KWARTALNIK PEDAGOGICZNY 2024
NUMER IV(274)
ISSN 0023-5938; e-ISSN 2657-6007

https://doi.org/10.31338/2657-6007.kp.2024-4.7

Andrzej Bogdański
Akademia Sztuki Wojennej[*]
E-mail: a.bogdanski@akademia.mil.pl
ORCID: 0000-0002-3443-0741

Kształcenie i doskonalenie żołnierzy w zakresie cyberbezpieczeństwa w Siłach Zbrojnych Rzeczypospolitej Polskiej: analiza wpływu rozwoju technologii informatycznych[**]

Summary

SOLDIER TRAINING AND DEVELOPMENT IN CYBERSECURITY IN THE POLISH ARMED FORCES: ANALYSIS OF THE IMPACT OF TECHNOLOGICAL ADVANCEMENTS[**]

This research investigates how the increasing number of basic and specialised IT services, along with technical-organisational solutions and command support systems, influences the training and development of soldiers in the Signal and IT troops regarding cybersecurity. Conducted during exercises such as Brama Mazowsza, Świder, Twierdza, Brama, and major drills like Dragon and Anakonda, the study includes observations and interviews from workshops codenamed Aster. The practical aim was to identify potential changes in training methods due to the implementation and expansion of ICT systems. The study highlights how converging telecommunication and computer networks onto a unified IP platform impacts training processes. It discusses the skills required for military IT specialists and examines the determinants affecting training in Signal and IT units. The research question addressed was: What are the differences between civilian and military IT training? Findings suggest integrating specialised commercial courses into training programmes, emphasising practical aspects such as attack simulations. Recommendations include establishing help desk and service desk units and enhancing integration between stationary and mobile transmission segments. These findings are crucial for strengthening national cybersecurity resilience amid growing hybrid threats.

---

[*] Adres: Aleja Generała Antoniego Chruściela „Montera" 103, 00-910 Warszawa
[**] Finansowanie publikacji: Uniwersytet Warszawski

Keywords: training of military IT specialists, development of military IT specialists; training and development in cybersecurity; signal; help desk; service desk

Wstęp

Wieloletnie obserwacje, wywiady z ekspertami, przeprowadzone przeze mnie badania podczas największych ćwiczeń z wojskami (w latach 2015–2018) są źródłem prezentowanych tu refleksji i wniosków na temat kształcenia żołnierzy w zakresie cyberbezpieczeństwa. W czasie ćwiczeń zrealizowałem obserwację bez interwencji, nie brałem udziału w eksploatacji usługi teleinformatycznych, natomiast przygotowywałem wdrożenie i monitorowałem system teleinformatyczny w zakresie bezpieczeństwa. Proces obserwacji okazał się przydatny w zakresie określenia stopnia wykorzystania usług teleinformatycznych oraz wpływu ich rozwoju na kształcenie i doskonalenie żołnierzy w omawianym tu zakresie. Obserwacje pozwoliły mi pozyskać materiał badawczy i realizowałem je w ramach ćwiczeń pod kryptonimem: Dragon-15, Anakonda-16, Dragon-17, Anakonda-18. Natomiast wywiady z ekspertami przeprowadziłem w ramach ćwiczeń studyjnych organizowanych przez Akademię Sztuki Wojennej w latach 2022–2024. Mowa o ćwiczeniach pod kryptonimem: Świder-22, Brama Mazowsza-22, Twierdza-23, Świder-23, Brama-23, Twierdza-24. Wywiady z ekspertami pozwoliły mi dokonać korekty programów kształcenie i doskonalenie w zakresie cyberbezpieczeństwa kierowniczej kadry dowódczej Sił Zbrojnych Rzeczypospolitej Polskiej. Ponieważ zmieniały się okoliczności wywiadu posługiwałem się wywiadem niestandaryzowanymi, zadając tylko jedno lub kilka pytań wcześniej niezaplanowanych, a wynikających z przebiegu sytuacji badawczych (Kwieciński, Śliwerski, 2006, s. 40).

W przywołanych już tu ćwiczeniach brali udział słuchacze oficerowie starsi w stopniu majora, którzy w ramach Kursów Dowódców Batalionów i Wyższych Kursów Sztabowych zostali przygotowani do stanowisk zaszeregowanych do stopnia podpułkownik. Wywiady z ekspertami były realizowane w sposób jawny z pełną świadomością celu zadawanych pytań przez udzielających odpowiedzi. Zakres pytań dotyczył sposobu przygotowania przyszłych podwładnych, żołnierzy informatyków do realizacji postawionych zadań. Badania od 2022 r. miały charakter uczestniczący. Podczas ćwiczeń studyjnych byłem opiekunem doradcą słuchaczy w zakresie łączności informatyki oraz cyberbezpieczeństwa. Doświadczona kadra oficerska zwłaszcza oficerowie pełniący służbę na stanowiskach szefów sekcji dowodzenia i łączności pułków i brygad oraz na stanowiskach zastępców dowódców batalionów dowodzenia posiada szereg doświadczeń, na bazie których sformułowano poniższe wnioski. Wywiady były realizowane indywidualnie oraz w małych grupach 3–4 osobowych, co pozwoliło mi dokonać konfrontacji poglądów

ekspertów. Podczas prowadzenia badań w latach 2015–2018 zgodnie z decyzją nr 68/MON Ministra Obrony Narodowej z dnia 6 marca 2014 r., zmieniającą decyzję w sprawie prowadzenia badań społecznych w resorcie obrony narodowej, posiadałem upoważnienie/zgodę Ministra Obrony Narodowej (Decyzja…, 2014, s. 2), Dowódcy Generalnego Rodzajów Sił Zbrojnych oraz organizatora systemów teleinformatycznych Komendanta Centrum Wsparcia Systemów Dowodzenia Dowództwa Generalnego Rodzajów Sił Zbrojnych. Natomiast prowadzenie badań naukowych w tym wywiadów przez nauczycieli akademickich w ramach ćwiczeń studyjnych organizowanych przez Akademię Sztuki Wojennej nie wymagało specjalnej zgody.

Prezentowana przez mnie problematyka wymagała zapoznania się z już istniejącymi publikacjami z zakresu kształcenia i doskonalenia w Siłach Zbrojnych Rzeczypospolitej Polskiej. Zagadnienia zawarte w tym artykule były wcześniej poruszane w literaturze przedmiotu m.in. przez Zbigniewa Leśniewskiego (zob. 2020, 2021) oraz Mirosława Laskowskiego (2016) w tekście *Treści szkolenia w Siłach Zbrojnych Rzeczypospolitej Polskiej*, który ukazał się w monografii *Edukacja jutra. Oferta edukacyjna odpowiedzią na problemy współczesności* (Leśniewski, 2020, s. 179), a także w rozdziale *Kierunki rozwoju Sił Zbrojnych i ich implikacje szkoleniowe*, wydanym w monografii *Edukacja zorientowana na ucznia i studenta* (Leśniewski, 2021, s. 145–166), tego samego autora. Obszerne dzieło dotyczące systemu kształcenia *Modele kształcenia a przystosowanie zawodowe młodych oficerów Wojska Polskiego* opracował Mirosław Laskowski (2016, s. 13).

Wymienione tu publikacje przedstawiają ogólny program kształcenia w Siłach Zbrojnych Rzeczypospolitej Polskiej oraz wpływ kierunków rozwoju SZRP na kształcenie żołnierzy w odniesieniu do wszystkich korpusów i grup osobowych. Jednak nie odnoszą się do systemu kształcenia i doskonalenia żołnierzy wojsk łączności i informatyki. Ten artykuł jest w pewnym stopniu próbą wypełnienia tej luki.

Nieodzowne stało się więc zadanie sobie pytania: czym jest kształcenie żołnierzy? *Nowy słownik pedagogiczny* Wincentego Okonia definiuje kształcenie jako system działań zmierzający do tego, aby uczącej się jednostce lub zbiorowej jednostce umożliwić poznanie świata włącznie z nauką, sztuką i techniką; przygotowanie do zmieniania świata poprzez rozwinięcie kwalifikacji fizycznych i umysłowych, zdolności i uzdolnień; kształtowanie indywidulanej osobowości (Okoń, 1998, s. 382). Według internetowej encyklopedii PWN kształcenie to ogół czynności i procesów umożliwiających ludziom poznanie. Proces kształcenia opiera się na nauczaniu i uczeniu się (encyklopedia.pwn.pl, 2024).

W odniesieniu do szkolenia żołnierzy warto przytoczyć definicję kształcenia obronnego Bogdana Szulca. Zakłada on, że kształcenie obronne to proces obejmujący ogół czynności nauczających (nauczycieli, instruktorów, dowódców itp.) i uczących się (uczniów, studentów, pracowników, żołnierzy, policjantów itp.), prowa-

dzących do opanowania przez tych drugich określonego zasobu wiedzy obronnej oraz nabycia umiejętności i nawyków w zakresie określonej działalności obronnej, a także rozwinięcia i nich zdolności, zainteresowań, postaw, przekonań i poglądów związanych z szeroko rozumianą obronnością w celu czynnego uczestnictwa w państwowym oraz w regionalnych systemach obronnych (Huzarski, Wołejszo, 2014, s. 195). Mamy definicję kształcenia obronnego. Czym zatem jest kształcenie żołnierzy czy też dydaktyka wojskowa? Współcześnie pod pojęciem dydaktyka rozumieć można kształcenie i samokształcenie (Pilch, 2003, s. 797). Przyjmuję więc, że: kształcenie w Siłach Zbrojnych Rzeczypospolitej Polskiej to zespół czynności i proces początkowy, prowadzący do opanowania wiedzy. Dokształcanie zaś, także w ramach samokształcenia, to doskonalenie żołnierzy, w procesie czy też poprzez cykl procesów, pozwalających pogłębić i pozyskać dalszą wiedzę teoretyczną oraz umiejętności praktyczne z określonej dziedziny. Tematyka kształcenia kandydatów i żołnierzy zawodowych w Siłach Zbrojnych Rzeczypospolitej Polskiej regulowana jest przez odpowiednie przepisy, w tym przede wszystkim przez Ustawę z 11 marca 2022 r. o obronie ojczyzny, która wyróżniała kształcenie kandydatów do zawodowej służby wojskowej i doskonalenie żołnierzy w różnych formach realizowane w centrach i ośrodkach szkolenia. Kształcenie kandydatów do zawodowej służby wojskowej oraz żołnierzy zawodowych odbywa się w:

- uczelniach wojskowych w przypadku kształcenia na potrzeby korpusu oficerów zawodowych;
- centrach szkolenia w przypadku kształcenia na potrzeby korpusu oficerów zawodowych absolwentów studiów wyższych posiadających tytuł zawodowy magistra lub równorzędny, w ramach kursu oficerskiego;
- szkołach podoficerskich w przypadku kształcenia na potrzeby korpusu podoficerów zawodowych;
- ośrodkach szkolenia lub centrach szkolenia w przypadku kształcenia na potrzeby korpusu szeregowych zawodowych (Ustawa…, 2024, s. 82). Niemniej jednak przedmiotowa ustawa stwierdza, że kształcenie może odbywać się również w uczelniach wyższych, szkołach i ośrodkach szkolenia innych niż wojskowe.

Zasadniczym celem kształcenia jest przygotowanie kandydatów na oficerów do dowodzenia (kierowania) i realizacji zadań na pierwszym stanowisku służbowym w warunkach pokojowego funkcjonowania Sił Zbrojnych Rzeczypospolitej Polskiej (SZ RP), kryzysu i wojny. Powyższy akt prawny stanowi ogólny zarys podstaw prawnych kształcenia w Siłach Zbrojnych Rzeczypospolitej Polskiej (Decyzja…, 2020, s. 2).

Wiedza i umiejętności z zakresu cyberbezpieczeństwa powinny być, moim zdaniem, wymagane u wszystkich żołnierzy, a zwłaszcza tych służących w batalionach dowodzenia, co wielokrotnie podkreślałem w czasie zajęć z kandydatami na dowódców batalionów. Z badań realizowanych przeze mnie podczas największych ćwiczeń

wojskowych wynika, że głównym zadaniem specjalistycznego batalionu dowodzenia jest osiąganie, a także doskonalenie zdolności do zabezpieczenia funkcjonowania stanowiska dowodzenia oraz rozwinięcie i eksploatacja teleinformatycznych systemów wsparcia dowodzenia. Na podstawie analizy dokumentów, wywiadów oraz obserwacji, stwierdziłem, że w batalionach dowodzenia nie występowali żołnierze specjaliści korpusu osobowego kryptologii czy cyberbezpieczeństwa (Rozporządzenie…, 2022, s. 22), a jedynie żołnierze korpusu osobowego łączności i informatyki. Byli to żołnierze wyznaczeni na etaty w Zespołach Wsparcia Teleinformatycznego oraz wybrani żołnierze obsługujący aparatownie: Węzły Teleinformatyczne, Zintegrowane Węzły Teleinformatyczne, Ruchome Węzły Łączności Cyfrowej, Przenośno-przewoźne Terminale Satelitarne, obsługi radiostacji, ponadto etaty specjalistyczne administratorów występowały w wybranych batalionach dowodzenia w nowo powstałych drużynach administratorów. Warunkiem bezpieczniej eksploatacji teleinformatycznych systemów wsparcia dowodzenia jest odpowiednie przygotowanie żołnierzy wojsk łączności i informatyki, także w zakresie cyberbezpieczeństwa. Rzetelna wiedza teoretyczna oraz umiejętności praktyczne specjalistów łączności czy informatyki pozwalały także zdobyć kompetencje w zakresie cyberbezpieczeństwa.

Celem artykułu było określenie wpływu zwiększającej się liczby informatycznych usług podstawowych i dedykowanych, a także rozwiązań techniczno-organizacyjnych systemów wsparcia dowodzenia na proces kształcenia i doskonalenie żołnierzy wojsk łączności i informatyki w zakresie cyberbezpieczeństwa.

Jako cel praktyczny (Pelc, 2012, s. 15) przyjąłem określenie prawdopodobnego kierunku zmiany w sposobie kształcenia i doskonalenie w aspekcie wdrażania i rozbudowy systemów teleinformatycznych oraz eksploatowanych usług. Przedstawiłem umiejętności jakie powinni osiągnąć specjaliści informatycy wojskowi w celu skutecznej realizacji zadań, scharakteryzowałem dobre praktyki wykorzystywane w systemie wsparcia teleinformatycznego helpdesk i service desk.

Celem poznawczym było zidentyfikowanie determinantów wpływających na procesy kształcenia i doskonalenie specjalistycznego wojsk łączności i informatyki w jednostkach liniowych.

Problem badawczy zawarłem w pytaniu: Jakie były różnice między kształceniem i doskonaleniem informatyków w środowisku cywilnym, a wojskowych?

Środowisko wojskowe a środowisko cywilne

Według opinii ekspertów kształcenie i doskonalenie specjalistów informatyków w środowisku wojskowym i cywilnym różni się głównie kontekstem i specyficznymi wymaganiami, wynikającymi z charakteru realizowanych zadań. To, co odróżnia śro-

dowisko wojskowe to dobór kandydatów, który jest pierwszym etapem (Laskowski, 2018, s. 50). W środowisku wojskowym priorytetem jest bezpieczeństwo narodowe. Kształcenie informatyków w wojsku obejmuje specjalistyczne zagadnienia z zakresu cyberbezpieczeństwa, obrony przed atakami cybernetycznymi oraz bezpiecznej wymiany informacji. Z moich badań wynika, że zagadnienia te nie są realizowane systemowo, a jedynie w ramach doskonalenia. Informatycy w wojsku mogą być zaangażowani w specjalistyczne dziedziny, takie jak komunikacja satelitarna, analiza danych wywiadowczych, czy też projektowanie systemów wspierających operacje wojskowe. Wojskowi specjaliści informatycy muszą przestrzegać surowych zasad etycznych i prawnych, zwłaszcza w kontekście bezpieczeństwa. Służba w siłach zbrojnych jest ściśle regulowana przepisami dotyczącymi tajemnicy państwowej. Wojskowi informatycy przygotowywani są do pracy w warunkach polowych i gotowi są do szybkiej reakcji na zmieniające się sytuacje. To wymaga umiejętności dostosowania się do różnych środowisk pracy. Kształcenie i doskonalenie wojskowych informatyków obejmuje często korzystanie z wysoko specjalizowanych narzędzi i technologii, które są dostosowane do unikalnych wymagań wojskowych. Wojskowi informatycy muszą rozumieć strukturę organizacyjną i procesy decyzyjne w ramach sił zbrojnych, co jest kluczowe dla efektywnej integracji technologii z celami operacyjnymi. Wojskowi informatycy mogą uczestniczyć w doskonaleniu w warunkach bojowych i symulacjach, tak aby przetestować ich umiejętności w warunkach zbliżonych do rzeczywistych. W opinii autora kształcenie należy rozpocząć od solidnych podstaw w dziedzinie informatyki, w tym systemów operacyjnych, sieci komputerowych, baz danych. Specjaliści informatycy powinni być zaznajomieni z najnowszymi technologiami i trendami w dziedzinie informatyki.

Formy kształcenia i doskonalenia

Kształcenie i doskonalenia specjalistów wojsk łączności i informatyki na potrzeby poprawy bezpieczeństwa cyberprzestrzeni SZ RP realizowane jest systemowo w odniesieniu do specjalności wojskowej w korpusie łączności i informatyki. Bardzo ważnym czynnikiem powinien być dobór właściwych kandydatów. Mowa tu o absolwentach techników elektroniczno-informatycznych w specjalnościach: programista, informatyk, teleinformatyk, mechatronik, automatyk czy elektronik. W mojej ocenie tak wyselekcjonowani kandydaci powinni zostać poddani kształceniu w wojskowych ośrodkach kształcenia.

Uczelnia wojskowa przygotowuje oficerów do objęcia pierwszego stanowiska służbowego oraz daje podwaliny do dalszego rozwoju i awansu na kolejne stopnie wojskowe. Jednak przygotowanie do pełnienia bardziej odpowiedzialnych funk-

cji wymaga niezbędnego doświadczenia, które każdy oficer może nabyć dopiero podczas praktycznego wykonywania obowiązków na kolejnych stanowiskach służbowych. Należy przy tym pamiętać, że wysoka specjalizacja pracy, różnorodność sprzętu, pełne uzawodowienie oraz wielokierunkowość działań dowódców czynią proces przygotowania kadry oficerskiej bardziej skomplikowanym, rozciągniętym w czasie i realizowanym coraz częściej w zmieniających się warunkach. W czasie rekrutacji oraz selekcji kandydatów na żołnierzy zawodowych stosowane są reguły określone przez resort, a sam proces kształcenia przyszłych oficerów stara się nadążyć za aktualnymi potrzebami polskich sił zbrojnych usiłując sprostać nowym wyzwaniom własnej oraz sojuszniczej strategii bezpieczeństwa (Gutt, 2011, s. 98).

Od młodego oficera wymaga się także zdolności do samokształcenia, pogłębiania wiedzy specjalistycznej oraz umiejętności niezbędnych na zajmowanym stanowisku. Powinien on też wyróżniać się niezbędną wiedzą specjalistyczną w zakresie pozwalającym na wykorzystanie możliwości bojowych powierzonego sprzętu oraz prowadzenie bieżącej obsługi technicznej tego sprzętu. Widać zatem, że sylwetka osobowo-zawodowa absolwenta uczelni wojskowej, obejmuje wzajemnie uzupełniające się wiedzę i umiejętności, kwalifikacje oraz kompetencje zawodowe i społeczne, umożliwiające funkcjonowanie w przestrzeni różnych kultur (Sikora, 2015, s. 455).

Główną rolę w kształceniu i doskonaleniu przyszłych i obecnych kadr, według mnie, powinny odgrywać ośrodki wojskowe, które można podzielić na uczelnie wyższe, szkoły podoficerskie, centra i ośrodki kształcenia. Do uczelni wyższych zaliczono: Akademię Sztuki Wojennej, Wojskową Akademię Techniczną, Akademię Marynarki Wojennej, Lotniczą Akademię Wojskową i Akademię Wojsk Lądowych. Podczas prowadzenia badań w zakresie kształcenia i doskonalenia z obszaru cyberbezpieczeństwa poddałem analizie kształcenie i doskonalenie w wybranych szkołach podoficerskich: Szkoła Podoficerska Wojsk Lądowych w Poznaniu, Szkoła Podoficerska Sił Powietrznych w Dęblinie, Szkoła Podoficerska Marynarki Wojennej w Ustce, Szkoła Podoficerska Żandarmerii Wojskowej w Mińsku Mazowieckim, Szkoła Podoficerska Wojsk Specjalnych i Szkoła Podoficerska Sonda w Zegrzu i Toruniu. Ponadto w czasie prowadzenia badań funkcjonowały: Centrum Szkolenia Wojsk Lądowych w Poznaniu, Centrum Szkolenia Wojsk Inżynieryjnych i Chemicznych we Wrocławiu, Centrum Szkolenia Artylerii i Uzbrojenia w Toruniu, Centrum Szkolenia Sił Powietrznych w Koszalinie, Centrum Szkolenia Inżynieryjno-Lotniczego w Dęblinie, Centrum Szkolenia Marynarki Wojennej w Gdyni, Centrum Szkolenia Wojsk Specjalnych w Krakowie, Wojskowe Centrum Kształcenia Medycznego w Łodzi, Centrum Szkolenia Artylerii i Uzbrojenia w Toruniu i Centrum Szkolenia Łączności i Informatyki w Zegrzu.

W związku z wysoką specjalizacją ośrodków wojskowych scharakteryzuję jedynie wybrane studia i kursy w Wydziale Wojskowym Akademii Sztuki Wojennej

w Warszawie, Wojskowej Akademii Technicznej w Warszawie i Centrum Szkolenia Łączności i Informatyki w Zegrzu.

Kształcenie i doskonalenie kadry oficerskiej

Akademia Sztuki Wojennej kształciła studentów cywilnych oraz doskonaliła żołnierzy słuchaczy studiów podyplomowych i słuchaczy kursów kwalifikacyjnych. Wyższy Kurs Sztabowy przeznaczony był dla kandydatów na stanowisko oficera sztabowego szczebla taktycznego oraz operacyjnego – strategicznego o stopniu etatowym podpułkownika. Celem kursu było przygotowanie oficerów do objęcia stanowisk służbowych w strukturach dowództw i sztabów SZ RP, natomiast celem Kursu Dowódców Batalionów było przygotowanie oficerów do objęcia stanowisk dowódców batalionów, równorzędnych (Joniak, 2022, s. 5). Słuchacze Wyższego Kursu Sztabowego oraz Kursu Dowódców Batalionów w ciągu czteromiesięcznego cyklu doskonalenia realizowali dziesięć godzin zajęć z cyberbezpieczeństwa, w tym cztery godziny wykładów i sześć godzin ćwiczeń. Tematyka cyberbezpieczeństwa poruszana była także na zajęciach z łączności i informatyki, a specjaliści korpusów osobowych łączności i informatyki oraz kryptologii i cyberbezpieczeństwa w obrębie przedmiotu dowodzenie rodzajami wojsk dodatkowo realizowali tematykę cyberbezpieczeństwa w wymiarze dodatkowych 30 godzin ćwiczeń. W ramach badań poddałem analizie specjalistyczną ofertę Wydziału Wojskowego, który kształcił także studentów cywilnych na poziomie studiów I i II stopnia na kierunkach: dowodzenie i obronność oraz doskonalenie na studiach podyplomowych ochrona i bezpieczeństwo cyberprzestrzeni. W toku specjalistycznego kształcenia na studiach pierwszego stopnia na kierunku dowodzenie, studenci przyswajali wiedzę z zakresu cyberbezpieczeństwa w ramach przedmiotu elementy wsparcia teleinformatycznego w dowodzeniu, realizowanym w wymiarze łącznym 40 godzin: 10 godzin wykładu i 30 godzin ćwiczeń (Pilarski, 2023, s. 2). Natomiast w zakresie specjalistycznego kształcenia na studiach pierwszego stopnia na kierunku obronność, studenci przyswajali wiedzę dotyczącą cyberbezpieczeństwa na przedmiotach: podstawy bezpieczeństwa architektury systemów teleinformatycznych oraz podstawy sieci i systemów teleinformatycznych łącznie w wymiarze 60 godzin, w tym: 20 godzin wykładów i 40 godzin ćwiczeń, także w trybie niestacjonarnym (Zawadzki, 2020, s. 2). Natomiast celem kształcenia na studiach podyplomowych na kierunku ochrona i bezpieczeństwo cyberprzestrzeni było przygotowanie:

> […] wojskowych, cywilnych kadr z obszaru cyberbezpieczeństwa do rozwiązywania problemów w dziedzinie bezpieczeństwa przetwarzanej informacji na poszczególnych poziomach dowodzenia, jak również kierowania państwa. Na specjalistycznych studiach podyplomowych

w ramach modułu podstawowego słuchacze realizują zajęcia z przedmiotów: systemy i sieci teleinformatyczne, informatyczne wspomaganie procesów decyzyjnych, działania hybrydowe w cyberprzestrzeni (Stolarz, 2023, s. 15).

Ponadto w zestawieniu studiów podyplomowych i kursów realizowanych w Akademii Sztuki Wojennej można było odnaleźć tygodniowy kurs dla operatorów systemu symulacyjnego JTLS[1] oraz 5-dniowy specjalistyczny kurs administratorów technicznych i scenariusza ćwiczenia w module wspomagającym zarządzanie ćwiczeniem JEMM[2].

Wojskowa Akademia Techniczna (WAT) kształciła w ramach studiów cywilnych, wojskowych i podyplomowych. W obrębie studiów cywilnych I stopnia najwięcej zagadnień związanych z cyberbezpieczeństwem zawierały programy studiów na kierunku informatyka następujące specjalności: informatyczne systemy zarządzania, internetowe technologie multimedialne, kryptologia, mobilne systemy komputerowe, sieci teleinformatyczne i systemy informatyczne. W programie studiów wojskowych o kierunku informatyka występowały trzy specjalności: kryptologia, sieci teleinformatyczne i systemy informatyczne. Warto wspomnieć o studiach na poziomie I i II stopnia w pokrewnym kierunku elektronika i telekomunikacja o specjalności systemy informatyczne.

W ofercie studiów podyplomowych sugerowanych oficerom młodszym przez Wojskową Akademię Techniczną najwięcej zagadnień związanych z cyberbezpieczeństwem zawierały programy studiów z zakresu organizacji i eksploatacji systemów informacyjnych dla oficerów przewidzianych do objęcia stanowisk specjalistycznych w zakresie eksploatacji systemów informacyjnych.

Natomiast w toku kursów organizowanych przez Wojskową Akademię Techniczną najwięcej zagadnień związanych z cyberbezpieczeństwem zawierał program kursu eksploatacja systemów łączności i informatyki. Kurs był przeznaczony dla oficerów zajmujących stanowiska w Sekcji Wsparcia Dowodzenia i Łączności w sztabie brygady. Godny zainteresowania był miesięczny kurs administracja sieciami teleinformatycznymi i zarządzanie bazami danych, przeznaczony dla żołnierzy zawodowych korpusu osobowego łączności i informatyki, którzy zajmowali stanowiska w pionie szczególnym. Przydatny w zakresie cyberbezpieczeństwa był także kurs z zakresu eksploatacji systemów teleinformatycznych i administrowania sieciami dla żołnierzy korpusu osobowego łączności i informatyki zajmujących stanowiska administratorów. Wartościowy w zakresie cyberbezpieczeństwa był także kurs Systemy łączności i informatyki Sił Zbrojnych Rzeczypospolitej Polskiej przeznaczony dla oficerów młodszych korpusu osobowego łączności i informatyki

[1] Mowa o systemie symulacji pola walki JTLS – Joint Theatre Level Simulation.

[2] Mowa o usłudze podawania wiadomości JEMM – Joint Exercise Management Module.

zajmujących stanowiska w pionie sztabowym i zabezpieczenia. Cenny w kontekście cyberbeprbezpieczeństwa był miesięczny kurs kwalifikacyjny z zakresu budowy wojskowych systemów łączności i informatyki, przeznaczony dla oficerów z wykształceniem II stopnia, którzy byli planowani do objęcia stanowisk zaszeregowanych do stopnia etatowego majora w korpusie osobowym łączności i informatyki w grupie osobowej technicznej.

Kształcenie i doskonalenie kadry podoficerskiej

Równie istotne jak szkolenie oficerów było kształcenie i doskonalenie kadry podoficerskiej. Z przeprowadzonych przeze mnie badań wynika, że prym w kształceniu i doskonaleniu podoficerów w zakresie cyberbezpieczeństwa wiodło Centrum Szkolenia Łączności i Informatyki w Zegrzu. Głównym zadaniem Centrum było kształcenie i doskonalenie kadr łączności na potrzeby Sił Zbrojnych RP:

- żołnierzy zawodowych i pracowników wojska na kursach doskonalenia zawodowego;
- żołnierzy służby przygotowawczej;
- słuchaczy studium oficerskiego;
- słuchaczy szkoły podoficerskiej;
- studentów Wydziału Elektroniki i Cybernetyki WAT – udział w kształceniu;
- studentów Wydziału Mechatroniki Akademii Marynarki Wojennej – udział w kształceniu.

Najbardziej wartościowe pod względem wiedzy teoretycznej i umiejętności praktycznych z obszaru cyberbezpieczeństwa były kursy doskonalące z zakresu administracji sieciami teleinformatycznymi dla administratorów sieci teleinformatycznych oraz kursy doskonalące, dotyczące podstaw administracji systemami operacyjnymi Windows. Z moich obserwacji wynika, że kursy podstawowe powinny być realizowane dla wszystkich specjalistów informatyki, a kolejne kursy specjalistyczne, dla konkretnej, wyselekcjonowanej grupy. Zakres wiedzy powinien być ściśle powiązany z konkretną specjalnością.

Doskonalenie żołnierzy na kursach komercyjnych

W trakcie prowadzenia badań Centrum Szkolenia Łączności i Informatyki w Zegrzu w znaczniej części zmodyfikowało swoją propozycję kształcenia. Nie miało jednak wystarczającej kompleksowej oferty kursów specjalistycznych, dlatego doskonalenie żołnierzy odbywało się także w ramach kursów komercyjnych. Priorytetem stały się kursy z zakresu rozwiązań opartych o technologie firmy Cisco oraz

kursy oparte o technologie firmy Microsoft, ukierunkowane na eksploatację usług oferowanych w wojskowych systemach teleinformatycznych (Bogdański, Zelichowski, 2013, s. 5). W zakresie technologii Cisco Centrum oferowało szereg certyfikacji skoncentrowanych na różnych obszarach sieci komputerowych. Wybór właściwego kursu zależał od konkretnych zadań żołnierzy. Oto kilka popularnych certyfikacji.

Cisco Certified Network Associate to podstawowa certyfikacja, która była skierowana głównie do osób na początku kariery w dziedzinie sieci komputerowych. Kurs obejmował podstawy konfiguracji, obsługi i utrzymania sieci Cisco. Zaawansowane kursy są realizowane nie tylko w oparciu o ośrodki komercyjne, ale także o Eksperckie Centrum Szkolenia Cyberbezpieczeństwa.

Cisco Certified Network Professional – Certyfikacja dla średniozaawansowanych specjalistów sieciowych.

Dostępne były także kursy, takie jak Routing and Switching, Security, Data Center itp. Cisco Certified Internetwork Expert (CCIE) to jedna z najbardziej zaawansowanych certyfikacji Cisco. CCIE koncentrował się na zaawansowanych umiejętnościach projektowania, implementacji i utrzymania rozległych sieci Cisco.

Natomiast najbardziej zaawansowany kurs z zakresu cyberbezpieczeństwa Cisco Certified CyberOps Associate potwierdzał wiedzę i umiejętności potrzebne zespołom Security Operations Center do wykrywania zagrożeń cyberbezpieczeństwa i reagowania na nie. Egzamin z CyberOps Associate obejmował wiedzę i umiejętności związane z koncepcjami bezpieczeństwa, monitorowaniem bezpieczeństwa, analizą opartą na hostach, analizą włamań do sieci oraz politykami i procedurami bezpieczeństwa.

Badania własne pokazały niewystarczalność ofert kształcenia. Na przykład w Centrum Szkolenia Łączności i Informatyki w Zegrzu propozycja kończyła się na kursach podstawowych. W ograniczonym także zakresie Centrum realizowało kursy z technologii Microsoft. Na rynku komercyjnym ośrodki doskonalenia oferowały różnorodne kursy, zarówno online, jak i w formie tradycyjnych kursów, obejmujące obszar zarządzania systemami, chmurą, aplikacjami oraz rozwoju oprogramowania. Oto kilka podstawowych kursów i certyfikacji Microsoft, które mogłyby być interesujące dla różnych profesjonalistów cyberbezpieczeństwa: Microsoft Certified Azure Fundamentals – certyfikacja dla osób, które chcą zdobyć podstawową wiedzę na temat platformy chmurowej Microsoft Azure. Modern Desktop Administrator Associate – certyfikacja dla specjalistów zajmujących się administracją systemów Windows w środowisku korporacyjnym. Microsoft Certified Azure Administrator Associate to pogłębienie wiedzy dla administratorów chmury, obejmuje umiejętności z zakresu konfiguracji, zarządzania i monitorowania usług w Azure. Na kurs Microsoft 365 Certified Modern Desktop Administrator Associate powinni być skierowani specjaliści Cyber zajmujący się konfiguracją, zarządzaniem

i zabezpieczaniem środowiska Microsoft 365. Ponadto kluczowa jest wiedza z zakresu bezpieczeństwa cybernetycznego, skupiająca się na detekcji i reagowaniu na incydenty.

Biorąc pod uwagę szeroki wachlarz form kształcenia na początek drogi, rekomenduję kursy w dwóch podstawowych obszarach: rozwiązań sieciowych i systemowych w oparciu o produkty Cisco oraz kursy z systemów serwerowych i usług Microsoft. Uzupełnieniem powinny być rozwiązania z zakresu wirtualizacji, jeśli nie są oparte na rozwiązaniach Microsoft (Bogdański, Barański, 2014, s. 167). W każdym z tych obszarów można wyróżnić podobszary technologii i poziomy.

Budowana przez ostatnie dziesięciolecia sieć łączności i informacji Sił Zbrojnych RP składa się z różnych elementów oferujących alternatywne usługi i wykorzystujących różne rodzaje transmisji. W ostatnich latach czas poświęcony na misje stabilizacyjne i budowania pokoju pokazał, jak ważne jest posiadanie zintegrowanego systemu łączności, który oferowałby wysoki poziom funkcjonalności, a także opierałby się na niewielkiej ilości sprzętu, a tym samym wymagałby mniejszej liczby personelu operacyjnego do jego obsługi. Na współczesnych polach walki spotykamy się z coraz nowocześniejszymi technologiami, które pozwalają nam świadczyć usługi informacyjno-komunikacyjne na najwyższym poziomie, np. technologia transmisji oparta na podejściu połączeniowym – Multiprotocol Label Switching Transport Profile. Umożliwia tworzenie inteligentnych połączeń punkt–punkt, wprowadza zarządzanie jakością usług, ochronę procesu etykietowania oraz kompleksową administrację i zarządzanie (Bogdański, Sielwanowski, 2014, s. 86).

Ponadto badania wykazały, że potrzeby szkoleń były nieporównywalnie większe niż możliwości wojskowych ośrodków kształcenia i doskonalenia kadr. Z moich badań wynika, że nie wszyscy żołnierze spełniają minimalne wymagania w zakresie podstawowej wiedzy technicznej. Wydajnym i skutecznym rozwiązaniem może być pozyskanie kandydatów z korpusu szeregowych zawodowych. Jak pokazały badania, ograniczeniem w doskonaleniu była ścieżka kariery w korpusie oficerów dowódcy plutonów dowodzenia po trzyletniej kadencji na stanowisku musieli uzupełnić wiedzę pozyskaną podczas studiów, ponieważ realizowane obowiązki służbowe spowodowały, że ich wiedza była mocno nieaktualna, a umiejętności nabyte w procesie kształcenia wymagały praktyki. W przypadku korpusu podoficerów zaobserwowałem inne przyczyny. W mojej ocenie powodem słabego wykształcenia podoficerów był krótki 12-miesięczny okres przygotowania podoficera. W trakcie badań realizowanych podczas ćwiczeń i certyfikacji oraz warsztatów spotkałem bardzo małą grupę absolwentów dwuletniej Szkoły Chorążych Wojsk Łączności i Informatyki w Zegrzu oraz dwu- i trzyletniej Szkoły Chorążych Wojsk Łączności z Legnicy. Niemniej jednak porównanie wiedzy teoretycznej i umiejętności praktycznych obecnych absolwentów szkół podoficerskich z wiedzą i doświadczeniem

oraz umiejętnościami absolwentów dwu- i trzyletnich szkół chorążych okazało się korzystne dla absolwentów zlikwidowanych szkół chorążych.

Wnioski z ćwiczeń

Cennym źródłem obserwacji w zakresie umiejętności praktycznych był dla mnie proces przygotowań do największych ćwiczeń w Wojsku Polskim w latach 2016–2023 oraz ich realizacja w zakresie wsparcia teleinformatycznego. Żołnierze specjaliści informatycy w ramach ćwiczeń pod kryptonimami Anakonda-16, Dragon-17, Anakonda-18 pełnili rolę Service desk i Sieciowego Centrum Operacyjnego Network Operations Center. Powołano Organizację Zarządzania Usługami. Ćwiczenia pod kryptonimem Anakonda-16 i Anakonda-18 pozwoliły zaobserwować relacje administratorów poziomu organizatora systemu z administratorami lokalnymi. Współpraca wymagała szczegółowego instruowania tych ostatnich. Przełożeni zauważyli potrzebę kursów zarówno podstawowych, jak i specjalistycznych oraz zgrywających w zakresie cyberbezpieczeństwa. Jak wynika z badań, w pierwszym etapie należy w ramach batalionów dowodzenia brygad powołać komórki helpdesk, a w batalionach dowodzenia dywizji także service desk, które powinny realizować zadania z zakresu zarządzania incydentami, zarządzania problemami oraz zarządzania zmianą i konfiguracją. W ramach service desk u działającego na rzecz stanowiska dowodzenia dywizji należy stworzyć punkt kontaktowy.

W kolejnym etapie w zależności od charakteru i zadań jednostki wojskowej należy rozważyć powołanie kolejne komórki odpowiedzialnej za zarządzanie poziomem usług, zarządzanie dostępnością i zarządzanie przepustowością. W mojej opinii podejście do budowy komórek wsparcia teleinformatycznego zgodnie z Information Technology Infrastructure Library (ITIL) pozwoli w dalszej perspektywie osiągnąć znaczącą poprawę wydajności i efektywności w realizacji postawionych zadań.

Dobre praktyki

Systemy teleinformatyczne eksploatowane w ramach misji oraz na ćwiczeniach dostarczały usługi zgodnie z ideą Federated Mission Networking, wspieraną przez Technology for Information, Decision and Execution Superiority. Idea Federated Mission Networking (Bogdański, 2022, s. 49–67) opierała się na kodeksie postępowania dla działów informatyki, tj. Information Technology Infrastructure Library (ITIL). Zgodnie z ITIL możliwa była:

- automatyzacja procesów obsługi zgłoszeń;
- przetwarzanie wsadowe, które umożliwiało wykonanie pewnych obciążeń w zaplanowanym czasie;

- planowanie zadań IT wykonywanych we właściwym czasie, uwzględniające potrzeby związane z obsługą procesów, automatyzacja systemów otwartych, serwerów i baz danych;
- zagadnienia związane z redukcją ilości zadań wykonywanych ręcznie, aby usprawnić obsługę procesów;
- monitorowanie proaktywne w perspektywie usług;
- przeniesienie zadań zarządzanych centralne z helpdesk pierwszego poziomu do service desk oraz wykorzystanie możliwości lepszej współpracy żołnierzy.

Rzetelna wiedza teoretyczna oraz umiejętności praktyczne żołnierzy powinny być wspierane przez specjalistyczne oprogramowanie, czego przykładem jest oprogramowanie IT Service Management Software.

Podsumowanie

Badania były realizowane podczas procesów kształcenia i doskonalenia kandydatów i czynnych żołnierzy zawodowych w ramach ćwiczeń studyjnych Brama Mazowsza, Świder, Twierdza, Brama oraz podczas największych – w Siłach Zbrojnych Rzeczpospolitej Polskiej – ćwiczeń z wojskami pod kryptonimami Dragon i Anakonda. Realizowane przez mnie obserwacje oraz wywiady, także podczas warsztatów wojsk łączności i informatyki pod kryptonimem Aster, bezpośrednio poprzedzały największe ćwiczenia prowadzone przez Dowództwo Generalnie i Dowództwo Operacyjne Rodzajów Sił Zbrojnych.

Celem badań było określenie wpływu zwiększającej się liczby informatycznych usług podstawowych i dedykowanych, a także rozwiązań techniczno-organizacyjnych systemów wsparcia dowodzenia na proces kształcenia i doskonalenia żołnierzy wojsk łączności i informatyki w zakresie cyberbezpieczeństwa. Zwiększone wykorzystywanie technologii informatycznych w działaniach bojowych było naturalnym krokiem ewolucji. Wcześniej niezależne, galwanicznie oddzielone sieci telekomunikacyjne i komputerowe obecnie dzięki platformie IP konwergują do jednej wspólnej sieci teleinformatycznej. Coraz bardziej zyskuje na znaczeniu problematyka wsparcia procesu dowodzenia. Zwiększająca się liczba usług teleinformatycznych i technologii miała kluczowy wpływ na ewolucję procesów kształcenia i doskonalenia. Jako cel praktyczny artykułu przyjąłem określenie prawdopodobnego kierunku zmiany w sposobie kształcenia i doskonalenia w aspekcie wdrażania i rozbudowy systemów teleinformatycznych oraz eksploatowanych usług.

Na podstawie przeprowadzonych badań nasuwa się wniosek, że uzupełnieniem form kształcenia i doskonalenia w ramach resortu obrony narodowej powinny być kursy i doskonalenia komercyjne. W związku z tym przedstawiłem umiejęt-

ności, jakie powinni osiągnąć specjaliści informatycy wojskowi w celu skutecznej realizacji zadań, scharakteryzowałem dobre praktyki wykorzystywane w systemie wsparcia teleinformatycznego helpdesk i service desk. Celem poznawczym było zidentyfikowanie determinantów wpływających na procesy kształcenia i doskonalenia specjalistycznego wojsk łączności i informatyki w jednostkach liniowych. Problem badawczy sprecyzowałem formułując następujące pytanie: Jakie były różnice między kształceniem i doskonaleniem wojskowych a informatyków w środowisku cywilnym? Z przeprowadzonej analizy wynika, że kształcenie i doskonalenie informatyków w środowisku cywilnym i wojskowym różniło się specyficznymi wymaganiami wynikającymi z charakteru zadań, jakie były stawiane żołnierzom. W środowisku wojskowym priorytetem jest bezpieczeństwo.

Na podstawie badań doszedłem do wniosku, że kształcenie i doskonalenie informatyków na potrzeby resortu obrony narodowej powinno obejmować specjalistyczne zagadnienia z zakresu cyberbezpieczeństwa, obrony przed atakami cybernetycznymi oraz bezpiecznej wymiany informacji. Jak wynika z przeprowadzonych przeze mnie badań, te zagadnienia nie były realizowane systemowo, a jedynie w ramach doskonalenia. Wojskowi informatycy często muszą przestrzegać surowych zasad etycznych i prawnych, szczególnie w kontekście bezpieczeństwa, a zwłaszcza obronności. Służba w siłach zbrojnych jest ściśle regulowana przepisami dotyczącymi tajemnicy państwowej. Kształcenie i doskonalenie wojskowych informatyków obejmuje często korzystanie z wysoko specjalizowanych narzędzi i technologii, które są dostosowane do wyjątkowych wymagań wojskowych. Według mnie kształcenie należy rozpoczynać od dostarczenia solidnych podstaw w dziedzinie informatyki, w tym systemów operacyjnych, sieci komputerowych, baz danych. Specjaliści informatycy powinni być zaznajomieni z najnowszymi technologiami i trendami w dziedzinie informatyki. W ramach badań dokonałem analizy kształcenia i doskonalenia kandydatów na żołnierzy w kontekście administrowania eksploatacją usług informatycznych podczas ćwiczeń, z naciskiem na zagadnienia związane z cyberbezpieczeństwem. Wynikające z badań wnioski wskazują na konieczność zorganizowania kursów specjalistycznych, prowadzonych przez ekspertów w zakresie cyberbezpieczeństwa, a w pierwszej kolejności przeprowadzenia kursów obejmujących podstawowe zagadnienia cyberbezpieczeństwa, takie jak identyfikacja zagrożeń, analiza ryzyka, zabezpieczenia sieciowe.

Następny etap to wprowadzenie w zagadnienia związane z bezpieczeństwem informacji i ochroną danych. W dalszej kolejności rekomenduję przeprowadzenie kursów specjalistycznych, obejmujących obszary, takie jak penetrowanie systemów, detekcja intruzów, analiza malware'u, zarządzanie zdarzeniami bezpieczeństwa. Jak również poszerzenie oferty o elementy praktyczne, takie jak symulacje ataków, laboratoria praktyczne i scenariusze, aby umożliwić specjalistom zdobycie praktycznego doświadczenia.

W wymiarze praktycznym, w pierwszym etapie należałoby w ramach batalionów dowodzenia brygad powołać komórki helpdesk, a w batalionach dowodzenia dywizji, także service desk, które powinny realizować zadania z zakresu zarządzania incydentami, zarządzania problemami oraz zarządzania zmianą i konfiguracją. W ramach service desk u działającego na rzecz stanowiska dowodzenia dywizji należy stworzyć punkt kontaktowy. W kolejnym etapie w zależności od charakteru i zadań jednostki wojskowej należałoby rozważyć powołanie kolejne komórki odpowiedzialnej za zarządzanie poziomem usług, zarządzanie dostępnością i zarządzanie przepustowością. W mojej opinii podejście do budowy komórek wsparcia teleinformatycznego zgodnie z ITIL, pozwoli w dalszej perspektywie osiągnąć znaczącą poprawę wydajności i efektywności w realizacji postawionych zadań. W zakresie cyberbezbezpieczeństwa kluczowym dla specjalistów wojsk łączności i informatyki będzie rozwijanie zdolności do efektywnego wykorzystania bezpiecznego dzierżawionego stacjonarnego potencjału zarządzanego przez Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni. Osiągnięcie zdolności do integracji stacjonarnego i mobilnego segmentu transmisyjnego poprzez budowę punktów dostępowych na węzłach łączności. Rozwijanie zdolności umożliwiających współpracę komórek wsparcia teleinformatycznego jednostek liniowych z organizatorami eksploatowanych systemów teleinformatycznych. Zaprezentowane tu wyniki badań są według mnie szczególnie istotne dla podnoszenia odporności państwa w zakresie cyberbezpieczeństwa, ze względu na nowe wyzwania stawiane przed Siłami Zbrojnymi Rzeczypospolitej Polskiej w zakresie zagrożeń hybrydowych, zwłaszcza w domenie cyberprzestrzennej.

References

Bogdański, A. (2022). Federated Mission Networking w ujęciu narodowych dokumentów doktrynalnych: aspekt bezpieczeństwa teleinformatycznego. W: M. Marczyk, M. Stolarz, B. Terebiński (red.), *Bezpieczeństwo działań w cyberprzestrzeni: wybrane aspekty*, t. 2. *Techniczne aspekty cyberprzestrzeni* (s. 49–68). Warszawa: Wydawnictwo Akademii Sztuki Wojennej.

Bogdański, A., Sielwanowski, M. (2014). Information and Communication Networks of Modern Battlefield, Security Forum 2014 (s. 86–96). Banska Bystrica: Univerzita Mateja Bela v Banskej Bystricy,

Bogdański, A., Barański, Ł. (2014). Wybrane rozwiązania oraz usługi wdrożone w sieciach teleinformatycznych Wojsk Lądowych. *Bezpieczeństwo i Administracja – Zeszyty Naukowe Wydziału Bezpieczeństwa Narodowego Akademii Obrony Narodowej*, 1(1), 167–180.

Bogdański, A., Zelichowski, A. (2013). Możliwości wykorzystania wojskowych sieci informatycznych w celu prowadzenia badań społecznych w resorcie obrony narodowej. *Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia*, 2, 5–19.

Decyzja nr 68/MON Ministra Obrony Narodowej z dnia 6 marca 2014 r. zmieniająca decyzję w sprawie prowadzenia badań społecznych w resorcie obrony narodowej. Dziennik Urzędowy Ministra Obrony Narodowej, 2014 poz. 78.

Decyzja nr 88/MON Ministra Obrony Narodowej z dnia 30 czerwca 2020 r. w sprawie Standardu Kształcenia Wojskowego dla kandydatów na oficerów – minimalne wymagania programowe. Dziennik Urzędowy Ministra Obrony Narodowej, 2020 poz. 107.

Gutt, P. (2011). Dobór kadr oficerskich w Wojskach Lądowych SZRP jako przykład realizacji wybranego elementu funkcji personalnej w organizacji publicznej. *Współczesne Zarządzanie*, 1, 97–105.

Huzarski, M., Wołejszo, J. (red.). (2014). *Leksykon obronności Polska i Europa*. Warszawa: Wydawnictwo Bellona.

Joniak, J. (red.). (2022). *Program szkolenia Wyższy Kurs Sztabowy (WKS)*. Warszawa: Wydawnictwo Akademii Sztuki Wojennej.

Kwieciński, Z., Śliwerski, B. (red.). (2006). *Pedagogika. Podręcznik akademicki*, t. 1. Warszawa: Wydawnictwo Naukowe PWN.

Laskowski, M. (2016). *Modele kształcenia, a przystosowanie zawodowe młodych oficerów Wojska Polskiego*. Warszawa: Wydawnictwo Difin.

Laskowski, M. (2018). *System kształcenia oficerów Siłach Zbrojnych RP*. Warszawa: Wydawnictwo Akademii Sztuki Wojennej.

Leśniewski, Z. (2020). Treści szkolenia w Siłach Zbrojnych Rzeczypospolitej Polskiej. W: A. Kamińska-Małek, P. Oleśniewicz (red.), *Edukacja jutra. Oferta edukacyjna odpowiedzią na problemy współczesności*, t. 1 (s. 169–181). Warszawa: Wydawnictwo Akademii Sztuki Wojennej.

Leśniewski, Z. (2021). Kierunki rozwoju Sił Zbrojnych i ich implikacje szkoleniowe. W: A. Karpińska, W. Wróblewska, P. Remża (red.), *Edukacja zorientowana na ucznia i studenta* (s. 145–166). Białystok: Wydawnictwo Uniwersytetu w Białymstoku.

Okoń, W. (1998). *Nowy słownik pedagogiczny*. Warszawa: Wydawnictwo Akademickie Żak.

Pelc, M. (2012). *Elementy metodologii badań naukowych*. Warszawa: Wydawnictwo Akademii Obrony Narodowej.

Pilarski, G. (2023). *Karta przedmiotu Elementy wsparcia teleinformatycznego w dowodzeniu*. Warszawa: Wydawnictwo Akademii Sztuki Wojennej.

Pilch, T. (red.). (2003). *Encyklopedia pedagogiczna XXI wieku*. Warszawa: Wydawnictwo Akademickie Żak.

Rozporządzenie Ministra Obrony Narodowej z dnia 13 czerwca 2022 r. w sprawie korpusów osobowych, grup osobowych i specjalności wojskowych. Dz. U. 2022 poz.1333 (2020) (Polska).

Sikora, K. (2016). *Kompetencje społeczne dowódców pododdziałów wojskowych*. Warszawa: Wydawnictwo Wojskowe Centrum Edukacji Obywatelskiej.

Stolarz, M. (2023). *Program studiów 'Ochrona i bezpieczeństwo cyberprzestrzeni'*. Warszawa: Wydawnictwo Akademii Sztuki Wojennej.

Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny. Dz. U. 2024 poz. 248.

Zawadzki, T. (2020). *Karty przedmiotów Podstawy bezpieczeństwa architektury systemów teleinformatycznych i Podstawy sieci i systemów teleinformatycznych*. Warszawa: Wydawnictwo Akademii Sztuki Wojennej.