©Wydawnictwo UR 2019
ISSN 2080-9069
ISSN 2450-9221 online

„Edukacja – Technika – Informatyka" nr 1/27/2019
www.eti.rzeszow.pl
DOI: 10.15584/eti.2019.1.27

MARLENA LOREK[1], **ANDRZEJ PIECZYWOK**[2]

Rola edukacji dla bezpieczeństwa w kontekście zagrożeń cyberprzestępczością

The Role of Education for Security in the Context of Cybercrime Threats

[1] Doktor, Politechnika Rzeszowska, Wydział Zarządzania, Zakład Nauki o Bezpieczeństwie, Polska
[2] Doktor habilitowany profesor nadzwyczajny, Uniwersytet Kazimierza Wielkiego, Instytutu Techniki, Zakład Problemów Bezpieczeństwa i Ochrony Pracy, Polska

Streszczenie

W niniejszym artykule zaprezentowano wyzwania stojące przed edukacją dla bezpieczeństwa w dobie społeczeństwa informacyjnego i zagrożeń związanych z cyberprzestępczością. W związku ze zmianami technologicznymi, które zachodzą w szybko i gwałtownie zmieniającym się współczesnym społeczeństwie, pojawiają się nowe kategorie zagrożeń dla bezpieczeństwa współczesnego człowieka. W rezultacie skuteczna i efektywna edukacja dla bezpieczeństwa musi reagować na zmiany, które przejawiają się w postaci nowych zagrożeń.

Słowa kluczowe: bezpieczeństwo, edukacja dla bezpieczeństwa, społeczeństwo informacyjne, cyberprzestępczość

Abstract

This article presents the challenges facing education for security in the era of information society and threats related to cybercrime. Due to technological changes, new categories of threats to the security of modern man appear. As a result, effective and effective education for safety must respond to changes that are manifested in the form of new threats.

Keywords: security, education for security, information society, cybercrime

Wstęp

Za Suchodolskim należy przyjąć, że podstawową dewizą życia i edukacji jest hasło: „Rozumieć świat – kierować sobą". W rezultacie podejmowanej od najmłodszych lat edukacji młodzi ludzie powinni nabyć umiejętność rozpoznawania współczesności, zachodzących w niej zjawisk i procesów, a także występujących uwarunkowań. Przed współczesnymi instytucjami szeroko ro-

zumianej edukacji stoi zadanie zbudowania społeczeństwa informacyjnego, które funkcjonuje w sieci różnego rodzaju zależności i powiązań, zaawansowanych technologii.

Jedną z ważnych sfer współczesnego życia jest bezpieczeństwo pojmowane zupełnie inaczej niż kiedyś. Doszły nowe dziedziny życia, które stają się celem ataków. Edukacja dla bezpieczeństwa musi znaleźć odpowiedź na pojawiające się wyzwania. Jednym z takich wyzwań jest cyberprzestępczość.

W niniejszym artykule zostaną zaprezentowane oczekiwania dotyczące skutecznej edukacji dla bezpieczeństwa.

Cyberprzestępczość jako nowe wyzwanie w sferze bezpieczeństwa

Społeczeństwo informacyjne żyje jakby w dwóch równoległych światach – realnym i wirtualnym. Od pewnego czasu obserwuje się zjawisko przenoszenia w świat wirtualny niepożądanych zjawisk ze świata realnego. Nowym zagrożeniem jest cyberprzestępczość. Rozwija się ona w cyberprzestrzeni. Pojęcie *cyberprzestrzeń* wywodzi się z dwóch słów:

– *cyber* – słowo to wiąże się z nowymi, elektronicznymi technologiami, jest używane w znaczeniu informatycznym (interaktywnym) i oznacza wszystko, co dotyczy komputerów,

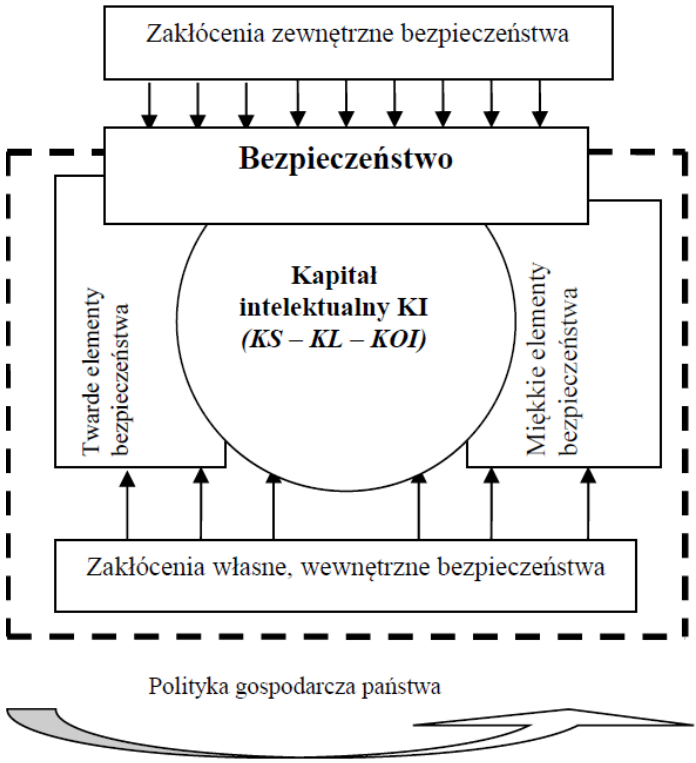
– *space* – przestrzeń.

Madej (2005, s. 489) zwraca uwagę na to, że obecnie odchodzi się od pojmowania bezpieczeństwa jako dotyczącego wyłącznie sfery militarnej, ewentualnie uzupełnionej o pewne aspekty ekonomiczne. Podkreśla on dalej, że jest to rezultatem „uznania za treść bezpieczeństwa obok przetrwania państwa jako jednostki geopolitycznej i utrzymania przez nie integralności terytorialnej takich elementów jak szeroko rozumiana jakość życia jego ludności, jej dobrobyt, zachowanie specyficznej tożsamości czy pewność szans dalszego rozwój. W efekcie wyróżnia się dziś – oprócz «twardego bezpieczeństwa» obejmującego sferę wojskową (a w pewnym stopniu sferę ekonomiczną) – także jego «miękki wymiar» uwzględniający wiele innych, często niejednoznacznie rozgraniczonych, nakładających się aspektów tego zagadnienia: kulturowy (społeczny), ekologiczny, technologiczny, humanistyczny czy demograficzny".

Ponieważ współczesny świat oparty jest na informacji, strategicznego znaczenia zaczyna nabierać kapitał intelektualny, który akumulowany jest w trakcie całożyciowego procesu uczenia się.

Stam i Bontis stwierdzają: „Kapitał intelektualny kraju to nieobserwowalny zasób wszystkich podmiotów funkcjonujących na jego terytorium, tj. mieszkańców, jednostek gospodarczych, instytucji i organizacji, a także społeczności i jednostek administracyjnych, który jest źródłem generowania aktualnego rozwoju zarówno ekonomicznego, jak i społecznego, oraz źródłem dobrobytu społecznego i wzrostu społecznego w przyszłości. Zasób ten wyznacza składniki materialne i niematerialne" (Andriessen, Stam, 2004; Bontis, 2004, s. 13–39).

Kapitał intelektualny należy postrzegać jako zasadniczy czynnik spajający twarde i miękkie elementy bezpieczeństwa, jak pokazano na rysunku 1.



Legenda:
KI – kapitał intelektualny
KS – kapitał społeczny
KL – kapitał ludzki
KOI – kapitał organizacyjno-innowacyjny

Rysunek 1. Kapitał intelektualny łączący twarde i miękkie podstawy bezpieczeństwa

Źródło: Jaruszewski (2012), s. 68.

Kapitał intelektualny tworzą obywatele danej społeczności, w tym uczniowie i studenci, którzy zdobywając wiedzę, budują przyszłą przewagę konkurencyjną na rynku informacji i wiedzy, które jako bogactwo muszą być odpowiednio chronione.

Termin *bezpieczeństwo na zewnątrz* precyzuje ochronę przed *zagrożeniami dla środowiska,* w tym dla człowieka, w którym pracuje system komputerowy. Zagrożenia te są najczęściej spowodowane nieprawidłowym działaniem tego systemu. Dotyczy to przede wszystkim tzw. przemysłowych systemów sterowa-

nia, np. monitorujących stan pacjenta w szpitalu, sterujących robotami na zautomatyzowanej taśmie produkcyjnej, nadzorujących ruch kolejowy.

Natomiast termin *bezpieczeństwo do wewnątrz* precyzuje ochronę przed *zagrożeniami dla informacji* przechowywanej, przetwarzanej oraz przesyłanej w sieci lub systemie teleinformatycznym. Odnosi się to przede wszystkim do sieci teleinformatycznych biur, banków, organizacji naukowych itd. To rozróżnienie znajduje swoje odbicie w praktyce nie tylko w różnych unormowaniach, ale też w strukturze cyklu życia systemów oraz sposobie ich wytwarzania oraz utrzymywania (Kisielnicki, Letkiewicz, Rajchel, Ura, 2010, s. 93).

Cyberprzestępczość ma różne oblicza:

– blokowanie atakowanego systemu (DoS),
– korzystanie z oprogramowania umożliwiającego wejście do serwerów omijając zabezpieczenia (*back door*),
– podszywanie się pod innego nadawcę (*spoofing*),
– podszywanie się pod inny komputer (IP spoofing),
– przechwytywanie haseł i loginów, „podsłuchiwanie sieci" (*sniffing*),
– skanowanie w celu poznania rodzaju zabezpieczeń oraz konfiguracji atakowanego systemu,
– wirusy, robaki komputerowe oraz bomby logiczne,
– włamania do komputerów (*hacking*),
– włamania do komputerów w celu uzyskania korzyści (*cracking*),
– wykorzystywanie istniejących błędów w systemie operacyjnym (*exploity*),
– wyłudzanie poufnych informacji (*phishing*).

Katalog ten nie jest zamknięty, ponieważ bardzo szybko tworzą się nowe typy zagrożeń w społeczeństwie informacyjnym.

Rysunek 2. Cechy współczesnego terroryzmu ponowoczesnego

Źródło: Marcinkowski (2012), s. 182.

Szczególne miejsce w zakresie cyberprzestępczości zajmuje cyberterroryzm (Aleksandrowicz, 2008, s. 35–36), który jest działaniem bardzo agresywnym i asymetrycznym. Charakteryzuje się zastraszaniem społeczności internetowej nowymi formami zagrożeń, np.:

– atakami hakerów na bazy wojskowe, policyjne, służb państwowych, na banki czy urzędy administracji publicznej itp.,

– sparaliżowaniem systemów komputerowych (np. sterującego zaopatrzeniem miasta w wodę, energię elektryczną).

Na rysunku 2 przedstawiono zgeneralizowane cechy charakterystyczne współczesnego terroryzmu ponowoczesnego. Ma on wyraźne cechy koherencji, a swoimi korzeniami sięga procesów globalizacyjnych w gospodarce światowej.

Współczesny człowiek musi być przygotowany na to, by poradzić sobie z tymi nakreślonymi wyżej zagrożeniami, ale także kolejnymi, które na pewno się pojawią. Ważne miejsce w walce z niepożądanymi zachowaniami i zjawiskami w sieci spełnia edukacja dla bezpieczeństwa.

Edukacja dla bezpieczeństwa jako element walki z cyberprzestępczością

We współczesnym świecie bezpieczeństwo bez wątpienia stało się wartością, której znaczenie docenia większa część społeczeństwa.

W świetle informacji zawartych w poprzedniej części artykułu można wskazać następujące podstawowe skutki będące wynikiem braku bezpieczeństwa w cyberprzestrzeni:

– kradzież danych,
– ujawnienie danych poufnych,
– utratę danych,
– włamanie do systemu informatycznego,
– zablokowanie dostępu do usług,
– zafałszowanie informacji.

Te zagrożenia mogę dotknąć każdego człowieka. Edukacja dla bezpieczeństwa musi uwzględniać pojawianie się nowych zagrożeń i uczyć, jak zachować się wobec nich. Ważna jest więc edukację dla bezpieczeństwa publicznego jako ogół oddziaływań oświatowo-wychowawczych zmierzających do kształtowania świadomości prawnej społeczeństwa oraz postaw i zachowań w sytuacjach zagrażających obywatelom i porządkowi publicznemu, ale też edukacja dla bezpieczeństwa działalności w sieci. Edukacja taka ma zatem ścisły związek z przygotowaniem społeczeństwa do właściwych zachowań w sytuacji zagrożenia.

Stępień (1994, s. 11) definiuje edukację dla bezpieczeństwa jako „określony system dydaktyczno-wychowawczej działalności rodziny, szkoły, wojska, środków masowego przekazu, organizacji młodzieżowych i stowarzyszeń, zakładów pracy oraz instytucji państwowych i samorządowych ukierunkowanej na upowszechnienie systemu wartości, upowszechnienie wartości i kształtowanie umiejętności ważnych dla zapewnienia bezpieczeństwa narodowego”.

Młodzi ludzie muszą uzyskać informacje na temat zagrożeń czyhających w sieci i sposobów uchronienia się przed nimi. W związku z tym musi w swoich programach zawierać problematykę szeroko rozumianego bezpieczeństwa informacyjnego, która to wiedza będzie wciąż aktualizowana.

„Droga do lepszego poznania i rozumienia świata wiedzie właśnie przez edukacje, oparta jednak na nowym paradygmacie – poznania sposobów i możliwości zdobywania wiedzy niezbędnej do dobrego funkcjonowania w zmiennej i napiętnowanej ryzykiem rzeczywistości" (Pieczywok, 2012, s. 9–10).

Za Rudnickim (1994, s. 63) można wyróżnić też różne dziedziny edukacji w tym zakresie:

– edukację dla bezpieczeństwa ekologicznego – oddziaływania oświatowo-wychowawcze ukierunkowane na kształtowanie harmonijnego współżycia ludzi z przyroda oraz postaw i zachowań w sytuacji zagrożeń ekologicznych,

– edukację dla bezpieczeństwa gospodarczego – oddziaływania oświatowo-wychowawcze ukierunkowane na kształtowanie świadomości ekonomicznej społeczeństwa,

– edukację dla bezpieczeństwa militarnego – ogół oddziaływań obejmujących kształcenie i wychowanie obronne społeczeństwa, ukierunkowanych na zachowanie niepodległości narodu i państwa oraz ochronę życia i zdrowia ludzi w stanach zagrożenia wojennego i wojny,

– edukację dla bezpieczeństwa politycznego – oddziaływania oświatowo-wychowawcze ukierunkowane na kształtowanie kultury politycznej oraz postaw wobec zagrożeń politycznych,

– edukację dla bezpieczeństwa psychospołecznego – oddziaływania oświatowo-wychowawcze ukierunkowane na kształtowanie moralności społeczeństwa oraz postaw wobec zagrożeń psychospołecznych,

– edukację dla bezpieczeństwa publicznego – oddziaływania oświatowo-wychowawcze ukierunkowane na kształtowanie świadomości prawnej i postaw w sytuacji zagrożenia obywateli i porządku publicznego,

Istotny elementem edukacji dla bezpieczeństwa jest propagowanie idei współodpowiedzialności za kwestie bezpieczeństwa. Współcześni ludzie muszą mieć przekonanie, że zapewnienie bezpieczeństwa nie jest tylko obowiązkiem państwa, administracji rządowej czy samorządowej, ale także każdego pojedynczego obywatela. Bez wcielenia w życie tej zasadniczej idei nie będzie można mówić o skutecznym systemie bezpieczeństwa.

Podsumowanie

Ochrona bezpieczeństwa i porządku publicznego jest jednym z najważniejszych i mających najstarszą tradycję zadań publicznych. Współcześnie jednak bez odpowiedniego wsparcia ze strony społeczeństwa wszelkie działania wydają się niewystarczające.

Ważne jest włączenie w system ogniw ochrony bezpieczeństwa szeregowych obywateli. Ne jest to kwestia zrzucenia na ich barki zadań przynależnych administracji, ale wzmocnienie frontu działań w walce z zagrożeniami.

W programach edukacji dla bezpieczeństwa muszą zostać uwzględnione nowe wyzwania w sferze bezpieczeństwa związane z cyberprzestrzenią i cyberprzestępczością. Szybkie reagowanie na nowe zagrożenia pozwoli na zachowanie poczucia bezpieczeństwa na satysfakcjonującym jednostkę poziomie.

Aktualizacja katalogu zagrożeń, w tym tych związanych z cyberprzestępczością, oraz opracowywanie skutecznych środków przeciwdziałania im i ochrony przed nimi pozwoli na minimalizację strat i zwiększy poziom bezpieczeństwa.

„Priorytetowym efektem kształcenia nie jest zdobycie wiedzy, lecz umiejętności i kompetencji społecznych umożliwiających podjęcie właściwych reakcji na symptomy zagrożenia i umiejętne wsparcie lub organizacja działań niwelujących konsekwencje ich wystąpienia czy oddziaływania" (Mickiewicz, 2015, s. 144).

Literatura

Aleksandrowicz, T. (2008). *Terroryzm międzynarodowy*. Warszawa: Wyd. Akademickie i Profesjonalne.

Andriessen, D.G., Stam, Ch.D. (2004). *Measuring the Lisbon Agenda. The Intellectual Capital of the European Union*. Center for Research in Intellectual Capital.

Bontis, N. (2004). National Intellectual Capital Index. A United Nations Initiative for the Arab Region. *Journal of Intellectual Capital, 5*(1), 13–39.

Jaruszewski, W.K. (2012). *Kapitał intelektualny jako cel ataków terrorystycznych na świecie*. W: T. Bąk (red.), *Przeciwdziałanie zagrożeniom terrorystycznym podczas imprez masowych w aspekcie EURO 2012* (s. 65–84). Kraków–Rzeszów–Zamość: Konsorcjum.

Kisielnicki, J., Letkiewicz, A., Rajchel, K., Ura, E. (2010). *Zarządzanie kryzysowe w administracji publicznej*. Warszawa: Wyd. WSIZiA-WSPwS.

Madej, M. (2005). *Terroryzm i inne zagrożenia asymetryczne w świetle współczesnego pojmowania bezpieczeństwa narodowego i międzynarodowego – próba teoretycznej konceptualizacji*. W: R. Kuźniar (red.), *Porządek międzynarodowy u progu XXI wieku. Wizje – koncepcje – paradygmaty* (497-517). Warszawa: Wyd. UW.

Marcinkowski, C. (2012). Bezpieczeństwo transgraniczne a globalizacja i potencjalna koherencja zagrożeń terrorystycznych w aspekcie EURO 2012. W: T. Bąk (red.), *Przeciwdziałanie zagrożeniom terrorystycznym podczas imprez masowych w aspekcie EURO 2012* (s. 175–184). Kraków–Rzeszów–Zamość: Konsorcjum.

Mickiewicz, P. (2014). Ewolucja pojęcia „bezpieczeństwo państwa" w polskich dokumentach strategicznych jako determinanta zmian programu kształcenia przedmiotu edukacja dla bezpieczeństwa. W: B. Wiśniewska-Paz (red.), *Socjologia LXIV. Edukacja a bezpieczeństwo w różnych wymiarach i kontekstach. Formacje militarne i paramilitarne wobec wyzwań edukacyjnych* (s. 143–154). Wrocław: Wyd. UW.

Pieczywok, A. (2012). *Edukacja dla bezpieczeństwa wobec zagrożeń i wyzwań współczesności*. Warszawa: Wyd. AON.

Rudnicki, B. (1994). Edukacja dla bezpieczeństwa i jej interpretacja. W: R. Stępień (red.), *Edukacja dla bezpieczeństwa, materiały z konferencji naukowej 23–24 maja 1994 r*. Warszawa: Wyd. AON.

Stępień, R. (red.) (1998). *Koncepcje i kierunki przemian edukacji dla bezpieczeństwa*. Warszawa: Wyd. AON.