DOI: 10.52694/ThPSR.2024.3.1

Katarzyna Batorowska

Bezpieczeństwo informacyjne z punktu widzenia pracodawcy i pracownika

Information security from the perspective of the employer and employee

Przedmiotem artykułu jest bezpieczeństwo informacyjne. Celem rozważań ustanowiono identyfikację rozbieżności i pokrewieństw w rozumieniu przez pracodawców i pracowników organizacji pojęcia „bezpieczeństwo informacyjne". Zastosowano metodę badawczą jaką jest wywiad ekspercki. Przeprowadzono go z przedstawicielami kadry kierowniczej organizacji oraz jej pracownikami. Zebrany materiał wykorzystano opisując Case Study odnoszący się do bezpieczeństwa informacyjnego w organizacji. Wykazano, że rozbieżności definicyjne mogą oddziaływać na osiągnięcie przez organizację sukcesu. Wyniki badań można zastosować w obszarze zarządzania organizacją.

Słowa kluczowe: bezpieczeństwo informacyjne, pracodawca, pracownik, organizacja, zarządzanie bezpieczeństwem informacji

The subject of the article is information security. The aim of the article is to identify differences and similarities in the understanding of the concept of information security by employers and employees of a selected organization. The research method is an expert interview conducted with representatives of the organization's management staff and its employees. The Case Study method was used. The author showed that definitional discrepancies pose a challenge to the development of the organization. The research results presented in this article can be applied to research on organizational management methods.

Key words: information security, employer, employee, organization, information security management

Wprowadzenie

Pojęcie „bezpieczeństwo państwa" zostało wprowadzone do literatury przedmiotu w drugiej połowie XIX wieku. Jego etymologia odnosi się do łacińskiego słowa *securitas*, czyli stan bezpieczny. Jeszcze w XX wieku bezpieczeństwo było rozumiane jako wolność od zagrożeń lub wolność od strachu i lęku. Naukowiec tamtego okresu Arnold Wolfers, zaproponował definicję bezpieczeństwa z położeniem akcentu na jego obiektywny i subiektywny charakter. W sensie obiektywnym bezpieczeństwo to stan braku zagrożeń dla wartości nabytych, natomiast w sensie subiektywnym to brak strachu, że wartości te zostaną zaatakowane[1]. Naukowiec Daniel Frey definiuje pojęcie „bezpieczeństwo" również w wymiarze obiektywnym i subiektywnym. W pierwszym przypadku dzieli je na dwa stany: stan bezpieczeństwa i stan braku bezpieczeństwa. Na podstawie dostępnych informacji człowiek ocenia w sposób obiektywny czy istnieją przesłanki identyfikujące zagrożenie czy ich nie ma. W przypadku stanu braku bezpieczeństwa podejmuje adekwatne działania zmierzające do minimalizacji negatywnych skutków tego zagrożenia. W przypadku stanu bezpieczeństwa nie jest konieczne podejmowanie działań. Natomiast w przypadku bezpieczeństwa rozumianego w sposób subiektywny, rozróżnia inne dwa stany, tj. stan obsesji i stan fałszywego bezpieczeństwa. Stan obsesji uzewnętrznia się, kiedy na podstawie dostępnych informacji, człowiek identyfikuje istnienie zagrożenia, gdy faktycznie poziom tego zagrożenia jest minimalny lub go nie ma. W wyniku błędnego oszacowania ryzyka człowiek podejmuje działania nieadekwatne do występującego zagrożenia. Natomiast w przypadku drugim, człowiek po przeprowadzonej analizie sytuacji nie stwierdza zagrożenia lub stwierdza zaistnienie tylko minimalnego szkodliwego oddziaływania.

W obiektywnej analizie danych i faktów zagrożenie dla człowieka istnieje nadal i może go dotyczyć w sposób bezpośredni. W tym przypadku reakcja człowieka może być również nieadekwatna do zaistniałej sytuacji[2]. Z przywołanego sposobu definiowania bezpieczeństwa wynika konieczność prowadzenia wnikliwej analizy informacji umożliwiającej identyfikację zagrożeń, a następnie wybór odpowiedniej formy reakcji na nie. Konsekwencją błędnie przeprowadzonej analizy informacji

[1] A. Wolfers, *Discord and Collaboration. Essays on International Politics*, Baltimore 1962, s. 150.
[2] D. Frei, *Sicherheit, Grundfragen der Weltpolitik*, Kohlhammer, Stuttgart 1997, s. 17–21.

na temat generowanych przez środowisko człowieka zagrożeń jest tzw. fałszywe poczucie bezpieczeństwa.

Powyższą refleksję uzupełnia definicja bezpieczeństwa opracowana przez Biuro Bezpieczeństwa Narodowego, w której traktowane jest ono jako: „teoria i praktyka zapewniająca możliwość przetrwania i realizacji własnych interesów przez dany podmiot, w szczególności poprzez wykorzystanie szans (okoliczności sprzyjających), podejmowanie wyzwań, redukowanie ryzyk oraz przeciwdziałanie (zapobieganie i przeciwstawianie się) wszelkiego rodzaju zagrożeniom dla podmiotu i jego interesów”[3]. Zaprezentowano w niej podział na kategorie rozróżniające pojęcie ‘bezpieczeństwo’ w zależności od podmiotu którego dotyczy i obszaru jego funkcjonowania. Wydzielono podejście z perspektywy nauk o bezpieczeństwie i nauk o obronności, akcentując w tym pierwszym czynnik niemilitarny wpływający na rozumienie bezpieczeństwa w obliczu dokonujących się zmian cywilizacyjnych.

W wyniku rozwoju nowych technologii informacyjno-komunikacyjnych, a także intensyfikacji procesów globalizacyjnych i ich wpływu na każdą płaszczyznę funkcjonowania człowieka doszło do demilitaryzacji pojęcia bezpieczeństwo, co zmusiło badaczy do rozumienia go w szerszym znaczeniu[4]. Kolejnym czynnikiem wpływającym na metamorfozę rozumienia pojęcia bezpieczeństwa jest przypisywanie informacji różnych funkcji, np.: sterującej, opiniotwórczej, demokratyzującej, wychowawczej, integracyjnej, motywacyjnej, terapeutycznej, czynnika kulturotwórczego, śladu ludzkiego bytowania, kapitału, towaru przeznaczonego do wymiany, zasobu do wykorzystania w przyszłości, „łagodnej siły”, atrybutu władzy itp. Dlatego bezpieczeństwo informacyjne dotyczące człowieka należy rozpatrywać w tak szerokim obszarze. Nie można go ograniczać tylko do ochrony informacji i infrastruktury teleinformatycznej. Nie bez powodu w normie ISO-IEC 27001:2022 bezpieczeństwo informacyjne jest traktowane jako proces stanowiący wyzwanie dla całej organizacji, a nie wyłącznie problemem technologiczny czy informatyczny[5].

---

[3] *Bezpieczeństwo*, Mini słownik BBN, strona główna Biura Bezpieczeństwa Narodowego, https://www.bbn.gov.pl/pl/form/dodaj3,MINI-Slownik-BBN-Propozycje-nowych-terminow.html, (dostęp: 06.10.2024).

[4] M. Cieślarczyk, *Relacje między bezpieczeństwem i obronnością w kontekście wąskiego i szerokiego rozumienia tych zjawisk*, [w:] *Elementy teorii i praktyki transdyscyplinarnych badań problemów bezpieczeństwa,* t. 6: W poszukiwaniu relacji między bezpieczeństwem a obronnością, J. Ważniewska (red.), Siedlce 2017, s. 243–262.

[5] *Bezpieczeństwo informacyjne, cyberbezpieczeństwo i ochrona prywatności – Systemy Zarządzania Bezpieczeństwem Informacji – Wymagania*. ISO-IEC 27001:2022 Akademia TÜV NORD POLSKA 2023.

Zarządzanie systemami bezpieczeństwa informacyjnego odnosi się także do zasobów informacyjnych w wymiarze personalnym, społecznym, zawodowym, gospodarczym, politycznym, stanowiąc podstawę rozwoju tych sektorów. Dlatego metody gromadzenia, przetwarzania, zabezpieczania, dzielenia się informacją wymagają nowej analizy i ustrukturyzowania metod i narzędzi również w zakresie zarządzania ich bezpieczeństwem.

Pojęcie bezpieczeństwa jest analizowane jako stan, jako wartości i jako potrzeba człowieka. W literaturze naukowcy niejednokrotnie odwołują się do piramidy potrzeb Maslowa, w której potrzeba bezpieczeństwa stanowi kolejną potrzebę zaraz po tych fizjologicznych[6]. Bezpieczeństwo rozpatrywane w ujęciu potrzeby człowieka można przełożyć również na jego sposoby postrzegania rzeczywistości poprzez jego fizyczne, psychiczne, kulturowe i środowiskowe uwarunkowania umożliwiające przetwarzanie informacji. W tym miejscu należy nawiązać do wcześniejszego rozpatrywania pojęcia „bezpieczeństwo" przez Daniela Frei.

Pojęcie „bezpieczeństwo" można rozpatrywać z perspektywy różnych nauk, w tym nauk o bezpieczeństwie, nauk o zarządzaniu i jakości (mowa o zarządzaniu bezpieczeństwem), nauk o komunikacji społecznej i mediach, a także psychologii (subiektywne rozumienie bezpieczeństwa, manipulacja poczuciem bezpieczeństwa) czy socjologii (wpływ bezpieczeństwa na procesy społeczne). W wyniku lawinowego rozwoju technologii informacyjno-komunikacyjnych i przyspieszenia procesów globalizacji, zwiększył się popyt na informację spełniająca normy jakościowe (wiarygodną, rzetelną, dokładną, kompletną aktualną, adekwatną, integralną itp.). Dlatego też istotnym obszarem definiowania bezpieczeństwa stało się w ostatnich latach bezpieczeństwo informacyjne.

W ramach badań nad pojęciem „bezpieczeństwo" w środowisku informacyjnym, konieczne stało się łączenie go z takimi słowami kluczowymi, jak poczucie bezpieczeństwa informacyjnego, kultura organizacyjna, świadomość społeczna. W przypadku pierwszego terminu mowa o subiektywnym postrzeganiu bezpieczeństwa przez człowieka (odwołanie do D. Frei). W przypadku drugim mowa o zbiorze norm społecznych i systemów wartości, które są unikatowe dla danej zbiorowości a stanowią formę motywacji dla jej członków do rozwoju. Stanowi swoisty klimat tej zbiorowości wynikający ze sposobów zarządzania tą zbiorowością, jej celem, tradycją i wiedzą posiadaną przez jej członków. Normy

[6] A. Maslow, *Motywacja i osobowość*, Warszawa 1990, s 54–62.

są obowiązkowe dla członków w celu zapewnienia ciągłości działania i kształtowania poczucia bezpieczeństwa[7]. Natomiast w przypadku trzecim mowa o całokształcie wierzeń, przekonań, jakie obowiązują daną społeczność. Można ją traktować jako przeciwieństwo świadomości indywidualnej, gdzie podstawą są potrzeby jednostki. Świadomość indywidualna nie zawsze odzwierciedla potrzeby grupy. Obejmuje również całokształt norm światopoglądowych, tradycyjnych, politycznych, religijnych na jakiej podstawie podejmowane są działania przez jej członków. Czyli na świadomość społeczną składają się opinie, poglądy i postawy członków danej grupy[8]. Podsumowując, pojęcie „bezpieczeństwo" coraz częściej jest rozpatrywane z perspektywy psychologicznych i kulturowych uwarunkowań człowieka, które umożliwiają ocenę stanu bezpieczeństwa w bezpośrednim i pośrednim wymiarze. Składają się na nie czynniki i blokady wynikające z uwarunkowań psychologicznych, kulturowych, politycznych, ekonomicznych, generowane przez jednostkę, kolektyw, grupę.

Pojęcie bezpieczeństwa informacyjnego w literaturze przedmiotu

W literaturze przedmiotu można wskazać wiele definicji pojęcia „bezpieczeństwo informacyjne", odwołujących się do takich kwestii jak ochrona informacji niejawnych, zabezpieczanie systemów teleinformatycznych czy infrastruktury informacyjnej. Przykładem takiej definicji bezpieczeństwa informacyjnego, gdzie podmiotem jest państwo, jest przytoczona powyżej definicja zaproponowana przez Biuro Bezpieczeństwa Narodowego. Bezpieczeństwo informacyjne identyfikowane jest z „transsektorowym obszarem bezpieczeństwa i odnosi się do środowiska informacyjnego (w tym cyberprzestrzeni) państwa. Jest też utożsamiane z procesem, którego celem jest zapewnienie bezpiecznego funkcjonowania państwa w przestrzeni informacyjnej poprzez panowanie we własnej, wewnętrznej, krajowej infosferze oraz poprzez efektywną ochronę

[7] *Kultura organizacyjna*, strona Encyklopedia Zarządzania, https://mfiles.pl/pl/index.php/Kultura_organizacyjna (dostęp: 06.10.2024).

[8] *Świadomość społeczna*, strona Encyklopedia PWN, https://encyklopedia.pwn.pl/haslo/;3984380, (dostęp: 06.10.2024).

interesów narodowych w zewnętrznej (obcej) infosferze. Osiąga się je poprzez realizacje takich zadań jak: zapewnienie adekwatnej ochrony posiadanych zasobów informacyjnych oraz ochrony przed wrogimi działaniami dezinformacyjnymi i propagandowymi (w wymiarze defensywnym) przy jednoczesnym zachowaniu zdolności do prowadzenia wobec ewentualnych przeciwników (państw lub innych podmiotów) działań ofensywnych w tym obszarze. Zadania te konkretyzowane są w strategii (doktrynie) bezpieczeństwa informacyjnego (operacyjnej i preparacyjnej), a dla ich realizacji utrzymuje się i rozwija odpowiedni system bezpieczeństwa informacyjnego"[9]. Definicja ta obejmuje takie kwestie jak ochrona infrastruktury informacyjnej oraz realizację interesów podmiotu w tym obszarze. Transformacja definicyjna pojęcia „bezpieczeństwo informacji" następuje m.in. poprzez odwołanie jej do integralności i dostępu do informacji, np. K. Liedel podaje: „bezpieczeństwo informacji bardzo często rozumiane jest jako ochrona informacji przed niepożądanym (przypadkowym lub świadomym) ujawnianiem, modyfikacja, zniszczeniem lub uniemożliwieniem jej przetwarzania"[10] lub odwołaniu się do ustrukturyzowaniu metodologicznego względem organizacji bezpieczeństwa informacyjnego. P. Potejko traktuje bezpieczeństwo informacyjne jako: „zbiór działań, metod oraz procedur podejmowanych przez uprawnione podmioty, zmierzających do zapewnienia integralności gromadzonych, przechowywanych, przetwarzanych zasobów informacyjnych poprzez zabezpieczenie ich przed niepożądanym, nieuprawnionym ujawnieniem, modyfikacją lub zniszczeniem"[11]. W obu przypadkach autorzy definicji zwrócili uwagę na kwestię zarządzania bezpieczeństwem informacji przez podmiot, w tym ustrukturyzowania metod zabezpieczania informacji oraz kwestię dostępu, zmierzających do zachowania integralności zasobów umożliwiających sprawną realizacje procesu informacyjnego. Mimo że te definicje silnie korespondują z definicją pierwszą, należy wskazać jej transformację w obszarze zastosowania do innych podmiotów, takich jak państwo oraz posadowienie na centralnym miejscu człowieka jako podmiotu bezpieczeństwa.

[9] *Bezpieczeństwo informacyjne państwa*, strona Biura Bezpieczeńśwta Narodowego, https://www.bbn.gov.pl/pl/form/dodaj3,MINI-Slownik-BBN-Propozycje-nowych-terminow.html, (dostęp: 06.10.2024).
[10] K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2008, s. 19.
[11] P. Potejko, *Bezpieczeństwo informacyjne*, [w:] K.A. Wojtaszczyk, A. Materska-Sosnowska (red.), *Bezpieczeństwo państwa*, Warszawa 2009, s. 193.

Natomiast w odniesieniu do kwestii społecznych i środowiskowych mających wpływ na podmiot bezpieczeństwa, należy przytoczyć definicję bezpieczeństwa informacyjnego sformułowaną przez A. Bógdał-Brzezińską i M.F. Gawryckiego. Jest ono „działem bezpieczeństwa, uznającym wzrost roli informacji w podtrzymywaniu stabilności współczesnych gospodarek i systemów społecznych. Bezpieczeństwo informacyjne w szerszym wymiarze obejmuje zabezpieczanie przed atakiem sieciowym i skutkami takiego ataku fizycznego, który niósłby destrukcje dla funkcjonowania nowoczesnego państwa”[12]. Zmian w sposobie definiowania bezpieczeństwa informacyjnego oraz uwypuklania elementów niemilitarnych można doszukać się w transformacji społecznej, kulturowej, gdzie żywotną kwestią staje się dostęp do informacji oraz jej rzetelność i aktualność. Dostrzegalne jest to także w rozwoju nowych technologii umożliwiającym jednostce dostęp do informacji, co wymusiło określenie granic jej zabezpieczania. Przykładem takiego przedstawienia pojęcia jest sformułowana przez L. Korzeniowskiego definicja bezpieczeństwa informacyjnego podmiotu (człowieka lub organizacji), przez które należy rozumieć możliwość pozyskania dobrej jakości informacji oraz ochrony posiadanej informacji przed jej utratą”[13]. Można zauważyć, że zmiana sposobu definiowania obejmuje zmianę podmiotu bezpieczeństwa oraz wskazanie prawa do informacji dla tego podmiotu. Czyli metody zabezpieczające informację służą ochronie tego prawa, z zastrzeżeniem, że obejmuje ono prawo do rzetelnej informacji. Kolejnym przykładem definicji uwzględniającej element funkcjonowania podmiotu w sposób transpodmiotowy, gdzie informacja stanowi jeden z podstawowych zasobów nieodzownych dla sprawnego funkcjonowania tegoż podmiotu jest definicja J. Janczaka i A. Nowaka. Obecnie bezpieczeństwo informacyjne danego podmiotu jest traktowane nie odrębnie, lecz wielopłaszczyznowo z uwzględnieniem otoczenia (środowiska), które ma wpływ na poziom tego bezpieczeństwa, także z odwołaniem się do społeczeństwa informacyjnego. Za tak rozumianym bezpieczeństwem informacyjnym optują także E. Nowak i M. Nowak, uznając, że najistotniejszym czynnikiem jego zaistnienia są czynniki zewnętrzne wpływające na ten podmiot[14].

[12] A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 323.
[13] L. Korzeniowski, *Podstawy nauk o bezpieczeństwie*, Warszawa, s. 147.
[14] E. Nowak, M. Nowak, *Zarys teorii bezpieczeństwa narodowego*, Warszawa 2011, s. 103.

Definiowanie pojęcia bezpieczeństwa informacyjnego w ujęciu psychologicznym, związane jest głównie z systemem wartości i potrzebami człowieka, w tym z poczuciem jego bezpieczeństwa. W obszarze zainteresowań psychologów i badaczy interdyscyplinarnych znajduje się analiza przyczyn, rozwoju i następstw subiektywnego rozumienia bezpieczeństwa informacyjnego. Rozpatrywane są także zagrożenia z nim związane, m.in. manipulacja informacją, sterowanie zachowaniami, kształtowanie opinii, wywieranie wpływu czy manipulacja percepcją człowieka lub kolektywu. W ujęciu psychologicznym, pojęcie bezpieczeństwa informacyjnego odwołuje się do jego subiektywnie odczuwanego poczucia i umiejętności obiektywnego osądu sytuacji informacyjnych. To poczucie bezpieczeństwa jest podstawą efektywnego funkcjonowania jednostki, natomiast poczucie bezpieczeństwa informacyjnego jest podstawą efektywnego funkcjonowania jednostki w społeczeństwie informacyjnym. Naukowcy wskazują na takie czynniki kształtujące poczucie bezpieczeństwa informacji, jak tradycja i kultura lokalna, aktywność obywatelska, działalność na rzecz społeczeństwa, a także posiadana wiedza, doświadczenie i kompetencje umożliwiające analizę krytyczną informacji. Można wiec odwołać się do pojęcia kultury organizacyjnej rozpatrywanej na szczeblu społeczności lokalnej (ta perspektyw badawcza dotyczy analizy otoczenia podmiotu bezpieczeństwa). Pojęcie poczucia bezpieczeństwa informacyjnego można badać w perspektywie jednostkowej, ale też grupowej, zespołowej, kolektywnej, analizując poziom świadomości społecznej w danej organizacji. Ta świadomość społeczna może być koncentrowana na postrzeganiu bezpieczeństwa informacyjnego oraz umiejętności identyfikacji zagrożeń informacyjnych w środowisku.

Na bazie kolektywnej świadomości kształtowana jest opinia na rzecz potencjalnego zagrożenia, a następnie dobierana odpowiednia metoda przeciwdziałania jego negatywnym skutkom. Tak rozumiane kolektywne pojęcie „poczucia bezpieczeństwa informacyjnego" może być analizowane z perspektywy nauk o zarządzaniu i jakości[15]. Zakładając, że wszyscy członkowie danej organizacji tworzą kolektyw w ramach wspólnie realizowanego celu oraz bazują na zbiorze informacji, stanowiącym podstawowe aktywo organizacji. Na podstawie kolektywnej wiedzy i sposobów komunikacji kształtowana jest opinia i poczucie na temat zagrożeń

[15] T. Zarycki, *Świadomość jako wiedza o kontekście działania społecznego: od psychologii społecznej do sztucznej inteligencji*, [w:] W. Kulesza, H. Manzer (red.), *Rola świadomości w świecie ponowoczesnym*, Academica Wydawnictwo Akademickie SWPS, 2009, s. 171–186.

wewnętrznych i zewnętrznych względem organizacji i jej członków. Konsekwencją tego kolektywnego poczucia bezpieczeństwa informacyjnego jest sposób kolektywnej reakcji na te zagrożenia, motywacji do działania wspólnego na rzecz zapewnienia stanu bezpieczeństwa. W celu kształtowania obiektywnego poczucia bezpieczeństwa informacyjnego konieczne jest zapewnienie dostępu do informacji dla wszystkich członków oraz jednolite rozumienie bezpieczeństwa informacyjnego dzięki wdrażanym systemom zarządzania bezpieczeństwem informacji w organizacji.

Podsumowując, pojęcie „bezpieczeństwa informacyjnego" ewaluujące w świecie dynamicznych przemian cywilizacyjnych jest rozpatrywane w literaturze przedmiotu przez pryzmat wielu dziedzin naukowych. Rozważania dotyczą również wymiaru interdyscyplinarnego. Akcent rozważań został zmieniony z militarnego na niemilitarny, gdzie podmiot stanowi człowiek oraz społeczność, a nie wyłącznie państwo, i w którym bezpieczeństwo człowieka w relacji z informacją, a nie sama informacja (dane) staje się priorytetem. Wskazano na takie elementy jak dostęp do informacji spełniającej normy jakościowe.

W badaniach naukowych uzewnętrzniono różnorodność rozumienia pojęcia „bezpieczeństwo informacyjne", którego skuteczność zależy od sposobu funkcjonowania grupy (jednolitość, synergia, opinie, przekonania, oczekiwania). Różnorodność definiowania może stanowić przeszkodę w skutecznym działaniu grupy, jeżeli uzna ona za priorytet tylko ochronę danych i infrastruktury teleinformatycznej organizacji albo skoncentruje się tylko na bezpieczeństwie człowieka wchodzącego w relacje z informacją. Zrównoważone działania w obu tych obszarach uwzględniające obowiązujące przepisy, procedury i normy, których realizacja wynika z prawidłowego zarządzania systemem bezpieczeństwa informacyjnego, pozwolą organizacji na stworzenie bezpiecznego środowiska informacyjnego, a pracownikom zapewnią komfort funkcjonowania w obiektywnym poczuciu bezpieczeństwa informacyjnego. Poczucie bezpieczeństwa informacyjnego pracowników wynikające z pozytywnych ocen uzyskanych przez organizację w ramach zewnętrznego audytu SZBI wpływa na skuteczności działania firmy i jej konkurencyjność na rynku pracy. Konieczne jest podjęcie badań nad przyczynami i konsekwencjami wynikającymi z tych rozbieżności w perspektywie nauk o zarządzaniu i jakości.

Rozumienie pojęcia bezpieczeństwa informacyjnego przez pracodawcę i pracownika – studium przypadku

Rozumienie pojęcia „bezpieczeństwo informacyjne" przez członków organizacji, w tym identyfikacja rozbieżności i cech wspólnych jemu przypisanych, umożliwia skonkretyzowanie potrzeb organizacji w zakresie bezpieczeństwa informacyjnego. W przypadku braku zrozumienia konieczne są szkolenia nie tylko w zakresie ochrony informacji, ale też kształtowania świadomości informacyjnej pracowników. Do wykształcenia w członkach organizacji dojrzałych zachowań informacyjnych przyczyniają się kultywowane przez kulturę organizacyjną postawy i wartości przejawiane przez pracowników wobec informacji. Zachowania informacyjne odnoszą się do wszelkich aktywności członków organizacji związanych z poszukiwaniem, gromadzeniem, zabezpieczaniem, generowaniem, wykorzystywaniem i dzieleniem się informacją[16]. Należy założyć, że jeżeli zachowania informacyjne wynikają z potrzeb informacyjnych, to aby je zrealizować, pracownicy będą dążyć do podwyższania swoich kompetencji informacyjnych i będą dbać o jakość informacji organizacji oraz jej bezpieczeństwo. Dojrzałe zachowania informacyjne pracowników kształtowane są w atmosferze kultury informacyjnej, za której rozwój odpowiedzialna jest organizacja. Kultura informacyjna kadry kierowniczej i personelu przekłada się w dużej mierze na poczucie bezpieczeństwa informacyjnego wszystkich członków organizacji. Można założyć, że sposób rozumienia pojęcia „bezpieczeństwo informacyjne" stanowi swego rodzaju klucz do rozumienia i interpretowania elementów tego bezpieczeństwa i budowania z nich bezpiecznego środowiska informacyjnego. Dlatego zasadne jest przeprowadzenie identyfikacji sposobu rozumienia pojęcia „bezpieczeństwo informacyjne" z wyszczególnieniem poszczególnych elementów składowych badanego pojęcia. W ramach niniejszej pracy, autor wytypował obszar badawczy, jakim była organizacja. Populację badawczą stanowiło miasto Sucha Beskidzka (województwo małopolskie). Na podstawie identyfikacji wszystkich funkcjonujących na tym obszarze organizacji, nastąpiła ich kategoryzacja z wyszczególnieniem: administracji publicznej, usług, instytucji porządku publicznego. Z tej puli wytypowano dwie grupy respondentów – pracodawców i pracowników

[16] S. Cisek, *Zachowania informacyjne- wybrane aspekty*, Biuletyn EBIB, nr. 3 (173), 2017, s. 2–3.

organizacji. Dobór próby badawczej został uzasadniony chęcią zbadania grupy nadrzędnej w hierarchii organizacji, która jest odpowiedzialna za tworzenie norm, procedur, zarządzeń związanych z bezpieczeństwem informacji w organizacji (czyli pracodawców), a która tworzy je w oparciu o przedstawione definicje bezpieczeństwa informacyjnego. Drugą badaną grupę stanowili odbiorcy treści, norm, wykonawcy procedur ustanowionych przez kierownictwo czyli pracownicy. Dobór próby badawczej był celowy, nielosowy. Liczba respondentów stanowiła 49 osób. Wybraną przez autora metodą badawczą była metoda jakościowa, metoda sondażu diagnostycznego. Zastosowano metodę wywiadu eksperckiego, przeprowadzonego na podstawię opracowanego kwestionariusza wywiadu. Badanie zostało przeprowadzone w metodą jeden na jeden (badacz i respondent). Drugą metodą zastosowaną w niniejszej pracy było studium przypadku. Wybranym obszarem były organizacje funkcjonujące na terenie Suchej Beskidzkiej[17]. Celem niniejszej pracy była identyfikacja rozbieżności i cech wspólnych w rozumieniu pojęcia „bezpieczeństwo informacyjne" przez pracodawców i pracowników. Natomiast przedmiotem badań było bezpieczeństwo informacyjne. Głównym problemem badawczym było znalezienie odpowiedzi na pytanie jakie są rozbieżności i pokrewieństwa w rozumieniu pojęcia bezpieczeństwa informacyjnego przez pracowników i pracodawców oraz jakie są konsekwencje szerokiego lub wąskiego rozumienia przez respondentów pojęcia „bezpieczeństwo informacyjne"[18]. Przygotowane narzędzia badawcze miały na celu zapewnienie obiektywizmu. Przyjęte założenia teoretyczne i metodologiczne odnoszą się do nauk społecznych, jednakże zawierają także elementy interdyscyplinarne[19]. Przeprowadzone badania obejmują trzy obszary tematyczne.

Wytypowani respondenci mieli odpowiedzieć na pytanie (forma otwarta), jak rozumieją pojęcie bezpieczeństwa informacyjnego. Następnie mieli wskazać, czym się różni ono od bezpieczeństwa informatycznego. Następnie respondenci mieli wskazać, jak rozumieją pojęcie poczucie bezpieczeństwa informacyjnego. Po przeprowadzonych badaniach autor sformułował następujące wnioski:

[17] W. Grzegorczyk, *Studium przypadku jako metoda badawcza i dydaktyczna w naukach o zarządzaniu*, [w:] W. Grzegorczyk (red.), *Wybrane problemy zarządzania i finansów. Studia przypadków*, pod red. Łódź 2015, s. 9–11.

[18] A. Lipski, *Metody badań społecznych*, Prace naukowe, nr 149, 2012, s. 2–5.

[19] Ł. Sułkowski, *Metodologia nauk o zarządzaniu*, Przegląd Organizacji, nr 10 (777), 2004, s. 7–10.

1. Pierwsze pytanie o charakterze definicyjnym dotyczyło wskazania przez respondentów słów kluczowych, które identyfikują oni z pojęciem bezpieczeństwa informacyjnego. Pytanie zostało postawione w celu identyfikacji przez autora sposobu rozumienia pojęcia bezpieczeństwa informacyjnego. Respondenci zaliczeni do kategorii „kierownik" (dane pozyskane z metryki kwestionariusza wywiadu) wskazywali następujące słowa kluczowe (największy wskaźnik liczby powtarzających się słów kluczowych):
   - „bezpieczeństwo danych chronionych prawnie",
   - „zapewnienie ochrony informacji służbowych w sieci telekomunikacyjnej i mediach społecznościowych",
   - „zbiór procedur i systemów teleinformatycznych, które zapewniają jednostce ochronę baz danych i informacji".

   Natomiast w grupie respondentów zakwalifikowanych do grupy „pracownik" najczęściej powtarzającą się odpowiedzią były słowa:
   - „ochrona danych",
   - „ochrona przechowywanych w bazach danych informacji służbowych",
   - „zbiór procedur i systemów teleinformatycznych, które zapewniają jednostce ochronę baz danych i informacji".

   Natomiast w przypadku identyfikacji zagrożeń bezpieczeństwa informacyjnego, które w kolejnej części badania respondenci mieli za zadanie wskazać (celem pytania była analiza związku rozumienia bezpieczeństwa informacyjnego z potencjalnymi zagrożeniami) respondenci zaliczeni do grupy „kierownik" najczęściej zaliczali:
   - „ataki na infrastrukturę informacyjną",
   - „nie stosowanie się do procedur ochrony informacji",
   - „błąd człowieka".

   Z kolei wśród odpowiedzi respondentów z kategorii „pracownik" najczęściej wskazywanymi przez nich zagrożeniami były:
   - „ataki na bazy danych",
   - „ataki zewnętrzne na bazy danych",
   - „brak wsparcia ze strony kierownictwa w zakresie przeciwdziałania zagrożeniom bezpieczeństwa informacyjnego"[20].

[20] K. Batorowska, *Poczucie bezpieczeństwa informacyjnego w społeczności lokalnych w aspekcie wybranych zagrożeń cywilizacyjnych na przykładzie miasta Sucha Beskidzka*, praca doktorska, Uniwersytet w Siedlcach, Siedlce 2023, s. 215–216.

2. W drugiej części badania respondenci mieli wskazać słowa kluczowe, które utożsamiają z pojęciem poczucia bezpieczeństwa informacyjnego. W przypadku tej części badania respondenci również zostali podzieleni na kategorię pracowników i kierowników. Pytanie miało formę otwartą. W przypadku obu grup respondentów, odpowiedzi były tożsame z tymi wskazanymi w odniesieniu do wcześniejszego pytania. Należy zatem postawić wniosek, ze respondenci nie identyfikują różnic w rozumieniu tych dwóch pojęć[21].
3. W trzeciej części badania respondenci mieli wskazać rozbieżności i pokrewieństwa między pojęciami bezpieczeństwa informacyjnego a bezpieczeństwa informatycznego. Najczęściej udzielanymi odpowiedziami zarówno w grupie respondentów w kategorii „pracownik" i „kierownik" były:
   - „bezpieczeństwo systemów teleinformatycznych i infrastruktury informacyjnej",
   - „ochrona danych służbowych i osobowych",
   - „ochrona danych przed nieupoważnionym dostępem".

   Najczęściej respondenci podczas badania nie rozumieli odrębności pojęć, wskazując, że już udzielili odpowiedzi na wskazane pytanie[22].

   Jako główne wnioski po przeprowadzonym badaniu dotyczącym rozumienia pojęcia bezpieczeństwa informacyjnego należy wskazać:
   - pojęcie „bezpieczeństwo informacyjne" jest utożsamiane z poczuciem bezpieczeństwa informacyjnego i bezpieczeństwem informatycznym;
   - pojęcie „bezpieczeństwo informacyjne" jest utożsamiane przez wszystkich respondentów z ochroną danych, baz danych, infrastruktury teleinformatycznej;
   - zarówno przedstawiciele kategorii „kierownik", jak i „pracownik" wskazali nadrzędność procedur i norm obowiązujących w celu zapewnienia bezpieczeństwa informacyjnego;
   - następnie jako główny czynnik kształtowania bezpieczeństwa informacyjnego została wskazana ochrona baz danych, infrastruktury informacyjnej i systemów teleinformatycznych, co może również zostać uznane za potwierdzenie utożsamiania bezpieczeństwa informacyjnego z bezpieczeństwem informatycznym;

[21] Tamże, s. 218–219.
[22] Tamże, s. 220–223.

- w przypadku kadry kierowniczej najważniejsze są podstawy prawne dla zapewnienia bezpieczeństwa infrastruktury informacyjnej, natomiast pracownicy ich nie zidentyfikowali;
- w przypadku zagrożeń dla bezpieczeństwa informacyjnego w kategorii „kierownik" można wskazać na identyfikacje zagrożeń pochodzenia wewnętrznego, natomiast w przypadku kategorii „pracownik" takiej identyfikacji brak, natomiast zwrócono uwagę na problem ataków zewnętrznych na wewnętrzne zasoby informacyjne;
- w przypadku kategorii „pracownik" należy wskazać, że zostało zidentyfikowane jako zagrożenie brak wsparcia od kierownictwa dla pracowników w obszarze przeciwdziałania zagrożeniom bezpieczeństwa informacyjnego.

Podsumowując, rozumienie pojęcia „bezpieczeństwo informacyjne" przez wszystkich respondentów ogranicza się do ochrony infrastruktury informacyjnej i przestrzegania procedur i norm obowiązujących w sektorze bezpieczeństwa informacyjnego. Największym pokrewieństwem w rozumieniu tego pojęcia przez wszystkich badanych było utożsamianie go z strefą informatyczną, bez odwołania do strefy społecznej czy psychicznej. Natomiast w przypadku pracowników wskazano na potrzebę uzyskania gwarancji wsparcia od kierownictwa w zakresie przeciwdziałania zagrożeniom bezpieczeństwa informacyjnego, co sugeruje odwołanie się do potrzeby kształtowania kultury organizacyjnej opartej na zasadzie wsparcia i zaufania. Natomiast tej kwestii nie wskazała kadra kierownicza. Można więc sformułować wniosek, że dla kadry kierowniczej najważniejszą kwestią jest zgodność działań z obowiązującą podstawą prawną, wypracowanymi procedurami i normami oraz ochrona infrastruktury informacyjnej.

Natomiast pracownicy oczekują zmiany w postrzeganiu bezpieczeństwa informacyjnego w organizacji, co sugeruje odmienność ich potrzeb w tym zakresie. Ta rozbieżność może stanowić płaszczyznę umożliwiającą rozwój organizacji i jej kultury organizacyjnej lub przestrzeń podatności na zagrożenia wewnętrzne i zewnętrzne. W przypadku kultury organizacyjnej należy wskazać, że kadra kierownicza wskazała pracownika jako potencjalne zagrożenie dla bezpieczeństwa informacyjnego, co sugeruje, że potrzeba umacniania zaufania w organizacji jest jednostronna. Zapewnienie bezpieczeństwa informacyjnego w wyniku kontroli przestrzegania nakazów, przepisów i procedur, oznacza preferowanie systemu kar i eliminowanie dialogu, dzięki któremu możliwy jest rozwój. Konkludując, rozumienie pojęcia bezpieczeństwa informacyjnego przez obie grupy

respondentów jest dalekie od ustaleń naukowców i ekspertów w dziedzinie bezpieczeństwa informacyjnego.

Podsumowanie

Rozumienie pojęcia bezpieczeństwa informacyjnego przez pryzmat bezpieczeństwa infrastruktury informacyjnej i ochrony zasobu informacyjnego nie stanowi odpowiedzi na wyzwania, przed jakimi stoi współczesna organizacja, a wynikających z globalizacji, przemian cywilizacyjnych i tempa rozwoju technologii informacyjno-komunikacyjnych. W literaturze przedmiotu wskazano, że przemiany społeczne stanowią podstawę kształtowania nowych wyzwań dla bezpieczeństwa informacyjnego zwłaszcza wynikających z popularności mediów społecznościowych. Następnie wskazano, że clue bezpieczeństwa informacyjnego obecnie zajmuje człowiek/jednostka, która poprzez wykształcenie dojrzałych zachowań informacyjnych wpływa na stan bezpieczeństwa informacyjnego. Jednym z czynników wpływających na bezpieczeństwo informacyjne jest psychika człowieka i jego umiejętność krytycznej analizy informacji. Przeniesienie centrum uwagi badaczy bezpieczeństwa informacyjnego na człowieka jest uzasadnione, ale niedocenione przez respondentów biorących udział w badaniu. Należy wskazać, że rozbieżności w rozumieniu bezpieczeństwa informacyjnego dotyczą: potrzeb pracowników skierowanych do kadry kierowniczej oraz potrzeb kierownictwa, które własne poczucie bezpieczeństwa informacyjnego traktuje nadal w sposób subiektywny, pomimo zidentyfikowanych współczesnych zagrożeń, czego konsekwencją jest niezabieganie o rozwój świadomości informacyjnej i społecznej pracowników. Reasumując, zostały zidentyfikowane rozbieżności i pokrewieństwa w rozumieniu wskazanego pojęcia. Zdiagnozowano niewystarczający poziom świadomości istnienia zagrożeń dla bezpieczeństwa informacyjnego, brak możliwości porozumienia i nawiązania współpracy pomiędzy wszystkimi członkami organizacji w celu przeciwdziałania tym zagrożeniom. Skrytykowano sposób motywowania pracowników do respektowania procedur bezpieczeństwa informacyjnego opartych na systemie kar, z pominięciem rozwijania kultury bezpieczeństwa informacyjnego[23].

[23] H. Batorowska, *Kultura bezpieczeństwa informacyjnego w środowisku walki o przewagę informacyjną*, Kraków 2021, s. 383.

Bibliografia

Literatura:

Batorowska H., *Kultura bezpieczeństwa informacyjnego w środowisku walki o przewagę informacyjną*, Kraków 2021.

Batorowska K., *Poczucie bezpieczeństwa informacyjnego w społeczności lokalnych w aspekcie wybranych zagrożeń cywilizacyjnych na przykładzie miasta Sucha Beskidzka*, praca doktorska, Uniwersytet w Siedlcach, Siedlce 2023.

Bezpieczeństwo informacyjne, cyberbezpieczeństwo i ochrona prywatności – Systemy Zarządzania Bezpieczeństwem Informacji – Wymagania. ISO-IEC 27001:2022 Akademia TÜV NORD POLSKA 2023.

Bógdał-Brzezińska A., Gawrycki M.F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Oficyna Wydawnicza ASPRA-JR, Warszawa 2003.

Cieślarczyk M., *Relacje między bezpieczeństwem i obronnością w kontekście wąskiego i szerokiego rozumienia tych zjawisk*, [w:] Elementy teorii i praktyki transdyscyplinarnych badań problemów bezpieczeństwa, t. 6: W poszukiwaniu relacji między bezpieczeństwem a obronnością, J. Ważniewska (red.), Wydawnictwo UPH, Siedlce 2017.

Cisek S., *Zachowania informacyjne- wybrane aspekty*, Biuletyn EBIB, nr 3 (173), 2017.

Frei D., *Sicherheit, Grundfragen der Weltpolitik*, Kohlhammer, Stuttgart 1997.

Grzegorczyk W., *Studium przypadku jako metoda badawcza i dydaktyczna w naukach o zarządzaniu, w Wybrane problemy zarządzania i finansów. Studia przypadków*, pod red. W. Grzegorczyk, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2015.

Korzeniowski L., *Podstawy nauk o bezpieczeństwie*, Warszawa.

Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2008.

Lipski A., *Metody badań społecznych*, Prace naukowe, Uniwersytet Ekonomiczny w Katowicach, nr 149, 2012.

Maslow A., *Motywacja i osobowość*, Warszawa 1990.

Nowak E., Nowak M., *Zarys teorii bezpieczeństwa narodowego*, Warszawa 2011.

Potejko P., *Bezpieczeństwo informacyjne*, [w:] K.A. Wojtaszczyk, A. Materska-Sosnowska (red.), *Bezpieczeństwo państwa*, Warszawa 2009.

Sułkowski Ł., *Metodologia nauk o zarządzaniu*, Przegląd Organizacji, nr 10 (777), 2004.

Wolfers A., *Discord and Collaboration. Essays on International Politics*, Johns Hopkins Press, Baltimore 1962.

Zarycki T., *Świadomość jako wiedza o kontekście działania społecznego: od psychologii społecznej do sztucznej inteligencji*, [w:] W. Kulesza, H. Manzer (red.), *Rola*

świadomości w świecie ponowoczesnym, Academica Wydawnictwo Akademickie SWPS, 2009.

Źródła internetowe:

Bezpieczeństwo informacyjne państwa, strona Biura Bezpieczeństwa Narodowego, https://www.bbn.gov.pl/pl/form/dodaj3,MINI-Slownik-BBN-Propozycje-nowych--terminow.html, (dostęp: 06.10.2024).

Bezpieczeństwo, Mini słownik BBN, strona główna Biura Bezpieczeństwa Narodowego, https://www.bbn.gov.pl/pl/form/dodaj3,MINI-Slownik-BBN-Propozycje-nowych--terminow.html, (dostęp: 06.10.2024).

Kultura organizacyjna, strona Encyklopedia Zarządzania, https://mfiles.pl/pl/index.php/Kultura_organizacyjna (dostęp: 06.10.2024).

Świadomość społeczna, strona Encyklopedia PWN, https://encyklopedia.pwn.pl/haslo/;3984380, (dostęp: 06.10.2024).