Interdyscyplinarne Studia Społeczne
Numer 1 (3), 2017

Krzysztof Ciemcioch
Politechnika Łódzka, Centrum Komputerowe

Cyfrowe bezpieczeństwo uczniów w szkole – wyzwania i zagrożenia

Streszczenie: Szkoła jako instytucja użytku publicznego zobowiązana jest do zapewnienia swoim uczniom maksymalnego bezpieczeństwa, tego fizycznego, ale również tego związanego z bezpieczeństwem cyfrowym. W artykule autor przybliża wyzwania, jakie są stawiane przed szkołami w Polsce dla zapewnienia odpowiedniego poziomu bezpieczeństwa uczniów i pracowników placówek oświatowych oraz najważniejsze zagrożenia, których oddziaływanie wpływa zarówno na zdrowie psychiczne jak i fizyczne osób narażonych na te niebezpieczeństwa. Niniejszy tekst może stanowić dobry punkt wyjścia dla lepszego przygotowania uczniów, nauczycieli i rodziców do identyfikowania, wykrywania, zabezpieczania się przed cyberzagrożeniami, które są ujęte również w strategii rozwoju i bezpieczeństwa państwa. Zagrożenia związane z korzystaniem z sieci przez dzieci i młodzież (również dorosłych) nie tylko w szkołach, można ściśle połączyć z ogólnymi zagrożeniami bezpieczeństwa informacyjnego.

Słowa kluczowe: cyfrowa szkoła, cyfrowy uczeń, cyfrowy nauczyciel, bezpieczeństwo informacyjne, zagrożenia w sieci, bezpieczeństwo cyfrowe

Wstęp

Żyjemy w społeczeństwie informacyjnym, w czasach szybko zmieniającej się rzeczywistości cyfrowej. Wszelkie zmiany zachodzące na świecie, zarówno te polityczne, gospodarcze, ale przede wszystkim technologiczne, powodują zmiany w świadomości społeczeństwa. Zmiany te w głównej mierze dotyczą powszechnego dostępu do informacji. Analizując badania *Diagnozy Społecznej* na przestrzeni kilku lat można zaobserwować ciągły wzrost dostępu do sieci internetowej przez społeczeństwo w różnych grupach wiekowych (Batorski 2015, s. 373). Postęp technologiczny w postaci mobilnego dostępu do sieci internetowej pozwolił jeszcze skuteczniej czerpać z dostępu do informacji. Polacy chętnie korzystają z tej formy pozyskiwania różnego rodzaju informacji, która potrzebna jest im do zaspokojenia codziennych czynności. Społeczeństwo w natłoku wiadomości musi zadbać o podnoszenie własnych kompetencji cyfrowych, niezbędnych do gromadzenia, przetwarzania, ochrony i odpowiedniego wykorzystania danych i informacji.

Celem artykułu jest wskazanie najważniejszych zagrożeń płynących z sieci dla uczniów (nie tylko w murach szkolnych) oraz sposoby na zabezpieczenie ich przed niepowołanym wykorzystaniem w placówkach oświatowych. W artykule autor przybliża wyzwania, jakie są stawiane przed szkołami w Polsce dla zapewnienia odpowiedniego poziomu bezpieczeństwa uczniów

i pracowników placówek oświatowych. Edukacja młodego pokolenia dotycząca bezpieczeństwa informacyjnego, bezpiecznego korzystania z sieci internetowej jest najważniejszym zadaniem nie tylko dla nauczycieli, ale również dla rodziców. Ważnym aspektem jest również świadomość ciągłego podnoszenia własnych kompetencji w zakresie możliwości i niebezpieczeństw cyberprzestrzeni (Andrzejewska 2014). Jak wynika z badań, społeczeństwo zdaje sobie sprawę z zagrożeń, ale niestety nie wszyscy wiedzą jak je rozpoznawać i jak się przed nimi chronić, nie posiadają to tego odpowiedniego przygotowania i kompetencji (Tomczyk, Srokowski 2016). Niniejszy tekst może stanowić dobry punkt wyjścia dla lepszego przygotowania uczniów, nauczycieli i rodziców do identyfikowania, wykrywania, zabezpieczania się przed cyberzagrożeniami, które są ujęte również w strategii rozwoju i bezpieczeństwa państwa (*Doktryna bezpieczeństwa informacyjnego RP* 2015).

Bezpieczeństwo informacyjne

Bezpieczeństwo informacyjne to bardzo rozległy temat obejmujący swoim zasięgiem większość dziedzin życia ludzkiego, które związane jest nierozłącznie z wszelkimi formami (także werbalnymi) wymiany, przechowywania i przetwarzania informacji (Liderman 2012, s. 22). Już od początków działalności człowieka informacja była źródłem bardzo pożądanym, można rzec, iż ten kto posiadał informacje w większości przypadków wykorzystywał ją dla osiągnięcia własnych celów – przede wszystkim zdobycia dóbr materialnych, lepszego statusu społecznego oraz władzy. Konieczność ciągłego gromadzenia informacji, przetwarzania jej i manipulowania nią, wywołała również potrzebę odpowiedniego zabezpieczania jej, tzw. ochronę informacji. „Zatem informacja i działania mające na celu jej wykorzystanie i ochronę towarzyszyły człowiekowi od zawsze, ale w ostatnich latach wraz z coraz szybszym rozwojem techniki i związanymi z tym zmianami cywilizacyjnymi nabrały szczególnego znaczenia" (Liderman 2012, s.11).

Zagadnienia o zarządzaniu bezpieczeństwem w życiu człowieka oraz o ochronie informacji były podejmowane znacznie wcześniej przed tym, kiedy to W.I. Jaroczkin wskazał potrzebę wyodrębnienia nowej dyscypliny naukowej – securitologii (Jaroczkin 2000). W Polsce również naukowcy podejmowali badania dotyczące bezpieczeństwa (zob: Świniarski 1999, s. 20; Pioch, 2004, s. 9; Korzeniowski 2008), co w efekcie przyniosło zaliczenie nauk o bezpieczeństwie do obszaru i dziedziny nauk społecznych (za: Liderman 2012; Dz. U. Nr 179 z dn. 8.08.2011, poz. 1065).

Dynamicznie rozwijająca się gospodarka oraz rozwój telefonii komórkowej, mobilnych urządzeń z dostępem do sieci internetowej i ciągły nieograniczony rozwój usług i portali społecznościowych spowodowały, iż zapewnienie bezpieczeństwa informacyjnego stało się jednym z najważniejszych zadań, nie tylko pojedynczych firm, ludzi zajmujących się zabezpieczaniem

informacji (z racji wykonywanego zawodu), ale również globalnie, dla wszystkich państw, które są świadome nieodpowiedniego wykorzystania informacji. Dzisiejsze społeczeństwo informacyjne zdaje sobie sprawę z ważności posiadania informacji, jej gromadzenia, przetwarzania oraz ryzyka zagrożeń, jakie niesie za sobą jej przechowywanie (Globan-Klas, Sienkiewicz 1999). Aleksandrowicz charakteryzuje to społeczeństwo cechami konstytutywnymi, poprzez: nadanie „zasobom informacyjnym rangi zasobów strategicznych" oraz „bezpieczeństwem informacyjnym jako istotnym elementem bezpieczeństwa społecznego" (Aleksandrowicz 2016, s. 24-25).

Analizując wyniki z badań dotyczące społeczeństwa informacyjnego w Polsce, można zauważyć, iż od kilkunastu lat zwiększa się zapotrzebowanie na zdobywanie informacji za pośrednictwem sieci szerokopasmowego Internetu poprzez komputer, a w ostatnich latach poprzez telefon lub smartfon (Jasiewicz 2017; Batorski 2016). Na potwierdzenie wcześniejszych badań można przytoczyć badania prowadzone przez Fundację Orange, z których wynika, że Polacy chętnie korzystający z informacji zgromadzonych w Internecie uważają je za godne zaufania (21% całkowicie wiarygodne, 45% godne zaufania) (*Kompetencje cyfrowe młodzieży w Polsce (14-18 lat)* 2013). Niestety bez odpowiedniej edukacji nie jesteśmy w stanie zachować odpowiedniego bezpieczeństwa związanego z selekcją informacji, jakie docierają do nas. Widać, że nie zawsze społeczeństwo ma czas lub umiejętności by weryfikować zdobyte informacje, co wiąże się ze zwiększonym zagrożeniem bezpieczeństwa informacyjnego. Piotr Sienkiewicz pisze, że „o bezpieczeństwie jest sens mówić, jeżeli istnieje – realne bądź potencjalne – niebezpieczeństwo, czyli zagrożenia, które niosą za sobą nie zawsze uświadomione ryzyko" (Sienkiewicz, 2015 s. 7).

Zawsze istnieje ryzyko, że informacje znalezione w internecie okażą się niewiarygodne, specjalnie spreparowane, by wprowadzić odbiorców w błąd. W obecnej rzeczywistości dezinformacja, manipulacja, trollowanie są na porządku dziennym. Katarzyna Derlatka opisuje cztery czynniki mające wpływ na treść przekazu prezentowanych informacji, jako przyczynę tego zjawiska oraz zwraca uwagę, iż na tego typu zagrożenia informacyjne szczególnie narożne „są dzieci i ludzie z niskim wykształcaniem" (Derlatka 2016). Dlatego jednym z najważniejszych działań „w tworzeniu bezpiecznego społeczeństwa jest […] szeroko rozumiana edukacja na rzecz bezpieczeństwa. Poprzez odpowiednie przygotowanie społeczeństwa, od najmłodszych lat, można wykryć i przeciwdziałać różnym zagrożeniom. Jedną z podstawowych dróg kształtowania bezpieczeństwa informacyjnego jest edukacja, która wpływa na postawy, wartości, zachowania i umiejętności niezbędne w zapobieganiu, radzeniu sobie w sytuacji zagrożeń a także niwelowaniu ich skutków" (Piotrowski 2012, s. 7).

Zagrożenia płynące z sieci

W literaturze związanej z bezpieczeństwem informacyjnym można znaleźć różne klasyfikacje, podziały zagrożeń oddziałowujących na państwa, firmy, szkoły oraz jednostki. Lidia Więcaszek-Kuczyńska podjęła próbę zebrania i przedstawienia najważniejszych tez i opinii badaczy, z których wynika, „iż źródłem zagrożeń bezpieczeństwa informacyjnego jest człowiek […], który może wykorzystywać różnorakie techniki włamań do systemów informacyjnych" (Więcaszek-Kuczyńska 2014, s. 218-219).

W zmieniającym się cyfrowym świecie, lista i skala potencjalnych zagrożeń płynących ze świata wirtualnego ulega nieustannym modyfikacjom i ciągle się wydłuża. Łukasz Tomczyk i Łukasz Srokowski po przeprowadzonych badaniach dotyczących „teoretycznych aspektów kompetencji związanych z bezpieczeństwem cyfrowym w polskich szkołach" zwrócili uwagę na fakt, że „wszystkie grupy badanych wykazują niewystarczający poziom kompetencji do radzenia sobie z zagrożeniami cyfrowymi" (Tomczyk, Srokowski 2016). Autorzy raportu wykazali, że dla każdej z badanych grup wiekowych zagrożenia są podobne, choć wraz ze wzrostem wieku badanych, pojawiają się nowe zagrożenia, do walki z którymi nie posiadają odpowiednich kompetencji.

Zagrożenia związane z korzystaniem z sieci przez dzieci i młodzież (również dorosłych) nie tylko w szkołach, można ściśle połączyć z ogólnymi zagrożeniami bezpieczeństwa informacyjnego. Poniżej przedstawiam opracowane na podstawie zebranej literatury najważniejsze zagrożenia, których oddziaływanie wpływa zarówno na zdrowie psychiczne jak i fizyczne osób narażonych na te niebezpieczeństwa. W literaturze przedmiotu można znaleźć podziały na zagrożenia o charakterze technicznym, społecznym i zdrowotnym, które mogą się łączyć i występować łącznie w różnych kategoriach.

Podział zagrożeń:

1. Zagrożenia zdrowotne.
    a. Choroby układu wzrokowego.
    b. Choroby układu mięśniowo-szkieletowego (szczególnie kręgosłup i kończyny górne – nadgarstki).
    c. Choroby układu krążeniowego (szczególnie kończyn dolnych)
    d. Choroby psychiczne – lęki, depresje itd.

2. Zagrożenia społeczne.

   a. Niebezpieczne treści – prezentujące przemoc, okrucieństwo wobec ludzi i zwierząt, nawoływanie do nietolerancji (mowa nienawiści) i wrogości wobec innych narodów i kultur (hejt internetowy), zażywania niebezpiecznych i szkodliwych używek, a nawet samookaleczeń i samobójstw, treści wywołujące u odbiory negatywne emocje, werbowanie do sekt.

   b. Trollowanie – zachowanie mające na celu przeszkodzenie w dyskusji, poprzez zadawanie dużej ilości zbędnych pytań, napastliwość, próbę ośmieszania, wywoływanie burzliwej dyskusji, prowadzącej do kłótni; metoda najczęściej wykorzystywana na forach internetowych, w mediach społecznościowych.

   c. Reklamy w internecie – treści reklam niedostosowane do wieku oglądających, manipulacja świadomością internauty.

   d. Naruszenia praw autorskich – nielegalne przesyłanie danych, archiwizowanie danych w sieci pochodzących z nielegalnej dystrybucji i rozpowszechnianie plików i danych chronionych prawem autorskim.

   e. Niebezpieczne kontakty, uwodzenie w internecie (child grooming) – dzieci (poniżej 15 r.ż.) samodzielnie korzystające z internetu są narażone na kontakty z obcymi osobami podszywającymi i podającymi za kogoś innego niż są w rzeczywistości. Działania podejmowane przez sprawcę nastawione są na nawiązanie więzi emocjonalnej z dzieckiem w celu zdobycia jego zaufania, uwiedzenia i wykorzystania.

   f. Seksting, prowokacyjne zachowania i aktywność seksualna – szczególnie niebezpieczna gdy traktowana jest jako źródło dochodu osób nieletnich, ryzykowne zachowania dzieci przed kamerami internetowymi oraz urządzeniami mobilnymi (smartfonami).

   g. Agresja elektroniczna (cyberprzemoc) – rodzaj przemocy takiej jak: wyzywanie, ośmieszanie, prześladowanie, oczernianie, poniżanie kogoś w internecie lub przy użyciu urządzeń mobilnych.

   h. Nadużywanie internetu (uzależnienie od internetu, infoholizm, siecioholizm) – związane jest przede wszystkim z czasem spędzonym w sieci internetowej, intensywnością korzystania z internetu, przy równoczesnym zaniedbywaniu innych aktywności, co wpływa na pogorszenie podstawowych sfer życia człowieka.

i. Zagrożenia prywatności – brak odpowiednich ustawień szczególnie w korzystaniu z portali społecznościowych może spowodować nieprzyjemności poprzez np. kradzież tożsamości, publikację niechcianych materiałów na swoim koncie.

3. Zagrożenia techniczne.

a. Słabe hasła – zbyt krótkie i bazujące na popularnych słowach kluczowych hasło może być powodem włamań i utraty danych i środków pieniężnych w przypadku bankowości internetowej.

b. Szkodliwe oprogramowanie (malware) – złośliwe oprogramowanie mające na celu zniszczenie komputera i wszelkich danych w nim zapisanych. Najczęściej spotykane to : wirusy komputerowe, konie trojańskie, robaki oprogramowanie szpiegujące itd.

c. Ransomware – wirus, który wymusić okup na użytkowniku, poprzez blokadę lub szyfrowanie dysku. Po zapłaceniu okupu nie ma gwarancji odzyskania swoich wszystkich danych i nie ma pewności, czy ataki tego typu nie będą następowały w przyszłości.

d. Spam – niechciane wiadomości elektroniczne, szczególnie masowo wysyłane reklamy, fałszywe faktury, wysyłane z przejętych kont pocztowych lub wyspecjalizowanych firm reklamowych.

e. Zagrożenia przez surfowanie (*drive by download*) - przeglądanie i pobieranie plików ze stron www, ściąganie szkodliwego oprogramowania z zainfekowanych serwisów korzystając z przeglądarki internetowej.

f. BOTnety – sieci atakujących komputerów przejętych przez cyberprzestępców najczęściej poprzez szkodliwe oprogramowanie, sprawcy mogą dokonywać nielegalnych operacji bez wiedzy właściciela komputera.

g. Ataki typu blokowanie usług (DoS, DDoS) – atak powodujący blokadę serwisów internetowych poprzez zalewanie z internetu dużą ilością danych, z którymi serwer nie może sobie poradzić, powiązane jest to z BOTnetami.

h. Ataki socjotechniczne (phishing) – nakłanianie użytkowników metodami socjotechnicznymi do ujawniania swoich danych wrażliwych, szczególnie chodzi o wyłudzenie loginów, identyfikatorów, haseł, numerów i dat ważności kart kredytowych, by posłużyły w późniejszym czasie do dokonywania oszustw. Najczęściej informacje przesyłane poprzez pocztę elektroniczną bądź jako okazje na portalach społecznościowych.

i. Włamania na strony internetowe lub do wewnętrznych systemów komputerowych (serwer i sieci LAN) – możliwość utraty danych np. osobowych, finansowych; strona www może być podmieniona, dzięki czemu może zawierać szkodliwe oprogramowanie lub przekierowywać na niepożądane strony; poprzez sieci LAN możliwość pobierania duże ilości nielegalnego oprogramowania, możliwość wykorzystania komputerów w sieci do stworzenia BOTnetu i ataków typu Dos.

Źródło: opracowanie własne na podstawie: Andrzejewska 2013; Korusiewicz 2007; Liderman 2012; Lizut 2015; Makaruk 2013; Pyżalski 2012; Sokół 2004; Tomczyk, Srokowski 2016; Więcaszek-Kuczyńska 2014; Wrona 2014.

Powyższa lista nie wyczerpuje wszystkich istniejących zagrożeń i każdy czytelnik może do niej dołożyć własne lub nowopowstające zagrożenia. Przedstawione zostały najczęściej występujące niebezpieczeństwa na które narażone są osoby korzystające z sieci internetowej nie tylko w placówkach oświatowych, ale i poza fizycznymi murami szkoły. Lista może być dobrym punktem wyjścia przy omawianiu zagrożeń i zachowań w sieci z uczniami na lekcji oraz do tworzenia planów reagowania w sytuacjach występowania tego typu sytuacji kryzysowych.

Bezpieczeństwo cyfrowe (informacyjne) w szkołach

Szkoła jako instytucja użytku publicznego zobowiązana jest do zapewnienia swoim uczniom maksymalnego bezpieczeństwa, tego fizycznego, ale również tego związanego z bezpieczeństwem cyfrowym. Wychodząc naprzeciw wyzwaniom współczesnego świata, dla zapewnienia odpowiedniego poziomu bezpieczeństwa, szkoła powinna działać na dwóch równoległych płaszczyznach: administracyjno-inwestycyjnej i dydaktyczno-wychowawczej. Pierwsza daje możliwość dyrekcji wyposażenia szkoły w zabezpieczoną infrastrukturę informatyczną, stanowiącą „istotny fundament organizacji szkoły, i to zarówno na gruncie dydaktyczno-wychowawczym, opiekuńczym, jak i zarządzania instytucją" (Stachecki 2013).

Placówka organizująca przestrzeń dostępu do sieci internetowej, platformy edukacyjne oraz dostęp do zasobów umieszczonych w chmurach, musi być wyposażona w profesjonalne urządzenia informatyczne, zapewniające możliwość nadzorowania całej sieci szkolnej. Urządzenia wykorzystywane do tworzenia sieci nie powinny być dedykowane do użytku domowego, ponieważ nie gwarantują one dobrego poziomu bezpieczeństwa. Podstawą infrastruktury informatycznej jest zakup wydajnego, dobrej jakości serwera z macierzą dyskową (wraz z oprogramowaniem), która umożliwi codzienne wykonywanie kopii bezpieczeństwa danych oraz zastosowanie rutera klasy UTM do administrowania siecią LAN w szkole. Urządzenia tego typu posiadają możliwości konfiguracji m.in. zapory sieciowej, wykrywania i blokowania prób włamań do systemu,

ograniczania niechcianych wiadomości poprzez program antywirusowy oraz kontrolowanie treści dostępnych przez użytkowników sieci. (Andrzejewski 2016) Wykorzystanie rutera pozwala na skonfigurowanie i zabezpieczenie sieci, tak by mogła powstać osobna infrastruktura zapewniająca nieograniczoną działalność związaną z zarządzaniem placówką, szczególnie od strony kadrowo-księgowej oraz podsieć obsługującą pracownie dydaktyczne, czyli podsieć na komputery w salach lekcyjnych i pracowniach komputerowych (obie sieci zabezpieczone hasłami). Szkoła powinna również posiadać osobną bezprzewodową sieć Wi-Fi dla gości, z której mogą również korzystać uczniowie w trakcie przerw.

Dorota Janczak zwraca uwagę właśnie na to, że „musimy zadbać o bezpieczeństwo uczniów (ograniczanie dostępu do nieodpowiednich treści, zabezpieczenie przed włamaniami, wirusami itd.) oraz o bezpieczeństwo danych przechowywanych w szkole. Dlatego udostępniana sieć Wi-Fi musi być odpowiednio zabezpieczona przed atakami z zewnątrz, filtrowana i oddzielona od sieci administracyjnej szkoły" (Janczak 2013, s. 35-36). Opisane działania są niestety wprowadzane w niewielkiej liczbie szkół. Piotr Plichta przytacza dane MEN, z których wynika, że w rzeczywistości sytuacja placówek oświatowych nie jest najlepsza pod względem bezpieczeństwa online, ponieważ „wbrew ustawowym wymogom 62% szkół nie zabezpieczyło dostępu uczniów do treści internetowych (chodzi o ustawienia sieci internet dostępnej przez szkolną infrastrukturę), które mogą stanowić zagrożenie dla ich prawidłowego rozwoju" (Plichta 2017). Planując budowę sieci lub rozbudowę istniejącej infrastruktury należy wziąć również pod uwagę najnowsze trendy w edukacji, takie jak „BYOD (*Bring Your Own Device*, czyli: przynieść własne urządzenie)" (Stachecki 2013; zob. Janczak 2013). Każdy uczeń, nauczyciel, rodzic, gość w szkole może połączyć się własnym urządzeniem do sieci szkolnej, przez co na małej powierzchni skupiona zostaje większa, nie zawsze do określenia liczba urządzeń. Powoduje to duże obciążenie sieci i urządzeń, co może być zagrożeniem dla stabilności działania łącza internetowego.

Dlatego już na etapie planowania tego typu inwestycji szkolnej należy brać pod uwagę wszystkie możliwości wykorzystania i obciążenia sieci oraz łącza, by dobrać odpowiednie urządzenia i przede wszystkim, by zakupiona przepustowość łącza internetowego nie powodowała problemów z dostępem do danych. Połączenie wszystkich komputerów i innych urządzeń dostępowych (drukarek, skanerów, itd.) w szkole infrastrukturą sieciową z serwerem oraz ruterem, daje administratorowi możliwość właściwego zadbania o bezpieczeństwo cyfrowe uczniów i nauczycieli. Fundacja Odkrywców Innowacji zaproponowała trzypoziomowy model bezpieczeństwa infrastruktury IT, który może być punktem wyjścia przy planowaniu i wdrażaniu dostępu do sieci internetowej dla placówek oświatowych (Lizut 2015). Za bezpieczeństwo na tej płaszczyźnie odpowiedzialna jest dyrekcja placówki oraz powołany administrator sieci, nie zawsze zatrudniony w placówce, który pełni rolę przede wszystkim techniczną i doradczą (przy zakupach).

Szczególną uwagę placówki oświatowe przywiązują do wdrażania polityki bezpieczeństwa i procedur związanych z ochroną danych osobowych, ze względu na powszechne przechowywanie ich i przetwarzanie przy użyciu systemów informatycznych (zob. GIODO, 2007). Krzysztof Liderman wskazuje na to, „że informacja stała się istotnym czynnikiem decydującym […] o bezpieczeństwie nie tylko pojedynczych ludzi czy organizacji, ale całych państw" (Liderman 2012, s.11-12). Oznacza to, że również szkoły zobowiązane są do ochrony informacji związanych z danymi swoich uczniów, ich rodziców, nauczycieli i innych pracowników. Jednak jak wynika z badań firmy Librus „młodzież w wieku szkolnym nie przywiązuje wystarczającej wagi do bezpieczeństwa w sieci, a rodzice nie zdają sobie sprawy z zagrożeń wynikających z niewiedzy swoich dzieci" (Edunews.pl 2017). Najczęstszym błędem popełnianym w sieci jest udostępnianie własnych danych osobowych na portalach społecznościowych, na stronach sklepów podczas robienia zakupów, niezachowywanie prywatności, upublicznianie własnego wizerunku. Badania na zlecenie Komisji Europejskiej w 2011 roku wykazały, iż „74% badanych uważa, że dzielenie się informacjami prywatnymi ma coraz większe znaczenie w życiu nowoczesnego człowieka […] Wśród osób, które korzystają z sieci społecznościowych, niemal 80% zamieściło na jednej z nich swoje prawdziwe imię i nazwisko, a około połowa dołączyła fotografie (51%) oraz informacje o narodowości (47%)" (Kołodziejczyk 2014, s. 79).

Edukacja na rzecz bezpieczeństwa informacyjnego wplata się w działania szkoły związane z drugą płaszczyzną dydaktyczno-wychowawczą. Chodzi tu przede wszystkim o uświadamianie uczniom oraz rodzicom, jak ważne w codziennym życiu jest zachowanie cyfrowego bezpieczeństwa. Nauczyciele podejmują problematykę i zagadnienia związane z bezpiecznym korzystaniem z sieci internetowej, by wykształcić w uczniach właściwą postawę i odpowiedzialność w użytkowaniu sieci, „co będzie procentowało odpowiedzialnymi działaniami także poza szkolnym środowiskiem. Żadne, nawet najlepsze urządzenia, nie zastąpią rozwagi i świadomości zagrożeń użytkowników szkolnej sieci. Uczniowie muszą wiedzieć, że każdy odpowiada za swoje zachowania w internecie, bo nie jest w nim anonimowy" (Andrzejewski 2016). Tematyka bezpieczeństwa cyfrowego (również informacyjnego) w szkołach podejmowana jest nie tylko na zajęciach z informatyki, ale także podczas różnych konkursów, projektów edukacyjnych związanych z ogólnopolskimi i światowymi kampaniami, np.: Dzień Bezpiecznego Internetu[1], Bezpiecznie Tu i Tam[2]. Nauczyciele wykorzystujący urządzenia i dostęp do sieci internetowej

---

[1] Dzień Bezpiecznego Internetu (DBI) obchodzony jest z inicjatywy Komisji Europejskiej od 2004 roku. Początkowo wydarzenie to świętowały jedynie państwa europejskie, ale już od lat DBI przekracza granice Europy angażując państwa z całego świata. Z pełną listą zaangażowanych państw i instytucji oraz podjętymi przez nie działaniami można zapoznać się na stronie www.saferinternetday.org. http://www.saferinternet.pl/menu/projekty/projekty-edukacyjne/dzien-bezpiecznego-internetu.html [dostęp: 23.09.2017].

[2] Fundacja Orange, *Bezpiecznie Tu i Tam*, https://fundacja.orange.pl/nasze-programy/bezpiecznie-tu-i-tam/ [dostęp: 23.09.2017].

podczas swoich zajęć przedmiotowych mają obowiązek zwracania uwagi na istniejące zagrożenia czyhające w sieci, ale zarazem powinni wskazywać na metody wykrywania i procedury reagowania na zagrożenia. Świadoma edukacja przyczynia się do zminimalizowania istniejących zagrożeń. Nauczyciele w szkole oraz rodzice w domu, muszą być przygotowani do pomagania swoim podopiecznym w bezpiecznym, codziennym funkcjonowaniu w dwóch równoległych światach - realnym i wirtualnym. Wymaga to ciągłego uaktualniania wiedzy na temat zagrożeń, ponieważ „nauczyciele oceniają swój poziom wiedzy na temat bezpieczeństwa online jako przeciętny" (Makaruk 2013, s. 6) oraz podnoszenia swoich kompetencji kluczowych, w tym kompetencji informatycznych i informacyjnych, które obecnie stały się jednymi z najważniejszych (Wojnarowska 2016; Komisja Europejska 2007). Poprzez rozwijanie tych kompetencji nauczyciele swobodniej wchodzą w relacje z uczniami, dla których cyfrowe i realne środowisko tworzą naturalny świat. Pełna współpraca w procesie dydaktycznym z odpowiednim, bezpiecznym użytkowaniem nowoczesnych urządzeń przyczynia się do podnoszenia umiejętności wykorzystania technologii cyfrowych, przez co skutkować będzie w udanym życia zawodowym w przyszłości. Natomiast Anna Andrzejewska wskazuje, że „nowe kompetencje nauczyciela są nie tylko związane ze znajomością języków obcych i kompetencjami w zakresie informatyki, biegłością w komunikowaniu się oraz umiejętnością uczenia się przez całe życie. Coraz częściej ważnym aspektem staje się przygotowanie pedagogów do zagrożeń, jakie stwarzają nowe technologie informacyjno-komunikacyjne tworzące cyberprzestrzeń, w której nie tylko funkcjonuje, ale także aktywnie uczestniczy młode pokolenie" (Andrzejewska 2014, s. 17-18).

Edukacja o bezpieczeństwie cyfrowym i zapobieganie zagrożeniom

W *Standardzie bezpieczeństwa online placówek oświatowych* zawarte zostały działania w ramach profilaktyki zapobiegania występowaniu cyberproblemów. Nauczyciele i rodzice powinni zapoznać się z tymi opracowaniami, by zdobyć odpowiednią wiedzę i być przygotowanym w razie konieczności udzielenia pomocy poszkodowanym lub interweniować w przypadku wykrycia sprawcy niepożądanych działań w internecie oraz wiedzieć z jakimi służbami podjąć współpracę w zakresie bezpieczeństwa cyfrowego. Publikacja zawiera przykładowe procedury wobec wybranych zagrożeń i szczegółowy opis działań jakie powinny być spełnione przez nauczyciela, rodzica, placówkę w przypadku interwencji (również w formie grafik) (Lizut 2015). Każde działania profilaktyczne prowadzą do zminimalizowania wystąpienia niepożądanych działań i uchronienie uczniów przed przykrymi skutkami bezmyślnego poruszania się po cyfrowym świecie. Ewa Krzyżak-Szymańska i Andrzej Szymański „wskazują, z jakimi wyzwaniami muszą się zmierzyć opiekunowie i wychowawcy, aby skutecznie zapobiegać istniejącym zagrożeniom młodego pokolenia w cyfrowym świecie" (Krzyżak-Szymańska, Szymański 2014, s. 198).

Autorzy przedstawiają również szereg działań profilaktycznych na rzecz bezpieczeństwa w sieci, które prowadzone są w Polsce przez różne fundacje. „Przykładem większych takich systemowych akcji jest kampania «Dziecko w sieci» oraz równie duża kampania «STOP Cyberprzemocy». […] W Polsce funkcjonuje również program «Safer Internet», którego Polskie Centrum Programu tworzą Fundacja Dzieci Niczyje (FDN) [obecnie Fundacja Dajemy Dzieciom Siłę – przyp. K.C.] oraz Naukowa i Akademicka Sieć Komputerowa (NASK)" (Krzyżak-Szymańska, Szymański 2014, s. 207).

Powyżej wymienione działa są promowane przez Ministerstwo Edukacji Narodowej w kampanii „*Bezpieczna szkoła +"*[3], gdzie na stronie internetowej są dostępne różne programy i podejmowane projekty dotyczące bezpieczeństwa w szkołach, również bezpieczeństwa informacyjnego i cyfrowego działające na terenie całego kraju. Zamieszczone tam materiały oraz linki do serwisów i platform edukacyjnych są doskonałym kompendium wiedzy dotyczącej bezpieczeństwa dzieci i młodzieży w szkołach. Dzięki tym działaniom nauczyciele, rodzice mogą wspomóc się podczas edukowania dzieci i młodzieży oraz samodoskonalić własne kompetencje związane z cyfrowym bezpieczeństwem. Ważnym elementem przeciwdziałania wszelkim formom zagrożeń wpływającym na bezpieczeństwo w szkołach jest możliwość zgłaszania naruszeń na specjalne telefony zaufania i infolinie, których numery są dostępne również na stronie kampanii.

W dniu 27 września 2017 r. minister Anna Zalewska podpisała i przekazała do szkół dokument opisujący działania profilaktyczne, procedury, zbiór dobrych praktyk oraz szczegółowe wskazówki związane z zapewnieniem bezpieczeństwa fizycznego i cyfrowego w szkołach (Ministerstwo Edukacji Narodowej 2017). Dokument jest poradnikiem dla dyrektorów i nauczycieli, którzy stają przed wyzwaniem wprowadzenia procedur bezpieczeństwa cyfrowego w środowisku szkolnym z jednoczesnym zaangażowaniem wszystkich członków społeczności szkolnej. Działania te należy rozpocząć od wprowadzenia profilaktyki, która bazuje na planowym wdrażaniu poszczególnych działań polityki bezpieczeństwa cyfrowego w szkole, w ramach szkolnego programu wychowawczo-profilaktycznego i inwestycyjnego.

[3] Ministerstwo Edukacji Narodowej, https://bezpiecznaszkola.men.gov.pl/aktualnosci/ [dostęp: 15.10.2017].

Rysunek 1. Elementy profilaktyki dla zapewnienia bezpieczeństwa uczniów w środowisku cyfrowym.

Źródło: opracowanie własne na podstawie Ministerstwo Edukacji Narodowej, (2017). *Bezpieczna szkoła. Zagrożenia i zalecane działania profilaktyczne w zakresie bezpieczeństwa fizycznego i cyfrowego uczniów.*

Marcin Bochenek zaproponował wprowadzenie następujących typów działań profilaktycznych, które powinny być realizowane przez specjalnie powołane zespoły do spraw bezpieczeństwa online w placówkach oświatowych:

1. Działania diagnostyczne
    a. Ocena stanu bezpieczeństwa technicznego palcówki oświatowej
    b. Ocena stanu bezpieczeństwa w aspekcie społeczno-wychowawczym

2. Działania informacyjne
    a. Akcje informacyjne
    b. Opracowanie szkolnej procedury reagowania
3. Działania szkoleniowe i edukacyjne
    a. Edukacja dotycząca bezpieczeństwa online i zagrożeń w Internecie
    b. Edukacja medialna: kompetencje informacyjne
4. Działania wychowawcze
    a. Kształtowanie poprawnych postaw
    b. Zmiana postaw wadliwych

Źródło: opracowanie na podstawie Bochenek, M. (2015). *Typy działań profilaktycznych* [w:] Lizut, J. (red.), *Standard bezpieczeństwa online placówek oświatowych*, Warszawa: Fundacja Odkrywców Innowacji, s. 11.

Podjęcie działań związanych z niwelowaniem zagrożeń poprzez wprowadzanie poszczególnych procedur bezpieczeństwa daje nadzieję na zwiększenie cyberbezpieczeństwa oraz podjęcie poprawnych działań przez całą społeczność szkolną. Nadzór nad koordynacją wdrażania poszczególnych etapów rekomenduje się organowi prowadzącemu palcówkę przy jednoczesnym wsparciu zarówno uczniów jak i rodziców. Zacieśnia to współpracę pomiędzy grupami w społeczności szkolnej oraz daje poczucie większego zaufania w podejmowanych decyzjach.

Bez odpowiedniego podejścia do profilaktyki działań związanych z bezpieczeństwem cyfrowym niemożliwe byłoby egzekwowanie procedur reagowania w przypadku wystąpienia jakichkolwiek zagrożeń. Dokument *Bezpieczna szkoła…* oddany do placówek oprócz samych działań profilaktycznych, zawiera również obowiązujące przepisy prawa, na które należy się powoływać w przypadku wykrycia zagrożeń bezpieczeństwa fizycznego i cyfrowego uczniów. Przedstawiony pakiet działań w sytuacjach kryzysowych dla najczęściej występujących zagrożeń nie zawsze jest wystarczający, ale powinien stanowić punkt wyjścia do rozpoczęcia prac związanych z opracowywaniem nowych procedur, ponieważ „nie istnieje «złota recepta», którą zastosować można we wszystkich przypadkach zagrożeń. Dyrektorzy i nauczyciele muszą uwzględniać kontekst indywidualnych przypadków, a także ich szkolne i środowiskowe tło […]" (Ministerstwo Edukacji Narodowej 2017).

Podsumowanie

Problematyka cyfrowego bezpieczeństwa dzieci i młodzieży od kilku lat jest podejmowana przez wielu badaczy, odbywają się w tym temacie konferencje krajowe i międzynarodowe, dzięki czemu jest możliwość szerokiego zapoznania się z istniejącymi zagrożeniami oraz działaniami eliminującymi te zagrożenia poprzez profilaktykę i edukację. Zjawisko to również chętnie podejmowane jest przez nauczycieli, wychowawców, rodziców dla podniesienia większego bezpieczeństwa uczniów w szkołach. Tempo i rozwój technologii spowodowały, iż temat ten jest ciągle aktualny, omawiane są istniejące i znane zagrożenia, wprowadzane są procedury i regulaminy. Jednak powstawanie kolejnych wynalazków, rozwój telefonii komórkowej, sieci bezprzewodowych i internetu spowodował nową falę zagrożeń czyhających na młode pokolenie w wirtualnym świecie. „Zagrożenia człowieka w cyberprzestrzeni nie są już procesem, lecz stają się niepokojącym, nieznanym i niezbędnym jeszcze zjawiskiem społeczno-pedagogicznym. Ich skutkiem staje się dynamiczne wdrażanie różnorodnych zastosowań w szkole, pracy zawodowej i innych aktywnościach jednostki" (Bednarek 2017, s. 55).

Nauczyciele świadomi współczesnych zagrożeń płynących z cyfrowego (wirtualnego) świata oraz najnowocześniejszych technologii powinni stawiać przede wszystkim na edukację w zakresie bezpiecznego poruszania się i zachowania w sieci oraz podejmować dialog z młodym pokoleniem w celu utrzymania dobrych relacji nauczyciel - uczeń. „Nauczyciel ma trudne zadanie, by nauczyć dziecko dokonywania świadomego i odpowiedzialnego korzystania i poruszania się w sieci, by uchronić dziecko od tych złych meandrów cyberprzestrzeni. Rolą współczesnego nauczyciela jest nauczyć, by uczniowie odróżnili fikcję od rzeczywistości, wskazywać kierunek, wspierać dziecko w procesie samodzielnego zdobywania wiedzy, informacji oraz wartościowania rzeczywistości. Dobrze ukierunkować, gdzie i jak mają tę wiedzę zdobywać, oraz apelować o rozwagę w momencie zagrożenia" (Andrzejewska 2014, s. 28).

Współczesna cyfrowa szkoła powinna być wyposażona w odpowiednio zabezpieczoną szerokopasmową sieć z dostępem do internetu, urządzenia i oprogramowanie dające poczucie bezpieczeństwa z niech korzystających, ale przede wszystkim pracujący w niej nauczyciele winni być przeszkoleni i przygotowani do pracy z wykorzystaniem technologii informacyjno-komunikacyjnej. W obecnej rzeczywistości szkoła nie jest już ograniczona tylko do murów szkoły, ale przenika do równoległego wirtualnego świata. Dlatego ważne jest by edukacja dotycząca bezpiecznego wykorzystania sieci i nowych technologii podejmowana była nie tylko przez samych nauczycieli i rodziców, ponieważ „bezpieczeństwo dzieci w cyberprzestrzeni, przeciwdziałanie zagrożeniom oraz minimalizowanie ich skutków to pedagogiczne wyzwanie dla całego społeczeństwa" (Andrzejewska 2013, s.9).

Bibliografia

Aleksandrowicz, T. R. (2016). *Podstawy walki informacyjnej*, Warszawa: Editions Spotkania.

Andrzejewska, A. (2013). *Bezpieczeństwo uczniów w cyberprzestrzeni*, Trendy nr 1/2013, s. 9-15.

Andrzejewska, A. (2014). *Nowe kompetencje nauczycieli w zakresie możliwości i niebezpieczeństw cyberprzestrzeni* [w:] *Zagrożenia cyberprzestrzeni i świata wirtualnego*, J. Bednarek, A. Andrzejewska (red.), Warszawa: Wydawnictwo Difin.

Andrzejewski, D. (2016). *Odpowiedzialni użytkownicy internetu* [w:] *Przestrzeń wirtualna i technologiczna. Przestrzenie edukacji 21. Otwieramy szkołę! Tom 2*, K. Górkiewicz, (red.) Warszawa: Publikacja powstała w ramach projektu „Educational Spaces 21. Open up!".

Batorski, D. (2015). *Technologie i media w domach i w życiu Polaków. Diagnoza Społeczna 2015*, *Warunki i Jakość Życia Polaków - Raport*. Warszawa: Rada Monitoringu Społecznego, Contemporary Economics, 9/4, 373-395. DOI:10.5709/ce.1897-9254.192, http://www.diagnoza.com/pliki/raporty/Diagnoza_raport_2015.pdf [dostęp: 26.07.2017].

Bednarek, J. (2017). *Wyzwania edukacyjne w kontekście aktywności człowieka w przestrzeni cyfrowej*, Edukacja i Dialog Nr 01/02 (292/293) 2017.

Doktryna bezpieczeństwa informacyjnego RP, Projekt z dnia 24 lipca 2015, Biuro Bezpieczeństwa Narodowego, https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf, [dostęp 25.07.2017].

Edunews.pl, (2017). *Uczniowie nie dbają o bezpieczeństwo w sieci*, http://www.edunews.pl/badania-i-debaty/badania/3918-uczniowie-nie-dbaja-o-bezpieczenstwo-w-sieci [dostęp: 17.07.2017].

Fundacja Orange, (2013). *Kompetencje cyfrowe młodzieży w Polsce (14-18 lat)*, Warszawa.

GIODO Generalny Inspektor Danych Osobowych, (2007). *ABC bezpieczeństwa danych osobowych przetwarzanych przy użyciu systemów informatycznych*, Warszawa: Wydawnictwo Sejmowe, opracował Andrzej Kaczmarek.

Goban-Klas, T., Sienkiewicz, P. (1999). *Społeczeństwo informacyjne: Szanse, zagrożenie, wyzwania;* Kraków: Wydawnictwo Fundacji Postepu Telekomunikacji.

Janczak, D. (2013). *BYOD w szkole – BY ODkrywać e-dukację*, Mazowiecki Kwartalnik Edukacyjny Meritum 4(31) 2013,s. 34-37.

Jasiewicz, J. *Kompetencje cyfrowe Polaków*, dostępny w Internecie: http://sdsi.pti.org.pl/index.php/pol/content/download/1166/5982/file/Jasiewicz%20-%20kompetencje%20cyfrowe%20Polak%C3%B3w.pdf [dostęp: 10.06.2017].

Kołodziejczyk, Ł. (2014). *Prywatność w Internecie: postawy i zachowania dotyczące ujawniania danych prywatnych w mediach społecznych*, Warszawa: Wydawnictwo Stowarzyszenia Bibliotekarzy Polskich.

Komisja Europejska, (2007). *Kompetencje kluczowe w uczeniu się przez całe życie. Europejskie Ramy Odniesienia*, Luksemburg: Urząd Oficjalnych Publikacji Wspólnot Europejskich.

Korusiewicz, A. (2007). *Zagrożenia w sieci Internet*, Warszawa: Wydawnictwo Centrum Edukacji Bibliotekarskiej, Informacyjnej i Dokumentacyjnej.

Korzeniowski, L. F. (2008). *Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych*, Kraków: EAS.

Krzyżak, E., Szymański, A. (2014). *Nowe wyzwania profilaktyki w kontekście zagrożeń dzieci i młodzieży*, [w:] *Zagrożenia cyberprzestrzeni i świata wirtualnego*, J. Bednarek, A. Andrzejewska (red.), Warszawa: Wydawnictwo Difin.

Liderman, K. (2012). *Bezpieczeństwo informacyjne*, Warszawa: Wydawnictwo Naukowe PWN SA.

Lizut, J. (red.), (2015). *Standard bezpieczeństwa online placówek oświatowych*, Warszawa: Fundacja Odkrywców Innowacji.

Makaruk, K. (2013), *Nauczyciel sieci,* [w:] *Szkolne standardy bezpieczeństwa dzieci i młodzieży online*, K. Makaruk i in. (red.), Warszawa: Fundacja Dzieci Niczyje.

Ministerstwo Edukacji Narodowej, (2017). *Bezpieczna szkoła. Zagrożenia i zalecane działania profilaktyczne w zakresie bezpieczeństwa fizycznego i cyfrowego uczniów*, Warszawa: Departament Wychowania i Kształcenia Integracyjnego. https://bezpiecznaszkola.men.gov.pl/bezpieczna-szkola-zagrozenia-i-zalecane-dzialania-profilaktyczne-w-zakresie-bezpieczenstwa-fizycznego-i-cyfrowego-uczniow/ [dostęp: 15.10.2017].

Piocha, S. (2004). *Makroekonomia a problemy bezpieczeństwa* [w:] *Problemy bezpieczeństwa ekonomicznego wobec procesów globalizacji*, S. Piocha (red.), Koszalin: PTE.

Piotrowski A. (red.), (2012). *Edukacja dla bezpieczeństwa. Media a bezpieczeństwo. Edukacyjne konteksty bezpieczeństwa* t. 2., Poznań: Wydawnictwo Wyższej Szkoły Bezpieczeństwa w Poznaniu.

Plichta, P. (2017). *Edukacja dzieci i młodzieży w Polsce – wybrane wyzwania i obszary nierówności*. Dziecko Krzywdzone. Teoria, badania, praktyka, 16(1) 2017, s. 146-171.

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

Sienkiewicz, P. (red.), (2015). *Inżynieria systemów bezpieczeństwa*, Warszawa: Polskie Wydawnictwo Ekonomiczne.

Sokół, R. (2004). *ABC ochrony przed wirusami*, Gliwice: Wydawnictwo Helion.

Stachecki, D. (2013). *Bezpieczeństwo szkolnej infrastruktury informatycznej* [w:] *Szkolne standardy bezpieczeństwa dzieci i młodzieży online*, K. Makaruk i in. (red.), Warszawa: Fundacja Dzieci Niczyje.

Świniarski, J. (1999). *Filozoficzne podstawy edukacji dla bezpieczeństwa*, Warszawa: Egros.

Tomczyk, Ł., Srokowski, Ł. (2016). *Kompetencje w zakresie bezpieczeństwa cyfrowego w polskiej szkole. Raport z badań*, Tarnów: Stowarzyszenie „Miasta w Internecie", https://www.cyfrowobezpieczni.pl/biblioteka-materialow/wszystkie?search=Raport+z+bada%C5%84 [dostęp: 15.06.2017].

Więcaszek-Kuczyńska, L. (2014). *Zagrożenia bezpieczeństwa informacyjnego*, OBRONNOŚĆ, Zeszyty Naukowe 2(10)/2014, s. 210-233.

Wojnarowska, M. (2016). *Kompetencje kluczowe – przygotowanie do życia*, TRENDY nr 4/2016, s. 9-14.

Ярочкин, ВИ, (2000). Секьюритология – наука о безопасности жизнедеятельности, Издательство «Ось-89», Москва.

Summary: School as a public institution is obliged to provide students with maximum safety, in both real and digital world. In the following article the author presents challenges that schools in Poland have to face in order to ensure the appropriate security standards for both students and workers of these educational institutions. He also points the main kinds of dangers which may influence the physical and psychological health of the people who encounter them. The text below may become a starting point for a better preparation of students, teachers and parents to identify, reveal and protect themselves from cyber-threats (included in the state's strategy for development and security). The threats connected with using the world wide web (not only at school) by children, youth, as well as adults, can closely be linked with the general threats for IT security.

Key words: digital school, digital student, digital teacher, IT security, world wide web threats, digital safety.

Krzysztof Ciemcioch, magister inżynier informatyki, wykładowca akademicki, trener, ekspert szkoleń z nowych mediów w edukacji. Autor publikacji związanych z praktycznym wykorzystaniem multimedialnych narzędzi w procesie kształcenia. Obszar zainteresowań zawodowych: nowe media w edukacji, mobilna edukacja, bezpieczeństwo w sieci, skład publikacji (DTP). Zawodowo związany z Politechniką Łódzką Centrum Komputerowym, Miejską Siecią Komputerową LODMAN, Uczelnią Nauk Społecznych oraz Ośrodkiem Rozwoju Kompetencji Edukacyjnych (ORKE)

Kontakt z autorem: krzysztof.ciemcioch@gmail.com