

Nowoczesne Systemy Zarządzania
Zeszyt 19 (2024), nr 1 (styczeń-marzec)
ISSN 1896-9380, s. 39-54
DOI: 10.37055/nasz/192813

Modern Management Systems
Volume 19 (2024), No. 1 (January-March)
ISSN 1896-9380, pp. 39-54
DOI: 10.37055/nasz/192813



Instytut Organizacji i Zarządzania
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna
w Warszawie

Institute of Organization and Management
Faculty of Security, Logistics and Management
Military University of Technology
in Warsaw

Poczucie bezpieczeństwa informacyjnego w świecie VUCA

A sense of information security in the VUCA world

Katarzyna Hilaria Batorowska

Uniwersytet w Siedlcach
kasia.hilaria@onet.pl; ORCID: 0000-0002-9707-5804

Abstrakt. Świat VUCA cechuje się zmiennością, niepewnością, złożonością i niejednoznacznością czynników zewnętrznych, które wpływają na jednostkę oraz całe społeczeństwa. W świecie tym człowiek narażony jest wciąż na nowe niebezpieczeństwa, które ze względu na zmienność warunków musi umieć dostrzec, zdefiniować i przygotować się do konfrontacji z nimi. Efemeryczność takiej egzystencji przekłada się na brak poczucia bezpieczeństwa, czyli osiągnięcie stanu, w którym podmiot nie odczuwa zagrożeń będących konsekwencją korzystania z informacji niespełniającej norm jakościowych oraz z utraty całości lub części swoich aktywów informacyjnych. Świat VUCA jest efektem procesów globalizacyjnych, rozwoju technologicznego, a także zderzenia cywilizacji i przenikania się kultur. Powstała pod wpływem tych czynników płynność i zmienność środowiska zmusza człowieka do poszukiwania nowych metod zarządzania bezpieczeństwem i ryzykiem, dostosowywanych do aktualnych potrzeb. Świat VUCA wymaga zmiany potrzeb informacyjnych i zachowań informacyjnych, które wynikają ze wzrastającego poziomu świadomości informacyjnej oraz potrzeby poczucia bezpieczeństwa. Stanowi to wyzwanie dla władz i środowiska edukacyjnego poszukującego odpowiedzi na pytanie, jak kształtować aktywne podmioty bezpieczeństwa na potrzeby kraju, świadome współczesnych wyzwań i zagrożeń. W artykule omówiono czynnik odpowiedzialny za uwrażliwienie jednostki na zagrożenia generowane przez świat VUCA, a jest nim edukacja dla bezpieczeństwa informacyjnego. Celem opracowania była identyfikacja metod wdrażania programu edukacji dla bezpieczeństwa informacyjnego oraz skuteczność tej edukacji przekładająca się na uodpornienie edukowanych na zagrożenia związane z konsekwencjami stresu informacyjnego, nadprodukcji informacji, nieradzenia sobie z ryzykiem, niepewnością, nieumiejętnością zarządzania informacją, niewystarczającymi kompetencjami cyfrowymi, a więc na te zagrożenia, które utrudniają jednostce zapanowanie nad zmiennością, niepewnością, złożonością i niejednoznacznością. W artykule wykorzystano metodę jakościową i analizę zawartości treści programów edukacji dla bezpieczeństwa informacyjnego. Postawiono problem badawczy: czy program edukacji dla bezpieczeństwa informacyjnego skutecznie kształtuje odporność ludzi na zagrożenia informacyjne? Sformułowano też hipotezę badawczą: kierowane do młodzieży programy

edukacji dla bezpieczeństwa informacyjnego nie kształtują w sposób wystarczający ich odporności w patogennym środowisku informacyjnym. Przeprowadzone badania ukazały obszary w programach edukacji dla bezpieczeństwa informacyjnego wymagające uzupełnienia oraz potrzebę zmian w procesie ich wdrażania. Płynność świata VUCA wymaga kształtowania umiejętności nie tylko technicznych, lecz także społecznych, emocjonalnych oraz informacyjnych. Uznano, że rola nauczyciela, pedagoga i psychologa szkolnego jest kluczowa w kształtowaniu kultury bezpieczeństwa informacyjnego jednostki i że poziom tej kultury przekłada się na obiektywne odczuwanie przez nią poczucia bezpieczeństwa informacyjnego, a więc radzenia sobie z zagrożeniami, jakie niesie ze sobą świat VUCA.

Słowa kluczowe: poczucie bezpieczeństwa informacyjnego, świat VUCA, środowisko bezpieczeństwa informacyjnego, decydent lokalny, podatność i odporność społeczeństwa na zagrożenia

Abstract. The VUCA world is characterized by variability, uncertainty, complexity and ambiguity of external factors that affect individuals and entire societies. In this world, man is constantly exposed to new dangers, which, due to the changeability of conditions, he must be able to perceive, define and prepare to confront them. The ephemerality of such an existence translates into a lack of sense of security, i.e. achieving a state in which the entity does not feel threats resulting from the use of information that does not meet quality standards and from the loss of all or part of its information assets. The VUCA world is a consequence of globalization processes, technological development, as well as the clash of civilizations and the interpenetration of cultures. The fluidity and variability of the environment resulting from these factors forces people to look for new methods of security and risk management, adapted to current needs. The VUCA world requires a change in information needs and information behaviors resulting from the increasing level of information awareness and the need to feel safe. This is a challenge for the authorities and the educational community looking for answers on how to shape active security entities for the country's needs, aware of contemporary challenges and threats. The article discusses the factor responsible for sensitizing an individual to the threats generated by the VUCA world, which is education for information security. The aim of the article was to identify methods of implementing an education program for information security and the effectiveness of this education, which translates into immunizing educated people against the threats related to the consequences of information stress, information overproduction, failure to cope with risk, uncertainty, inability to manage information, insufficient digital competences, and therefore to those threats that make it difficult for an individual to cope with variability, uncertainty, complexity and ambiguity. The article uses a qualitative method, content analysis of information security education programs. The article poses a research problem: does the information security education program effectively shape people's resistance to information threats? A research hypothesis was also formulated: information security education programs dedicated to young people do not sufficiently shape their resilience in a pathogenic information environment. The conducted research revealed areas in information security education programs that require supplementation and the need for changes in the process of their implementation. The fluidity of the VUCA world requires developing not only technical but also social, emotional and information skills. It was recognized that the role of a teacher, pedagogue and school psychologist is crucial in shaping the information security culture of an individual and that the level of this culture translates into the individual's objective sense of information security, and thus coping with the threats posed by the VUCA world.

Keywords: sense of information security, VUCA world, information security environment, local decision-maker, society's vulnerability and resistance to threats

Wprowadzenie

Rozwój technologii informacyjno-komunikacyjnych zapewnił człowiekowi dostęp do zróżnicowanych źródeł informacji, umożliwiając mu tworzenie własnych opinii, pozwalając na podstawie tych danych formułować obiektywne sądy i ułatwiając podejmowanie racjonalnych decyzji. W czasach powszechnego dostępu do

kultury kontaktu i jej dominacji imperatyw dzielenia się wiedzą i informacjami, podejmowania współpracy nie tylko sprzyja rozwojowi, lecz także umożliwia podnoszenie świadomości i uważności na potencjalne zagrożenia mające miejsce w globalnym świecie. Wynikają one z zacierania się granic, kultur i światopoglądów reprezentowanych przez poszczególne grupy użytkowników informacji, co wiąże się z kwestiami, takimi jak poufność danych, rozprzestrzenianie się treści o tematyce polityczno-ideologicznej czy odrębne wzory kulturowo-religijne. Wyzwaniem dla świata staje się zapewnienie integralności społeczeństw, ich humanizacja, propagowanie postaw tolerancji i współżycia narodów. Zagrożeniem jest mowa nienawiści, dyskryminacja, postawy wrogie i agresywne względem zarówno poszczególnych jednostek, jak i całych narodów (Wódka, 2016, s. 159-160).

Nowe technologie informacyjno-komunikacyjne umożliwiają nawiązywanie współpracy (partnerstwa) w różnych obszarach aktywności człowieka. Równocześnie sprzyjają one rozprzestrzenianiu się różnych ideologii i teorii inicjujących zmiany społeczne, polityczne czy gospodarcze, powstawaniu grup przestępczych (np. cyberterrorystów) oraz dążeniu do dominacji informacyjnej z użyciem różnych narzędzi walki informacyjnej, takich jak dezinformacja i manipulacja medialna. Infoagresor może przez dobór informacji, sposób ich przedstawienia, interpretacji komunikatów i architekturę informacji wpływać na kształtowanie opinii i nastrojów społecznych. Odbiór komunikatu wiąże się z selekcją, analizą dostępnych informacji oraz interpretacją tekstu przez skojarzenia, odniesienia czy wiedzę zastałą. Nadawca informacji, wywołując reakcję emocjonalną na komunikat, wpływa na sposób interpretacji tekstu, realizm treści, poczucie łączności z postaciami oraz odbiór przesłań perswazyjnych i zmianę nastrojów czy aktywności odbiorcy (Michalczyk, 2017, s. 11-12). Odbiór komunikatu ma charakter psychiczny, emocjonalny, dlatego też proces komunikacji powinien być traktowany w sensie psychicznym związanym z refleksyjnością, symbolizmem i intencjonalnością. W świecie VUCA, który charakteryzuje się zmiennością, a także niejednoznacznością wynikającą z trudności rozumienia rzeczywistości, z interpretacji błędów poznawczych i intencjonalności nadawców informacji z jednoczesną nadmiarowością informacji i wielością źródeł informacji, odbiorca komunikatu stoi przed zadaniem dokonania jego natychmiastowej analizy i krytycznej oceny, odrzucenia informacji nadmiarowej i rezygnacji z emocjonalnej reakcji. Brak oparcia na stałych zasadach, których w świecie VUCA nie ma, bo wszystko w nim jest płynne, wciąż się dezaktualizuje, zanim zdąży przybrać konkretną formę, powoduje dysonans poznawczy człowieka oraz podatność na różnego rodzaju manipulacje poglądami i ideami (Bennett, Lemoine, 2014, s. 6). Działania manipulacyjne, którym ulega człowiek, mogą być niezamierzone lub celowo wywołane przez agresora dla celów osobistych, politycznych, gospodarczych i innych. Nadmiar informacji i ograniczenia biologiczne człowieka związane z jego percepcją ułatwiają infoagresorom manipulowanie swoimi ofiarami. Pozyskują ich aprobatę, wsparcie, zakorzeniają postawy bierności lub wrogości wykorzystywane

przeciwko obranym obiektom (Bodenhausen, Perry, 2009, s. 1-3). Jeżeli odbiorca informacji nie posiada kompetencji emocjonalnych, w tym samokontroli, umiejętności nazwania emocji i nie zna konsekwencji, jakie te stany emocjonalne mogą wywołać, równocześnie nie posiada wystarczających kompetencji informacyjnych pozwalających na analizę i krytyczną ocenę, obiektywizm, odrzucenie emocjonalnych zakłamań, stanowi potencjalny przedmiot działań manipulacyjnych i narzędzie wykorzystywane w walce informacyjnej (Matczak, Knopp, 2013, s. 139).

Akronim VUCA, który został po raz pierwszy wprowadzony w 1985 roku, oznacza: V – *volatility* (zmienny), U – *uncertainty* (niepewny), C – *complexity* (złożony), A – *ambiguity* (niejednoznaczny). Świat VUCA to taki, który musi radzić sobie z permanentnymi zmianami i niepewnościami. Nawiązuje to zmienności tempa rozwoju technologicznego, zmian rynku i jego potrzeb (w tym zmienności potrzeb kompetencji i umiejętności wymaganych od użytkownika informacji) (Musiał, 2021, s. 69-70).

Zagrożenia w świecie VUCA generują również niepewność, brak przewidywalności, prawdopodobieństwo wystąpienia pewnych zdarzeń oraz brak zrozumienia i świadomości problemów i wydarzeń. Aby temu zapobiec, człowiek musi mieć wiedzę o świecie potrzebną do zrozumienia emitowanych treści. Niestety wiedza w zmiennym świecie VUCA jest niepełna, fragmentaryczna, niedoskonała i wciąż się dezaktualizuje. Nadprodukcja informacji zmusza do ciągłej selekcji źródeł, do tworzenia nowych kryteriów podziału i doboru komunikatów, wymaga od naszego umysłu wybiórczości, porządkowania, klasyfikowania, odrzucania i ponownego zestawiania. A to wymaga nieustannej aktywności intelektualnej i ciągłego poszerzania swojej wiedzy o świecie. Dlatego wyzwaniem dla współczesnego człowieka jest permanentna edukacja. Za wyrobienie nawyku kształcenia się przez całe życie odpowiedzialny jest rząd, system edukacji i oświaty oraz różne instytucje wspierające. Łączy się to z kwestią obowiązkowej edukacji medialnej, informacyjnej i technologicznej (cyfrowej) oraz z kształtowaniem kompetencji w tym zakresie, a przede wszystkim kultury informacyjnej i medialnej dającej człowiekowi poczucie przynależności do społeczeństwa informacyjnego i możliwość korzystania z jego dobrodziejstw. Szczególne znaczenie w świecie VUCA można przypisać edukacji medialnej (np. edukacji medialnej 3.0) propagującej etykę wśród dysponentów mediów, w tym etykę dziennikarską, oraz wśród wszystkich twórców i nadawców informacji. Mogą oni w sposób zaplanowany wpływać na zmiany nastrojów społecznych, wzniecać poczucie lęku lub niepokoju, przyczyniając się tym samym do zmiany postrzegania rzeczywistości przez indagowany podmiot i niedostrzegania przez niego stanu zagrożenia (Tołwiński, 2016, s. 149-157).

Kwestia subiektywizmu i obiektywizmu w postrzeganiu i odczuwaniu bezpieczeństwa informacyjnego była rozważana m.in. przez Daniela Freia. Zaproponowany przez niego podział na stan bezpieczeństwa, stan braku bezpieczeństwa i na stan patologii urzeczywistnia sposób postrzegania i identyfikacji zagrożeń wyrażający

się w zachowaniach jednostki doświadczającej takiego stanu. W przypadku stanu braku bezpieczeństwa jednostka prawidłowo identyfikuje zagrożenia zewnętrzne i podejmuje kroki w celu przeciwdziałania nim. W sytuacji stanu bezpieczeństwa zaś jednostka nie identyfikuje żadnych zagrożeń (adekwatnie do rzeczywistości). Z kolei w razie zaistnienia patologii, w tym stanu obsesji, jednostka identyfikuje zagrożenia nieadekwatnie do stanu rzeczywistego, a jej zachowanie jest niewspółmierne do tej sytuacji. Przykładem może być mowa nienawiści lub panika moralna. W stanie fałszywego bezpieczeństwa jednostka identyfikuje zagrożenia zewnętrzne, ale nie podejmuje działań (postawa bierna, zrzeczenie się odpowiedzialności). Poczucie bezpieczeństwa informacyjnego jest więc w dużym stopniu zależne od posiadanych informacji i zdolności do ich interpretacji (Grzebiela, 2018, s. 90-91).

Poczucie bezpieczeństwa informacyjnego w świecie VUCA zależy od umiejętności informacyjnych w zakresie wyszukiwania i pozyskiwania informacji (sprawności techniczne) oraz w zakresie interpretacji informacji, w tym identyfikacji przekazów perswazyjnych i dekodowania intencji nadawców informacji, a także umiejętności obiektywnego (nieopartego na emocjach) osądu treści. Wyzwanie to leży po stronie instytucji odpowiedzialnych za program edukacji dla bezpieczeństwa informacyjnego oraz jego promocji. Wychowanie dojrzałych informacyjnie obywateli wymaga współpracy instytucji edukacyjnych z instytucjami publicznymi, w tym instytucji porządku publicznego (np. policji, wojska, straży pożarnej) odpowiedzialnych za zarządzanie informacją w sytuacjach kryzysowych.

Synergia wynikająca ze współpracy instytucji publicznych, edukacyjnych i porządku publicznego na rzecz realizacji projektów edukacji dla bezpieczeństwa informacyjnego powinna przejawiać się lepszym opanowaniem technik zarządzania informacją i musi dotyczyć wszystkich płaszczyzn (cyfrowa, tradycyjna, społeczna, zawodowa, personalna), na które świat VUCA oddziałuje, a w których jednostka funkcjonuje. Poczucie bezpieczeństwa informacyjnego może być różne w zależności od płaszczyzny, w jakiej użytkownik się porusza. Władze dzięki promowaniu kultury bezpieczeństwa informacyjnego w społeczeństwie mają możliwość kształtowania poczucia tego bezpieczeństwa lub jego braku w tych obszarach.

Środowisko bezpieczeństwa informacyjnego jest wielopłaszczyznowe i obejmuje sferę materialną, prawno-organizacyjną i niematerialną (psychiczną, duchową). Świadomość uzyskania wsparcia od władz w obszarze ochrony własnych zasobów informacyjnych, zachowania prywatności, tożsamości i gwarancji dostępu do informacji publicznej itp. stanowi podstawę kształtowania poczucia bezpieczeństwa obywateli.

Celem opracowania jest identyfikacja metod wdrażania programu edukacji dla bezpieczeństwa informacyjnego oraz skuteczność tej edukacji w obszarze uwrażliwienia i uodpornienia podmiotu edukacji na zagrożenia generowane przez współczesne środowisko informacyjne utrudniające jednostce racjonalne funkcjonowanie w świecie VUCA. Na potrzeby artykułu sformułowano następującą hipotezę: edukacja

dla bezpieczeństwa informacyjnego nie kształtuje wystarczającej odporności podmiotu na zagrożenia w obszarze bezpieczeństwa informacyjnego i niezadowolająco wzmacnia jego obiektywne poczucie bezpieczeństwa informacyjnego.

Uzyskanie odpowiedzi na postawiony problem badawczy jest wynikiem analizy literatury przedmiotu na temat poczucia bezpieczeństwa informacyjnego w strukturach lokalnych oraz analizy rozumienia pojęcia „bezpieczeństwo informacyjne”, bo ono determinuje rozumienie terminu „poczucie bezpieczeństwa informacyjnego”. Rozpatrywanie tego problemu pod kątem nowych zagrożeń typowych dla świata VUCA jest próbą skonkretyzowania potrzeb edukacyjnych pozwalających podmiotowi nie tylko przetrwać w tym środowisku, lecz również rozwijać się w nim.

Bezpieczeństwo informacyjne jest łączone w literaturze przedmiotu z pojęciem bezpieczeństwa informatycznego czy bezpieczeństwa informatyzacji. Krzysztof Liedel traktuje bezpieczeństwo informacyjne jako uprawnienie polityki gwarantującej państwu i podmiotom, które chroni, istnienie, przetrwanie i swobodny rozwój (Batorowska, 2021, s. 337). Najczęściej w definicjach bezpieczeństwa informacyjnego uwaga skoncentrowana jest na zbiorze działań na rzecz zabezpieczania, gromadzenia, przetwarzania zasobów informacyjnych, ochrony infrastruktury informacyjnej w celu zapewnienia integralności, poufności przed niepożądanym, nieuprawnionym ujawnieniem, modyfikacją czy zniszczeniem (Alkowski, 2015, s. 88). Autor tekstu przyjmuje definicję bezpieczeństwa informacyjnego, sformułowaną przez Elżbietę Urę i Stanisława Pieprznego, w której bezpieczeństwo informacyjne jest zmienne i jest związane ze źródłem zagrożeń celem ochrony oraz rodzajem zasobów będących chronionymi (Ura, Pieprzny, 2014, s. 18-20). Obejmuje ona kwestie, takie jak intencjonalność, zmienność zasobów i okoliczności ich zabezpieczania. Bezpieczeństwo informacyjne w literaturze z zakresu nauk o bezpieczeństwie rzadko ukazywane jest w sposób interdyscyplinarny, np. z perspektywy psychologii, socjologii czy kulturoznawstwa. W świecie VUCA, w którym zmienność jest podstawowym wyznacznikiem, konieczne jest rozpatrywanie tej kwestii w ujęciu szerszym.

Program edukacji dla bezpieczeństwa informacyjnego powinien być odzworowaniem wskazanej powyżej definicji bezpieczeństwa informacyjnego i powinien wynikać z założenia o zmienności źródeł zagrożenia, celów i podmiotów chronienia. Metody, narzędzia dydaktyczne oraz zakres przekazywanej wiedzy muszą nawiązywać do zmiennych potrzeb i zmiennych form zagrożeń i wyzwań. Cechą systemu edukacji kształtującej poczucie bezpieczeństwa informacyjnego (na bazie stanu bezpieczeństwa lub jego braku, a nie patologii) jest elastyczność i zdolność do adaptacji.

1. Weryfikacja literatury

Pojęcie bezpieczeństwa informacyjnego należy łączyć z pojęciem środowiska informacyjnego, które wpływa na funkcjonowanie systemu bezpieczeństwa informacyjnego w sektorach publicznym, prywatnym i obywatelskim. Wpływa ono na kształtowanie postaw, zachowań informacyjnych, społecznych oczekiwań i przyzwolenia na reakcje, oddziałując na poczucie bezpieczeństwa w sferze informacyjnej. Głównym kreatorem środowiska informacyjnego ucznia jest władza lokalna i przedstawiciele oświaty (Batorowska, 2021, s. 339). Bezpieczeństwo informacyjne podmiotu wynika z uprawianej przez władze polityki informacyjnej. W literaturze przedmiotu wskazano, że odpowiada ona za wyjaśnienie procesów społecznych, gospodarczych i politycznych zachodzących w podmiocie, jest formą zarządzania informacją w tym podmiocie, wykorzystuje metody i narzędzia prowadzenia dialogu, współpracy i partnerstwa. Dzięki niej władze promują postawy obywatelskie i partycypacyjne w społecznościach lokalnych. Polityka informacyjna służy także promocji zachowań prewencyjnych względem potencjalnych zagrożeń, w tym informacyjnych (Batorowska, 2021, s. 430-434). W tej perspektywie o bezpieczeństwie informacyjnym traktuje Bogusława Dobek-Ostrowska, która zwraca uwagę na zależność między formą komunikacji publicznej władzy z obywatelami a ich zaangażowaniem we współpracę i przeciwdziałanie zagrożeniom. Z kolei Stanisław Michałowski konkluduje, że sprawny obieg informacji w podmiocie stanowi podstawę kształtowania odporności na zagrożenia informacyjne (Dobek-Ostrowska, 2007; Michałowski, 2006). W ujęciu interdyscyplinarnym pojęcie bezpieczeństwa informacyjnego powinno nawiązywać do uprawianej polityki informacyjnej i uwzględniać kwestie, takie jak public relations, partycypacja społeczna czy dojrzałość informacyjna użytkowników informacji.

Jednakże w literaturze przedmiotu odnotowano brak publikacji analizujących zależność pomiędzy umiejętnością zarządzania informacją przez obywateli a wzrostem poziomu ich poczucia bezpieczeństwa informacyjnego. Prowadzone przez autorkę artykułu badania na temat poczucia bezpieczeństwa informacyjnego społeczności lokalnych w aspekcie wybranych zagrożeń cywilizacyjnych na przykładzie społeczności Suchej Beskidzkiej udokumentowały istnienie tej korelacji. Związek między instytucjonalną edukacją skierowaną na bezpieczeństwo informacyjne i zaangażowaniem przedstawicieli władz lokalnych w proces wdrażania takich programów jest widoczny w prowadzonych audytach w obszarze zagrożeń informacyjnych w instytucjach publicznych, a także we wzroście świadomości informacyjnej obywateli i ich poczucia bezpieczeństwa informacyjnego. Wskazano, że subiektywne podejście do poczucia bezpieczeństwa informacyjnego jednostki przekłada się na jego zdolność do przeciwdziałania zagrożeniom i radzenia sobie w sytuacji wystąpienia ryzyka.

Ważną kwestią związaną z poczuciem bezpieczeństwa informacyjnego jako atrybutu bezpieczeństwa informacyjnego jest bezpieczeństwo interpersonalne. Definiowane jako stan wolny od zagrożenia, w przypadku którego jednostka ma zagwarantowaną ochronę przed wszelkimi zagrożeniami oraz możliwość rozwoju. Brak tej gwarancji lub zaistnienie innego zagrożenia (również w ujęciu subiektywnego postrzegania świata przez jednostkę) prowadzi do napięcia, strachu, lęku wywołanego bodźcem (informacją) na jednostkę oraz ma wpływ na jej zdolność do podjęcia działania (Ropski, 2021, s. 345-346).

Z perspektywy legislacyjnej poczucie bezpieczeństwa (w tym informacyjnego) należy łączyć ze świadomością istnienia wielu aktów prawnych, które regulują działania związane z łamaniem praw człowieka czy dyskryminacją bądź używaniem mowy nienawiści. Jednym z najważniejszych dokumentów w tym obszarze jest prawo cywilne, w tym art. 24 k.c., czy prawo karne, w tym art. 119 k.k., a także prawo międzynarodowe, np. Europejska Konwencja Praw Człowieka i Podstawowych Wolności.

Jak zaznaczono, poczucie bezpieczeństwa informacyjnego i bezpieczeństwo informacyjne jest zależne od świadomości użytkownika informacji na temat potencjalnych zagrożeń i możliwości przeciwdziałania im, dlatego w definicji bezpieczeństwa informacyjnego należy wyeksponować czynnik wychowawczy i edukacyjny.

Kluczowe znaczenie odgrywa nauczyciel, który w świecie VUCA jest przewodnikiem, ułatwiającym poruszanie się w płynnym otoczeniu, trenerem w radzeniu sobie z ryzykiem, lękiem, niepewnością i liderem, wzorem do naśladowania przez ucznia. Pisze o tym Kirk Lawrence w publikacji pt. *Developing Leader in a VUCA Environment*, traktując nauczyciela jako menedżera odpowiedzialnego za kształtowanie kultury organizacyjnej, w której ceni się dialog, współpracę, sprawstwo i umiejętność oceny ryzyka (Lawrence, 2013, s. 2-13). Na kluczowe znaczenie kultury szkoły we wdrażaniu innowacyjnych programów edukacji wskazali również John E. Farley i Michael W. Flota. Według nich kultura organizacyjna wpływa na kształt środowiska społecznego i informacyjnego oraz umożliwia dokonanie w nim zmiany nieodzownej do adaptacji w nowej rzeczywistości VUCA. Może zapobiegać zagrożeniom wynikającym z emocjonalności przekazu i manipulacji treścią kulturowo-ideologiczną (Farley, Flota, 2017, s. 1-17).

W aspekcie zarządzania bezpieczeństwem informacyjnym i kształtowania poczucia bezpieczeństwa informacyjnego na uwagę zasługuje refleksja podjęta przez Jacka M. Barbaleta. Wskazał on, że emocje ludzkie wpływają na poziom racjonalności i obiektywizmu dokonywanego przez nich oglądu rzeczywistości. Brak tych cech skutkuje powstawaniem podziałów społecznych, wykluczaniem, etykietowaniem, naznaczaniem grup i jednostek. Zarządzanie emocjami jest niezbędne do zarządzania bezpieczeństwem podmiotu w każdej sferze (Barbalet, 1998, s. 29-80).

W wyniku powyższego w definicji bezpieczeństwa informacyjnego powinny znaleźć się odniesienia do zarządzania emocjami i kulturą. Jednakże obecnie obowiązująca definicja bezpieczeństwa informacyjnego nie uwzględnia zagrożeń charakterystycznych dla świata VUCA, związanych z nadmiarem bodźców, stresem informacyjnym, ścisłą koegzystencją człowieka z nowymi technologiami, głównie AI, strachem przed tą technologią, nieumiejętnością zarządzania lękiem, stresem, ryzykiem, niemożnością pozyskania wystarczającej wiedzy i nieodzownych kompetencji do zrozumienia zmiennego, niepewnego, złożonego i niejednoznacznego świata, który w szybkim tempie ewoluuje w kierunku ludzko-sztucznego świata rządzącego się algorytmami niezrozumiałymi dla większości ludzi.

2. Metodyka badań

W celu analizy programów edukacji dla bezpieczeństwa informacyjnego pod kątem kształtowania umiejętności informacyjnych, emocjonalnych i społecznych zastosowano metodę analizy zawartości treści dokumentów. Badania zostały przeprowadzone na terenie miasta Sucha Beskidzka, w stolicy powiatu suskiego i w jego centrum edukacyjnym i oświatowym. Respondenci pochodzili z placówek zajmujących się edukacją i kulturą.

Konstrukcję warsztatu badawczego oparto na wytycznych zamieszczonych w pracy Piotra Sowizdraniuka, który analizę treści odnosi do konkretnego problemu, przypisując jej właściwość identyfikacji zależności, pokrewieństw i wykluczających się elementów (Sowizdraniuk, 2017, s. 87-88).

Badania poczucia bezpieczeństwa informacyjnego w ujęciu interdyscyplinarnym objęły następujące dyscypliny: nauka o bezpieczeństwie, pedagogika, psychologia i kulturoznawstwo. Celowość zastosowania ujęcia interdyscyplinarnego wynikała z charakteru analizowanego środowiska VUCA (zmiennosc, niepewnosć, złożonosć, niejednoznacznosć) (Czupryński, 2017, s. 12-17).

Pełne wyniki badań nad poczuciem bezpieczeństwa informacyjnego społeczności lokalnych pod kątem wybranych zagrożeń cywilizacyjnych zostały zaprezentowane w pracy doktorskiej K. Batorowskiej pt. *Poczucie bezpieczeństwa informacyjnego społeczności lokalnych w aspekcie wybranych zagrożeń cywilizacyjnych na przykładzie społeczności Suchoj Beskidzkiej* (Batorowska, 2023).

Podstawą teoretyczną badań jest założenie, że człowiek podejmuje racjonalne decyzje na podstawie pozyskanych umiejętności intelektualnych związanych z analizą, syntezą, uogólnianiem, abstrahowaniem itp., a także dzięki sukcesywnie rozwijanim kompetencjom informacyjnym. Człowiek staje się aktywnym podmiotem bezpieczeństwa tylko wówczas, gdy osiągnie pożądaną poziom dojrzałości informacyjnej i jest świadomy swoich działań oraz bierze za nie odpowiedzialność.

3. Wyniki

Badania dotyczyły analizy programów edukacji dla bezpieczeństwa informacyjnego realizowanych w edukacji instytucjonalnej (od przedszkola do szkolnictwa wyższego) i pozaszkolnej (kształcenie ustawiczne) oraz w ośrodkach o charakterze kulturowym (biblioteki pedagogiczne, centra kultury). Badano metody wdrażania programu oraz umiejętności uczestników tych szkoleń po ich zakończeniu.

W edukacji instytucjonalnej w zakresie bezpieczeństwa informacyjnego dominowało kształcenie kompetencji technicznych, zarówno w kształceniu ogólnym, jak i zawodowym. Kształcenie kompetencji emocjonalnych było realizowane głównie na poziomie edukacji podstawowej. Na poziomie szkoły średniej przygotowanie emocjonalne do racjonalnego funkcjonowania w społeczeństwie powierzono pedagogom szkolnym. Na poziomie szkolnictwa średniego, wyższego i ustawicznego przekazywana wiedza i szkolone sprawności są związane z zarządzaniem bezpieczeństwem informacji, ale tylko w aspekcie technicznym i informatycznym (Batorowska, 2023, s. 350-352).

Na poziomie edukacji przedszkolnej są kształtowane kompetencje społeczne, w tym umiejętność pracy w grupie. Na poziomie edukacji wczesnoszkolnej są to kompetencje społeczne i emocjonalne. Na tym poziomie nauczyciel przyjmuje rolę wychowawcy i koncentruje uwagę na wdrażaniu tych kompetencji.

W liceach i technicach kształcenie w zakresie bezpieczeństwa informacyjnego realizowane jest w ramach edukacji informatycznej i technicznej. Nie przewidziano kształcenia umiejętności emocjonalnych czy informacyjnych (jako odrębnego przedmiotu). Rola nauczyciela koncentruje się na przekazywaniu wiedzy, nie realizuje się wychowania do informacji (wychowania informacyjnego). Nauczyciela w rozwiązywaniu problemów wynikających z funkcjonowania ucznia w środowisku nadmiaru informacji i uzależnienia od technologii informacyjnych wspiera psycholog i pedagog szkolny (Batorowska, 2023, s. 352-254).

Edukacja dla bezpieczeństwa informacyjnego na poziomie szkolnym uwzględnia tematykę ochrony informacji i zasobów informacyjnych, szczególnie ochronę danych osobowych, znajomość przepisów RODO, prawo dostępu do informacji publicznej, korzystanie z technologicznych zabezpieczeń własnych danych, znajomość cyberzagrożeń, a nawet tematykę higieny cyfrowej i ochrony prywatności (Liceum Ogólnokształcące nr 1 im. Marii Skłodowskiej-Curie w Suchoj Beskidzkiej, 2024).

W szkole zawodowej kompetencje i wiedza z zakresu bezpieczeństwa informacyjnego realizowana jest na lekcjach programowania, informatyki, techniki fotograficznej i technik multimedialnych (Zespół Szkół im. W. Witosa w Suchoj Beskidzkiej, 2024). Edukacja dla bezpieczeństwa informacyjnego obejmuje tylko wybrane kierunki kształcenia, więc nie obejmuje wszystkich uczniów.

W edukacji ustawicznej oferowanej przez podmiot, taki jak Centrum Kształcenia Dorosłych, kształtowane są umiejętności techniczne i informatyczne podczas

kursów z zakresu obsługi komputera, programowania i zakładania stron internetowych. Oferta obejmująca szkolenie kompetencji społecznych, emocjonalnych i psychologicznych jest skierowana do przedstawicieli oświaty, w tym nauczycieli. Odnotowano brak szkoleń dla szeroko rozumianych użytkowników informacji, którzy chcieliby podnosić poziom swoich kompetencji informacyjnych, medialnych, cyfrowych i emocjonalnych (Beskidzkie Centrum Kształcenia Dorosłych. Centrum Kształcenia Ustawicznego, 2024).

Instytucje zajmujące się działalnością kulturalną mają w swojej ofercie także szkolenia doskonalące kompetencje informacyjne i społeczne, np. szkolenia dotyczące tworzenia tekstów czy zastosowania innych aplikacji, a także szkolenia patriotyczne (Pedagogiczna Biblioteka Wojewódzka, Filia w Suchej Beskidzkiej, 2024). Prowadzone są też warsztaty, których celem jest zachowanie i promocja lokalnej kultury (Centrum Kultury i Filmu w Suchej Beskidzkiej, 2024), ale nie prowadzi się szkoleń stricte poświęconych bezpieczeństwu informacyjnemu.

Edukacja dla bezpieczeństwa informacyjnego realizowana przez instytucje lokalne sprowadza się do kształcenia kompetencji technicznych i informatycznych oraz przekazywania treści o zagrożeniach i wyzwaniach współczesnego świata, takich jak cyberzagrożenia i cyberterrorizm, głównie na lekcjach informatyki i wiedzy o społeczeństwie. Nie ma kursów podnoszących świadomość informacyjną mieszkańców i traktujących problemy bezpieczeństwa informacyjnego w sposób interdyscyplinarny. Umiejętności emocjonalne wprawdzie są kształtowane, ale w ramach indywidualnych spotkań prowadzonych przez psychologa czy pedagoga szkolnego.

Z powyższego wynika, że poczucie bezpieczeństwa informacyjnego badanej grupy opiera się na przeświadczeniu, iż jest w stanie zapewnić go wiedza i umiejętności informatyczne własne lub instytucji za to odpowiedzialnych. Zagrożeń dla bezpieczeństwa środowiska informacyjnego nie dostrzegają w cechach świata VUCA. Nie widzą potrzeby wprowadzania alternatywnych metod nauczania, które pozwoliłyby rozwijać specjalistyczne kompetencje informacyjne i podnosić poziom świadomości informacyjnej (LeBlanc, 2018, s. 3-4).

Reasumując, poczucie bezpieczeństwa informacyjnego kształtowane jest na podstawie:

- wiedzy o zagrożeniach bezpieczeństwa informacyjnego i formach przeciwdziałania im;
- wiedzy o ochronie danych, przepisach RODO i zabezpieczeniach teleinformatycznych;
- możliwości dostępu do informacji publicznej i realizacji własnych potrzeb informacyjnych;
- przeświadczenia, że państwo i inne podmioty państwowe będą odpowiedzialne za ochronę informacji dzięki ustawodawstwu oraz że zapewnią nam jako użytkownikom informacji bezpieczne korzystanie z usług informacyjnych;

- znajomości obowiązujących zasad, które pozwolą bezpiecznie posługiwać się informacjami i nimi zarządzać;
- własnych sprawności technologicznych i możliwości własnego sprawstwa;
- przeświadczenia, że nasze dane są dobrze chronione w systemach informacyjnych;
- znajomości architektury informacji.

Konieczne jest poszukiwanie alternatywnych rozwiązań dydaktycznych w celu podnoszenia sprawczości i świadomości ucznia dzięki jego motywacjom i zaangażowaniu w rozwój osobisty.

4. Dyskusja

W świecie VUCA wyzwaniem staje się skuteczność w sferze społecznej, ekonomicznej, politycznej czy technologicznej oparta na zdolnościach dostosowania się do potrzeb i zmian modelu zarządzania. Opracowanie i wdrażanie dobrych praktyk związanych z podnoszeniem umiejętności adaptacji do zmiennych warunków ma początek w systemie edukacji. I to system edukacji musi być elastyczny i dostosowywać podstawy programowe oraz metody i techniki ich realizacji do dynamicznie zmieniających się warunków życia w środowisku informacyjnym. Konieczna jest współpraca instytucji edukacyjnych z instytucjami odpowiedzialnymi za bezpieczeństwo obywateli w środowisku informacyjnym. Wiąże się to z redefinicją sposobu zarządzania kadrą szkolną przez dyrektora (Waller, Lemoine, Mense et al., 2019, s. 73-74).

Nauczyciel w świecie VUCA musi przejawiać odporność psychiczną, radzić sobie ze stresem i kontrolować emocje. Powinien umieć budować swój wizerunek i wyróżniać się charyzmą, dając przykład do naśladownictwa postaw, idei i zachowań (Musiał, 2021, s. 76-77). W ten sposób może promować edukację. Dlatego konieczne jest przygotowanie nauczycieli, np. w zakresie stosowania metody Just-in-Time Learning lub pełnienia roli coacha (Nikolić, Milovanović, 2021, s. 61-63).

Wzmacnianie poczucia bezpieczeństwa informacyjnego podmiotów funkcjonujących w świecie VUCA sprowadza się do zwiększenia ich odporności na te zagrożenia. Wymaga od władz lokalnych większej dbałości o sprawne zarządzanie informacją, szczególnie jej transfer między władzą a mieszkańcami, oraz uprawianie transparentnej polityki informacyjnej zbudowanej na społecznym łańdźcu informacyjnym. Budowanie społecznego bezpieczeństwa informacyjnego, a na jego kanwie poczucia bezpieczeństwa informacyjnego obywateli wymaga nawiązywania współpracy i partnerstwa ponadregionalnego dla celów edukacyjnych (Beaulieu, van Dalen-Oskam, van Zundert, 2012, s. 112-115), w tym dla edukacji dla bezpieczeństwa informacyjnego.

Podsumowując, tworzenie środowiska bezpieczeństwa informacyjnego wymaga od władz lokalnych analizy środowiska lokalnego, rozumienia społeczno-kulturowych uwarunkowań, a następnie wspólnego z nim budowania ładu informacyjnego. Działania takie ograniczą bierność obywateli do inicjatyw partycypacyjnych i przeciwdziałac będą negatywnym skutkom zagrożeń bezpieczeństwa informacyjnego (Kizza, Kizza, 2007, s. 1-21, 137-179).

Wnioski

Celem artykułu było zidentyfikowanie metod wdrażania edukacji dla bezpieczeństwa informacyjnego w środowisku lokalnym i jej wpływ na kształtowanie poczucia bezpieczeństwa informacyjnego członków społeczności. Cel ten został osiągnięty. Metody wdrażania edukacji dla bezpieczeństwa informacyjnego zaliczyć można do tradycyjnych i są one realizowane głównie podczas zajęć z przedmiotu informatyka. Edukacja ta nie obejmuje wszystkich uczniów, jeżeli realizowana jest na zajęciach specjalistycznych lub nieobowiązkowych. Na postawione w artykule pytanie: czy edukacja dla bezpieczeństwa informacyjnego kształtuje odporność uczących się na zagrożenia generowane w środowisku informacyjnym?, można odpowiedzieć następująco: formy edukacji dla bezpieczeństwa informacyjnego są niewystarczające, aby w sposób obiektywny kształtować poczucie bezpieczeństwa informacyjnego w podmiotach funkcjonujących w świecie VUCA. Konieczne jest wdrażanie szkoleń cyklicznych i obowiązkujących wszystkich uczniów, zawierających problematykę inteligencji emocjonalnej, odporności psychicznej na manipulację informacją i manipulację medialną, świadomości i uodpornienia na celowe wywołanie niepokoju czy lęku w społeczeństwie. Edukacja na rzecz bezpieczeństwa informacyjnego odpowiedzialna za jakość poczucia bezpieczeństwa informacyjnego obywateli niejednokrotnie tego stanu nie tylko nie przybliży do stanu obiektywnego bezpieczeństwa, lecz wręcz skieruje go w stronę stanu patologii.

BIBLIOGRAFIA

- [1] ALKOWSKI, P., 2015. *Bezpieczeństwo informacyjne – zarys wybranych aspektów w kontekście bezpieczeństwa państwa*, [w:] Guzik-Makaruk, E.M., Pływaczewska, E.W. (red.), *Współczesne oblicza bezpieczeństwa*, Białystok: Wydawnictwo Temida 2, s. 87-99.
- [2] BARBALET, J.M., 1998. *Emotion, Social Theory, and Social Structure. A Macrosociological Approach*, London: Cambridge University Press.
- [3] BATOROWSKA, H., 2021. *Bezpieczeństwo informacyjne*, [w:] Wasiuta, O., Wasiuta, S. (red.), *Encyklopedia bezpieczeństwa*, t. 1, Kraków: Libron, s. 337-343.
- [4] BATOROWSKA, K., 2021. *Polityka informacyjna*, [w:] Wasiuta, O., Wasiuta, S. (red.), *Encyklopedia bezpieczeństwa*, t. 3, Kraków: Libron, s. 430-434.

- [5] BATOROWSKA, K., 2023. *Poczucie bezpieczeństwa informacyjnego społeczności lokalnych w aspekcie wybranych zagrożeń cywilizacyjnych na przykładzie społeczności Suchej Beskidzkiej* [praca dyplomowa – doktorat], Siedlce: Uniwersytet w Siedlcach.
- [6] BEAULIEU, A., VAN DALEN-OSKAM, K., VAN ZUNDEBT, J., 2012. *Between tradition and Wen 2.0: eLaborate as a Social Experiment in Humanities Scholarship*, [w:] Takseva, T. (red.), *Social Software and the Evolution of User Expertise: Future Trends in Knowledge Creation and Dissemination*, Hershey: Information Science Reference s. 112-129.
- [7] BENNETT, N., LEMOINE, G.J., 2014. What a Difference a Word Makes: Understanding Threats to Performance in a VUCA World, *Business Horizons*, vol. 57, nr 3, s. 311-317.
- [8] BESKIDZKIE CENTRUM KSZTAŁCENIA DOROSŁYCH. CENTRUM KSZTAŁCENIA USTAWICZNEGO, 2024. *Oferta kursów*, <http://www.bncdn.pl/teachers/offer> (dostęp: 20.01.2024).
- [9] BODENHAUSEN, G.V., PEERY, D., 2009. Social Categorization and Stereotyping In vivo: The VUCA Challenge, *Social and Personal Psychology Compass*, vol. 3, nr 2, s. 133-151.
- [10] CENTRUM KULTURY I FILMU W SUCHEJ BESKIDZKIEJ, 2024. *Zajęcia*, <https://ckifsucha.pl/zajecia/> (dostęp: 20.01.2024).
- [11] CZUPRYŃSKI A., 2017. *Kryteria dyscypliny naukowej*, [w:] Czupryński, A., Wiśniewski, B., Zbożina, J. (red.), *Nauki o bezpieczeństwie. Wybrane problemy badań*, Józefów: CNBOP-PIB, s. 9-17.
- [12] DOBEK-OSTROWSKA, B., 2007. *Podstawy komunikowania społecznego*, Wrocław: Wydawnictwo Astrum.
- [13] FARLEY, J.E., FLOTA, M.W., 2017. *Culture and Social Structure*, [w:] Farley, J.E., Flota, M.W., *Sociology*, New York: Routledge.
- [14] GRZEBIELA, K., 2018. Pojęcie i istota bezpieczeństwa informacyjnego, *Kultura bezpieczeństwa. Nauka – Praktyka – Refleksje*, nr 30, s. 87-101.
- [15] KIZZA, J., KIZZA, M., 2007. *Securing the Information Infrastructure*, New Delhi: CyberTech Publishing.
- [16] LAWRENCE, K., 2013. *Developing Leaders in a VUCA Environment*, UNC Executive Development, <https://www.emergingrnleader.com/wp-content/uploads/2013/02/developing-leaders-in-a-vuca-environment.pdf>, s. 1-15 (dostęp: 20.01.2024).
- [17] LEBLANC, P., 2018. Higher Education in a VUCA World, *Change: The Magazine of Higher Learning*, vol. 50, nr 3-4, s. 23-26.
- [18] LICEUM OGÓLNOKSZTAŁCĄCE IM. MARII SKŁODOWSKIEJ-CURIE W SUCHEJ BESKIDZKIEJ, 2024. *Pedagog i psycholog szkolny*, <https://losucha.pl/pedagog-szkolny/> (dostęp: 20.01.2024).
- [19] MATCZAK, A., KNOPF, K., 2013. *Znaczenie inteligencji emocjonalnej w funkcjonowaniu człowieka*, Warszawa: Wydawnictwo Stowarzyszenia Filomatów.
- [20] MICHALCZYK, S., 2017. Kognicje i emocje w procesie recepcji mediów, *Rocznik Prasoznawczy*, nr 11, s. 11-31.
- [21] MICHAŁOWSKI, S., 2006. *Władza lokale a media: zarządzanie informacją, public relations, promocja jednostek samorządu terytorialnego*, Lublin: Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej.
- [22] MUSIAŁ, E., 2021. *Nauczyciel w świecie VUCA – co to znaczy?*, [w:] Kaźmierczak, D., Ropski, J., Wasiuta, O., Zakrzewski, W. (red.), *Edukacja w świecie VUCA. Szanse, wyzwania, zagrożenia*, Kraków: Libron, s. 67-84.
- [23] NIKOLIĆ, T.M., MILOVANOVIĆ, M., 2021. *Innovative approach to personalized teaching and learning in the VUCA world*, [w:] *12th International Conference on eLearning (eLearning-2021)*, Belgrad 2021, <https://dimps-erasmus.com/file/documents/Proceedings%20-%202012th%20International%20Conference%20on%20e-Learning%202021.pdf#page=60>, s. 60-65 (dostęp: 20.01.2024).

-
- [24] PEDAGOGICZNA BIBLIOTEKA WOJEWÓDZKA FILIA W SUCHEJ BESKIDZKIEJ, 2024. *Kursy online*, <https://moodle.pbw.edu.pl/> (dostęp: 20.01.2024).
- [25] ROPSKI, J., 2021. *Bezpieczeństwo interpersonalne*, [w:] Wasiuta, O., Wasiuta, S. (red.), *Encyklopedia bezpieczeństwa*, t. 1, Kraków: Libron, s. 344-349.
- [26] SOWIZDRANIUK, P., 2017. *Wybrane metody oraz techniki i narzędzia jakościowe w badaniach bezpieczeństwa*, [w:] Czupryński, A., Wiśniewski, B., Zbrojna, J., (red.), *Nauki o bezpieczeństwie. Wybrane problemy badań*, Józefów: CNBOP-PIB, s. 79-90.
- [27] TOŁWIŃSKI, M., 2016. *Etyczny aspekt bezpieczeństwa informacyjnego. Przypadek etyki dziennikarskiej i aksjologii informacji*, [w:] Kubiak, M., Topolewski, S., (red.) *Bezpieczeństwo informacyjne w XXI wieku*, Siedlce–Warszawa: Pracownia Wydawnicza Wydziału Humanistycznego UPH, s. 149-158.
- [28] WALLER, R., LEMOINE, P.A., MENSE, E.G., GARRETSON, CH.J., RICHARDSON, M.D., 2019. Global Higher Education in a VUCA World: Concerns and Projections, *Journal of Education and Development*, vol. 3, nr 2, s. 72-74.
- [29] WÓDKA, M., 2016. *Wyzwania dla bezpieczeństwa informacyjnego w Polsce i Unii Europejskiej*, [w:] Kubiak, M., Topolewski, S. (red.) *Bezpieczeństwo informacyjne w XXI wieku*, Siedlce–Warszawa: Pracownia Wydawnicza Wydziału Humanistycznego UPH, s. 159-176.
- [30] URA, E., PIEPRZNY S. (red.), 2015. *Bezpieczeństwo wewnętrzne państwa*, Rzeszów: Wydawnictwo Uniwersytetu Rzeszowskiego.
- [31] ZESPÓŁ SZKÓŁ IM. W. WITOSA W SUCHEJ BESKIDZKIEJ, 2024. *Kierunki kształcenia*, <https://zsw-sucha.pl/szkola/ckz-2/> (dostęp: 20.01.2024).