WIEDZA OBRONNA 2025, Vol. 293 No. 4
ISSN: 2658-0829 (Online) 0209-0031 (Print)
Journal homepage: http://wiedzaobronna.edu.pl
DOI: https://doi.org/10.34752/c5b05194

ANDRZEJ BOGDAŃSKI *
Akademia Sztuki Wojennej, Warszawa, Polska

TECHNOLOGIE WSPIERAJĄCE PRZESYŁANIE CHRONIONYCH INFORMACJI

TECHNICAL SOLUTIONS THAT CAN ENSURE SECURE EXCHANGE OF INFORMATION WITHIN UNIFORMED SERVICES

ABSTRAKT: W artykule autor przedstawił wybrane aspekty dotyczące realizacji technicznych rozwiązań w oparciu o dynamiczne tworzoną infrastrukturę teleinformatyczna, które mogą zapewnić bezpieczną wymianę informacji w ramach służb mundurowych, także na potrzeby o ochrony ludności i obrony cywilnej. Celem badań była identyfikacja możliwości dostosowania systemu transmisyjnego Sił Zbrojnych Rzeczypospolitej Polskiej na potrzeby bezpiecznej wymiany informacji w ramach służb mundurowych. Głównym problemem badawczym, który autor sobie postawił było uzyskanie odpowiedzi na pytanie: W jaki sposób można zaadoptować rozwiązania stosowana w SZ RP dla zwiększenia bezpieczeństwa transmisji w systemach łączności służbach mundurowych? Autor scharakteryzował wybrane rozwiązania zaimplementowane w resortowych systemach teleinformatycznych, opisał mechanizmy trasowania, tunelowania i szyfrowania realizujące zadania na potrzeby zachowania poufność, integralność, dostępność i autentyczność informacji[1].Przedstawił modelową strukturę węzła dostępowego wchodzącego w skład węzła łączności, topologię węzłów dostępowych oraz organizację dynamicznych tuneli. Scharakteryzował wybrane mechanizmy w oparciu o jeden i kilka redundantnych środków transmisyjnych.

SŁOWA KLUCZOWE: bezpieczeństwo transmisji, cyberbezpieczeństwo, wirtualne sieci prywatne, szyfrowanie.

ABSTRACT: In the article, the author presented selected aspects related to the implementation of technical solutions based on dynamically created ICT infrastructure, which can ensure secure information exchange within uniformed services, including for the purposes of civil protection and civil defense. The aim of the article was to answer the question: Is it possible to adapt the transmission system of the Armed Forces of the Republic of Poland to enable secure information exchange within uniformed services?

The main research problem posed by the author was to find an answer to the question: How should an information exchange system be organized within the services in order to enhance the capability to carry out assigned tasks in the area of crisis management? The author characterized selected solutions implemented in ministerial ICT systems, described routing, tunnelling, and encryption mechanisms used to ensure data confidentiality, availability, integrity, and non-repudiation. He presented a model structure of an access node that is part of a communication node, the topology of access nodes, and the organization of dynamic tunnels. Selected mechanisms were characterized based on one or several redundant transmission means.

KEYWORDS: transmission security, cybersecurity, virtual private networks, encryption.

[1] Zob. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa Dz.U.2024.1077 t.j

* **dr Andrzej Bogdański**, War Studies University, Warszawa, Polska
https://orcid.org/0000-0002-3443-0741 a.bogdanski@akademia.mil.pl
Copyright (c) 2025 Andrzej Bogdański. This work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License.

WPROWADZENIE

Sytuacja problemowa

Zapewnienie sprawnie działającego, bezpiecznego systemu łączności jest jednym z fundamentalnych czynników umożliwiających właściwe funkcjonowanie nowoczesnych sił zbrojnych. W ostatnich latach przed Siłami Zbrojnymi RP, oprócz wyzwań związanych z koniecznością doskonalenia swojej sprawności na ćwiczeniach i treningach, stanęły nowe związane z zagrożeniem na granicy i klęskami żywiołowymi. Wojsko Polskie skutecznie zastosowało nowoczesne rozwiązania teleinformatyczne, umożlwiające zaspokojenie potrzeb w zakresie łączności zarówno w czasie ćwiczeń jak i w realizacji zadań z zakresu zarządzania kryzysowego czy ochrony granicy państwowej. Zaimplementowane rozwiązania umożliwiły zbudowanie logicznej, bezpiecznej i wirtualnej sieci na szkielecie istniejącej infrastruktury stacjonarnej resortu obrony narodowej, uzupełnionej o elementy mobilne. Rozwój systemów determinował implementację nowych technologii, ponieważ wzrosła ilość przekazywanych informacji. Zdolność do dowodzenia ma tym większą efektywność, im pewniej i szybciej będzie realizowana wymiana informacji. Zadaniem systemu łączności powinno być zapewnienie przekazywania informacji w sposób wierny, skryty i terminowy[2] , co zapewniają współczesne systemy transmisyjne SZ RP oparty na fizycznie wydzielonej infrastrukturze resortu obrony narodowej IP-RON[3]. Zdaniem autora scharakteryzowane w artykule rozwiązania zbudowane na infrastrukturze resortu obrony narodowej oraz zabezpieczone narodowymi technologiami kryptograficznymi mogą dawać gwarancję przekazywania informacji w sposób wierny, skryty i terminowy jednocześnie gwarantując dostępność, poufność, autentyczność i integralność przesyłanych informacji[4]. Pojęcie triada CIA jest podstawą bezpieczeństwa informacji i pojawia się w praktycznie każdej normie lub polityce dotyczącej ochrony danych. Pojęcia pochodzą od ang. *confidentiality*, *integrity*, *availability* i tak poufność (ang. *confidentiality*) to zapewnienie, że tylko upoważnione osoby mają dostęp do informacji. Chodzi zatem o ochronę przed nieautoryzowanym ujawnieniem danych. Integralność (ang. *integrity*) to gwarancja, że dane nie zostały zmodyfikowane w sposób nieautoryzowany – są kompletne, dokładne i spójne. Natomiast dostępność (ang. *availability*) to zapewnienie, że dane i systemy są dostępne dla uprawnionych użytkowników wtedy, kiedy są potrzebne. Praktyczny sposób implementacji rozwiązań, a zwłaszcza nieopisanego powyżej atrybutu niezaprzeczalności poświęcili swoje badania Strzałek i Pałka w pracy naukowej pt. Problematyka poufności, autentyczności, integralności oraz niezaprzeczalności danych w systemach wieloagentowych[5], [6].

---

[2] B. Terebiński, Teleinformatyka wojskowa, Akademia Sztuki Wojennej, Warszawa, 2022, s. 63.

[3] M. Marczyk, B. Terebiński, System łączności brygady obrony terytorialnej (BOT) w wojskowym systemie telekomunikacyjnym, Bellona, Warszawa 2021, s. 14, DOI:10.5604/01.3001.0015.6659.

[4] M. Strzałek, P. Pałka, Problematyka poufności, autentyczności, integralności oraz niezaprzeczalności danych w systemach wieloagentowych, Politechnika Warszawska, 2012, s. 221, https://delibra.bg.polsl.pl/Content/76503/BCPS-86045_2012_Problematyka-poufnos_0000.pdf (dostęp: 12.12.2024).

[5] M Strzałek, P. Pałka, Problematyka poufności, autentyczności, integralności oraz niezaprzeczalności danych w systemach wieloagentowych https://delibra.bg.polsl.pl/Content/76503/BCPS-86045_2012_Problematyka-poufnos_0000.pdf STUDIA INFORMATICA, nr 2b (106) Vol. 33 wydawnictwo Politechnika Warszawska, Warszawa 2012, s. 221, (dostęp: 07.04.2025).

[6] Ibidem

Ponadto, nie można zapomnieć o atrybucie niezaprzeczalności informacji. Autor rozumie ten atrybut jako sytuację, w której nadawca informacji nie może zaprzeczyć, że ją wysłał, odbiorca nie może zaprzeczyć, że ją otrzymał. Oznacza to, że istnieją dowody potwierdzające, iż konkretna osoba lub system uczestniczył w wymianie informacji.

CELE BADAŃ

Cel główny badań

Analiza funkcjonalna eksploatowanych w Siły Zbrojne Rzeczypospolitej Polskiej systemów teleinformatycznych pozwoliła autorowi na zdefiniowanie celu głównego badań, którym była identyfikacja możliwości dostosowania systemu transmisyjnego Sił Zbrojnych Rzeczypospolitej Polskiej na potrzeby bezpiecznej wymiany informacji w ramach służb mundurowych. Autor realizował badania w odniesieniu do najbardziej liczebnych służb mundurowych, a mianowicie Policji, Państwowej Straży Pożarnej i Straży Granicznej.

Cele szczegółowe badań

Jako cel praktyczny[7] autor przyjął scharakteryzowanie sposobu działania oraz metodę wdrożenia konkretnych rozwiązań teleinformatycznych, które mogą podnieść bezpieczeństwo transmisji podczas wymiany informacji w ramach służb mundurowych.

Celem poznawczym[8] było zidentyfikowanie determinantów, a zwłaszcza ograniczeń wpływających na możliwość integracji systemów teleinformatycznych na poziomie transmisyjnym służb mundurowych w celu osiągnięcia interoperacyjności.

PROBLEMY BADAWCZE

Główny problem badawczy

Główny problem badawczy autor przedstawił w postaci pytania: W jaki sposób zaimplementować zaawansowane rozwiązania teleinformatyczne do systemów teleinformatycznych służb podległych szefowi Ministerstwa Spraw Wewnętrznych i Administracji na potrzeby wymiany informacji w celu zwiększenia zdolności do realizacji postawionych zadań?

Szczegółowe problemy badawcze

W jaki sposób rozbudować infrastrukturę teleinformatyczną resortu obrony narodowej na potrzeby realizacji postawionych zadań?

W jaki sposób zintegrować systemy transmisyjne Ministerstwa Obrony Narodowej i Ministerstwa Spraw Wewnętrznych i Administracji na poziomie sieci szkieletowej?

Jak zapewnić bezpieczeństwo przesyłanych między służbami mundurowymi resortów MON i MSWiA informacji niejawnych?

W jaki sposób zapewnić interoperacyjność usług telefonii i wideo telefonii między służbami mundurowymi resortów MON i MSWiA?

---

[7] M. Pelc, Elementy metodologii badań naukowych, Akademia Obrony Narodowej, Warszawa 2012, s. 15.

[8] Ibidem.

HIPOTEZY BADAWCZE

Hipoteza główna

Służby mundurowe posiadają podobne technologie sieciowe co daje możliwość integracji systemów teleinformatycznych na poziomie niższych warstw sieciowych. Ministerstwo Obrony Narodowej i Ministerstwo Spraw Wewnętrznych i Administracji posiadają grupę usług podstawowych takich jak telefonia czy wideotelefonia w ramach, których przesyłanie informacji między systemami różnych resortów jest możliwe do zrealizowania przy niewielkim nakładzie pracy administratorów w zakresie konfiguracji usług. Dlatego też autor przyjął hipotezę badawczą: wymiana informacji w ramach służb przy zastosowaniu komercyjnych usług podstawowych jest możliwa do osiągnięcia pod warunkiem zaimplementowania takich samych standardów transmisyjnych po stronie dołączanego komponentu.

Hipotezy szczegółowe

Po uzupełnieniu infrastruktury stacjonarnej o środki transmisyjne wykorzystywane w resorcie obrony narodowej jest możliwe stworzenie sieci podkładowej umożliwiającej przepływy informacyjne między służbami na potrzeby realizacji postawionych zadań.

Integracja systemów transmisyjnych Ministerstwa Obrony Narodowej i Ministerstwa Spraw Wewnętrznych i Administracji jest możliwa przy zaimplementowaniu ogólnodostępnych protokołów sieciowych.

Możliwe jest zapewnienie bezpieczeństwa przesyłanych między resortami informacji niejawnych w oparciu o komercyjne lub dedykowane urządzenia szyfrujące.

Interoperacyjność usług telefonii i wideotelefonii między służbami mundurowymi resortów MON i MSWiA można zapewnić poprzez zaimplementowanie uniwersalnego stosu protokołów sygnalizacyjnych lub wdrożenie technologii opartej o powszechnie dostępne rozwiązania komercyjne.

METODY BADAWCZE

Przedstawione w artykule wyniki badań mają swoje źródło w wieloletnich obserwacjach oraz wywiadach z ekspertami. Podczas największych ćwiczeń z wojskami w latach 2015-2018 autor realizował obserwację niekontrolowaną[9] badacz podjął decyzję, że nie będzie brał udziału w eksploatacji usług teleinformatycznych, natomiast przygotowywał wdrożenia oraz monitorował system teleinformatyczny w zakresie bezpieczeństwa i dostępności usług telefonii i wideotelefonii. Proces obserwacji był przydatny w zakresie określenia stopnia wykorzystania usług teleinformatycznych oraz możliwości integracji usług kilku systemów teleinformatycznych. Obserwacje pozwoliły pozyskać materiał badawczy i były realizowane w ramach ćwiczeń pod kryptonimem: DRAGON-15, ANAKONDA-16, DRAGON-17, ANAKONDA-18. Natomiast wywiady z ekspertami autor przeprowadził w ramach ćwiczeń studyjnych organizowanych przez Akademię Sztuki Wojennej w latach 2022-2024. Mowa o ćwiczeniach pod kryptonimem: BRAMA MAZOWSZA-22, TWIERDZA-23, ŚWIDER-23, BRAMA-23, TWIERDZA-24, RYGLOWY ŚWIDER-24. Ponadto autor

[9] J. Lofland i in., Analiza układów społecznych. Przewodnik metodologiczny po badaniach jakościowych, Wydawnictwo Naukowe Scholar, Warszawa 2009.

posługiwał się wywiadem niestandaryzowanymi zadający tylko jedno lub kilka pytań wcześniej niezaplanowanych, a wynikających z przebiegu sytuacji badawczych. W ramach badań autor poddał analizie dostępną dokumentację techniczną. Porównywał także dokumenty planistyczne z obrazem pochodzącym z obserwacji.

ŚRODKI TRANSMISYJNE

Według autora artykułu największym przełomem okazały się największe ćwiczenia SZ RP pod kryptonimem ANAKONDA-16, podczas którego pierwszy raz uruchomiono rozległy system teleinformatyczny przetwarzający informacje o klauzuli do NATO RESTRICTED[10] i do ZASTRZEŻONE[11] włącznie. Natomiast podczas ćwiczenia pod kryptonimem ANAKONDA-16 po raz pierwszy podniesiono klauzulę przetwarzanych informacji do NATO SECRET[12] włącznie. Niemniej jednak wymiana informacji z układem pozamilitarnym w tym, ze służbami MSWiA nie była realizowana w oparciu o systemy przetwarzające informacje niejawne. Na rys. nr 1 autor przedstawił faktyczną wymianę informacji niejawnych w systemach teleinformatycznych.

Rys. 1.
Faktyczna wymiana informacji w niejawnych systemach teleinformatycznych

Źródło: opracowanie własne autora.

W związku z potrzebą wymiany informacji między służbami mundurowymi podczas działań kryzysowych (powódź, ochrona granicy państwa) już na etapie planowania i przygotowania działań w ramach fazy tworzenia procedur, planów oraz rozwijania zasobów potrzebnych do skutecznej reakcji na kryzys, konieczne i możliwe jest uzupełnienie szkieletu sieci teleinformatycznej

[10] Klauzule tajności NATO, https://bip.abw.gov.pl/bip/informacje-niejawne-1/ochrona-informacji-nie/153,ochrona-informacji-niejawnych-miedzynarodowych-w-sferze-cywilnej-i-wojskowej.html#2 (dostęp: 12.12.2024).

[11] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, t.j. Dz. U. z 2024 r. poz. 632, 1222, https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/ochrona-informacji-niejawnych-17646871 (dostęp: 12.12.2024).

[12] Zob. Klauzule tajności NATO https://bip.abw.gov.pl/bip/informacje-niejawne-1/ochrona-informacji-nie/153,ochrona-informacji-niejawnych-miedzynarodowych-w-sferze-cywilnej-i-wojskowej.html#2 (dostęp: 12.12.2024).

o mobilne elementy transmisyjne w postaci przenośno-przewoźnego terminala satelitarnego[13] oraz rozbudowanie systemu stacjonarnego o elementu podsystemu radioliniowo-kablowego w oparciu o ruchomy węzeł łączności cyfrowej[14] co pozwoli dołączyć kolejne dynamicznie powstające lokalizacje także te innych służb mundurowych. Na rysunkach nr 2 i 3 autor przedstawił środki transmisyjne możliwe do wykorzystania na potrzebę rozbudowy infrastruktury stacjonarnej resortu obrony narodowej.

Rys. 2.
Przenośno-Przewoźny Terminal Satelitarny PPTS-1,8 v.2

Źródło: https://wzl1.com.pl/produkt/przenosno-przewozny-terminal-satelitarny-ppts-18-v2, (dostęp:12.12.2024).

Rys. 3.
Ruchomy Węzeł Łączności Cyfrowej RWŁC-10/T

Źródło: https://www.wzl1.com.pl/produkt/ruchomy-wezel-lacznosci-cyfrowej-rwlc-10-t (dostęp: 12.12.2024).

Równie dużym wyzwaniem może być zachowanie integralności danych. Niemniej jednak z pomocą przyszły nowoczesne technologie sieciowe: tunelowanie i szyfrowania transmisji danych. Główny problem badawczy implikował kierunek dociekań autora w zakresie charakterystyki i zasad działania eksploatowanych rozwiązań.

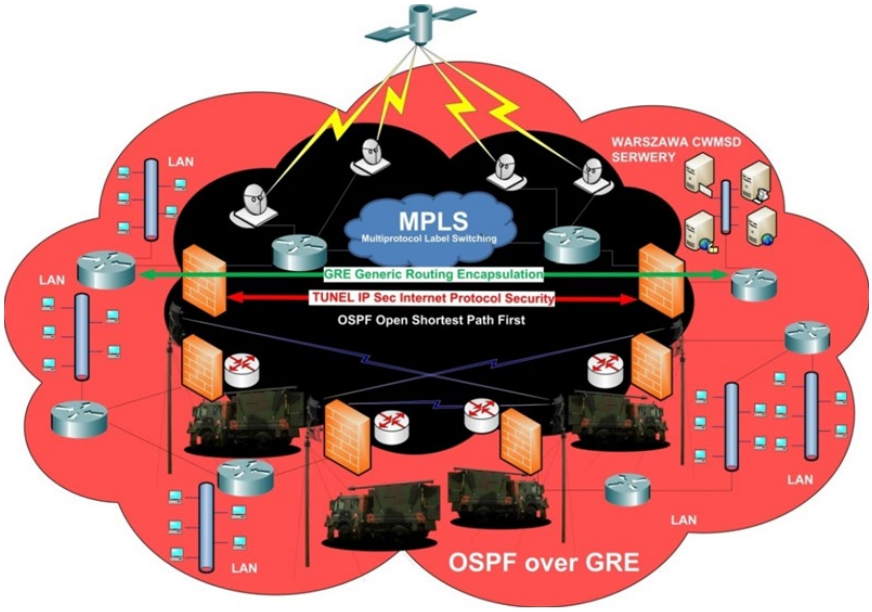
[13] Przenośno-Przewoźny Terminal Satelitarny PPTS-1,8 v.2, https://www.wzl1.com.pl/produkt/przenosno-przewozny-terminal-satelitarny-ppts-18-v2, (dostęp: 12.12.2024).

[14] Ruchomy Węzeł Łączności Cyfrowej RWŁC-10/T, https://www.wzl1.com.pl/produkt/ruchomy-wezel-lacznosci-cyfrowej--rwlc-10-t, (dostęp: 12.12.2024).

CHARAKTERYSTYKA ZAIMPLEMENTOWANYCH ROZWIĄZAŃ

Idee bezpiecznej wirtualnej sieci prywatnej Virtual Private Network VPN[15] opartej o protokoły trasowania oraz przełączania etykiet w oparciu o technologię Multiprotocol Label Switching MPLS[16] w sposób poglądowy autor przedstawił na rysunku nr 4.

Rys.4.
Schemat poglądowy rozwiązań zaimplementowanych w systemie teleinformatycznym



Źródło: A. Bogdański, M. Sielwanowski, *Information and Communication Networks of Modern Battlefield* [w.] *Security Forum 2014*, Univerzita Mateja Bela v Banskej Bystricy, Banska Bystrica Słowacja 2014, s. 90.

W technologii MPLS na brzegu sieci do pakietu dołączany był dodatkowy nagłówek, zwany etykietą wejściową, w którym znajdowała się informacja o następnym punkcie sieci, do którego pakiet miał dotrzeć. Pomiędzy punktami brzegowymi sieci podkładowej, gdzie znajdowały się adaptacyjne urządzenia zabezpieczające, budowany był tunel wykorzystujący protokół bezpiecznej wymiany informacji IP Sec[17] , który zapobiegał nieautoryzowanemu dostępowi. Natomiast tunel GRE[18] umożliwiał bezpieczną komunikację pomiędzy podsieciami, przez czarną chmurę[19], która była przezroczysta dla protokołu OSPF[20]. Urządzeniem szyfrującym mógł być dowolny

[15] Struktura sieci i metody projektowania z wykorzystanie IPSEC, PKI, SSL, https://www.vsx.pl/struktura-sieci-ipsec-ike-p-ki-ssl, (dostęp: 12.12.2024).

[16] E. Rosen i inni, MPLS Label Stack Encoding, RFC 3032, IETF, 2001, DOI: 10.17487/RFC3032, https://www.rfc-editor.org/info/rfc3032, (dostęp: 12.12.2024).

[17] IP Sec. Internet Protocol Security to zbiór protokołów służących implementacji bezpiecznych połączeń oraz wymiany kluczy szyfrowania pomiędzy komputerami Zob. Y. Nir, ChaCha20, Poly1305, and Their Use in the Internet Key Exchange Protocol (IKE) and IPsec, RFC 634, IETF, 2015, DOI:10.17487/RFC7634, https://www.rfc-editor.org/info/rfc7634, (dostęp: 12.12.2024).

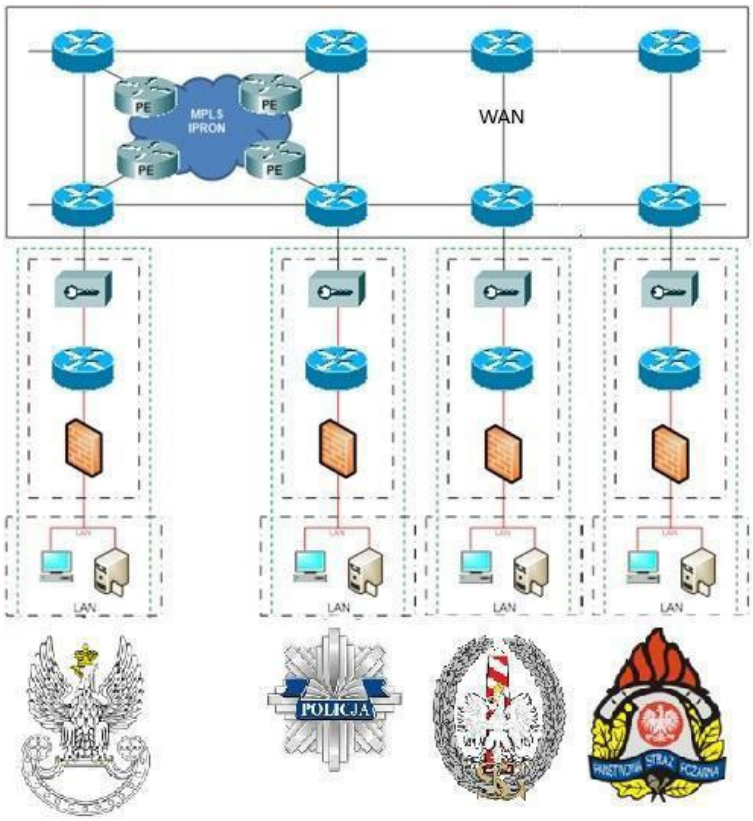
[18] GRE Generic Routing Encapsulation to o protokół tunelowania opracowany przez Cisco Systems, który może kapsułkować szeroką gamę protokołów warstwy sieciowej w wirtualnych łączach punkt-punkt lub łączach punkt-wielopunkt w sieci protokołu internetowego. Zob. C. Pignataro; R. Bonica; S. Krishnan. IPv6 Support for Generic Routing Encapsulation (GRE), 2015, IETF, DOI:10.17487/RFC7676, https://www.rfc-editor.org/info/rfc7676, (dostęp: 12.12.2024).

[19] Czarna chmura to obszar sieci transmisyjnej, gdzie enkapsulowany ruch sieciowy może być przesłany także przez otwarte komercyjne środki transmisyjne.

[20] OSPF Open Shortest Path First to protokół trasowania oparty na analizie stanu łącza gdzie pierwszeństwo ma najkrótsza ścieżka Zob. R. Valadas, Protokoły OSPF i IS-IS: od zasad routingu stanu łącza do technologii, CRC Press, 2018,

odpowiedni do danego systemu teleinformatycznego szyfrator np. urządzenie kryptograficzne, urządzenie podwójnego zastosowania Cisco ASA[21], czy komercyjny router wyposażony we wspomnianą powyżej technologię IP Sec. W związku z brakiem dostępu do dokumentacji technicznej urządzeń komercyjnych w Siłach Zbrojnych RP od 2016 roku urządzenia podwójnego zastosowania był sukcesywne wymieniane na narodowe lub koalicyjne rozwiązania szyfrujące, urządzenia kryptograficzne. Węzeł łączności zawierał od jednego do kilku węzłów dostępowych po jednym dla każdego z eksploatowanych systemów teleinformatycznych. Zwyczajowo węzły łączności zapewniały dostęp do kilku systemów teleinformatycznego wsparcia dowodzenia[22], dlatego posiadał kilka urządzeń szyfrujących oddzielnych dla każdego systemu teleinformatycznego lub jego instancji. Topologię systemu transmisyjnego i sposób dołączenia węzłów klienckich służb mundurowych podległych szefowi MSWiA przedstawiono na rys. nr 5.

Rys. 5.
Topologia systemu transmisyjnego, dołączenie kolejnych lokalizacji służb mundurowych podległych szefowi MSWiA



Źródło: Opracowanie własne na podstawie slajdu z prezentacji z końcowej konferencji planistycznej do ćwiczenia pod kryptonimem DRAGON-15, autor pierwowzoru M. Gruszka[23].

DOI:10.1201/9780429027543, https://doi.org/10.1201/9780429027543, (dostęp:12.12.2024).

[21] Cisco ASA Cisco Adaptive Security Appliances to linia urządzeń zabezpieczeń sieciowych firmy Cisco Systems. Zob. M. Lewis, Intro to Cisco ASA, NCC Group, 2017, https://research.nccgroup.com/2017/09/20/cisco-asa-series-part-one-intro-to-the-cisco-asa, (dostęp: 12.12.2024).

[22] P. Dela (red.) Vademecum łącznościowca, sygn. S/8571, Akademia Obrony Narodowej, Warszawa, 2012, s. 150.

[23] Idee struktury sieci szkieletowej oraz kluczowe elementy dołączanych komponentów zaproponowała M. Gruszka. Pomysł był wielokrotnie modyfikowany i dostosowywany do potrzeb konkretnej instancji systemu teleinformatycznego.

ZASADA DZIAŁANIA ZAPROPONOWANYCH ROZWIĄZAŃ

Zadaniem wspomnianego wcześniej protokołu OSPF było wybranie najkrótszej trasy do celu. Komunikacja pomiędzy lokalnymi sieciami była szyfrowana symetrycznie[24]. Rozwiązanie to cechowała duża szybkość i wydajność, a także skalowalność. Możliwa była także implementacja rozwiązania systemu zarządzania jakością usług QoS[25] co nie było bez znaczenia podczas transmisji cyfrowego głosu za pomocą protokołu VoIP[26] oraz obrazu i głosu w ramach wideokonferencji[27]. Rozwiązania związane z routingiem i tunelowaniem rozwijały się w sposób bardzo dynamiczny. Wprowadzono w szkielecie protokół routingu BGP[28], a połączenia pomiędzy sieciami lokalnymi oparto były na technologii DMVPN[29]. Punkt styku pomiędzy węzłem łączności, a systemem transmisyjnym był ustanowiony na węźle dostępowym. Wszystkie podsystemy transmisyjne były podłączane bezpośrednio do niego. Kolejną wykorzystywaną technologią był wirtualne trasowanie i przekazywanie Virtual Routing and Forwarding VRF[30]. VRF to technologia, która umożliwiała jednoczesne współistnienie wielu instancji tablicy routingu w tym samym routerze. „Wirtualne routing i przekazywanie dzieli router fizyczny na wiele routerów wirtualnych. Magistrali sterowania i płaszczyzny danych są izolowane w każdym wirtualnym routerze; ruch nie przepływa przez wirtualne routery. Funkcja VRF umożliwia jednoczesne współistnienie wielu instancji niezależnych tabel routingu w ramach tego samego routera. Liczba maksymalnych konfigurowalnych plików VRF w przełączniku zależy od platformy”[31]. Na rysunku nr 6 przedstawiono przykładową konfigurację wirtualnego trasowania i przekazywania Virtual Routing and Forwarding.

---

[24] Szyfrowanie symetryczne to algorytm kryptograficzny, który do szyfrowania i deszyfrowania tekstu jawnego wykorzystuje te same klucze. B. Schneier, Kryptografia dla praktyków: protokoły, algorytmy i programy źródłowe w języku C. Warszawa: Wydawnictwa Naukowo-Techniczne, 2002, s. 30-31

[25] QoS Quality of Service, jakość usługi, całość charakterystyk usługi telekomunikacyjnej stanowiących podstawę do wypełnienia wyrażonych i zaspokajanych potrzeb użytkownika tej usługi. Zob. R. S. Zahidur, Advanced Quality of Service (QoS), OmniScriptum GmbH & Co. KG, 2020, Saarbrücken Niemcy, s. 7.

[26] VOIP Voice over Internet Protocol, cyfrowa telefonia. Zob. J. Albritton, A. Ortiz, R. Wines i inni, Video Teleconferencing for Disease Prevention, Diagnosis, and Treatment, National Library of Medicine, Rockville Pike, USA, s. 256–266. DOI:10.7326/M21-3511, https://pubmed.ncbi.nlm.nih.gov/34871056, (dostęp: 13.12.2024).

[27] Zob. A. Bogdański, Ł. Barański, Wybrane rozwiązania oraz usługi wdrożone w sieciach teleinformatycznych Wojsk Lądowych, Selected solutions and services implemented in land forces ict networks, [w:] Bezpieczeństwo i Administracja. Zeszyty Naukowe Wydziału Bezpieczeństwa Narodowego nr 1 (1) 2014, wydanie 1, Akademia Obrony Narodowej, Warszawa 2014, s. 167–180, ISSN 2084-7297.

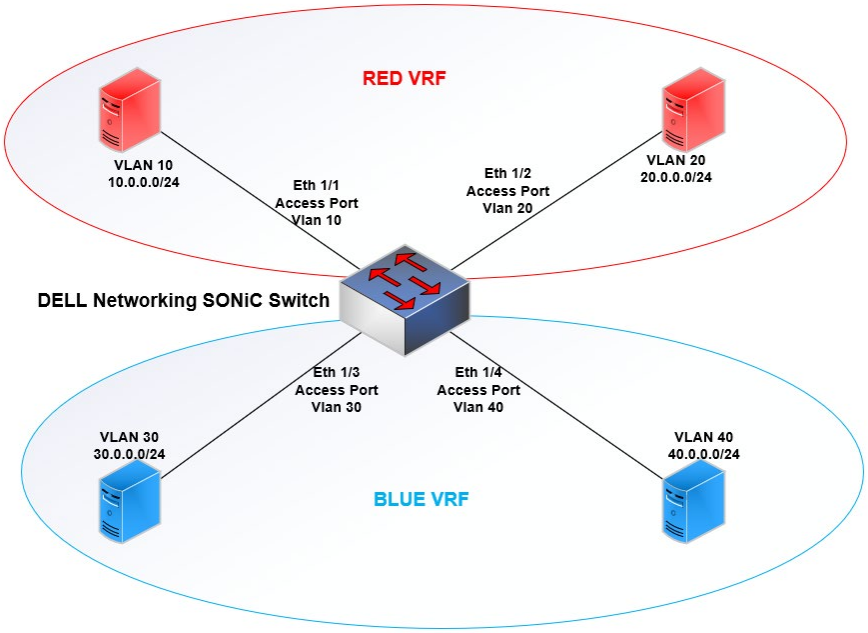
[28] S. Hares, A. Retana, BGP-4 Implementation Report, RFC 4276, IETF, 2006, DOI:10.17487/RFC4276, https://datatracker.ietf.org/doc/html/rfc4276, (dostęp: 13.12.2024).

[29] DMVPN Dynamic Multipoint Virtual Private Network. Zob. S. H. Kurniadi, E. Utami, F. W. Wibowo, Building Dynamic Mesh VPN Network using MikroTik Router, 2018, DOI:10.1088/1742-6596/1140/1/012039, ISSN 1742-6596, https://iopscience.iop.org/article/10.1088/1742-6596/1140/1/012039, (dostęp: 13.12.2024).

[30] VRF Virtual Routing and Forwarding. Zob. Virtual Route Forwarding Design Guide, https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucme/vrf/design/guide/vrfDesignGuide.html

[31] Dell Networking SONiC: Konfigurowanie wirtualnego routingu i przekazywania, https://www.dell.com/support/kbdoc/pl-pl/000218893/dell-networking-sonic-how-to-configure-virtual-routing-and-forwarding-vrf, (dostęp: 13.12.2024).

Rys. 6.
Przykładowa konfiguracja wirtualnego trasowania Virtual Routing and Forwarding



Źródło: https://www.dell.com/support/kbdoc/pl-pl/000218893/dell-networking-sonic-how-to-configure-virtual-routing-and-forwarding-vrf (dostęp: 13.12.2024).

Tunel GRE umożliwiające bezpieczną komunikację pomiędzy podsieciami, była przezroczysta dla protokołu OSPF. Ponadto tunele były budowane dynamicznie w oparciu o redundantne koncentratory. Powyższe poglądowe schematy przedstawiały wykorzystane mechanizmy w oparciu o jeden środek transmisyjny. W tym przypadku oparte o transmisję przez RWŁC[32]. Aby zachować redundancje w zakresie szkieletu należy zaplanować alternatywną transmisję w oparciu o PPTS[33]. Na potrzeby dołączenia kilku redundantnych środków transmisji wykorzystano znany z Internetu protokołu oparty o routing do sąsiada BGP. Rozróżniamy dwie formy sąsiedztwa zestawionej sesji, Internal BGP (iBGP)[34] oraz External BGP (eBGP)[35]. Sesje *Internal* były zestawione z routerem z naszego własnego systemu autonomicznego AS[36], a sesje typu *External* były wszystkimi sesjami zestawionymi z routerami poza naszym systemem autonomicznym. Połączenia budowane były w oparciu o zbiór protokołów służących implementacji bezpiecznych połączeń oraz wymiany kluczy IP Sec. Router kliencki zapewniał dostęp sieci lokalnej do rozległej sieci transmisyjnej. Na jego bazie tworzone były tunele tworzące logiczną sieć wymiany danych. Urządzenie szyfrujące zapewniały poufność i integralność wymienianych informacji. Na bazie tych urządzeń budowane były tunele zgodnie z hierarchią przepływu danych. Router agregacyjny budował kanały, tunele dla poszczególnych sieci, budując logiczną infrastrukturę transmisyjną

[32] Zob. M. Marczyk, Wojskowe węzły teleinformatyczne w systemie obronnym państwa, Akademia Sztuki Wojennej, Warszawa 2016, s. 41, ISBN 9788375235289.

[33] Ibidem.

[34] iBGP, Internal Border Gateway Protocol, jest kluczowym elementem nowoczesnej infrastruktury sieciowej, szczególnie w dużych sieciach korporacyjnych, https://www.noction.com/resource_center/ibgp, (dostęp: 13.12.2024).

[35] eBGP, Jak skonfigurować External BGP, https://networklessons.com/bgp/how-to-configure-ebgp-external-bgp

[36] Podstawą funkcjonowania BGP jest system autonomiczny, Autonomous System, AS, czyli sieć lub grupa sieci pod wspólną administracją i ze wspólną polityką trasowania. A Border Gateway Protocol 4 (BGP-4) RFC 1771 ciąg systemów autonomicznych, będących ścieżką do docelowej sieci IP, https://datatracker.ietf.org/doc/html/rfc1771, (dostęp: 13.12.2024).

oraz agregował je w jeden strumień transmisyjny. Zaplanowano kanały VPN, które były tworzone w oparciu o tunele GRE i osobne instancje tablic routingu VRF. Kanały VPN tworzono zgodnie z kierunkiem przepływu danych w sieciach klienckich w topologii koncentrator i niższy szczebel w strukturze, a w szczególnych przypadkach mogły być wykonywane dodatkowe połączenia w celu zapewnienia niezawodność lub replikacji danych. Do tworzenia kanałów VPN należało użyć technologii tunelowania wielopunktowego z uwagi na możliwość dynamicznego zestawiania połączeń pomiędzy klientami, a dla dodatkowych połączeń standardowych tuneli. Aby rozwiązać wspomniany problem replikacji danych pomiędzy głównym i zapasowym stanowiskiem dowodzenia zaplanowano dodatkowe wirtualne redundantne połączenia. Na tej samej zasadzie tworzone były tunele IP Sec i tunele wymiany danych pomiędzy routerami klienckimi. Koncentratory wyznaczono w punktach agregacyjnych wynikających z kierunku przepływu danych. Urządzenia podstawowe były umieszczane na stanowisku dowodzenia. Dopiero na tak przygotowanej infrastrukturze funkcjonowały usługi podstawowe telefonia VoIP, wideotelefonia VTC[37] czy usługi dedykowane NATO FAS[38]. Koncepcja kolejnych iteracji integracji, docelowo dołączenie służb mundurowych podległych szefowi MSWiA do instancji narodowej OPER-T Systemu Teleinformatycznego Polish Mission Network zgodnie z ideą Federated Mission Networking przedstawiono na rys nr 7[39].

Rys. 7
Możliwa wymiana informacji w niejawnych systemach teleinformatycznych

Źródło: opracowanie własne autora.

[37] E. Jackman, New Video Conferencing System Streamlines Firefighter Training, Peoria, Arizona: Peoria Times, 2010, https://www.peoriatimes.com/articles/2010/02/19/news/news06, (dostęp: 12.12.2024).

[38] NATO Functional Area Service. Zob. A. Bogdański, Przeznaczenie podstawowych usług funkcjonalnych NATO FAS - wymagania stawiane administratorom usług w zakresie wsparcia teleinformatycznego, [w:] Przegląd Sił Zbrojnych 2022, nr 5, s. 64-65, ISSN 2353-1975, https://zbrojni.blob.core.windows.net/pzdata2/TinyMceFiles/psz5_2022.pdf, (dostęp: 13.12.2024).

[39] A. Bogdański, Federated Mission Networking w ujęciu narodowych dokumentów doktrynalnych: aspekt bezpieczeństwa teleinformatycznego w Bezpieczeństwo działań w cyberprzestrzeni: wybrane aspekty. T. 2, Techniczne aspekty cyberprzestrzeni, red. M. Marczyk, M. Stolarz, B. Terebiński, Akademia Sztuki Wojennej, Warszawa, 2022, ISBN 978-83-8263-226-2.

USŁUGI PODSTAWOWE TELEFONIA i WIDEOTELEFONIA

Wdrożenie telefonii i wideotelefonii w zintegrowanym systemie teleinformatycznym służb mundurowych resortów MON i MSWiA jest możliwe w oparciu o urządzenia końcowe wspierające uniwersalny stos protokołów H323[40] lub protokół SIP[41]. Podczas prowadzonych badań potencjał telefonii VoIP oparty był na rozwiązaniach (centralach telefonicznych) Cisco Call Manager[42], który ewoluowały do Cisco Unified Communications Manager[43]. CUCM to oprogramowanie zarządzające urządzeniami i połączeniami VoIP. Usługa ta współpracowała z usługą Cisco WebEx[44] posiadającą zdolność udostępniania dokumentu, aplikacji czy pulpitu, współcześnie wspomaganą także przez sztuczną inteligencję. Tak zbudowany system umożliwiał samodzielne prezentowanie treści[45]. W praktyce podczas realizacji badań, obserwacji funkcjonowały niezależne usługi telefonii VoIP oraz system wideokonferencyjny VTC. Lokalnie na stanowiskach dowodzenia brygad telefonia VoIP zbudowana była na bazie Cisco Call Manager Express (CME)[46] przekształcony w 2020 roku do centralnie zarządzanego Cisco Unified Communications Manager Express (CUCME)[47]. Lokalne centrale telefoniczne Cisco Call Manager Express stały się rozwiązaniem redundantnym przejmującym zadani w przypadku braku połączenia ze szkieletem sieci.

Dodatkowo infrastruktura zawierała bramę głosową Gate Keeper (GK)[48] służącą do kierowania routingu telefonicznego do odpowiednich lokalizacji. W systemie teleinformatycznym eksploatowanym podczas ćwiczeń funkcjonowały niezależne usługi telefonii VoIP oraz wideokonferencyjny VTC. Pełna integracja usług na bazie Cisco Unified Communication Manager nastąpiła dopiero w 2019 roku. Od 2020 roku infrastruktura zawierała media serwer integrujący wszystkie elementy, łącznie z jednolitym z planem numerowym.

Jako urządzenia końcowe VoIP wykorzystywane były telefony firmy Cisco. Systemy telekonferencyjne VTC mogły funkcjonować w oparciu o niezależne mostki wideokonferencyjne. Integracja nastąpiła za pomocą brzegowych bram głosowych Session Border Controller (SBC)[49]. Każdy SBC terminował strumień głosowy połączeń wychodzących na zewnątrz i przekazywał je dalej, maskując adres urządzenia końcowego. Routing telefoniczny był oparty na zasadzie hop-by-hop.

---

[40] M. Bromirski, Telefonia VoIP. Multimedialne sieci IP., Warszawa: BTC, 2006, s. 9, ISBN 83-60233-07-1.

[41] J. Rosenberg i inni, SIP: Session Initiation Protocol, RFC 3261, IETF, 2002, s. 10, DOI: 10.17487/RFC3261, https://datatracker.ietf.org/doc/html/rfc3261#page-9, (dostęp: 13.12.2024).

[42] Cisco Unified Communications Manager (CallManager) https://www.cisco.com/c/en/us/products/unified-communications/unified-communications-manager-callmanager/index.html, (dostęp: 13.12.2024).

[43] Ibidem.

[44] AI-driven collaboration and customer experience, https://www.webex.com, (dostęp: 13.12.2024).

[45] Zob. A. Bogdański, A. Zelichowski, Możliwości wykorzystania wojskowych sieci informatycznych w celu prowadzenia badań społecznych w resorcie obrony narodowej, Obronność Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej, nr 2(6), 2013, Warszawa s. 17, ISSN: 2299-2316.

[46] Cisco Unified Communications Manager Express, https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-express/series.html, (dostęp: 13.12.2024).

[47] Ibidem.

[48] Understanding H.323 Gatekeepers, https://www.cisco.com/c/en/us/support/docs/voice/h323/5244-understand-gatekeepers.html, (dostęp: 13.12.2024).

[49] J. Hautakorpi, G. Camarillo, R. Penfield i inni, Requirements from SIP (Session Initiation Protocol) Session Border Control Deployments, 2018, IETF. DOI:10.17487/RFC5853, (dostęp: 13.12.2024).

Pełny routing telefoniczny pomiędzy jednostkami podległymi zapewniał przełożony. Jednostki podległe musiały skonfigurować domyślne połączenie do przełożonego oraz dodatkowo mogły skonfigurować połączenia bezpośrednie z sąsiadami i zapasowe połączenie domyślne poprzez sąsiada. Protokołem sygnalizacyjnym łączącym elementy brzegowe był protokół SIP.

Usługa wideokonferencyjna podczas międzynarodowych ćwiczeń pod kryptonimem ANAKONDA-14 oparta była na mostku Cisco TelePresence MCU 3450. W czasie kolejnych ćwiczeń eksploatowano mostek telekonferencyjny typu Cisco TelePresence MCU 4515. Wyżej wymienione urządzenia posiadały funkcjonalność Gate Kiper o potencjale jedynie 25 terminali końcowych oraz możliwość zestawienia kilku konferencji jednocześnie, z zastrzeżeniem maksymalnej liczby do 15 użytkowników z jakością HD lub do 30 użytkowników ze standardową niższą jakością. W związku z dużym zapotrzebowaniem na usługę VTC system został rozbudowany o strażnika stref i dodatkowy mostek Cisco TelePresence MCU 4210, znajdujący się w zapasowej lokalizacji. W trakcie ćwiczenia doposażono system w kolejne dwa zintegrowane mostki Cisco TelePresence MCU 5320. Dodatkowo wojska specjalne eksploatowały własny mostek Cisco TelePresence MCU 4205. Wszystkie terminale VTC były objęte procesem rejestracyjnym. Terminale mogły bezpośrednio wydzwaniać się między sobą, zarówno po IP, jak i po numerach. Ponadto terminale firm trzecich np. Polycom (obecnie Poly firmy HP)[50] posiadały niezależną funkcjonalność wideokonferencji, mogły zestawiać własne wideokonferencje do maksymalne 4 użytkowników[51].

Rys. 8
Wykorzystanie terminala Cisco TelePresence VX Tactical w warunkach polowych

Źródło: https://www.dekom.com/en/video-conferencing/product/cisco-telepresence-vx-tactical, (dostęp: 13.12.2024).

PODSUMOWANIE

Poruszana tematyka nie została wyczerpana, a artykuł został oddany do wydawnictwa przed wejściem w życie ustawy z dnia 5 grudnia 2024 r. *o ochronie ludności i obronie cywilnej*[52]. Reali-

[50] Polycom video- conferencing, https://www.hp.com/gb-en/poly/video-conferencing.html, (dostęp: 13.12.2024).

[51] Zob. A. Bogdański, Bezpieczne usługi podstawowe wykorzystywane w działaniach na potrzeby ochrony ludności w warunkach wojny. W: Ochrona ludności w czasie wojny w Ukrainie, red. B. Pacek, D. Kaźmierczak, P. Pacek, Rytm Oficyna Wydawnicza, Siedlce, 2024, s. 212-228, ISBN 978-83-67927-26-0

[52] Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U.2024.1907)

zowane obecnie badania dotyczą możliwej integracji usług podstawowych opartych o produkty firmy Microsoft oraz ewentualną możliwość udostępnienia usług z pakietu NATO FAS (Functional Area Services), na potrzeby systemu ochrony ludności i obrony cywilnej dla którego przedmiotowa ustawa stworzyła podwaliny.

Badania eksploatowanych w SZ RP systemów teleinformatycznych, w szczególności rozwiązań technicznych podnoszących bezpieczeństwo transmisji pozwoliło autorowi na sformułowanie odpowiedź na pytanie: Czy jest możliwe dostosowanie systemu transmisyjnego SZ RP na potrzeby bezpiecznej wymiany informacji w ramach służb mundurowych? Scharakteryzowane w oparciu o wieloletnie badania rozwiązania dostępne na rynku komercyjnym potwierdzają hipotezę postawioną przez autora. Wymiana informacji w ramach służb zarówno na poziomie niższych warstw sieciowych, od dostępu do sieci do warstwy transportowej, ale także na poziomie warstwy aplikacji przy zastosowaniu komercyjnych usług podstawowych jest możliwa do osiągnięcia. Służby mundurowe posiadają podobne technologie sieciowe co daje możliwość integracji systemów teleinformatycznych. MON i MSWiA posiadają grupę usług podstawowych takich jak telefonia czy wideotelefonia w ramach, których przesyłanie informacji między systemami różnych resortów jest możliwe do zrealizowania przy niewielkim nakładzie pracy administratorów w zakresie konfiguracji usług. Przedmiotowe standardy zostały szczegółowo scharakteryzowane w artykule, omówiono także sposób implementacji konkretnych rozwiązań. W oparciu o badania autor twierdzi, że po uzupełnieniu infrastruktury stacjonarnej o środki transmisyjne wykorzystywane w resorcie obrony narodowej jest możliwe stworzenie sieci podkładowej umożliwiającej przepływy informacyjne między służbami na potrzeby realizacji postawionych zadań w zakresie. Badania wykazały, że integracja systemów transmisyjnych MON i MSWiA. jest możliwa przy zaimplementowaniu ogólnodostępnych protokołów sieciowych. Ponadto możliwe jest zapewnienie bezpieczeństwa przesyłanych między resortami informacji niejawnych w oparciu o komercyjne lub dedykowane urządzenia szyfrujące. Interoperacyjność usług telefonii i wideotelefonii między służbami mundurowymi resortów MON i MSWiA można zapewnić poprzez zaimplementowanie uniwersalnego stosu protokołów sygnalizacyjnych, jest możliwe wdrożenie technologii opartej o powszechnie dostępne rozwiązania komercyjne, niemniej jednak o pełnej interoperacyjność systemów teleinformatycznych można mówić dopiero po osiągnięciu zdolności udostępnianie dedykowanych usług innym służbom. Jak wynika z badań realizowanych podczas największych ćwiczeń międzynarodowych, udostępnienie usługi VoiP i usługi wideokonferencji jest możliwe. Autor wykrył także ograniczenia wpływające na możliwość integracji w ramach służb mundurowych systemów teleinformatycznych, zarówno na poziomie transmisyjnym jak i usług. Aby scharakteryzowane technologie wdrożyć niezbędnym jest przygotowane odpowiedniej liczby specjalistów w zakresie technologii sieciowych oraz usług podstawowych zarówno po stronie Sił Zbrojnych Rzeczypospolitej Polskiej jak i służb mundurowych podległych pod szefa Ministerstwa Spraw Wewnętrznych i Administracji. Czas i koszty przygotowania personelu zależą od zakresu obowiązków specjalistów. Wymagają one jednak specjalistycznego przeszkolenia żołnierzy, funkcjonariuszy lub pracowników cywilnych służb posiadających unikatową wiedzę z zakresu technologii sieciowych. To tylko pierwszy

etap. Badania prowadzone przez autora w zakresie integracji usług podstawowych opartych o technologie firmy Microsoft to kolejne poważne, niemniej jednak realizowalne wyzwanie.

Dzięki rozwiązaniom przedstawionym w powyższym artykule, systemy teleinformatyczne eksploatowane w SZ RP mogą dawać gwarancję bezpieczeństwa w zakresie dostępności, poufność, autentyczność i integralność przesyłanych informacji. Redundancja w zakresie transmisji zapewnia stałą dostępność do usług. Autor w powyższym artykule nie tylko scharakteryzował, ale także przedstawił sposób wdrożenia i ewolucję wybranych rozwiązań zapewniających powyższe wymagania. Celem badań była identyfikacja możliwości dostosowania systemu transmisyjnego Sił Zbrojnych Rzeczypospolitej Polskiej na potrzeby bezpiecznej wymiany informacji w ramach służb mundurowych. Głównym problemem badawczym, który autor sobie postawił było uzyskanie odpowiedzi na pytanie: W jaki sposób można zaadoptować rozwiązania stosowana w SZ RP dla zwiększenia bezpieczeństwa transmisji w systemach łączności służbach mundurowych? Adaptacja rozwiązań wykorzystywanych w SZ RP do zapewnienia bezpieczeństwa transmisji w łączności służb mundurowych może zostać przeprowadzona dzięki zastosowaniu komercyjnych technologii, takich jak wspomniane w treści artykułu oferowane przez firmy Cisco Systems czy Polycom HP. Zmiana urządzeń szyfrujących z komercyjnych na urządzenia kryptograficzne umożliwi w przyszłości podniesienie klauzuli przetwarzanych informacji zgodnie z potrzebami organizatora systemu teleinformatycznego, a zwłaszcza zgodnie z wymaganiami w zakresie bezpieczeństwa użytkowników danego systemu. Podniesienie klauzuli przetwarzanych informacji pozwoli na wykorzystanie systemu teleinformatycznego na potrzeby działań operacyjnych przy współudziale służb mundurowych podległych szefowi MWSiA. Ze względu na jawny charakter publikacji autor przedstawił wybrane tylko jawne dostępne rozwiązania. W kolejnym etapie prac badawczych autor planuje skupić uwagę na badaniu problemów związanych z integracją innych usług podstawowych, zarządzaniem poziomem usług, zarządzaniem dostępnością i przepustowością łączy. Nie mniej istotne będą kwestie bezpieczeństwa teleinformatycznego uwzględniające zagadnienia dotyczące kryptografii. Integracja systemów teleinformatycznych eksploatowanych przez Siły Zbrojne RP z systemami teleinformatycznymi służb mundurowych podległych MWSiA z punktu widzenia bezpieczeństwa narodowego jest według autora sprawą kluczową. Może usprawnić wymianę informacji w czasie pokoju, kryzysu, a zwłaszcza ewentualnej wojny. W przyszłości autor widzi możliwość wymiany informacji także na niższych poziomach: dowódcy dywizji, brygady czy pułku z komendantem wojewódzkim policji, komendantem wojewódzkim państwowej straży pożarnej czy komendantem oddziału straży granicznej. Integracja systemów teleinformatycznym na poziomie taktycznym będzie przedmiotem kolejnych badań autora, a zagadnienia z nią związane autor zgłębia w ramach obecnie prowadzonych ćwiczeń z udziałem układu pozamilitarnego.

BIBLIOGRAFIA

REFERENCES LIST

PIŚMIENNICTWO

LITERATURE

Terebiński B., Teleinformatyka wojskowa, Akademia Sztuki Wojennej, Warszawa, 2022, ISBN 978-83-8263-158-6.

Marczyk M., Terebiński B., System łączności brygady obrony terytorialnej (BOT) w wojskowym systemie telekomunikacyjnym, Bellona, Warszawa 2021, DOI:10.5604/01.3001.0015.6659 .

Strzałek M., Pałka P., Problematyka poufności, autentyczności, integralności oraz niezaprzeczalności danych w systemach wieloagentowych, Politechnika Warszawska, 2012, https://delibra.bg.polsl.pl/Content/76503/BCPS-86045_2012_Problematyka-poufnos_0000.pdf.

Pelc M., Elementy metodologii badań naukowych, Akademia Obrony Narodowej, Warszawa 2012, ISBN 978-83-7523-167-0.

Rosen E. i inni, MPLS Label Stack Encoding, RFC 3032, IETF, 2001, DOI: 10.17487/RFC3032, https://www.rfc-editor.org/info/rfc3032.

Schneier B., Kryptografia dla praktyków: protokoły, algorytmy i programy źródłowe w języku C. Warszawa: Wydawnictwa Naukowo-Techniczne, 2002, ISBN 83-204-2678-2.

Nir Y, ChaCha20, Poly1305, and Their Use in the Internet Key Exchange Protocol (IKE) and IPsec, RFC 634, IETF, 2015, DOI:10.17487/RFC7634, https://www.rfc-editor.org/info/rfc7634.

Pignataro C., Bonica R., Krishnan S., IPv6 Support for Generic Routing Encapsulation (GRE), IETF, 2015, DOI:10.17487/RFC7676, https://www.rfc-editor.org/info/rfc7676.

Valadas R., Protokoły OSPF i IS-IS: od zasad routingu stanu łącza do technologii, CRC Press, 2018, DOI:10.1201/9780429027543, https://doi.org/10.1201/9780429027543.

Lewis M., Intro to Cisco ASA, NCC Group, 2017, https://research.nccgroup.com/2017/09/20/cisco-asa-series-part-one-intro-to-the-cisco-asa.

Dela P. (red.) Vademecum łącznościowca, sygn. S/8571Akademia Obrony Narodowej, Warszawa, 2012.

Zahidur R. S., Advanced Quality of Service (QoS), OmniScriptum GmbH & Co. KG, 2020, Saarbrücken Niemcy.

Albritton J., Ortiz A., Wines R. i inni, Video Teleconferencing for Disease Prevention, Diagnosis, and Treatment, National Library of Medicine, Rockville Pike, USA.

Hares S., Retana A., *BGP-4 Implementation Report*, RFC 4276, IETF, 2006, DOI:10.17487/RFC4276, https://datatracker.ietf.org/doc/html/rfc4276.

Kurniadi S. H., Utami E., Wibowo F. W., Building Dynamic Mesh VPN Network using MikroTik Router, 2018, DOI:10.1088/1742-6596/1140/1/012039, ISSN 1742-6596.

Bogdański A, Barański Ł, Wybrane rozwiązania oraz usługi wdrożone w sieciach teleinformatycznych Wojsk Lądowych, Selected solutions and services implemented in land forces ict networks, [w:] Bezpieczeństwo i Administracja. Zeszyty Naukowe Wydziału Bezpieczeństwa Narodowego nr 1 (1) 2014, Akademia Obrony Narodowej, Warszawa, 2014, ISSN 2084-7297.

Marczyk M., Wojskowe węzły teleinformatyczne w systemie obronnym państwa, Akademia Sztuki Wojennej, Warszawa, 2016, ISBN 9788375235289.

E. Jackman, New Video Conferencing System Streamlines Firefighter Training, Peoria, Arizona: Peoria Times, 2010, https://www.peoriatimes.com/articles/2010/02/19/news/news06.

Bogdański A., Przeznaczenie podstawowych usług funkcjonalnych NATO FAS - wymagania stawiane administratorom usług w zakresie wsparcia teleinformatycznego, [w:] Przegląd Sił Zbrojnych 2022, nr 5, Warszawa, ISSN 2353-1975.

Bogdański A., Federated Mission Networking w ujęciu narodowych dokumentów doktrynalnych: aspekt bezpieczeństwa teleinformatycznego w Bezpieczeństwo działań w cyberprzestrzeni : wybrane aspekty. T. 2, Techniczne aspekty cyberprzestrzeni, red. Marczyk M., Stolarz M., Terebiński B., Akademia Sztuki Wojennej, Warszawa, 2022, ISBN 978-83-8263-226-2.

Bromirski M., Telefonia VoIP. Multimedialne sieci IP., Warszawa: BTC, 2006, ISBN 83-60233-07-1.

Rosenberg J. i inni, *SIP: Session Initiation Protocol,* RFC 3261, IETF, 2002, DOI: 10.17487/RFC3261, https://datatracker.ietf.org/doc/html/rfc3261#page-9

Bogdański A., Zelichowski A., Możliwości wykorzystania wojskowych sieci informatycznych w celu prowadzenia badań społecznych w resorcie obrony narodowej, Obronność Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej, nr 2(6), 2013, Warszawa, ISSN 2299-2316.

Hautakorpi J., Camarillo G., Penfield R.i inni, Requirements from SIP (Session Initiation Protocol) Session Border Control Deployments, 2018, IETF. DOI:10.17487/RFC5853.

Bogdański A., Bezpieczne usługi podstawowe wykorzystywane w działaniach na potrzeby ochrony ludności w warunkach wojny. W: Ochrona ludności w czasie wojny w Ukrainie, Rytm Oficyna Wydawnicza, Siedlce, 2024, red. B. Pacek, D. Kaźmierczak, P. Pacek, U2024, ISBN 978-83-67927-26-0.

ŹRÓDŁA

SOURCES

Ustawa z dnia 5 lipca 2018 r.o krajowym systemie cyberbezpieczeństwa Dz.U.2024.1077 t.j

https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/krajowy-systemcyberbezpieczenstwa-18746756

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, t.j. Dz. U. z 2023 r. poz. 122, z 2024 r. poz. 834, 1222, 1473. 1572, https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/zarzadzanie-kryzysowe-17348453

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, t.j. Dz. U. z 2024 r. poz. 632, 1222, https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/ochrona-informacji-niejawnych-17646871.

Klauzule tajności NATO, https://bip.abw.gov.pl/bip/informacje-niejawne-1/ochrona-informacji-nie/153,ochrona--informacji-niejawnych-miedzynarodowych-w-sferze-cywilnej-i-wojskowej.html#2.

Przenośno-Przewoźny Terminal Satelitarny PPTS-1,8 v.2, https://www.wzl1.com.pl/produkt/przenosno-przewozny-terminal-satelitarny-ppts-18-v2.

Ruchomy Węzeł Łączności Cyfrowej RWŁC-10/T, https://www.wzl1.com.pl/produkt/ruchomy-wezel-lacznosci--cyfrowej-rwlc-10-t.

Struktura sieci i metody projektowania z wykorzystanie IPSEC, PKI, SSL, https://www.vsx.pl/struktura-sieci-ipsec-ike-pki-ssl.

Dell Networking SONiC: Konfigurowanie wirtualnego routingu i przekazywania, https://www.dell.com/support/kbdoc/pl-pl/000218893/dell-networking-sonic-how-to-configure-virtual-routing-and-forwarding-vrf.

iBGP, *Internal Border Gateway Protocol, jest kluczowym elementem nowoczesnej infrastruktury sieciowej, szczególnie w dużych sieciach korporacyjnych*, https://www.noction.com/resource_center/ibgp.

eBGP, Jak skonfigurować External BGP, https://networklessons.com/bgp/how-to-configure-ebgp-external-bgp

A Border Gateway Protocol 4 (BGP-4) RFC 1771, https://datatracker.ietf.org/doc/html/rfc1771.

Cisco Unified Communications Manager (CallManager) https://www.cisco.com/c/en/us/products/unified-communications/unified-communications-manager-callmanager/index.html.

AI-driven collaboration and customer experience, https://www.webex.com.

Cisco Unified Communications Manager Express, https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-express/series.html.

Understanding H.323 Gatekeepers, https://www.cisco.com/c/en/us/support/docs/voice/h323/5244-understand-gatekeepers.html.

Polycom video- conferencing, https://www.hp.com/gb-en/poly/video-conferencing.html.

Wykorzystanie terminala Cisco TelePresence VX Tactical w warunkach polowych https://www.dekom.com/en/video-conferencing/product/cisco-telepresence-vx-tactical.

OPEN ACCESS

Copyright (c) 2025 Andrzej Bogdański

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License