EUROPEJSKI INSTYTUT
BEZPIECZEŃSTWA WEWNĘTRZNEGO

Nowoczesne technologie na rzecz bezpieczeństwa

praca zbiorowa
redakcja naukowa – dr hab. Wojciech Filipkowski

Gdynia 2015

Recenzent:
dr hab. Grzegorz Krasnodębski

Redakcja naukowa:
dr hab. Wojciech Filipkowski

Redakcja techniczna, opracowanie graficzne, skład, projekt okładki:
Paweł Domański, Bartłomiej Pączek

ISBN: 978-83-941308-7-9

Wydawca:
Wydawnictwo BP
tel. +48 887 021 030
e-mail: bartlomiej@paczek.eu

Współwydawcy:
Akademia Marynarki Wojennej
Wydział Dowodzenia i Operacji Morskich
www.amw.gdynia.pl

Europejski Instytut Bezpieczeństwa Wewnętrznego
ww.eibw.org

SPIS TREŚCI

dr hab. Wojciech FILIPKOWSKI
Dyrektor ds. naukowych
Europejski Instytut Bezpieczeństwa Wewnętrznego

WPROWADZENIE

Europejski Instytut Bezpieczeństwa Wewnętrznego (EIBW) został powołany do życia w dniu 13 lutego 2014 r., kiedy to została podpisana stosowna deklaracja przez wybrane osoby prawne[1]. Swoją siedzibę ma w Gdańskim Parku Naukowo Technologicznym im. Profesora Hilarego Koprowskiego[2]. Idea leżąca u jego podstaw oraz miejsce jego funkcjonowania zdecydowały, że został on powołany w formie otwartego klastra przedsiębiorców. Zrzesza przede wszystkim podmioty gospodarcze zainteresowane rozwojem technologii w obszarze bezpieczeństwa, ale także instytucje badawcze, instytuty, podmioty sektora publicznego oraz instytucje otoczenia biznesu. Koordynatorem klastra została spółka kapitałowa prawa handlowego EIBW sp. z o.o., która w aktywny sposób już od wielu lat angażuje się w działalność B+R poprzez realizację projektów badawczych i wdrożeniowych.

Pierwszymi sygnatariuszami porozumienia byli:

- Microsystem sp. z o.o.[3];
- Muzeum Historyczne Miasta Gdańska[4];
- Pomorskie Centrum Przetwarzania Danych sp. z o.o.[5];
- Fido Intelligence sp. z o.o.[6];
- Symona Group sp. z o.o.[7];
- Kancelaria Adwokacka Janusz Kaczmarek[8];
- Akademia Marynarki Wojennej im. Bohaterów Westerplatte w Gdyni[9];

1 Oficjalna strona internetowa: http://www.eibw.org/ oraz konto na Twitterze: @EuInstBW.
2 Oficjalna storna internetowa: http://www.gpnt.pl/.
3 Oficjalna storna internetowa: http://www.microsystem.com.pl/.
4 Oficjalna storna internetowa: http://www.mhmg.pl/.
5 Oficjalna storna internetowa: http://www.pcpd.pl/.
6 Oficjalna storna internetowa: http://fidointelligence.pl/.
7 Oficjalna storna internetowa: http://symonagroup.eu/.
8 Oficjalna storna internetowa: http://janusz-kaczmarek.pl.
9 Oficjalna storna internetowa: http://www.amw.gdynia.pl/.

- DGT sp. z o.o.[10];
- Gesit sp. z o.o.[11];
- Laboratorium Przetwarzania Obrazu i Dźwięku sp. z o.o.[12].

Forma klastra daje szansę równego wpływu wszystkich zrzeszonych w nim podmiotów na kierunki rozwoju EIBW, a także koniecznością samofinansowania się instytutu. Natomiast przejrzyste zasady uczestniczenia w nim oraz wewnętrzna polityka rozgraniczania interesu indywidualnych partnerów oraz interesu samego EIBW zapewnia tę względną samodzielność i niezależność.

EIBW stanowi efektywne połączenie i wykorzystanie potencjału przedsiębiorców, instytucji otoczenia biznesu, jednostek naukowo-badawczych, uczelni wyższych, organizacji pozarządowych, osób indywidualnych – w celu wprowadzenia na rynek wyników badań na rzecz bezpieczeństwa, a także budowania i promowania gospodarki opartej na wiedzy. U podstaw jego działań przyjęto założenie, wedle którego gospodarka winna wykorzystywać w sposób maksymalny innowacyjność opartą na szeroko zakrojonych badaniach naukowych – zwłaszcza w tzw. wschodzących dziedzinach nauki. Natomiast w ramach współpracy z jednostkami państwowymi działającymi na rzecz poprawy bezpieczeństwa, uczelniami wyższymi oraz przedsiębiorcami, tworzymy płaszczyznę dla powstawania oraz wdrażania także produktów podwójnego zastosowania (*dual-use*).

EIBW w swoich pracach specjalizuje się w obszarze bezpieczeństwa IT, telekomunikacyjnego, energetycznego, *business intelligence, open source intelligence* oraz szeroko rozumianego bezpieczeństwa i porządku publicznego. Kluczowymi dla niego są zagadnienia związane ze zjawiskami przestępczości zorganizowanej, terroryzmu (w tym cyberterroryzmu), bezpieczeństwa państwa, podmiotów gospodarczych i obywateli, zarządzania kryzysowego. W jego ramach prowadzone są badania interdyscyplinarne, obejmujące wspólne zainteresowania technologii, prawa, kryminologii, kryminalistyki.

W ocenie wielu ekspertów jednym z największych wyzwań polskiej nauki i gospodarki jest komercyjne wykorzystanie wyników badań, celem podniesienia konkurencyjności oferowanych towarów i usług poprzez wdrażanie opracowywanych innowacji. Dotyczy to także sektora bezpieczeństwa polskiej gospodarki. Zwłaszcza, że szereg technologii opracowanych na potrzeby organów państwowych – po odpowiedniej adaptacji – może mieć zastosowanie przez sektor prywatny (tzw. technologie *dual-use*). Jednakże w swoich działaniach nie ograniczamy się do tego wąskiego rozumienia tego pojęcia. Zakładamy, że możliwe jest wykorzystanie nowo powstających technologii (zwłaszcza

[10] Oficjalna storna internetowa: http://www.dgt.pl.
[11] Oficjalna storna internetowa: http://www.gesit.pl.
[12] Oficjalna storna internetowa: http://lpod.pl/.

informacyjnych) na rzecz zapewnienia bezpieczeństwa państwa i jego obywateli oraz porządku publicznego. Przygotowane przez nas spotkania udowadniają, że transfer wiedzy i technologii jest możliwy w obu kierunkach. Innymi słowy są takie technologie i rozwiązania, które to mogą być wykorzystywane dla naszego wspólnego dobra – w jednakowy sposób – zarówno przez sektor prywatny, jak i publiczny. Tytułem przykładu, można w tym zakresie wymienić następujące konferencje, seminaria i spotkania:

- seminarium zorganizowane w dniu 28 kwietnia 2015 r. przez Laboratorium Przetwarzania Dźwięku i Obrazu pt.: „Współpraca polsko-niemiecka w zakresie innowacji - szanse i możliwości" z udziałem przedstawicieli Instytutu Fraunhofera;
- konferencja pt. „Nowoczesne technologie w łączności na rzecz rozwoju inteligentnych miast" (10-11 marca 2015 r.)[13];
- seminarium EIBW pt. „Nowoczesne technologie na rzecz bezpieczeństwa. Zagadnienia dual-use", które odbyło się przy okazji Konferencji Rozwoju, Przedsiębiorczości i Innowacji „VENTURE DAY 2014" (20 listopada 2014 r.);
- IV Konferencja Naukowa Bezpieczeństwa i Obronności Security & Defence zorganizowana przez Wydział Dowodzenia i Operacji Morskich Morskiego Akademii Marynarki Wojennej oraz Koło Naukowe Bezpieczeństwa we współpracy z EIBW (13 – 14 maja 2014 r.)[14].

Efektem powyższych działań są przygotowane opracowania, które znalazły się w niniejszej pracy zbiorowej. Część z nich powstała na potrzeby poszczególnych naszych konferencji, seminariów i spotkań, ale znajdują się tutaj także inne opracowania inspirowane tematem zastosowania technologii *dual-use* z punktu widzenia różnych obszarach wiedzy. Często podkreślamy w swoich wystąpieniach, że nie tylko rozwój samych technologii jest istotny, ale także kontekst prawny, kryminalistyczny i kryminologiczny ich stosowania. Dotykamy takich kwestii jak dopuszczalność stosowania, a nawet możliwość prowadzenia badań nad niektórymi technologiami, możliwościami ich wykorzystania przez sektor publiczny i prywatny, a także ich skutecznością, przydatności. Analizy powinny także dotykać kwestii możliwych potencjalnych nadużyć w tym zakresie i jednocześnie sposób ochrony społecznie aprobowanych dóbr prawnych.

[13] Zob. http://www.eibw.org/news-konferencja-nowoczesne-technologie-w-cznoci-na-rzecz-rozwoju-inteligentnych-miast,87.html.

[14] Zob. http://www.eibw.org/news-iv-konferencja-naukowa-bezpieczestwa-i-obronnoci-security-defence-wspczesne-uwarunkowania-bezpieczestwa-europejskiego,70.html.

W niniejszej pracy zbiorowej zamieszczono dziewięć opracowań uporządkowanych alfabetycznie według nazwisk ich autorów. Taki układ był podyktowany przede wszystkim różnorodnością prezentowanych tematów.

Pierwsze z opracowań opublikowanych w niniejszej pracy zbiorowej, autorstwa M. Ceremugi, M. Maziejuka, R. Jóźwika oraz A. Zalewskiej, nosi tytuł „Zastosowanie różnicowej spektrometrii ruchliwości jonów DMS do detekcji par wybranych związków chemicznych". Autorzy zaprezentowali zastosowanie tytułowej metody w obszarze zapewnienia bezpieczeństwa i porządku publicznego. Pozwala ona na wykrywanie nawet śladowych ilości szerokiej gamy związków chemicznych, w tym gazów bojowych, materiałów wybuchowych, narkotyków. Ponadto metodę można zaimplementować w postaci urządzenia mobilnego, co zwiększa zakres jej zastosowania. Opracowanie zawiera także część empiryczną zawierającą wyniki badań uzyskanych w wyniku zatasowania opisywanej metody.

A. Czyżewski, A. Korzeniewski, P. Odya oraz P. Szczuko przygotowali opracowanie pt. „Metody badania oddziaływania przydrożnych reklam na kierowców z zastosowaniem technologii multimedialnej". Zawiera ono założenie systemu multimedialnego pozwalającego na ocenę zagrożeń wynikających z obecności reklam w obrębie dróg. Po jego wdrożeniu możliwe będzie podniesienie poziomu bezpieczeństwa w ruchu drogowym, gdyż dostarczy on wiarygodnych danych i informacji o tym, jak statyczne i dynamiczne reklamy w pasie ruchu drogowego mają wpływ na kierowców, a tym samym na ilość wypadków i kolizji. W konsekwencji może to prowadzić do zaproponowania zmian w regulacjach prawnych odnoszących się do bezpieczeństwa w ruchu drogowym, czy też prawie budowlanym.

S. Gajewski, M. Gajewska oraz R. Katulski są autorami opracowania pt. „Nowoczesne rozwiązania trankingowe na potrzeby służb – system LTE". Autorzy przedstawili w sposób szczegółowy rozwiązania systemów trankingowych-dyspozytorskich opartych na systemie LTE. Podkreślono efektywność dla organów państwowych rozwiązania w postaci odrębnego systemu trankingowego LTE/TDD pracującego w oparciu o infrastrukturę publicznych sieci komórkowych. Nikt nie kwestionuje znaczenia przesyłania danych i informacji w sytuacjach kryzysowych, ale także codziennej pracy tychże organów. Autorzy proponują rozwiązanie służące usprawnieniu tego procesu. Nawiązują także do kwestii integracji swojego rozwiązani z systemem TETRA oraz dalszej ewolucji systemów bezpiecznej komunikacji na potrzeby organów państwowych.

J. Grubicka w opracowaniu pt. „Konwergencja technologiczna a system bezpieczeństwa informacji" zaprezentowała szereg zagadnień związanych z dostępem i ochroną danych i informacji we współczesnym świecie. Skupiła się w szczególności nad kwestiami zabezpieczeń i szyfrowania danych podczas transmisji w sieciach Wi-Fi np. w sieciach domowych, czy też przedsiębiorstw. Czasem nawet najprostsze rozwiązania mogą stanowić pierwszy próg do sfor-

sowania przez osoby, które chciałyby wykorzystać taką sieć do celów niezgodnych z prawem.

K. Kocur-Bera oraz M. Dudzińska są autorkami opracowania zatytułowanego „Zarządzanie geoinformacją na potrzeby związane z bezpieczeństwem przestrzeni". Jest to jedno z najbardziej dynamicznie rozwijających się współcześnie rozwiązań technologicznych znajdujących swoje zastosowanie w co raz to nowych obszarach. Jednym z nich jest zapewnienie bezpieczeństwa. Autorki dokonały prezentacji potencjalnych źródeł danych i informacji. Ponadto wskazały na możliwości jakie daje tworzenie na ich podstawie map zagrożeń lub ryzyka, które mogą być wykorzystane w sytuacjach kryzysowych celem zapewnienia bezpieczeństwa i porządku publicznego.

E. Kowalewska – Borys oraz D. Dajnowicz przygotowały opracowanie o charakterze prawniczym pt. „Udostępnianie danych billingowych jako obowiązek firm telekomunikacyjnych w zakresie umożliwiania kontroli operacyjnej. Jest to jedno z opracowań w niniejszym zbiorze, które zajmuje się prezentacją kwestii prawnych. W tym przypadku poruszane są kwestie z zakresie obowiązków firm telekomunikacyjnych w zakresie udostępniania określonych kategorii danych o swoich klientach stosownym organom państwowym. Problemem nie jest w przypadku rozwiązanie technologiczne, ale prawne ustanawiające ramy dopuszczalności oraz zakresu przekazywania tego typu danych na potrzeby czynności operacyjno-rozpoznawczych i procesowych.

Autorzy M. Sokół, A. Meksuła, M. Sokół, W. Kamiński w swoim opracowaniu pt. „Techniki rozszerzonej rzeczywistości i ich zastosowanie w systemach klasy dual-use" zawarli szereg rozważań o charakterze teoretycznym oraz praktycznym odnoszących się do zagadnień łączenia elementów wirtualnych z rzeczywistymi. Szczególnie interesująco przestawia się autorskie rozwiązanie wielodotykowego wyświetlacza holograficznego 3D. Może on znaleźć szereg zastosowań praktycznych w sferze militarnej oraz cywilnej, np. w meteorologii, architekturze, komunikacji, logistyce, nawigacji, hydrologii, robotyce, biomechanice, geologii, ekologii, reklamie i marketingu, a także w edukacji i rozrywce. Jednocześnie należy podkreślić, iż nie jest to rozwiązanie futurystyczne, gdyż już w chwili obecnej są możliwości pozwalające na wdrażanie w życie tych śmiałych zamierzeń. W pracy przedstawiono ogólną koncepcję systemów rozszerzonej rzeczywistości i technik łączących w sobie elementy świata realnego oraz tzw. rzeczywistości wirtualnej. W sposób szczególny praca została poświęcona wyświetlaczom holograficznym 3D, które mogą znaleźć szerokie zastosowanie m.in. w systemach klasy dual-use. W artykule wskazano także kilka przykładów praktycznych zastosowań wielodotykowego wyświetlacza holograficznego 3D, który powstaje obecnie w Laboratorium Przetwarzania Obrazu i Dźwięku Sp. z o.o. Wyświetlacz holograficzny 3D, opracowywany obecnie przez LPOD, zapewni wyświetlanie realistycznego obrazu i interaktywnego interfejsu bez potrzeby używania specjalnych okularów lub hełmów.

P. Szczuko jest autorem opracowania pt. „Monitoring i poszanowanie prywatności – nowa metoda anonimizacji danych wizyjnych". Stanowi ono przykład jak kwestie technologiczne i prawnicze wchodzą ze sobą w interakcję. Autor przedstawia opracowaną przez siebie koncepcję pseudonimizacji danych wizyjnych. Polega ona na automatycznym zastępowaniu sylwetek osób wirtualnymi postaciami, naśladującymi realnie wykonywane czynności. Takie rozwiązanie chroni wizerunek osób, a tym samym ich prywatność wszędzie tam, gdzie dla prawidłowego wykonywania czynności związanych z bezpieczeństwem i porządkiem publicznym nie jest konieczne ustalanie tożsamości danej osoby.

M. Zachara w swoim opracowaniu pt. „Identyfikacja nietypowych zapytań do serwisów www" przedstawia autorską koncepcję metody ochrony serwisów internetowych. Opiera się ona na identyfikacji typowych i nietypowych wzorców zachowań ich użytkowników. Jest to tematyka bardzo aktualna i stale goszcząca na łamach prasy fachowej, gdyż nasze społeczeństwo w różnych obszarach swojej aktywności polega na dostępie do informacji poprzez internet. Przedstawiona została metoda modelowania zachowań użytkowników za pomocą grafu, a także zaproponowano rozwiązanie opierające się na współpracy grupy serwerów w celu dzielenia się informacjami i zbiorowej detekcji niebezpiecznych zachowań. Autor nie tylko zaprojektował, ale także zaimplementował prototyp swojego systemu. W ramach podsumowania odniósł się do wniosków płynących z analizy jego funkcjonowania.

Szczególnym obszarem zainteresowań wszystkich Autorów jest co prawda bezpieczeństwo i porządek publiczny, ale nic nie stoi na przeszkodzie, aby rozszerzyć badania o inne obszary wiedzy i gospodarki. Oddając niniejszą pracę zbiorową w ręce czytelników, mamy nadzieję sprowokować dyskusję nad pojęciem technologie *dual-use* oraz możliwościami, jakie niosą ze sobą dla sektora prywatnego i publicznego.

**Michał CEREMUGA, Mirosław MAZIEJUK,
Roman JÓŹWIK, Anna ZALEWSKA**
Wojskowy Instytut Chemii i Radiometrii

ZASTOSOWANIE RÓŻNICOWEJ SPEKTROMETRII RUCHLIWOŚCI JONÓW DMS DO DETEKCJI PAR WYBRANYCH ZWIĄZKÓW CHEMICZNYCH

WPROWADZENIE

Do najczęściej stosowanych metod służących do detekcji substancji w ilościach śladowych należą techniki oparte o zjawisko ruchliwości jonów (ang*. Ion mobility spectrometry* – IMS i *High-field Asymmetric Waveform Ion Mobility Spectrometry – FAIMS*). Metoda różnicowej spektrometrii ruchliwości jonów (DMS) wywodząca się z FAIMS stwarza możliwość wysokoczułej detekcji par wielu związków chemicznych za pomocą mobilnych urządzeń skriningowych. W Wojskowym Instytucie Chemii i Radiometrii skonstruowany został spektrometr DMS, który znajduje zastosowanie w wykrywaniu związków chemicznych w medium gazowym. Jego wysokie parametry detekcyjne pozwalają na detekcję gazów bojowych na poziomie dziesiętnych części ppb, a możliwość równoczesnej detekcji jonów dodatnich i ujemnych pochodzących od zjonizowanej próbki analitu znacznie zwiększa jego możliwości aplikacyjne, co zostało potwierdzone za pomocą licznych prób eksperymentalnych.

RÓŻNICOWA SPEKTROMETRIA RUCHLIWOŚCI JONÓW

Różnicowa spektrometria ruchliwości jonów (*ang. Differential Ion Mobility Spectrometry, DMS*) należy do grupy metod opartych o zjawisko ruchliwości jonów i może być wykorzystana w przenośnych urządzeniach skriningowych, w celu umożliwienia wysokoczułej detekcji szerokiej gamy związków chemicznych, a przede wszystkim gazów bojowych, materiałów wybuchowych, lotnych związków organicznych jak i narkotyków. Możliwości detekcyjne aparatów wykorzystujących metodę DMS opierają się na występowaniu różnic w ruchliwościach jonów (K) w zmiennym polu elektrycznym zgodnie z zależnością opisaną wzorem [1]:

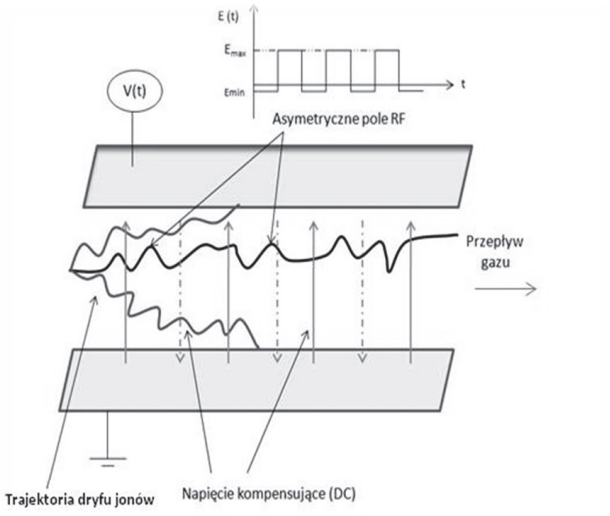
$$K(E/N) = K_0 \cdot [1 + \alpha(E/N)]$$

gdzie:

K – ruchliwość jonu, $cm^2/(V \cdot s)$,
E – natężenie pola elektrycznego, V/cm,
K_0 – ruchliwość zredukowana jonów dla słabego pola elektrycznego, $cm^2/(V \cdot s)$,
N – ilość molekuł gazu w objętości 1 cm^3, E/N – nazywane jest liczbą Towendsa Td i wyraża wielkość natężenia pola do ilości molekuł gazu w objętości 1 cm^3 (1 Td = $1 \cdot 10^{-17}$ $V \cdot cm^2$),
α(E/N) – zależność zmiany ruchliwości zredukowanej w funkcji natężenia pola elektrycznego i gęstości molekularnej,
K(E/N) – ruchliwość jonów w zależności od liczby Towendsa.

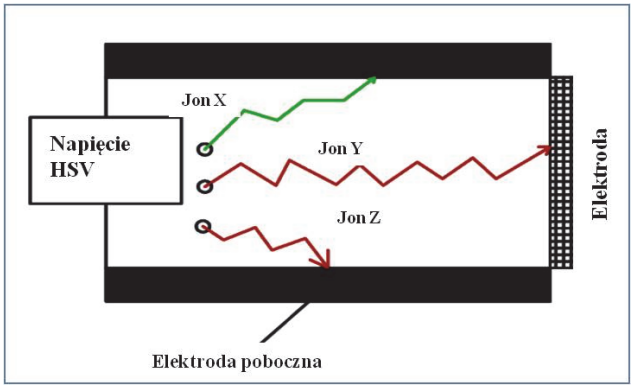
Zwiększanie pola elektrycznego (DMS) do kilkunastu kV/cm prowadzi do nieliniowości, w wyniku czego ruchliwość jonów zmienia się w funkcji pola elektrycznego. Charakter tych zmian jest zależny m.in. od rodzaju jonów, ich masy, kształtu oraz ich temperatury efektywnej. Ruchliwość jonów jest w tym przypadku zależna od E oraz od liczby cząsteczek gazu (N) i można ją przedstawić w postaci funkcji K (E/N).

Wysokie i asymetryczne napięcie (HSV lub RF) przyłożone jest prostopadle do kierunku gazu stanowiąc tym samym pole separacyjne (Rys. 1).

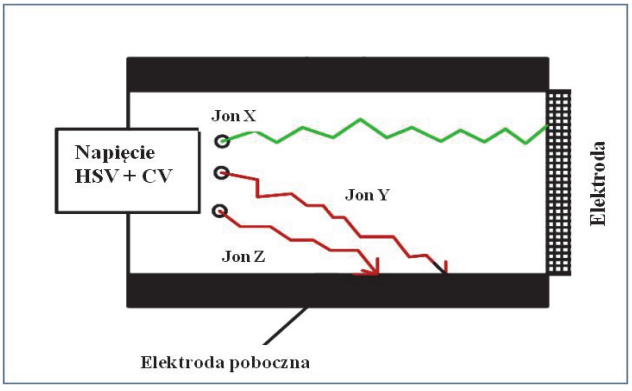


Rys. 1. Diagram przedstawiający trajektorię dryfu jonów w metodzie DMS [2]

Pod jego wpływem ruchliwości jonów stają się zależne od natężenia pola elektrycznego co wcale nie determinuje detekcji badanego analitu. Wysokie napięcie powoduje zmianę trajektorii dryfu jonów w wyniku czego uderzają one w elektrody poboczne i ulegają neutralizacji. W takim przypadku ich detekcja jest niemożliwa. Możliwość „wychwytu" (wykrycia) jonów przez elektrodę może nastąpić poprzez przyłożenie różnych napięć kompensujących (CV, ang. *Compensation Voltage*), co uwidocznione zostało „ideowo" na schematach jako tory różnych jonów (x, y, z), a w praktyce odzwierciedla się w ilości i położeniu pików sygnałów alarmowych na skali sygnalizacji aparatu (Rys. 2 i 3).



Rys. 2. Dryf jonów w zmiennym polu elektrycznym [2]



Rys. 3. Dryf jonów w zmiennym polu elektrycznym
i przyłożonym napięciu kompensującym CV [2]

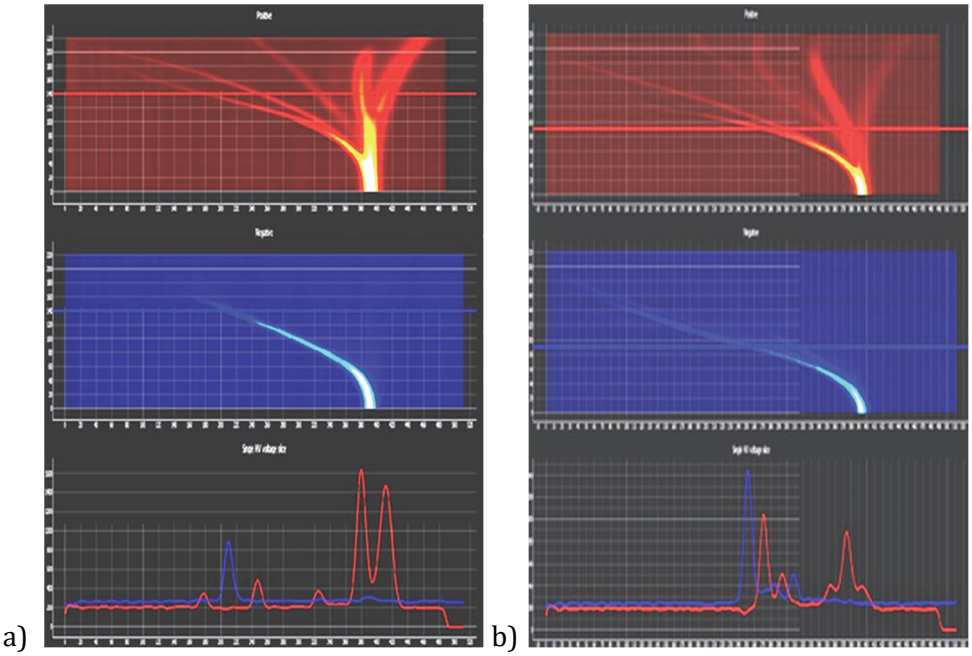
Pod wpływem przyłożonego napięcia kompensującego jon X, który wcześniej nie był wykrywany (Rys. 2), dociera do elektrody pomiarowej i jest rejestrowany dla wartości napięcia kompensującego CV (Rys. 3). W tym przypadku jony Y i Z neutralizują się na ściankach i nie są wykrywane [1-5].

Podsumowując przedstawioną krótką charakterystykę można stwierdzić, że metoda DMS oparta jest na występowaniu różnej zależności ruchliwości jonów (K) przy różnych natężeniach pola elektrycznego (E). Jest więc metodą wykorzystującą wyznaczone drogą doświadczalną charakterystyki i umożliwiającą w ten sposób wykrywanie par na bardzo wysokim poziomie czułości.

PRZYRZĄD ROZPOZNANIA SKAŻEŃ

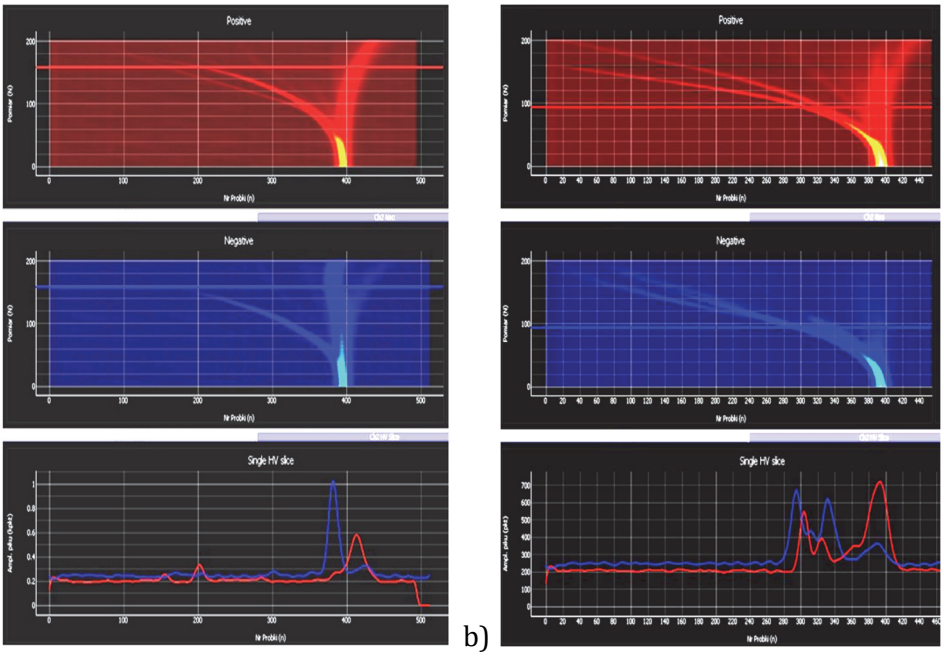
Szeroka gama metod służących wykrywaniu śladowych ilości związków chemicznych pozwoliła na stworzenie różnych systemów detekcyjnych, które powinny spełniać szereg wymagań, aby znalazły szersze zastosowanie jako przenośne aparaty skriningowe. Najważniejsze z nich to: rozmiar, mobilność, próg czułości, sposób pobierania próbki, zakres wykrywanych związków, czas analizy, cena. W Wojskowym Instytucie Chemii i Radiometrii wykonano urządzenie dedykowane wykrywaniu bojowych środków trujących (*Przyrząd Rozpoznania Skażeń, PRS-1*), które wykorzystuje metodę DMS. Innowacyjne rozwiązania zastosowane w tym urządzeniu powodują, że parametry techniczne takiego przyrządu są bardzo wysokie – jedne z najlepszych na świecie. Detektor ten umożliwia wykrywanie skażeń chemicznych na bardzo niskim poziomie stężeń przy zachowaniu bardzo krótkiego czasu detekcji. Wstępne prace badawcze wykazały przydatność tego urządzenia nie tylko do detekcji bojowych środków trujących ale także materiałów wybuchowych czy narkotyków. Zdefiniowano także model symulacyjny za pomocą którego można określić optymalne warunki pracy spektrometru. Sygnalizator skażeń chemicznych PRS-1 umożliwia detekcję i identyfikację gazów na podstawie analizy rejestrowanych charakterystycznych spektrogramów, a opracowany opis matematyczny usprawnia proces identyfikacji wykrywanej substancji.

Poniżej przedstawiono przykładowe spektrogramy otrzymane podczas detekcji gazów bojowych, materiałów wybuchowych oraz substancji psychoaktywnych, narkotyków (Rys. 4-6).



Rys. 4. Spektrogram dla: a) somanu, b) tabunu

Otrzymywane w trakcie badań spektrogramy składają się z trzech części. Pierwsza oznaczona kolorem czerwonym stanowi widmo dla jonów dodatnich w całym zakresie napięcia asymetrycznego HSV, druga (kolor niebieski) odpowiada jonom ujemnym, a trzecia przedstawia piki jonów dodatnich i ujemnych otrzymane dla wybranej wartości napięcia HSV. Analizując powyższe spektrogramy można zauważyć występowanie charakterystycznych sygnałów w trybie jonów dodatnich dla obydwu analitów, jednakże różnią się one wartościami napięcia kompensującego, a więc znajdują się w innym położeniu na skali spektrogramu. W przypadku materiałów wybuchowych otrzymywane są sygnały charakterystyczne zarówno w trybie jonów dodatnich jak i ujemnych, co można zaobserwować na poniższych spektrogramach (Rys. 5).

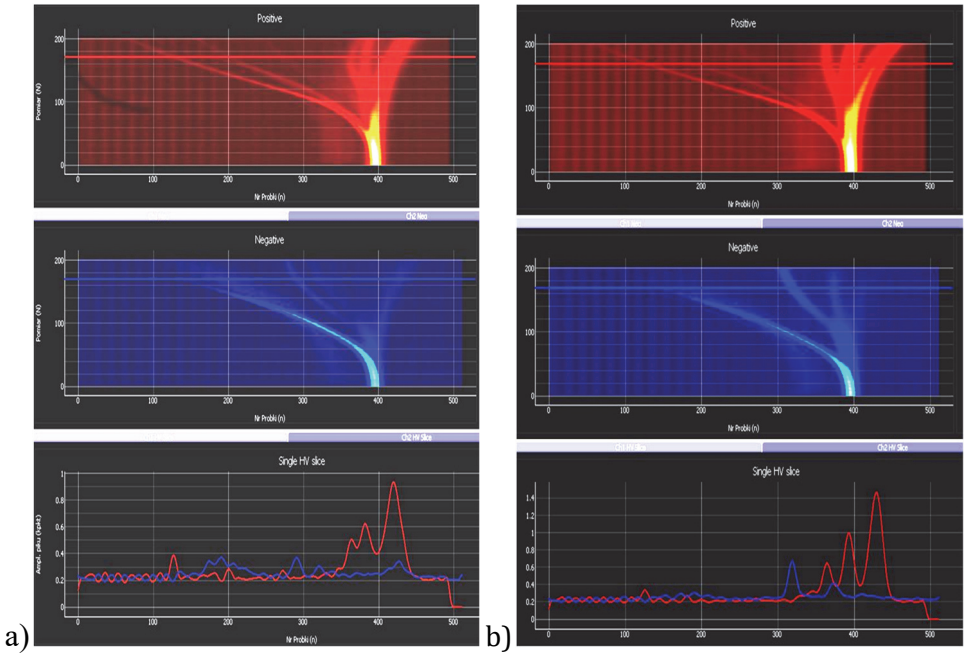


a) b)

Rys. 5. Spektrogram dla: a) trotylu, b) heksogenu

W przypadku trotylu i heksogenu (Rys. 5) widoczne są piki zarówno w trybie jonów dodatnich jak i ujemnych. Dla TNT początkowo dla napięcia 600 V można zaobserwować po dwa piki dodatnie i ujemne, z których jednym jest RIP (ang. Reactant Ion Peak). Wraz ze wzrostem napięcia następuje zanik RIP oraz rozdzielenie pików charakterystycznych dla 2,4,6-TNT (780V HSV).

Przyrząd PRS-1 wykorzystujący w swoim działaniu metodę DMS powinien umożliwiać detekcję szerokiej gamy lotnych związków chemicznych i dlatego też podjęto się prób wykrycia par związków o działaniu psychoaktywnym i narkotycznym. Poniżej umieszczono przykładowe spektrogramy otrzymane podczas detekcji par mefedronu i amfetaminy (Rys. 6).



Rys. 6. Spektrogram dla: a) mefedronu, b) amfetaminy

Analizując powyższe spektrogramy można zauważyć, że w obu przypadkach uzyskano sygnały charakterystyczne w trybie jonów dodatnich w postaci trzech dobrze rozdzielonych pików. Jednakże cechują się one inną amplitudą i przy napięciu 945 V HSV posiadają inna charakterystykę. Dodatkowo należy podkreślić, iż w przypadku amfetaminy widoczne są również sygnały w trybie jonów ujemnych, które nie występują w przypadku mefedronu.

PODSUMOWANIE

Różnicowa spektrometria ruchliwości jonów (DMS) może być wykorzystana w przenośnych urządzeniach skriningowych, w celu umożliwienia wysokoczułej detekcji wielu związków chemicznych, a przede wszystkim gazów bojowych, materiałów wybuchowych jak i narkotyków. Spektrometr PRS-1 opracowany i wykonany w Wojskowym Instytucie Chemii i Radiometrii stanowi innowacyjne rozwiązanie i umożliwia równoczesną detekcję w trybie jonów dodatnich i ujemnych, co zapewnia zwiększenie liczby wykrywanych związków chemicznych i poprawę selektywności. Otrzymane spektrogramy różnią się między sobą i umożliwiają wyodrębnienie pików i punktów charakterystycznych dla danego analitu, a dodatkowo świadczą o szerokich możliwościach de-

tekcyjnych urządzenia i otwierają drogę do podjęcia prac mających na celu umożliwienie skutecznej identyfikacji i eliminację sygnałów pozytywnie fałszywych. Przedstawione w niniejszej pracy wyniki badań wskazują, iż jest możliwa detekcja nie tylko gazów bojowych, ale również materiałów wybuchowych, substancji psychoaktywnych czy innych lotnych związków organicznych spektrometrem PRS-1, jednakże niezbędne jest wykonanie prac dostosowujących aparat do specyfiki danej grupy związków.

LITERATURA

[1] Shvartsburg A.A., *Differential Ion Mobility Spectrometry: Nonlinear Ion Transport and Fundamentals of FAIMS*, CRC Press, 299, 2008.

[2] Zalewska A., Innovative screening device for high-sensitive chemical vapors detection, *EYEC Monograph, Edition*: 4, Warsaw University of Technology, Faculty of Chemical and Process Engineering, 194-206, 2015.

[3] Buryakov I.A., Krylov E.V., Nazarov E.G., Rasulev U.K., A new method of separation of multi-atomic ions by mobility at atmospheric pressure using a high-frequency amplitude-asymmetric strong electric field, *International Journal of Mass Spectrometry and Ion Processes*, 128, 3, 143–148, 1993.

[4] Borsdorf H., Mater T., Electric field dependence of ion mobilities of aromatic compounds with different ionic mass and different functional groups, *International Journal for Ion Mobility Spectrometry*, 13, 103–108, 2010.

[5] Eiceman G.A., Karpas Z., Ion Mobility Spectrometry, Second Edition, *Taylor & Francis Groupz*, 2005.

A. CZYŻEWSKI, A. KORZENIEWSKI, P. ODYA, P. SZCZUKO
Politechnika Gdańska,
Wydział Elektroniki, Telekomunikacji i Informatyki,
Katedra Systemów Multimedialnych

METODY BADANIA ODDZIAŁYWANIA PRZYDROŻNYCH REKLAM NA KIEROWCÓW Z ZASTOSOWANIEM TECHNOLOGII MULTIMEDIALNEJ

STRESZCZENIE

Istotnym problemem z punktu widzenia bezpieczeństwa ruchu drogowego jest właściwa lokalizacja reklam statycznych i dynamicznych w otoczeniu pasa drogowego. Celem niniejszej publikacji, nakierowanym na wspomaganie rozwiązywania wynikających z tego tytułu problemów, jest przedstawienie zakresu możliwych do wykonania, szeroko zakrojonych, wielopłaszczyznowych badań, wykorzystujących nowoczesne rozwiązania technologiczne, pozwalające na obiektywną ocenę zagrożeń wynikających z obecności reklam w obrębie dróg. Jako narzędzia badawcze zostały zaproponowane systemy śledzenia reakcji kierowców, oparte na wykorzystaniu zaawansowanej technologii multimedialnej. Systemy te mogą zostać zintegrowane w rzeczywistym pojeździe, umożliwiając badania w warunkach rzeczywistych lub jako element rozbudowanego symulatora jazdy. Ponadto elementem proponowanych badań jest sprawdzenie opinii kierowców z użyciem ankietyzacji oraz analiza wypadkowości w ruchu drogowym odbywającym się w sąsiedztwie reklam drogowych.

Słowa kluczowe:
reklamy, tablica reklamowa, drogi, bezpieczeństwo ruchu drogowego

WSTĘP

Brak odpowiednio szczegółowych zaleceń i przepisów regulujących problem lokalizacji reklam statycznych i dynamicznych w pasie drogowym i w bezpośrednim jego sąsiedztwie w kontekście bezpieczeństwa ruchu drogowego, to istotny problem zarządów dróg. Sytuacja ta może być ponadto źródłem potencjalnych problemów we współpracy z firmami zarządzającymi tego typu nośnikami reklamowymi, a w określonych sytuacjach może ponadto wpływać na ruch pojazdów. Obecne regulacje, m.in. Ustawa o drogach publicznych. art 42, 43 są zbyt ogólne i zwykle nie są przestrzegane. Szczególnie istotne z punku widzenia opisywanych badań są ustalenia Konwencji Wiedeńskiej o ruchu drogowym z dnia 8 listopada 1968 roku, ratyfikowanej przez Państwo Polskie 24 lutego 1988 roku. Artykuł 4, ustęp d, punkt ii tej Konwencji dotyczy: „umieszczania tablic, ogłoszeń, oznaczeń lub urządzeń, które mogłyby być mylnie wzięte za znaki lub inne urządzenia służące do kierowania ruchem albo mogłyby pomniejszać ich widoczność lub skuteczność bądź też oślepiać użytkowników drogi lub odwracać ich uwagę i zagrażać przez to bezpieczeństwu ruchu".

Celem nadrzędnym proponowanych badań, nakierowanych na wspomaganie rozwiązywania powyżej określonych problemów, jest przedstawienie metod przeprowadzenia szeroko zakrojonych, wielopłaszczyznowych eksperymentów, wykorzystujących nowoczesne rozwiązania technologiczne, pozwalające na obiektywną ocenę zagrożeń wynikających z obecności reklam, jak i bazujących na ocenach subiektywnych, pozyskiwanych przy udziale specjalistów z dziedziny psychologii i psychofizjologii percepcji. Do prawidłowej realizacji poszczególnych etapów badawczych należy zaprojektować i oprogramować innowacyjne instalacje badawcze, obejmujące m. in. specjalne wyposażenie pojazdu testowego, symulator jazdy oraz monitoring ruchu drogowego, wykorzystujący zaawansowane metody analizy obrazu. Ze względu na pozyskiwanie danych z wielu rodzajów źródeł, np. ze statystyk wypadkowości i ankietowych badań psychologicznych, sformułowanie wniosków stanie się możliwe w następstwie fuzji wielowymiarowych danych i przeprowadzenia ich inteligentnej, wielowymiarowej analizy z użyciem systemu wydobywania wiedzy w formie reguł decyzyjnych.

STAN WIEDZY

Problem oddziaływania reklam umieszczonych w pasie drogowym (lub w jego pobliżu) narasta od wielu lat. Badania prowadzone w innych krajach (np. USA) pokazują, że obiekty znajdujące się w pasie drogowym i w jego pobliżu mają istotny wpływ na zachowanie się kierowców [28][29]. W Polsce tego typu kompleksowe badania nie były prowadzone na odpowiednią skalę.

Prowadzenie pojazdu jest złożonym procesem, w którym zidentyfikować można bardzo wiele elementów wpływających na bezpieczeństwo, prawidłowe wykonywanie manewrów, skuteczne i celowe kontrolowanie pojazdu, komfort, stan psychiczny i mentalny kierowców. W procesie tym występują obiekty oddziałujące ze sobą w sposób fizyczny (pojazdy, piesi, oświetlenie, liczba obiektów odwracających uwagę, ich rozmieszczenie, typy, rozmiary, itd.) oraz obiekty świadomie i nieświadomie percypowane przez użytkownika drogi, wpływające na jego stan wewnętrzny (znaki, reklamy) [1][26][30][33][41].

W celu stworzenia warunków do pozyskania możliwie dokładnego opisu tego procesu, jego wnikliwego badania, oceny interakcji i stanów, konieczne jest określenie najważniejszych czynników, podmiotów, cech i sposobów ich obiektywnego pomiaru. Przyjmuje się, że prowadzenie samochodu realizowane jest w dużym stopniu poprzez czynności wykonywane odruchowo, czyli poza świadomą kontrolą kierowcy. Każde pojawienie się nietypowego bodźca może jednak wpłynąć negatywnie na ten proces, możliwości przetwarzania informacji przez człowieka są bowiem ograniczone [2][11]. Reakcje kierowcy będą wówczas opóźnione, co może przyczynić się do zaistnienia kolizji lub wypadku. Taka sytuacja występuje najprawdopodobniej w przypadku reklam, gdyż mogą one skupiać uwagę kierowcy i zaburzać proces prowadzenia samochodu. Badania prowadzone w różnych krajach pokazały, że skupienie wzroku poza drogą na czas dłuższy niż dwie sekundy znacząco wpływa na zwiększenie ryzyka wystąpienia wypadku [13]. Stąd też konieczne jest sprawdzenie, czy reklamy są w stanie przyciągnąć uwagę i wzrok kierowcy na dłuższy czas. Niezbędne jest w tym celu wykorzystanie odpowiedniego systemu śledzenia wzroku, który pozwoli ocenić miejsce skupiania wzroku badanej osoby. Tego typu rozwiązania oparte na oryginalnej technologii śledzenia wzroku były stosowane przez zespół Katedry Systemów Multimedialnych do wyznaczania stopnia koncentracji uwagi, do nawiązywania komunikacji z osobami zdiagnozowanymi jako pacjenci w stanie wegetatywnym [17][18], sterowania odległymi kamerami za pomocą wzroku, syntezy mowy sterowanej wzrokowo i in. [4][14][16]. W literaturze można także odnaleźć liczne odniesienia do zastosowań związanych z oceną zachowań kierowców [10][23].

Dodatkowym problemem podczas prowadzenia pojazdu może być efekt ściągania uwagi, który jest znany i badany od lat 60. ubiegłego stulecia, występujący przede wszystkim w warunkach współdziałania dwóch zmysłów wzroku i słuchu, gdzie definicyjnie określa się go jako: zmianę percepcji kierunku źródła dźwięku, którego położenie nie pokrywa się ze związanym z nim bodźcem wzrokowym). Tłumaczony jest również jako „efekt zbliżenia obrazu" (ang. *image proximity effect*) [6][7]. Wynika on bezpośrednio z faktu, że do ludzkiej świadomości trafia zdecydowanie najwięcej informacji dostarczanych przez zmysł wzroku. W proponowanych badaniach efekt ten można określić jako zależność

pomiędzy położeniem bodźca wzrokowego i zawartością tego bodźca, na których skupiany jest wzrok osoby badanej, a wpływem ściągającym obrazu [12][19][20][21][22]. W proponowanych badaniach szczególna uwaga zostanie poświęcona reklamom dynamicznym, a zwłaszcza możliwym wpływom na działanie organu wzroku.

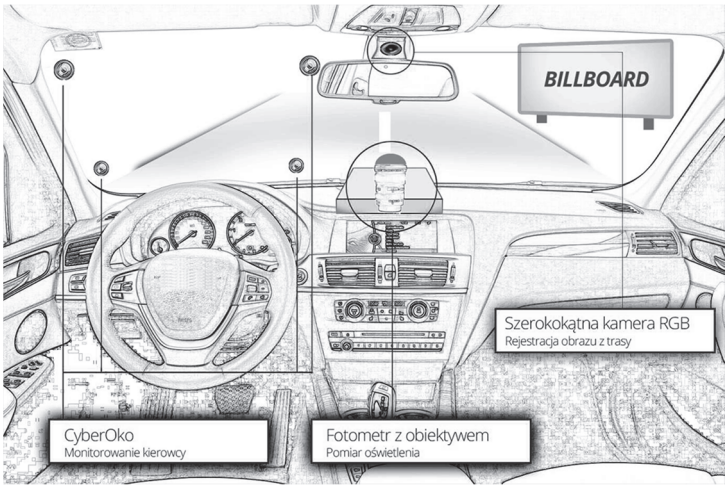
Nagłe oślepienie na skutek gwałtownej zmiany jasności może być niebezpieczne nawet, gdy kierowca nie zwraca wzroku ku reklamie. Dotyczy to zwłaszcza warunków wieczornych i nocnych i może być przyczyną występowania niebezpiecznych sytuacji. Zespół badawczy Katedry Systemów Multimedialnych posiada doświadczenie związane z technologią śledzenia wzroku i jej zastosowaniami, m. in. w badaniu uwagi i wpływu ściągającego [14][16][17][19][20][21][22]. Nowe pole zastosowań opracowanych rozwiązań, jakim jest badanie wpływu reklam na uwagę kierowców, umożliwi efektywne wykorzystanie doświadczeń zgromadzonych przez zespół, który zrealizował wyżej wymienione eksperymenty badawcze.

W przypadku opisywanej metody badawczej najpoważniejszym problemem, wskazywanym także przez innych badaczy, jest wpływ świadomości osoby badanej, odnośnie jej uczestniczenia w eksperymencie. Był to jeden z powodów, dla których zdecydowano się wykorzystać w projekcie bezkontaktowy system śledzenia wzroku (zamiast nagłownego okulografu), co stanowi podejście zarówno bardziej praktyczne jak i oryginalne oraz pozwala zredukować szereg niekorzystnych czynników towarzyszący badaniom i obniżających wiarygodność osiąganych wyników.

Istotną grupę nośników reklamowych umieszczanych w obrębie pasa drogowego stanowią reklamy dynamiczne, wykorzystujące ekrany LED. Ze względu na ich jasność (przekraczającą często 5000 nitów) i zmienność prezentowanych treści, wydają się być one największym zagrożeniem dla uczestników ruchu drogowego. Firmy oferujące emisje przygotowywanych przez klientów spotów reklamowych na ekranach LED podają niekiedy zasady tworzenia spotów reklamowych dla tego typu nośników, np. zalecają wykorzystanie kontrastowych, nasyconych barw, wskazują, że wielkość liter powinna zawierać się w przedziale 10-15% wysokości wyświetlanego obrazu. Jednocześnie odradzają stosowanie szybkich zmian obrazu, dużej ilości informacji w jednym czasie oraz koloru białego na dużych powierzchniach, argumentując powyższe właśnie względami bezpieczeństwa uczestników ruchu drogowego. Założenia te, o charakterze raczej arbitralnym, wymagają starannej weryfikacji eksperymentalnej.

NARZĘDZIA BADAWCZE

W ramach badań przydatne byłoby wykorzystanie pojazdu eksperymentalnego wyposażonego w sprzęt pozwalający na ilościową analizę wpływu różnego rodzaju czynników rozpraszających uwagę kierowcy. Jednym z najważniejszych elementów takiego pojazdu jest system umożliwiający śledzenie miejsc skupiania wzroku kierowcy. Tego typu podejście bywało przyjmowane w analogicznych badaniach, niemniej jednak dzięki postępowi w dziedzinie technologii systemów śledzących wzrok, planowane jest mierzenie, oprócz kierunku patrzenia, także zachowania źrenic, co umożliwi ocenę zjawiska akomodacji źrenicy i refrakcji soczewki. Jest to szczególnie ważne w przypadku reklam dynamicznych (LED), w przypadku których, na skutek zmian jasności prezentowanych treści może nastąpić zaburzenie funkcjonowania oka. Tego typu badania były do tej pory prowadzone w bardzo wąskim zakresie (głównie w symulatorach). Na rys. 1 zobrazowano projektowane wyposażenie pojazdu eksperymentalnego, które umożliwi badanie reakcji kierowców w trakcie mijania reklam drogowych a także pomiary fotometryczne oraz rejestrację filmową przejazdu dla celów analitycznych i wykorzystania materiału filmowego w symulatorze jazdy.

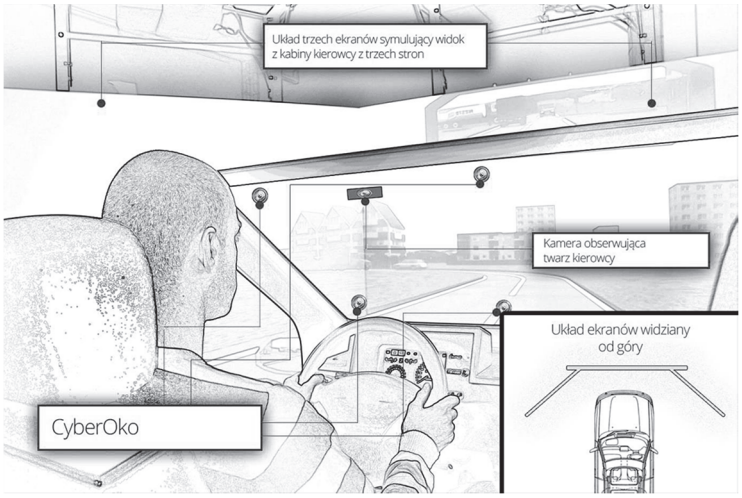


Rys. 1. Wyposażenie pojazdu do prowadzenia badań reakcji, do pomiarów i rejestracji

Trasy przejazdów odpowiednio wyposażonego pojazdu badawczego zostaną wytyczone w taki sposób, by możliwa była ocena zachowania się kierowców w zbliżonych sytuacjach. Niemniej jednak, trudno będzie zapewnić każdemu kierowcy dokładnie takie same warunki przejazdu (np. ze względu na zmienne natężenie ruchu). Wyniki zostaną, zatem, poddane pogłębionym analizom, co

w efekcie pozwoli na ustalenie wytycznych odnośnie preferowanych sposobów rozmieszczania nośników reklamowych. Do analizy wyświetlanego obrazu można przyjąć wybrane niskopoziomowe deskryptory wizji standardu MPEG 7. Dla przykładu analiza deskryptorów: Color Layout, Dominant Color oraz Scalable Color pozwoli na zbadanie wystąpień poszczególnych kolorów w reklamie zarówno w dziedzinie RGB, jak i YCbCr. Możliwe też jest wyznaczenie koloru reprezentatywnego dla poszczególnych składowych przestrzeni. Z kolei wyznaczenie histogramów (liczba wystąpień danego koloru w bloku) pozwoli na określenie koloru dominującego (Dominant Color) [27]. Dodatkowo w badaniach wykorzystane będą deskryptory kształtu i ruchu, tak aby było możliwe wyznaczenie korelacji z odpowiedziami uzyskanymi w ankietach wypełnianych przez respondentów, jak również z parametrami uzyskiwanymi z pomiarów za pomocą systemu fiksacji wzroku, np. map cieplnych (ang. *heat map*) oraz map przejść (ang. *gaze plot*) [12][19][20][21][22]. Przykładowo, w przypadku reklam telewizyjnych jedną z ważniejszych regulacji jest zalecenie dotyczące używania kolorów w materiale reklamowym - EBU Technical Recommendation R103-2000 „Tolerances on "Illegal" colours in television" [5][40]. Gama dostępnych wartości w przestrzeni barw YUV stosowanej w systemach telewizyjnych jest większa niż kombinacje, które mogą zostać wytworzone przy rzeczywistym złożeniu sygnałów podstawowych RGB. Jeśli sygnał w przestrzeni YUV zostanie zmanipulowany, możliwe jest pojawienie się tzw. nielegalnych kolorów. Stacje telewizyjne zabezpieczają się przed ich powstawaniem, zaznaczając w dokumentacji technicznej dostarczanej twórcom reklam, że w przypadku pojawienia się kolorów niezgodnych z zaleceniami normy EBU R103, reklama nie zostanie wyemitowana. Dlatego wydaje się istotne zbadanie tych aspektów w kontekście reklam świetlnych umieszczanych na billboardach.

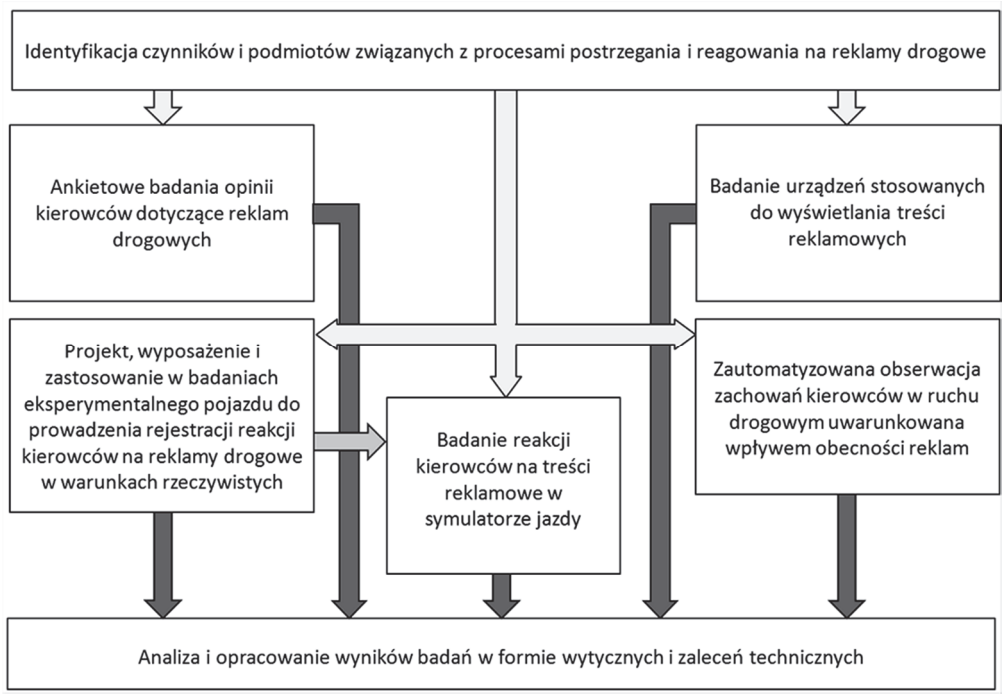
Istotna część badań może także odbywać się w środowisku laboratoryjnym, gdzie, z użyciem symulatora jazdy (rys. 2), odtwarzane powinny być warunki prowadzenia pojazdu. W sposób kontrolowany zmieniana będzie treść i parametry reklamy i symulowane będą typowe zdarzenia w ruchu drogowym oraz zagrożenia, m.in. pieszy na drodze, olśnienie i oślepienie kierowcy światłem reklamy i inne istotne czynniki zidentyfikowane podczas realizacji pierwszego etapu badań. Badanie laboratoryjne mogą wykorzystywać ponadto kontaktowy pomiar sygnałów EEG, szczególnie potencjału wywołanego P100, związanego z działaniem ośrodka widzenia w mózgu. Wyniki z symulacji powinny zostać porównane z wynikami z rzeczywistych przejazdów, w celu określenia stopnia występujących korelacji między nimi. Wykorzystanie symulatora pozwoli w sposób powtarzalny i bezpieczny przetestować zachowania kierowcy. Jako bodziec mogą zostać wykorzystane wirtualne trasy odtworzone w środowisku 3D o wysokim realizmie obrazu oraz szerokokątne panoramy uzyskiwane przez łączenie materiałów wideo zarejestrowanych kamerami umieszczonymi na pojeździe.



Rys. 2. Ilustracja koncepcji symulatora jazdy.
Opcjonalnym wyposażeniem jest kask EEG

OPIS METODY BADAWCZEJ

Na kompletną metodologię badawczą składa się siedem etapów. Ich tematy i występujące pomiędzy nimi zależności przedstawia graf z rys. 3. Ostatecznie zaproponowane badania mogą posłużyć do analizy wielostronnych wyników badań i przedstawienia wynikających z nich wniosków w formie wytycznych i zaleceń technicznych, dotyczących wymaganych parametrów reklam i ich usytuowania w otoczeniu pasa drogowego.



Rys. 3. Kolejne etapy badań i zależności pomiędzy nimi

Po pogłębieniu analiz, np. w następstwie przeprowadzenia analizy wypadkowości w miejscach występowania reklam, przeanalizowaniu wiedzy z zakresu psychologii behawioralnej i psychofizjologii percepcji wzrokowej (z udziałem specjalistów z tej dziedziny), zidentyfikowaniu zagadnień natury prawnej i odnośnych przepisów administracyjnych, mogą zostać ostatecznie zidentyfikowane czynniki i podmioty mające wpływ na sposób organizowania i prowadzenia badań eksperymentalnych. Dane na temat wypadków i kolizji można pobierać z Systemu Ewidencji Wypadków i Kolizji (SEWIK – http://sewik.pl). System SEWIK, jako samodzielna baza danych o zdarzeniach drogowych, powstał w 1995 r. i posiadał strukturę dostosowaną do bezpośredniej obsługi na poziomie komend wojewódzkich Policji, (które raz w miesiącu przekazywały dane do Komendy Głównej Policji). W lipcu 2006 r. system SEWIK został zcentralizowany, zmodyfikowany o nowe parametry analityczne i włączony do zakresu Krajowego Systemu Informacji Policyjnej (KSIP), do którego dostęp mają wszystkie jednostki Policji. Od dnia 1 lipca 2006 r. kwestie związane z funkcjonowaniem tego systemu reguluje zarządzenie nr 635 Komendanta Głównego Policji z dnia 30 czerwca 2006 r. w sprawie metod i form prowadzenia przez Policję statystyki zdarzeń drogowych (Dz. Urz. KGP z dnia 31 lipca 2006 r. Nr 11, poz. 67). Rozbudowa systemu polegała m.in. na zintegrowaniu rozproszonych

do tej pory danych w centralnej bazie (KSIP) oraz na rozszerzeniu i ulepszeniu wcześniej eksploatowanej aplikacji. SEWIK jest centralnym zbiorem informacji o osobach uczestniczących w zdarzeniach drogowych: kierujących – sprawcach i poszkodowanych. W systemie dostępne są informacje, takie jak: czas i miejsce powstawania wypadków, rodzaje wypadków, ich ofiary, bezpieczeństwo pieszych, nietrzeźwi uczestnicy, a także wypadki śmiertelne z udziałem cudzoziemców. W systemie dostępne są zdarzenia (wypadki i kolizje) z terenu kilkunastu największych polskich miast, począwszy od 2007 roku. Dane w systemie są opracowywane na podstawie eksportu z policyjnej ewidencji wypadków i kolizji, udostępnianego przez Komendę Główną Policji dla sieci Miasta dla Rowerów. Dane Komendy Głównej Policji gromadzone są zaś w oparciu o „Kartę zdarzenia drogowego". Karta zdarzenia drogowego jest dwustronnym formularzem, składającym się z części nagłówkowej, szkicu miejsca zdarzenia oraz 12 tabel. Karta ta jest sporządzana przez funkcjonariusza Policji. Należy zauważyć iż, mimo, że osoby sprawujące merytoryczny nadzór nad prawidłowym funkcjonowaniem systemu posiadają odpowiednie przeszkolenie i kwalifikacje (stosownie do zajmowanego stanowiska), to interpretując zestawienia z systemu, koniecznym będzie, aby wziąć pod uwagę zdarzające się w systemie błędy (czynnik ludzki) oraz fakt, że pewna część zdarzeń nie jest zgłaszana Policji. Dostęp do systemu jest publiczny, aczkolwiek wymagane jest logowanie.

Źródłem danych dla potrzeb analiz mogą stać się ponadto wyniki ankietyzacji kierowców zebrane w ramach realizacji drugiego etapu prac badawczych. Opracowanie treści ankiet jest samo w sobie istotnym zagadnieniem badawczym o charakterze interdyscyplinarnym, wymagającym współpracy specjalistów z dziedziny inżynierii ruchu drogowego, policji i psychologów. Zadanie tego typu było już podejmowane, bowiem istnieją publikacje dotyczące badań prowadzących za granicą na podobne tematy [32], jednak występujący brak opracowań ankiet odnoszących się do krajowej specyfiki ruchu drogowego, opinii polskich kierowców i specjalistów, wymaga podjęcia tego zagadnienia po raz kolejny. W ramach kolejnego etapu prac powinno zostać zaplanowane wykonanie analiz ilości światła emitowanego bądź odbijanego od nośników reklamowych [8]. Badania z dziedziny percepcji wykazują, że gdy w polu widzenia znajduje się obiekt wyraźnie jaśniejszy lub ciemniejszy od otoczenia, to uwaga wzrokowa jest na niego kierowana bezwiednie. O zmroku oczy kierowcy kompensują niski poziom oświetlenia, stając się bardziej wrażliwymi na światło, co powoduje jeszcze większą podatność na rozproszenie uwagi lub oślepienie [24]. Zagadnienia te wymagają bliższego zbadania w warunkach zarówno rzeczywistych, jak i symulowanych. Zakłada się, że w warunkach rzeczywistych reakcje kierowców będą badane wewnątrz samochodu, ale także będzie zewnętrznie monitorowany sposób poruszania się pojazdów w ruchu drogowym w zależności od obecności i treści wyświetlanych reklam za pomocą monitoringu wizyjnego. Ponieważ można oczekiwać, że innowacyjne metody analizy obrazu, badania reakcji i łącznego

przetwarzania wielowymiarowych danych dostarczą dużej liczby wyników, to w ramach ostatniego etapu badań powinna zostać przewidziana ich analiza i na tej podstawie powinno nastąpić sformułowanie wytycznych i zaleceń technicznych, które są oczekiwanym rezultatem realizacji projektu.

Identyfikacja czynników i podmiotów związanych z procesami postrzegania i reagowania na reklamy drogowe

W kontekście identyfikacji powyższych czynników i podmiotów badane powinny być między innymi następujące parametry:

- fizyczne związane z kierowcą (ostrość widzenia, stosowana korekcja wzroku, wysokość siedzenia, odległość od szyby przedniej, wysokość horyzontu optycznego ponad płaszczyzną jezdni) [36];
- behawioralne kierowcy (stopień skupienia uwagi, kierunek patrzenia, czas zatrzymywania wzroku na elementach sceny, czas reakcji);
- pojazdu (wielkość przedniej szyby, wysokość siedzenia nad powierzchnią jezdni, prędkość chwilowa jazdy);
- drogi (skręt, nachylenie, liczba pasów, typ jezdni, obecne w danym miejscu oznakowanie i jego rozmieszczenie względem pojazdu i billboardów, topologia skrzyżowań, dojazdów, szerokość pasów zieleni) i ruchu drogowego (natężenie, płynność, wpływ sygnalizacji świetlnej);
- pogody i nasłonecznienia;
- historii wypadkowości z podziałem na typ zdarzenia, pory dnia, roku [34] oraz lokalizację [9].

Istotny w planowanych badaniach jest zestaw parametrów reklam drogowych, w tym przewidywane atrybuty, których lista w toku badań może zostać rozwinięta:

- treść (obrazy, tekst, wielkość elementów, ich nacechowanie emocjonalne);
- treść dynamiczna (zmiany koloru, kontrastu, migotanie, charakter ruchu, wielkość elementów ruchomych);
- orientacja i położenie względem jezdni;
- jednolitość, kierunkowość i siła świecenia.

Wstępnie przetestowane powinny być sposoby pomiaru chwilowych cech behawioralnych kierowcy, takie jak śledzenie punktu fiksacji wzroku (rejestracja obiektów przyciągających uwagę i czas zatrzymania wzroku), aktywność traktu wzrokowego i reakcja na bodziec (potencjał P100 w pomiarze EEG), czas

reakcji (rozpoczęcie hamowania po zauważeniu zagrożenia). Na drodze obserwacji, ankiet i analizy statystycznej prowadzonych w ramach pozostałych etapów, mogą zostać określone współzależności i związki przyczynowo skutkowe pomiędzy poszczególnymi czynnikami i podmiotami.

Ankietowe badania opinii kierowców dotyczące reklam drogowych

Tworzenie ankiety stanowi jeden z newralgicznych etapów całościowego badania. Przygotowana ankieta powinna zostać skorelowana z badaniami laboratoryjnymi (badania respondentów w warunkach wirtualnego, symulowanego środowiska pomiarowego, rozmiary reklam i ich parametry kontrolowane) oraz z pomiarami w warunkach rzeczywistych. Z tego względu pytania zawarte w ankiecie powinny mieć odniesienie do uwarunkowań miejsca, tj. teren miejski, teren przemysłowy, teren zabudowany poza miastem, teren zielony – parki krajobrazowe; rodzaj drogi (droga szybkiego ruchu, autostrada, droga krajowa, itd.); odległość od drogi, kąt ustawienia tablic reklamowych w stosunku do drogi, topologia drogi: prosty odcinek drogi, krzywizna; zmienne warunki pogodowe; pora dnia/nocy. Kolejnym elementem ankiety powinny być pytania dotyczące zawartości wyświetlanej reklamy, zawartych w niej kolorów, częstości zmian sceny w obrębie jednej reklamy oraz pomiędzy reklamami. Dodatkowo pytania powinny też dotyczyć oceny stanu wzroku respondenta (prawidłowe widzenie, jeśli wada wzroku, to jakiego typu, jeśli korekcja wady wzroku, to czy noszone są przez kierowcę okulary, czy soczewki kontaktowe), wrażliwość na światło, itp. Elementem łączącym badania ankietowe, laboratoryjne oraz rzeczywiste powinna być odpowiedź, w jakim stopniu wystąpi wpływ ściągający wzrok powodowany reklamą świetlną. Zastosowanie systemu śledzenia punktu fiksacji wzroku w proponowanych badaniach pozwoli na zbadanie wpływu uwarunkowań dotyczących wyświetlanych reklam na percepcję.

Wynik, czyli stworzona ankieta, powinna być prawidłowo interpretowana zarówno przez różne wyszukiwarki internetowe, jak również w przypadku korzystania z Internetu w warunkach mobilnych. Z kolei po stronie serwera może zostać wykorzystany język obiektowy PHP. Oprogramowanie tego typu można uruchamiać nie tylko na serwerze IIS (Windows), ale również w chmurze Windows Azure.

Badanie urządzeń stosowanych do wyświetlania treści reklamowych

Na tym etapie może zbadany zostać poziom luminancji występujący w przypadku obecnie stosowanych nośników reklamowych, zależnie od lokalizacji i pory dnia lub nocy [8][24]. W przypadku reklam dynamicznych (ekrany

LED) ocenie podlegać powinno światło emitowane bezpośrednio przez ekran, w przypadku reklam tradycyjnych zaś - światło odbite od powierzchni billboardu. Do badania luminancji wykorzystany powinien być fotometr z odpowiednimi obiektywami. Pomiary będą wykonane dwiema metodami: z wykorzystaniem przystawki do mierzenia luminancji oraz bez niej. Właściwa przystawka pozwala uzyskać precyzyjne wyniki pomiaru luminancji dla małego kąta padania światła, przy czym może się okazać, że bardziej praktyczne będzie użycie fotometru bez przystawki. Metodologia użycia luksomierza zakłada pomiar całkowitego oświetlenia w danej lokalizacji z włączonym oraz wyłączonym oświetleniem badanego nośnika reklamowego. Stosując następnie odpowiednie przekształcenia, można uzyskać różnicę w poziomie luminancji sceny z nośnikiem i bez niego, co wyraża luminancję samego nośnika reklamowego. Opisana metoda jest niewrażliwa na niewielkie zmiany kąta pomiaru, co znacznie usprawnia cały proces pomiarowy. Dodatkowo autorskim pomysłem na pomiar luminancji nośników reklamowych jest wykorzystanie kamer rejestrujących obraz z wnętrza pojazdu. Zmiana parametrów rejestrowanego obrazu z zachowaniem ekspozycji na stałym poziomie umożliwi wyznaczenie poszukiwanej wielkości luminancji. Metoda ta, jako eksperymentalna, wymaga jednak sprawdzenia i porównania z ocenami prowadzonymi w oparciu o wskazania luksomierza. W ramach prac, poza zmierzeniem luminancji nośników reklamowych, mierzone powinny być także ich wymiary fizyczne i umiejscowienie względem drogi. Wszystkie pomiary powinny być wykonywane w różnych porach dnia i nocy, by pokryć możliwie szeroki zakres zmienności całej sceny. Uwzględnić należy także ograniczone kąty świecenia ekranów LED (typowo ok. 120 stopni w poziomie i 50 stopni w pionie).

Projekt, wyposażenie i zastosowanie w badaniach eksperymentalnego pojazdu do prowadzenia rejestracji reakcji kierowców na reklamy drogowe w warunkach rzeczywistych

Prowadzenie badań związanych z percepcją reklam statycznych i dynamicznych przez kierowcę wymaga wykonania licznych przejazdów testowych, podczas których mierzone będą reakcje kierowcy oraz rejestrowane (w celu dalszej analizy) parametry przejazdu (np. zmiany prędkości). Elementem niezbędnym do realizacji badań jest eksperymentalny pojazd, który powinien zostać wyposażony w następujący sprzęt:

- okulograf bezkontaktowy - umożliwi ocenę miejsca skupienia wzroku kierowcy wraz z czasem skupienia, analizowana będzie także średnica źrenicy w celu oceny procesu akomodacji i refrakcji oka;

- fotometr - służący do oceny natężenia światła otoczenia oraz natężenia światła pochodzącego od reklam dynamicznych;
- kamera stereoskopowa rejestrująca obraz przed samochodem - pozwoli to na późniejsze nałożenie na zarejestrowany obraz informacji z okulografu (takich jak np. punkty skupiania wzroku);
- zestaw kamer wysokiej rozdzielczości, umożliwiających rejestrację obrazu w zakresie 360 stopni wokół samochodu - zapis obrazu z kamer będzie wykorzystany podczas badań w symulatorze oraz posłuży do oceny natężenia ruchu;
- kamera rejestrująca twarz kierowcy – dla potrzeb oceny zachowania kierowcy;
- rejestrator GPS - w celu kontrolowania trasy oraz rejestracji parametrów jazdy (np. prędkość, częstość zmiany pasów);
- akcelerometr - w celu rejestracji danych na temat hamowania i przyspieszania pojazdu;
- system do transmisji danych wykorzystujący połączenie w standardzie LTE - w celu umożliwienia transmisji danych w czasie rzeczywistym.

Badania powinny być wykonane dla większej grupy (np. 60 kierowców) podzielonych na trzy kategorie:

- młodzi kierowcy - w wieku 18-30 lat, nie więcej niż 10 lat z prawem jazdy;
- kierowcy dojrzali - w wieku 30-60 lat, prawo jazdy od więcej niż 10 lat;
- kierowcy w podeszłym wieku - powyżej 60 roku życia, jak wykazują badania w tej grupie wiekowej występuje pogorszenie własności poznawczych, co może oznaczać, że będą one w odmienny sposób narażone na wpływ reklam [39].

Rekrutowane powinny być wyłącznie osoby, które w okresie trzech lat poprzedzających datę badania nie były sprawcami wypadków drogowych, a liczba punktów karnych w dniu prowadzenia badania nie przekraczała 5. Tym samym ograniczone zostanie ryzyko zafałszowania wyników badań przez osoby łamiące przepisy i jeżdżące w sposób niebezpieczny. Przejazdy testowe muszą obejmować różne kategorie dróg, które mogą zostać wytyczone w ten sposób, by możliwa była rejestracja zachowań kierowcy:

- w obszarze miejskim - przy dużym natężeniu ruchu, stosunkowo nieduże prędkościach średnich, a zarazem przy obecności największej liczby reklam;
- na drogach poza obszarem zabudowanym - przy większych dopuszczalnych prędkościach, konieczności wyprzedzania pojazdów, ale mniejszej liczbie reklam;

– na drogach ekspresowych i autostradach - przy prędkościach powyżej 100km/h, także z możliwością korzystania z więcej niż jednego pasa w danym kierunku. Drogi tego typu uchodzą za najbezpieczniejsze, ale przy dużej prędkości każde odwrócenie uwagi kierowcy od drogi wiąże się z większym niebezpieczeństwem. Ze względu na istniejące przepisy, format oraz lokalizacja nośników reklamowych wzdłuż dróg ekspresowych i autostrad jest jednak ograniczona [38].

Ze względu na stopień angażowania uwagi kierowcy i związane z tym zmęczenie, można przyjąć, że jedna z tras prowadzić będzie w obszarze miejskim, druga poza obszarem miejskim, w tym na drogach ekspresowych lub autostradach. Długość trasy może wynosić ok. 15-20 km dla obszaru miejskiego i ok. 40-50 km dla obszaru poza miastem. Dla każdej trasy i każdego kierowcy przejazdy powinny odbywać się zarówno w dzień, jak i w nocy. Kolejność przejazdów (miasto/poza miastem, dzień/noc) powinna być zmieniana. Przejazdy nie powinny się odbywać w warunkach ekstremalnie odbiegających od typowych (tzn. śnieżyca, ulewa, mgła), w takiej sytuacji przejazd winien być przerywany. Każda trasa powinna zostać dobrana w taki sposób, by kierowca minął określoną liczbę reklam każdego rodzaju (tzn. billboard o powierzchni 12m^2, billboard o powierzchni 18m^2, citylight oraz reklamę LED). W przypadku odcinków wiodących drogami ekspresowymi i autostradami ocenie mogą podlegać także nośniki reklamowe o innych formatach. Zaplanowane powinno zostać także wykupienie czasu emisji na billboardach w celu umieszczenia przekazów o określonej treści i kolorystyce w celu uzyskania wyników odniesienia.

Ponieważ testy odbywać się będą na istniejących drogach publicznych i w obecności innych pojazdów, nie wydaje się możliwe zachowanie stałych warunków (np. natężenie ruchu, korki) dla wszystkich kierowców. Jednak dzięki zapisowi obrazu z kamery rejestrującej obraz wokół samochodu oraz danych GPS, możliwe stanie się uwzględnienie natężenia ruchu jako jednego z parametrów wpływających na uzyskiwane wyniki. W procesie analizy wykorzystane mogą zostać algorytmy automatycznej detekcji pojazdów opracowane w Katedrze Systemów Multimedialnych [35]. Dobór tras przejazdu powinien uwzględniać istotny czynnik - znajomość danej trasy przez kierowcę. Tzw. „jazda na pamięć" powoduje bowiem, że osoba nie zwraca uwagi na elementy, które są jej znane. Jednocześnie poświęca mniej uwagi na sam proces prowadzenia samochodu, bo zna drogę, wie np. jak wyprofilowany jest łuk, gdzie może dojść do niebezpiecznej sytuacji. Stąd też trasy przejazdu winny zostać dobrane w taki sposób, by nie pokrywały się z odcinkami pokonywanymi przez kierowcę na co dzień.

Badanie reakcji kierowców na treści reklamowe w symulatorze jazdy reklamy drogowe w warunkach rzeczywistych

Celem tego etapu badań jest wytworzenie stanowiska laboratoryjnego do emisji bodźców i do pomiaru reakcji badanej osoby. W środowisku testowym odtworzone może zostać wnętrze pojazdu (szyba, kierownica i pedały, elementy deski rozdzielczej, wykonane na drukarce 3D lub zakupione) i otoczenia pojazdu (emisja dźwięku silnika i projekcja odpowiednio spreparowanego obrazu monitorami wielkoformatowymi, monitorami autostereoskopowymi, nie wymagającymi okularów do projekcji treści 3D lub rzutnikami z przodu i po bokach kabiny). Pomiar świadomej reakcji polegać może na wciśnięciu przycisku, hamulca, itp. w chwili zauważenia znaku drogowego, pieszego, zmiany świateł, zagrożenia. Z kolei do pomiaru reakcji nieświadomej zastosowane może być badanie fiksacji wzroku i potencjału wywołanego EEG-P100. Przebadane i określone powinny zostać:

- wpływ efektu olśnienia światłem billboardu (czas i poziom emisji) na czas readaptacji do widzenia zmierzchowego i nocnego [26][30][31][36][37];
- minimalna odległość czasowa poprawnej percepcji treści znaku drogowego po percepcji bodźców wizualnych reklamy [1][33];
- oddziaływanie treści reklam na rozumienie znaków drogowych i na ocenę sytuacji na drodze [26][30][41].

Bodźce wizualne mogą pochodzić z dwóch źródeł:

- filmy przedstawiające przejazd wybraną trasą, zarejestrowane systemem opracowanym w ramach poprzedniego etapu, połączone w obraz panoramiczny o wysokiej rozdzielczości, otaczający badanego;
- interaktywna symulacja prowadzenia pojazdu, w środowisku wirtualnym o wysokim realizmie obrazu, która pozwala na modyfikowanie elementów drogi, warunków widoczności, treści reklamy i innych aspektów.

Dla przypadku środowiska wirtualnego przygotowane mogą być trasy (co najmniej 10 tras) odtwarzające wcześniej sfilmowane rzeczywiste odcinki drogi, w celu porównania wyników uzyskiwanych dla bodźca filmowego i wirtualnego oraz określenia korelacji z danymi zebranymi w trakcie ruchu rzeczywistego przejazdu. Opracowana powinna być procedura testowa i sposób doboru bodźców redukujące efekty zapamiętywania trasy i znaków przez badanego tak, aby mógł on/ona wielokrotnie brać udział w badaniu.

Sprawdzenie na jakich elementach i na jak długi czas badana osoba sku-

pia uwagę powino być przeprowadzone z wykorzystaniem urządzenie do śledzenia wzroku, np. CyberOko [15]. Rozwiązany zostanie problem identyfikacji obiektu przyciągającego uwagę pomimo występowania jego ciągłego ruchu w prezentowanym obrazie. Analiza danych dostarczy obiektywnej miary stopnia skupienia uwagi na drodze i czasu rozproszenia uwagi przez elementy na poboczu. Drugi pomiar wykorzysta wzrokowe potencjały wywołane (ang. *visual evoked potentials*) – sygnały rejestrowane na powierzchni głowy przy pomocy elektrod. Typowo w celu określenia aktywności mózgu związanej z przetwarzaniem bodźca wizualnego (np. w diagnozie przecięcia nerwu wzrokowego, jaskry, stwardzenia rozsianego) rejestruje się najbardziej dominujący załamek o latencji około 100 milisekund i o dodatnim zwrocie. Badanie to umożliwia obiektywną ocenę działania drogi wzrokowej i reakcji mózgu na bodziec. Subiektywne aspekty, np. rozumienie sceny (znaków, sytuacji na drodze) mierzone będą mogły być z wykorzystaniem urządzeń wejściowych: kierownicy, pedałów (m.in. hamowanie w reakcji na zagrożenie) oraz ekranu dotykowego z listą wyboru (m.in. pytania o treść znaku) do badania świadomej percepcji znaków po prezentacji bodźca. Jednocześnie realizowany pomiar potencjału P100 pozwoli określić zależność pomiędzy wydłużeniem uświadomionej percepcji, a parametrami reklamy i złożonością sceny. W celu zobiektywizowania wyników zaproponowana powinna zostać odpowiednia metoda pomiaru wizualnej złożoności sceny i zweryfikowana zostanie korelacja tej miary ze stopniem (spadku/zaburzenia) koncentracji.

Zautomatyzowana obserwacja zachowań kierowców w ruchu drogowym uwarunkowana wpływem obecności reklam

Wymienione powyżej cele eksperymentów badawczych mogą zostać osiągnięte w oparciu o metody wizji komputerowej, przetwarzające obraz z kamer obserwujących ruch w pobliżu miejsc, gdzie umieszczone są nośniki reklamowe. Pozyskane sygnały będą korelowane z sygnałami z systemu śledzenia punktu fiksacji wzroku i kamer zamontowanych w pojeździe. Podejście takie umożliwia analizowanie zachowań kierowców nie tylko w ujęciu jednostki (*per kierowca*), ale również w ujęciu całościowym (ruch uliczny; tworzenie się korków z powodu reklamy ustawionej w pobliżu drogi). Analiza obrazu z kamer pozwoli określić zarówno płynność ruchu przy billbordzie z reklamą, jak również możliwe będzie opisanie stopnia zajętości jezdni. Zachowanie kierowców może zostać zamodelowane za pomocą zestawu parametrów takich, jak odległości pomiędzy pojazdami i średnia prędkość jazdy. Te parametry mogą ulegać zmianie w sąsiedztwie reklamy. W ten sposób możliwe jest wykrycie zachowań takich, jak zwolnienie w okolicy billbordu, nieświadome skręcanie w stronę reklamy, czy też opóźnione reakcje na sygnały świetlne wysyłane przez

sygnalizację świetlną. Przydatne jest przy tym doświadczenie w analizie ruchu drogowego i wykrywania zdarzeń, które mogą w nim wystąpić [35] jak również w modelowaniu zachowania obiektów na obszarze nadzorowanym przez kamery systemu monitoringu wizyjnego [3][25]. Zaletą analizowania zachowań kierowców z wykorzystaniem systemu monitoringu zewnętrznego jest obiektywizacja wyników, wynikająca z nieświadomego udziału kierowców w eksperymencie. W oparciu o metody statystyki sprawdzona może zostać istotność różnic wyników otrzymanych dla billboardu wyświetlającego specjalnie przygotowane treści, o różnym stopniu absorbowania uwagi. W szczególności sprawdzone powinny zostać reakcje kierowców na treść billboardu, którą stanowić powinny jednolite czarne tło, symulujące wyłączenie billboardu.

Analiza i opracowanie wyników badań w formie wytycznych i zaleceń technicznych

Zbiorcza analizy wyników powinna mieć charakter erudycyjny, ale nie wyłącznie, ponieważ może przebiegać także z wykorzystaniem zaawansowanych metod analizy danych, tzn. narzędzi statystycznych i opartych na inteligentnych metodach wydobywania wiedzy. To drugie podejście jest uzasadnione wielodziedzinowym charakterem badań, których wyniki będą miały zróżnicowaną formę i charakter, począwszy od danych pochodzących z szeroko zakrojonej ankietyzacji, poprzez analizę wypadkowości, pomiary parametrów technicznych wyświetlaczy reklam i określania deskryptorów emitowanego materiału reklamowego, po wyniki badań biometrycznych kierowców w warunkach symulowanych i rzeczywistych oraz dane pochodzące z monitorowania ruchu drogowego w otoczeniu reklam.

REZULTATY BADAŃ

Realizacja proponowanych badań umożliwi skonstruowanie symulatora jazdy, opracowanie algorytmów analizy multimodalnych danych oraz zbadanie wpływu reklam przy drogach na percepcję kierowcy. Te elementy mogą stanowić środowisko dla dalszego rozwoju badań nad percepcją i zachowaniem. Ponadto wyniki będą mogły zostać wykorzystane w celu administracyjnego uregulowania problemu lokalizacji reklam statycznych i dynamicznych w pasie drogowym i w bezpośredniej jego bliskości. W przypadku reklam dynamicznych określone zostaną także zasady emisji materiału oraz doboru jasności paneli w celu uniknięcia nie tylko nadmiernego skupienia uwagi kierowcy, ale także oślepienia kierowcy, zwłaszcza w niesprzyjających warunkach, gdy łatwo doprowadzić do sytuacji, w której wymagana jest nagła akomodacja oka.

Ze względu na prowadzenie badań z udziałem dużej grupy kierowców, w różnych warunkach (atmosferycznych, oświetleniowych, ruchowych) możliwe stanie się zdefiniowanie wytycznych odnośnie lokalizacji nośników reklamowych. Nacisk powinien być położony na zalecenia dotyczące czterech najczęściej spotykanych rodzajów nośników reklamowych:

- billboard statyczny o wymiarach 6x3m (powierzchnia 18m^2);
- billboard statyczny o wymiarach 5,04x2,38m (powierzchnia 12m^2);
- reklama LED - typowe reklamy tego typu mają powierzchnię ok. 20-30m^2 i charakteryzują się rozdzielczością w granicach od 576x288 do 640x480;
- tzw. citylight - nośnik o wymiarach 1,2x1,8m, podświetlany, umieszczany najczęściej na przystankach komunikacji miejskiej.

Głównym założeniem odnoszącym się do perspektywy wdrożenia opracowanych w ramach badań wytycznych, dotyczących sposobów prezentowania treści reklamowych, jest zwiększenie bezpieczeństwa ruchu drogowego. W przypadku stwierdzenia naruszenia regulacji przez zarządcę reklamy ustawionej przy drodze, na której doszło do kolizji bądź wypadku, możliwe będzie ponadto wyciągnięcie konsekwencji wobec tego zarządcy w oparciu o konkretnie sprecyzowany wykaz niezgodności z zaleceniami. Najważniejszy podmiot – ludzki, jest pierwszoplanowym adresatem obszaru wykorzystania wyników tego typu badań, poprzez pośredni wpływ na ochronę życia i zdrowia, potencjalne zmniejszenie zmęczenia powodowanego prowadzeniem pojazdów. Pod uwagę mogą być też brane wątki biznesowe, ponieważ ograniczenie liczby wypadków i kolizji drogowych może przyczynić się do zwiększenia konkurencyjności agencji ubezpieczeniowych wskutek zmniejszenia środków wydawanych na likwidację szkód.

PODZIĘKOWANIA

Autorzy pragną w tym miejscu zamieścić podziękowanie dla pana Pawła Spaleniaka, pracownika Katedry Systemów Multimedialnych Politechniki Gdańskiej, za wykonanie koncepcyjnych szkiców (rys. 1 i rys. 2), wykorzystanych w niniejszej publikacji.

BIBLIOGRAFIA

[1] Castro, C., Martos, F.J., *Effect of background complexity in perception of traffic signs: the distracting effect of advertisements in the proximity of the sign*. General Psychology, 1998.

[2] Cooper, P.J, Zheng, Y., Richard, Ch., Vavrik, J., Heinrichs, B., Siegmund G., *The impact of hands-free message reception/response on driving task performance*, Accident Analysis and Prevention, No. 35, pp. 23-35, 2003.

[3] Czyżewski, A., Lisowski, K., *Employing flowgraphs for forward route reconstruction in video surveillance system*; Journ. of Intelligent Information Systems, pp. 1 - 15, 2013.

[4] Czyżewski, A., Łopatka, K., Kun*ka, B., Rybacki, R., Kostek, B.,* Speech synthesis controlled by eye gazing; 129th Convention of the Audio Engineering Society, Paper No. 8165, San Francisco, USA, 4.11.2010 - 7.11.2010.

[5] EBU Technical Recommendation R103-2000 „Tolerances on "Illegal" colours in television".

[6] Gardner, M.B., "Proximity *Image Effect in Sound Localization*", J. Acoust. Soc. Amer. vol. 43, 163, 1968.

[7] Gooding, L., "*The effect of viewing distance and disparity on perceived depth*", Stereoscopic Displays and Applications – II, Spie Proceedings, vol. 1457, 259-266, 1991.

[8] Illuminating Engineering Society of North America, IESNA Lighting Handbook, 2000.

[9] *Interaktywna mapa wypadków i baza danych*, Polskie Obserwatorium Bezpieczeństwa Ruchu Drogowego: https://www.obserwatoriumbrd.pl

[10] Inman, V.W., Balk, S.A., Perez, W.A., *Traffic Control Device Conspicuity*, National Highway Traffic Safety Administration, Report No. FHWA-HRT-13-044, August 2013.

[11] Kang, J.J., Bian, Z., Andersen, G.J., *Crash Risk: Eye Movement as Indices for Dual Task Driving Workloa*d, Proc. Of the Fifth International Driving Symposium on Human Factors in Driver Assessment, Training and Vehicle Design, pp. 356-362, Big Sky, USA, 2009.

[12] Kaszuba, K., Kostek, B., *Brain-computer interaction based on EEG signal and gaze-tracking information*, Elektronika, 5, 21 – 26, 2012.

[13] Klauer, S.G., Dingus, T.A., Neale, V.L., Sudweeks, J.D., Ramsey, D.J., *The Impact of Driver Inattention on Near-Crash/Crash Risk: An Analysis Using the*

100-Car Naturalistic Driving Study Data, National Highway Traffic Safety Administration, Report No. DOT HS 810 594, April 2006.

[14] Kulasek, Ł., Kunka, B., Czyżewski, A., *Badanie rozpoznawania twarzy przez człowieka z wykorzystaniem systemu śledzenia fiksacji wzroku Cyber-Oko*; Elektronika, No. 1/2011, pp. 29-31, 2011.

[15] Kunka, B., *System śledzenia punktu fiksacji wzroku jako narzędzie wspierające badania korelacji wzrokowosłuchowych*. Rozprawa doktorska, Politechnika Gdańska, promotor Prof. Bożena Kostek, 2011.

[16] Kunka, B., Czyżewski A., Kostek B., *Concentration tests. An application of gaze tracker to concentration exercises*; 1st International Conference on Computer Supported Education, pp. 66, Lizbona, Portugalia, 23.3.2009 - 26.3.2009.

[17] Kunka, B., Czyżewski, A., Kwiatkowska, A., *Awareness Evaluation of Patients in Vegetative State Employing Eye-Gaze Tracking System*; International Journal on Artificial Intelligence Tools (IJAIT), No. 2, vol. 21, pp. 1-11, 2012.

[18] Kunka, B., Czyżewski, A., Kwiatkowska, A., *Interaction with post-comatose patients employing video-based eye-gaze tracking system*; XVIII Krajowa Konferencja Biocybernetyki i Inżynierii Biomedycznej, Gdańsk, Polska, 10.10.2013 - 12.10.2013.

[19] Kunka, B., Kostek, B., *Objectivization of Audio-Visual Correlation Analysis, Archives Acoustics*, 37, 1, 63 – 72, 2012.

[20] Kunka, B., Kostek, B., *New Aspects of Virtual Sound Source Localization Research*, Audio Eng. Soc. , 61, 5, 280-289, 2013.

[21] Kunka, B., Kostek, B., *Exploiting audio-visual correlation by means of gaze tracking*, International Journal of Computer Science and Applications, Multimedia - Applications and Processing, 7, 3, 104 -123, 2010.

[22] Kunka, B., Kostek, B., Kulesza, M., Szczuko, P., Czyzewski, A., *Audio-Visual Correlation Analysis Employing Gaze-Tracking and Quality of Experience Methodology*, Human-Computer Interaction in Knowledge-based Environments Special Issue of the Intelligent Decision Technologies Journal, Intelligent Decision Technologies 4(3): 217-227, 2010.

[23] Lappi, O., Pekkanen, J., Itkonen, T.H., *Pursuit Eye-Movements in Curve Driving Differentiate between Future Path and Tangent Point Models*, PLOS ONE, Vol. 8, Issue 7, July 2013.

[24] Lewin, I., *Digital Billboard Recommendations and Comparisons to Conventional Billboards*, Lighting Sciences, Inc., 2009

[25] Lisowski, K., Czyżewski, A., *Modelling Object Behaviour in a Video Surveillnace System Using Pawlak's Flowgraph*; MCSS 2014 - Multimedia Communications, Services and Security, pp. 122 - 136, Kraków, Polska, (2014).

[26] Molino, J. A., Wachtel, J., J. E. Farbry, M. B. Hermosillo, T. M. Granda, *The Effects of Commercial Electronic Variable Message Signs (CEVMS) on Driver Attention and Distraction: An Update*. US Dept. of Transportation, Federal Highway of Transportation, 2009.

[27] Multimedia Description Schemes, http://mpeg.chiariglione.org/standards/mpeg-7/multimediadescription-schemes (data dostępu 29.03.2015).

[28] Perez, W.A., Bertola, M.A., Kennedy, J.F., Molino J.S., *Driver Visual Behavior in the Presence of Commercial Electronic Variable Message Signs (CEVMS)*, National Highway Traffic Safety Administration, Report No. FHWAHEP-11-014, March 2011.

[29] Perez, W., Bertola, M.A., *The Effect of Visual Clutter on Driver Eye Glance Behavior*, Proc. of the Sixth International Driving Symposium on Human Factors in Driver Assessment, Training and Vehicle Design, pp. 180-186, Lake Tahoe, USA, 2011.

[30] Perez, W. A., Bertola, M. A., J. F. Kennedy, J. A. Molino, *Driver Visual Behavior in the Presence of Commercial Electronic Variable Message Signs (CEVMS)*. US Dept. of Transportation, Federal Highway of Transportation, 2012. http://www.fhwa.dot.gov/real_estate/oac/visual_behavior_report/final/cevmsfinal.pdf

[31] Polska norma PN – EN 13201:2007 *Oświetlenie dróg*.

[32] Sisiopiku, V. P., Islam, Md M., Wittig, S., Welburn, S. C., Stavrinos, D., *Perceived and Real Impacts of Digital Advertising Billboards on Driving Performance*; Proceedings of the 5th International Conference on Applied Human Factors and Ergonomics AHFE 2014, Kraków, Poland 19-23 July 2014

[33] Summala, H., Hietamäki, J., *Drivers' immediate responses to traffic signs*. Ergonomics 27(2), pp. 205-216, 1984.

[34] Symon, E., *Statystyki wypadków*. Wydział Ruchu Drogowego, Biura Prewencji i Ruchu Drogowego KGP, 2015: http://statystyka.policja.pl/download
/20/156960/Raportroczny2014r.pdf

[35] Szwoch, G., Dalka, P., *Detection of vehicles stopping in restricted zones in video from surveillance cameras*. 7th International Conference Multimedia

Communications, Services and Security MCSS, Springer Communications in Computer and Information Science, vol. 429, pp. 242 - 253, Springer, 2014.

[36] *Śmigacz, A., Badania* kierowców – kontrastometria. Expert Medyczny (3), 2002,http://www.emedyk.pl/artykul.php?idartykul_rodzaj=72&idartykul=590

[37] Tarnowski, A., *Widzenie zmierzchowe a bezpieczeństwo na drogach*. Transport samochodowy (1), Wydawnictwo ITS, Warszawa 2012. http://www.its.waw.pl/transportsamochodowy/Numer_1_2012,0,3091,1.html

[38] Ustawa z dnia 21 marca 1985 r. o drogach publicznych (tekst jednolity: Dz. U. 2013 r. poz. 260).

[39] Wang, D.-Y.D., Entsminger, S., *Age and Attentional Capacity*, Proc. of the Fifth International Driving Symposium on Human Factors in Driver Assessment, Training and Vehicle Design, pp. 427-432, Big Sky, USA, 2009.

[40] Waugh, B., *Color boosts brain performance and receptivity to advertising*, depending on task: UBC study, http://www.eurekalert.org/pub_releases/2009-02/uobc-cbb020409.php (data dostępu 29.03.2015).

[41] Whitaker, L. A., Sommer, R., *Perception of* traffic guidance signs containing conflicting symbol and direction information. Ergonomics 29(5), pp. 699-711, 1986.

**Sławomir GAJEWSKI, Małgorzata GAJEWSKA,
Ryszard KATULSKI**
Politechnika Gdańska,
Wydział Elektroniki, Telekomunikacji i Informatyki,
Katedra Systemów i Sieci Radiokomunikacyjnych

NOWOCZESNE ROZWIĄZANIA TRANKINGOWE NA POTRZEBY SŁUŻB – SYSTEM LTE

STRESZCZENIE

W opracowaniu przedstawiono rozwiązania systemów trankingowych-dyspozytorskich opartych na systemie LTE. Omówiono rozwiązanie w postaci odrębnego systemu trankingowego LTE/TDD oraz scharakteryzowano koncepcję systemu trankingowego LTE/FDD pracującego w oparciu o infrastrukturę publicznych sieci komórkowych.

Słowa kluczowe:
LTE, tranking, system dyspozytorski

WSTĘP

Wymagania co do właściwości systemów dyspozytorskich-trankingowych pozostają w ścisłej zależności od potrzeb odbiorców. Z tego względu nieco inne wymagania stawia np. policja czy straż graniczna, a trochę inne potrzeby dotyczą np. instytucji transportowych (np. kolej, transport drogowy, porty handlowe i transport morski) oraz duże przedsiębiorstwa (np. fabryki, stocznie).

Ważnym aspektem decydującym o przydatności takich systemów jest rozległość infrastruktury systemowej, czyli również obszar pokrycia radiowego. Jest to szczególne istotne, ponieważ specyfika systemu dyspozytorskiego zależy od tego czy ma on pracować lokalnie na jakimś obszarze, czy też jego obszar pokrycia ma obejmować np. całe państwo.

Ponadto może to być infrastruktura niezależna – wówczas gdy służba oczekuje systemu, który jest jej własnością i nikt nie ma do niego dostępu, ani nie może korzystać z jego infrastruktury. Natomiast jest możliwe również wy-

korzystanie infrastruktury zależnej od operatora telekomunikacyjnego, np. komórkowego albo wykorzystanie współdzielonej infrastruktury systemu dyspozytorskiego.

System może również pracować jako system zamknięty lub otwarty. W pierwszym przypadku nie ma możliwości komunikacji z takim systemem z telekomunikacyjnych sieci zewnętrznych. Natomiast w drugim przypadku funkcjonuje styk np. z siecią Internet, PSTN (ang. Public Switched Telephone Network) czy siecią komórkową. Ostatecznie o przydatności systemu dla służb decyduje również zapewniany przez niego poziom bezpieczeństwa transmisji i zabezpieczeń kryptograficznych.

Rozwiązania trankingowe dla służb, bazujące na systemie TETRA (ang. *Trans European Trunked Radio*) lub DMR (ang. *Digital Mobile Radio*) [1, 2], które są obecnie najbardziej popularne w Polsce, posiadają dzisiaj silną konkurencję w postaci systemu LTE (ang. *Long Term Evolution*). LTE może bowiem stanowić interesującą przeciwwagę dla tych systemów z uwagi na swój ogromny potencjał rozwojowy i znacznie lepsze właściwości techniczne. Nie ma wątpliwości, że systemy TETRA i DMR w znacznym stopniu spełniają oczekiwania odbiorców, szczególnie w zakresie funkcji dyspozytorskich, usług głosowych oraz bezpieczeństwa transmisji. Dlatego wciąż są one głównymi rozwiązaniami stosowanymi w praktyce przez służby i instytucje. Jednak nie sposób nie zauważyć bardzo dynamicznego rozwoju ogólnodostępnych systemów komórkowych – w chwili obecnej LTE, które zmieniły i w dalszym ciągu zmieniają oblicze współczesnej radiokomunikacji, a w konsekwencji - również systemów dyspozytorskich. Standaryzacja TETRY i DMR jest wciąż dynamiczna, a systemy te stanowią bezpieczne i dobre narzędzie dla służb. Obydwa te profesjonalne systemy posiadają wiele zalet bardzo ważnych z punktu widzenia różnych służb, np. kolejowych, straży granicznej, policji, wojska, pogotowia itd. Stawiają one jednak w zamian bardzo liczne ograniczenia.

Rozwój technologiczny TETRY i DMR, szczególnie ze względu na wąskie kanały częstotliwościowe, nie nadąża za ogólnodostępnymi systemami komórkowymi, które oferują coraz większe szybkości przesyłania danych oraz niezwykle szeroki wachlarz usług. Ponadto upowszechnianie dostępności TETRY i DMR wymaga budowy kosztownej infrastruktury technicznej, czemu budżety służb mundurowych najczęściej nie są w stanie sprostać. Z tego powodu tempo budowy tych systemów i ich unowocześniania jest bardzo powolne i obarczone ograniczeniami, zwłaszcza w zakresie efektywności widmowej i osiąganych szybkości transmisji.

Zatem mimo wielu zalet systemów TETRA i DMR coraz bardziej widoczna jest ich słabość aplikacyjna. Dlatego w ostatnich latach więcej czasu poświęca się wykorzystaniu publicznych systemów komórkowych na potrzeby systemów dyspozytorskich. Wprowadza to oczywiście nowe ograniczenia, ale otwiera także zupełnie nowe możliwości w zakresie realizacji usług. Ogólnodo-

stępne sieci komórkowe pozwalają na wydzielenie pewnych zasobów systemowych na potrzeby rozwiązań dyspozytorskich, oferują o wiele większe pasmo częstotliwościowe, efektywność widmową oraz osiągane szybkości transmisji i umożliwiają wykorzystanie gotowej infrastruktury, co stanowi ich oczywisty atut.

DLACZEGO SYSTEM DYSPOZYTORSKI LTE ?

Jak wiadomo, system LTE jest nowoczesnym systemem komórkowym zapewniającym bardzo szybką transmisję danych, w celu elastycznej realizacji usług telekomunikacyjnych i inteligentnego przekazu danych w sieci radiokomunikacyjnej i szkieletowej, wyłącznie w trybie komutacji pakietów. Tak definicja systemu oznacza, że sieć komunikacyjna systemu LTE jest w istocie siecią typu „all IP", w której nie funkcjonuje już transmisja realizowana w trybie komutacji kanałów.

Wykorzystanie takiego systemu do celów dyspozytorskich- trankingowych może być interesujące z uwagi na to, że:

- szerokopasmowa transmisja danych otwiera nowe możliwości usługowe w zakresie nowoczesnego trankingu – dotychczas pojęcie trankingu ograniczało się do realizacji usług przesyłania sygnałów mowy;
- istnieje gotowa infrastruktura telekomunikacyjna, a więc nie ma konieczności – chociaż jest możliwość – budowy własnej sieci i zarządzania rozległą infrastrukturą;
- poziom bezpieczeństwa w sieci jest porównywalny z bezpieczeństwem sieci Internet z możliwością wykorzystania wirtualnych sieci prywatnych (ang. *Virtual Private Networks* –VPN);
- jest możliwe budowanie sieci prywatnych LTE, zwłaszcza w trybie TDD (ang. *Time Division Duplex*) – także odizolowanych od Internetu i od pozostałych sieci komórkowych, a więc o podwyższonym poziomie bezpieczeństwa;
- jest możliwa integracja z sieciami TETRA lub DMR w zakresie zdefiniowanym przez usługobiorcę, aczkolwiek LTE docelowo może osiągnąć zdolność całkowitego zastąpienia TETRY, w tym również dla zastosowań np. policyjnych;
- istnieje realna perspektywa pokrycia radiowego całego kraju przez sieć LTE.

ROZWIĄZANIA SYSTEMOWE LTE W TRYBIE TDD

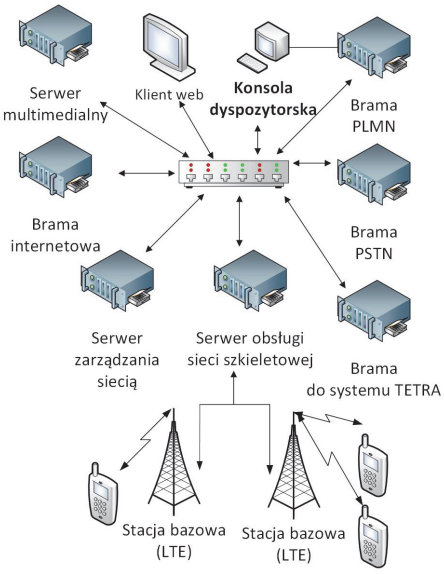
System LTE umożliwia obecnie tworzenie rozwiązań dyspozytorskich, przy czym rozwiązania firmowe koncentrują się zwłaszcza na systemie LTE pracującym w trybie dupleksu czasowego TDD. Dzieje się tak, dlatego że kanały częstotliwościowe w systemie LTE mają o wiele większą szerokość od kanałów TETRY czy DMR. Najwęższy możliwy kanał ma szerokość 1,4 MHz, a najczęściej proponuje się użycie do celów trankingowych kanałów o szerokości 5 MHz. Jest oczywiste, że nie łatwo wydzielić kanały o takiej szerokości z dostępnego pasma, dla potrzeb licznych podmiotów zainteresowanych wdrożeniem systemu trankingowego LTE. Dlatego dominującym rozwiązaniem w tym przypadku z pewnością stanie się system LTE/TDD, który wymaga użycia tylko jednego kanału dla obu kierunków transmisji – od stacji bazowej do ruchomych oraz od stacji ruchomych do bazowej.

Proponowane systemy trankingowe LTE/TDD są systemami prywatnymi, pracującymi niezależnie od publicznych sieci komórkowych, co często stanowi warunek konieczny. Stanowią one pełnowartościowy substytut takich systemów jak TETRA, ale zapewniający znacznie poszerzoną gamę usług, zwłaszcza związanych z transmisją sygnałów obrazu i danych. W chwili obecnej producenci sprzętu radiokomunikacyjnego opracowują i doskonalą rozwiązania systemowe oparte na technologii LTE, dedykowane do celów dyspozytorskich [3, 4], pracujące w trybie TDD.

Wykorzystanie trybu dupleksu czasowego TDD daje również możliwość swobodnego kształtowania wykorzystania zasobów radiowych systemu, dzięki przesyłaniu w obu kierunkach transmisji (w górę i w dół) sygnałów w tym samym kanale częstotliwościowym. Odbywa się to dzięki możliwości niezależnego przydziału ramek czasowych, a więc również zasobów czasowo-częstotliwościowych dla obu kierunków transmisji.

Przykładową architekturę systemu LTE/TDD w roli systemu dyspozytorskiego przedstawiono na rys. 1. Główne właściwości takiego rozwiązania obejmują w szczególności:

- wydzieloną i niezależną od innych systemów radiokomunikacyjnych (komórkowych) sieć szkieletową, w znacznym stopniu uproszczoną w porównaniu do sieci szkieletowej LTE w trybie FDD;
- tranking realizowany w oparciu o sieć dedykowanych stacji bazowych;
- serwery dyspozytorskie i multimedialne;
- zespoły serwerowe do celów komunikacji z sieciami zewnętrznymi.



Rys. 1. Przykładowa architektura systemu dyspozytorskiego LTE/TDD

Podstawowe funkcje komunikacji w sieci szkieletowej systemu trankingowego LTE/TDD pełnią urządzenia sieciowe w postaci serwera obsługi sieci szkieletowej oraz serwera zarządzania siecią. Umożliwiają one komunikację wewnątrz wydzielonej infrastruktury sieci trankingowej LTE, rozbudowę tej sieci oraz zarządzanie jej zasobami, a także sprawowanie całościowej kontroli nad systemem.

Na uwagę zasługują tu także rozbudowane funkcje multimedialne realizowane z użyciem zespołu serwerów oznaczonych na rys. 1 jako serwer multimedialny. W rzeczywistości może być to zespół zawierający serwer dyspozytorski i przetwarzania danych oraz serwer rejestracji i odtwarzania danych multimedialnych, a także inne urządzenia, jak klient sieci web, konsola dyspozytorska itp.

System trankingowy LTE/TDD zawiera również konsolę dyspozytorską, bramy wyjściowe do sieci zewnętrznych, w tym: sieci komórkowych (brama PLMN), telefonicznych (brama PSTN), bramę do systemu TETRA, bramę internetową itp.

PROPOZYCJA WYKORZYSTANIA SIECI PUBLICZNEJ LTE DO CELÓW TRANKINGOWYCH I DYSPOZYTORSKICH

W ramach proponowanej koncepcji, na cele dyspozytorskie może zostać wydzielona dedykowana infrastruktura sprzętowa i programowa, co umożliwi

rozszerzenie funkcjonalności systemu LTE, który w tym przypadku pracuje w trybie dupleksu częstotliwościowego FDD (ang. *Frequency Division Duplex*). Nowe funkcje systemowe mogą być realizowane niezależnie od udziału operatora komórkowego, aczkolwiek w tym przypadku nie jest możliwe tworzenie odrębnej infrastruktury szkieletowej i dostępowej. Natomiast realizacja funkcji dyspozytorskich odbywa się prawie wyłącznie w wysokich warstwach sieciowych. Rozwiązanie takie posiada szereg zalet i wad w odniesieniu do systemu LTE/TDD.

Możliwość wykorzystania gotowej infrastruktury sieciowej (publicznej) LTE ogranicza koszty budowy infrastruktury i jej utrzymania, a więc umożliwia korzystanie z usług dyspozytorskich podmiotom, których nie stać na budowę i eksploatację odrębnej sieci oraz nie wymaga zakupu prawa do korzystania z kanału częstotliwościowego itp. Niewątpliwie stanowi to ogromną zaletę dla wielu podmiotów. Ponadto wykorzystanie systemu ogólnodostępnego poszerza również znacznie zakres dostępnych usług oraz zasięg sieci radiokomunikacyjnej.

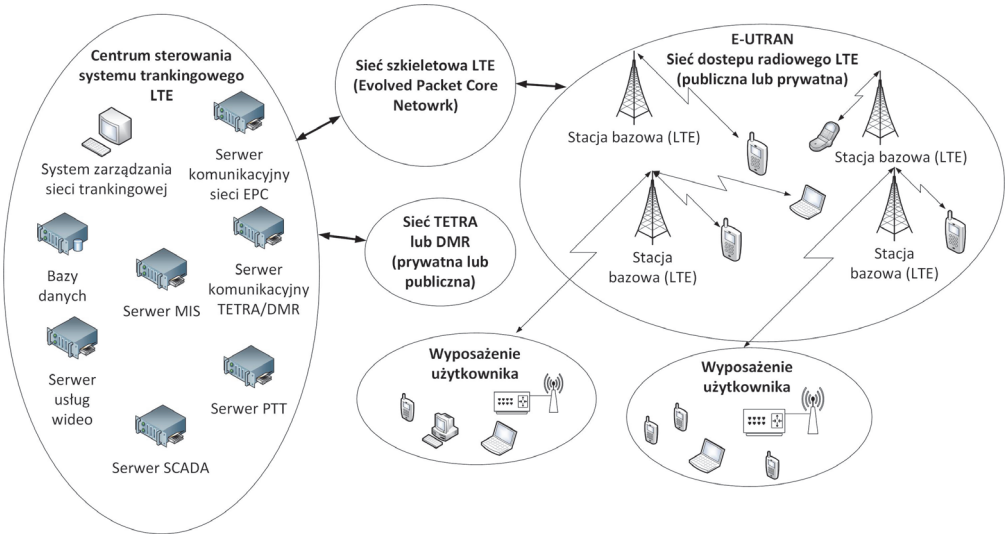
Natomiast największą wadą takiego rozwiązania jest niemalże niemożliwe sprawowanie efektywnego nadzoru nad zasobami sieciowymi i infrastrukturą komunikacyjną, a także utrudnione (a więc również kosztowne) lub niemożliwe zrealizowanie priorytetyzacji połączeń, a także zależność od operatora sieci komórkowej i uzależnienie od zewnętrznego obciążenia sieci.

Mimo to, system taki może posiadać własny podsystem zarządzania oraz zespół urządzeń i serwerów wspomagających jego funkcje dyspozytorskie. Ponadto przy zastosowaniu tuneli wirtualnej sieci prywatnej VPN jest możliwe osiągnięcie pewnej izolacji od dostępu użytkowników nieuprawnionych i zapewnienie znacznego poziomu bezpieczeństwa transmisji, porównywalnego do systemów bankowych. Jednak nigdy nie będzie on taki, jak w systemie działającym odrębnie, a system będzie w większym stopniu narażony na ataki intruzów w sieci telekomunikacyjnej.

Warto podkreślić, że jest możliwe także blokowanie zasobów systemu LTE na potrzeby dyspozytorskie w celu zwiększenia jego niezawodności w trakcie np. zarządzania kryzysowego. Jest to rozwiązanie kosztowne, ale możliwe.

ARCHITEKTURA SYSTEMU DYSPOZYTORSKIEGO LTE/FDD W SIECI PUBLICZNEJ

W ramach proponowanego rozwiązania zostaje wydzielony obszar funkcjonalny, który nazwano „Centrum sterowania systemu trankingowego LTE", który stanowi serce działania systemu trankingowego, co pokazano na rys. 2.



Rys. 2. Architektura proponowanego rozwiązania systemu trankingowego LTE/FDD

Jak widać, system trankingowy LTE może z tego poziomu komunikować się oraz współdziałać z systemami TETRA i/lub DMR w pełnym lub ograniczonym zakresie, który zależy od przyjętych rozwiązań dedykowanych dla danej instytucji, służby itp. Jednak podstawę komunikacji w systemie trankingowym stanowi komunikacja poprzez publiczną sieć LTE, czyli łączność za pośrednictwem sieci szkieletowej LTE pod nazwą EPC (ang. *Evolved Packet Core Network*).

Należy zauważyć, że system trankingowy pracuje w trybie komutacji pakietów, podobnie jak system komórkowy, co daje możliwość zwiększenia efektywności transmisji w porównaniu z komutacją kanałów. Rozwiązanie to pozwala na tworzenie wewnętrznych sieci prywatnych VPN w celu zwiększenia bezpieczeństwa transmisji. Natomiast komunikacja z systemem TETRA może odbywać się również w trybie komutacji kanałów. Do realizacji łączności jest konieczne wykorzystanie terminali wielosystemowych.

Dostęp radiowy do terminali użytkowników odbywa się za pośrednictwem sieci dostępowej systemu LTE pn. E-UTRAN (ang. *Enhanced-Universal Terrestrial Radio Access Network*), z wykorzystaniem węzłów (stacji) bazowych tego systemu (ang. *Node B*).

Obszar działania użytkowników końcowych obejmuje niemalże dowolny sprzęt zaliczany do wyposażenia użytkownika CPE (ang. *Customer Premises Equipment*). Przykładowo, jest możliwe tworzenie sieci wewnętrznych w oparciu o dodatkowe wyposażenie użytkowników i zastosowanie routingu (np. *Wi-Fi*). Oczywiście funkcję terminali użytkowników mogą stanowić urządzenia różnego rodzaju, w tym laptopy, smartfony i in., a do CPE zaliczyć można rów-

nież: telefony, rutery, switch'e, lokalne bramy (ang. *gateways*), urządzenia STB (ang. *Set-Top-Box*), urządzenia peryferyjne w tym wyposażenie terminali ruchomych, adaptery sieciowe dla sieci lokalnych LAN, punkty dostępowe itp. Przy czym można tu również wykorzystać terminale o podwyższonej odporności (np. na wodę, uszkodzenia mechaniczne itp.), tak jak w klasycznych systemach trankingowych-dyspozytorskich.

Centrum sterowania systemu trankingowego LTE może zawierać różne elementy sieciowe umożliwiające realizację odmiennych usług transmisji danych, usług głosowych i in. W zależności od potrzeb oraz użytkowanych systemów. W skład centrum mogą wchodzić:

- system zarządzania systemem trankingowym;
- wspomagające bazy danych;
- serwer komunikacyjny do współpracy z siecią komórkową LTE;
- węzeł komunikacyjny dla sieci TETRA lub DMR;
- serwer usługowy dla systemu zarządzania informacją MIS (ang. *Management Information System*);
- serwer sterowania i akwizycji danych SCADA (ang. *Supervisory Control and Data Aquisition*);
- serwer usług wideo;
- klasyczny serwer dla usług typu PTT (ang. Push-to-Talk), typowy dla systemów trankingowych i in.

Powyższa lista nie jest zamknięta i faktyczny dobór usług i sprzętu zależy od potrzeb odbiorcy systemu. Jak widać, znaczna część wyżej wymienionych urządzeń obejmuje usługi wymagające szerokiego pasma transmisyjnego i dużych szybkości transmisji, które obecnie mogą być dostępne wyłącznie w systemach komórkowych, takich jak LTE.

System może umożliwić realizację wielu usług, które w ogólności nie były wcześniej dostępne dla systemów dyspozytorskich. Do usług tych należą np.:

- usługi sterowania przemysłowego oraz akwizycji danych, tzw. SCADA, realizujące transmisję szerokopasmową sygnałów wizyjnych oraz szybką transmisję danych, oraz umożliwiające akwizycję informacji różnego rodzaju, obiektów przemysłowych oraz baz wojskowych, policyjnych itp.;
- lokalne i rozległe systemy zarządzania informacją MIS, czyli systemy komputerowe dla biznesu i innych organizacji, przeznaczone do rejestrowania i analizy danych z różnych jednostek organizacyjnych oraz ich dostarczania do jednostek nadrzędnych (zarządzających), w postaci

uporządkowanej, aktualnej i odpowiednio przetworzonej, np. stanów magazynowych, danych statystycznych, raportów finansowych itd.;
- usługi wideo, w tym bezprzewodowe, np. do transmisji sygnałów multimedialnych i monitoringu przemysłowego np. rafinerii, gazociągów, portów, stoczni i in. oraz do przesyłania filmów różnego pochodzenia i przeznaczenia.

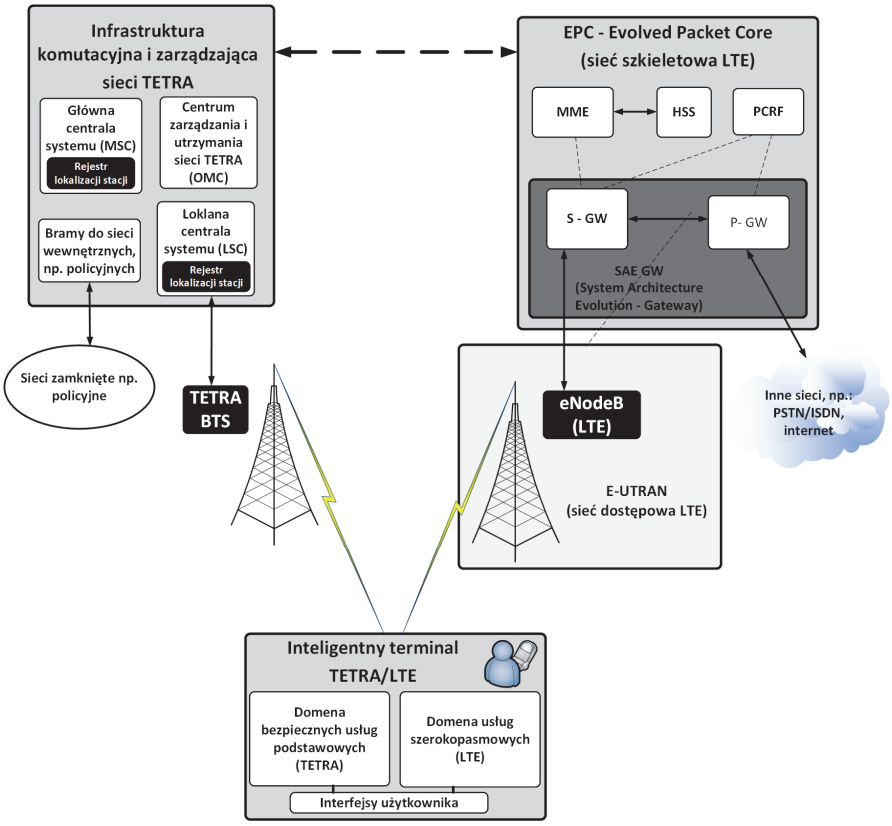
PROBLEM INTEGRACJI SYSTEMÓW LTE I TETRA

Upowszechnienie się dyspozytorskich rozwiązań dla LTE będzie zapewne coraz większe, ponieważ system ten pod względem osiąganych szybkości transmisji uważa się powszechnie za przełomowy. Niezależnie więc od rozwoju TETRY czy DMR jako systemów dedykowanych dla zastosowań specjalnych, należy się spodziewać zarówno niezależnie działających rozwiązań dyspozytorskich LTE, jak i rozwiązań integrujących system TETRA z LTE. Jest oczywiste, że szybka transmisja danych w systemie TETRA nigdy nie będzie możliwa w takim zakresie jak w LTE i nigdy nie osiągnie tak dużego stopnia nowoczesności. Tempo rozwoju LTE jest dla TETRY niedoścignione, bo potencjał firm zajmujących się wdrażaniem LTE jest sumarycznie o wiele większy niż potencjał firm wdrażających TETRĘ.

Wiele firm zajmujących się LTE proponuje jednak rozwiązania integrujące TETRĘ z LTE, co przy jednoczesnym rozwoju usług dyspozytorskich w LTE staje się bardzo interesujące. Już w chwili obecnej niektórzy potentaci na rynku TETRY, mający także swój udział w LTE, projektują i testują urządzenia, które mogą jednocześnie obsługiwać zarówno TETRĘ, jak i LTE. Przy takim podejściu TETRA ewoluować będzie w kierunku integracji z LTE.

Jedną z koncepcji rozwoju procesu integracyjnego jest oferta realizacji usług pn. „TETRA za pośrednictwem LTE" (ang. TETRA *Communications over* LTE) [3]. Propozycja ta obejmuje uruchomienie w sieci LTE pełnego zbioru usług typowych dla TETRY i wprowadzenie do użytku odpowiednio zaprojektowanych terminali dwusystemowych lub wielosystemowych. Terminale takie będą uodpornione mechanicznie i odporne na narażenia, podobnie jak w klasycznej TETRZE. Nie można więc wykluczyć pełnego zastąpienia TETRY przez LTE w miarę upływu czasu.

Pierwotna droga ewolucji TETRY w kierunku LTE obejmuje usługi szybkiej transmisji danych wymagające szerokiego pasma transmisyjnego, a więc np. usługi multimedialne, złożoną obsługę baz danych, transmisję obrazów, sygnałów audiowizualnych itp. Natomiast rdzeń obsługi połączeń głosowych w tym przypadku może na długo pozostać raczej po stronie TETRY.



Oznaczenia: MME – Mobility Management Entity (moduł zarządzania mobilnością), HSS – Home Subscribtion Server (baza danych użytkowników), P-GW – Packet Data Network Gateway (brama wyjściowa), S-GW – Serving Gateway (podstawowy serwer usługowy), eNodeB – stacja bazowa, PCRF - Policy and Charging Resource Function (moduł zarządzania usługami i parametrami QoS)

Rys. 3. Architektura systemu integrującego systemy TETRA i LTE z zachowaniem ich niezależności infrastrukturalnej

Podstawą współpracy obu systemów jest zachowanie granicy pomiędzy oprogramowaniem terminala wspierającym TETRĘ a oprogramowaniem wspierającym LTE. Jest to rozwiązanie proponowane z uwagi na wysoki poziom bezpieczeństwa TETRY, które jednakowoż nie musi być zawsze stosowane. Jednak dzięki temu mamy możliwość udostępnienia usług LTE, przy jednoczesnym zachowaniu integralności, hermetyczności i wysokiego poziomu bezpieczeństwa TETRY, poprzez izolację obu systemów.

Tego typu problem jest analizowany ze względu na zgłaszane potrzeby służb, które wciąż unikają korzystania z sieci otwartych. Jasne, że przy takim ujęciu TETRA może dalej pozostać zamknięta dla służb i nie musi być narażona na ewentualny dostęp osób niepowołanych z sieci publicznej. Tworzenie sieci

zamkniętych stanowi bowiem typowy sposób zabezpieczania specjalnych systemów komputerowych przed ingerencją osób niepowołanych ze świata zewnętrznego.

Na rys. 3 przedstawiono architekturę systemu do integracji TETRY z LTE z zachowaniem ich niezależności. Jak widać, zostały tu całkowicie rozdzielone obszary zarządzania sieciami, a przerywana strzałka łącząca sieci symbolizuje jedynie opcjonalną, ewentualną możliwość wprowadzenia komunikacji obu sieci z pominięciem terminali użytkownika. W ogólności jednak sieci szkieletowe obu systemów pozostają rozdzielone, podobnie jak sieci dostępowe. W przedstawionym wariancie nie ma też możliwości komunikacji z sieci zewnętrznych obsługiwanych przez LTE do sieci TETRA i odwrotnie z sieci zewnętrznych obsługiwanych przez TETRĘ do LTE. Oznacza to, że dla obszaru działania TETRY jest możliwy wyłącznie dostęp do komputerowych sieci zamkniętych. Natomiast dostęp do sieci publicznych, z terminala użytkownika jest możliwy wyłącznie poprzez sieć LTE. Z pośrednictwem sieci LTE mogą być realizowane zarówno usługi głosowe, jak i szerokopasmowe.

Inteligentny terminal TETRA-LTE posiada dwie całkowicie rozdzielne domeny, w których zdefiniowano wyłącznie możliwość niezależnej realizacji usług podstawowych TETRY albo możliwość realizacji usług podstawowych i szerokopasmowych poprzez sieć LTE. Dzięki temu nie ma możliwości dotarcia do danych przesyłanych w sieci TETRA z sieci LTE i odwrotnie. Całość funkcjonalna połączona jest jedynie interfejsami użytkownika.

WNIOSKI

Nie ma wątpliwości, że rozwiązania dyspozytorskie oparte na systemie LTE będą coraz popularniejsze. Rozwój będzie dotyczył zarówno niezależnie działających rozwiązań dyspozytorskich LTE pracujących w trybie TDD jako oddzielne systemy trankingowe, jak i systemów pracujących w trybie FDD z użyciem infrastruktury publicznych sieci komórkowych. Budowa tych rozwiązań może jednak wiązać się z koniecznością ich integracji z systemem TETRA i/lub DMR, co może stanowić warunek konieczny wykorzystania systemu LTE do celów dyspozytorskich przez niektóre podmioty, zwłaszcza te które z sieci TETRA czy DMR korzystają już obecnie.

Jest jasne, że szybka transmisja danych w systemie TETRA nigdy nie będzie możliwa w takim zakresie jak w LTE i nigdy nie osiągnie tak dużego stopnia nowoczesności, nawet w przypadku upowszechnienia się podsystemu TEDS (ang. *TETRA Enhanced Data Service*). Tempo rozwoju LTE jest dla TETRY niedoścignione, bo potencjał firm zajmujących się wdrażaniem LTE jest sumarycznie o wiele większy niż potencjał firm wdrażających TETRĘ.

Ponadto system LTE został już przyjęty przez ITU w poczet systemów spełniających wymagania co do bezpieczeństwa, rekomendowanych dla służb. Oznacza to w dalszej perspektywie duże prawdopodobieństwo niemalże całkowitego wyparcia TETRY przez LTE.

Praca została sfinansowana przez Narodowe Centrum Badań i Rozwoju w ramach projektu nr umowy DOBR/0022/R/ID1/2013/03.

BIBLIOGRAFIA

[1] Gajewski S., Gajewska M., Katulski R., *Trunked Radio Solutions for Special Applications*, International Journal of Electronics and Telecommunications Vol 60, No 4, 2014.

[2] Gajewski S., Sokół M., Gajewska M., *Data Protection and Crypto Algorithms' Performance in RSMAD*, IEEE 73rd Vehicular Technology Conf., VTC Spring 2011, Budapest, Hungary, May 2011.

[3] D. Hartman, M. Stephan, X. Cao, D. Wermser, M. Zeuschner, R. Hunger, F. Andjelo, *Initial Development of a SIP-/RTP-based Core Network for the TETRA Mobile Radio System Aiming at Transparent Availability of its Features in LTE*, 16 VDE/ITG Fachtagung Mobilkommunikation, Osnabruck, 2011.

[4] Materiały firmowe Huawei Technologies Co., LTD.

MODERN TRUNKING SOLUTIONS FOR SERVICES – THE LTE SYSTEM

ABSTRACT

In the paper solutions of tranking-dispatch systems based on the LTE system are presented. The solution in the form of separate LTE/TDD trunking system is discussed, and the concept of the LTE/FDD trunking system operating in the infrastructure of public, mobile networks is characterised.

Joanna GRUBICKA
Instytut Bezpieczeństwa Narodowego
Akademia Pomorska w Słupsku

KONWERGENCJA TECHNOLOGICZNA A SYSTEM BEZPIECZEŃSTWA INFORMACJI

STRESZCZENIE

W dobie dzisiejszych czasów zmiany, wywoływane przez konwergencję usług oraz dostęp do najnowszych informacji cyfrowych jest kluczem do wykorzystywania nowoczesnych technologii, a także wpływa na funkcjonowanie gospodarki rynkowej. Źródła informacji z branży IT nieustannie donoszą o atakach ukierunkowanych na firmy, szpiegostwo oraz o wzrastającej liczbie kradzieży laptopów, zagubionych kart pamięci oraz smartfonów. W tych okolicznościach bezpieczeństwo poufnych danych staje się priorytetem dla zarówno małych, jak i dużych przedsiębiorstw. W artykule przedstawiono przykładowe incydenty oraz wskazano możliwe do wykorzystania rozwiązania bezpieczeństwa informacji w sieciach Wi-Fi.

WSTĘP

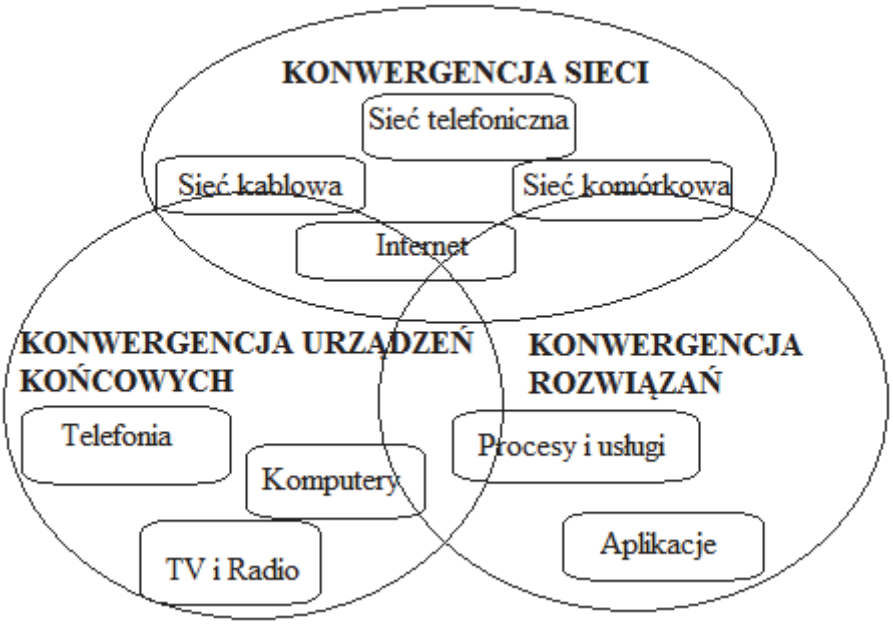
Jeszcze do niedawna tradycyjne środki przekazu informacji takie jak dane, głos, Internet, TV były używane w specjalnie do tego celu wydzielonych odrębnych sieciach telekomunikacyjnych i komputerowych. Rozwiązanie takie stopniowo jest wypieranei zastąpione nowoczesnymi sieciami konwergentnymi. Zjawisko to jest odpowiedziąna zmieniające się realia, zmienność i dynamikę rozwoju współczesnej gospodarki światowej oraz na tworzenie się nowej rzeczywistości, w której trwa nieustanny przepływ towarów, usług i nowych technologii. Oznacza to zmianę warunków życia ludzi, nadając im niejednokrotnie nową formę i uwarunkowania. Siłami napędowymi konwergencji w obszarze e-usług staje się bowiem: Internet, biznes elektroniczny (ang. *e-business*); szybki rozwój aplikacji informatycznych i multimedialnych oraz

wzrost mocy obliczeniowej komputerówi spadek ich cen[1]. Termin konwergencja, pojawiający się w publikacjach o tematyce technicznej, biznesowej, handlowej w obszarze komunikacji elektronicznej, dotyczy zjawisk zachodzących głównie we współczesnych mediach, informatyce i telekomunikacji. Wśród nich wymienić należy: łączny przekaz informacji głosowych i danych, współistnienie przełączania kanałów i pakietów, integracja przekazów głosu przez sieci IP (np. ang. *Voice over Internet Protocol, Voice over Frame Relay*), współdziałanie telefonu z komputerem (np. ang. *Call Center*), integracja sieci lokalnych z rozległymi, współdziałanie sieci bezprzewodowych i przewodowych[2]. Stąd też zmiany w sektorze technologii informacyjno-komunikacyjnych określane są również jako proces „konwergencji technologii informacyjnej[3]", w którym integracja komputerów i telekomunikacji w jednolity system przetwarza i wymiana informacji stworzyła nową architekturę informacyjną, zespalając wszystkie typy i funkcję kanałów komunikacyjnych służących do transmisji głosu, obrazu, danych oraz aplikacji w jedną wielousługową, szerokopasmową sieć opartą na protokole IP (ang. *Internet Protocol*). Obrazowy pogląd na istotę konwergencji przedstawia rysunek 1.

1 J. Grubicka, *Konwergencja w obszarze e-usług a bezpieczeństwo*, Acta Pomerania Chojnice, 2014, s. 152.

2 A. Urbanek, *Czas konwergencji (I) , Networld* Wrzesień 1999.

3 J. Chustecki, T. Janoś, Routery i przełączniki - konwergencja i gigabity*, NetWorld* Listopad 2006.



Rysunek 1. Obszary konwergencji informatyki i telekomunikacji

Są to zarówno płaszczyzny działalności nie istniejące poprzednio, jak też nowe sposoby wykorzystania i łączenia dotychczasowych produktów i usług. Nowe obszary. powstające jako wynik badań naukowych oraz przez podział istniejących dziedzin, są tworzone i rozwijane przez przedsiębiorstwa, działające w pokrewnych sektorach. Rozwój każdej z tych dziedzin jest uzależniony i jednocześnie warunkuje rozwój innej. Wzajemna ich integracja sprzyja powstawaniu zupełnie nowych produktów i rynków lub powoduje całkowitą zmianę reguł i zasad postępowania na dotychczasowych rynkach[4]. Z procesem cyfryzacji i konwergencji urządzeń i sieci dochodzi przede wszystkim do konwergencji usług. Biznes internetowy należy do najbardziej dynamicznie rozwijających się sektorów krajowej gospodarki w ostatnich latach, ale także nowym sposobem na świadczenie usług, m.in. w usługach administracji, medycznych, edukacyjnych, w handlu, w usługach finansowych, turystycznych, ubezpieczeniowych, kultury i innych. Powszechnie używane przez konsumentów konwergencje usług dostępu do informacji umożliwiają na większą standaryzację i obsługi e-klientów. Konwergencja technologiczna, np. w obszarze sieci komunikacyjnych pozwala przedsiębiorstwom, e-klientom m.in. na: zwiększenie ela-

[4] Z. Pierścionek, *Nowe kierunki rozwoju przedsiębiorstw*, [w:] *Strategie rozwoju współczesnych przedsiębiorstw*, red. nauk. Pierścionek Z., Poznańska K., SGH, Warszawa, 2000, s. 13.

styczności biznesowej, redukcję kosztów, zwiększenie przewagi konkurencyjnej, jedność środowiska informatycznego, integralność danych, ułatwienie zarządzania systemami, uproszczenie procesu obsługi, skrócenie czasu dotarcia produktów i usług dla klienta, skrócenie czasu i częstotliwości szkoleń pracowniczych, a w przypadku konieczności utrzymywania więzi z klientami – na możliwość obsługi poprzez wiele kanałów kontaktu z personelem firmy, np. poprzez mail, Skype'a, czy komunikator GG.

Posiadanie dostępu do sieci staje się wymogiem koniecznym dla dobrego funkcjonowania w życiu publicznym. Dotyczy to nie tylko osób prywatnych, a więc posiadaczy komputerów podłączonych do Internetu, właścicieli telefonów komórkowych, smartfonów itp., ale również przedsiębiorstw oraz państwowych i społecznych instytucji, dających możliwość skorzystania z Internetu w miejscu pracy[5]. W tym kontekście mówi się także o ogólnej koncepcji e-urzędów, dzięki którym instytucje mogą łatwiej komunikować się między sobą, a petenci lub klienci uzyskują łatwiejszy kontakt z firmami oraz urzędami[6]. E-konsumenci współczesnych usług doświadczają konwergencji tzw. „konwergencji miejsca" i konwergencji technologii. Zachodzi bowiem proces zacierania granic między jego miejscem pracy i domem. Natomiast cyfrowe, sieciowe oprogramowanie służy pracy kreatywnej, ale także zrządzaniu tą pracą i kontroli. Określa się tym mianem upodobnianie się urządzeń, które zaczynają pełnić podobne funkcje, choć pierwotnie nie były ze sobą technicznie spokrewnione, zarówno na poziomie państw, jak i przedsiębiorstw, to konwergencja technologiczna. Zachodzi na płaszczyźnie infrastruktury i transportowania, czemu odpowiada konwergencja urządzeń, usług i konwergencji siec[7]. Konwergencja dokonuje się w efekcie ludzkich działań, decyzji, określania celów, oceny efektów. Zjawisko konwergencji oznacza poważne wyzwania dla tradycyjnych modeli biznesowych, ale stanowi zarazem zagrożenie dla firm, którym nie uda się wykorzystywać konwergencji i pozostaną w tyle w konkurencyjnym wyścigu.

---

5 A. Białas, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Wydawnictwa Naukowo-Techniczne, Warszawa, 2006.

6 J. Grubicka, E. Matuska, *Bezpieczeństwo konsumenta jako uczestnika e-rynku*, w: Lisiaka H., Stach W., (red) *Bezpieczeństwo współczesnego świata. Historia i bezpieczeństwo publiczne*, Instytut Naukowo Wydawniczy Maiuscula, Poznań 2012, s. 45.

7 T. Białobłocki, J. Moroz, *Nowoczesne techniki informacji i komunikacji – ich rozwój i zastosowanie*, [w:] *Społeczeństwo informacyjne. Istota, rozwój, wyzwania*, Warszawa 2006, s. 132.

SPOŁECZEŃSTWO INFORMACYJNE WOBEC DYNAMIKI PROCESU KONWERGENCJI TECHNOLOGICZNEJ

W literaturze wskazuje się na trzy etapy procesu tworzenia społeczeństwa informacyjnego. Pierwszy etap to powstanie przedsiębiorstw i korporacji tworzących nowe techniki informacyjno-komunikacyjne, drugi to informatyzacja podstawowych działów gospodarki i instytucji, a trzeci to wykorzystywanie w szerokim zakresie nowych technologii do codziennego życia8. Szybki rozwój sieci teleinformatycznych i postęp w tej dziedzinie umożliwił włączenie się do światowego systemu gospodarczego nowym firmom, które wcześniej pozbawione były takiej możliwości. Za pomocą telefonu komórkowego, telefaksu, a zwłaszcza Internetu przeprowadza się coraz więcej transakcji handlowych. E-usługi umożliwiają dokonywanie czynności ekonomicznie i efektywnie, a także pozwalają na bardziej elastyczne funkcjonowanie firm, na koncentrowaniu się w tworzeniu nowych produktów i usług, które wygenerują przychody. Wyrazem takiego postępu procesu technologicznego jest kreowanie społeczeństwa informacyjnego. Powoduje to, iż członek społeczeństwa informacyjnego uzyskuje dostęp do szerokiego zakresu zasobów oferowanych w sieci dotyczących dóbr i usług konsumpcyjnych9. E – biznes wykorzystuje szereg aplikacji internetowych, do których między innymi zaliczyć możemy pocztę, strony i witryny WWW, czy też banery oraz inne środki reklamy. To wszystko ma jeden cel, którym mianowicie jest dotarcie do jak największej grupy potencjalnych klientów i odbiorców.

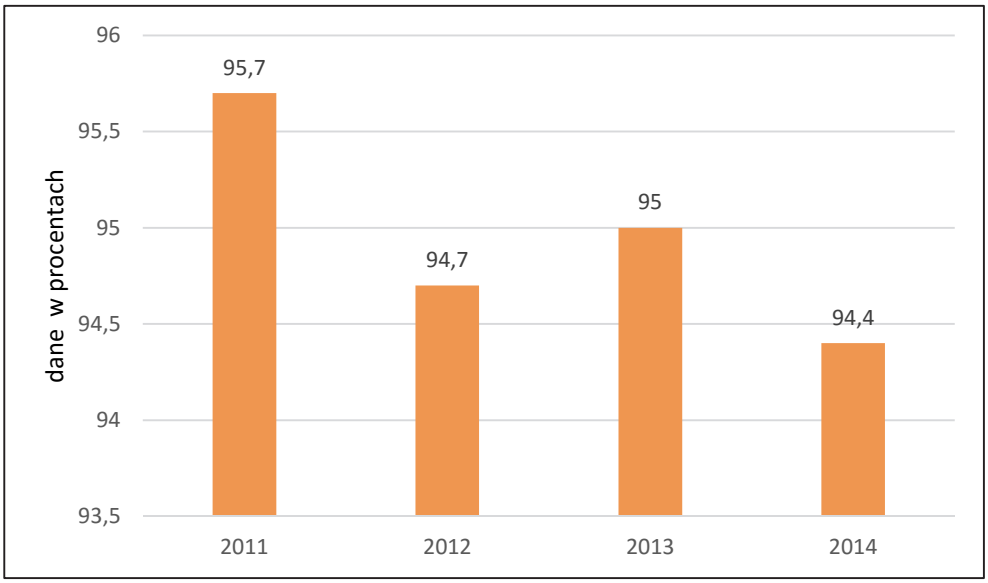
Większe przedsiębiorstwa bywają całkowicie skomputeryzowane, wyposażone w stałe łącze. Coraz powszechniejsze staje się posiadanie przez firmy witryn internetowych, dzięki którym firma jest lepiej znana nie tylko w Polsce, ale także poza jej granicami. Według danych Głównego Urzędu Statystycznego, pod koniec 2014 roku 94 % przedsiębiorstw wykorzystywało komputery w celu prowadzenia swojego biznesu, z kolei 93% miało dostęp do Internetu. Jeśli chodzi o kwestie marketingowe, 65 % przedsiębiorstw posiadało własną stronę internetową[10], przedstawia to wykres 1, który przedstawia jaki procent przedsiębiorstw wykorzystuje komputery. Dane dotyczą lat 2010-2014.

8 A. Dąbrowska., M. Janoś – Kresło, A.Wódkowski, *E-usługi a społeczeństwo informacyjne*, Difin, Warszawa, 2009, s. 26.

9 Ibidem, s. 46.

10 Społeczeństwo informacyjne w Polsce w 2014r., Główny Urząd Statystyczny, 2014.

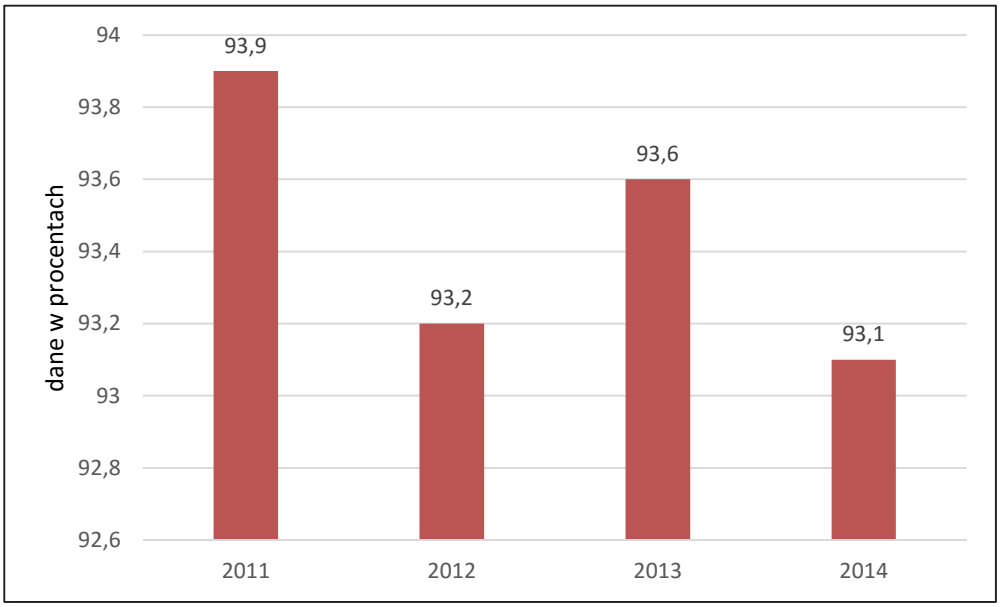
Wykres 1. Procent przedsiębiorstw wykorzystujących komputery



Źródło: Opracowanie własne na podstawie: Społeczeństwo informacyjne w Polsce w 2014r., Główny Urząd Statystyczny, 2014, s. 4.

Na podstawie wykresu 1 można zauważyć, że w roku 2014 w Polsce odnotowano spadek liczby przedsiębiorstw korzystających z komputerów w stosunku do roku 2013. Podobnie wygląda sytuacja w przypadku dostępu przedsiębiorstw do Internetu, co zostało przedstawione na wykresie 2.

Wykres 2. Procent przedsiębiorstw z dostępem do Internetu



Źródło: Opracowanie własne na podstawie: Społeczeństwo informacyjne w Polsce w 2014r., Główny Urząd Statystyczny, 2014, s. 4.

Z jednej strony Internet przyczynia się do rozwoju sektora biznesowego i gospodarczego. Umożliwia on dotarcie do nowych klientów poprzez nowe możliwości reklamy. Ułatwia także kontakt z klientem oraz stwarza nowe sposoby sprzedaży. Z drugiej strony, firma podpięta do Internetu jest narażona na szereg nowych zagrożeń, takich jak Rozproszona Odmowa Usługi czy kradzież. Pierwsze zagrożenie może uniemożliwić prawidłowe funkcjonowanie serwerów, na których znajduje się nasza strona czy usługi. Tym samym, niemożliwy jest kontakt z klientem czy możliwość dalszego oferowania naszych usług. Przy okazji ataku mogą zostać także wykradzione np. dane osobowe naszych klientów i powiązane z nimi informacje niejawne takie jak hasła czy loginy. Tak było w przypadku firmy Sony, kiedy to 4 lata temu z ich usługi sieciowej PlayStation Network, umożliwiającej grę online, kupowanie nowych gier oraz kontakt z innymi graczami, wykradziono dane 77 milionów użytkowników, w tym adresy e-mail, loginy, hasła czy numery kart kredytowych[11]. Drugi przykład zagrożeń, czyli kradzież, spotkał wytwórnię Sony Music. Krótko po ataku na PlayStation Network, w skutek kolejnego, nazwanego największym w historii rynku muzycznego, ataku cybernetycznego, hackerzy wykradli z serwerów tej

[11] http://www.tvn24.pl/wiadomosci-ze-swiata,2/sony-przeprasza-i-wzmacnia-bezpieczenstwo,169620.html [dostęp: 20.05.2015]

firmy 50 tysięcy plików z piosenkami Michaela Jacksona, do których prawa firma Sony nabyła wcześniej za około 250 mln dolarów[12].

Jak pokazuje historia Sony, należy pamiętać, iż chociaż Internet daje wiele możliwości, może także nieść za sobą wiele zagrożeń, które, jeśli zostaną zlekceważone, będą skutkować przykrymi konsekwencjami materialnymi czy wizerunkowymi. Dlatego tak ważne jest dostrzeganie tych zagrożeń, ale przede wszystkim przeciwdziałać przestępczości internetowej przed ciągłą edukację oraz prewencję w tej dziedzinie.

BEZPIECZEŃSTWO INFORMACJI W SIECIACH WI-FI

Wraz z postępem technologii, praca staje się coraz wygodniejsza. Ludzie upraszczają dotąd wykonywane czynności. Ciężko wyobrazić sobie jakikolwiek obszar działania człowieka, który mógłby całkowicie funkcjonować bez baz danych, kodu programu lub komunikacji w sieci. Gdy coś staje się coraz łatwiejsze, niewymagające uwagi często popadamy w rutynę. Brak chęci, czy zbytnia pewność siebie mogą prowadzić do popełniania błędów. Człowiek mając do czynienia z coraz większym postępem technologicznym traci czujność i zbytnio ufa technologii. Szczególnie niebezpieczne jest to w przypadku ochrony informacji, gdzie ich znaczna większość przesyłana jest za pośrednictwem Internetu, często bezprzewodowego, bardziej zagrożonego podsłuchem. Za pomocą popularnej technologii Wi-Fi oraz punktów dostępu można w wygodny sposób połączyć się bezprzewodowo z Internetem. Jednak w praktyce wyciek informacji jest bardziej prawdopodobny niż w przypadku sieci kablowej. Punkty dostępu Wi-Fi są dziś bardzo rozpowszechnione. Występują w domach, pociągach, autobusach, w centrach handlowych, instytucjach publicznych, itp. Podzielić te sieci można na publiczne oraz prywatne, posiadające autoryzację lub nie i takie, które posiadają zabezpieczenia w postaci szyfrowania i sieci nieszyfrowane. Sieci domowe, publiczne, itp. nie zawsze są szyfrowane, więc każdy może uzyskać do nich dostęp. Chcąc przesyłać ważne informacje za pośrednictwem sieci Wi-Fi trzeba zwrócić uwagę na poziom jej zabezpieczeń. Tworząc własną sieć bezprzewodową w pewnym stopniu można wprowadzić pewne mechanizmy bezpieczeństwa, np. odpowiednio konfigurując punkt dostępu, jednakże kiedy korzystamy z innej sieci nie ma się wiele możliwości. Można jedynie zabezpieczyć mobilne urządzenie, komputer, lub inny sprzęt, z którego korzysta się. W bezprzewodowej sieci Wi-Fi najczęściej styczność napotyka się z punktem dostępu, nazywanym routerem. Pośredniczy on między jakimś urządzeniem mającym dostęp do Internetu, a siecią Internet, która tworzy połączone ze sobą

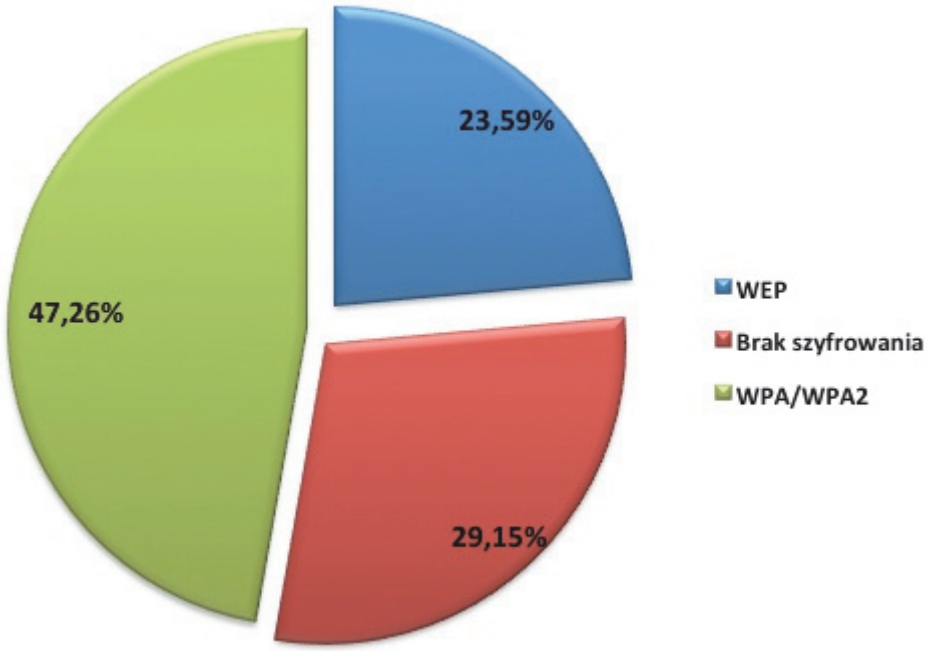
[12] http://www.tvn24.pl/kultura-styl,8/ukradli-pliki-jacksona-za-250-mln-dol,202665.html [dostęp: 20.05.2015]

serwery świadczące rozmaite usługi oraz przechowujące informacje. Router jest w tym wypadku bramą dostępową, czyli przechodzi przez niego cały ruch sieciowy. Podłączony jest on do sieci za pomocą kabla LAN (ang. *Local Area Network*), anteny radiowej, lub innego złącza, udostępniającego Internet od dostawcy, tzw. ISP (ang. *Internet Service Provider*). Do routera za pomocą kabla LAN lub bezprzewodowo podłączane są urządzenia chcące połączyć się z Internetem. Urządzenia takie, to np. komputery stacjonarne, ipody, laptopy, drukarki, telefony IP, tablety, telewizory, konsole do gier, itp. Cała komunikacja odbywa się za pośrednictwem fal elektromagnetycznych, za pomocą komunikacji cyfrowej z urządzeniami, którą zapewniają niezbędne układy elektroniczne oraz protokoły. W celu umożliwienia komunikacji punkt dostępu oraz np. laptop, posiadający bezprzewodową kartę sieciową, muszą się „widzieć" we wspólnym zasięgu. Zależnie od mocy użytych nadajników i rzeźby terenu dystans taki wynosi od kilku do kilkudziesięciu metrów. Kiedy oba urządzenia: karta sieciowa oraz router są oparte o ten sam standard, lub inne, zgodne wstecznie ze sobą zachodzi możliwość połączenia. Konieczne jest by punkt dostępu rozgłaszał swoją nazwę SSID. Kolejna metoda połączenia polega na podaniu nazwy SSID (ang. *service set identifier*) punktu dostępowego, który tą nazwę ukrywa. Można więc ukryć swój router w sieci, jednak nie jest to zbyt skuteczne zabezpieczenie, ponieważ istnieje oprogramowanie zdolne poprzez nasłuch Wi-Fi pozyskać nazwę SSID. Taki tryb pracy punktu dostępowego przekładać się może na zmniejszoną efektywność przepływu danych, na skutek czego pogarsza się jakość połączenia. Gdy powyższe warunki są osiągnięte, zaczyna się nawiązanie połączenia z siecią Wi-Fi. Może to przebiegać na dwa sposoby: punkt dostępu wymaga, bądź nie wymaga uwierzytelnienia, czyli autoryzacji nowych urządzeń. Tryb ten nazywa się WPS (*ang. Wi-Fi Protected Setup*). Zazwyczaj oparty jest on o rozpoznawanie urządzeń po ich adresie fizycznym MAC (*ang. Media Access Control*) karty sieciowej. Jest to niepowtarzalny adres dla każdej karty sieciowej, nadany przez producenta w drodze produkcji. Składa się on z 48 bitów, np. 00:0B:C3:5C:D2:A3, gdzie pierwsze 24 bity tego adresu oznaczają producenta karty sieciowej. Proces autoryzacji realizuje się za pośrednictwem ręcznego wprowadzenia do puli akceptowalnych, bądź blokowanych adresów MAC, tworzy się wtedy tzw. „białe" i „czarne" listy adresów MAC. Można także wcisnąć odpowiedni przycisk na punkcie dostępowym i urządzeniu, które chce się nim połączyć. Umożliwia to w ciągu 2 minut podłączenie nowego urządzenia do routera, które w sposób automatyczny będzie dopuszczone. Metoda ta została uznana za niezbyt bezpieczną, ponieważ w ten sposób intruz może łatwo ominąć wszystkie zabezpieczenia, natomiast metoda oparta o filtrowanie adresów MAC też nie daje stuprocentowej pewności na dopuszczenie pożądanych urządzeń, ponieważ gdy zostanie pozyskany przez intruza adres MAC dopuszczonego przez punkt dostępu urządzenia, można przy użyciu odpowiedniego oprogramowania adres ten zmienić i podszyć się pod autoryzo-

wane urządzenie. Przejście przez proces uwierzytelniający daje nam dostęp do sieci, pod warunkiem, że nie jest szyfrowana i nie wymagane jest podanie klucza. Wymiana informacji pomiędzy punktem dostępu a innym, podłączonym do niego urządzeniem wymaga podziału transmitowanych danych na pakiety, czyli paczki informacji. Wysyłane dane są podzielone na wiele paczek, których nadawanie zaczyna się od nagłówka, czyli informacji o nadawcy, adresacie, dodatkowo przesyłane są informacje o dacie, sumie kontrolnej, itp., oraz dane zawierające właściwą treść. Ta forma transmisji umożliwia kontrolę nad pakietami, w przypadku zagubienia lub zakłócenia transportu któregoś z nich. Ma to na celu uniknięcie błędów, ponieważ maszyny będą wysyłać utracone pakiety aż do pełnego ich skompletowania. Kiedy pakiety są przesyłane jawnie mogą łatwo zostać odczytane w ich postaci źródłowej. Dane, które odbierane są przez kartę sieciową Wi-Fi, za pomocą stosownej aplikacji komputerowej można w łatwy sposób „podejrzeć". Zazwyczaj karta sieciowa działa w takim trybie, że odrzuca wszystkie pakiety, niezaadresowane do niej. Istnieją jednak aplikacje, tzw. sniffery, uznawane za oprogramowanie legalne, służące do monitoringu sieci, pozwalające zmienić konfigurację karty sieciowej, przez co odbierać będzie wszystkie informacje, nawet te nieprzeznaczone dla niej. Pakiety takie kierowane do innych użytkowników stanowić mogą np. fragmenty stron internetowych albo pobieranych plików. Oprogramowanie takie może być wykorzystywane w niewłaściwy sposób, np. przez hackerów. Sniffery mają wbudowane filtry, pozwalające intruzowi w dokładny sposób przefiltrować pakiety pod kątem użyteczności. Dane szczególnie wrażliwe mogą stanowić, np. dane logowania do stron internetowych, kiedy nie wykorzystujemy bezpieczniejszego protokołu HTTPS (*ang. Hypertext Transfer Protocol Secure*), tylko protokół HTTP (*ang. Hypertext Transfer Protocol*), w którym ustanowienie nawet długiego hasła, może niewiele dać. Istnieją jednak pewne mechanizmy pozwalające w jakiejś części utrudnić włamywaczowi dostęp do sieci. W sieciach Wi-Fi, szczególnie domowych często zapomina się zmienić domyślnego loginu i hasła dostępu do panelu administracyjnego punktu dostępu, niezmieniany bywa też jego domyślny adres IP. Zazwyczaj login i hasło w takich sieciach to „admin" i „password", natomiast adres punktu dostępowego to zazwyczaj 192.168.0.1 lub 192.168.1.1. Ustawienie innej nazwy i hasła, które są bardziej skomplikowane i dłuższe mogą odciąć nieautoryzowany dostęp do naszego urządzenia. Zmiana adresu IP z domyślnego na inny może zniechęcić włamywacza do jego odszukania. Gdy nie zmienia się tych ustawień następstwem jest odcięcie od Internetu, czy zmienienie ustawień routera lub przywrócenie go do ustawień fabrycznych, oraz innych nieprzyjemnych dla użytkownika tego konsekwencji. Nie zawsze jednak mamy ten komfort, aby korzystać z własnej sieci bezprzewodowej. Jeśli tak się zdarzy, to nawet gdy sieć do której się podłączamy nie jest zaszyfrowana, są metody, które umożliwiają zabezpieczenie swojego urządzenia, np. laptopa, przed podsłuchem fali radiowej. Gdy już w przeglądarce

ustawimy korzystanie z bezpieczniejszego protokołu HTTPS, możemy dodatkowo zaimplementować inne mechanizmy bezpieczeństwa. Jednym z nich jest szyfrowanie poczty wychodzącej od nas, aby nikt nieautoryzowany nie mógł jej odczytać. Istnieją także programy anonimizujące, które czynią komunikację z Internetem trudną do podsłuchania. Programy takie łączą się z Internetem za pomocą serwerów pośredniczących, które ukrywają adres IP naszego komputera, a także szyfrują całą transmisję. W ten sposób nawet jeśli dane w niezabezpieczonej sieci zostaną przechwycone, stają się nieprzydatne. Istnieje szereg możliwości przechwycenia komunikacji w Internecie, więc ryzyko podsłuchania danych jest duże. Trzeba więc dołożyć wszelkich starań, aby zabezpieczyć sieć, zwłaszcza bezprzewodową. Ma to szczególne odniesienie do przesyłu przez taką sieć informacji niejawnych, wrażliwych danych np. firmowych albo innych instytucji. Należy więc położyć szczególny nacisk na szyfrowanie danych płynących przez naszą sieć bezprzewodową[13]. Szyfrowanie polega na przetwarzaniu danych w taki sposób, aby stały się nieczytelne i zabezpieczone przed nieautoryzowanym dostępem, dzięki czemu mogą z nich korzystać jedynie pożądani odbiorcy. Jest to bardzo prosta i zarazem bezpieczna koncepcja. Jeżeli w żaden sposób nie można odszyfrować, zapoznać się lub skorzystać z informacji, stają się one bezwartościowe. Dlatego też poświęcanie środków na uzyskanie dostępu do zaszyfrowanych informacji całkowicie mija się z celem[14].

[13] E-Terroryzm.pl_Wydanie-specjalne-nr-II.pdf.2013. s.64-67 [dostęp 16.05.2015]
[14] http://www.kaspersky.pl/about.html?s=newsspecial&newsid=2001 [dostęp 23.07.2015]



Rysunek. 2 Statystyki zabezpieczenia sieci Wi-Fi z roku 2012[15]

Osoby, które znajdują się w zasięgu sieci bezprzewodowej mogą „podsłuchiwać" transmisję sieciową, wykorzystując programy przechwytujące pakiety, jeśli więc sieć nie jest zabezpieczona, każdy może się do niej podłączyć i korzystać z jej zasobów bez zgody i wiedzy jej właściciela. Czasem włamywacze pragną jedynie skorzystać z dostępu do Internetu na innego użytkownika koszt, ale niekiedy mogą wykorzystać daną sieć do celów przestępczych, np. podszyć się pod inny adres IP i wykonać, np. atak sieciowy lub inne niepożądane rzeczy. By uniknąć takich nieprzyjemnych incydentów należy zabezpieczyć sieć wykorzystują mechanizm szyfrujący. Już od początku lat 90, wraz z rozwojem standardu 802.11, tworzone są mechanizmy szyfrowania. Pierwszym z nich jest WEP (*ang. Wired Equivalent Privacy*).

[15] Źródło: http://websecurity.pl/wp-content/uploads/2013/01/klp_wifi_czestochowa1.jpg [dostęp 16.05.2015]

Mechanizm ten służy do zabezpieczania informacji transmitowanych w sieci Wi-Fi, szyfruje transmisję pomiędzy punktem dostępu bezprzewodowymi kartami sieciowymi, podłączonymi do niego. W technice WEP korzysta się z algorytmu szyfrowania strumienia, inaczej RC4. Algorytm RC4 jest szybki i prosty w działaniu, jego zastosowanie nie spowalnia zbytnio sieci w stosunku do innych algorytmów, o większym poziomie skomplikowania. Działanie metody WEP jest oparte na wygenerowaniu czterech 64 bitowych kluczy szyfrowania różniących się od siebie, klucze 128 bitowe lub 256 bitowe stosowane są jako rozszerzenie standardu WEP i nie są dostępne na wszystkich urządzeniach. Klucze takie można utworzyć ręcznie, wybierając losowo dziesięć liczb szesnastkowych, lub skorzystać z generatora kluczy. Następnie należy przydzielić wygenerowane klucze do wszystkich kart sieciowych Wi-Fi, które mają uzyskać połączenie z routerem. Proces ten nosi miano dystrybucji kluczy, jest to krytyczny zabieg tyczący się bezpieczeństwa sieci bezprzewodowej. Jeśli punkt dostępu oraz karty sieciowe, które należą do sieci, wprowadziły wszystkie cztery klucze, można wtedy uruchomić szyfrowanie WEP. Po tej operacji wymiana informacji między kartami bezprzewodowymi, a punktem dostępu jest szyfrowana. Za pomocą tego mechanizmu nie można zarządzać kluczami szyfrującymi, ani dystrybuować kluczami automatycznie. Mechanizm WEP nie jest w stanie ukryć także ruchu sieciowego pomiędzy użytkownikami sieci bezprzewodowej, zatem można łatwo wyśledzić przesyłane pakiety. Ta metoda nie uwierzytelnia także użytkowników, bowiem sprawdza wyłącznie klucze szyfrowania, nie jest sprawdzany identyfikator użytkownika, hasło, adres IP. Obecnie mechanizm WEP wychodzi już z użycia, z wprowadzeniem na rynek nowszych urządzeń sieciowych, mogących obsłużyć bardziej skomplikowane mechanizmy szyfrowania, bowiem nie daje on już należytej ochrony sieciom Wi-Fi. Wszystko ulega zmianie gdy w roku 2001 trójosobowy zespół naukowców, w składzie: A. Stubblefield, J. Ioannidis i A. D. Robin z laboratorium AT&T Labs publikuje wyniki badań, z ataku na algorytm RC4 w celu zdobycia hasła do sieci chronionej techniką WEP. Z czasem dochodzi więc do pojawienia się szeregu narzędzi, które udostępnione zostają w sieci Internet do łamania haseł. Wraz z upływem lat, w celu poprawy bezpieczeństwa sieci, w roku 2003 „na szybko" stworzony zostaje kolejny standard szyfrowania o nazwie WPA, obecny szczególnie w urządzeniach standardu 802.11g. Standard ten naprawia niedoskonałości wykryte w standardzie WEP. Poprawiona zostaje długość klucza wynosząca teraz 128 bitów, przez co atak słownikowy staje się prawie niemożliwy do wykonania. Klucze szyfrowania zmieniają się automatycznie, co pewien okres czasu, a ich wymiana dokonuje się w zaszyfrowany sposób, więc czas na podsłuchanie pakietów staje się zbyt krótki. Technika WPA wnosi również do poprawy bezpieczeństwa sieci bezprzewodowej mechanizm uwierzytelniania. Uwierzytelnienie to jest obustronne, znaczy to, że punkt dostępu zostaje uwierzytelniony u klienta, a klient tak samo w punkcie dostępu. Stanowi to dobre

zabezpieczenie przed atakiem MITM, tzw. „człowiek pośrodku" (*ang. Man in the Middle*). Atak ten polega na zainstalowaniu przez intruza fałszywego punktu dostępu, który udaje prawdziwy punkt dostępu, gdy klient połączy się z nim, intruz może uzyskać dostęp do informacji w sieci Wi-Fi. Technologia WPA pozwala także na sprawdzenie, czy pakiety nie zostały zmienione w drodze do routera. Mechanizm WPA nie pozostaje jednak wolny od wad, którą jest np.: wyłączenie punktu dostępu na czas 1 minuty, gdy otrzyma uszkodzone pakiety, mogące sugerować atak hackera, jednak mogące zostać łatwo przygotowane za pomocą ataku odmowy usługi, czyli DoS (*ang. Denial of Service*), w celu zakłócania pracy punktu dostępowego.

Mechanizm WPA zostaje zaprojektowany, aby sprawdzał się zarówno w dużych sieciach firmowych, tzw. trybie Enterprise (ang. Przedsiębiorstwo), jaki i małych sieciach domowych, tzw. trybie Personal (ang. Osobisty). W większych sieciach, które są centralnie zarządzane mechanizm WPA wymienia klucze i uwierzytelnia użytkowników korzystając z serwera RADIUS (*ang. Remote Authentication Dial In User Service*). Serwer ten centralnie zarządza uwierzytelnieniem w sieci i przydziela klucze szyfrujące. Gdy punkt dostępu pragnie podłączyć klienta do sieci, w pierwszej kolejności pyta o pozwolenie serwer RADIUS, jest to mechanizm uwierzytelnienia. Trochę inaczej sprawa wygląda w mniejszych sieciach, np. domowych, nieposiadających serwera RADIUS. W takim wypadku punkt dostępu przejmuje rolę uwierzytelnienia użytkowników. Klucze muszą zostać ręcznie przydzielone punktowi dostępu oraz kartom sieciowym, aby każde z urządzeń w sieci Wi-Fi zapisały w swej pamięci klucz, przed włączeniem mechanizmu WPA. Taki klucz nazywa się kluczem wstępnie przydzielonym, czyli PSK (*ang. Pre Shared Key*). Procedura przydzielania klucza jest taka sama jak w mechanizmie WEP, czyli trzeba podejść po kolei do wszystkich urządzeń i wpisać klucz. Jeśli dojdzie do uwierzytelnienia klienta, dochodzi do wymiany kluczy. Jest to proces wzajemnego uzgadniania, dzielący się na cztery etapy, przebiega on w trybie zaszyfrowanym. Proces kończy się przez ustanowienie kluczy służących do późniejszego szyfrowania. Po zakończeniu tych operacji następuje połączenia klienta z siecią, zaś transmisja między punktem dostępu a klientem staje się szyfrowana. W odróżnieniu od mechanizmu WEP, w którym klucz szyfrujący nie ulega zmianie przez długi okres czasu, co umożliwia zebranie wystarczającej liczby pakietów do odtworzenia tego klucza, technologia WPA wprowadza protokół TKIP (ang. *Temporal Key Integrity Protocol*). Klucz zmieniany jest automatycznie, co pewien okres czasu, który ustala właściciel sieci. Kiedy czas zmiany klucza ustawiony jest na przesłanie przez sieć określonej liczby pakietów, atakujący nie może skompletować wystarczającej liczby pakietów by złamać klucz. Czas zmiany klucza ustawiany jest w punkcie dostępu, zazwyczaj domyślna wartość wnosi 1 godzinę, warto jednak skrócić też czas, np. do 15 minut, wtedy jeśli sieć działa z maksymalną przepustowością, włamywacz nie ma szans zebrać potrzebnych

pakietów, w celu złamania szyfru wykorzystującego algorytm RC4. Z algorytmu tego korzysta nadal mechanizm WPA, ponieważ jest szybki, łatwy do wdrożenia, oraz w małym stopniu obciąża procesor znajdujący się w punkcie dostępu i karcie sieciowej. Oprócz algorytmu RC4 w mechanizmie WPA, teoretycznie dostępny jest także algorytm AES (*ang. Advanced Encryption Standard*). Ta technika jest silniejszym zabezpieczeniem niż algorytm RC4, wymaga on jednak znacznie większej ilości pamięci oraz mocy obliczeniowej od procesora, która może nie być wystarczająca, dla urządzeń w tamtym czasie[16]. Uzupełnieniem mechanizmu WPA w 2004 roku zostaje standard WPA2, znany też jako 802.11i. Wprowadza on dodatkowo nowy protokół CCMP (*ang. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*). Wykonuje on takie same funkcje jak protokół TKIP, z tym, że rozwiązuje on problemy dręczące algorytm WEP. W protokole CCMP zawarty jest algorytm AES, oparty o 128 bitowy, 192 bitowy lub 256 bitowy klucz szyfrujący. Poziom bezpieczeństwa w tej metodzie jest znacznie wyższy niż w metodzie TKIP. Metoda CCMP stosowana jest w nowszych urządzeniach, ponieważ jest wymagana w celu uzyskania prędkości transmisji w sieci, większych, niż 54Mb/s. Obecnie najmocniejszym typem szyfrowania dla sieci Wi-Fi jest metoda WPA2-PSK z algorytmem AES 256 bit. Prace nad kolejnym algorytmem szyfrowania WPA3 wciąż trwają. Wraz z rozwojem technologii moc obliczeniowa komputerów wzrasta, więc kwestią czasu jest aby szyfr został złamany. Potrzeba więc opracowywania nowych technologii i bardziej skomplikowanych form zabezpieczeń, by uchronić się przed hackerami.

PODSUMOWANIE

Wraz z upływem czasu technologia idzie naprzód, wprowadzane są coraz bardziej zaawansowane rozwiązania. Nie inaczej jest w sferze technologii internetowych, które ciągle ewoluują. Sieci bezprzewodowe Wi-Fi stanowią dziś nieodzowną część technologii dostępu do ogólnoświatowej sieci Internet. Za ich pośrednictwem w prosty sposób możemy wysyłać i odbierać informacje w różnej postaci. Postęp technologiczny w sferze sieci bezprzewodowych umożliwia coraz szybszą i prostszą wymianę informacji. Obecnie sieci Wi-Fi znajdują się w większości domostw mających dostęp do Internetu, w instytucjach publicznych, centrach handlowych, itp. Żyć w przekonaniu, że cyberprzestępcy nie będą pozyskiwać informacji prywatnych, ponieważ nie są wystarczająco ważne i nie będą celem ich ataków, a duże korporacje, firmy posiadają bezcenne dla przestępców informacje. Wychodząc z takiego założenia może okazać się że padniemy ofiarą hakerów. Ich powszechność przyczynić się

[16] J. Duntemann, *Przewodnik po sieciach Wi-Fi*. Nakom 2006. S.301-321.

może do zwiększonej aktywności osób chcących wykraść ważne dla nas informacje przesyłane za pośrednictwem tychże sieci. Największym, choć nie jedynym zagrożeniem dla sieci bezprzewodowych standardu Wi-Fi jest podsłuch. Dzięki analizie zebranych pakietów można odszyfrować hasło do sieci i uzyskać do niej nieautoryzowany dostęp. Zabezpieczeniem przed tym są coraz bardziej zaawansowane techniki szyfrujące i metody uwierzytelnia użytkownika. Zagadnienie tyczące rozwoju i bezpieczeństwa sieci bezprzewodowych Wi-Fi jest szczególnie istotnym w dzisiejszych czasach, bowiem duża ilość informacji przekazywana jest drogą elektroniczną przez sieci bezprzewodowe. W wyniku wprowadzenia komputerów w życiu społeczeństwa informacyjnego oraz dynamicznego rozwoju konwergencji technologicznej pojawiła się potrzeba stworzenia narzędzi służących do ochrony przechowywanych, przesyłanych i przetwarzanych danych w systemach lub sieciach teleinformatycznych przed nieuprawnionym dostępem, zniszczeniem lub ujawnieniem. Rodzaj podjętych przedsięwzięć oraz zakres stosowanych środków ochrony jest bardzo szeroki i zależy między innymi od rodzaju i stopnia tajności informacji przetwarzanych w tych systemach lub sieciach. Dla obecnej rewolucji informacyjnej i jej konsekwencji gospodarczych ogromne znaczenie jest powiązanie dwóch odrębnych początkowo technologii - technologii komunikacji związanych z transmisją danych z technologiami komputerowymi mającymi wpływ na przetwarzanie tych danych[17], jednakże przy wyborze mechanizmów ochrony informacji w systemie lub sieci teleinformatycznej należy przyjąć następujące zasady. Przede wszystkim informacja powinna być chroniona od momentu jej powstania do momentu celowego zniszczenia po jej wykorzystaniu. Po drugie każda informacja opracowana, przechowywana oraz przesyłana w systemie teleinformatycznym powinna być zabezpieczona przed dekonspiracją i modyfikacją, ponieważ w wyniku świadomego lub nieświadomego „ataku" ze strony użytkowników lub celowej ingerencji przez intruza może wystąpić zmiana stanu systemów lub sposobu działania18. Dlatego też szczególnie powinno zwracać się w elemencie bezpieczeństwa łączności na następujące komponenty: zabezpieczenia kryptograficzne oraz bezpieczeństwo transmisji.

[17] J. Grubicka. Un(safety)-globalization and technological convergence as the element of building information socjety, ISSN 2345-0282 (online) http://jssidoi.org/jesi/aims-and-scope-of-research, Litwa 2015.

[18] http://www.kaspersky.pl/about.html?s=newsspecial&newsid=2001 [dostęp 23.05.2015]

BIBLIOGRAFIA

[1] Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Wydawnictwa Naukowo-Techniczne, Warszawa, 2006.

[2] Białobłocki T., Moroz J.*, Nowoczesne techniki informacji i komunikacji – ich rozwój i zastosowanie*, [w:] *Społeczeństwo informacyjne. Istota, rozwój, wyzwania*, Warszawa 2006.

[3] Chustecki C.,Janoś T.Routery i przełączniki - konwergencja i gigabity, NetWorld Listopad 2006.

[4] Dąbrowska A., Janoś– Kresło M.. Wódkowski A, E-usługi a społeczeństwo informacyjne, Difin, Warszawa, 2009.

[5] Duntemann J.*Przewodnik po sieciach Wi-Fi*. Nakom 2006.

[6] E-Terroryzm.pl_Wydanie-specjalne-nr-II.pdf. 2013.

[7] Grubicka J. *Konwergencja w obszarze e-usług a bezpieczeństwo*, Acta Pomerania Chojnice, 2014.

[8] Grubicka J., Matuska E. *Bezpieczeństwo konsumenta jako uczestnika e-rynku*, w: Lisiaka H., Stach W., (red) *Bezpieczeństwo współczesnego świata. Historia i bezpieczeństwo publiczne*, Instytut Naukowo Wydawniczy Maiuscula, Poznań 2012.

[9] Grubicka J*. Un(safety)-globalization and technological convergence as the element of building information socjety*, ISSN 2345-0282 (online) http://jssidoi.org/jesi/aims-and-scope-of-research, Litwa 2015.

[10] Pierścionek Z. *Nowe kierunki rozwoju przedsiębiorstw, [w:] Strategie rozwoju współczesnych przedsiębiorstw*, red. nauk. Pierścionek Z., Poznańska K., SGH, Warszawa, 2000,s.13.

[11] Urbanek A. *Czas konwergencji (I) , Networld* Wrzesień 1999.

[12] http://www.kaspersky.pl/about.html?s=newsspecial&newsid=2001

[13] http://websecurity.pl/wp-content/uploads/2013/01/klp_wifi_czestochowa1.jpg

[14] http://www.tvn24.pl/wiadomosci-ze-swiata,2/sony-przeprasza-i-wzmacnia-bezpieczenstwo,169620.html

[15] http://www.tvn24.pl/kultura-styl,8/ukradli-pliki-jacksona-za-250-mln-dol,202665.html

TECHNOLOGICAL CONVERGENCE AND INFORMATION SECURITY SYSTEM

ABSTRACT

These days changes brought about by service convergence as well as access to the latest digital information are the key to use modern technologies. It also influences the functioning of market economy. Information sources of IT continuously report attacks directed at companies, spying and an increasing number of laptop thefts, lost memory cards and smart phones. In such circumstances security of confidential data is becoming a priority for both small as well as big companies. The article presents exemplary incidents and shows possible to use solutions of security information in WiFi networks.

Katarzyna KOCUR-BERA, Małgorzata DUDZIŃSKA
Uniwersytet Warmińsko-Mazurski,
Wydział Geodezji, Inżynierii Przestrzennej i Budownictwa, Katedra Analiz Geoinformacyjnych i Katastru

ZARZĄDZANIE GEOINFORMACJĄ NA POTRZEBY ZWIĄZANE Z BEZPIECZEŃSTWEM PRZESTRZENI

STRESZCZENIE

Głównym celem badań jest analiza źródeł informacji o przestrzeni, które mogą być wykorzystane do celów zarządzania bezpieczeństwem przestrzeni. Pozwalają one na budowanie - kreowanie map zagrożeń, map ryzyka i innych dokumentów kartograficznych, które mogą być wykorzystane w konkretnych sytuacjach kryzysowych. Coraz nowocześniejsze urządzania, które dostarczają szereg sygnałów, po przekodowaniu i przekształceniu mogą stanowić doskonałą informację będącą podstawą podejmowania decyzji zarządczych. Dotyczy to w szczególności zobrazowań satelitarnych, które obrazują różne momenty czasowe. Mogą one stanowić podstawę podejmowania decyzji zarządczych na różnych etapach zarządzania kryzysowego, a także bezpośrednio po wystąpieniu kryzysu. Dane te obecnie dostępne dla podmiotów cywilnych, w latach dziewięćdziesiątych były dostępne wyłącznie dla celów militarnych.

Słowa kluczowe:
geoinformacja, kształtowanie przestrzeni bezpiecznej, źródła informacji, dual-use

WSTĘP

Geoinformacja jest najważniejszym elementem zbiorów danych przestrzennych infrastruktury danego kraju. Istnieje wiele definicji geoinformacji. Wszystkie odnoszą się do zbioru informacji, które mają odnośnik lokalizacyjny, dzięki czemu można je wizualizować w konkretnym miejscu w przestrzeni. Podejmowanie decyzji związanych z przestrzenią można oprzeć o zestaw informacji uzyskanych z połączenia geoinformacji z różnych źródeł danych. Prze-

strzeń jest specyficznym zbiorem pewnej liczby faktów o charakterystycznych zależnościach. W zależności od tego, jakie elementy ją tworzą oraz jakie zachodzą w niej relacje wyróżnia się różne rodzaje przestrzeni (geodezyjna, geograficzna, przyrodnicza, ekonomiczna, społeczna, kulturowa, i inne) [2]. Sens przestrzeni nadaje człowiek przez swoją obserwację, dzięki swojemu doświadczeniu i skłonności do klasyfikowania oraz przez swoją działalność wynikającą z chęci korzystania z własności przestrzeni zgodnego ze swoimi aktualnymi potrzebami [1]. Kształtując przestrzeń bezpieczną należy zapewnić warunki do reagowania na różne zagrożenia, takie jak zagrożenia zdrowia i życia ludności, katastrofy i klęski żywiołowe, zagrożenia gospodarcze i ekonomiczne państwa, przestępczość i akty terroryzmu. Wynika z tego, iż w przestrzeni bezpiecznej nie unikniemy zagrożeń, ale możemy tak ją ukształtować, aby zminimalizować ich wystąpienie i skutki. Analizując związki pomiędzy formą zabudowy a poziomem poczucia bezpieczeństwa można wyróżnić kilka cech przestrzeni bezpiecznej. Według Newmana [9] przestrzeń bezpieczna powinna charakteryzować się terytorialnością (poprzez wprowadzenie symbolicznych barier), nadzorem (możliwość wykonywania wizualnego nadzoru), zadbaniem (właściwe utrzymanie mienia), użytkowaniem oraz szeroko podjętym działaniom w celu eliminacji różnym zagrożeniom (działania społeczne).

W procesie zarządzania przestrzenią można wyróżnić wiele grup informacji o świecie rzeczywistym, niezbędnych do podejmowania działań zmierzających do kreowania przestrzeni bezpiecznej. W zasadzie każda informacja o przestrzeni jest istotna, chociaż nie zawsze od razu jesteśmy w stanie ją wykorzystać. Pozyskiwane dane mają najczęściej różnorodny charakter, w zależności od źródła, z których się je pozyskuje. Nowoczesne technologie pozwalają pozyskać dane w sposób bezpośredni, jako tzw. dane pierwotne lub pośredni (dane wtórne). Są one gromadzone w postaci cyfrowej np. dane pozyskane wprost z przestrzeni kosmicznej za pośrednictwem satelitów, systemów nawigacji satelitarnej, zdjęć lotniczych, systemów monitoringu, czy wyniki pomiarów geodezyjnych w postaci wektorowej. Dane wtórne występują w postaci cyfrowej lub analogowej i pierwotnie uzyskano je do innych celów (np. fiskalnych) w związku z czym muszą być przeniesione do formatu cyfrowego. Zaliczyć można tutaj dane o użytkowaniu gruntów wraz z informacją dotyczącą praw do nieruchomości, dane fizyczne, jak topografia terenu, pokrycie terenu, sytuacja geologiczna, jakość gleb, czy grupa danych związanych z wartością, a także informacje pochodzące ze środowiska społecznego, kulturowego, politycznego, gospodarczego kraju lub regionu. Bardzo często granice pomiędzy danymi pierwotnymi i wtórnymi się zacierają [7]. Pozyskiwanie danych pierwotnych obejmuje bezpośrednie pomiary obiektów, do których zaliczamy także obserwacje satelitarne. Można stwierdzić, iż zrewolucjonizowały one sposób myślenia o problemach współczesnego świata, zmieniły perspektywę z jakiej analizowano przyczyny oraz skutki procesów i zjawisk naturalnych i antropo-

genicznych. Dane teledetekcyjne wraz z danymi naziemnymi (in-situ), dają pełny obraz kondycji Ziemi oraz zjawisk na niej zachodzących. Z analizy danych wydobywa się ogrom informacji, od oceny suszy w skali kraju i prognozy wzrostu roślin po wielkość osiadania gruntu liczoną w milimetrach. Satelitarne obserwacje Ziemi są jednym z najlepszych źródeł pozyskiwania dużej ilości danych w krótkim czasie. Przyjmując najprostsze kryterium przeznaczenia, satelity obserwacyjne dzieli się na (1) wojskowe – dostarczające informacje na potrzeby obronności i szeroko pojmowanego bezpieczeństwa; (2) badawcze – stosowane dla celów meteorologicznych, naukowych, testowych i edukacyjnych oraz (3) komercyjne – stosowane do generowania produktów i usług przeznaczonych na rynek użytkowników publicznych i niepublicznych.

Satelitarna obserwacja Ziemi znalazła zastosowanie w następujących dziedzinach: (1) geodezja i gospodarka przestrzenna (wykonywanie i aktualizacja map, w tym map cyfrowych, wykonywanie cyfrowych modeli terenów, monitoring aktualnego stanu zagospodarowania terenu, planowanie przestrzenne aglomeracji miejskich, inwentaryzacja majątku samorządów, kataster nieruchomości); (2) badania i ochrona środowiska (obserwacje meteorologiczne i prognozowanie pogody, śledzenie zmian zachodzących w środowisku naturalnym, ocena zmian procesów klimatycznych, globalnego ocieplenia i wpływu działalności człowieka, ocena produkcji pierwotnej na obszarach lądowych i w akwenach, ocena stanu zagrożeń i zanieczyszczeń środowiska, szacowanie stanu zdrowotności roślinności, detekcja obszarów zagrożonych i zdegradowanych, monitorowanie zanieczyszczeń na powierzchni morza, przewidywanie i ocena zniszczeń dokonanych przez kataklizmy przyrodnicze, badania geologiczne, w tym poszukiwanie surowców naturalnych powierzchniowych i podpowierzchniowych; (3) rolnictwo (monitorowanie struktury działek rolnych, system kontroli upraw, szacowanie plonów, szacowanie strat w zbiorach na skutek susz, powodzi, szkodników biologicznych, szacowanie infrastruktury wiejskiej); (4) leśnictwo (wielkoobszarowa inwentaryzacja stanów lasów, tworzenie leśnych baz numerycznych, ocena kondycji lasów, np. stopień zaatakowania przez szkodniki, szacowanie stopnia wysuszenia lasów, wykrywanie nielegalnej wycinki lasów, wyznaczanie granicy rolno-leśnej; (5) sektor bezpieczeństwa (monitorowanie przestrzegania traktatów międzynarodowych, pozyskiwanie informacji strategicznych, rozpoznanie pola walki, ocena działań i inne, ocena zagrożeń (mapy ryzyka) i ostrzeganie przed klęskami żywiołowymi i awariami przemysłowymi, ocena skutków klęsk żywiołowych, aktualizacja map i monitoring określonych obszarów dla potrzeb służb ratowniczych, policji, straży granicznej i innych, (6) hydrologia (informacje dla katastru wodnego, charakterystyka zanieczyszczeń obszarowych, określenie stanu biologicznego środowiska wodnego, wyznaczanie obszarów narażonych na niebezpieczeństwo powodzi, wyznaczanie stref i obszarów ochronnych [8].

Wykorzystanie danych satelitarnych z roku na rok wzrasta. Ocenia się, że nawet 80% decyzji w sektorze publicznym podejmowanych jest w oparciu o dane geoprzestrzenne pozyskiwane w ten sposób. Głównymi użytkownikami danych są: administracja centralna i samorządowa, wojsko i sektor bezpieczeństwa, służby państwowe w zakresie zarządzania kryzysowego, pozarządowe organizacje niosące pomoc, przedsiębiorstwa komercyjne rozwijające niestandardowe aplikacje przy wsparciu produktów obserwacji satelitarnej Ziemi, instytucje naukowo-badawcze oraz przeciętny obywatel posiadacz przenośnego terminala wielofunkcyjnego.

Na początku lat dziewięćdziesiątych XX wieku rząd USA zdecydował o udostępnieniu szeregu technologii kosmicznych sektorowi komercyjnemu, co pozwoliło na szybszy rozwój systemów komercyjnych oferujących obrazy o bardzo wysokiej rozdzielczości. W ostatnich latach można zaobserwować, zwłaszcza w Europie, rozwój systemów podwójnego zastosowania (tzw. dual-use) – te same satelity mogą wykonywać misje dla potrzeb sektora bezpieczeństwa i dla celów cywilnych [6].

CEL I METODA BADAŃ

Celem głównym badań jest omówienie zagadnienia zarządzania geoinformacją, na potrzeby związane z bezpieczeństwem przestrzeni. Skupiono się głównie na: omówieniu faz zarządzania przestrzenią w sytuacjach kryzysowych, identyfikacji źródeł danych geinformacyjnych, wskazaniu lokalizacji internetowych, gdzie dane geoinformacyjne można pozyskać, omówieniu zakresu informacyjnego inicjatywy Copernicus powołanej, do celów sprawniejszego zarządzania przestrzenią oraz na podstawie studium przypadków wskazano możliwości wykorzystania danych satelitarnych w różnych sytuacjach kryzysowych. Na wszystkich etapach badań zwrócono uwagę na zagadnienie dual-use, które zakłada wykorzystanie danych wojskowych, do realizacji celów cywilnych (takie znaczenie tego zagadnienia przyjęto w artykule). W badaniach wykorzystano analizę literatury oraz materiałów źródłowych oraz stron internetowych.

Zarządzanie w sytuacjach kryzysowych rozpatrywane jest w aspekcie czterech faz obejmujących różne rodzaje podejmowanych działań:

1. **zapobieganie**, rozumiane jako działania, które eliminują lub redukują prawdopodobieństwo wystąpienia sytuacji kryzysowych albo ograniczają ich potencjalne skutki poprzez: (a) analizę (kategoryzację) zagrożeń, (b) ocenę wrażliwości społeczeństwa na zagrożenia, (c) regulacje prawne, (d) racjonalne planowanie zagospodarowania przestrzennego, (e) odpowiednie gospodarowanie budżetem, (f) ocenę potencjalnych

strat ludzkich, mienia i infrastruktury spowodowanych przez katastrofę, (g) określenie planu działań zapobiegawczych, (h) określenie zasad i sposobów kontroli i nadzoru;

2. **przygotowanie**, rozumiane jako opracowanie planu działań, które należy podjąć w sytuacjach kryzysowych, a także działania mające na celu powiększenie zasobów sił i środków niezbędnych do efektywnego reagowania, poprzez: (a) budowę centrum reagowania kryzysowego, (b) określenie zasad komunikacji, (c) określenie systemów monitorowania, (d) organizację systemów ostrzegania i alarmowania, (e) określenie procedur zwracania się o pomoc i jej udzielania, (f) określenie zasad stosowania przymusu prawnego w stosunku do ludności, organizacji pozarządowych i sektora prywatnego, (g) tworzenie baz magazynowych oraz gromadzenie informacji o możliwościach pozyskiwania środków i materiałów, (h) opracowanie baz danych, (i) edukację społeczeństwa, (j) doskonalenie służb ratowniczych, (k) uzyskanie akceptacji społecznej poniesionych kosztów, (l) uaktualnianie elementów przygotowania;
3. **reagowanie**, rozumiane jako zespół przedsięwzięć następujących po wystąpieniu sytuacji kryzysowej, których celem jest zahamowanie jej rozwoju, dostarczenie pomocy poszkodowanym i ograniczenie wtórnych zniszczeń i strat, poprzez: (a) zarządzanie informacją, (b) informowanie ludności, (c) uruchomienie systemów ostrzegania i alarmowania, (d) natychmiastową reakcję ludności lokalnej, (e) uruchomienie procedur, (f) uruchomienie struktur ratowniczych, (g) uruchomienie procesu ewakuacji, (h) neutralizowanie ognisk zagrożeń, (i) organizowanie samopomocy społecznej, (j) wsparcie operacji przez siły zbrojne, (k) udział organizacji społecznych i humanitarnych, (l) uruchomienie ochrony psychologicznej ofiar;
4. **odbudowa**, rozumiana jako działania mające na celu przywrócenie stanu sprzed sytuacji kryzysowej, a ponadto takie odtworzenie infrastruktury, która będzie mniej wrażliwa na katastrofę, poprzez: (a) szacowanie szkód, (b) zapewnianie pomocy ludności, (c) leczenie i rehabilitację poszkodowanych, (d) wypłacanie odszkodowań, (e) informowanie ludności o prawach i obowiązkach, (f) odtwarzanie i uzupełnianie zapasów, przywracanie stanu gotowości służb ratowniczych, (g) przywracanie równowagi i bezpieczeństwa ekologicznego, (h) odbudowę i przywracanie sprawności infrastruktury, (i) odtwarzanie baz materiałowych, (j) inicjatywy legislacyjne, (k) sprawne administrowanie, (l) realizację zobowiązań – rozliczenie kosztów reagowania, (ł) podsumowanie i wyciągnięcie wniosków, (m) modyfikację i aktualizację planów reagowania, (n) opracowanie sprawozdań, raportów, itp. [3, 12].

Wszystkie fazy zarządzania kryzysowego wymagają szerokiej gamy informacji. W tabeli nr 1 zestawiono przedmiot, typ i źródła danych pozyskiwane przez jednostki cywilne, rządowe i wojskowe, które mogą być wykorzystane na każdym z etapów zarządzania kryzysowego.

Tabela nr 1. Zestawienie danych dotyczących źródeł danych, przedmiotu danych oraz ich typu

Przedmiot danych	Źródło danych	Typ danych
Mapy podstawowe		
Osnowa geodezyjna	Narodowe Służby Geodezyjno-Kartograficzne, np. United States Geological Survey	Definicje układów współrzędnych i odwzorowań
Ogólne mapy topograficzne	Narodowe Służby Geodezyjno-Kartograficzne oraz agencje wojskowe, np. US National Geospatial - Inelligence Agency	Wiele typów danych od szczegółowych do średnioskalowych
Wysokość terenu	Narodowe Służby Geodezyjno-Kartograficzne, agencje wojskowe, kilku dostawców komercyjnych, np. Narodowe Służby Geodezyjno-Kartograficzne, SPOT Image, NASA	Cyfrowy model terenu oraz mapy poziomicowe na lokalnym, regionalnym i globalnym poziomie szczegółowości
transport	Rządy i kilku dostawców komercyjnych, np. Tele Atlas, NAVTEQ	Bazy danych sieci ulic i dróg na poziomie krajowym
hydrologia	Narodowe Służby Geodezyjno-Kartograficzne i agencje rządowe	Narodowe bazy danych hydrologicznych
Nazwy geograficzne	Narodowe Służby Geodezyjno-Kartograficzne, inne agencje rządowe i dostawcy komercyjni	Skorowidze nazw i współrzędnych obiektów geograficznych na poziomach globalnym i krajowym
Obrazy satelitarne	Dostawcy komercyjni i wojskowi np. LANDSAT, SPOT, IRS, IKNOS, QUICKBIRD	Dane o nominalnej rozdzielczości przestrzennej od 0,3 do 100 m
Zdjęcia lotnicze	Wiele prywatnych i publicznych agencji	Szeroki zakres skal od 1:500 do 1:20 000
Ochrona środowiska		
Mokradła	Narodowe agencje, np. US National Wetlands Inventory	Rządowe spisy mokradeł
Źródła zanieczyszczeń	Narodowe Agencje Ochrony Środowiska, np. US Enviornmental Protection Agency	Szczegółowe dane dotyczące źródeł zanieczyszczeń
Ekoregiony świata	WWF (World Wildlife Fund for Nature)	Typy środowiska, obszary i gatunki zagrożone

Zagrożenie powodziowe	Wiele narodowych i regionalnych agencji rządowych, np. Federal Emergency Management Agency	Obszary zagrożone powodzią w poszczególnych krajach
Zagadnienia społeczno-ekonomiczne		
Liczba ludności	Rządy i dostawcy komercyjni (dane przetworzone)	Dane spisowe zazwyczaj co 10 lat, w pozostałych latach dane szacunkowe
Społeczeństwo	Prywatne agencje, np. CACI, EXPERIAN	Na podstawie spisów ludności i innych danych społeczno-ekonomicznych
Geodemografia	Prywatne Agencje, np. Claritas i EBIS	Wiele typów danych w różnych skalach i cenach
Własność gruntów	Agencje rządowe	Ulice, nieruchomości i dane katastralne
Podział administracyjny	Agencje rządowe	Możliwe do uzyskania mapy w skalach od 1:5000 do 1:750000

Źródło: opracowanie własne na podstawie [7]

Zobrazowania satelitarne coraz powszechniej są stosowane na każdym z etapów zarządzania przestrzenią. Przez lata były dostępne wyłącznie dla wojska i środowisk naukowych, obecnie są osiągalne praktycznie dla każdego, kto posiada komputer lub telefon komórkowy. Liczne serwisy internetowe oferują wysokorozdzielcze dane satelitarne i lotnicze oraz połączone z nimi dwu- i trójwymiarowe mapy sieci komunikacyjnej, ukształtowania terenu, lokalizacji ważnych lub ciekawych miejsc. Posiadają one wiele informacji, pozwalają jednak użytkownikowi jedynie na bierne zapoznawanie się z publikowanymi zasobami. Nie jest możliwe samodzielne pozyskiwanie obrazów, samodzielne ich wizualizowanie w sposób odpowiadający potrzebom użytkownika, czy wreszcie samodzielne przetwarzanie danych do postaci map tematycznych. Konieczne jest sięgnięcie po materiał źródłowy – zobrazowania satelitarne w postaci oryginalnej. W tabeli nr 2 zestawiono portale internetowe, z których można za opłatą lub bez niej pozyskać szereg zobrazowań satelitarnych w zależności od rozdzielczości przestrzennej.

Tabela 2. Zestawienie danych związanych z możliwością pozyskania zdjęć satelitarnych o różnej rozdzielczości

Nazwa satelity/radaru	Adres internetowy
Bardzo wysoka rozdzielczość przestrzenna	
Typowe dane bardzo wysokiej rozdzielczości (VHR) oferują rozdzielczość powyżej 5 metrów, z dostrzegalną współcześnie tendencją schodzenia poniżej jednego metra. Pozyskiwanie danych VHR to domena firm komercyjnych. Oferują klientom zazwyczaj jedynie produkty niskich poziomów, tj. nieinterpretowane do produktów tematycznych.	
Dane optyczne (promieniowanie widzialne i podczerwień)	
Kompsat-2; Formosat-2; SPOT-5	http://www.spotimage.com/; http://www.geosystems.pl
GeoEye-1; Ikonos; OrbView-2	http://www.geoeye.com;
QuickBird	http://www.geoeye.com; http://www.smallgis.pl
WorldView-1, WorldView-2	http://www.digitalglobe.com; http://www.smallgis.pl
RapidEye	http://www.rapideye.de;
Cartosat-2; IRS-P5	http://www.euromap.de; http://www.nrsc.gov.in/
IRS-P6/LISS-4	http://www.euromap.de; http://www.geosystems.pl; http://www.nrsc.gov.in/
IRS-1C/1D PAN	http://www.euromap.de; http://www.nrsc.gov.in
CBRES 2B-HRC	http://www.satimagingcorp.com;
ALOS-PRISM	http://earth.esa.int/dataproducts
Dane radarowe	
TerraSAR-X / TanDEM-X	http://infoterra.de; http://www.geosystems.com.pl
COSMO-SkyMed	http://www.e-geos.it; http://www.cosmo-skymed.it/
RadarSat-2	http://www.radarsat2.info; http://gs.mdacorporation.com; http://www.geosystems.pl
Wysoka rozdzielczość przestrzenna	
Najlepszym przykładem danych wysokiej rozdzielczości (*high resolution*, HR) są zobrazowania sensorów serii satelitów Landsat. Charakteryzuje je rozdzielczość przestrzenna powyżej 30-50 metrów, przy rozdzielczości czasowej kilkunastu dni i kilku kanałach spektralnych, obejmujących promieniowanie widzialne, bliską podczerwień i podczerwień termalną. Satelity dostarczające danych HR to zarówno przedsięwzięcia naukowe oraz rządowe, jak i (szczególnie w ostatnich dekadach) przedsięwzięcia komercyjne. Użytkownikom oferowane są przede wszystkim dane nieinterpretowane, ale także dane tematyczne (mapy pokrycia terenu, mapy temperatury radiacyjnej, mapy deformacji terenu itp.). Optyczne i radarowe zobrazowania HR są najczęściej poszukiwanymi danymi satelitarnymi.	

Dane optyczne (widzialne i podczerwień)	
Landsat MSS/TM/ETM+; EO-1 Hyperion/ALI	http://earthexplorer.usgs.gov
ASTER	https://wist.echo.nasa.gov; http://imsweb.aster.ersdac.or.jp
DMC	http://www.dmcii.com
SPOT 1-5	http://www.spotimage.com
PROBA CHRIS i HRC; ALOS-AVNIR2	http://earth.esa.int/dataproducts
IRS-P6/LISS-3; IRS-P6/AWIFS	http://www.nrsc.gov.in; http://www.euromap.de; http://earth.esa.int/dataproducts
IRS-1C/1D LISS3;	http://www.nrsc.gov.in; http://www.euromap.de
CBRES 1-2/2B; CBERS-2	http://www.satimagingcorp.com
Dane radarowe	
RadarSat-2	http://www.radarsat2.info; http://gs.mdacorporation.com; http://www.geosystems.pl;
ALOS-PALSAR	http://earth.esa.int/dataproducts
TerraSAR-X / TanDEM-X	http://infoterra.de; http://www.geosystems.com.pl
COSMO-SkyMed	http://www.e-geos.it; http://www.cosmo-skymed.it
ENVISAT-ASAR; ERS-SAR	http://earth.esa.int/dataproducts
Średnia i mała rozdzielczość przestrzenna	
Dane o rozdzielczości poniżej 50 metrów są umownie nazywane danymi średniej rozdzielczości (*moderate resolution,* MR), a poniżej kilki kilometrów danymi niskiej rozdzielczości (*low resolution*, LR). Dzięki zmniejszeniu rozdzielczości przestrzennej, obrazy mogą być uzyskiwane dla większego obszaru (duże pole widzenia sensorów), do tego w dużej liczbie kałów spektralnych i z dużą rozdzielczością czasową (kilka-kilkadziesiąt razy dziennie). Dane MR i LR znajdują zastosowanie w monitoringu lądów, atmosfery i oceanów w małej dużej skali. Tego typu aplikacje są już często przedsięwzięciami naukowymi, stąd większość danych MR i LR jest udostępniana przez instytucje naukowe lub agencje kosmiczne, sporadycznie przez firmy komercyjne.	
Dane optyczne (widzialne i podczerwień)	
MODIS-Level 1 i atmosfera	http://ladsweb.nascom.nasa.gov
MODIS-Oceany	http://oceancolor.gsfc.nasa.gov
MODIS-Kriosfera	http://nsidc.org/data/modis/
MODIS-Lądy	http://edcdaac.usgs.gov/dataproducts.asp
MERIS	http://earth.esa.int/dataproducts
AVHRR	http://archive.eumetsat.int; http://www.class.noaa.gov
Meteosat MVIRI i SEVIRI	http://archive.eumetsat.int; http://www.ssec.wisc.edu/datacenter/archive.html

GOES Imager i Sounder	http://www.class.noaa.gov; http://www.ssec.wisc.edu/datacenter/archive.html
IRS-1C/1D WIFS - 180 m	http://www.nrsc.gov.in/; http://www.euromap.de
CBRES 1-2/2B/ WFI; CBRES 1-2/2B / IRMSS	http://www.satimagingcorp.com
Dane radarowe	
ALOS-PALSAR	http://earth.esa.int/dataproducts
COSMO-SkyMed	http://www.e-geos.it; http://www.cosmo-skymed.it
RadarSat-2	http://www.radarsat2.info; http://gs.mdacorporation.com; http://www.geosystems.pl
ENVISAT-ASAR	http://earth.esa.int/dataproducts
Cyfrowe modele terenu	
Uzupełnieniem danych obrazowych są cyfrowe modele terenu (d*igital elevation model*, DEM). Niektóre z wymienionych powyżej satelitów/sensorów pozwalają na tworzenie tego typu danych. DEM jako produkt jest wtedy publikowany/sprzedawany na równi z obrazami satelitarnymi, najczęściej obejmuje też identyczny obszar, jak typowa scena. Istnieją jednak także modele o charakterze globalnym - obejmujące cały świat mozaiki DEM z wielu przelotów danego sensora.	
SRTM (90m)	http://srtm.csi.cgiar.org
ASTER-GDEM (30m)	http://www.gdem.aster.ersdac.or.jp; https://wist.echo.nasa.gov
Katalogi danych - Poszukiwanie i zamawianie danych satelitarnych ułatwiają katalogi danych online. Do najobszerniejszych należą prowadzone przez ESA i NASA	
EOLi (Earth Observation Link)	http://catalogues.eoportal.org/eoli.html
WIST (Warehouse Inventory Search Tool)	https://wist.echo.nasa.gov

Mówiąc o bezpieczeństwie przestrzeni nie można wspomnieć o inicjatywie pod nazwą *Copernicus*. Jest to nowa nazwa Programu Obserwacji Ziemi Komisji Europejskiej, dawniej GMES (Global Monitoring for Environment and Security), oznaczających Globalny Monitoring Środowiska i Bezpieczeństwa. Jest to inicjatywa, podjęta w końcu lat 90. przez Unię Europejską, która zakłada wykorzystywanie danych z wielu typów satelitów, będących pod zarządem różnych organizacji: Komisji Europejskiej (DG Enterprise), Europejskiej Agencji Kosmicznej (ESA), Europejskiej Organizacji Eksploatacji Satelitów Meteorologicznych (EUMETSAT), przedsiębiorstw sektora kosmicznego, organizacji krajowych i konsorcjów międzynarodowych. Inicjatywa ma na celu opracowanie metod monitorowania stanu środowiska z pułapu satelitarnego, lotniczego i naziemnego [5, 8]. Dane gromadzone są za pomocą satelitów oraz pomiarów naziemnych. Ich przetwarzanie pozwolą na świadczenie usług in-

formacyjnych pozwalających na skuteczniejsze zarządzanie środowiskiem oraz poprawę bezpieczeństwa obywateli Unii Europejskiej. Dzięki tej inicjatywie przewiduje się, że możliwe będzie szybsze i sprawniejsze reagowanie w przypadku katastrof naturalnych, efektywniejsze korzystanie z zasobów naturalnych, lepszy monitoring jakości i czystości wód, powietrza itd.

Copernicus został ustanowiony rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 911/20101 [11]. Stanowi on kluczowy element polityki Unii Europejskiej w dziedzinie przestrzeni kosmicznej zgodnie z art. 189 Traktatu o funkcjonowaniu Unii Europejskiej, który pozwala UE na prowadzenie działalności związanej z przestrzenią kosmiczną. *Copernicus* jest także jednym z programów, które mają być zrealizowane w ramach strategii „Europa 2020" na rzecz inteligentnego i trwałego wzrostu gospodarczego.

Główne obszary zastosowania danych satelitarnych to (1) obserwacje lądów (pokrycie terenu i jego zmiany, wilgotność gruntu, stan upraw, wskaźniki roślinności i biomasy, temperatura powierzchni lądu, rozwój zabudowy i infrastruktury transportowej, wykrywanie samowoli budowlanych, rolnictwo precyzyjne, deforestacja i nielegalne karczowanie lasów, deformacje skorupy ziemskiej, osiadanie terenów nad kopalniami, trójwymiarowe modele terenu, zjawisko miejskiej wyspy ciepła; (2) obserwacje oceanów (zasolenie, temperatura wód powierzchniowych, zawartość materii organicznej, zmiany poziomu oceanu, wskazywanie optymalnych obszarów połowów, zasięg i zwartość lodu morskiego; (3) obserwacje atmosfery (monitoring pogody, stężenia gazów śladowych, w tym cieplarnianych, aerozole naturalne i antropogeniczne, monitoring pyłów wulkanicznych, prognozowanie i śledzenie intensywnych burz, pomiary temperatury powietrza i wilgotności); (4) zarządzanie kryzysowe (wsparcie na etapach zapobiegania, przygotowania do, reagowania w trakcie i odbudowy po zdarzeniu kryzysowym - powodzie, pożary, trzęsienia ziemi, epidemie, susze, wybuchy wulkanów, awarie przemysłowe); (4) opracowywanie scenariuszy symulacyjnych, wsparcie pomocy humanitarnej, szacowanie strat i ocena skutków, kartowanie w czasie rzeczywistym; (5) bezpieczeństwo publiczne (zarządzanie flotą morską, szczelność granic państwowych, wykrywanie wycieków ropy i oleju ze statków, monitoring infrastruktury krytycznej, egzekwowanie międzynarodowych porozumień, wsparcie misji pokojowych). W tabeli nr 3 przedstawiono obszar zainteresowania realizowany w inicjatywie *Copernicus*.

Copernicus został ustanowiony rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 911/20101 [11]. Stanowi on kluczowy element polityki Unii Europejskiej w dziedzinie przestrzeni kosmicznej zgodnie z art. 189 Traktatu o funkcjonowaniu Unii Europejskiej, który pozwala UE na prowadzenie działalności związanej z przestrzenią kosmiczną. Copernicus jest także jednym z programów, które mają być zrealizowane w ramach strategii „Europa 2020" na rzecz inteligentnego i trwałego wzrostu gospodarczego.

Główne obszary zastosowania danych satelitarnych to (1) obserwacje lądów (pokrycie terenu i jego zmiany, wilgotność gruntu, stan upraw, wskaźniki roślinności i biomasy, temperatura powierzchni lądu, rozwój zabudowy i infrastruktury transportowej, wykrywanie samowoli budowlanych, rolnictwo precyzyjne, deforestacja i nielegalne karczowanie lasów, deformacje skorupy ziemskiej, osiadanie terenów nad kopalniami, trójwymiarowe modele terenu, zjawisko miejskiej wyspy ciepła; (2) obserwacje oceanów (zasolenie, temperatura wód powierzchniowych, zawartość materii organicznej, zmiany poziomu oceanu, wskazywanie optymalnych obszarów połowów, zasięg i zwartość lodu morskiego; (3) obserwacje atmosfery (monitoring pogody, stężenia gazów śladowych, w tym cieplarnianych, aerozole naturalne i antropogeniczne, monitoring pyłów wulkanicznych, prognozowanie i śledzenie intensywnych burz, pomiary temperatury powietrza i wilgotności); (4) zarządzanie kryzysowe (wsparcie na etapach zapobiegania, przygotowania do, reagowania w trakcie i odbudowy po zdarzeniu kryzysowym - powodzie, pożary, trzęsienia ziemi, epidemie, susze, wybuchy wulkanów, awarie przemysłowe); (4) opracowywanie scenariuszy symulacyjnych, wsparcie pomocy humanitarnej, szacowanie strat i ocena skutków, kartowanie w czasie rzeczywistym; (5) bezpieczeństwo publiczne (zarządzanie flotą morską, szczelność granic państwowych, wykrywanie wycieków ropy i oleju ze statków, monitoring infrastruktury krytycznej, egzekwowanie międzynarodowych porozumień, wsparcie misji pokojowych). W tabeli nr 3 przedstawiono obszar zainteresowania realizowany w inicjatywie *Copernicus*.

Tabela 3. Obszary zainteresowania realizowane w inicjatywie Copernicus

Obszar zainteresowania	Zakres tematyczny	Produkty i usługi
Usługi dla zapewnienia bezpieczeństwa	- nadzór morski: granice morskie, nielegalni imigranci, przemyt i nielegalny handel, - piractwo, wrażliwe ładunki itd., - nadzór nad infrastrukturą: granice lądowe, infrastruktura krytyczna np. rurociągi, - wsparcie dla działań pokojowych: monitoring populacji, zasobów np. wody, - rozeznanie i wczesne ostrzeganie, - wsparcie dla operacji w zarządzaniu kryzysowym.	- serwisy rozpoznania i wczesnego ostrzegania w celu zapobiegania rozprzestrzeniania się kryzysu i przestrzegania traktatów, wyznaczanie wskaźników kryzysu, krytycznych zasobów, identyfikacja nielegalnej działalności, monitoring dróg i granic; - serwisy do zarządzania kryzysowego: przygotowanie na kryzys i jego planowanie, przygotowanie planu awaryjnego, ocena szkód i odbudowy, wsparcie odbudowy po kryzysie, - monitoring dużych obszarów w czasie zbliżonym do rzeczywi-

		stego, nadzór i system alarmowy w „gorących punktach" (hot spots), monitoring szlaków wodnych; - prototyp portalu dla zarządzania i harmonizacji różnych typów serwisów w bezpiecznej sieci usług;
Monitorowanie powierzchni Ziemi	- wykorzystanie terenu i zmian pokrycia terenu, - przepuszczalność gleb, - jakość i dostępność wody - koncentracja na identyfikacji i zarządzaniu składnikami odżywczymi oraz wielkości pestycydów w obiegu wody, - planowanie przestrzenne, - gospodarka leśna, - bilans węgla, - globalne zagrożenia plonów rolnych;	- serwisy dostarczające mapy lądów oferują informacje o pokryciu, użytkowaniu i zmianach pokrycia terenu, jak też biofizyczne parametry jako wkład do bardziej zaawansowanych produktów; - serwisy dostarczające informacje oferują konkretne dane na potrzeby europejskiej polityki dotyczącej ochrony środowiska i międzynarodowych umów dotyczących zmian klimatu, bezpieczeństwa żywnościowego i zrównoważonego rozwoju w Afryce (przepływ rzeki, zużycie wody, ilość wód podziemnych, poziom i właściwości jezior, pokrycie śnieżne, pokrywa śnieżna i ekwiwalent wodny śniegu, objętość oraz zasięg lodowców i czasz lodowcowych, wieczna zmarzlina i grunt okresowo zamarzający, 20 albedo, pokrycie terenu (w tym typ wegetacyjny), Leaf Area Index (LAI), biomasa, zaburzenia pożarowe, wilgotność gleby (powierzchniowo i strefa korzeniowa); - Urban Atlas - zawiera 19 klas tematycznych wraz z minimalną rozdzielczością terenową 0.25 ha dla klas miejskich i 1 ha dla pozostałych; - pokrycie terenu CORINE (Corine Land Cover - CLC) - jedyna zharmonizowana europejska baza danych pokrycia terenu - oferuje 44 klasy tematyczne; przyczynia

		się do powstania i prezentacji 5 wysokorozdzielczych warstw (nieprzepuszczalne obszary, lasy, łąki, małe zbiorniki wodne, tereny podmokłe);
Monitorowanie mórz i oceanów	- bezpieczeństwo morskie, - zanieczyszczenia i jakość wód, - zarządzanie zasobami morskimi, - zmiany klimatu, - prognozy sezonowe, - działalność przybrzeżna, - badanie pokrywy lodowej morza, - monitorowanie/wykrywanie wycieków ropy naftowej;	- Serwis V0 (obecny - pozwala na swobodny dostęp do regionalnego, europejskiego i światowego katalogu produktów, który został stworzony dzięki poprzednim projektom, takim jak MERSEA, MARCOAST, POLARVIEW, ECOOP, GLOBCOLOR); - V1 Service (w pełni zintegrowany system oferuje dostęp do jednej bazy i bezpośredni dostęp do wszystkich produktów; serwis zawiera funkcjonalności dyrektywy INSPIRE: odnajdywanie, wizualizację, ściąganie, inne narzędzia oraz 24/7 sekcję pomocy); - obejmuje 7 obszarów geograficznych: Morze Śródziemne, Morze Czarne, Północno-Zachodni Szelf, obszar IBI-ROOS (the Iberia-Biscay Ireland Regional Maritime Area), Morze Bałtyckie, Morze Arktyczne, Wszechocean (ocean światowy); - podstawowe dane klimatyczne: powierzchniowo: temperatura powierzchni morza, zasolenie powierzchni morza, poziom morza, lód morski, stan morza, kolor morza (IOP + Chl_a), pojemność absorpcyjna morza na dwutlenek węgla; podpowierzchniowo: temperatura, zasolenie, prądy morskie, składniki odżywcze, dwutlenek węgla, pierwiastki śladowe, fitoplankton;
Monitorowanie atmosfery	- zmiany klimatu, - jakość powietrza, - gazy cieplarniane, - gazy aktywne,	- Europejski Serwis Jakości Powietrza, Skład Atmosfery, Serwis UV i Energii Słonecznej, Serwis Klimatyczny;

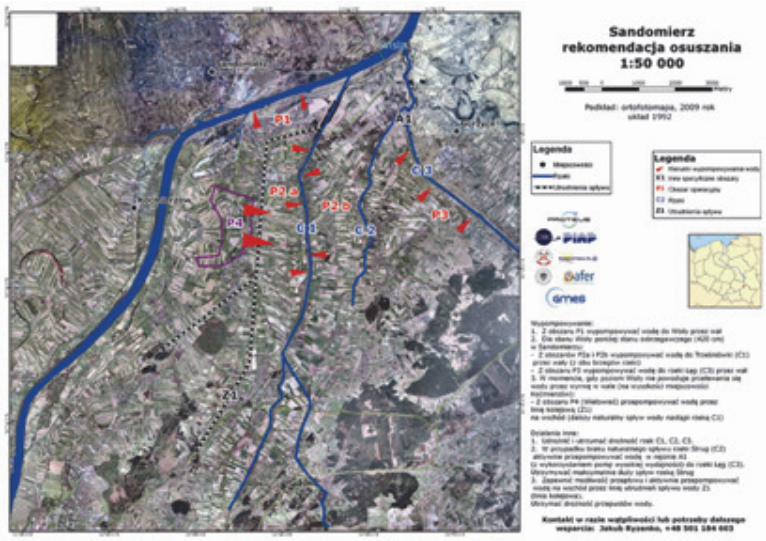
	- warstwa ozonu i promieniowanie UV, - aerozole.	- mapy i dane na potrzeby regionalnej prognozy jakości powietrza, ocena jakości powietrza, identyfikacja źródeł zanieczyszczenia, przygotowanie narzędzi do oceny kontroli pomiaru jakości powietrza, wkład w lokalne prognozy jakości powietrza, jakość powietrza a zdrowie - serwis ostrzegawczy; - wsparcie dla realizowania polityki i pochodnych serwisów;
Wsparcie dla zarządzania kryzysowego	- ochrona obywateli, - pomoc humanitarna, - kryzys bezpieczeństwa, - katastrofy naturalne - powodzie, pożary, osuwiska, huragany, trzęsienia ziemi, wybuchy wulkanów, - kryzysy humanitarne, np. susza, - kryzysy cywilno-militarne.	- przewidywanie: ocena i planowanie strategii interwencji; zapobieganie: wdrażanie środków wykonawczych aby zmniejszyć szkodliwe skutki; aktywna interwencja: poprawa operacji przy ratowaniu; po kryzysie: stwierdzanie strat, pomoc przy usuwaniu skutków, aktualizowanie bazy danych; - serwis reagowania kryzysowego (GMES Emergency Response Service) dostępny 24/7; - sporządzanie map referencyjnych, map oceny ryzyka, dalsze produkty potrzebne w czasie kryzysu, np. modele powodzi i analizy modeli ryzyka powodzi, modele wczesnego ostrzegania, mapy do odbudowy po katastrofie, aktualizacja informacji na tematy "gorące"; - światowa baza geograficzna gotowa przed zdarzeniem (mapy referencyjne sporządzane w ciągu mniej niż 6 godzin).

Jak widać z dotychczas przedstawionych analiz literatury, dane satelitarne oferują szeroki zakres danych, które można wykorzystać w celach zarządzania przestrzenią bezpieczną, a także dla celów bezpieczeństwa przestrzeni.

STUDIUM PRZYPADKU – ZASTOSOWANIE DANYCH SATELITARNYCH W WYBRANYCH SYTUACJACH - TAKŻE KRYZYSOWYCH

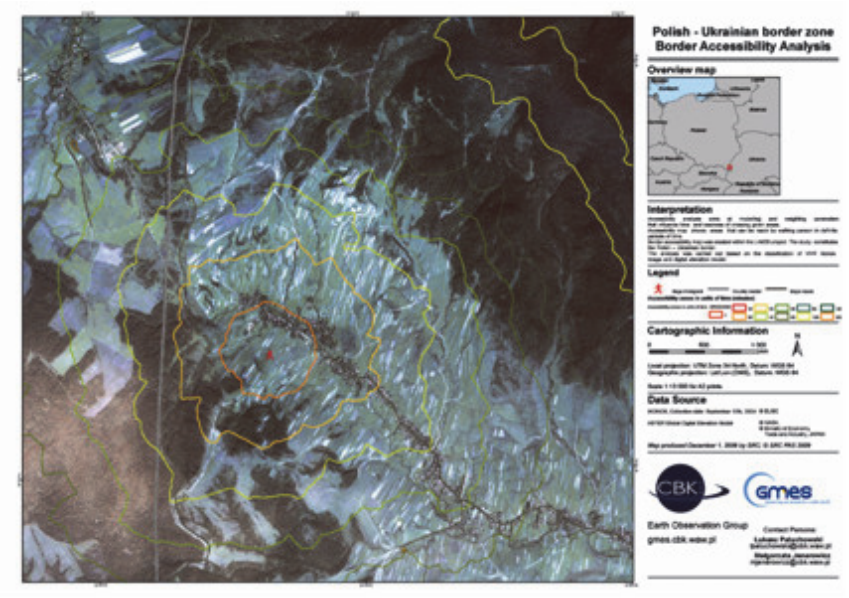
- **Powodzie** - są jedną z najczęstszych klęsk żywiołowych, które zagrażają mieszkańcom Europy Środkowej. Bezpośrednią przyczyną powodzi są intensywne deszcze lub gwałtowne roztopy, jednak na wielkość skutków powodzi, zarówno finansowych, jak i ludzkich, wpływ ma także gospodarka przestrzenna. Techniki teledetekcyjne wspierają walkę z powodzią przed, w trakcie oraz po wystąpieniu żywiołu. Satelity obserwacyjne dostarczają aktualnych zdjęć terenów zagrożonych i już zalanych. Pozwalają z wyprzedzeniem tworzyć scenariusze rozwoju wydarzeń, symulując wszelkie warianty (optymistyczne i pesymistyczne). W pierwszych dwóch fazach zarządzania kryzysowego (zapobieganie i przygotowanie) dane satelitarne pozwalają wyznaczyć w oparciu o cyfrowe modele rzeźby terenu - teoretyczne zasięgi wody powodziowej, zobrazować wały wzdłuż rzeki wraz z informacją o stopniu nasiąknięcia wodą (np. za pomocą informacji przekazywanej radiowo z czujników umieszczonych wewnątrz wałów). Dane takie należałoby na bieżąco analizować oraz wykonywać symulacje dotyczące prawdopodobieństwa przerwania wałów, a także możliwego obszaru zagrożonego zalaniem. W trzeciej fazie zarządzania kryzysowego dzięki zdjęciom satelitarnym możemy otrzymać zobrazowany teren zalany wodą, a połączony z modelem rzeźby terenu pozwala wyznaczyć jej głębokość w różnych częściach zalanego obszaru. Wykorzystując dodatkowe dane o zabudowie i liczbie ludności możemy wyznaczyć liczbę osób zagrożonych oraz najkrótsze drogi do punktów ewakuacyjnych. W ostatniej fazie zarządzania kryzysowego (odbudowa) na podstawie map satelitarnych i danych terenowych szacuje się skalę strat (także na terenach leśnych), wskazuje zasięgi działań rekonstrukcyjnych, a także zbiera dane dla studiów klimatycznych oraz dla gospodarki przestrzennej do celów kontroli kierunków zabudowy. Wielkoobszarowe rozlewiska często wymagają długotrwałej akcji wypompowywania wody i osuszania terenu. Mapy i modele hydrologiczne umożliwiają wskazanie niecek bezodpływowych oraz optymalne lokalizacje pomp wysokiej wydajności.
- **Pożary obszarów leśnych** - to zagrożenie częste i powodujące duże straty społeczne, ekonomiczne i ekologiczne. Modelowanie geoinformatyczne w oparciu o dane satelitarne i dodatkowe dane przestrzenne pozwala na identyfikację i inwentaryzację zagrożeń pożarowych, określenie ich źródeł, analizę ryzyka wystąpienia oraz prognozę skutków pożarów. W wyniku interpretacji zobrazowań teledetekcyjnych powstają i są stale aktualizowane bazy danych potencjalnych źródeł

ognia (np. domostwa, linie kolejowe, strefy biwakowe). Możliwość faktycznego wystąpienia pożaru zależy jednak w dużej mierze od podatności terenu na tego typu żywioł (ryzyka zaistnienia pożaru). Prawdopodobieństwo wystąpienia pożaru w danym regionie można określić przez analizę statystyczną lub strukturalną. Wykorzystane mogą być w tym celu zarówno dane satelitarne (najlepiej informują o rzeczywistym zasięgu pożaru, jednak nie zawsze są w stanie precyzyjnie wskazać czas rozpoczęcia i zakończenia epizodu), jak i terenowe (informację o czasie trwania zjawiska, długości akcji gaśniczej, użytym sprzęcie). Ocena prawdopodobieństwa wystąpienia pożaru poprzez analizę strukturalną skupia się na biofizycznych właściwościach terenu – m.in. typie siedliskowym lasu, ukształtowaniu powierzchni, odległości do infrastruktury drogowej lub kolejowej. Badane są, więc czynniki mające wpływ na powstanie pożaru. Wiele z wymaganych danych o środowisku może zostać zebrane zdalnie – za pomocą sensorów satelitarnych. W przypadku pożarów lasów prowadzi się stałe obserwacje satelitarne stanu roślinności i warunków meteorologicznych w celu określenia stopnia zapalności lasu. W czasie trwania pożaru satelity dostarczają aktualnych danych o aktywnych pożarach i kierunku rozprzestrzeniania się ognia, co pomaga sprawniej koordynować akcję gaśniczą. Po ugaszeniu pożaru satelity ułatwiają ocenę wielkości strat, a w dłuższym horyzoncie czasowym umożliwiają śledzenie procesu odbudowy ekosystemu leśnego.



Rysunek 1. Przykład mapy z rekomendacją osuszania po wystąpieniu powodzi w 2010 roku. Źródło: [13]

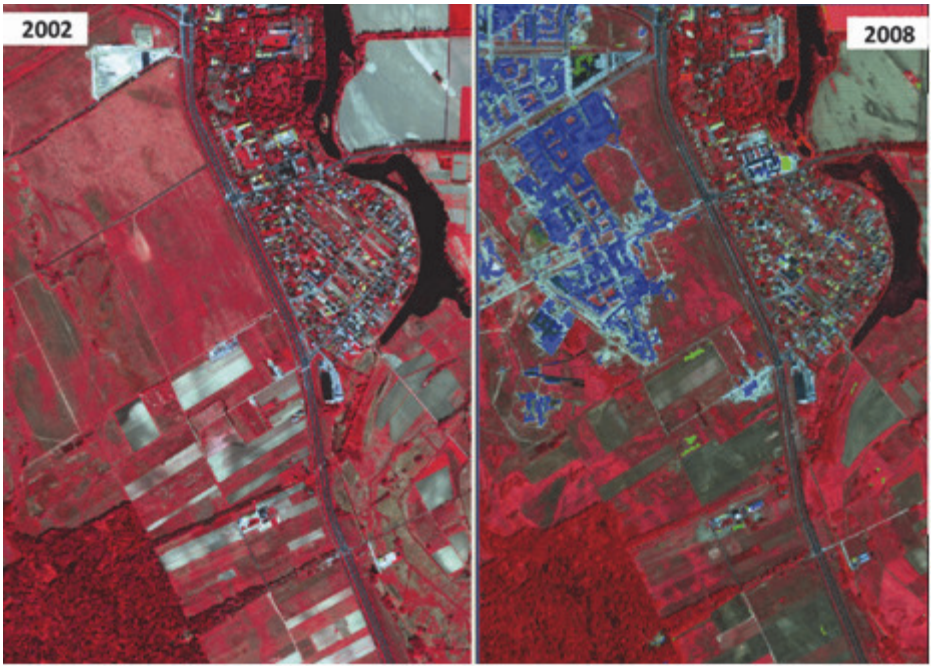
- **Lawiny śnieżne** - są zjawiskiem lokalnym, charakterystycznym dla terenów górskich. Ze względu na bezpieczeństwo i niedostępność obszarów występowania lawin, najtańszymi i najefektywniejszymi metodami kartowania lawinowego są teledetekcja i GIS. Modele zagrożenia lawinowego mają na celu wyznaczenie obszarów schodzenia lawin, określenie maksymalnego zasięgu lawin oraz oszacowanie częstości ich występowania. Mapy zagrożenia lawinowego wykorzystują numeryczne modele terenu, w oparciu o które wyznacza się strefy startu, tranzytu i zatrzymywania się lawin. W dalszej kolejności uwzględniana jest szorstkość powierzchni w obrębie stref startu, determinująca stabilność śniegu. O szorstkości, a więc typie i gęstości roślinności informują mapy pokrycia terenu opracowywane w oparciu o optyczne i radarowe zobrazowania satelitarne. Częstość występowania lawin jest silnie powiązana z warunkami meteorologicznymi – przede wszystkim z występowaniem opadów śniegu oraz warunkami termicznymi w poszczególnych częściach stoku. Ze względu na zbyt małą liczbę stacji meteorologicznych w rejonach górskich, niezbędne informacje uzyskuje się przez analizę danych satelitarnych o dużej rozdzielczości czasowej. Informacja o dobowych zmianach temperatury powierzchni śniegu pozwala wnioskować o stabilności śniegu.
- **Bezpieczeństwo granic** - odgrywa kluczową rolę w rozwoju polityki bezpieczeństwa Unii Europejskiej. W odpowiedzi na obawy organizacji i instytucji państw europejskich związane z nielegalnym transgranicznym ruchem migracyjnym, zaproponowany został system monitorowania terenów przygranicznych. Jego istotną częścią są obserwacje satelitarne i analizy geoinformatyczne. Szczelność granicy utrudnia wszelkie próby nielegalnego jej przekroczenia. By dowiedzieć się czy i na ile granice są szczelne wykonuje się analizy przenikalności granic. Tworzone mapy wskazują łatwość, z jaką nielegalny imigrant może przemieszczać się po obszarze przygranicznym (pod uwagę brana jest łatwość chodzenia w różnych warunkach terenowych i możliwość pozostania niewidocznym dla obserwatora). Na prędkość ruchu pieszego ma wpływ typ terenu (np. las, góry, równiny) oraz sieć dróg. Możliwość ukrycia się imigranta warunkowana jest przez typ obszaru, w jakim się on znajduje, np. teren zamieszkały, łatwo dostępny, lub silnie uczęszczany. Źródłem informacji o topografii są dane satelitarne - cyfrowe modele terenu. W podobny sposób analizować można przejezdność – zdolność ruchu kołowego po określonym terenie przygranicznym.



Rysunek 2. Przykład mapy z analizą przenikalności granic. Źródło: [13]

- **Konflikty, wojny domowe oraz akcje humanitarne**. Struktury mieszkalne obozów przesiedleńców to głównie prowizoryczne szałasy lub namioty. Informacja na temat liczby osób zamieszkujących obóz, będący obszarem cechującym się szybkimi zmianami populacji, ma fundamentalne znaczenie w planowaniu i skutecznym zarządzaniu akcjami humanitarnymi. Często jednak pozyskanie dokładnych i bezpośrednich danych na temat populacji jest niemożliwe ze względu na warunki bezpieczeństwa panujące w obozach. Techniki cyfrowego przetwarzania danych satelitarnych oraz modelowania informacji przestrzennej umożliwiają wykrycie pojedynczych szałasów i namiotów, a następnie oszacowanie gęstości zaludnienia. Wyniki analiz wykorzystywane są przez Organizację Narodów Zjednoczonych w ramach Światowego Programu Żywnościowego – największej organizacji charytatywnej na świecie, zwalczającej głód.
- **Planowanie przestrzenne i urbanizacja** - to jeden z głównych kierunków zmian współczesnego świata, odbicie zachodzących w nim procesów społecznych, ekonomicznych i demograficznych. W tym kontekście poprawna gospodarka przestrzenna staje się podstawą polityki zrównoważonego rozwoju każdego kraju. Gwarancją jakości dokumentów planistycznych jest aktualność zawartych w nich informacji o stanie przestrzeni miejskiej. By zapewnić aktualność danych, konieczny jest monitoring inwestycji budowlanych i infrastrukturalnych, szybkie

i sprawne wykrywanie samowoli budowlanych, waloryzowanie jakości i dostępności przestrzeni publicznej. Brak takiej informacji utrudnia, a często uniemożliwia, tworzenie skutecznych strategii rozwoju miast. Połączenie danych satelitarnych z np. z ewidencją gruntów i budynków, daje ogromny zbiór danych, które odpowiednio wykorzystane, pozwalają wnioskować o dotychczasowym kierunku rozwoju miasta, ułatwiają planowanie polityki urbanistycznej oraz pomagają w jej realizacji.



Rysunek 3. Przykład map zabudowy miasta z dwóch okresów czasowych 2002 i 2008 roku. Źródło: [13]

– **Okrywa śnieżna** - jest jednym z najbardziej charakterystycznych wyznaczników pory zimowej. Jej obecność wpływa na zmianę struktury bilansu energii – śnieg odbija dużo więcej promieniowania niż niepokryta śniegiem roślinność, co powoduje ochładzanie atmosfery. Jednocześnie pokrywa śnieżna jest formą retencji wody, uwalnianej do środowiska z nastaniem wiosny lub nadejściem odwilży. Pojawienie się śniegu wpływa także na nasze codzienne życie utrudniając komunikację, a szybko topniejący śnieg może powodować wzrost poziomu rzeki i wiosenne powodzie. Monitoring występowania i zmian zasięgu pokrywy śnieżnej jest jednym z podstawowych aspektów obserwacji pogody i klimatu. Dane satelitarne pozwalają na uzyskanie pełnego obrazu

sytuacji,
co jest pomocne np. przy prognozowaniu warunków hydrologicznych dla rolnictwa lub szacowaniu wydatków związanych z odśnieżaniem dróg.

- **Azotany** w wodach podziemnych i powierzchniowych - powodują eutrofizację rzek i jezior oraz wykwity toksycznych alg [4]. W celu kontroli dostawy azotanów do środowiska Rada Unii Europejskiej uchwaliła tzw. „dyrektywę azotanową", obligującą państwa Unii do wyznaczenia obszarów szczególnie narażonych na spływ azotanów ze źródeł rolniczych. Nacisk na rolnictwo wynika z ilości azotanów wprowadzanych do obiegu właśnie przez tą gałąź gospodarki. Tradycyjne metody wyznaczania obszarów wrażliwych wykorzystują naziemne sieci pomiarów stężenia azotanów w glebie i w wodzie. Ze względu na duże koszty i małą precyzję terenową tych metod, do analiz włączono również GIS i teledetekcję. Stopień zagrożenia zanieczyszczeniami szacuje się poprzez określenie wrażliwości terenu oraz presji, jaka jest na niego wywierana. Wrażliwość zależy od typu użytkowania terenu, rodzaju gleby i jej zdolności sorpcyjnych, przepuszczalności, ilości opadów. W efekcie dalszych analiz powstają mapy głębokości przemieszczania się wód opadowych, możliwości ich spływu powierzchniowego, jak również określone zostaje prawdopodobieństwo przedostania się zanieczyszczeń do wód. Rolnictwo wywiera presję na teren poprzez nawożenie mineralne nawozami sztucznymi i nawożenie organiczne związane z hodowlą zwierząt. Część danych uzyskuje się z bezpośrednich pomiarów terenowych, ale można je następnie korelować ze wskaźnikami otrzymywanymi ze zdjęć satelitarnych. Dzięki temu możemy kartować zróżnicowanie przestrzenne wysokich i niskich zawartości azotanów w glebie na bardzo dużym obszarze.
- **Klimat** – zobrazowania satelitarne zapewniają ciągłe pokrycie danymi całej planety i jako jedyna technika obserwacyjna oferuje w pełni globalne badania środowiska atmosferycznego. Tradycyjne dane naziemne są uzyskiwane dla niewielkiej liczby lokalizacji, przez co ich rola obecnie redukuje się do funkcji punktu odniesienia dla danych satelitarnych.

WNIOSKI

Zobrazowania satelitarne mogą być wykorzystywane w wielu obszarach naszego życia. Dzięki nowym technologiom są coraz częściej podstawą podejmowanych decyzji związanych z przestrzenią. Techniki przetwarzania oraz możliwości wykorzystania danych satelitarnych bardzo rozwinęły się po

udostępnieniu ich do celów cywilnych. Obecnie pozwalają m.in. na monitorowanie chronionych ekosystemów i terenów o szczególnych wartościach przyrodniczych, są cenne dla planowania przestrzennego, a także pozwalają kształtować i zarządzać przestrzenią w taki sposób, aby przebywanie w niej było bezpieczne dla człowieka. W dobie wielu niepokojów politycznych, zmian klimatu oraz zagrożeń powodowanych przez zdarzenia ekstremalne coraz częściej nękających kulę ziemską, zobrazowania satelitarne są błyskawicznym i bezpiecznym sposobem pozyskiwania geoinformacji o przestrzeni.

BIBLIOGRAFIA

[1] Bajerowski T. *Niepewność w dynamicznych układach przestrzennych.* Wyd. UWM, Olsztyn, 2003.

[2] Cymerman R. *Planowanie i zagospodarowanie przestrzenne w gospodarce nieruchomościami*. Wyd. EDUCATERRA sp z o.o. Olsztyn, 2001.

[3] Kocur-Bera K. *Przestrzenne uwarunkowania zarządzania kryzysowego*. Acta Scientiarum Polonorum, seria: Administratio Locorum 11 (4), 2012, s. 55-64.

[4] Kocur-Bera K., 2012. *Identyfikacja zagrożeń występujących na obszarach wiejskich*. Infrastruktura i Ekologia Terenów Wiejskich – 2/III, PAN Kraków. s. 31-45.

[5] Królikowski K., Trzaskalska-Stroińska O., Skrzyński Z. *Bezpieczeństwo i obrona w europejskiej polityce kosmicznej*. Magazyn FAKTY 6 (72) listopad/grudzień 2014.

[6] Kwietniewski M. *GIS w wodociągach i kanalizacji*. PWN, Warszawa, 2013.

[7] Longley P.A., Goodchild M.F., Maguire D.J., Rhind D.W. GIS teoria i praktyka. PWN, Warszawa, 2006.

[8] Mikołajek-Zielińska B. *Europejski program globalnego monitoringu środowiska i bezpieczeństwa Copernicus*, 2013. https://www.nauka.gov.pl/g2/oryginal/2013_09/ff067cae5d64bea78d1d85cb33cc03a8.pdf

[9] Newman O. *Defensible space. People and design in the violent city*. Architectural Press, London, 1972.

[10] Pałys M., Antosz M., Pałys M., Durlej J., Latos D., Małetka G. *Obciążenia środowiskowe dróg oraz systemy pomiarowe w budownictwie drogowym*. Rozdział w monografii p.t. LIII TECHNICZNE DNI DROGOWE. SBN 978-83-89661-25-x, 2010, GDDKIA oddział w Łodzi.

[11] *Rozporządzenie Parlamentu Europejskiego i Rady* (UE) nr 911/20101.

[12] Sienkiewicz-Małtyjurek K., Krynojewski F. R. *Zarządzanie kryzysowe w administracji publicznej. Zarządzanie bezpieczeństwem*. Wydawnictwo Difin S.A., Warszawa, 2010, str. 220.

[13] http://zoz.cbk.waw.pl/index.php/pl/ dostęp 10.01.2015.

GEOINFORMATION MANAGEMENT FOR SECURITY SPACE

ABSTRACT

The main aim of the research is to analyze the sources of information about space that can be used for security management space. They allow you to create hazard maps, risk maps and other cartographic documents, which can be used in specific crises. More modern satellite equipment that provide a range of signals, when encoded and may be converted into an excellent information underpinning management decision-making. This applies in particular satellite images that illustrate the various points of time. They are the basis for management decision-making at various stages of crisis management, as well as immediately after the onset of the crisis. This data is now available for civilian actors, in the nineties were available only for military purposes.

Ewa KOWALEWSKA – BORYS, Diana DAJNOWICZ
Wydział Prawa Uniwersytetu w Białymstoku

UDOSTĘPNIANIE DANYCH BILLINGOWYCH JAKO OBOWIĄZEK FIRM TELEKOMUNIKACYJNYCH W ZAKRESIE UMOŻLIWIANIA KONTROLI OPERACYJNEJ

STRESZCZENIE

Obserwując codzienne doniesienia medialne dostrzec można, że problematyka legalności i dopuszczalności korzystania przez organy ścigania z danych gromadzonych i przechowywanych przez usługodawców oraz dostawców telekomunikacyjnych wciąż wywołuje niemałe kontrowersje. Należy mieć jednak na uwadze, iż w niektórych przypadkach uzasadnionego podejrzenia popełnienia określonego przestępstwa, skuteczne pozyskanie dowodów gwarantują jedynie instrumenty kontroli operacyjnej, których stosowanie regulują m. in. przepisy ustawy o Policji, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu czy Centralnym Biurze Antykorupcyjnym. Wykorzystywanie środków technicznych umożliwiających w niejawny sposób pozyskiwanie i utrwalanie niezbędnych informacji przekazywanych za pośrednictwem sieci telekomunikacyjnych musi się jednak odbywać z poszanowaniem obowiązującego porządku prawnego oraz przy jak najmniejszej ingerencji w prawa i wolności chronione Konstytucją Rzeczpospolitej Polskiej a także w celu zapewnienia społeczeństwu bezpieczeństwa.

Słowa kluczowe:
kontrola operacyjna, organy ścigania, postępowanie karne, dane billingowe, prawo telekomunikacyjne

WSTĘP

Środki masowego przekazu coraz częściej w swoich doniesieniach podejmują tematykę legalności i dopuszczalności korzystania przez organy ścigania z danych gromadzonych i przechowywanych przez usługodawców oraz dostawców telekomunikacyjnych. Inicjowanie debaty publicznej na ten temat

uwidacznia, jak wiele kontrowersji budzi przedmiotowe zagadnienie, które przede wszystkim rozpatrywane jest pod kątem poszanowania praw i wolności obywateli oraz ich ochrony przed nadmierną inwigilacją ze strony państwa. Z jednej strony wskazuje się, że udostępnianie danych przez firmy telekomunikacyjne podmiotom państwowym pozwala w pełniejszy sposób chronić społeczeństwo przed współczesnymi zagrożeniami, zwłaszcza przed coraz to bardziej nowoczesnymi formami przestępczości, głównie o charakterze zorganizowanym bądź terrorystycznym. Z drugiej strony podnosi się, iż korzystanie przez organy ścigania z danych telekomunikacyjnych ujawniających wieloaspektowe informacje dotyczące życia obywateli, to nadmierna ingerencja władzy państwowej w sferę życia prywatnego jednostki, która tylko i wyłącznie naraża społeczeństwo na pogwałcenie ich praw i w konsekwencji godzi w poczucie bezpieczeństwa. Duża dyskusyjność problematyki bez wątpienia ukazuje, jak znacząca jest potrzeba szczegółowego pochylenia się nad zagadnieniem pozyskiwania i udostępniania danych telekomunikacyjnych o obywatelach.

ISTOTA DZIAŁALNOŚCI OPERACYJNEJ

Organy, których priorytetowym elementem funkcjonowania jest ściganie przestępstw, są prawnie zobowiązane, aby w obliczu zaistnienia uzasadnionego podejrzenia popełnienia czynu zabronionego, wszcząć i następnie przeprowadzić postępowanie przygotowawcze, w toku którego docelowo powinien zostać skompletowany materiał dowodowy, potwierdzający fakt popełnienia przestępstwa. Istotne znaczenie dla skutecznego pozyskiwania dowodów ma działalność operacyjna, której przebieg i sposoby realizowania prawodawca określił m. in. na gruncie przepisów ustawy z dnia 6 kwietnia 1990 r. o Policji[1], ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[2], ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym[3], ustawy z dnia 12 października 1990 r. o Straży Granicznej[4] czy też ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego[5].

Działalność operacyjna, określana również jako czynności operacyjno – rozpoznawcze, to wyodrębniony system poufnych lub tajnych działań podejmowanych przez organy ścigania, które mimo, że są prowadzone poza proce-

[1] Dz. U. 1990, nr 30, poz. 179 ze zm.
[2] Dz. U. 2002, nr 74, poz. 676 ze zm.
[3] Dz. U. 2006, nr 104, poz. 708 ze zm.
[4] Dz. U. 1990, nr 78, poz. 462 ze zm.
[5] Dz. U. 2006, nr 104, poz. 709 ze zm.

sem karnym, to służą realizacji aktualnych bądź też przyszłych celów tego procesu oraz wykorzystywane są do zapobiegania i zwalczania przestępczości i innych prawnie określonych zagrożeń społecznych[6]. W ramach wykonywania czynności operacyjno – rozpoznawczych stosowane są wybrane metody operacyjne, będące celowymi zachowaniami i środkami, które w połączeniu z pozyskanymi przez organy wiedzą oraz doświadczeniem, umożliwiają zrealizowanie wyznaczonych celów operacyjnych[7]. Wskazuje się, że najczęściej wykorzystywanymi w toku działalności operacyjnej metodami są przede wszystkim: współpraca z osobowymi źródłami informacji, inwigilacja oraz infiltracja środowisk przestępczych, przedsięwzięcie werbunkowe, kombinacja operacyjne, kontrolowane wręczenie bądź przyjęcie korzyści majątkowej, a także kontrola operacyjna[8].

Metoda operacyjna w postaci kontroli operacyjnej została określona m.in. w art. 19 ust. 6 ustawy o Policji, art. 17 ustawy o Centralnym Biurze Antykorupcyjnym, art. 9e ustawy o Straży Granicznej, art. 36c ustawy o kontroli skarbowej, art. 27 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Zgodnie z treścią regulacji wymienionej w pierwszej kolejności, tj. art. 19 ust. 6 ustawy o Policji, kontrola operacyjna jest prowadzona niejawnie i polega na kontrolowaniu treści korespondencji i zawartości przesyłek oraz na stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie – w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych. Przedmiotowa metoda może mieć zastosowanie jedynie w sytuacji, gdy inne środki okazały się bezskuteczne albo najprawdopodobniej będą nieprzydatne lub nieskuteczne (zasada subsydiarności) w danej sprawie, a także jedynie wówczas, gdy dotyczyć będą czynów wymienionych w art. 19 ust. 1 ustawy o Policji, czyli przestępstw:

1) przeciwko życiu, określonych w art. 148–150 ustawy z dnia 6 czerwca 1997 r. - Kodeks karny[9],
2) określonych w art. 134, art. 135 § 1, art. 136 § 1, art. 156 § 1 i 3, art. 163 § 1 i 3, art. 164 § 1, art. 165 § 1 i 3, art. 166, art. 167, art. 173 § 1 i 3, art. 189, art. 189a, art. 211a, art. 223, art. 228 § 1 i 3-5, art. 229 § 1 i 3-5, art. 230 § 1, art. 230a § 1, art. 231 § 2, art. 232, art. 245, art. 246, art. 252 § 1-3, art. 258, art. 269, art. 280-282, art. 285 § 1, art. 286 § 1, art. 296 § 1-

[6] T. Hanausek, *Kryminalistyka. Zarys wykładu*, Kraków 2005, s. 133.
[7] *Ibidem*, s. 135.
[8] R. Teluk, *Inwigilacja i infiltracja jako efektywne metody uzyskiwania informacji operacyjnych na temat środowiska przestępczego lub kryminogennego*, Zeszyty Prawnicze 2014, nr 14.1, s. 180.
[9] Dz. U. 1997, nr 88, poz. 553 ze zm.

3, art. 296a § 1, 2 i 4, art. 299 § 1-6 oraz art. 310 § 1, 2 i 4 Kodeksu karnego,
3) określonych w art. 46 ust. 1, 2 i 4, art. 47 oraz art. 48 ust. 1 i 2 ustawy z dnia 25 czerwca 2010 r. o sporcie[10],
4) przeciwko obrotowi gospodarczemu, określonych w art. 297-306 Kodeksu karnego, powodujących szkodę majątkową lub skierowanych przeciwko mieniu, jeżeli wysokość szkody lub wartość mienia przekracza pięćdziesięciokrotną wysokość najniższego wynagrodzenia za pracę określonego na podstawie odrębnych przepisów,
5) przeciwko wolności seksualnej i obyczajności, gdy pokrzywdzonym jest małoletni albo gdy treści pornograficzne, o których mowa w art. 202 Kodeksu karnego, obejmują udział małoletniego,
6) skarbowych, jeżeli wartość przedmiotu czynu lub uszczuplenie należności publicznoprawnej przekraczają pięćdziesięciokrotną wysokość najniższego wynagrodzenia za pracę określonego na podstawie odrębnych przepisów,
7) skarbowych, o których mowa w art. 107 § 1 ustawy z dnia 10 września 1999 r. – Kodeks karny skarbowy[11],
8) nielegalnego wytwarzania, posiadania lub obrotu bronią, amunicją, materiałami wybuchowymi, środkami odurzającymi lub substancjami psychotropowymi albo ich prekursorami oraz materiałami jądrowymi i promieniotwórczymi,
9) określonych w art. 8 ustawy z dnia 6 czerwca 1997 r. - Przepisy wprowadzające Kodeks karny[12],
10) określonych w art. 43-46 ustawy z dnia 1 lipca 2005 r. o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów[13],
11) ściganych na mocy umów i porozumień międzynarodowych.

Podmioty, które wykonują działalność telekomunikacyjną, jak również świadczą usługi pocztowe, są prawnie zobligowane do zapewnienia na własny koszt odpowiednich warunków organizacyjnych oraz technicznych, które umożliwią organom skuteczne prowadzenie kontroli operacyjnej[14].

[10] Dz. U. 2014, poz. 715.
[11] Dz. U. 1999, nr 83, poz. 930 ze zm.
[12] Dz. U. nr 88, poz. 554 ze zm.
[13] Dz. U. nr 169, poz. 1411 ze zm.
[14] E. Gruza, *Czynności operacyjno – rozpoznawcze, w: Kryminalistyka – czyli rzecz o metodach śledczych*, E. Gruza, M. Goc, J. Moszczyński, Warszawa 2008, s. 69.

DANE TELEKOMUNIKACYJNE W ŚWIETLE TRUDNOŚCI DEFINICYJNYCH I KONSTYTUCYJNOŚCI PRZEPISÓW

Powołując uregulowania wyrażone w art. 19 ustawy o Policji, należy mieć na uwadze, iż są one wysoce dyskusyjne i wywołują szereg kontrowersji, które niejako stały się przyczyną bliższego pochylenia się nad zagadnieniem ich legalności przez Trybunał Konstytucyjny. W dniach 1, 2 i 3 kwietnia oraz 30 lipca 2014 r. Trybunał rozpoznawał połączone wnioski złożone przez Rzecznika Praw Obywatelskich i Prokuratora Generalnego, które dotyczyły określenia katalogu zbieranych informacji o jednostce za pomocą środków technicznych w toku działań operacyjnych a także zasad niszczenia pozyskanych danych[15]. Zgodnie z wyrokiem wydanym przez Trybunał Konstytucyjny dnia 30 lipca 2014 r.[16] art. 19 ustawy o Policji w zakresie, w jakimi nie ujmuje gwarancji niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów zawierających informacje objęte zakazami dowodowymi, co do których sąd nie uchylił uprzednio tajemnicy zawodowej albo uchylenie to okazało się niedopuszczalne, został uznany jako niezgodny z Konstytucją Rzeczpospolitej Polskiej, a konkretnie z:

1. prawem do obrony we wszystkich stadiach postępowania karnego (art. 42 ust. 2 Konstytucji),
2. prawem do ochrony życia prywatnego (art. 47 Konstytucji),
3. zasadą wolności i ochrony tajemnicy komunikowania się (art. 49 Konstytucji),
4. prawem do ochrony informacji o sobie (art. 51 ust. 2 Konstytucji) oraz
5. zasadą wolności słowa (art. 54 ust. 1 Konstytucji).

Niezgodność art. 19 ustawy o Policji z powyższymi uprawnieniami i obowiązkami konstytucyjnymi została orzeczona w związku z ograniczaniem prawa obywateli do korzystania z konstytucyjnych praw i wolności, o których to stanowi art. 31 ust. 3 Konstytucji. Z uwagi na stwierdzoną niezgodność przepisy art. 19, z dniem 7 lutego 2016 r., utracą moc we wskazanym zakresie.

Pomimo istnienia licznych wątpliwości dotyczących zgodności z zasadami konstytucyjnymi pozyskiwania oraz utrwalania informacji przekazywanych za pośrednictwem sieci telekomunikacyjnych, nie można zaprzeczyć temu, że owe pozyskiwanie i utrwalanie wiadomości niejednokrotnie jest działaniem

[15] Komunikat prasowy Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. wydany po rozprawie w sprawie o sygn. K 23/11, http://trybunal.gov.pl/rozprawy/komunikaty-prasowe/komunikaty-po/art/7005-okreslenie-katalogu-zbieranych-informacji-o-jednostce-za-pomoca-srodkow-technicznych-w-dzialani/, dn. 21.04.2015 r.

[16] Dz. U. 2014, poz. 1055.

niezbędnym, a nawet obligatoryjnym, podczas skutecznego realizowania celów pracy operacyjnej. Uzyskiwanie informacji we wskazany sposób kojarzone jest przede wszystkim z problematyką stosowania podsłuchu operacyjnego, czy też podsłuchu procesowego. Kontrola operacyjna łączy się jednak również z kwestią uzyskiwania przez organy ścigania oraz prokuraturę tzw. bilingów, czyli wykazów połączeń telefonicznych oraz danych abonentów, odnoszących się do pozostających w zainteresowaniu organów ścigania numerów telefonów, na które składają się informacje o:

a) dacie i godzinie rozpoczęcia połączenia, czasie jego trwania i godzinie zakończenia,
b) rodzaju i ewentualnej modyfikacji połączenia poprzez stwierdzenie, iż doszło do połączenia głosowego, nadesłania wiadomości tekstowej bądź multimedialnej, przekierowania połączenia na określony numer abonencki lub wykonania połączenia alarmowego,
c) numerze inicjującym połączenie,
d) numerze technicznym sektora stacji bazowej, w zasięgu którego, w momencie zakończenia połączenia, znajdował się numer telefonu sieci operatora,
e) numerze IMEI (International Mobile Equipment Identity), czyli inaczej o numerze seryjnym urządzenia, w którym podczas połączenia numer abonencki wywołujący/przyjmujący połączenie funkcjonował w sieci operatora przedstawiającego wykaz,
f) numer wywoływany,
g) numer techniczny sektora stacji bazowej, w którego zasięgu znajdował się numer wywoływany w chwili zakończenia połączenia[17].

Ponadto wskazać należy, że w tzw. billingu mogą się również znaleźć adresy BTS dla użytkownika inicjującego połączenie (kolumna opcjonalna pojawia się tylko wtedy, gdy w zapytaniu wybrany został typ billingu „z identyfikacją BTS") oraz dla użytkownika – odbiorcy.

W polskim porządku prawnym brak jest aktualnie legalnej definicji bilingu, jednak w kontekście przedmiotowego opracowania niezbędne jest podjęcie próby wytłumaczenia tego pojęcia. Pomóc w tym mogą przepisy Prawa telekomunikacyjnego, a konkretnie art. 2, w którym to zdefiniowano pojęcia takie jak „połączenie" oraz „połączenie telefoniczne"[18]. Zgodnie z treścią art. 2 pkt 24a pierwsze pojęcie to jest fizyczne lub logiczne połączenie telekomunikacyjnych urządzeń końcowych, które pozwala na przesłanie przekazów teleko-

[17] J. Misztal-Konecka, J. Konecki, *Billing jako dowód w postępowaniu w sprawach o wykroczenia*, Państwo i Prawo 2010, nr 7, s. 79.

[18] A. Staszak, *Prawne podstawy dopuszczalności żądania bilingów*, Przegląd Bezpieczeństwa Wewnętrznego 2011, nr 4, s. 75.

munikacyjnych. W pkt 26 natomiast wskazano, iż połączeniem telefonicznym jest połączenie ustanowione przy pomocy publicznie dostępnej usługi telekomunikacyjnej, umożliwiającej dwukierunkową łączność głosową. W związku z wymienionymi definicjami istotna jest również treść art. 80 ust. 1 Prawa telekomunikacyjnego, w którym to określono, iż dostawca usług telekomunikacyjnych dostępnych publicznie dostarcza każdemu swojemu abonentowi nieodpłatnie, wraz z każdą fakturą, wykaz wykonanych usług telekomunikacyjnych, który zawiera wiadomości o zrealizowanych odpłatnych połączeniach ze wskazaniem, dla każdego typu połączeń, liczby jednostek rozliczeniowych, które odpowiadają wartości połączeń zrealizowanych przez abonenta. Na podstawie wymienionych definicji wyodrębnionych ze wskazanych przepisów możliwe jest określenie pojęcia bilingu jako wykazu wszystkich połączeń telefonicznych, jakie zostały przez abonenta wykonane oraz odebrane[19].

Zgodnie z treścią art. 20c ustawy o Policji w celu zapobiegania lub wykrywania przestępstw Policja może mieć udostępniane dane, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne[20], tzw. dane telekomunikacyjne, do których zaliczają się dane bilingowe wykazujące niezbędne informacje o wykonywanych połączeniach. Co więcej, Policja może te dane także przetwarzać w sytuacjach, gdy wymaga tego postępowanie. Podmiot prowadzący działalność telekomunikacyjną udostępnia informacje telekomunikacyjne nieodpłatnie:

1) policjantowi wskazanemu w pisemnym wniosku Komendanta Głównego Policji lub komendanta wojewódzkiego Policji albo osoby przez nich upoważnionej,
2) na ustne żądanie policjanta posiadającego pisemne upoważnienie Komendanta Głównego Policji lub komendanta wojewódzkiego Policji albo osoby przez nich upoważnionej,
3) za pośrednictwem sieci telekomunikacyjnej policjantowi posiadającemu pisemne upoważnienie Komendanta Głównego Policji lub komendanta wojewódzkiego Policji albo osoby przez nich upoważnionej.

Co istotne, w odniesieniu do art. 20c ustawy o Policji również pojawiły się wątpliwości dotyczące jego zgodności z Konstytucją, w konsekwencji czego jego treść także stała się przedmiotem wniosków Rzecznika Praw Obywatelskich i Prokuratora Generalnego skierowanych do Trybunału Konstytucyjnego. Zgodnie ze wspomnianym już wyrokiem Trybunału z dnia 30 lipca 2014 r. art. 20c ust. 1 ustawy o Policji został uznany za niezgodny z Konstytucją w zakresie zasady ochrony życia prywatnego (art. 47 Konstytucji) oraz zasady wolności i ochrony tajemnicy komunikowania się (art. 49 Konstytucji) w związku z ogra-

[19] *Ibidem*, s. 75.
[20] Dz. U. nr 171, poz. 1800 ze zm.

niczeniami w zakresie korzystania z konstytucyjnych wolności oraz praz (art. 31 ust. 3 Konstytucji). Trybunał stwierdził, że art. 20c ust. 1 ustawy o Policji nie można uznać za zgodny z Konstytucją ponieważ nie przewiduje on niezależnej kontroli udostępnianych danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne. Stwierdzenie niekonstytucyjności art. 20c ust. 1 ustawy o Policji skutkować będzie tym, iż z dniem 7 lutego 2016 r. nastąpi utrata jego mocy.

Orzeczenie niezgodności art. 20c ust. 1 ustawy o Policji z Konstytucją RP nie wyklucza stosowania dalszych ustępów przedmiotowego artykułu, w związku z czym obowiązek nieodpłatnego udostępniania danych telekomunikacyjnych, przez podmioty prowadzące działalność telekomunikacyjną, uprawnionym do uzyskiwania tego rodzaju informacji osobom, pozostaje w mocy. W przypadku udostępnienia danych za pośrednictwem sieci telekomunikacyjnej, udostępnianie danych telekomunikacyjnych odbywa się bez udziału pracowników podmiotu prowadzącego działalność telekomunikacyjną lub przy niezbędnym ich udziale, jeżeli możliwość taka jest przewidziana w porozumieniu zawartym pomiędzy Komendantem Głównym Policji a tym podmiotem. Udostępnienie Policji danych telekomunikacyjnych może nastąpić za pośrednictwem sieci telekomunikacyjnej, jeżeli:

1) wykorzystywane sieci telekomunikacyjne zapewniają:
a) możliwość ustalenia osoby uzyskującej dane, ich rodzaju oraz czasu, w którym zostały uzyskane,
b) zabezpieczenie techniczne i organizacyjne uniemożliwiające osobie nieuprawnionej dostęp do danych;
2) jest to uzasadnione specyfiką lub zakresem zadań wykonywanych przez jednostki organizacyjne Policji albo prowadzonych przez nie czynności.

Materiały uzyskane w wyniku udostępnienia danych telekomunikacyjnych, które zawierają informacje mające znaczenie dla postępowania karnego, Policja przekazuje właściwemu miejscowo i rzeczowo prokuratorowi, natomiast uzyskane w ten sposób materiały, które nie zawierają informacji mających znaczenie dla postępowania karnego, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu.

OBOWIĄZKI PODMIOTÓW WYKONUJĄCYCH DZIAŁALNOŚĆ TELEKOMUNIKACYJNĄ

Określony tryb ujawniania danych niezbędnych przy wykonywaniu czynności operacyjno – rozpoznawczych przez funkcjonariuszy Policji wymaga rzetelności, sumienności i szybkości działania ze strony podmiotu wykonującego działalność telekomunikacyjną, który ponadto obowiązany jest do zachowa-

nia w tajemnicy treści danych ujawnionych Policji. Obowiązkiem udostępnienia przez operatora publicznej sieci telekomunikacyjnej oraz dostawcę publicznie dostępnych usług telekomunikacyjnych objęte są dane niezbędne do:

1) ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego:
a) inicjującego połączenie,
b) do którego kierowane jest połączenie;
2) określenia:
a) daty i godziny połączenia oraz czasu jego trwania,
b) rodzaju połączenia,
c) lokalizacji telekomunikacyjnego urządzenia końcowego.

Kwestię tę reguluje rozporządzenie Ministra Infrastruktury z dnia 28 grudnia 2009 r. w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania[21].

Na mocy przepisu art. 20c ust. 6 ustawy o Policji ustawodawca przewidział, że materiały uzyskane w wyniku czynności podjętych na podstawie art. 20c ust. 2 tej ustawy, które zawierają informacje mające znaczenie dla postępowania karnego, Policja przekazuje właściwemu miejscowo i rzeczowo prokuratorowi. Oznacza to więc, że w postępowaniu karnym uzyskiwanie wykazów połączeń drogą czynności operacyjno – rozpoznawczych prowadzonych na podstawie art. 20c ustawy o Policji jest jak najbardziej możliwe, natomiast wątpliwości budzi zakres jego wykorzystania[22].

Podstawę prawną do wystąpienia przez prokuratora o przekazanie danych telekomunikacyjnych stanowi art. 218 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego[23]. Zgodnie ze wskazanym przepisem podmioty prowadzące działalność telekomunikacyjną obowiązane są wydać prokuratorowi (sądowi) na żądanie, zawarte w postanowieniu dane, o których mowa w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, jeżeli mają one znaczenie dla toczącego się postępowania karnego. Prawo do otwierania lub zarządzania otwarcia tych danych przysługuje prokuratorowi bądź sądowi.

W art. 218 § 2 k.p.k. wskazano, iż postanowienie o żądaniu wydania danych telekomunikacyjnych doręcza się abonentowi telefonu lub nadawcy, któ-

[21] Dz. U. nr 226, poz. 1828.

[22] W. Kotowski, *Komentarz do art. 20c ustawy o Policji, w: Ustawa o Policji. Komentarz*, Warszawa 2012, s. 460 i nast.; zob. A. Szumski, *Rola czynności operacyjno-rozpoznawczych w uzyskiwaniu dowodów w procesie karnym*, Nowa Kodyfikacja Prawa Karnego 2010, t. 26, s. 195.

[23] Dz. U. 1997, nr 89, poz. 555 ze zm.

rego wykaz połączeń lub innych przekazów informacji dotyczy, przy czym doręczenie takiego postanowienia może zostać odroczone na czas oznaczony, niezbędny ze względu na dobro sprawy, lecz nie później niż do czasu prawomocnego zakończenia postępowania. Ponadto, na podstawie art. 218a k.p.k., podmioty prowadzące działalność telekomunikacyjną obowiązane są niezwłocznie zabezpieczyć, na żądanie prokuratora lub sądu, zawarte w postanowieniu, na czas określony, nie przekraczający jednak 90 dni, dane informatyczne przechowywane w urządzeniach zawierających te dane na nośniku lub w systemie informatycznym. Również w tym wypadku doręczenie postanowienia prokuratora lub sądu może zostać odroczone w czasie.

Zgodnie z treścią art. 180c ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne podmiot świadczący usługi telekomunikacyjne ma obowiązek wydać informacje pozwalające na:

- ustalenie zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego inicjującego połączenie, oraz tego, do którego kierowane jest połączenie;
- określenie daty i godziny połączenia oraz czasu jego trwania, rodzaju połączenia, lokalizacji telekomunikacyjnego urządzenia końcowego.

Ponadto art. 180d prawa telekomunikacyjnego stanowi, że przedsiębiorcy telekomunikacyjni są obowiązani do zapewnienia warunków dostępu i utrwalenia oraz udostępnienia uprawnionym podmiotom, a także prokuratorowi, na własny koszt, przetwarzanych przez siebie danych, określonych w art. 159 ust. 1 pkt 1 i 3 – 5, art. 161 oraz art. 179 ust. 9, związanych ze świadczoną usługą telekomunikacyjną. Z treści wskazanych przepisów wynika zatem, iż podmioty, które prowadzą działalność komunikacyjną, obowiązane są wydać Policji, jak również prokuratorowi:

- dane dotyczące użytkownika;
- dane transmisyjne, które oznaczają dane przetwarzane dla celów przekazywania komunikatów w sieciach telekomunikacyjnych lub naliczania opłat za usługi telekomunikacyjne, w tym dane lokalizacyjne, które oznaczają wszelkie dane przetwarzane w sieci telekomunikacyjnej lub w ramach usług telekomunikacyjnych, wskazujące na położenie geograficzne urządzenia końcowego użytkownika publicznie dostępnych usług telekomunikacyjnych;
- dane o lokalizacji, które oznaczają dane lokalizacyjne wykraczające poza dane niezbędne do transmisji komunikatu lub wystawienia rachunku;
- dane o próbach uzyskania połączenia między zakończeniami sieci, w tym dane o nieudanych próbach połączeń, oznaczających połączenia między telekomunikacyjnymi urządzeniami końcowymi lub zakończe-

niami sieci, które zostały zestawione i nie zostały odebrane przez użytkownika końcowego lub nastąpiło przerwanie zestawianych połączeń (art. 159 § 1 pkt 1 i 3–5 prawa telekomunikacyjnego);

- przetwarzane przez siebie dane dotyczące użytkownika będącego osobą fizyczną takie jak: imię i nazwisko, imiona rodziców, miejsce i data urodzenia, adres miejsca zamieszkania oraz adres korespondencyjny, jeżeli jest on inny niż adres miejsca zamieszkania, numer ewidencyjny PESEL (w przypadku obywatela Rzeczpospolitej Polskiej), nazwę, serię i numer dokumentów potwierdzających tożsamość, zaś w przypadku cudzoziemca, który nie jest obywatelem państwa członkowskiego albo Konfederacji Szwajcarskiej – numeru paszportu lub karty pobytu, zawarte w dokumentach potwierdzających możliwość wykonania zobowiązania wobec dostawcy publicznie dostępnych usług telekomunikacyjnych wynikającego z umowy o świadczenie usług telekomunikacyjnych, inne dane przetwarzane, za zgodą użytkownika będącego osobą fizyczną, w związku ze świadczoną usługą telekomunikacyjną, a w szczególności numer konta bankowego lub karty płatniczej, a także adres poczty elektronicznej oraz numery telefonów kontaktowych (art. 161 prawa telekomunikacyjnego),
- dane zawarte w prowadzonym przez przedsiębiorcę telekomunikacyjnym elektronicznym wykazie abonentów, użytkowników lub zakończeń sieci, uwzględniającym dane uzyskane przy zawarciu umowy (art. 179 ust. 9 prawa telekomunikacyjnego).

W kontekście uzyskiwania danych telekomunikacyjnych istotne znaczenie ma treść art. 180a ust. 1 pkt 1 prawa telekomunikacyjnego, zgodnie z którym operator publicznej sieci telekomunikacyjnej oraz dostawca publicznie dostępnych usług telekomunikacyjnych są obowiązani na własny koszt zatrzymywać i przechowywać dane, o których mowa w art. 180c, generowane w sieci telekomunikacyjnej lub przez nich przetwarzane, na terytorium Rzeczypospolitej Polskiej, przez okres 12 miesięcy, licząc od dnia połączenia lub nieudanej próby połączenia. Z dniem upływu wskazanego okresu operator bądź dostawca są zobowiązanie dane te niszczyć, z wyjątkiem jednak tych, które zostały zabezpieczone zgodnie z odrębnymi przepisami. Nadmienić również wypada, iż do dnia 21 stycznia 2013 r. okres przechowywania danych telekomunikacyjnych wynosił 24 miesiące[24].

Odnosząc powyższe regulacje do postępowań karnych stwierdzić należy, iż największe znaczenie będzie tutaj miała regulacja przepisu art. 20c usta-

[24] Art. 180a ust. 1 pkt 1 prawa telekomunikacyjnego został zmieniony przez art. 1 pkt 128 lit. a) ustawy z dnia 16 listopada 2012 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw, Dz. U. 2012, poz. 1445.

wy o Policji, który umożliwia wystąpienie o przekazanie danych telekomunikacyjnych już na etapie czynności rozpoznawczych, a zatem we wstępnej fazie postępowania. Jeżeli natomiast rozważa się przydatność tego rodzaju danych dla postępowania karnego, to wydaje się, że najistotniejsze znaczenie będą miały dane dotyczące położenia urządzeń końcowych, czy odbiorców końcowych, miejsc logowań poszczególnych telefonów, a także dane pozwalające na identyfikację abonentów, z którymi nawiązywano połączenia z telefonu pozostającego w zainteresowaniu śledztwa. Powyższe informacje pozwalają bowiem na określenie miejsca albo wielu miejsc pobytu sprawców przestępstwa, ewentualnie ich ofiar (np. w sytuacji uprowadzenia, wzięcia lub przetrzymywania zakładnika), a także trasy ich przemieszczania się. W omawianym kontekście zwrócić uwagę należy, iż w ramach postępowań karnych w zasadzie niemożliwe jest pozyskanie danych personalnych abonenta telefonu. Powyższe wynika z faktu, iż w większości wypadków sprawcy przestępstw działają w ramach profesjonalnie zorganizowanych grup przestępczych, którzy do kontaktów używają telefonów komórkowych działających w systemie pre – paid[25] . Ponadto najczęściej korzystają oni z co najmniej kilku kart SIM, które po jednorazowym wykorzystaniu ulegają zniszczeniu. Tym niemniej pozyskanie danych telekomunikacyjnych ma istotne znaczenie dowodowe, ponieważ pozwala na ustalenie, czy z danego telefonu kontaktowano się z innymi osobami, a jeśli tak, kim są te osoby i gdzie się znajdowały w chwili kontaktu, itp. Powyższe informacje mogą doprowadzić do ustalenia danych personalnych osób kontaktujących się ze sprawcami czynów zabronionych, zaś na dalszym etapie postępowania mogą także pozwolić na identyfikację samych sprawców, a nawet grupy sprawców.

Wykazy połączeń telefonicznych uzyskane w trybie art. 20c ustawy o Policji są elementem pracy operacyjnej, a ich wartość dowodowa zależy od zakresu oraz sposobu ich wprowadzenia do procesu, natomiast tzw. bilingi pozyskane w trybie art. 218 k.p.k. stanowią w postępowaniu karnym dowód, który oceniany jest przez prokuratora i sąd na takich samych zasadach, jak inne dowody, przede wszystkim zgodnie z zasadą swobodnej oceny dowodów wynikającej z art. 7 k.p.k.. Wykorzystywanie danych telekomunikacyjnych w postaci wykazów połączeń musi jednak przebiegać zgodnie z zasadami ochrony obywatela przewidzianymi w przepisach Konstytucji, lecz nie tylko, bowiem standardy postępowania w przedmiotowych sytuacjach określane są również na gruncie takich aktów prawnych jak Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności.

[25] B. Kaszowska, Porwanie osoby dla okupu w świetle art. 252 kodeksu karnego, Prokuratura i Prawo 2004, nr 10, s. 45.

WNIOSKI

Reasumując, wskazać należy, iż polskie organy ścigania mają możliwość wykorzystywania, w toku swoich czynności rozpoznawczo – operacyjnych, informacji gromadzonych przez podmioty realizujące działalność telekomunikacyjną, w tym kompletowanych przez nie wykazy połączeń abonentów sieci. Co więcej, usługodawcy telekomunikacyjni są prawnie zobowiązani, aby umożliwiać organom wykonywanie ich obowiązków i zadań w zakresie kontroli operacyjnej. Pomimo, że tego rodzaju metody działania operacyjnego wywołują szereg kontrowersji, nie należy tych czynności demonizować ani wykluczać, bowiem ich zastosowanie zwiększa znacząco szanse na skuteczne zwalczanie i przeciwdziałanie przestępczości. Współczesny rozwój technologiczny poszerza możliwości działania organów ścigania, ale również i grup przestępczych. W związku z tym wykorzystywanie wszelkich środków telekomunikacyjnych, które pozwalają zebrać kompletny materiał dowodowy, stanowi gwarancję bezpieczeństwa publicznego, w skali nie tylko naszego kraju, lecz także w odniesieniu do bezpieczeństwa międzynarodowego. Nie można zaprzeczyć, że korzystanie z wykazów połączeń telekomunikacyjnych może dostarczyć organom precyzyjne dane również o życiu prywatnym jednostek, lecz prawodawca jasno wskazał, że korzystanie z tych wiadomości powinno następować jedynie z poszanowaniem obowiązującego porządku prawnego, zwłaszcza zaś konstytucyjnie gwarantowanych praw i wolności, oraz jeśli następuje to dla bezpieczeństwa społeczeństwa bądź też zapobiegania, wykrywania oraz ścigania przestępstw.

BIBLIOGRAFIA

[1] Gruza E., M. Goc, J. Moszczyński, *Kryminalistyka – czyli rzecz o metodach śledczych*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008.

[2] Hanausek T., *Kryminalistyka. Zarys wykładu*, Wolters Kluwer, Kraków, 2005.

[3] Kaszowska B., *Porwanie osoby dla okupu w świetle art. 252 kodeksu karnego*, „Prokuratura i Prawo", 2004, nr 10, s. 42-53.

[4] Kotowski W., *Ustawa o Policji. Komentarz*, Wolters Kluwer, Warszawa, 2012.

[5] Misztal-Konecka J., Konecki J., *Billing jako dowód w postępowaniu w sprawach o wykroczenia*, „Państwo i Prawo", 2010, nr 7, s. 78-87.

[6] Staszak A., Prawne podstawy dopuszczalności żądania bilingów, „Przegląd Bezpieczeństwa Wewnętrznego", 2011, nr 4, s. 72-86.

[7] Szumski A., *Rola czynności operacyjno-rozpoznawczych w uzyskiwaniu dowodów w procesie karnym*, „Nowa Kodyfikacja Prawa Karnego", 2010, t. 26, s. 195-208.

[8] Teluk R., *Inwigilacja i infiltracja jako efektywne metody uzyskiwania informacji operacyjnych na temat środowiska przestępczego lub kryminogennego*, „Zeszyty Prawnicze", 2014, nr 14.1, s. 177-196.

[9] Komunikat prasowy Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. w sprawie o sygn. K 23/11, http://trybunal.gov.pl/rozprawy/komunikaty-prasowe/komunikaty-po/art/7005-okreslenie-katalogu-zbieranych-informacji-o-jednostce-za-pomoca-srodkow-technicznych-w-dzialani/, dn. 21.04.2015 r.

[10] Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 5 marca 2014 r. w sprawie ogłoszenia jednolitego tekstu ustawy o sporcie, Dz. U. 2014, poz. 715.

[11] Rozporządzenie Ministra Infrastruktury z dnia 28 grudnia 2009 r. w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania, Dz. U. Nr 226, poz. 1828.

[12] Ustawa z dnia 1 lipca 2005 r. o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów, Dz. U. Nr 169, poz. 1411 ze zm.

[13] Ustawa z dnia 10 września 1999 r. Kodeks karny skarbowy , Dz. U. 1999, nr 83, poz. 930 ze zm.

[14] Ustawa z dnia 12 października 1990 r. o Straży Granicznej, Dz. U. 1990, nr 78, poz. 462 ze zm.

[15] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, Dz. U. Nr 171, poz. 1800 ze zm.

[16] Ustawa z dnia 16 listopada 2012 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw, Dz. U. 2012 poz. 1445.

[17] Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Dz. U. 2002, nr 74, poz. 676 ze zm.

[18] Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny, Dz. U. 1997, nr 88, poz. 553 ze zm.

[19] Ustawa z dnia 6 czerwca 1997 r. - Kodeks postępowania karnego, Dz. U. 1997, nr 89, poz. 555 ze zm.

[20] Ustawa z dnia 6 czerwca 1997 r. - Przepisy wprowadzające Kodeks karny Dz. U. Nr 88, poz. 554 ze zm.

[21] Ustawa z dnia 6 kwietnia 1990 r. o Policji, Dz. U. 1990, nr 30, poz. 179 ze zm.

[22] Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym, Dz. U. 2006, nr 104, poz. 708 ze zm.

[23] Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, Dz. U. 2006, nr 104, poz. 709 ze zm.

[24] Wyrok Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. sygn. akt K 23/11, Dz. U. 2014, poz. 1055.

BILING DATA SHARING AS A RESPONSIBILITY OF TELECOMMUNICATION COMPANIES IN TERMS OF ENABLING OPERATIONAL CONTROL

ABSTRACT

Following the daily media news can be seen that the issue of legality and acceptability of usage by law enforcement of data collected and stored by service providers and telecommunications service providers still causes considerable controversy. I has to be consulted that in some cases of reasonable suspicion of committing a specific crime, an effective evidence sourcing can be only guaranteed by the operational control instruments, that usage of which is regulated by i.a. law acts of Police, Internal Security Agency, the Intelligence Agency and the Central Anti-Corruption Bureau. The use of technical sources which enable to acquire and sustain the necessary information transmitted through telecommunications networks in a covert way. However, it must be carried out in compliance with the existing legal order and to ensure the public safety.

**Marcin SOKÓŁ, Aleksandra MEKSUŁA,
Magdalena SOKÓŁ**
Laboratorium Przetwarzania Obrazu i Dźwięku Sp. z o.o.
Gdański Park Naukowo-Technologiczny

Wojciech KAMIŃSKI
Kancelaria Adwokatów i Radców Prawnych Pawłowski
Kamiński Skromak Dąbrowska i Partnerzy
Sp. Partnerska
Gdański Park Naukowo-Technologiczny

TECHNIKI ROZSZERZONEJ RZECZYWISTOŚCI I ICH ZASTOSOWANIE W SYSTEMACH KLASY DUAL-USE[1]

STRESZCZENIE

W pracy przedstawiono ogólną koncepcję systemów rozszerzonej rzeczywistości i technik łączących w sobie elementy świata realnego oraz tzw. rzeczywistości wirtualnej. W sposób szczególny praca została poświęcona wyświetlaczom holograficznym 3D, które mogą znaleźć szerokie zastosowanie m.in. w systemach klasy dual-use. W artykule wskazano także kilka przykładów praktycznych zastosowań wielodotykowego wyświetlacza holograficznego 3D, który powstaje obecnie w Laboratorium Przetwarzania Obrazu i Dźwięku Sp. z o.o. Wyświetlacz holograficzny 3D, opracowywany obecnie przez LPOD, zapewni wyświetlanie realistycznego obrazu i interaktywnego interfejsu bez potrzeby używania specjalnych okularów lub hełmów.

Słowa kluczowe:
dual-use, hologramy, rozszerzona rzeczywistość

[1] Niniejsza praca badawcza powstała jako rezultat projektu: *„Opracowanie innowacyjnej technologii wyświetlacza holograficznego 3D”* (Projekt: POIG.01.04.00-22-068/12) współfinansowanego z Europejskiego Funduszu Rozwoju Regionalnego, w ramach Programu Operacyjnego Innowacyjna Gospodarka, Priorytet I – „Badania i rozwój nowoczesnych technologii”, Działanie 1.4 – Wsparcie projektów celowych.

WSTĘP

Przykładem zastosowania systemów bazujących na technikach *rozszerzonej rzeczywistości* jest technologia zastosowana w wyświetlaczu holograficznym 3D opracowywanym przez Laboratorium Przetwarzania Obrazu i Dźwięku Sp. z o.o. (LPOD). W laboratoriach LPOD trwają obecnie zaawansowane prace nad innowacyjną technologią wyświetlacza holograficznego 3D z tzw. funkcją wielokrotnego dotyku *(ang. multitouch display)*, której istotę przedstawiono w sposób poglądowy na rys. 1.

Kluczowymi cechami niniejszego rozwiązania są jego wszechstronność oraz praktyczność zastosowań, co szerzej opisano w dalszej części pracy. W aspekcie technicznym, istota działania opracowywanego w LPOD wyświetlacza holograficznego opiera się na zsynchronizowaniu nagrania z kamery z zaawansowaną aplikacją, a następnie przesłaniu odpowiednio dostosowanego obrazu osobno do każdej z gałek ocznych użytkownika/obserwatora. Zaawansowany system kamer zsynchronizowany jest z systemem projekcji, który zapewni, że właściwy obraz dotrze odpowiednio do prawego i lewego oka każdego z obserwatorów. Dzięki temu procesowi następuje wyświetlanie obrazu w formacie 3D wraz z interaktywnym interfejsem (tzw. wirtualny pulpit) bez potrzeby używania specjalnych okularów lub hełmów.

Rys. 1. Przykład ekranu wykorzystującego technikę umożliwiającą kontrolowanie interfejsów graficznych więcej niż dwoma palcami jednocześnie [1]

Dodatkową cechą przedmiotowego wyświetlacza jest fakt, że kilku widzów może jednocześnie, w czasie rzeczywistym, obserwować wyświetlane obrazy holograficzne, które są w sposób dynamiczny i spersonalizowany dostosowywane do odbioru przez każdego z obserwatorów. Uzyskanie opisanego efektu było możliwe po pomyślnym przeprowadzeniu szeregu badań przemysłowych, między innymi w zakresie redukcji szumów, optoelektronicznej rekonstrukcji hologramów cyfrowych, opracowania algorytmów cyfrowego przetwarzania hologramów, kontroli głębi ostrości w obrazie 3D, komputerowego przetwarzania graficznego cyfrowych hologramów i interpretacji informacji zakodowanych w cyfrowym hologramie i programowania systemów wspomagania komputerowego, projektowania i analizy układu systemu optycznego.

Dzięki opracowywanemu wyświetlaczowi użytkownik będzie mógł doświadczyć rzeczywistego trójwymiarowego obrazu bez konieczności posiadania dodatkowego sprzętu. Ponadto, będzie mógł tworzyć i użytkować wirtualne pulpity, które wyświetlać będą aplikacje komputerowe, filmy i inne treści audiowizualne.

TECHNIKI ROZSZERZONEJ RZECZYWISTOŚCI - PODSTAWOWE POJĘCIA I TERMINY

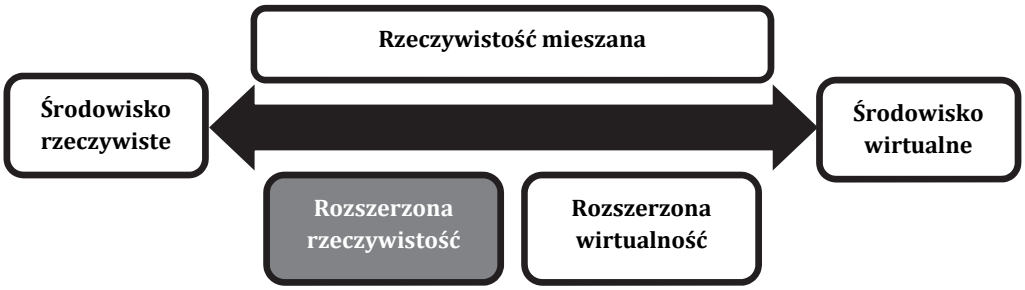
Zagadnienie **rozszerzonej rzeczywistości** *(ang. augmented reality, AR)* autor [2] definiuje, jako obszar badań naukowych, związany z łączeniem obrazu świata rzeczywistego z elementami stworzonymi przy wykorzystaniu technologii informatycznych. Z kolei autorzy [3] definiują rozszerzoną rzeczywistość w sposób bardziej ogólny, jako pewnego rodzaju metodologię pracy z systemami informatycznymi, polegającą na nakładaniu wirtualnych informacji na rzeczywiste obiekty. Nie stanowi ona jednak – z czym zgadza się większość opracowań naukowych z tej dziedziny – rzeczywistości wirtualnej, w której całość postrzeganego obrazu świata wygenerowana jest komputerowo. Rozszerzona rzeczywistość w przeciwieństwie do **rzeczywistości wirtualnej** *(ang. virtual reality, VR)*, nie generuje bowiem zupełnie nowego, wirtualnego obrazu rzeczywistości postrzeganego w trzech wymiarach, lecz poszerza i w specyficzny sposób uzupełnia ten, który realnie istnieje i może być dostrzegany przez obserwatora [2]. Taki kierunek przyjmują również badania naukowe w dziedzinie AR – koncentrują się one na wykorzystywaniu obrazu świata rzeczywistego oraz na rozbudowywaniu go lub na „poszerzaniu" rzeczywistości o dodatkowe wirtualne elementy, wygenerowane przy pomocy techniki komputerowej.

Badacze koncentrując się wokół zagadnienia rzeczywistości rozszerzonej definiują ją także niekiedy, jako rozszerzenie środowiska rzeczywistego, które postrzegane jest za pomocą ludzkich zmysłów takich jak wzrok, słuch, dotyk i węch oraz wzbogaconego przez wirtualne informacje generowane oraz dostarczane przez odpowiednie urządzenia. Autorzy pracy [4] dowodzą, że aby z powodzeniem łączyć dwa światy (rzeczywisty i wirtualny), systemy wykorzystujące techniki rozszerzonej rzeczywistości muszą charakteryzować się podstawowymi właściwościami, takimi jak np.:

- połączenie rzeczywistych i wirtualnych obiektów w spójnym logicznie środowisku rzeczywistym,
- wykonywanie zadań interaktywnie oraz w czasie rzeczywistym lub quasi-rzeczywistym,
- wzajemne dostrojenie (uporządkowanie) obiektów rzeczywistych i wirtualnych względem siebie.

Przedstawione powyżej podstawowe cechy AR zdefiniował i jako pierwszy opisał autor [5], który zwrócił szczególną uwagę na interaktywność w czasie rzeczywistym oraz na umożliwienie ruchu w trzech wymiarach. Warto również zauważyć, że niektórzy badacze zagadnienia AR definiują także zjawisko **pomniejszonej rzeczywistości** *(ang. diminished reality, DR)*. Wywodzi się ono z obserwacji nad aplikacjami oraz systemami stosowanymi w systemach AR, które wymagają usuwania rzeczywistych obiektów zamiast dodawania obiektów wirtualnych. W większości badań zjawisko takie postrzegane jest jednak jako podrozdział danej dziedziny nauki lub zagadnienie wpisujące się w charakterystykę AR, nie zaś jako odrębnie funkcjonujące zagadnienie [6]. Jak zostało już nadmienione w niniejszym opracowaniu, rozszerzona rzeczywistość wywodzi się niejako z rozszerzenia obszaru rzeczywistości wirtualnej, w którym oprogramowanie informatyczne kreuje nowe środowiska wizualne. Jak wynika z analizy literatury przedmiotu, AR nie tworzy wirtualnej rzeczywistości (wirtualnego świata) doświadczalnej w trzech wymiarach, lecz uzupełnia jedynie rzeczywistość o dodatkowe elementy, których specyfika zależy o uwarunkowań aplikacyjnych danego systemu AR. Posługując się np. rozwiązaniami technicznymi takimi jak system kamer połączonych z komputerem oraz czujnikami położenia, system klasy AR może np. realizować funkcje związane z rozpoznawaniem obiektów świata rzeczywistego w otoczeniu, a następnie nakładać na nie wirtualne wytworzone informacje – daje to ogromny potencjał aplikacyjny takim systemach, dzięki wyświetlaniu wirtualnych obiektów w świecie rzeczywistym, w atrakcyjnej dla użytkownika formie. W odróżnieniu od rzeczywistości rozszerzonej – rzeczywistość wirtualna ograniczona jest do wyświetlania jedynie obiektów generowanych komputerowo, które nie wchodzą w interakcje z obiektami rzeczywistymi [3].

Zależności oraz relacje między światem rzeczywistym a wirtualnym opisali autorzy [6], którzy opracowali i zaprezentowali model wzajemnych relacji obu światów. Stworzyli oni koncepcję schematu ciągłości rzeczywistość-wirtualność *(ang. virtuality continuum, VC)*, na bazie którego zdefiniowana została tzw. **rzeczywistość mieszana***(ang. mixed reality, MR),* obrazując tym samym m.in. obszar występowania zjawiska rozszerzonej rzeczywistości.



Rysunek 1. Schemat ciągłości rzeczywistość–wirtualność
(opracowanie na podstawie: [7])

Według koncepcji autorów [7] należy przyjąć, że jednym z końców przedstawionego schematu jest środowisko rzeczywiste, a drugim natomiast – środowisko wirtualne. Rozszerzona rzeczywistość umiejscowiona jest wówczas bliżej środowiska rzeczywistego. Rozszerzona wirtualność z kolei znajduje się natomiast bliżej środowiska wirtualnego. Im bardziej system zbliża się w kierunku wirtualnej rzeczywistości tym bardziej zredukowana zostaje liczba elementów rzeczywistych. Zgodnie z tą koncepcją rzeczywistość może być rozszerzana o wirtualne elementy, a wirtualność o elementy rzeczywiste. Ten obszar wzajemnych relacji nazwany został **rozszerzoną wirtualnością** *(ang. augmented virtuality, AV)* oraz umiejscowiony w obrębie schematu – tuż przy środowisku wirtualnej rzeczywistości. Model zaproponowany przez autorów [7] jest do dziś dnia podstawą do klasyfikacji wszystkich zdefiniowanych systemów, w których stykają się ze sobą światy – rzeczywisty i wirtualny [2]. Opracowanie to stanowi fundament do dalszych prac badawczych oraz prób przedstawiania nowych klasyfikacji omawianych zagadnień, których podejmują się kolejni badacze[2].

Współcześnie rozwój badań w dziedzinie rozszerzonej rzeczywistości pozwolił na wyjście rozwiązań technologicznych oraz zastosowań systemów bazujących na AR poza fazę prototypów laboratoryjnych. Rozwój technologiczny pozwolił na wyeliminowanie wielu problemów natury technicznej, które do tej pory ograniczały możliwości szerokiego zastosowania technik AR na różnorodnych polach potencjalnych aplikacji klasy *dual-use*[3]. Można więc stwierdzić, że

[2] Jednym z przykładów opracowań przedstawiających inny rodzaj klasyfikacji różnego rodzaju rzeczywistości, który wywodzi się ze schematu Milgrama i Kishino, jest klasyfikacja zaprezentowana w pracy autorstwa [8]: Marc Aurel Schnabel, Xiangyu Wang, Hartmut Seichter, Tom Kvan, *From virtuality to reality and back,* IASDR07 International Association of Societies of Design Research, The Hong Kong Polytechnic University, 2007, s. 9-10.

[3] **Systemy klasy dual-use** - systemy, które bezpośrednio lub po przeprowadzeniu niewielkich prac dostosowawczych mogą znaleźć zastosowanie zarówno cywilne, jak i militarne.

postęp technologiczny końca XX i początku XXI wieku, umożliwił urzeczywistnienie wielu rozwiązań i zastosowań, które pierwotnie traktowane były jedynie jako projekty czysto futurystyczne.

Planowanie, wdrażanie i tworzenie systemów bazujących na technikach AR stało się w ostatniej dekadzie intensywnie rozwijającą się dziedziną nauki, a co za tym idzie, również przemysłu. Systemy oparte na AR znajdują obecnie powszechne zastosowanie w wielu obszarach gospodarki takich jak: architektura, komunikacja, logistyka, nawigacja, hydrologia, geologia, ekologia, marketing, technologie wykorzystywane w edukacji i rozrywce. Zastosowania wdrożeń wykorzystujących elementy rozszerzonej rzeczywistości znalazły swoje miejsce również w obszarach tak kluczowych dla rozwoju gospodarczego i społecznego państw, jak medycyna oraz szerokorozumiane systemy bezpieczeństwa wewnętrznego i zewnętrznego. Zastosowania militarne [8], jak i cywilne zyskały na znaczeniu i obejmują coraz to szersze aspekty ludzkiego życia. W kolejnym rozdziale niniejszego opracowania zaprezentowane zostaną bliżej rozwiązania technologiczne oraz przykłady zastosowania technik opartych na AR w systemach i urządzeniach klasy dual-use.

WYBRANE PRZYKŁADY PRAKTYCZNYCH ZASTOSOWAŃ TECHNIK AR W SYSTEMACH DUAL-USE

Jak zostało już wstępnie nadmienione we wcześniejszych rozdziałach tej pracy, dynamiczny rozwój technologiczny ostatnich dwóch dekad spowodował znaczne rozszerzenie się pola dla potencjalnych zastosowań systemów bazujących na *AR*. W niniejszym rozdziale zaprezentowane zostaną przykłady praktycznych zastosowań technik *rozszerzonej rzeczywistości* w oparciu o kilka reprezentatywnych przykładów, które po przeprowadzeniu pewnych prac dostosowawczych na poziomie sprzętowo-programowym, będą mogły znajdować również inne zastosowania aplikacyjne.

Wielodotykowy wyświetlacz holograficzny 3D opracowywany w laboratoriach LPOD jest przykładem rozwiązania, bazującego na technikach *rozszerzonej rzeczywistości,* które będzie mogło znaleźć bardzo szerokie zastosowanie w wielu obszarach, zarówno cywilnych, jak i militarnych. Zakres możliwych zastosowań praktycznych takiego wyświetlacza uwarunkowany jest w znacznej mierze od rozwoju różnego rodzaju aplikacji, które będą w stanie wykorzystać pełnię możliwości sprzętowych przedmiotowego wyświetlacza.

Jednym z przykładowych zastosowań omawianego wyświetlacza holograficznego 3D są systemy komunikacji. Ten obszar wdrożeń projektowanego wyświetlacza 3D cechuje się bardzo dużym potencjałem w zakresie zainteresowania potencjalnych użytkowników oraz możliwości komercjalizacji. Wpisuje

się on bowiem w jedną z podstawowych potrzeb człowieka jaką jest porozumiewanie się a tym samym przekazywanie informacji. W ramach omawianego obszaru zastosowań, wyświetlacz holograficzny stanowi idealne rozwiązanie technologiczne do zastosowania w usługach wideokonferencji o ultrarealistycznej jakości wyświetlanego obrazu holograficznego. Usługa komunikacyjna wykorzystująca realistyczną projekcję może w znaczący sposób uatrakcyjnić oraz usprawnić sposób przekazywania treści audiowizualnych. Analizę korzyści oraz przewagę zdalnych wideokonferencji wykorzystujących techniki *AR* nad tradycyjnymi wideokonferencjami odnaleźć można w opracowaniach autorów zajmujących się niniejszą dziedziną [2]. W opracowaniach tych podnosi się m.in. kwestię niebywałej użyteczności jaką może zapewnić wyświetlacz 3D – jest nią swoiste „uwolnienie" użytkownika od własnego biurka oraz umożliwienie mu uczestnictwa w konferencji z dowolnej lokalizacji. Zastosowanie wyświetlacza holograficznego 3D pozwoli w tym przypadku również na łatwiejsze odczuwanie obecności zdalnych uczestników rozmowy oraz na odczytywanie niewerbalnych sygnałów wysyłanych przez rozmówców. Usługi oparte na technologii hologramów 3D mogą znaleźć zastosowanie w komunikacji biznesowej oraz we wszystkich dziedzinach życia społecznego i politycznego, które opierają się na różnego rodzaju rozmowach, negocjacjach, debatach i dyskusjach. W sytuacjach takich obecność czy raczej wrażenie niemalże namacalnej obecności i bliskości rozmówcy może przyczynić się do znacznego ułatwienia procesu komunikacji, a tym samym przynieść wiele obopólnych korzyści oraz wypracowanych w ten sposób rozwiązań. Z tych samych przyczyn zastosowanie opracowywanego wyświetlacza holograficznego 3D odnajdzie się również bardzo dobrze w zastosowaniach typu militarnego. Możliwa jest bowiem realizacja tzw. holopołączeń, które zostaną wykorzystane w komunikacji na linii dowództwo sztabu – kontyngent wojska przebywający na misji w odległym miejscu lub wspomniany już kontyngent – a rodziny żołnierzy oddalone często o tysiące kilometrów. Holograficzne wideorozmowy, będą możliwe dzięki wyposażeniu telefonów lub specjalnie do tego stworzonych mobilnych urządzeń wyposażonych w tzw. mikroprojektory holograficzne. Warto również podkreślić fakt, że przedmiotowy wyświetlacz holograficzny, dzięki wykorzystaniu zaawansowanych rozwiązań sprzętowo-programowych będzie w stanie realistycznie odwzorować wszystkie ruchy i okazywane emocje rozmówców, tworząc w pewnym sensie nową jakość w formie komunikacji [10]. Nie do przecenienia zdaje się bowiem wartość dodana jaką niosłaby ze sobą tego typu komunikacja wzbogacona rozwiązaniami, które umożliwia wyświetlacz holograficzny 3D opracowywany przez LPOD.

Zastosowania o charakterze militarnym stanowią jeden z głównych obszarów potencjalnej implementacji systemów opracowanych na bazie AR. Dzięki realistycznej wizualizacji trójwymiarowej oferowanej przez opracowywany wyświetlacz 3D, możliwe stanie się np. planowanie misji wojskowych przy uwzględnieniu o wiele większej liczby czynników niż było to możliwe do tej pory.

Dowódca mający podgląd na wszystkie swoje oddziały znajdujące się w terenie, będzie miał możliwość reagowania i podejmowania decyzji taktyczno-operacyjnych w czasie rzeczywistym (np. zmiana taktyki, zadań oraz położenia poszczególnych jednostek poprzez gesty wykonywane rękoma i wydawane komendy głosowe). Możliwe stanie się również opracowanie aplikacji, które umożliwią relokację wirtualnych dronów znajdujących się w przestrzeni 3D w inne miejsce tej wirtualnej przestrzeni, co w rzeczywistości skutkowało będzie zmianą położenia lub trajektorii rzeczywistych obiektów na realnym polu walki. Aplikacje wykorzystujące techniki obrazowania 3D pozwolą również na wizualizację oraz symulację pola walki dzięki obrazowaniu ukształtowania terenu oraz dostarczania dodatkowych informacji na temat lokalizacji obiektów [11].

Innym przykładem możliwej implementacji proponowanego rozwiązania technologicznego wizualizacji 3D w systemach klasy dual-use są zastosowania w lotnictwie (zarówno cywilnym, jak i wojskowym). Po przeprowadzeniu pewnych prac dostosowawczych możliwe będzie bowiem zastosowanie opracowywanego w LPOD wyświetlacza holograficznego np. w samolotach, w celu realistycznej wizualizacji ukształtowania terenu z wykorzystaniem technik holograficznych (użytecznych np. w procesie podchodzenia statku powietrznego do lądowania). Systemy tego typu, przedstawiając realistyczną projekcję map terenu, powinny umożliwić obserwację przez wielu użytkowników przy możliwości uzyskania obrazu autostereoskopowego oraz pełnej paralaksy 3D. Podobnie jak w przypadku holograficznych wyświetlaczy map terenu rozwiązanie to wykorzystywać będzie ludzki system obrazowania i postrzegania, przy możliwościach wykonywania połączeń z wykorzystaniem realistycznych technik obrazowania. Dzięki wykorzystaniu opracowanego w LPOD wyświetlacza holograficznego 3D oraz dedykowanego oprogramowania możliwe stanie się rozwijanie zaawansowanych, w pełni interaktywnych systemów planowania misji i lotów wojskowych oraz cywilnych. Takie systemy umożliwiać będą holograficzne zobrazowanie ograniczeń w przestrzeni powietrznej pod kątem kartograficznym w połączeniu z informacjami meteorologicznymi, pozwolą również na uzyskanie autostereoskopowego odwzorowania przestrzeni.

Kolejnym znaczącym obszarem, w którym znajdują swoje zastosowanie systemy wizualizacji holograficznej 3D jest medycyna. Na tym polu istnieje wiele potencjalnych możliwości wdrażania opracowywanych technologii bazujących na systemach *rozmytej rzeczywistości*. W przypadku wyświetlaczy holograficznych niezwykle ciekawym i atrakcyjnym obszarem ich zastosowania jest możliwość holograficznych rekonstrukcji (w formie projekcji holograficznych 3D) obrazu z tomografów komputerowych lub skanerów wykorzystujących zjawisko rezonansu magnetycznego (MRI). Przy wykorzystaniu hologramu, odpowiednio przeszkolony specjalista będzie w stanie zaobserwować dużą liczbę szczegółów obrazowania, ze względu na to, że możliwe będzie oglądanie wielu płaszczyzn

projekcyjnych jednocześnie. Zaprojektowana przez LPOD, innowacyjna funkcjonalność wielokrotnego dotyku w wyświetlaczu 3D, teoretycznie umożliwi chirurgom zdalne uczestniczenie w operacji. Dzięki wykorzystaniu interaktywnych mechanizmów obrazowania holograficznego lekarze biorący udział w zdalnej operacji chirurgicznej będą mieli możliwość wskazywania punktów lub pól operacyjnych, które np. w rzeczywistej sali operacyjnej zostaną wyświetlone bezpośrednio na ciele operowanego.

Zaprezentowane przykłady zastosowań wielodotykowego wyświetlacza 3D opracowywanego przez LPOD, które przedstawione zostały w niniejszym opracowaniu ograniczone zostały do grupy reprezentatywnych zastosowań, które nie wykluczają jednak szerszego pola potencjalnych zastosowań opracowanej technologii. Wyświetlacz holograficzny 3D będzie mógł znaleźć również inne zastosowania aplikacyjne w obszarach takich jak: meteorologia, architektura, komunikacja, logistyka, nawigacja, hydrologia, robotyka, biomechanika, geologia, ekologia, reklama i marketing, techniki wykorzystywane w edukacji i rozrywce.

Konstrukcja oraz możliwości aplikacyjne wyświetlacza holograficznego 3D, który opracowywany jest przez badaczy z LPOD wpisuje się w oczekiwania naukowców odnośnie przewidywanych kierunków rozwoju systemów opartych na *AR* oraz ich zastosowań technologicznych [2]. Proponowane przez LPOD rozwiązania wykraczają już nawet w chwili obecnej poza obszar zagadnień, które prognozowane były kilka lat temu jako kierunek rozwoju tej dziedziny.

WNIOSKI

Dynamiczny rozwój techniki prowadzi do konieczności opracowania nowych systemów wizualizacyjnych m.in. w zakresie wizualnej analizy danych. Rozwój technik *rozszerzonej rzeczywistości* stał się inspiracją do opracowania w LPOD intuicyjnego, interaktywnego, wizualnego interfejsu wykorzystującego techniki holograficzne oraz zaawansowane technologicznie platformy wieloprocesorowe, sprzętowo-programowe architektury oraz systemy akcelerujące. Aktualnie, prowadzone są w LPOD prace dostosowawcze oraz badania w dwóch głównych płaszczyznach: symulowanie warunków oraz rozszerzona rzeczywistość.

PODZIĘKOWANIA

Niniejsza praca badawcza powstała jako rezultat projektu: „Opracowanie innowacyjnej technologii wyświetlacza holograficznego 3D" (Projekt: POIG. 01.04.00-22-068/12) współfinansowanego z Europejskiego Funduszu Rozwoju Regionalnego, w ramach Programu Operacyjnego Innowacyjna Gospodarka, Priorytet I – „Badania i rozwój nowoczesnych technologii", Działanie 1.4 – Wsparcie projektów celowych.

BIBLIOGRAFIA

[1] http://www.engadget.com/2010/04/20/synaptics-extends-multitouch-gesture-suite-to-linux-chrome-os-i/ [6.02.2015].

[2] Pardel P., *Przegląd ważniejszych zagadnień rozszerzonej rzeczywistości*, „Studia Informatica", Gliwice 2009, t. 30, nr 1(82), s. 25-64.

[3] Bartosik M., Filip A., Kozera P., *Poszerzona rzeczywistość w edukacji, E-edukacja – analiza dokonań i perspektyw rozwoju*, Fundacja Promocji i Akredytacji Kierunków Ekonomicznych, Warszawa 2009, s. 144-149.

[4] Nektarios N. Kostaras, Michalis N. Xenos, *Assessing the Usability of Augmented Reality Systems*, 13th Panhellenic Conference on Informatics, 09/2009, Corfu; Greece 2009, s. 197-201.

[5] Azuma R.T., *A survey of Augmented Reality*, Presence: Teleoperators and Virtual Environments 6(4), 1997, s. 355-385.

[6] Azuma R.T., Baillot Y., Behringer R., Feiner S., Julier S., MacIntyre B., *Recent Advances in Augmented Reality*, IEEE Computer Graphics and Applications 21:6 (2001), s. 34-47.

[7] Milgram P., Kishino F., *A Taxonomy of Mixed Reality Visual Displays*, IEICE Trans. Information Systems, vol. E77-D, no. 12, 1994, s. 1321-1329.

[8] http://teambluehci.blogspot.com [06.02.2015].

[9] Schnabel M. A.,Wang X., Seichter H., Kvan T., *From virtuality to reality and back*, IASDR07 International Association of Societies of Design Research, The Hong Kong Polytechnic University, 2007, s. 1-15.

[10] Kuechler M., Kunz A., *HoloPort - a device for simultaneous video and data conferencing featuring gaze awareness*, Virtual Reality Conference, March 2006, s. 81-88.

[11] Julier S., Lanzagorta M., Baillot Y., Rosenblum L., Feiner S., Hollerer T., Sestito S., *Information filtering for mobile augmented reality*, Proceedings of IEEE and ACM International Symposium on Augmented Reality, ISAR 2000, s. 3-11.

[12] http://www.engadget.com/2010/04/20/synaptics-extends-multitouch-gesture-suite-to-linux-chrome-os-i/ [6.02.2015].

TECHNIQUES OF AUGUMENTED REALITY AND THEIR APPLICATION IN THE DUAL-USE CLASS SYSTEMS

ABSTRACT

The paper presents the general concept of augmented reality systems and techniques that combine elements of the real world and virtual reality. In particular, the work has been devoted to the 3D holographic displays for that may be widely used the dual-use class systems. The article also identifies some examples of practical applications of the holographic 3D display with multitouch function, which is currently being built at the Laboratory of Image and Sound Processing. Developed by LPOD holographic 3D display will provide a realistic picture and interactive interface without the need for special glasses or helmets.

Piotr SZCZUKO
Wydział Elektroniki, Telekomunikacji i Informatyki,
Politechnika Gdańska

MONITORING I POSZANOWANIE PRYWATNOŚCI – NOWA METODA ANONIMIZACJI DANYCH WIZYJNYCH

STRESZCZENIE

W rozdziale poruszany jest aspekt prywatności osób rejestrowanych w nagraniach monitoringu wizyjnego. Systemy monitoringu często są nadzorowane na żywo przez operatorów, a przez to dochodzić może do naruszeń, udostępniania mediom materiału bez zgody utrwalonych w nim osób, podglądania miejsc prywatnych. Kamery posiadają możliwość automatycznego zasłaniania wybranych miejsc kadru, jednakże jest to skuteczne wyłącznie dla stałych elementów sceny i nie chroni prywatności osób poruszających się w przestrzeni publicznej. W rozdziale opisano autorską koncepcję pseudonimizacji danych wizyjnych: tworzenia „wizualnej parafrazy" dla oryginalnej treści, dzięki automatycznemu zastępowaniu sylwetek osób wirtualnymi postaciami, naśladującymi podstawowe czynności. Uzyskiwany materiał wideo daje operatorowi świadomość sytuacji i pozwala na realizację podstawowych celów. Metoda może mieć zastosowanie w monitoringu, w przygotowywaniu nagrań do prezentacji w mediach i w innych formach publikacji obrazu, w których tożsamość prezentowanych osób nie jest istotna.

Słowa kluczowe:
prywatność, monitoring, anonimizacja, rzeczywistość wirtualna, animacja komputerowa

WPROWADZENIE

Poczucie bezpieczeństwa jest podstawową potrzebą każdego człowieka. Obecnie powszechne są dwa sprzeczne trendy związane z bezpieczeństwem – instalowanie kamer monitoringu w miejscach publicznych oraz ochrona prywatności, wizerunku, danych osobowych w mediach i życiu codziennym.

Pomimo powszechnej dostępności na rynku kamer i dużej łatwości ich instalacji i tworzenia nowych systemów monitoringu brak jest ścisłych regulacji dotyczących stosowania technologii rejestracji wizyjnej w miejscach publicznych. Jednocześnie obecność kamer ma dwojaki wpływ na poczucie bezpieczeństwa. Po pierwsze może wywoływać poczucie, że teren monitorowany musi być niebezpieczny, gdyż instalowanie kamer musi być czymś uzasadnione. Po drugie rozmywa odpowiedzialność, tj. świadkowie zdarzeń mogą czuć się zwolnieni z obowiązku reagowania, skoro incydent utrwalany jest przez kamery i to zadaniem operatora monitoringu jest reagować. W rozdziale tym poruszane są jednakże inne ważne aspekty stosowania monitoringu, mianowicie zabezpieczanie wizerunku osób i rejestrowanego materiału przed niepowołaną publikacją.

MONITORING WIZYJNY I PRYWATNOŚĆ

Wraz z postępem technologii monitoringu wizyjnego konieczne staje się opracowanie metod zabezpieczania wizerunku i prawa do poszanowania prywatności. Systemy monitoringu wizyjnego często nadzorowane są na żywo przez operatorów, a przez to dochodzić może do naruszeń, np. udostępniania mediom materiału bez zgody utrwalonych w nim osób lub podglądania miejsc prywatnych ulokowanych w zasięgu kamer: okien, tarasów, itp. Skala tego zjawiska jest duża, gdyż wysokorozwinięte aglomeracje miejskie monitorowane są przez setki kamer. Przykładowo w Londynie pojedyncza osoba rejestrowana jest kilkadziesiąt razy każdego dnia.

Nowoczesne kamery cyfrowe posiadają możliwość automatycznego zasłaniania wybranych miejsc kadru, zawierających dane identyfikujące (np. twarz, numer rejestracyjny pojazdu, itp.) [7]. Najczęściej stosowane są proste operacje na obrazie: rozmywanie, wycinanie, mozaikowanie, jednakże mogą one zaburzyć czytelność obrazu i wpłynąć na zrozumiałość obserwowanych zdarzeń, dokładność oceny sytuacji, postrzeganą liczbę osób. Ponadto oprogramowanie wbudowane w kamery pozwala definiować strefy prywatności, np. zasłonić obszar okien. Jednakże jest to skuteczne wyłącznie dla stałych elementów sceny i nie chroni prywatności osób poruszających się w przestrzeni publicznej.

Wobec powyższego proponowane jest zastosowanie tzw. pseudonimizacji danych wizyjnych: tworzenie „wizualnej parafrazy" dla oryginalnej treści. Zastępowanie informacji, np. obrazów twarzy, nazwisk, danych osobowych i innych danych wrażliwych to proces nazywany anonimizacją. Jego wariantem jest pseudonimizacja, polegająca na tym, że konkretna osoba na czas przetwarzania danych otrzymuje stały pseudonim. Tworzona jest pewna parafraza tre-

ści oryginalnej, nieniosąca tej samej zawartości informacyjnej, a zastępująca ją i redukująca. Dla obrazu osoby rejestrowanego przez kamerę parafrazą będzie obraz sylwetki wirtualnej, która nie posiada identycznych cech osobowych, ma anonimową twarz, a współdzieli tylko wzrost i sposób poruszania się.

W miejsce osób obecnych przed kamerą wstawione zostają obrazy wirtualnych, animowanych sylwetek, naśladujących wybrane czynności obserwowanych osób: chód, bieg [14][30]. Takie przetwarzanie strumienia wizyjnego działać powinno w czasie rzeczywistym, z możliwie małym opóźnieniem, pozwalając na monitorowanie na żywo, a ponadto uwzględniać liczbę osób w kadrze, ich lokalizację, kierunek i prędkość poruszania. W kolejnych podrozdziałach opisano sposób wydobywania istotnych parametrów z obrazu i wykorzystanie ich do pozycjonowania sylwetek 3D i animowania ich zgodnie z rzeczywistym ruchem marszu lub biegu.

Aby zapewnić operatorowi możliwie najlepszy ogląd sytuacji do tworzenia zanonimizowanego strumienia wideo stosowana jest technika rzeczywistości wzbogaconej (ang. *augmented reality* AR), polegająca na uzupełnianiu obrazu rzeczywistego elementami wirtualnymi. Popularne jest wykorzystanie kamery w telefonie oraz GPS i kompasu i uzupełnianie obrazu rzeczywistych budynków, ulic i zabytków na ekranie telefonu etykietami, opisami, odnośniki, itp. [22][29][42].

Wzbogacanie rzeczywistości możliwe jest też poprzez zastosowanie znaczników z czarno-białym wzorem. Aplikacja komputerowa znajduje je w strumieniu z kamery i przedstawia użytkownikowi obraz, w którym wzór ten zastępowany jest elementem wirtualnym, orientowanym, skalowanym i przesuwanym zgodnie z pozycją znacznika [31]. Zaawansowane AR występuje także w technikach telewizyjnych: studio lub plan wzbogacane są wirtualnymi obiektami, z którymi aktorzy wchodzić mogą w interakcję. Dla zwiększenia realizmu odpowiednie metody generowania obrazu 3D symulują oświetlenie i cienie zgodne z warunkami w studio [25].

Autor proponuje zastosowanie technologii AR do przetwarzania strumieni wideo w monitoringu. W tym wypadku obraz tła wzbogacany jest elementami wirtualnymi, awatarami zastępującymi rzeczywiste osoby, naśladującymi podstawowe czynności i zachowanie.

Pozyskiwanie z obrazu z kamer informacji o zachowaniu osób jest nazywane bezkontaktową rejestracją ruchu (ang. *motion capture*). Dla uzyskania precyzyjnych danych o położeniu ciała w przestrzeni konieczne jest stosowanie wielu kamer, kosztownej obliczeniowo optymalizacji i rozstrzygania konfliktów [19]. Najpopularniejszą metodą estymacji pozy jest synteza i porównanie [18]. Polega na tworzeniu wielu hipotetycznych póz w pamięci komputera (przedstawianych jako obiekty trójwymiarowe) i sprawdzaniu zgodności między pozą każdego z modeli a aktualnie obserwowanym układem ciała osoby w płaskim obrazie z kamery. Brane są pod

uwagę parametry pozy, jej poprawność biomechaniczna i ciągłość ruchu z poprzednich chwil czasu [4][11][34][35]. Podejście to jest niestety wymagające i złożone obliczeniowo.

W prezentowanych badaniach przyjęto założenie o uproszczeniu problemu bezkontaktowej obserwacji ruchu ciała. Brak wymogu wysokiej zgodności i poprawności ruchu pozwala na przyspieszenie obliczeń (oczekiwane jest przetwarzanie co najmniej 25 klatek na sekundę). Do opisu parametrów ruchu wykorzystywane są wobec tego wyłącznie parametry obwiedni sylwetki, z których estymowane są inne dane: prędkość ruchu, sposób poruszania (marsz, bieg), położenie w przestrzeni. Ostatecznie, w porównaniu do oryginalnego obrazu, zauważalne mogą być różnice między generowanym modelem 3D a rzeczywistą sylwetką, jednakże są one dopuszczalne, o ile zachowana jest zgodność położenia w kadrze, orientacji i sposobu poruszania się.

ANALIZA STRUMIENI WIZYJNYCH I WYKRYWANIE OBIEKTÓW

Anonimizacja możliwa jest dzięki zastępowaniu całych sylwetek osób obecnych w kadrze kamery automatycznie generowanymi wirtualnymi postaciami, pozbawionymi cech osobowych. Poniżej pokrótce opisano zastosowane metody analizy materiału wizyjnego i wykrywania obiektu ruchomego i określania jego położenia w kadrze. Informacje o zmianach położeń w czasie i o rozmiarach obiektów wykorzystywane są w autorskiej metodzie wytwarzania wirtualnego obrazu sylwetek poruszających się po monitorowanym obszarze. Wirtualne postacie umieszczane są w miejscach odpowiadających pozycjom rzeczywistych osób i animowane w sposób naśladujący podstawowe czynności tych osób. W ten sposób uzyskiwany jest materiał wideo pozbawiony cech osobowych, dający operatorowi świadomość sytuacji i pozwalający na realizację podstawowych celów monitoringu.

Algorytm analizy obrazu z kamery musi w pierwszym kroku wykrywać obiekty ruchome i śledzić ich ruch w czasie, gromadząc w ten sposób parametry wykorzystywane przez moduł animowania i generowania obrazu obiektów wirtualnych. W literaturze opisywane jest kilka metod wykrywania i śledzenia [2][3][12][13][15][16][32][38], poniżej przytoczono założenia stosowanej metody modelowania i odejmowania tła i filtracji Kalmana [10][24].

Detekcja obiektów

W celu wykrywania obiektów realizowany jest proces modelowania tła, typowy dla zastosowań monitoringu [9][37]. Zakłada się, że kolor każdego

piksela zmienia się w czasie obserwacji, co wyrażane jest parametrami rozkładu gaussowskiego. Dla każdej klatki strumienia wideo dokonuje się aktualizacji modelu, co pozwala uwzględniać zjawiska takie jak zmiana oświetlenia, cienie, cykliczny ruch roślinności, itp. Dla każdego piksela obecnej klatki obrazu wyznacza się jego odstępstwo od modelu i, jeżeli jest ono dostatecznie duże, klasyfikuje się go jako należącego do obiektu pierwszoplanowego lub do tła. Piksele obiektów tworzą maskę binarną (rys. 1b), która następnie jest przetwarzania morfologicznie – odszumiana, wygładzana [9]. Indywidualne, odseparowane od siebie regiony w masce traktowane są jako właściwe obiekty i wpisywane są w prostokątne obwiednie (ang. *bounding box*).

Śledzenie obiektów

Śledzenie wykrytych obiektów wykorzystuje filtrację Kalmana [10], która polega na przetwarzaniu zmiennych w czasie parametrów obwiedni: pozycji *x*, *y*, rozmiaru (szerokość, wysokość) *height, width*, odchyłek tych wartości Δ*x*, Δ*y*, Δ*height*, Δ*width*. Zakłada się, że obserwowane parametry są niedokładne i zaszumione, wobec czego należy estymować wartości prawidłowe, biorąc pod uwagę wcześniejsze wartości i dotychczasowy trend i bezwładność zmian. Filtracja Kalmana skutkuje płynniejszymi zmianami położeń i rozmiarów obwiedni obiektów i umożliwia skuteczne rozstrzyganie kolizji (dwa obiekty mijają się) i chwilowych przesłonięć obiektów [10]. Dzięki filtracji obwiednia dokładniej podąża za ruchem rzeczywistego obiektu.

Rys. 1. Proces detekcji i śledzenia obiektów: a) klatka oryginalna, b) maski wykrytych obiektów, c) wyznaczone obwiednie po filtracji Kalmana

Kalibracja kamery i wspólny układ odniesienia

Wyniki przetwarzania obrazu, tj. parametry obwiedni obiektów, wykorzystywane są jako dane wejściowe na etapie animowania i renderowania elementów wirtualnych wzbogacających oryginalny obraz. Aby uzyskać prawidłowe odwzorowanie perspektywy, proporcje, lokalizacje i rozmiary obiektów wirtualnych konieczne jest ustalenie wspólnego układu odniesienia

dla przestrzeni rzeczywistej, dla płaszczyzny kadru i dla trójwymiarowego środowiska wirtualnego. W tym celu wyznaczane są parametry przekształceń pomiędzy wszystkimi trzema przestrzeniami. Wykorzystywany jest model projekcyjny [23], uwzględniający występowanie skrótu perspektywicznego, zgodny ze sposobem rejestrowania obrazu przez ludzkie oko i obiektyw kamery, tzn. rozmiary obiektów znajdujących się daleko są mniejsze [6]. Wyznaczana jest macierz przekształcenia (1):

$$T = \begin{bmatrix} A & D & G \\ B & E & H \\ C & F & I \end{bmatrix} \tag{1}$$

T pozwala ona na znajdowanie współrzędnych u, v w przestrzeni wirtualnej dla dowolnej pozycji piksela x, y w obrazie. W tym celu realizowane jest następujące przeliczenie (2)(3):

$$\mathrm{u} = \frac{\mathrm{u_p}}{\mathrm{w_p}} \tag{2}$$

$$\mathrm{v} = \frac{\mathrm{v_p}}{\mathrm{w_p}} \tag{3}$$

gdzie, dla danych współrzędnych x, y zachodzi:

$$\begin{gathered} [\mathrm{u_p} \quad \mathrm{v_p} \quad \mathrm{w_p}] = [\mathrm{x} \quad \mathrm{y} \quad 1] \cdot \mathrm{T} \\ \mathrm{u_p} = \mathrm{Ax} + \mathrm{By} + \mathrm{C} \\ \mathrm{v_p} = \mathrm{Dx} + \mathrm{Ey} + \mathrm{F} \\ \mathrm{w_p} = \mathrm{Gx} + \mathrm{Hy} + \mathrm{I} \end{gathered} \tag{4}$$

I ostatecznie uzyskiwane są współrzędne dla środowiska wirtualnego:

$$\mathrm{u} = \frac{\mathrm{Ax+By+C}}{\mathrm{Gx+Hy+I}} \quad \text{oraz} \quad \mathrm{v} = \frac{\mathrm{Dx+Ey+F}}{\mathrm{Gx+Hy+I}} \tag{5}$$

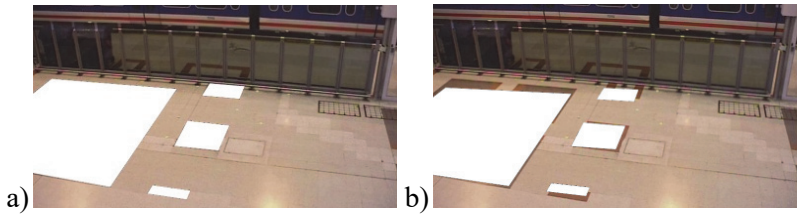
W celu określenia nieznanych współczynników transformacji T, konieczne jest dostarczenie co najmniej 4 próbek: par punktów o znanych koordynatach w obu przestrzeniach, tzn. u, v w metrach w rzeczywistej lokalizacji i odpowiadających im współrzędnych x, y pikseli. Gdy macierz T zostanie wyznaczona, obliczana jest macierz odwrotna, pozwalająca na transformację przestrzeni w drugą stronę.

Dla lokalizacji rozważanej w opisywanych badaniach dostępne jest 8 par punktów (rys. 2c). Każda zmiana parametrów kamery (położenie, zoom, orientacja), wpływa na współczynniki transformacji i wymaga powtórzenia obliczeń (1)–(5).

Rys. 2. Kard z sekwencji testowej i transformacja przestrzeni: a) obraz oryginalny, b) obraz po transformacji z metrów na piksele (każde 72 piksele w pionie i poziomie odpowiadają 1 metrowi na płaszczyźnie podłogi), c) współrzędne punktów odniesienia

W celu prawidłowego wyświetlania obiektów trójwymiarowych dokonać należy kalibracji kamery wirtualnej. Parametry zniekształceń obrazu, ogniskowa, orientacja oraz wysokość zamontowania kamery rzeczywistej, użytej w nagraniu i wirtualnej muszą być zgodne. W ogólności konieczne jest estymowanie warunków rejestracji i w tym celu wykorzystuje się powszechnie metodę kalibracji Tsai [39]. Po skonfigurowaniu kamery wirtualnej w sposób zbieżny z rzeczywistą otrzymywane są wirtualne obrazy o identycznej perspektywie, skalowaniu obiektów i tym samym układzie odniesienia.

Potwierdzenie prawidłowej kalibracji uzyskuje się poprzez generowanie obiektów 3D korespondujących z rzeczywistymi elementami obserwowanej sceny, np. filarami, drzwiami (rys. 3).



Rys. 3. Odtworzenie rzeczywistych elementów w środowisku wirtualnym: a) wynik dla prawidłowej kalibracji, b) wynik dla nieprawidłowej kalibracji

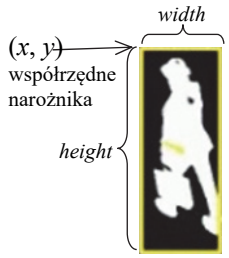
Parametry obwiedni obiektu

Początkowe etapy analizy obrazu, tj. wykrywanie obiektów, generowanie obwiedni, filtracja jej parametrów, śledzenie i transformacja współrzędnych do docelowego układu odniesienia dają w rezultacie zestaw parametrów (rys. 4):

- identyfikator obiektu (nadawany automatycznie);
- numer obecnej klatki wideo;
- współrzędne w pikselach górnego lewego narożnika obwiedni (x,y);

– rozmiar obwiedni *width* i *height*.

Na potrzeby kolejnych etapów przetwarzania parametry zapisywane są w składni XML (ang. *Extensible Markup Language*), wzorowanej na powszechnym formacie zapisu danych referencyjnych dla algorytmów widzenia komputerowego ViperGT [40].



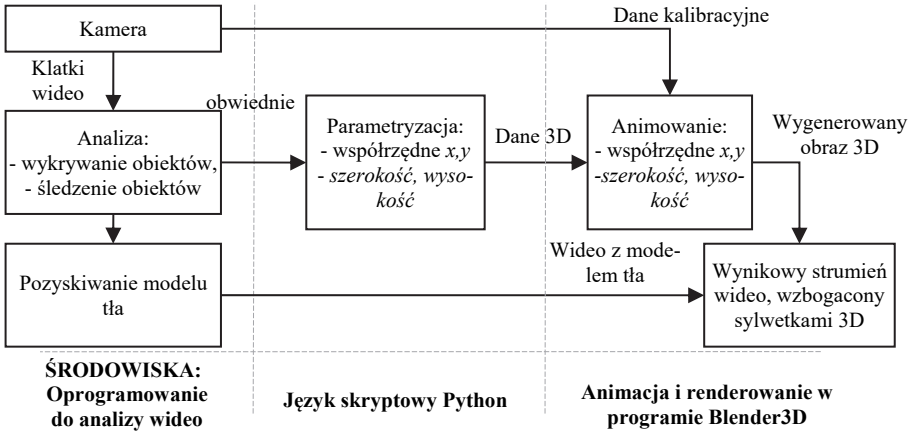

```
<object framespan="12:180" id="1" name="Person">
 <attribute name="Name">
  <data:svalue value="P_1"/>
 </attribute>
 <attribute name="Location">
  <data:bbox framespan="1:1" height="49" width="90" x="547" y="523"/>
  [...]
  <data:bbox framespan="10:10" height="55" width="95" x="554" y="548"/>
 </attribute>
</object>
```

Rys. 4. Graficzna reprezentacja parametrów obwiedni i format ich zapisu

NOWA METODA ANONIMIZACJI – WIZUALNA PARAFRAZA

Tworzenie wizualnej parafrazy, zastępnika dla danych identyfikujących osobę, odbywa się poprzez wytwarzanie wirtualnego obrazu sylwetek poruszających się po monitorowanym obszarze. Postacie te umieszczane są w miejscach odpowiadających pozycjom rzeczywistych osób i animowane w sposób naśladujący podstawowe czynności. W ten sposób uzyskiwany jest materiał wideo pozbawiony cech osobowych, dający operatorowi świadomość sytuacji i pozwalający na realizację podstawowych celów monitoringu.

Wejściowy strumień wideo analizowany jest w czasie rzeczywistym w celu detekcji, lokalizowania i śledzenia osób w obrazie i opis najważniejszych cech: pozycji, zajmowanego obszaru, orientacji w kadrze, prędkości i kierunku ruchu. Następnie uwzględniane jest pole widzenia kamery i jej orientacja oraz przekształcenie między przestrzeniami kadru, środowiska 3D i rzeczywistymi wymiarami, czego efektem jest oszacowanie minimalnego i maksymalnego dopuszczalnego rozmiaru obiektów 3D i ograniczeń prędkości poruszania się. W wyniku tego postępowania generowane są wirtualne postacie nakładane na rzeczywisty obraz (rys. 5).



Rys. 5. Schemat blokowy przetwarzania danych: bloki funkcjonale, przepływ danych oraz wykorzystywane środowiska

Analiza wideo wykonywana w pierwszym etapie wykorzystuje oprogramowanie wykonane w Politechnice Gdańskiej, które oferuje funkcje detekcji i śledzenia obiektów w obrazie. Opis algorytmów wykracza poza zakres tematyki rozdziału, a wyczerpująco dokumentują je liczne publikacje [8][10][20][36]. Materiałem badawczym były nagrania PETS [28], prezentujące typową aktywność osób w holu dworca. Wynikiem są obwiednie prostokątne obiektów i maski binarne dokładnie wskazujące piksele należące do wykrytych obiektów.

Parametry obwiedni (rozmiar, położenie i zmiany w czasie), wykorzystywane są do sterowania animacjami awatarów. Wzrost wirtualnej postaci wynika z wysokości obwiedni, jej położenie zgodne jest z lokalizacją obwiedni, orientacja i prędkość poruszania określane są na podstawie wektora przemieszczenia obwiedni. Z prędkości przeliczonej na jednostki [m/s] wyznacza się rodzaj ruchu, to czy osoba stoi, idzie, czy biegnie [27][41]. Typ ruchu wpływa na prędkość przemieszczania awatara oraz sposób animacji jego kończyn.

Na potrzeby realizacji opisywanej aplikacji przyjęte zostały następujące założenia:

- ruch odbywa się po powierzchni podłoża – dolna krawędź obwiedni leży na podłodze, czyli jej współrzędna z wynosi 0 [m] w przestrzeni 3D;
- podłoże jest płaskie, opisane płaszczyzną z=0;
- kamera jest skalibrowana, jej parametry są znane i zostały wykorzystane do konfiguracji kamery wirtualnej, generującej obrazy awatarów.

W oprogramowaniu do animacji i tworzenia grafiki Blender3D [26] możliwe jest stosowanie skryptów automatyzujących wykonywanie zadania, pisanych w języku Python [1]. W ten sposób na podstawie danych wejściowych tworzone są automatycznie odpowiednie obiekty trójwymiarowe: kamera, podłoże i jednorodne, bezkierunkowe źródło białego światła. Aby umożliwić poprawne pozycjonowanie awatarów w obrazie z kamery, przyjmowany jest układ odniesienia zgodny z rzeczywistym, ustalonym na etapie kalibracji kamery. Jak wspomniano wcześniej, możliwe jest przeliczanie współrzędnych pomiędzy tymi układem wirtualnym, rzeczywistym i pozycjami pikseli w obrazie [33].

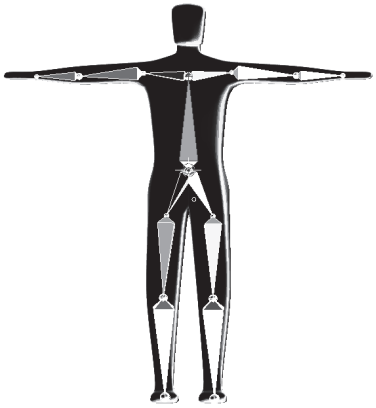
Animacja wirtualnej postaci

Każda osoba przemieszczająca się w polu widzenia kamery zastępowana jest awatarem, animowanym automatycznie poprzez uwzględnianie ruchu obwiedni wykrytej osoby:

- zmiany położenia w scenie 3D w oparciu o współrzędne obwiedni x, y;
- zmiany orientacji sylwetki względem kamery, obrót modelu 3D wokół osi pionowej;
- zmiany układu kończyn ciała, cykliczny ruch symbolizujący czynności stania, chodu i biegu.

Dwie pierwsze operacje na modelu 3D nazywane są globalnymi i wymagają operowania na tzw. głównej kości modelu (rys. 6), ostatnia, lokalna modyfikacja czynności działa na zasadzie nadawania kościom modelu odpowiednich orientacji. Zmiany orientacji kończyn w czasie dostosowywane są do aktualnej estymowanej prędkości ruchu rzeczywistej osoby.

Użyty awatar to postać humanoidalna, bez cech osobowych i rysów twarzy (rys. 6). Szkielet, składający się z hierarchicznie połączonych kości, wykonany został zgodnie ze standardem BVH popularnym w technice rejestracji ruchu (ang. *motion capture*) [5], co ułatwia rozbudowę zestawu wykonywanych akcji. Dopuszczalne obroty kości ograniczone zostały do zakresów biomechanicznie poprawnych dla ludzkiego ciała (np. łokieć może mieć kąt zgięcia od 0 do 180 stopni). Wizualizacja postaci za pomocą prostego awatara ma na celu nie rozróżnianie osób, tylko dostarczanie anonimowego obrazu z kamery monitoringu, dającego orientacyjne informacje o liczbie osób, ich lokalizacji i tempie poruszania.



Rys. 6. Model awatara 3D z widocznymi kośćmi

Przetwarzanie parametrów ruchu

Szacowanie rzeczywistych rozmiarów obiektu nie jest zadaniem trywialnym, gdyż zwykle w początkowej fazie widoczności tylko część wizerunku osoby znajduje się w kadrze. Wówczas wzrost szacowany jest jako średni, ok. 160cm i w trakcie obserwacji poruszającej się osoby i generowania kolejnych klatek jest korygowany, aż do pełnej widoczności i zgodności ze wzrostem osoby.

Parametry obwiedni obiektu wykorzystywane są do określania prędkości (6), kierunku ruchu (7) oraz położenia animowanego awatara (7).

$$\begin{aligned} V_x(t) &= \big(x(t) - x(t-1)\big) \\ V_y(t) &= \big(y(t) - y(t-1)\big) \\ V(t) &= \sqrt{V_x^2(t) + V_y^2(t)} \end{aligned} \tag{6}$$

$$\theta(t) = \begin{cases} \operatorname{acos}\left(\frac{V_x(t)}{V(t)}\right) \cdot \frac{180}{\pi} \cdot \operatorname{sign}\left(V_y(t)\right) & \text{dla } V_y(t) \neq 0 \\ 0 & \text{dla } V_y(t) = 0 \ \text{ i } \ V_x(t) \geq 0 \\ 180 & \text{dla } V_y(t) = 0 \ \text{ i } \ V_x(t) < 0 \end{cases} \tag{7}$$

$$\begin{aligned} x_{loc}(t) &= x(t) + \frac{\text{width}}{2} \\ y_{loc}(t) &= y(t) + \text{height} \end{aligned} \tag{8}$$

W wykorzystywanym środowisku animacji Blender3D istnieje możliwość użycia poleceń języka Python do automatycznej kontroli animacją, poło-

żeniem, prędkością i wyglądem obiektów [1]. W tym celu odpowiedni skrypt odczytuje wyznaczone wartości V, x, y, *height*, θ i odpowiednio pozycjonuje główną kość szkieletu postaci: lokalna oś OX kości orientowana jest w kierunku azymutu θ, umieszczana we współrzędnych (x, y) i z=0 (na podłożu), skalowana do rozmiaru *height*, co wpływa na rozmiary i położenia wszystkich kości szkieletu i na wygląd siatki 3D opisującej obiekt.

Uzyskana w powyższy sposób trójwymiarowa scena jest renderowana – generowany jest obraz z wirtualnej, skalibrowanej kamery, zgodny z perspektywą rzeczywistej sceny. Wynik nakładany jest na obraz modelowanego tła, pozbawionego obiektów pierwszoplanowych. W przypadku ciągłych zmian tła, stosowany statystyczny opis kolorów pikseli generuje adekwatnie zmienne tło. Wobec powyższego wynikowy model zgodny jest z aktualnym obrazem sceny dla każdej kolejnej klatki strumienia wideo.

WNIOSKI

W rozdziale opisano metodę analizy obrazu z kamery i tworzenia wizualnej parafrazy – animowanych awatarów naśladujących zachowanie osób obecnych w kadrze. Uzyskiwane nagania poddane zostały ocenie subiektywnej [17], badającej zrozumiałość prezentowanego przekazu pod kątem rozpoznawania liczby osób i ich zachowania przez operatora. Świadomość sytuacyjna operatora nie jest ograniczona w trakcie prezentacji tak zmodyfikowanego strumienia wideo. Jednakże w obrazie pomijane są obiekty dodatkowe, np. niesione torby, plecaki, bagaże na kółkach czy wózki, dlatego dokładne znaczenie sceny nie może być w pełni odtworzone z anonimowego obrazu.

Przyszłe prace dedykowane będą rozwiązaniu problemu wspomnianych obiektów, poprzez zastępowanie ich ogólnym prostopadłościennym modelem o wymiarach i orientacji zgodnej z wykrywanym obiektem.

Prezentowana metoda może być połączona z algorytmem automatycznego wykrywania zdarzeń: naruszenia obszaru chronionego, ruchu pod prąd, a także krzyku i wzywania pomocy [3][21][24][32]. W tych przypadkach uczestnik zdarzenia może być symbolizowany awatarem wyróżnionym wizualnie (np. migającym, obwiedzionym czytelnym znacznikiem).

W potencjalnych praktycznych zastosowaniach zakłada się, że oryginał nagrania jest dostępny w formie zaszyfrowanej, wymagającej autoryzacji użytkownika z odpowiednimi uprawnieniami a wersja anonimowa służy wyłącznie do prezentacji operatorowi na żywo.

Opracowana metoda może mieć zastosowanie w anonimizacji strumieni z monitoringu, w przygotowywaniu nagrań wideo do prezentacji w mediach i innych formach publikacji obrazu, w których tożsamość prezentowanych osób nie jest istotna.

P o d z i ę k o w a n i a

Prace zostały sfinansowane przez ARTEMIS Joint Undertaking i Narodowe Centrum Badań i Rozwoju w ramach projektu badawczego COPCAMS (http://copcams.eu), umowa nr 332913.

BIBLIOGRAFIA

[1] Anders MJ., *Blender 2.49 Scripting*, Packt Publishing, 2010.

[2] Atrey PK., El Saddik A., Kankanhalli MS., *Effective multimedia surveillance using a human-centric approach*. Multimedia Tools and Applications, Vol. 51, Issue 2, Springer, 2011, 697-721.

[3] Ballan L., Bertini M., Del Bimbo A., Seidenari L., Serra G., *Event detection and recognition for semantic annotation of video*. Multimedia Tools and Applications, Vol. 51, Issue 1, Springer, 2011, 279-302.

[4] Bratt B., *Rotoscoping*. Focal Press, 2012.

[5] *Biovision Hierarchy*, http://en.wikipedia.org/wiki/Biovision_Hierarchy

[6] Cederberg JN., *Projective Geometry*. A Course in Modern Geometries, Undergraduate Texts in Mathematics, Springer, 2001, 213-313.

[7] Cichowski, J.; Czyzewski, A. *Reversible video stream anonymization for video surveillance systems based on pixels relocation and watermarking*. Computer Vision Workshops (ICCV Workshops), 2011 IEEE International Conference, 2011, 1971-1977.

[8] Czyżewski A., Szwoch G., Dalka P., Szczuko P., Ciarkowski A., Ellwart D., Merta T., Łopatka K., Kulasek Ł., Wolski J., *Multi-stage video analysis framework*, [w:], *Video Surveillance, Chapter 9*, red. Weiyao Lin, Intech, 2011, 145-171.

[9] Dalka P*., Detection and Segmentation of Moving Vehicles and Trains Using Gaussian Mixtures, Shadow Detection and Morphological Processing*, Machine Graphics and Vision, Vol. 15, No. 3/4, 2006, 339 – 348.

[10] Dalka P., Szwoch G., Szczuko P., Czyżewski A., *Video Content Analysis in the Urban Area Telemonitoring System*, [w:] *Multimedia Services in Intelligent Environments,* red. G.A. Tsihrintzis, Springer-Verlag Berlin Heidelberg, 2010, 241-261.

[11] Deutscher, J., Blake, A., Reid, I.D.: *Articulated body motion capture by annealed particle filtering*. In: Proc. IEEE Conf. on Computer Vision and Pattern Recognition, 2000, 126–133.

[12] Gao T., Li G., Lian S., Zhang J., *Tracking video objects with feature points based particle filtering*. Multimedia Tools and Applications, Volume 58, Issue 1, Springer, 2012, 1-21.

[13] Ghazal M., Vázquez C., Amer A., *Real-time vandalism detection by monitoring object activities*. Multimedia Tools and Applications, Vol. 58, Issue 3, Springer, 2012, 585-611

[14] Goffredo M., Bouchrika I., Carter JN., Nixon MS., *Performance analysis for automated gait extraction and recognition in multi-camera surveillance*. Multimedia Tools and Applications, Vol. 50, Issue 1, Springer, 2010, 75-94.

[15] Guo C., Liu D., Guo Y., Sun Y., *An adaptive graph cut algorithm for video moving objects detection*. Multimedia Tools and Applications, Volume 72, Issue 3, Springer, 2014, 2633-2652.

[16] Höferlin B., Höferlin M., Weiskopf D., Heidemann G., *Information-based adaptive fast-forward for visual surveillance*. Multimedia Tools and Applications, Vol. 55, Issue 1, Springer, 2011, 127-150.

[17] *ITU-T recommendation* P.800: Methods for subjective determination of transmission quality (http://www.itu.int/rec/T-REC-P.800-199608-I/en), 1996.

[18] Kakadiaris, I., Metaxas, D.: *Model-based estimation of 3D human motion*. IEEE Tran. Pattern Analysis and Machine Intelligence, Vol. 22, No. 12, 2000, 1453–1459.

[19] Kehl, R., Van Gool, L.: *Markerless tracking of complex human motions from multiple views*. Computer Vision and Image Understanding Vol. 104, No. 2-3, 2006, 190–209.

[20] Kotus J., Dalka P., Szczodrak M., Szwoch G., Szczuko P., Czyżewski A., *Multimodal Surveillance Based Personal Protection System*. Signal Processing: Algorithms, Architectures, Arrangements, and Applications (SPA), Poznan, 2013, 100-105.

[21] Kotus J., Łopatka K., Czyżewski A., *Detection and localization of selected acoustic events in acoustic field for smart surveillance applications*. Multimedia Tools and Applications, Vol. 68, Issue 1, Springer, 2014, 5-21.

[22] Krolewski J., Gawrysiak P., *The Mobile Personal Augmented Reality Navigation System*. Man-Machine Interactions Vol. 2, Springer, 2011.

[23] Laveau S., Faugeras O., *Oriented projective geometry for computer vision*. Computer Vision ECCV, Lecture Notes in Computer Science Vol. 1064, Springer, 1996, 147-156.

[24] Lavee G., Khan L., Thuraisingham B., *A framework for a video analysis tool for suspicious event detection*. Multimedia Tools and Applications, Vol. 35, Issue 1, Springer, 2007, 109-123.

[25] Moshkovitz M., *The Virtual Studio: Technology and Techniques*. Focal Press, 2000.

[26] Mullen T., *Mastering Blender*, Sybex, 2012.

[27] Novaes RD., Dourado VZ. *Usual gait speed assessment in middle-aged and elderly Brazilian subjects*. Brazilian Journal of Physical Therapy, Vol.15, No 2, 2011, 117-122. doi: http://dx.doi.org/10.1590/S1413-35552011000200006

[28] *PETS 2006 Benchmark Data*, IEEE Conference on Computer Vision and Pattern Recognition, www.cvg.rdg.ac.uk/PETS2006/data.html, 2006.

[29] Rumiński D., Walczak K., *Creation of Interactive AR Content on Mobile Devices*. Business Information Systems Workshops, Springer, 2013.

[30] Samangooei S., Nixon MS., *Performing content-based retrieval of humans using gait biometrics*. Multimedia Tools and Applications, Volume 49, Issue 1, Springer, 2010, 195-212.

[31] Schreer O., Kauff P., Sikora T., 3D *Videocommunication: Algorithms, concepts and real-time systems in human centred communication*. Wiley, 2005.

[32] Simon C., Meessen J., De Vleeschouwer Ch., *Visual event recognition using decision trees*. Multimedia Tools and Applications, Vol. 50, Issue 1, Springer, 2010, 95-121.

[33] Szwoch G., Dalka P., Czyżewski A., *Spatial Calibration of a Dual PTZ-Fixed Camera System for Tracking Moving Objects in Video*. Journal of Imaging Science and Technology (JIST), Vol. 57, No. 2, 2013, 1-10.

[34] Szczuko P., *Hierarchical Estimation of Human Upper Body Based on 2D Observation Utilizing Evolutionary Programming and "Genetic Memory"*. Multimedia Communications, Services and Security, Communications in Computer and Information Science, Vol. 149, Springer, 2011, 82-90.

[35] Szczuko P., *Genetic programming extension to APF-based monocular human body pose estimation*. Multimedia Tools and Applications, Vol. 68, Springer, 2014, 177-192.

[36] Szwoch G., Dalka P., Ciarkowski A., Szczuko P., Czyzewski A., *Visual Object Tracking System Employing Fixed and PTZ Cameras*. Journal of Intelligent Decision Technologies, Vol. 5, No. 2, 2011, 177 – 188. http://iospress.metapress.com/content/m5060n24tk125406/?p=2aa903da834b4371955e56c56b058b6b&pi=5

[37] Szwoch G., Dalka P., *Layered background modeling for automatic detection of unattended objects in camera images*. WIAMIS 2011: 12th International Workshop on Image Analysis for Multimedia Interactive Services, Pre-print No. 50, Delft 2011.

[38] Tavli B., Bicakci K., Zilan R., Barcelo-Ordinas JM., *A survey of visual sensor network platforms*. Multimedia Tools and Applications, Vol. 60, Issue 3, Springer, 2012, 689-726.

[39] Tsai RY, *A versatile camera calibration technique for high-accuracy 3D machine vision metrology using off-the-shelf TV cameras and lenses*. IEEE Journal of Robotics and Automation, Vol. 3 No. 4, 1987, 323–344.

[40] University of Maryland, *Guide to Authoring Media Ground Truth with Vi-PER-GT*, http://viper-toolkit.sourceforge.net/docs/gt/

[41] Uustal H., Baerga E., Gait Analysis, [w:] *Physical Medicine and Rehabilitation Board Review*, red. S Cuccurullo, Demos Medical Publishing, New York, 2004. http://www.ncbi.nlm.nih.gov/books/NBK27235/

[42] *Wikitude, augmented reality platform*, http://www.wikitude.com/

VISUAL MONITORING AND PRIVACY PROTECTION – NEW METHOD FOR ANONYMIZATION

ABSTRACT

The chapter describes and addresses personal privacy concerns related to widespread application of visual surveillance. Monitoring systems are supervised by operators, thus the human factor must not be neglected – privacy of persons recorded by numerous cameras should be protected against eavesdropping and uninformed publications in media. Typically a digital camera allows to obscure parts of the frame, by creating so called privacy mask, but it is efficient only for

static elements of the scene and does not protect persons moving through the observed area and public spaces. Therefore a concept of anonymization and pseudonymization of images is proposed, based on creating visual paraphrase of the original image of the person, replacing the whole silhouette. A 3D technology of augmented reality and avatars are applied. Such a virtual figure is animated to follow the location of a real person and mimic the type of ones movement. In the chapter a method of video analysis, motion parameterization, and generation of virtual figures is presented. The result video stream provides the operator with general situational awareness, and allows to perform monitoring goals. This method can be used in visual surveillance and for fast preparation of materials to be published in media without violating the privacy of bystanders, or in any other forms of image presentations, where the identity of people should be protected.

Marek ZACHARA
AGH University of Science and Technology

IDENTYFIKACJA NIETYPOWYCH ZAPYTAŃ DO SERWISÓW WWW

STRESZCZENIE

Niniejszy artykuł prezentuje nowe metody ochrony serwisów internetowych, oparte na identyfikacji typowych i nietypowych wzorców zachowań ich użytkowników. W szczególności przedstawiona została metoda modelowania tych zachowań za pomocą grafu, a także współpraca grupy serwerów w celu dzielenia się informacjami i zbiorowej detekcji niebezpiecznych zapytań. Artykuł zawiera też opis skonstruowanego prototypu systemu, implementującego opisane metody, oraz wnioski z analizy jego funkcjonowania.

Słowa kluczowe:
aplikacje www, ataki, detekcja anomalii

WSTĘP

Coraz większa część aktywności ludzi przenosi się do internetu. Obejmuje to zarówno sprawy prywatne, biznesowe, jak i urzędowe (np. polska platforma ePUAP). Można bezpiecznie założyć, że będziemy obserwować dalszy wzrost udziału komunikacji internetowej w zakresie obsługi spraw oficjalnych i urzędowych, choćby ze względu na fakt powołania pod koniec 2011 w Polsce ministerstwa Administracji i Cyfryzacji. Unia Europejska również określa informatyzację i dostęp do internetów jako jeden ze swoich priorytetów, wyznaczając komisarza ds. wspólnego cyfrowego rynku (ang. Digital Single Market) w randze wiceprezydenta.

Niestety, wraz ze wzrostem ilości treści i możliwości usług internetowych rośnie też ich atrakcyjność dla (potencjalnych) przestępców, natomiast świadomość zagrożeń i wiedza na temat bezpieczeństwa wśród twórców i administratorów tych serwisów często nie nadąża za potrzebami. Dla potwierdzenia tego faktu poniżej przedstawione zostało krótkie streszczenie kilku adekwatnych raportów.

Skala zagrożeń

Trudno jest dokładnie zdiagnozować ogólny stopień bezpieczeństwa sieci. Pewny pogląd dają jednak raporty przygotowywane przez firmy zajmujące się profesjonalnie tym tematem. I tak, iVIZ w swoim raporcie z 2013 r. [4] podaje, że 99% z ok. 300 testowanych serwisów ich klientów posiadało przynajmniej jedną podatność na atak, przy średnio 35 takich podatnościach w serwisie. 82% z tych podatności to były błędy krytyczne.

WhiteHat podaje nieco mniejszą wartość - ok. 86% testowanych serwisów posiadało przynajmniej jedną poważną podatność przy średnio 56 odkrytych podatnościach w każdym serwisie [10]. Symantec, w raporcie „Internet Security Threat Report" z 2013 [9] podaje jeszcze mniejszą (choć w dalszym ciągu znaczną) liczbę - 53% serwisów zawierających podatności na ataki, przy czym w tym przypadku można domniemywać, że było to mniej szczegółowe badanie (automatyczne, średnio ok. 1400 serwisów dziennie). Więcej szczegółów na temat form ataków i rodzajów podatności można znaleźć w [5].

Biorąc powyższe dane pod uwagę, można bezpiecznie ocenić, że zdecydowana większość serwisów internetowych (poza nielicznymi wyjątkami) zawiera istotne błędy pozwalające atakującym na wykorzystanie ich podatności.

Podsumowanie ryzyka

Jak widać, bezpieczeństwo serwisów internetowych pozostawia wiele do życzenia. Biorąc pod uwagę potencjalne skutki ataków (np. przejęcie konta użytkownika, wykonanie nieautoryzowanych transakcji, kradzież tożsamości itp.), a także możliwość konstruowania ataków na inne elementy wewnętrznej sieci, widać, że jest to istotny problem społeczno-techniczny. Opracowanie i wprowadzenie metod redukujących to ryzyko jest więc istotnym zagadnieniem rozwojowym. W niniejszym artykule opisane zostały nowe, opracowane metody ochrony serwisów internetowych poprzez identyfikację nietypowych (potencjalnie groźnych) zapytań

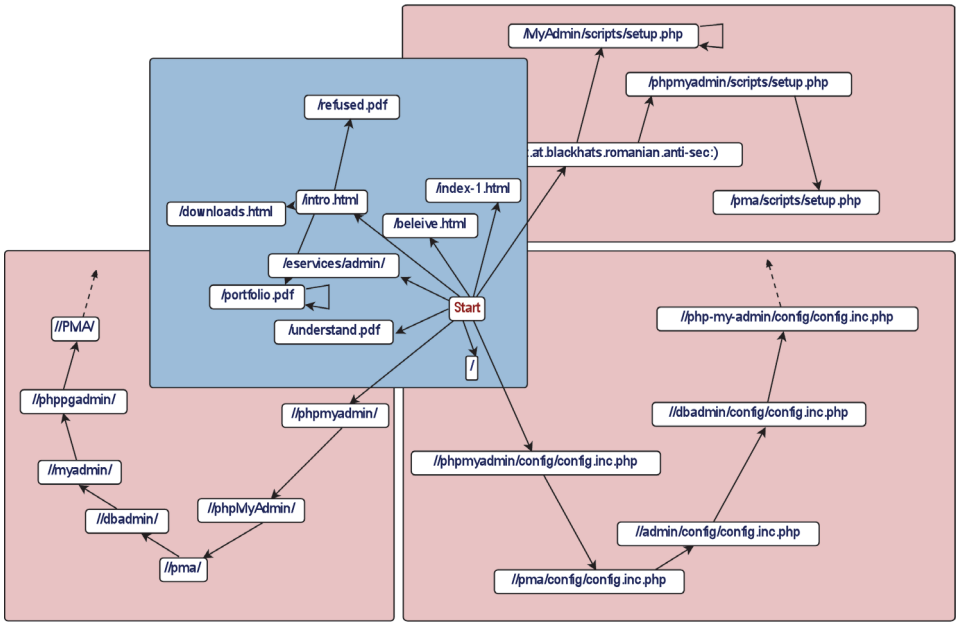
METODY OCHRONY

Proponowana metoda ochrony serwisów internetowych polega na monitorowaniu zapytań (ang. *request*) przychodzących od danego użytkownika, a następnie tworzeniu modelu zachowań dla całej grupy użytkowników. Dzięki temu możliwe jest wyodrębnienie pozytywnych wzorców zachowań, wynikających z zachowań większości użytkowników serwisu, a na tej podstawie identyfikacja zachowań nietypowych – potencjalnie

groźnych. Poniżej przedstawione zostaną dwie (częściowo niezależne) metody. Jedna oparta na opisanej metodzie pozytywnych wzorców zachowań użytkowników jednego serwisu oraz druga, wykorzystująca kolektywną wiedzę grupy serwisów internetowych. Obie te metody należą do technik wykrywania anomalii, wykorzystywanych już do wcześniej do celu identyfikacji ataków [1], [7], [8].

Identyfikacja nietypowych zachowań

Poniższy rysunek nr 1 ilustruje przykładowe (autentyczne) sekwencje zapytań użytkowników przychodzące do monitorowanego serwera. Na niebieskim tle przedstawione zostały sekwencje zapytań od „uczciwych" użytkowników, pozostałe ilustrują zaś próby ataku.



Rys. 1. Przykładowe sekwencje zapytań

Rysunek ten ilustruje też sposób reprezentacji zachowań użytkowników, polegający na użyciu do tego zadania skierowanego grafu G, w którym węzły V odpowiadają kolejnym zapytaniom, natomiast krawędzie E oznaczają ich sekwencje.

$$G = (V, E_w) \tag{1}$$

W opracowanej metodzie użyty został graf skierowany ważony - każde przejście pomiędzy stronami zwiększa o jeden wagę danej krawędzi.

W rezultacie po *t* cyklach, suma wag *k* wynosi:

$$k = t(r_a - r_r) \tag{2}$$

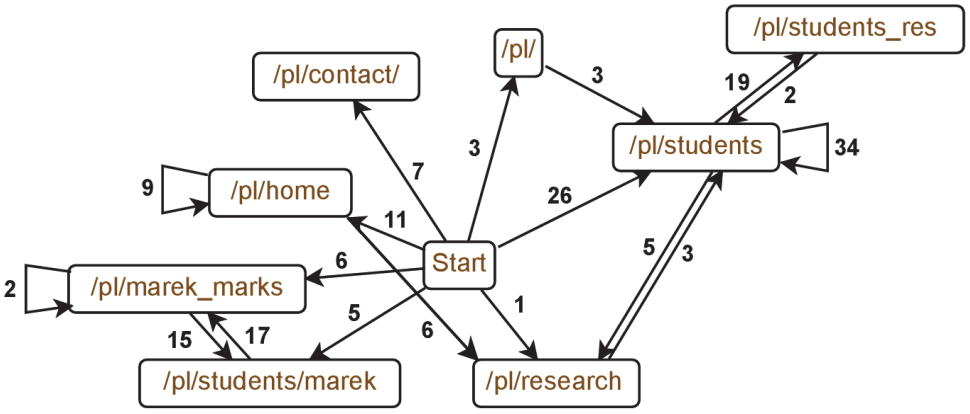
Gdzie r_a i r_r to odpowiednio ilość dodawanych i usuwanych wag w jednostce czasu. Ponieważ nie da się przewidzieć dokładnie, ile będzie wynosiła wartość r_a, nie należy ustalać stałej wartości usuwania wag z grafu. W opracowanej metodzie przyjęto, że w każdym cyklu (jednostce czasu) usuwany jest pewien procent p krawędzi. W związku z tym ilość wag po n cyklach jest określona wzorem:

$$k_n = (1-p)(k_{n-1} + r_a * t) \tag{3}$$

Który można rozwinąć, przyjmując r_t jako średnią ilość przychodzących zapytań:

$$k_n = ((1-p)^n + \ldots + (1-p)) * r_t \tag{4}$$

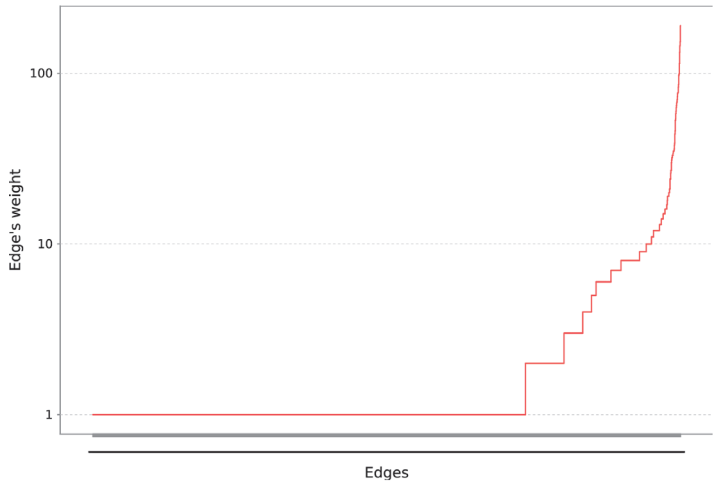
Która to wartość jest zawsze zbieżna dla 0 < p < 1. Otrzymujemy zatem stabilny układ, w którym waga danej krawędzi odpowiada względnej częstotliwości danego przejścia (w stosunku do sumy wag krawędzi wychodzących z danego węzła). Przykład takiego grafu, dla serwisu internetowego autora artykułu został przedstawiony na rysunku 2.



Rys. 2. Przykład modelu zachowań reprezentowanego przez graf ważony

Analizując każde nowe przychodzące zapytanie w kontekście zbudowanego grafu możliwa jest identyfikacja zapytań „podejrzanych", które nie są zgodne z typowymi zachowaniami. Zapytania takie będą bowiem relatywnie rzadkie (poniżej 1%) dla normalnego serwisu obsługującego setki

użytkowników. Rysunek 3 przedstawia przykładowy rozkład wag dla niedużego serwisu B2B. Jak można zauważyć, jest istotna różnica pomiędzy dużą grupą zapytań „pojedynczych", niepowtarzających się w trakcie badania, oraz grupą typowych, powtarzających się dziesiątki czy setki razy.



Rys. 3. Rozkład wag grafu dla przykładowego serwisu. Na osi poziomej znajdują się kolejne wagi krawędzi grafu, posortowane według wartości

Wspólna weryfikacja zagrożeń

Poza lokalnym modelowaniem i identyfikacją nietypowych zapytań, możliwe jest również wykorzystanie rozproszonej wiedzy wielu serwerów w celu poprawy skuteczności i jakości detekcji (a przede wszystkim redukcji tzw. '*false positives*'). Opracowana metoda opiera się na fakcie dużej powtarzalności wzorców ataku, co wynika z tego, iż znaczna ich część jest prowadzona albo przez tzw. *'script kiddies*' – czyli młodzież ściągającą gotowe narzędzia z Internetu [6], bądź też przez malware. Tezę tą wspiera m.in. wspomniany wcześniej raport Symantec, w którym napisano że tylko w jednym miesiącu (05.2012) malware o nazwie LizaMoon był odpowiedzialny za ponad milion zakończonych sukcesem ataków typu *SQL Injection*.

Bazując na tych założeniach opracowany został sposób wymiany informacji pomiędzy serwerami pozwalający na identyfikację powtarzających się wzorców zapytań przychodzących do różnych serwerów – dzięki czemu możliwe jest istotne zwiększenie pewności poprawnej identyfikacji. Każdy z serwerów prowadzi ocenę na bazie własnego modelu zachowań, uwzględniając dodatkowo raporty opublikowane przez inne serwery –

i publikując swoje wyniki (listę zapytań ocenionych jako podejrzane).

Ponieważ publikacja przez serwer treści zapytań (a nawet URL-i) nie jest możliwa ze względu na ryzyko ujawnienia poufnych informacji, wykorzystany został mechanizm generowania tzw. skrótów kryptograficznych (ang. *hash*). Porównując takie skróty opublikowane przez inne serwery ze skrótami wygenerowanymi lokalnie, serwer uzyskuje ew. potwierdzenie, że identyczne zapytanie zostało wysłane do innego serwera – i przez niego również ocenione jako podejrzane. Pozwala to praktycznie w 100% wyeliminować potencjalne fałszywe alarmy (choć kosztem spadku detekcji prawdziwych ataków).

Przykład takiej listy komunikatów publikowanych przez serwer znajduje się na listingu 1. Poza skrótami MD5, każdy komunikat może zawierać też informację o rodzaju raportu (T:M lub T:B – odpowiednio zapytanie o nieistniejący zasób lub zachowanie nietypowe) oraz czas incydentu (A:32 oznacza 32 godziny temu). Dane te nie są niezbędne, ale stanowić dodatkową informację dla algorytmów podejmowania decyzji w sprawie postępowania z analizowanym zapytaniem.

```
{ T:M, A:57, MD5:2cf1d3c7fe2eadb66fb2ba6ad5864326 }
{ T:M, A:53, MD5:2370f28edae0afcd8d3b8ce1d671a8ac }
{ T:M, A:32, MD5:2f42d9e09e724f40cdf28094d7beae0a }
{ T:B, A:31, MD5:8f86175acde590bf811541173125de71 }
{ T:M, A:24, MD5:eee5cd6e33d7d3deaf52cadeb590e642 }
{ T:B, A:17, MD5:bd9cdbfedca98427c80a41766f5a3783 }
```

Listing 1. Przykładowa lista komunikatów podejrzanych zapytań.

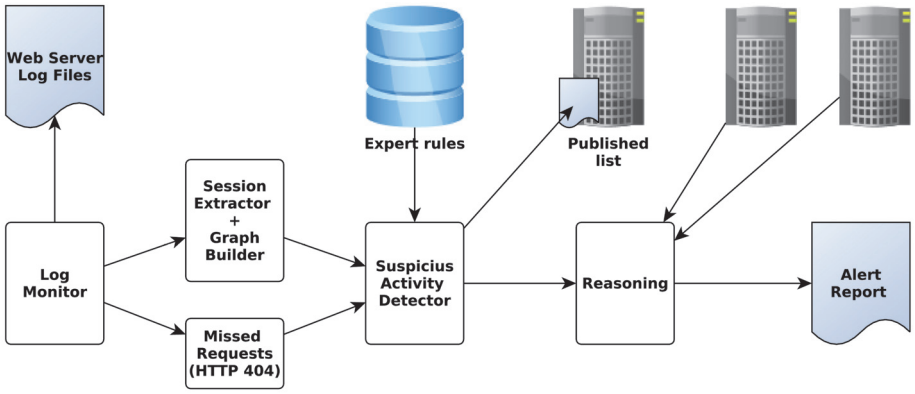
Sposoby podejmowania decyzji co do konkretnego zapytania na podstawie posiadanej wiedzy pozostają otwartym obszarem badawczym, rozwój ich uzależniony jest od wdrożenia opracowanych metod, co pozwoliłoby na zebranie odpowiedniego zbioru danych statystycznych. Podsumowując tą metodę, należy wspomnieć, że bazuje ona na kilku założeniach. Dotyczą one charakteru ataków, które można przy jej pomocy identyfikować. Są to w szczególności:

- zapytania nietypowe, wychodzące poza standardowe ścieżki (ang. *page flow*) użycia aplikacji;
- ataki powtarzalne – prowadzone przez automatyczne skrypty i/lub złośliwe oprogramowanie (ang. *malware*);
- ataki rozproszone, stosowane wobec grupy serwerów, bez konkretnego celu – mające na celu znalezienie takich, które posiadają podatności, które mogą być wykorzystane.

Należy też pamiętać, że praktycznie nie ma możliwości zagwarantowania 100% bezpieczeństwa żadnego systemu informatycznego – i odpowiednio zdeterminowana grupa (wyposażona w odpowiednie narzędzia) jest w stanie uzyskać dostęp praktycznie do każdego jednego systemu (patrz przykład StuxNet).

PROTOTYP

Na potrzeby weryfikacji opracowanych metod skonstruowany został prototyp systemu, wykonany w języku Java. Prototyp ten działa na zasadzie monitorowania logów serwera WWW (Apache), budowania odpowiednich modeli, analizy i raportowania. Schemat poglądowy modułów został przedstawiony na rysunku 4.



Rysunek 4. Schemat poglądowy prototypu systemu

Kolejne wpisy w dzienniku zdarzeń (log) web serwera są parsowane, a następnie tworzony jest graf modelu zachowań (opisany wcześniej). Przejścia pomiędzy stronami, które nie mają wsparcia w przygotowanym grafie (oraz wszystkie zapytania o nieistniejące strony – błąd 404) są przekazywane do modułu identyfikującego, który to moduł po uwzględnieniu grupy zdefiniowanych reguł (np. dotyczących ignorowania zapytań przez przeglądarkę o ikonę strony – '*favicon.ico*'). Przekazuje potencjalnie podejrzane zapytania do ostatniego modułu (Reasoning) oraz aktualizuje publikowaną listę *hash-y*.

Ostatni moduł ocenia stopień pewności co do zidentyfikowania podejrzanego zapytania, uwzględniając ew. zgłoszenie identycznych problemów przez inne współpracujące serwery i raportuje, w czasie rzeczywistym, zidentyfikowane zagrożenia.

Wstępne wyniki

Prototyp systemu został przebadany w testowym środowisku składającym się z trzech publicznych serwisów internetowych. Były „to relatywnie małe serwisy, otrzymujące poniżej 10 tys. zapytań miesięcznie. Prototyp systemu poprawnie zidentyfikował ponad 30% potencjalnie niebezpiecznych zapytań (co zostało obliczone w stosunku do „ręcznie" przeanalizowanych/oznaczonych zapytań). Należy podkreślić, że wynik ten został osiągnięty bez konieczności nauki/konfigurowania a'priori systemu, oraz bez jednego fałszywego alarmu (ang. *false positive*). Istotnym ograniczeniem wpływającym na wyniki było małe środowisko testowe – jedynie trzy serwery i mała liczba zapytań dziennych. Z pewnością zarówno zwiększenie liczby współpracujących serwisów jak i ruchu (ilości zapytań do serwisów) podniosłoby istotnie poziom detekcji.

PODSUMOWANIE

Opracowane metody i przygotowany prototyp systemu oferuje interesujące i unikalne cechy. W szczególności pozawala na identyfikację potencjalnie groźnych zapytań kierowanych do serwera – w czasie rzeczywistym i to bez konieczności specyficznej konfiguracji. Dużą ich zaletą jest brak konieczności wcześniejszego uczenia za pomocą zbioru pozytywnych wzorców [2], [7]. Pozwala to na uzyskanie dodatkowej warstwy ochrony aplikacji internetowych, przy minimalnych kosztach. Ponieważ nie ma możliwości zagwarantowania 100% bezpieczeństwa systemów informatycznych – szczególnie tych podłączonych do internetu - zadaniem administratorów jest więc generalnie podwyższanie poziomu ochrony tak, aby zatrzymać jak największą grupę potencjalnych 'włamywaczy'. Opisane metody wpisują się w koncepcję tzw. '*defense in depth'* [3].

Opisane metody dobrze wbudowują się w ten model postępowania. Oferują relatywnie duży wzrost ochrony systemu przy niewielkich kosztach i niewielkiej uciążliwości (są 'przeźroczyste' dla użytkowników a przy tym nie generują praktycznie fałszywych alarmów dla administratorów).

BIBLIOGRAFIA

[1] Auxilia, M., Tamilselvan, D., *Anomaly detection using negative security model in web application*. International Conference on Computer Information Systems and Industrial Management Applications (CISIM), 2010. pp. 481—486.

[2] Cova, M., Balzarotti, D., Felmetsger, V., Vigna, G., *Swaddler: An Approach for the Anomaly-Based Detection of State Violations in Web Applications. W Lecture Notes in Computer Science: Recent Advances in Intrusion Detection*, Kruegel, C., Lippmann, R., Clark, A. (eds.), Springer Berlin Heidelberg 2007. pp. 63--86.

[3] Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments. http://www.nsa.gov/ia/_files/support/defenseindepth.pdf

[4] iVIZ: *Web Application Vulnerability Statistics Report. (2013) http://www.securitybistro.com/?p=4966*

[5] Johari, R., Sharma, P., *A Survey on Web Application Vulnerabilities (SQLIA, XSS) Exploitation and Security Engine for SQL Injection*, International Conference on Communication Systems and Network Technologies (CSNT), 2012. pp. 453—458.

[6] Kayne, R.: *What Are Script Kiddies*. http://www.wisegeek.com/what-are-script-kiddies.htm

[7] Kruegel, C., Vigna, G., *Anomaly Detection of Web-Based Attacks*. ACM Press 2003.

[8] Kruegel, C., Vigna, G., Robertson, *A multi-model approach to the detection of web-based attacks*. „Computer Networks" 2005, 48(5), pp. 717—738.

[9] Symantec: *Internet Security Threat Report*. (2013) http://www.symantec.com/security_response/publications/threatreport.jsp

[10] WhiteHat: *Website Security Statistics Report*. (2013) http://info.whitehatsec.com/2013-website-security-report.html

IDENTIFICATION OF UNUSUAL QUERIES TO WWW SERVICES

ABSTRACT

Internet services and applications are nowadays a common tool of communication between the organization and its external entities (both individuals and other organizations). It is a convenient tool both for the owners of such services and its users. Unfortunately, the specific construction of such applications

results in lack of universal methods of protection against multi-class vulnerabilities. The most common vulnerabilities can be found on the list of OWASP[1] Top 10, and in the reports of security-related companies (including Symantec, WhiteHat or iViz) that indicate that the vast majority of examined servers have multiple (potentially critical) vulnerabilities. Because it is difficult to develop a static method of protection of Internet applications, the article presents an alternative solution based on the creation of patterns of behaviour, identification of unusual behaviours of users and the collective assessment of queries. Presented methods, based on the graph representations and analysis together with distributed decision-making schemes, allow to effectively minimise certain classes of threats of Internet servers, without requiring significant expenditures on implementation and maintenance. They can be used in a wide class of Internet services, with particular value for sites with heavy traffic, thanks to the efficiency of data storage in the structure of graphs and more effective separation of unusual behaviour from large pool of correct behaviours.

[1] OWASP - Open Web Application Security Project