktywnością ich dzieci, a także w sytuacji braku realnych kompetencji informatyczno-medialnych rodziców, ograniczającego możliwości uzyskania wsparcia przez dzieci.

3. METODOLOGIA BADANIA

3.1 DOBÓR PRÓBY BADAWCZEJ ORAZ KONSTRUKCJA NARZĘDZIA

Próba badawcza została dobrana w oparciu o dane zastane uzyskane od Stowarzyszenia „Miasta w Internecie" w podziale na uczniów, rodziców i nauczycieli. Badania zostały przeprowadzone w okresie 10 września – 20 października 2016 roku we wszystkich województwach oraz typach szkół objętych działaniami projektu „Cyfrowobezpieczni.pl".

Niniejsze badania są jednymi z największych analiz poziomu bezpieczeństwa cyfrowego w Polsce. Dzięki bardzo dużej liczbie zebranych ankiet udało się osiągnąć wysoką rzetelność badawczą. Błąd statystyczny w grupie uczniów wyniósł mniej niż 1,1%, co jest według wiedzy autorów, najlepszym wskaźnikiem osiągniętym kiedykolwiek w Polsce w ramach tego typu analiz.

Grupa	Nauczyciele	Rodzice	Uczniowie
Próba badawcza	1233	1900	10720
Błąd statystyczny	<3%	<2,5%	<1,1%

Grupy objęte badaniami zostały podzielone dodatkowo według etapu edukacyjnego (szkoła podstawowa, gimnazjum, ponadgimnazjalna). W ten sposób wyodrębnione warstwy umożliwiły stworzenie łącznie 12 narzędzi badawczych (3 grupy podmiotowe x 4 etapy edukacyjne). Działanie to miało na celu wygenerowanie narzędzi adekwatnych do cech swoistych badanej populacji z uwzględnieniem kryterium rozwojowego. Dla wyodrębnionych subpopulacji opracowano 12 narzędzi (dla każdej z grup badawczych oddzielne).

Każda z badanych osób wypełniała ankietę internetową, udostępnioną szkołom poprzez system testowania wiedzy online. W wyniku wypełnienia ankiety, której komponentem był test kompetencyjny oraz formularz zbierający informacje o zmiennych niezależnych, każdy z badanych uzyskiwał wynik na skali od 0 do 100%. Wyniki te następnie były agregowane dla poszczególnych grup badanych – osobno dla rodziców, osobno dla uczniów, osobno dla nauczycieli.

W początkowej fazie badań, w ramach każdej z trzech wyżej wymienionych grup badawczych założono maksymalny błąd statystyczny poniżej 3%, przy minimalnym 95% poziomie ufności. W ramach doboru próby badawczej z całkowitej populacji został zastosowany interwał losowania z tablic

(danych udostępnionych przez zamawiającego w formie pliku xls). Otrzymane dane pozwoliły na pogrupowanie szkół według wielkości, ze względu na liczbę uczniów objętych działaniami (małe szkoły – do 150 uczniów, średnie szkoły – 150-400 uczniów, duże szkoły – powyżej 400 uczniów). Tego typu grupowanie dało szansę na jeszcze bardziej precyzyjne wyznaczanie operatu losowania w każdej ze szkół.

Operat losowania został obliczony zgodnie z losowym doborem próby wyznaczanym m.in. przez metodykę statystyki opisowej (Nachmias, Nachmias, 2001; Rubacha, 2008; Babbie, 2009, s. 225-228). Należy podkreślić, że prowadzone do tej pory badania w podobnej tematyce np. „Dzieci Sieci" (zespół projektowy: dr Grzegorz Stunża, dr Piotr Siuda – Instytut Kultury Miejskiej) wyznaczyły nowe sposoby doboru próby badawczej polegającej na zwiększaniu badanej populacji ze względu na słaby odsetek zwrotu wypełnionych narzędzi przyporządkowanych dla techniki sondażu diagnostycznego. Tego typu rozwiązanie zostało zastosowane również w niniejszych badaniach w celu zachowania wyznaczonego przez zamawiającego poziomu ufności 95%. Zmniejszenie operatu losowania skutkowało osiągnięciem przyjętych założeń związanych z przyjętym błędem oraz poziomem ufności. Jednocześnie w sposób kontrolowany zwiększono poziom ufności do wartości 99% dla grupy uczniów.

Za wszystkie działania związane z doborem próby oraz techniczną dystrybucją narzędzi badawczych odpowiedzialny był koordynator badań, realizujący działania techniczne. Koordynator wspomagany był przez zespół badawczy, projektujący narzędzia oraz dokonujący obliczeń.

Poniżej zaprezentowano charakterystykę prób badawczych, których odpowiedzi zostały poddane analizie.

		Klasy 1-3 SP	Klasy 4-6 SP	Gimnazja	Szkoły ponadgimnazjalne
Nauczyciele	Kobieta	N= 217; 96,44%	N= 245; 77,04%	N= 336; 79,06%	N= 183; 68,03%
	Mężczyzna	N= 8; 3,56%	N= 73; 22,96%	N= 89; 20,94%	N= 86; 31,97%
Rodzice	Kobieta	N= 438; 84,07%	N= 394; 83,65%	N= 509; 78,67%	N= 201; 72,04%
	Mężczyzna	N= 83; 15,93%	N= 77; 16,35%	N= 138; 21,33%	N= 78; 27,96%
Uczniowie	Kobieta	N = 2159 (bez podziału na płeć)	N= 1540; 49,84%	N= 1844; 50,56%	N=908; 49,13%
	Mężczyzna		N= 1550; 50,16%	N= 1803; 49,44%	N= 940; 50,87%

3.2 TEST KOMPETENCYJNY ORAZ MODUŁ MIERZĄCY ZMIENNE NIEZALEŻNE

Ze względu pionierski charakter badań oraz główny cel badania: diagnozę poziomu wiedzy oraz postaw osób badanych w początkowej, przedszkoleniowej fazie realizacji projektu Cyfrowobezpieczni.pl, przyjęto hipotezę badawczą, zgodnie z którą: wszystkie 12 wyodrębnionych prób badawczych cechuje się zmiennym poziomem kompetencji cyfrowych warunkowanych szeregiem zmiennych niezależnych (środowiskowych i indywidualnych). W celu zweryfikowania hipotezy skonstruowano narzędzie obejmujące zarówno część testową, jak też itemy charakteryzujące szczegółowo cechy badanej populacji.

Głównym elementem każdego z kwestionariuszy badawczych był test kompetencyjny sprawdzający poziom wiedzy oraz umiejętności. Test kompetencyjny uzupełniało narzędzie ilościowe mierzące postawy badanych wobec: ICT, procesu wychowania oraz tematyki pokrewnej. Poprzez udzielanie odpowiedzi na kolejne pytania badani zdobywali punkty, przeliczane następnie na wynik końcowy. W ramach każdego z badanych obszarów uczestnicy mogli uzyskać wyniki 0 do 100%. Wynik ten wskazywał na poziom kompetencji w danym obszarze.

Za każde pytanie dotyczące wiedzy oraz umiejętności można było uzyskać maksymalnie 3 punkty (9 punktów na każdy obszar). Z kolei brak dobrej odpowiedzi w pytaniu jednokrotnego wyboru skutkował przyznaniem zera punktów. W sytuacji pytań wielokrotnego wyboru wskazanie złej odpowiedzi skutkowało przyznaniem1 punktu, natomiast poprawne odpowiedzi sumowane były do 3 punktów w każdym z pytań.

Wszystkie analizowane obszary wyznaczone były przez trzy pytania, dające perspektywę uzyskania 100% dla każdego z obszarów. Zastosowanie takiej strategii badawczej związane było z zachowaniem optymalnego doboru liczby pytań do całkowitej długości narzędzia badawczego. Dodatkowo w ramach obliczeń dokonano uśrednienia wyników ze wszystkich obszarów. Działanie to dało możliwość zaprezentowania średniej wartości poziomu kompetencji cyfrowych w zakresie profilaktyki zagrożeń elektronicznych.

Każdy z ankietowanych otrzymał na koniec badania informację zwrotną o treści „w badaniu uzyskałeś wynik x %", gdzie x oznaczał ostateczną wartość procentową. Wynik ten był podstawą wszystkich dalszych obliczeń dokonywanych w ramach badania i stanowił jednocześnie punkt wyjściowy dla formułowania obszarów wymagających wsparcia. Ponadto ze względu na edukacyjny charakter niniejszych badań autorzy założyli, iż pojawienie się wyniku końcowego będzie służyło motywacyjnie w obszarze samokształcenia uczestników badania.

Itemy dotyczące postaw oraz charakteryzujące próbę służyły w badaniu jako zmienne niezależne. Narzędzie poprzedzone zostało listem wprowadzającym, w ramach którego został zaprezentowany cel badań, przebieg, informacje o anonimowości. Narzędzie składało się z 18 pytań mierzących poziom kompetencji cyfrowych w zakresie zagrożeń elektronicznych:

- 4 pytania mierzące sposoby wykorzystania nowych mediów oraz procesy wychowawcze dotyczące nowych mediów, 3 pytania oceniające poziom własnych kompetencji cyfrowych, 7 pytań charakteryzujących próbę badawczą (ankietowane osoby) – narzędzie adresowane do pedagogów,
- 2 pytania na temat zasad wychowania do nowych mediów w środowisku rodzinnym, 3 pytania oceniające poziom kompetencji cyfrowych respondentów, 7 pytań charakteryzujących próbę badawczą (ankietowane osoby) – narzędzie adresowane do rodziców,
- 2 pytania dotyczące systemu wychowania do nowych mediów w środowisku rodzinnym, 3 pytania związane z oceną kompetencji cyfrowych rodziców oraz samooceną w tym samym zakresie, 7 pytań charakteryzujących próbę badawczą (ankietowane osoby) – narzędzie adresowane do uczniów.

Narzędzie badawcze zostało skonstruowane w oparciu o analizę aktualnej literatury w zakresie pedagogiki mediów oraz wskazania podmiotu zamawiającego działania badawcze (Stowarzyszenia „Miasta w Internecie"). Wszystkie 12 narzędzi zostało poddanych badaniom pilotażowym (ponad 5% badanej populacji). Na podstawie zebranych uwag dokonano modyfikacji w aspekcie leksykalnym. Ponadto wszystkie narzędzia zostały poddane konsultacjom, w których uczestniczyli przedstawiciele strony zamawiającej oraz dwóch niezależnych ekspertów reprezentujących Uniwersytet Pedagogiczny w Krakowie (Wydział Pedagogiczny) oraz Uniwersytet Łódzki (Wydział Nauk o Wychowaniu).

3.3 PROBLEMY BADAWCZE

Pytania badawcze wynikają z głównych obszarów tematycznych przyporządkowanych do poszczególnych grup docelowych, objętych projektem „Cyfrowobezpieczni.pl". Zakres obszarów szkoleniowych, a zatem i obszarów badawczych, pozwolił na wyodrębnienie 12 grup.

Dla każdej z grup przyporządkowano odrębny zestaw testów warunkowany zadaniami rozwojowymi, etapem edukacji, pełnionymi rolami oraz związanymi z tym wymaganiami warunkującymi posiadanie należytej, wiedzy, umiejętności i postaw. Dla każdego z problemów badawczych zaprojektowano adekwatny zestaw pytań szczegółowych, testujących poziom wiedzy, umiejętności oraz diagnozujących postawy dotyczące zagrożeń elektronicznych. Wszystkie uzyskane odpowiedzi

stanowiły jednocześnie składowe kompetencji cyfrowych. W celu uściślenia zakresu objętego pomiarem dla każdego problemu badawczego przyporządkowano zestaw wskaźników.

Postawy zostały poddane klasyfikacji tabelarycznej bez punktowej oceny oraz odnoszenia tym samym do całkowitego wyniku końcowego.

	Klasy 1-3 SP	Klasy 4-6 SP	Gimnazja	Szkoły ponadgimnazjalne
Nauczyciele	Grupa 1	Grupa 2	Grupa 3	Grupa 4
Uczniowie	Grupa 5	Grupa 6	Grupa 7	Grupa 8
Rodzice	Grupa 9	Grupa 10	Grupa 11	Grupa 12

Grupa 1 – nauczyciele w klasach 1-3 SP

1) Jaki jest poziom wiedzy i umiejętności nauczycieli, potrzebnych do przeciwdziałania zagrożeniom związanym z:
   a. **ergonomią korzystania z urządzeń cyfrowych** (wyznaczniki: W – wiedza na temat maksymalnego bezpiecznego czasu spędzanego przed ekranem, W – wiedza na temat negatywnych konsekwencji zbyt długiego korzystania z narzędzi cyfrowych, W – wiedza na temat konsekwencji umiejscowienia komputera w pokoju dziecka, K – umiejętność realistycznej oceny różnorodnych treści dostępnych w sieci),
   b. **wiarygodnością informacji dostępnych w Internecie** (wyznaczniki: W – wiedza na temat mechanizmów weryfikacji informacji w Wikipedii, K – umiejętność wykrycia plagiatu w pracy ucznia, K – umiejętność oceny wiarygodności serwisów internetowych),
   c. **reklamami w Internecie** (wyznaczniki: W – wiedza na temat konsekwencji kliknięcia przez ucznia w reklamę, W – znajomość portali wolnych od reklam, W – wiedza na temat związków między korzystaniem w nowych mediów, a nawykami żywieniowymi dziecka),
   d. **kontaktami z innymi użytkownikami sieci** (wyznaczniki: W – znajomość portali i narzędzi umożliwiających kontakt uczniów z nieznajomymi w sieci, K – umiejętność skonstruowania właściwego przekazu dla ucznia, związanego z badaną kompetencją),
   e. **hasłami, loginami i nieprzestrzeganiem zasad bezpiecznego logowania** (wyznaczniki: K – umiejętność wybrania optymalnego hasła do ważnego serwisu, W – wiedza na temat zasad bezpieczeństwa w sieci),
   f. **ochrony przed wirusami** (wyznaczniki: K – umiejętność wyboru właściwego sposobu zabezpieczania komputera przed wirusami, W – podstawowa wiedza na temat mechanizmów działania wirusów komputerowych, W – realistyczna ocena możliwości spowodowania uszkodzenia komputera poprzez ściągnięcie wirusów przez uczniów w wieku 1-3)

2) Jakie są dominujące postawy nauczycieli w odniesieniu do wykorzystywania Internetu i narzędzi cyfrowych przez uczniów?

Grupa 2 – nauczyciele w klasach 4-6 szkół podstawowych

1) Jaki jest poziom wiedzy i umiejętności nauczycieli, potrzebnych do przeciwdziałania zagrożeniom związanym z:
   a. **ergonomią korzystania z urządzeń cyfrowych** (wyznaczniki: W – wiedza na temat maksymalnego bezpiecznego czasu spędzanego przed ekranem, W – wiedza na temat negatywnych konsekwencji zbyt długiego korzystania z narzędzi cyfrowych, W – wiedza na temat konsekwencji umiejscowienia komputera w pokoju dziecka, K – umiejętność realistycznej oceny różnorodnych treści dostępnych w sieci),
   b. **bezpieczeństwem własnego wizerunku** (wyznaczniki: W – wiedza na temat portali, stron i narzędzi umożliwiających publikowanie treści w sieci oraz mechanizmów rozprzestrzeniania się tych informacji, K – realistyczna ocena konsekwencji działań podejmowanych w sieci przez uczniów klas 4-6),
   c. **wiarygodnością informacji dostępnych w Internecie** (wyznaczniki: W – wiedza na temat mechanizmów weryfikacji informacji w Wikipedii, K – umiejętność wykrycia plagiatu w pracy ucznia, K – umiejętność oceny wiarygodności serwisów internetowych),
   d. **naruszeniami praw autorskich** (wyznaczniki: K – umiejętność właściwego zdefiniowania sytuacji prawnej w przypadku pobrania pliku z popularnego serwisu sieciowego (K – umiejętność właściwej oceny prawnej sytuacji, w której uczeń dokonuje plagiatu, K – umiejętność odróżnienia użytku dozwolonego od czynu zabronionego w zakresie prawa autorskiego),
   e. **kontaktami z innymi użytkownikami sieci** (wyznaczniki: W – znajomość portali i narzędzi umożliwiających kontakt uczniów z nieznajomymi w sieci, K – umiejętność skonstruowania właściwego przekazu dla ucznia, związanego z badaną kompetencją),
   f. **hasłami, loginami i nieprzestrzeganiem zasad bezpiecznego logowania** (wyznaczniki: K – umiejętność wybrania optymalnego hasła do ważnego serwisu, W – wiedza na temat zasad bezpieczeństwa w sieci)?
2) Jakie są dominujące postawy nauczycieli w odniesieniu do wykorzystywania Internetu i narzędzi cyfrowych przez uczniów?

Grupa 3 – nauczyciele w gimnazjach

1) Jaki jest poziom wiedzy i umiejętności nauczycieli, potrzebnych do przeciwdziałania zagrożeniom związanym z:
   a. **kontaktami z innymi użytkownikami sieci** (wyznaczniki: W – znajomość popularnych aplikacji używanych przez młodzież, K – umiejętność ustalania zasad prywatności, W – wiedza na

temat kreowania własnego wizerunku poprzez konta w serwisach społecznościowych niedostępne dla rodziców)

b. **sekstingiem i naruszeniami prywatności** (W – wiedza na temat popularnych aplikacji oraz sekstingu, W – wiedza na temat zjawiska aplikacji seksting, W- wiedza na temat zjawiska powielania informacji)
c. **naruszeniami praw autorskich** (W – wiedza na temat prawa ochrony własności intelektualnej, W - wiedza na temat prawnych następstw związanych z pobieraniem filmów z nielegalnych źródeł, P – postawy wobec piractwa komputerowego, K - kompetencje oceny legalności źródła oprogramowania)
d. **wiarygodnością informacji dostępnych w Internecie** (W – wiedza na temat mechanizmów konstruowania najpopularniejszej encyklopedii internetowej, K – umiejętność sprawdzenia źródła informacji, W - wiedza na temat wiarygodności informacji otrzymanej drogą e-mailową)
e. **cyberprzemocą** (W - wiedza na temat mechanizmów związanych z cyberprzemocą, P - postawy wobec cyberprzemocy, W - wiedza na temat mechanizmów związanych z cyberprzemocą, K – umiejętność zabezpieczania materiałów dotyczących cyberprzemocy),
f. **wykonywaniem operacji finansowych w sieci** (W – wiedza na temat rodzajów oprogramowania, W – wiedza na temat połączeń szyfrowanych, W – wiedza na temat możliwości zabezpieczenia nowych mediów przed zagrożeniami związanymi z płatnościami elektronicznymi)

2) Jakie są dominujące postawy nauczycieli w odniesieniu do wykorzystywania Internetu i narzędzi cyfrowych przez uczniów?

Grupa 4 – nauczyciele w szkołach ponadgimnazjalnych

1) Jaki jest poziom wiedzy i umiejętności nauczycieli, potrzebnych do przeciwdziałania zagrożeniom związanym z:
   a. **nieświadomym kreowaniem swojego wizerunku w Internecie** (W - wiedza na temat prawnych następstw związanych z wykorzystywaniem wizerunku, W - znajomość popularnych portali społecznościowych używanych przez młodzież, W – wiedza na temat kreowania własnego wizerunku poprzez konta w serwisach społecznościowych niedostępne dla rodziców),
   b. **sekstingiem i naruszeniami prywatności** (W - wiedza na temat popularnych aplikacji oraz sekstingu, W - wiedza na temat sekstingu, W - wiedza na temat zjawiska selfie),
   c. **naruszeniami praw autorskich** (W - wiedza na temat terminologii związanej z nielegalnym oprogramowaniem, W - wiedza na temat prawnych następstw związanych z pobieraniem filmów z nielegalnych źródeł, P – postawy wobec piractwa komputerowego, K - kompetencje oceny legalności źródła oprogramowania),

   d. **wiarygodnością informacji dostępnych w Internecie** (W - wiedza na temat mechanizmów konstruowania najpopularniejszej encyklopedii internetowej, K - umiejętność sprawdzenia źródła informacji, K – umiejętność sprawdzenia wiarygodności sprzedawcy w sklepie internetowym).
   e. **cyberprzemocą** (W – wiedza na temat mechanizmów związanych z cyberprzemocą, K – umiejętność zabezpieczania materiałów dotyczących cyberprzemocy),
   f. **wykonywaniem operacji finansowych w sieci** (W – wiedza na temat przestępstw internetowych związanych z bankowością internetową, K – umiejętność sprawdzenia połączenia szyfrowanego, W – wiedza na temat możliwości zabezpieczenia nowych mediów przed zagrożeniami związanymi z płatnościami elektronicznymi)
2) Jakie są dominujące postawy nauczycieli w odniesieniu do wykorzystywania Internetu i narzędzi cyfrowych przez uczniów?

Grupa 5 – uczniowie w klasach 1-3 szkół podstawowych

1) Jaki jest poziom wiedzy i umiejętności uczniów, potrzebnych do przeciwdziałania zagrożeniom związanym z:
   a. **ergonomią korzystania z urządzeń cyfrowych** (wyznacznik: K – umiejętność określenia właściwej postawy przed komputerem).
   b. **wiarygodnością informacji dostępnych w Internecie** (wyznacznik: K – umiejętność wyboru właściwego drugiego źródła, służącego do weryfikacji informacji znalezionych w Internecie),
   c. **kontaktami z innymi użytkownikami sieci** (wyznacznik: K – umiejętność podjęcia właściwej decyzji w sytuacji potencjalnie niebezpiecznego kontaktu z nieznajomym w Internecie),
   d. **hasłami, loginami i nieprzestrzeganiem zasad bezpiecznego logowania** (wyznacznik: K - umiejętność wyboru właściwego hasła do portalu z grami sieciowymi)
2) Jakie są dominujące postawy uczniów w odniesieniu do wykorzystywania przez nich Internetu i narzędzi cyfrowych?

Grupa 6 – uczniowie w klasach 4-6 szkół podstawowych

1) Jaki jest poziom wiedzy i umiejętności uczniów, potrzebnych do przeciwdziałania zagrożeniom związanym z:
   a. **ergonomią korzystania z urządzeń cyfrowych** (wyznaczniki: W – wiedza na temat maksymalnego bezpiecznego czasu spędzanego przed ekranem, W – wiedza na temat negatywnych konsekwencji zbyt długiego korzystania z narzędzi cyfrowych, W – wiedza na temat konsekwencji umiejscowienia komputera w pokoju dziecka, K – umiejętność realistycznej oceny różnorodnych treści dostępnych w sieci)
   b. **bezpieczeństwem własnego wizerunku** (wyznaczniki: W – wiedza na temat portali, stron i narzędzi umożliwiających publikowanie treści w sieci oraz mechanizmów

rozprzestrzeniania się tych informacji, K – realistyczna ocena konsekwencji działań podejmowanych w sieci przez uczniów klas 4-6),

c. **wiarygodnością informacji dostępnych w Internecie** (wyznaczniki: W – wiedza na temat mechanizmów weryfikacji informacji w Wikipedii, K – umiejętność wykrycia plagiatu w pracy ucznia, K – umiejętność oceny wiarygodności serwisów internetowych),
d. **naruszeniami praw autorskich** (wyznaczniki: K – umiejętność właściwego zdefiniowania sytuacji prawnej w przypadku pobrania pliku z popularnego serwisu sieciowego, K – umiejętność właściwej oceny prawnej sytuacji, w której uczeń dokonuje plagiatu, K – umiejętność odróżnienia użytku dozwolonego od czynu zabronionego w zakresie prawa autorskiego),
e. **kontaktami z innymi użytkownikami sieci** (wyznaczniki: W – znajomość portali i narzędzi umożliwiających kontakt uczniów z nieznajomymi w sieci, K – umiejętność skonstruowania właściwego przekazu dla ucznia, związanego z badaną kompetencją),
f. **hasłami, loginami i nieprzestrzeganiem zasad bezpiecznego logowania** (wyznaczniki – K – umiejętność wybrania optymalnego hasła do ważnego serwisu, W – wiedza na temat zasad bezpieczeństwa w sieci)

2) Jakie są dominujące postawy uczniów w odniesieniu do wykorzystywania przez nich Internetu i narzędzi cyfrowych?

Grupa 7 – uczniowie w gimnazjach

1) Jaki jest poziom wiedzy i umiejętności nauczycieli, potrzebnych do przeciwdziałania zagrożeniom związanym z:
   a. **kontaktami z innymi użytkownikami sieci** (W - wiedza na temat możliwości umieszczania zdjęć w serwisach internetowych, W- wiedza na temat serwisów geolokalizacyjnych, W - wiedza na temat budowania relacji z innymi użytkownikami w portalach internetowych),
   b. **sekstingiem i naruszeniami prywatności** (W - wiedza na temat technicznych możliwości powielania danych w sieci, W - wiedza na temat zjawiska sekstingu, K - umiejętność reagowania w sytuacjach próby wymuszenia danych poufnych),
   c. **naruszeniami praw autorskich** (W – wiedza na temat terminologii związanej z nielegalnym oprogramowaniem, W - wiedza na temat prawnych następstw związanych z pobieraniem filmów z nielegalnych źródeł, P – postawy wobec piractwa komputerowego, K – kompetencje oceny legalności źródła oprogramowania),
   d. **wiarygodnością informacji dostępnych w Internecie** (W – wiedza na temat mechanizmów konstruowania najpopularniejszej encyklopedii internetowej, W – wiedza na temat korzystania z portalu internetowego, K - umiejętność rozróżniania informacji prawdziwych od fałszywych w serwisach informacyjnych),

e. **cyberprzemocą** (W - wiedza na temat mechanizmów związanych z cyberprzemocą, W - wiedza na temat rodzajów cyberprzemocy oraz konsekwencji, W - wiedza na temat technicznych i społecznych aspektów warunkujących cyberprzemoc),
f. **wykonywaniem operacji finansowych w sieci** (W - wiedza na temat poziomu bezpieczeństwa poszczególnych e-usług, K - umiejętność zachowania bezpieczeństwa w sytuacji phisingu, W - wiedza na temat połączeń szyfrowanych)

2) Jakie są dominujące postawy uczniów w odniesieniu do wykorzystywania przez nich Internetu i narzędzi cyfrowych?

Grupa 8 – uczniowie w szkołach ponadgimnazjalnych

1) Jaki jest poziom wiedzy i umiejętności uczniów, potrzebnych do przeciwdziałania zagrożeniom związanym z:
   a. **nieświadomym kreowaniem swojego wizerunku w Internecie** (W - wiedza na temat archiwizacji materiałów audiowizualnych przez Google, W - wiedza na temat targetowania reklam, W – wiedza na temat kreowania własnego wizerunku poprzez konta w serwisach społecznościowych za sprawą komentarzy innych osób)
   b. **sekstingiem i naruszeniami prywatności** (W - wiedza na temat prawnych następstw kradzieży tożsamości, W - wiedza na temat zjawiska naruszenia wizerunku oraz technicznych aspektów ochrony danych, K - umiejętność usuwania zdjęć indeksowanych przez najpopularniejszą w Polsce wyszukiwarkę internetową),
   c. **naruszeniami praw autorskich** (W – wiedza na temat terminologii związanej z nielegalnym oprogramowaniem, W - wiedza na temat prawnych następstw związanych z pobieraniem filmów z nielegalnych źródeł, P – postawy wobec piractwa komputerowego, K - kompetencje oceny legalności źródła oprogramowania),
   d. **wiarygodnością informacji dostępnych w Internecie** (W - wiedza na temat mechanizmów konstruowania najpopularniejszej encyklopedii internetowej, K - umiejętność wartościowania źródła informacji, K - umiejętność sprawdzenia wiarygodności sprzedawcy w sklepie internetowym),
   e. **cyberprzemocą** (W - wiedza na temat mechanizmów związanych z cyberprzemocą, W - wiedza na temat rodzajów cyberprzemocy, K – umiejętność zabezpieczania materiałów dotyczących cyberprzemocy),
   f. **wykonywaniem operacji finansowych w sieci** (W - wiedza na temat sposobów zabezpieczania komputera, K - umiejętność tworzenia silnych haseł, W – wiedza na temat bezpieczeństwa sieci)?
2) Jakie są dominujące postawy uczniów w odniesieniu do wykorzystywania przez nich Internetu i narzędzi cyfrowych?

Grupa 9 – rodzice w klasach 1-3 szkół podstawowych

1) Jaki jest poziom wiedzy i umiejętności rodziców, potrzebnych do przeciwdziałania zagrożeniom związanym z:
    a. **ergonomią korzystania z urządzeń cyfrowych** (wyznaczniki: W – wiedza na temat maksymalnego bezpiecznego czasu spędzanego przed ekranem, W – wiedza na temat negatywnych konsekwencji zbyt długiego korzystania z narzędzi cyfrowych, W – wiedza na temat konsekwencji umiejscowienia komputera w pokoju dziecka, K – umiejętność realistycznej oceny różnorodnych treści dostępnych w sieci),
    b. **wiarygodnością informacji dostępnych w Internecie** (wyznaczniki: W – wiedza na temat mechanizmów weryfikacji informacji w Wikipedii, K – umiejętność wykrycia plagiatu w pracy ucznia, K – umiejętność oceny wiarygodności serwisów internetowych),
    c. **reklamami w Internecie** (wyznaczniki: W – wiedza na temat konsekwencji kliknięcia przez ucznia w reklamę, W – znajomość portali wolnych od reklam, W – wiedza na temat związków między korzystaniem w nowych mediów, a nawykami żywieniowymi dziecka),
    d. **kontaktami z innymi użytkownikami sieci** (wyznaczniki: W – znajomość portali i narzędzi umożliwiających kontakt uczniów z nieznajomymi w sieci, K – umiejętność skonstruowania właściwego przekazu dla ucznia, związanego z badaną kompetencją),
    e. **hasłami, loginami i nieprzestrzeganiem zasad bezpiecznego logowania** (wyznaczniki: K – umiejętność wybrania optymalnego hasła do ważnego serwisu, W – wiedza na temat zasad bezpieczeństwa w sieci),
    f. **ochrony przed wirusami** (wyznaczniki: K – umiejętność wyboru właściwego sposobu zabezpieczania komputera przed wirusami, W – podstawowa wiedza na temat mechanizmów działania wirusów komputerowych, W – realistyczna ocena możliwości spowodowania uszkodzenia komputera poprzez ściągnięcie wirusów przez uczniów w wieku 1-3)
2) Jakie są dominujące postawy rodziców w odniesieniu do wykorzystywania Internetu i narzędzi cyfrowych przez ich dzieci?

Grupa 10 – rodzice w klasach 4-6 szkół podstawowych

1) Jaki jest poziom wiedzy i umiejętności rodziców, potrzebnych do przeciwdziałania zagrożeniom związanym z:
    a. **ergonomią korzystania z urządzeń cyfrowych** (wyznaczniki: W – wiedza na temat maksymalnego bezpiecznego czasu spędzanego przed ekranem, W – wiedza na temat negatywnych konsekwencji zbyt długiego korzystania z narzędzi cyfrowych, W – wiedza na temat konsekwencji umiejscowienia komputera w pokoju dziecka, K – umiejętność realistycznej oceny różnorodnych treści dostępnych w sieci),

b. **bezpieczeństwem własnego wizerunku** (wyznaczniki: W – wiedza na temat portali, stron i narzędzi umożliwiających publikowanie treści w sieci oraz mechanizmów rozprzestrzeniania się tych informacji, K – realistyczna ocena konsekwencji działań podejmowanych w sieci przez uczniów klas 4-6),
c. **wiarygodnością informacji dostępnych w Internecie** (wyznaczniki: W – wiedza na temat mechanizmów weryfikacji informacji w Wikipedii, K – umiejętność wykrycia plagiatu w pracy ucznia, K – umiejętność oceny wiarygodności serwisów internetowych),
d. **naruszeniami praw autorskich** (wyznaczniki: K – umiejętność właściwego zdefiniowania sytuacji prawnej w przypadku pobrania pliku z popularnego serwisu sieciowego, K – umiejętność właściwej oceny prawnej sytuacji, w której uczeń dokonuje plagiatu, K – umiejętność odróżnienia użytku dozwolonego od czynu zabronionego w zakresie prawa autorskiego),
e. **kontaktami z innymi użytkownikami sieci** (wyznaczniki: W – znajomość portali i narzędzi umożliwiających kontakt uczniów z nieznajomymi w sieci, K – umiejętność skonstruowania właściwego przekazu dla ucznia, związanego z badaną kompetencją),
f. **hasłami, loginami i nieprzestrzeganiem zasad bezpiecznego logowania** (wyznaczniki: K – umiejętność wybrania optymalnego hasła do ważnego serwisu, W – wiedza na temat zasad bezpieczeństwa w sieci)

2) Jakie są dominujące postawy rodziców w odniesieniu do wykorzystywania Internetu i narzędzi cyfrowych przez ich dzieci?

Grupa 11 – rodzice w gimnazjach

1) Jaki jest poziom wiedzy i umiejętności rodziców, potrzebnych do przeciwdziałania zagrożeniom związanym z:
   a. **kontaktami z innymi użytkownikami sieci** (W - wiedza na temat możliwości umieszczania zdjęć w serwisach internetowych, K - umiejętność korzystania z serwisu geolokalizacyjnego, W – wiedza na temat serwisów społecznościowych oraz funkcjonowania smartfonów),
   b. **sekstingiem i naruszeniami prywatności** (W - wiedza na temat technicznych możliwości powielania danych w sieci, W - wiedza na temat zjawiska sekstingu, K - umiejętność realizowania profilaktyki medialnej I i II stopnia w zakresie e-zagrożeń w zakresie sekstingu, P - postawy rodziców wobec sekstingu),
   c. **naruszeniami praw autorskich** (W – wiedza na temat terminologii związanej z nielegalnym oprogramowaniem, W - wiedza na temat prawnych następstw związanych z pobieraniem filmów z nielegalnych źródeł, P – postawy wobec piractwa komputerowego, K- rodzic posiada kompetencje oceny legalności źródła oprogramowania),
   d. **wiarygodnością informacji dostępnych w Internecie** (W - wiedza na temat mechanizmów konstruowania najpopularniejszej encyklopedii internetowej, W - wiedza na temat

mechanizmów związanych z wynikami wyszukiwana, K - umiejętność sprawdzenia wiarygodności sprzedawcy w serwisie aukcyjnym),

e. cyberprzemocą (W - wiedza na temat mechanizmów związanych z cyberprzemocą, W - wiedza na temat rodzajów cyberprzemocy, W – wiedza na temat postępowania w sytuacji długotrwałego nękania – stalkingu),

f. wykonywaniem operacji finansowych w sieci (W - wiedza na temat przestępstw internetowych związanych z bankowością internetową, K – umiejętność sprawdzenia autentyczności strony internetowej banku internetowego, W – wiedza na temat możliwości zabezpieczenia nowych mediów przed zagrożeniami związanymi z płatnościami elektronicznymi)?

2) Jakie są dominujące postawy rodziców w odniesieniu do wykorzystywania Internetu i narzędzi cyfrowych przez ich dzieci?

Grupa 12 – rodzice w szkołach ponadgimnazjalnych

1) Jaki jest poziom wiedzy i umiejętności rodziców, potrzebnych do przeciwdziałania zagrożeniom związanym z:

   a. nieświadomym kreowaniem swojego wizerunku w Internecie (W - wiedza na temat możliwości umieszczania zdjęć w serwisach internetowych, K - umiejętność zabezpieczania własnych danych np. w postaci zdjęć w portalu społecznościowym, W – wiedza na temat kreowania własnego wizerunku poprzez konta w serwisach społecznościowych niedostępne dla rodziców),

   b. sekstingiem i naruszeniami prywatności (W - wiedza na temat udostępniania danych przez dzieci i młodzież w przestrzeni mediów sieciowych, W- wiedza na temat zjawiska sekstingu, K - umiejętność usuwania zdjęć indeksowanych przez najpopularniejszą w Polsce wyszukiwarkę internetową),

   c. naruszeniami praw autorskich (W – wiedza na temat terminologii związanej z nielegalnym oprogramowaniem, W - wiedza na temat prawnych następstw związanych z pobieraniem filmów z nielegalnych źródeł, P – postawy wobec piractwa komputerowego, K - rodzic posiada kompetencje oceny legalności źródła oprogramowania),

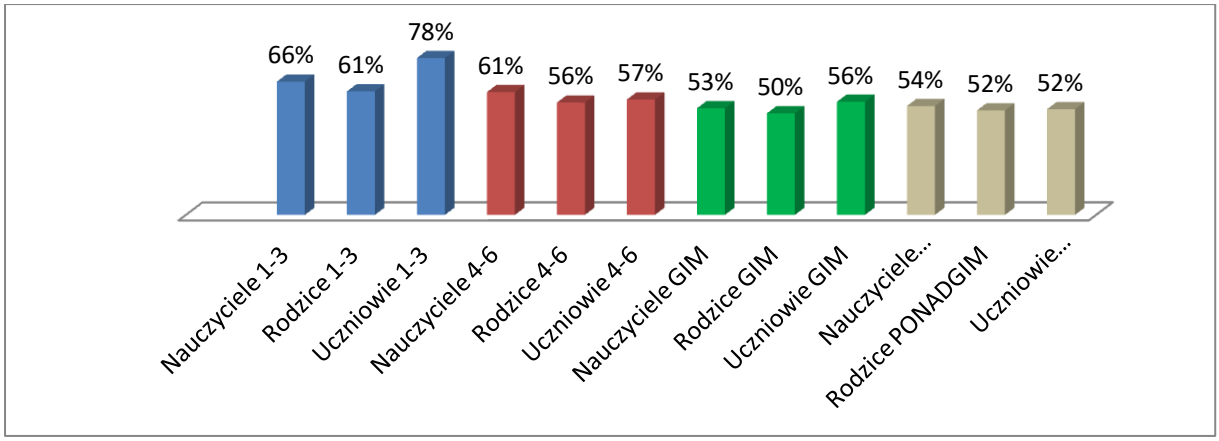
   d. wiarygodnością informacji dostępnych w Internecie (W - wiedza na temat mechanizmów konstruowania najpopularniejszej encyklopedii internetowej, K - umiejętność sprawdzenia źródła informacji, K - umiejętność sprawdzenia wiarygodności sprzedawcy w sklepie internetowym),

   e. cyberprzemocą (W - wiedza na temat mechanizmów związanych z cyberprzemocą, W- wiedza na temat rodzajów cyberprzemocy, K – umiejętność zabezpieczania materiałów dotyczących cyberprzemocy),

f. **wykonywaniem operacji finansowych w sieci** (W - wiedza na temat przestępstw internetowych związanych z bankowością internetową, K - umiejętność sprawdzenia połączenia szyfrowanego, W – wiedza na temat możliwości zabezpieczenia nowych mediów przed zagrożeniami związanymi z płatnościami elektronicznymi)?

2) Jakie są dominujące postawy rodziców w odniesieniu do wykorzystywania Internetu i narzędzi cyfrowych przez ich dzieci?

4. WYNIKI BADANIA POZIOMU KOMPETENCJI CYFROWYCH W ZAKRESIE BEZPIECZEŃSTWA CYFROWEGO



W ramach analizy zostały uśrednione wyniki dla każdej z 12 grup uczestniczących w badaniu. Ze względu na fakt, że grupa uczniów klas 1-3 badana była narzędziem innego rodzaju (kartą pracy, zamiast testu słownego), jej wyniku nie należy porównywać z pozostałymi 11 grupami i jego prezentowanie ma charakter jedynie poglądowy.

Spośród badanych grup najwyższy poziom kompetencji cyfrowych (informatyczno-medialnych) prezentowali nauczyciele uczący w klasach 1-3, a także rodzice uczniów 1-3. Możliwe są dwa wyjaśnienia tego faktu. Po pierwsze wynika to zapewne z faktu, że zagrożenia dla najmłodszych dzieci mają względnie prosty charakter, a rodzice na tym etapie rozwoju dziecka są najbardziej zaangażowani w opiekę i organizowanie warunków bezpiecznej zabawy i nauki swoich dzieci. Po drugie, można założyć, że rodzice tych uczniów są najmłodszymi spośród badanej grupy, w dużej

części między trzydziestym a czterdziestym rokiem życia. Oznacza to, że należą do pierwszego pokolenia dorastającego w otoczeniu narzędzi cyfrowych i wiele z badanych zagrożeń znają już z własnego doświadczenia.

W grupach rodziców, nauczycieli i uczniów z klas starszych szkoły podstawowej poziom kompetencji cyfrowych jest niższy (najniższy w grupie rodziców - co jest zresztą charakterystyczną cechą we wszystkich grupach wiekowych). Jest to również jedyna grupa, w której nauczyciele wykazali się większą kompetencją, niż ich uczniowie.

Z wiekiem ucznia poziom zagrożeń cyfrowych zaczyna wzrastać, osiągając pełny zakres w gimnazjum. Czynnikiem bardzo niekorzystnym jest duża podatność młodzieży w tym okresie rozwojowym na wpływy otoczenia zewnętrznego. Korespondują z tym wyniki badań wskazujące, że grupa gimnazjalna wymaga zdecydowanie największej uwagi wychowawczej i wsparcia. Zarówno w odniesieniu do uczniów, jak i nauczycieli. Co istotne, nie chodzi o samą formułę edukacji na poziomie kształcenia gimnazjalnego, jako osobnej szkoły, ale o etap rozwojowy uczniów w tym wieku i związane z tym okresem występujące zagrożenia prawidłowego przebiegu procesu rozwoju.

Grupą wymagającą największego wsparcia edukacyjnego w zakresie kompetencji cyfrowych, która wykazuje się najniższym poziomem kompetencji są rodzice uczniów w wieku gimnazjalnym. Średni wynik w tej grupie wyniósł zaledwie 50% możliwych prawidłowych odpowiedzi. Oznacza to, że w zasadzie na co drugie pytanie objęci badaniami rodzice odpowiedzieli niewłaściwie. Ekstrapolując wyniki testu na rzeczywiste zachowania, może to oznaczać, że w co drugiej sytuacji stanowiącej jakiegoś rodzaju zagrożenie dla ich dzieci nie potrafiliby rozpoznać danego zagrożenia lub zareagować adekwatnie do rodzaju tego zagrożenia.

Również w grupie uczniów ponadgimnazjalnych prezentowany poziomi kompetencji informacyjno-medialnych nie jest wysoki. Ich wzrost w stosunku do gimnazjów ma charakter raczej symboliczny. Oznacza to, że szczególnym wsparciem edukacyjnym powinni być objęci wszyscy uczniowie wchodzący w okres dojrzewania.

Ogólne wyniki należy interpretować, jako dowód na zdecydowanie zbyt niski poziom kompetencji cyfrowych wszystkich grup badanych: zarówno nauczycieli, rodziców, jak i uczniów. Najwyższy osiągnięty wynik, a więc 66% w grupie nauczycieli w klasach 1-3 to nadal zdecydowanie zbyt mało, aby móc ocenić sytuację jako zadowalającą.

4.1 SZKOŁA PODSTAWOWA 1 – 3

W klasach 1-3 szkół podstawowych wyzwania i zagrożenia mają charakter głównie techniczny. Podstawowym problemem, mającym wpływ na aktywność najmłodszych dzieci w sieci, jest respektowanie zasad ergonomii ich aktywności edukacyjnej i zabawy z wykorzystaniem nowych technologii. Zbyt długi czas spędzany przed monitorem tabletu czy smartfona, niewłaściwa pozycja zagrażająca rozwojowi układu szkieletowo-mięśniowego, negatywny wpływ ekranów na wzrok i słuch – to zjawiska obserwowane na co dzień w życiu tysięcy najmłodszych uczniów. Pozytywny jest fakt, iż jest to problem, z którego zdają sobie sprawę zarówno rodzice, jak i dzieci, wykazując się ponadprzeciętnie dużą wiedzą. Ponad trzy czwarte dorosłych i niemal wszystkie dzieci odpowiadało poprawnie na zadane pytania.

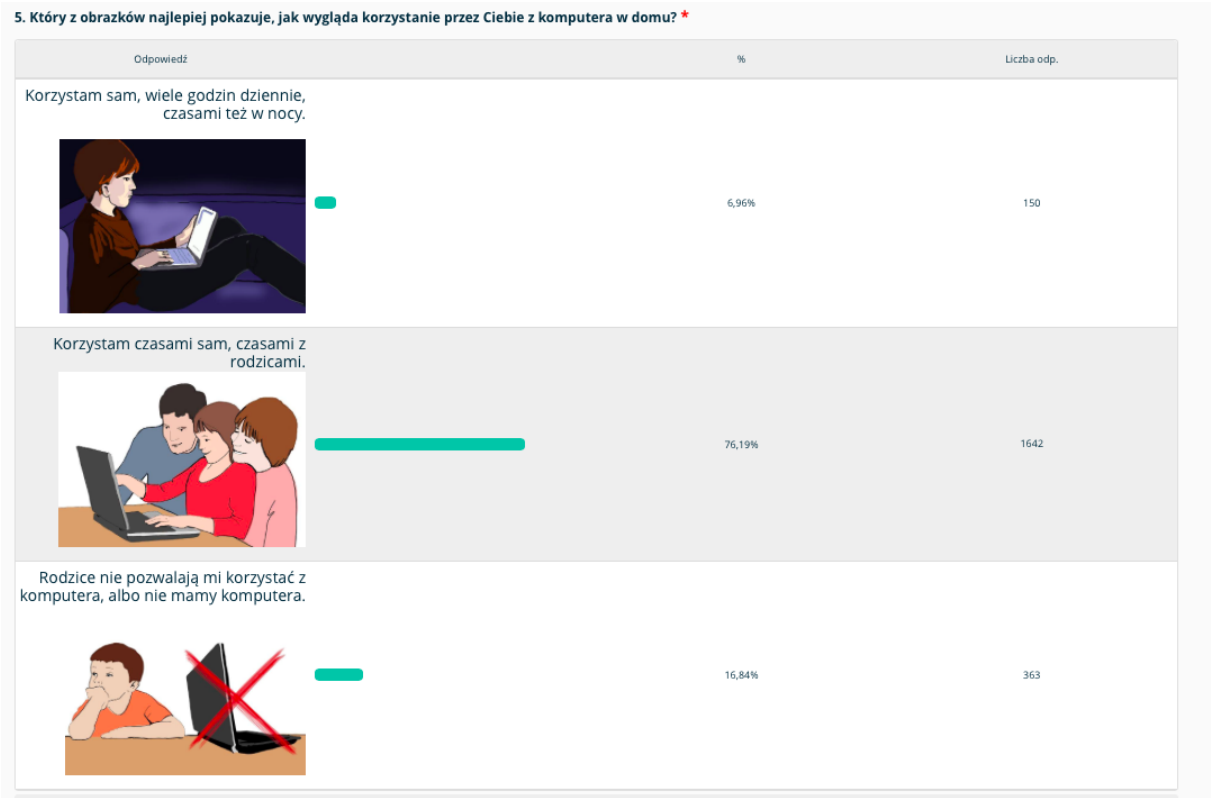
W interpretacji wysokiego wskaźnika prawidłowych odpowiedzi dzieci należy uwzględnić fakt, że uczniowie klas 1-3 byli badani za pomocą innego narzędzia, niż pozostałe grupy – a mianowicie za pomocą karty pracy opracowanej w formie komiksów. Forma narzędzia ułatwiała właściwe zrozumienie treści pytań przez uczniów. Co więcej, ze względu na możliwości percepcyjne najmłodszych uczniów, otrzymali oni znacznie mniej pytań, niż rodzice i nauczyciele, a liczba obszarów badawczych została ograniczona do czterech z sześciu. W pozostałych warstwach wiekowych wszystkie trzy grupy badanych otrzymały takie same pytania.

Obszarem, w którym zaobserwowano zdecydowanie najniższe wyniki, są: loginy, hasła i bezpieczne logowanie. Zarówno dorośli, jak i dzieci mieli problemy z odpowiedziami w zadaniach polegających na stworzeniu optymalnie bezpiecznego hasła. Szczególnie widoczne było to wśród dzieci, które często jako hasło wybierały po prostu imię albo imię i rok urodzenia – podobnie robiła także część rodziców. Również zasady bezpiecznego logowania, stron uwierzytelnionych i podobnych tematów dla większości badanych stanowiły duże wyzwanie.

Grupa	ŚREDNI WYNIK	N – ilość osób objętych badaniem	ERGONOMIA KORZYSTANIA Z NARZĘDZI CYFROWYCH	WIARYGODNOŚĆ INFORMACJI DOSTĘPNYCH W INTERNECIE	WPŁYW REKLAM NA DZIECI	BEZPIECZEŃSTWO W KONTAKCIE Z INNYMI UŻYTKOWNIKAMI SIECI	LOGINY, HASŁA I BEZPIECZNE LOGOWANIE	OCHRONA PRZED WIRUSAMI
Nauczyciele	66%	222	78%	60%	64%	50%	64%	79%
Rodzice	61%	512	74%	65%	60%	50%	47%	70%
Uczniowie	78%	2146	96%	83%	-	85%	46%	-

4.1.1 Uczniowie

Ze względu na wiek najmłodszych uczestników badania, przygotowane dla nich narzędzie badawcze miało inny charakter, niż w pozostałych grupach badanych. W miejsce relatywnie długiego formularza z pytaniami wprowadzono pytania i odpowiedzi ilustrowane rysunkami w formie komiksowej. Jak wskazał pilotaż, tak opracowana karta pracy była dobrze dostosowana do możliwości percepcyjnych uczniów. Wiązało się to niestety z koniecznością zmniejszenia liczby poruszanych problemów – z 6 do 4, a także zmniejszenia liczby pytań dodatkowych do dwóch.



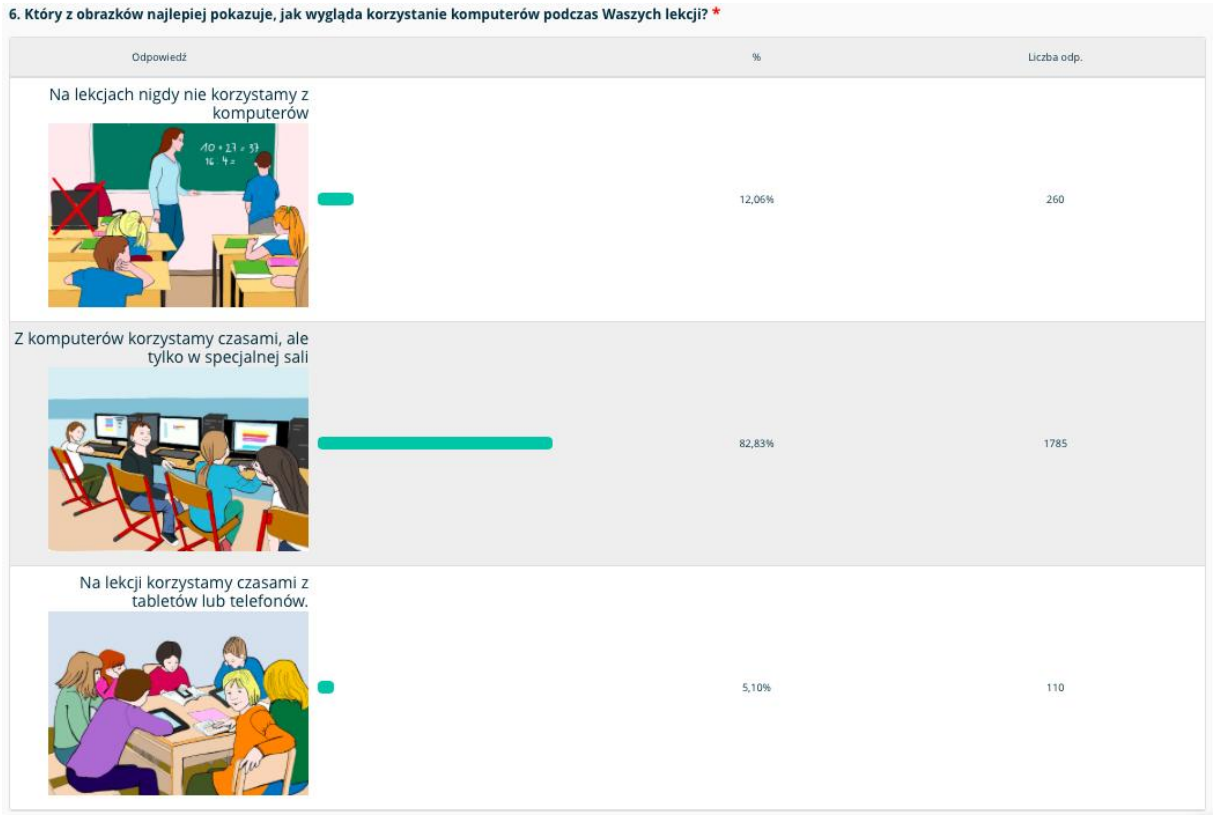
Pierwsze z pytań dodatkowych dotyczyło sposobu korzystania z urządzeń cyfrowych przez uczniów. Na bazie rekonesansu jakościowego, przeprowadzonego we wcześniejszej fazie projektu podczas spotkań z uczniami z klas 1-3, wytypowano trzy najczęściej występujące modele korzystania.

1. Pierwszy z nich opisuje styl korzystania urządzeń cyfrowych przez ucznia bez nadzoru rodziców, często przez wiele godzin, również w nocy. Niektórzy uczniowie opisywali swój czas spędzany przed komputerem jako „bez ograniczeń" lub „nawet do rana". Biorąc pod uwagę, że mówimy o dzieciach w wieku 6-9 lat, jest to dość niepokojące zjawisko, chociaż częstotliwość jego występowania jest ograniczona. W badaniu jedynie niepełne 7% uczniów stwierdziło, że jest to typowy sposób korzystania przez nich z urządzeń cyfrowych.

2. Drugi model opisuje styl korzystania urządzeń cyfrowych przez ucznia pod opieką rodziców – czasami samodzielnie, czasami razem z nimi. Kluczowa w wypowiedziach uczniów była tu rola rodziców, którzy wspierali dzieci i wspólnie z nimi oglądali treści w sieci. Na to także położono nacisk podczas konstrukcji obrazkowej części odpowiedzi. Taki model jako obowiązujący w domu wskazała najliczniejsza grupa uczniów – bo aż 76% badanych.

3. Trzeci model przedstawia sytuację, w której uczniowie nie mają w ogóle dostępu do świata cyfrowego. Przy czym model ten nie różnicuje powodów, dla których nowe technologie są poza zasięgiem uczniów. Może to wynikać zarówno z decyzji rodziców, jak i z warunków finansowych oraz braku urządzeń umożliwiających dostęp do sieci. Taki model wskazało blisko 17% badanych.

Wypływa z tego wniosek, że rodzice najmłodszej grupy najwyraźniej starają się uczestniczyć w życiu cyfrowym swoich dzieci. Jednak ich dobre chęci stoją w kontraście z brakami kompetencyjnymi, wykazanymi w badaniu dorosłych, a opisanymi poniżej.

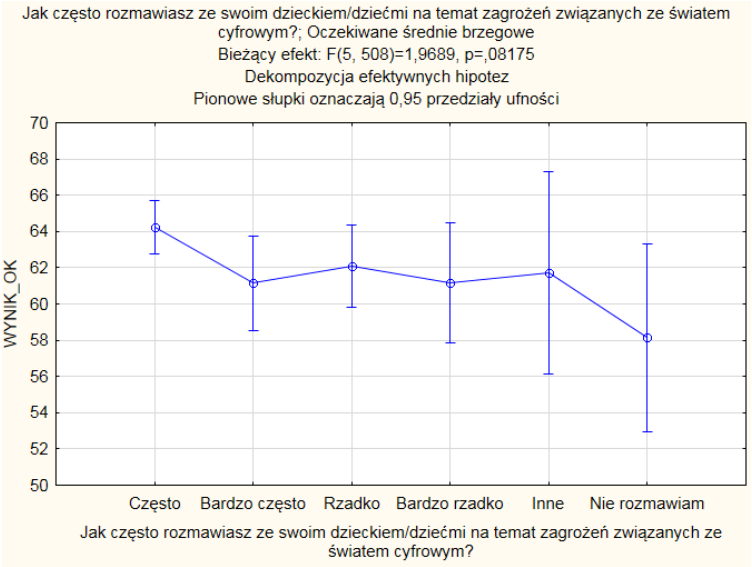


Drugie z pytań dodatkowych, skierowanych do uczniów klas 1-3 dotyczyło obowiązującego modelu korzystania z narzędzi cyfrowych w szkole. Tu także wyodrębniono trzy najczęściej występujące modele: 1) brak korzystania z komputerów na lekcjach, 2) korzystanie wyłącznie w sali informatycznej, 3) korzystanie z tabletów lub smartfonów w trakcie lekcji.

Jak wskazują wyniki model „sali informatycznej" jest najbardziej powszechny w realiach szkół uczestniczących w badaniu. Wskazało go ponad 82% uczniów. 12% stwierdziło, że nigdy nie korzystają z narzędzi cyfrowych, a jedynie 5% wybrało model mieszany, w którym świat cyfrowy i tradycyjny przenikają się w obrębie jednych zajęć dydaktycznych.

Ograniczenie kontaktu ze światem cyfrowym wyłącznie do osobnej pracowni informatycznej stanowi zaprzeczenie misji edukacyjnej szkoły, która powinna przygotowywać dzieci do funkcjonowania w rzeczywistości społeczno-kulturowej. A ta z perspektywy uczniów jest rzeczywistością dualną, cyfrową i analogową, które się wzajemnie przeplatają. Model „cyfrowej wyspy" w analogowym morzu nie oddaje realiów świata poza szkołą, a więc - niejako z definicji - nie jest w stanie uczniów przygotowywać do skutecznego radzenia sobie z wyzwaniami społeczeństwa informacyjnego.

4.1.2 Rodzice



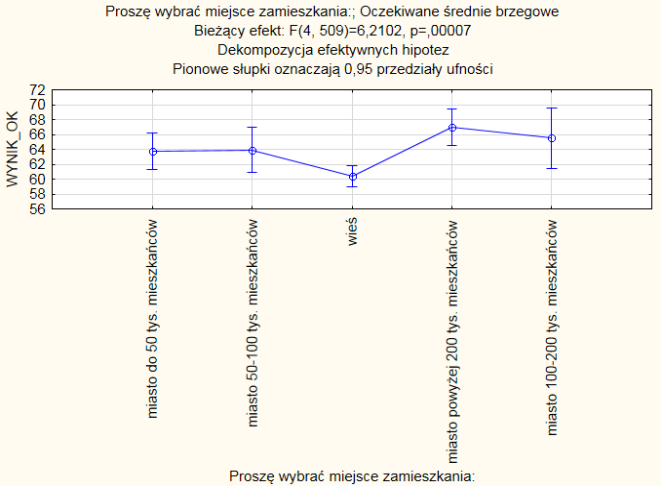
Interesujący wynik udało się uzyskać w kontekście pytania dotyczącego częstotliwości rozmów z dziećmi na temat zagrożeń w świecie cyfrowym. Na podstawie analizy powiązania wyników badania kompetencji cyfrowych z tym pytaniem można stwierdzić, że najwyższy poziom w teście kompetencyjnym ujawnili ci rodzice, którzy rozmawiają ze swoimi dziećmi często, a najniższy ci rodzice, którzy nie rozmawiają w ogóle.

Badanie nie pozwala ustalić, które zjawisko jest przyczyną, a które skutkiem. Można jednak podejrzewać, że występuje tu błędne koło: rodzice nie mający kompetencji nie rozmawiają z dziećmi o zagrożeniach świata cyfrowego, przez co nie mają okazji się niczego o tym świecie dowiedzieć i ich poziom kompetencji pozostaje niski. Na szczęście grupa ta jest najmniej liczna. Nigdy o tym nie rozmawia tylko 4% rodziców, podczas gdy często blisko połowa, bo aż 47% rodziców.

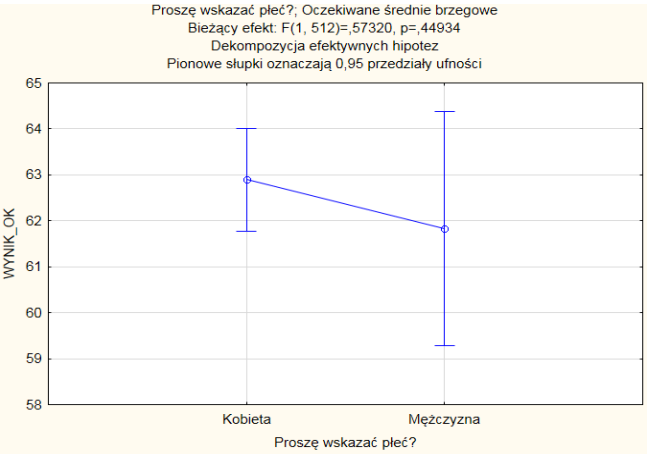
19. Jak często rozmawiasz ze swoim dzieckiem/dziećmi na temat zagrożeń związanych ze światem cyfrowym? *

Odpowiedź	%
Nie rozmawiam	4,03%
Bardzo rzadko	9,60%
Rzadko	20,35%
Często	47,79%
Bardzo często	14,78%
Inne	3,45%

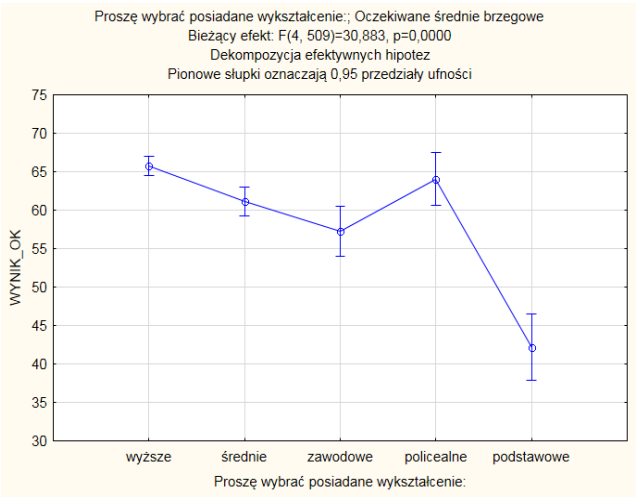
Miejsce zamieszkania ma znaczący wpływ na poziom kompetencji cyfrowych rodziców. Zdecydowanie najwyższy poziom wiedzy i umiejętności mają rodzice zamieszkujący duże i bardzo duże miasta, najniższy zaś rodzice zamieszkujący na wsi. Co więcej, ta linia trendu utrzymuje się także dla pozostałych kategorii. Mieszkańcy małych miast mają poziom kompetencji nieco niższy niż mieszkańcy dużych, za to większy niż mieszkańcy terenów wiejskich.



Płeć rodziców nie miała większego wpływu na ich wyniki. Statystycznie nieco wyższy poziom wspomnianych kompetencji ujawniają matki najmłodszych uczniów. Stanowiły one 84% próby w tej grupie wiekowej, a jedynie 16% odpowiedzi pochodziło od ojców. Różnica w wynikach jest jednak poniżej granicy błędu statystycznego dla tej grupy badanych.



Dużo większy wpływ na wynik osiągnięty w badaniu ma wykształcenie respondentów. Zachodzi tu całkowita korelacja – im wyższy poziom wykształcenia, tym wyższy średni wynik w teście kompetencyjnym w danej podgrupie. Co istotne, grupa rodziców z najniższym wykształceniem uzyskała średni wynik aż o jedną trzecią niższy, niż grupa z wykształceniem wyższym. Wprawdzie grupa ta jest nieliczna w stosunku do grupy osób wykształconych. Wykształcenie podstawowe zadeklarowało jedynie 4,41% rodziców dzieci z klas 1-3, niemniej osoby te mają największą trudność z radzeniem sobie z wyzwaniami świata cyfrowego.

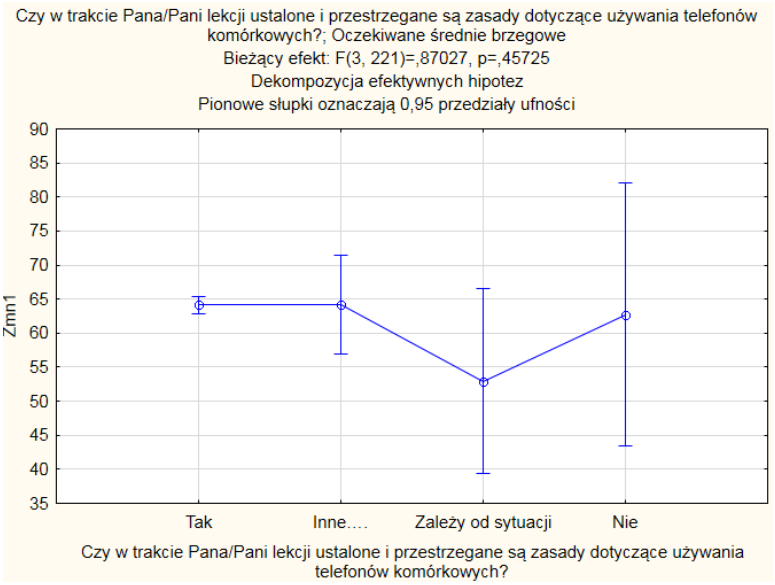


4.1.3 Nauczyciele

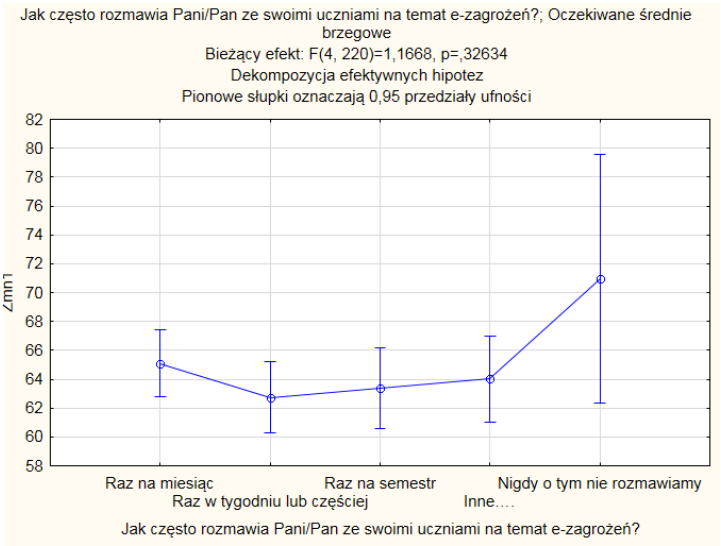
Pytania dodatkowe, zadawane poza testem kompetencji każdej z grup nie były jednorodne stosownie do realiów edukacji szkolnej w różnych grupach wiekowych uczniów. Przykładem takiego pytania dodatkowego skierowanego do nauczycieli było: „Czy na ich lekcjach są wypracowane jakieś zasady dotyczące korzystania z telefonów komórkowych?". Co ciekawe zarówno nauczyciele, którzy stosują takie zasady, jak i pozostali, którzy takich zasad nie respektują, uzyskali podobne wyniki w teście

kompetencyjnym. Jedyna grupa, która wykazała się znacząco niższym poziomem kompetencji to nauczyciele, którzy wybrali opcję „zależy od sytuacji".

Można postawić tu hipotezę, wymagającą dalszego zbadania, że ta elastyczność w podejściu jest wynikiem niewystarczającej wiedzy na temat świata cyfrowego. Problemem, wartym dodatkowego zbadania w badaniach jakościowych jest odbiór takiej postawy nauczyciela przez uczniów i jej wpływ na wyniki nauczania.



Co interesujące, nie da się ustalić żądanej korelacji zestawiając poziom kompetencji nauczycieli i częstotliwość ich rozmów z uczniami na temat zagrożeń w świecie cyfrowym. Wygląda na to, że świadomość niebezpiecznych mechanizmów w Internecie nie wpływa na częstość podejmowania takich rozmów.

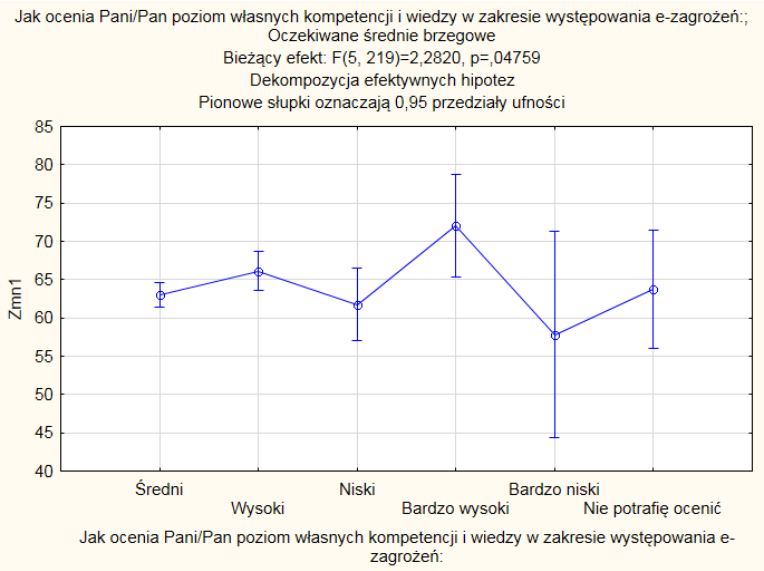


Niemal wszyscy badani nauczyciele rozmawiają ze swoimi uczniami na tematy związane z zagrożeniami cyfrowymi. Jedynie 2% nauczycieli stwierdziło, że nigdy takich rozmów nie prowadzi. 98% zadeklarowało, że takie rozmowy prowadzą, choć ich częstotliwość jest bardzo różna.

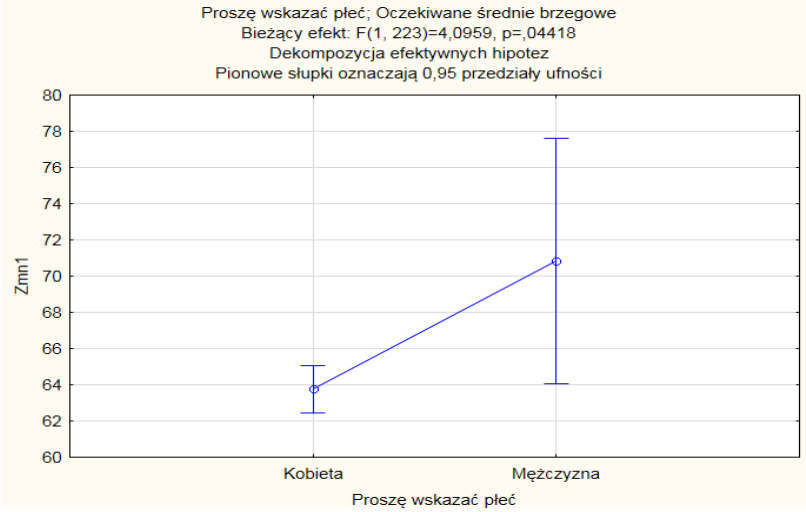
19. Jak często rozmawia Pani/Pan ze swoimi uczniami na temat e-zagrożeń? *

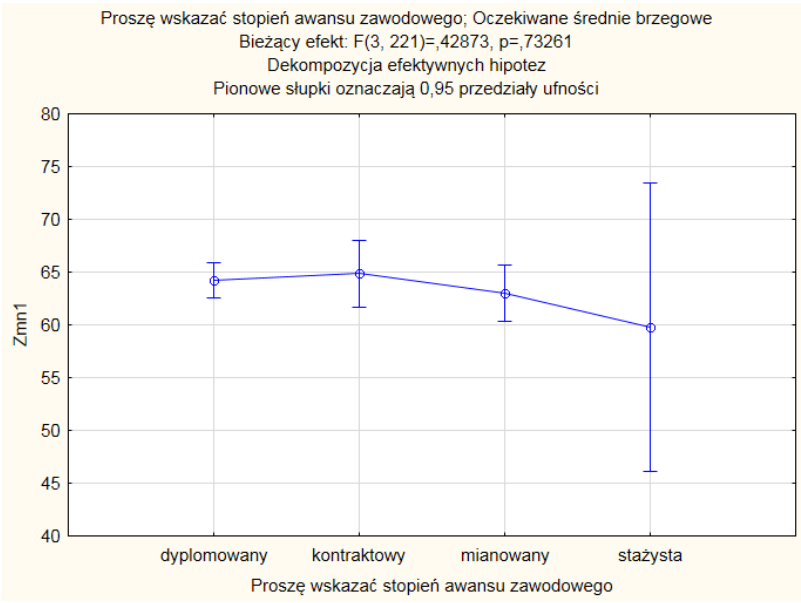
Odpowiedź	%
Nigdy o tym nie rozmawiamy	2,22%
Raz na semestr	20,89%
Raz na miesiąc	30,67%
Raz w tygodniu lub częściej	27,56%
Inne....	18,67%

Nauczyciele uczestniczący w badaniu wykazali się wysoką samoświadomością w kwestii swoich kompetencji cyfrowych. Najwyższy wynik w teście uzyskali ci, którzy określali swój poziom kompetencji jako bardzo wysoki, a najniższy ci, którzy określili go jako bardzo niski. Można to także interpretować jako dowód na wysoką trafność testu diagnostycznego wykorzystanego w badaniu.



Wśród 225 badanych nauczycieli z klas 1-3 większość stanowią kobiety (217 osób), a jedynie 8 osób to mężczyźni. Należy podkreślić, że wspomniana grupa 8 nauczycieli (mężczyzn) wykazała się statystycznie nieco wyższym poziomem kompetencji informacyjno-medialnych, niż kobiety. Jednak taka znacząca dysproporcja ze względu na płeć w strukturze próby nie pozwala na wyciągnięcie bardziej ogólnych, generalizujących wniosków w tym względzie.



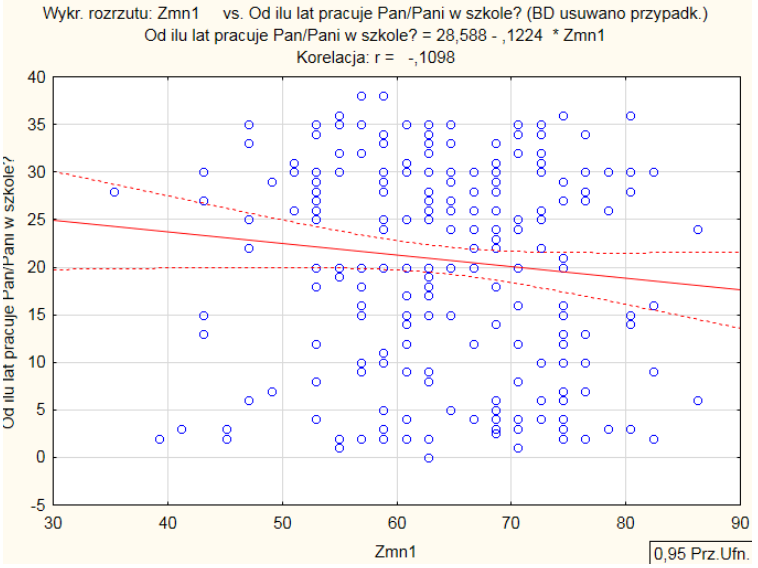


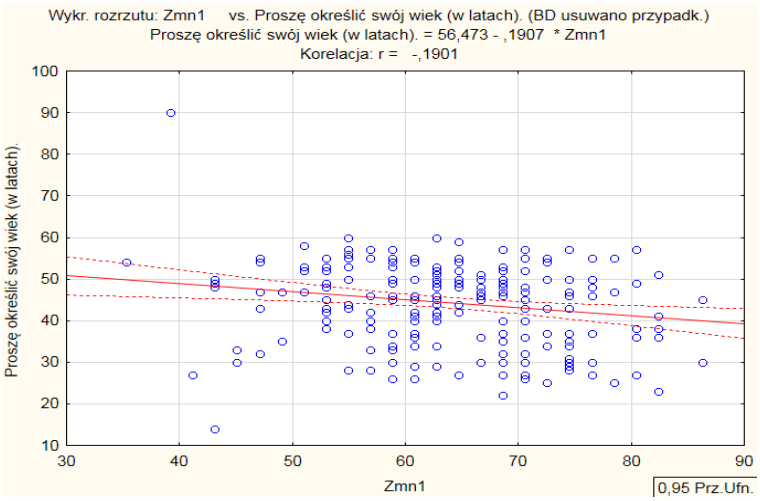
Badanie nie wykazało powiązania wyników testu z poziomem awansu zawodowego. Najniższy poziom kompetencji cyfrowych wykazała grupa nauczycieli stażystów, a więc rozpoczynających drogę zawodową. Jednak nauczyciele kontraktowi osiągnęli wynik nieco wyższy, niż nauczyciele mianowani i dyplomowani. Może to także wynikać ze struktury próby - zdecydowaną przewagę mieli w niej (podobnie jak i w całej populacji) nauczyciele dyplomowani, stanowiący blisko 60% uczestników badania, podczas gdy nauczyciele stażyści stanowili poniżej 1% badanych.

Badania pozwoliły natomiast zweryfikować związek stażu liczonego w latach z poziomem kompetencji nauczycieli w zakresie przeciwdziałania zagrożeniom cyfrowym. Wystąpiła tu niewielka korelacja (r = -,01).

Oznacza ona, że nauczyciele z krótkim stażem osiągają nieco lepsze wyniki, niż nauczyciele z długim stażem, jednak związek ten ma niską moc predykcyjną, jako że dla każdej długości stażu występowało bardzo duże zróżnicowanie wyników. Analogiczny brak silnego związku wystąpił w zestawieniu

wyników testu kompetencyjnego z wiekiem nauczycieli. Linia trendu jest nieco pochyła, nie pozwala to jednak na postawienie definitywnych wniosków, ani w odniesieniu do nauczycieli o większym stażu pracy, ani w odniesieniu do nauczycieli o krótszym stażu pracy.





4.1.4 Wnioski i rekomendacje - szkoła podstawowa: klasy 1-3

1. Średnie wyniki testu kompetencyjnego dla nauczycieli i rodziców są niskie w zdecydowanej większości obszarów tematycznych. Oznacza to, że obydwie grupy powinny zostać objęte szerokim wsparciem szkoleniowym w zakresie nabycia i podnoszenia kompetencji zagrożeń w świecie cyfrowym oraz możliwych strategii przeciwdziałania im.
2. Wśród uczniów klas 1-3 konieczne jest wsparcie zwłaszcza w zakresie wiedzy na temat loginów, haseł i zasad bezpiecznego logowania. Wielu uczniów wybierało jako ich zdaniem prawidłowe, hasło zbudowane na bazie swojego imienia, bądź imienia i roku urodzenia. Jest to problem

istotny także dla rodziców, a nawet nauczycieli – mimo wyższego średnio wyniku niż pozostałe grupy.

3. Znaczący problem z radzeniem sobie z zagrożeniami dla bezpieczeństwa dzieci w kontakcie z nieznajomymi w sieci mają zarówno rodzice, jak i nauczyciele. Może wynikać to z przekonania, że w dzieci w tym wieku nie mają jeszcze wielu okazji do takich kontaktów. Jest to jednak pogląd błędny. Mimo, że największa popularność korzystania z platform społecznościowych występuje faktycznie znacznie później, to już siedmio- i ośmiolatkowie mogą wejść w kontakt z obcymi w sieci, poprzez korzystanie z portali związanych np. z grami sieciowymi lub w serwisie Youtube.
4. Konieczne jest zwiększenie częstości rozmów na tematy bezpieczeństwa cyfrowego w trakcie lekcji. Jeżeli jedynie jedna czwarta nauczycieli prowadzi takie rozmowy raz na tydzień, a pozostali rzadziej, nieregularnie w nieokreślonej częstotliwości, to z punktu widzenia ucznia takie działania nie mogą być efektywne edukacyjnie i wychowawczo.
5. Oprócz lekcji dedykowanych wyłącznie bezpieczeństwu cyfrowemu, tematykę tę powinno się wplatać także do innych zajęć szkolnych. Chodzi m.in. o unaocznianie właściwych sposobów wyszukiwania informacji lub też akcentowanie zasad ergonomii korzystania z urządzeń cyfrowych, np. właściwej postawy siedzenia przed komputerem lub z tabletem.
6. Niezwykle ważnym problemem jest przeważający w klasach 1-3 model pracy uczniów z technologiami cyfrowymi wyłącznie w salach informatycznych. Jeżeli dodać do tego fakt, że sale często ustawione są w taki sposób, że uczniowie siedzą plecami do siebie i twarzami do ściany, jest to wyjątkowo niesprzyjające uczeniu się, Uczniowie są niejako odseparowani od siebie, funkcjonują poza środowiskiem społecznym. Takie warunki uczenia się w ogóle nie odzwierciedlają rzeczywistości uczestniczenia we współczesnym świecie cyfrowym.
7. W grupie rodziców wsparcia edukacyjnego wymagają szczególnie mieszkańcy wsi oraz osoby z wykształceniem podstawowym i średnim. Ponieważ czynniki: wykształcenia i miejsca zamieszkania często wiążą się ze sobą, ujawnia się potrzeba działania edukacyjnego na terenach wiejskich, której znaczenie wydaje się szczególnie duże.
8. Ważnym aspektem działań edukacyjnych jest także wzmocnienie świadomości rodziców w zakresie znaczenia rozmów z dziećmi na temat zagrożeń w świecie cyfrowym. Blisko jedna trzecia rodziców stwierdziła, że prowadzi takie rozmowy rzadko lub bardzo rzadko. Oznacza to, że ich dzieci mogą być zupełnie pozbawione wsparcia ze strony dorosłych, jak bowiem wskazano wyżej, również znaczna część nauczycieli prowadzi takie rozmowy bardzo rzadko.

4.2 SZKOŁA PODSTAWOWA – KLASY 4-6

Przejście do drugiego etapu edukacyjnego jest dla uczniów znaczącą cezurą. W obecnym systemie oznacza nie tylko pojawienie się nowych przedmiotów, ale ogólną zmianę warunków organizacji procesu kształcenia. Jedną „panią" zastępuje teraz grupa nauczycieli przedmiotowych, a funkcja wychowawcza spada zwykle na barki nauczyciela wychowawcy.

Jednocześnie uczniowie wchodzą w zupełnie nowy etap rozwoju społecznego. Ich zainteresowania rozszerzają się. Dzieci dużo łatwiej wchodzą w nowe relacje, ale także – co najważniejsze – coraz istotniejsze stają się więzi z rówieśnikami, którzy powoli przejmują rolę autorytetu i podstawowego źródła wartości, norm i przekonań. Co prawda, uczniowie w klasach 4-6 nie doświadczają jeszcze buntu typowego dla okresu gimnazjalnego, ale już stopniowo kwestionują autorytet dorosłych. To „uwalnianie" się spod władzy dorosłych powoduje, że są oni narażeni na znacznie więcej zagrożeń w świecie cyfrowym, niż ich młodsi koledzy i koleżanki.

Jak jednak wskazują wyniki badań, do radzenia sobie z tymi zagrożeniami nie są przygotowani specjalnie dobrze, ani oni sami, ani ich rodzice i nauczyciele. Wyniki w teście kompetencyjnym wykazują, że wymienione grupy badanych znajdują się w przedziale od 56% do 61% prawidłowych odpowiedzi. Oznacza to stosunkowo duże prawdopodobieństwo niewłaściwego ich reagowania w różnych sytuacjach stanowiących dla nich sytuację nową, zaskakującą, której nie będą postrzegać w kategoriach potencjalnego zagrożenia.

Najlepszy wynik odnotowany w grupie nauczycieli (61%) nie daje wystarczającej gwarancji bezpieczeństwa właściwego wsparcia wychowawczego uczniów. O pięć punktów procentowych niższy (56%) wynik rodziców wskazuje, że jest bardzo wiele sytuacji potencjalnie niebezpiecznych i pytań ze strony uczniów, na które nie mają od kogo uzyskać merytorycznego wsparcia i prawidłowej odpowiedzi.

Największy deficyt wiedzy w tej grupie wiekowej występuje na temat prawa autorskiego. Zarówno uczniowie, jak i rodzice i nauczyciele nie mają odpowiedniej, a często żadnej orientacji w tym obszarze. Nie znają zasad właściwego cytowania, mają problem z odróżnieniem plagiatu od użytku dozwolonego, nie znają relacji prawnych tworzonych przez wykorzystywanie licencji Creative Commons.

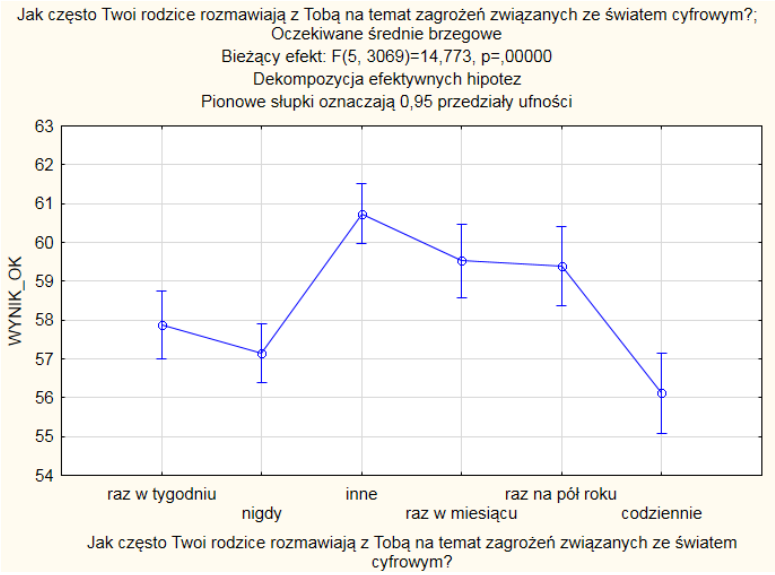
Statystycznie najlepiej radzą sobie wszyscy z kwestiami ergonomii korzystania z urządzeń cyfrowych. To pozytywny przejaw świadomości sposobu użytkowania nowych technologii w kontekście prozdrowotnym, np. niewłaściwego ułożenia kręgosłupa jako potencjalnej przyczyny przyszłych problemów zdrowotnych. Jednak niektóre z pozostałych zagrożeń, takie jak np. kontakt z innymi

użytkownikami lub niewłaściwe kreowanie własnego wizerunku należą do grupy niebezpieczeństw o poważniejszym znaczeniu. Mogą one prowadzić do bezpośredniego i niemal natychmiastowego zagrożenia życia lub zdrowia uczniów w wyniku popełnienia nawet jednego błędu.

Grupa	ŚREDNI WYNIK	N – ilość osób objętych badaniem	ERGONOMIA KORZYSTANIA Z NARZĘDZI CYFROWYCH	WIARYGODNOŚĆ INFORMACJI DOSTĘPNYCH W INTERNECIE	BEZPIECZEŃSTWO W KONTAKCIE Z INNYMI UŻYTKOWNIKAMI SIECI	LOGINY, HASŁA I BEZPIECZNE LOGOWANIE	BEZPIECZEŃSTWO WIZERUNKU W INTERNECIE	PRAWO AUTORSKIE
Nauczyciele	61%	316	73%	63%	61%	57%	71%	39%
Rodzice	56%	466	74%	51%	55%	53%	68%	32%
Uczniowie	57%	3072	51%	59%	80%	63%	57%	32%

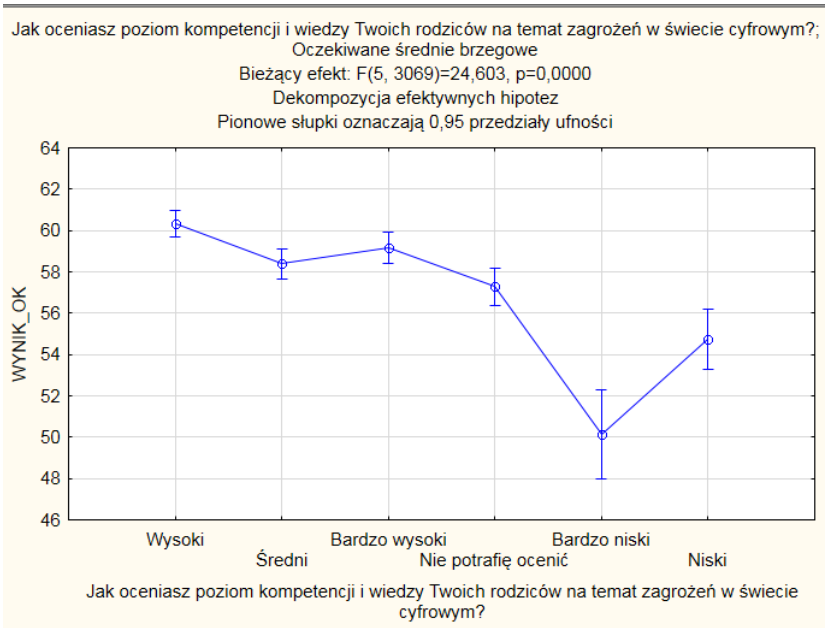
4.2.1 Uczniowie

Uczniowie w klasach 4-6 są w stanie posługiwać się komputerami w stopniu wystarczającym, aby mogli wziąć udział w badaniu w formie analogicznej do grupy osób dorosłych. Wytworzyło to możliwość zadania im wielu dodatkowych pytań, pozwalających opracować znacznie bardziej rozbudowany i detaliczny portret tej grupy wiekowej.

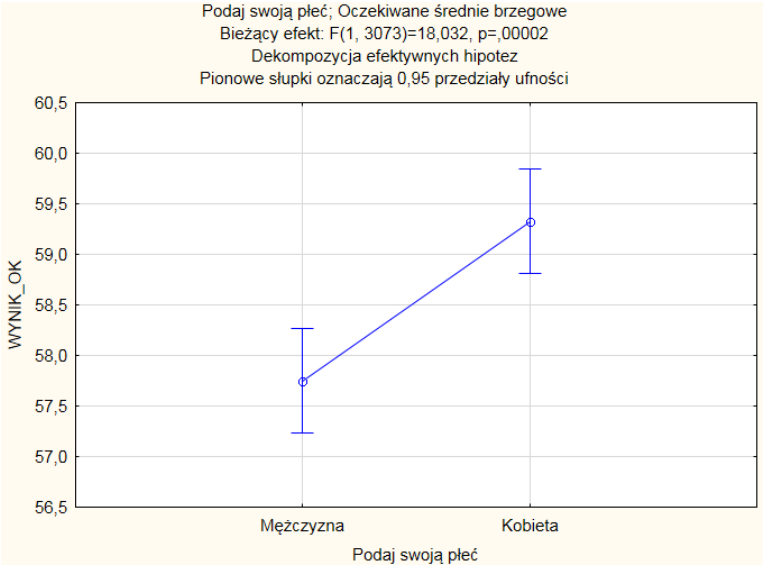


Niezwykle ciekawy jest wynik zestawienia kompetencji informatyczno-medialnych uczniów z częstotliwością rozmów prowadzonych z rodzicami na temat zagrożeń w świecie cyfrowym. Jak się okazuje, sam fakt rozmowy nie jest wystarczający. Nie da się wykluczyć, że wiele z takich rozmów ma charakter zbyt ogólnych stwierdzeń, ostrzeżeń, nakazów lub zakazów, ewentualnie prowadzi do ujawniania niekompetencji rodziców w różnych obszarach uczestnictwa w świecie cyfrowym. Stają się one wówczas nieskuteczne, ponieważ w niewielkim stopniu wspierają rozwój uczniów w konkretnych sytuacjach problemowych, wymagających konkretnych rozwiązań i propozycji postępowania.

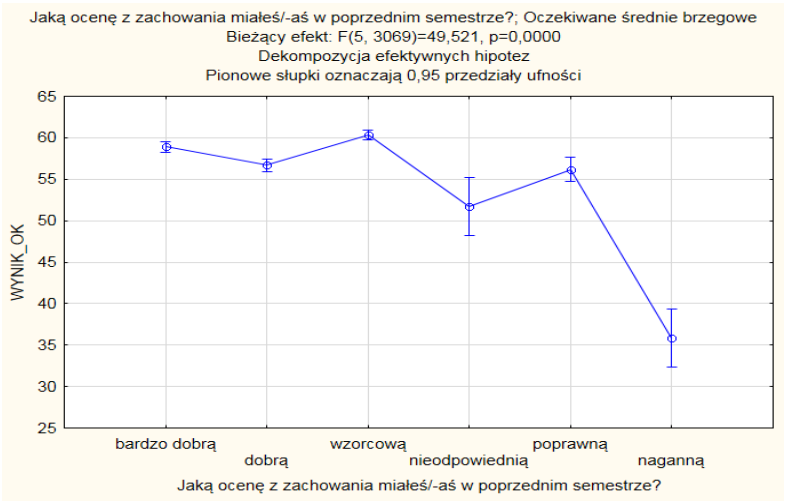
Czynnikiem silnie skorelowanym z poziomem kompetencji cyfrowych uczniów jest sposób, w jaki odnoszą się do kompetencji ich rodziców. Uczniowie, którzy uznali swoich rodziców za bardzo kompetentnych lub kompetentnych, uzyskali najwyższe wyniki w teście kompetencji cyfrowych. Uczniowie zaś, którzy swoich rodziców ocenili jako mało kompetentnych lub niekompetentnych, sami również w teście zdobyli znacząco niższe wyniki.



Uczniowie w klasach 4-6 to najmłodsza grupa wiekowa, dla której możliwe było porównanie poziomu kompetencji cyfrowych.



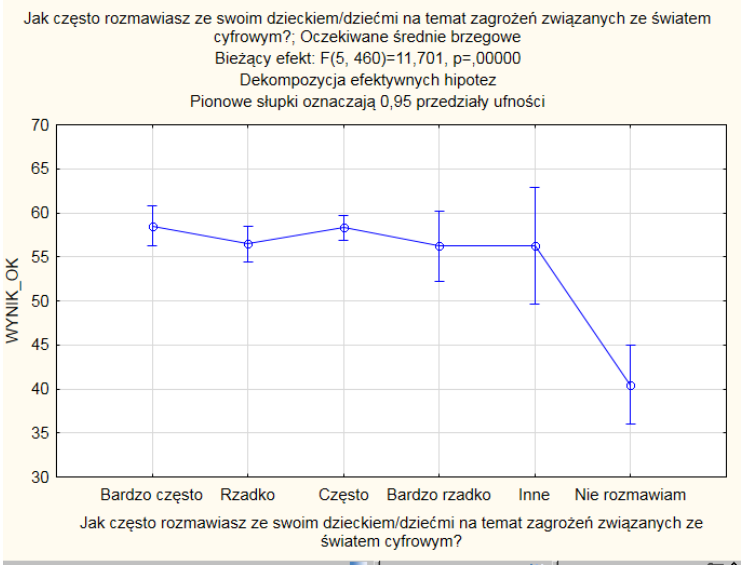
Interesująca jest analiza kolejnego obszaru związana z zestawieniem ocen uczniów z zachowania z wynikiem w teście kompetencji cyfrowych. Jak się okazuje uczniowie mający oceny wzorowe wykazali średnio także najwyższe kompetencje w badaniu. Co więcej, korelacja między ocenami z zachowania a średnim wynikiem kompetencji była istotna statystycznie. Obniżenie oceny z zachowania o jeden stopień koreluje z obniżeniem średniego wyniku w badaniu. Najniższy poziom odnotowali uczniowie o ocenach nagannych.



4.2.2 Rodzice

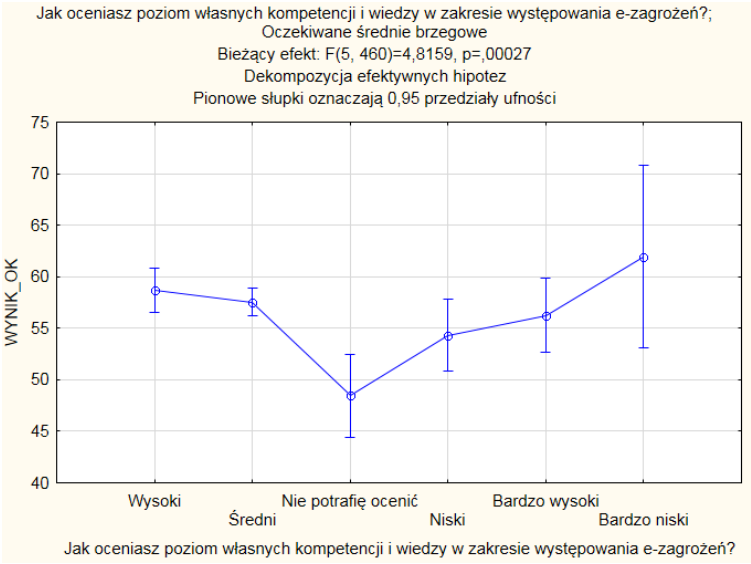
Rodzice, którzy nie rozmawiają ze swoimi dziećmi na tematy związane z zagrożeniami w świecie cyfrowym, mają przeciętnie najniższe wyniki w badaniu. Różnica w stosunku do pozostałych grup wynosi niemal 15 punktów procentowych. Wszystkie pozostałe grupy rodziców, zarówno tych

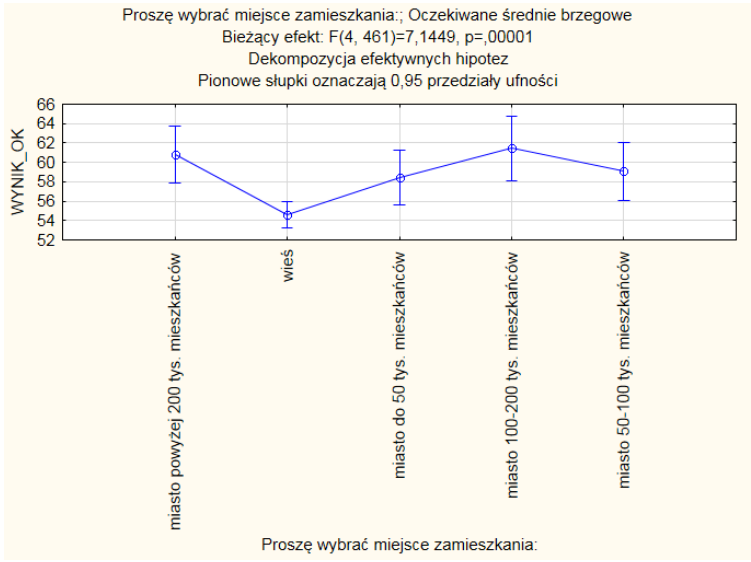
rozmawiających bardzo często, jak i tych, którzy rozmawiają raczej rzadko, mają dość podobny poziom kompetencji cyfrowych w badanym zakresie.



Jest to spójne z danymi pochodzącymi od uczniów, u których częstotliwość rozmów z rodzicami nie miała znaczącego wpływu na ich poziom kompetencji cyfrowych. Znacznie ważniejsza była realna wiedza rodziców i ich orientacja w cyfrowym świecie. Ten czynnik przekładał się znacząco na poziom kompetencji uczniów. Wynik ten z kolei jest całkowicie spójny z rezultatami odpowiedzi na następne pytanie, w ramach którego rodzice oceniali własne kompetencje cyfrowe. Ci z nich, którzy uznali, że mają wysoki poziom wiedzy i umiejętności, faktycznie uzyskali najwyższe wyniki. Ci zaś, którzy zadeklarowali brak wystarczającej znajomości zagrożeń świata cyfrowego, zdobyli średnio znacząco mniej punktów.

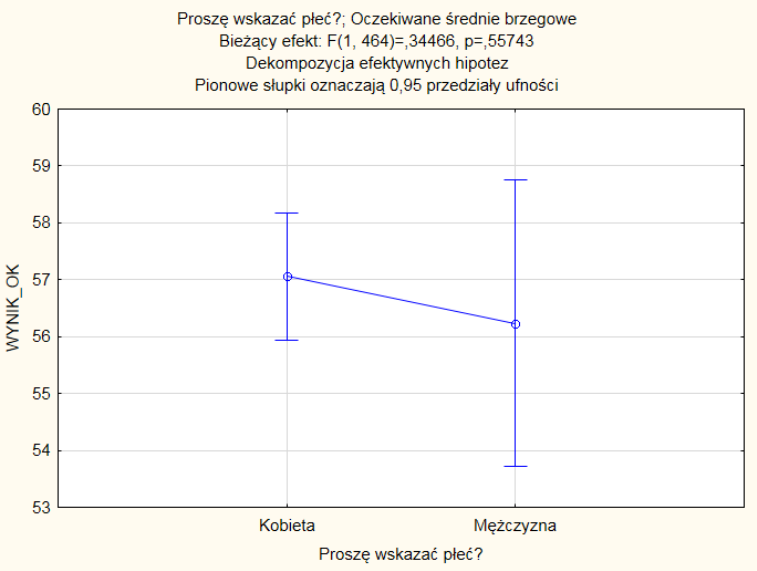
To ważne zjawisko, ponieważ w części popularnego przekazu w środowiskach edukacyjnych panuje przekonanie, że najważniejsze dla ochrony dzieci przed zagrożeniami jest to, aby dużo z nimi rozmawiać. Niniejsze badanie wskazuje, że znacznie istotniejsze jest to, czy rodzice mają wystarczająco dużą wiedzę w tym zakresie, którą mogą dzielić się z dzieckiem podczas rozmowy wychowawczej.

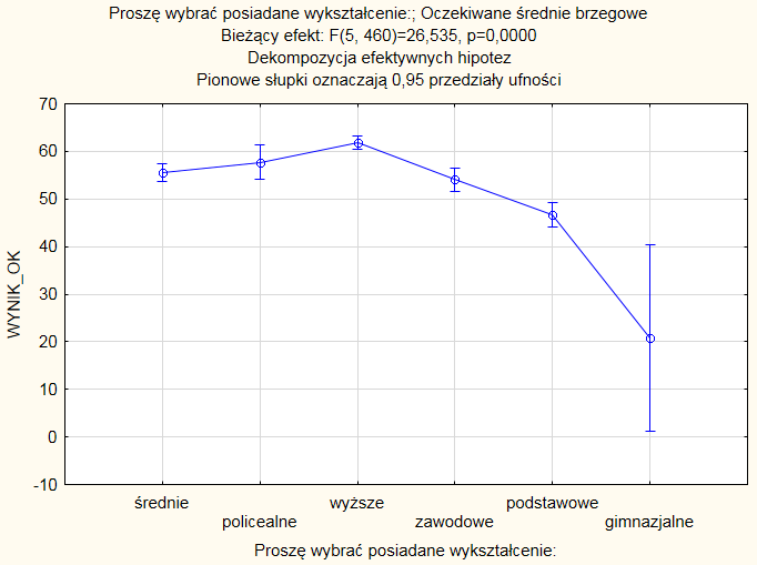




Statystycznie najsłabiej wypadli w badaniu rodzice dzieci, mieszkający na wsi. Wyniki te są spójne z wcześniej zaprezentowanymi i w oczywisty sposób stanowią potwierdzenie związku między miejscem zamieszkania, a poziomem zagrożenia, którego podłożem są niewystarczające kompetencje cyfrowe.

Nie uchwycono natomiast w badaniach związku pomiędzy płcią badanych rodziców, a ich wynikami w teście kompetencyjnym. Podobnie jak we wcześniej sekwencji analizy wyników badań, kobiety i mężczyźni wykazali się bardzo podobnym poziomem kompetencji informacyjno-medialnych.





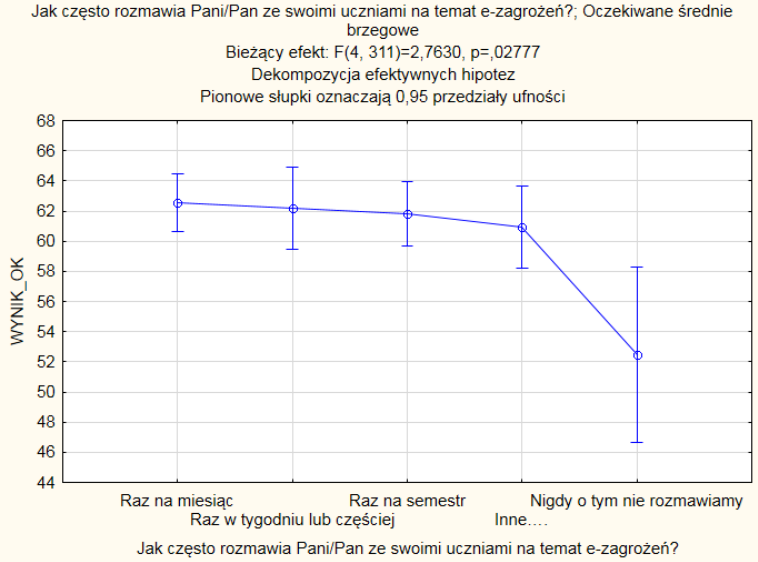
Podobnie jak w grupie rodziców uczniów klas 1-3, także u rodziców dzieci z klas 4-6 można zauważyć znaczący związek pomiędzy poziomem wykształcenia, a kompetencjami w świecie cyfrowym. Najwyższy poziom tych kompetencji mają rodzice z wykształceniem wyższym, a wraz z coraz niższym poziomem wykształcenia ujawnia się coraz niższy średni poziom ich kompetencji cyfrowych.

Kolejne interesujące informacje przyniosło zapytanie rodziców, czy w szkole ich dzieci miało miejsce naruszenie bezpieczeństwa cyfrowego. 8% rodziców stwierdziło, że taka sytuacja miała miejsce (nota bene, jest to dość wysoki wynik), a blisko 19% podało odpowiedź przeciwną. Najbardziej istotny wszakże okazuje się fakt, że aż 73% rodziców nie wiedziało jak odpowiedzieć na to pytanie. Wskazuje to na bardzo słabą relację komunikacyjną i zarazem słaby kontakt rodziców ze szkołą. Co sprawia, że w kwestii tak istotnej jak bezpieczeństwo ich dzieci w świecie cyfrowym, rodzice po prostu nie mają wystarczających informacji przekazywanych na bieżąco przez nauczycieli.

23. Czy w Państwa szkole zdarzył się przypadek naruszenia bezpieczeństwa cyfrowego? *

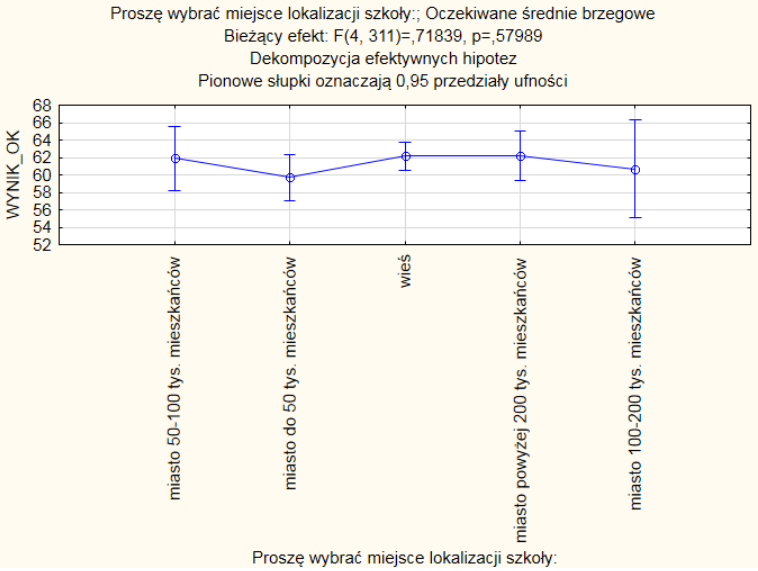
Odpowiedź	%	Liczba odp.
Tak	8,07%	38
Nie	18,90%	89
Nie wiem	73,04%	344

4.2.3 Nauczyciele

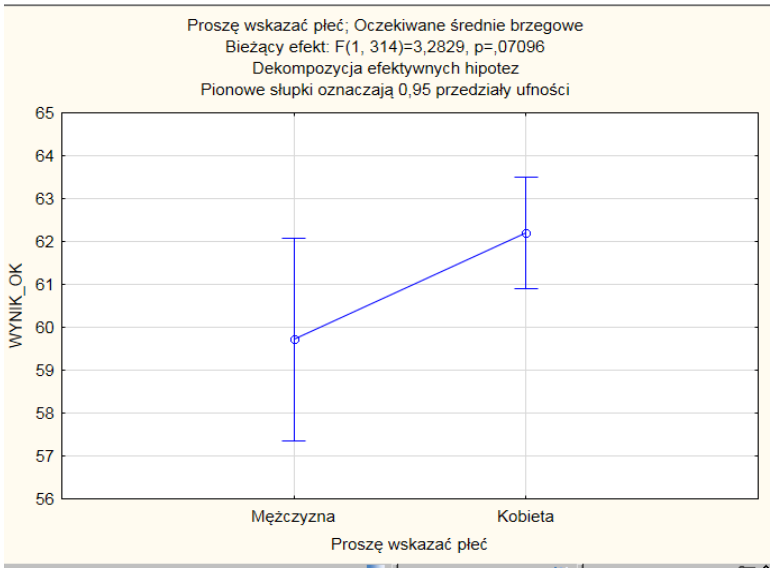


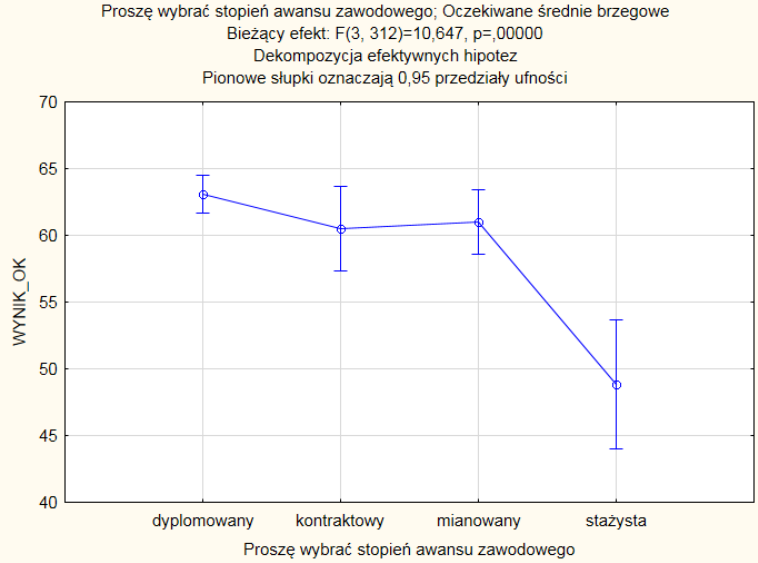
Podobnie jak rodzice także nauczyciele, którzy nigdy nie rozmawiają ze swoimi uczniami na temat zagrożeń cyfrowych, mają najniższe wyniki w badaniu kompetencji cyfrowych. Pozostałe grupy nauczycieli mają dość podobne wyniki. Można to interpretować analogicznie, jak w kontekście rodziców - przyczyną rzadkich rozmów nauczycieli z uczniami na ten temat jest deficyt kompetencji cyfrowych tych pierwszych. Domyka się wówczas błędne koło „niemocy" pedagogicznej nauczycieli w przygotowywaniu uczniów do skutecznej ich ochrony przez zagrożeniami w świecie cyfrowym.

W przypadku nauczycieli z klas 4-6 nie pojawił się, tak jak w innych grupach, związek między miejscem zamieszkania a kompetencjami informacyjno-medialnymi w badanym obszarze. Różnice między miejscem zamieszkania miały wartość poniżej błędu statystycznego. Można to interpretować jako zjawisko niezależne od miejsca zamieszkania i pracy. Wiąże się to z faktem, iż nauczyciele biorą udział w zbliżonych szkoleniach oraz zdobywają wiedzę z podobnych źródeł, a więc kształtują podobne zakresy kompetencji informatyczno-medialnych. Widać tu wyraźny kontrast w zestawieniu z rodzicami, u których nie występował ten właśnie czynnik. Dlatego w tej grupie badanych różnice związane z miejscem zamieszkania mogły sięgać nawet 12 punktów procentowych.



Płeć nauczycieli nie miała większego wpływu na wynik. Dwa punkty procentowe przeciętnej różnicy są różnicą mniejszą niż błąd statyczny.

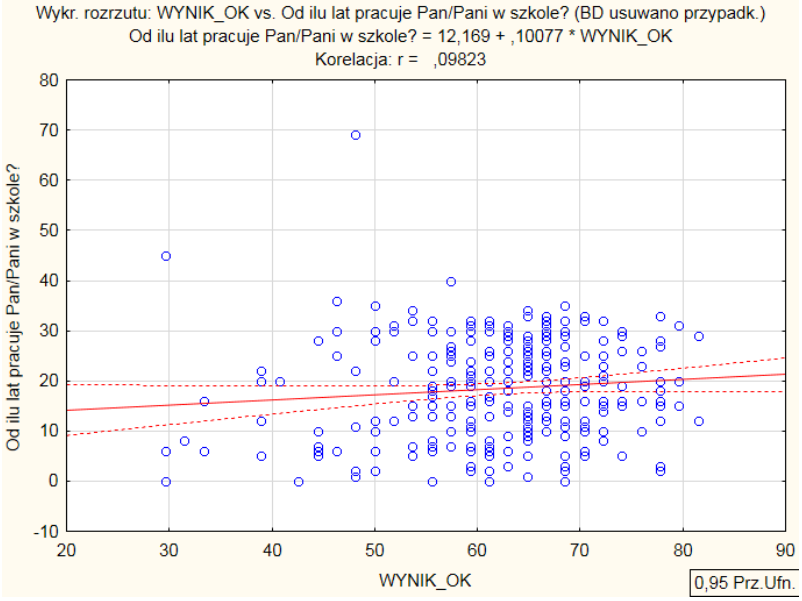


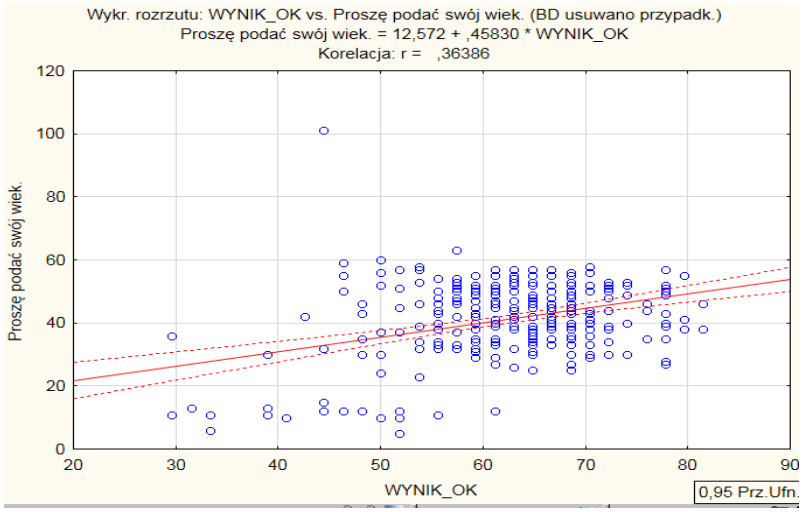


Podobnie jak wśród nauczycieli uczących dzieci w klasach 1-3, jedynie wyniki nauczycieli stażystów znacząco odbiegają od pozostałych badanych. Różnica ta jest bardzo duża. Średni wynik w przypadku stażystów był o ponad dziesięć punktów procentowych niższy, niż w pozostałych grupach.

Nie da się także powiązać lat stażu w szkole ze współczynnikiem korelacji Pearsona, który wynosi jedynie 0,09. Oznacza to bardzo słabą korelację. Jednak w przypadku nauczycieli „przedmiotowców" znacznie wyraźniej niż w przypadku nauczycieli nauczania początkowego widać związek wieku z poziomem kompetencji cyfrowych. Korelacja wyniosła tutaj aż 0,36, co jest jednym z najsilniejszych związków w badaniu.

Oznacza to, że statystycznie im większy staż pracy nauczyciela w klasach 4-6, tym wyższy poziom jego wiedzy na temat zagrożeń związanych ze światem cyfrowym. Jest to spójne z wcześniejszymi wnioskami. Prawdopodobnym źródłem niskiego poziomu wiedzy najmłodszych stażem nauczycieli są słabości kształcenia informatycznego i medialnego nauczycieli w trakcie studiów, powiązane z niedostosowaniem uczelni pedagogicznych do najnowszych trendów. W efekcie znacznie ważniejsze od wykształcenia na uczelni okazuje się doświadczenie w zawodzie i zdobywane w miarę mijających lat kompetencje społeczne oraz lepsze rozumienie mechanizmów i zjawisk zachodzących wśród uczniów.





4.2.4 Wnioski i rekomendacje - szkoła podstawowa: klasy 4-6

1. Średnie wyniki testu kompetencyjnego zarówno dla uczniów klas 4-6, jak i ich rodziców oraz nauczycieli są dość niskie. Ich zakres mieszczący się w przedziale od 57% do 61% wskazuje na konieczność pracy edukacyjnej ze wszystkimi grupami badanymi w celu podniesienia poziomu kompetencji informacyjno-medialnych.
2. Obszarem szczególnie wymagającym wsparcia jest wiedza o zasadach prawa autorskiego. Żadna z badanych grup nie przekroczyła tutaj progu 40% prawidłowych odpowiedzi, przewidzianego dla tego zakresu tematycznego bezpieczeństwa cyfrowego.
3. W obszarze bezpieczeństwa w kontakcie z innymi użytkownikami sieci największą wiedzę mają uczniowie, przewyższając w tym zakresie swoich rodziców i nauczycieli o około dwadzieścia punktów procentowych. Oznacza to, że wartościową inicjatywą byłoby organizowanie takich form

współpracy, w których to uczniowie mogliby przekazywać im wiedzę o bezpieczeństwie cyfrowym.

4. Nauczyciele są z kolei najlepiej zorientowani, jeżeli chodzi o zasady wiarygodności informacji w sieci (kompetencje medialne). Znacząco przewyższają tu rodziców, dla których jest to temat znacznie mniej rozpoznany (aż 12 pp. różnicy)
5. Uczniowie wykazują duże deficyty wiedzy w zakresie bezpieczeństwa kształtowania wizerunku w Internecie. Co, biorąc pod uwagę etap rozwojowy, stanowi duże zagrożenie dla właściwego przebiegu procesu rozwoju w sferze społecznej, a może skutkować także przekraczaniem norm obyczajowych i prawnych. Niska świadomość istoty zagrożeń zwiększa prawdopodobieństwo wyrządzenia sobie realnej krzywdy, a także umiejętności skutecznego radzenia sobie w różnych sytuacjach komunikowania się z otoczeniem w świecie cyfrowym. Pozytywnym prognostykiem są zdecydowanie wyższe wyniki nauczycieli (71%, a więc o 14 pp. więcej, niż uczniowie). Mają oni o wiele większą świadomość zagrożeń i mogą stanowić skuteczne wsparcie uczniów.
6. Jak wskazuje analiza pytań dodatkowych i ich związku z wynikami testu kompetencyjnego, duże znaczenie dla kształtowania się kompetencji cyfrowych w grupie najmłodszych uczniów ma poziom e-kompetencji ich rodziców. Okazuje się natomiast, że małe znaczenie ma to, jak często rodzice rozmawiają ze swoimi dziećmi na temat ryzyka i zagrożeń w świecie cyfrowym. Wyniki badania nie negują wartości tych rozmów, jednak jako warunek niezbędny ich skuteczności w przedmiocie badania, wskazują wysoki poziom kompetencji cyfrowych rodziców.
7. W przypadku nauczycieli nie jest najistotniejsze, w jakiej miejscowości mieści się szkoła. Uniformizacja wiedzy i kompetencji, z racji wykonywanego zawodu niweluje wpływ tego czynnika, który bardzo mocno oddziałuje z kolei na zakres i dynamikę aktualizowania kompetencji cyfrowych rodziców. Przedstawiciele tej grupy ze środowiska wiejskiego mają znacznie niższe wyniki w badaniu kompetencji informacyjno-medialnych.
8. Badanie nauczycieli z klas 4-6 wskazuje, że poziom kompetencji związanych z zagrożeniami świata cyfrowego wzrasta wraz z ich stażem pracy. Oznacza to, że szczególnie należy wspierać w kształtowaniu kompetencji informacyjno-medialnych nauczycieli o najkrótszym stażu pracy, ze szczególnym uwzględnieniem nauczycieli stażystów.

4.3 GIMNAZJA

Z zestawionych danych wyłania się obraz zróżnicowanego poziomu kompetencji cyfrowych badanych grup w gimnazjach. Najwyższy poziom kompetencji służących niwelowaniu zagrożeń w świecie cyfrowym posiadają uczniowie. Względnie wysoki poziom wiedzy o negatywnych zjawiskach powiązanych z bezpieczeństwem cyfrowym prezentują zarówno nauczyciele, uczniowie, jak i ich

rodzice. Mają dobrą orientację w tematyce mechanizmów i przeciwdziałania cyberprzemocy oraz zagrożeń wynikających z kontaktu z innymi użytkownikami sieci. Natomiast brak właściwej orientacji ujawnił się w zakresie prawa autorskiego, a szczególnie w kontekście: legalności użytkowanego oprogramowania, wykorzystania materiałów multimedialnych w procesie edukacyjnym oraz moralnej oceny pobierania w sposób „nielegalny" plików z sieci.

Elementem wymagającym szczególnej uwagi jest wzmacnianie kompetencji związanych z wykonywaniem przez młode osoby operacji finansowych w sieci. Niewątpliwie korzystne edukacyjnie byłoby rozbudowanie programu kształcenia o tematykę techniczno-społecznych kwestii zakupów i transferów w sieci.

Grupa	ŚREDNI WYNIK	N – ilość osób objętych badaniem	WIARYGODNOŚĆ INFORMACJI DOSTĘPNYCH W INTERNECIE	BEZPIECZEŃSTWO W KONTAKCIE Z INNYMI UŻYTKOWNIKAMI SIECI	BEZPIECZEŃSTWO WIZERUNKU W INTERNECIE	PRAWO AUTORSKIE	CYBERPRZEMOC	OPERACJE FINANSOWE
Nauczyciele	53%	423	34,82%	72,97%	59,20%	43,61%	83,09%	49,48%
Rodzice	50%	632	49,42%	62,69%	54,09%	34,56%	75,45%	57,10%
Uczniowie	56%	3643	69,32%	66,23%	64,00%	24,05%	68,37%	32,61%

4.3.1 Uczniowie

Co czwarty uczeń podkreśla, że w jego szkole zdarzył się przypadek związany z naruszeniem bezpieczeństwa cyfrowego. Jednak ponad połowa uczniów nie jest w stanie udzielić jednoznacznie odpowiedzi lub nie potrafi przełożyć terminu „bezpieczeństwo cyfrowe" na konkretne zagrożenia cyfrowe.

Czy w Twojej szkole zdarzył się przypadek naruszenia bezpieczeństwa cyfrowego?

Odpowiedź	%	Liczba
Tak	26,76%	975
Nie	18,00%	656
Nie wiem	55,24%	2013

Niemalże co czwarty uczeń zauważył, że w szkole realizowane były działania związane z podnoszeniem bezpieczeństwa cyfrowego, np. w formie spotkań ze specjalistami, konkursów, warsztatów, czy też lekcji wychowawczych. Ponad połowa badanych nie była jednak w stanie udzielić

prawidłowej odpowiedzi na pytanie o programy edukacyjne i działania szkoły w zakresie profilaktyki zagrożeń cyfrowych.

Czy w Twojej szkole wdrożone są już jakieś programy i działania inne niż projekt Cyfrowobezpieczni.pl, mające na celu profilaktykę zagrożeń cyfrowych?

Odpowiedź	%	Liczba
Tak	27,83%	1014
Nie	17,32%	631
Nie wiem	54,86%	1999

Jedynie w jednej czwartej ankietowanych przypadków uczniowie mają ustalone reguły bezpiecznego użytkowania nowych mediów. Podobna ich liczba deklaruje, że ich zachowania zależne są od specyficznych okoliczności, a więc sytuacji niewpisujących się w żadne reguły. Z kolei ponad 42% uczniów nie ma ustalonych reguł w tym zakresie. Grupa ta wymaga szczególnego wsparcia edukacyjnego realizowanego w ramach projektu Cyfrowobezpieczni.pl.

Czy w domu są ustalone i przestrzegane zasady dotyczące używania Internetu (np. godziny używania sieci, rodzaj instalowanych programów, lista odwiedzanych stron)?

Odpowiedź	%	Liczba
Tak	25,54%	931
Nie	42,14%	1536
Zależy od sytuacji	28,01%	1021
Inne*	4,31%	157

Dialogowe formy wychowawcze realizowane są systematycznie jedynie wśród 25% ankietowanych uczniów. Prawie 40% uczniów nigdy nie rozmawia z rodzicami na temat zagrożeń w sieci.

Jak często Twoi rodzice rozmawiają z Tobą na temat zagrożeń związanych ze światem cyfrowym?

Odpowiedź	%	Liczba
codziennie	5,71%	208
raz w tygodniu	7,63%	278
raz w miesiącu	12,37%	451
raz na pół roku	19,37%	706
nigdy	38,13%	1390
inne*	16,79%	612

Jedynie 14,68% badanych uczniów gimnazjów nie potrafi ocenić poziomu kompetencji związanych z zagadnieniem zagrożeń cyfrowych. Z przekazu uczniów wynika, że ich rodzice (38%) cechują się

wysokim lub bardzo wysokim poziomem wiedzy i umiejętnościami pozwalającymi przeciwdziałać zagrożeniom cyfrowym. 16% cechuje się niskim i bardzo niskim wskaźnikiem kompetencji w analizowanym zakresie.

Jak oceniasz poziom kompetencji i wiedzy Twoich rodziców w zakresie występowania e-zagrożeń

Odpowiedź	%	Liczba
Bardzo wysoki	14,35%	523
Wysoki	23,95%	873
Średni	30,75%	1121
Niski	10,07%	367
Bardzo niski	6,20%	226
Nie potrafię ocenić	14,68%	535

Wśród uczniów gimnazjów samoocena własnego poziomu kompetencji w zakresie efektywnego korzystania z komputera i Internetu kształtuje się na bardzo wysokim poziomie. Niemalże co czwarty uczeń deklaruje, że jego umiejętności są zaawansowane.

Jak oceniasz poziom własnych kompetencji i wiedzy w zakresie obsługi urządzeń cyfrowych (komputer, internet)?

Odpowiedź	%	Liczba
Bardzo wysoki	22,63%	825
Wysoki	38,52%	1404
Średni	28,31%	1032
Niski	2,63%	96
Bardzo niski	1,29%	47
Nie potrafię ocenić	6,61%	241

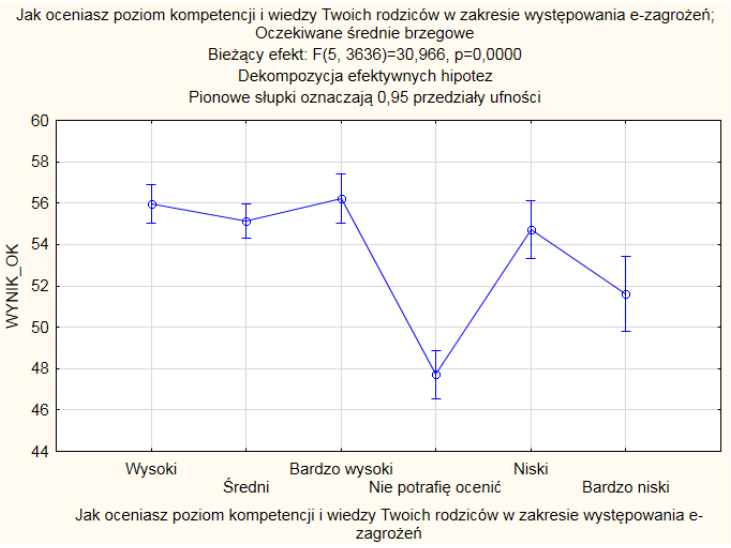
Inaczej rozkłada się w tej grupie badanych samoocena własnych umiejętności w zakresie obsługi mobilnych urządzeń cyfrowych, typu tablet i smartfon. Z deklaracji uczniów wynika, że jedynie 16% posiada kompetencje cyfrowe na poziomie średnim. Zdecydowana większość uczniów uznaje swoje kompetencje jako zaawansowane (poziom wysoki lub bardzo wysoki). Taki stosunek do własnych kompetencji w tym zakresie wiąże się zapewne z tym, że urządzenia mobilne stanowią najczęściej użytkowane przez młodzież urządzenia cyfrowe.

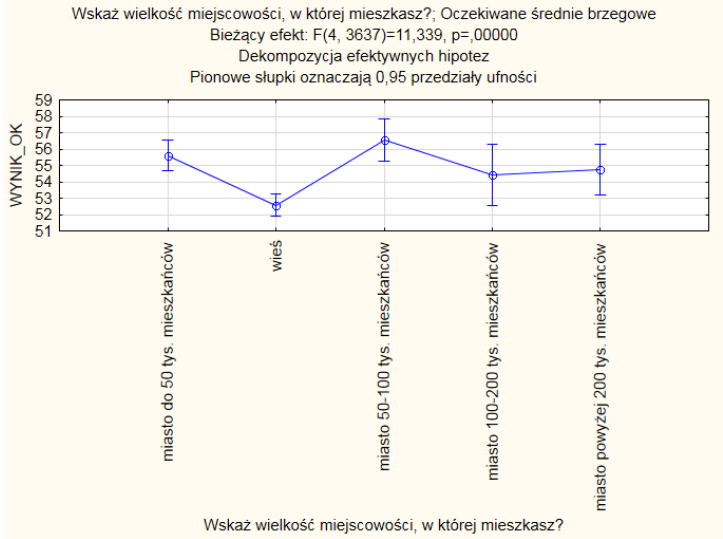
Jak oceniasz poziom własnych kompetencji i wiedzy w zakresie obsługi urządzeń cyfrowych typu tablet, smartfon?

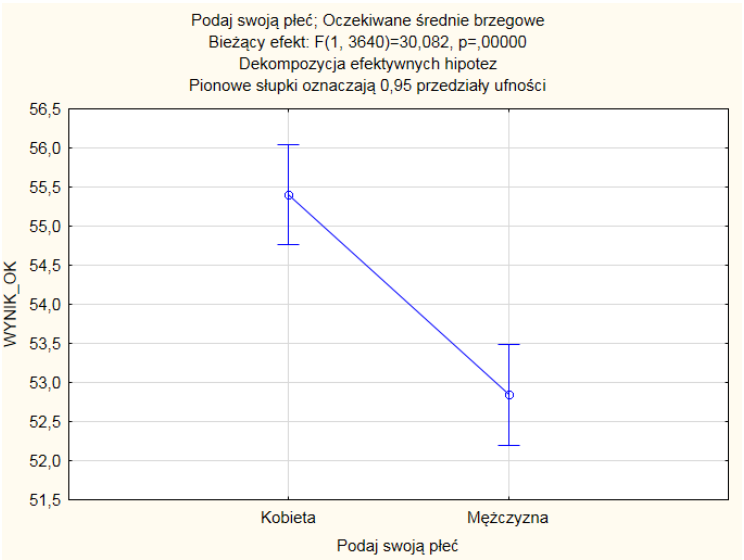
Odpowiedź	%	Liczba
Bardzo wysoki	38,02%	1386
Wysoki	37,59%	1370
Średni	16,95%	618
Niski	1,89%	69
Bardzo niski	1,21%	44
Nie potrafię ocenić	4,33%	158

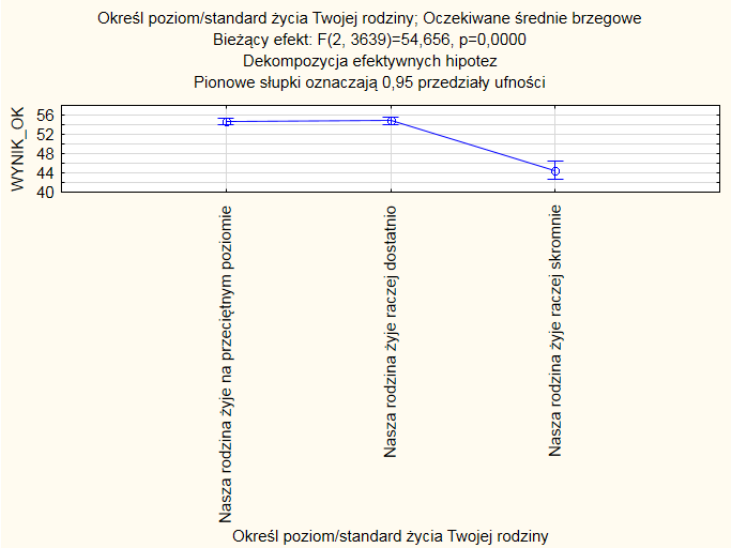
Kompetencje cyfrowe rodziców przekładają się na poziom bezpieczeństwa cyfrowego uczniów. Zależność ta nie jest co prawda znacząca, lecz zauważalna w analizie wyników badań. Ich miejsce zamieszkania również przekłada się na jakość kompetencji w zakresie zagrożeń cyfrowych. Mieszkańcy miast osiągają nieco wyższe wyniki w teście kompetencyjnym, niż pozostałe grupy badanych z obszarów wiejskich.

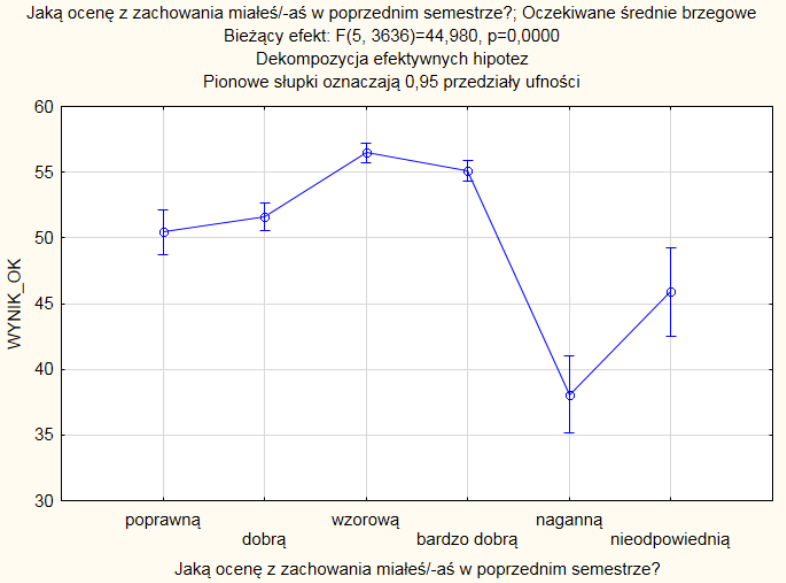
Interesująca zależność wyłania się, gdy weźmiemy pod uwagę minimalne różnice pomiędzy dziewczętami osiągającymi kilkupunktową przewagę nad chłopcami. Ocena zamożności własnej rodziny istotnie warunkuje poziom kompetencji informacyjno-medialnych, podobnie jak ich ocena z zachowania.




Wskaż wielkość miejscowości, w której mieszkasz?; Oczekiwane średnie brzegowe
Bieżący efekt: F(4, 3637)=11,339, p=,00000
Dekompozycja efektywnych hipotez
Pionowe słupki oznaczają 0,95 przedziały ufności
WYNIK_OK
59
58
57
56
55
54
53
52
51
miasto do 50 tys. mieszkańców
wieś
miasto 50-100 tys. mieszkańców
miasto 100-200 tys. mieszkańców
miasto powyżej 200 tys. mieszkańców
Wskaż wielkość miejscowości, w której mieszkasz?


Podaj swoją płeć; Oczekiwane średnie brzegowe
Bieżący efekt: F(1, 3640)=30,082, p=,00000
Dekompozycja efektywnych hipotez
Pionowe słupki oznaczają 0,95 przedziały ufności
WYNIK_OK
56,5
56,0
55,5
55,0
54,5
54,0
53,5
53,0
52,5
52,0
51,5
Kobieta
Mężczyzna
Podaj swoją płeć


Określ poziom/standard życia Twojej rodziny; Oczekiwane średnie brzegowe
Bieżący efekt: F(2, 3639)=54,656, p=0,0000
Dekompozycja efektywnych hipotez
Pionowe słupki oznaczają 0,95 przedziały ufności
WYNIK_OK
56
52
48
44
40
Nasza rodzina żyje na przeciętnym poziomie
Nasza rodzina żyje raczej dostatnio
Nasza rodzina żyje raczej skromnie
Określ poziom/standard życia Twojej rodziny



4.3.2 Rodzice

Ponad 11% rodziców twierdzi, że w gimnazjum, w którym uczy się jego dziecko, zdarzył się przypadek naruszenia bezpieczeństwa cyfrowego. Ponad 70% rodziców lub opiekunów nie jest w stanie określić, czy w środowisku szkolnym miały miejsce przypadki określane, jako zachowania ryzykowne związane z uczestnictwem uczniów w cyberprzestrzeni.

Czy w Państwa szkole zdarzył się przypadek naruszenia bezpieczeństwa cyfrowego?

Odpowiedź	%	Liczba
Tak	11,37%	73
Nie	18,38%	118
Nie wiem	70,25%	451

Ponad 22% rodziców deklaruje, że w jego szkole realizowane są programy przeciwdziałania zagrożeniom cyfrowym. Co dziesiąty uważa, że placówka edukacyjna nie podejmuje tego typu aktywności. Zdecydowana większość ankietowanych nie jest w stanie jednoznacznie określić, czy szkoła posiada rozwiązania w zakresie profilaktyki bezpieczeństwa cyfrowego.

Czy w Państwa szkole wdrożone są już jakieś programy i działania inne niż projekt Cyfrowobezpieczni.pl, mające na celu profilaktykę zagrożeń cyfrowych?

Odpowiedź	%	Liczba
Tak	22,27%	143
Nie	10,75%	69
Nie wiem	66,98%	430

Co drugi rodzic wskazuje, że w środowisku domowym są ustalone i przestrzegane zasady użytkowania mediów cyfrowych. Jedynie 8% deklaruje, że tego typu sytuacja nie ma miejsca. Co trzeci rodzic podkreśla, że przestrzeganie reguł jest determinowane kontekstem sytuacyjnym. Zmienność sytuacji wymusza przestrzeganie reguł lub ich tymczasowe unieważnienie.

Czy w domu są ustalone i przestrzegane zasady dotyczące używania Internetu przez dziecko (np. godziny używania sieci, rodzaj instalowanych programów, lista odwiedzanych stron)?

Odpowiedź	%	Liczba
Tak	50,16%	322
Nie	8,72%	56
Zależy od sytuacji	31,00%	199
Nie jestem w stanie skontrolować aktywności dziecka w Internecie	7,48%	48
Inne	2,65%	17

Kwestia znaczenia wychowawczego profilaktyki bezpieczeństwa cyfrowego poprzez rozmowy z dziećmi jest dostrzegalna we wskazaniach rodziców. Zdecydowana większość rodziców deklaruje, iż często rozmawia ze swoimi dziećmi na temat zagrożeń cyfrowych.

Jak często rozmawia Pan/Pani ze swoim dzieckiem na temat zagrożeń związanych ze światem cyfrowym?

Odpowiedź	%	Liczba
Codziennie	14,02%	90
raz w tygodniu	22,59%	145
raz w miesiącu	29,28%	188
raz na pół roku	12,93%	83
Nigdy	7,79%	50
inne*	13,40%	86

Jedynie co dwudziesty rodzic uczniów gimnazjów deklaruje, że posiada bardzo wysoki poziom wiedzy na temat zagrożeń cyfrowych. Z kolei już co piąty twierdzi, że tematyka zagrożeń cyfrowych jest mu znana w stopniu wysokim. Najliczniejsza grupa rodziców (51%) stwierdza, że ich poziom wiedzy jest zróżnicowany, lecz raczej oceniany jako średni.

Jak Pan/Pani ocenia poziom własnych kompetencji i wiedzy w zakresie wiedzy na temat występowania e-zagrożeń?

Odpowiedź	%	Liczba
Bardzo wysoki	5,30%	34
Wysoki	19,31%	124

Średni	51,09%	328
Niski	12,77%	82
Bardzo niski	3,43%	22
Nie potrafię ocenić	8,10%	52

Zaledwie co dziesiąty rodzic wyjawił, że posiada niski poziom kompetencji w tym obszarze. Co dwudziesty - nie potrafi zdiagnozować poziomu własnych kompetencji cyfrowych.

Jak Pan/Pani ocenia poziom własnych kompetencji i wiedzy w zakresie obsługi urządzeń cyfrowych (komputer, Internet)?

Odpowiedź	%	Liczba
Bardzo wysoki	8,10%	52
Wysoki	22,90%	147
Średni	50,62%	325
Niski	11,06%	71
Bardzo niski	1,71%	11
Nie potrafię ocenić	5,61%	36

Najwięcej osób deklaruje średni poziom samooceny własnych kompetencji związanych z obsługą urządzeń cyfrowych. Rozkład odpowiedzi w obszarze samooceny kompetencji zbliżony jest do rozkładu normalnego. Poniższe odpowiedzi są zbliżone do odpowiedzi dotyczących samooceny w zakresie efektywnego użytkowania komputera i Internetu.

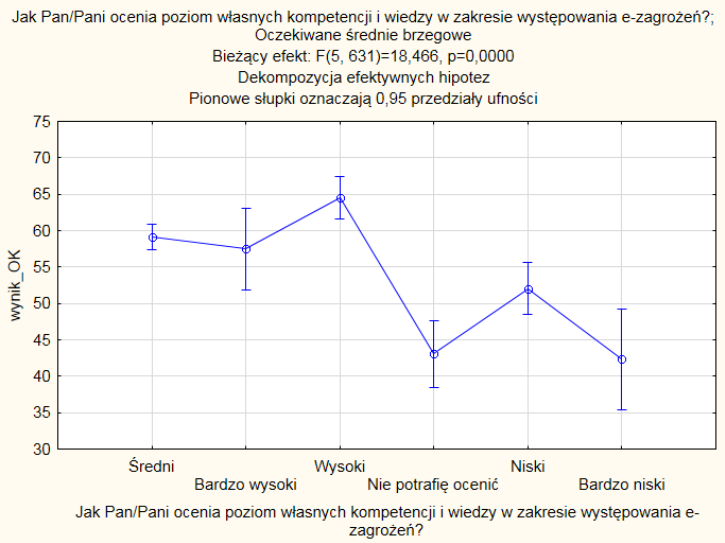
Jak Pan/Pani ocenia poziom własnych kompetencji i wiedzy w zakresie obsługi urządzeń cyfrowych typu tablet, smartfon?

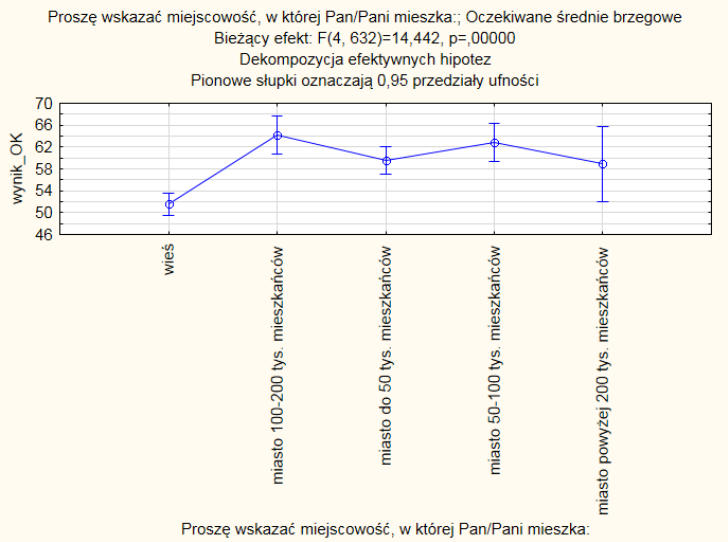
Odpowiedź	%	Liczba
Bardzo wysoki	9,03%	58
Wysoki	21,50%	138
Średni	49,84%	320
Niski	13,71%	88
Bardzo niski	1,87%	12
Nie potrafię ocenić	4,05%	26

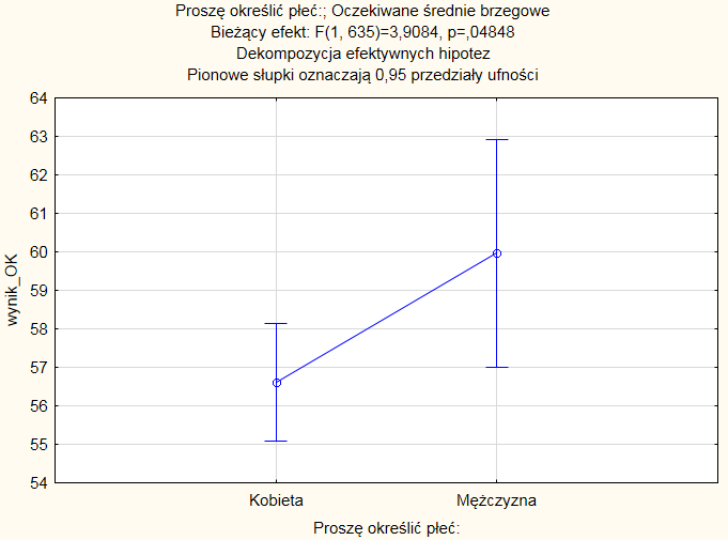
Analiza współzależności prowadzi do wniosku, że do kluczowych czynników determinujących poziom kompetencji związanych z bezpieczeństwem cyfrowym należy zaliczać takie zmienne niezależne, jak: rodzaj posiadanego wykształcenia, miejsce zamieszkania, samoocenę własnych kompetencji w analizowanym zakresie oraz płeć.

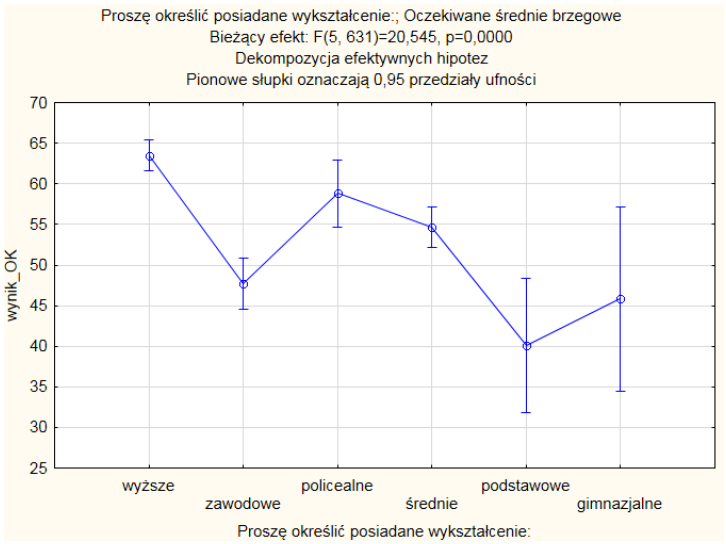
Wraz z deklarowanym poziomem własnych kompetencji cyfrowych, uzyskano wyższe wyniki w teście kompetencyjnym. Wiąże się to ze świadomością rodziców pożądanych sposobów użytkowania nowych technologii oraz ich wiedzą na temat potencjalnych zagrożeń cyfrowych.

Kobiety w grupie rodziców cechują się nieco niższym poziomem kompetencji cyfrowych niż mężczyźni. Zależność ta jest istotna statystycznie. Również miejsce zamieszkania determinuje poziom kompetencji cyfrowych. Czynnikiem równie istotnym jest wykształcenie rodziców. Osoby posiadające wyższe wykształcenie uzyskały o wiele wyższy wynik punktowy w teście kompetencyjnym, niż rodzice słabiej wykształceni.









4.3.3 Nauczyciele

Ankietowani nauczyciele gimnazjów posiadają większą od rodziców świadomość potrzeb profilaktyki edukacyjnej w zakresie zagrożeń cyfrowych oraz konkretnych przypadków naruszania bezpieczeństwa cyfrowego wśród uczniów. Wynika to ze stosunkowo niewielkiej wiedzy rodziców na temat funkcjonowania szkoły w zakresie bezpieczeństwa cyfrowego, a także bieżących zdarzeń w jej środowisku, o których nie zawsze są na bieżąco informowani przez nauczycieli i uczniów. Ponad 1/3 placówek szkolnych miała do czynienia z sytuacjami wymienionymi w części teoretycznej niniejszego raportu w ramach projektu Cyfrowobezpieczni.pl.

Czy w Państwa szkole zdarzył się przypadek naruszenia bezpieczeństwa cyfrowego?

Odpowiedź	%	Liczba
Tak	31,60%	134
Nie	28,30%	120
Nie wiem	40,09%	170

W ponad połowie szkół wdrożone zostały procedury związane z profilaktyką zachowań ryzykownych w zakresie e-zagrożeń. Należy podkreślić, że zainteresowanie nauczycieli tym obszarem zagadnień jest ograniczone. Aż co czwarty nauczyciel nie jest w stanie jednoznacznie określić, czy są w szkole prowadzone działania w tym zakresie.

Czy w Państwa szkole wdrożone są już jakieś programy i działania inne niż projekt Cyfrowobezpieczni.pl, mające na celu profilaktykę zagrożeń cyfrowych?

Odpowiedź	%	Liczba
Tak	53,30%	226
Nie	22,64%	96
Nie wiem	24,06%	102

Zdecydowana większość nauczycieli deklaruje, że w ich szkołach wprowadzono jednoznacznie ustalone reguły użytkowania nowych mediów i są one przestrzegane. Jedynie co dwudziesty nauczyciel twierdzi, że reguły te są uznaniowe, warunkowane okolicznościami. Ponadto ponad 6% twierdzi, iż nie jest w stanie wyegzekwować zakazu użytkowania telefonów komórkowych wśród swoich uczniów.

Czy w trakcie moich lekcji są ustalone i przestrzegane zasady dotyczące używania telefonów komórkowych?

Odpowiedź	%	Liczba
Tak	87,50%	371
Nie	0,47%	2
Zależy od sytuacji	4,48%	19
Nie jestem w stanie skontrolować aktywności wszystkich uczniów w trakcie lekcji	6,37%	27
Inne.*	1,18%	5

Tematyka zagrożeń cyfrowych jest regularnie obecna w procesie wychowawczym, realizowanym przez pedagogów na etapie edukacji gimnazjalnej. Zdecydowana większość nauczycieli deklaruje, że przynajmniej raz w miesiącu realizuje rozmowy wychowawcze o tej tematyce.

Jak często Pani/Pan rozmawia ze swoimi uczniami na temat e-zagrożeń?

Odpowiedź	%	Liczba
Nigdy o tym nie rozmawiamy	5,19%	22
Raz na semestr	36,32%	154
Raz na miesiąc	31,37%	133
Raz w tygodniu lub częściej	13,44%	57
Inne.*	13,68%	58

Nauczyciele oceniają najczęściej swój poziom wiedzy w zakresie zagrożeń cyfrowych jako średniozaawansowany. Niespełna co czwarty nauczyciel twierdzi, że czuje się pewnie (poziom wysoki) w tematyce e-zagrożeń. Z kolei 17% twierdzi, że ma w tym obszarze wiedzę niską albo bardzo niską. W szczególności ta grupa wymaga wsparcia edukacyjnego w ramach projektu Cyfrowobezpieczni.pl.

Jak Pani/Pan ocenia poziom własnych kompetencji i wiedzy w zakresie e-zagrożeń?

Odpowiedź	%	Liczba
Bardzo wysoki	3,77%	16
Wysoki	17,92%	76
Średni	57,78%	245
Niski	13,21%	56
Bardzo niski	4,01%	17
Nie potrafię ocenić	2,83%	12
Inne.*	0,47%	2

Nieco wyższy poziom samooceny własnych kompetencji cyfrowych w grupie nauczycieli odnosi się do efektywnego korzystania z komputera oraz Internetu. Poziom kompetencji własnych w tym aspekcie jest bardzo wysoko oceniany przez co dwudziestego nauczyciela gimnazjum. Natomiast co trzeci nauczyciel uważa, że dysponuje kompetencjami cyfrowymi na poziomie wysokim. Podobnie jak w poprzednim kryterium badawczym najliczniejszą grupę stanowią nauczyciele oceniający własne kompetencje na średnim poziomie.

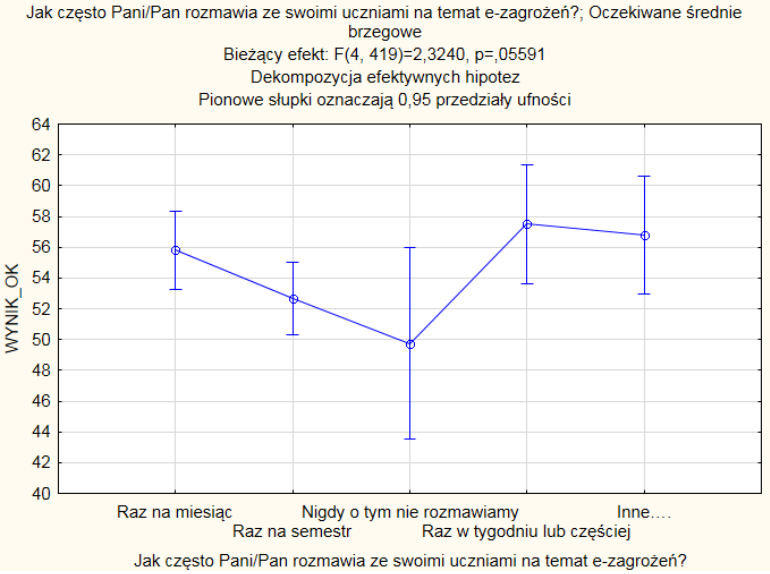
Jak Pani/Pan ocenia poziom własnych kompetencji i wiedzy w zakresie obsługi urządzeń cyfrowych (komputer, internet)?

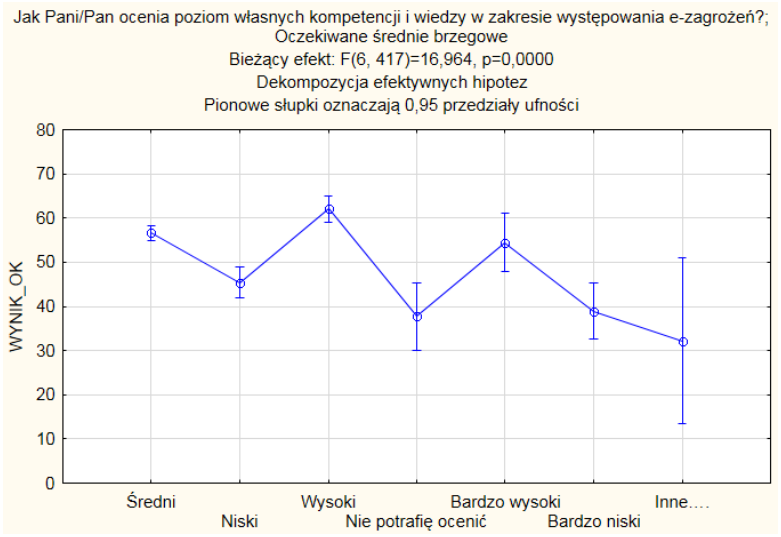
Odpowiedź	%	Liczba
Bardzo wysoki	5,90%	25
Wysoki	30,42%	129
Średni	53,30%	226
Niski	6,84%	29

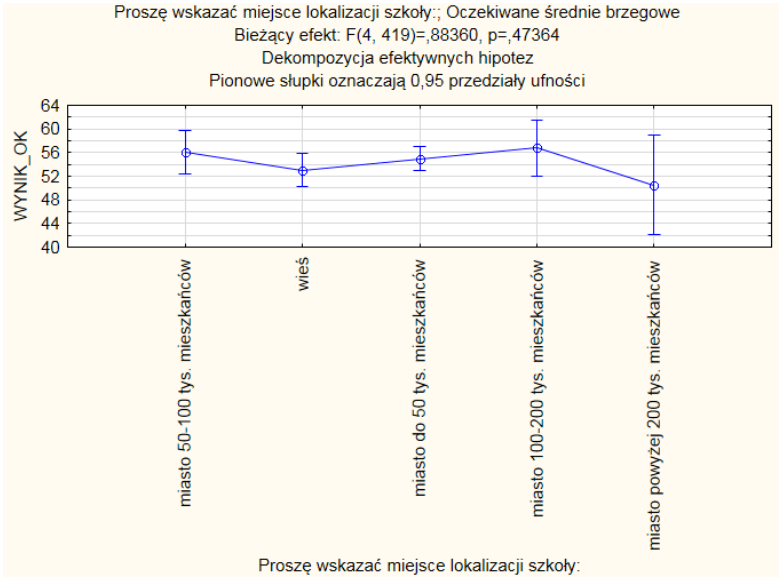
Bardzo niski	2,12%	9
Nie potrafię ocenić	0,94%	4
Inne*	0,47%	2

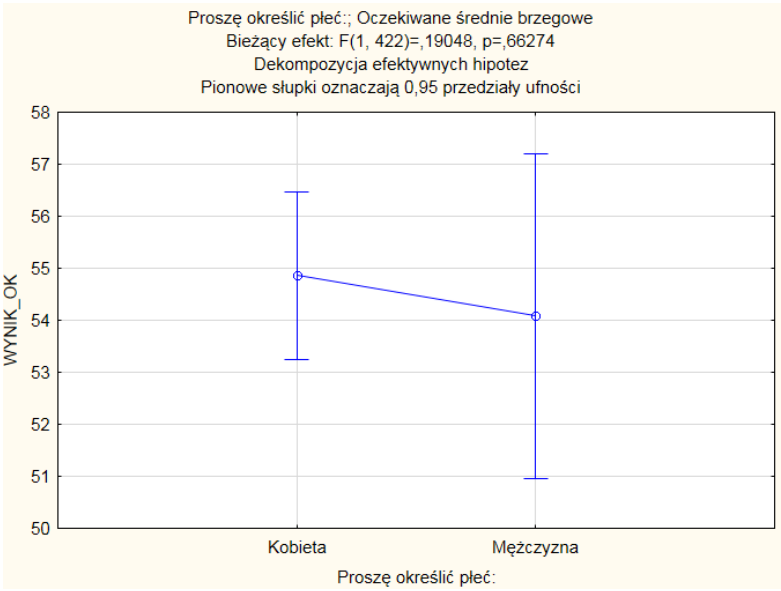
Analizując powyższe dane można zauważyć, iż nauczyciele gimnazjum podejmujący w trakcie lekcji zagadnienia związane z profilaktyką zachowań ryzykownych w przestrzeni mediów sieciowych osiągają wyższe wyniki w teście kompetencyjnym. Jednakże, zależność ta nie jest istotna statystycznie. Samoocena poziomu własnych umiejętności i wiedzy wśród nauczycieli przekłada się na wynik testu kompetencyjnego. Pedagodzy posiadający wyższą samoocenę równocześnie osiągają wyższe wyniki z testu.

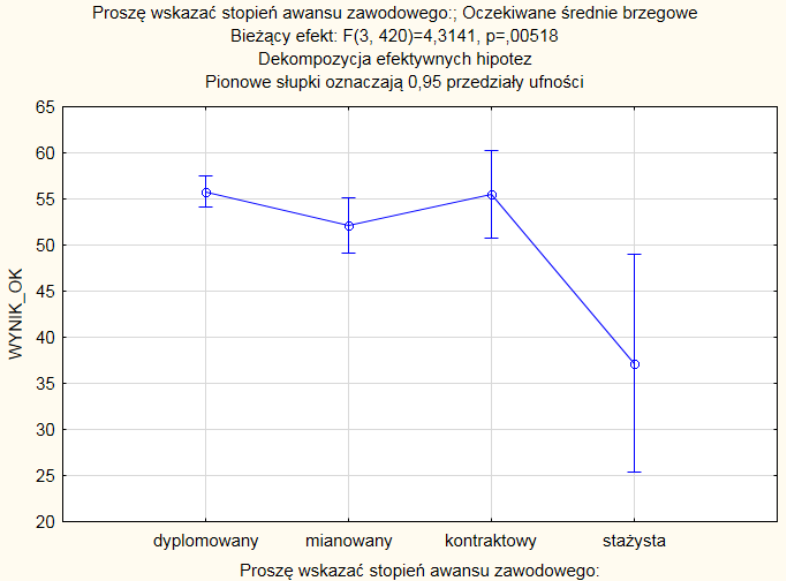
Miejsce lokalizacji gimnazjum w żaden sposób nie wpływa na wiedzę nauczycieli na temat zagrożeń cyfrowych. Podobny brak zależności występuje ze względu na płeć w tej grupie badanych. Natomiast stopień awansu zawodowego warunkuje wynik końcowy testu kompetencyjnego. Zjawisko to może być związane ze zgromadzonym doświadczeniem dydaktyczno-wychowawczym i przebytymi kursami.




Jak Pani/Pan ocenia poziom własnych kompetencji i wiedzy w zakresie występowania e-zagrożeń?;
Oczekiwane średnie brzegowe
Bieżący efekt: F(6, 417)=16,964, p=0,0000
Dekompozycja efektywnych hipotez
Pionowe słupki oznaczają 0,95 przedziały ufności
WYNIK_OK
80
70
60
50
40
30
20
10
0
Średni
Wysoki
Bardzo wysoki
Inne....
Niski
Nie potrafię ocenić
Bardzo niski

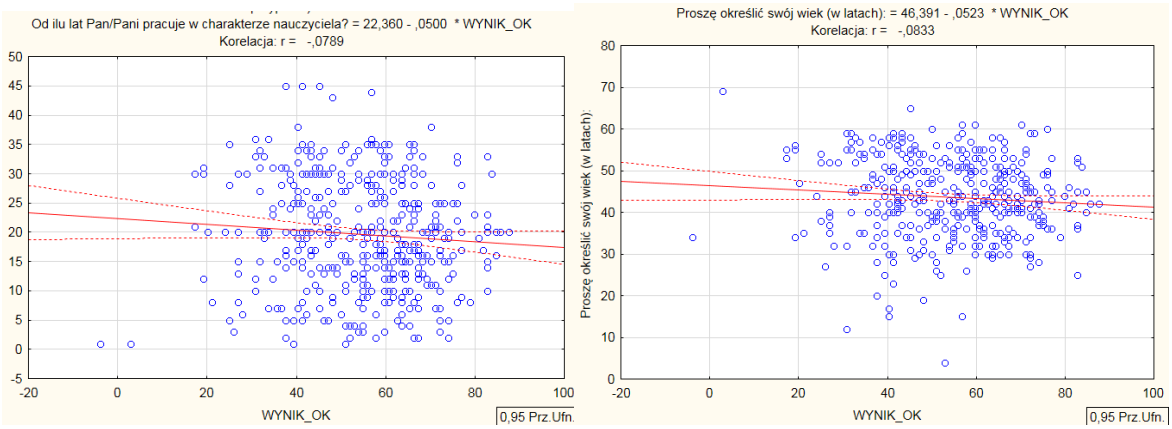

Proszę wskazać miejsce lokalizacji szkoły:; Oczekiwane średnie brzegowe
Bieżący efekt: F(4, 419)=,88360, p=,47364
Dekompozycja efektywnych hipotez
Pionowe słupki oznaczają 0,95 przedziały ufności
WYNIK_OK
64
60
56
52
48
44
40
miasto 50-100 tys. mieszkańców
wieś
miasto do 50 tys. mieszkańców
miasto 100-200 tys. mieszkańców
miasto powyżej 200 tys. mieszkańców
Proszę wskazać miejsce lokalizacji szkoły:


Proszę określić płeć:; Oczekiwane średnie brzegowe
Bieżący efekt: F(1, 422)=,19048, p=,66274
Dekompozycja efektywnych hipotez
Pionowe słupki oznaczają 0,95 przedziały ufności
WYNIK_OK
58
57
56
55
54
53
52
51
50
Kobieta
Mężczyzna
Proszę określić płeć:



Nie występuje jednoznaczna korelacja pomiędzy wynikami w teście kompetencyjnym, a stażem pracy oraz wiekiem.

Analiza wyników badań prowadzi do wniosku o zasadności objęcia wsparciem edukacyjnym w ramach projektu Cyfrowobezpieczni.pl. szkół usytuowanych na wsi wiejskich i w mniejszych miejscowościach, a także pedagogów w początkowym okresie zatrudnienia.



4.3.4 Wnioski i rekomendacje – gimnazjum

Na podstawie analizy danych dotyczących poziomu kompetencji związanych z bezpieczeństwem cyfrowym oraz uwzględnieniem szczegółowego ich odniesienia do szeregu zmiennych wskazujących na relację z poziomem bezpieczeństwa cyfrowego, można sformułować szereg postulatów, pozwalających na wyprofilowanie działań minimalizujących zagrożenia cyfrowe wśród uczniów, rodziców i nauczycieli.

Najważniejsze wnioski i rekomendacje:

1. Uczniowie, rodzice oraz nauczyciele z gimnazjum charakteryzują się średnim poziomem kompetencji informacyjno-medialnych w zakresie zagrożeń cyfrowych.
2. Zagadnienia cyberprzemocy na stałe wpisały się w programy profilaktyki szkolnej. Nauczyciele coraz częściej posiadają doświadczenia związane z przeciwdziałaniem i rozwiązywaniem problemów z cyberprzemocą. Jest to efekt rozwijania kompetencji informacyjno-medialnych i wychowawczych przez pedagogów realizujących działania wśród cyfrowych autochtonów. Niemniej jednak rozwój nowych technologii wymusza na pedagogach dokształcanie się, również w zakresie nowych form i możliwości technicznych przeciwdziałania cyberprzemocy. Koresponduje to z ujęciami tego zjawiska przez znanych badaczy pedagogiki mediów (Pyżalski, 2011; Pyżalski, 2012) oraz szczególnym zainteresowaniem instytucji kreujących rozwiązania sprzyjające podnoszeniu poziomu bezpieczeństwa w szkole (NIK, Kuratoria Oświaty, Fundacja Dzieci Niczyje – Dajemy Dzieciom Siłę).
3. Szczególnego wsparcia edukacyjnego wymagają badani w zakresie prawa autorskiego, co ujawnia się m.in. w postaci braków podstawowej wiedzy dotyczącej pobierania pików (oprogramowania oraz materiałów audiowizualnych).
4. Tej samej rangi obszar tematyczny, który wymaga wsparcia edukacyjnego to zakupy przez Internet. Chodzi o praktyczną umiejętność sprawdzania wiarygodności sprzedawców, technicznych aspektów funkcjonowania stron internetowych wymagających podania danych poufnych.
5. Elementem programowym wymagającym wsparcia edukacyjnego jest również tematyka ochrony danych związanych z kreowaniem wizerunku w sieci. Należy tutaj zwrócić szczególną uwagę na składowe wizerunku oraz mechanizmy związane z powielaniem danych (zob. Tomczyk, Kopecky, 2016) za pomocą usług sieciowych.
6. Niemalże połowa nauczycieli podkreśla, że w ich szkole brakuje wiedzy na temat systemowych rozwiązań wzmacniających kompetencje w zakresie zagrożeń cyfrowych.
7. Co czwarty nauczyciel ocenia własne kompetencje cyfrowe, jako niskie lub bardzo niskie, co znajduje wyraz w wynikach testu kompetencyjnego nt. profilaktyki, mechanizmów i działań minimalizujących zagrożenia elektroniczne. Grupa ta wymaga szczególnej uwagi w ramach projektowania przyszłych działań edukacyjnych w ramach projektu Cyfrowobezpieczni.pl.
8. Ze względu na najniższe wyniki testu kompetencyjnego grupą wymagającą szczególnego wsparcia edukacyjnego są nauczyciele stażyści. Niskie kompetencje cyfrowe powiązane są w tym przypadku z niewystarczającym przygotowaniem w zakresie edukacji medialnej (Tomczyk et. al., 2015), realizowanej w toku studiów wyższych. Nauczyciele podejmujący pracę, zazwyczaj są osobami kończącymi studia kierunkowe z kilkuset godzinnym przygotowaniem pedagogicznym, które nie obejmuje zagadnień bezpieczeństwa cyfrowego.

Istnieje zatem konieczność przygotowania nie tylko jednorazowych kursów, lecz również - jak postulują nauczyciele - materiałów dydaktycznych umożliwiających im samokształcenie (np. w trybie online). Materiały te powinny obejmować treści dotyczące praktycznych aspektów dotyczących najczęściej pojawiających się sytuacji problemowych oraz sposobów przeciwdziałania i rozwiązywania problematyki bezpieczeństwa cyfrowego.

9. Ważne jest również wzmocnienie kompetencji wychowawczych rodziców oraz ukazanie różnych aspektów profilaktyki zagrożeń cyfrowych, w szczególności w grupach oceniających poziom własnych kompetencji informacyjno-medialnych jako bardzo niski, niski i średni.
10. Rodzice wykazują się relatywnie małą wiedzą i praktycznymi umiejętnościami przydatnymi do właściwego reagowania w sytuacjach problemowych związanych z ryzykownymi zachowaniami dzieci (uczniów szkół gimnazjalnych) w środowisku mediów sieciowych i szkolnym.
11. Szczególnym wsparciem edukacyjnym należy objąć grupę rodziców deklarujących faktyczną bezsilność wychowawczą w relacji z dziećmi (uczniami szkół gimnazjalnych), nieprzestrzegającymi reguł korzystania z nowych mediów.
12. Wyniki badań wskazują na zasadność wypracowania nowych treści i metod kształcenia (również w aspekcie edukacji pozaformalnej) podnoszących poziom kompetencji w zakresie zagrożeń cyfrowych oraz świadomości całokształtu ich znaczenia.
13. Rodzice posiadający niższe wykształcenie oraz mieszkający w mniejszych miejscowościach i na wsiach osiągają niższe wyniki testu kompetencyjnego, zatem grupa ta wymaga specjalnego wsparcia edukacyjnego.

4.4 Szkoła ponadgimnazjalna

Uczniowie, rodzice oraz nauczyciele związani ze szkołą ponadgimnazjalną cechują się zbliżonym poziomem kompetencji cyfrowych, jak analogiczne grupy na etapie edukacji gimnazjalnej. Osiągnięty średni wynik testu potwierdza hipotezę roboczą, iż kompetencje w zakresie zagrożeń cyfrowych wymagają wzmocnienia poprzez działania realizowane w ramach edukacji formalnej i pozaformalnej (takich jak projekt Cyfrowobezpieczni.pl), a także poprzez kreowanie rozwiązań umożliwiających samokształcenie.

Obszarem tematycznym wymagającym szczególnego wsparcia jest problematyka prawa autorskiego (m.in. związana z pobieraniem i udostępnianiem plików, użytkowaniem programów komputerowych dostępnych w sieci, zwiększaniem wiedzy na temat odpowiedzialności prawnej i finansowej).

W porównaniu z młodszą grupą uczniów, młodzież pobierająca naukę w szkole ponadgimnazjalnej cechuje się wyższym poziomem kompetencji cyfrowych związanych z operacjami finansowymi.

Relatywnie wysokim poziomem kompetencji związanych z przeciwdziałaniem cyberprzemocy charakteryzują się pedagodzy, a nieco mniejszym rodzice oraz uczniowie. Kwestią wymagającą szczególnej uwagi jest przygotowanie programów kształcenia oraz działań edukacyjnych podwyższających poziom bezpieczeństwa cyfrowego w zakresie oceny wiarygodności informacji (wszystkie trzy grupy) oraz ochrony wizerunku uczniów w sieci.

Grupa	ŚREDNI WYNIK	N – ilość osób objętych badaniem	WIARYGODNOŚĆ INFORMACJI DOSTĘPNYCH W INTERNECIE	BEZPIECZEŃSTWO W KONTAKCIE Z INNYMI UŻYTKOWNIKAMI SIECI	BEZPIECZEŃSTWO WIZERUNKU W INTERNECIE	PRAWO AUTORSKIE	CYBERPRZEMOC	OPERACJE FINANSOWE
Nauczyciele	54%	257	48,01%	44,40%	73,45%	49,41%	73,65%	61,02%
Rodzice	52%	260	56,06%	43,33%	68,51%	38,58%	64,18%	56,92%
Uczniowie	52%	1787	62,72%	59,69%	54,15%	32,21%	57,16%	63,19%

4.4.1 Uczniowie

Niemalże co drugi z ankietowanych uczniów szkół ponadgimnazjalnych potwierdza, że w jego szkole zdarzył się przypadek naruszenia bezpieczeństwa cyfrowego. W toku testowania narzędzia badawczego uczniowie podkreślali, że naruszenie bezpieczeństwa cyfrowego kojarzy im się z sytuacją krytyczną mającą miejsce w sieci lub zainicjowaną wydarzeniem w sieci, której powaga i możliwe konsekwencje wymagają interwencji osób dorosłych cieszących się ich zaufaniem.

Czy w Twojej szkole zdarzył się przypadek naruszenia bezpieczeństwa cyfrowego?

Odpowiedź	%	Liczba
Tak	18,20%	336
Nie	29,14%	538
Nie wiem	52,65%	972

W szkołach uczestniczących w badaniu zajęcia związane z podnoszeniem poziomu bezpieczeństwa cyfrowego zostały ocenione jako przydatne przez 23% uczniów. Przydatność tych zajęć wiąże się ze spełnieniem kryterium powiązania treści kształcenia z tematyką zagrożeń cyfrowych. Zdecydowana

większość uczniów nie jest w stanie powiedzieć, czy w szkole są realizowane inne działania edukacyjne w zakresie e-zagrożeń, niezwiązane merytorycznie z projektem „Cyfrowobezpieczni.pl". Prowadzi to do wniosku, że nauczyciele w tych szkołach nie angażują się w organizowanie zajęć i różnych form edukacyjnych podejmujących problematykę bezpieczeństwa cyfrowego.

Czy w Twojej szkole wdrożone są już jakieś programy i działania inne niż projekt Cyfrowobezpieczni.pl, mające na celu profilaktykę zagrożeń cyfrowych?

Odpowiedź	%	Liczba
Tak	23,40%	432
Nie	21,02%	388
Nie wiem	55,58%	1026

Ponad połowa ankietowanych uczniów przyznaje, że rodzice nie wyznaczają im zasad określających szczegółowe sposoby użytkowania mediów cyfrowych. Natomiast około jedna trzecia twierdzi, że aktywność rodziców w tym zakresie jest wymuszona sytuacjami trudnymi wymagającymi ich interwencji pedagogicznej.

Czy w domu są ustalone i przestrzegane zasady dotyczące używania Internetu (np. godziny używania sieci, rodzaj instalowanych programów, lista odwiedzanych stron)?

Odpowiedź	%	Liczba
Tak	15,71%	290
Nie	53,52%	988
Zależy od sytuacji	27,36%	505
Inne*	3,41%	63

Połowa ankietowanych uczniów twierdzi, iż ich rodzice nigdy nie rozmawiali z nimi na temat zagrożeń związanych ze światem cyfrowym. Podniesienie poziomu wiedzy rodziców w zakresie zagrożeń cyfrowych wydaje się jednym z kluczowych czynników zwiększających bezpieczeństwo współczesnego uczniów.

Jak często Twoi rodzice rozmawiają z Tobą na temat zagrożeń związanych ze światem cyfrowym?

Odpowiedź	%	Liczba
Codziennie	6,07%	112
raz w tygodniu	5,53%	102
raz w miesiącu	11,21%	207
raz na pół roku	19,45%	359
Nigdy	47,18%	871
inne*	10,56%	195

Rozkład oceny poziomu kompetencji cyfrowych rodziców na temat e-zagrożeń przyjmuje postać zbliżoną do rozkładu normalnego w populacji. Niespełna 30% uczniów deklaruje, że ich rodzice lub opiekunowie prawni dysponują wysokim poziomem wiedzy i umiejętności pozwalających na podnoszenie poziomu bezpieczeństwa cyfrowego.

Jak oceniasz poziom kompetencji i wiedzy Twoich rodziców w zakresie występowania e-zagrożeń?

Odpowiedź	%	Liczba
Bardzo wysoki	9,75%	180
Wysoki	19,83%	366
Średni	33,37%	616
Niski	13,33%	246
Bardzo niski	9,05%	167
Nie potrafię ocenić	14,68%	271

Deklarowany poziom samooceny kompetencji w zakresie obsługi komputera i Internetu tworzy obraz świadczący o tym, iż młodzież w wieku ponadgimnazjalnym jest dobrze praktycznie przygotowana do efektywnego korzystania z urządzeń cyfrowych. Jedynie 6% respondentów ocenia własne umiejętności, jako niskie lub bardzo niskie.

Jak oceniasz poziom własnych kompetencji i wiedzy w zakresie obsługi urządzeń cyfrowych (komputer, internet)?

Odpowiedź	%	Liczba
Bardzo wysoki	21,51%	397
Wysoki	36,40%	672
Średni	30,50%	563
Niski	4,66%	86
Bardzo niski	1,52%	28
Nie potrafię ocenić	5,42%	100

Podobnie do wyników uzyskanych w grupie uczniów w wieku gimnazjalnym, odsetek odpowiedzi w grupie uczniów ze szkół ponadgimnazjalnych, którzy oceniają własne kompetencje informacyjno-medialne na wysokim i bardzo wysokim poziomie jest zbliżony do wyników w grupie gimnazjalistów. Najwyższa samoocena uczniów odnosi się korzystania z urządzeń mobilnych typu smartfon, czy też tablet. Urządzenia te są obecnie najbardziej popularne i najczęściej wykorzystywane przez młodzież. Dane te potwierdzają roboczą hipotezę zakładającą zachodzenie relacji pomiędzy częstotliwością korzystania z urządzeń cyfrowych, a samooceną poziomu kompetencji cyfrowych.

Jak oceniasz poziom własnych kompetencji i wiedzy w zakresie obsługi urządzeń cyfrowych typu tablet, smartfon?

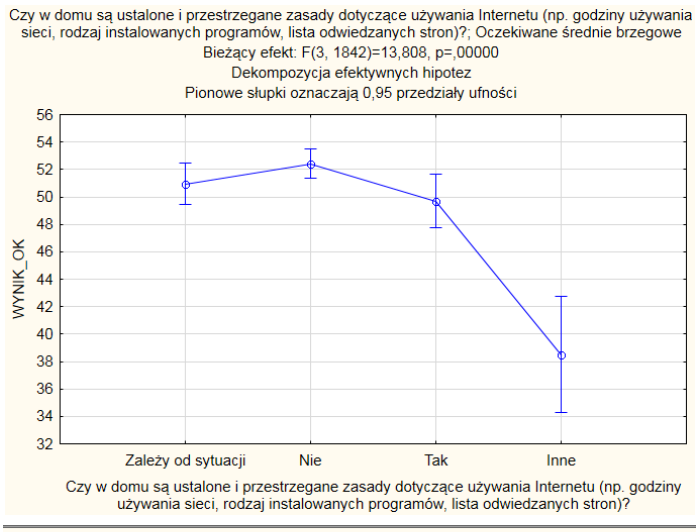
Odpowiedź	%	Liczba
Bardzo wysoki	34,07%	629
Wysoki	41,28%	762
Średni	16,03%	296
Niski	2,93%	54
Bardzo niski	1,73%	32
Nie potrafię ocenić	3,95%	73

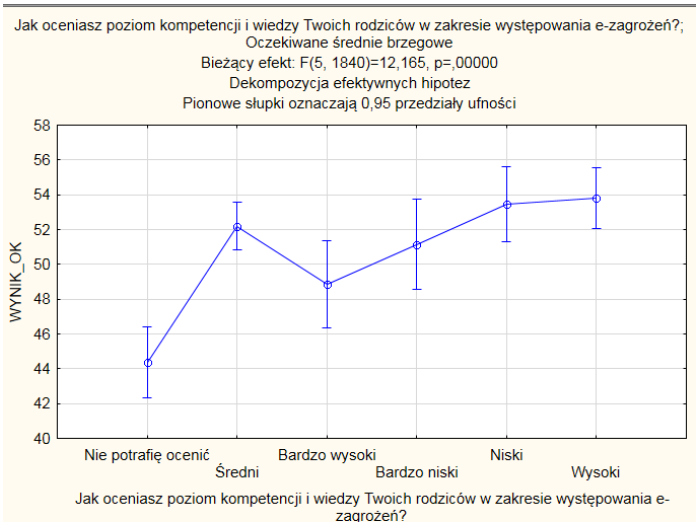
Kontrola rodzicielska uczniów w wieku ponadgimnazjalnym, związana ze sposobami użytkowania mediów cyfrowych, nie wpływa na wyniki testu kompetencyjnego uczniów dotyczącego bezpieczeństwa cyfrowego. Ocena poziomu kompetencji cyfrowych rodziców w opiniach uczniów nie znajduje przełożenia na wyniki dotyczące ich poziomu e-kompetencji.

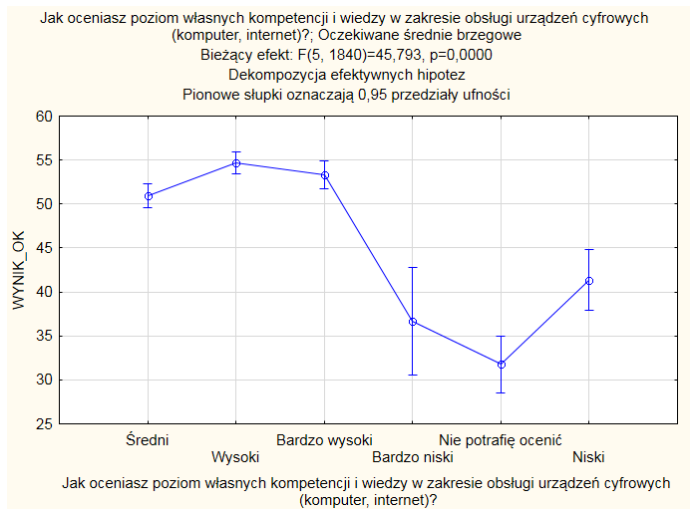
Należy jednak podkreślić, że poziom samooceny własnych kompetencji w zakresie użytkowania komputera i Internetu przekłada się istotnie statystycznie na wynik testu kompetencyjnego. Osoby deklarujące wysoki poziom wiedzy i umiejętności osiągnęły wyższe wyniki w teście sprawdzającym poziom kompetencji związanych z zagrożeniami cyfrowymi.

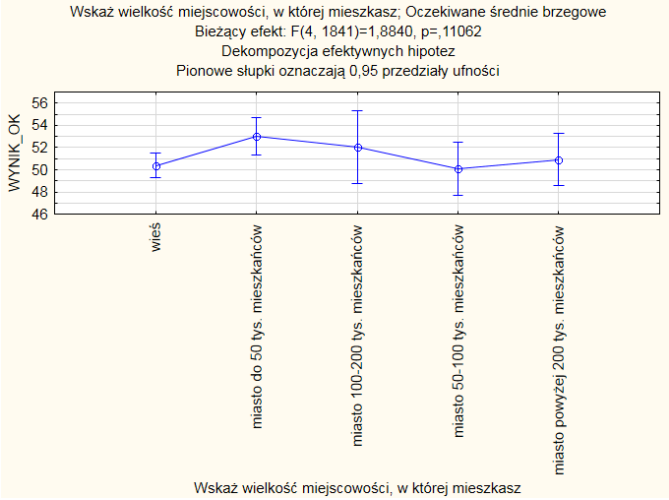
Z kolei miejsce lokalizacji szkoły nie determinuje istotnie statystycznie poziomu kompetencji, jednakże uczniowie z mniejszych miejscowości osiągnęli w teście średnio niższe wyniki, niż pozostałe grupy. Wyniki testów nie są istotnie statystycznie powiązane z płcią (różnice pomiędzy średnimi wartościami są mało istotne).

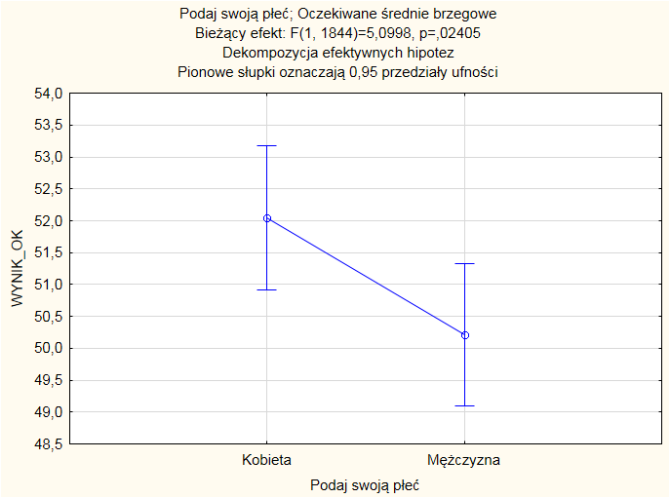
Znaczenie ma natomiast sytuacja materialna rodziny, która warunkuje poziom wyników testu kompetencyjnego w obszarze bezpieczeństwa cyfrowego. Osoby z mniej zamożnych rodzin osiągają mniej korzystny wynik końcowy z testu. Istnieje zależność między wysokimi wynikami testu kompetencyjnego a wysokimi ocenami z zachowania, jednakże zależność ta posiada wiele zmiennych pośredniczących nieuwzględnionych w niniejszym badaniu.

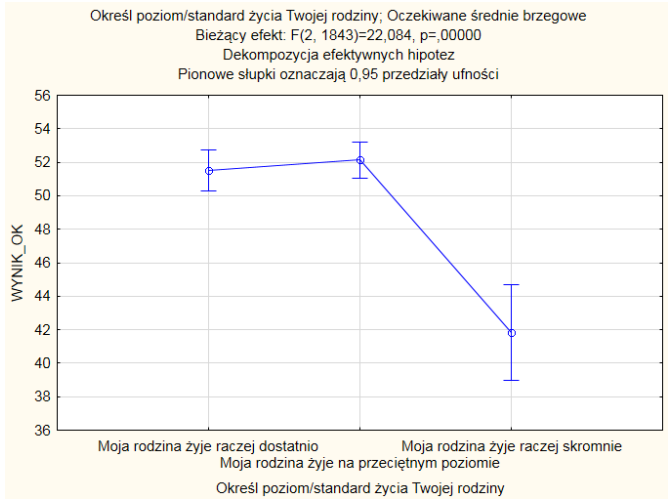

Czy w domu są ustalone i przestrzegane zasady dotyczące używania Internetu (np. godziny używania sieci, rodzaj instalowanych programów, lista odwiedzanych stron)?; Oczekiwane średnie brzegowe
Bieżący efekt: F(3, 1842)=13,808, p=,00000
Dekompozycja efektywnych hipotez
Pionowe słupki oznaczają 0,95 przedziały ufności
WYNIK_OK
56
54
52
50
48
46
44
42
40
38
36
34
32
Zależy od sytuacji
Nie
Tak
Inne
Czy w domu są ustalone i przestrzegane zasady dotyczące używania Internetu (np. godziny używania sieci, rodzaj instalowanych programów, lista odwiedzanych stron)?

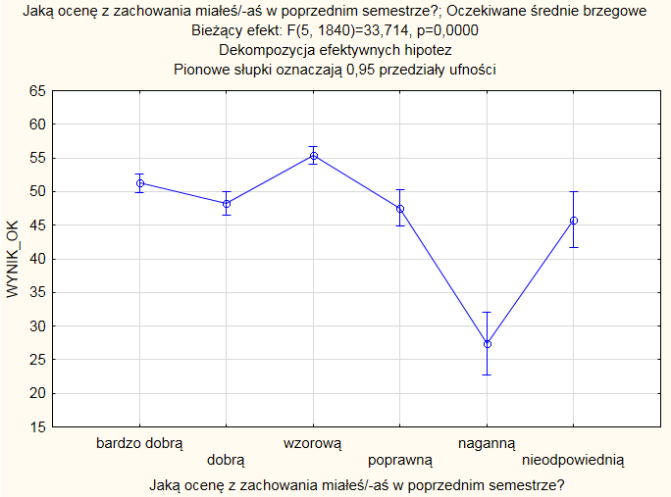

Jak oceniasz poziom kompetencji i wiedzy Twoich rodziców w zakresie występowania e-zagrożeń?; Oczekiwane średnie brzegowe
Bieżący efekt: F(5, 1840)=12,165, p=,00000
Dekompozycja efektywnych hipotez
Pionowe słupki oznaczają 0,95 przedziały ufności
WYNIK_OK
58
56
54
52
50
48
46
44
42
40
Nie potrafię ocenić
Średni
Bardzo wysoki
Bardzo niski
Niski
Wysoki
Jak oceniasz poziom kompetencji i wiedzy Twoich rodziców w zakresie występowania e-zagrożeń?


Jak oceniasz poziom własnych kompetencji i wiedzy w zakresie obsługi urządzeń cyfrowych (komputer, internet)?; Oczekiwane średnie brzegowe
Bieżący efekt: F(5, 1840)=45,793, p=0,0000
Dekompozycja efektywnych hipotez
Pionowe słupki oznaczają 0,95 przedziały ufności
WYNIK_OK
60
55
50
45
40
35
30
25
Średni
Wysoki
Bardzo wysoki
Bardzo niski
Nie potrafię ocenić
Niski
Jak oceniasz poziom własnych kompetencji i wiedzy w zakresie obsługi urządzeń cyfrowych (komputer, internet)?


Wskaż wielkość miejscowości, w której mieszkasz; Oczekiwane średnie brzegowe
Bieżący efekt: F(4, 1841)=1,8840, p=,11062
Dekompozycja efektywnych hipotez
Pionowe słupki oznaczają 0,95 przedziały ufności
WYNIK_OK
56
54
52
50
48
46
wieś
miasto do 50 tys. mieszkańców
miasto 100-200 tys. mieszkańców
miasto 50-100 tys. mieszkańców
miasto powyżej 200 tys. mieszkańców
Wskaż wielkość miejscowości, w której mieszkasz


Podaj swoją płeć; Oczekiwane średnie brzegowe
Bieżący efekt: F(1, 1844)=5,0998, p=,02405
Dekompozycja efektywnych hipotez
Pionowe słupki oznaczają 0,95 przedziały ufności
WYNIK_OK
54,0
53,5
53,0
52,5
52,0
51,5
51,0
50,5
50,0
49,5
49,0
48,5
Kobieta
Mężczyzna
Podaj swoją płeć


Określ poziom/standard życia Twojej rodziny; Oczekiwane średnie brzegowe
Bieżący efekt: F(2, 1843)=22,084, p=,00000
Dekompozycja efektywnych hipotez
Pionowe słupki oznaczają 0,95 przedziały ufności
WYNIK_OK
56
54
52
50
48
46
44
42
40
38
36
Moja rodzina żyje raczej dostatnio
Moja rodzina żyje raczej skromnie
Moja rodzina żyje na przeciętnym poziomie
Określ poziom/standard życia Twojej rodziny



4.4.2 Rodzice

Zdecydowana większość rodziców uczniów ze szkół ponadgimnazjalnych nie jest w stanie ocenić, czy w szkole ponadgimnazjalnej, do której uczęszcza ich dziecko zdarzył się przypadek naruszenia bezpieczeństwa cyfrowego. Świadczy to o tym, że wraz z wyższym etapem szkolnym maleje zainteresowanie rodziców aktywnością ich dziecka w Internecie oraz w placówce edukacyjnej.

Czy w Państwa szkole zdarzył się przypadek naruszenia bezpieczeństwa cyfrowego?

Odpowiedź	%	Liczba
Tak	8,86%	24
Nie	31,37%	85
Nie wiem	59,78%	162

Jedynie 17% rodziców deklaruje, że wie iż w szkole jego dziecka wdrożone są procedury pozwalające na zwiększenie bezpieczeństwa cyfrowego. W sytuacji tak niskiego odsetka wypowiedzi wydaje się, że istnieje potrzeba podjęcia działań edukacyjnych mających na celu podwyższanie świadomości rodziców związanej z bezpieczeństwem cyfrowym w szkole.

Czy w Państwa szkole wdrożone są już jakieś programy i działania inne niż projekt Cyfrowobezpieczni.pl, mające na celu profilaktykę zagrożeń cyfrowych?

Odpowiedź	%	Liczba
Tak	17,34%	47
Nie	14,39%	39
Nie wiem	68,27%	185

Liczba odpowiedzi deklarujących wprowadzenie w szkole reguł związanych z użytkowaniem nowych mediów jest zauważalnie wyższa wśród rodziców w porównaniu z deklaracjami uczniów w tym samym pytaniu. Niemalże co piąty rodzic deklaruje, że jego dziecko nie ma w szkole ustalonych reguł związanych z użytkowaniem nowych mediów. Okazyjny model kontroli rodzicielskiej w jednej trzeciej przypadków warunkowany jest sytuacyjnie. Świadczy to o zmienności reguł wychowawczych dotyczących użytkowania nowych mediów, determinowanych ewentualnym wystąpieniem sytuacji trudnej, która wywołuje zwiększoną uwagę aktywnością młodego człowieka w sieci.

Czy w domu są ustalone i przestrzegane zasady dotyczące używania Internetu przez dziecko (np. godziny używania sieci, rodzaj instalowanych programów, lista odwiedzanych stron)?

Odpowiedź	%	Liczba
Tak	31,00%	84
Nie	18,08%	49
Zależy od sytuacji	34,32%	93
Nie jestem w stanie skontrolować aktywności dziecka w Internecie	15,50%	42
Inne	1,11%	3

Rozkład odpowiedzi dotyczących wprowadzania rozwiązań sprzyjających podnoszeniu bezpieczeństwa cyfrowego ,obejmujących formy dialogu wychowawczego w domu rodzinnym jest niezwykle zbliżony do rozkładu normalnego cech w środowisku społecznym. Wyniki te są zbliżone do wypowiedzi rodziców uczniów w wieku gimnazjalnym.

Jak często Pan/Pani rozmawia ze swoim dzieckiem na temat zagrożeń związanych ze światem cyfrowym?

Odpowiedź	%	Liczba
Codziennie	12,18%	33
raz w tygodniu	17,34%	47
raz w miesiącu	23,62%	64
raz na pół roku	22,14%	60
Nigdy	12,92%	35
inne*	11,81%	32

Zdecydowana większość rodziców ocenia poziom własnych kompetencji cyfrowych jako średni. Kilkanaście procent badanych dorosłych deklaruje, że posiada wysoki bądź niski poziom wiedzy i umiejętności w analizowanym zakresie. Warto jednak podkreślić, że deklaracja poziomu kompetencji informacyjno-medialnych nie ma jednoznacznego przełożenia na wyniki testu kompetencyjnego w grupie, która oceniła własne kompetencje jako bardzo wysokie.

Jak Pan/Pani ocenia poziom własnych kompetencji i wiedzy w zakresie zabezpieczenia się przed ryzykiem e-zagrożeń?

Odpowiedź	%	Liczba
Bardzo wysoki	9,59%	26
Wysoki	17,34%	47
Średni	42,07%	114
Niski	15,87%	43
Bardzo niski	6,64%	18
Nie potrafię ocenić	8,49%	23

Rodzice oceniają poziom własnych kompetencji związanych z użytkowaniem mediów cyfrowych na niższym poziomie, niż ich dzieci. Osiągnięcie wysokiego poziomu bezpieczeństwa cyfrowego wymaga rozwinięcia również kompetencji odnoszących się do użytkowania oprogramowania i sprzętu.

Jak Pan/Pani ocenia poziom własnych kompetencji i wiedzy w zakresie obsługi urządzeń cyfrowych (komputer, internet)?

Odpowiedź	%	Liczba
Bardzo wysoki	10,33%	28
Wysoki	22,51%	61
Średni	47,97%	130
Niski	9,96%	27
Bardzo niski	5,90%	16
Nie potrafię ocenić	3,32%	9

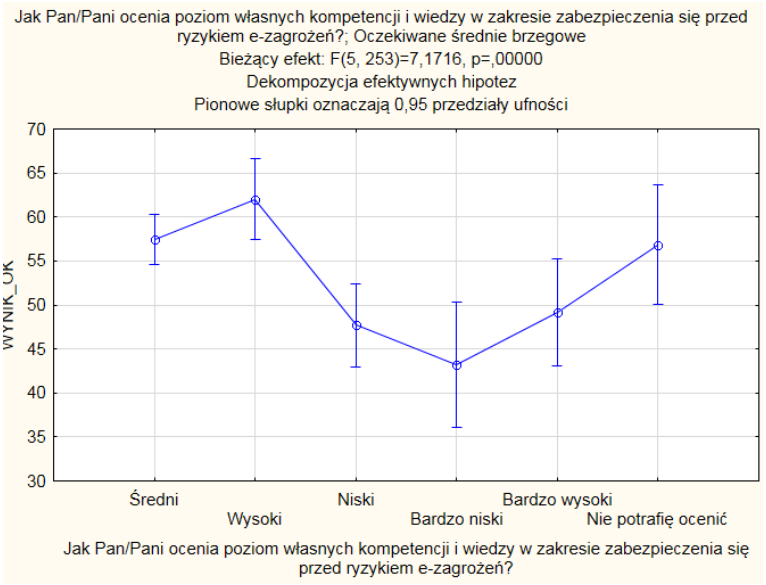
Podobny do powyższych rozkład odpowiedzi występuje w przypadku oceny użytkowania urządzeń mobilnych, takich jak tablet i smartfon. Różnica w tym aspekcie jest zauważalna głównie pomiędzy młodzieżą oraz rodzicami. Rodzice deklarują o wiele niższy poziom kompetencji użytkowania urządzeń typu tablet oraz smartfon. Może to wiązać się, z jednej strony, z mniejszym zakresem potrzeb korzystania z tych urządzeń przez rodziców, a z drugiej strony, z bardziej asekuracyjną oceną własnych kompetencji, niż ma to miejsce w przypadku młodzieży.

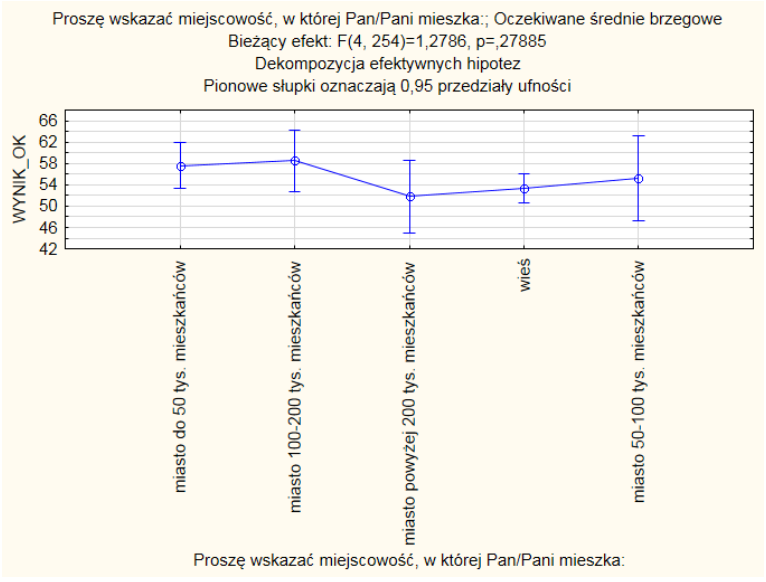
Jak Pani/Pan ocenia poziom własnych kompetencji i wiedzy w zakresie obsługi urządzeń cyfrowych typu tablet, smartfon?

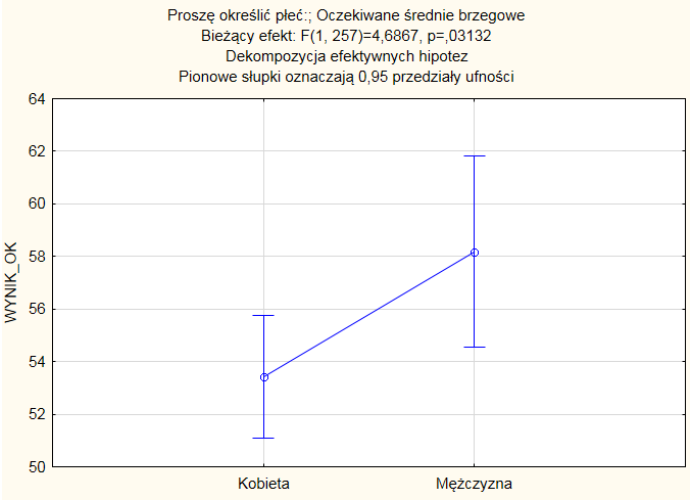
Odpowiedź	%	Liczba
Bardzo wysoki	12,92%	35
Wysoki	22,88%	62
Średni	44,65%	121

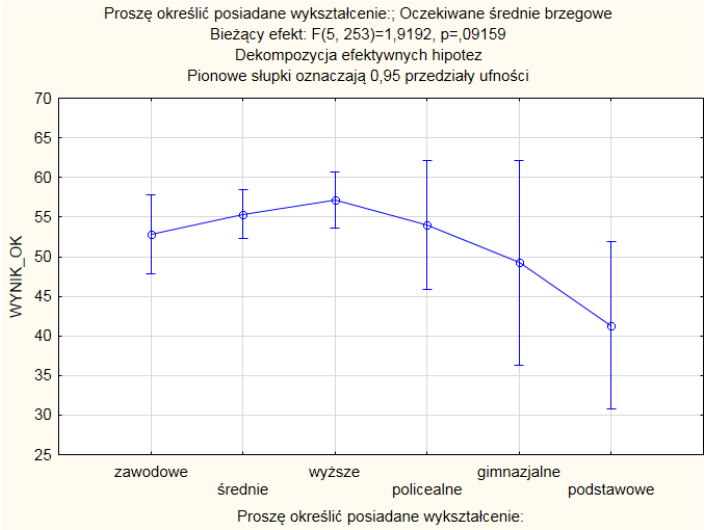
Niski	12,92%	35
Bardzo niski	4,06%	11
Nie potrafię ocenić	2,58%	7

Nie stwierdzono zależności między wynikami testu kompetencyjnego rodziców uczniów szkół ponadgimnazjalnych a ich miejscem zamieszkania. Wyniki testu kompetencyjnego w grupie rodziców uczniów szkół ponadgimnazjalnych kształtują się odmiennie, niż w grupie rodziców uczniów szkół gimnazjalnych. Ojcowie osiągają nieco wyższy wynik w teście kompetencyjnym, niż matki. Warto jednak zaznaczyć, że pomimo istotności statystycznej różnica wyników końcowych nie jest w tym przypadku szczególnie istotna. Wynik ten należy uwzględnić w projektowaniu działań edukacyjnych rozwijających kompetencje cyfrowe rodziców w kontekście minimalnych różnic w przedziale wartości średnich. Wynik testu kompetencyjnego jest warunkowany posiadanym wykształceniem, jednakże różnice te nie są istotne statystycznie.









4.4.3 Nauczyciele

Niemalże co piąty nauczyciel podkreśla, że w szkole zdarzył się przypadek naruszenia bezpieczeństwa cyfrowego. Ponad połowa nie jest jednak w stanie wypowiedzieć się lub sklasyfikować destruktywnych wydarzeń związanych z jego naruszaniem.

Czy w Państwa szkole zdarzył się przypadek naruszenia bezpieczeństwa cyfrowego?

Odpowiedź	%	Liczba
Tak	17,16%	46
Nie	28,73%	77
Nie wiem	54,10%	145

W zdecydowanej większości szkół nie wdrożono programów podwyższania poziomu bezpieczeństwa cyfrowego. Ponadto, niemalże połowa ankietowanych nauczycieli nie jest w stanie jednoznacznie

wypowiedzieć się, czy ich szkoła ma wdrożone systemowe działania w zakresie profilaktyki zagrożeń cyfrowych.

Czy w Państwa szkole wdrożone są już jakieś programy i działania inne niż projekt Cyfrowobezpieczni.pl, mające na celu profilaktykę zagrożeń cyfrowych?

Odpowiedź	%	Liczba
Tak	29,85%	80
Nie	26,87%	72
Nie wiem	43,28%	116

Zdecydowana większość nauczycieli podkreśla, że w trakcie lekcji obowiązują ustalone zasady związane z używaniem telefonów komórkowych. Z kolei co dziesiąty nauczyciel deklaruje, że nie jest w stanie skontrolować aktywności wszystkich uczniów w tym zakresie ich aktywności.

Czy w trakcie Pana/Pani lekcji są ustalone i przestrzegane zasady dotyczące używania telefonów komórkowych przez uczniów?

Odpowiedź	%	Liczba
Tak	71,64%	192
Nie	2,24%	6
Zależy od sytuacji	13,06%	35
Nie jestem w stanie skontrolować aktywności wszystkich uczniów w trakcie lekcji	11,19%	30
Inne.*	1,87%	5

Realizacja zajęć wychowawczych na temat bezpieczeństwa cyfrowego jest dla nauczycieli kwestią istotną, o czym świadczą wyniki badania zawarte w poniższej tabeli. Niemalże co czwarty nauczyciel rozmawia ze swoimi uczniami na temat zagrożeń elektronicznych średnio raz w miesiącu. Z kolei ok. 12% pedagogów zwraca uwagę, że dialog z uczniami na ten temat rozpoczyna się dopiero w przypadku wystąpienia sytuacji naruszenia bezpieczeństwa cyfrowego na terenie szkoły lub poza szkołą.

Jak często Pani/Pan rozmawia ze swoimi uczniami na temat e-zagrożeń?

Odpowiedź	%	Liczba
Nigdy o tym nie rozmawiamy	11,94%	32
Raz na semestr	41,42%	111
Raz na miesiąc	24,25%	65
Raz w tygodniu lub częściej	10,45%	28
Inne*	11,94%	32

Nauczyciele najczęściej oceniają poziom własnych kompetencji w aspekcie zagrożeń cyfrowych jako średni. Grupą, która wydaje się wymagać szerokozakresowego wsparcia edukacyjnego rozwijającego kompetencje cyfrowe są w szczególności: nauczyciele deklarujący niskie kompetencje (19%) oraz nauczyciele deklarujący bardzo niskie kompetencje (niespełna 5%).

Jak Pani/Pan ocenia poziom własnych kompetencji i wiedzy w zakresie występowania e-zagrożeń?

Odpowiedź	%	Liczba
Bardzo wysoki	3,73%	10
Wysoki	16,79%	45
Średni	48,51%	130
Niski	19,03%	51
Bardzo niski	4,85%	13
Nie potrafię ocenić	7,09%	19
Inne.	0,00%	0

Nauczyciele coraz częściej oceniają własne kompetencje związane z użytkowaniem urządzeń cyfrowych jako wysokie. Jest to związane z częstym udziałem w szkoleniach podnoszących kompetencje cyfrowe. Jedynie niespełna 12% nauczycieli podkreśla, że ich wiedza i umiejętności związane z użytkowaniem urządzeń cyfrowych są na niskim lub bardzo niskim poziomie.

Jak Pani/Pan ocenia poziom własnych kompetencji i wiedzy w zakresie obsługi urządzeń cyfrowych (komputer, internet)?

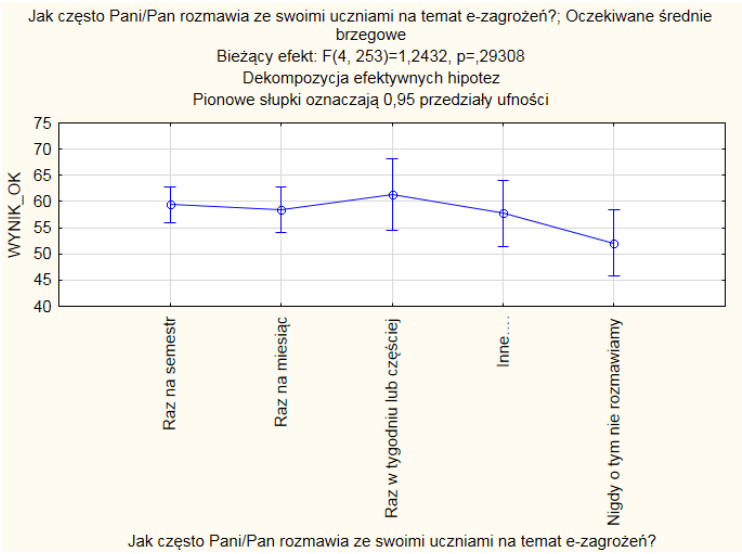
Odpowiedź	%	Liczba
Bardzo wysoki	9,70%	26
Wysoki	29,10%	78
Średni	45,52%	122
Niski	9,70%	26
Bardzo niski	2,24%	6
Nie potrafię ocenić	3,36%	9
Inne*	0,37%	1

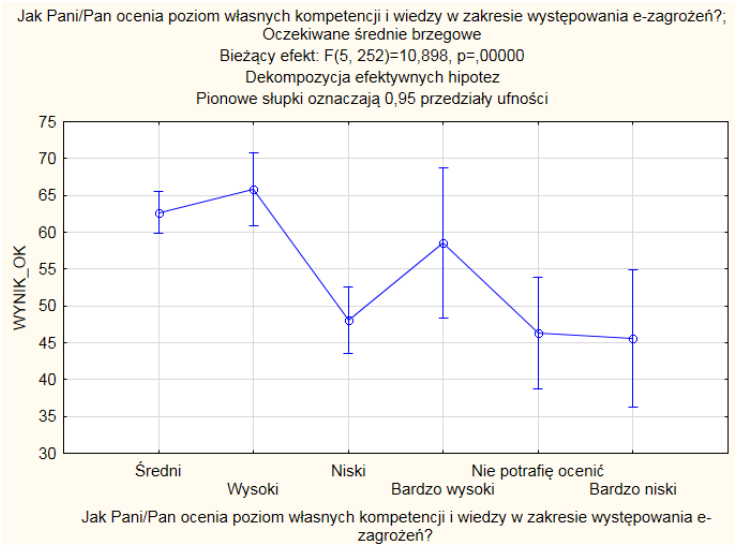
W przypadku nauczycieli szkół ponadgimnazjalnych nie występuje zależność pomiędzy częstością realizowanych zajęć w zakresie profilaktyki zagrożeń cyfrowych a wynikiem testu kompetencyjnego.

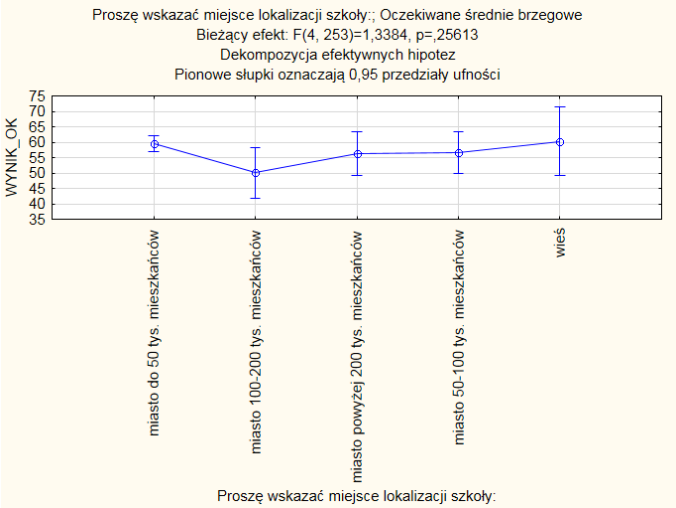
Poziom samooceny kompetencji w zakresie zagrożeń cyfrowych jest skorelowany z wynikiem testu kompetencyjnego. Wyższa ocena własnych kompetencji wiąże się z wyższym wynikiem końcowym testu. Świadczy to pozytywnie o trafności samooceny nauczycieli szkół ponadgimnazjalnych.

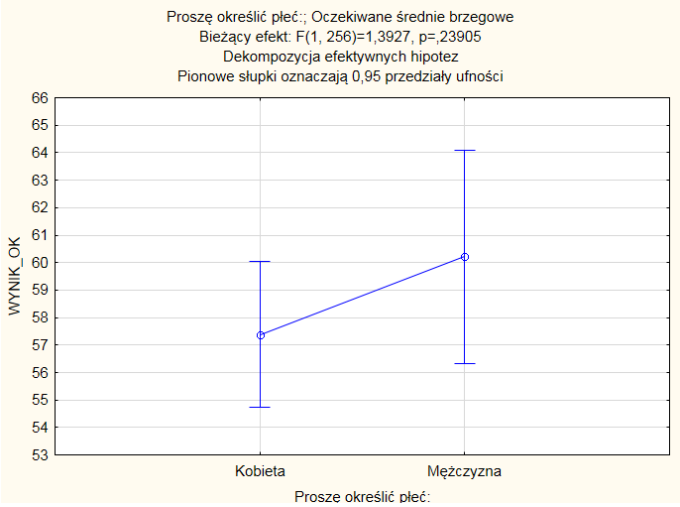
Badanie nie wykazało różnic pomiędzy nauczycielami szkół miejskich i wiejskich. Nauczyciele płci męskiej osiągają nieco wyższe wyniki w teście kompetencyjnym, niż nauczycielki. Jednakże zależność ta nie jest istotna z punktu widzenia analizy statystycznej.

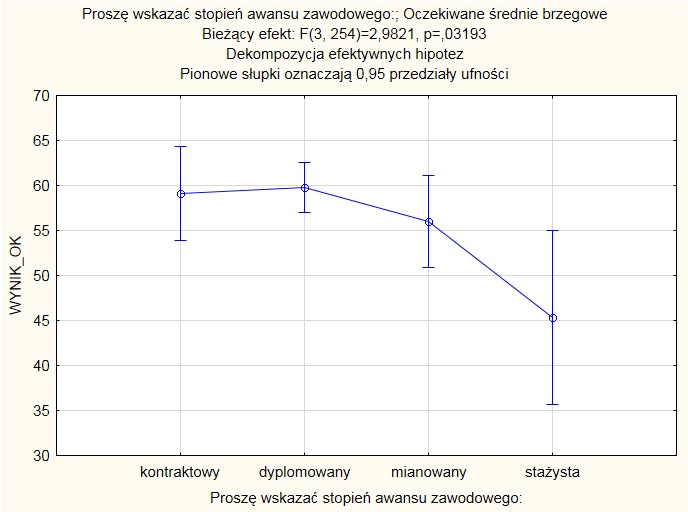
Podobnie jak w przypadku nauczycieli pracujących w szkołach gimnazjalnych i podstawowych występuje potrzeba objęcia wsparciem edukacyjnym nauczycieli stażystów, rozpoczynających ścieżkę kariery zawodowej. Wynika to z faktu, iż nauczyciele stażyści osiągają znacznie niższe wyniki niż kadra nauczycielska o większym stażu pracy zawodowej.

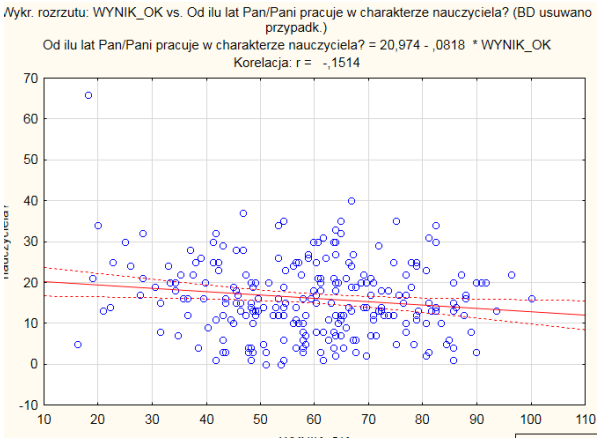


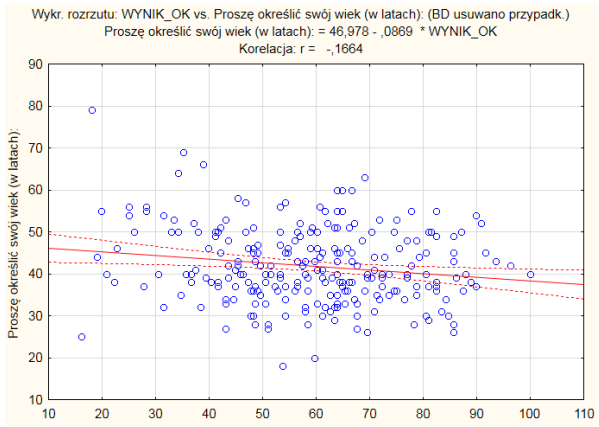



Proszę wskazać miejsce lokalizacji szkoły:; Oczekiwane średnie brzegowe
Bieżący efekt: F(4, 253)=1,3384, p=,25613
Dekompozycja efektywnych hipotez
Pionowe słupki oznaczają 0,95 przedziały ufności
WYNIK_OK
75
70
65
60
55
50
45
40
35
miasto do 50 tys. mieszkańców
miasto 100-200 tys. mieszkańców
miasto powyżej 200 tys. mieszkańców
miasto 50-100 tys. mieszkańców
wieś
Proszę wskazać miejsce lokalizacji szkoły:


Proszę określić płeć:; Oczekiwane średnie brzegowe
Bieżący efekt: F(1, 256)=1,3927, p=,23905
Dekompozycja efektywnych hipotez
Pionowe słupki oznaczają 0,95 przedziały ufności
WYNIK_OK
66
65
64
63
62
61
60
59
58
57
56
55
54
53
Kobieta
Mężczyzna
Prosze określić płeć:


Proszę wskazać stopień awansu zawodowego:; Oczekiwane średnie brzegowe
Bieżący efekt: F(3, 254)=2,9821, p=,03193
Dekompozycja efektywnych hipotez
Pionowe słupki oznaczają 0,95 przedziały ufności
WYNIK_OK
70
65
60
55
50
45
40
35
30
kontraktowy
dyplomowany
mianowany
stażysta
Proszę wskazać stopień awansu zawodowego:





4.4.4 Wnioski i rekomendacje – szkoła ponadgimnazjalna

Analiza odpowiedzi uczniów, rodziców i nauczycieli w kontekście wyników testu kompetencyjnego obejmującego treści z zakresu: wiarygodności informacyjnej dostępnych w Internecie, bezpieczeństwa w kontakcie z innymi użytkownikami sieci, bezpieczeństwa wizerunku w Internecie, prawa autorskiego, cyberprzemocy, operacji finansowych, pozwoliła na wyciągnięcie następujących wniosków:

1. Osiągnięty średni wynik poziomu kompetencji cyfrowych dotyczących zagrożeń cyfrowych świadczy o konieczności zaplanowania w skali kraju działań edukacyjnych zwiększających kompetencje informacyjno-medialne i ogólną świadomość problematyki zagrożeń cyfrowych. Działania te powinny obejmować nauczycieli i uczniów, a także ich rodziców traktowanych jako zintegrowanych podmiotów uczestniczących w procesie wychowawczym.
2. Treści modyfikowanych programów kształcenia oraz działań edukacyjnych realizowanych w ramach edukacji pozaformalnej (np. projekt Cyfrowobezpieczni.pl) powinny uwzględniać zagadnienia prawa ochrony własności intelektualnej, ochrony wizerunku w sieci oraz oceny wiarygodności wyszukiwanych w sieci informacji.
3. Spośród objętych badaniami respondentów, nauczyciele charakteryzują się dobrym przygotowaniem do rozwiązywania problemów związanych z cyberprzemocą. Świadczy to o znajomości zagadnienia oraz posiadanych już doświadczeniach zawodowych sprzyjających samodzielnemu podnoszeniu wiedzy w tym zakresie.
4. Ankietowani uczniowie w ponad 70% twierdzą, że w szkole nie są realizowane zajęcia związane z podnoszeniem bezpieczeństwa cyfrowego lub nic o nich nie wiedzą. Oznacza to, że konieczne są działania edukacyjne o charakterze systemowym zmieniające ten stan rzeczy w skali ogólnopolskiej.

5. Niemalże połowa uczniów nie rozmawiała nigdy ze swoimi rodzicami na temat zagrożeń cyfrowych. Zmiana takiego stanu rzeczy jest kluczowa dla poprawy bezpieczeństwa cyfrowego uczniów. Warto również podkreślić, że projekty edukacyjne podnoszące poziom bezpieczeństwa cyfrowego powinny być adresowane przede wszystkim do rodziców niepodejmujących tego zagadnienia w procesie wychowawczym.
6. Większość uczniów ocenia własne kompetencje cyfrowe jako wysokie lub bardzo wysokie. Indywidualne deklaracje w tym zakresie korespondują z wynikami testu kompetencyjnego.
7. Dla celów poznawczych istnieje potrzeba podejmowania dalszych badań uwzględniających w przedmiotowej problematyce badawczej szereg zmiennych pośredniczących takich, jak: styl wychowawczy, rodzaj relacji pomiędzy dzieckiem a rodzicem, struktura i specyfika funkcjonowania środowiska rodzinnego, szkolnego i rówieśniczego.
8. Wymagane jest wdrożenie procedur zwiększających bezpieczeństwo cyfrowe w szkołach ze względu na małą wiedzę w tym zakresie nauczycieli i uczniów.
9. Rodzice deklarują o wiele wyższy poziom kontroli rodzicielskiej w zakresie użytkowania nowych mediów niż ich dzieci – uczniowie uczestniczący w badaniu.
10. Ocena własnych kompetencji związanych z bezpieczeństwem cyfrowym przekłada się na wynik testu kompetencyjnego.
11. Generalnie rodzice uczestniczący w badaniu oceniają własne kompetencje cyfrowe na o wiele niższym poziomie, niż ich dzieci. Istnieje zatem potrzeba objęcia tej grupy wsparciem edukacyjnym, mającym na celu systematyczne podwyższanie kompetencji w aspekcie problematyki zagrożeń cyfrowych i użytkowania urządzeń cyfrowych.
12. Większość nauczycieli (ponad 70%) deklaruje przestrzeganie podczas zajęć zasady zakazu użytkowania telefonów komórkowych. Jedynie 11% respondentów twierdzi, że nie jest w stanie skontrolować wszystkich uczniów i wymusić na nich podporządkowanie się tej zasadzie.
13. Ponad 24% nauczycieli wymaga objęcia szczególnym wsparciem edukacyjnym ze względu na ocenę własnych kompetencji na poziomach niskim oraz bardzo niskim.
14. Poziom samooceny własnych kompetencji informacyjno-medialnych przekłada się na wynik testu kompetencyjnego określającego stopień wiedzy na temat zagrożeń cyfrowych.
15. Grupą wymagającą szczególnego wsparcia edukacyjnego w ramach projektu Cyfrowobezpieczni.pl są, podobnie jak w pozostałych typach szkół, nauczyciele stażyści (osiągający zdecydowanie najniższe wyniki na tle nauczycieli o dłuższym stażu pracy).
16. Wiek i staż pracy są w małym stopniu powiązane z osiąganym wynikiem testu kompetencyjnego. Jednak taka korelacja jest zauważalna. Wraz z liczbą lat stażu pracy nieznacznie obniża się wynik końcowy testu kompetencyjnego.

5. WNIOSKI I REKOMENDACJE SYSTEMOWE: JAK PODNIEŚĆ POZIOM KOMPETENCJI BADANYCH GRUP W ZAKRESIE BEZPIECZEŃSTWA CYFROWEGO?

Zebrane dane umożliwiają sformułowanie nie tylko wniosków z analizy wyników badań, ale także na przedstawienie rekomendacji na temat dalszych działań edukacyjnych, realizowanych w ramach projektu Cyfrowobezpieczni.pl i innych inicjatyw. Przy założeniu, że jednym z kluczowych celów projektu jest podniesienie kompetencji cyfrowych wszystkich trzech grup badanych (nauczycieli, uczniów i rodziców), rekomendujemy następujące działania:

5.1 ZMIANY W RAMACH PODSTAWY PROGRAMOWEJ

Podstawowym wnioskiem z badań jest konieczność wprowadzenia całkowicie nowego podejścia do pracy dydaktycznej wykorzystującej technologie cyfrowe w szkole. Obecnie powszechny jest model pracowni informatycznej będącej osobną salą dydaktyczną, który symbolicznie odzwierciedla sposób myślenia o świecie cyfrowym, jako odrębnym wycinku rzeczywistości. Takie myślenie redukuje wieloaspektowe ujmowanie nowych technologii do treści przedmiotu znanego pod nazwą informatyka. To jednak nie wyczerpuje potrzeb poznawczych współczesnych uczniów w całokształcie aktywności w cyberprzestrzeni.

Model ten odbiega daleko od rzeczywistości, w której świat cyfrowy przenika wszystkie sfery i obszary. Nie jest już dzisiaj możliwe odseparowanie wykorzystania technologii cyfrowych od rozwoju uczniów w innych obszarach.

Dlatego też jako jeden z wniosków z niniejszego badania postulujemy wykorzystywanie urządzeń cyfrowych we wszystkich przedmiotach, zarówno w szkole podstawowej, jak i szkołach ponadpodstawowych. Optymalnymi narzędziami do takiej pracy edukacyjnej (na bieżącym etapie

rozwoju technologii) są laptopy, tablety i smartfony. Ujmując temat ten w ramy podstawy programowej, rekomendujemy:

1. Wprowadzenie w szerokim zakresie treści programowych dotyczących prawa autorskiego na lekcjach wychowawczych, języka polskiego oraz zajęciach w obszarze technologii informacyjnej. Efekty z tego zakresu powinny obejmować w szczególności następujące obszary:
    a. umiejętność rozpoznawania użytku dozwolonego
    b. zasady cytowania
    c. wykorzystywanie „otwartych licencji"
    d. kształtowanie świadmości konsekwencji wynikających z łamania prawa autorskiego.
2. Wprowadzenie na lekcjach języka polskiego na etapie szkoły podstawowej treści oraz metod kształtujących praktyczne umiejętności w zakresie:
    a. krytycznej analizy znajdowanych w Internecie informacji;
    b. zasad wyszukiwania wiarygodnych informacji w Internecie.
3. Wprowadzenie w ramach zajęć komputerowych już w pierwszym etapie szkoły podstawowej wiedzy i praktycznych umiejętności, związanych z:
    a. tworzeniem bezpiecznych loginów i haseł;
    b. zasadami bezpiecznego logowania;
    c. zasadami przechowywania haseł;
    d. zagrożeniami związanymi z próbami wyłudzania haseł.
4. Wprowadzenie w ramach edukacji wczesnoszkolnej tematyki:
    a. reagowania na niewłaściwe zachowania innych użytkowników cyberprzestrzeni;
    b. zasad bezpieczeństwa w zakresie podawania w internecie swoich danych osobowych.
5. Wprowadzenie w ramach przedmiotu „wychowanie do życia w rodzinie":
    a. tematyki profilaktyki I, II i III stopnia w obszarze sekstingu.
6. Wprowadzenie w ramach przedmiotu edukacja dla bezpieczeństwa szeregu tematów związanych z bezpieczeństwem cyfrowym, w szczególności dotyczących:
    a. operacji finansowych;
    b. cyberprzemocy (kształtowaniem zachowań społecznie odpowiedzialnych w sytuacji bycia świadkiem przemocy).

5.2 UKIERUNKOWANIE DZIAŁANIA NA NAJSŁABSZE OBSZARY

Na podstawie badań można wyłonić newralgiczne obszary deficytów kompetencyjnych w odniesieniu do poszczególnych grup i kategorii wiekowych. W poniższej tabeli oznaczamy obszary, na których warto się skupić w pracy z beneficjentami projektu. Są to tematy, w których badani wykazali się najmniejszymi kompetencjami.

Poniższa tabela przedstawia zestawienie dwóch tematów, które uzyskały najniższy wynik w każdej z 12 grup badanych.

	Uczniowie	Rodzice	Nauczyciele
Klasy 1-3 szkoły podstawowej	Loginy, hasła i bezpieczne logowanie Bezpieczeństwo w kontakcie z innymi użytkownikami	Loginy, hasła i bezpieczne logowanie Bezpieczeństwo w kontakcie z innymi użytkownikami	Bezpieczeństwo w kontakcie z innymi użytkownikami Wiarygodność informacji dostępnych w Internecie
Klasy 4-6 szkoły podstawowej	Prawa autorskie Ergonomia korzystania z narzędzi cyfrowych	Prawa autorskie Wiarygodność informacji w Internecie	Prawa autorskie Hasła, loginy i bezpieczne logowanie
Gimnazjum	Prawa autorskie Bezpieczeństwo operacji finansowych w sieci	Prawa autorskie Wiarygodność informacji dostępnych w Internecie	Prawa autorskie Wiarygodność informacji dostępnych w Internecie
Szkoły ponadgimnazjalne	Prawa autorskie Cyberprzemoc	Prawa autorskie Bezpieczeństwo w kontakcie z innymi użytkownikami	Bezpieczeństwo w kontakcie z innymi użytkownikami Wiarygodność informacji dostępnych w sieci

Wiedza na temat zakresów tematycznych, w których uczniowie i ich rodzice, a także nauczyciele osiągali najsłabsze wyniki testu kompetencyjnego pozwala ukierunkować przyszłe działania na obszary związane z największym ryzykiem zagrożeń cyfrowych. Przykładowo rodzice uczniów w klasach 4-6 szkoły podstawowej w pytaniach związanych z tematem ergonomii korzystania z urządzeń cyfrowych uzyskali 73% punktów – nie jest to wynik optymalny, jednak z pewnością znacznie bardziej potrzebne jest dostarczenie im wiedzy na temat praw autorskich. W tym bowiem aspekcie średni wynik wyniósł zaledwie 32%. Co istotne, ten wynik powtórzył się w grupie uczniów, z czego można wyciągnąć wniosek, że rodzice nie są w stanie wesprzeć bardziej swoich dzieci w rozwijaniu kompetencji cyfrowych, ponieważ już przekazali im wszystko, co wiedzieli. I okazało się to zdecydowanie zbyt mało.

Dlatego w ramach organizowanych w szkołach Dni Bezpieczeństwa Cyfrowego rekomendujemy skupienie uwagi prowadzących spotkania na tych zakresach wiedzy, które najbardziej wymagają rozbudowania i poszerzania merytorycznego. Biorąc pod uwagę czas, który każdy z edukatorów cyfrowych spędzi w szkole, powinno dać to najlepsze rezultaty.

5.3 Koncentracja na najmniejszych miejscowościach

Jak wynika z analiz zmiennych niezależnych, zdecydowanie najniższe poziomy kompetencji cyfrowej ujawniły się w przypadku badanych z obszarów wiejskich, zwłaszcza grupy rodziców. Na terenie większych miejscowości także widać tendencję do osiągania wyższych wyników testu kompetencyjnego adekwatnie do wielkości miejscowości. Największy deficyt wiedzy i umiejętności w tym zakresie występuje w szkołach zlokalizowanych na wsi. Dlatego w miarę możliwości rekomendowane jest objęcie, jak największą liczbą działań edukacyjnych szkół z niewielkich miejscowości i wsi.

5.4 Wsparcie najmłodszych nauczycieli

Jak wskazują dalsze analizy, zdecydowanie najsłabiej w badaniach wypadają nauczyciele najkrócej pracujący. Stoi to w sprzeczności ze zdroworozsądkowym założeniem, że najmłodsi pracownicy szkół będą najlepiej radzili sobie z zagrożeniami świata cyfrowego, w którym przecież niedawno dorastali. Jednak ustalenia te znajdują potwierdzenie w wynikach badań realizowane w 2014 roku w woj. małopolskim (Grynienko et al., 2014). Wskazują one na to, że zdolność pozytywnego

wykorzystywania technologii cyfrowych jest największa w grupie nauczycieli w wieku 40-55 lat, podczas, gdy najsłabiej radzą sobie z tym nauczyciele dopiero zatrudnieni.

Przyczyną takiego zjawiska jest zapewne dość często ignorowany fakt, że głównymi kompetencjami pedagogicznymi potrzebnymi nauczycielowi do efektywnej pracy zawodowej są umiejętności społeczne i dydaktyczne, nabywane poprzez doświadczenie zbierane latami. Dotyczy to wszystkich obszarów pracy nauczycielskiej, zarówno skutecznej dydaktyki, jak i pracy wychowawczej (tu zapewne najbardziej). Dlatego też zachęcamy do zwrócenia uwagi w projektowaniu działań edukacyjnych w ramach programu na nauczycieli o najkrótszym stażu pracy. Jedną z propozycji może być organizowanie wyłącznie dla nich obozów wakacyjnych w ramach projektu Cyfrowobezpieczni.pl

Podsumowując: ze względu na dynamikę projektu i czas, który edukatorzy spędzą w szkołach, rekomendujemy skoncentrowanie w sferze organizacji działań edukacyjnych na szkołach z obszarów wiejskich i na najmłodszych stażem nauczycielach, a w sferze merytorycznej na tych aspektach kompetencji informacyjno-medialnych, w których badani ujawnili największe braki.

Taki sposób działania jest najlepszym sposobem na uzyskanie wzrostu poziomu kompetencji informacyjno-medialnych wśród uczestników projektu.

6. BIBLIOGRAFIA

Andrzejewska, A., Bednarek, J. (2014). *Seksting*, [w:] J. Lizut (red.), Zagrożenia cyberprzestrzeni. Kompleksowy program dla pracowników służb społecznych, Wyd. Wyższa Szkoła Pedagogiczna, Warszawa, s.158-162.

Cipresso, P., Gaggioli, A., Serino, S., Cipresso, S., & Riva, G. (2012). How to Create Memorizable and Strong Passwords. Journal of Medical Internet Research, 14(1), e10. doi:10.2196/jmir.1906

Cornish, L. S. (2014). 'Mum, can I play on the internet?' Parents' understanding, perception and responses to online advertising designed for children. *International Journal Of Advertising*, *33*(3), 437-473. doi:10.2501/IJA-33-3-437-473

Curnutt, H. (2012). Flashing Your Phone: Sexting and the Remediation of Teen Sexuality. *Communication Quarterly*, *60*(3), 353-369. doi:10.1080/01463373.2012.688728

Del Rey, R., Casas, J. A., Ortega-Ruiz, R., Schultze-Krumbholz, A., Scheithauer, H., Smith, P., ... Plichta, P. (2015). Structural validation and cross-cultural robustness of the European Cyberbullying Intervention Project Questionnaire. Computers in Human Behavior, 50, 141–147. doi:10.1016/j.chb.2015.03.065

Duranowski, W. (2014). Podstawowe zagrożenia zdrowotne związane z używaniem komputera I internet, [w:] J. Lizut (red.), Zagrożenia cyberprzestrzeni. Kompleksowy program dla pracowników służb społecznych, Wyd. Wyższa Szkoła Pedagogiczna, Warszawa 2014, s.65-76.

EFREMOVA, M. A., & AGAPOV, P. V. (2016). Crimes against Information Security: International Legal Aspects of Fighting and Experience of Some States. *Journal Of Internet Banking & Commerce*, *21*(S3), 1-11.

Fan, W., & Yeung, K. (2011). Online social networks—Paradise of computer viruses. *Physica A*, *390*(2), 189-197. doi:10.1016/j.physa.2010.09.034

Fanning, K. (2015). Minimizing the Cost of Malware. *Journal Of Corporate Accounting & Finance (Wiley)*, *26*(3), 7-14. doi:10.1002/jcaf.22029

Fastyn, T. (2016). *Raport: Wzrost cyberzagrożeń na smartfonach o 98 procent*, http://www.cyberdefence24.pl/440740,raport-wzrost-cyberzagrozen-na-smartfonach-o-98-procent

Ferrillo, P., & Singer, R. (2015). Is Employee Awareness and Training the Holy Grail of Cybersecurity?. *Corporate Governance Advisor*, *23*(3), 10-13.

Filiciak, M., Danielewicz, M., Halawa, M., Mazurek, P., Nowotny, A. (2010). Młodzi i Media: Nowe Media a Uczestnictwo w Kulturze. Szkoła Wyższa Psychologii Społecznej, Warszawa.

Frania, M. (2014a). New Educational Trends Connected with the Development of Media and Innovative Technologies – A Few Reflections on the Future Perspectives on Learning and Teaching. *JESR*. doi:10.5901/jesr.2014.v4n4p232

Frania, M. (2014b). Selected aspects of media literacy and new technologies in education as a challenge of Polish reality. *Perspectives of Innovations, Economics and Business*, 14(2), 109–112. doi:10.15208/pieb.2014.13

Goldsborough, R. (2006). Phishing scams find easy bait through e-mail. *New Orleans Citybusiness (1994 To 2008)*, *27*(20), 20.

Grynienko, K., Hofman, D., Kuczyńska, A., Srokowski, Ł. (2013). *Innowacyjne zastosowania narzędzi w kształceniu – raport z badań*, Stowarzyszenie „Miasta w Internecie", Tarnów.

Hamel, L. M., & Robbins, L. B. (2013). Computer- and web-based interventions to promote healthy eating among children and adolescents: a systematic review. *Journal Of Advanced Nursing*, *69*(1), 16-30. doi:10.1111/j.1365-2648.2012.06086.x

Hatalska, N. (2016). *Rola blogerów i youtuberów we współczesnym świecie* / raport, BlogForum, Gdańsk.

Hatfield, M., Parsons, R., & Ciccarelli, M. (2016). The development and validation of the Healthy Computing Questionnaire for Children (HCQC). *Work*, *54*(2), 389-399. doi:10.3233/WOR-162324

Hinduja, S., Patchin, J. (2011). *Cyberbullying: Identification, Prevention and Response*, Dude Publishing, United States of America 2011.

Hinduja, S., Patchin, J.W. (2009). *Cyberbullying Research Summary: Emotional and Psychological Consequences*, „Cyberbullying Research Center", nr 1-2, 2009.

Juszczyk, S. (2003). *Edukacja medialna w społeczeństwie informacyjnym*. Adam Marszałek. Toruń.

Juszczyk, S. (2005). *Badania ilościowe w naukach społecznych. Szkice metodologiczne / Quantitative research in the social sciences. Methodological sketches /*, Śląska Wyższa Szkoła Zarządzania, Katowice.

Kędzierska, B. (2005). *Informatyczne kształcenie i doskonalenie nauczycieli*. Wydawnictwo Naukowe Akademii Pedagogicznej, Kraków.

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

Kopecky, K. (2010). *Cyber grooming danger of cyberspace*, NET UNIVERSITY, Olomouc.

Kopecký, K. (2017). Online blackmail of Czech children focused on so-called "sextortion" (analysis of culprit and victim behaviors). Telematics and Informatics, 34(1), 11–19. doi:10.1016/j.tele.2016.04.004

Kopecký, K., Szotkowski , R. (2014) FORMAL AND SEMANTIC ANALYSIS OF COMPUTER PASSWORDS OF CZECH INTERNET USERS, *EDULEARN14 Proceedings*, pp. 2794-2798.

Kopecký, K., & Szotkowski, R. (2017). Cyberbullying, cyber aggression and their impact on the victim – The teacher. Telematics and Informatics, 34(2), 506–517. doi:10.1016/j.tele.2016.08.014

Kopecký, K., Szotkowski, R., Krejčí, V. (2012). *Nebezpečí internetové komunikace III (4-8)*. Olomouc: Univerzita Palackého.

Kopecký, K., Szotkowski, R., Krejčí, V., (2014). *Nebezpečí internetové komunikace IV / Dangers of Internet communication IV/*. Olomouc. Pedagogická fakulta, Univerzita Palackého v Olomouci.

Kowalczyk, C. M., & Royne, M. B. (2016). Exploring the influence of mothers' attitudes toward advertising on children's consumption of screen media. *International Journal Of Consumer Studies*, *40*(5), 610-617. doi:10.1111/ijcs.12306

Kubiatko, M. (2013). The Comparison of Different Age Groups on the Attitudes toward and the Use of ICT. *Educational Sciences: Theory And Practice*, *13*(2), 1263-1272.

Lampe, J. R. (2013). A VICTIMLESS SEX CRIME: THE CASE FOR DECRIMINALIZING CONSENSUAL TEEN SEXTING. *University Of Michigan Journal Of Law Reform*, *46*(2), 703-736.

Lange, R., Osiecki, J. (2014), *Nastolatki wobec Internetu /Teens and Internet/*, Pedagogium, Warszawa.

Livingstone, S., Bober, M. (2006). *Regulating the internet at home: contrasting the perspectives of children and parents* In: Buckingham, David and Willett, Rebekah, (eds.) *Digital Generations: Children, Young People and New Media*. Lawrence Erlbaum Associates, Mahwah, N.J., 93-113.

Morbitzer, J. (2007). *Edukacja wspierana komputerowe a humanistyczne wartości pedagogiki*, Wyd. Naukowe Akademii Pedagogicznej, Kraków.

MOSOROV, V., & NIEDŹWIEDZIŃSKI, M. (2014). ANALIZA STRAT EKONOMICZNYCH SPOWODOWANYCH PRZESTĘPCZOŚCIĄ INTERNETOWĄ. *Studia I Materialy Polskiego Stowarzyszenia Zarzadzania Wiedza / Studies & Proceedings Polish Association For Knowledge Management*, (71), 129-140.

New viruses expected. (2006). *Communications News*, *43*(2), 10.

NIK (2014), *Przeciwdziałanie zjawiskom patologii wśród dzieci i młodzieży szkolnej*, Najwyższa Izba Kontroli, Warszawa.

Orange (2015). *Bezpieczne media. Poradnik dla rodziców*, Warszawa.

Ólafsson, K., Livingstone, S., & Haddon, L. (2013). *Children's Use of Online Technologies in Europe. A review of the European evidence base*. LSE, London: EU Kids Online

Peryt-Poręba, A. (2011). Akademicka pedeutologia informatyczno-medialna przyszłych nauczycieli polonistów, in: http://www.ktime.up.krakow.pl/symp2011/referaty2011/peryt.pdf

Prensky, M. (2001). *Digital natives, digital immigrants*, On the Horizon, MCB University Press, Vol. 9 No. 5

Pricewaterhouse Coopers (2014). *Analiza wpływu zjawiska piractwa treści wideo na gospodarkę w Polsce*, Katowice.

Pyżalski, J. (2011). *Agresja elektroniczna wśród dzieci i młodzieży*. Gdańskie Wydawnictwo Psychologiczne, Gdańsk.

Pyżalski, J. (2012). *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży*. Oficyna Wydawnicza Impuls, Kraków.

Pyżalski, J. (2016). COUNTRY REPORT FOR POLAND, [w:] Cyberbullying among young people, Brussels: Policy Department for Citizen's Rights and Constitutional Affairs.

Rubacha, K. (2008). *Metodologia badań nad edukacją.* Warszawa: Wydawnictwa Akademickie i Profesjonalne.

Ševčíková, A. (2016). Girls' and boys' experience with teen sexting in early and late adolescence. *Journal Of Adolescence*, *51*156-162. doi:10.1016/j.adolescence.2016.06.007

Siemieniecki, B. (2008). *Pedagogika medialna*. PWN. Warszawa

Siuda, P., Stunża, G., (2012). *Dzieci Sieci: kompetencje komunikacyjne najmłodszych: raport z badań /Children in cybernetwork: the youngest communication skills: research report/*, Instytut Kultury Miejskiej, Gdańsk.

Siuda, P., Stunża, G.D., Dąbrowska, A.J., Klimowicz, M., Kulczycki, E., Piotrowska, R., Rozkosz, E., Sieńko, M., Stachura, K. (2013). Dzieci Sieci 2.0: Kompetencje Komunikacyjne Młodych. Instytut Kultury Miejskiej, Gdańsk.

SLABBERT, I., MENTZ, E., & OOSTHUIZEN, I. (2014). Die ergonomies ideale rekenaarlokaal vir die daarstel van leerdergeborgenheid. *Suid-Afrikaanse Tydskrif Vir Natuurwetenskap En Tegnologie*, *54*(1), 111-128.

Soontae, A., & Kang, H. (2014). Advertising or games? Advergames on the internet gaming sites targeting children. *International Journal Of Advertising*, *33*(3), 509-532. doi:10.2501/IJA-33-3-509-532

Szpunar, M. (2008). Wikipedia-zbiorowa mądrość czy kolektywna głupota?. E-mentor nr 5 (27) / 2008, 11-15.

Szpunar, M. (2016). *Kultura cyfrowego narcyzmu*, Wydaw. AGH, Kraków.

Tam, L., Glassman, M., & Vandenwauver, M. (2010). The psychology of password management: a tradeoff between security and convenience. *Behaviour & Information Technology*, *29*(3), 233-244. doi:10.1080/01449290903121386

Teen Online & Wireless Safety Survey (2009). *Cyberbullying, Sexting and Parental Control*, Cox Communications Teen Online & Wireless Safety Survey. In Partnership with National Center for Missing and Exploited Children (NCMEC) and John Wlash (fielded among young people 13-18), Teen Online & Wireless Safety Survey 2009

Temple, J. R., Le, V. D., van den Berg, P., Ling, Y., Paul, J. A., & Temple, B. W. (2014). Brief report: Teen sexting and psychosocial health. *Journal Of Adolescence*, *37*(1), 33-36. doi:10.1016/j.adolescence.2013.10.008

Tomczyk, Ł. (2014). Pedagogiczno-techniczne uwarunkowania ochrony wizerunku w sieci, [w:] J. Lizut, A. Wrońska (red.), E-zagrożenia nowym wyzwaniem dla służb społecznych, Wydaw. Wyższa Szkoła Pedagogiczna, Warszawa, s.48-57

Tomczyk, Ł. (2015). Specifics of Electronic Aggression Basing on Research Results in Silesian Voivodship (Poland), "Acta Universitatis Matthaei Belii", č. 15, s.242-255.

Tomczyk, Ł., & Kopecký, K. (2016). Children and youth safety on the Internet: Experiences from Czech Republic and Poland. Telematics and Informatics, 33(3), 822–833. doi:10.1016/j.tele.2015.12.003

Tomczyk, Ł., Szotkowski, R., Fabiś, A., Wąsiński, A., Chudý, Š., & Neumeister, P. (2015). Selected aspects of conditions in the use of new media as an important part of the training of teachers in the Czech Republic and Poland - differences, risks and threats. Education and Information Technologies. doi:10.1007/s10639-015-9455-8

Urbanowicz, J. (2015). Ściąganie plików z sieci, [w:] Wrzesień-Gandolfo A. (red.), *Bezpieczeństwo dzieci online. Kompendium wiedzy dla rodziców i nauczycieli*, Wydaw. NASK i Fundacja Dzieci Niczyje, Warszawa.

Valcke M., Bonte S., De Wever B., Rots I. (2010). *Internet parenting styles and the impact on Internet use of primary school children*, Computers & Education, Volume 55, Issue 2, September 2010, Pages 454-464

Wąsiński, A., Tomczyk, Ł. (2015). Factors reducing the risk of internet addiction in young people in their home environment. Children and Youth Services Review, 57, 68–74. doi:10.1016/j.childyouth.2015.07.022

Wąsiński, A., Tomczyk, Ł. (2011). Aktywność młodzieży oraz rola rodziców w przestrzeni mediów sieciowych w perspektywie zagrożeń netoholizmem na przykładzie badań własnych, [w:] Z. Zieliński (red.) Rola informatyki w naukach ekonomicznych i społecznych. Innowacje i implikacje interdyscyplinarne, Tom 1, Wyższa Szkoła Handlowa, Kielce, s.178-195

Wojtas, M. (2015). *Uwodzenie dzieci w internecie i inne niebezpieczne kontakty*, [w:] Wrzesień-Gandolfo A. (red.), *Bezpieczeństwo dzieci online. Kompendium wiedzy dla rodziców i nauczycieli*, Wydaw. NASK i Fundacja Dzieci Niczyje, Warszawa.

Woo, E. H., White, P., & Lai, C. W. (2016). Impact of information and communication technology on child health. *Journal Of Paediatrics & Child Health*, *52*(6), 590-594. doi:10.1111/jpc.13181

Wrzesień-Gandolfo, A. (2015). *Reklama i marketing online skierowane do dzieci*, [w:] Wrzesień-Gandolfo A. (red.), *Bezpieczeństwo dzieci online. Kompendium wiedzy dla rodziców i nauczycieli*, Wydaw. NASK i Fundacja Dzieci Niczyje, Warszawa.

Wyrostkiewicz, M. (2009). Piractwo komputerowe – problem nie tylko prawny. *Biuletyn Żydowskigo Instytutu Historycznego*, 1/2009, 122-127.