POLITECHNIKA
OPOLSKA

PRZEGLĄD NAUK STOSOWANYCH

pod redakcją
Mariusza Rząsy

nr 19

Wydział Ekonomii i Zarządzania
Opole, 2018

Przegląd Nauk Stosowanych

Nr 19

ISSN 2353-8899

Przegląd Nauk Stosowanych Nr 19 (2)

Redakcja: Mariusz R. Rząsa

Wszystkie artykuły zostały ocenione przez dwóch niezależnych recenzentów

All contributions have been reviewed by two independent reviewers

Projekt okładki: Krzysztof Kasza

Opracowanie graficzne: Oficyna Wydawnicza Politechniki Opolskiej

Wydanie I, 2018 r.

ISSN 2353-8899

Spis treści

SŁOWO WSTĘPNE

Ten numer Przeglądu Nauk Stosowanych poświęcony jest w całości ogólnopolskiej konferencji naukowej zatytułowanej „Praktyczne aspekty i możliwości wykorzystania potencjału naukowo- badawczego oraz transfer wiedzy pomiędzy sektorem nauki, a jednostkami Krajowej Administracji Skarbowej", która odbyła się w Opolu w dniach 13-14 marca 2018 r. z inicjatywy Izby Administracji Skarbowej w Opolu i Politechniki Opolskiej. W niniejszym numerze Przeglądu Nauk Stosowanych zamieszczono informacje o konferencji oraz opublikowano wybrane artykuły autorów wystąpień konferencyjnych. Wśród autorów artykułów są zarówno pracownicy naukowi uczelni, jak również pracownicy i funkcjonariusze jednostek Krajowej Administracji Skarbowej. Wiele artykułów posiada dwóch autorów reprezentujących obydwa środowiska, co dowodzi współpracy pomędzy tymi sektorami.

Głównym celem tego naukowego wydarzenia była dyskusja i wymiana doświadczeń pomiędzy środowiskiem naukowym uczelni a przedstawicielami izb administracji skarbowej z całego kraju dotycząca możliwych form i obszarów zacieśnienia współpracy obu środowisk. W trakcie dwóch dni konferencji teoretycy i praktycy mogli spotkać się i podyskutować o możliwościach oraz korzyściach, jakie daje partnerstwo nauki z administracją skarbową. Ku satysfakcji Organizatorów konferencja charakteryzowała się wysokim poziomem merytorycznym dyskusji, a jej tematyka spotkała się z dużym zainteresowaniem przedstawicieli obu środowisk. Mamy nadzieję, że publikacja będzie nie tylko źródłem wiedzy, dobrych praktyk,ale także inspiracją dla innych jednostek administracji publicznej.

Paweł Cybulski
Podsekretarz Stanu
Zastępca Szefa Krajowej Administracji Skarbowej
Ministerstwo Finansów
ul. Świętokrzyska 12
00-916 Warszawa
pawel.cybulski@mf.gov.pl

Justyna BIOŁY-KOBYLAŃSKA

KONFERENCJIA „PRAKTYCZNE ASPEKTY I MOŻLIWOŚCI WYKORZYSTANIA POTENCJAŁU NAUKOWO-BADAWCZEGO ORAZ TRANSFER WIEDZY POMIĘDZY SEKTOREM NAUKI, A JEDNOSTKAMI KRAJOWEJ ADMINISTRACJI SKARBOWEJ”

Ogólnopolska konferencja naukowa pt. „ Praktyczne aspekty i możliwości wykorzystania potencjału naukowo-badawczego oraz transfer wiedzy pomiędzy sektorem nauki a jednostkami Krajowej Administracji Skarbowej”, zorganizowana przez Izbę Administracji Skarbowej w Opolu oraz Wydział Ekonomii i Zarządzania Politechniki Opolskiej, odbyła się Opolu w dniach 13-14 marca 2018 r. Wydarzenie honorowym patronatem objęli: Szef Krajowej Administracji Skarbowej- Marian Banaś, Minister Nauki i Szkolnictwa Wyższego-Jarosław Gowin oraz Prezydent Miasta Opola-Arkadiusz Wiśniewski. Wzięli w nim udział przedstawiciele Ministerstwa Finansów, izb administracji skarbowej i urzędów celno-skarbowych z całej Polski oraz kadra naukowa Politechniki Opolskiej.

W spotkaniu nauki z administracją uczestniczył Paweł Cybulski, Podsekretarz Stanu w Ministerstwie Finansów, Zastępca Szefa Krajowej Administracji Skarbowej (fot.1), a także Arkadiusz Wiśniewski, Prezydent Miasta Opola.

Fotografia 1. Minister Paweł Cybulski wita uczestników konferencji

Źródło: Politechnika Opolska fot. Krzysztof Kasza (13.03.2018)

Konferencję otworzyli Barbara Bętkowska-Cela, Dyrektor Izby Administracji Skarbowej w Opolu oraz – w imieniu Rektora prof. dr hab.inż. Marka Tukiendorfa - prof. dr hab. inż. Krzysztof Malik, Prorektor ds. studenckich i inwestycji. Organizatorzy witając przybyłych uczestników spotkania zachęcali do otwartej dyskusji, zgłaszania pomysłów oraz rozwiązań wspierających przepływ wiedzy i innowacji pomiędzy dwoma środowiskami. W swoim wystąpeniu minister Paweł Cybulski wyraził to słowami „ Bardzo się cieszę, że doszło do tego spotkania, a właściwie wydarzenia, które jednoczy ze sobą dwa światy - świat nauki i świat administracji" Dziękując Organizatorom za zaproszenie podkreślał znaczenie współpracy pomiędzy uczelniami a jednostkami administracji dla budowy państwa nowoczesnego i innowacyjnego. Plan na rzecz odpowiedzialnego rozwoju nie ma szans powodzenia bez efektywnej współpracy sektorów nauki i szkolnictwa wyższego z biznesem i administracją. „Musimy zmienić paradygmat naszego myślenia, stać się Kolumbem w naszych działaniach, wypłynąć na nieznane wody i odkryć nowy nieznany ląd" – podkreślał.

IDEA I CEL KONFERENCJI

Pomysł na zorganizowanie konferencji poświęconej współpracy pomiędzy sektorem nauki a jednostkami administracji skarbowej narodził się jesienią 2017 r. Izba Administracji Skarbowej w Opolu i Politechnika Opolska współdziałając na mocy zawartego porozumienia z powodzeniem realizowały wspólne projekty i przedsięwzięcia (fot.2).

Doświadczenia we współpracy zainspirowały partnerów do podzielenia się dobrymi praktykami z innymi jednostkami oraz przeniesienia wypracowanego wspólnie innowacyjnego modelu współdziałania w zakresie kształcenia nowoczesnych kadr na grunt ogólnopolski. Zamierzeniem Organizatorów było, by konferencja stała się forum wymiany doświadczeń i dobrych praktyk pomiędzy jednostkami administracji skarbowej, a uczelnią wyższą oraz spotkaniem, w trakcie którego oba środowiska mogłyby wspólnie poszukiwać nowych form współdziałania i rozwiązań sprzyjających transferowi wiedzy, kompetencji, umiejętności i innowacji pomiędzy uczelniami wyższymi a administracją.

Wydarzenie naukowe miało stać się również okazją do zdefiniowania wzajemnych oczekiwań oraz wskazania ewentualnych barier utrudniających współpracę pomiędzy sektorem nauki i jednostkami administracji skarbowej.

Fotografia 2. Tydzień Skarbowo-Celny na Politechnice Opolskiej.
Jedna ze wspólnych inicjatyw uczelni i Izby Administracji Skarbowej w Opolu

Źródło: Politechnika Opolska fot. Krzysztof Kasza (7.11.2017)

TEMATYKA PANELI DYSKUSYJNYCH

Konferencja przebiegała w formie dyskusji panelowych, w których uczestniczyli przedstawiciele zarówno świata nauki, jak i administracji skarbowej. W sześciu sesjach tematycznych wzięło udział w sumie 20 prelegentów. Formuła wydarzenia sprzyjała wymianie doświadczeń i opinii pomiędzy uczestnikami konferencji, reprezentującymi oba środowiska.

Pierwszego dnia odbyły się cztery sesje tematyczne. W pierwszej zatytułowanej „Model współpracy Politechniki Opolskiej z jednostkami Krajowej Administracji Skarbowej w zakresie kształcenia nowoczesnych kadr" udział wzięli: prof. dr hab. Krzysztof Malik, Prorektor Politechniki Opolskiej, który moderował dyskusję, Paweł Cybulski, Podsekretarz Stanu, Zastępca Szefa Krajowej Administracji Skarbowej, Barbara Bętkowska-Cela, Dyrektor Izby Administracji Skarbowej w Opolu, dr Agnieszka Dornfeld-Kmak, Zastępca Dyrektora Izby Administracji Skarbowej w Opolu, dr Brygida Klemens, Prodziekan ds. Dydaktyki Wydziału Ekonomii i Zarządzania Politechniki Opolskiej oraz dr Urszula Romaniuk z Wydziału Ekonomii i Zarządzania tej uczelni (fot.3). W dyskusji szczególną uwagę poświęcono innowacyjnemu modelowi współpracy w zakresie kształcenia nowoczesnych kadr, wypracowanemu przez Izbę Administracji Skarbowej w Opolu i Politechnikę Opolską. Rozmawiano m.in. o współpracy w zakresie organizacji staży, praktyk zawodowych oraz wizyt studyjnych dla studentów w jednostkach organizacyjnych i centrach kompetencyjnych admini-

stracji skarbowej, programie tworzenia przez studentów projektów, prototypów i analiz w ramach zaliczenia prac licencjackich, magisterskich i inżynierskich, spełniających oczekiwania jednostek Krajowej Administracji Skarbowej, a także współpracy jednostek administracji skarbowej z uczelnią przy opracowywaniu programów studiów. Uczestnicy panelu przedstawiając główne założenia modelu wskazywali na korzyści, jakie przynosi on jego wszystkim interesariuszom.

Fotografia 3. Dyskusja panelowa. Od lewej: dr A.Dornfeld - Kmak, P.Cybulski, B. Bętkowska-Cela, dr U.Romaniuk, dr B. Klemens, prof. dr hab. K.Malik

Źródło: Politechnika Opolska fot. Krzysztof Kasza (13.03.2018)

W kolejnym panelu pod nazwą „Nowoczesne narzędzia i technologie informatyczne poprawiające efektywność funkcjonowania jednostek sektora finansów publicznych", moderowanym przez Barbarę Bętkowską-Celę, Dyrektora Izby Administracji Skarbowej w Opolu, rozmawiano na temat możliwości współpracy uczelni i administracji skarbowej w obszarze projektowania narzędzi informatycznych wspomagających i wspierających kierownika jednostki, np. we właściwym sprawowaniu kontroli zarządczej. Do dyskusji panelistów z poprzedniej sesji dołączyli:Barbara Hetmańska, Kanclerz Politechniki Opolskiej i dr inż. Michał Podpora z Wydziału Elektrotechniki, Automatyki i Informatyki Politechniki Opolskiej.

Następną sesję pod nazwą „Nowoczesne narzędzia i technologie informatyczne wspierające procesy analityczne" moderował dr hab. inż. Mariusz Rząsa, a udział w niej wzięli: Przemysław Krawczyk, Dyrektor Departamentu Kontroli i Analiz Ekonomicznych w Ministerstwie Finansów, Przemysław Koch, Pełnomocnik Ministra Finansów ds. Informatyzacji, Arkadiusz Szlękowski z Opol-

skiego Urzędu Celno-Skarbowego w Opolu oraz mgr inż. Tomasz Turba z Politechniki Opolskiej. Dyskusja dotyczyła perspektyw współpracy w obszarze projektowania zaawansowanych narządzi analitycznych. W trakcie sesji zaprezentowano przykłady projektów Ministerstwa Finansów oraz wykorzystywanych przez resort nowoczesnych technologii do analizy bardzo dużych zbiorów danych. Rozmawiano również o praktycznym zastosowaniu narzędzi informatycznych w pracy analityków oraz perspektywach rozwoju analityki w jednostkach administracji skarbowej. Przedstawiciele resortu finansów wskazywali na możliwości współpracy ze środowiskiem naukowych w zakresie transferu wiedzy z zakresu zaawansowanej analityki oraz przy opracowywaniu algorytmów dostosowanych do konkretnych procesów. Dyskutowano również o bezpieczeństwie baz danych w kontekście wymiany informacji i przekazywania wyników procesów, algorytmów, czy oprogramowania pomiędzy współpracującymi jednostkami.

Fotografia 4. Dyskusja panelowa. Od lewej: Przemysław Krawczyk, Przemysław Koch, Arkadiusz Szlękowski, Tomasz Turba, dr hab .inż. Mariusz Rząsa

Źródło: Politechnika Opolska fot. Krzysztof Kasza (13.03.2018)

Pierwszy dzień konferencji zakończył panel „Nowe rozwiązania i narzędzia IT wspierające zwalczanie przestępstw gospodarczych", który moderował mł. insp. Rafał Kokot z Centrum Kompetencyjnego E-Kontrola Opolskiego Urzędu Celno-Skarbowego w Opolu, jednostki centralnej Krajowej Administracji Skarbowej zajmującej się identyfikowaniem naruszeń prawa w sieci Internet. W dyskusji uczestniczyli: nadkom. Tadeusz Szymbert, Naczelnik Wydziału Nadzoru z Departamentu Zwalczania Przestępczości Ekonomicznej w Ministerstwie Finansów, Marcin Kopczyk z Izby Administracji Skarbowej w Warsza-

wie, podinsp. Wojciech Zimoch z Centrum Technicznego Informatyki Śledczej Opolskiego Urzędu Celno-Skarbowego w Opolu oraz ze strony Politechniki Opolskiej: dr inż. Michał Podpora i mgr inż. Tomasz Turba. W trakcie sesji zaprezentowane zostały nowoczesne narzędzia wspomagające wykrywanie naruszeń prawa wykorzystywane przez Krajową Administrację Skarbową. Eksperci rozmawiali na temat możliwości współpracy z uczelnią w zakresie projektowania systemów informatycznych dla jednostek administracji skarbowej spełniających konkretne oczekiwania organów Państwa, obejmujących swych działaniem zarówno clearnet jak i darknet, m.in. systemu do asocjacyjnego wyszukiwania lokalizacji internetowych o ustalonym, zadanym wzorcu, czy też narzędzi niezbędnych do pozyskiwania, gromadzenia i zabezpieczania dowodów elektronicznych przez informatyków śledczych.

Drugi dzień konferencji rozpoczęła dyskusja na temat współpracy w zakresie konstruowania narzędzi i aparatury do wykrywania, pomiaru i analizy różnych materiałów i substancji oraz innych urządzeń, które znalazłyby zastosowanie w prowadzonych przez administrację skarbową kontrolach. Panel zatytułowany „Nowoczesne narzędzia, urządzenia pomiarowe i technika laboratoryjna wspomagające kontrole w jednostkach KAS" moderował nadkom. Piotr Kraczmar, Kierownik Oddziału Celnego w Nysie, a wzięli w nim udział: insp. Robert Ehrmann, Kierownik Laboratorium Celno-Skarbowego w Otwocku, mł. rachm. Wojciech Gęsikowski z Centrum RTG w Gdyni oraz dr hab. inż. Mariusz Rząsa z Politechniki Opolskiej. Uczestnicy konferencji, a zwłaszcza przedstawiciele uczelni, mieli okazję obejrzeć prezentację dotyczącą stosowanych podczas kontroli celno-skarbowych technik i urządzeń do poboru próbek, wysłuchać prelekcji na temat badań różnych materiałów i substancji w specjalistycznych laboratoriach Krajowej Administracji Skarbowej oraz wykorzystania mobilnych i stacjonarnych urządzeń RTG. Poznanie przez środowisko nauki dostępnych narzędzi oraz aparatury laboratoryjnej i rentgenowskiej zainicjowało dyskusję na temat możliwości wykorzystania potencjału naukowego uczelni w pracach nad doskonaleniem, bądź tworzeniem prototypów nowych urządzeń spełniających oczekiwania administracji skarbowej.

Dwudniową debatę na temat współpracy pomiędzy sektorem nauki a administracją skarbową zakończyła sesja pt. „Transfer wiedzy, kompetencji i umiejętności pomiędzy uczelniami wyższymi a jednostkami Krajowej Administracji Skarbowej", moderowana przez dr Agnieszkę Dornfeld-Kmak, Zastępcę Dyrektora Izby Administracji Skarbowej w Opolu. Uczestniczyli w niej: Barbara Bętkowska-Cela, Dyrektor Izby Administracji Skarbowej w Opolu, prof. dr hab. Krzysztof Malik, Prorektor Politechniki Opolskiej oraz Arkadiusz Wiśniewski, Prezydent Miasta Opola.

Fotografia 5. Panel podsumowujący konferencję. Od lewej:
prof. dr hab. Krzysztof Malik, Arkadiusz Wiśniewski-Prezydent Opola,
Barbara Bętkowska-Cela.

Źródło: Politechnika Opolska fot. Krzysztof Kasza (14.03.2018)

Zaproszenie do dyskusji Prezydenta Miasta zainicjowało debatę na temat roli samorządu w procesie inicjowania współpracy nauki z administracją, instrumentów, jakimi dysponuje na rzecz pobudzania innowacji oraz źródeł finansowania nowatorskich projektów. Uczestnicy konferencji zgodzili się, że partnerstwo uczelni wyższych z administracją skarbową jest wyzwaniem, które opłaca się podejmować, a kluczowe w nawiązaniu współpracy są przede wszystkich otwartość i zainteresowanie obu stron.

PODSUMOWANIE I PIERWSZE EFEKTY KONFERENCJI

Dwudniowe spotkanie przedstawicieli świata nauki i jednostek Krajowej Administracji Skarbowej okazało się bardzo wartościowe dla obu stron, o czym między innymi świadczyły dyskusje po każdym panelu tematycznym, a także ożywione rozmowy kuluarowe. Konferencja stała się nie tylko doskonałą platformą wymiany opinii i doświadczeń pomiędzy środowiskiem nauki i jednostkami administracji skarbowej, a także okazją do wzajemnego poznania, budowania zaufania i określenia wzajemnych oczekiwań.

Istotnym rezultatem konferencji jest wyniesione przez uczestników przekonanie, że współpraca pomiędzy administracja skarbową i sektorem nauki jest nie tylko możliwa, ale także konieczna i może przynieść obu stronom długofalowe i wymier-

ne korzyści. Dla jednostek Krajowej Administracji Skarbowej takie partnerstwo jest szansą na dostęp do najnowszej wiedzy, nowoczesnych rozwiązań organizacyjnych oraz innowacyjnych technologii. Dla środowisk naukowych to okazja do pozyskania dodatkowych środków na prowadzenie badań, pomysłów na prace badawcze, ale także poprawy jakości kształcenia oraz podniesienia prestiżu uczelni.

Okazało się, że nawiązany w trakcie konferencji dialog bardzo szybko zaowocował kolejnym projektem Politechniki Opolskiej i Izby Administracji Skarbowej w Opolu. W efekcie wspólnych rozmów strony podjęły decyzję o utworzeniu koła naukowego przy Politechnice Opolskiej, którego członkowie przy współudziale specjalistów z administracji skarbowej zajmą się projektowaniem i konstruowaniem narzędzi informatycznych odpowiadających konkretnym potrzebom jednostek Krajowej Administracji Skarbowej. Współpracę w zakresie realizacji tego projektu zadeklarował także Prezydent Opola, który obiecał wesprzeć inicjatywę grantami finansowymi. Rozmowy kadry naukowej Politechniki Opolskiej z praktykami reprezentującymi jednostki administracji skarbowej z całego kraju otworzyły tej uczelni drogę do nawiązania współpracy z administracją skarbową na poziomie krajowym. Spotkanie eksperta Politechniki Opolskiej, zajmującego się od wielu lat komputerową techniką pomiarową ze specjalistą w zakresie urządzeń rentgenowskich reprezentującego administrację skarbową, do jakiego doszło podczas konferencji, zaowocowało wizytą studyjną przedstawiciela tej uczelni w Centrum RTG w Gdyni.

Organizatorzy przedsięwzięcia mają nadzieję, że zainicjowana podczas konferencji dyskusja obu środowisk i nawiązane kontakty przyniosą długofalowe efekty w postaci efektywnej współpracy, skutkującej pełnym wykorzystaniem potencjału uczelni w praktyce.

PODZIĘKOWANIA

W organizację Ogólnopolskiej konferencji **„**Praktyczne aspekty i możliwości wykorzystania potencjału naukowo- badawczego oraz transfer wiedzy pomiędzy sektorem nauki, a jednostkami Krajowej Administracji Skarbowej" zaangażowany był szereg osób:

Rada Naukowa Konferencji:

- prof. dr hab. inż. Marek Tukiendorf, Rektor Politechniki Opolskiej
- prof. dr hab. Krzysztof Malik, Prorektor Politechniki Opolskiej
- Barbara Hetmańska, Kanclerz Politechniki Opolskiej
- dr Brygida Klemens, Prodziekan ds. Dydaktyki Wydziału Ekonomii i Zarządzania, Politechnika Opolska
- dr Urszula Romaniuk,Wydział Ekonomii i Zarządzania Politechniki Opolskiej
- dr hab. inż. Mariusz Rząsa, Wydział Mechaniczny, Politechnika Opolska
- dr inż. Michał Podpora, Politechnika Opolska
- Barbara Bętkowska-Cela, Dyrektor Izby Administracji Skarbowej w Opolu
- dr Agnieszka Dornfeld-Kmak, Zastępca Dyrektora Izby Administracji Skarbowej

Uczestnicy paneli dyskusyjnych:

- prof. dr hab. Krzysztof Malik, Prorektor Politechniki Opolskiej
- Barbara Hetmańska, Kanclerz Politechniki Opolskiej
- dr Brygida Klemens, Prodziekan ds. Dydaktyki Wydziału Ekonomii i Zarządzania, Politechnika Opolska
- dr Urszula Romaniuk ,Wydział Ekonomii i Zarządzania, Politechnika Opolska
- dr hab. inż. Mariusz Rząsa, Wydział Mechaniczny, Politechnika Opolska
- dr inż. Michał Podpora, Politechnika Opolska
- mgr inż. Tomasz Turba, Politechnika Opolska
- Barbara Bętkowska-Cela, Dyrektor Izby Administracji Skarbowej w Opolu
- dr Agnieszka Dornfeld-Kmak, Zastępca Dyrektora Izby Administracji Skarbowej
- Przemysław Krawczyk, Dyrektor Departamentu Kontroli i Analiz Ekonomicznych, Ministerstwo Finansów
- Przemysław Koch-Pełnomocnik Ministra Finansów ds. Informatyzacji
- nadkom. Tadeusz Szymbert, Naczelnik Wydziału Nadzoru, Departament Zwalczania Przestępczości Ekonomicznej, Ministerstwo Finansów
- Marcin Kopczyk, Izba Administracji Skarbowej w Warszawie
- insp. Robert Ehrmann, Kierownik Laboratorium Celno-Skarbowego w Otwocku, Izba Administracji Skarbowej w Warszawie
- mł. rachm. Wojciech Gęsikowski, Centrum RTG w Gdyni, Izba Administracji Skarbowej w Gdańsku
- Arkadiusz Szlękowski, Opolski Urząd Celno-Skarbowy w Opolu
- podinsp. Wojciech Zimoch, Centrum Techniczne Informatyki Śledczej, Opolski Urząd Celno-Skarbowy w Opolu
- mł. insp. Rafał Kokot ,Centrum Kompetencyjne E-Kontrola, Opolski Urząd Celno-Skarbowy w Opolu
- nadkom. Piotr Kraczmar, Kierownik Oddziału Celnego w Nysie

Goście honorowi:

- Paweł Cybulski**,** Podsekretarz Stanu w Ministerstwie Finansów, Zastępca Szefa Krajowej Administracji Skarbowej
- Piotr Patroński, Dyrektor Departamentu Informatyzacji, Ministerstwo Finansów
- Arkadiusz Wiśniewski, Prezydent Miasta Opola

Patronat

- Marian Banaś, Szef Krajowej Administracji Skarbowej
- Jarosław Gowin, Minister Nauki i Szkolnictwa Wyższego
- Arkadiusz Wiśniewski, Prezydent Miasta Opola

Pragniemy podziękować również wszystkim, którzy przyczynili się do powstania niniejszego numeru Przeglądu Nauk Stosowanych, w szczególności autorom artykułów i wydawnictwu.

Justyna Bioły-Kobylańska
Izba Administracji Skarbowej w Opolu
ul. Ozimska 19
45-057 Opole
justyna.bioly-kobylanska@mf.gov.pl

Krzysztof MALIK
Barbara BĘTKOWSKA-CELA
Agnieszka DORNFELD-KMAK

MODEL WSPÓŁPRACY IZBY ADMINISTRACJI SKARBOWEJ W OPOLU Z POLITECHNIKĄ OPOLSKĄ

Streszczenie: Wielorakość i złożoność problemów społecznych, jakie pojawiły się w ostatnich latach, a zwłaszcza problemów dotyczących rynku pracy powoduje konieczność współdziałania sektora nauki, administracji i biznesu. Współpraca międzysektorowa jest obecnie czynnikiem determinującym rozwój gospodarczy, zwłaszcza w kontekście przepływu wiedzy oraz transferu innowacyjnych rozwiązań technicznych, technologicznych pomiędzy jednostkami partnerskimi. W artykule zaprezentowano wypracowany model współpracy pomiędzy Izbą Administracji Skarbowej w Opolu a Politechniką Opolską w zakresie kształcenia nowoczesnych kadr.

Słowa kluczowe: model współpracy, administracja skarbowa, Politechnika Opolska, rozwój regionalny.

MODEL OF COOPERATION BETWEEN THE REVENUE ADMINISTRATION REGIONAL OFFICE IN OPOLE WITH OPOLE UNIVERSITY OF TECHNOLOGY

Summary: The multiplicity and complexity of social problems that arose in last years, and especially a problem concerning the labour market is a reason of the necessity of the cooperation of science, administration and business areas. Intersection cooperation is currently a factor that determines the economic development, especially in the context of the knowledge and the transfer of innovative technical solutions as well as technological between partner article presents the model of cooperation developed between The Revenue Administration Agency in Opole and the University of Technology in Opole in terms of providing the education for personnel.

Keywords: institutional cooperation model, Revenue Administration Regional Office in Opole, Opole University of Technology, regional development

1. WSTĘP

Dynamicznie zmieniająca się sytuacja społeczna, gospodarcza i polityczna, spowolnienie gospodarcze, negatywna sytuacja demograficzna, konieczność zwiększenia liczby trwałych miejsc pracy i dostosowania ich do potrzeb nowoczesnej gospodarki to wyzwania wymagające zmiany podejścia do problematyki rozwoju regionalnego. Coraz częściej mówi się o rozwoju zrównoważonym,

czyli takim rozwoju „w którym potrzeby obecnego pokolenia mogą być zaspokojone bez umniejszania szans przyszłych pokoleń na ich zaspokojenie”[1].

Rozwój regionalny jest jednym z najważniejszych zadań realizowanych przez administrację publiczną. Zgodnie z najpowszechniejszą definicją wiąże się on ze wzrostem potencjału gospodarczego regionu, który pociąga za sobą trwałą poprawę standardów życia mieszkańców regionu i wzrost jego konkurencyjności [Wlaźlak 2010]. Rozwój regionalny determinuje rozwój gospodarczym kraju przyczyniając się do ogólnego wzrostu i dobrobytu.

Obecnie rozwój regionalny zależy w dużej mierze od istnienia środowiska przedsiębiorczości, działającego stymulująco na podejmowanie nowych przedsięwzięć i ich realizację. Wielorakość i złożoność problemów społecznych, jakie pojawiły się w ostatnich latach wymaga także szerokiego współdziałania wszystkich stron życia społecznego, czyli współpracy międzysektorowej. Współpracą tą możemy określić zdolność budowania relacji pomiędzy różnymi sektorami- publicznym, prywatnym i społecznym, na rzecz osiągania wspólnych celów, umiejętność zespołowego wykonywania zadań i wspólnego rozwiązywania problemów.

W nowych realiach motorem dla wzrostu gospodarczego są niewątpliwie wiedza, innowacje, badania naukowe i umiejętności ich komercjalizacji, ale także metody generowania nowych idei i pomysłów, czy umiejętne zarządzanie wiedzą i technologią. Istotną cechą procesów innowacyjnych jest ich lokalny i regionalny charakter, dlatego podkreśla się znaczenie właściwej polityki regionalnej w ich kreowaniu. Źródłem nowych idei i technologii coraz częściej nie są przedsiębiorstwa, lecz środowisko o charakterze niegospodarczym, jak na przykład uczelnie wyższe, ośrodki naukowe i akademickie.

Komercjalizacja wiedzy i transfer innowacji wymagają więc współdziałania, zaś rozwój regionalny coraz bardziej zależy od umiejętności budowania relacji partnerskich między podmiotami reprezentującymi różne sfery działalności. W konsekwencji realizowana współpraca zainteresowanych jednostek w obszarze transferu wiedzy i technologii powinna doprowadzić do wzrostu innowacyjności gospodarki.

Kluczowe znaczenie dla rozwoju regionu ma współpraca administracji, nauki i biznesu w zakresie tworzenia oraz przepływu informacji nowoczesnych technologii. Rolą władz regionalnych powinno być tworzenie w regionach korzystnych warunków sprzyjających zbliżeniu i zacieśnieniu współpracy - zwłaszcza środowisk nauki, administracji i biznesu oraz powiązanie ich wzajemnych relacji tak, aby strony dostrzegły korzyści i zalety wynikające z partnerstwa. Jednostki, które współpracują w regionach powinny m.in. dzielić się wiedzą, ustalić jasne zasady współpracy oraz swobodnie się komunikować.

[1] Gerwin Marcin, Plan zrównoważonego rozwoju dla Polski: lokalne inicjatywy rozwojowe, 2008.

Najszersze możliwości i kompetencje względem wspierania innowacyjności w regionach ma samorząd województwa. Do jego zadań należy m.in. wyznaczanie kierunków i prowadzenie polityki innowacyjnej oraz stymulowanie sfery gospodarczej i społecznej do przejawiania aktywności w tym zakresie. Podstawą przemian regionów są ich strategie, wyznaczające główne kierunki rozwoju województwa na przyszłość.

W województwie opolskim dokumentem wyznaczającym kierunki jego rozwoju jest Strategia Rozwoju Województwa Opolskiego do 2020 r. Realizacja wskazanych strategicznych celów służyć ma osiągnięciu wizji województwa jako regionu wielokulturowego, w którym na pierwszym miejscu są jego mieszkańcy: wykształceni, otwarci na zmianę, wiedzę i innowacje, a także aktywni – na rynku pracy i poza nim, województwa z atrakcyjną ofertą rynku pracy, edukacyjną, kulturalną i gospodarczą, zachęcającą do wyboru tego regionu jako miejsca do zamieszkania, wypoczynku, inwestycji i rozwoju działalności innowacyjnej.

Dwa strategiczne cele wskazane w Strategii to:

- przygotowane do rynku pracy aktywne społeczeństwo,
- budowanie konkurencyjnej gospodarki opartej na innowacyjności i współpracy z nauką.

Punktem wyjścia do nawiązania współpracy między Izbą Administracji Skarbowej w Opolu a Politechniką Opolską była wymiana doświadczeń między środowiskiem nauki i praktykami, ukierunkowana zarówno na rozwój współpracujących organizacji jak na rozwój regionalny. Współczesna administracja skarbowa stanowi obszar wykorzystywania zarówno wysokich technologii (informatycznych, komunikacyjnych, logistycznych, bezpieczeństwa), jak i nowoczesnych rozwiązań zarządczych. Świat nauki zatem w dużej mierze jest zbliżony do jednostek KAS. W tym kontekście istotne jest wspólne kształtowanie programów kształcenia przyszłych absolwentów ukierunkowanych na potrzeby regionalnego i krajowego rynku pracy. W związku z powyższymi przesłankami współpracy formułowano następującą tezę dla dalszych badań: Wdrażanie zorientowanych na gospodarkę i administrację publiczną, inteligentnych programów kształcenia ogólnoakademickiego i praktycznego jest skutecznym i efektywnym czynnikiem wsparcia zrównoważonego rozwoju regionu i kraju.

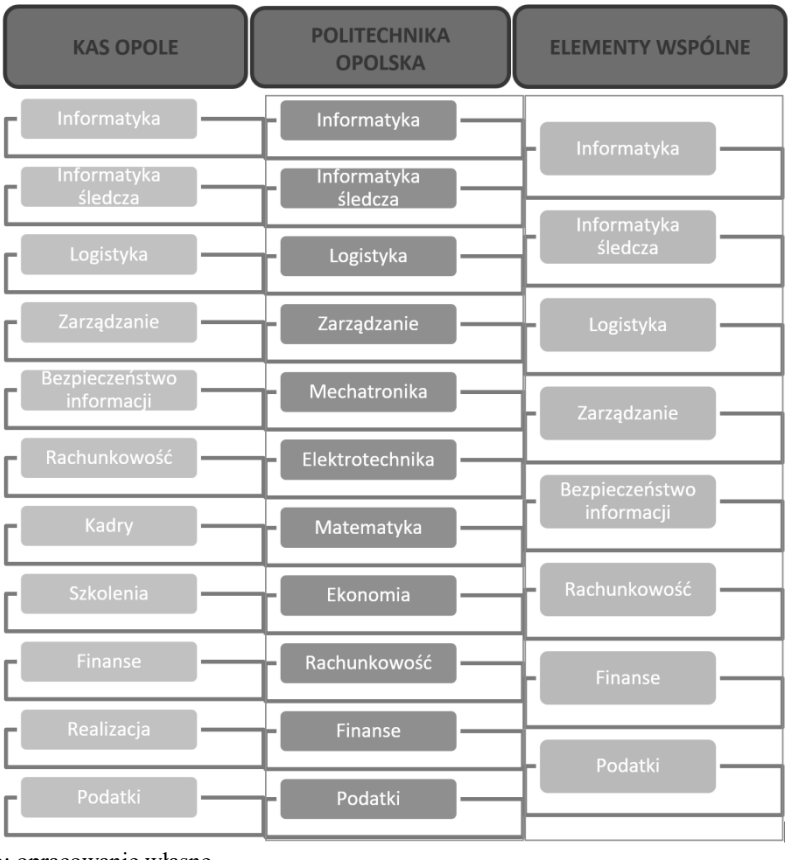
Jednak takie rozwiązania w zakresie rozwijania wiedzy, umiejętności i kompetencji absolwentów ukierunkowanych na wsparcie regionalnej gospodarki i administracji wymagają ściślejszej współpracy jednostek i określonego wsparcia normatywnego i strategicznego.

Stąd celem opracowania jest wskazanie obszarów i dobrych praktyk takiej współpracy, a także identyfikacja potencjalnych jej efektów zarówno w wymiarze jednostek, jak i całego regionu.

2. MODELOWANIE OBSZARÓW WSPÓŁPRACY

Aby zaprojektować kierunki i wagi współpracy przystąpiono do opracowania modelu obszarów współpracy (MOW) (rys.1). Poddano analizie zakres realizowanych zadań badawczych przez poszczególne wydziały oraz prowadzone kierunki i specjalności studiów na Politechnice Opolskiej. Następnie określono iloczyn kartezjański obszarów działań i celów wspólnych Politechniki Opolskiej oraz Izby Administracji Skarbowej w Opolu. Identyfikacja obszarów wspólnych korzyści stanowiła warunek konieczny określenia płaszczyzny współpracy w zbliżonych elementach działania, tak aby móc określić udział praktycznych efektów kształcenia przez Izbę Administracji Skarbowej w Opolu w dotychczasowych i projektowanych programach kształcenia realizowanych przez Politechnikę Opolską. W trakcie analizy okazało się, iż elementów wspólnych jest bardzo dużo.

Rysunek 1. Model obszarów wspólnych Izby Administracji Skarbowej w Opolu i Politechniki Opolskiej.



Źródło: opracowanie własne

3. DOBRE PRAKTYKI WSPÓŁPRACY

Pierwszym aspektem współpracy badanych jednostek było zorganizowanie „Tygodnia Celno-Skarbowego" dla studentów i wykładowców na wydziałach Politechniki Opolskiej (rys.2).

Rysunek 1. Plakat „Tydzień Celno-Skarbowy na Politechnice Opolskiej".

Źródło: opracowanie własne

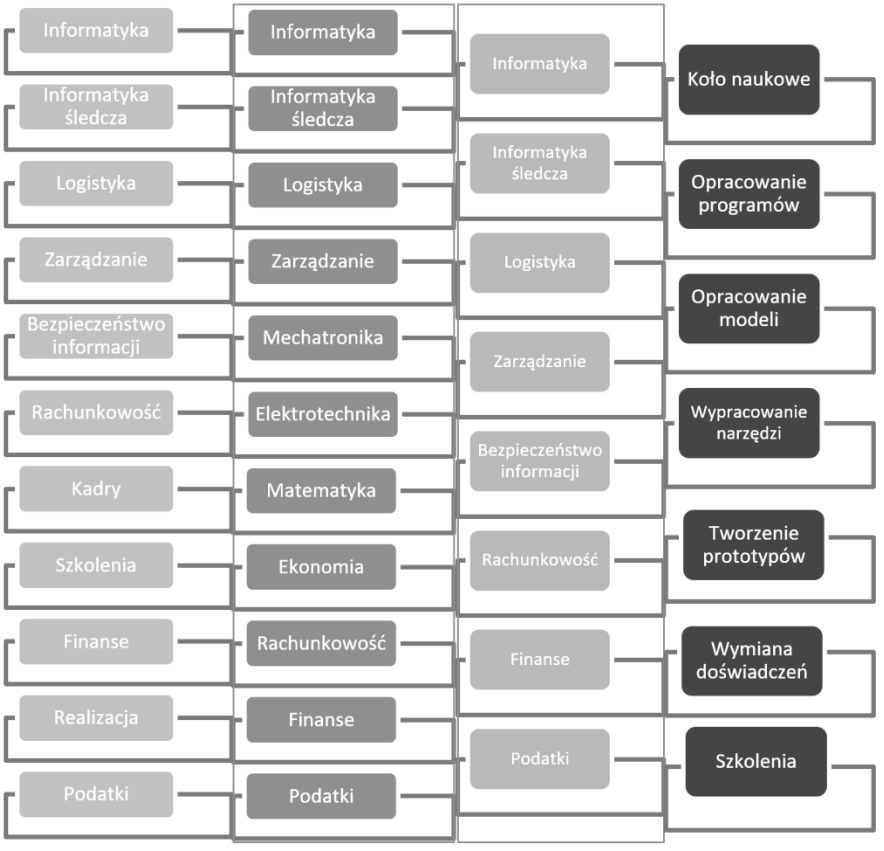
Tydzień Celno-Skarbowy cieszył się bardzo dużym zainteresowaniem. W tym czasie na czterech wydziałach zorganizowano dyskusje ze studentami na temat:

- Krajowa Administracja Skarbowa - rola i zadania. Program współpracy Politechniki Opolskiej z Izbą Administracji Skarbowej w Opolu;
- Jednolity plik kontrolny JPK;
- Zwalczanie przestępczości przez Służbę Celno-Skarbową;

- Rola psów służbowych w Krajowej Administracji Skarbowej;
- Zwalczanie przestępstw popełnianych w sieci Internet;
- Wykorzystanie narzędzi informatyki śledczej w zwalczaniu przestępczości.

Zainteresowanie prezentowaną tematyką było bardzo duże. W związku z powyższym zidentyfikowano idee projektów wspólnych (rys. 3)

Rysunek 3. Obszary i działania (projekty) wspólne.



Źródło: opracowanie własne

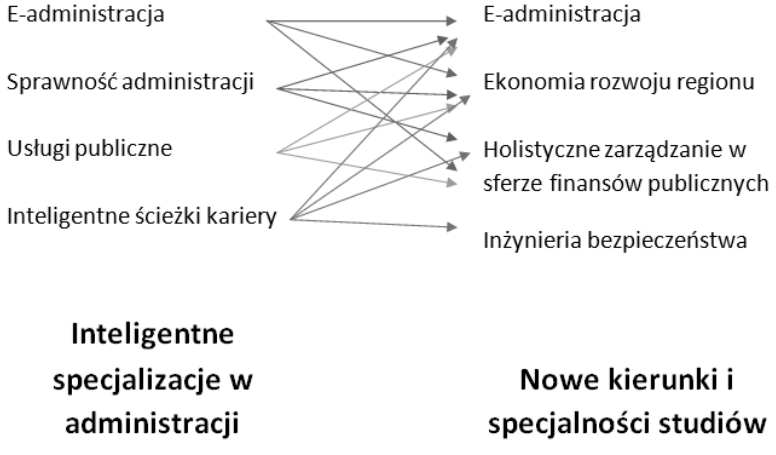
Izba Administracji Skarbowej zaproponowała zorganizowanie staży i praktyk zarówno dla studentów, jak i praktyków akademickich. W ramach tej inicjatywy zorganizowano m.in. staże i praktyki studenckie:

- praktyki dla studentów o profilu ogólnoakademickim w wymiarze 160 godzin,
- praktyki dla studentów o profilu praktycznym w wymiarze co najmniej 3 miesiące,
- staże i praktyki dla pracowników Politechniki Opolskiej- w wymiarze od 1 miesiąca do 1 roku.

Każdy student ma możliwość odbycia stażu lub praktyki w siedzibie Izby Administracji Skarbowej w Opolu, podległym Urzędzie Celno-Skarbowym w Opolu lub jednym z Urzędów Skarbowych Opolszczyzny: Pierwszy Urząd Skarbowy w Opolu, II Urząd Skarbowy w Opolu, Opolski Urząd Skarbowy, Urząd Skarbowy w Brzegu, Urząd Skarbowy w Strzelcach Opolskich, Urząd Skarbowy w Kędzierzynie –Koźlu, Urząd Skarbowy w Nysie, Urząd Skarbowy w Namysłowie, Urząd Skarbowy w Prudniku, Urząd Skarbowy w Kluczborku, Urząd Skarbowy w Głubczycach, Urząd Skarbowy w Oleśnie, Urząd Skarbowy w Krapkowicach.

Politechnika Opolska w oparciu o analizę regionalnych dokumentów strategicznych i operacyjnych zaprojektowała określone nowe kierunki i specjalizacje studiów i studiów podyplomowych związanych z administracją publiczną, w tym skarbową (rys. 4).

Rysunek 4. Kierunki i specjalizacje studiów i studiów podyplomowych zaprojektowane w oparciu o analizę Regionalnego Programu Operacyjnego Województwa Opolskiego 2014-2020.



Źródło: opracowanie własne

Zdecydowano o potrzebie ściślejszego powiązania nowych kierunków i specjalności studiów z potrzebami regionalnej administracji skarbowej. Dlatego kolejnym aspektem współpracy było zorganizowanie kierunków studiów z przygotowaniem praktycznym. W celu „upraktycznienia" poszczególnych kierunków studiów kadra zarządzająca brała udział w konsultowaniu programów i efektów kształcenia dla kierunków: Ekonomia I i II stopnia oraz Administracja I stopnia o profilu praktycznym. Ponadto z kadrą zarządzającą Izby Administracji Skarbowej w Opolu skonsultowano sylabusy z wybranych przedmiotów.

W oparciu o takie ramy współpracy przygotowano między innymi:

- Studia licencjackie i magisterskie dające możliwość praktycznych zajęć w Izbie Administracji Skarbowej i jednostkach podległych oraz studia kierunkowe z możliwością odbycia części zajęć praktycznych w Izbie Administracji Skarbowej w Opolu
- Studia podyplomowe w zakresie tematycznym:
- ✓ Holistyczne zarządzanie w sektorze finansów publicznych – unikatowy kierunek dla kadry zarządzającej;
- ✓ Informatyka śledcza;
- ✓ Zarządzanie bezpieczeństwem informacji;
- ✓ Europejskie standardy rachunkowości sektora publicznego.

Owo upraktycznienie dotyczy także tematyki prac dyplomowych. Aktualnie wybrane zostały przez studentów prace dyplomowe na kierunku Ekonomia II stopnia, na specjalności Ekonomia i finanse w przedsiębiorstwie. Przykładowe tematy wybranych prac dyplomowych brzmią:

- Syntetyczna ocena kondycji finansowej przedsiębiorstwa;
- Kreatywna księgowość a słynne upadki wielkich międzynarodowych korporacji;
- Bit-coin – waluta czy spekulacyjny instrument finansowy;
- Crowd funding jako źródło społecznego finansowania przedsiębiorstw;
- Wpływ obciążeń podatkowych na wynik z działalności przedsiębiorstwa.

4. KORZYŚCI INTERESARIUSZY WSPÓŁPRACY: PODSUMOWANIE

Zgodnie z modelem społecznych grup interesów (social stakeholder model), tylko uzyskiwanie założonych korzyści każdej z grup interesariuszy stanowi warunek konieczny rozwoju zrównoważonego współpracujących organizacji.

Dzięki dostosowaniu kwalifikacji absolwentów do potrzeb gospodarki i administracji oraz projektowaniu wspólnych badań naukowych i działań popularyzujących wiedzę o administracji skarbowej wszyscy interesariusze takiej współpracy odnoszą określone korzyści krótko- i długoterminowe. Z uwagi na ich czterowymiarowość – korzyści te określono mianem poczwórnej dywidendy (tab. 1).

Tabela 1. 4 × dywidenda interesariuszy współpracy.

1.	**Korzyści dla studentów:** Perspektywa trwałej pracy w przedsiębiorstwach i jednostkach sfery finansów publicznych (SFP). Samorozwój w sferze zawodowej – *smart jobs*
2.	**Korzyści dla przedsiębiorstw i instytucji SFP:** Możliwości wyboru najlepiej dopasowanych do potrzeb, innowacyjnych absolwentów; wzrost efektywności funkcjonowania I rozwoju organizacji

3. **Korzyści dla gospodarki i administracji:** Poprawa efektywności nakładów na szkolnictwo wyższe, zmniejszenie bezrobocia, poprawa jakości świadczenia usług publicznych i sprawności systemu podatkowego
4. **Korzyści dla uczelni:** Trwała liczba ukierunkowanych na rynek pracy kandydatów aplikujących na nowoczesne programy studiów spójne z potrzebami gospodarki i administracji (przygotowanie praktyczne praktykantów, przygotowanie praktyczne stażystów, udział w przygotowaniu przez praktyków sylabusów, wspólne projekty badawcze)

Źródło: opracowanie własne

W ramach korzyści dla administracji publicznej, określono już występujące korzyści współpracy z uczelnią dla Izby Administracji Skarbowej w Opolu (prekursora takiego modelu obszarów współpracy), w tym:

- pozyskanie stażystów,
- pozyskanie praktykantów,
- przygotowanie stażystów i praktykantów do pracy w Izbie Administracji Skarbowej,
- praktyki dla wykładowców,
- tworzenie prototypów narzędzi,
- tworzenie programów informatycznych,
- wspólne panele dyskusyjne służące dalszej wymianie doświadczeń i pomysłów.

Zatem teza badawcza sformułowana na wstępie tego opracowania o korzyściach społecznych interesariuszy z wdrażania zorientowanych na gospodarkę i administrację publiczną, inteligentnych programów kształcenia została potwierdzona. Trwałość zidentyfikowanych korzyści (tzw. poczwórna dywidenda) społecznych interesariuszy stanowi istotną przesłankę rozwoju zrównoważonego w wymiarze regionalnym.

Literatura:

[1] Wlaźlak K.:, *Rozwój regionalny jako zadanie administracji publicznej,* Warszawa, Oficyna Wolters Kluwer Business, 2010.

[2] Charkiewicz J., Dziemianowicz W., Błajet P., Baczyńska N., Smolik A.: *Analiza stanu innowacyjności województwa opolskiego,* Warszawa:, Geoprofit, 2010,

[3] Raport końcowy z badania pn. *Ocena działań badawczo-rozwojowych oraz innowacyjnych podejmowanych w ramach unijnych projektów na rzecz wzrostu konkurencyjności Opolszczyzny*, Opole, Pracownia Badań i Doradztwa „Re-Source" Korczyński Sarapata Sp. j., na zlecenie Urzędu Marszałkowskiego Województwa Opolskiego, 2012.

[4] Pierwsze kroki na rynku pracy. *Ogólnopolskie badanie studentów i absolwentów, Deloitte i Katedra Rozwoju Kapitału Ludzkiego Szkoły Głównej Handlowej w Warszawie*, Warszawa 2010, materiał powielony.

[5] Nowak M., Mażewska M., Mazurkiewicz S.: *Współpraca ośrodków innowacji z administracją publiczną*, broszura PARP, 2011.
[6] Strategia Rozwoju Województwa Opolskiego do 2020 r.

prof. dr hab. Krzysztof Malik
Politechnika Opolska
Wydział Ekonomii i Zarządzania
ul. Luboszycka 7 45-036 Opole
k.malik@po.opole.pl

Barbara Bętkowska-Cela
Izba Administracji Skarbowej w Opolu
ul. Ozimska 19, 45-057 Opole
barbara.betkowska-cela@mf.gov.pl

dr Agnieszka Dornfeld-Kmak
Izba Administracji Skarbowej w Opolu
ul. Ozimska 19, 45-057 Opole
agnieszka,dornfeld-kmak@mf.gov.pl

Krzysztof MALIK
Barbara BĘTKOWSKA-CELA
Agnieszka DORNFELD-KMAK

CZY WARTO SKONSOLIDOWAĆ SYSTEMY ZARZĄDZANIA? ANALIZA DOKONANA W OPARCIU O SYSTEMY ZARZĄDZANIA W KRAJOWEJ ADMINISTRACJI SKARBOWEJ

Streszczenie: W artykule przedstawiono podejście do konsolidacji systemów zarządzania uwzględniając zarządzanie ryzykiem w systemach: kontrola zarządcza, System Zarządzania Bezpieczeństwem Informacji oraz zarządzanie kryzysowe. Zaprezentowano m.in. w jaki sposób jednolicie zarządzać ryzykiem we wszystkich systemach, tak aby to samo ryzyko w danym obszarze przy uwzględnień tych samych czynników warunkujących powstanie ryzyka oraz mechanizmów kontrolnych zawsze osiągało taki sam poziom ryzyka.

Słowa kluczowe: konsolidacja systemów zarządzania.

ARE THE MANAGEMENT SYSTEMS WORTH TO CONSOLIDATE - ANALYSIS MADE ON THE BASIS OF THE MANAGEMENT SYSTEM IN THE NATIONAL REVENUE ADMINISTRATION

Summary: The Article presents the approach to consolidate the management system regarding the risk management in the systems: management control, System of Information Safety System and Crisis Management. It was presented how to manage the risk in all systems to that the risk in definite area, considering the same factors of risk origin and control mechanisms, always attain the same risk level.

Keywords: management systems consolidation.

1. WSTĘP

W każdej Jednostce Sektora Finansów Publicznych występuje szereg systemów zarządzania. Izby Administracji Skarbowej należą do Jednostek Sektora Finansów Publicznych. Najważniejsze systemy zarządzania występujące w Krajowej Administracji Skarbowej to: kontrola zarządcza, System Zarządzania Bezpieczeństwem Informacji, bezpieczeństwo teleinformatyczne, ciągłość działania, zarządzanie kryzysowe, audyt wewnętrzny, kontrola wewnętrzna.

Każdy z tych systemów charakteryzuje się elementem zarządzania ryzykiem, na który składa się identyfikacja ryzyka, jego analiza oraz wskazanie mechanizmów zapobiegawczych - zaradczych powstawaniu ewentualnych nieprawidłowości.

Autorzy w niniejszej publikacji przedstawili konsolidację trzech systemów zarządzania, takich jak: kontrola zarządcza, System Zarządzania Bezpieczeństwem Informacji z uwzględnieniem zapisów RODO[2] oraz zarządzanie kryzysowe.

2. ANALIZA SYSTEMÓW ZARZĄDZANIA

Punktem wyjścia do całościowej analizy jest wskazanie, iż kontrola zarządcza jako główny i najważniejszy element zarządzania organizacji zawiera w sobie wszystkie systemy zarządzania. W oparciu o sprawnie funkcjonującą kontrolę zarządczą kierownik jednostki dokonuje oceny stanu zarządzania jedynką składając oświadczenie o stanie kontroli zarządczej. Tym samym wskazuje poziom zarządzania w swojej jednostce.

Zgodnie z art. 68 ust. 1 „Kontrolę zarządczą w jednostkach sektora finansów publicznych stanowi ogół działań podejmowanych dla zapewnienia realizacji celów i zadań w sposób zgodny z prawem, efektywny, oszczędny i terminowy”[3]. W tym ust. ustawodawca wskazał główne założenia kontroli zarządczej w Jednostkach Sektora Finansów publicznych.

W ust. 2 Ustawodawca wskazał .„że celem kontroli zarządczej jest zapewnienie w szczególności:

- zgodności działalności z przepisami prawa oraz procedurami wewnętrznymi;
- skuteczności i efektywności działania;
- wiarygodności sprawozdań;
- ochrony zasobów;
- przestrzegania i promowania zasad etycznego postępowania;
- efektywności i skuteczności przepływu informacji;
- zarządzania ryzykiem[4].

Kolejnym systemem zarządzania, w którym występuje system zarządzania ryzykiem jest System Zarządzania Bezpieczeństwem Informacji. Zgodnie z KRI[5] – § 20. 1. „Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprze-

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

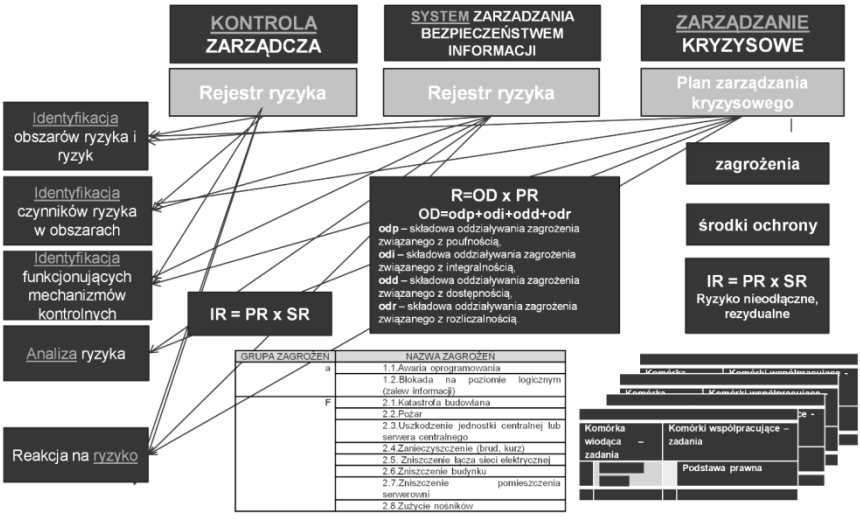
[3] Kontrola zarządcza została uregulowana w art. 68 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych

[4] Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych

[5] Krajowe Ramy Interoperacyjnosci – Rozporządzanie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017, poz. 2247)

czalność i niezawodność” [6]. Tym samym Ustawodawca wskazał, iż zgodnie z KRI zapewnienie przez kierownictwo jednostki systemu bezpieczeństwa odbywa się między innymi poprzez: przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy ” [7].

Diagram 1. Elementy wspólne i oddzielne systemów zarządzania.



Źródło: http://www.ptzp.org.pl/files/konferencje/kzz/artyk_pdf_2015/T2/t2_0099.pdf

Zgodnie z KRI § 20. 3. „Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą” w tym właśnie zakresie wskazano Normę PN-ISO/IEC 27005:2014-01. Norma PN-ISO/IEC 27005:2014-01 stanowi: „Zaleca się, aby podejście do zarządzania ryzykiem w bezpieczeństwie informacji było dostosowane do zarządzania ryzykiem organizacji” [8]. Nie mniej jednak warto do zarządzania ryzy-

[6] Rozporządzanie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017, poz. 2247)

[7] § 20 ust. 2 pkt. 3 Rozporządzanie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017, poz. 2247)

[8] Technika informatyczna -- Techniki bezpieczeństwa -- Zarządzanie ryzykiem w bezpieczeństwie informacji.

kiem oraz oceny jednostki wskazać jeszcze Normę PN-ISO 31000:2012. Norma PN-ISO 31000:2012 zaleca: „aby organizacje opracowały, wdrożyły i ciągle doskonaliły strukturę ramową, której celem jest integracja procesu zarządzania ryzykiem z całościowym ładem organizacyjnym, a także z jej strategią i planowaniem, zarządzaniem, procesami raportowania, politykami, wartościami i kulturą ”[9].

„Zarządzanie kryzysowe to działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym, która polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej”[10].

Na diagramie 1 zaprezentowano elementy wspólne oraz oddzielne systemów zarządzania takich jak: kontrola zarządza, System Zarządzania Bezpieczeństwem Informacji oraz zarządzanie kryzysowe. Zobrazowano tu na czym polega identyfikacja czynników ryzyka, identyfikacja ryzyk, funkcjonujących mechanizmów kontrolnych, analizy ryzyka oraz reakcji na ryzyko. Wskazano, jakie są podobieństwa oraz minimalne różnice w trzech systemach w zakresie prowadzenia procesów zarządzania ryzykiem. Proces zarządzania ryzykiem przedstawiono na przykładzie obszaru danych osobowych w związku z RODO.

Tabela 1. Identyfikacja obszarów ryzyka i ryzyka w obszarze danych osobowych w systemach zarządzania.

System	Kontrola zarządcza	System Zarządzania Bezpieczeństwem Informacji	Zarządzanie kryzysowe
Obszar ryzyka	Bezpieczeństwo informacji i danych	Bezpieczeństwo informacji i danych	Bezpieczeństwo informacji i danych
Ryzyka w obszarze	• Utrata danych • Ujawnienia danych • Brak danych • itp	• Utrata danych • Ujawnienia danych • Brak danych • itp	• Utrata danych • Ujawnienia danych • Brak danych • itp

Źródło: opracowanie własne

[9] Zarządzanie ryzykiem -- Zasady i wytyczne.

[10] Art. 2 - Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2007 Nr 89 poz. 590).

Pierwszym etapem procesu zarządzania ryzykiem w zidentyfikowanych systemach zarządzania na przykładzie danych osobowych jest dokonanie identyfikacji obszarów ryzyka oraz ryzyk w obszarach (tab. 1). Jest to element niezbędny pokazujący, iż obszar danych osobowych jest wspólny dla wszystkich trzech systemów i w związku z powyższym ryzyka w tych tym obszarze w tych systemach są takie same. W poniższej tabeli zawarto przykład identyfikacji i analizy ryzyka oraz ryzyk w obszarze danych osobowych.

Tabela 2. Identyfikacja czynników warunkujących powstanie ryzyka w obszarze danych osobowych w systemach zarządzania

System	Kontrola zarządcza	System Zarządzania Bezpieczeństwem Informacji	Zarządzanie kryzysowe
Obszar ryzyka	Bezpieczeństwo informacji i danych	Bezpieczeństwo informacji i danych	Bezpieczeństwo informacji i danych
Czynniki warunkujące powstanie ryzyka w obszarze	• Niezabezpieczenie informacji i danych • Niewłaściwe obchodzenie się z danymi • Brak nadzoru i kontroli • Brak procedur • Brak szkoleń • itp.	• Niezabezpieczenie informacji i danych • Niewłaściwe obchodzenie się z danymi • Brak nadzoru i kontroli • Brak procedur • Brak szkoleń • itp.	• Niezabezpieczenie informacji i danych • Niewłaściwe obchodzenie się z danymi • Brak nadzoru i kontroli • Brak procedur • Brak szkoleń • itp.

Źródło: opracowanie własne

Drugim etapem w procesie zarządzania ryzykiem jest zidentyfikowanie czynników warunkujących powstanie ryzyka. Tym samym dokonano identyfikacji czynników warunkujących powstanie ryzyka w obszarze danych osobowych w systemach zarządzania (tab. 2). W związku z tym, iż obszar ryzyka oraz ryzyka w obszarze były takie same, tym samym czynniki warunkujące powstanie tych ryzyk też były identyczne w tych trzech systemach. Tabela 3 przedstawia szczegółową analizę w tym zakresie.

We wszystkich trzech analizowanych systemach ,w obszarze dane osobowe ryzyka są takie same, czynniki warunkujące powstanie ryzyk też są identyczne, w związku powyższym funkcjonujące mechanizmy kontrolne też są takie same. Szczegółowe dane zawiera tabela 3.

Tabela 3. Identyfikacja funkcjonujących mechanizmów kontrolnych w obszarze danych osobowych w systemach zarządzania

System	Kontrola zarządcza	System Zarządzania Bezpieczeństwem Informacji	Zarządzanie kryzysowe
Obszar ryzyka	Bezpieczeństwo informacji i danych	Bezpieczeństwo informacji i danych	Bezpieczeństwo informacji i danych
Czynniki warunkujące powstanie ryzyka w obszarze	• Niezabezpieczenie informacji i danych • Niewłaściwe obchodzenie się z danymi • Brak nadzoru i kontroli • Brak procedur • Brak szkoleń • itp.	• Niezabezpieczenie informacji i danych • Niewłaściwe obchodzenie się z danymi • Brak nadzoru i kontroli • Brak procedur • Brak szkoleń • itp.	• Niezabezpieczenie informacji i danych • Niewłaściwe obchodzenie się z danymi • Brak nadzoru i kontroli • Brak procedur • Brak szkoleń • itp.

Źródło: opracowanie własne

Trzecim etapem zarządzania ryzykiem jest dokonanie analizy ryzyka. Mimo, iż obszar ryzyka jest taki sam, takie same też są ryzyka w obszarze oraz czynniki warunkujące te ryzyka to wyniki analizy ryzyka są już diametralnie inne (tab.4). Odmienne wyniki spowodowane są różnym podejściem do analizy ryzyka - zastosowaniem różnych metod analizy oraz różnych poziomów ryzyk – inne przedziały wartości punktowej dla ryzyka niskiego, inne dla średniego, a jeszcze inne dla wysokiego. Zastosowanie takich metod spowodowało, iż to samo ryzyko w różnych systemach ma różną wartość, a tym samym różny poziom wartości ryzyka. W przypadku systemu kontroli zarządczej ryzyko przybiera najwyższy poziom ryzyka czyli wartość 25. W przypadku Systemu Zarządzania Bezpieczeństwem Informacji ryzyko, mimo iż ma poziom wartości 40, nie wymaga działań zaradczych, natomiast w przypadku zarządzania kryzysowego ryzyko przybiera wartość 6 i też wymaga działań zaradczych. Przedstawiono to w tabeli poniżej, a szczegółowe analizy zawarto w diagramach od 2 do 4.

Tabela 4. Wartości ryzyk po przeprowadzeniu analizy ryzyka w obszarze danych osobowych w systemach zarządzania

System	Kontrola zarządcza	System Zarządzania Bezpieczeństwem	Zarządzanie kryzysowe
Wartość ryzyka po analizie	25 - wysokie	40- niskie	6- średnie
Działania	Wymaga działań	Akceptowalne	Wymaga działań

Źródło: opracowanie własne

W przypadku kontroli zarządczej przyjęto „metodę analizy 5x5". Ustalono, iż wartość ryzyka niskiego jest na poziomie od 1 do 6, ryzyka średniego od 8 do 12 , ryzyka wysokiego od 15 do 15. Takie podejście do analizy ryzyka w obszarze danych osobowych spowodowało oszacowanie wartości ryzyka na 25, co z kolei odpowiada wysokiemu poziomowi ryzyka (diag. 2).

Diagram 2. Wartości ryzyk po przeprowadzeniu analizy ryzyka w obszarze danych osobowych w systemach zarządzania

SKUTEK	katastrofalny	5	10	15	20	25
	poważny	4	8	12	16	20
	średni	3	6	9	12	15
	mały	2	4	6	8	10
	nieznaczny	1	2	3	4	5
PRAWDOPODOBIEŃSTWO		bardzo rzadkie lub prawie niemożliwe	małe	średnie	wysokie	prawie pewne
Niska 1-6		Średnia 8-12		Wysoka 15-25		

Źródło: opracowanie własne

W przypadku Systemu Zarządzania Bezpieczeństwem Informacji zastosowano „metodę analizy 10x10". Zastosowanie takiego podejścia spowodowało,

iż ryzyko danych osobowych w tym systemie oszacowane zostało na 40 punktów (diag. 3).

Diagram 3. Wyniki analizy ryzyka w obszarze danych osobowych w systemie kontroli zarządczej

ODDZIAŁYWANIE											
		10	20	30	40	50	60	70	80	90	100
		9	18	27	36	45	54	63	72	81	90
		8	16	24	32	40	48	56	64	72	80
		7	14	21	28	35	42	49	56	63	70
		6	12	18	24	30	36	42	48	54	60
	Katastrofalne	5	10	15	20	25	30	35	40	45	50
	Poważne	4	8	12	16	20	24	28	32	36	40
	Średnie	3	6	9	12	15	18	21	24	27	30
	Małe	2	4	6	8	10	12	14	16	18	20
	Nieznaczne	1	2	3	4	5	6	7	8	9	10
	Niska 1-40		Średnia 41-74				Wysoka 75-100				

Źródło: opracowanie własne

W związku z tym iż przyjęto, że od 1 do 40 wartość ryzyka jest niska, ryzyko to zostało zakwalifikowane jako ryzyko niskie. W przypadku kontroli zarządczej nie mieściłoby się w skali analizy ryzyka.

W przypadku systemu zarządzania kryzysowego zastosowano, tak jak w przypadku kontroli zarządczej, „metodę analizy ryzyka 5x5" (diag.4). Jednak w tym przypadku ustalono inne poziomy ryzyka. Ryzyko niskie kształtuje się na poziomie od 1 do 4, średnie na poziomie od 4 do 12 (4 tylko wówczas, gdy prawdopodobieństwo lub oddziaływanie mają wartość co najmniej 4), wysokie od 15 do 25.

Pod dokonaniu szczegółowej analizy ryzyka w obszarze dane osobowe w trzech systemach należy stwierdzić, że przyjmując różnorodne podejście do analizy ryzyka to samo ryzyko w różnych obszarach, mimo takich samych czynników ryzyka oraz funkcjonujących mechanizmów kontrolnych będzie miało różną wartość, a tym samym różny poziom ryzyka.

Diagram 4. Wyniki analizy ryzyka w obszarze danych osobowych w systemie zarządzania kryzysowego

Źródło: opracowanie własne

Tabela 5. Reakcja na zidentyfikowane ryzyko przy zastosowaniu różnego podejścia do analizy ryzyka w obszarze danych osobowych w systemach zarządzania

System	Kontrola zarządcza	System Zarządzania Bezpieczeństwem	Zarządzanie kryzysowe
Wartość ryzyka po analizie	25 - wysokie	40-niskie	6- średnie
Działania	Wymaga działań	Akceptowalne	Wymaga działań
Reakcja na ryzyko	• Szczegółowa analiza działań • Opracowanie procedur • Aktualizacja procedur • Stały monitoring czynników ryzyka	• Nie wymaga działań	• Aktualizacja procedur • Stały monitoring czynników ryzyka

Źródło: opracowanie własne

W analizowanym przypadku ryzyko danych osobowych w systemie kontroli zarządczej jest na poziomie wysokim i wymaga natychmiastowych działań zaradczych, aby zminimalizować poziom ryzyka do poziomu akceptowalnego

w jednostce – poziom niski. W systemie zarządzania kryzysowego jest na poziomie średnim w związku z czym wymaga przeglądu i stałego monitoringu, tak aby nie dopuścić do podwyższenia poziomu ryzyka do wysokiego. W przypadku Systemu Zarządzania Bezpieczeństwem Informacji ryzyko w obszarze danych osobowych jest na poziomie niskim, czyli akceptowalnym.

3. PODSUMOWANIE

W przypadku, kiedy w jednostce jest kilka systemów zarządzania opartych o system zarządzania ryzykiem, niezbędne jest ustalenie jednej metodyki analizy ryzyka do wszystkich systemów. Zastosowanie jednej metodyki przyczyni się miedzy innymi do: jednolitego podejścia do zarządzania ryzykiem (jednolite zasady postępowania), oszczędności czasu przez pracowników, „trzymania" ryzyka w jednym ręku, niepowielania dokumentów, a co najważniejsze oszczędności środków w jednostce.

Literatura:

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
[2] Rozporządzanie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017, poz. 2247).
[3] art. 68 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.
[4] art. 2 - Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2007 Nr 89 poz. 590).
[5] Norma PN-ISO/IEC 27005:2014-01.
[6] Norma PN-ISO 31000:2012.

prof. dr hab. Krzysztof Malik
Politechnika Opolska
Wydział Ekonomii i Zarządzania
ul. Luboszycka 7 45-036 Opole
k.malik@po.opole.pl

Barbara Bętkowska-Cela
Izba Administracji Skarbowej w Opolu
ul. Ozimska 19, 45-057 Opole
barbara.betkowska-cela@mf.gov.pl

dr Agnieszka Dornfeld-Kmak
Izba Administracji Skarbowej w Opolu
ul. Ozimska 19, 45-057 Opole
agnieszka,dornfeld-kmak@mf.gov.pl

Robert EHRMANN

LABORATORIA KRAJOWEJ ADMINISTRACJI SKARBOWEJ

Streszczenie: Artykuł prezentuje laboratoria w jakie jest wyposażona Krajowa Adninistracja Skarbowa na terenie Polski. Zawiera on krótki zarys historyczny powstawania laboratoriów oraz uzasadnia celowość ich powstania. W pracy opisano jaką rolę odgrywają tego rodzaju laboratoria w działalności urzędów celno-skarbowych. Przedstawiono przykładowe wyposażenie, zwracając uwagę na cel i zakres prowadzonych badań.

Słowa kluczowe: laboratorium, badania laboratoryjne.

LABORATORY OF NATIONAL REVENUE ADMINISTRATION

Summary: The paper presents a description of the tasks performed by the laboratories in which the National Revenue Administration in Poland is equipped. It contains a brief outline of the historical reasons for the formation of laboratories and the desirability of their creation. The work describes the role of such laboratories in the activities of customs and tax offices. Exemplary equipment is presented, paying attention to the purpose and scope of the research.

Keywords: laboratory, labor tests.

1. WSTĘP

Laboratoria celno–skarbowe funkcjonujące w strukturach Krajowej Administracji Skarbowej zostały utworzone w wyniku działań dostosowawczych podjętych w latach 90 – tych przez administracje celne krajów aspirujących do członkostwa w Unii Europejskiej. Osiągnięcie zdolności do stosowania wspólnej polityki gospodarczej, handlowej oraz celnej, związane było z koniecznością przeprowadzenia transformacji administracji celnej, w szczególności z utworzeniem laboratoriów celnych. Z założenia placówki takie realizują w Unii Europejskiej szereg znaczących zadań, związanych z wykonywaniem badań próbek towarów, dostarczaniem naukowych ekspertyz potrzebnych przy wprowadzaniu w życie regulacji UE we wszystkich zagadnieniach związanych z Taryfą Celną, klasyfikacją i nomenklaturą. Laboratoria odgrywają istotną rolę w walce z nielegalnym handlem i oszustwami, a także coraz aktywniej biorą udział w zwalczaniu fałszerstw i podróbek towarów, stają się - w walce przeciw terroryzmowi- zapleczem naukowo technicznym funkcjonariuszy działających bezpośrednio w terenie. Bardzo istotnym faktem było wskazanie laboratoriów jako skutecznego narzędzia chroniącego życie i zdrowie ludzi oraz zwierząt, a także środowiska naturalnego przed napływem na obszar UE różnorodnych substancji niebezpiecznych.

2. HISTORIA POWSTANIA LABORATORIÓW KAS

W październiku 1997 roku utworzono pierwszą placówkę - Centralne Laboratorium Celne, które rozpoczęło swoją działalność jako Wydział w ówczesnym Departamencie Taryf Celnych i Reguł Pochodzenia Towarów Głównego Urzędu Ceł.

Należy pamiętać, że był to zaledwie pierwszy etap i jeden ze środków służących do realizacji celu, jakim było uzyskanie przez polską administrację celną gotowości operacyjno-technicznej do wykonywania efektywnej kontroli celnej i skutecznego zwalczania przestępczości celnej.

Założeniem było utworzenie w Polsce sieci laboratoriów, składającej się z jednostki centralnej, posiadającej szerokie możliwości badawcze i najbardziej wszechstronne wyposażenie analityczne, oraz mniejszych laboratoriów regionalnych, które stanowić powinny pierwszą linię wsparcia kontroli granicznej.

W latach 1999-2004 utworzone zostały kolejne laboratoria celne: w Białymstoku (1999 r.), w Koroszczynie (2001 r.), w Przemyślu (2003 r.) oraz w Gdyni (2003 r.). Proces tworzenia sieci laboratoriów celnych w administracji celnej został zakończony w połowie 2004 r.

Jednocześnie rozpoczęto realizację drugiego etapu przystosowania do wymogów stawianych przez Unię Europejską, tj. wdrażanie systemów zarządzania oraz spełnienie wymagań zawartych w międzynarodowej normie PN-EN ISO/IEC 17025 „Ogólne wymagania dotyczące kompetencji laboratoriów badawczych i wzorcujących". W 2003 roku Centralne Laboratorium Celne jako pierwsze uzyskało certyfikat akredytacji laboratorium badawczego (Nr AB 411) wydany przez Polskie Centrum Akredytacji. Następnie akredytację uzyskiwały:

- w 2004 r.- Laboratorium Celne w Białymstoku - AB 501,
- w 2005 r.- Laboratorium Celne w Koroszczynie - AB 656,
- w 2007 r.- Laboratorium Celne w Przemyślu – AB 826,
- w 2008 r. - Laboratorium Celne w Gdyni – AB 907.

Od chwili uzyskania akredytacji system zarządzania we wszystkich laboratoriach podlega ciągłemu rozwojowi. Wdrożenie systemu zarządzania oraz uzyskanie akredytacji przyniosło wiele wymiernych korzyści, w tym:

- udowodnione kompetencje do wykonywania badań,
- wzrost wiarygodności uzyskiwanych wyników badań,
- potwierdzenie bezstronności i rzetelności działania,
- wprowadzenie efektywnego systemu dokumentowania,
- zapewnienie dobrej praktyki profesjonalnej na każdym etapie wykonywania badań.

Akredytacja daje gwarancję, że akredytowane przez Polskie Centrum Akredytacji usługi (w tym przypadku badania) są godne zaufania i akceptowane na rynkach europejskich i światowych.

Obecnie w sieci laboratoriów KAS stosowanych jest łącznie 160 akredytowanych metod pomiarowych i analitycznych.

Jednocześnie, wysoki poziom wyników badań i ich wiarygodność, zapewnia prowadzona w laboratoriach bieżąca kontrola jakości badań, polegająca na regularnym monitorowaniu jakości uzyskiwanych wyników, poprzez następujące działania:

- udział w badaniach biegłości i/lub porównaniach międzylaboratoryjnych (PT/ILC),
- korzystanie z certyfikowanych materiałów odniesienia,
- powtórne badanie próbek przez te same lub inne osoby,
- badanie próbek przy użyciu różnych metod badawczych,
- prowadzenie sprawdzeń bieżących i okresowych wyposażenia pomiarowego przy wykorzystaniu wzorców i materiałów odniesienia.

3. ZAKRES DZIAŁAŃ LABORATORIÓW KAS

Wykonując regulaminowe zadania, sieć laboratoriów KAS wspiera działania kontrolne, przyczyniając się tym samym do zwiększania poboru ceł i podatków oraz ochrony przed przywozem towarów mogących stanowić zagrożenie dla zdrowia i bezpieczeństwa obywateli lub środowiska naturalnego.

Na rys.1 przedstawiono przykładową aparaturę analityczno-badawczą, stanowiącą wyposażenie laboratoriów celno-skarbowych. Na tego rodzaju aparaturze obecnie laboratoria KAS wykonują badania:

- dotyczące ustalania prawidłowej klasyfikacji taryfowej i rozstrzygania sporów klasyfikacyjnych towarów - zgodnie z wymogami Wspólnotowej Taryfy Celnej (w tym badania wykonywane dla potrzeb Wiążącej Informacji Taryfowej oraz Wiążącej Informacji Akcyzowej),
- prowadzonej przez KAS kontroli przywozu, wywozu i tranzytu towarów podlegających ograniczeniom pozataryfowym, w szczególności ze względu na ochronę życia i zdrowia ludzi, ochronę środowiska i bezpieczeństwa państwa,
- -dla potrzeb organów KAS, realizujących zadania m.in. w sprawowaniu szczególnego nadzoru podatkowego i egzekwowaniu należnych kwot podatku VAT i akcyzy,
- - w ramach prowadzonej przez KAS kontroli próbek artykułów rolno – spożywczych objętych Wspólną Polityką Rolną, w tym określanie zawartości tych składników, od których naliczane są refundacje wywozowe - wypłacane przez ARR.

Rysunek 1. Przykładowa aparatura analityczno-badawcza

Źródło: opracowanie własne

Szeroko pojęta ochrona życia oraz zdrowia obywateli stanowi obecnie najintensywniej rozwijający się obszar działalności laboratoriów KAS. W szczególności działalność w tym zakresie związana jest z realizacją zapisów ustawy z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii.

Ww. ustawa uprawnia jednostki organizacyjne Krajowej Administracji Skarbowej przy wykonywaniu zadań określonych ustawą z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej do wchodzenia w posiadanie środków odurzających, substancji psychotropowych lub ich preparatów oraz prekursorów kategorii 1 w ilościach niezbędnych do przeprowadzenia badań potwierdzających popełnienie przestępstwa.

4. PRZYKŁADOWE BADANIA

Rysunek 2. Przykłady opakowań środków zastępczych (dopalaczy) badanych w Centralnym Laboratorium Celno-Skarbowym.

Źródło: opracowanie własne

Dla przykładu, w 2017 r. do Centralnego Laboratorium Celno-Skarbowego wpłynęło 2478 próbek podejrzanych o zawartość środków odurzających lub substancji psychoaktywnych wykazanych w załącznikach do ustawy o przeciwdziałaniu narkomanii, jak również mogących zawierać substancje psychoaktywne nie wykazane w załącznikach do ww. ustawy - tj. nowe substancje psychoaktywne i środki zastępcze – „dopalacze". W wyniku przeprowadzonych badań w 1658 próbkach stwierdzono obecność środków odurzających lub substancji

psychoaktywnych, natomiast w 274 próbkach wykazano obecność nowych substancji psychoaktywnych i środków zastępczych.

Środkiem zastępczym nazywamy produkt zawierający co najmniej jedną nową substancję psychoaktywną lub inną substancję o podobnym działaniu na ośrodkowy układ nerwowy, który może być użyty zamiast środka odurzającego lub substancji psychotropowej.

Istotnym jest, że od października 2011 r. w ramach realizacji podpisanego porozumienia pomiędzy Szefem ówczesnej Służby Celnej i Dyrektorem Krajowego Biura do Spraw Przeciwdziałania Narkomanii o współdziałaniu Służby Celnej i Krajowego Biura do Spraw Przeciwdziałania Narkomanii w zakresie wymiany informacji w ramach Systemu Wczesnego Ostrzegania o Nowych Narkotykach, Centralne Laboratorium Celno-Skarbowe sporządza i przesyła raporty zawierające wykazy zidentyfikowanych substancji stanowiących środki odurzające i substancje psychotropowe.

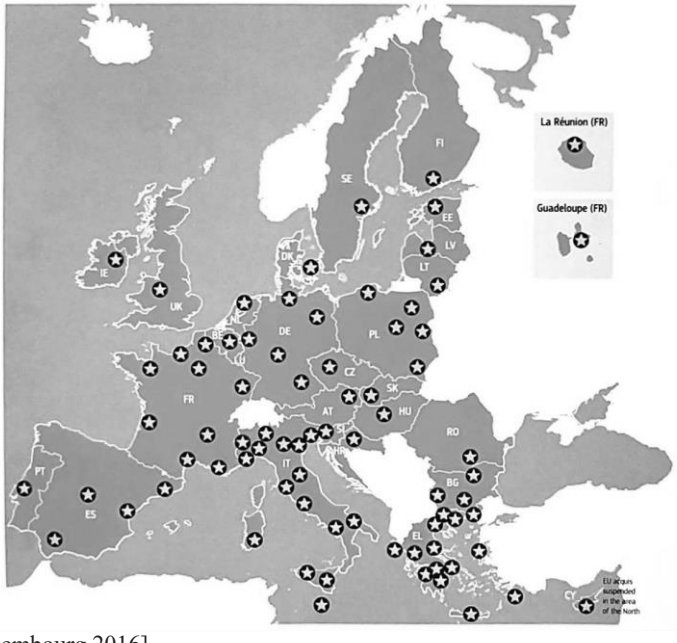
Raporty przesyłane przez Centralne Laboratorium Celno-Skarbowe do KBPN wchodzą w skład corocznego raportu krajowego, który następnie kierowany jest do Europejskiego Centrum Monitorowania Narkotyków i Narkomanii (EMCDDA). Na podstawie danych krajowych, EMCDDA opracowuje coroczny raport o stanie problemu narkotykowego w Europie. Uczestnictwo laboratoriów KAS we wspólnym w UE systemie zbierania danych, przyczynia się do generowania coraz bardziej rzetelnych danych, dotyczących zjawiska narkomanii na poziomie europejskim.

5. WSPÓŁPRACA MIĘDZYNARODOWA

Polskie laboratoria KAS wraz z laboratoriami celnymi poszczególnych krajów członkowskich UE tworzą Europejską sieć laboratoriów celnych, które współpracują ze sobą w ramach grupy powołanej przez Komisję Europejską - CLEN - Customs Laboratories European Network (niegdyś GCL – Group of Customs Laboratories).

Europejska sieć laboratoriów pracuje nad zapewnieniem spójnej wykładni norm technicznych w całej Unii Europejskiej. Pracownicy polskich laboratoriów biorą czynny udział w pracach grupy CLEN, poprzez regularny udział w badaniach biegłości i porównaniach międzylaboratoryjnych, seminariach, warsztatach oraz pracach grup roboczych powoływanych przez Komisję Europejską.

Rysunek 3. Europejska sieć laboratoriów



Źródło: [Luxembourg 2016]

Ważnym osiągnięciem grupy CLEN było opracowanie i udostępnienie elektronicznego podręcznika „SAMANCTA". Elektroniczny podręcznik „SAMANCTA" przeznaczony jest dla funkcjonariuszy organów celnych oraz podatkowych. W podręczniku zgromadzone zostały szczegółowe informacje z zakresu poboru i zabezpieczania próbek towarów, które są następnie przesyłane do badań laboratoryjnych.

Literatura:

[1] Luxembourg: Publications Office of the European Union, 2016; European Customs Laboratories, Experience you can rely on".
[2] Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (tekst jednolity Dz.U. z 2018 r. poz. 1030).
[3] Rozporządzenie Ministra Zdrowia z dnia 7 sierpnia 2017 r. w sprawie wykazu nowych substancji psychoaktywnych (Dz.U. z 2017 r. poz. 1582).

insp. Robert Ehrmann
Centralne Laboratorium Celno-Skarbowe
Mazowiecki Urząd Celno-Skarbowy
05-402 Otwock, ul. Kolorowa 13
e-mail robert.ehrmann@mf.gov.pl

Piotr KRACZMAR
Mariusz R. RZĄSA

PROBLEMATYKA POBORU PRÓBEK W CYSTERNACH PRZEWOŻĄCYCH MATERIAŁY PODLEGAJĄCE KONTROLI CELNO-SKARBOWEJ

Streszczenie: W pracy opisano problemy, z jakimi spotykają się służby celno-skarbowe podczas kontroli przewożonych materiałów płynnych. Opisano podstawowe metody poboru próbek oraz narzędzia, jakie są stosowane. Zwrócono uwagę na problemy, jakie w praktyce nastręcza stosowanie tych metod i narzędzi. Przeprowadzono analizę problematyki pomiarów oraz zwrócono uwagę na obszary, w których pożądana jest współpraca ze specjalistami z ośrodków akademickich.

Słowa kluczowe: próbki, cysterna, paliwa, alkohol,

PROBLEMS OF SAMPLING OF MATERIALS SUBJECT TO CUSTOMS AND TAX CONTROL TRANSPORTED BY TANKS

Summary: The paper describes the problems faced by customs and tax control during the inspection of transported liquid materials. The basic methods of sampling and the tools used are described. Attention is drawn to the problems that occur in practice when using these methods and tools. An analysis of the measurement problems was carried out and on this basis, areas in which cooperation with specialists from university.

Keywords: samples, tank, fuel, alcohol

1. WSTĘP

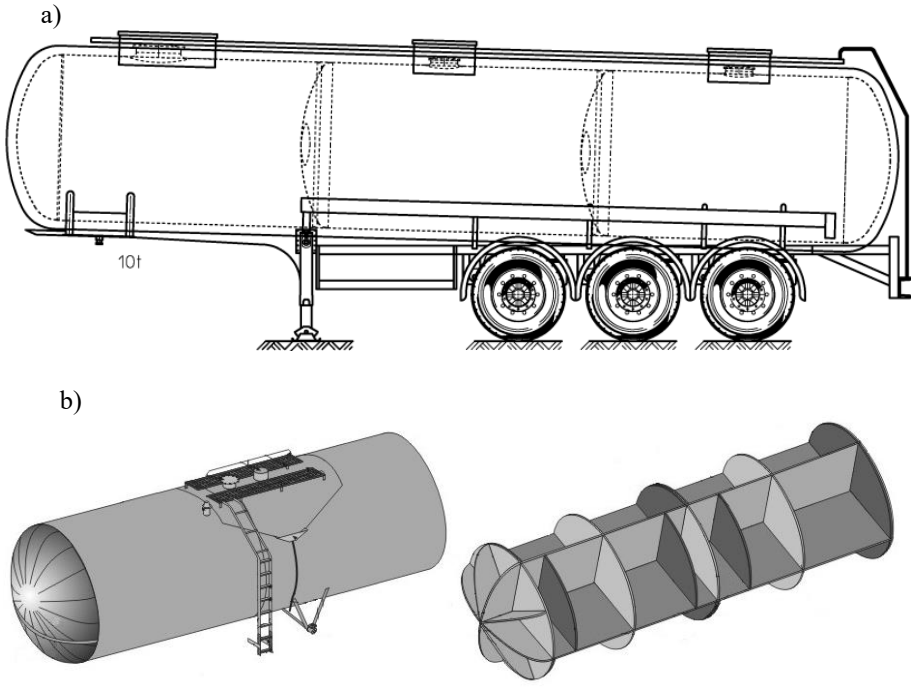
Zgodnie z ustawą o Krajowej Administracji Skarbowej [Ustawa z dnia 16 listopada 2016r], kontroli celno-skarbowej podlegają między innymi paliwa, alkohole i oleje napędowe. Ponadto kontroli podlegają wszystkie przewożone towary zakwalifikowane, jako towary celne [Rozporządzenie Parlamentu Europejskiego i Rady (EU) NR 952/2013], towary w procedurze zawieszenia poboru akcyzy [Ustawa z dnia 6 grudnia 2008r] oraz towary objęte ustawą SENT [Ustawa 9 marca 2017r]. Kontrola polega między innymi na weryfikacji tożsamości towaru i jego nienaruszalności oraz sprawdzeniu czy przewożone towary są zgodne z deklaracją, co do rodzaju i jakości. Kontrola taka jest podstawą do sprawdzenia prawidłowego rozliczenia należności z tytułu podatków i ceł. Tego rodzaju kontrole mają znaczenie gospodarcze, gdyż chronią one polski i europejski rynek przed nielegalnymi towarami lub niespełniających odpowiednich norm, a nawet szkodliwymi. Tego rodzaju działania stabilizują rynek umożliwiając rozwijanie się zdrowej konkurencji oraz gwarantują stabilność legalnie

i zgodnie z prawem działających firmy. Działania kontroli celno-skarbowej w obszarze kontroli artykułów spożywczych ograniczają niebezpieczeństwo zatrucia się ludzi i zwierząt. W ostatnich latach wielokrotnie odnotowywano przypadki zatruć alkoholem niewidomego pochodzenia. Ochrona konsumenta przed towarami niewiadomego pochodzenia czy wręcz trującymi [Raport] stanowi bardzo ważny aspekt natury moralno prawnej.

Z uwagi, iż materiały płynne stanowią bardzo dużą grupę towarów przewożonych różnego rodzaju cysternami, konieczna jest rzetelna kontrola przewożonych płynów. Jednym z podstawowych elementów mających wpływ na rzetelną ocenę przewożonego płynu jest sposób poboru próbek do badania. Krajowa Administracja Skarbowa dysponuje wykwalifikowaną kadrą oraz nowoczesnym sprzętem do poboru prób, zarówno w trakcie transportu jak i miejscu wytwarzania oraz konsumpcji towarów. W niniejszej pracy przedstawiono .m.in sprzęt, jakim dysponują urzędy celno-skarbowe oraz zwrócono uwagę na problemy związane ze specyfiką poboru próbek.

2. PROBLEMATYKA POBORU PRÓBEK

Rysunek 1. Typowe cysterny do przewozu materiałów płynnych
a) cysterna samochodowa, b) cysterna kolejowa



Źródło: https://www.feldbinder.com/pl/site__90/, https://modelik.pl/nr-kat-1218-406-ra-p-347.html.

Na rynku polskim transport materiałów płynnych, w tym paliw, alkoholi i olejów, najczęściej odbywa się za pomocą cystern zamontowanych na samochodach (rys.1a) lub wagonach kolejowych (rys.1b), a także w mniejszej skali paletopojemnikami. Cysterny samochodowe są jedno lub wielo-komorowe. Cysterny kolejowe najczęściej buduje się jako jednokomorowe. Większość cystern posiada włazy górne tzw. rewizyjne, aczkolwiek tych samych włazów używa się również do napełniania cystern. Ze względu na ochronę środowiska obecnie do napełniania cystern materiałami lotnymi używa się króćców (zaworów) spustowych z systemem odprowadzania oparów.

Zgodnie z obowiązującymi przepisami sposób poboru próbek jest określony polskimi normami [Polska Norma PN-EN ISO 3170, Polska Norma PN-A-79521, Polska Norma PN-83 N-03010]. Próbobiorca, czyli osoba pobierająca próbki, winna posiadać stosowne uprawnienia i wiedzę na temat poboru próbek. Parametrami,które należy określić przed przystąpieniem do poboru, są rodzaj materiału oraz jednorodność w przekroju poprzecznym. Na tej podstawie należy określić liczbę i punkty poboru próbek oraz opracować plan poboru próbek. Prawidłowe wykonanie tych czynności gwarantuje reprezentatywność pobieranego materiału. Podczas przygotowywania tych czynności niezbędne jest przeanalizowanie dokumentów przewozowych, oględziny środka transportu oraz uwzględnienie informacji otrzymanych od przewoźnika.

Czynności te stają się znacznie trudniejsze w sytuacji, gdy sprawdzana jest cysterna, w której przemycany jest jakiś towar. W takiej sytuacji często dokumenty przewozowe są sfałszowane, a przewoźnik zataja pewne informacje. Próbobiorca w takiej sytuacji w dużej mierze musi bazować na własnej wiedzy i doświadczeniu. Wymaga to znajomości budowy typowych cystern oraz fizyki zachowania się cieczy podczas transportu w cysternie. Z uwagi na zróżnicowanie przewożonych cieczy niejednokrotnie konieczna jest znaczna wiedza z zakresu mechaniki płynów. Niejednokrotnie celowa jest konsultacja z ekspertem z zakresu pomiarów parametrów płynów. Eksperci tacy rzadko są zatrudnieni w urzędach celno-skarbowych, a konsultacje takie powodują znaczne wydłużenie czasu przeprowadzanej kontroli.

Różnorodność w budowie cystern nie tylko wymaga dostosowania narzędzi probierczych, ale również nastręcza zróżnicowanych problemów podczas poboru próbek oraz przy opracowaniu planu poboru próbek. Cysterny wielokomorowe z reguły nastręczają mniej problemów. Pojemności komór są znacznie mniejsze od pojemności cystern, oraz komory nie posiadają dodatkowych przegród (falochronów). Stąd opracowując plan poboru próbek należy uwzględnić jedynie skłonności mieszaniny cieczy do rozwarstwienia w wyniku leżakowania w cysternie. Znacznie trudniejsze jest opracowanie planu poboru dla cystern jednokomorowych . W tego rodzaju cysternach, ze względu na bezpieczeństwo transportu, przestrzeń wewnątrz cysterny jest przedzielona szeregiem grodzi oraz krat. Kraty poziome znacząco utrudniają dostęp do dolnych pokładów przewożonego płynu.

Napełniając, czy opróżniając całą cysternę sumaryczna ilość mieszaniny cieczy składającej się z kilku komponentów nie ulegnie zmianie. Jednak podczas transportu niejednokrotnie dochodzi do rozwarstwienia nie tylko w kierunku pionowym, ale również na długości cysterny w obszarach pomiędzy grodziami. Uwzględnienie tych zjawisk wymaga znacznej wiedzy z zakresu mechaniki płynów, co uzasadnia potrzebę współpracy z ośrodkami akademickimi.

Procedura poboru próbek przewiduje pobór odpowiedniej liczby tzw. próbek jednostkowych (pierwotnych), z których następnie przygotowuje się próbki ogólne, z których z kolei przygotowuje się próbki laboratoryjne. Sposób poboru winien zapewnić nie tylko reprezentatywność próbki, ale także dalsze postępowanie nie może zmienić właściwości pobranego materiału.

3. PROBLEMATYKA POBORU PRÓBEK Z CYSTERN I ZBIORNIKÓW STACJONARNYCH

Różnorodność w budowie cysterny oraz wielość przewożonych towarów wymusza konieczność posiadania bardzo zróżnicowanych urządzeń do pobierania próbek. Jednym z problemów jest zminimalizowanie liczby urządzeń do poboru (próbopobieranika), co wymusza konicznośc zwiększenia uniwersalności posiadanych urządzeń probierczych. Typowe urządzenia do poboru próbek są zdeterminowane normą PN-EN ISO 3170 oraz PN-A-79521.

W przypadku poboru substancji płynnych ze zbiorników (stacjonarnych czy cystern samochodowych bądź kolejowych) najczęściej stosowanymi metodami poboru są: pobór punktowy lub przekrojowy. Przy metodzie punktowej należy pobrać odpowiednią ilość prób punktowych zalecanych przez normę w zależności od typu zbiornika i wysokości słupa cieczy oraz rodzaju towaru. Następnie wartości pomiarowe z poszczególnych próbek są uśredniane. Metoda ta jest obarczona znacznym błędem w przypadku cieczy rozwarstwionych, gdy rozkład koncentracji poszczególnych frakcji jest rozkładem nieliniowym na wysokości cysterny. W takich przypadkach bardziej reprezentatywnym jest pobór próbki przekrojowej. Pobór polega na opuszczaniu zbiornika pobierczego ze stałą prędkością zanurzania. Podczas opadania zbiornika na dno cysterny następuje nieprzerwany i ze stałym strumieniem pobór cieczy. W wyniku takiego pomiaru w zbiorniczku znajduje się uśredniona wartość cieczy pobranej na całej wysokości cysterny.

Nie bez znaczenia na jakość pobieranej cieczy mają warunki otoczenia, dlatego poboru należy dokonywać w odpowiednio przygotowanym miejscu, nienarażonym na opady, zanieczyszczenia czy nadmierną temperaturę. Próbobiorca musi posiadać czystą odzież ochronną, a sprzęt do poboru musi być czysty i suchy, zaś w przypadku towarów lotnych posiadać możliwość schłodzenia naczyń i próbek. Próbopobieralniki i opakowania na próbki muszą być suche i wolne od zanieczyszczeń, a w momencie poboru należy przepłukać je pobieraną cieczą. Wymóg ten niejednokrotnie nastręcza wielu trudności, gdyż niektóre produkty np. ropopochodne są trudne do usunięcia. Niejednokrotnie niektóre elementy próbopobieralnika są elementami jednorazowymi. Poszukiwanie no-

wych rozwiązań technicznych i materiałowych jest bardzo istotnym problemem w kontekście wykorzystania aparatury probierczej w procesach kontroli.

W przypadku mniejszych zbiorników, komór lub gdy istnieje taka możliwość (zbiornik posiada mieszadła, pompę obiegową) można towar wymieszać celem jego ujednorodnienia. Oceniając jednorodność płynu należy uwzględnić rodzaj towaru (możliwość rozwarstwienia), temperaturę, czas, w którym towar pozostawał w bezruchu lub który upłynął od załadunku, kształt, budowę i wielkość zbiornika. Czas mieszania będzie uzależniony od stopnia rozwarstwienia cieczy. Określenie minimalnego czasu mieszania niejednokrotnie wymaga posiadania specjalistycznej wiedzy technicznej.

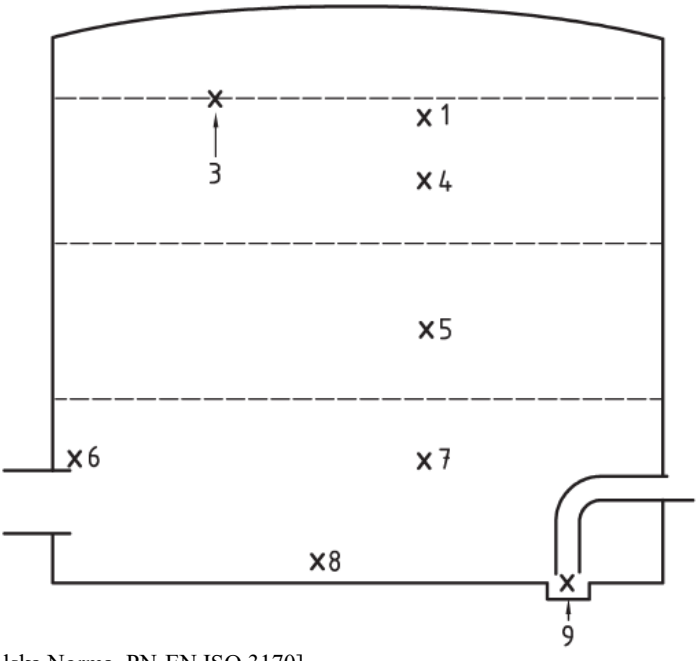
Odrębnym zagadnieniem jest pobór próbek ze zbiorników hermetycznych i z wytycznymi dotyczącymi transportu niektórych towarów (alkohol odwodniony, towary z frakcjami bardzo lotnymi itp.). W takim przypadku pobór próbek należy przeprowadzić z króćców załadunkowo-rozładunkowych. Niejednokrotnie kontrolę przeprowadza się podczas załadunku lub rozładunku cysterny. W tym celu na króciec załadunkowo/wyładunkowy zakłada się specjalną przejściówkę, która jest wyposażona jest w kranik do poboru próbek. Stosując pobór próbek przy załadunku lub wyładunku towaru należy wcześniej w planie poboru próbek przewidzieć liczbę i ilość pobranych próbek pierwotnych z odpowiednim zapasem, gdyż po zakończeniu czynności nie będzie możliwości dobrania próbek.

4. BUDOWA I RODZAJE URZĄDZEŃ DO POBORU PRÓBEK

Przy poborze próbek ze zbiorników o wysokości do 2 m, poboru próbki można dokonać przy pomocy pipety, natomiast przy większych zbiornikach należy zastosować specjalną metodę poboru próbki przekrojowej za pomocą zgłębnika lub alternatywnie za pomocą pompki podciśnieniowej do poboru próbek.

Przy poborze próbek metodą punktową wyróżnia się kilka charakterystycznych punktów poboru próbki. Do najbardziej typowych należą punkty określone w Polskiej Normie PN-EN ISO 3170. Wyróżnia się próbkę szczytową x1, powierzchniową x3, górną x4, środkową x5, dolną x7, denną x8, z poziomu rury odpływowej lub wylotu x6 oraz z odstojnika x9 (*Rys 3*). W zależności od parametru jaki jest badany, należy wybrać odpowiednie miejsce poboru lub kompilację tych miejsc. Przykładowo, aby zbadać zawartość wody w paliwie – najbardziej reprezentatywna będzie próbka denna lub z odstojnika. W celu zbadania znacznika i barwnika dla olejów opałowych odpowiednie będzie dowolnie miejsce. W przypadku zbadania tożsamości towaru pod kątem taryfikacji konieczna jest kompilacja próbki górnej, środkowej i dolnej.

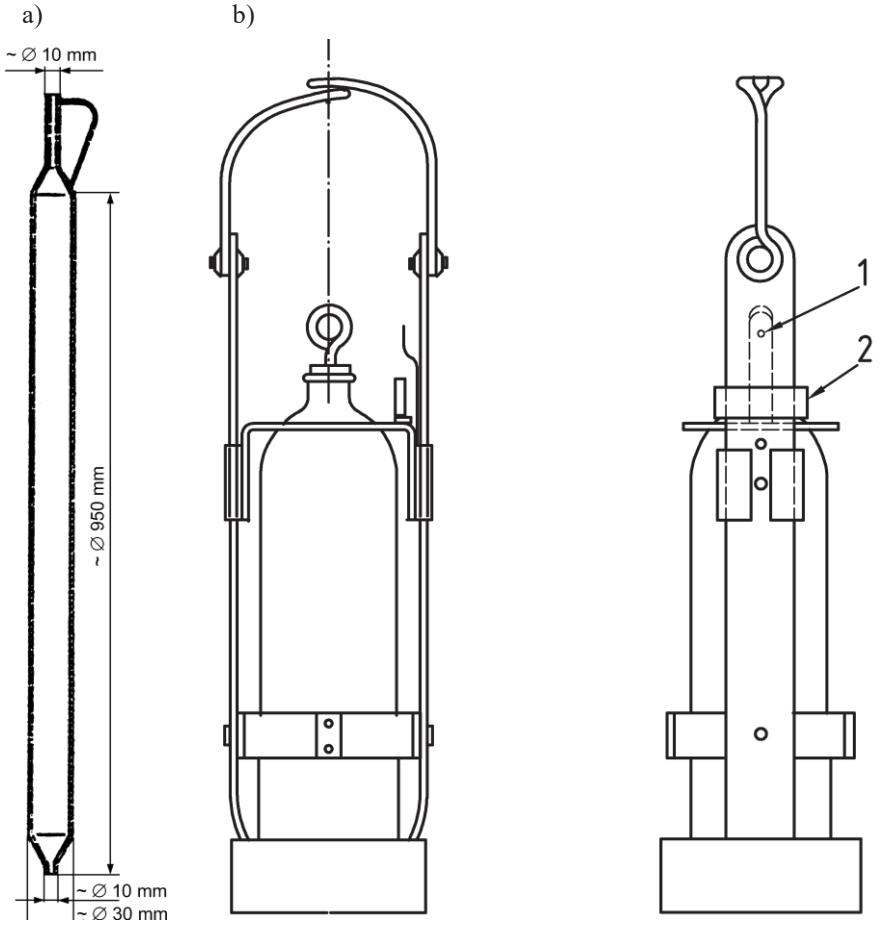
Rysunek 3. Miejsca poboru próbek



Źródło: [Polska Norma PN-EN ISO 3170].

Na rysunku 4 przedstawiono typowe urządzenia do poboru próbek punktowych. Pipety (rys.4a) mogą być stosowane do poboru próbek ze zbiorników o głębokości poniżej 1m. Są one stosowane najczęściej do poboru próbek z paletopojemników. W przypadku cystern często stosuje się różnego rodzaju butelki do poboru próbek punktowych (rys.4b). Zasada działania polega na tym, że butelkę z zamkniętym zaworem wlotowym *1* zanurza się wraz z koszem obciążającym *2* w zbiorniku. Gdy butelka opuszczana za pomocą linki zaczepionej za uchwyt kosza zostanie zanurzona do wybranej głębokości następuje otwarcie zaworu wlotowego poprzez pociągnięcie drugiej linki, która zaczepiona jest do spustu zaworu wlotowego. Po napełnieniu butelki jest ona wyciągana wraz z koszem obciążającym.

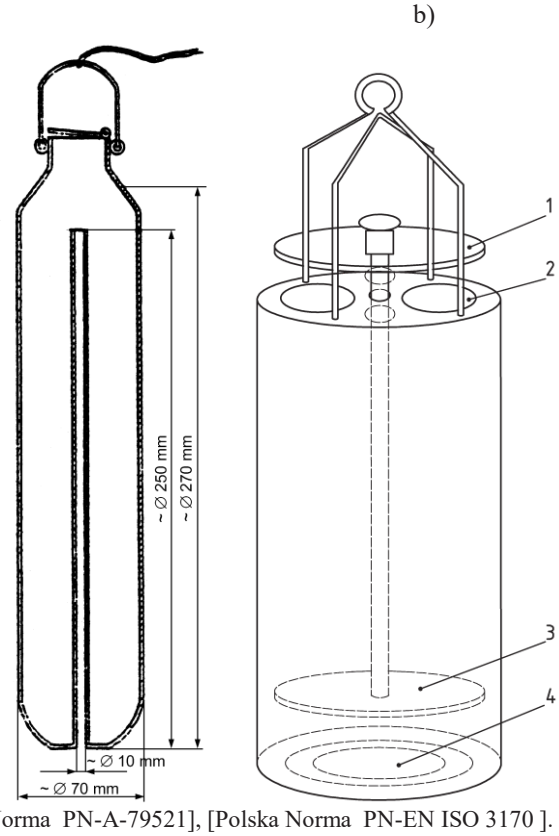
Rysunek 4. Urządzenia do poboru próbek punktowych:
a) pipeta, b) butelka do poboru próbek



Źródło: [Polska Norma PN-A-79521], [Polska Norma PN-EN ISO 3170].

Do poboru próbek przekrojowych stosuje się różnego rodzaju zgłębniki (rys.5). Zgłębniki dzieli się ze względu na kierunek napełniania tj. od góry, od dołu lub dwukierunkowe. Zgłębniki posiadają system zamykania i otwierania zgłębnika podczas jego ruchu w cieczy. Zasadę działania zgłębników zobrazowano na rysunku 5b. Podczas opuszczania zgłębnika ze stałą prędkością powstaje ciśnienie dynamiczne, które powoduje otwarcie zaworu *3*. Poprzez otwór *4* następuje napełnianie komory zgłębnika. Szybkość napełniania jest uzależniona od lepkości badanej cieczy oraz powierzchni otworów odpowietrzających *2*. Z tego względu bardzo istotne jest dobranie odpowiedniej prędkości opuszczania zgłębnika. W chwili zmiany kierunku (wyciągania zgłębnika) siła dynamiczna będzie działała na zawór *1* powodując zamknięcie komory zgłębnika i zachowania w nim przekrojowej zawartości cieczy pobranej.

Rysunek 5. Zgłębnik do poboru próbek przekrojowych:
a) do cieczy o małej lepkości, b) do cieczy o dużej lepkości.



Źródło: [Polska Norma PN-A-79521], [Polska Norma PN-EN ISO 3170].

Próbkę przekrojową należy pobrać w taki sposób, aby przez cały czas przechodzenia próbopobieralnika przez badaną ciecz napełnił się on równomiernie. W przypadku gdyby ilość pobranej próbki byłaby niewystarczająca do utworzenia odpowiedniej wielkości próbki ogólnej (musi wystarczyć na minimum trzy próbki laboratoryjne – próbka świadek, próbka dla strony, próbka na badania laboratoryjne) w celu uśrednienia wartości powtarza się pobieranie kilkakrotnie.

Całkowicie oddzielną problematykę stanowi zachowanie odpowiednich zasad BHP i ppoż. Wielokrotnie sprawdzaniu podlegają substancje lotne, łatwopalne, wybuchowe, żrące lub trujące. Problematyka ta jednak nie jest częścią tej pracy. Wymaga to zachowania odpowiednich środków bezpieczeństwa.

5. PODSUMOWANIE

Z przedstawionej w pracy problematyki wynika, że zagadnienie poboru próbek wymaga specjalistycznej wiedzy z zakresu mechaniki płynów oraz znajomości własności reologicznych płynów. Niejednokrotnie potrzebna jest duża

znajomość własności materiałowych oraz wiedza z zakresu metrologii. Posiadanie tak rozległej wiedzy przez funkcjonariuszy kontroli celno-skarbowej w praktyce jest nieosiągalne. Ponadto ilość kontroli wykonywanych przez Krajową Administrację Skarbową oraz różnorodność towaru zmusza urzędy do podjęcia współpracy z instytucjami naukowymi. Przykładem jest podjęta współpraca między Izbą Administracji Skarbowej w Opolu a Politechniką Opolską.

Literatura:

[1] Ustawa z dnia 16 listopada 2016r. *o Krajowej Administracji Skarbowej* tj. Dz.U. z 2018r. poz. 508 ze zmianami,
[2] Rozporządzenie Parlamentu Europejskiego i Rady (EU) NR 952/2013 z 9 października 2013r. *ustanawiające unijny kodeks celny* Dz.U.UE.L. z 2013r. nr 269.1 ze zmianami,
[3] Ustawa z dnia 6 grudnia 2008r. *o podatku akcyzowym* tj. Dz.U. z 2017r. poz. 43 ze zmianami
[4] Ustawa 9 marca 2017r, *o systemie monitorowania drogowego przewozów towarów* DzU z 2017r. poz. 708 ze zmianami,
[5] Zatrucia metanolem w Czechach, Polsce i na Słowacji w drugiej połowie 2012r. W Czechach z powodu zatrucia metanolem zmarło 38 osób (nie licząc osób które straciły wzrok), należy nadmienić, że byli to zwykli konsumenci (przeważnie nienadużywający alkoholu), którzy okazjonalnie kupili w sklepach alkohol!
[6] Krajowa Administracja Skarbowa posiada 5 własny certyfikowanych laboratoriów i jest w trakcie realizacji wyposażenia każdej Izby Administracji Skarbowej w laboratoria mobilne.
[7] Polska Norma PN-EN ISO 3170 *Ciekłe przetwory naftowe*. *Ręczne pobierani próbek*
[8] Polska Norma PN-A-79521 *Produkty i półprodukty spirytusowe*. *Pobieranie próbek*,
[9] Polska Norma PN-83 N-03010 *Statystyczna Kontrola Jakości – Losowy wybór jednostek produktu do próbki*,

mgr inż. Piotr Kraczmar
Krajowa Administracja Skarbowa
Izba Administracji Skarbowej w Opolu
Opolski Urząd Celno-Skarbowy w Opolu
Kierownik Oddziału Celnego w Nysie
ul. Otmuchowska 50, 48-300 Nysa
e-mail piotr.kraczmar@mf.gov.pl

dr hab. inż. prof. PO Mariusz R. Rząsa
Politechnika Opolska
Wydział Mechaniczny (Katedra Techniki Cieplnej i Aparatury Przemysłowej)
45-271 Opole, ul. Mikołajczyka 5
e-mail m.rzasa@po.opole.pl

Mariusz R. RZĄSA

WPŁYW LICZBY PRÓBEK NA ODCHYLENIE UŚREDNIONEGO PARAMETRU CIECZY POBRANEJ Z CYSTERNY

Streszczenie: Praca zawiera analizę wpływu liczby pobranych próbek na wynik uśrednienia wartości jednego z parametrów charakteryzującego badaną ciecz. Zagadnienie to jest istotne w procesie kontroli celno-skarbowej podczas transportu materiałów ciekłych. Na wynik kontroli ma duży wpływ miejsce i liczba pobranych próbek w celu uśrednienia wartości mierzonego parametru. W artykule przeprowadzono teoretyczną analizę wpływu liczby próbek na wartość uśrednienia. Przeprowadzono symulację obliczenia wartości średniej dla przykładowych nieliniowych rozkładów parametru X o znanej wartości średniej.

Słowa kluczowe: wartość średnia, próbkowanie, metrologia.

IMPACT OF NUMBER OF SAMPLES ON THE ERROR OF AVERAGE VALUE OF LIQUID PARAMETER WHICH HAS BEEN TAKEN FROM THE TANK

Summary: The work contains an analysis of the influence of the number of samples taken on the result of averaging the value of one of the parameters characterizing the test liquid. This issue is important in the process of customs and tax control during the transport of liquid materials. The control result is influenced by the place and the number of samples taken to average the value of the parameter being measured. In the paper presents a theoretical analysis of the influence of the number of samples on the averaging value. The calculation of the mean value for exemplary nonlinear distributions of the X parameter with a known mean value was simulated.

Keywords: average value, sampling, metrology.

1. WSTĘP

Obecnie do magazynowania i przewozu materiałów płynnych stosuje się różnego rodzaju cysterny lub zbiorniki [Różycki M 2007: 19-26]. Wiele cieczy jakie są magazynowane stanowią emulsje [Polska Norma PN-EN ISO 3170]. Emulsja jest to mieszanina kilku cieczy, które nie rozpuszczają się w sobie, a ich zmieszanie następuje w wyniku mechanicznego rozdrobnienia cząstek cieczy. Emulsja nie jest stabilną mieszaniną, po pewnym czasie dochodzi do rozwarstwienia cieczy [Wiśniowski R., Skrzypaszek K 2006: 523-532]. Na szybkość procesu rozwarstwiania niejednokrotnie mają wpływ takie czynniki jak temperatura lub ciśnienie. Mieszaniny mogą być pochodzenia naturalnego bądź syntetycznego. W wyniku rozwarstwiania się cieczy następuje zmiana własności mieszaniny [Brandt S. 1999] wraz z wysokością cieczy znajdującej się w cyster-

nie (rys.1). Przykładem może być mleko. Mleko magazynowane w zbiorniku ulega rozwarstwieniu. Frakcje tłuszczowe pod wpływem sił wyporu przemieszczają się w górny obszar zbiornika, natomiast wodne składniki mleka osiadają na dnie. W wyniku tego uzyskuje się niejednorodną zawartość tłuszczu wraz ze zmianą wysokości.

Zjawisko rozwarstwiania się cieczy stanowi problem podczas przeprowadzania różnego rodzaju kontroli materiałów płynnych. Sposób poboru próbek przy kontroli własności cieczy jest określony odpowiednimi normami [Pułkowski M., Domański W. 2010: 9-13]. Normy te określają zarówno liczbę próbek jakie należy pobrać, miejsca ich poboru oraz sposób uśrednienia. Z uwagi na bardzo dużą różnorodność cieczy nie jest możliwe opracowanie norm dla wszystkich cieczy jakie są używane w przemyśle. Znaczną trudność w tym zagadnieniu stanowi fakt, że rozkład niejednorodności nie musi być rozkładem liniowym [Gupta R., Mauri R., Shinnar R. 1999: 2418-2424]. Bardzo często rozkład ten jest nieliniowy wykładniczo lub logarytmicznie.

Rys. 1. Rozwarstwienie cieczy w zbiornikach a) poziomych b) pionowych.

a) b)

Źródło: https://www.pl.endress.com/pl/aktualnosci/newsroom/Szerok-gama-produkt%C3%B3w -do- pomiar%C3%B3w

W pracy przedstawiono analizę wpływu liczby pobranych próbek na błąd uśrednienia wartości dla rozkładów nieliniowych. Wyniki analizy przeprowadzano dla symulowanych rozkładów wykładniczych i logarytmicznych. Opracowanie to może posłużyć do szacowania niepewności pomiarów podczas dokonywania kontroli cieczy magazynowanej w zbiornikach, w których wymieszanie zawartości zbiornika jest bardzo trudne lub niemożliwe (np. cysterny kolejowe) [Perez-Elvira S. I., Sapkaite I., Fdz-Polanco F. 2016: 699-704].

2. PODSTAWY TEORETYCZNE UŚREDNIANIA WARTOŚCI

W zbiornikach do przewozu i magazynowania materiałów płynnych poboru próbek najczęściej dokonuje się poprzez otwory załadunkowo wyładowcze, znajdujące się w górnej części zbiornika. Rozwiązanie to znacznie utrudnia pobranie próbek z całej objętości zbiornika. Typowy zatem jest pobór próbek jedynie z obszaru znajdującego się pionowo pod otworem załadowczo wyładowczym. Powoduje to, że zbór próbek składa się z szeregu próbek pobranych z różnych głębokości zanurzenia. W związku z tym uśrednianie następuje po linii prostej. W pracy nie analizuje się wpływu kształtu zbiornika oraz czynników zewnętrznych na niejednorodność w przestrzeni zbiornika. Analizę ograniczono jedynie do faktu, że taka niejednorodność występuje i jak wpływa na wynik uśredniania. Założono, że rozkład niejednorodności ma miejsce jedynie w pionie. Wartość średnią z funkcji ograniczonej oblicza się na podstawie zależności:

$$X_S = \frac{1}{H}\int_0^H X(h)dh \tag{1}$$

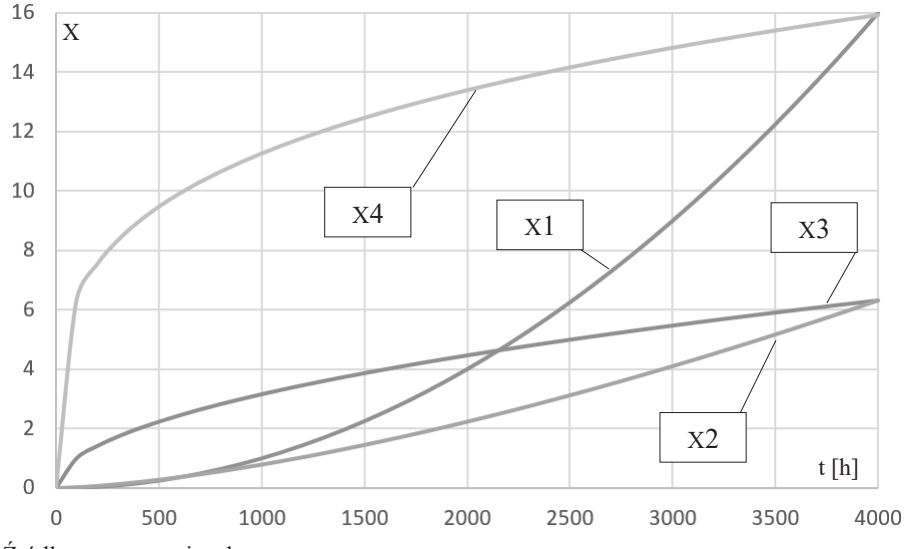
gdzie: X_S-wartość średnia z funkcji rozkładu parametru X(h), H – wysokość słupa cieczy.

W praktyce najczęściej nie dysponuje się funkcją rozkładu wybranego parametru, a jedynie punktowymi wartościami próbek pobranych z różnych wysokości słupa cieczy [Brandt S. 1999]. Stąd funkcja uśredniania przyjmuje postać dyskretną:

$$X_S = \frac{1}{H}\sum_{n=1}^{N} X(n)\cdot h_n \tag{2}$$

gdzie: *X(n)*-wartość z próbki pobranej z wysokości h_n.

Rys. 2. Charakterystyki nieliniowego rozkładu wartości X



Źródło: opracowanie własne

W badaniach założono, że próbki są pobierane ze stałym skokiem wysokości h_n. Założono cztery nieliniowe rozkłady wartości parametru *X(h)* (rys.2). Dwie funkcje rozkładu mają charakter potęgowy z wykładnikiem potęgi odpowiednio $X_1=h^2/1000000$ i $X_2=h^{1.5}/40000$ oraz dwa rozkłady pierwiastkowe $X_3=h^{0.5}/10$ i $X_4=2h^{0.25}$. Współczynniki funkcji dobrano w taki sposób aby uzyskać dwie pary możliwie symetrycznych nieliniowych rozkładów funkcji X(h).

Rzeczywistą wartość średnią dla poszczególnych rozkładów obliczono z zależności (1) w przedziale od 0-4000. Wartości te wynoszą odpowiednio:

X1= 21333.33 X2= 10119,29 X3= 16865,5 X4= 50897,33

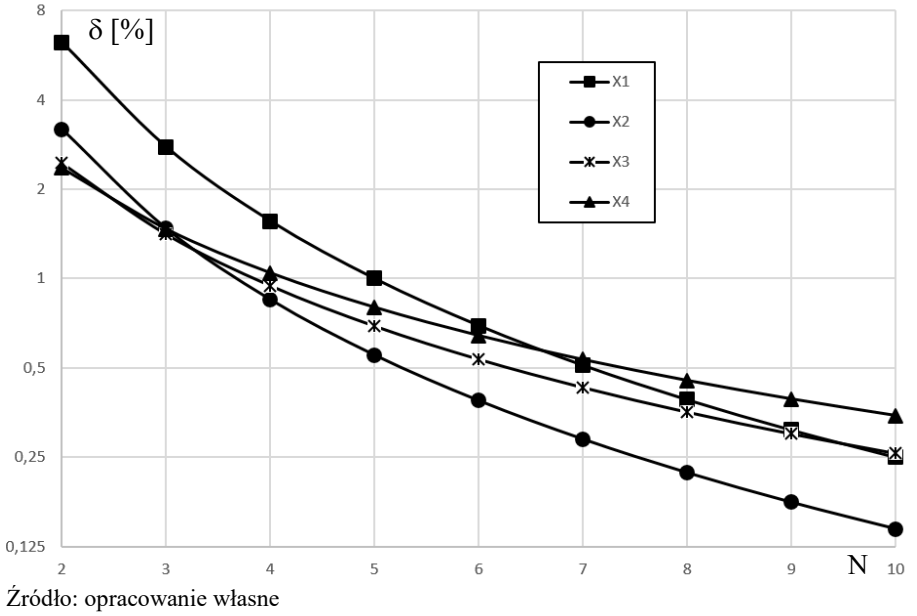
3. WYNIKI BADAŃ

Przeprowadzono badania wpływu liczby próbek na wartość średnią. Dla rozkładów wartości X przedstawionych na rysunku 2 wygenerowano różne wartości próbek. Próbki reprezentowały punkty charakterystyki, których rozkład był regularny względem osi h. Liczbę punktów przyjęto od 2 do 10. Procentową odchyłkę od wartości średniej obliczono na podstawie wzoru:

$$\delta = \frac{(X1 - X_S)}{X1} 100\% \tag{3}$$

gdzie: X_S-wartość średnia obliczona na podstawie wzoru (2), X1- rzeczywista wartość średnia obliczona na podstawie wzoru (1).

Rysunek 3. Odchyłki wartości średniej w zależności od liczby próbek



Źródło: opracowanie własne

Jak wynika z przedstawionych charakterystyk większą podatność na niejednorodny rozkład wykazują ciecze, których rozkład ma charakter wykładniczy. Im większy wykładnik potęgi tym większe wartości odchylenia. Nasuwa to wniosek, iż w przypadku badania tego rodzaju cieczy należy zwiększyć liczbę pobieranych próbek. Z kolei dla rozkładów o charakterze pierwiastkowym odchylenia dla małej liczby próbek mają zbliżone do siebie wartości. Jednakże większy wykładnik pierwiastka powoduje, że wraz ze wzrostem liczby próbek wartość odchylenia znacznie szybciej zmierza do zera.

4. PODSUMOWANIE

W pracy przeprowadzono teoretyczną analizę wpływu liczby próbek podczas uśredniania wartości mierzonego parametru cieczy pobranej z cysterny. Na podstawie przeprowadzonej analizy stwierdza się, że dla liczby próbek powyżej trzech odchylenie jest mniejsze od 5% niezależnie od charakterystyki rozkładu. Graniczna wartość 5%, ma znaczenie, gdyż większość producentów typowych cieczy przyjmuje wartość 5% jako tolerancję technologiczną. Oczywiście podczas kontroli należy uwzględnić prawdopodobieństwo zsumowania odchyłki mierzonej i odchyłki technologicznej danego produktu. Rozsądne jest zatem zwiększenie marginesu tolerancji przy kwalifikowaniu nieprawidłowości.

Literatura:

[1] Różycki M.: *Praktyka przewozu w cysternach*, Ogólnopolskie Seminarium Szkoleniowe „Czy przewóz drogowy towarów niebezpiecznych w cysternach może być bezpieczny?", Tarnów, 25-26 maja 2007 r., s. 19-26.

[2] Polska Norma PN-EN ISO 3170 Ciekłe przetwory naftowe. Ręczne pobierani próbek

[3] Pułkowski M., Domański W.: *Bezpieczeństwo transportu drogowego paliw płynnych w cysternach*, Bezpieczeństwo pracy 09/2010, s. 9-13.

[4] Perez-Elvira S. I., Sapkaite I., Fdz-Polanco F.: *Separate digestion of liquid and solid fractions of thermally pretreated secondary sludge. Assessment and global evaluation*, Brazilian Journal of Chemical Engineering, Vol.33 no. 04, October-December 2016, s. 699-704.

[5] Gupta R., Mauri R., Shinnar R.: *Phase Separation of Liquid Mixtures in the Presence of Surfactants*, Industrial & Engineering of Chemictry Research, 38/1999, s. 2418-2424.

[6] Wiśniowski R., Skrzypaszek K.: *Analiza modeli reologicznych stosowanych w technologiach inżynierskich*, Wiertnictwo Nafta Gaz, Tom 23/1 2006, s. 523-532.

[7] Brandt S.: *Metody statystyczne i obliczeniowe analizy danych*, Warszawa PWN 1999

dr hab. inż. prof. PO Mariusz R. Rząsa
Politechnika Opolska
Wydział Mechaniczny (Katedra Techniki Cieplnej i Aparatury Przemysłowej)
45-271 Opole, ul. Mikołajczyka 5
e-mail m.rzasa@po.opole.pl

Przemysław KRAWCZYK
Przemysław MISIURSKI

ANALIZA DANYCH PODATKOWYCH – ZARYS PROBLEMU

Streszczenie: W artykule przedstawiono zarys problemu analizy danych podatkowych wynikający z przetwarzania przez organy administracji skarbowej coraz to większej liczby danych pochodzących m.in. z Jednolitych Plików Kontrolnych (JPK). Zaprezentowano teoretyczne aspekty eksploracji danych oraz przedstawiono dostępne oprogramowanie pozwalające na dokonywanie złożonych analiz. W dalszej kolejności przedstawiono narzędzia stosowane w pracy analityka administracji skarbowej.

Słowa kluczowe: eksploracja danych, analiza danych, JPK

ANALYSIS OF TAX DATA - OUTLINE OF THE PROBLEM

Summary: The article presents an outline of the problem of tax data analysis resulting from the processing by tax administration authorities of an ever-increasing number of data originating, i.a. from Standard Audit File for Tax (JPK). The theoretical aspects of data mining and the available software allowing for complex analyses are presented. Subsequently, the tools used in the work of the tax administration analyst are presented.

Keywords: data mining, data analysis, Standard Audit File for Tax

1. WSTĘP

Celem niniejszego artykułu jest przedstawienie podstawowych informacji nt. analizy danych podatkowych. Administracja skarbowa stara się wdrożyć zcentralizowany model zarządzania danymi. Model ten opiera się na założeniu, że tylko w ten sposób można zapewnić odpowiednią wydajność poprzez tworzenie dużych raportów (raporty oparte o dane z JPK), które po dodatkowej „obróbce" przekazywane są do użytkowników końcowych tj. pracowników działów czynności sprawdzających lub analiz odpowiednio urzędów skarbowych i urzędów kontroli celno-skarbowej.

Systemy informatyczne, w tym systemy analityczne, powinny mocniej wspierać administrację skarbową w realizacji celów. Celami tymi jest zapewnienie bezpieczeństwa finansowego Polski, w tym efektywnego poboru podatków i ceł. Realizacji tych celów służy proces centralizacji baz danych, centralizacji procesu analiz, monitorowania poziomu ryzyka podatkowego, a także centralizacja typowania podmiotów do kontroli. Obecnie ogromnym wyzwaniem jest dynamiczny wzrost wolumenu gromadzonych i przetwarzanych przez administrację skarbową danych dotyczących podatników, ich zachowań oraz szeroko

pojętego otoczenia biznesowego. Stąd od jakości zastosowanych narzędzi informatycznych w dużej mierze zależy efektywność działań.

Proces centralizacji baz danych opiera się na stworzeniu jednego źródła danych w postaci tzw. „Fundamentu Danych", na którym gromadzone byłyby dane wykorzystywane w analizach. Proces ten obejmuje konieczność integracji z kilkudziesięcioma źródłami danych (baz danych). Rozwiązanie to obejmuje dane zarówno o podatnikach, deklaracje podatkowe, ewidencje JPK-VAT składane co miesiąc i zawierające zestawianie wszystkich faktur oraz inne informacje gromadzone lub wytwarzane przez administrację skarbową.

Fundament Danych pozwoli nie tylko na zgromadzenie danych w jednym miejscu, ale także umożliwi optymalizację wykonywania obliczeń. W powyższym celu wykorzystywane są rozwiązania analityczne, oparte na relacyjnych bazach danych, jak i na technologii baz grafowych. Możliwe jest stosowanie szerokiego spektrum technik analitycznych, w szczególności technik eksploracji danych oraz technik SNA analizy sieciowej lub społecznej analizy sieciowej badania sieci społecznej, wykorzystujące teorię sieci i koncentrujące się na analizie stosunków pomiędzy elementami sieci (jednostkami, organizacjami itp.). W analizie sieciowej nacisk kładzie się na relacje i ich wzorce, z których wynikają szanse i ograniczenia dla węzłów sieci.

2. JEDNOLITY PLIK KONTROLNY - ZAKRES DANYCH WEJŚCIOWYCH

Zgodnie z wytycznymi międzynarodowych organizacji gospodarczych takich jak OECD[11], IMF[12] w ostatnich latach rozpoczął się proces upraszczania i ujednolicania rozliczeń podatkowych. Działania te mają na celu doprowadzić do poprawy przejrzystości transakcji finansowych. W związku z tymi działaniami, jednym z rozwiązań zarekomendowanych przez OECD, jest jednolity, międzynarodowy standard rozliczeń podatkowych, tzw. SAF-T (Standard Audit File for Tax). W wielu krajach europejskich funkcjonuje już SAF-T. Również Polska w 2016 roku wprowadziła swój model raportowania danych tzw. Jednolity Plik Kontrolny. Dzięki niemu organy administracji skarbowej mogą w łatwy sposób analizować sytuację podatkową firm i upłynnić ściągalność podatku VAT [ttps://businessinsider.com.pl/firmy/przepisy/ile-firm-zlozylo-jpk-vat-za-styczen-2018/01htqrn]. Jednolity Plik Kontrolny jest zbiorem (bazą) danych, tworzonym z systemów informatycznych przedsiębiorcy, zawierającym informacje o operacjach gospodarczych za dany okres, mającym układ i format umożliwiający jego łatwe przetwarzanie. Inaczej mówiąc, jest to standard, według którego przekazuje się dane do organów podatkowych [http://chem-eng.utoronto.ca/~datamining/dmc/data_mining.htm].

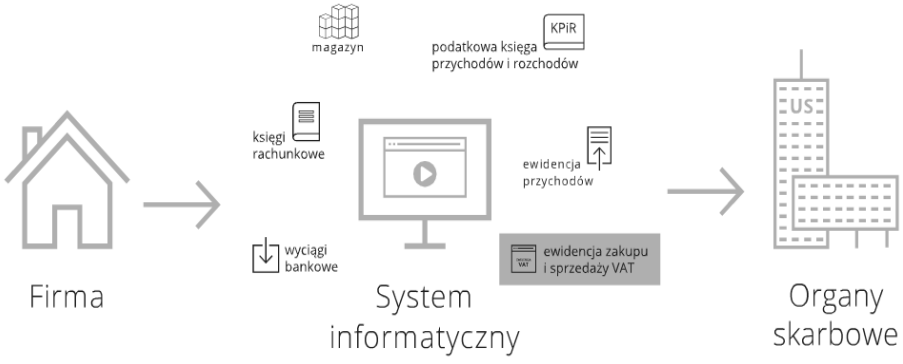
[11] *Organisation for Economic Co-operation and Development - OECD - Organizacja Współpracy Gospodarczej i Rozwoju*

[12] International Monetary Fund - IMF Międzynarodowy Fundusz Walutowy

Jednolity Plik Kontrolny został wprowadzony ustawą z 10 września 2015 r. o zmianie ustawy – Ordynacja Podatkowa (Dz.U. z 2015 r. poz. 1649) w dodanym art. 193a, który w *§ 1* mówi: w przypadku prowadzenia ksiąg podatkowych przy użyciu programów komputerowych, organ podatkowy może żądać przekazania całości lub części tych ksiąg oraz dowodów księgowych za pomocą środków komunikacji elektronicznej lub na informatycznych nośnikach danych, w postaci elektronicznej odpowiadającej strukturze logicznej, o której mowa w § 2, wskazując rodzaj ksiąg podatkowych oraz okres, którego dotyczą [Ustawa z dnia 10 września 2015r.].

Elektroniczne raportowania miesięczne na cele podatku VAT (bez wezwania organu podatkowego) są obowiązkowe dla dużych jednostek od lipca 2016, małe i średnie podmioty obowiązek takiego raportowania mają od stycznia 2017 [Voss G. 2017]. Od 1 stycznia 2018 roku wszyscy przedsiębiorcy zarejestrowani jako czynni podatnicy podatku VAT (w tym mikroprzedsiębiorcy), mają obowiązek przesłania do organów skarbowych tzw. JPK_VAT w formie elektronicznej (poglądowy schemat przekazania niezbędnych danych prezentuje rysunek 1). Według Ministerstwa Finansów za miesiąc styczeń pliki JPK_VAT przesłało 1,5 mln przedsiębiorców [ttps://businessinsider.com.pl/firmy/przepisy/ile-firm-zlozylo-jpk-vat-za-styczen-2018/01htqrn].

Rysunek 1. Schemat przekazania danych JPK



Źródło: http://www.edat.pl/enova365/jednolity-plik-kontrolny

Formalności związane z Jednolitym Plikiem Kontrolnym wymusiły na przedsiębiorcach stosowanie odpowiednich systemów informatycznych, które ułatwiają przesłanie danych do organów administracji skarbowej. Tak duża ilość danych wysyłana przez podmioty gospodarcze wymaga również od instytucji skarbowych stosowania odpowiednich narzędzi informatycznych przeznaczonych do ich analizy i ich eksploracji w celu pozyskania odpowiedniej wiedzy analitycznej.

3. EKSPLORACJA DANYCH

Obecnie jedną z najdynamiczniej rozwijanych dziedzin informatyki jest eksploracja danych (ang. data mining). Duże zainteresowanie eksploracją danych wynika w głównej mierze z problemu efektywnego i racjonalnego wykorzystania danych nagromadzonych w bazach danych przez ogromną liczbę przedsiębiorstw, jak również instytucji administracji publicznej czy ośrodków naukowych [Morzy T. 1999].

Według definicji eksploracja danych to proces odkrywania wzorców, reguł, zależności w dużych zbiorach danych (hurtownie danych). Zasadniczym celem eksploracji danych jest wydobycie nowej – nieznanej informacji z baz danych lub ze zbiorów wiedzy [Olszak C.M., Bartuś K. 2009], [Racka K. 2015]. Eksploracja danych integruje wiele dyscyplin wśród których można wymienić: statystykę, sztuczną inteligencję, systemy bazodanowe, optymalizację [Morzy T. 1999].

Rysunek 2. Eksploracja danych

Źródło: opracowanie własne n/p http://chem-eng.utoronto.ca/~datamining/dmc/ data_mining.htm.

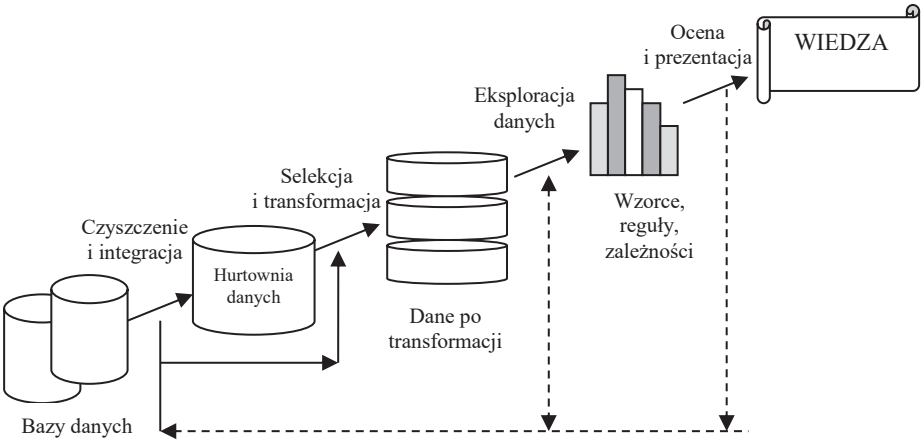
Eksploracja danych stanowi jeden z etapów procesu tworzenia wiedzy z baz danych. Proces ten składa się z następujących kroków [Morzy T. 1999], [Racka K. 2015]

- czyszczenie danych - usuwanie błędnych danych wynikających z pomyłek operatora lub danych powielonych;
- integracja danych - łączenie danych pochodzących z różnych źródeł o niejednolitej strukturze i różnorakich modelach danych;
- wybieranie danych - wybór danych niezbędnych do przeprowadzenia analizy;

- transformacja danych - przetworzenie lub łączenie danych w formy odpowiednie do eksploracji;
- eksploracja danych - wydobycie z danych odpowiednich wzorców i zależności
- ocena i prezentacja odkrytych wzorców, reguł, zależności - identyfikacja odkrytych wzorców i prezentacja odkrytej wiedzy docelowym użytkownikom.

Zależności pomiędzy eksploracją danych a pozostałymi etapami procesu pozyskiwania wiedzy prezentuje rysunek 3.

Rysunek 3. Eksploracja danych jako jeden z kroków w procesie odkrywania wiedzy



Źródło: Opracowanie własne na podstawie [Ejsmont K., Krystosiak K., Lipiak J. 2015], [Han J., Kamber M. 2001], [Racka K. 2015].

Eksploracja danych jest najistotniejszym elementem procesu pozyskiwania wiedzy. Pozostałe etapy tego procesu są albo czynnościami rutynowymi w porównaniu do eksploracji danych, albo są nierozłącznie związane z samą eksploracją [Ejsmont K., Krystosiak K., Lipiak J. 2015]. W literaturze przedmiotu wymienia się sześć metod eksploracji danych [Morzy T. 1999], [Racka K. 2015]:

1. **Wyszukiwanie asocjacji -** jest to najszersza klasa metod obejmująca odkrywanie różnego rodzaju nieznanych zależności w bazie danych. Metody w tej klasie obejmują głównie odkrywanie asocjacji pomiędzy obiektami.
2. **Klastrowanie - metoda grupowania** - celem tych metod jest znajdowanie w bazie danych skończonych podzbiorów (klas, grup) , które posiadają podobne cechy. W metodach tych liczba potencjalnych klastrów nie jest znana, stąd, proces grupowania przebiega, najczęściej, w dwóch cyklach: cykl zewnętrzny przebiega po liczbie możliwych klastrów, cykl wewnętrzny próbuje znaleźć optymalny podział obiektów pomiędzy klastry.

3. **Odkrywanie wzorców sekwencji** - celem tych metod jest odkrywanie czasowych wzorców zachowań, na podstawie analizy danych zmieniających się w czasie.
4. **Odkrywanie klasyfikacji** - celem tych metod jest znajdowanie zależności pomiędzy klasyfikacją obiektów a ich charakterystyką.
5. **Odkrywanie podobieństw w przebiegach czasowych -** celem tych metod jest znajdowanie podobieństw w przebiegach czasowych opisujących określone procesy.
6. **Wykrywanie zmian i odchyleń -** metody te pozwalają na znajdowanie różnic pomiędzy aktualnymi a oczekiwanymi wartościami danych.

W praktyce stosowanie różnych metod eksploracji danych dla tego samego zagadnienia może okazać się korzystniejsze, gdyż zastosowanie jednej metody może nie być wystarczające do całościowego rozwiązania rozpatrywanego problemu [Racka K. 2015].

Do skutecznego przeprowadzenia procesu analizy danych, prócz dobrej znajomości badanej dziedziny, zbioru danych, czy wybrania właściwej techniki eksploracji, niezbędnym jest wykorzystanie odpowiedniego oprogramowania.

Na rynku oprócz programów komercyjnych takich firm jak: HP, IBM, MICROSFT, ORACLE, SAS Institute, StatSoft dostępna jest duża liczba programów niekomercyjnych oferujących rozwiązania z zakresu eksploracji danych [Racka K. 2015]. Listę przykładowych programów do eksploracji danych przedstawia tabela 1.

Tabela 1. Lista przykładowych darmowych programów do eksploracji danych

Nazwa programu	Typ licencji
CMSR DATA Miner	Licencja akademicka na trzy lata, wersja darmowa na 6 miesięcy
Databionic ESOM Tools	GNU GPL
ELKI	AGPL
KNIME	GNU GPL
Mloss	GNU GPL
Mlpy	GNU GPL
Orange	GNU GPL
Projekt R	GNU GPL
Rapid Miner	AGPL/ Proprietary (prawnie zastrzeżone)
Rattle GUI	GNU GPL
SCaViS	jądro silnika programu GPL, instalacja, dokumentacja, podzespoły darmowe ale nie do celów komercyjnych
SenticNEt API	Darmowy z umieszczeniem informacji: Copyright © 2012 Yuri Malheiros
Weka 3	GNU GPL

Źródło: [Racka K. 2015]

Duża grupa programów wymienionych w powyższej tabeli to programy na licencji GNU GPL, która daje możliwość użytkownikowi uruchamiania programu dowolną liczbę razy, a udostępniony kod źródłowy programu można modyfikować na własne potrzeby, a także rozpowszechniać. Natomiast licencja AGPL jest licencją wolnego oprogramowania uruchamianego przez sieć. Programy na licencji AGPL są rozbudowywane i zmieniane na potrzeby odbiorców przez dużą liczbę informatyków [Racka K. 2015].

Do głównych zalet niekomercyjnych programów zalicza się przede wszystkim fakt, że użytkownicy mają do nich darmowy dostęp, a praca na tych programach daje wiele możliwości obliczeniowych użytkownikom dorównując, a często przewyższając jakościowo programy komercyjne [Racka K. 2015].

4. ANALIZA DANYCH PODATKOWYCH - WYKORZYSTYWANE NARZĘDZIA

Wykorzystywane w pracy analityka administracji skarbowej narzędzia, to oprócz programów komercyjnych, także KNIME i Neo4j. KNIME Analytics Platform jest otwartym oprogramowaniem analitycznym wykorzystywanym w celu integracji rozwiązań i technologii informatycznych oraz informacyjnych. Pozwala na wykonywanie analiz i obliczeń statystycznych, jak również drążenie danych, wykrywanie wiedzy z danych, stosowanie metod sztucznej inteligencji, wdrażanie automatycznych rozwiązań analitycznych czy procesów ETL. Platforma udostępniona jest na licencji GNU General Public License, Version 3. Posiada ponad 2000 modułów, setki gotowych do uruchomienia przykładów, możliwość zwiększenia funkcjonalności poprzez instalacje dodatkowych rozszerzeń.

KNIME jest ciekawym rozwiązaniem dla badaczy danych. Posiada forum dyskusyjne, kanał na YouTube oraz pełną dokumentację dostępną z poziomu aplikacji. Pakiety instalacyjne dostępne są dla systemów: Microsoft Windows, Linux, Mac. Istnieje również wersja SDK pozwalająca tworzyć własne moduły.

KNIME jest oprogramowaniem opartym na graficznym interfejsie użytkownika. Procesy tworzy się głównie w sposób graficzny poprzez wykorzystanie gotowych modułów (nodes), które połączone ze sobą tworzą przepływy analityczne (Workflow). Takie podejście pozwala na łatwe zrozumienie zadań wykonywanych w przepływie, powtarzalność analiz, zapewnienie jakości danych oraz pewność wyników.

Integracja rozwiązań zapewnia ogromną funkcjonalność narzędzia. W Knime korzystając z rozszerzeń można m.in. wykonywać skrypty pisane w językach: java, python, R czy perl. Dodatki umożliwiają dostęp do algorytmów z aplikacji WEKA, wszelkich relacyjnych baz danych, takich jak: Microsoft SQL Server, IBM DB2, Oracle DB, PostgreSQL, MySQL, Firebird, SQLite oraz innych posiadających sterownik JDBC. Można również uzyskać dostęp do systemów Big Data jak Apache Hadoop, Hive, grafowych baz danych (Neo4j) czy baz NoSQL (MongoDB). Rozszerzenia powodują, że jest to kompletne środowisko dla analityka.

KNIME pozwala na wykorzystanie metodologii takich jak: analizy statystyczne, big data, text mining, patterns matching, web mining, ETL (Extract, Transform and Load), EDA - exploratory data analysis), Data mining, SNA – (Social network analysis), GIS – wizualizację danych na mapach, wizualizację danych (wykresy) oraz tworzenie raportów opartych na przygotowanych szablonach.

Neo4j to grafowa baza danych umożliwiająca przechowywanie grafów, pozwalająca na bardzo szybkie i proste przeszukiwanie zależności oraz powiązań. Platforma posiada wersję „Neo4j Community Edition" opartą na licencji GNU General Public License, Version 3.

Zaletą jest brak sztywnych tabel czy schematów znanych z relacyjnych baz danych. Baza posiada 4 podstawowe typy obiektów: NODE, RELATIONSHIPS, PROPERTIES, LABELS. Nodes reprezentują dowolne obiekty umieszczone w bazie, a RELATIONSHIPS określają relacje/zależności pomiędzy obiektami. Obiekty oraz relacje mogą posiadać dodatkowe atrybuty (PROPERTIES). Szczególnym typem jest LABELS – semantyczny typ danych dla obiektów i relacji.

Praca na bazie wykorzystuje język CQL (Cypher Query Language) podobny do SQL, prosty w nauce i wykorzystaniu języka zapytań i manipulacji na danych. Nawiązuje do ascii-art. Interfejs dostępowy do bazy jest możliwy poprzez CLI (linię komend), przeglądarkę – własny portal www lub interfejs API.

Baza pozwala na dużo szybsze wyszukiwanie skomplikowanych powiązań bazując na grafach, zastępując skomplikowane, wielopoziomowe złączenia JOIN znane z SQL i relacyjnych baz danych.

Język Cypher pozwala na dopasowywanie obiektów i relacji. Pozwala tworzyć, uaktualniać, usuwać obiekty, relacje, nazwy semantyczne i właściwości. Neo4j posiada również możliwość wykorzystania wyzwalaczy (constraints) i indeksów w celu zwiększenia wydajności. Na danych można wykonywać operacje arytmetyczne czy agregację danych.

Bazę można zasilać wykorzystując język Cypher, importować dane z plików CSV oraz baz danych.

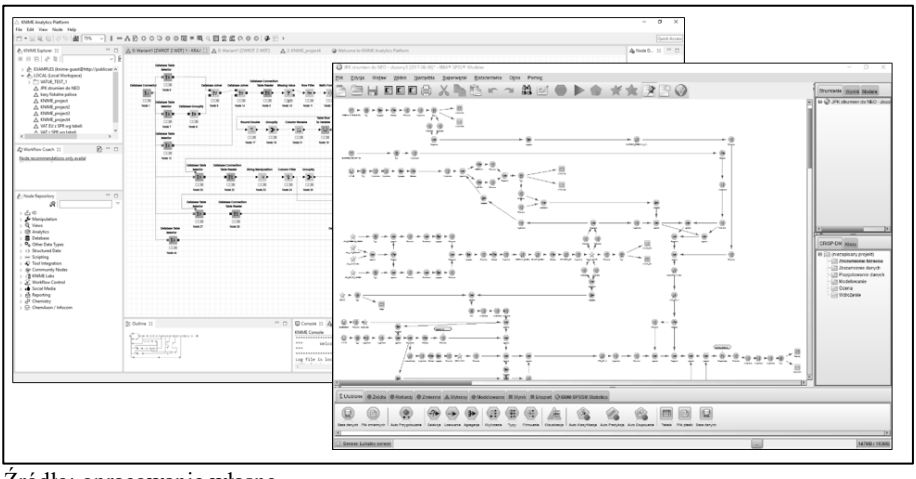
Baza wspiera również możliwość instalacji rozszerzeń zwiększających funkcjonalność. Daje to np. bezpośredni dostęp do danych z baz relacyjnych, dodatkowych algorytmów analiz sieciowych, interfejsów dla języków programowania, takich jak java, python, dotnet, ruby czy php. Możliwa jest wizualizacja danych oraz analiza w aplikacjach dedykowanych do SNA jak Gephi.

5. PROCES ANALIZY DANYCH PODATKOWYCH

Celem optymalnego wykorzystania stosowanych technik analitycznych jest dwuetapowe, hybrydowe podejście, łączące najlepsze praktyki w zakresie identyfikacji ryzyka na poziomie obiektów oraz przepływów. Wyraźne rozdzielenie warstwy obiektów oraz przepływów gwarantuje skalowalność oraz pełną konfigurowalność na podstawie przyjętych warunków brzegowych.

Identyfikacja podmiotów podwyższonego ryzyka oraz łańcuchów/sieci powiązań transakcyjnych z wykorzystaniem wyżej opisanych rozwiązań jest procesem złożonym. W pierwszym kroku prowadzona jest integracja oraz podstawowe czyszczenie danych, pozwalające na wygenerowanie zbioru analitycznego. Kolejny etap polega na nałożeniu na warstwę obiektów (także warstwę powiązań) wyników reguł biznesowych – indukowanych i ewaluowanych m.in. z wykorzystaniem algorytmów drzew decyzyjnych, pozwalających na oznaczenie podmiotów (stanowiących wierzchołki sieci transakcyjnej), spełniających cechy wskazujące na ryzyko udziału w procederze wyłudzenia skarbowego wraz ze wskazaniem prawdopodobnej roli obiektu.

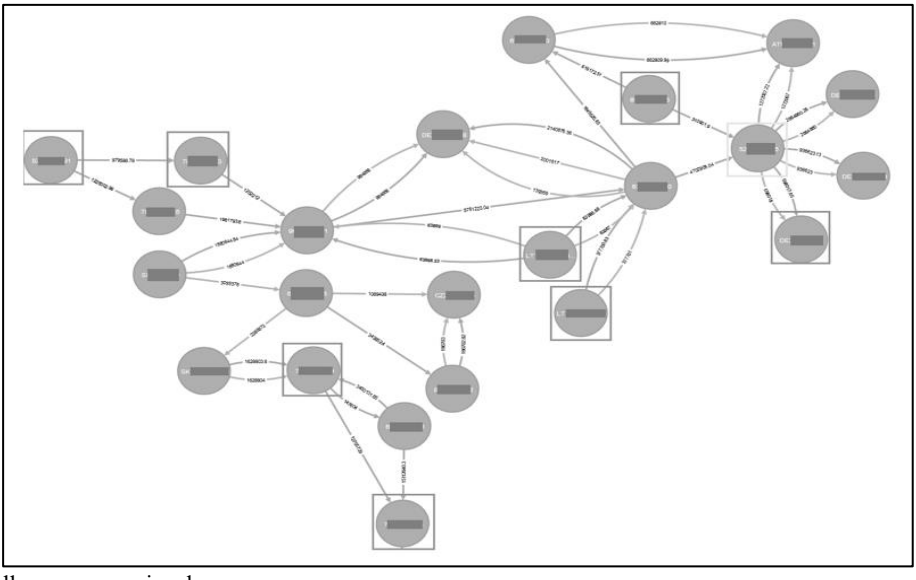
Rysunek 3. Przykład zastosowania narzędzi do analizy danych



Źródło: opracowanie własne.

W drugim etapie następuje integracja ww. zbiorów w bazie grafowej Neo4j, a także wygenerowanie sieci, zawierających obiekty, spełniające wyspecyfikowane we wcześniejszych krokach kryteria reguł biznesowych. Dla tak przedstawionych relacji generowane jest w narzędziu analitycznym otoczenie dalsze, pozwalające zidentyfikować potencjalne źródła towaru lub beneficjentów oszustwa.

Rysunek 4. Przykład zastosowania bazy grafowej Neo4j



Źródło: opracowanie własne

Docelowo w warstwie analitycznej rozwiązanie takie gwarantuje możliwość wykorzystania nowoczesnych technik statystycznej analizy danych wykraczających poza elementarne operacje matematyczne oraz standaryzację formy uzyskiwanych wyników wpływającą bezpośrednio na efektywność oceny operacyjnej podmiotu kwalifikowanego/podatnika lub zorganizowanej grupy podmiotów działających w celu wykorzystania sektora finansowego do wyłudzeń skarbowych

6. PODSUMOWANIE

Rozważania zaprezentowane w niniejszym artykule potwierdzają, że metody eksploracji danych mają zastosowanie w wielu obszarach nauki i życia gospodarczego. Są również wykorzystywane przez jednostki administracji skarbowej w celu efektywniejszej analizy danych skarbowych wysyłanych do urzędów przez podmioty gospodarcze. Przedstawiony w artykule opis stanowi jedynie zarys zagadnienia analizy danych podatkowych. Ciągle wyzwaniem jest zapewnienie dobrej jakości danych, w tym kwestia czyszczenia danych. Praca z danymi podatkowymi stanowi ogromne wyzwanie. Aby sprostać temu wyzwaniu pożądane jest zapewnienie odpowiedniej współpracy z ośrodkami akademickimi.

Literatura:

[1] Ejsmont K., Krystosiak K., Lipiak J.: *Zastosowanie wybranej techniki eksploracji danych w przemyśle poligraficznym*, Opole, Innowacje w Zarządzaniu i Inżynierii Produkcji. T.2*.,* 2015.

[2] Han J., Kamber M.: *Data mining: Concepts and Techniques*, Morgan Kaufmann Publishers, Academic Press, 2001.

[3] Morzy T.: *Eksploracja danych: problemy i rozwiązania,* Zakopane, V Konferencja PLOUG, 1999.

[4] Olszak C.M., Bartuś K.: *Analiza i ocena wybranych modeli eksploracji danych*, Opole, Komputerowo Zintegrowane Zarządzanie. Tom II. 2009.

[5] Racka K.: *Metody eksploracji danych i ich zastosowanie*, Zeszyty Naukowe PWSZ w Płocku, Nauki Ekonomiczne, t. XXI, 2015.

[6] Świder K., Jędrzejec B.: *Zaawansowane metody analizy danych i niekomercyjne pakiety analityczne w systemach wspomagania decyzji na potrzeby administracji publicznej źródła internetowe*, Warszawa, Technologie informatyczne w administracji publicznej, KAE SGH, 2014.

[7] Ustawa z dnia 10 września 2015 r. *o zmianie ustawy – Ordynacja Podatkowa* (Dz.U. z 2015 r. poz. 1649 z poźn. zm.).

[8] Voss G.: *Rachunkowość w procesie cyfryzacji - obszary ryzyka*, Warszawa, Studia i prace Kolegium Zarządzania Finansów Zeszyt Naukowy 157, 2017.

Źródła internetowe

[9] Business Insider Polska ttps://businessinsider.com.pl/firmy/przepisy/ile-firm-zlozylo-jpk-vat-za-styczen-2018/01htqrn [dostęp 18.06.2017].

[10] Data mining http://chem-eng.utoronto.ca/~datamining/dmc/data_mining.htm [dostęp 27.06.2017]

[11] Edat.pl http://www.edat.pl/enova365/jednolity-plik-kontrolny [dostęp 26.06.2017]

[12] Kariera w finasach, *Big data w służbie fiskusa: czas na globalny urząd skarbowy?* https://www.karierawfinansach.pl/artykul/wiadomosci/big-data-w-sluzbie-fiskusa-czas-na-globalny-urzad-skarbowy [dostęp 16.06.2017].

[13] Serwis informacyjno-usługowy dla przedsiębiorców Biznes.gov.pl, https://www.biznes.gov.pl/pl/firma/podatki-i-ksiegowosc/chce-prowadzic-ksiegowosc/jednolity-plik-kontrolny-jpk [dostęp 16.06.2017].

Przemysław Krawczyk
Dyrektor Departamentu Nadzoru nad Kontrolami
Krajowa Administracja Skarbowa

dr inż. Przemysław Misiurski
Politechnika Opolska
Wydział Ekonomii i Zarządzania
ul. Luboszycka 7, 45-036 Opole
e-mail: p.misiurski@po.opole.pl

Wojciech ZIMOCH

NARZĘDZIA INFORMATYKI ŚLEDCZEJ W SŁUŻBIE ZWALCZANIA PRZESTĘPCZOŚCI EKONOMICZNEJ

Streszczenie: Wyzwaniem dla współczesnych inżynierów staje się dostarczanie obecnemu społeczeństwu narzędzi pozwalających na coraz sprawniejszy przepływ informacji w formie cyfrowej. Z jednej strony narzędzia te pozwalają na błyskawiczną wymianę komunikatów, z drugiej pozwalają na tworzenie dokumentów, baz danych itp. Cyfryzacja wkrada się w każdy zakamarek dzisiejszego życia, również do świata przestępczego. Dlatego służby odpowiedzialne za zwalczanie przestępczości również powinny mieć możliwość wykorzystania technologii cyfrowej do podjęcia skutecznych działań w obszarach, które nadzorują. Z uwagi na olbrzymie zaawansowanie współczesnej technologii nie są one jednak w stanie same wytworzyć potrzebnych narzędzi. Otwiera się tutaj olbrzymi obszar do działania dla środowiska naukowego, a w szczególności uczelni technicznych, które przy współdziałaniu ze służbami ,dysponując odpowiednim zapleczem kadrowym i organizacyjnym, są w stanie wytworzyć narzędzia m.in. w obszarze informatyki śledczej, której zadaniem jest dostarczanie dowodów cyfrowych prowadzącym dochodzenia. Narzędzia te oczywiście powinny posiadać określone funkcjonalności i spełniać elementarne wymogi.

Słowa kluczowe: informatyka śledcza, dowód cyfrowy, przestępczość.

FORENSIC TOOLS FOR THE PROVISION OF ECONOMIC CRIME

Abstract: The challenge for modern engineers is to provide the public with tools that enable an increasingly efficient flow of information in digital form. On the one hand, these tools enable an exchange of instant message. On the other hand, it allows us to make documents, databases, etc. Digitization is present in almost every aspect of today's life, including the criminal world. Therefore, services responsible for combating crime should also be able to use digital technology to take effective action in the areas they oversee. However, due to the enormous advancement of modern technology, they are not able to create the tools they need. This problem may introduce us to some possibilities for the scientific community, in particular for technical universities. These institutions are able to create the tools needed in the area of computer forensics, that aims to provide digital evidence to investigators. To do so they have to cooperate with the services, staff and organizational resources. Of course, these tools should provide certain level of functionality and should also meet elementary requirements.

Keywords: forensic, digital evidence, criminality.

1. WSTĘP

Cyfryzacja dotyka nas z każdej strony. Zagląda do życia prywatnego i służbowego. Stanowi podstawowy element rzeczywistości, a technologie informatyczne stają się istotnym narzędziem wspomagającym wykonywanie pracy, służącym do przekazywania informacji, czy po prostu do rozrywki. Nie inaczej dzieje się w obszarze przestępczości. Na tym polu technologię wykorzystuje zarówno jedna i druga strona barykady. Technika komputerowa bardzo pomaga w popełnianiu przestępstw czy wykroczeń, ale również coraz lepiej służy organom ścigania do ich wykrywania. Aby ujawniania te były możliwe należy poznać i stale ulepszać dostępne narzędzia informatyczne wykorzystywane m.in. do walki z przestępczością ekonomiczną. Narzędzia te zdają egzamin w takich obszarach jak analiza ryzyka, informatyka śledcza czy analiza kryminalna i chociaż te dyscypliny się przenikają, to każda z nich stanowi autonomiczny instrument. Aby efekty w zakresie zwalczania przestępczości były najlepsze całkowita autonomia nie jest jednak wskazana, a konieczne jest współdziałanie.. Gdy informatyk śledczy dostarcza olbrzymią ilość danych, analityk kryminalny może poddać je poszerzonej dedukcji, a osoba prowadząca dochodzenie pozyskać niezbite i celne dowody przestępczej działalności na podstawie których można określić nowe ryzyka np. w obszarze przestępczości ekonomicznej. Zdiagnozowane obszary z kolei przyczyniają się do lepszej prewencji i skuteczniejszego typowania do kontroli. Pozwala to na angażowanie sił i środków dokładnie tam, gdzie występują zagrożenia naruszenia prawa.

W nowoczesne narzędzia cyfrowe: oprogramowanie i sprzęt obowiązkowo powinna być dziś wyposażona każda służba powołana do egzekwowania prawa. Technologia cyfrowa to obecnie nie tylko alternatywa dla dotychczas wykorzystywanych narzędzi kontrolnych i procesowych, ale konieczność i przyszłość sprawnej walki z przestępczością, w tym z przestępczością ekonomiczną. Należy jednak pamiętać, że służby, chociaż są beneficjentami technologii cyfrowych, to same nie są autorami narzędzi, z których korzystają. Stają się one tylko i wyłącznie użytkownikami tych produktów, które dostarczają producenci. Warto podkreślić, że rynek narzędzi tego rodzaju jest rynkiem niszowym i hermetycznym. Istnieją oczywiście bezpłatne, powszechnie dostępne narzędzia do odzyskiwania danych, ale tylko te płatne i profesjonalne zapewniają odpowiedni poziom uzyskiwanych wyników. W obszarze konstruowania profesjonalnych narzędzi informatycznych wykorzystywanych w analizie kryminalnej, informatyce śledczej czy analizie ryzyka istnieje właśnie olbrzymie pole dla pracy naukowej, która dostarczałaby praktyczne, a nie teoretyczne rozwiązania, możliwe do wykorzystania w pracy służb. Niewątpliwie przy opracowaniu tych narzędzi pomocne byłyby same służby, kierunkując i testując zaproponowane narzędzia.

2. DOWÓD CYFROWY

Aby właściwie przedstawić problem wykorzystania narzędzi informatycznych w zwalczaniu przestępczości należy poprawnie zdefiniować pojęcie dowodu elektronicznego. Tutaj w pierwszej kolejności nasuwa się skojarzenie z urządzeniem,

które służy nam do komunikacji, pracy, które wykorzystujemy do pisania, obliczeń, zestawień, projektowania, odtwarzania multimediów, a przechodząc na język informatyków - do przetwarzania danych. To właśnie komputer, czy telefon komórkowy stanowi zainteresowanie śledczych, kiedy jest mowa o zabezpieczeniu dowodów. Gdy się jednak dłużej zastanowimy, to okazuje się, że nie sprzęt, który wykorzystujemy jest ważny, a wytworzone i przechowywane na nim dane. To one stanowią dowód w sprawie i to właśnie te dane nazywamy dowodem cyfrowy. Zabezpieczony materiał cyfrowy określa jego twórcę, wskazuje na czas, a nawet miejsce jego wytworzenia, określa nadawców i odbiorców wiadomości, zawiera określone treści, wskazuje użytkowników urządzeń, czy opisuje daną sytuację.

Biorąc pod uwagę sposób wytworzenia danych można je podzielić na:

- dane wytworzone przez użytkownika – np. pisma napisane przy pomocy edytorów tekstu, wiadomości poczty elektronicznej i komunikatorów, notatki i zapisy elektronicznych kalendarzy, prezentacje,
- dane wygenerowane samodzielnie przez urządzenia do przetwarzania danych – np. zapisy transakcji bankowych, wykazy połączeń, tzw. metadane, czyli dane o danych (np. gdzie i kiedy, przy pomocy jakiego urządzenia zostało wykonane zdjęcie cyfrowe), symulacje komputerowe, efekty obróbki materiału zdjęciowego czy filmowego,
- dane mieszane, czyli generowane przez człowieka i komputer – np. pliki arkuszy kalkulacyjnych, rejestry handlowe, skany dokumentów.

3. INFORMATYKA ŚLEDCZA – NARZĘDZIE POZYSKANIA DOWODÓW CYFROWYCH

Jednym z podstawowych narządzi wspomagania dzisiejszej kontroli jest informatyka śledcza. Można powiedzieć, że informatyka wyodrębniła się z nauk matematycznych. Z biegiem lat i rozwojem technologii stała się samoistną gałęzią nauki, swoistym połączeniem nauk ścisłych oraz techniki. Naturalną konsekwencją takiego stanu rzeczy było pojawienie się kolejnych specjalizacji w obrębie tej nowej dziedziny wiedzy. Podobnie jak w przypadku takich dyscyplin jak np. medycyna czy technika, w informatyce również zaczęto wykorzystywać specjalistyczną wiedzę do działań wspomagających stosowanie i egzekwowanie prawa. Medycyna sądowa czy technika kryminalistyczna są dzisiaj dyscyplinami bez których nie można wyobrazić sobie pracy służb. Obecnie do grona dziedzin nauki wspomagających zwalczanie przestępczości dołączyła informatyka poprzez jej gałąź, jaką jest informatyka śledcza.

Chcąc krótko zdefiniować tę dziedzinę nauki możemy powiedzieć, że jest to wykorzystywanie wiedzy informatycznej w praktyce. Nasuwa się wówczas kolejne pytanie, na czym ono jednak polega. Trzeba w tym miejscu zauważyć, że informatyka śledcza jest częścią kryminalistyki, która zgodnie z definicją Tadeusza Hanauska, jest nauką *o taktycznych zasadach i sposobach oraz o technicznych metodach i środkach rozpoznawania, a także wykrywania prawnie określonych, ujemnych zjawisk społecznych, a w szczególności przestępstw i ich sprawców oraz udowad-*

niania istnienia lub braku związku między osobami a zdarzeniami.[13] Można z tego wywieść, że również informatyka śledcza ma za zadanie dostarczyć dowody w prowadzonym dochodzeniu czy śledztwie. Aby je pozyskać i wykorzystać później w procesie karnym, podobnie jak każdy inny dowód, muszą one być odnalezione, zabezpieczone, przeanalizowane i odpowiednio zaprezentowane. Można zatem informatykę śledczą zdefiniować jako praktyczne wykorzystanie wiedzy o lokalizowaniu, pozyskiwaniu, analizowaniu, zabezpieczaniu i prezentacji dowodów elektronicznych. Aby jeszcze lepiej zdefiniować to określenie przychodzi na myśl bardziej obrazowe porównanie. Porównując pracę informatyka do czynności przesłuchania można powiedzieć, że informatycy śledczy „przesłuchują" nośniki danych, a jeszcze dobitniej, biorąc pod uwagę jedno z najpowszechniej wykorzystywanych obecnie urządzeń - „spowiadają telefony". Gdyby się głębiej nad tym zastanowić to ta alegoria ma mocne zakorzenienie w rzeczywistości. W dawnych czasach informacja była przekazywana ustnie, później pisemnie. Dzisiaj jest przekazywana przy pomocy technologii cyfrowych. Dawniej, aby otrzymać rzeczywisty obraz sprawy należało „wydobyć" prawdę z osoby przesłuchiwanej lub zdobyć odpowiedne dokumenty zawierające zapisy odnoszące się do niej. Obecnie wiele potrzebnych informacji można odcyfrować z danych zawartych w urządzeniach, z których każdy z nas korzysta na co dzień. Współczesna technologia pozwala nie tylko na prosty odczyt danych, które są jawne, ale również np. na odczyt danych skasowanych. Pozwala także na prześledzenie naszej aktywności w sieci, na wskazanie miejsc, w których przebywaliśmy czy odczytanie naszej korespondencji. W czasach gdy do prowadzenia korespondencji wykorzystywano wyłącznie papier jego zniszczenie, o ile nikt nie wykonał odpisu z oryginału, było równoznaczne z unicestwieniem dowodu. Dzisiaj list elektroniczny (e-mail) istnieje w wielu kopiach. Można go odnaleźć na komputerze lub smartfonie nadawcy, na serwerach poczty wychodzącej i przychodzącej, a nawet- dzięki programom zwanym „klientami poczty"- np. na komputerze odbiorcy korespondencji. Głośnym przykładem wykorzystania dowodów elektronicznych w postaci korespondencji e-mailowej w procesie karnym była sprawa katastrofy budowlanej na terenie Międzynarodowych Targów Katowickich w roku 2006. W sprawie tej prokurator posiadał m.in. dowody w postaci e-maili na to, że członkowie zarządu byli świadomi zagrożenia, ale mimo tego nie podjęli stosownych działań. Innym spektakularnym przykładem wykorzystania informatyki śledczej była głośna sprawa Katarzyny Waśniewskiej, dzieciobójczyni z Sosnowca, w której udało się odtworzyć historię jej wizyt na stronach internetowych i przez to wskazać na poszlaki świadczące o przygotowywaniu zabójstwa. Śledczy m.in. wykazali, że oskarżona poszukiwała w sieci odpowiedzi na takie pytania jak: „jak zabić bez śladów", „czy można zabić bez pozostawienia śladów", „dochodzenie policyjne przy zaczadzeniu tlenkiem węgla", „zasiłek pogrzebowy niemowlaka", „pochówek dzieci martwo urodzonych", „kremacja niemowlaka cena", „nieumyślne spowodo-

[13] Hanausek T.: *Kryminalistyka – zarys wykładu*, wyd. Zakamycze 2005 r., s. 23.

wanie śmierci" oraz „cennik trumien dla dzieci w miejskim zakładzie pogrzebowym”[14].

Chcąc uszczegółowić definicję informatyki śledczej uwzględniając jej poszczególne elementy należy przyjąć, że to wiedza o:

1. lokalizowaniu dowodów cyfrowych, czyli ich odnajdywaniu na różnego rodzaju nośnikach (dyski twarde komputerów, dyskietki, płyty CD, pamięci przenośne, serwery, telefony komórkowe itp.), a także internetowych nośnikach danych (portale społecznościowe, dyski w chmurze czy wyszukiwarki internetowe)[15],
2. pozyskiwaniu, czyli ich odczytaniu z urządzeń lub sieci (w tym również pozyskaniu danych skasowanych lub zaszyfrowanych),
3. analizowaniu, czyli przeszukiwaniu baz danych pod określonym kątem (np. wyszukiwaniu określonych adresatów korespondencji elektronicznej), wyszukiwaniu powiązań pomiędzy danymi,
4. zabezpieczeniu, czyli procesowym zabezpieczeniu dowodów cyfrowych np. w postaci kopii binarnych całych nośników czy kopii plików (kopie uwierzytelnione tzw. sumą kontrolną, którą to operację można porównać do potwierdzenia dokumentu „za zgodność z oryginałem”,
5. prezentacji, czyli takim przedstawieniu dowodów cyfrowych (zapisaniu w określonym formacie), który pozwala na ich odtworzenie przy pomocy standardowych, ogólnie dostępnych programów (np. programu MS Office czy odtwarzacza plików multimedialnych - WMP). Odpowiednia prezentacja pozwala na poddanie zgromadzonych danych dalszej analizie, np. przez analityków kryminalnych lub na prostą prezentację dowodów na sali sadowej.

Wskazany wyżej podział wyznacza funkcjonalność narzędzi, którymi posługują się informatycy śledczy, a które mogłoby dostarczyć środowisko naukowe. Można je podzielić na narzędzia do:

1. procesowego pobierania i zabezpieczania (akwizycji) danych zgromadzonych na nośnikach fizycznych, w tym wykonywania kopii całych nośników,
2. procesowego pobierania i zabezpieczania danych z pamięci ulotnych (RAM) i pracujących systemów komputerowych, w tym kopii wyodrębnionych plików (live forensic),
3. pozyskiwania i analizy danych pochodzących z urządzeń mobilnych (Mobile Forensic),
4. pozyskiwania i analizy zapisu dźwięku i obrazu,
5. odzyskiwania danych,
6. analizy pobranych danych,
7. pozyskanie danych z pojazdów samochodowych,

[14] Artykuł na portalu WP wiadomości z dnia 03-09-2013, *Katarzyna W. skazana na 25 lat więzienia za zabójstwo córki Magdy* (http://wiadomosci.wp.pl/katarzyna-w-skazana-na-25-lat-wiezienia-za-zabojstwo-corki-magdy-6031331089179265a)

[15] Jakub Dzikowski, *Uniwersytet Ekonomiczny w Poznaniu: Wyszukiwanie danych osobowych w Internecie dla celów Informatyki Śledczej*, STUDIA OECONOMICA POSNANIENSIA 2013,vol.1,no.2(251)

8. pozyskiwania danych pochodzących z sieci (chmury obliczeniowej).

Pierwsza grupa narzędzi to najczęściej sprzęt pozwalający na realizację naczelnego motta, którym kierują się informatycy śledczy, czyli „widzę wszystko, nie zmieniam nic". Do grupy tej zaliczają się tzw. blokery zapisu, duplikatory czy kopiarki dysków, posiadające funkcję blokady zapisu. Można w uproszczeniu stwierdzić, że pozwalają one na wykonanie procesowej kopii binarnej dysku, która jest identyczna z oryginałem, przy czym oryginał danych pozostaje „nietknięty".

Drugą grupę stanowią programy pozwalające na wykonanie czynności z zakresu informatyki śledczej na pracującym systemie. Muszą one dać możliwość szybkiego zabezpieczenia danych, do których po wyłączeniu komputera dostęp będzie niemożliwy, np. z uwagi na szyfrowanie lub wyłączenie opcji archiwizowania zapisu rozmów z komunikatorów. Z drugiej strony winny one umożliwiać pobranie danych w sytuacji, gdy niemożliwe jest wyłączenie np. pracujących serwerów. W tym przypadku oczekiwane narządzie powinno umożliwić celowane (technika *Triage*) pobranie, na miejscu realizacji, tylko istotnego dla sprawy materiału dowodowego i pominięcie kopiowania nieistotnych danych.

Trzecia grupa to zwykle narzędzia sprzętowo-programowe, które pozwalają na dostęp do danych zgromadzonych na urządzeniach mobilnych (telefony komórkowe, tablety, nawigacje GPS, itp.)[16]. Sprzęt taki wykorzystywany jest głównie przez organy ścigania lub inne służby powołane do ochrony państwa. Funkcjonariusze tych służb oczekują, aby narzędzia te gwarantowały nie tylko wysoką skuteczność, ale również w wielu przypadkach - pełną mobilność. Sprzęt taki powinien umożliwiać wyodrębnianie, dekodowanie i analizę danych z wszelkich urządzeń mobilnych. Powinien zapewniać dostęp nie tylko do urządzeń niezabezpieczonych, ale również do sprzętu zabezpieczonego np. hasłem czy poprzez znak graficzny (pattern lock). Precyzując- narzędzie to musi posiadać funkcjonalność pozwalającą na logiczną i fizyczną ekstrakcję danych, czyli dać dostęp do systemu plików, haseł i każdego rodzaju danych zgromadzonych na urządzeniu mobilnym, także tych usuniętych i chronionych.

Czwartą grupę stanowią oprogramowanie lub zestawy składające się z urządzeń i programów, których zadaniem jest pozyskanie, zdekodowanie, obróbka i ponowne zgranie danych, stanowiących zapis dźwięku, obrazu lub nagrań video. Wymagania stawiane dedykowanemu oprogramowaniu to przede wszystkim: możliwość dekodowania materiału video z różnych typów rejestratorów (różne typy plików), automatycznego wyodrębnienia wskazanych obiektów (np. identyfikacja twarzy, sekwencje ruchu, sekwencje w danym obszarze), wyboru/indeksowania określonego czasu i terminu nagrania. Oczywiście oczekiwane narzędzie musi również posiadać

[16] Wiodącymi produktami komercyjnymi (zestawy oprogramowanie + osprzęt) wykorzystywanymi obecnie przez organy ścigania oraz firmy z branży informatyki śledczej i odzyskiwania danych są m.in. UFED firmy Cellebrite oraz XRY firmy MSAB

pełną zdolność do odzyskiwanie danych, które z różnych przyczyn zostały uszkodzone lub skasowane[17].

Narzędzia reprezentujące piątą i szóstą grupę najczęściej występują na rynku jako koherentne oprogramowanie posiadające taką funkcjonalność, jak[18]:

- możliwość przeglądania przestrzeni wolnej i nieprzydzielonej,
- odzyskanie danych, w tym odzyskiwanie w trybie RAW,
- ustalanie cech charakterystycznych podłączanych nośników,
- przeszukiwanie przestrzeni „slack",
- możliwość przeglądania atrybutów oraz uprawnień dotyczących plików,
- umożliwienie dostępu do alternatywnego strumienia danych (ADS),
- indeksowanie plików oraz metadanych,
- obsługa bazy danych NIST (NSRL),
- możliwość analizowania sygnatur plików,
- możliwość analizowania pamięci RAM,
- możliwość analizy backup-ów urządzeń mobilnych,
- umożliwienie analizy metadanych plików (EXIF),
- możliwość analizy entropii,
- umożliwienie analizowania rejestrów systemowych.

Nowym wyzwaniem dla informatyki śledczej jest zabezpieczanie danych generowanych przez pojazdy samochodowe. Postęp w zakresie cyfryzacji nie ominął również takiej dziedziny jak motoryzacja, a można wręcz powiedzieć, że zaczyna w niej dominować. Współczesny samochód nie może się już poruszać bez zintegrowanej z układami mechanicznymi elektroniki. Większa część układów samochodu jest sterowana komputerowo, co wiąże się z przetwarzaniem danych, ale również ich archiwizacją. Dane dotyczące np. parametrów pracy czy błędów silnika nie będą istotne w prowadzonych dochodzeniach przeciwko przestępczości ekonomicznej. Jednak dzisiejsze samochody „pamiętają" dużo więcej. W zależności od wyposażenia możemy spodziewać się danych geolokalizacyjnych, w tym informacji o przebytych trasach wraz ze znacznikami czasowymi, jak również danych o inicjowanych lub odbieranych połączeniach. Te ostatnie informacje mogą pochodzić z urządzeń pokładowych, bądź z urządzeń przyłączanych do systemów samochodu, jak np. telefon komórkowy, tablet czy laptop podłączony poprzez Bluetooth.

Ostatnią grupę stanowią narzędzia do analizy i zabezpieczania danych w rozległych sieciach komputerowych (cloud computing[19]). Jeszcze do niedawna, aby

[17] Narzędzia wykorzystywane dopozyskiwania tego typu danych to to m.in. DVR Examiner firmy DME Forensics lub HX-Recovery for DVR

[18] Przykładem takiego profesjonalnego narzędzia, którego funkcjonalność odpowiada wyszczególnionej, jest program EnCase® Forensic firmy OpenText Corp wcześniej Guidance Software

[19] *Chmura obliczeniowa* (również przetwarzanie w chmurze, ang. cloud computing) – model przetwarzania danych oparty na użytkowaniu usług dostarczonych przez usługodawcę (wewnętrzny dział lub zewnętrzna organizacja).

pozyskać dowody cyfrowe np. korespondencję elektroniczną czy dane księgowe, wystarczało zatrzymać urządzenia, na których dane te były przechowywane, a które znajdowały się w posiadaniu kontrolowanych czy firm (komputery osobiste, firmowe serwery, telefony komórkowe, itp.). Obecnie, szczególnie z uwagi na olbrzymią ilość danych, nie są już one przechowywane w pamięci posiadanych urządzeń, ale na specjalnych zewnętrznych, odpowiednio zabezpieczonych serwerach u dostawców świadczących takie usługi. Osoby prywatne w systemach chmurowych przechowują swoje np. zdjęcia, muzykę, filmy. Firmy zamiast rozrywki przesyłają do wirtualnego magazynu ważne dane w postaci np. dokumentacji księgowej czy wytarzanych w firmie dokumentów. Wyzwaniem staje się więc prawidłowe procesowe zabezpieczenie tych danych i dotarcie przez informatyka śledczego do wirtualnych sejfów. Nie zagłębiając się w problemy natury prawnej dotyczące globalnego charakteru sieci Internet (serwery - magazyny danych nie znajdują się w państwie, w którym prowadzone jest kontrola lub postępowanie) do rozwiązania jest coraz więcej problemów technicznych, związanych przede wszystkim brakiem fizycznego dostępu do komputera, jak również zabezpieczeniem dostępu poprzez różne sposoby uwierzytelnienia, szyfrowanie czy olbrzymią ilość danych. Problemem jest nie tylko zdobycie samych danych, ale również ustalenie ich położenia (lokalizacji serwerów) oraz zabezpieczenie przed ich zdalnym skasowaniem. W sytuacji posiadania danych problemem jest ustalenie- kto i gdzie je wytworzył. Wszystko to i wiele nie innych problemów powinno znaleźć rozwiązanie w opracowywanych narzędziach dla informatyków śledczych, mających za zadanie zabezpieczanie danych w chmurze.

Dodatkowym nowym wyzwaniem jest skonstruowanie narzędzia umożliwiającego identyfikację i zabezpieczenie kryptowalut, które będzie działać niezależnie od rodzaju badanego urządzenia, przeznaczonego do wykonywania transakcji w obszarze kryptowalut np. przy użyciu tzw. portfeli, czyli miejsca służącego do przechowywania elektronicznego pieniądza (kluczy prywatnych). Oczekiwana funkcjonalność w tym zakresie mogłaby się sprowadzać do automatyzacji rozpoznawania odpowiedniego kodu oraz umożliwienia dokonania zabezpieczenia odnalezionej kryptowaluty.

4. TWORZENIE NARZĘDZI INFORMATYKI ŚLEDCZEJ

Dowód elektroniczny, a przez to informatyka śledcza, zaczynają pełnić kluczową rolę w procesie karnym spełniając dwie podstawowe funkcje:

- informacyjną – czyli ukierunkowaną na odnalezienie wskazówek pomocnych w prowadzeniu dochodzenia,
- dowodową – czyli ukierunkowaną na dostarczanie dowodów popełnienia określonych czynów.

Podkreślenia wymaga fakt, że obie funkcje są ze sobą nierozerwalnie związane i nawzajem się przenikają. Pozyskane dane mogą stanowić wszak nie tylko wskazówkę, ale zarazem dowód w sprawie.

Aby w pełni korzystać z dobrodziejstwa jakim jest dowód cyfrowy potrzebna jest nie tylko specjalistyczna wiedza informatyka śledczego, ale dostarczenie mu narzędzia, które cały proces akwizycji, analizy i zabezpieczenie danych ułatwi i zautomatyzuje. W innym przypadku praca wykonywana przez specjalistę wymagałaby każdorazowego poświęcenia ogromnej ilości czasu na „ręczne" pozyskanie elektronicznego materiału dowodowego. Tutaj otwiera się olbrzymie pole dla działań świata naukowego, aby we współpracy z organami ścigania dostarczać im nowe i coraz lesze narzędzia sprzętowe i programowe do informatyki śledczej. Taką możliwość daje odpowiednie zaplecze kadrowe i sprzętowe uczelni oraz czas, który może być poświęcony na badania i wdrożenie. Pracownicy naukowi dają także gwarancję tego, że narzędzia informatyki śledczej będą spełniały elementarne warunki, jakimi są:

- połączenie zasad prawa z techniką komputerową - sprzęt i oprogramowanie musi pozwolić na otrzymywanie wyników, które w procesie karnym mogą zostać zweryfikowane,
- zapewnienie powtarzalności wyników,
- automatyzacja czynności,
- czytelność i prostota interfejsu,
- maksymalna uniwersalność narzędzia w określonym obszarze (np. w obszarze urządzeń mobilnych) - dostęp do różnych formatów danych,
- dostęp do wszystkich metadanych,
- zapewnienie dostępu do danych „ulotnych",
- czytelność generowanych raportów – raport powinien być zrozumiały dla osób bez wykształcenia informatycznego,
- możliwość zrzutu zabezpieczonego materiału do popularnych formatów (np. pdf, doc, docx, xls,xlsx, avi, mp4 itp.),
- umożliwienie indeksowania badanego materiału (np. z uwagi na znaczniki czasowe),
- ingerencja w badany system komputerowy lub urządzenie w minimalnym, niezbędnym zakresie (bez otwierania niepotrzebnych okien i programów; bez niepotrzebnego zamykania już uruchomionych, itd.),

Niektórzy mogą powiedzieć, że takie narzędzia już na rynku istnieją, a służby i firmy działające w tym obszarze są w ich posiadaniu. Jednak z całą stanowczością trzeba stwierdzić, że ciągły, błyskawiczny rozwój technologii cyfrowej tworzy olbrzymi obszar do zagospodarowania, a istniejące narzędzia wymagają ciągłej aktualizacji i dostosowania do nowości. Nie one są również doskonałe i nie potrafią poradzić sobie ze wszystkimi urządzeniami, zabezpieczeniami czy rodzajami danych. Tak więc wejście w obszar tworzenia narzędzi dla informatyki śledczej, a przy tym współdziałanie uczelni ze służbami, jest ze wszech miar przydane i zapewnia korzyści dla obu stron tym bardziej, że działanie to nie kończy się wraz z wytworzeniem produktu, ale jest to proces ciągły, który nie ma ram czasowych. W dobie błyskawicznego rozwoju technologii cyfrowej i urządzeń na niej bazujących brak stałej aktualizacji wytworzonych narzędzi oraz wsparcia dla produktu postawiłby pod

znakiem zapytania sens jego tworzenia. Funkcjonalność takiego produktu w krótkim czasie stałaby się niewystarczająca, a z czasem narzędzie to byłoby bezużyteczne. Konstruowanie narzędzi dla informatyki śledczej zapewni uczelni technicznej możliwość tworzenia nie tylko teoretycznych rozwiązań, ale konkretnych produktów wykorzystywanych w praktyce, wymuszając na kadrze uczelni ciągły rozwój. Drugiej stronie zapewni to dostęp do innowacyjnych rozwiązań, które mogą zastąpić używane technologie lub okazać się ich uzupełnieniem.

Literatura:

[1] Hanausek T.: *Kryminalistyka – zarys wykładu*, Zakamycze 2005 r., s. 23.
[2] Jakub Dzikowski, *Wyszukiwanie danych osobowych w Internecie dla celów Informatyki Śledczej,* Uniwersytet Ekonomiczny w Poznaniu: STUDIA OECONOMICA POSNANIENSIA 2013,vol.1,no.2(251)
[3] Arkadiusz Lach,: *Dowody elektroniczne w procesie karnym,* Dom Organizatora Toruń 2004
[4] Cory Altheide, Harlan Carvey: *Informatyka śledcza. Przewodnik po narzędziach open source*, Helion, 2014
[5] Artur M. Kalinowski,: *Metody inwigilacji i elementy informatyki śledczej,* CSH, Kwidzyń 2011
[6] Przemysław Gwizd, *Analiza danych w informatyce śledczej; Bezpieczeństwo: teoria i praktyka*: czasopismo Krakowskiej Szkoły Wyższej im. Andrzeja Frycza Modrzewskiego 7/4, 43-58 (2013)
[7] Czasopismo*: Magazyn informatyki śledczej i bezpieczeństwa IT,* Wydawca Media Sp. z o.o. [https://magazyn.mediarecovery.pl/]

Źródła internetowe

[8] portal WP, wiadomości z dnia 03-09-2013, Katarzyna W. skazana na 25 lat więzienia za zabójstwo córki Magdy [dostęp: http://wiadomosci.wp.pl/katarzyna-w-skazana-na-25-lat-wiezienia-za-zabojstwo-corki-magdy-6031331089179265a]
[9] EnCase® Forensic [dostęp: https://www.guidancesoftware.com/encase-forensic]
[10] Cellebrite [dostęp: https://www.cellebrite.com/en/home/]
[11] MSAB [dostęp: https://www.msab.com/]
[12] Berla CorporationB [dostęp: https://berla.co/]
[13] DME Forensics [dostep: https://dmeforensics.com/dvr-examiner/]
[14] HX Recovery for DVR [dostęp: http://www.hxdvr.com/]

podinsp. mgr inż. Wojciech Zimoch
Izba Administracji Skarbowej w Opolu / Opolski Urząd Celno-Skarbowy w Opolu
Centrum Techniczne Informatyki Śledczej KAS
e-mail: wojciech.zimoch@mf.gov.pl

Rafał KOKOT
Tomasz TURBA

ZARYS HISTORYCZNY SIECI DARKNET ORAZ ASPEKTY LEGALNEGO I NIELEGALNEGO WYKORZYSTANIA TECHNOLOGII TOR

Streszczenie: Artykuł opisuje zarys historyczny sieci darknet oraz legalne i nielegalne zastosowania anonimowej technologii opartej o sieć TOR. W kolejnych rozdziałach została opisana historia powstania, zalety i wady rozwiązania oraz potencjalne kierunki rozwoju i wykorzystania technologii w przyszłości w kontekście działań służb zwalczających przestępczość w Internecie, a także po stronie zwykłego użytkownika pragnącego zachować anonimowość w sieci.

Słowa kluczowe: sieć tor, darknet, deepweb, anonimowość.

HISTORICAL OUTLINE OF DARKNET AND THE LEGAL AND ILLEGAL ASPECTS OF USE THE TOR TECHNOLOGY

Summary: Article describes the legal and illegal uses of anonymous technology based on the Tor network. The following chapters describe the history of uprising, the advantages and disadvantages of the solution, and the potential trends for the development and use of technologies in the futures in context of the customs service to fight cybercrime, as well as for the ordinary user wishing to remain anonymous online.

Keywords: tor, darknet, deepweb, anonymity.

1. HISTORIA POWSTANIA SIECI DARKNET

Od początku powstania sieci Internet zaczęto zastanawiać się nad problemem wolności i anonimowości w Internecie. Stale pojawiają się kontrowersje i spory pomiędzy zwolennikami pełnej swobody i anonimowości w sieci, a stronnikami prawnego ograniczania korzystania z zasobów Internetu. W latach siedemdziesiątych, w zasadzie równocześnie, z sieci ARPANET [Biddle 2002: 3] ewoluowały dwie technologie – Internet znany dzisiaj każdemu oraz „Darknet" -określany ogólnie -zbiorem technologii wyizolowanych sieci zapewniających anonimowość, stworzonych do celów bezpieczeństwa. Określenie „Darknet" pojawiło się w 2002 w publikacji pracowników firmy Microsoft [Biddle 2002: 10] i od tej pory oficjalnie zaczęto używać tego pojęcia do ukrytej części internetu. Ludzie od zawsze kopiowali zawartość sieci, jednak w przeszłości większość tych obiektów musiała reprezentować policzalną, walutową wartość. Nielegalne działania w tym zakresie zostały zatrzymane dzięki wprowadzeniu przepisów prawa patentowego i ekonomicznego. Dzisiaj trudność polega na

tym, że przestępstwo kradzieży intelektualnej może być nienamacalne. Z reguły przestępstwa komputerowe są zapisem bitów i bajtów przetłumaczonych w sposób zrozumiały dla odbiorcy. Wraz z przyspieszeniem technologicznym w zakresie rozszerzenia dostępności sieci Internet na cały świat, wiele aspektów prawnych do dzisiaj nie jest uregulowanych, nie wspominając o trudności w nadążaniu nad opanowaniem nowych technologii przez człowieka. Jednakże istnieje prosta i tania możliwość pozyskania dobrej jakości pożądanej treści. Największym wyzwaniem jest sformułowanie, czy kontent może być dystrybuowany legalnie, jeżeli tak- to w jakim zakresie. Prawo autorskie strzeże legalności kopiowania i dystrybuowania cennych danych, ale ochrona tego prawa w ogólnodostępnej i szybkiej sieci jest trudna i stanowi ogromne wyzwanie dla regulatorów. Typowym przykładem ideologii stojącej za określeniem „darknet" jest kreatywność twórców oprogramowania, którzy mają na celu udostępnianie plików audio. Po raz pierwszy zostało to spopularyzowane przez aplikację Napster jeszcze przed czasem, gdy nagrywarki CD stały się ogólnodostępne [Goos 2016: 172]. Można powiedzieć, że udostępnianie plików na dużą skalę miało miejsce od początku pojawienia się komputerów klasy PC. Idea darknetu opiera się na trzech założeniach podstawowych:

- każdy szeroko rozproszony plik będzie dostępny dla części użytkowników w formie umożliwiającej kopiowanie i dystrybuowanie,
- użytkownicy będą kopiować i udostępniać pliki ,jeżeli jest to możliwe i interesujące,
- użytkownicy są połączeni bezpośrednimi węzłami o wysokiej przepustowości.

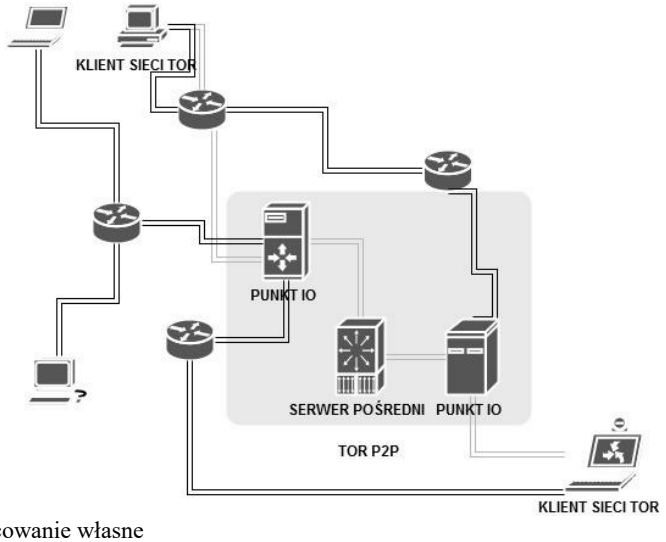
Darknet jest więc siecią dystrybucyjną, która rośnie wraz z ze zwiększoną liczbą udostępnianych plików bądź treści. Jedną z podstawowych implikacji jest założenie, że każdy system ochrony treści zostanie złamany i dojdzie do wycieku do w/w sieci, ponieważ część użytkowników – ekspertów bezpieczeństwa – pokona większość mechanizmów zabezpieczania przed kopiowaniem. Ważne jest też zrozumienie pojęcia „szeroko rozproszonego pliku" – ma to na celu uchwycenie pojęcia dystrybucji na rynku masowym dla milionów, praktycznie anonimowych użytkowników. Jest to założenie sprzeczne w zakresie ochrony tajemnic wojskowych, przemysłowych lub osobistych, które zazwyczaj nie są szeroko rozpowszechniane. Warto w tym momencie zwrócić uwagę na mechanizmy inżynierii społecznych stosowanych na portalach społecznościowych. Użytkownicy sami publikują i udostępniają tam swoje treści, pozostawiając wieczny ślad [Goos 2016: 176]. W kontekście służb mundurowych – wszelkie ślady mogące potwierdzić działalność podejrzanego użytkownika mogą być wykorzystane do jego zatrzymania. Pomimo, że nadal to tylko bity danych, to jednak ich cena na czarnym rynku niebotycznie wzrasta każdego dnia [Gorle 2015: 9]. Na cenę danych także ogromny wpływ miało niedawno wprowadzone rozporządzenie Parlamentu Europejskiego i Rady (UE) GDPR 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych, w Polsce noszące skrótową nazwę „RODO".

Pomimo, że rozporządzenie niesie za sobą wartość dodaną w postaci podnoszenia świadomości użytkowników i przedsiębiorców o przetwarzaniu danych i potrzebie zachowania ich bezpieczeństwa, to jednak na nielegalnych forach sieci darknet dało się zauważyć wzmożone podnoszenie cen związanych z wyciekami danych.

2. MODEL I EWOLUCJA SIECI NIELEGALNEJ DYSTRYBUCJI

Sieć darknet jest siecią dystrybucyjną która związuje ze sobą wstrzykiwanie plików i danych do sieci poprzez udostępnienie ich określonym użytkownikom. Opiera się na założeniu, że użytkownicy zainteresują się danymi i zaczną je kopiować dla siebie, a także udostępniać dla innych. Tak jak inne sieci tego typu (np. Napster, Gnutella), sieć darknet może zostać zamodelowana jako graf bezpośredni z krawędziami oznaczonymi. Graf ma po jednym wierzchołku dla każdego użytkownika (hosta), a dla każdej pary wierzchołków do których skierowana jest krawędź - jeśli obiekty mogą być kopiowane pomiędzy nimi. Etykiety brzegowe mogą służyć do modelowania istotnych informacji na temat topologii fizycznej sieci i mogą zawierać informację do których zalicza się: przepustowość, dostępność, priorytet i opóźnienie. Wierzchołki charakteryzowane są biblioteką obiektu (np. zbiór filmów), ilością żądań dostępu do obiektu od innych wierzchołków, a także spełnionych żądań do obiektów (kopiowanie zakończone sukcesem).

Rysunek 1. Schemat sieci TOR



Źródło: Opracowanie własne

By sieć darknet mogła prawidłowo funkcjonować niezbędne jest spełnienie kilku wymagań związanych z procesem przepływu danych, do których zalicza się:

1. Wymaganie związane z kompromisem udostępnienia danych w sposób technologicznie umożliwiający przesłanie obiektów do sieci poprzez ich konwersję. Jako przykład podaje się konwersję oryginalnego formatu wideo AVC na MP4 lub z XVID.
2. Istnienie mechanizmów magazynowania i replikacji danych w celu zezwolenia tworzenia i kopiowania danych przez użytkowników w sieci typu peer-to-peer (P2P). Jako przykład dzisiaj podaje się dysk twardy komputera, lub pamięć przenośną.
3. Istnienie urządzeń lub oprogramowania renderującego dane pozyskane z sieci. Dawniej były to przenośne odtwarzacze muzyki, odtwarzacze płyt DVD. Dzisiaj mówi się o oprogramowaniu i kodekach potrafiących obsługiwać konkretny standard kompresji i konwersji (np. K-Lite Codec-Pack, VLC Media Player).

Sieć darknet w rdzennej koncepcji musi spełniać następujące wymagania technologiczne:

1. Dowolna sieć darknet wymaga istnienia węzłów, które operują jako źródła przechwytywania danych. Użytkownicy wskazują co udostępniają w sieci i czekają na innych użytkowników chcących pozyskać dane.
2. Jeżeli istnieje nadawca, to musi w sieci istnieć także odbiorca operujący na tych samych zasadach. W dzisiejszych sieciach zwykle użytkownik jest jednocześnie nadawcą (seeder) i odbiorcą (leecher).
3. Łącza transmisyjne są niezbędne do transferowania obiektów (ich kopii) pomiędzy węzłami. W dzisiejszych czasach wykorzystuje się połączenie internetowe do nawiązania szyfrowanego połączenia z siecią darknet (np. za pomocą przeglądarki TOR Onion Browser).
4. Wyszukiwarki lub inne mechanizmy rozpoznawania nowych i istniejących użytkowników w celu odnalezienia pożądanej treści/danej.
5. Sieć może szyfrować wiele mikro-sieci wewnątrz struktury uniemożliwiając namierzenie użytkownika, zapewniając dzięki temu anonimowość

Można sklasyfikować różne manifestacje istnienia sieci darknet, które pojawiły się w ostatnich kilku latach ze względu na spełnienie pięciu podstawowych założeń opisanych wyżej. Także ze względu na analizę słabości i punktów ataków. Jako system, sieć darknet jest obiektem wielu ataków. Identyfikacja i powstrzymanie naruszeń prawa w sieci Internet w drodze postępowania sądowego jest wyzwaniem dla służb, zwłaszcza w kontekście problemu anonimowości. Dodatkowym problemem jest masowe też „wstrzykiwanie" i testowanie złośliwego oprogramowania bez kontroli. Wirusy, malware oraz spam stają się coraz bardziej szkodliwe.

Na początku lat 90-tych dystrybuowanie danych komputerowych było organizowane w obrębie grup znajomych. Do głównego nurtu danych należały wówczas muzyka i proste programy komputerowe (dyskietkowe). Urządzenia obsługujące były powszechnie dostępne, a sposób ich użytkowania nie decydo-

wał o legalności zastosowania. Przekazywanie danych w żaden sposób nie było regulowane i nie istniały formalne zabezpieczenia systemowe przed kopiowaniem. Nawet jeżeli istniały, to sposób zabezpieczenia był na tyle trywialny, że nie wymagał specjalnego instruktażu wykonawczego. Głównym źródłem transmisji danych były osoby same w sobie, które wymieniały dane „z ręki do ręki" lub za pośrednictwem poczty „pantoflowej" – głównego sposobu dystrybucji danych na owe czasy. Główną wadą takiej sieci było opóźnienie w dostępie do danych. Pozyskiwanie danych z sieci darknet (nazwanej wówczas po prostu „czarnym rynkiem") za pomocą linii modemowej o przepustowości 56.6 Kbps, kopiowanie oraz dystrybuowanie - mogło trwać tygodniami. Dodatkowym problemem był brak istnienia wyspecjalizowanej wyszukiwarki.

W roku 1998 powstała nowa forma darknetu ze względu na znaczące postępy technologiczne w kilku obszarach. Internet wszedł do głównego nurtu kultury i powoli stawał się głównym medium do transmisji danych prywatnych i służbowych. Kontynuacja spadków cenowych sprzętu komputerowego zapewniała zwiększenie dostępności do sieci Internet. Wraz ze wzrostem mocy obliczeniowej pojawiły się nowe algorytmy kompresji danych, gdzie nawet przy stosunkowo niskich przepustowościach (1 Mbps) pobranie pliku w formacie MP3 nie zajmowało już dużo czasu. Rok 1998 został określony także jako rok, w którym skok technologiczny spowodował, że komputery klasy PC przekroczyły granicę, w której ich moc obliczeniowa mogła służyć do odtwarzania multimediów. Wraz ze wzrostem w/w. czynników, pojawiały się pierwsze nielegalne sieci nazwane potocznie „Warez" z serwerami w Internecie w scentralizowanej strukturze. Sieć oparta o pocztę „pantoflową" została wyparta siecią Internet, gdzie dostęp jest znacznie szybszy i istnieją wyszukiwarki oraz sposoby komunikacji z innymi użytkownikami. Jednakże wraz z pozyskiwaniem plików z serwerów FTP oraz HTTP – użytkownik zawsze pozostawiał po sobie ślad w postaci adresu IP, znaczników czasu i celu pobierania. Spowodowało to początkową lawinę procesów o naruszenie praw autorskich, więc scentralizowany darknet stosunkowo szybko zniknął z głównego nurtu Internetu.

Zrozumienie problemu „anonimowości" stało się ważnym aspektem do rozwiązania i zaczęto powracać do koncepcji połączenia peer-to-peer. Jedną z pierwszych sieci opartych o protokół P2P był Napster [Goos 2016: 180] uruchomiony w 1999 r. oraz Gnutella o otwartym kodzie źródłowym [Goos 2016: 180]. Jednakże pierwsza sieć była scentralizowaną, zarządzaną siecią przez jedną firmę, a Gnutella nie zachowywała żadnych reguł anonimowości, gdyż opierała się o protokół adresowania IPv4 nadawcy i odbiorcy. Dzisiaj w pełni rozproszone systemy P2P nie posiadają pojedynczych punktów awarii, jak było w przypadku Napstera, co doprowadziło do jego upadku po skutecznych atakach DDoS. W systemach opartych o Gnutellę można było zaobserwować dwie słabości: pobieranie bez skrupułów, brak anonimowości. Systemy P2P często są określane jako zdecentralizowane sieci zawierające kopie danych rozproszone pomiędzy hostami. Liczne badania wskazują, że w typowych sieciach istniały tzw. „super peery" czyli osoby, które udostępniały znacznie więcej danych niż

pobierały. Natomiast całą resztę sieci tworzyli użytkownicy „żerujący" na nich, czyli pobierający dane, a nie udostępniający, co w znacznym stopniu inhibitowało dynamikę rozwoju takiej sieci. Należało więc wprowadzić system tzw. hierarchii bądź nagradzania osób bardziej zaangażowanych w rozwój sieci. Na kanwie Gnutelli powstały takie projekty jak KazaA, czy eDonkey który przekształcił się w eMule. Następnie w roku 2008 zapanowała era protokołu BitTorrent, trwająca do dzisiaj. Jednak z boku tych sieci, niezależnie od idei pobierania rozwija się sieć TOR – sieć nie bezpośrednio związana z przechowywaniem danych, a z zachowaniem anonimowości. Pojęcie DarkNet zostało całkowicie wchłonięte jako podsieć oparta o technologię TOR.

3. SPECYFIKACJA SIECI TOR I SPOSÓB GROMADZENIA DANYCH

TOR jest nabierającym popularności systemem wzmagającym prywatność użytkownika w celu strzeżenia jego prawa do prywatności w Internecie od analizy ruchu sieciowego uruchomionego przez nieglobalnych adwersarzy. Ponieważ TOR zapewnia usługę anonimowości z wykorzystaniem TCP przy stosunkowo małym opóźnieniu i wysokiej przepustowości – jest idealnym systemem do interakcji z użytkownikiem, do których zaliczyć można: przeglądanie sieci web, udostępnianie plików i komunikatory internetowe. Technologia TOR nakłada warstwę anonimowości na warstwę TCP tworząc ścieżkę trzy-punktową przez którą routery TOR używają warstwowego szyfrowania podobnego do onion routingu [Kobayashi 2016: 17]. Informacja o trasach jest przesyłana przez grupę autorytatywnych serwerów. W uproszczeniu, wszelka komunikacja TCP użytkownika jest tunelowana w jednym węźle, który rotuje w czasie. Trzy punkty sieci TOR są określane jako: wejściowy router TOR, pośredni router TOR oraz wyjściowy router TOR. Tylko wejściowy router TOR jest w stanie obserwować ruch od oryginatora w celu nabycia wiedzy o hoście docelowym. Dodatkowo w celu zapewnienia niskich opóźnień, sieć TOR nie wymusza retransmisji zgubionych pakietów. W celu lepszego zrozumienia funkcjonowania sieci w realnym świecie, został skonfigurowany router o przepustowości 1 Gbps dołączony do sieci globalnej [Goos 2016: 184] zgodnie z topologią rys. 1. W celu zbierania statystyk należało zdefiniować polityki określające co i z którego miejsca należy zbierać, by reprezentowało to wartość statystyczną. Zdecydowano się na przechwytywanie logów z węzłów nawiązujących połączenie z routerem oraz kierowanymi dalej przez badany router. Dodatkowo należało zebrać wystarczającą ilość do przechwytywania nagłówków protokołów warstwy aplikacji modelu ISO/OSI z ruchu wychodzącego od routera. W Tabeli 1 zostały opisane protokoły warstwy siódmej, które zostały przechwycone wraz ze wskazaniem ilości. Jednakże nie da się jednoznacznie stwierdzić, czy ruch był ruchem interaktywnym, jak w przypadku typowego ruchu protokołu HTTP/HTTPS w Internecie, czy też pobieraniem plików za pośrednictwem tego protokołu (co jest często spotykane w sieci TOR i BitTorrent).

Tabela 1. Zebrane protokoły warstwy aplikacji

PROTOKÓŁ	LICZBA POŁĄCZEŃ	LICZBA DANYCH
HTTP + SSL	13 145 103	422 GB
BitTorrent	438 395	285 GB
SMTP	7611	291 MB
FTP	1337	792 MB

Źródło: http://www.bearcave.com/misl/misl_tech/msdrm/darknet.htm

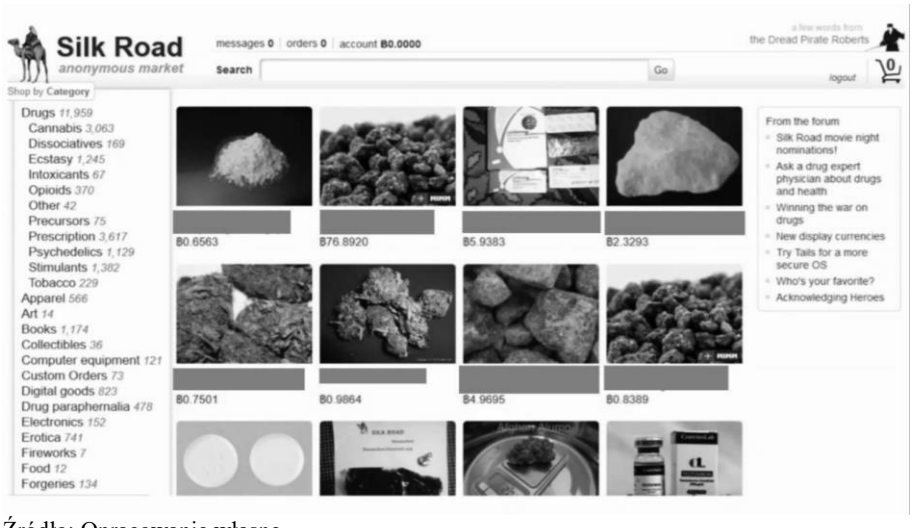
Ponieważ ruch sieciowy protokołu HTTP zdecydowanie dominuje w statystykach połączeń do routera należało przyjąć kryterium wskazujące, które połączenie mogło być interaktywne, a które nie. Dla danych statystycznych przyjęto, że ruch powyżej 1 MB danych stanowił połączenia nieinteraktywne przy założeniu, że strony internetowe w sieci TOR nie mają skomplikowanej konstrukcji. Zaledwie 3.5 % danych zostało w ten sposób określone [http://www.bearcave.com/misl/misl_tech/msdrm/darknet.htm]. Jednakże najbardziej znaczącym protokołem w stosunku liczby połączeń TCP jest protokół BitTorrent, który wykorzystywał nieproporcjonalnie dużą wartość pobieranych danych. Można było się spodziewać, że względu na fakt, że protokół jest częścią klienta P2P (np. uTorrent) służącego do pobierania plików. Jednakże pełna liczba połączeń TCP po protokole HTTP może wskazywać, że jest to ruch przechodzący przez anonimowych klientów usługi proxy. Niezwykłą obserwacją jest także fakt, że na liście znajdują się trzy protokoły uznawane za niebezpieczne. Protokoły POP, SMTP oraz FTP bez szyfrowania SSL są stosunkowo proste do przechwycenia i rozszyfrowania komunikacji w postaci otwartego tekstu. Sieć TOR multipleksuje połączenia TCP tego samego węzła, co oznacza, że przechwycenie ruchu jest stosunkowo prostsze niż w tradycyjnym Internecie (składanie pakietów i numerów kontrolnych). Biorąc pod uwagę stosunkowo dużą ilość niebezpiecznego ruchu, który można obserwować, to istnieje wielka zachęta dla potencjalnych napastników tworzących złośliwe oprogramowanie na stronach internetowych do infekowania komputera użytkownika.

4. NIELEGALNE SPOSOBY ZASTOSOWANIA SIECI TOR

Nie podlega dyskusji, że technologia TOR oraz wczesna sieć DarkNet dzisiaj stanowią jedną całość. Ideologiczna sieć DarkNet służy do dystrybucji, współdzielenia nielegalnych treści, a technologia TOR zapewnia anonimowość, a tym samym pewien sposób bezkarności. Jednoznacznie nazwany dzisiaj współczesny DarkNet, jest magistralą łączącą ideę nielegalnego współdzielenia i pozyskiwania danych z wykorzystaniem technologii TOR. Sieć DarkNet oparta o TOR jest dzisiaj jednym z głównych kanałów komunikacji przestępców oraz

serwisów oferujących nielegalne usługi i towary. Jednym z najbardziej znanych sklepów jest Silk Road (rys.2) oferujący międzynarodową sprzedaż narkotyków.

Rysunek 2. Zrzut ekranu ze sklepu Silk Road w sieci DarkNet



Źródło: Opracowanie własne

Niestety sieci DarkNet nikt nie kontroluje i nie jest ona w żadnym stopniu ustandaryzowana.

Co więcej, ideologicznie, samoczynnie zachęca do bycia przestępcą operując socjotechnicznie na wartościach takich jak ciekawość czy pobudzenie. Zgodnie z badaniami przedstawionymi wyżej, ruch w sieci nie jest w większości przypadków szyfrowany. Powodowałoby to dodatkowy impakt i trudności w działaniu, co negatywnie wpłynęłoby na popularność serwisów. Jednakże użytkownicy korzystający z sieci DarkNet muszą być świadomi, że poza infekcją swojego komputera w pewien sposób narażają się służbom monitorującym. Użytkownik ciekawy sieci DarkNet z reguły łączy się ze swojego domowego komputera, od jednego dostawcy Internetu. W przypadku wykrycia przez dostawcę anomalnego ruchu ze znacznikami wskazującymi na ruch DarkNet – służby mogą poprosić o logi od operatora, by jednoznacznie namierzyć użytkownika. Oczywiste jest, że z racji braku kontroli, nie ma formalnie mechanizmu pomocy w przypadku zostania ofiarą oszustwa. Najczęściej dochodzi do utraty pieniędzy, nieuprawnionego lub nieświadomego przekazania danych osobowych. Handel fałszywymi dokumentami (rys.3) jest bardzo powszechny w sieci DarkNet i stanowi główne źródło zarobkowania przestępców, którzy swoją płatność otrzymują w krypto-walucie (także anonimowej) – głównie BitCoin (BTC) i Monero (XMR).

Rysunek 3. Zrzut ekranu ze sklepu oferującego fałszywe paszporty do UK

Źródło: Opracowanie własne

Rysunek 4. Zrzut ekranu ze oferującego usługi płatnego zabójstwa

Źródło: Opracowanie własne

Znacznie rzadziej spotyka się strony z „poważniejszymi" usługami, jak płatne zabójstwo (rys.4) czy strony terrorystyczne. Przestępcy administrujący tymi stronami mają świadomość, że upublicznienie nawet w anonimowej sieci powoduje potencjalne zostawianie śladów i namierzenie przez służby. Dlatego tak jak

w życiu realnym, tak samo w sieci DarkNet istnieje łańcuch powiązań i zaufanych osób (w tym wypadku – zaufanych węzłów), które udostępniają „klientom" hiperłącze TOR do usługi, gdy zostaną oni zweryfikowani.

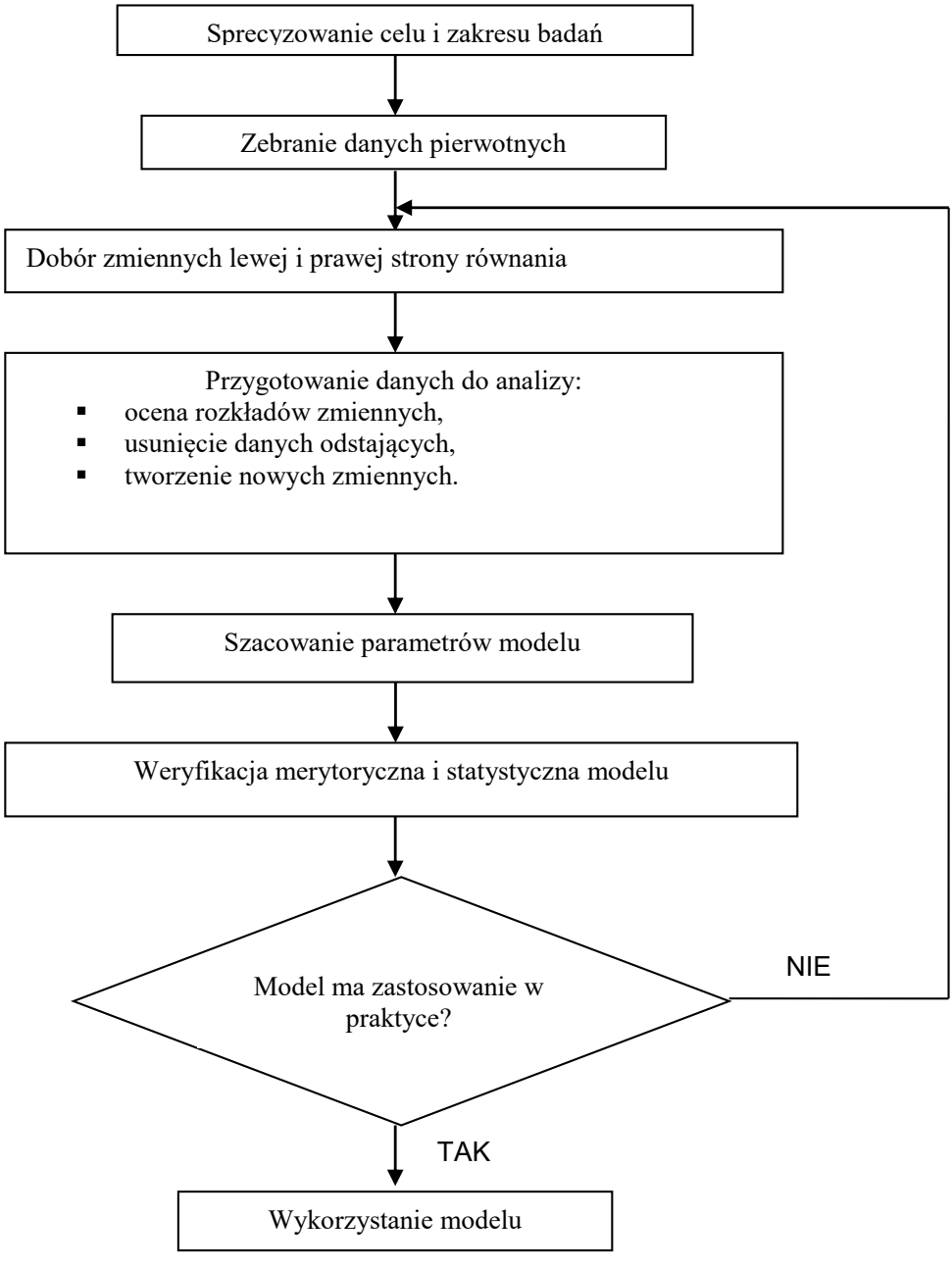
5. LEGALNE SPOSOBY ZASTOSOWANIA SIECI TOR

Nie podlega też dyskusji, że sieć TOR sama w sobie nie jest zagrożeniem technologicznym, a jedynie umożliwia pewną dystrybucję treści, których legalność jest ustanawiana warstwy wyżej – na podłożu regulacji prawnych. Jednoznacznie ideowo sieć TOR jest bardzo dobrym rozwiązaniem technologicznym, zwłaszcza w kontekście wprowadzonej dyrektywy RODO. Technologia ta zapewnia użytkownikowi anonimowość do której ma on prawo. Dodatkowo istnieje sporo serwisów w DarkNecie oferujących profesjonalne szyfrowanie VPN za niewielkie pieniądze, co daje użytkownikowi możliwość przesyłania newralgicznych plików w sposób zabezpieczony. Rozważyć należy także sytuację, w której użytkownik często do wykonania jakiejś czynności w aplikacji internetowej, zobowiązany jest podać swój adres e-mail. Nie chce jednak tego robić i w tym momencie musi z usługi zrezygnować lub skazać się na „wieczny" spam na swojej skrzynce. Usługi DarkNetu oferują jednorazowe konta e-mail potrzebne do rejestracji, a później „zapomnienie o nich", tym samym użytkownik może zachować czystość swojej skrzynki e-mail. Jednym z największych profitów ostatnich lat jest niewątpliwie pojawienie się serwisu WikiLeaks. Serwis służy do informowania społeczeństwa o wyciekach poufnych dokumentów rządowych. Przeglądając tradycyjny Internet, użytkownik bardzo często nie wie że jego zachowania i dane osobowe są właśnie przetwarzane. Przykładem jest usługa AdContent, AdWords od firmy Google lub Cortana z systemu Windows firmy Microsoft. Wszystkie te usługi łączy jeden cel – profilowanie reklamy dostarczanej do użytkownika w celu trafienia w jego gusta, co spowoduje jego zainteresowanie i zakup. Prawidłowo wyświetlane nam reklamy zawdzięczamy głównie wyszukiwarce Google, która kataloguje wszelkie możliwe dane. W/w. wyszukiwarka ogranicza także pewne wyniki wyszukiwań, co nie każdemu może się podobać. W sieci DarkNet, a także w Internecie powstała konkurencja – wyszukiwarka DuckDuckGo, która nie indeksuje wszystkiego co robi użytkownik, nie dostarcza reklam, a także nie blokuje dostępu do dowolnych treści. Jest to niewątpliwie ważny aspekt w dobie ochrony danych osobowych.

6. PODSUMOWANIE

W artykule opisano historyczny zarys sieci określanej jako „Darknet" (tzw. czarny rynek), który wyewoluował do postaci technologicznej z pomocą sieci TOR, która zapewnia anonimowość. Pomimo, że przesłanki do stworzenia sieci TOR są znane, to jednak należy poddać wątpliwość, czy nie jest to kolejna z usług po nawigacji satelitarnej GPS, Google'u oraz Facebook'u, która została udostępniona ludzkości za darmo, a tak naprawdę jest kolejnym narzędziem służb specjalnych do kontroli wszystkiego, co się dzieje na świecie. Sieć TOR

może służyć zarówno rozwiązaniom legalnym, jednak z uwagi na zebrane staty-



Mariusz R. RZĄSA
Wojciech GĘSIKOWSKI

TECHNIKI KOMPUTEROWE WSPOMAGAJĄCE ANALIZĘ OBRAZÓW RTG W KONTROLI CELNO-SKARBOWEJ

StreszczeniePraca zawiera opis stosowanych systemów RTG w kontroli celno-skarbowej. Przedstawiono przykładowe rozwiązania, jakie są powszechnie stosowane do wykrywania materiałów przemycanych przez granice państwowe. Proces wizualnej analizy zdjęć pochodzących ze skanera RTG przez człowieka należy do bardzo uciążliwych. Powodem tego jest duża liczba obrazów i wrażliwość wynikająca z konieczności analizy bardzo dużej liczby szczegółów o niezbyt dużym kontraście. Przedstawione w pracy rozwiązania mogą w znacznym stopniu wspomagać proces wizualnej analizy obrazów, zmniejszając w ten sposób zmęczenie człowieka podczas wielogodzinnej pracy.

Słowa kluczowe: kontrola celno-skarbowa, skaner RTG, analiza obrazu.

COMPUTER TECHNIQUES SUPPORTING IMAGES ANALYSIS OF X-RAYS SCANERS IN THE CUSTOMS AND TAX CONTROL

Summary: The paper contains a description of of X-ray scanners used in customs and tax control. The work contains a description of the principle of operation of X-ray scanners used in customs and tax control. Contains examples of solutions which are widely used for the detection of smuggled FOR IN borders. The process of visual analysis of images derived from X-ray scanner for a man to be very cumbersome. The reason for this is the large number of images and the perceptiveness resulting from the need to analyze a very large number of details with not very high contrast. The solutions presented in the paper can significantly support visual analysis of images, thus reducing human fatigue during long hours of work.

Keywords: customs and tax control, X-ray scanner, images analisys.

1. WSTĘP

Urządzenia rentgenowskie od wielu już lat stanowią powszechną i niejednokrotnie jedyną metodę kontroli celno-skarbowej. Stosuje się je tam, gdzie potrzebna jest bezpieczna, nieinwazyjna oraz szybka kontrola przewożonych ładunków i środków przewozowych. Kontrola RTG polega na prześwietlaniu promieniami badanego obiektu promieniami X, które odkrył niemiecki fizyk Konrad Wilhelm Roentgen (1845-1923). W 1896 roku we Francji, promienie X wykorzystywane już były w medycynie do diagnozowania gruźlicy a podczas I wojny światowej za pomocą promieni X poszukiwano kul i odłamków w ciałach rannych żołnierzy.

Obecnie promienie X stosuje się w :

- procesie prześwietlania bagaży, towarów, środków przewozowych wszędzie tam, gdzie wymagane jest zachowanie procedur bezpieczeństwa,
- w defektoskopii konstrukcji stalowych (wykrywaniu wad metali),
- w mikroskopach elektronowych, cyklotronach, akceleratorach,
- w badaniach pierwiastkowego składu chemicznego substancji oraz struktur kryształów.

Wzmożoną kontrolę ładunków z wykorzystaniem systemów rentgenowskich podjęto wraz z narastającym ryzykiem zagrożenia terrorystycznego począwszy od lat 80-tych XX wieku, aż do 11 września 2001 r., gdzie międzynarodowa siatka zwana „Al Kaidą", dokonała największego w dziejach ataku terrorystycznego – zamachu na World Trade Center w Nowym Jorku i Pentagon w Waszyngtonie.

Pierwsze systemy rentgenowskie do prześwietlania kontenerów (container inspection system), opracowała na początku lat 80-tych XX wieku niemiecka firma „Heimann", która w swoich urządzeniach wykorzystała niedrogie i średniej energii lampy rentgenowskie o energii 300 keV. W 1991 r. podobny system o energii 420 keV zainstalował też w jednym z brytyjskich portów morskich „Rapiscan". W 1994 roku mobilne urządzenie rentgenowskie z lampą o energii 450 keV skonstruowała amerykańska firma „AS&E Cargo Search". Oprócz lamp rentgenowskich, jako źródło promieniowania wykorzystywane były także pierwiastki promieniotwórcze takie jak cez i kobalt („Vacis"), o enrgii do 1,3 MeV oraz liniowe akceleratory elektronowe („Varian", „Bechtel"), które pozwalały wyzwolić energię od 2-16 MeV. Co ciekawe, pierwszy tego typu system mobilny o energii 6 MeV został zainstalowany w 1989 roku w Vodkinsku (byłe ZSRR, obecnie Rosja) do weryfikacji zawartości głowic bojowych produkowanych tam rakiet, co było z kolei związane z realizacją podpisanego w 1979 roku traktatu „SALT II" (Strategic Arms Limitation Treaty), ustalającego limity ilościowe i jakościowe systemów broni strategicznej [Drzewowski M., Stefaniak G. 2014:30-33].

W 1992 roku „Sysoscan" opracował pierwsze urządzenie rentgenowskie podwójnej energii (dual energy) o enrgii 2,5 MeV. Wykorzystanie tej technologii w zastosowaniach cywilnych datuje się na połowę lat 90-tych ubiegłego stulecia, kiedy to powstały m.in. mobilne wersje skanerów wykorzystujących lampy rentgenowskie (np. Smiths Silhouette ScanMobile o energii 140-300 keV), pierwiastki promieniotwórcze (m.in. Rapiscan Mobile Imaging System o energii 1MeV oraz Mobile Vacis o energii 1,3 MeV) oraz akceleratory liniowe (m.in. mobilny CX-25000 Mobile Cargo System firmy L-3 Communications o energii 2,5 MeV i przestawny Heimann CAB 2000 o energii 2,5 MeV).

Urządzenia rentgenowskie okazały się niezwykle skuteczne w walce z nielegalnym przemytem narkotyków, materiałów wybuchowych i broni. Wraz z systematycznym rozwojem źródeł promieniowania i technik detekcji, z czasem zaczęły się też pojawiać skanery dużej energii (8-10 MeV). W 1991 roku, na granicy Chin i Hongkongu w Shenzhen zostały np. zainstalowane dwa ogromne

systemy rentgenowskie „British Aerospace", wykorzystujące akcelerator linowy „Varian" (typu Linatron) o energii 9 MeV. Rok później „Heimann" opracował system Hi-Co-Scan o energii 8 MeV, natomiast amerykańska „DARPA" (Defense Advanced Research Projects Agency/Agencja Zaawansowanych Projektów Badawczych w Obszarze Obronności) opracowała, zbudowane na bazie akceleratorów liniowych „Siemens Vanguard" i systemu obrazowania „Heimann". Dwa eksperymentalne urządzenia rentgenowskie podwójnej energii 10 MeV były testowane w Houston (od 1992 r.) i Tacoma (od 1993 r.).

Obecnie skanery rentgenowskie są również powszechnie stosowane przy kontroli bagaży i ładunków na lotniskach oraz w morskich terminalach promowych. Pierwsze tego typu urządzenia oparte na fluoroskopowym systemie skanowania powstały w 1965 roku, a wersja „cyfrowa" pojawiła się w 1974 r., następnie system tzw. promieni odbitych „backskatter" w 1986 r., Skaner z tzw. dyskryminacją towarów, wykrywający m.in. materiały wybuchowe pojawił się w 1992r. Systematycznie ewoluowały również wielkogabarytowe skanery rentgenowskie (m.in. do prześwietlania wagonów kolejowych), przybywa też ich producentów, np. w 1997 r. powstała chińska firma „Nuctech", która ma już dzisiaj 60% udziału w globalnym rynku technologii używanych na przejściach granicznych do prześwietlania pojazdów i kontenerów. Firma ta, jako jedyna, posiada też w naszym kraju swoją montownię w Kobyłce k. Warszawy.

Wydajność współczesnych systemów rentgenowskich oceniana jest w oparciu o pięć podstawowych wskaźników zgodnych ze standardami ASTM (American Society for Testing and Materials/Amerykańskie Stowarzyszenie Badań i Materiałów):

- głębokość penetracji stali (np. min. 320 mm),
- jakość obrazu (m.in. zdolność wykrycia przewodu miedzianego o grubości 1 mm),
- kontrast obrazu (zdolność wykrycia płytki stalowej o wymiarach 400 mm x 400 mm będącej za inną płytą stalową o grubości m.in. 100 mm),
- dawka promieniowania (np. < 1 mSv/rok, 1 milisiwert na rok)
- przepustowość prześwietlanych kontenerów/samochodów ciężarowych (np. 20 na godz.)

Ze względu bezpieczeństwo oraz dopuszczalne wskaźniki napromieniowania żywności przyjmuje się, że górna granica energii dla prześwietlanych ładunków wynosi 9 MeV, co wynika z faktu, że promieniowanie nie kumuluje się w prześwietlanych obiektach,.

Krajowa Administracja Skarbowa (KAS) odgrywa kluczową rolę w ochronie szeroko rozumianych interesów Wspólnoty Europejskiej. Jednym z jej podstawowych zadań jest utrzymywanie stałej równowagi pomiędzy potrzebą ochrony społeczeństwa i podmiotów gospodarczych Wspólnoty, a ułatwieniami w obrocie towarowym. Stąd działając w szybko zmieniającym się i pełnym wyzwań środowisku, organy celno-skarbowe muszą być w stanie utrzymać najwyższy poziom usług, świadczonych na rzecz obywateli i podmiotów gospodarczych w Unii Europejskiej. W tym celu stosuje nieinwazyjne metody kontroli, wspo-

magające nadzór oraz usprawniające przepływ towarów i technologii. Wdraża także systemowe rozwiązania doskonalące metody pracy i zapewniające koordynację podejmowanych działań w tej dziedzinie.

Wielkogabarytowe urządzenia RTG w Krajowej Administracji Skarbowej wykorzystywane są do zapewnienia ochrony społeczeństwa, środowiska i rynku, zapewniając możliwość elastycznego reagowania przez Służbę Celno-Skarbową na potrzeby i wyzwania otoczenia, gwarantują nieinwazyjną obsługę ładunków oraz ich nienaruszalność. Powinny również zapewnić bezpieczeństwo, oszczędność czasu i obniżenie kosztów obsługi. Krajowa Administracja Skarbowa znajduje się w światowej czołówce państw stosujących tzw. inteligentne technologie.

Rysunek 1. Mobilne urządzenie RTG Nuctech THSCAN MT1213DE (Gdańsk Port)

Źródło: opracowanie własne

Rentgenowskie systemy inspekcyjne, oprócz tego, że stanowią ważny element prewencyjny, są głównie wykorzystywane przez funkcjonariuszy Krajowej Administracji Skarbowej do:

- sprawdzania zawartości pojazdów, kontenerów, wagonów i innych środków przewozowych,
- weryfikacji list przewozowych z rzeczywistym stanem przetworzonych towarów i wykrywania niezadeklarowanych towarów,
- ujawniania zmian konstrukcyjnych w środkach przewozowych dokonanych w celach przemytniczych oraz niezadeklarowanych towarów,
- zwiększenia zakresu ewentualnych przeszukiwań redukując kontrolę fizyczną, a przy tym skracając znacząco jej czas,

Rysunek 2. Kolejowe urządzenie RTG Rapiscan Eagle R90 (Medyka)

Źródło: opracowanie własne

Pierwszy skaner rentgenowski, mobilny Smiths Silhouette ScanMobile o energii 140 keV umożliwiający penetrację stali do 28 mm pojawił się w ówczesnej Izbie Celnej w Białymstoku w 1997 roku, gdzie „pracował" przez kolejnych 15 lat. Obecnie Służba Celno-Skarbowa dysponuje 196-oma urządzeniami RTG, kilka wybranych przedstawiono na rysunkach 1-3. Obecnie służby celno-skarbowe dysponują 38-oma wielkogabarytowymi urządzeniami RTG do kontroli samochodów ciężarowych/kontenerów/wagonów kolejowych.

Wielkogabarytowe urządzenia RTG w zależności od przeznaczenia i posadowienia, posiadają energię od 300 keV do 9 MeV. Jedenaście urządzeń to skanery „dwuenergetyczne" o podwójnej mocy akceleratora: dwa o energii 9/6 MeV (kolejowe przejścia graniczne w Medyce oraz Terespolu) oraz dziewięć o energii 6/3 MeV. KAS posiada także trzy skanery mobilne typu AS&E Z-Backscatter VAN (ZBV) o energii 225 keV, w których wykorzystuje się tzw. promienie odbite (*backscatter*). Z 38 urządzeń RTG, 12 dostarczyła firma „*Smiths Heimann*", 11 – „*Rapiscan*" (rys.4), 12 – „*Nuctech*", 3 – „*AS&E*". Są one wykorzystywane na drogowych, kolejowych oraz morskich przejściach granicznych na terenie właściwości miejscowej siedmiu Izb Administracji Skarbowej: w Białymstoku, Lublinie, Olsztynie, Gdańsku, Rzeszowie, Zielonej Górze i Szczecinie. W ramach uszczelniania granicy corocznie planuje się instalację kolejnych urządzeń tego typu [Gęsikowski W., Drzewowki M. 2013: 45-47].

Rysunek 3. Kolejowe urządzenie RTG Nuctech RF90 (Terespol)

Źródło: opracowanie własne

Obecnie w ciągu roku średnio w całym kraju za pomocą wielkogabarytowych urządzeń RTG przeprowadzane jest około pół miliona kontroli RTG, w tym około tysiąc kończy się wynikiem pozytywnym. Najczęściej przemycanymi towarami są wyroby tytoniowe, narkotyki, bursztyny, towary niezadeklarowane, nielegalni imigranci,Przy pomocy urządzeń RTG można wykryć także niedozwolone skrytki w przekonstruowanych środkach przewozowych.

Dzięki wykorzystaniu wielkogabarytowych urządzeń RTG możliwe jest znaczne skrócenie czasu kontroli. Funkcjonariusz celno-skarbowy dokonujący analizy obrazu RTG, powinien niezwłocznie po prześwietleniu stwierdzić, czy zachodzi potrzeba przeprowadzenia kontroli manualnej lub użycie psa, czy też dany kontener może zostać zwolniony. Na przejściach granicznych, charakteryzujących się wzmożonym przepływem środków przewozowych, często bywa, że średni czas na podjęcie decyzji to około 3 minuty. W portach morskich w obrębie terminali kontenerowych sytuacja przedstawia się nieco inaczej. Funkcjonariusze zajmujący się interpretacją obrazów mają na podjęcie decyzji, o której mowa powyżej, znacznie więcej czasu, niż ich koledzy na drogowych i promowych przejściach granicznych. Wynika to z faktu, że kontenery, zanim dotrą do portu przeznaczenia, przemierzają zwykle długą drogę morską. Komórki analizy ryzyka, w oparciu o dane zawarte w tzw. „manifestach załadunkowych", które

docierają do nich z odpowiednim wyprzedzeniem oraz na podstawie dostępnych informacji decydują, które kontenery zostaną poddane kontroli celno-skarbowej i w jakim zakresie. Kontener, który został wytypowany do kontroli RTG jest „zatrzymany" w systemie terminala kontenerowego i dopiero po podjęciu wszystkich zaplanowanych wobec niego działań kontrolnych może opuścić terminal. Operatorzy RTG mają więc niemal nieograniczony czas na dokonanie analizy obrazu RTG.

Rysunek 4. Obraz RTG prezentujący mobilne urządzenie RTG (Rapiscan MXR3040) wykonane urządzeniem wyposażonym w podwójną energię (Rapiscan G60)

Źródło: opracowanie własne

W związku z wzrastającą corocznie ilością wielkogabarytowych urządzeń RTG, wykorzystywanych w procesie kontroli celno-skarbowej w 2011 roku ówczesne kierownictwo Służby Celnej powołało Centrum RTG - jednostkę centralną, która zapewnia kompleksową koordynację i monitoring efektywności wykorzystania posiadanych przez KAS urządzeń rentgenowskich, wspomaga procesy zarządzania tym zasobem oraz prowadzi szkolenia dla krajowych i zagranicznych funkcjonariuszy wykonujących zadania z zakresu obsługi urządzeń rentgenowskich i interpretacji obrazów.

Oficjalne otwarcie Krajowego Centrum RTG jako komórki organizacyjnej ówczesnej Izby Celnej w Gdyni, nastąpiło 8 października 2011 roku w Gdańskim Parku Naukowo-Technologicznym. Centrum składa się z:

- Centralnego Repozytorium Obrazów (CRO) - gromadzi obrazy RTG wraz z danymi towarzyszącymi. W oparciu o jego bazę tworzone są specjalistyczne biblioteki materiałów porównawczych, jak również przeprowadzane specjalistyczne analizy tematyczne,
- Centrum Analizy Obrazów (CAO) - zapewnia profesjonalne wsparcie funkcjonariuszom celnym obsługującym urządzenia RTG w procesie decyzyjnym związanym z analizą obrazu, jak również w zakresie analizy zebranych w repozytorium obrazów RTG poprzez dostępne oprogramowanie inspekcyjne

do urządzeń Rapiscan, Nuctech oraz Smiths & Heimann pod kątem szkoleniowo-dydaktycznym,
- Centrum Monitorowania Wykorzystania (CMW) – odpowiada za optymalizację wykorzystania urządzeń skanujących i procesów zarządczych zasobami Służby Celnej oraz kontrolami z wykorzystaniem urządzeń skanujących w skali ogólnokrajowej. Wspólnie z Centrum Analizy Obrazu, zapewnia wsparcie analityczne jednostkom organizacyjnym KAS,
- Centrum Doskonalenia Zawodowego (CDZ) – stanowi swoistą platformą szkoleniową zapewniającą w ramach jednolitego systemu szkoleń właściwe przygotowanie krajowych i zagranicznych funkcjonariuszy celnych w zakresie obsługi urządzeń RTG i interpretacji obrazu.

Z technicznego punktu widzenia operator urządzenia RTG odpowiedzialny za interpretację obrazu RTG może polegać jedynie na własnym doświadczeniu oraz narzędziach obróbki obrazu dostępnych na konkretnym urządzeniu w ramach interfejsu. Póki co nie ma narzędzi automatycznego wskazywania nieprawidłowości w obrazie rentgenowskim, które mogłyby wesprzeć operatora w podejmowaniu decyzji, którego zadaniem jest identyfikować znajdujące się na obrazie obiekty oraz miejsca wymagające kontroli fizycznej.

2. ZASADA DZIAŁANIA URZĄDZEŃ RTG

Badania radiograficzne polegają na prześwietleniu obiektu promieni Rentgena, a następnie zarejestrowaniu na kliszy fotograficznej stopnia absorpcji promenowania przez materiał prześwietlany [Zuev V.M., Kapustin V.I., Karpenko A.I., Van'kowa N.E.: Lipiński T., Szabracki P. 2006: 208-211]. Osłabienie wiązki promieniowania jest opisane równaniem absorbcji Beera [Senczyk D. 2011]:

$$I = I_0 \cdot e^{-\mu x} \tag{1}$$

gdzie: I-natężenie premiowania X po przejściu przez obiekt, I_0 - natężenie premiowania X emitowane ze źródła, μ - liniowy współczynnik absorbcji, x - droga przebyta przez wiązkę promieniowania.

Stopnień naświetlenia kliszy fotograficznej zależy od rodzaju materiału prześwietlanego, natężenia wiązki promieniowania oraz od czasu naświetlania. Wszelkiego rodzaju niejednorodności w spoinie charakteryzują się różnymi współczynnikami absorpcji, co w powoduje różny stopień naświetlenia kliszy fonograficznej. W konsekwencji obserwuje się ciemniejsze obszary w miejscach, gdzie współczynniki absorpcji materiału były mniejsze [Senczyk D. 2011].

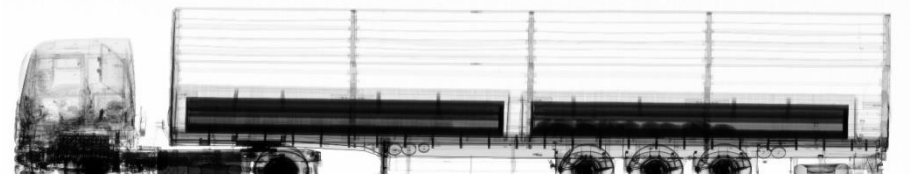
Obecnie zapisu obrazu pochodzącego ze skanera RTG dokonuje się w sposób cyfrowy, a kliszę fotograficzną zastąpiono przetwornikiem CCD. Posiadanie cyfrowych obrazów umożliwia nie tylko ich obejrzenie w powiększeniu, lecz również ich komputerową obróbkę [Gomes J., Velho L. 1997: 91-95].

3. KOMPUTEROWA ANALIZA OBRAZU

Idea komputerowej metody wspomagającej proces analizy obrazów RTG podczas kontroli celno-granicznej polega na wyostrzeniu pewnych elementów obrazu, aby umożliwić kontrolującemu dostrzeżenie anomalii. Standardowy obraz RTG jest obrazem czarnobiałym, w którym poszczególne piksele różnią się od siebie skalą szarości. Jedną z najprostszych metod wyostrzającą anomalia jest zastosowanie progowania. Polega to na ustawieniu odpowiedniego progu wartości nasycenia, a następnie wydzieleniu obszarów, w których występuje duża absorpcja promieniowania. W ten sposób minimalizuje się ilość szczegółów, a wyostrza się pewne obszary. Powoduje to, że łatwiej jest się skupić na dostrzeżeniu anomalii. W celu lepszego zobrazowania anomalii autorzy opracowali kilka metod filtracji i przetwarzania obrazu.

Rysunek 5. Widok samochodu prześwietlonego metodą RTG
a) zdjęcie RTG, b) zdjęcie po binaryzacji.

a)



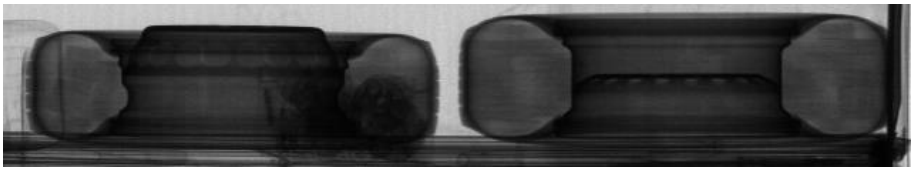
b)

Źródło: opracowanie własne

Na rysunku 5 przedstawiono przykładowe zdjęcie ciężarówki, która przewozi elementy betonowe. W przypadku zdjęcia z rysunku 5a widoczne zaciemnienie miejsca w elemencie ulokowanym z tyłu naczepy może ujść uwadze osobie analizującej to zdjęcie. W przypadku rysunku 5b widać wyraźne anomalia w drugim przewożonym elemencie betonowym. Opisana metoda nie ma na celu przeprowadzenia rozpoznania lub autowykrywania lub zastąpienia człowieka, ma ona jedynie wzbudzić podejrzenie w stosunku do pewnych obszarów, które powinny być dokładniej zbadane.

Rysunek 6. Papierosy ukryte w kole zapasowym ciężarówki
a) zdjęcie RTG b) zdjęcie po binaryzacji.

a)



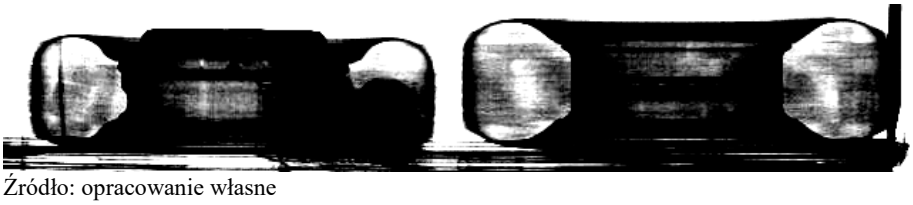
b)

Źródło: opracowanie własne

Innym rozwiązaniem zaproponowanym przez autorów jest progowanie. Zastosowanie progowania niekoniecznie musi ułatwić ocenę. W niektórych przypadkach może wręcz uniemożliwić prawidłową ocenę. Przykładem jest obraz z rysunku 6a, gdzie w kołach zapasowych ukryto papierosy. Na rysunku 6a widać delikatny zarys paczek papierosów ukrytych z oponach koła zapasowego. Zastosowanie progowania spowodowało, że delikatny zarys całkowicie zaniknął (rys. 6.b). Obserwując jedynie obraz z rysunku 6b można stwierdzić, że w kołach zapasowych nie ukryto żadnych przedmiotów.

Niejednokrotnie w celu uwydatnienia pewnych szczegółów wystarczająca jest zmiana kontrastu i nasycenia obserwowanego obrazu (rys.7). W tym przypadku bardzo wyraźnie widać, że we wnętrzu koła zapasowego ukryto jakieś przedmioty.

Rysunek 7. Papierosy ukryte w kole zapasowym ciężarówki po zastosowaniu zmiany kontrastu i nasycenia.



Źródło: opracowanie własne

Autorskim pomysłem jest zastosowanie filtracji RGB dla obrazów będących zapisem skali szarości [Rząsa M., Sowa-Watrak A. 2017: 61-64]. Innym rozwiązaniem jest analiza obrazu z zastosowaniem filtracji RGB. Polega ona na tym, że obraz w skali odcieni szarości przedstawia się w palecie kolorów RGB. Paleta RGB to paleta składająca się z trzech podstawowych kolorów (czerwony,

zielony i niebieski), za pomocą których wyświetlany jest piksel o dowolnym kolorze na obrazie. Intensywność nasycenia poszczególnych barw z palety jest zgodna z modelem YUV. Powoduje to, że każdemu pikselowi wyświetlanemu w skali szarości, są przyporządkowane odpowiednie wartości kolorów (R-read, G-green, B-blue) z palety RGB. A zatem wartość stopnia szarości przy uwzględnieniu, że ludzkie oko jest bardziej wyczulone na kolor zielony, a najmniej na kolor niebieski opisuje zależność:

$$GS = 0.299 \cdot R + 0.587 \cdot G + 0.144 \cdot B \tag{2}$$

gdzie: *GS* - wartość skali szarości, *R, G, B* – wartości nasycenia kolorów *RGB*

Jak wynika z zależności *(2)* posiadając obraz czarnobiały w skali odcieni szarości możliwe jest jego zapisanie w formacie kolorowym RGB. W ten sposób uzyskuje się więcej danych do komputerowej analizy, ponieważ każdy piksel obrazu jest opisany za pomocą trzech wartości odpowiednio dla koloru czerwonego, zielonego i niebieskiego. Stanowi to dodatkową możliwość analizy obrazu z uwzględnieniem jedynie wybranego koloru lub kombinacji dwóch z trzech kolorów. Własność ta umożliwia zastosowania filtrowania z wyodrębnieniem wybranych cech charakterystycznych analizowanego obrazu [Rząsa M., Sowa-Watrak A. 2017: 61-64].

Rysunek 8. Papierosy ukryte w kole zapasowym ciężarówki po zastosowaniu progowania z filtracją RGB

Źródło: opracowanie własne

Obraz ukrytych papierosów w kołach zapasowych ciężarówki po zastosowaniu progowania z filtracją RGB przedstawiono na rysunku 8. W tym przypadku widać wyraźnie, że przestrzeń w oponie koła zapasowego nie jest pusta, lecz jest wypełniona jakimś materiałem. Anomalie w obrazie są w tym przypadku bardzo wyraźnie widoczne.

4. PODSUMOWANIE

Przedstawione w pracy rozwiązanie wspomaga proces analizy obrazów RTG podczas kontroli granicznej. Wspomaganie komputerowe nie ujawnia elementów niewidocznych na zdjęciu RTG, jednak umożliwia ich znaczne wyostrzenie. Jest to o tyle pomocne, że w przypadku kontroli dużej liczby pojazdów na przej-

ściu granicznym analizowanie ledwie widocznych szczegółów zdjęcia RTG ma duży wpływ na zmęczenie osoby sprawdzającej. Osoba zmęczona bardzo łatwo może przeoczyć pewne szczegóły. Zaproponowane rozwiązanie selektywnie wyostrza obraz, powodując, że słabo widoczne elementy na obrazie RTG są dużo bardziej wyraźne. Powoduje to, że osobie sprawdzającej o wiele łatwiej jest dostrzec anomalie oraz zmniejsza zmęczenie podczas pracy. Jak wykazano w niniejszym artykule nie ma uniwersalnej metody, którą można zastosować do wszystkich rodzajów materiałów prześwietlanych. W praktyce bardzo pomocne może być zastosowanie kilku metod, a nawet opracowanie pewnych kombinacji składających się z kilku metod. W przypadku technik komputerowych łatwe jest zautomatyzowanie tego procesu, chociażby poprzez umożliwienie szybkiego wyświetlenia sekwencji zdjęć, w których każde zdjęcie przedstawia ten sam obraz, lecz z zastosowaniem innej metody komputerowego wspomagania analizy obrazu.

Literatura:

[1] Senczyk D.: *Metoda pomiaru współczynnika osłabienia promieniowania rentgenowskiego przez materię*, Stary Młyn, Krajowa Konferencja Badań Radiograficznych, 2011

[2] Rząsa M., Sowa-Watrak A.: *Algorytm analizy obrazu do diagnostyki połączeń spawanych,* Gdańska, Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej Nr 55/ 2017, s.61-64

[3] Drzewowski M., Stefaniak G.*: Systemy RTG do prześwietlania ładunków – nowoczesne i bezpieczne*, Wiadomości Celne Nr 1/2/2014 s. 30-33

[4] Gęsikowski W., Drzewowki M.: *Urządzenia rentgenowskie (RTG) w Służbie Celnej Krajowe Centrum RTG*, Wiadomości Celne Nr 1/2/2013 s. 45 - 47

[5] Gomes J., Velho L.: Image *Processing for Computer Graphics*, Springer Science + Business Media, New York, 1997, s. 91-95

[6] Zuev V.M., Kapustin V.I., Karpenko A.I., Van'kowa N.E.: Lipiński T., Szabracki P.: *X-ray testing and engineering diagnostics*, Russian Journal of Nondestructive Testing, March 2006, Volume 42, Issue 3, s. 208–211

dr hab. inż. Prof. PO Mariusz R. Rząsa
Politechnika Opolska
Wydział Mechaniczny (Katedra Techniki Cieplnej i Aparatury Przemysłowej)
45-271 Opole, ul. Mikołajczyka 5
e-mail m.rzasa@po.opole.pl

Młodszy Ekspert Służby Celno-Skarbowej Wojciech Gęsikowski
Izba Administracji Skarbowej w Gdańsku
Centrum RTG
80-172 Gdańska, ul. Trzy lipy 3
e-mail wojciech.gesikowski@gdy.mofnet.gov.pl

POLITECHNIKA OPOLSKA

ISSN 2353-8899