

Tomasz Warchol*

ROLA EDUKACJI POZAFORMALNEJ W KSZTAŁTOWANIU BEZPIECZEŃSTWA CYFROWEGO UCZNIÓW SZKÓŁ PODSTAWOWYCH

Streszczenie

Artykuł prezentuje zagadnienia związane z bezpieczeństwem cyfrowym uczniów szkół podstawowych w kontekście zagrożeń wynikających z współczesnych technologii cyfrowych. Obecnie coraz młodsi uczniowie stają się narażeni na zagrożenia związane z korzystaniem z Internetu. Aktualna podstawa programowa jest przepełniona treściami kształcenia, by znaleźć w niej miejsce na skuteczną edukację w zakresie bezpieczeństwa cyfrowego uczniów. Przedstawiona w artykule problematyka proponuje rozwiązania scharakteryzowanego problemu w formie edukacji pozaformalnej, ponieważ jest ona organizowana poza formalnym programem kształcenia, umożliwia świadome uczestnictwo uczniów w procesie kształcenia i skupia się na maksymalnej aktywizacji, samodzielności i uczeniu się uczniów przez praktyczne działanie. Takie podejście pozwala na realizację różnorodnych programów edukacyjnych, które umożliwiają bardziej efektywnie wspierać bezpieczeństwo cyfrowe uczniów szkół podstawowych. W artykule przedstawiono główne zagrożenia cyfrowe, takie jak: cyberprzemoc, nieświadome ujawnianie danych osobowych, uzależnienie od urządzeń elektronicznych, ataki *phishingowe* czy niebezpieczne zachowania online. Autor zwraca również uwagę na zagrożenia w tym zakresie związane ze zdrowiem psychicznym i fizycznym uczniów. W treści artykułu duży nacisk położono na argumentację, że edukacja pozaformalna stanowi idealne środowisko do realizacji zagadnień związanych z bezpieczeństwem cyfrowym uczniów, głównie dlatego, iż realizowana jest poza szkołą, przez podmioty zewnętrzne, co umożliwia dysponowanie większymi środkami na wykorzystywanie najnowszych technologii. Pozwala to na prowadzenie wirtualnych symulacji sytuacji internetowych, gier dydaktycznych i różnorodnych paneli dyskusyjnych. Artykuł zakończono omówieniem praktycznych programów edukacji pozaformalnej wspierających bezpieczeństwo cyfrowe uczniów. Autor wskazuje na inicjatywy, takie jak cybermentoring, kluby bezpiecznego Internetu, praktyczne szkolenia z cyberbezpieczeństwa oraz warsztaty dla rodziców. Podkreśla, że edukacja pozaformalna staje się coraz bardziej popularna i jest wspierana przez różnorodne inicjatywy społeczne oraz programy państwowe. Autor argumentuje, że przedstawione programy są niezbędne w szybko zmieniającym się środowisku społecznym i technologicznym.

Słowa kluczowe: bezpieczeństwo cyfrowe, edukacja pozaformalna, zagrożenia cyfrowe, uczniowie szkół podstawowych

* Uniwersytet Rzeszowski, e-mail: twarchol@ur.edu.pl, ORCID: 0000-0002-7978-8149.

Wstęp

Obecnie wraz z dostępem do technologii cyfrowych wszyscy uczniowie w szkołach podstawowych stają się coraz bardziej narażeni na różnorodne zagrożenia związane z korzystaniem z Internetu. Z tego względu, iż podstawa programowa edukacji formalnej znacząco przeciążona jest treściami, trudno w jej obszarze wygospodarować dodatkowe miejsce na prawidłową i skuteczną edukację uczniów w zakresie ich bezpieczeństwa cyfrowego. Wsparcia w tym zakresie należy upatrywać w działaniach wychodzących poza obszar formalnej edukacji, które mają charakter edukacji pozaformalnej i realizowane są w formie różnorodnych programów edukacyjnych¹.

Obecnie edukacja pozaformalna to forma uczenia się organizowana poza formalnymi programami kształcenia, w ramach której uczniowie mogą uzyskać kwalifikację zarejestrowaną. Uczniowie biorący udział w edukacji pozaformalnej przystępują świadomie do procesu kształcenia, a wykorzystywane w niej formy i metody kształcenia ukierunkowane są na ich aktywizację, samodzielność i uczenie się przez praktyczne działanie². Ze względu na specyfikę edukacji pozaformalnej, której głównym celem jest wspieranie edukacji formalnej, staje się ona idealnym środowiskiem, w ramach którego można realizować zagadnienia związane z kształtowaniem bezpieczeństwa cyfrowego uczniów.

Zagrożenia cyfrowe dla uczniów szkół podstawowych

Współczesna edukacja w zakresie bezpieczeństwa cyfrowego uczniów szkół podstawowych jest równie ważnym elementem, jak nauczanie matematyki, języka polskiego lub innego przedmiotu. Jest to bezpośrednio związane z tym, iż z zagrożeniami cyfrowymi uczniowie spotykają się już od najmłodszych lat szkolnych³. Badania wskazują, że pierwsza inicjacja z urządzeniem elektronicznym każdego dziecka następuje już w pierwszym roku jego życia⁴, a posiadanie i użytkowanie

¹ W. Stęchły, *Edukacja formalna wobec edukacji pozaformalnej i uczenia się nieformalnego*, Warszawa 2021, s. 6.

² S. Sławiński [i in.], *Słownik podstawowych terminów dotyczących krajowego systemu kwalifikacji*, Warszawa 2014, s. 13; T. Warchol, *Wybrane rodzaje aktywności uczniów szkoły podstawowej w edukacji pozaformalnej*, Rzeszów 2021, s. 35.

³ *Bezpieczna szkoła. Zagrożenia i zalecane działania profilaktyczne w zakresie bezpieczeństwa fizycznego i cyfrowego uczniów*, Warszawa 2017, s. 15–24.

⁴ A. Bąk, *Jak małe dzieci korzystają z urządzeń mobilnych? Raport na podstawie danych zebranych od rodziców*, „Dziecko Krzywdzone. Teoria, badania, praktyka”, 2015, vol. 14, no. 3, s. 57.

smartfonu rozpoczyna się w wieku 6 lat⁵. W związku z tym w szkole podstawowej prawie każdy uczeń posiada urządzenie mobilne na własny użytek i każdego dnia narażony jest na cyfrowe niebezpieczeństwo.

Zagrożenia cyfrowe dla uczniów szkół podstawowych wynikają z powszechności korzystania z technologii cyfrowych. Jednym z podstawowych zagrożeń w kontekście uczniów szkół podstawowych jest cyberprzemoc i nękanie online⁶. Przy powszechnym „byciu w Internecie” każdy uczeń mający dostęp do urządzenia mobilnego ciągle załogowany jest do różnych mediów społecznościowych, które są głównym środowiskiem dla narażenia się na agresję, wyśmiewanie, poniżanie, groźbę czy szantaż. Uczniowie szkół podstawowych nie zdają sobie również sprawy z bezpieczeństwa ich danych osobowych. Poprzez korzystanie z różnorodnych aplikacji i serwisów internetowych uczniowie przekazują różnorodne informacje o sobie. Dane, które są w użyciu innych osób, stanowią źródło korzyści finansowych, ponieważ mogą zostać wykorzystane w zakresie kradzieży tożsamości cyfrowej i dokonywania różnorodnych przestępstw internetowych w imieniu innej osoby⁷. W obiektywnej ocenie zagrożeń cyfrowych istotne jest również uzależnienie uczniów od nadmiernego korzystania z urządzeń elektronicznych⁸, gier, aplikacji czy mediów społecznościowych, które w konsekwencji mogą prowadzić do negatywnego rozwoju emocjonalnego i społecznego uczniów. Do ważnych kwestii należą również ataki *phishingowe*, podczas których uczniowie nieświadomie logują się do złośliwych aplikacji, w ten sposób padając ofiarą wyłudzeń danych do logowania, haseł czy poufnych informacji⁹.

Niestety, używanie mediów społecznościowych przez uczniów może wiązać się z niebezpiecznymi zachowaniami online, dotyczącymi udostępniania prywatnych zdjęć, spotykania się z nieznajomymi czy udziału w groźnych wyzwaniach internetowych. Takie sytuacje mogą doprowa-

⁵ *Badanie konsumenckie 2021 – dzieci, rodzice oraz nauczyciele*, Urząd Komunikacji Elektronicznej, <https://www.uke.gov.pl>, 25.11.2023 (25.11.2023).

⁶ D. Smahel [i in.], *EU Kids Online 2020: Survey results from 19 countries*, EU Kids Online 2020, s. 45–52; S. Hinduja, J.W. Patchin, *Cyberbullying: An Update and Synthesis of the Research*. In *Handbook of Bullying Prevention*, Springer 2018, s. 191–204.

⁷ K. Ciulkin-Sarnocińska, *Phishing – specyficzna forma pozyskiwania danych newralgicznych* [w:] *Współczesne oblicza bezpieczeństwa*, red. E.M. Guzik-Makaruk, W. Pływaczewski, Białystok 2015, s. 113–121.

⁸ *Badanie RPD: Dzieci chcą, ale już nie potrafią oderwać się od mediów społecznościowych*, Rzecznik Praw Dziecka, <https://brpd.gov.pl>, 14.01.2024 (14.01.2024).

⁹ I. Protasowicki, *Phishing jako zagrożenie bezpieczeństwa osobistego w sieci*, „Zeszyty Naukowe Wyższej Szkoły Informatyki Zarządzania i Administracji w Warszawie”, 2016, nr 14, s. 35–46.

dzieć do przestępstw typu *grooming* dziecięcy¹⁰, *sexting*¹¹. Zagrożenia cyfrowe obejmują również nawyki uczniów, które obecnie związane są z tym, aby nie aktualizować oprogramowania, nie odświeżać bazy wirusów programu antywirusowego, jak również używać haseł dostępowych minimalnie spełniających wymagania, czyli tylko 8 wymaganych znaków lub jeden więcej, wyłącznie jedna duża litera, jeden znak specjalny.

Zamykając klasyfikację, należy podkreślić, że największym problemem bezpośrednio wynikających z cyfrowych zagrożeń jest cyberzdrowie ucznia. Poprzez ciągły kontakt z urządzeniami elektronicznymi uczeń narażony jest na brak ruchu fizycznego, złe nawyki żywieniowe, jak również pogorszenie zdrowia psychicznego.

Zajęcia z bezpieczeństwa cyfrowego dla uczniów w formie edukacji pozaformalnej

Realizacja wymienionych zagadnień związanych z bezpieczeństwem cyfrowym uczniów obejmuje szeroki zakres różnorodnych treści. Ilość treści ściśle związanych z bezpieczeństwem cyfrowym, w których uczniowie powinni być zorientowani, jest ogromna, a postępujący rozwój technologiczny generuje ciągle nowe obszary zagrożeń cyfrowych.

Doraźnym działaniem edukacyjnym dla aktualnej sytuacji edukacji formalnej jest realizacja zajęć dodatkowych w formie edukacji pozaformalnej. Zajęcia takie mogą być prowadzone poprzez zewnętrzne instytucje na rzecz danej szkoły lub całkowicie poza jej murami¹². Nie jest niczym nowym, że uczniowie korzystają z dodatkowych form wsparcia edukacyjnego, aby zwiększać swoją wiedzę i umiejętności. Jak wynika z badań, aż 79% uczniów korzysta z dodatkowych lekcji realizowanych prywatnie¹³, dlatego dobrą inicjatywą jest rozwijanie zaplanowanych przez specjalistów działań, specjalnie zorganizowanych w formie edukacji pozaformalnej.

¹⁰ E. Truskołaska, *Grooming, czyli uwodzenie małoletnich przez internet – aspekty kryminologiczne oraz prawne*, „Prawo w Działaniu. Sprawy karne”, 2021, t. 47, s. 72–73; S. Craven, S. Brown, E. Gilchrist, *Sexual grooming of children: Review of literature and theoretical considerations*, „Journal of Sexual Aggression”, 2006, nr 12, s. 287–299.

¹¹ D. Siemieniecka, M. Skinińska, K. Majewska, *Cyberagresja – zjawisko, skutki, zapobieganie*, Toruń 2020, s. 188.

¹² I. Stalończyk, *Edukacja formalna i pozaformalna w procesie kształtowania społeczeństwa wiedzy*, „Nierówności Społeczne a Wzrost Gospodarczy”, 2014, nr 37, s. 320–327.

¹³ *Wpływ pandemii na prywatne zajęcia edukacyjne dzieci i młodzieży*, Giganci programowania, <https://www.giganciprogramowania.edu.pl>, 14.01.2024 (14.01.2024).

Uczenie się podczas zajęć w edukacji pozaformalnej ma wiele zalet w stosunku do lekcji odbywanych przez uczniów prywatnie. Dominująca w tej kwestii jest możliwość działań grupowych, czyli rozwijania współpracy i wymiany doświadczeń¹⁴. Uczniowie mogą w trakcie spotkań odgrywać różne role, realizując sytuacje rzeczywiste, które mogą ich spotkać podczas korzystania z różnorodnych portali społecznościowych, forów, czatów, gier komputerowych. Dodatkowo poprzez różnorodne doświadczenia z codzienności w zakresie bezpieczeństwa cyfrowego istnieje możliwość wymiany swoich opinii i uczenia się od siebie nawzajem. Jest to jeden z aspektów, który stanowi fundament kształcenia pozaformalnego¹⁵.

Kolejną kwestią stojącą za zaletami edukacji pozaformalnej są działania podejmowane w edukacji pozaformalnej. Wiązą się głównie z rozwijaniem praktycznych umiejętności z dokładnie opracowanymi scenariuszami zajęć¹⁶. W ten sposób edukacja opiera się wyłącznie na konkretnych działaniach, studiach przypadków, które są symulacją realnych sytuacji z życia uczniów mogących dotyczyć ich bezpieczeństwa.

Poprzez fakt, że edukacja pozaformalna zawsze objęta jest dedykowanym programem skierowanym do konkretnej grupy wiekowej, może maksymalnie koncentrować się na zagadnieniach, które dotyczą określonej grupy wiekowej. Pozwala to na osiągnięcie dużej skuteczności w aspekcie rozumienia i przystosowania treści do danej grupy wiekowej.

Inną kwestią przemawiającą za organizacją zajęć w formie edukacji pozaformalnej są nowoczesne narzędzia edukacyjne, które w formalnym kształceniu trudno zaoferować na takim poziomie¹⁷. Działania organizowane na poziomie edukacji pozaformalnej najczęściej wiążą się z wykorzystaniem zaawansowanych technologii, np. symulacji wirtualnych poprzez technologię VR, *chatbotów* wcielających się np. w przestępcę, który jest po drugiej stronie i zachowuje się jak w realnej sytuacji w mediach społecznościowych. Zajęcia w formie edukacji pozaformalnej charakteryzuje wysoka skuteczność, bo realizowane są z naciskiem na rozwój umiejętności praktycznych¹⁸. Podczas zajęć uczniom kreuje się

¹⁴ A. Marciniak, *Pozaformalne i nieformalne aspekty edukacji akademickiej*, „Ogrody Nauk i Sztuk”, 2013, nr 3, s. 46–53.

¹⁵ A. Szlęk, *Uczyć się inaczej – nowe kompendium wiedzy na temat edukacji pozaformalnej*, Warszawa 2013, s. 12.

¹⁶ T. Warchoń, *op.cit.*, s. 7.

¹⁷ K. Majchrzak, *O edukacyjnych badaniach w działaniu w teorii i praktyce*, „Studia Dydaktyczne”, 2014, nr 26, s. 207–218.

¹⁸ D. Murlowski [i in.], *Analiza oferty edukacyjnej formalnej i pozaformalnej oraz dostępnej oferty staży i praktyk i ich adekwatności do potrzeb pracodawców*, Warszawa 2020, s. 3–36.

sztuczne sytuacje związane z bezpieczeństwem online, tworzy działania mające na celu podniesienie świadomości w obszarze odpowiedzialnego korzystania z technologii, rozwijając przy tym krytyczne, obiektywne myślenie, a także umiejętność oceny ryzyka online. Ostatnią łączącą uczniów zaletą zajęć w formie edukacji pozaformalnej jest ich interaktywność¹⁹, a więc stosowanie metod pracy, do których należą warsztaty, gry dydaktyczne, dyskusje grupowe, odzwierciedlające w maksymalnym stopniu rzeczywistość.

Edukacja pozaformalna coraz częściej jest wykorzystywana i promowana przez różnorodne inicjatywy i programy społeczne. Jej wdrożenie do edukacji intensywnie podejmują organy państwowe, tworząc inicjatywy polegające na wspieraniu uczniów szkół podstawowych w różnorodnej tematyce.

Programy edukacji pozaformalnej wspierające bezpieczeństwo cyfrowe uczniów

Obecna polityka edukacyjna ma świadomość tego, że edukacji formalnej potrzebne są dodatkowe środki, inicjatywy, działania programowe, które będą wspierać szkołę w bardzo szybkim rozwoju społecznym i technologicznym²⁰. W związku z tym coraz częściej tworzone są inicjatywy mające na celu wspieranie uczniów szkół podstawowych w różnych obszarach edukacyjnych.

W obszarze analizowanego problemu dotyczącego kształtowania bezpieczeństwa cyfrowego jednym z programów jest cybermentoring. Jest to inicjatywa, która opiera się na tworzeniu programów edukacyjnych polegających na generowaniu sytuacji rzeczywistych w zakresie bezpieczeństwa cyfrowego, w których starsi uczniowie lub absolwenci szkół podstawowych pełnią rolę mentorów dla młodszych kolegów. W ramach takich zajęć uczniowie rozmawiają ze sobą, udzielając sobie praktycznych wskazówek w zakresie bezpiecznego korzystania z technologii i aplikacji wykorzystywanych np. do komunikacji. Takie zajęcia wzmacniają doświadczenia i wskazują praktyczne przypadki. Dodatkowym atutem jest możliwość dyskusji uczestników i wymiany poglądów.

¹⁹ B. Kamińska, K. Olsza, *Współczesne środki dydaktyczne i ich zastosowanie w działalności dydaktyczno-muzycznej szkolnictwa ogólnokształcącego*, „Muzyka – Historia – Teoria – Edukacja”, 2016, nr 6, s. 11–33.

²⁰ *Znajomość zagadnień finansowych w Polsce. Znaczenie, dane i oferta edukacyjna*, OECD, <https://www.oecd.org>, 14.01.2024 (14.01.2024).

Aranżowanie tego typu spotkań pozwala na zapoznanie się z możliwościami pomocy w przypadku cyberprzemocy²¹.

Innym przedsięwzięciem są kluby bezpiecznego Internetu, które polegają na zrzeszaniu uczniów np. w bibliotekach lub innych miejscach szkoły, gdzie realizowane są zajęcia w zakresie bezpieczeństwa cyfrowego²². Do pracy w takich klubach można zaangażować różnorodnych specjalistów, praktyków w obszarze „bezpiecznego Internetu”. Spotkania z taką osobą w klubie bezpiecznego Internetu mogą mieć charakter panelu dyskusyjnego, wykładu przedstawiającego sytuacje z życia każdego ucznia. W trakcie takich zajęć należy pamiętać o przekazywaniu jak największej liczby praktycznych porad w zakresie bezpieczeństwa, jak również wygospodarowaniu czasu na bezpośrednią możliwość zadawania pytań i udzielania odpowiedzi przez eksperta.

Istotne w kwestii zajęć pozaformalnych są również działania zmierzające do organizowania praktycznych szkoleń z zakresu cyberbezpieczeństwa. Podczas takich zajęć najważniejsze jest symulowanie różnorodnych sytuacji, prowadzenie zajęć w formie aktywnego udziału uczniów. Takie szkolenia powinny podnosić wiedzę uczniów w zakresie potencjalnych ataków hakerskich, korzystania z aplikacji i stron internetowych, tworzenia i zarządzania swoimi danymi i hasłami²³.

Do działań szkoły o charakterze pozaformalnym można również zaliczyć zajęcia z rodzicami, które będą bezpośrednio przekładać się na bezpieczeństwo ich dzieci w sieci. Warsztaty dla rodziców mogą mieć na celu dostarczenie wiedzy, umiejętności i narzędzi w zakresie wspierania bezpiecznego korzystania z technologii przez ich dzieci. Takie spotkania mogą mieć charakter spontaniczny, polegający na zwykłych rozmowach rodziców w gronie eksperta. Istotne jest, aby prowadziły do podejmowania wspólnej działalności rodzicielskiej w zakresie bezpieczeństwa ich dzieci w Internecie²⁴.

Dobłą inicjatywą podejmowaną jako forma edukacji pozaformalnej np. w domach kultury mogą być konkursy w zakresie bezpieczeństwa cyfrowego. Pozwoli to na uruchomienie aktywności poznawczej i jeszcze większej kreatywności ucznia, co może zaowocować lepszymi efek-

²¹ M. Adamska-Chudzińska, K. Blachnicka, *Mentoring w doświadczeniach polskich menedżerek*, „e-mentor”, 2023, nr 3, s. 32–42.

²² J. Bonar, *Czy szkoła jest miejscem twórczości rzeczywiście stymulowanej?* [w:] *Edukacja alternatywna w XXI wieku*, red. Z. Melosik, B. Śliwerski, Kraków 2010, s. 357–368.

²³ B. Radzka, J. Szaban, R. Trochimiuk, *Ocena efektywności szkoleń prowadzonych metodami tradycyjnymi i w formule edutainment*, „Edukacja Ekonomistów i Menedżerów”, 2019, nr 2, 109–119.

²⁴ M. Kędra, *Włączanie rodziców w edukację dzieci*, Warszawa 2019, s. 8.

tami ich prac. W ramach działań zadaniowych można zachęcać uczniów do tworzenia plakatów, filmów edukacyjnych, gier planszowych. Poprzez działalność artystyczną uczniowie mogą wyrażać zasady bezpieczeństwa, dlatego inicjatywy społeczne w zakresie prac plastycznych stanowią również duży potencjał w obszarze tworzenia bezpiecznego Internetu²⁵.

Wskazane propozycje działań bez wątpienia zwiększą potrzebną współczesnemu uczniowi świadomość bezpieczeństwa cyfrowego. Trudno stwierdzić, czy działania te będą skuteczne, ale bez wątpienia wdrożenie ich na szeroką skalę będzie stymulować nauczycieli uczniów szkół podstawowych, aby w ramach działań szkoły inicjować i podejmować współpracę z podmiotami zewnętrznymi i działać na rzecz ich wychowanków.

Zakończenie

Współczesne szkoły podstawowe, z uwagi na powszechny dostęp do technologii cyfrowych, stoją przed wyzwaniem związanym z koniecznością edukacji uczniów w zakresie bezpieczeństwa cyfrowego. W odpowiedzi na to wyzwanie edukacja pozaformalna staje się kluczowym środowiskiem wspierającym rozwój umiejętności związanych z bezpieczeństwem cyfrowym uczniów szkół podstawowych. Działania w ramach edukacji pozaformalnej mogą obejmować różnorodne formy, takie jak warsztaty, gry dydaktyczne, dyskusje grupowe czy symulacje wirtualne.

Programy edukacji pozaformalnej, wspierające bezpieczeństwo cyfrowe uczniów, obejmują różnorodne inicjatywy, takie jak cybermentoring, kluby bezpiecznego Internetu oraz praktyczne szkolenia z zakresu cyberbezpieczeństwa. Kluczowym elementem jest również zaangażowanie rodziców poprzez organizację warsztatów i spotkań, które pomagają w propagowaniu bezpiecznego korzystania z technologii wśród dzieci.

Wnioski te sugerują, że edukacja pozaformalna stanowi skuteczną i nowoczesną formę wsparcia dla szkół podstawowych w kształtowaniu bezpieczeństwa cyfrowego uczniów. Działania tych nie należy traktować jako zamiennika, lecz jako uzupełnienie edukacji formalnej, wnoszące praktyczne doświadczenia i umiejętności kluczowe w erze cyfrowej.

²⁵ A. Gielata, *Miejskie domy kultury jako instytucje kultury – miejsce w kulturze i gospodarce*, „Zeszyty Naukowe WSOWL”, 2012, nr 4, s. 187–191.

Bibliografia

- Adamska-Chudzińska M., Blachnicka K., *Mentoring w doświadczeniach polskich menedżerek*, „e-mentor”, 2023, nr 3.
- Badanie konsumenckie 2021 – dzieci, rodzice oraz nauczyciele, Urząd Komunikacji Elektronicznej, <https://www.uke.gov.pl>, 25.11.2023 (25.11.2023).
- Badanie RPD: Dzieci chcą, ale już nie potrafią oderwać się od mediów społecznościowych, Rzecznik Praw Dziecka, <https://brpd.gov.pl>, 14.01.2024 (14.01.2024).
- Bąk A., *Jak małe dzieci korzystają z urządzeń mobilnych? Raport na podstawie danych zebranych od rodziców*, „Dziecko Krzywdzone. Teoria, badania, praktyka”, 2015, vol. 14, no. 3.
- Bezpieczna szkoła. Zagrożenia i zalecane działania profilaktyczne w zakresie bezpieczeństwa fizycznego i cyfrowego uczniów, Warszawa 2017.
- Bonar J., *Czy szkoła jest miejscem twórczości rzeczywiście stymulowanej?* [w:] *Edukacja alternatywna w XXI wieku*, red. Z. Melosik, B. Śliwowski, Kraków 2010.
- Ciulkin-Sarnocińska K., *Phishing – specyficzna forma pozyskiwania danych newralgicznych* [w:] *Współczesne oblicza bezpieczeństwa*, red. E.M. Guzik-Makaruk, W. Pływaczewski, Białystok 2015.
- Craven S., Brown S., Gilchrist E., *Sexual grooming of children: Review of literature and theoretical considerations*, „Journal of Sexual Aggression”, 2006, nr 12.
- Financial Literacy in Poland: Relevance, evidence and provision*, OECD, <https://www.oecd.org>, 14.01.2024 (14.01.2024).
- Hinduja S., Patchin J.W., *Cyberbullying: An Update and Synthesis of the Research. Handbook of Bullying Prevention*, Springer 2018.
- Kamińska B., Olsza K., *Współczesne środki dydaktyczne i ich zastosowanie w działalności dydaktyczno-muzycznej szkolnictwa ogólnokształcącego*, „Muzyka – Historia – Teoria – Edukacja”, 2016, nr 6.
- Majchrzak K., *O edukacyjnych badaniach w działaniu w teorii i praktyce*, „Studia Dydaktyczne”, 2014, nr 26.
- Marciniak A., *Pozaformalne i nieformalne aspekty edukacji akademickiej*, „Ogrody Nauk i Sztuk”, 2013, nr 3.
- Murłowski D. [i in.], *Analiza oferty edukacyjnej formalnej i pozaformalnej oraz dostępnej oferty staży i praktyk i ich adekwatności do potrzeb pracodawców*, Warszawa 2020.
- Protasowicki I., *Phishing jako zagrożenie bezpieczeństwa osobistego w sieci*, „Zeszyty Naukowe Wyższej Szkoły Informatyki, Zarządzania i Administracji w Warszawie”, 2016, nr 14.
- Siemieniecka D., Skinińska M., Majewska K., *Cyberagresja – zjawisko, skutki, zapobieganie*, Toruń 2020.
- Ślawiński S. [i in.], *Słownik podstawowych terminów dotyczących krajowego systemu kwalifikacji*, Warszawa 2014.
- Smahel D. [i in.], *EU Kids Online 2020: Survey results from 19 countries*, EU Kids Online 2020.
- Stalończyk I., *Edukacja formalna i pozaformalna w procesie kształtowania społeczeństwa wiedzy*, „Nierówności Społeczne a Wzrost Gospodarczy”, 2014, nr 37.
- Stęchły W., *Edukacja formalna wobec edukacji pozaformalnej i uczenia się nieformalnego*, Warszawa 2021.

- Szłęk A., *Uczyć się inaczej – nowe kompendium wiedzy na temat edukacji pozaformalnej*, Warszawa 2013.
- Truskolaska E., *Grooming, czyli uwodzenie małoletnich przez internet – aspekty kryminologiczne oraz prawne*, „Prawo w Działaniu. Sprawy karne”, 2021, t. 47.
- Warchoł T., *Wybrane rodzaje aktywności uczniów szkoły podstawowej w edukacji pozaformalnej*, Rzeszów 2021.
- Wpływ pandemii na prywatne zajęcia edukacyjne dzieci i młodzieży*, Giganci programowania, <https://www.giganciprogramowania.edu.pl>, 14.01.2024 (14.01.2024).

The Role of Non-Formal Education in Shaping the Digital Safety of Primary School Students

Abstract

The article discusses issues related to the digital safety of primary school students in the context of threats arising from contemporary digital technologies. Nowadays, even younger students are increasingly exposed to risks associated with using the Internet. The current curriculum is packed with educational content, but finding space for effective education in the field of digital safety for students is crucial. The problem presented in the article suggests solutions in the form of non-formal education, as it is organized outside the formal education program. This allows students to consciously participate in the learning process and focuses on maximum activation, independence, and learning through practical action. Such an approach enables the implementation of various educational programs aimed at more effectively supporting the digital safety of primary school students. The article outlines major digital threats such as cyberbullying, inadvertent disclosure of personal data, addiction to electronic devices, phishing attacks, and unsafe online behaviors. The author also highlights the threats to students' mental and physical health in this regard. The article emphasizes the argument that non-formal education provides an ideal environment for addressing issues related to the digital safety of students. This is mainly because it is conducted outside of school by external entities, allowing for greater resources to be allocated to the use of the latest technologies. This enables the conduct of virtual simulations of online situations, educational games, and various discussion panels. The article concludes with a discussion of practical non-formal education programs supporting the digital safety of students. The author points out initiatives such as cyber-mentoring, safe Internet clubs, practical cybersecurity training, and workshops for parents. It is stressed that non-formal education is becoming increasingly popular and is supported by various social initiatives and government programs. The author argues that these programs are essential in a rapidly changing social and technological environment.

Keywords: digital safety, non-formal education, digital threats, primary school students