Tomasz Siemianowski[1]

Wybrane zagrożenia internetowe i porady dotyczące zapewnienia dziecku bezpieczeństwa w Internecie

„Bezpieczeństwo jest jedną z podstawowych wartości w życiu każdego człowieka. Jest podstawą egzystencji i bytu jednostek, grup, a także narodów. Z punktu widzenia jednostki, czy też grup, wartość ta jest niestabilna, wymaga ciągłej walki o jej utrzymanie. Bezpieczeństwo rozumiane jest jako stan niezagrożenia, spokoju, pewności”[2].

Z kolei „Środowisko bezpieczeństwa — to innymi słowy wszelkie, zewnętrzne i wewnętrzne, militarne i niemilitarne (polityczne, ekonomiczne, społeczne, kulturowe, informacyjne itp.) warunki bezpieczeństwa, warunki realizacji interesów danego podmiotu w dziedzinie bezpieczeństwa i osiągania ustalonych przezeń celów w tym zakresie. Charakteryzowane mogą być najpełniej przy pomocy czterech podstawowych kategorii, jakimi są: szanse, wyzwania, ryzyka i zagrożenia”[3].

W ramach siatki pojęciowej bezpieczeństwa wymienić należy także termin „kultura bezpieczeństwa”. Jest to „wzór podstawowych założeń, wartości, norm, reguł, symboli i przekonań, wpływających na sposób postrzegania wyzwań, szans i (lub) zagrożeń, a także sposób odczuwania bezpieczeństwa i myślenia o nim oraz związany z tym sposób zachowania i dziania (współdziałania) podmiotów, w różny sposób przez te podmioty wyuczonych i wyartykułowanych w procesach szeroko rozumianej edukacji, w tym również w naturalnych

[1] Nadkom. dr Tomasz Siemianowski — w Policji pracuje od 1995 r. Od początku związany jest z tematyką policyjnych systemów informatycznych. Obecnie jest adiunktem Instytutu Nauk o Bezpieczeństwie Wydziału Bezpieczeństwa Wewnętrznego i Nauk Prawnych Wyższej Szkoły Policji w Szczytnie. W 2013 r. na Wydziale Dowodzenia i Operacji Morskich Akademii Marynarki Wojennej w Gdyni uzyskał stopień doktora nauk społecznych w zakresie specjalności bezpieczeństwa wewnętrznego. Organizator i uczestnik konferencji w kraju i za granicą. Autor publikacji z zakresu baz danych wykorzystywanych w Policji oraz technologii internetowych używanych do zwalczania przestępczości internetowej wobec małoletnich.

Adres do korespondencji: <t.siemianowski@wspol.edu.pl>.

[2] M. Szymczak (red.), *Słownik języka polskiego*, t. 1, Warszawa 1978, hasło: bezpieczeństwo, s. 147.

[3] S. Koziej, *Strategiczne środowisko bezpieczeństwa międzynarodowego i narodowego w okresie pozimnowojennym*, Warszawa 2010, s. 4.

procesach wewnętrznej integracji i zewnętrznej adaptacji oraz w innych procesach organizacyjnych, a także w procesie umacniania szeroko (nie tylko militarnie) rozumianej obronności, służących w miarę harmonijnemu rozwojowi tych podmiotów i osiąganiu przez nie najszerzej rozumianego bezpieczeństwa, z pożytkiem dla siebie, ale i otoczenia"[4].

„W dobie społeczeństwa informacyjnego (cyberspołeczeństwa), gdy coraz więcej dziedzin naszego życia jest uzależnionych od sprawnego i niezawodnego funkcjonowania technologii i produktów sektora IT (*Information Technology*), stosownie do stopnia nasycenia sprzętem komputerowym wzrasta zagrożenie techniczne i społeczne właśnie ze strony zaawansowanej technologii. Zagrożenia mogą mieć różne przyczyny i źródła, a ich konsekwencje mogą być mniej lub bardziej groźne dla współczesnej cywilizacji. Jak wykazują profesjonalne badania statystyczne dominującą liczbowo kategorią zagrożeń są zagrożenia bezpośrednio generowane przez personel obsługujący systemy i sieci komputerowe oraz przez mniej lub bardziej świadomych użytkowników. Człowiek i jego wiedza (lub niewiedza) oraz ewentualne motywacje stanowią podstawowe źródło zagrożeń w erze społeczeństwa informacyjnego"[5].

Internet inspiruje dzieci do komunikacji, kreatywności i uczenia się. Stanowi zbiór sieci, które udostępniają usługi oraz stosują zgodne protokoły. Jest wynalazkiem, którego nikt w pełni nie kontroluje, gdyż nie jest to możliwe z uwagi na zasięg, który osiąga. Odnosząc się do powyższych słów, trzeba zaznaczyć, że technologie cyfrowe zapewniają bogactwo możliwości, łącząc np. naukę z rozrywką, a mimo to ich użytkownicy zdają sobie sprawę z zagrożeń (związanych z cyberzagrożeniami), które prowadzą do przeróżnych szkód. Media cyfrowe, z których korzystają małoletni, wciąż się zmieniają, a w konsekwencji tego pojawiają się zarówno nowe zagrożenia, jak i zagadnienia tyczące się korzystania z sieci internetowych. Chociaż Internet jest doskonałym źródłem różnych informacji, ważne jest, aby jego najmłodsi użytkownicy byli chronieni przed zagrożeniami, które mogą napotkać. Zaznaczyć trzeba, że cyberzagrożenia wymierzone są zarówno w małoletnich, jak i w dane znajdujące się na urządzeniach, przy pomocy których korzystają oni z sieci. Niestety umiejętność obsługi urządzeń przez małoletnich nie idzie w parze ze świadomością zagrożeń, na które są narażeni.

Uwrażliwienie społeczeństwa na zagrożenia płynące z cyberprzestrzeni i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami wymaga ciągłej współpracy administracji publicznej m.in. z organizacjami pozarządowymi, ośrodkami akademickimi, operatorami usług kluczowych i dostawcami usług cyfrowych, natomiast edukację w zakresie cyberbezpieczeństwa należy rozpoczynać już na etapie kształcenia wczesnoszkolnego.

Aby zapewnić dzieciom bezpieczeństwo w Internecie, w 2008 r. utworzona została Brytyjska Rada ds. Bezpieczeństwa Dzieci w Internecie (dalej jako: UKCCIS), której celem jest połączenie ze sobą organów ścigania,

[4] M. Cieślarczyk, *Kultura bezpieczeństwa i obronności*, Siedlce 2010, s. 210.

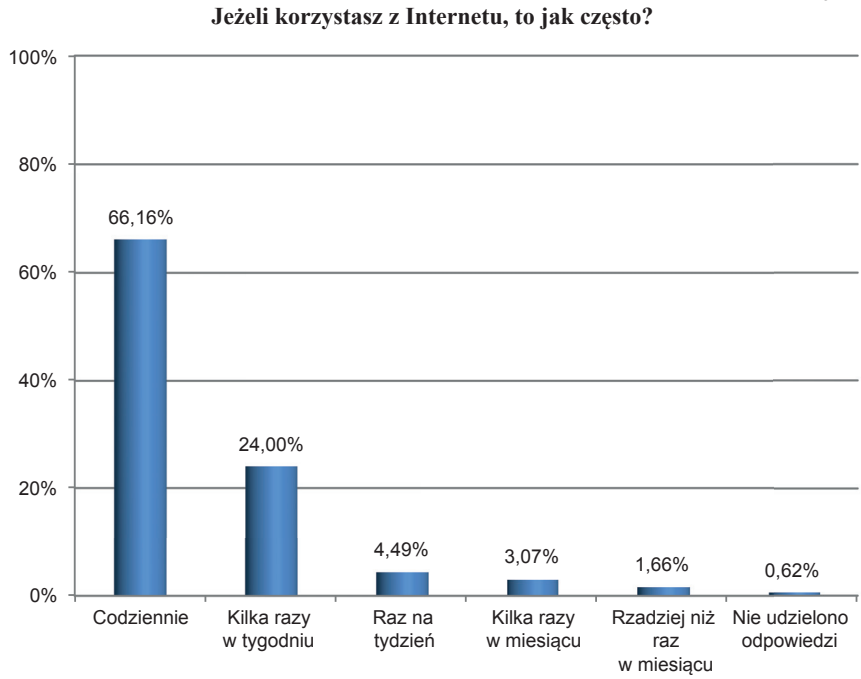
[5] K. Ficoń, *Inżynieria zarządzania kryzysowego. Podejście systemowe*, Warszawa 2007, s. 102.

środowisk akademickich, a także przedstawicieli sektora prywatnego, organizacji pozarządowych i wolontariuszy w celu współpracy nad nowymi strategiami w zakresie aktualnych problemów dotyczących korzystania z Internetu.

Brytyjska Rada ds. Bezpieczeństwa Dzieci w Internecie identyfikuje, opiniuje i zestawia informacje pochodzące z istotnych wyników badań i informuje o tym zainteresowane strony, a także organizuje seminaria mające na celu rozwiązywanie pojawiających się problemów i tworzy serię kluczowych tematów badawczych.

W niniejszym artykule autor wykorzystał wyniki własnych badań dotyczących cyberprzemocy, które przeprowadził wśród ponad 2800 uczniów szkół podstawowych i gimnazjalnych województwa warmińsko-mazurskiego w celu uchwycenia empirycznych trendów korzystania z Internetu. Wobec tego należy stwierdzić, że sposób użytkowania sieci internetowych przez małoletnich zmienia się w zależności od innowacji technologicznych, społecznych czy rynkowych, zaś samo wykorzystanie Internetu jest związane przede wszystkim z płcią, wiekiem, statusem społeczno-ekonomicznym dzieci oraz lokalizacją i dostępem do urządzeń wyposażonych w możliwość połączenia z sieciami internetowymi. Ponadto trzeba dodać, że niewielka ilość dzieci pozostaje bez dostępu do Internetu, a dla większości z nich korzystanie z niego zajmuje coraz więcej czasu, co obrazuje poniższe zestawienie:

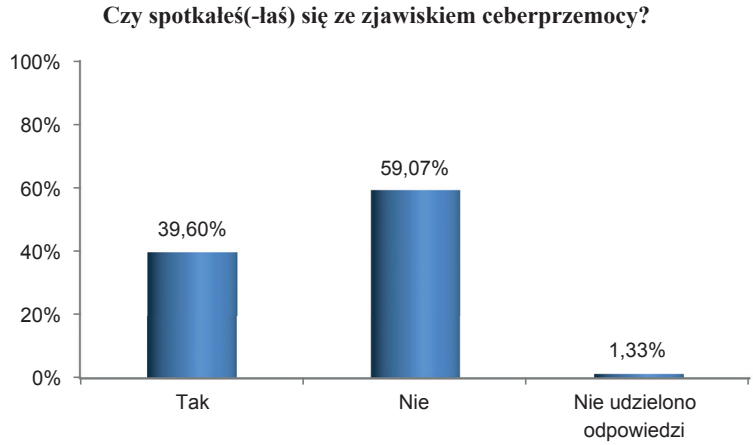
Wykres 1



Źródło: opracowanie własne

W ostatnich latach, w ocenie autora, nastąpił wzrost ryzyka internetowego związanego z podwyższoną liczbą krzywdzących i szerzących nienawiść treści. Do najpoważniejszych zagrożeń, na które narażone są dzieci, zaliczyć można **przemoc i pornografię**. Małoletni twierdzą, że spotykają się z wymienionymi zagrożeniami najczęściej w witrynach do udostępniania filmów, a także serwisach społecznościowych oraz grach. Skalę styczności ze zjawiskiem cyberprzemocy przez dzieci obrazuje poniższy wykres:

Wykres 2



Źródło: opracowanie własne

Wspomnieć należy, że istnieją różne współzależności między zagrożeniami internetowymi, np. cyberprzemoc, pornografia, *sexting*, więc małoletni narażeni na jeden rodzaj ryzyka mogą być również podatni na inne. Dzieci rozwijają się poznawczo, emocjonalnie, w zakresie potrzeb tożsamościowych, relacji społecznych i potrzeby wsparcia, a także ich kultur rówieśniczych, jednak trudno jest określić moment, w którym ulegają one swoistym zagrożeniom internetowym.

Odnosząc się do tematyki związanej z działalnością UKCCIS i wspomnianej w jej ramach współpracy różnych środowisk, trudno jest jednoznacznie wskazać co i dlaczego działa niewłaściwie. Szkoły stosują różne procedury dotyczące wdrażania priorytetów w zakresie e-bezpieczeństwa, ale takie techniki zwykle przyjmują standardowe podejście i nie zawsze mogą być dostosowane do jednostkowych potrzeb dzieci. Kampanie informacyjno-edukacyjne podnoszące świadomość rosnącej liczby zagrożeń internetowych, takie jak np. Dzień Bezpiecznego Internetu, mają kluczowe znaczenie dla zmiany postaw i praktyk wśród nieletnich. Z kolei rodzice stosują różne strategie mediacji, m.in. kontrolę techniczną, zasady regulujące dostęp i korzystanie z Internetu, rozmowy z dziećmi na temat konsekwencji ich działań w Internecie, jednak luki w umiejętnościach rodziców wpływają na mniejszą skuteczność w działaniach, które podejmują. Rodzice preferują narzędzia kontrolne, które są im znane, chyba że niepożądany

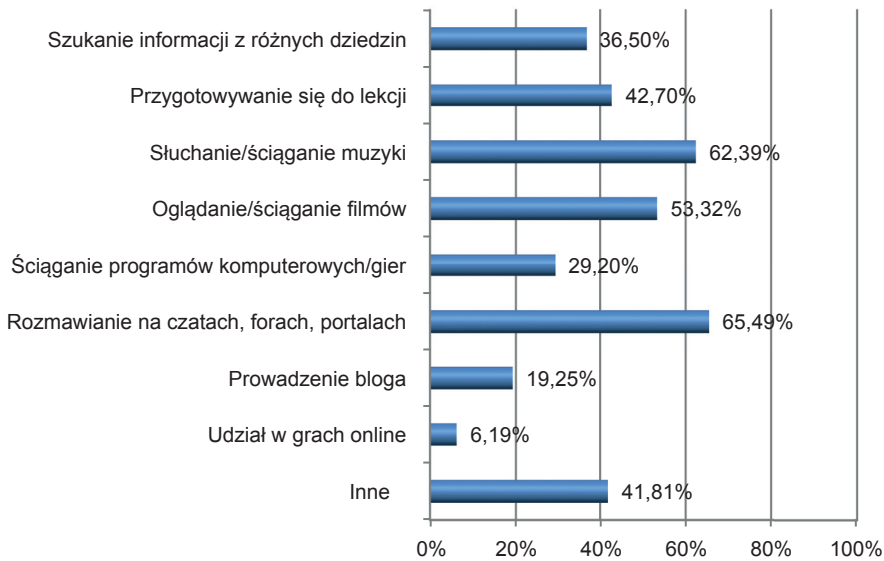
incydent wymaga od nich przyjęcia nowego podejścia bądź rozwiązania problemu. Istnieje także szereg inicjatyw branżowych w postaci umów i inicjatyw poszczególnych firm, ale pojawiają się również fakty sugerujące, że przemysł mógłby zrobić więcej, aby wzmocnić partnerstwo oparte na współpracy — szczególnie z organami ścigania.

Budowa cyfrowej odporności dzieci powinna skupiać się bliżej na rozwijaniu umiejętności krytycznych i kompetencji technicznych w zakresie edukacji, a także na wspieraniu dzieci w poruszaniu się w Internecie i poza nim poprzez konstruktywne i świadome praktyki rodzicielskie oraz zapewnienie bezpieczeństwa i poszanowania prywatności od samego początku.

Technologia cyfrowa i korzystanie z Internetu stają się integralną częścią życia małoletnich. Ważne jest zrozumienie pozytywnych motywacji dzieci i wyborów podczas korzystania z Internetu. Młodzi ludzie widzą pozytywną rolę działań za pośrednictwem sieci komputerowej (ang. *online*) w odniesieniu do wyrażania siebie, łączenia ludzi oraz szanowania i doceniania różnic między nimi. Badania pokazują, że małoletni korzystają z Internetu z różnych powodów, co obrazuje poniższe zestawienie:

Wykres 3

Jeżeli Ty lub Twoi znajomi korzystacie z Internetu, to w jakim najczęściej celu?



Źródło: opracowanie własne

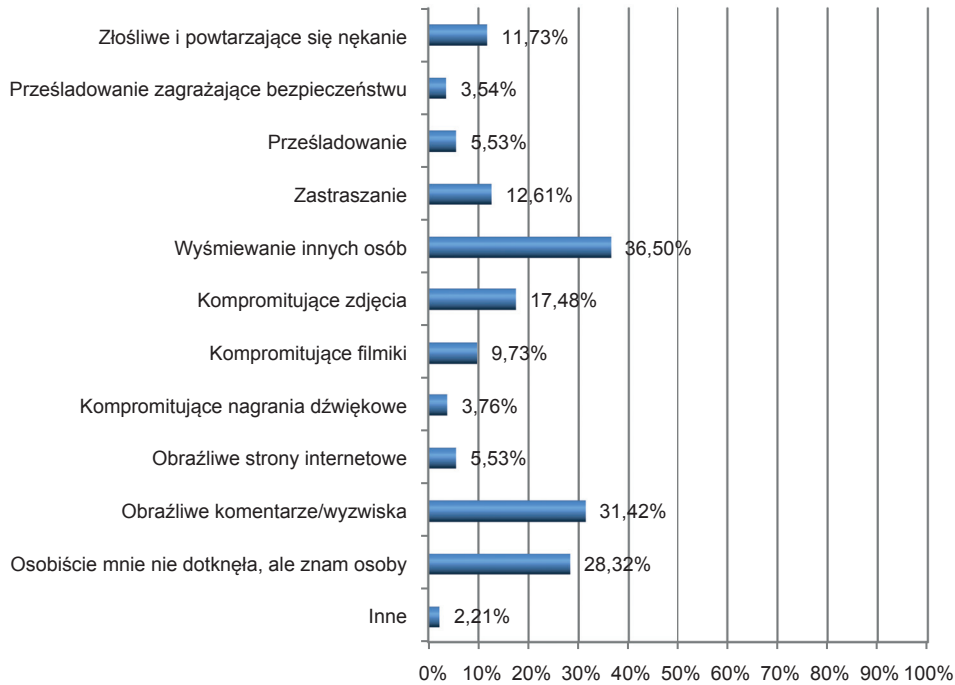
Można zauważyć, że Internet pozwala małoletnim stać się twórcami treści oraz odbiorcami, budując ich kompetencje, zaufanie, a także umożliwiając im udział w ich kulturze rówieśniczej i szerszym społeczeństwie.

Podczas gdy małoletni i dorośli odnoszą się do wielu z wyżej wymienionych działań pozytywnie, korzystanie z możliwości Internetu samo w sobie

może być ryzykowne, np. dodawanie nowych osób do kontaktów może być doskonałym sposobem na zawarcie nowych przyjaźni, ale może również doprowadzić do kontaktu dzieci z potencjalnie obraźliwymi nieznajomymi. Umiejętność małoletnich w korzystaniu z Internetu i powiązanych z nim aplikacji do nękania i zastraszania cały czas budzi troskę rodziców i nauczycieli, a także samych dzieci i młodzieży. Młodzi ludzie zgłaszają różne formy cyberprzemocy, w szczególności prześladowanie, zastraszanie, obrażanie, co zostało zobrazowane na poniższym wykresie:

Wykres 4

Jeżeli spotkałeś(-łaś) się ze zjawiskiem ceberprzemocy (obojętnie kogo dotyczyło), to było to:

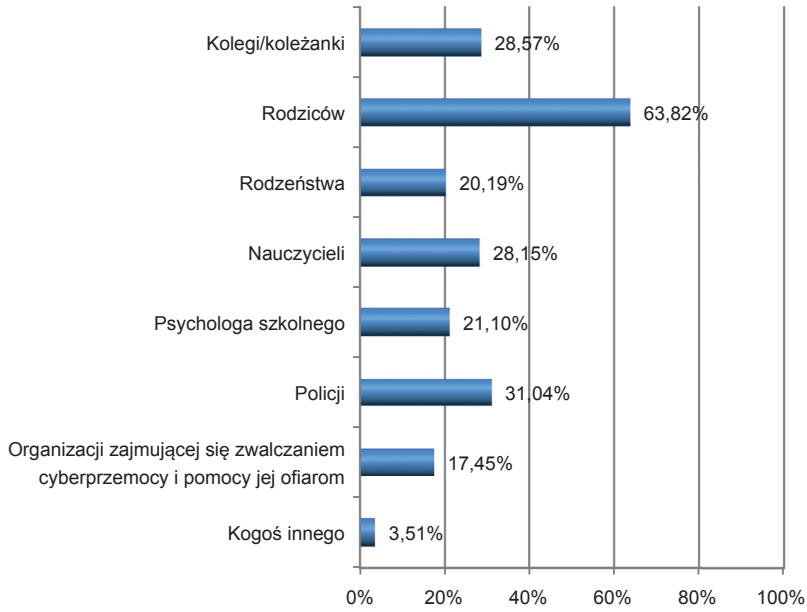


Źródło: opracowanie własne

Dzieci na ogół potrafią poradzić sobie z doświadczeniem negatywnych komentarzy, które nie są bezpośrednio ukierunkowane na nie, jednak gdy zachowanie innych użytkowników Internetu staje się bardziej osobiste i ukierunkowane na nie, czują się bardziej zagrożone. W tych momentach dzieci częściej szukają pomocy u rodziców i znajomych bądź zgłaszają swoje problemy m.in. na platformach mediów społecznościowych, policji czy w organizacjach pozarządowych (wykres 5). Kiedy doświadczenia są trwałe, dzieci mają trudności z powiedzeniem o zagrożeniach komukolwiek, a to pogarsza negatywny wpływ ich doświadczeń.

Wykres 5

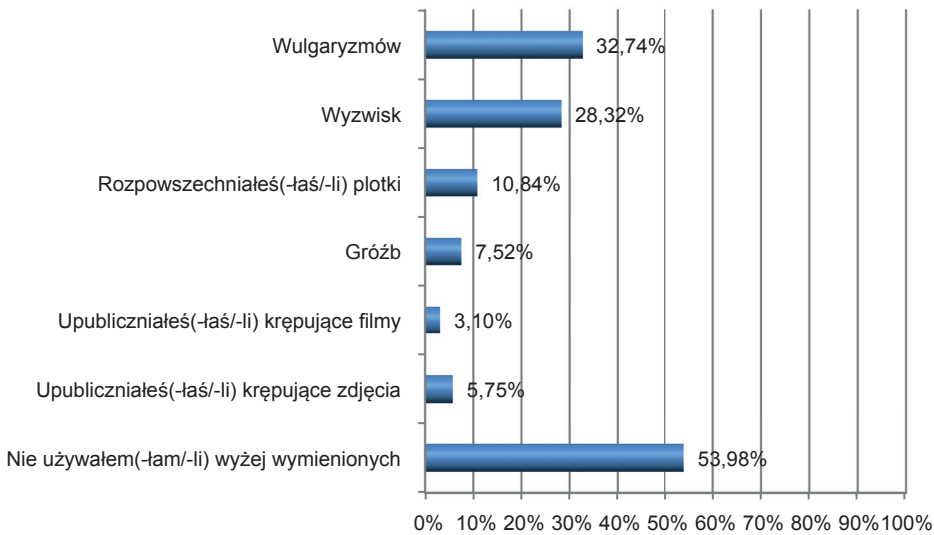
Gdybyś szukał(-ła) pomocy dotyczącej cyberprzemocy, to zwróciłbyś(-łabyś) się do:



Źródło: opracowanie własne

Wykres 6

Czy Ty lub Twoi znajomi kiedykolwiek używaliście w Internecie:



Źródło: opracowanie własne

Natura internetowej nienawiści, na którą narażeni są młodzi ludzie, to w szczególności wulgaryzmy, wyzwiska, groźby, upubliczniane filmy i zdjęcia (wykres 6). Często tego typu zachowania doprowadzają młodych ludzi do niezrozumienia, dlaczego inni chcą ich skrzywdzić. Negatywne skutki cyberdokuczania obejmują obniżenie samooceny, trudności z nawiązywaniem relacji, a także problemy ze zdrowiem psychicznym.

Postęp technologiczny i rozwój kultury medialnej wykształca w społeczeństwie nowe trendy i zachowania. Jednym ze znamion zachowań wśród współczesnej młodzieży jest *sexting* — zjawisko, które powstało na początku XXI w. Etymologia słowa wywodzi się z języka angielskiego i jest ono połączeniem dwóch słów *sex* (odnoszącego się do współżycia seksualnego) i *texting* (odnoszącego się do pisania wiadomości)[6]. *Sexting* jest jednym w wielu zachowań zaliczanych do cyberprzemocy.

„Sexting oznacza wysyłanie roznegliżowanych zdjęć lub krótkich filmów o treści erotycznej do innej osoby. Zazwyczaj przesyłanie takich materiałów odbywa się za pomocą telefonu komórkowego lub smartfona i Internetu. Możemy tu wyróżnić dwa rodzaje zachowań: samoistne wykonanie fotografii lub krótkiego filmu i dobrowolne wysłanie do osoby, z którą nie wiąże nadawcy relacja seksualna, oraz samoistne wykonanie własnej fotografii lub filmu (bądź zgoda na wykonanie tej czynności przez osobę zaufaną) i dobrowolne wysłanie bądź przekazanie osobie (chłopakowi, dziewczynie), z którą wiąże nadawcę relacja seksualna”[7].

Mając na uwadze charakter zdjęć i filmików, zjawisko określane jest również jako autopornografia. Dzieci traktują to jako dobrą zabawę i nie zdają sobie sprawy z zagrożeń wynikających z takiego zachowania. Zdjęcia czy filmy wysyłane są najczęściej w celu zrobienia osobie żartu, ośmieszenia i upokorzenia jej, ale także szantażu, aby wymusić na niej określone działanie. Rozpowszechnianie zdjęć i filmów *online* przez małoletnich jest częścią codziennego ich życia, a tworzenie i dzielenie się swoimi wyobrażeniami seksualnymi ciągle budzi niepokój wszystkich zainteresowanych stron.

Powszechny i łatwy dostęp do Internetu, zarówno dorosłych, jak i dzieci oraz młodzieży, stworzył zagrożenie na niespotykaną dotąd skalę w postaci prezentowania treści pornograficznych — również z udziałem osób małoletnich. Pornografia jest obecna w kulturze informacyjnej głównie za pośrednictwem Internetu, zaś kontakt z pornografią, a także inicjacja seksualna zaczynają się w coraz młodszym wieku. Wyniki badań wskazują, że kontakt małoletnich z treściami pornograficznymi często odbywa się w sposób niezamierzony, np. poprzez otwieranie wyskakujących okienek, złudnie nazwanych witryn czy reklam na nielegalnych stronach streamingowych (z transmisją na żywo). W różny sposób odbywa się pozycjonowanie zasobów, polepszając widzialność danej witryny i promując

[6] T. Biernat, J. Gierszewski, *Wielowymiarowość bezpieczeństwa środowiska wychowawczego*, Chojnice 2014, s. 20.

[7] W. Ronatowicz, *Ryzykowne zachowania seksualne dzieci, młodzieży i młodych dorosłych w kontekście korzystania z technologii cyfrowych*, „Rocznik Lubuski” 2014, t. 40, cz. 1, s. 130.

odpowiednią stronę w wyszukiwarce. Wobec tego narażenie na pornografię ma negatywny wpływ na przekonania seksualne dzieci i młodzieży.

W literaturze przedmiotu można odnaleźć podział na trzy grupy przestępczości zawiązanej w pornografią. „W pierwszej grupie znajdować się będą te przestępstwa, które pozbawione są fizycznego kontaktu i polegają zasadniczo na ekshibicjonizmie, fetyszyzmie, prezentowaniu pornografii oraz robieniu zdjęć dziecka w pornograficznych celach. Do grupy drugiej autor zalicza te z przestępstw, które są związane z fizycznym kontaktem z dzieckiem, i zalicza tu np. różnego rodzaju pieszczoty z dzieckiem, posiadające wyraźnie seksualny charakter, oraz masturbację, stosunki analne i seksualne. W grupie ostatniej ulokowane zostały akty fizyczne, posiadające znamiona gwałtu, wywołujące w danej chwili bądź później różnego typu uszkodzenia ciała ofiary”[8]. Zaznaczyć tutaj trzeba, że grupy przestępcze skupiają swoją działalność na terenach, na których czują się anonimowo, a działania policji są mało skuteczne.

„Zasadnicze problemy prawno-karne związane z szeroko pojętą pornografią zostały rozstrzygnięte już wiele lat temu. Rozwój technologiczny i społeczny przynosi jednak ze sobą kolejne wątpliwości i dylematy dotyczące tej problematyki”[9].

Odnosząc się do krótkiej charakterystyki wybranych zagrożeń wobec małoletnich użytkowników Internetu, nasuwa się pytanie: jak reagować na zagrożenia i w jaki sposób zapewnić bezpieczeństwo małoletnim w Internecie?

Aby ustrzec się od zagrożeń związanych z korzystaniem ze smartfonów i innych urządzeń zapewniających dostęp do Internetu, należy zastosować się do kilku podstawowych porad przedstawionych poniżej:

1. Rodzic:

a) rozmawiaj z dzieckiem na temat bezpiecznego korzystania z Internetu — będzie ono wtedy wiedziało, że z napotkanym problemem może udać się do rodzica. Z kolei rodzicowi pomoże to zrozumieć kwestię ewentualnych niebezpieczeństw,
b) omów z dzieckiem netykietę internetową, tj. zasady kultury oraz przyzwoitego zachowania w Internecie,
c) poznawaj sieć razem z dzieckiem — wskazanie właściwych zachowań, a także potencjalnych zagrożeń przyczyni się do wzrostu świadomości dziecka na temat tego, jakie treści znajdują się w Internecie,
d) wyjaśnij dziecku w jaki sposób może korzystać z prywatności ustawień, aby mieć gwarancję, że jedynie dodani znajomi widzą zamieszczone przez nie posty i obrazy,
e) ustal dziecku limity korzystania z Internetu,

[8] M. Podgajna-Kuśmierek, *Pedofilia: zarys zagadnienia*, Kraków 2003, s. 34.

[9] K. Gienas, *Pseudopornografia dziecięca oraz posiadanie treści pornograficznych z udziałem małoletnich z punktu widzenia funkcjonowania Internetu — dylematy ustawodawcy* [w:] J. Kosiński (red.), *Przestępczość teleinformatyczna*, Szczytno 2004, s. 49–50.

f) przed wręczeniem dziecku nowego urządzenia zainstaluj na nim oprogramowanie zabezpieczające, chroniące przed cyberzagrożeniami i blokujące nieodpowiednie treści oraz systematycznie je aktualizuj;

2. Dziecko:

a) nie pozwalaj nikomu używać smartfona podczas Twojej nieobecności,
b) blokuj klawiaturę urządzenia po każdym użyciu,
c) używaj zabezpieczenia w postaci kodu pin,
d) nie podawaj swoich numerów komórkowych w trakcie rozmów prowadzonych w Internecie, aby uniknąć stalkingu,
e) nie odpowiadaj na wiadomości otrzymane od nieznajomych,
f) nie wysyłaj prywatnych zdjęć, filmów osobom nieznanym, a także sprawdź ustawienia oznaczania, tj. tagowania (ang. *tagging*), aby podczas udostępniania zdjęć, Twoja tożsamość nie została ujawniona,
g) nie uruchamiaj podejrzanych linków załączonych do wiadomości,
h) nie przekazuj smartfonów do nieautoryzowanych punktów serwisowych, aby uniknąć powielenia treści,
i) wyczyść wszystkie informacje przechowywane w urządzeniu przed jego sprzedażą,
j) utrzymuj fizyczną kontrolę nad urządzeniem, aby uniknąć kradzieży,
k) w przypadku kradzieży telefonu powiadom najbliższą jednostkę policji oraz dostawcę w celu zablokowania urządzenia.

Mówiąc o bezpieczeństwie internetowym małoletnich, w opinii autora artykułu należy położyć nacisk w szczególności na niżej wymienione zadania:

— rozszerzanie międzynarodowego zasięgu w zakresie komunikacji i wymiany informacji,
— zabieganie o dostosowywanie krajowych norm do prawa międzynarodowego,
— wymianę poglądów pomiędzy ekspertami w zakresie wymiany dobrych praktyk,
— dbałość o ciągłe podnoszenie poziomu wiedzy oraz umiejętności kadry nauczycielskiej i innych profesjonalistów pracujących z dziećmi w trosce o ich bezpieczeństwo internetowe,
— mobilizowanie dzieci i młodzieży do brania udziału w konkursach dotyczących bezpieczeństwa online.

Zagrożenia internetowe ściśle powiązane są z **usługami** świadczonymi *online*. Poniżej przedstawiona została krótka charakterystyka tych usług, do których zalicza się:

1. **Czatowanie** — odbywa się za pomocą serwisów, poprzez które można prowadzić rozmowę. Mogą to być oczywiście wiadomości tekstowe, połączenia głosowe lub połączenia wideo. Czatowanie to doskonały sposób na pozostawianie w kontakcie ze znajomymi, a także zawieranie nowych znajomości. Aby zachować bezpieczeństwo podczas czatowania, należy pamiętać o kilku podstawowych zasadach:

a) mieć pewność z kim prowadzona jest rozmowa i prowadzić ją „twarzą w twarz”,

b) wystrzegać się osób, które zasłaniają się brakiem kamery internetowej lub jej awarią,
c) wystrzegać się udostępniania jakichkolwiek danych osobowych osobom, których nie znamy,
d) stworzyć listę znajomych i blokować osoby niepożądane w kontaktach,
e) sprawdzić, w jaki sposób zapisywać rozmowy z czatów,
f) zachować ostrożność, gdyż osoba po drugiej stronie kamery może nagrywać rozmowę,
g) rodzice powinni dokładnie zapoznać się z czatem, z którego korzystają ich dzieci;

2. **Udostępnianie i pobieranie treści** — to działanie związane z przesyłaniem informacji, jak np. teksty, zdjęcia, filmy i inne. Dzielenie się takimi informacjami może skutkować tym, że udostępnione treści mogą zostać rozpowszechnione bez zgody autora i pozostawać w Internecie przez dłuższy okres. W związku z tym należy pamiętać o:

a) zapoznaniu się z ustawieniami prywatności, aby nikt nie był w stanie przejąć kontroli nad naszą treścią,
b) zachowaniu prywatnych danych osobowych, jak np. nazwa szkoły, adres e-mail, numer telefonu, data urodzenia, i udostępnianiu ich tylko osobom, które znamy i którym ufamy,
c) ignorowaniu stron nieznanych i budzących podejrzenia co do zawartości,
d) nieotwieraniu w wiadomościach e-mail załączników i linków podejrzanie wyglądających bądź takich, których się nie spodziewamy,
e) przestrzeganiu praw autorskich, gdyż pobrany materiał może pochodzić z nielegalnego źródła, a także zawierać wirusy, które mogą wyrządzić szkody na komputerze,
f) stosowaniu programów antywirusowych i zapór ogniowych,
g) poprawnym wylogowaniu z witryny po jej użyciu;

3. **Granie w gry** — może stanowić zabawę przy wykorzystaniu smartfonów, komputerów, konsoli do gier, a także współzawodnictwo w wirtualnym świecie 3D. Grając, należy pamiętać o:

a) obowiązujących zasadach, a także szanowaniu innych uczestników,
b) wyborze takiej nazwy użytkownika, aby nie ujawniała danych osobowych czy szczegółów profilu społecznościowego,
c) możliwościach zablokowania osób niepożądanych,
d) stosowaniu regularnych przerw w grze, a także pilnowaniu nieprzekraczania granic czasowych mogących mieć negatywny wpływa na zdrowie,
e) korzystaniu (przy zakupie gier) z europejskiego systemu oceniania gier komputerowych (ang. *Pan European Game Information*),
f) korzystaniu z gier od legalnych i renomowanych dostawców usług internetowych;

4. **Dokonywanie zakupów** — to działanie pozwalające na prowadzenie transakcji online. Należy pamiętać, że zakupy takie mogą przynosić korzyści, ale także ryzyko natknięcia się na oszustów, dlatego też trzeba pamiętać o tym, że:

a) „nie wszystko złoto, co się świeci", co oznacza, że zbyt korzystna oferta internetowa nie zawsze musi być prawdziwa i tak dobra, jak się wydaje,
b) należy sprawdzać obiektywne opinie o sprzedawcach internetowych,
c) można paść ofiarą oszustwa internetowego, jeśli nie sprawdzi się sklepu internetowego, np. jego fizycznego adresu, danych kontaktowych, numeru telefonu itp.

Mimo nowych technologii oraz dostosowywania do nich systemu prawnego, społeczeństwo wciąż będzie narażone na porażki aż dostatecznie nie rozwinie swojego systemu bezpieczeństwa polegającego na wzajemnym informowaniu o zagrożeniach płynących ze strony Internetu.

Metodą prawdopodobnie najlepszą zapewniającą ochronę w wirtualnym świecie jest opieka i pomoc rodziców. Nic nie zastąpi wspólnego surfowania rodziców z dziećmi (połączonego z edukacją w zakresie wykorzystania zasobów internetowych, a także unikania internetowych zagrożeń), gdyż to człowiek stanowi najsłabsze ogniwo wszelkich systemów zabezpieczeń — także internetowych.

Słowa kluczowe: Internet, dziecko, małoletni, sieć ogólnoświatowa, wirtualny świat, Policja

Keywords: Internet, child, World Wide Web, virtual world, Police

Streszczenie: Zarówno w świecie realnym, jak i w cyberprzestrzeni przestępcy wykorzystują nowoczesne technologie do popełniania złych czynów. Zapobieganie i zwalczanie zagrożeń występujących w Internecie wymaga współpracy organów ścigania, wymiaru sprawiedliwości, placówek edukacyjno-wychowawczych oraz organizacji pozarządowych. W artykule podjęto próbę spojrzenia na aspekt bezpieczeństwa internetowego małoletnich i zawarto w nim podstawowe informacje dotyczące wybranych zagrożeń internetowych, a także porady dotyczące zapewnienia dziecku bezpieczeństwa w Internecie.

Summary: In the real world as well as in cyberspace, criminals use modern technologies to commit bad deeds. Preventing and combating threats occurring on the Internet requires cooperation of law enforcement agencies, the judiciary, educational institutions and non-governmental organizations. The article attempts to look at the aspect of internet security for minors and contains basic information about selected online threats, as well as advice on ensuring the child's safety on the Internet.