Edyta Banaszak
Akademia Nauk Stosowanych WSGE
im. A. De Gasperi
E-mail: edyta.banaszak@wsge.edu.pl
ORCID: orcid.org/0000-0002-9178-7886

DOI: doi.org/10.13166/awsge/187751

EDUKACJA DO CYBERBEZPIECZEŃSTWA W POLSKICH SZKOŁACH JAKO PRÓBA ZASPOKOJENIA POTRZEBY BEZPIECZEŃSTWA W ŚWIECIE WIRTUALNYM

EDUCATION TO CYBERSECURITY IN POLISH SCHOOLS AS AN ATTEMPT TO SATISFY THE NEED FOR SECURITY IN THE VIRTUAL WORLD

Streszczenie: Współczesny człowiek znaczną część swojego życia spędza w rzeczywistości wirtualnej. Dlatego koniecznym jest, aby czuł się w niej bezpiecznie. Aby to było możliwe, osoba musi być przygotowana do bezpiecznego funkcjonowania w świecie wirtualny. Przygotowanie to może dokonywać się w różnych obszarach a jednym z podmiotów odpowiedzialnych za nie jest polski system oświaty. Artykuł podejmuje tematykę edukacji do bezpieczeństwa w cyberprzestrzeni.

Słowa kluczowe: *cyberbezpieczeństwo, edukacja do bezpieczeństwa, polska oświata, bezpieczeństwo cyfrowe, edukacja do cyberbezpieczeństwa, potrzeba funkcjonowania z cyberprzestrzeni*

Abstract: Modern human being spends a significant part of his or her life in virtual reality. Therefore, it is necessary for him or her to feel safe in it. For this to be possible, a person must be prepared to function safely in the virtual world. This preparation may take place in various areas and one of the entities responsible for it is the Polish education system. The work deals with the subject of education for security in cyberspace.

Keywords: *cybersecurity, education for security, Polish education, digital security, education for cybersecurity, the need of functioning in cyberspace*

Wprowadzenie

Współczesny człowiek znaczną część swojego życia spędza w rzeczywistości wirtualnej. Dlatego koniecznym jest, aby czuł się w niej bezpiecznie. Aby to było możliwe, osoba musi być przygotowana do bezpiecznego funkcjonowania w świecie wirtualny. Przygotowanie to może dokonywać się w różnych obszarach a jednym z podmiotów odpowiedzialnych za nie jest polski system oświaty. Artykuł podejmuje tematykę edukacji dla bezpieczeństwa w cyberprzestrzeni. Edukacja dla bezpieczeństwa jest istotnym elementem procesu kształcenia i wychowania realizowane w polskich szkołach. Niemniej ważna jest edukacja dla bezpieczeństwa w cyberprzestrzeni. Prawo do bezpiecznego funkcjonowania w cyberprzestrzeni wynika z naszej potrzeby do bezpieczeństwa i jednym z zadań szkół jest zaspokajanie tej potrzeby.

Wybór takiego tematu spowodowany jest dwoma głównymi powodami. Jednym z nich jest fakt, iż współczesny człowiek spędza coraz więcej swojego czasu w świecie wirtualnym. Drugim powodem dokonania takiego wyboru tematu pracy jest fakt, iż różnego rodzaju raporty i dane wskazują, iż pojawia się coraz więcej zagrożeń. Cyberzagrożenia są coraz powszechniejsze i na coraz bardziej zaawansowanym poziomie. Dlatego też, każdy człowiek wchodząc do świata wirtualnego musi być przygotowany, aby tam bezpiecznie funkcjonować. Owo przygotowanie winno dokonać się poprzez proces kształcenia i wychowania realizowany w polskich szkołach.

Przedmiotem opracowania jest Edukacja dla bezpieczeństwa w cyberprzestrzeni realizowana w polskich szkołach, to jest na poziomie szkoły podstawowej (I i II etap edukacyjny) oraz szkoły średniej (III etap edukacyjny).

Celem jest sprawdzenie poziomu, zakresu i skuteczności tego przygotowania oraz jaki jest poziom bezpieczeństwa cyfrowego (wiedza, umiejętności oraz kompetencje) w postrzeganiu uczniów szkół podstawowych i szkół średnich.

Artykuł będzie próbował odpowiedzieć na powyżej postawione pytania. Dokonano założenia, że szkoła w Polsce nie w pełni przygotowuje do życia i funkcjonowania w świecie cyfrowym. To znaczy, iż poziom i zakres edukacji do cyberbezpieczeństwa nie jest wystarczający a polski uczeń nie ma poczucia bycia przygotowanym przez szkołę do funkcjonowania w świecie wirtualnym, zakres przygotowania przez szkołę nie jest wystarczający.

W artykule użyte zostały dwie metody a mianowicie badanie dokumentów oraz sondaż diagnostyczny. W ramach badań własnych przeanalizowane zostaną treści zawarte w takich dokumentach jak – podstawa programowa dla szkoły podstawowej oraz podstawa programowa dla szkoły średniej. Dokumenty te zostaną przeanalizowane przede wszystkich w obszarze przedmiotu Edukacja dla bezpieczeństwa oraz Informatyka. Celem zastosowania tej metody jest sprawdzenie czy treści zawarte we wspomnianych dokumentach i wskazane sposoby ich realizacji są odpowiednie, wystarczające i czy przygotowują ucznia do radzenia sobie z zagrożeniami w świecie cyfrowym.

Druga metoda, to sondaż diagnostyczny, gdzie jako technika badawcza zostanie użyta ankieta skierowana do uczniów szkół podstawowych oraz uczniów szkół średnich. Narzędziem badawczym będzie tutaj kwestionariusz ankiety. Celem zastosowania tej metody będzie sprawdzenie, w jaki sposób nauczanie zasad cyberbezpieczeństwa w szkole jest widziane oczyma najważniejszego podmiotu tego procesu, a mianowicie oczami ucznia. Ankieta da więc odpowiedź na wiele kwestii i wskaże czy w swoim subiektywnym odczuciu, uczeń polskiej szkoły (na jej różnych poziomach) czuje się przygotowanym do życia we współczesnym świecie, którego duża część to obszar wirtualny.

Bezpieczeństwo i cyberbezpieczeństwo

W celu właściwego opisania danej rzeczywistości konieczne jest określenie i zdefiniowanie podstawowych pojęć i terminów dotyczących danego obszaru tematycznego. Rozdział dotyczy kwestii bezpieczeństwa, dlatego koniecznym jest zdefiniowanie czym jest bezpieczeństwo oraz jakie są jego rodzaje, typy oraz w jaki sposób klasyfikuje się bezpieczeństwo. Bezpieczeństwo to jedna z tych wartości i jednocześnie potrzeb, które są bardzo pożądane przez człowieka. Bezpieczeństwo określić można jako rzeczywistość odwrotnie proporcjonalną do pojawiających się zagrożeń (M. Sitek, 2018, s. 178). Bezpieczeństwo jest jednym z podstawowych praw człowieka, gdyż wynika z elementarnych potrzeb ludzkich. Jeśli spojrzymy na ludzkie potrzeby zgodnie z koncepcją Abrahama Masłowa, to potrzeba bezpieczeństwa znajduje się na drugim poziomie piramidy zaraz po potrzebach egzystencjalnych takich jak życie, pożywienie, mieszkanie, odzież, prokreacja. Oznacza to, iż każdy człowiek ma potrzebę bezpieczeństwa i w oparciu o tą potrzebę ma do bezpieczeństwa prawo (por. M. Sitek, 2018, s. 38-43).

Pojęcie bezpieczeństwa nie ma swojej definicji w polskiej konstytucji. Słowo to w ustawie zasadniczej pojawia się 5 razy – w artykule 5, kiedy mowa o tym, iż Rzeczypospolita zapewnia bezpieczeństwo obywateli, w artykule 45, ust. 2, kiedy mowa jest o wyłączeniu jawności rozprawy sądowej ze względu na bezpieczeństwo państwa, w artykule 74, gdzie mowa jest o obowiązku zapewnienia przez władze publiczne bezpieczeństwa ekologiczne oraz w artykule 146, ust. 4, gdzie znajduje się lista obowiązków Rady Ministrów i tam w punktach 7 i 8 pojawia się obowiązek zapewnienia bezpieczeństwa zarówno wewnętrznego, jak i zewnętrznego (Dz. U. 1997, nr 78, poz. 483 z późn. zm.).

Termin bezpieczeństwo może być definiowany i opisywany na różne sposoby. W. Pokruszyński mówi, że termin ten jest bardzo trudny do zdefiniowania, gdyż jest to zjawisko obejmujące swoim zakresem wiele dyscyplin i specjalności naukowych (Pokruszyński, 2010, s. 8). Ten sam autor chcąc zdefiniować bezpieczeństwo na bardzo ogólnym poziomie, cytuje definicję zawartą w Słowniku Nauk Społecznych UNESCO autorstwa D. Lernera, gdzie bezpieczeństwo jest utożsamiane z pewnością i oznacza brak zagrożeń. Bezpieczeństwo to również

swego rodzaju zdolność do przetrwania, pewnego rodzaju niezależność, tożsamość oraz możliwość rozwoju (Pokruszyński, 2012, s. 62).

Współczesny człowiek nie żyje już tylko w świecie realnym. Spędza on również znaczną część swojego życia w świecie wirtualnym – cyfrowym. Dane 2023 wskazują, iż na 8,1 mld populacji, z telefonów komórkowych korzysta 68% populacji, z Internetu – 64,4,5% a z mediów społecznościowych 98,4%. Liczby te z roku na rok rosną (DATAREPORTA.COM, https://datareportal.com/reports/digital-2023-global-overview-report).

Powyższe dane wskazują, iż obecność człowieka w cyberprzestrzeni jest niezaprzeczalna i na pewno nie marginalna, ale bardzo znacząca. Przestrzeń wirtualna, zwana też światem wirtualnym, cyberprzestrzenią lub światem cyfrowym rozwija się bardzo szybko i bardzo sprawnie. Coraz więcej rodzajów ludzkiej aktywności, dotyczącej życia prywatnego, rodzinnego, zawodowego, rozrywki i stosunków społecznych jest przenoszonych do przestrzeni wirtualnej. Z każdym rokiem, coraz więcej ludzi wchodzi w ten świat i tam funkcjonuje równolegle do świata rzeczywistego. Dlatego współczesny człowiek musi być świadomy czym jest owa cyberprzestrzeń i jak w niej bezpiecznie funkcjonować.

Każdy rodzaj bezpieczeństwa jest istotny, ale w obecnym czasie, konieczne jest pochylenie się nad dwoma szczególnymi pojęciami, a mianowicie czym jest cyberprzestrzeń i związane z nią cyberbezpieczeństwo.

Termin cyberprzestrzeń jest używany bardzo często i jest to słowo, które w ostatnich czasach staje się coraz bardziej popularne. Niemniej jednak, dla przeciętnego użytkownika cyberprzestrzeni, jest to termin trudny do zdefiniowania a nawet bardzo tajemniczy (B. Sitek, 2016, s. 73).

Sam termin cyberprzestrzeń został użyty po raz pierwszy w 1984 roku przez Williama Gibsona w powieści Burning Chrome. Wygenerowany przez komputer świat immersyjnej, wirtualnej rzeczywistości, którą amerykański klasyk cyberpunkowych powieści nazywał też matrycą (matrix), spowodował wypromowanie Trylogii Gibsona, a zwłaszcza jej pierwszego tomu pt.: Neuromancer. Powszechny dostęp do Internetu oraz filmy oparte na gibsonowskich motywach stały się przyczyną spopularyzowania pojęcia cyberprzestrzeń (Wasilewski, 2013, s. 226).

Jeden z opisów czym jest cyberprzestrzeń daje nam Słownik języka polskiego PWN, w którym czytamy, że jest to *przestrzeń wirtualna, w której*

odbywa się komunikacja między komputerami połączonymi siecią internetową (https://sjp.pwn.pl/sjp/cyberprzestrze%C5%84;2553915).

Definicję cyberprzestrzeni publikuje również Słownik terminów militarnych i pokrewnych Departamentu Obrony USA (Department of Defense Dictionary of Military and Associeted Terms), gdzie czytamy, iż jest to *globalna domena w środowisku informacyjnym składająca się ze współzależnych sieci infrastruktury informatycznej i danych rezydentów, w tym Internetu, sieci telekomunikacyjne, systemów komputerowych oraz wbudowanych procesorów i kontrolerów* (https://irp.fas.org/doddir/dod/jp1_02.pdf, s. 58).

W naszym kraju, termin cyberprzestrzeń opisany został między innymi w Ustawie o stanie wojennym, gdzie ustawodawca dowodzi, iż jest to *Przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne, w rozumieniu art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. Nr 64, poz. 565, z późn. zm.) wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami* (Dz.U.2016.851 t.j.).

Po zdefiniowaniu pojęcia cyberprzestrzeń, warto dokonać również opisu pojęcia cyberbezpieczeństwa. Jedną z definicji cyberbezpieczeństwa znaleźć możemy w Ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. W artykule 2, punkt 4 podano, iż jest to *odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy* (Dz. U. 2018, poz. 1560).

Termin cyberbezpieczeństwo definiowany jest również w źródłach anglojęzycznych i tam często nazywany jest *computer security* – bezpieczeństwo komputerowe. Przykład takiej definicji znaleźć można w Słowniku terminów militarnych i pokrewnych Departamentu Obrony USA, który mówi, iż cyberbezpieczeństwo, to *zapobieganie uszkodzeniom, ochrona i renowacja komputerów, systemów łączności elektronicznej, usług łączności elektronicznej, komunikacji kablowej i komunikacji elektronicznej, w tym informacji w nich zawartych, w celu zapewnienia ich dostępności, integralności, uwierzytelniania, poufności i niezaprzeczalności* (https://irp.fas.org/doddir/dod/jp1_02.pdf, s. 57).

Jak widać na podstawie powyższych rozważań, cyberprzestrzeń i cyberbezpieczeństwo to dwa pojęcia, które są bardzo często używane przez różne osoby,

ale nie zawsze w pełni znane jest znaczenie tych pojęć. Większość ludzi w Polsce i na świecie jest użytkownikami świata wirtualnego, a więc cyberprzestrzeni i większość z nich, musi zadbać o swoje bezpieczeństwo w tym obszarze.

Zagrożenia w obszarze cyberprzestrzeni

Zagrożenia pojawiają się zarówno w świecie realnym jak i wirtualnym. Wśród tych zagrożeń mamy takie, które mają charakter globalny i są niebezpieczne dla państw czy społeczeństwa oraz takie, które mają charakter bardziej personalny i dotykają lub mogą dotykać pojedynczego człowieka. Jest to temat szczególnie ważny, gdyż z uwagi na doświadczenia związane z pandemią covid19, wiele obszarów działalności człowieka, które przed pandemią realizowane były w świecie realnym, z uwagi na lockdowny, restrykcje i ograniczenia zostały przeniesione do cyberprzestrzeni. Dlatego też ważnym jest, aby ta rzeczywistość była niezawodna i bezpieczna.

Temat zagrożeń zostanie przedstawiony i opisany w oparciu o raporty Agencji Unii Europejskiej ds. Cyberbezpieczeństwa Takie ujęcie tematyki zagrożeń wydaje się słuszne, ze względu na jego aktualność oraz fakt, iż są to analizy globalne.

Raport Agencja Unii Europejskiej ds. cyberbezpieczeństwa z października 2022 roku wskazuje na najczęściej pojawiające się zagrożenia. W opisywanym okresie dużym problemem były zagrożenia cyberprzestrzeni związane z sytuacja geopolityczną, w tym z wojną w Ukrainie. Niemniej jednak wskazuje się również na zagrożenia dotykające każdego zwykłego obywatela. Raport wskazuje na osiem najczęściej pojawiających się zagrożeń, którymi są: programowanie ransomware, złośliwe oprogramowanie (malware), zagrożenia inżynierii społecznej, zagrożenia dla danych, zagrożenia dostępności (Denial of Service), zagrożenia internetowe, dezinformacja, ataki na łańcuch dostaw (ENISA, 2022a, s. 4).

W opisywanym raporcie pojawiło się również nowe zagrożenie a mianowicie inżynieria społeczna. Zgodnie z raportem są to działania, których celem jest wykorzystanie ludzkiego błędu a nawet skłonienie człowieka do popełnienia błędu, gdzie w oparciu o ten błąd nastąpi nieuprawniony dostęp do informacji. Działania przestępców zmierzają do przekonania ofiary, aby otworzyła dokument, plik lub e-mail, do odwiedzin spreparowanej strony internetowej

lub udzielenia nieautoryzowanego dostępu do danych lub usług. W procesie manipulacji wykorzystuje się technologię, ale aby przestępcy mogli osiągnąć sukces konieczne jest tutaj popełnienie błędu przez ofiarę. Działania prowadzą do innych zagrożeń takich jak różnego rodzaju phishing, kompromitacja poczty służbowej – BEC), oszustwa, podszywanie się pod inną osobę lub fałszerstwa (ENISA, 2022a, s. 8).

Przeprowadzone analizy pojawiających się różnych zagrożeń oraz sytuacji w kontekście zarówno globalnym jak i lokalnym wskazuje, że wraz z postępującą transformacją cyfrową, pojawiać się będą coraz bardziej wyrafinowane działania cyberprzestępców. ENISA, na podstawie analizy czynników ekonomicznych, politycznych, społecznych i technologicznych, przewiduje, iż w nadchodzących latach będziemy musieli zmierzyć się z dziesięcioma największymi zagrożeniami. Według prognozy ENISE, będą to:

1. użycie złośliwego oprogramowania w celu przeprowadzenia ataków na łańcuchy dostaw;
2. dobrze przygotowane i zaawansowane kampanie dezinformacyjne;
3. cyfrowa inwigilacja, której skutkiem będzie znaczna utrata prywatności w świecie wirtualnym;
4. wykorzystywanie błędów człowieka oraz słabości starszych systemów;
5. ataki skierowane na wybrane ofiary za pomocą danych generowanych przez inteligentne systemy i narzędzia;
6. ataki na infrastrukturę kosmiczną, która zdaniem ekspertów jest słabo zabezpieczona;
7. zaawansowane ataki hybrydowe dotykające zarówno świat realny jak i świat wirtualny;
8. przeprowadzanie ataków hackerskich na podmioty, które wykazują niskie kompetencje w zakresie cyberbezpieczeństwa;
9. ataki cybernetyczne na globalnych dostawców usług w obszarze technologii informacyjno-komunikacyjnych skutkujące tym, iż nastąpi wstrzymanie dostępu do infrastruktury krytycznej;
10. wykorzystanie i nadużycie sztucznej inteligencji oraz manipulacje algorytmami sztucznej inteligencji (ENISA, 2022b).

Ważnym aspektem wyłaniającym się z prognoz jest fakt, iż ENISA mówi o zagrożeniach związanych z funkcjonowaniem sztucznej inteligencji i jej algorytmów. Jest to bardzo ważne wskazanie. Na ogół przedstawia się AI w pozytywnym świetle i pozytywnym kontekście. I rzeczywiście, jej działanie może być dużym wsparciem dla działalności pojedynczej jednostki, ale też całych instytucji lub firm.

Niemniej jednak, jak każde narzędzie, sztuczna inteligencja nie jest ani dobra, ani zła, natomiast wszystko zależy od tego, jak zostanie wykorzystana. Jeśli jest używana np. do identyfikacji poczty typu SPAM w naszej skrzynce poczty elektronicznej, to jest to działanie pomocne i pożądane. Jeśli natomiast w wyniku manipulacji lub nadużyć w działaniu algorytmu, którym posługuje się AI, człowiek wykona jakieś niechciane działanie lub podejmie niepożądaną decyzję, to narzędzie wspierające działania ludzkie może stać się wielkim zagrożeniem. Konieczne są wiec odpowiednie regulacje i monitoring tego obszaru.

Realizacja edukacji dla cyberbezpieczeństwa w polskich szkołach

Edukacja do bezpieczeństwa, szczególnie edukacja do bezpieczeństwa w cyberprzestrzeni to proces, które winien być realizowany przez różne podmioty, w tym przez system oświaty i edukacji.

Polski system oświaty, ma ogromny wpływ na działanie i funkcjonowanie społeczeństwa jako całości i jego poszczególnych elementów. Ponadto, praktycznie każdy przechodzi przez system oświaty na takim lub innym poziomie, gdyż w Polsce mamy obowiązek szkolny. Większość więc członków społeczeństwa w pewnym momencie swojego życia staje się elementem składowym systemu oświaty.

I w ten sam sposób, w jaki szkoła uczy nas pisać, czytać i liczyć oraz całej masy innych bardziej lub mnie przydatnych rzeczy, powinna również uczyć bezpiecznego funkcjonowania w świecie. Wspomniany już wcześniej punkt 21, artykuły 1, ustawy z dnia 14 grudnia 2016 roku – Prawo oświatowe, wyraźnie mówi, iż system oświaty powinien między innymi zapewnić *upowszechnianie wśród dzieci i młodzieży wiedzy o bezpieczeństwie oraz kształtowanie właściwych postaw wobec zagrożeń, w tym związanych z korzystaniem*

z technologii informacyjno-komunikacyjnych, i sytuacji nadzwyczajnych (Dz.U. z 2017 r. poz. 59, z późn. zm.).

Analiza podstawy programowej kształcenia ogólnego w szkole podstawowej oraz podstawy programowej kształcenia ogólnego w liceum ogólnokształcącym, technikum oraz szkołach branżowych II stopnia to pierwsza z metod badawczych, której zadaniem jest zweryfikowanie stanu faktycznego dotyczącego realizacji przygotowania uczniów do bezpiecznego funkcjonowania w świecie wirtualnym. Zastosowanie tej metody pozwoli na stwierdzenie czy istnieją obiektywne możliwości, aby edukacja do cyberbezpieczeństwa była realizowana w polskich szkołach.

Jednym ze sposobów realizacji tego zadania postawionego przed polskim systemem oświatowym przez ustawodawcę jest realizacja w polskich szkołach przedmiotu o nazwie edukacja dla bezpieczeństwa (EDB). Wraz z reformą, która weszła w życie od roku szkolnego 2017/2018 i zmianą podstawy programowej, przedmiot ten jest obecnie nauczany w szkole podstawowej, na II etapie edukacji (klasy IV – VIII) oraz w szkołach ponadgimnazjalnych.

Na poziomie szkoły podstawowej, przedmiot ten ma na celu przygotowanie uczniów do odpowiedniego zachowania w przypadkach zagrożenia zdrowia i życia a jedną z najważniejszych umiejętności jest udzielanie pierwszej pomocy (Dz. U. z 2017, poz. 356). W celach kształcenia na tym poziomie wymaga się od ucznia rozumienia istoty bezpieczeństwa państwa, przygotowania do działań w sytuacjach nadzwyczajnych takich jak katastrofy i wypadki masowe, umiejętności z zakresu podstaw udzielania pierwszej pomocy oraz prezentowania postaw prozdrowotnych (Dz. U. z 2017, poz. 356). Analiza treści nauczania pokazuje, iż uczeń winien być zorientowany w takich tematach jak między innymi: składniki bezpieczeństwa państwa, rola organizacji międzynarodowych w zapewnianiu Polsce bezpieczeństwa, zachowanie w sytuacjach katastrof oraz wypadków masowych takich jak pożar, powódź, śnieżyca czy katastrofa chemiczna a nawet atak terrorystyczny, pierwsza pomoc przedmedyczna oraz szereg kwestii związanych z edukacją zdrowotną (Dz. U. z 2017, poz. 356).

Natomiast jeśli chodzi o kontynuację nauczania tego przedmiotu na poziomie szkoły ponadpodstawowej, to jest to realizowane w zakresie podstawowym i jego głównym założeniem jest teoretyczne i praktyczne przygotowanie do

działania w sytuacjach trudnych i kryzysowych, które są zagrożeniem dla zdrowia i życia. Również na tym etapie umiejętności udzielania pierwszej pomocy oraz edukacja zdrowotna należą do najważniejszych tematów (Dz. U. z 2018, poz. 467). W celach kształcenia podstawa programowa wskazuje na cztery działy, to jest: bezpieczeństwo państwa, przygotowanie do działań ratowniczych w sytuacjach nadzwyczajnych, podstawy pierwszej pomocy oraz edukacja zdrowotna. Jeśli chodzi o treści nauczania, to również na tym etapie uczeń winien znać między innymi strukturę obronności państwa, geopolityczne aspekty bezpieczeństwa, zagrożenia terrorystyczne, zasady ochrony ludności i obrony cywilnej w sytuacjach nadzwyczajnych zagrożeń, zasady pierwszej pomocy oraz tematykę związaną z edukacją prozdrowotną (Dz. U. z 2018, poz. 467). W ty miejscu warto też zwrócić uwagę, iż w dziale pierwszym – Bezpieczeństwo państwa, jako ostatnią 15 treść podano – *wyjaśnia znaczenie cyberprzemocy i zna procedury postępowania w przypadku jej wystąpienia oraz wskazuje niewłaściwe zachowania dotyczące cyberprzemocy i wie, jaka powinna być na nie właściwa reakcja* (Dz. U. z 2018, poz. 467). Jest to jedyne miejsce, w podstawie programowej dotyczącej tego przedmiotu, gdzie użyto słowa *cyber* ale ograniczono je jedynie do kwestii związanych z cyberprzemocą.

W roku 2022, Minister Edukacji i Nauki podpisał rozporządzenia zmieniające podstawy programowe, które wprowadziły zmiany w nauczaniu przedmiotu edukacja dla bezpieczeństwa, na poziomie szkoły podstawowej (Dz. U. 2022, poz. 1717) oraz szkole ponadpodstawowej (Dz. U. 2022, poz. 1705). Podstawowy obszar na obu poziomach dotyczy zamiany edukacji zdrowotnej na edukację obronną. Ponadto, w podstawie dla szkół podstawowych dodany w ostatnim obszarze tematy związane z cyberbezpieczeństwem w wymiarze wojskowym (Dz. U. 2022, poz. 1717) a w podstawie dla szkół ponadpodstawowych, kwestie cyberzagrożeń w wymiarze cywilnym w obszarze bezpieczeństwo państwa oraz tematykę cyberbezpieczeństwa w aspekcie wojskowym, w obszarze edukacja obronna (Dz. U. 2022, poz. 1705).

Podsumowując, przedmiot edukacja dla bezpieczeństwa jest obszarem nauczania, który w sposób szczególny dedykowany jest zagadnieniom bezpieczeństwa. Poruszane są tam bardzo różnorodne zagadnienia, ale kwestia cyberbezpieczeństwa jest albo w ogóle nieobecna lub traktowana bardzo marginalnie. W podstawie programowej dla tego przedmiotu przed ostatnią

reformą, tematy bezpieczeństwa w cyberprzestrzeni praktycznie nie istnieją. W podstawie programowej po reformie, kwestia ta ograniczona jest zaledwie do cyberprzemocy. Dopiero ostatnia nowelizacja podstawy programowej z 2022 roku, która weszła w życia od 1 września 2022 roku, dokonuje rozszerzenia tej tematyki, ale też ma swoje ograniczenia.

Wydawać by się mogło, iż edukacja w obszarze cyberbezpieczeństwa dokonuje się w polskiej szkole przede wszystkim na przedmiocie specjalnie do tego dedykowanym, to jest na edukacji dla bezpieczeństwa. Analiza założeń tego przedmiotu, przedstawiona powyżej pokazuje, że jednak tak nie jest lub jest w bardzo ograniczonym zakresie. Warto więc przeanalizować szerzej treści nauczania w polskich szkołach, aby zobaczyć czy i w jakim zakresie polski uczeń ma szanse zdobyć wiedzę, umiejętności oraz kompetencje dotyczące tego obszaru.

Przede wszystkim warto spojrzeć na podstawy programowe nauczania w polskich szkołach, aby zobaczyć czy treści dotyczące cyberprzestrzeni oraz cyberbezpieczeństwa są realizowane podczas innych przedmiotów. Warto też przeanalizować inne formy nauczania, w tym udział szkół i uczniów w różnego rodzaju programach i projektach ukierunkowanych na tą tematykę.

Jak to już zostało wspomniane, podczas zajęć z edukacji dla bezpieczeństwa, realizowane są bardzo różne treści, ale zagadnienie cyberbezpieczeństwa praktycznie tam nie istnieje. Wprawdzie, w 2022 roku, dokonano pewnych zmian, gdzie edukacja zdrowotna została zamieniona na edukację obronną i gdzie dodano kilka tematów związanych z cyberbezpieczeństwem. Niemniej jednak, trzeba wskazać, iż przedmiot edukacja dla bezpieczeństwa, to nie jest przedmiot, podczas realizacji którego polski uczeń nabyłby gruntowną wiedzę na temat radzenia sobie w cyberprzestrzeni.

W odniesieniu do powyższych stwierdzeń pojawia się pytanie, czy polski uczeń pozbawiony jest możliwości nabycia wiedzy, umiejętności i kompetencji w zakresie bezpiecznego funkcjonowania w wirtualnym świecie. Odpowiedź na tak postawione pytanie nie może być jedynie oparta na treściach programowych realizowanych na poszczególnych etapach podczas poszczególnych przedmiotów. Szkoła to nie tylko przedmioty, ale również udział uczniów, w różnego rodzaju projektach i programach. Są to programy społeczne, rządowe lub implementowane przez organizacje pozarządowe. Ich celem jest podnoszenie poziomu wiedzy, umiejętności i kompetencji uczniów w tym

zakresie oraz podniesienie świadomości na temat zagrożeń związanych z cyberprzestępczością. Bardzo ważną częścią tych programów, co wymaga pochowały i podkreślenia jest nauka praktycznych umiejętności w obszarze korzystania z nowoczesnych technologii w sposób bezpieczny dla siebie i innych. Implementacja różnych projektów i programów jest godna pochwały, ale problem polega na tym, iż są to wydarzenia, zdarzenia czy sytuacje jednostkowe lub czasowe a nie systematyczne przekazywanie wiedzy czy nabywanie umiejętności lub kompetencji.

Jak to zostało już wykazane wcześniej, przedmiot edukacja dla bezpieczeństwa nie jest miejscem, gdzie uczeń polskiej szkoły otrzymałby gruntowne przygotowanie do bezpiecznego funkcjonowania w cyberprzestrzeni. Biorąc pod uwagę powyższe względy, należy dokonać szerszej analizy dokumentów, to jest podstawy programowej, aby stwierdzić czy może na innych przedmiotach, owe treści są realizowane. Aby sprawdzić, czy i w jakim zakresie ów rodzaj edukacji jest realizowany w polskiej szkole, dokonano analizy podstawy programowej dla szkoły podstawowej oraz podstawy programowej dla liceum ogólnokształcącego, technikum oraz szkół branżowych II stopnia.

W podstawie programowej dla szkoły podstawowej, słowo BEZPIECZEŃSTWO pojawia się kilkadziesiąt razy, ale tylko raz w kontekście bezpieczeństwa cyfrowego, w podstawie programowej przedmiotu informatyka, gdzie w dziale Przestrzeganie prawa i zasad bezpieczeństwa jest wskazanie, że uczeń *opisuje kwestie etyczne związane z wykorzystaniem komputerów i sieci komputerowych, takie jak: bezpieczeństwo, cyfrowa tożsamość, prywatność, własność intelektualna, równy dostęp do informacji i dzielenie się informacją* (Dz. U. z 2017, poz. 356).

Natomiast słowo CYBER, w podstawie programowej szkoły podstawowej pojawia się zaledwie cztery razy. Pierwszy z tych przypadków nie jest istotny z punktu widzenia tej analizy, gdyż jest to tytuł utworu Stanisława Lema – *Cyberiada*, z listy lektur. Kolejnym przypadkiem jest podstawa programowa przedmiotu wiedza o społeczeństwie, gdzie w dziale Nieletni wobec prawa, jest wskazanie, iż uczeń *przedstawia korzyści i zagrożenia wynikające z korzystania z zasobów Internetu; rozpoznaje przemoc w cyberprzestrzeni i wyjaśnia, jak należy na nią reagować*. Trzeci przypadek, to przedmiot wychowanie do życia w rodzinie, gdzie w dziale dojrzewanie, mamy wymaganie, iż uczeń *zna*

zagrożenia okresu dojrzewania, takie jak: uzależnienia chemiczne i behawioralne, presja seksualna, pornografia, cyberseks, prostytucja nieletnich; potrafi wymienić sposoby profilaktyki i przeciwdziałania. Ostatnim miejscem, gdzie występuje interesujący nas termin jest przedmiot Etyka, który jak powszechnie wiadomo nie jest przedmiotem dla wszystkich. W dziele Człowiek wobec innych, znajduje się wymaganie, iż uczeń *rozpoznaje i charakteryzuje różne przejawy przemocy; wyjaśnia pojęcie cyberprzemocy* (Dz. U. z 2017, poz. 356).

Analiza podstawy programowej kolejnego etapu edukacyjnego, to jest dla liceum technikum oraz szkoły branżowej II stopnie (w dwóch opcjach dla uczniów po gimnazjum oraz po ośmioletniej szkole podstawowej) pokazuje, iż słowo BEZPIECZEŃSTWO jest tam użyte ponad 100 razy. Niemniej należy stwierdzić, że są to tak naprawdę trzy podstawy programowe do trzech różnych typów szkół. Mimo tak licznego użycia tego słowa, w kontekście interesującego nas cyberbezpieczeństwa lub bezpieczeństwa cyfrowego występuje ono zaledwie kilka razu. Jednym z takich przypadków jest przedmiot Podstawy przedsiębiorczości, gdzie uczeń *analizuje oferty usług banków komercyjnych i spółdzielczych oraz spółdzielczych kas oszczędnościowo-kredytowych w zakresie kont osobistych, kart płatniczych, lokat terminowych, kredytów i pożyczek oraz oferty pozabankowych instytucji pożyczkowych, uwzględniając realną stopę procentową, a także dostrzega zagrożenia i rozumie zasady bezpieczeństwa przy korzystaniu z bankowości elektronicznej* (Dz. U. z 2018, poz. 467).

Ponadto, w przedmiocie Informatyka mamy fragmenty dotyczące cyberbezpieczeństwo, gdzie, w treściach szczegółowych mamy wskazania, iż uczeń *projektuje i tworzy relacyjną bazę złożoną z wielu tabel oraz sieciową aplikację bazodanową dla danych związanych z rozwiązywanym problemem, formułuje kwerendy, tworzy i modyfikuje formularze oraz raporty, stosuje język SQL do wyszukiwania informacji w bazie i do jej modyfikacji, uwzględnia kwestie integralności danych, bezpieczeństwa i ochrony danych w bazie*, *stosuje dobre praktyki w zakresie ochrony informacji wrażliwych (np. hasła, pin), danych i bezpieczeństwa systemu operacyjnego, objaśnia rolę szyfrowania informacji* oraz *opisuje szkody, jakie mogą spowodować działania pirackie w sieci, w odniesieniu do indywidualnych osób, wybranych instytucji i całego społeczeństwa*. Ponadto, pewne nawiązania do bezpieczeństwa cyberprzestrzeni czy bezpieczeństwa w sieci mamy w warunkach realizacji podstawy programowej oraz w treściach

programowych dla przedmiotu język mniejszości narodowych (Dz. U. z 2018, poz. 467).

Dodatkowo, słowo CYBER pojawia się w omawianej podstawie programowej 8 razy, czyli 2 razy więcej niż w podstawie programowej dla szkoły podstawowej. Niemniej jednak to podwojenie liczby jest pozorne, gdyż jak zostało to wspomniane powyżej są to trzy różne podstawy programowe. Dlatego warto skupić się na podstawie programowej dla liceum ogólnokształcącego i technikum, gdzie wspomniane słowo występuje 4 razy. Pierwszym przypadkiem, są założenia ogólne do podstawy programowej, gdzie w najważniejszych umiejętnościach wymienia się *umiejętność sprawnego posługiwania się nowoczesnymi technologiami informacyjno – -komunikacyjnymi, w tym dbałość o poszanowanie praw autorskich i bezpieczne poruszanie się w cyberprzestrzeni*. Kolejnym miejscem jest wspominany już punkt 15, w treściach przedmiotu Edukacja dla bezpieczeństwa, który mówi, iż uczeń *wyjaśnia znaczenie cyberprzemocy i zna procedury postępowania w przypadku jej wystąpienia oraz wskazuje niewłaściwe zachowania dotyczące cyberprzemocy i wie, jaka powinna być na nie właściwa reakcja* (Dz. U. z 2018, poz. 467). W tym przypadku wyraz CYBER w połączeniu z przemocą pojawia się dwa razy.

Ostatnim miejscem wartym odnotowania jest przedmiot Etyka (czyli przedmiot nieobowiązkowy), gdzie w dziale Etyka a nauka i technika znaleźć można wymaganie, iż uczeń *identyfikuje i analizuje wybrane problemy moralne związane z postępem naukowo-technicznym (np. problem ochrony prywatności, ochrony praw autorskich, cyberprzemocy, rozwój sztucznej inteligencji, transhumanizm)* (Dz. U. z 2018, poz. 467).

Pozostałe miejsca, gdzie występuje termin CYBER to powtórzenie wcześniejszych wskazań, ale w odniesieniu do postawy programowej realizowanej na poziomie szkół branżowych II stopnia.

Drugą metodą badawczą, której celem jest zbadanie subiektywnych odczuć uczniów w obszarze cyberbezpieczeństwa jest sondaż diagnostyczny. Aby stwierdzić na ile uczniowie czują się bezpieczni w wirtualnym świecie i czy owe poczucie bezpieczeństwa zawdzięczają szkole, zastosowano technikę ankiety oraz narzędzie badawcze jakim jest kwestionariusz ankiety.

Ponieważ w analizie dokumentów skupiono się na podstawie programowej szkoły podstawowej oraz podstawie programowej liceum ogólnokształcącego

i technikum, na respondentów wybrano właśnie uczniów uczęszczających do tych rodzajów szkół.

Ankieta została przeprowadzona w dwóch grupach uczniów. Pierwszą grupę stanowiło 76 uczniów szkoły podstawowej klas VII i VIII. Drugą grupę stanowiło 82 uczniów liceum i technikum. Kwestionariusz ankiety został rozesłany za pomocą Internetu (media społecznościowe) oraz z wykorzystaniem nauczycieli pracujących we wspomnianych rodzajach szkół.

Jeśli chodzi o charakterystykę respondentów pierwszej grupy, to wśród 76 uczniów, 42 uczęszczało do klasy VII a 34 do klasy VIII. Wśród badanych 52 osoby były płci żeńskiej natomiast 24 reprezentowało płeć męską. Jeśli natomiast chodzi o miejsce zamieszkania, to znacząca większość, bo 51 respondentów było mieszkańcami miasta a 25 zamieszkiwało obszar wiejski.

W drugiej grupie respondentów z III etapu edukacji (liceum i technikum) na 82 osoby, 61 to uczniowie liceum ogólnokształcącego a 21 to uczniowie technikum. Jeśli chodzi o rozkład płci, to 52 respondentów płeć żeńska i 30 to płeć męska. Podobnie jak w pierwszej grupie, większość respondentów – 64 osoby zamieszkiwała miasto a 18 to mieszkańcy wsi.

Po dokonaniu krótkiej charakterystyki grup badawczych, zaprezentowane zostaną teraz wyniki badań. W ankiecie obie grupy odpowiadały na te same pytania.

Pierwsze pytanie dotyczyło ogólnego poczucia cyberbezpieczeństwa. W pierwszej grupie odpowiedzi, że tak udzieliło 12 respondentów, raczej tak – 19, raczej nie – 21, na pewno nie – 13, a nie potrafiło udzielić odpowiedzi – 11 osób.

W drugiej grupie, 21 respondentów udzieliło odpowiedzi tak, również 21 – raczej tak, raczej nie odpowiedziało 13, na pewno nie – 20 a nie potrafiło udzielić odpowiedzi 7. W tej grupie sytuacja wygląda lepiej, bo mniej niż połowa (blisko 49%) respondentów nie czuje się cyberbezpieczna.

Drugie pytanie dotyczyło oceny, jaką wystawiliby uczniowie swoim szkołom w obszarze przygotowania ich do bezpiecznego funkcjonowania w cyberprzestrzeni. Uczniowie mogli wystawić oceny w skali szkolnej, czyli od 1 do 6. W grupie reprezentującej szkołę podstawową wystawiono następujące oceny: ocena niedostateczna – 3, ocena dopuszczająca – 11, ocena dostateczna – 31, ocena dobra – 18, ocena bardzo dobra – 13, ocena celująca – 0.

Z odpowiedzi na to pytanie wynika, nikt w tej grupie nie wystawił oceny najwyższej a także pojawiają się oceny niedostateczne. Ponadto, najczęściej wystawianą oceną była ocena dostateczna. Średnia ocen dla grupy reprezentującej uczniów szkoły podstawowej to 3,36.

W drugiej grupie reprezentującej liceum i technikum, wystawiono następujące stopnie szkole: ocena niedostateczna – 4, ocena dopuszczająca – 14, ocena dostateczna – 42, ocena dobra – 1, ocena bardzo dobra – 10 oraz ocena celująca – 1.

Z odpowiedzi na to pytanie wynika, że w tej grupie, tylko jedna osoba wystawiła ocenę najwyższą. Są tutaj również oceny niedostateczne. Ponadto, najczęściej wystawianą oceną była ocena dostateczna. Średnia ocen dla drugiej grupy to 3,15.

Kolejne pytanie dotyczyło aktualności używanego oprogramowania antywirusowego w urządzeniach łączących się z Internetem. Jest to kwestia bardzo podstawowa i bardzo kluczowa. Tak naprawdę cyberbezpieczeństwo i bezpieczne funkcjonowanie w świecie wirtualnym rozpoczyna się od posiadania aktualnego i dobrze działającego oprogramowania. Wiedza na temat tego obszaru zabezpieczeń należy do najbardziej podstawowych kwestii.

W pierwszej grupie odpowiedzi pozytywnej, że ma takowe oprogramowanie udzieliło 24 respondentów, 15 stwierdziło, że nie ma, a aż 37 – nie wiedziało i nie potrafiło udzielić odpowiedzi na to pytanie.

W drugiej grupie, 34 osoby było przekonane, że posiadają aktualne zabezpieczeni antywirusowe, 12 odpowiedziało, że nie ma, a 36, że nie wie.

W tym pytaniu szczególnie rzuca się w oczy brak wiedzy na temat zabezpieczenia antywirusowego, które jest podstawową kwestią w obszarze bezpieczeństwa cyfrowego. W pierwszej grupie brak wiedzy odnośnie tak ważnego aspektu deklaruje blisko 49% respondentów. W drugiej grupie liczba ta wynosi prawie 45%.

Pytanie numer 4 dotyczyło anonimowości w Internecie. W grupie uczniów szkoły podstawowej, aż 31 respondentów jest przekonanych o anonimowości, 15 twierdzi, że takowej nie ma, 30 deklaruje brak wiedzy na ten temat. W grupie uczniów liceum i technikum, świadomość w tym aspekcie jest dużo lepsza. Jedynie 7 respondentów myśli, że jest anonimowa, 64 stwierdza, że nie i 11 nie posiada wiedzy. Widać tutaj dużą różnicę w świadomości pomiędzy obiema grupami, co zapewne jest spowodowane wiekiem i poziomem zaawansowania.

Kolejne pytanie sprawdzało bardzo podstawową zasadę bezpieczeństwa w sieci a mianowicie kwestie przekazywania informacji o sobie osobom poznanym w sieci. W tym wypadku, w pierwszej grupie, zaledwie 3 osoby odpowiedziały, iż nigdy takich informacji nie przekazują, 5 osób wskazało, iż robią to czasem, a 11, że sporadycznie. Aż 57 osób zadeklarowało, że przekazują takowe informacje, ale dotyczy to tylko adresu e-mail lub namiarów na swój profil w mediach społecznościowych.

W drugiej grupie, 11 osób nigdy nie przekazało żadnych swoich danych, 9 respondentów robi to czasem, a 4 sporadycznie. Również w tej grupie, znacząca większość bo aż 58 osób, przekazuje swoje dane kontaktowe czyli adres e-mail i informacje o swoich social mediach.

Wydaje się, że tak nagminne przekazywanie owych informacji w obu grupach spowodowane jest chęcią nawiązywania nowych kontaktów.

Swoistą kontynuacją pytania poprzedniego, było podjęcie kwestii umawiania się i spotykania z osobami poznanymi w Internecie. W pierwszej grupie proceder ten nie jest zbyt popularny. Tylko 12 osób odpowiedziało, że spotkało się w realu z osobą poznaną w świecie wirtualnym a 64 stwierdziły, że nie.

Trochę inaczej wygląda sytuacja w drugiej grupie, gdzie do spotkania przyznaje się 34 respondentów a 48 odpowiada, że nie.

Widoczna tutaj różnica najprawdopodobniej spowodowana jest wiekiem i poziomem kontroli rodzicielskiej.

Kolejne pytania dotyczyły kwestii bezpiecznego hasła. W pytaniu nr 7, w pierwszej grupie, 15 respondentów uważa, że używa bezpiecznych haseł, 14 uważa, że ich hasła bezpieczne nie są a aż 47 nie potrafi udzielić odpowiedzi na to pytanie.

W drugiej grupie sytuacja wygląda lepiej, gdyż 31 osób uważa, że ich hasła są bezpieczne, 12 – twierdzi, że nie są a 39 deklaruje brak wiedzy w ty temacie.

W pytaniu 8 respondenci mieli odpowiedzieć, czy wiedzą w jaki sposób tworzy się bezpieczne hasło. W pierwszej grupie tylko 11 odpowiedziało, że tak a 65, że nie.

W drugiej grupie, pozytywnej odpowiedzi udzieliło 39 uczniów a 43 przyznało, że nie zna zasad tworzenia bezpiecznego hasła.

Ów brak wiedzy na temat zasad tworzenia bezpiecznych haseł został potwierdzony w kolejnym pytaniu. Było to pytanie otwarte brzmiące – Co

to jest bezpieczne hasło. Zaledwie kilka osób potrafiło udzielić poprawnej i fachowej odpowiedzi – w pierwszej grupie 7 osób, w drugiej 13. Reszta albo próbowała coś tworzyć, co nie spełniało standardów poprawnej odpowiedzi albo napisała nie wiem.

W pytaniu 9 podjęto kwestię częstotliwości zmiany hasła. W grupie uczniów szkoły podstawowej, 12 odpowiedziało nigdy, 27 – tylko jeśli zapomnę, 8 dokonuje zmiany co najmniej raz w miesiącu, a 29 rzadziej niż raz na miesiąc.

W drugiej grupie reprezentującej uczniów III etapu edukacyjnego, nigdy hasła nie zmienia 19, tylko w przypadku zapomnienia zmiany dokonuje – 29, co najmniej raz w miesiącu robi to 11, a rzadziej niż raz na miesiąc 23 respondentów.

Dwa ostatnie pytania dotyczyły częstotliwości używania Internetu oraz ewentualnego uzależnienia od niego. W pierwszej grupie, tylko 2 uczniów spędza w wirtualnym świecie nie więcej niż 1 godzinę, 18 – używa Internetu od 2 do 3 godzin, 49 – od 4 do 6 godzin, a 7 przebywa w cyberprzestrzeni 7 lub więcej godzin.

W drugiej grupie tendencja jest podobna. Nie więcej niż 1 godzinę w Internecie spędza 4 respondentów, 19 – od 2 do 3 godzin, 51 – od 4 do 6 a 8 uczniów przebywa w świecie wirtualnym 7 lub więcej godzin. Deklaracje te pokazują, że najczęściej uczniowie spędzają od 4 do 6 godzin.

W związku z powyższym, zasadne było również zadanie pytania o ewentualne uzależnienie od Internetu. Na pytanie brzmiące – czy myślisz, że możesz być uzależniony od Internetu, w pierwszej grupie aż 59 osób odpowiedziało – nie, 4 – że jest to możliwe i 13 nie wie.

W drugiej grupie, odpowiedzi negatywnej udzieliło 49 osób, 11 respondentów przyznało, iż istnieje taka możliwość a 22 nie jest w stanie udzielić odpowiedzi.

Generalnie, odpowiedzi tutaj wskazują, iż większość respondentów nie widzi problemu z uzależnieniem, ale jest to tylko ich subiektywne odczucie. Ludziom nie jest łatwo przyznać się do uzależnienia, a po drugie, znaczący jest odsetek tych, którzy nie są w stanie odpowiedzieć na to pytanie. Brak odpowiedzi negatywnej – nie jestem świadczy o tym, iż nie przyznają się wprost do uzależnienia, ale mają w tej kwestii jakieś wątpliwości.

Zaprezentowany wyniki ankiety pokazują poziom przygotowania uczniów szkoły podstawowej oraz uczniów III etapu edukacyjnego do bezpiecznego

funkcjonowania w wirtualnym świecie. Część pytań dotyczyła subiektywnych odczuć respondentów a część miała za zadanie zweryfikowanie rzeczywistej wiedzy i umiejętności w badanym obszarze.

Obraz nauczania o cyberbezpieczeństwie w polskiej szkole – analiza i wnioski

Przeprowadzony przegląd literatury przedmiotu w tematyce cyberprzestrzeń, cyberbezpieczeństwo oraz zagrożenia cyberbezpieczeństwa a także badania własne z użyciem analizy treści kształcenia w szkołach podstawowych, liceach i technikach oraz ankieta na temat cyberbezpieczeństwa przeprowadzona wśród uczniów wskazanych poziomów edukacyjnych tworzy obraz nauczania o cyberbezpieczeństwie w polskiej szkole.

Dokonując analizy zaprezentowanych wyników badań, wskazać należy, iż problemem polskiej szkoły jest brak oddzielnego przedmiotu, który przekazywałby treści związane z bezpiecznym funkcjonowaniem w wirtualnym świecie. Wprawdzie, na II i III etapie edukacyjnym, podstawy programowe przewidują przedmiot nazywany edukacją dla bezpieczeństwa to jednak analiza treści programowych tego przedmiotu wskazuje, iż kwestie związane z cyberbezpieczeństwem są tam zupełnie pomijane lub traktowane bardzo marginalnie. W podstawie programowej przedmiotu edukacja dla bezpieczeństwa jest wiele bardzo przydatnych treści. Na pewno ważną rzeczą jest wyposażenie każdego ucznia w wiedzę i umiejętności praktyczne związane z udzielaniem pierwszej pomocy. Na pewno istotne są kwestie i zachowania prozdrowotne wycofane z podstawy programowej zmiany z 2022 roku i zastąpione kwestiami związanymi z obronnością kraju. Na pewno ważnym jest rozumienie istoty bezpieczeństwa państwa czy przygotowanie uczniów do działań w sytuacjach nadzwyczajnych zagrożeń (katastrof i wypadków masowych). Niemniej jednak należy powiedzieć, iż współczesny człowiek, szczególnie młody człowiek spędza w wirtualnym świecie znaczną część swojego życia. Dlatego nauczenie go bezpiecznego funkcjonowania w tym obszarze jest niemniej ważne a z punktu widzenia osobistego poczucia bezpieczeństwa wprost konieczne.

Edukacja dla cyberbezpieczeństwa może być realizowana nie tylko podczas dedykowanego przedmiotu, ale też podczas innych zajęć. Analiza całej podstawy programowej pokazuje, iż również na innych zajęciach temat cyberprzestrzeni i cyberbezpieczeństwa traktowany jest dość marginalnie. Mamy go na kilku przedmiotach, w tym na informatyce czy etyce (która nie jest obowiązkowa) a na III etapie edukacyjnym jeszcze na przedmiocie podstawy przedsiębiorczości. Podejmowane kwestie dotyczą jednak tylko cyberprzemocy czy bezpieczeństwa systemów informatycznych lub kwestii związanych z bezpiecznym korzystaniem z bankowości internetowej. Są to istotne kwestie i ważne, ale nie jedyne. Niestety, wiele obszarów zostało pominiętych.

Wprawdzie istnieją różnego rodzaju programy i projekty mające na celu zwiększenie poziomu bezpieczeństwa cyfrowego w szkole i wśród uczniów, które były lub są realizowane, ale są to sytuacje epizodyczne a nie ciągły proces kształcenia. Jako plus należy dodać, iż kwestie bezpieczeństwa cyfrowego powinny, zgodnie z rekomendacją, znaleźć się w programach profilaktyczno-wychowawczych. Niemniej jednak ich skuteczność jest dość ograniczona, często kwestie bezpieczeństwa cyfrowego nie są tam obecne lub są tak tylko w teorii.

Bardzo istotnym wnioskiem jest, iż sami uczniowie nie do końca mają poczucie bezpieczeństwa w cyberprzestrzeni. Ankieta pokazała, iż średnio połowa z nich nie posiada takiego poczucia. Wprawdzie przeprowadzony sondaż diagnostyczny nie ma charakteru badania reprezentatywnego, ale udzielone odpowiedzi są dość symptomatyczne i pokazują, że w tym obszarze jest problem.

Niepokojąca jest też ocena wystawiona przez uczniów szkole za poziom przygotowania do bezpiecznego funkcjonowania w świecie wirtualnym. Fakt, iż najczęściej wystawianą oceną jest dostateczny oraz że średnia ocen wystawionych przez uczniów w szkole podstawowej to 3,36 a w szkole średniej to 3,15 (w szkolnej skali 1 – 6) pokazuje, iż uczniowie nie widzą szkoły jako miejsca, które przygotowywałby ich do funkcjonowania w świecie wirtualnym.

Ankieta pokazała również, iż w wielu obszarach uczniowie nie są w stanie udzielić odpowiedzi, gdyż nie mają odpowiedniej wiedzy lub odpowiednich umiejętności. Nie potrafią odpowiedzieć czy ich hasło jest bezpieczne, nie zmieniają odpowiednio często swoich haseł, nie wiedzą czy posiadają aktualne oprogramowanie antywirusowe, przekazują swoje dane osobom poznanym

w Internecie lub spotykają się z takimi osobami. Nie musi to oznaczać nic złego, ale pokazuje obszar, który może powodować niepokój. Ponadto zdarza się, że ich wiedza jest błędna – część z nich ciągle myśli, iż jest anonimowa w sieci. Ów ogólny brak rozeznania w świecie wirtualnym potwierdza nie tylko ankieta zrobiona na grupie 158 respondentów, ale częste doniesienia medialne dotyczące utraty oszczędności całego życia poprzez nieodpowiedzialne zachowania związane z posiadanym kontem bankowym. Wiadomym jest, iż cyberprzestępcy mają coraz lepsze sposoby wyłudzania danych lub obejścia zabezpieczeń, ale często żadne zabezpieczenie nic nie da, jeśli zawiedzie czynnik ludzki. Jeśli co jakiś czas czytamy w mediach o osobach, które utraciły środki na koncie bankowym, gdyż podały nieznajomym osobom poprzez e-mail lub rozmowę telefoniczną swoje dane do logowani, to wniosek może być tylko jeden. Wielu z nas nie jest przygotowanym do bezpiecznego funkcjonowania w świecie wirtualnym.

Podsumowując analizę części teoretycznej i części badawczej tej pracy, stwierdzić należy, iż być może przygotowanie do bezpiecznego funkcjonowania w świecie wirtualnym realizowane przez polską szkołę istnieje, ale nie jest ono wystarczające i domaga się daleko idących zmian.

Zakończenie

Niniejsze opracowanie podejmuję tematykę ważną i istotną a mianowicie problematykę przygotowania polskiego ucznia do bezpiecznego funkcjonowania w świecie wirtualnym. Kwestia ta jest ważna, aktualna i istotna z dwóch zasadniczych powodów, Po pierwsze, współczesny człowiek spędza w wirtualnej rzeczywistości coraz więcej czasu i robi tam coraz więcej rzeczy. Po drugie, różne raporty wskazują, iż doświadczamy i będziemy doświadczać coraz większych, częstszych i bardziej niebezpiecznych zagrożeń w obszarze cyberprzestrzeni. W związku z powyższym, szkoła, która jest miejscem przekazywania wiedzy i umiejętności z różnych obszarów, winna również zająć się tym jakże ważnym obszarem funkcjonowania współczesnego człowieka. W ten sposób jedna z istotnych potrzeb uczniów – potrzeba właściwego funkcjonowania w świecie wirtualnym będą zaspokajane.

W oparciu o otrzymane dane należy stwierdzić, iż: szkoła w Polsce nie w pełni przygotowuje do życia i funkcjonowania w świecie cyfrowym. Oznacza to, iż: poziom i zakres edukacji do cyberbezpieczeństwa nie jest wystarczający oraz że polski uczeń nie ma poczucia bycia przygotowanym przez szkołę do funkcjonowania w świecie wirtualnym, zakres przygotowania przez szkołę nie jest wystarczający.

Bibliografia

Datareportal.com. (2023). Digital 2023: Global Overview Report. w: https://datareportal.com/reports/digital-2023-global-overview-report (10.05.2023).

ENISA. (2022a). ENISA Threat Landscape 2022. Dostęp on-line: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (20.12.2022),

ENISA. (2022b). Cybersecurity Threats Fast-Forward 2030: Fasten your Security-Belt Before the Ride! Dostęp on-line: https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030 (29.12.2022).

Hasło *cyberprzestrzeń*, w: Słownik języka polskiego PWN. Dostęp on-line: https://sjp.pwn.pl/sjp/cyberprzestrze%C5%84;2553915 (10.12.2022).

Hasło *cybersecurity* w: Joint publication 1-02. Department of Defense Dictionary of Military and Associeted Terms. Wydano 8 listopada 2010, teks poprawiony z dnia 15 lutego 2016. Dostęp on-line: https://irp.fas.org/doddir/dod/jp1_02.pdf (28.12.2022).

Hasło *cyberspace* w: Joint publication 1-02. Department of Defense Dictionary of Military and Associeted Terms. Wydano 8 listopada 2010, teks poprawiony z dnia 15 lutego 2016. Dostęp on-line: https://irp.fas.org/doddir/dod/jp1_02.pdf (28.12.2022).

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r., Dz. U. 1997, nr 78, poz. 483.

Pokruszyński, W. (2010). Teoretyczne Aspekty Bezpieczeństw. Podręcznik Akademicki. Józefów: Wydawnictwo Wyższej Szkoły Gospodarki Euroregionalnej im. Alcide De Gasperi.

Pokruszyński, W (2012). Bezpieczeństwo. Teoria i praktyka. Podręcznik akademicki. Józefów: Wydawnictwo Wyższej Szkoły Gospodarki Euroregionalnej im. Alcide De Gasperi.

Rozporządzenie Ministra Edukacji Narodowej z dnia 14 lutego 2017 r. w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnosprawnością intelektualną w stopniu umiarkowanym lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla szkoły specjalnej przysposabiającej do pracy oraz kształcenia ogólnego dla szkoły policealnej, Dz. U. 2017, poz. 356.

Rozporządzenie Ministra Edukacji Narodowej z dnia 30 stycznia 2018 r. w sprawie podstawy programowej kształcenia ogólnego dla liceum ogólnokształcącego, technikum oraz branżowej szkoły II stopnia, Dz. U. 2018, poz. 467.

Rozporządzenie Ministra Edukacji i Nauki z dnia 1 sierpnia 2022 r. zmieniające rozporządzenie w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnosprawnością intelektualną w stopniu umiarkowanym lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla szkoły specjalnej przysposabiającej do pracy oraz kształcenia ogólnego dla szkoły policealnej, Dz. U. 2022, poz. 1717.

Rozporządzenie Ministra Edukacji i Nauki z dnia 1 sierpnia 2022 r. zmieniające rozporządzenie w sprawie podstawy programowej kształcenia ogólnego dla liceum ogólnokształcącego, technikum oraz branżowej szkoły II stopnia, Dz. U. 2022, poz. 1705.

Sitek, M. (2016). Prawa (potrzeby) człowieka w ponowoczesności. Warszawa: Wydawnictwo C.H. Beck.

Sitek, M (2018). Prawne ramy bezpieczeństwa jednostki w cyberprzestrzeni. W: Journal of Modern Science, 2/37

Sitek, B. (2016). Zasady etyczne stosowane w cyberprzestrzeni. W: Nowoczesne narzędzia informatyczne w przeciwdziałaniu zagrożeniom bezpieczeństwa. Józefów: Wydawnictwo Wyższej szkoły Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie, p. 73.

Ustawa z dnia 14 grudnia 2016 r. – Prawo oświatowe. Dz.U. z 2017 r. poz. 59, ze zm.

Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U.2016.851 t.j.)

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz. U. 2018, poz. 1560.

Wasilewski, J. (2013). Zarys definicji cyberprzestrzeni. W: Przegląd Bezpieczeństwa Wewnętrznego, 5/9.