

# Andrzej Kowalski

---

## Analiza zarządzania systemami teleinformatycznymi w rejonie odpowiedzialności zespołu zarządzania wsparciem teleinformatycznym – administratorzy

---

Obronność - Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej nr 3(7), 98-112

---

2013

Artykuł został opracowany do udostępnienia w internecie przez Muzeum Historii Polski w ramach prac podejmowanych na rzecz zapewnienia otwartego, powszechnego i trwałego dostępu do polskiego dorobku naukowego i kulturalnego. Artykuł jest umieszczony w kolekcji cyfrowej [bazhum.muzhp.pl](http://bazhum.muzhp.pl), gromadzącej zawartość polskich czasopism humanistycznych i społecznych.

Tekst jest udostępniony do wykorzystania w ramach dozwolonego użytku.

AUTOR

plk mgr inż. Andrzej Kowalski  
zzwpkowalski@wp.mil.pl

## **ANALIZA ZARZĄDZANIA SYSTEMAMI TELEINFORMATYCZNYMI W REJONIE ODPOWIEDZIALNOŚCI ZESPOŁU ZARZĄDZANIA WSPARCIEM TELEINFORMATYCZNYM – ADMINISTRATORZY**

Łączność i informatyka zarówno w Siłach Zbrojnych RP, jak i środowisku cywilnym rozwijają się bardzo dynamicznie. To co wydaje się dzisiaj szczytem techniki to w krótkim czasie, nawet kilku miesięcy staje się przestarzałe. Nowe systemy teleinformatyczne zastępują stare, które bardzo szybko zdeaktywizują się, jeden świat informatyczny zamieniany jest na nowy.

Trwają rewolucyjne zmiany, a w tym wszystkim funkcjonują administratorzy sieci i systemów informatycznych (zwani w dalszej części administratorami), którzy odgrywają znaczącą rolę w tych przemianach. Muszą oni uczestniczyć we wszystkich aspektach przemian zachodzących w informatyce, modernizacji sieci informatycznych i właściwym ich zarządzaniu.

Aby nadażyć za rozwojem informatyki, konieczne są ciągle nowe inwestycje zarówno w sprzęt komputerowy, jak i bardzo kosztowne szkolenia ludzi, którzy odgrywają decydującą rolę w poszczególnych systemach tych nowoczesnych organizacji. Bez specjalistycznych szkoleń, sam sprzęt nie rozwiąże problemów, które ujawniają się w trakcie eksploatacji i modernizacji współczesnych systemów teleinformatycznych. Informatyzacja jest bardzo kosztowna, jednak ponoszone koszty opłacają się i sprawdza się to zarówno w działalności bieżącej, jak i wsparciu informatycznym organizowanych ćwiczeń i treningów sztabowych.

Ważną rolę w zarządzaniu sieciami informatycznymi stacjonarnymi i polowymi odgrywają administratorzy, którzy również biorą udział we wdrażaniu oprogramowania oraz szkoleniu użytkowników. Zabezpieczają ćwiczenia i treningi sztabowe. Każde ćwiczenie, czy trening wymusza opracowanie koncepcji zabezpieczenia go pod względem informatycznym. Aby system informatyczny funkcjonował poprawnie, niezbędne jest właściwe zaplanowanie tego systemu, co z kolei jest za każdym razem nowym wyzwaniem dla administratorów.

Przy dużym zgraniu współpracy administratorów na poszczególnych szczeblach dowodzenia odnoszone są sukcesy. Podkreślić trzeba, iż

współczesna teleinformatyka to ściśle współdziałanie administratorów-informatyków z łącznościowcami. Ćwiczenia i treningi sztabowe są sprawdzianem dla spięcia i prawidłowego zadziałania systemów polowych ze stacjonarnymi.

Administratorzy w dziedzinie administrowania zarówno systemami stacjonarnymi, jak i polowymi muszą być bardzo dobrze przygotowani do realizacji wielu trudnych zadań. Moim zdaniem, nie można dobrze zarządzać systemami informatycznymi, skupiając się tylko na zarządzaniu polowymi lub tylko stacjonarnymi systemami. Podobnie nie można oddzielić od siebie informatyki wojskowej od cywilnej, one się ze sobą zazębiają. Dobry zespół administratorów to tylko taki, który posiada i rozwija nieustannie swoją wiedzę z zakresu obu systemów.

Z moich obserwacji wynika, że w działalności bieżącej administratorzy-informatycy w wojsku przegrywają z łącznościowcami (są mniej doceniani) – szkoda, bo obie dziedziny powinny być traktowane na równi, jedna bez drugiej nie jest w stanie funkcjonować. Oczywiście jest to, że informatyków licznie jest zdecydowanie mniej niż łącznościowców i może jest to jedna z przyczyn takiego stanu. Mało słyszymy o zasługach odniesionych przez administratorów informatyków np. na odprawach w podsumowaniu zakończonych ćwiczeń czy treningów sztabowych, słyszy się tylko „dziękujemy łącznościowcom za włożony trud i pracę...”. O administratorach zapomina się, a przecież bez nich systemy informatyczne nie działałyby poprawnie, ćwiczenia i treningi sztabowe nie osiągnęłyby zakładanych celów.

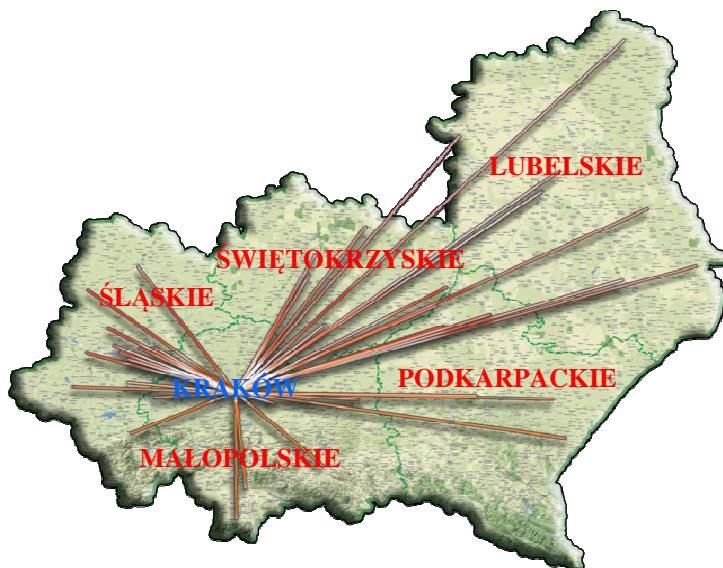
Jest to duży błąd dowódców, szefów czy komendantów. Nie docenianie administratorów i ich pracy, może doprowadzić do sytuacji, że najlepsi opuszczą Siły Zbrojne RP i przejdą do firm komercyjnych.

Firmy komercyjne informatyczne są dużą konkurencją dla wojska w dziedzinie kadrowo-finansowej, oferują o wiele wyższe stawki płacowe i często korzystniejsze warunki pracy. Sytuacja taka stanowi jedno z największych zagrożeń dla obsady stanowisk informatycznych. Teraz w dobie kryzysu wydaje się to nie mieć większego znaczenia, jednak jest to złudne wrażenie. Informatycy powinni mieć stworzoną drogę rozwoju zarówno pod względem szkoleniowym, jak i również finansowym, aby nie mogli być podkupieni przez konkurencję. A z tą drogą rozwoju jest różnie. Aktualnie w Siłach Zbrojnych występuje deficyt informatyków zwłaszcza w korpusie oficerów młodszych.

Moim zdaniem, trzeba objąć szczególną ochroną informatyków-administratorów, jak to można określić „z krwi i kości”.

Na podstawie zrealizowanych badań przeprowadzono analizę problematyki zarządzania systemami teleinformatycznymi rejonu południowo-

wschodniej części Polski, obejmującego 5 województw: świętokrzyskie, śląskie, małopolskie, lubelskie i podkarpackie<sup>1</sup>.



Źródło: opracowanie własne.

**Rys. 1. Rejon kraju objęty analizą**

Na 216 jednostek i instytucji wojskowych stacjonujących w rejonie, analizą objęto 202 jednostki i instytucje wojskowe, co łącznie stanowi 93,5%.

Celem analizy jest przedstawienie:

- wykorzystywania systemów i sieci teleinformatycznych wspomagających proces dowodzenia i działalność bieżącą jednostek i instytucji wojskowych;
- znaczenia administratorów zarządzających tymi systemami i sieciami teleinformatycznymi.

Administratorzy w skali sił zbrojnych stanowią niewielką grupę. Bardzo często są niedoceniani przez swoich przełożonych. Ich codzienna praca, zwykle, gdy sieć lub system teleinformatyczny działają prawidłowo, jest niezauważalna. Dopiero gdy sieć lub system teleinformatyczny pracują niepoprawnie lub nie działają, zaczynają się poszukiwania administratorów.

Wykorzystanie narzędzi informatycznych do automatyzacji procesu dowodzenia jest jednym z ważniejszych celów w strategii informatyzacji resortu Obrony Narodowej, a tym samym rola administratorów sieci i systemów informatycznych będzie nabierała coraz ważniejszego znaczenia.

---

<sup>1</sup> Badania przeprowadzono w drugiej połowie 2012 roku. Materiały z badań w zasobach Autora.

W objętych analizą 202 jednostkach i instytucjach wojskowych łącznie wyznaczonych jest 368 administratorów (etatowo lub nieetatowo). Z pozoru liczba ta wydaje się wystarczająca, jednak w praktyce i zarządzaniu systemami informatycznymi występuje wiele mankamentów opisanych szczegółowo w dalszej części artykułu.

**Tabela 1. Zestawienie podziału administratorów systemu MIL-WAN objętych analizą**

<b>ADMINISTRATORZY SYSTYEMU MIL-WAN</b>	
<b>GRUPA ZAWODOWA</b>	<b>ILOŚĆ</b>
<b>ADMINISTRATOR ETATOWY</b>	
I. Żołnierze zawodowi	
1. Mężczyźni	9
2. Kobiety	0
II. Pracownicy wojska	
1. Mężczyźni	16
2. Kobiety	0
<b>RAZEM:</b>	<b>25</b>
<b>ADMINISTRATOR NIEETATOWY</b>	
I. Żołnierze zawodowi	
1. Mężczyźni	85
2. Kobiety	0
II. Pracownicy wojska	
1. Mężczyźni	92
2. Kobiety	8
<b>RAZEM:</b>	<b>185</b>
<b>OGÓLEM:</b>	<b>210</b>

Źródło: opracowanie własne.

**Tabela 2. Zestawienie podziału wszystkich administratorów systemów teleinformatycznych objętych analizą**

<b>ADMINISTRATORZY WSZYSTKICH SYSTEMÓW INFORMATYCZNYCH</b>	
<b>GRUPA ZAWODOWA</b>	<b>ILOŚĆ</b>
I. Żołnierze zawodowi	
3. Mężczyźni	177
4. Kobiety	0
<b>RAZEM:</b>	<b>177</b>
II. Pracownicy wojska	
3. Mężczyźni	159
4. Kobiety	32
<b>RAZEM:</b>	<b>191</b>
<b>OGÓLEM:</b>	<b>368</b>

Źródło: opracowanie własne.

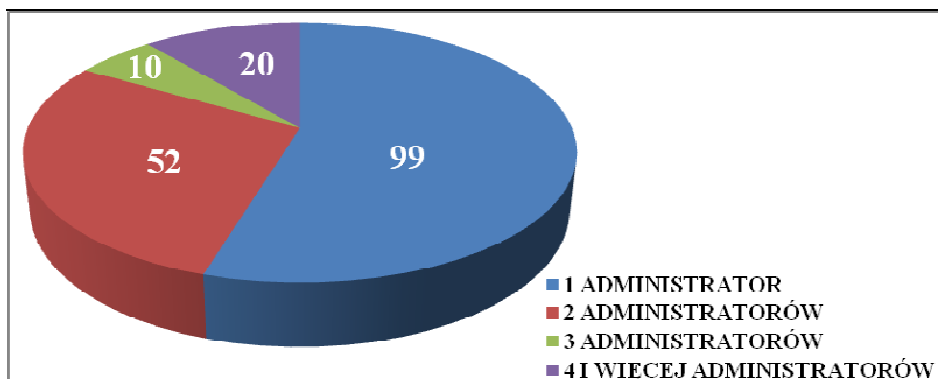
Przez wiele lat istniało przeświadczenie dowódców, szefów czy komendantów, aby w jednostkach uruchamiać serwery z różnymi bazami przeznaczonych tylko dla celów jednostki, czy instytucji wojskowej lub na potrzeby danego rodzaju sił zbrojnych. Takie rozwiązania były kosztowne zarówno ze względu na wyposażanie tych jednostek w sprzęt teleinformatyczny i oprogramowanie, jak i wydzielanie oraz remontowanie pomieszczeń przeznaczonych dla tych systemów. W przypadku braku właściwego oprogramowania, wytwarzano różnego rodzaju sposobami własne oprogramowanie. Systemy te nie były odpowiednio zintegrowane z innymi systemami przeznaczonymi dla tych samych celów. Nie były profesjonalnymi programami, nie uwzględniały wszystkich potrzeb użytkowników, co było zrozumiałe ze względu na brak określonych standardów, a spełniały wyłącznie podstawowe wymogi stawiane przez dane rozwiązania. Dorabiano więc nakładki programowe, co w efekcie końcowym podnosiło bardzo koszty ich eksploatacji i nie zawsze spełniało swoje role. Problemem również była administracja tych systemów, a konkretnie brak wystarczającej ilości administratorów tych systemów. W efekcie tych działań powstała bardzo duża liczba systemów informatycznych niekompatybilnych ze sobą.

W analizowanym rejonie na koniec grudnia 2012 r. występowało łącznie 78 systemów informatycznych z czego:

- 20 systemów obejmowało sprawy personalno-kadrowe,
- 16 systemów dotyczyło spraw finansowo-kadrowych,
- 10 systemów spraw logistycznych,
- 32 pozostałe obejmujące inne dziedziny działalności służbowej jednostek i instytucji wojskowych.

Rozwój informatyzacji ma na celu ograniczenie tak dużej ilości systemów i zastąpienie profesjonalnymi systemami. Między innymi wdrażany przez Departament Informatyki i Telekomunikacji oraz jednostki mu podległe Zintegrowany Wieloszczeblowy System Informatyczny Resortu Obrony Narodowej, który ma na celu, połączenie całej działalności kadrowo-finansowo-logistycznej. Duża liczba różnorodnych systemów w jednostkach organizacyjnych MON powoduje konieczność wyznaczania dla nich administratorów. W jednostkach, które posiadają kilka albo kilkanaście systemów, powstaje więc konieczność wyznaczenia kilku osób do pełnienia tych funkcji. Wykres 1. przedstawia ilość administratorów przypadających na jednostkę organizacyjną. Z wykresu wynika, że dowódcy, szefowie, komendanci wyznaczają w większości jednego lub 2 administratorów i nie są chętni do zwiększania tej liczby, głównie ze względu na ograniczenia etatowe. Liczba administratorów w jednostkach organizacyjnych nie ulegnie redukcji, nawet jeśli zmodernizowane zostaną systemy informatyczne. Konieczność wyznaczania osób do pełnienia funkcji administratora w jednostkach organizacyjnych wymuszają na dowódcach, szefach czy komendan-

tach różnego rodzaju ustawy i rozporządzenia, dotyczące głównie bezpieczeństwa tych systemów.



Źródło: opracowanie własne.

**Wykres 1. Liczba administratorów systemów informatycznych wyznaczonych do pełnienia swoich funkcji w jednej jednostce lub instytucji wojskowej**

Bez dobrej polityki kadrowej, wyznaczania właściwych osób na administratorów, nie będzie możliwe zapewnienie wysokiego poziomu świadczenia usług w eksploatowanych systemach teleinformatycznych, czy podsystemach funkcjonalnych, np. na potrzeby logistyki, kadr i finansów w jednostkach i instytucjach wojskowych lub w zakresie wsparcia teleinformatycznego na potrzeby ćwiczeń i treningów sztabowych.

Powszechnie przyjmuje się, że administratorem systemu nazywa się osobę (lub zespół osób), niepełniącą funkcji inspektora bezpieczeństwa teleinformatycznego, odpowiedzialną za funkcjonowanie systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego<sup>2</sup>.

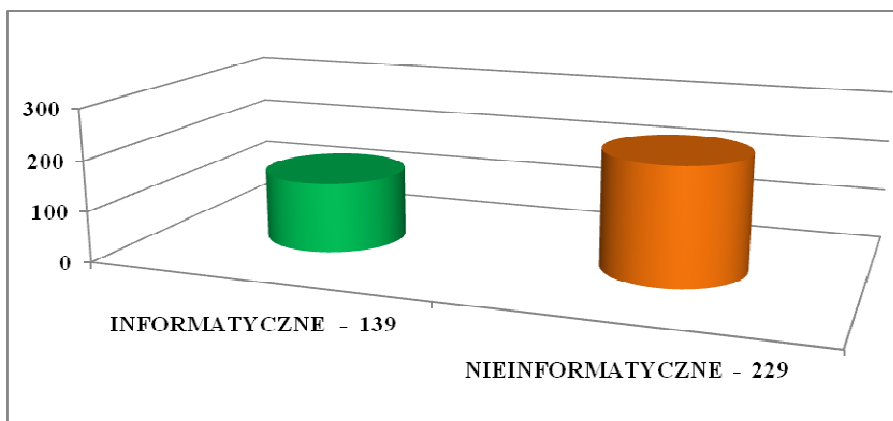
Nawiązując do tej definicji administratora systemu, dowódcy, szefowie, komendanci lub inne osoby funkcyjne w działalności bieżącej, na wnioski szefów sekcji, wydziałów, oddziałów (S-6, J-6) podają punkty do swoich rozkazów o następującej treści: *dla zapewnienia ciągłego monitoringu, serwisu technicznego i administrowania sieciami i systemami informatycznymi oraz prowadzenia bieżącej kontroli zdarzeń powstałych na urządzeniach kryptograficznych na administratora sieci lub systemu teleinformatycznego wyznaczam...* I od tego punktu administratorzy przyjmują pełną odpowiedzialność za funkcjonowanie sieci i systemów teleinformatycznych. Wydawałoby się, że właściwie wszystko jest już spełnione zgodnie z przepisami.

<sup>2</sup> Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, art. 52, ust. 1, pkt. 2.

Poza codziennymi obowiązkami administratorów, do których należy troska o zapewnienie dostępu do sieci informatycznych, aktualizowanie oprogramowania, szkolenie użytkowników, przeciwdziałanie zagrożeniom, walka z wirusami komputerowymi, administratorzy muszą systematycznie pogłębiać swoją wiedzę i czynnie uczestniczyć w modernizacji sieci i systemów informatycznych.

Poprzez systematyczne pogłębianie wiedzy informatycznej przez administratorów, następuje lepsze zarządzanie sieciami i systemami teleinformatycznymi, a tym samym zwiększa się bezpieczeństwo tych sieci.

Istnieje jednak duży problem z właściwym szkoleniem administratorów, ponieważ na nieetatowych administratorów wyznaczane są osoby, które często nie posiadają wykształcenia informatycznego (sytuację przedstawia wykres 2).

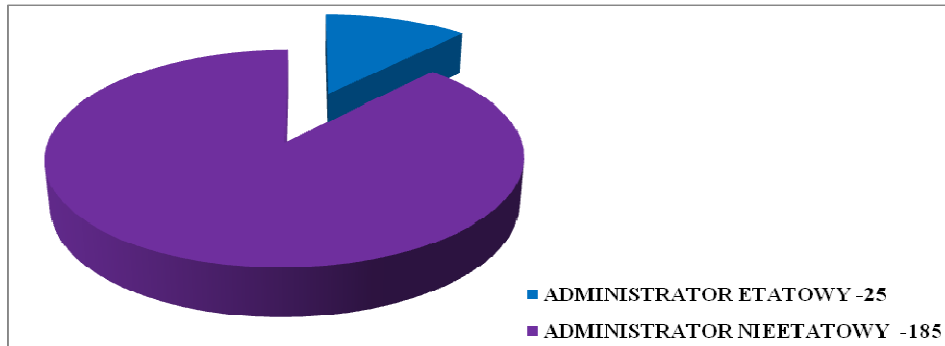


Źródło: opracowanie własne.

**Wykres 2. Rodzaj wykształcenia administratorów systemów informatycznych w jednostkach i instytucjach w rejonie objętym analizą**

Problemem również jest to, że w większości administratorami sieci i systemów teleinformatycznych są osoby, które pełnią tę funkcję nieetatowo (sytuację przedstawia wykres 3). Wykres ten przedstawia liczbę administratorów sieci MIL-WAN pełniących swoje funkcje jako etatowe i nieetatowe. Zauważalne jest, że administratorów nieetatowych jest zdecydowanie więcej niż etatowych, nieetatowi stanowią aż 88 %, co należy uznać za niepokojące zjawisko.





Źródło: opracowanie własne.

**Wykres 3. Podział administratorów systemu MIL-WAN w jednostkach i instytucjach stacjonujących w obszarze objętym analizą**

Przy takim stanie rzeczy trudno jest więc osiągnąć cel szkoleniowy, którym jest jak najlepsze przygotowanie i wyszkolenie administratorów do zarządzania sieciami i usługami teleinformatycznymi. Proces szkolenia jest zróżnicowany w zależności od tego, jaką rolę pełni administrator w systemie teleinformatycznym. Nie ma potrzeby szkolić wszystkich administratorów na najwyższych poziomach. Poziomy szkolenia muszą być zróżnicowane zarówno ze względu na rodzaj wykonywanej pracy, jak i ponoszone na ten cel wysokie koszty szkolenia. Jednak administratorzy powinni być objęci przynajmniej, niezbędnym zakresem szkoleń, przede wszystkim ze względu na potrzebę zwiększenia bezpieczeństwa systemów teleinformatycznych.

Aby podołać wymaganiom i być w stanie przyswoić specyficzną wiedzę przedstawianą na kursach dla administratorów, nie tylko powinni oni być pracownikami etatowymi, żołnierzami zawodowymi lub pracownikami wojska, ale mieć wykształcenie w specjalności łączność i informatyka. Administratorami nie powinni być amatorzy wykonujący swoje funkcje nieetatowo.

Rozwój informatyki pociąga za sobą generowanie nowej wiedzy i potrzebę podnoszenia zasobu tej wiedzy przez osoby administrujące systemy informatyczne.

Główną siecią informatyczną w Siłach Zbrojnych RP jest sieć MIL-WAN, która jest platformą dla wielu systemów informatycznych finansowych, logistycznych i kadrowych, w której działa poczta elektroniczna, strony www., dlatego poświęcono jej najwięcej zagadnień. Sieć ta musi być dostępna całodobowo siedem dni w tygodniu. Działanie tej sieci jest w pełni monitorowane przez administratorów. Prowadzona jest polityka bezpieczeństwa teleinformatycznego.

Na 202 stacjonujące jednostki i instytucje wojskowe objęte analizą, sieć MIL-WAN funkcjonowała pod koniec roku 2012 w 148 jednostkach i insty-

tucjach wojskowych, co stanowiło 73,3%. Zasięg funkcjonowania sieci MIL-WAN w kraju, będzie systematycznie wzrastał, jednak nigdy nie osiągnie poziomu 100%, ponieważ nie wszystkie jednostki i instytucje wojskowe będą miały potrzebę jej posiadania, a także nie będą spełniały wymagań do jej uruchomienia.

W latach 2011-2012 w Siłach Zbrojnych RP, poprzez wdrażanie i doskonalenie budowy sieci informatycznych przez Departament Informatyki i Telekomunikacji oraz jednostki mu podległe, nastąpił bardzo dynamiczny rozwój funkcjonowania potencjału sieci rozległych. Poprzez wdrażanie jednolitej sieci podkładowej zwanej MPLS<sup>3</sup> i zwiększanie przepływności pomiędzy poszczególnymi lokalizacjami jednostek, czy instytucjami wojskowymi, systematycznie następuje lepsze wykorzystanie i zarządzanie tymi łączami, a także zwiększa się możliwość udostępniania wielu użytkownikom innych usług wcześniej niemożliwych do świadczenia ze względów technicznych.

Technologia MPLS pozwala na jednym medium transmisyjnym uruchamiać wiele rodzajów sieci o różnych klauzulach (PF-WAN, MIL-WAN, systemy NATO, INTER-MON). Pozwoli to zabezpieczyć funkcjonowanie, wdrażanie i rozwijanie systemów/usług wspomagających działalność bieżącą resortu (VoIP/VTC, SI ARCUS) oraz systemów bezpieczeństwa teleinformatycznego.

Należy oceniać, że rok 2013 będzie kolejnym trudnym etapem wdrażania nowych systemów i oprogramowania, a w szczególności doskonalenia usługi VoIP/VTC. Będzie realizowane wsparcie teleinformatyczne wielu ćwiczeń i treningów sztabowych, a więc pokonywanie kolejnych wyzwań związanych z wdrożonymi i eksploatowanymi systemami informatycznymi. Kontynuowane będzie doskonalenie umiejętności w monitorowaniu, wykrywaniu występowania incydentów komputerowych oraz ochrony kryptograficznej informacji.

Walka z wirusami komputerowymi jest dla administratorów dużym wyzwaniem. Użytkownicy mają z roku na rok coraz lepszą świadomość zagrożeń, jakie mogą stworzyć wirusy. Widać w tej dziedzinie duży postęp spowodowany między innymi aktywną działalnością pionów ochrony informacji niejawnych, które uświadamiają kadry i pracownikom wojska, jak należy postępować w tej dziedzinie.

Informatyka zagościła w naszym życiu służbowym już na dobre. Nie jesteśmy już w stanie funkcjonować bez komputera, sieci MIL-WAN lub INTER-MON, telefonów komórkowych itp. Użytkownicy systemów informatycznych, jak to zwykle bywa, gdy sieci działają poprawnie, nie zwracają

---

<sup>3</sup> *Multiprotocol Label Switching* – technika stosowana przez routery, w której trasowanie pakietów zostało zastąpione przez tzw. przełączanie etykiet.

uwagi, że wielu informatyków i łącznościowców pracuje i daje z siebie wszystko, aby taki stan utrzymać.

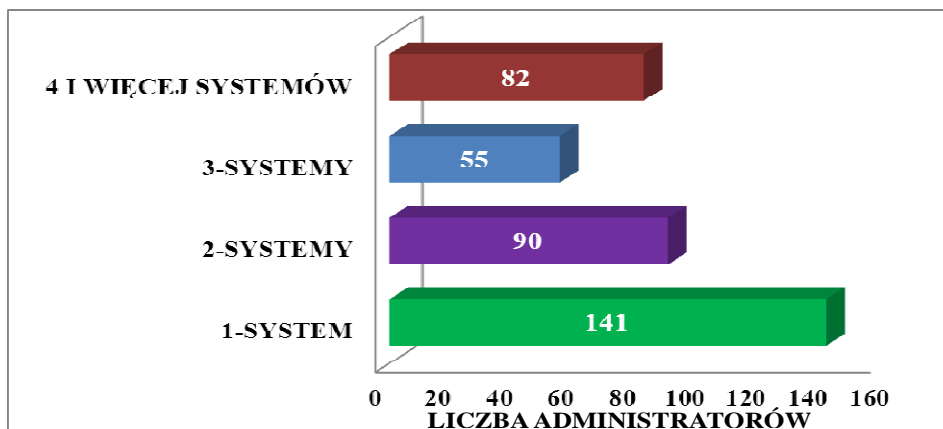
Aby usprawnić system pomocy użytkownikom systemów informatycznych rozpoczęto tworzenie modelowego systemu wsparcia technicznego tzw. HelpDesk, na różnych szczeblach zarządzania.

Pomysł jest bardzo dobry, natomiast aby on funkcjonował poprawnie, trzeba zaangażować bardzo dużo sił i środków. Żadna jednostka czy instytucja wojskowa bez właściwego wsparcia informatycznego użytkownika nie może poprawnie funkcjonować. Jesteśmy teraz na początku tworzenia właściwego sprawnego wsparcia użytkownika na wszystkich poziomach zarządzania. Teraz przy budowaniu coraz bardziej wydolnych, rozległych sieci teleinformatycznych jest nie tylko konieczne, lecz także możliwe. Kilka lat wcześniej nie było to możliwe ze względu na dużą liczbę lokalnych sieci. Właściwy system wsparcia użytkownika jest warunkiem koniecznym do efektywnego wykorzystania systemów i sieci teleinformatycznych. Budowany jest więc system wielopoziomowy mający w założeniu zarówno lokalną, jak i zdalną pomoc.

Budowany system wsparcia umożliwi:

- kompleksowe zarządzanie połączeniami przychodzącymi i wewnątrz sieci,
- obsługę zapowiedzi głosowych systemu wsparcia,
- uruchomienie automatycznego dyspozytora połączeń,
- monitorowanie pracy agentów systemu wsparcia,
- generowanie różnego typu raportów z pracy systemu wsparcia.

Ważne role pełnią tu więc administratorzy wyznaczeni na poszczególnych poziomach. Nie bez znaczenia jest więc, kto jest wyznaczony do pełnienia tej funkcji.

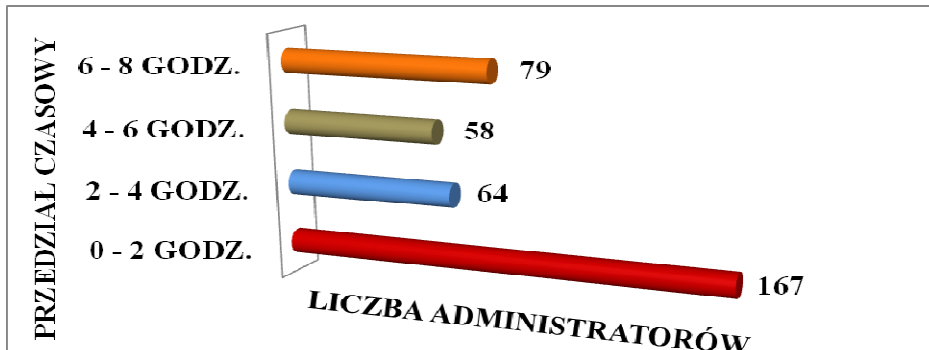


Źródło: opracowanie własne.

**Wykres 4. Liczba systemów informatycznych zarządzanych przez jednego administratora**

Bardzo często wyznacza się osoby do pełnienia roli administratorów w kilku systemach informatycznych. Zobrazowane jest to na wykresie 4. Jednym systemem zarządza tylko 1/3 wszystkich administratorów.

Innym istotnym czynnikiem wpływającym na właściwe administrowanie systemami informatycznymi jest czas przeznaczony na ten cel przez administratorów, co prezentuje wykres 5.

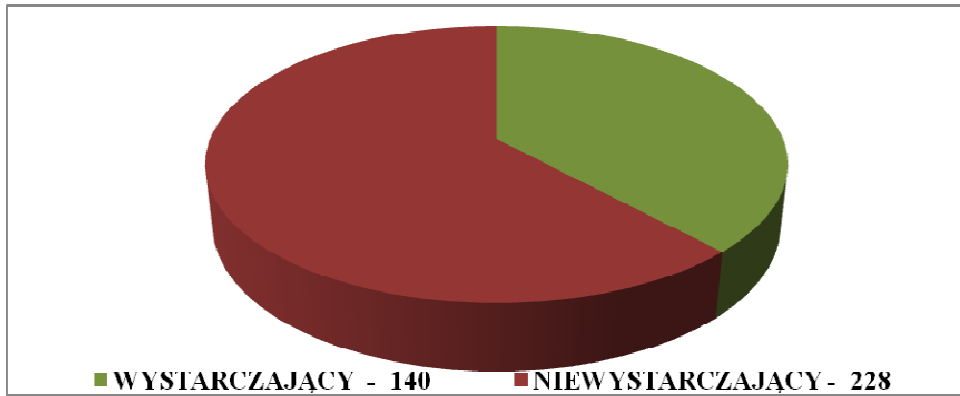


Źródło: opracowanie własne.

**Wykres 5. Czas poświęcony na zagadnienia informatyczne związane z zarządzaniem systemami informatycznymi przez administratorów w godzinach służbowych dziennie**

Z wykresu 5. wynika, że większość administratorów na ten cel przeznaczają od zera do dwóch godzin dziennie. Występują więc dni, że na zarządzanie systemami administratorzy nie przeznaczają z różnych powodów ani chwili. Taka sytuacja może być niebezpieczna w skutkach, a szczególnie groźna dla bezpieczeństwa teleinformatycznego systemu.

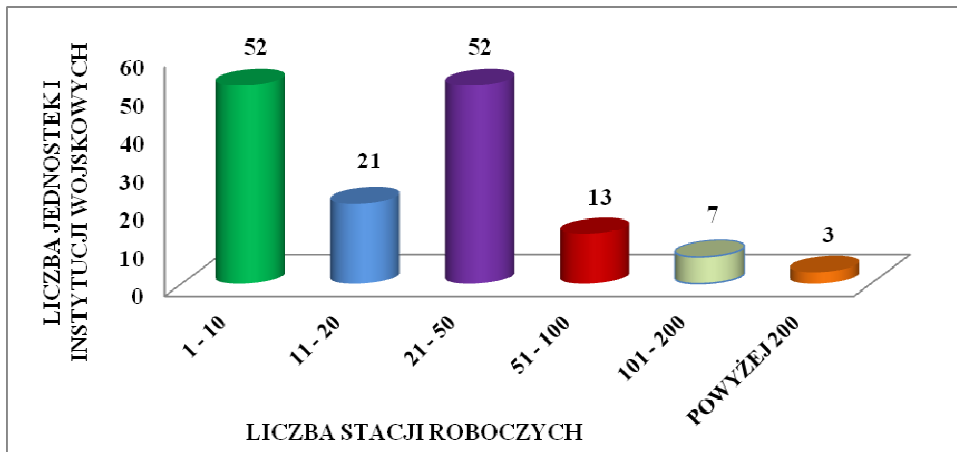
62% administratorów uważa, że przeznaczają zbyt mało czasu na zadania związane działalnością informatyczną. Należy sądzić, że jest to sygnał dla dowódców, szefów, komendantów, że należałoby odciążyć administratorów od innych obowiązków, aby mogli więcej czasu w godzinach służbowych poświęcić zagadnieniom związanym z działalnością informatyczną. Lekceważenie tej statystyki może doprowadzić do złego zarządzania systemami informatycznymi, a tym samym obniżenia bezpieczeństwa eksploatowanych systemów.



Źródło: opracowanie własne.

**Wykres 6. Uznanie przez administratorów przeznaczonego czasu na zagadnienia związane z informatyką za wystarczający lub nie**

Z przedstawionego wykresu 7. wynika, że należałoby zmienić sposób i wypracować właściwy system wyznaczania administratorów w jednostkach organizacyjnych MON.



Źródło: opracowanie własne.

**Wykres 7. Liczba stacji roboczych zainstalowanych w jednostce lub instytucji wojskowej stacjonującej w rejonie objętym analizą**

Można by przyjąć, że małe jednostki posiadające małą liczbę stacji roboczych, np. do 10 szt. mogłyby być wspierane przez administratorów etatowych z dużych jednostek przy podpisaniu stosownych porozumień pomiędzy jednostkami. W tak przyjętym rozwiązaniu wyznaczeni administratorzy w dużych jednostkach powinni być etatowi i mieć specjalność – łącz-

ność i informatyka. W tym układzie można by dla nich właściwie zaplanować i przeprowadzić szkolenia podnoszące ich kwalifikacje.

Budowanie tego systemu ma za zadanie osiągnięcie bardzo ważnego celu, jakim jest dostęp uprawnionych użytkowników do różnego rodzaju powstających baz danych np. Zintegrowanego Wieloszczeblowego Systemu Informatycznego Resortu Obrony Narodowej (ZWSIRON), Elektronicznego Systemu Obiegu Dokumentów ARCUS, zasobów Platformy e-learningowej Ministerstwa Obrony Narodowej oraz innych systemów na potrzeby rodzajów sił zbrojnych.

Na podstawie przeprowadzonej analizy można sformułować szereg wniosków, które pozwoliłyby poprawić zarządzanie systemami. Podstawą zmian jest:

1. Uznanie znaczenia, roli i wpływu administratorów w zarządzaniu systemami informatycznymi i bezpieczeństwie eksploatacji systemów na potrzeby jednostek organizacyjnych.

2. Wsparcie merytoryczne i udzielanie stosownej pomocy przez szefów oddziałów dowodzenia i łączności rodzajów sił zbrojnych dla dowódców, szefów, komendantów jednostek organizacyjnych przy tworzeniu obsad etatowych lub planów zatrudnienia.

3. Utworzenie w planie zatrudnienia jednostki organizacyjnej w ramach przydzielonych limitów finansowych stanowiska pracownika wojska – administratora systemów w przypadku, gdy nie ma możliwości stworzenia stanowiska etatowego administratora systemów dla żołnierza zawodowego.

Uwaga:

- Stanowiska etatowe dla kadry proponuję utworzyć w jednostkach organizacyjnych, w których występuje kilka systemów informatycznych i duża liczba stacji roboczych, a więc również duża liczba użytkowników. W tym przypadku można również utworzyć dodatkowo stanowisko administratora systemu w planie zatrudnienia dla pracownika wojska.

- Stanowiska w planach zatrudnienia jednostek organizacyjnych dla administratora systemu pracownika wojska, tam gdzie występuje mała liczba systemów informatycznych i użytkowników. Najlepszym rozwiązaniem byłoby utworzenie stanowisk etatowych administratorów, jednak takie poprawki wymagają zmian w stosownych decyzjach Ministra Obrony Narodowej w sprawie zatrudnienia i funduszu wynagrodzeń pracowników resortu obrony narodowej.

4. Dodanie zgodnie z procedurami do tabeli stanowisk, zaszeregowania i wymagań kwalifikacyjnych dla nierobotniczych stanowisk pracy w Ponadzakładowym Układzie Zbiorowym Pracy dla Pracowników Wojskowych Jednostek Organizacyjnych Sfery Budżetowej, zawartym w dniu 8.06.1998 roku wraz załącznikami stanowiska administratora systemów informatycznych z kategorią zaszeregowania, np. XIII-XV i wymaganiami kwalifikacyj-

nymi wykształcenia wyższego/średniego. Pozwoliłoby to na zatrudnienie specjalistów.

5. Opracowanie programów procesu szkolenia dla administratorów, odpowiadających powierzonym zadaniom w zarządzaniu systemami informatycznymi.

6. Objęcie ochroną kadrową administratorów, mające na celu zatrzymanie specjalistów administratorów w Siłach Zbrojnych RP.

Takie podejście i przyjęte rozwiązanie pozwolą podnieść jakość administrowania, tym samym działanie systemów teleinformatycznych. Zwłaszcza, że dynamika zmian wymusza pełną profesjonalizację tej odpowiedzialnej części nowoczesnej organizacji opartej na wiedzy.

Kolejnym zagadnieniem związanym z zarządzaniem systemami informatycznymi, zgodnie z Ustawą z dnia 5 sierpnia 2010r. o ochronie informacji niejawnych, jest wyznaczanie inspektora bezpieczeństwa teleinformatycznego użytkowanego systemu (zwanego w dalszej części inspektorem).

W mojej opinii, dobrze byłoby dokonać poprawek w sposobie wyznaczania osób, którym powierza się funkcje inspektora. Przy braku wystarczającej liczby specjalistów administratorów trudno jest wyznaczyć dobrego inspektora. Inspektor ma za zadanie kontrolować zgodność funkcjonowania eksploatowanego w danej jednostce organizacyjnej systemu teleinformatycznego z jego dokumentacją bezpieczeństwa. Powinien więc posiadać wiedzę co najmniej równą administratorowi, a najlepiej większą, aby móc dokonać właściwej kontroli. Niestety w jednostkach organizacyjnych dowódcy, szefowie czy komendanci, mają problemy z pozyskaniem specjalistów inspektorów. A szkoda, ponieważ ma to znaczący wpływ na organizację ochrony systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych w resorcie obrony narodowej. Szczególna rola inspektora bezpieczeństwa wynika również ze znaczenia bezpieczeństwa i zagrożeń wynikających z cyberprzestępczości itp.

Analiza obejmuje 93,5% jednostek i instytucji wojskowych w południowo wschodniej część kraju. Pozostały 6,5 procent stanowią w większości jednostki organizacyjne o małych strukturach i wymaganiach teleinformatycznych, np. Kluby Garnizonowe, Parafie, Pracownie Psychologiczne itp. Sądzę, że istnieje bardzo duże prawdopodobieństwo, iż w pozostałej części kraju występują podobne problemy w zarządzaniu sieciami i systemami teleinformatycznymi. Dlatego w skali Sił Zbrojnych RP należy zwrócić uwagę na ten aspekt zarządzania systemami i podniesienia rangi administratorów w strukturach jednostek organizacyjnych MON. W przeciwnym wypadku w mojej ocenie mogą występować nieprzewidziane negatywne sytuacje w pracy systemów teleinformatycznych, mające wpływ na proces dowodzenia, utrzymania i osiągania stopnia gotowości bojowej. Konsekwencje opóźnień w rozwiązaniu problematyki administratorów systemu mogą okazać się w przyszłości bardzo szkodliwe, kosztowne i trudne do naprawienia.

## **Bibliografia**

1. Decyzja Nr 7/MON Ministra Obrony Narodowej z dnia 20 stycznia 2012 r. w sprawie organizacji ochrony systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych w resorcie obrony narodowej.
2. *SWB dla Systemu Teleinformatycznego "MIL-WAN"*, wersja 5 z dnia 25 maja 2012 r.
3. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. 2010, nr 182, poz. 1228).

## **ANALYSIS OF TELEINFORMATIC (ICT) SYSTEMS MANAGEMENT IN THE AREA OF RESPONSIBILITY OF ICT SUPPORT MANAGEMENT TEAM – ADMINISTRATORS**

*Abstract:* The article features problems connected with ICT system management functioning in the Polish Armed Forces in the area of responsibility of ICT Support Management Team in Cracow. Special attention has been drawn to the role and importance of ICT administrators in these systems' management. The problems that the ICT administrators encounter in their activity have been presented. The topics of these problems include the system of administrators' training, their development path, the way of entrusting them administrator's duties as full-time administrators and freelances. Moreover, threats that may arise in ICT systems exploitation as a result of their improper management by untrained administrators have been exposed. Feasible ways of solving selected problems that having been implemented into a current activity will improve the security of ICT support for institutions and military units have been proposed.