NOWOCZESNE NARZĘDZIA informatyczne w przeciwdziałaniu zagrożeniom bezpieczeństwa

NOWOCZESNE NARZĘDZIA informatyczne w przeciwdziałaniu zagrożeniom bezpieczeństwa

Redakcja naukowa:
Bronisław Sitek, Józef Piotr Knap
Stanisław Sagan, Łukasz Roman

Józefów 2016

Nowoczesne narzędzia informatyczne
w przeciwdziałaniu zagrożeniom bezpieczeństwa

Redakcja naukowa:
Bronisław Sitek, Józef Piotr Knap
Stanisław Sagan, Łukasz Roman

Recenzent:
dr hab. Piotr Majer

Wydawca: Wydawnictwo Wyższej Szkoły Gospodarki
Euroregionalnej im. Alcide De Gasperi w Józefowie
05-410 Józefów, ul. Sienkiewicza 4
tel./faks: 48 22 789 19 03, www.wsge.edu.pl
e-mail: wydawnictwo@wsge.edu.pl
Nakład: 100 egz., objętość: 13,5 ark. wyd.

ISBN 978-83-62753-78-9

Projekt okładki, skład, łamanie:
Jadwiga Popowska

Korekta:
Dariusz Saracyn

Druk i oprawa:
INTER-BOOK
Paulina i Grzegorz Indrzejczyk s.c.
Wiejca 51
05-085 Kampinos

Spis treści

Wstęp

Cyberprzestrzeń jest dzisiaj jedną z głównych platform aktywności człowieka w skali jednostki, jak i zbiorowości. Dzięki komunikatorom społecznym powstał nowy wymiar komunikacji międzyludzkiej. Zwiększył się do niespotykanych rozmiarów krąg znajomych. Z kolei serwisy społecznościowe pozwalają nie tylko na kontaktowanie się z innymi, ale również na dzielenie się ze znajomymi zdjęciami, radosnymi czy smutnymi przeżyciami. Platformy handlowe pozwalają na zawieranie transakcji kupna i sprzedaży na zasadach zbliżonych do aukcji (oferta trwa w trybie online w Internecie) lub licytacji (wersja: *zaproponuj cenę*), które mają miejsce w realnym świecie. Kolejnym obszarem nowego wymiaru funkcjonowania człowieka są sklepy internetowe, dzięki którym można dokonać zakupu bez wychodzenia z domu. Stosunkowo nowym obszarem w cyberprzestrzeni jest szeroko oferowana bankowość internetowa, dostęp do zasobów bibliotecznych czy edukacja (e-learning).

Tak szerokie wykorzystywanie cyberprzestrzeni przez człowieka sprawia, że możemy mówić również o nowym wymiarze bezpieczeństwa. Dobrodziejstwo rozwoju cyberprzestrzeni niesie ze sobą liczne zagrożenia w obszarze cyberprzestrzeni. Jak ważna jest to kwestia, widać po tym, że od kilkunastu lat obserwuje się spadek przestępczości w liczbach bezwzględnych, rośnie zaś przestępczość dokonywana w cyberprzestrzeni. Media niemalże każdego dnia informują o atakach hakerskich na systemy informatyczne banków, ważnych instytucji państwowych, szpitali. Cyberprzestrzeń coraz bardziej wykorzystywana jest przez terrorystów, zwłaszcza z ISIS. Te przykłady pokazują, jak narastają problemy związane z zapewnieniem cyberbezpieczeństwa przez organy władzy państwowej czy jednostki badawcze.

Liczne zagrożenia dla cyberbezpieczeństwa sprawiają, że są one nie tylko przedmiotem zainteresowania odpowiednich służb każdego państwa czy też organizacji międzynarodowych, w tym i Unii Europejskiej, ale również stają się one przedmiotem badań naukowych. Opracowania zawarte w niniejszej publikacji dotyczą problemów miękkich, jak np. etyka w cyberprzestrzeni oraz ochrona prywatności osoby w przypadku inwigilacji. W opracowaniu tym są również kwestie związane z cyberbezpieczeństwem, a dotyczące bezpieczeństwa pacjentów w szpitalach. Autorzy opracowań zawartych w tej publikacji zastanawiali się również nad wykorzystaniem różnych cyberurządzeń do podniesienia poziomu cyberbezpieczeństwa.

Redaktorzy

ROBERT DĘBIŃSKI
Wyższa Szkoła Gospodarki Euroregionalnej
im. Alcide de Gasperi w Józefowie
porucznik.debinski@simplusnet.pl

NADUŻYCIE PRAWA DO WOLNOŚCI SŁOWA I SWOBODNEGO WYRAŻANIA OPINII – ZAGROŻENIEM DLA BEZPIECZEŃSTWA RELIGIJNEGO, NARODOWEGO I OSOBISTEGO

ABUSING THE RIGHT TO THE FREEDOM OF SPEECH AND TO THE FREE EXPRESSION OF OPINIONS AS A THREAT TO RELIGIOUS, NATIONAL AND PERSONAL SECURITY

ABSTRACT

Freedom is reflected in thinking, speaking out, in actions, and in behaviour. The right to the freedom of speech and to the free expression of opinions has come to form part of the catalogue of rights of every human being. This right is guaranteed by international documents with both a universal, and a regional reach, and also by countries' constitutions, for example, the Constitution of the Republic of Poland. The aforementioned documents also impose restrictions upon the right to the freedom of speech and to the free expression of opinions for the purpose of ensuring public safety and order, and also for the purpose of protecting the environment, health and public morality, or the freedom and the rights of other people.

Respecting the right to the freedom of speech and to the free expression of opinions constitutes a reflection of acknowledging human rights by the state. It lays the foundations of a democratic country. At the same time, the said right allows every human being for self-realisation. However, not all countries in the world abide by this rule. Also, not all citizens find the model of a democratic country appealing, which is why abuse ensues, threatening religious, national and personal security.

Keywords: *international law, every human being, freedom of conscience, right to the freedom of thought, human rights, restrictions of the right*

STRESZCZENIE

Wolność przejawia się w myśleniu, wypowiadaniu się, w czynach i zachowaniu. Prawo do wolności słowa i swobodnego wyrażania opinii znalazło swoje miejsce w katalogu praw należnych każdemu człowiekowi. Prawo to gwarantują dokumenty międzynarodowe o zasięgu uniwersalnym, jak i regionalnym, a także konstytucje państw, czego przykładem jest Konstytucja Rzeczypospolitej Polskiej. Wspomniane dokumenty również wprowadzają ograniczenia prawa do wolności słowa i wyrażania opinii w celu zapewnienia bezpieczeństwa lub porządku publicznego bądź dla ochrony środowiska, zdrowia i moralności publicznej albo wolności i praw innych osób.

Poszanowanie prawa do wolności słowa, wypowiedzi i swobodnego wyrażania opinii stanowi przejaw respektowania przez państwo praw człowieka. Stanowi fundament państwa demokratycznego. Dla każdego człowieka zaś wspomniane prawo jest sposobem na samorealizację. Jednak nie wszystkie państwa na świecie przestrzegają tej zasady. Również nie wszystkim obywatelom odpowiada model państwa demokratycznego. Dlatego pojawiają się nadużycia, które realnie zagrażają bezpieczeństwu religijnemu, narodowemu i osobistemu.

Słowa kluczowe: *prawo międzynarodowe, każdy człowiek, wolność sumienia, prawo do wolności myśli, prawa człowieka, ograniczenia prawa*

WPROWADZENIE

Do podstawowych praw w państwach demokratycznych należy prawo do wolności sumienia, myśli, słowa i swobodnego wyrażania opinii. Prawo do wolności wypowiedzi gwarantuje wolność wyrażania swoich poglądów za pomocą wszelkich dostępnych środków ich uzewnętrzniania.

Określenie siebie oznacza możliwość przyjęcia dowolnej koncepcji świata, celu życia oraz systemu wartości. To zaś ma wpływ na sposób postępowania danej osoby. Przyjęcie określonego światopoglądu, systemu wartości, wizji świata i człowieka może niekiedy stać się niebezpieczne. Wówczas pojawia się zagrożenie nie tylko dla przyjmującego, ale – co najgorsze – dla społeczeństwa. Taka sytuacja sprawia, że konieczne jest wprowadzenie ograniczeń w korzystaniu z prawa do wolności. Jednak nie stanowi to naruszenia zasady demokratycznego państwa prawa, lecz sprawia, że jest w nim niezbędne w celu zabezpieczenia państwa i obywateli przed nadużyciami i działaniami mogącym zagrozić bezpieczeństwu religijnemu, narodowemu i osobistemu. Kolejność zagrożeń bezpieczeństwa wskazana w tytule nie jest przypadkowa. W czasach współczesnych zauważa się tendencje ośmieszania osób religijnych, bezczeszczenia symboli religijnych, obrażania uczuć

religijnych na skutek nadużywania prawa do wolności słowa i swobodnego wyrażania opinii. W sytuacji nieszanowania wolności i praw innych osób mogą pojawiać się akty odwetu, a wraz z nimi tragiczne następstwa. Wówczas wskutek naruszenia bezpieczeństwa religijnego może zostać naruszone bezpieczeństwo narodowe bądź osobiste. Osoby, których uczucia religijne zostaną w jakiś sposób obrażone, mogą zostać sprowokowane do aktów terroru. Czy demokracja polega na tym, że wszystko wolno? Czy korzystając ze swoich praw, można naruszać prawa innych? Czy religia, szczególnie chrześcijańska, musi być przedmiotem drwin? Nie każda religia odwołuje się do przebaczenia i miłosierdzia, tak jak chrześcijaństwo. Dlatego za wszelkie akty zniewagi wielokrotnie brany jest odwet, często krwawy.

PODSTAWOWE POJĘCIA

Prawo – ogół przepisów, norm prawnych regulujących stosunki między ludźmi danej społeczności, określających zasady ich postępowania lub zawierających zakazy, których naruszenie zagrożone jest karą (Słownik, 1979, s. 912). Terminu „prawo" używa się w znaczeniu uprawnienia, czyli przysługującej określonemu podmiotowi możliwości zachowania się wywołującego skutki prawne (prawo do czegoś), przy czym zachowanie takie nie jest obowiązkiem podmiotu (Encyklopedia, 1999, s. 558).

Nadużyć – użyć czegoś w nadmiernych ilościach, ponad miarę, nieumiarkowanie; wykorzystać coś w niewłaściwy sposób, użyć czegoś niewłaściwie. Nadużycie – czyn niezgodny z prawem, zwłaszcza przestępstwo finansowe, sprzeniewierzenie, malwersacja. Nadużycie prawa – działanie osoby, które formalnie mieści się w zakresie dozwolonym przez normę prawną, ale jest sprzeczne ze społeczno-gospodarczym przeznaczeniem prawa lub zasadami współżycia społecznego (Słownik, 1979, s. 253).

Wolność – możliwość podejmowania decyzji zgodnie z własną wolą, nieskrępowanego działania, uwarunkowana ogółem czynników społeczno-moralnych; niezależność osobista, swoboda; całokształt warunków, stosunków poza więzieniem, zamknięciem (w przeciwieństwie do aresztowania, przymusowego odosobnienia kogoś, zamknięcia). Prawa obywateli wyznaczone przez dobro powszechne, interes narodowy i porządek prawny. Z ogólnie pojętej wolności wynikają tak zwane wolności obywatelskie sformułowane przez konstytucję i ustawodawstwo. Jest to zobowiązanie władzy państwowej do nieingerowania w określone sfery życia osobistego i publicznego obywateli

(Słownik, 1981, s. 748). Wolność to możliwość podejmowania decyzji i działania zgodnie ze swoim wyborem. Istnieje zależność pomiędzy wiedzą a wolnością. Polega to na tym, że posiadając większą wiedzę o tym, co jest możliwe, powiększa się horyzonty wolności. Możliwość wyboru jest uwarunkowana cechami wybierającego, sytuacją, w jakiej znajduje się, systemem wartości, które uznaje i szanuje, a także właściwie ukształtowanym sumieniem.

PRAWO DO WOLNOŚCI SUMIENIA

Z pojęciem wolności szeroko pojętej wiąże się pojęcie wolności religijnej związanej ze światopoglądem człowieka. Przez wolność religijną najogólniej można rozumieć „uprawnienie woli osoby ludzkiej, nieograniczonej żadnym przymusem, do samookreślania (...) w sprawach religijnych, w ramach celów religijnych i według norm prawno-religijnych" (Misztal, 1996, s. 44).

Powszechna Deklaracja Praw Człowieka z 1948 roku stanowi: „Każda osoba ma prawo do wolności myśli, sumienia i religii" (art. 18, Powszechna). Międzynarodowy Pakt Praw Obywatelskich i Politycznych z 1966 roku powtarza zapis Powszechnej Deklaracji Praw Człowieka z małymi różnicami: „Każdy ma prawo do wolności myśli, sumienia i wyznania" (art. 18 ust. 1, Międzynarodowy). Identyczny zapis w art. 9 zamieszcza Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności z 1950 roku. Wolność religijna jest określana współcześnie jako wolność sumienia i wyznania bądź religii. Jednak czytając dokumenty międzynarodowe czy konstytucje, można natrafić na różnorodność nazw i terminów, np. wolność wierzeń, wolność kultu, wolność myśli, przekonań czy opinii.

Przez prawo do wolności sumienia rozumie się uprawnienia człowieka do swobodnego wyboru, kształtowania i zmiany poglądów oraz przekonań dotyczących spraw religii bądź światopoglądu (Pietrzak, 1999, s. 20). Chodzi o wolność niczym nieograniczoną zewnętrznie – ani fizycznie, ani prawnie. Zatem będzie to wolność człowieka w zakresie wewnętrznym, niemożliwym do skutecznego uregulowania za pomocą norm prawnych. Istota wolności sumienia polega na możliwości swobodnego wyboru światopoglądu zarówno religijnego, jak i areligijnego. Natomiast w sferę normowaną przez prawo wchodzą jedynie akty zewnętrzne, podejmowane w celu zamanifestowania obranego zespołu przekonań (Mezglewski i in., 2008, s. 65).

Konstytucja Rzeczypospolitej Polskiej z 1997 roku stanowi: „Każdemu zapewnia się wolność sumienia i religii" (art. 53 ust. 1, Konstytucja). Gwa-

rantowana konstytucyjnie wolność sumienia oznacza swobodę określenia siebie w sprawach religijnych. Możliwość samookreślenia oznacza swobodę przyjęcia dowolnej koncepcji świata, celu życia człowieka oraz systemu wartości. W tym sensie jest to wolność pozostająca poza zakresem oddziaływania ustawodawcy, ponieważ poglądy, które nie są uzewnętrznione, nie mogą być normowane za pomocą przepisów prawnych. Możliwość samookreślenia ma zwykle swój wyraz zewnętrzny, stając się tym samym przedmiotem unormowań. Zaakceptowanie określonego światopoglądu religijnego zazwyczaj wiąże się z przystąpieniem do wspólnoty religijnej, w ramach której jest on przyjmowany (Mezglewski i in., 2008, s. 83). Natomiast akceptacja określonego systemu wartości, wizji świata i wizji człowieka może znaleźć odzwierciedlenie w wyborze określonego sposobu życia, a co za tym idzie, określonego sposobu postępowania. Decyzje w zakresie wewnętrznym, podjęte „w sumieniu", znajdują odzwierciedlenie w postępowaniu, czyli dokonują się na forum zewnętrznym.

Przyjęcie określonego światopoglądu, systemu wartości, wizji świata i człowieka może niekiedy stać się niebezpieczne. Zarówno dla przyjmującego, jak i społeczeństwa. Wręcz może stanowić zagrożenie. Problem pojawia się w źle ukształtowanym sumieniu, jak i w sposobie kształtowania danej osobowości. Problem również stanowią osoby wpływające na daną osobę i kształtujące jej osobowość. Chodzi o kształtowanie sumienia przez jakichś nauczycieli, moderatorów, którzy mają źle uformowane sumienie, a co za tym idzie zachwianą hierarchię wartości, wypaczoną wizję świata i człowieka. Tworzenie przez takie osoby pewnej ideologii i zaszczepianie jej w innych może okazać się tragiczne w skutkach.

Nakazy sumienia, według których postępuje człowiek i które są inspiracją do jego działania, kształtują się nie tylko pod wpływem idei i doktryn religijnych. We współczesnym świecie dostrzega się coraz silniejszy wpływ idei areligijnych i ateistycznych na rozwój myśli człowieka.

PRAWO DO WOLNOŚCI MYŚLI I SŁOWA

Prawo do wolności przejawia się w myśleniu, wypowiadaniu się, w czynach i zachowaniu. Myślenie, świadomość są niedostępne dla kontroli z zewnątrz. Jedyną uprawnioną instancją kontrolującą jest sam człowiek – autor tego typu wytworu. W tym obszarze człowiek ma swobodę nieograniczoną.

Powszechna Deklaracja Praw Człowieka stanowi: „Każda osoba ma prawo do wolności myśli (...)" (art. 18, Powszechna). Międzynarodowy Pakt Praw Obywatelskich i Politycznych powtarza zapis Powszechnej Deklaracji: „Każdy ma prawo do wolności myśli (...)" (art. 18 ust. 1, Międzynarodowy). W identyczny sposób stanowi Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności: „Każdy ma prawo do wolności myśli (...)" (art. 9, Konwencja).

Przez wolność myśli należy rozumieć wolność intelektualną, gromadzenia wiedzy i swobodę poszukiwania wyrazu własnej osobowości. Wolność myśli jest prawem do zastanawiania się nad słusznością wydarzeń, zjawisk, zapatrywań, a także do ich ujawniania bądź przemilczania. Myśl oznacza wykorzystywanie potencjału ludzkiego rozumu. Jest czynnością umysłu poza kontrolą społeczną. Prawo do wolności myśli jest zatem prawem absolutnym (Warchałowski, 2004, s. 81).

Słowo – wypowiadanie się ustne lub pisemne; mowa, język (Słownik, 1981, s. 258). Wolność słowa jest to prawo obywatela do swobodnego wypowiadania swoich myśli w słowie i piśmie (Słownik, 1981, s. 748). Z definicji tej wynika, jakoby wolność słowa wchodziła w zakres praw obywatelskich. Jednak jest to złudne, ponieważ jest to zakres praw człowieka. Podobnie dzieje się z prawem do głoszenia swoich poglądów i opinii. Również jest to prawo wchodzące w zakres praw człowieka, a nie praw obywatelskich nadanych przez jakąkolwiek władzę. Prawo do publicznego wyrażania własnego zdania oraz poglądów, a także jego poszanowania przez innych współcześnie jest uznawane jako standard norm cywilizacyjnych. Chociaż często nakładane są na nie pewne ograniczenia, np. w sprawach publicznego obrażania innych osób[1].

Powszechna Deklaracja Praw Człowieka stanowi: „Każda jednostka ma prawo do wolności poglądów i wypowiedzi; prawo to obejmuje nieskrępowaną wolność posiadania poglądów oraz poszukiwania, otrzymywania i przekazywania informacji oraz idei, wszelkimi środkami i bez względu na granice" (art. 19, Powszechna). Międzynarodowy Pakt Praw Obywatelskich i Politycznych powtarza zapis Powszechnej Deklaracji Praw Człowieka w bardziej konkretnej formie: „Każdy ma prawo do posiadania bez przeszkód własnych poglądów" (art. 19 ust. 1, Międzynarodowy). Wzoru-

[1] https://pl.wikipedia.org/wiki/Wolno%C5%9B%C4%87_s%C5%82owa [data dostępu: 12.10.2016].

jąc się na dokumentach międzynarodowych, Konstytucja Rzeczypospolitej Polskiej, stanowi: „Każdemu zapewnia się wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji" (art. 54 ust. 1, Konstytucja). Zagwarantowana przez Konstytucję Rzeczypospolitej Polskiej wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania ma szerokie znaczenie.

Wolność wypowiedzi gwarantuje wolność wyrażania swoich poglądów za pomocą wszelkich dostępnych środków ich uzewnętrzniania. Do takich środków można zaliczyć np.: gesty, dzieła sztuki, prasę, plakaty, telewizję, radio, Internet, koncerty, wystawy, odczyty. Wolność słowa to również dostęp do istniejących krajowych i zagranicznych źródeł informacji. Wolność ta przejawia się także w wolności poszukiwania informacji. Poszanowanie prawa do wolności słowa, wypowiedzi stanowi przejaw respektowania praw człowieka przez państwo. Dla każdego człowieka jest sposobem na samorealizację. Wolność wypowiedzi stanowi fundament państwa demokratycznego. Niestety, nie wszystkie państwa na świecie przestrzegają tej zasady. Niektóre z tych państw nawet określają siebie mianem państwa demokratycznego. Jednak praktyka pokazuje, że nie potrafią zaakceptować krytyki, która jest przecież przejawem wolności i prawem każdego człowieka, także obywatela, do swobodnego wypowiadania swoich poglądów.

PRAWO DO SWOBODNEGO WYRAŻANIA OPINII

Opinia – mniemanie, sąd, przekonanie, pogląd (Słownik, 1979, s. 527). Międzynarodowy Pakt Praw Obywatelskich i Politycznych w art. 19 ust. 2 stanowi: „Każdy człowiek ma prawo do swobodnego wyrażania opinii; prawo to obejmuje swobodę poszukiwania, otrzymywania i rozpowszechniania wszelkich informacji i poglądów, bez względu na granice państwowe, ustnie, pismem lub drukiem, w postaci dzieła sztuki bądź w jakikolwiek inny sposób według własnego wyboru" (art. 19 ust. 2, Międzynarodowy). Na temat wyrażania opinii wypowiada się również Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. W art. 10 ust. 1 stanowi: „Każdy ma prawo do wolności wyrażania opinii. Prawo to obejmuje wolność posiadania poglądów oraz otrzymywania i przekazywania informacji i idei bez ingerencji władz publicznych i bez względu na granice państwowe. Niniejszy przepis nie wyklucza prawa Państw do poddania procedurze zezwoleń przedsiębiorstw radiowych, telewizyjnych lub kinematograficznych" (art. 10 ust. 1, Konwencja).

Każdy człowiek bez żadnego wyjątku ma prawo do swobodnego wyrażania opinii i może z niego korzystać. Gwarantują to dokumenty międzynarodowe zarówno o zasięgu uniwersalnym, jak i regionalnym. Prawo to obejmuje poglądy, które mogą mieć subiektywny charakter. Wyrażają one spostrzeżenia, oceny, własne przeżycia i przemyślenia. To prawo każdego człowieka nie jest ograniczone granicami państwowymi. Nie dotyczy jednego czy własnego kraju, ale gdziekolwiek człowiek znajdzie się na świecie, jest podmiotem prawa do swobodnego wyrażania opinii. Dowolna również jest forma uzewnętrzniania swoich opinii, może mieć formę np. ustną, pisemną, drukowaną, gestów czy dzieła sztuki. Omawiane prawo ma ścisły związek z wolnością słowa, czyli ze swobodnym wyrażaniem, otrzymywaniem i przekazywaniem informacji. Wolność wyrażania opinii ma również ścisły związek z prawem do wolności sumienia i religii. Jest to jedno z najcenniejszych praw człowieka o charakterze osobistym, społecznym i politycznym. Stanowi wartość osobistą dla każdego człowieka, ponieważ jest sposobem jego samorealizacji i samookreślenia. Stanowi wartość społeczną, ponieważ jest sposobem wyrażania własnej opinii, jak i poznawania jej przez innych. Stanowi wartość polityczną, ponieważ służy wyrażaniu poglądów politycznych i procesowi przemian w funkcjonowaniu państwa.

Prawo do wolności wyrażania opinii dotyczy poglądów i informacji, które są przychylne odbiorcom. Zarówno sprawującym jakąkolwiek władzę, osobom ze świata polityki, jak i prywatnym osobom. Jednak prawo to obejmuje również swobodę wyrażania opinii nieprzychylnych, niepochlebnych, drażniących, nacechowanych krytyką. Wolność wyrażania opinii służy osiąganiu dobra, właściwych rozwiązań w życiu poszczególnych osób i całych społeczeństw. Prawo do swobodnego wyrażania opinii jest jednym z zasadniczych składników demokracji. Jego respektowanie zaś przez władzę stanowi przejaw poszanowania demokracji w danym państwie.

GRANICE PRAWA DO WOLNOŚCI SŁOWA I WYRAŻANIA OPINII

Granice prawa do wolności słowa i wyrażania opinii w pierwszej kolejności ustala osoba korzystająca z tej wolności. Decyduje o tym poczucie odpowiedzialności, realizacja swoich celów, dobra opinia, pozytywny wizerunek, a także poczucie bezpieczeństwa. Z poczuciem odpowiedzialności za wypowiadane słowo i wyrażaną opinią bywa bardzo różnie. W zależności

od kryterium, jakie stosuje dana osoba. Zatem granice tego prawa są różnie określane, a niekiedy w ogóle nie są brane pod uwagę. Istnieją również pewne społeczne granice wyznaczane np. przez rodzinę, szkołę, środowisko, miejsce pracy, organizacje społeczne, Kościół. Jednak największe znaczenie mają granice określone przez państwo (Łopatka, 1993, s. 22).

Powszechna Deklaracja Praw Człowieka, proklamując między innymi prawo do wolności wyrażania opinii, stanowi zarazem, że „Każdy człowiek ma obowiązki wobec społeczeństwa, bez którego niemożliwy jest swobodny i pełny rozwój jego osobowości" (art. 29 ust. 1, Powszechna). Jednak Powszechna Deklaracja nie wymienia tych obowiązków wobec społeczeństwa. Stanowi zaś o ograniczeniach. „W korzystaniu ze swych praw i wolności każdy człowiek podlega jedynie takim ograniczeniom, które są ustalone przez prawo wyłącznie w celu zapewnienia odpowiedniego uznania i poszanowania praw i wolności innych i w celu uczynienia zadość słusznym wymogom moralności, porządku publicznego i powszechnego dobrobytu demokratycznego społeczeństwa" (art. 29 ust. 2, Powszechna). W ten sposób został po raz pierwszy stworzony uniwersalny standard dopuszczalnych przez państwo ograniczeń wyrażania opinii.

Międzynarodowy Pakt Praw Obywatelskich i Politycznych w bardziej konkretnej formie stanowi o granicach prawa do wolności wyrażania opinii:

„2. Każdy człowiek ma prawo do swobodnego wyrażania opinii; prawo to obejmuje swobodę poszukiwania, otrzymywania i rozpowszechniania wszelkich informacji i poglądów, bez względu na granice państwowe, ustnie, pismem lub drukiem, w postaci dzieła sztuki bądź w jakikolwiek inny sposób według własnego wyboru.

3. Realizacja praw przewidzianych w ustępie 2 niniejszego artykułu pociąga za sobą specjalne obowiązki i specjalną odpowiedzialność. Może ona w konsekwencji podlegać pewnym ograniczeniom, które powinny być jednak wyraźnie przewidziane przez ustawę i które są niezbędne w celu:
   a) poszanowania praw i dobrego imienia innych;
   b) ochrony bezpieczeństwa państwowego lub porządku publicznego albo zdrowia lub moralności publicznej" (art. 19, Międzynarodowy).

Przepisy Międzynarodowego Paktu Praw Obywatelskich i Politycznych mają moc wiążącą dla państw – stron tego dokumentu. Przypominają, że korzystanie z wolności pociąga za sobą specjalne obowiązki i specjalną od-

powiedzialność. Określa dopuszczalne granice wolności wyrażania opinii. Powinny one być wyraźnie przewidziane przez prawo i konieczne w celu: poszanowania praw i dobrego imienia innych; ochrony bezpieczeństwa państwowego lub porządku publicznego albo zdrowia lub moralności publicznej. Niedopuszczalne zatem są ograniczenia w innych celach niż te przewidziane przez prawo.

Na temat prawa do wolności wyrażania opinii i jego granic wypowiada się również Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. W art. 10 gwarantuje to prawo, jak również wprowadza ograniczenia.

„1. Każdy ma prawo do wolności wyrażania opinii. Prawo to obejmuje wolność posiadania poglądów oraz otrzymywania i przekazywania informacji i idei bez ingerencji władz publicznych i bez względu na granice państwowe. Niniejszy przepis nie wyklucza prawa Państw do poddania procedurze zezwoleń przedsiębiorstw radiowych, telewizyjnych lub kinematograficznych.

2. Korzystanie z tych wolności pociągających za sobą obowiązki i odpowiedzialność może podlegać takim wymogom formalnym, warunkom, ograniczeniom i sankcjom, jakie są przewidziane przez ustawę i niezbędne w społeczeństwie demokratycznym w interesie bezpieczeństwa państwowego, integralności terytorialnej lub bezpieczeństwa publicznego ze względu na konieczność zapobieżenia zakłóceniu porządku lub przestępstwu, z uwagi na ochronę zdrowia i moralności, ochronę dobrego imienia i praw innych osób oraz ze względu na zapobieżenie ujawnieniu informacji poufnych lub na zagwarantowanie powagi i bezstronności władzy sądowej" (art. 10, Konwencja).

Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności nie posługuje się wzorem Powszechnej Deklaracji Praw Człowieka i nie zamieszcza ogólnej klauzuli ograniczającej. Ograniczenia praw i wolności gwarantowanych Konwencją dokonują się na podstawie klauzul szczegółowych. Jest ona bardziej restrykcyjna niż Międzynarodowy Pakt Praw Obywatelskich i Politycznych wobec prawa do wolności wyrażania opinii.

Konstytucja Rzeczypospolitej Polskiej z 1997 roku nie stanowi o granicach prawa do wolności wyrażania opinii. Jedynie zamieszcza ogólną klauzulę ograniczającą:

„2. Każdy jest obowiązany szanować wolności i prawa innych. Nikogo nie wolno zmuszać do czynienia tego, czego prawo mu nie nakazuje.

3. Ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw" (art. 31, Konstytucja).

Konstytucja odwołuje się do liberalnej koncepcji wolności, zgodnie z którą granicą wolności jednostki jest jednakowa wolność innych osób. Z tego wynika obowiązek każdego człowieka do poszanowania wolności i praw innych osób. Jest rzeczą oczywistą, że prawa, a szczególnie wolności, nie mogą być nieograniczone. Dlatego konieczne jest wyznaczenie granic. W celu niedoprowadzenia do naruszenia art. 31 ust. 2 wspomnianego dokumentu, aby zastosować ograniczenie wolności i prawa, należy łącznie spełnić określone warunki:

1. Ograniczenia wprowadza ustawa.
2. Ograniczenia są konieczne w celu zapewnienia bezpieczeństwa lub porządku publicznego bądź dla ochrony środowiska, zdrowia i moralności publicznej albo wolności i praw innych osób.

Konieczność wprowadzenia ograniczeń z powodu wymienionych przyczyn nie narusza zasady demokratycznego państwa prawa, lecz sprawia, że jest w nim konieczne. Ograniczenia te nie mogą naruszać istoty wolności i praw. Wprowadzenie ograniczeń powinno pozostawać w proporcji do ciężarów i niedogodności, które z tych ograniczeń wynikają dla społeczeństwa (Winczorek, 2008, s. 84).

KONSEKWENCJE NADUŻYCIA PRAWA DO WOLNOŚCI SŁOWA I WYRAŻANIA OPINII

Słowo jest nośnikiem informacji, prawdy, ale i kłamstwa. Może służyć wychowaniu, ale też demoralizacji. Słowo jest środkiem porozumiewania się, jak również konfliktu, manipulacji, agresji, oporu, nakłaniania do popełnienia przestępstwa, a także przestępstwa. Ograniczenia prawa do wolności słowa i wyrażania opinii prowadzą do narastania napięć społecznych, a niekiedy do wybuchu społecznego niezadowolenia i destrukcji. Jednak jak każda wolność człowieka – jest i musi być ograniczona. Konieczne staje się

wyznaczenie granicy pomiędzy używaniem a nadużywaniem. W przeciwnym razie może pojawić się zagrożenie bezpieczeństwa zarówno dla samego zainteresowanego, jak i społeczeństwa. Przykładów nadużycia prawa do wolności słowa i wyrażania opinii jest wiele. Niektóre przypadki przekroczenia granic prawa do wolności słowa i wyrażania opinii wywołały zagrożenie dla bezpieczeństwa religijnego, bezpieczeństwa narodowego, bezpieczeństwa osobistego, czy wręcz spowodowały tragedie wielu osób i społeczeństw.

W 2013 roku Islamskie Państwo w Iraku i Lewancie wypowiedziało Przymierze Umara z VII wieku, które regulowało wspólne życie chrześcijan i muzułmanów w Syrii. Przystąpiono wówczas do wojny z chrześcijanami, porywając i zabijając ich oraz profanując krzyże i świątynie[2]. Podczas wojny domowej radykalni islamiści skupieni wokół Islamskiego Państwa w Iraku i Lewancie oraz Islamskiego Frontu Syryjskiego dokonywali czystek etnicznych na chrześcijanach, alawitach, szyitach, Kurdach, a także umiarkowanych sunnitach. Spirala przemocy w ich wykonaniu rozpoczęła się masakrą chrześcijan w Ad-Duwajr 27 maja 2013 roku, kiedy to wymordowano niemal wszystkich mieszkańców wsi[3].

W Syrii pochodzący z Jordanii salaficki szejk Yasir al-Ajlawni wydał muzułmańskim bojownikom pozwolenie na gwałcenie chrześcijanek, gdyż nie jest to sprzeczne z islamem (Kłos, 2013, s. 9). Innym przejawem nadużycia prawa do wolności słowa i wyrażania opinii przez przywódców duchowych jest uskutecznianie propagandy wśród społeczności muzułmańskich żyjących szczególnie w Europie Zachodniej do podjęcia „świętej wojny" „domowymi sposobami", skierowanej do zachodnich społeczeństw i rządów. W czerwcu 2014 roku kalif Ibrahim wystosował apel – „szerzcie dżihad (...) i zabijajcie niewiernych, gdziekolwiek jesteście i w jakikolwiek sposób możecie" (Otłowski, 2015, nr 5, s. 84).

We współczesnym świecie nie tylko bezpieczeństwo religijne jest zagrożone, również narodowe. Istnieje realne zagrożenie nie tylko dla bezpieczeństwa religijnego mniejszości religijnych Bliskiego Wschodu, także dla społeczności europejskiej, wśród której znajdują się też obywatele Polski.

Dnia 7 stycznia 2015 roku dwaj francuscy muzułmanie pochodzenia algierskiego wdarli się do redakcji satyrycznego tygodnika „Charlie Hebdo"

[2] https://pl.wikipedia.org/wiki/Pa%C5%84stwo_Islamskie [data dostępu: 28.10.2016].

[3] https://pl.wikipedia.org/wiki/Pa%C5%84stwo_Islamskie [data dostępu: 28.10.2016].

w Paryżu znanego z częstego publikowania wulgarnych karykatur, wyszydzania symboli religijnych chrześcijaństwa, judaizmu i islamu. Zabili 12 osób (w tym 9 osób pracujących w redakcji, głównie dziennikarzy i rysowników, oraz 2 policjantów) i ranili 11 osób. Atak był następstwem nadużywania prawa do wolności słowa i wyrażania opinii przez redakcję gazety. „Charlie Hebdo" znajdował się na celowniku islamskich ekstremistów od lutego 2006 roku, kiedy to przedrukował karykatury Mahometa z duńskiego dziennika „Jyllands-Posten" uzupełnione o własne, nowe karykatury islamskiego proroka. Mimo że w 2011 roku siedziba doszczętnie spłonęła, a dyrektor wydawnictwa Charb wielokrotnie otrzymywał pogróżki i musiał korzystać z policyjnej ochrony, tygodnik nie rezygnował z kontrowersyjnych publikacji[4].

Kolejnym następstwem nadużywania prawa do wolności słowa i wyrażania opinii przez redakcję gazety „Charlie Hebdo" były protesty w Nigrze. Podczas dwudniowych (18–19 stycznia 2015 roku) antychrześcijańskich i antyfrancuskich zamieszek spłonęło 45 kościołów, 10 osób zginęło, a ponad 300 chrześcijan znalazło się pod ochroną wojska[5].

W Pakistanie zaś palono francuskie flagi. Protesty odbyły się także w Afganistanie, a prezydent tego kraju, Aszraf Ghani, potępił publikowanie karykatur Mahometa. Saudyjska Organizacja Współpracy Islamskiej zapowiedziała złożenie pozwu przeciw „Charlie Hebdo"[6].

„Charlie Hebdo" publikował karykatury nie tylko Mahometa, także duchownych i symboli innych religii.

Za obrażanie uczuć innych ludzi skrytykował francuską gazetę papież Franciszek. Powiedział on: „Każda religia ma swoją godność. Nie można prowokować i obrażać wiary innych osób albo robić sobie żartów z religii"[7].

Przywódcy Państwa Islamskiego i talibowie utożsamiają Zachód z chrześcijanami. Wszyscy biali Europejczycy i Amerykanie w ich optyce są chrześcijanami, którzy prowadzą krucjatę w innej formie niż dawniej. Wierzą,

---

[4] https://pl.wikipedia.org/wiki/Charlie_Hebdo [data dostępu: 01.11.2016].

[5] http://www.polskieradio.pl/5/3/Artykul/1355951,Manifestacje-przeciwko-karykaturom-Mahometa-W-stolicy-Nigru-spalono-w-weekend-45-kosciolow [data dostępu: 01.11.2016].

[6] http://www.tvp.info/18498848/plona-koscioly-i-francuskie-flagi-swiat-islamu-protestuje-przeciwko-charlie-hebdo [data dostępu: 01.11.2016].

[7] http://www.tvp.info/18498848/plona-koscioly-i-francuskie-flagi-swiat-islamu-protestuje-przeciwko-charlie-hebdo [data dostępu: 01.11.2016].

że Zachód – to znaczy chrześcijanie – chce dominacji i poniżenia muzułmanów. Podają przykład Iraku i Afganistanu. Wojska NATO w ich opinii to „krzyżowcy". Szkoły koraniczne przekonują młodych chłopców, że Allah wzywa ich do prowadzenia świętej wojny. Młodzi ludzie są nauczani, że jeśli zginą w walce z niewiernymi, natychmiast pójdą do nieba. Są przekonani, że Zachód wcześniej czy później ich zaatakuje. Dlatego nie mogą siedzieć bezczynnie. Im nie podoba się obecny quasi-demokratyczny system. Atakują szkoły, kościoły i inne obiekty, które w jakikolwiek sposób nawiązują do tradycji zachodniej. Agresja islamistów kieruje się ku rządom demokratycznym. Według nich „demokracja" to najgorsza z możliwych form rządów, gdyż oparta jest na woli narodu, a nie woli Boga – Allaha[8].

Papież Franciszek 16 marca 2015 roku potępił zamachy na dwa kościoły w chrześcijańskiej dzielnicy Lahore w Pakistanie. W ich wyniku zginęło 14 osób, a 78 zostało rannych. Wcześniej, w grudniu, talibowie dokonali masakry w jednej ze szkół publicznych w Peszawarze, do której uczęszczały dzieci oficerów pakistańskich. Siedmiu napastników weszło do szkoły publicznej i otworzyło ogień, zabijając 145 osób, w tym 132 uczniów w wieku od 8 do 18 lat. Talibowie przyznali się do wszystkich zamachów. Do szkół zaś trafiło ostrzeżenie kierowane do „apostatów" i „dyplomatów krzyżowców". Talibowie zagrozili atakami na wszystkie szkoły w całym Pakistanie, na misje chrześcijańskie i wszelkie instytucje związane z zachodnim systemem edukacji[9].

Granice prawa do wolności słowa i swobodnego wyrażania opinii są nagminnie łamane. Nadużycie prawa do wspomnianej wolności przybiera różne formy. Przykładem nadużycia prawa do wolności słowa i wyrażania opinii w Polsce, na szczęście niezwiązanym z przelewem krwi, był przypadek piosenkarki Doroty Rabczewskiej. W wywiadzie prasowym w 2009 roku opowiadała między innymi, że „bardziej wierzy w dinozaury niż w Biblię", bo – jej zdaniem – „ciężko wierzyć w coś, co spisał jakiś napruty winem i palący jakieś zioła". Kodeks karny stanowi, że kto obraża uczucia religijne innych osób, znieważając publicznie przedmiot czci religijnej, podlega grzywnie albo karze ograniczenia wolności do 2 lat więzienia. Konsekwen-

[8] http://www.pch24.pl/pakistanski-arcybiskup--wykreowani-przez-zachod-talibowie-prowadza-swieta-wojne-z-krzyzowcami,34966,i.html [data dostępu: 27.10.2016].

[9] http://www.pch24.pl/pakistanski-arcybiskup--wykreowani-przez-zachod-talibowie-prowadza-swieta-wojne-z-krzyzowcami,34966,i.html [data dostępu: 27.10.2016].

cją nadużycia wspomnianego prawa było 5 tysięcy złotych grzywny, które musiała zapłacić, za obrazę uczuć religijnych[10].

Nadużywanie prawa do wolności słowa i wyrażania opinii także godzi w bezpieczeństwo osobiste. Prawie codziennie media informują o pogróżkach, zastraszaniu, zwalnianiu z miejsc pracy, pobiciach wskutek korzystania z prawa do wolności słowa i wyrażania opinii, jak również z nadużywania tego prawa. O wielu zaś przypadkach zagrożenia bezpieczeństwa osobistego opinia publiczna nie dowiaduje się, ponieważ rozgrywa się to skrycie.

PODSUMOWANIE

Międzynarodowy Pakt Praw Obywatelskich i Politycznych stanowi: „Każdy człowiek ma prawo do swobodnego wyrażania opinii; prawo to obejmuje swobodę poszukiwania, otrzymywania i rozpowszechniania wszelkich informacji i poglądów, bez względu na granice państwowe, ustnie, pismem lub drukiem, w postaci dzieła sztuki bądź w jakikolwiek inny sposób według własnego wyboru" (art. 19 ust. 2, Międzynarodowy). Konstytucja Rzeczypospolitej Polskiej zaś precyzuje: „Każdy jest obowiązany szanować wolności i prawa innych. Nikogo nie wolno zmuszać do czynienia tego, czego prawo mu nie nakazuje" (art. 31 ust. 2, Konstytucja).

Wolność słowa i wyrażania opinii jest prawem przysługującym każdemu człowiekowi. Dlatego że jest prawem przysługującym każdemu człowiekowi, musi posiadać granice. Są one konieczne w państwie prawa, ponieważ niewłaściwe korzystanie z wolności jednego człowieka może naruszyć prawa innego człowieka. Ograniczenia pomniejszają sferę wolności, zatem muszą być ściśle sprecyzowane. Wymagane jest, aby były to takie ograniczenia, które wynikać będą z przepisów prawa (Łopatka, 1995, s. 43). Ustawodawca nie może więc dowolnie ustanawiać ograniczeń wolności. Dzięki temu podmioty uprawnione w zakresie korzystania z wolności słowa i wyrażania opinii zaznajomione są wcześniej z możliwościami i warunkami ograniczenia. Państwo powinno powiązać kryterium, jakim jest ,,przewidziane przez prawo", z jedną z podstaw ograniczających, którą może stanowić: bezpieczeństwo publiczne, porządek, zdrowie lub moralność publiczna albo prawa i wolności innych osób, tzn. uzasadnić wprowadzone ograniczenie ochroną interesów zbiorowych.

[10] http://www.polskieradio.pl/5/3/Artykul/628468,Doda-prawomocnie-skazana-za-obraze-uczuc-religijnych [data dostępu: 28.10.2016].

Interesującym przykładem nadużycia prawa do wolności słowa i wyrażania opinii jest przypadek Adama Darskiego „Nergala" w sprawie obrazy uczuć religijnych. W czasie jednego ze swoich koncertów podarł Biblię, kartki rzucił w publiczność i wypowiedział obraźliwe słowa godzące w uczucia religijne chrześcijan. Sąd Najwyższy w 2015 roku w Warszawie orzekł, że nie obraził on uczuć religijnych. Sąd bezzasadną nazwał kasację prokuratora i oskarżyciela posiłkowego. Konstytucja Rzeczypospolitej Polskiej mówi wprost: „Każdy jest obowiązany szanować wolności i prawa innych (...)" (art. 31 ust. 2, Konstytucja). Darski nie poniósł konsekwencji swego czynu. Jednak nie można mówić, że nie obraził uczuć religijnych. Ustawa zasadnicza stanowi o obowiązku szanowania wolności i prawa innych, a granica została przekroczona. Dowodem tego były protesty osób, których uczucia religijne zostały dotknięte oraz pojawił się pozew do sądu. Gdyby ten przypadek dotyczył świętej księgi islamu – Koranu, wyczyn Darskiego nie byłby wybaczony. Podobnie jak obraza uczuć religijnych muzułmanów dokonana przez redakcję gazety „Charlie Hebdo". Zachowania godzące w sferę uczuć religijnych są naruszeniem zasad bezpieczeństwa religijnego. Również mogą wywołać zagrożenie narodowe, w wyniku którego ucierpiałoby wiele niewinnych osób. W przypadku samego Darskiego zaś mogłyby być złamane zasady bezpieczeństwa osobistego.

Uczucia religijne są delikatną sferą w człowieku. Łatwo je urazić. Wskutek tego bezpieczeństwo religijne osób-wyznawców danej religii może zostać naruszone. Jednak konsekwencje związane z nadużyciem prawa do wolności słowa i wyrażania opinii mogą wywołać także zagrożenie dla bezpieczeństwa narodowego. Przejawy czyjegoś braku kultury, szacunku, buty i arogancji mogą odczuć niewinni ludzie. Stając się ofiarami jakiegoś aktu zemsty nawet na masową skalę.

Bibliografia

Encyklopedia prawa (1999). U. Kalina-Prasznic (red.), Wydawnictwo C.H. Beck, Warszawa.

Kłos A. (2013). *Fatwa zachęcająca do gwałtów na chrześcijankach*, [w:] „Niedziela. Tygodnik Katolicki", nr 16, s. 9.

Łopatka A. (1993). *Prawo do swobodnego wyrażania opinii*. Wydawnictwo Scholar, Warszawa.

Łopatka A. (1995). *Prawo do wolności myśli, sumienia i religii*. Wydawnictwo Scholar, Warszawa.

Mezglewski A., Misztal H., Stanisz P. (2008). *Prawo wyznaniowe*. Wydawnictwo C. H. Beck, Warszawa.

Misztal H. (1996). *Polskie prawo wyznaniowe,* t. I: *Zagadnienia wstępne. Rys historyczny*. Towarzystwo Naukowe Katolickiego Uniwersytetu Lubelskiego, Lublin.

Otłowski T. (2015). *Płomień świętej wojny*, [w:] „Polska Zbrojna", nr 5 (829), s. 80–84.

Pietrzak M. (1999). *Prawo wyznaniowe*. Wydawnictwo Prawnicze PWN, Warszawa.

Słownik języka polskiego (1979). M. Szymczak (red.): t. II. Państwowe Wydawnictwo Naukowe, Warszawa.

Słownik języka polskiego (1981). M. Szymczak (red.): tom III. Państwowe Wydawnictwo Naukowe, Warszawa.

Warchałowski K. (2004). *Prawo do wolności myśli, sumienia i religii w Europejskiej Konwencji Praw Człowieka i Podstawowych Wolności*. Towarzystwo Naukowe Katolickiego Uniwersytetu Lubelskiego, Lublin.

Winczorek P. (2008). *Komentarz do Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku*. Wydawnictwo Liber, Warszawa.

Źródła prawa

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku (Dz.U. 1997 nr 78 poz. 483).

Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności, Rzym, 4 XI 1950 (Dz.U. 1993 nr 61 poz. 284).

Międzynarodowy Pakt Praw Obywatelskich i Politycznych, Nowy Jork, 16 XII 1966 (Dz.U. 1977 nr 38 poz. 167).

Powszechna Deklaracja Praw Człowieka, Paryż, 10 XII 1948, [w:] *Prawa Człowieka, Dokumenty międzynarodowe,* B. Gronowska, T. Jasudowicz i C. Mika (red.), Wydawnictwo Comer, Toruń,1996, s. 15–20.

Źródła internetowe

https://pl.wikipedia.org/wiki/Wolno%C5%9B%C4%87_s%C5%82owa [data dostępu: 12.10.2016].

http://www.pch24.pl/pakistanski-arcybiskup--wykreowani-przez-zachod-talibowie-prowadza-swieta-wojne-z-krzyzowcami,34966,i.html [data dostępu: 27.10.2016].

https://pl.wikipedia.org/wiki/Pa%C5%84stwo_Islamskie [data dostępu: 28.10.2016].

http://www.polskieradio.pl/5/3/Artykul/628468,Doda-prawomocnie-skazana-za-obraze-uczuc-religijnych [data dostępu: 28.10.2016].

http://www.gazetaprawna.pl/artykuly/857312,sad-najwyzszy-adam-nergal-darski-nie-obrazil-uczuc-religijnych-co-zrobi-ryszard-nowak.html [data dostępu: 28.10.2016].

https://pl.wikipedia.org/wiki/Charlie_Hebdo [data dostępu: 01.11.2016].

http://www.polskieradio.pl/5/3/Artykul/1355951,Manifestacje-przeciwko-karykaturom-Mahometa-W-stolicy-Nigru-spalono-w-weekend-45-kosciolow [data dostępu: 01.11.2016].

http://www.tvp.info/18498848/plona-koscioly-i-francuskie-flagi-swiat-islamu-protestuje-przeciwko-charlie-hebdo [data dostępu: 01.11.2016].

http://www.tvp.info/18498848/plona-koscioly-i-francuskie-flagi-swiat-islamu-protestuje-przeciwko-charlie-hebdo [data dostępu: 01.11.2016].

MARIUSZ WÓDKA
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
m.wodka@wp.pl

WPŁYW MIGRACJI NA BEZPIECZEŃSTWO OBYWATELA I PAŃSTWA

THE IMPACT OF MIGRATION ON THE SECURITY OF THE CITIZEN AND THE STATE

ABSTRACT

The article is devoted to migration and multiple impact on social change, economic, cultural, including the drafting of threats to the security of the individual, the state, but also the region. Migration is in many ways motivated. It has its base cost (the difference in the level of development of life), ethnic, religious. The uncontrolled influx of people, it can become a destabilizing internal security of the country and disrupt the social sense of security, causingconflictsamong on national or religious (immigrants from Africa and countries of the Middle East). The problem intensifies increase in terrorist attacks, growth of religious fundamentalism and ethnic separatism. The scale of immigration is difficult to estimate. The uncontrolled influx of people change the image of the entire European Union, including Polish. Taken analysis shows that threats (potential and actual) result from the migration of the uncontrolled movement of people changing security environment of the citizen and the state.

Keywords: *migration, globalization, organized crime, security, the European Union*

STRESZCZENIE

Artykuł poświęcony jest procesom migracyjnym i ich wielorakiemu wpływowi na przemiany społeczne, gospodarcze, kulturowe, w tym stanowienie zagrożenia dla bezpieczeństwa jednostki, państwa, ale także regionu. Migracja jest wielorako motywowana. Ma swoje podłoże ekonomiczne (różnica w poziomie rozwoju życia), etniczne, religijne. Niekontrolowany napływ ludności może stać się elementem destabilizującym bezpieczeństwo wewnętrzne kraju oraz

zakłócić społeczne poczucie bezpieczeństwa, powodując konflikty m.in. na tle narodowościowym lub religijnym (imigranci z krajów afrykańskich i krajów Bliskiego Wschodu). Problem potęguje wzrost ataków terrorystycznych, narastanie fundamentalizmu religijnego oraz separatyzmu etnicznego. Skala imigracji jest trudna do oszacowania. Niekontrolowany napływ ludzi zmienia obraz całej Unii Europejskiej, w tym także Polski. Podjęta analiza przedstawia, jakie zagrożenia (potencjalne i realne) wynikają z migracji, z niekontrolowanego przepływu ludności zmieniającego środowiska bezpieczeństwa obywatela i państwa.

Słowa kluczowe: *migracja, globalizacja, przestępczość zorganizowana, bezpieczeństwo, Unia Europejska*

WPROWADZENIE

Od wieków ludność przemieszcza się, szukając lepszego bytu i standardów życiowych (czynnik dominujący). Przemieszcza się także w celach turystycznych i rekreacyjnych (dzięki nowej technice szybciej i częściej). Migrująca ludność wpływa na wielkość populacji danego kraju oraz staje się istotnym elementem międzynarodowych stosunków ekonomicznych, gospodarczych, społecznych. Niestety, w ostatnim czasie migracja – jako zjawisko powszechne w zglobalizowanym świecie – stała się problemem nie tylko całej Unii Europejskiej, ale i reszty świata. Narastające fale migracji w Europie, Afryce i na Bliskim Wschodzie (masowe i niekontrolowane przemieszczanie się ludności) oraz nierozerwalnie związana z nią globalizacja (jako proces ekonomiczny) stwarzają zagrożenia dla całej społeczności międzynarodowej.

Wszyscy odczuwamy zmiany, jakie zachodzą na arenie międzynarodowej – konflikty społeczne, kryzysy ekonomiczne oraz konflikty związane z bezpieczeństwem. „Otwarcie się na niekontrolowaną falę migracyjną to ufundowanie sobie w przyszłości powstania ludności drugiej kategorii, pozbawionej prawa do legalnego pobytu, a w konsekwencji prawa do pracy, miejsca zamieszkania, edukacji, posługi religijnej, opieki zdrowotnej oraz ubezpieczeń społecznych”[1].

Migrująca ludność powoduje sprzeczność i zróżnicowania interesów, generując niebezpieczeństwa powstania konfliktów zbrojnych wewnętrznych

[1] http://www.defence24.pl/278545,kryzys-migracyjny-zagrozeniem-dla-systemu-obronnego-polski.

i zewnętrznych, ataków terrorystycznych, powstawania gryp przestępczych o międzynarodowym zasięgu.

Migracja wywołuje negatywne konsekwencje na rynku pracy. Zarówno dla krajów, z których osoby emigrują (utrata wykwalifikowanej siły roboczej, zmiany demograficzne), jak i krajów przyjmujących (napływ taniej siły roboczej mogącej budzić niepokoje wśród społeczności lokalnych – utrata miejsc pracy, brak wzrostu płac czy zmniejszony postęp technologiczny). Zdarza się też bardzo często tak, że napływająca ludność, szczególnie z krajów Bliskiego Wschodu i z krajów afrykańskich, nie ma żadnego wykształcenia oraz doświadczenia zawodowego, co stanowi poważny problem w asymilacji ze społeczeństwem.

Do czynników powodujących zwiększenie migracji możemy zaliczyć:

- rozpad państw wielonarodowych,
- prześladowania polityczne i religijne,
- konflikty – etniczne, kulturowe, religijne, zbrojne,
- katastrofy naturalne i niszczenie środowiska naturalnego,
- łamanie praw człowieka,
- poszukiwanie wolności i dobrobytu,
- bieda,
- niekontrolowany wzrost liczby ludności.

Rozpatrując kwestie zmian w wyniku migracji i globalizacji, musimy odpowiedzieć sobie na pytania: Co to jest globalizacja i czy zagraża bezpieczeństwu na świecie? Czy postęp technologiczny wraz z otwarciem granic nie przyczyni się do starć na tle religijnym, ekonomicznym oraz społecznym?

Narastająca współzależność między państwami, grupami państw sprawia, że problemy mające charakter regionalny bądź narodowy stały się problemami globalnymi, a zagrożenie bezpieczeństwa jednego państwa może stanowić zagrożenie dla całego regionu. „Współczesne pojęcie bezpieczeństwa jest polisemantyczne i w zasadzie nie ma dzisiaj obszaru działalności, zarówno niematerialnej, jak i materialnej, w której bezpieczeństwo nie odgrywałoby istotnej roli" (J. Świniarski, 2001, s. 41–42).

Dynamiczne przeobrażania powstające w wyniku globalizacji i niekontrolowanej migracji powodują zmiany w pojęciu bezpieczeństwa i obronności państwa w związku z nowymi zagrożeniami, takimi jak:

- wzrost przestępczości,
- powstawanie zalążków przestępczości zorganizowanej, międzynarodowej,
  - handel ludźmi,
  - powstawanie fundamentalizmu religijnego.

Zapewnienie bezpieczeństwa poszczególnym jednostkom i całemu społeczeństwu wymaga zidentyfikowania i opisania tychże zagrożeń, których źródła są różnorodne – zachowania konkretnych jednostek lub grup społecznych.

BEZPIECZEŃSTWO I OCHRONA

Bezpieczeństwo państwa i porządek publiczny to wartości, które podlegać powinny szczególnej ochronie, a usuwanie niepewności, obaw i strachu to tworzenie nowoczesnych systemów bezpieczeństwa oraz formułowania zasad ich funkcjonowania. Zapewnienie odpowiedniego bezpieczeństwa dla obywateli wraz z zachowaniem stabilnego i efektywnego systemu gospodarczego to zadania priorytetowe dla rządów większości rozwiniętych państw naszego globu, a w szczególności dla Unii Europejskiej, której Polska jest członkiem (wstępując w szeregi Unii Europejskiej, staliśmy się częścią systemu politycznego dążącego do wzrostu gospodarczego w ramach procesu globalizacji i konkurującego z innymi gospodarkami). A główne czynniki warunkujące rozwój polityki bezpieczeństwa nie powinny mieć charakteru militarnego, ale społeczny, ekonomiczny, kulturalny oraz ekologiczny (XXI wiek to w głównej mierze pojawiające się zagrożenia niemilitarne). Bycie bowiem w strukturach unijnych to uczestnictwo w procesach przemian ogólnoświatowych mających na celu podnoszenie dobrobytu oraz zapewnienie bezpieczeństwa społeczeństwu. To także ścisła współpraca organów ścigania w walce z przejawami transgranicznej, transnarodowej przestępczości zorganizowanej. Przestępczości często powstającej w wyniku napływu osób o niejasnym pochodzeniu i wątpliwej reputacji, uwikłanych bądź będących w szeregach organizacji terrorystycznych. Przestępczości stanowiącej największe zagrożenie dla krajów Wspólnoty.

Lepsza integracja bezpieczeństwa to wykorzystanie najdoskonalszych rozwiązań operacyjnych i innowacji technologicznych oraz eliminacja zbędnych wydatków na rzecz użyteczności zasobów pozwalających na likwidację organizacji przestępczych. To także odpowiednia polityka dotycząca bezpieczeństwa państwa, która określana jest przez specjalistów jako

najwyższa wartość i cel zapewniający ochronę najważniejszych spraw, takich jak trwałość, byt, suwerenność (zanikająca w erze globalizacji, której miejsce zajmuje międzynarodowy układ sił wyznaczający granice interesów i strategii narodowych mających na celu osiągnięcie gigantycznych dochodów) czy też tożsamość narodowa wraz z wolnością sumienia i wyznania.

„Dlatego głównym wyzwaniem i szansą działania państwa oraz warunkiem skutecznej i dojrzałej demokracji jest pobudzenie, mobilizowanie i włączanie wszystkich obywateli w działalność propaństwową i proobywatelską, której jednym z przejawów jest aktywność w dziedzinie bezpieczeństwa narodowego, polegająca nie tylko na utrzymaniu stanu bezpieczeństwa, ale również na pomnażaniu na poziomie lokalnym, narodowym i międzynarodowym" [M. Kubiak, M. Minkina (red. nauk.), s. 151].

ZJAWISKO GLOBALIZACJI – ZAGROŻENIEM DLA BEZPIECZEŃSTWA

„Globalizacja jest zjawiskiem wielowymiarowym, pochodna przemian cywilizacyjnych, rozwoju i integracji gospodarki, ale także wielu niekorzystnych zjawisk, głównie tych, które pogłębiają różnice rozwojowe. Właśnie te zjawiska rodzą wiele nieznanych zagrożeń, które mają wpływ na stan bezpieczeństwa międzynarodowego" (D.J. Mierzejewski, 2011, s. 50).

Z jednej strony globalizacja to wykorzystywanie dorobku ludzkości, rozwój środków produkcji, zwiększanie wszelkich inwestycji w skali światowej, nieograniczony handel bez granic, umiędzynarodowienie gospodarki, instytucje finansowe, nowo powstające technologie. Z drugiej – tej negatywnej – to nierówny rozwój gospodarczy oraz wielorakie zagrożenia:

1. Ekonomiczne. Globalizacja sprzyja zaostrzeniu rywalizacji między państwami, co wpływa na obniżenie cen, ale przy tym prowadzi do pogorszenia się jakości produktów. Może także blokować rozwój przemysłu narodowego w krajach rozwijających się. Migracja ekonomiczna odbywa się w celu poprawy jakości bytu i standardów życiowych, lecz bardzo często narusza ustalone zasady społeczne, powodując konflikty pomiędzy mieszkańcami a ludnością napływającą.
2. Ekologiczne (zmiana klimatu, brak dostępu do wody pitnej, niszczenie i zanieczyszczanie środowiska naturalnego).
3. Społeczne (upadek wartości, tradycji, solidarności społecznej, powiększanie marginesu ubóstwa, wykluczenia społecznego).

4. Bezpieczeństwa (powstawanie i ekspansja nowych rodzajów przestępczości na dotąd niespotykaną skalę przyjmująca nowe ponadgraniczne i zorganizowane postacie).
5. Polityczne (migracja polityczna). Zjawisko spowodowane konfliktami wewnętrznymi i zewnętrznymi oraz efekt wojen i walk obozów politycznych. Przykładem mogą być migracje pracownicze ludności palestyńskiej – przedmiot ostrych tarć dyplomatycznych o międzyrządowym charakterze, a także migranci ekonomiczni z Azji Południowo-Wschodniej, Afryki, rejonu Maghrebu stanowiący zagrożenie dla wielu dziedzin bezpieczeństwa państw, w których chcą się osiedlić. Według greckich władz większość, bo blisko trzech na czterech, imigrantów przybywających do tego kraju znalazło się na greckim terytorium z przyczyn ekonomicznych, a nie z powodu wojny (tylko niewielka grupa Syryjczyków spełnia wymagania dotyczące uzyskania azylu).

PROBLEMY ZWIĄZANE Z MIGRACJĄ I GLOBALIZACJĄ

„Niestety, globalizacja nie rozwiązuje konfliktów politycznych ani społecznych, sporów pomiędzy państwami oraz członkami miejscowych społeczności. Rywalizacja o bezpieczeństwo nadal jest grą o sumie zerowej, tzn. wzmocnienie przeciwnika oznacza osłabienie własnych możliwości. Należy więc temu przeciwdziałać”[2]. Globalizacja a wraz z nią gwałtowne tempo zmian stwarza zagrożenia (negatywne społeczne efekty globalizacji) i problemy dotąd niespotykane (groźne zachowania przeciwników globalizacji zagrażające stabilności gospodarczej mogące zakończyć się ogólnoświatowym kryzysem), przekształcając międzynarodową przestrzeń w jedno wspólne miejsce.

Migracja natomiast stwarza nowe obszary ryzyka i wywiera pośredni lub bezpośredni wpływ na bezpieczeństwo zarówno wewnętrzne, jak i zewnętrzne państwa, jak i/a może przede wszystkim na bezpieczeństwo społeczeństwa. Państwa z niepokojem patrzą na tworzące się w zbiorowości międzynarodowej transnarodowe korporacje spekulujące na rynkach finansowych, międzynarodowe instytucje, ugrupowania terrorystyczne, ponadnarodowe syndykaty przestępcze, rozrastające się mniejszości narodowe tworzące nową mapę przestępczości. Szerzący się nie tylko w Europie fundamentalizm religijny, szczególnie islamski dążący do utworzenia

[2] http://www.politykaglobalna.pl/2010/03/globalizacja-a-bezpieczenstwo/.

Państwa Islamskiego opartego na Koranie(fundamentalizm, który uważa nowoczesność za zło konieczne, z którym trzeba walczyć).

Problemem dla wielu krajów jest także asymilacja i bezrobocie wśród napływającej ludności. „Obecność dużej liczby imigrantów, zwłaszcza tych wywodzących się z innych kręgów kulturowo-cywilizacyjnych i słabo zintegrowanych ze społeczeństwem przyjmującym, może generować silne napięcia społeczne, nierzadko znajdujące swe ujście w protestach i zamieszkach ulicznych, stanowiących poważne naruszenia porządku publicznego" (R. Raczyński, 2/2015).

Powstające nowe formy przestępstw wypierają tradycyjną przestępczość, a proces globalizacji skłania państwa do demokratyzowania gospodarek. Grupy przestępcze wchodzą do zglobalizowanego systemu i nie są już zjawiskiem marginalnym. Otwieranie granic powoduje niekontrolowany przepływ usług, towarów, technologii, informacji i ludzi. „Novum polega na zmianach ilościowych, ale i jakościowych. Konflikty pomiędzy państwami, przestępczość zorganizowana, terroryzm czy nielegalna imigracja nie są przecież czymś nieznanym, jednakże zmianie uległa zarówno ich skala i zdolność zagrożenia bezpieczeństwa państwa, jak również sposób wpływu na bezpieczeństwo i funkcjonowanie państw związany z procesami globalizacyjnymi, wykorzystaniem struktur sieciowych i nowoczesnych technologii" (T.R. Aleksandrowicz, 2011, s. 25).

Rośnie współzależność między najniebezpieczniejszymi rodzajami przestępstw: terroryzmem, handlem narkotykami, praniem brudnych pieniędzy, przestępstwami gospodarczymi i cyberprzestępczością. A gwałtowny postęp technologiczny sprawia, że świat stał się o wiele mniejszy, wzajemnie zależny i wrażliwszy niż kiedykolwiek wcześniej oraz coraz bardziej oddziaływujący na życie każdego z nas.

„Następstwa globalizacji są rozległe i różnorodne, zarówno dla kształtu (elementów, cech) porządku międzynarodowego, jak i podstawowych uczestników stosunków międzynarodowych – państw i tworzących je społeczeństw oraz narodów, lecz także dla podmiotów niepaństwowych, takich jak: międzynarodowe ugrupowania gospodarczo-polityczne, organizacje międzynarodowe, korporacje transnarodowe oraz organizacje pozarządowe"[3].

[3] http://stosunki-miedzynarodowe.pl/bezpieczenstwo/1089-wplyw-globalizacji-i-regionalizacji-na-bezpieczenstwo-miedzynarodowe.

WZROST ZORGANIZOWANEJ PRZESTĘPCZOŚCI W WYNIKU ZMIAN MIGRACYJNYCH I GLOBALIZACYJNYCH

„Sam proces globalizacji i integracji, prócz pozytywów rozwoju cywilizacji, wzrostu dobrobytu, dostarcza społeczności także skutki negatywne, m.in. pod postacią asymetrii gospodarczej, technologicznej, społecznej i kulturowej. Asymetrie te należy widzieć w obszarze całych organizacji i ich otoczeniu oraz w sferze sojuszy i porządku międzynarodowego. Globalny wymiar asymetrii przekłada się także na bezpieczeństwo narodowe i międzynarodowe w sensie fizycznym i socjologicznym oraz psychologicznym, w kontekście działania podmiotów, wykorzystywanych technologii, systemu wartości czy postrzegania perspektywy" (W. Pokruszyński, 2010, s. 68).

Przestępczość zorganizowana to zjawisko kryminalne o zasięgu międzynarodowym, niepodlegające ograniczeniom historycznym i terytorialnym, dla którego granice państw nie stanowią jakiejkolwiek bariery, przybierające bardzo często formy przestępczości gospodarczej i narkotykowej.

„Organizacje te i ich działania, nie tylko podważają działanie zdrowej gospodarki kontynentu (i tak osłabionej kryzysem gospodarczym), ale stanowią zagrożenie dla podstawowych zasad Unii Europejskiej, zobowiązanej do utworzenia »obszaru wolności, bezpieczeństwa i sprawiedliwości«"[4].

Przestępczość zorganizowana jest wypadkową zachodzących procesów w społeczeństwie, stymulowanych w większości zmianami procesów globalizacyjnych.

„Zorganizowane grupy przestępcze, składające się z członków, są elementami życia społecznego, niedającymi się wyizolować z otaczającego ich środowiska oraz współistniejącymi z legalnymi formami organizacji życia społecznego w różnych jego obszarach" (O. Krajniak, 2011, s. 15).

Zjawisko przestępczości zorganizowanej przejawia się przez:

a) istnienie trwałych struktur organizacyjnych prowadzących planowaną działalność przestępczą, ukierunkowaną na osiągnięcie maksymalnych korzyści materialnych,
b) zawodowy, nieograniczony terytorialnie charakter jej działalności przestępczej,

[4] http://www.cafebabel.pl/polityka/artykul/mala-europa-globalna-bogata-i-nieagresywna-mafia-europejska.html.

c) bezwzględną hermetyczność wewnętrzną i zewnętrzną struktur, używanie przemocy, szantażu i korupcji (W. Mądrzejowski, 2008, s. 36).

„Międzynarodowe grupy i organizacje przestępcze, wykorzystując postępujące ułatwienia w zakresie komunikacji, podróżowania, przepływu kapitału; dóbr i usług, prowadzą swą działalność w skali całego świata. Łączą się w nieformalne związki kapitałowe, komasują produkcję dla minimalizacji kosztów”[5].

Cele tych grup to osiąganie dochodów na nielegalnym obrocie towarami bądź też handlu ludźmi oraz osiąganie niczym nieograniczonej władzy (politycznej, gospodarczej). Cechy zorganizowanej przestępczości przejawiają się między innymi w odpowiednich sposobach działania i bycia, takich jak:

1) hierarchiczność (zarządzanie dużą grupą, od której wymaga się bezwzględnej lojalności i posłuszeństwa, zdrada kończy się śmiercią zdrajcy),
2) monopolistyczna kontrola lub ustanowienie sfer wpływu,
3) rządzenie według określonych reguł i regulacji,
4) wywieranie wpływu na rządzących oraz organy ścigania (otrzymywanie pomocy od skorumpowanych pracowników między innymi administracji państwowej i prawników),
5) korzystanie z pomocy specjalistów z określonych dziedzin gospodarki (kontrolowani przez przestępców doradcy, fachowcy wykrywają wszelkie luki prawne pozwalające prowadzić działalność przestępczą przez pewien okres, głównie w sektorach związanych z finansami i gospodarką, gdy nielegalne działania Policja odkrywa dopiero po pewnym czasie – tzn. w trakcie działalności operacyjno-procesowej).

Przestępczość zorganizowana działająca na zasadzie głębokiej konspiracji i terroru z roku na rok zatacza coraz szersze kręgi, z którymi krajowe organy ścigania w sposób niewystarczający sobie radzą, ponieważ nie dysponują odpowiednimi do tego środkami.

A „działalność tych grup grozi nie tylko utratą suwerenności państw, osłabieniem władzy, całkowitą utratą kontroli przez organy państwowe i podkopuje demokratyczne zasady instytucji publicznych, lecz ma także katastrofalne skutki gospodarcze w postaci destabilizacji finansów państwa

[5] http://www.kulturaswiecka.pl/node/74.

i obywateli. Zagrożenie to dotyczy wszystkich krajów, w tym również rozwijających się oraz przechodzących transformację ustrojową z gospodarki sterowanej centralnie do wolnorynkowej”[6].

Holdingi przestępcze działają na całym świecie, korzystając często z opóźnień prawodawstwa, poprzez swoje działania starają (próbują) się wszelkimi metodami oraz środkami obniżać, opóźniać działania organów ścigania, a także organów sprawiedliwości w wyegzekwowaniu prawa i ukaraniu sprawców.

„Dużo groźniejsze dla systemu bezpieczeństwa państw są natomiast długofalowe skutki aktywności transgranicznej przestępczości zorganizowanej, których źródeł upatrywać należy w tzw. wtórnym oddziaływaniu grup przestępczych. Biorąc pod uwagę to, iż w wyniku nielegalnej działalności zorganizowane grupy przestępcze osiągają określone korzyści materialne, trzeba założyć także, że zdobyte przez nie zasoby mogą i są wykorzystywane do wpływania na sytuację poszczególnych krajów, ich gospodarek, a w konsekwencji także na ich bezpieczeństwo” (P. Kuzior, 12 (54), 2008). Albowiem wraz z rozwojem przestępczości zorganizowanej rozwijają się także formy przestępczości z nią związane, między innymi: nielegalna migracji, handel ludźmi, korupcja, pranie brudnych pieniędzy, przestępczość gospodarcza, narkotykowa oraz przemyt. „Występują tu grupy przestępcze o wysoko zorganizowanych, niezwykle sprawnych strukturach. Zajmują się one przede wszystkim przemytem na dużą skale, fikcyjnym tranzytem, eksportem i reeksportem dużych ilości towarów, zwłaszcza alkoholu, papierosów, sprzętu elektronicznego oraz samochodów” (P. Kozłowski, 2004, s. 78).

Około połowy nielegalnie przekraczających granice korzysta z pomocy zorganizowanych grup przestępczych zajmujących się przerzutem ludzi, co w znaczący sposób przyczynia się do wzrostu zagrożenia bezpieczeństwa wewnętrznego UE.

„W strukturze każdej grupy przerzutowej można wyodrębnić trzy elementy:

1) mafia – organizuje i ochrania przerzut. Osoby tworzące tę grupę to ludzie różnych narodowości, na najniższym szczeblu są tu agenci, którzy zdobywają «klientów»;

[6] Problems and Dangers Posed by Organised Transnational Crime in the Various Regions of the Word, dokument NZ, E/CONF.88/2, 18 sierpnia 1994, s. 8.

2) pogranicze – zespoły dwunarodowościowe lub osoby znające język przerzucanej grupy i topografię terenu;
3) ludność miejscowa – współpracownicy lokalni (np. wewnątrz Polski załatwiają przerzucanym migrantom schronienie, wyżywienie, tymczasową pracę, transport i dokumenty)"[7].

Nielegalny przepływ ludności wynika przede wszystkim ze względów ekonomicznych (różnica w poziomie rozwoju życia pomiędzy bogatą Północą a biednym Południem), czystek etnicznych, katastrof humanitarnych, wojen domowych (Syria) oraz konfliktów wewnętrznych, a skala procederu jest trudna do oszacowania. Niekontrolowany przemyt ludzi zmienia obraz całej Unii Europejskiej, w tym także Polski. Każda fala uchodźców przybywa z różnych stron świata, z różnych kultur mających swoją specyfikę bycia, a raz uruchomione strumienie nielegalnych uchodźców trudno zatrzymać.

Nadmierny napływ ludności może destabilizować bezpieczeństwo wewnętrzne kraju oraz zakłócać życie społeczeństwa, powodując konflikty społeczne na tle narodowościowym, czego przykładem może być dzisiejszy problem nielegalnych emigrantów z krajów afrykańskich i krajów Bliskiego Wschodu. Nielegalny napływ imigrantów prowadzi bardzo często do wzrostu nastrojów radykalnych, rasistowskich i ksenofobicznych. Powoduje także rozwój różnych form ekstremizmu politycznego, stanowiącego bardzo poważne wyzwanie dla bezpieczeństwa i porządku publicznego państwa. Wiąże się to również ze wzrostem ataków terrorystycznych, rozwojem fundamentalizmu religijnego oraz separatyzmu etnicznego.

Także Polska traktowana jest przez emigrantów jako kraj tranzytowy i może stać się bazą logistyczną lub miejscem szkoleń dla terrorystów. Istnieje bowiem uzasadnione podejrzenie, że wśród tysięcy osób przekraczających granice część z nich może być powiązana z ekstremistycznymi organizacjami terrorystycznymi mogącymi planować zamachy lub w przyszłości zostać przez nich zwerbowana. Oprócz tego część nielegalnie przekraczających granice może zasilić zorganizowane grupy przestępcze lub samemu je tworzyć, stanowiąc zagrożenie dla bezpieczeństwa oraz sta-

[7] http://www.rocznikbezpieczenstwa.dsw.edu.pl/fileadmin/user_upload/wydawnictwo/RBM/RBM_artykuly/2006_18.pdf.

bilności państwa. Zorganizowane grupy przestępcze spoza UE odgrywają kluczową rolę w przemycie narkotyków (rozprowadzanie środków odurzających wśród tysięcy imigrantów w krajach ich pobytu) oraz przemycie i handlem ludźmi.

„Migracje to również zderzenie wielu kultur, które mogą prowadzić do nowych zjawisk patogennych, z którymi współczesne społeczeństwa europejskie nie miały od dawna lub nigdy wcześniej do czynienia (jak np. honorowe zabójstwa kobiet, małżeństwa małoletnich czy odnowienie instytucji wróżbity)" (J. Balicki, P. Stalker, 2006, s. 260).

BEZPIECZEŃSTWO PAŃSTWA A PODMIOT NIEPAŃSTWOWY

Podmiot niepaństwowy to przeważnie przeciwnik bardzo niebezpieczny, zagrażający sprawnemu działaniu struktur państwowych oraz szybko dostosowujący się do zmian zachodzących w kraju, mogący wykorzystywać ludność migrującą do swoich celów (przerzut członków organizacji mających za zadanie utworzenie bądź rozszerzenie struktur organizacji terrorystycznych oraz przygotowanie zamachów). Przeciwnik szybko reagujący na działania prowadzone przeciwko niemu, tworzący własne sposoby przeciwdziałania, penetrując nie tylko administrację, ale także służby odpowiedzialne za bezpieczeństwo państwa (policja, służby specjalne, wojsko).

Zapobieganie działaniom podmiotów niepaństwowych naruszającym dobro państwa i obywateli jest bardzo trudne, ponieważ skala działania jest bardzo duża, a metody trudne do wykrycia, jak również nieznany jest czas i miejsce ataku (działania organizacji terrorystycznych). Podmioty te to głównie organizacje o charakterze przestępczym lub terrorystycznym (transnarodowe organizacje przestępczości zorganizowanej i transnarodowe organizacje terrorystyczne, np. Al-Kaida, ETA, PIRA) oraz korporacje międzynarodowe (środki finansowe tych podmiotów przewyższają niekiedy budżet narodowy poszczególnych państw), swoim zasięgiem obejmujące niekiedy obszar całego świata.

PODSUMOWANIE

Globalizacja i migracja wywiera istotny wpływ na funkcjonowanie porządku publicznego, funkcjonowanie struktur bezpieczeństwa narodowego oraz wpływa na jego możliwości działania.

Ciągła i trwała współpraca w dziedzinie bezpieczeństwa umożliwi monitorowanie, zapobieganie oraz eliminowanie przestępczości powstającej w wyniku nielegalnej migracji na terenie Europy. Natomiast zwalczanie transnarodowej przestępczości to wspólne, międzynarodowe działania, a nie działania w ramach poszczególnych krajów.

Przeciwdziałania muszą być podejmowane z odpowiednim bezpiecznym wyprzedzeniem, chroniąc Unię i jej zewnętrzne granice. „Zapobieganie (tzw. profilaktyka) to działania zmierzające do eliminowania określonego zjawiska lub jego skutków uznawanych za niepożądane przez podmiot podejmujący te działania. Celem zapobiegania jest zmuszenie podmiotów do przestrzegania norm grupowych" (Kryminologia. Repetytorium, 2013, s. 163). A budowanie odpowiednich warunków poprzez nietworzenie nowych podziałów w Europie, dobre rządy krajowe oraz zapobieganie wszelkim konfliktom związanym z nielegalną migracją i przestępczością zorganizowaną wpłynie korzystnie na bezpieczeństwo Unii Europejskiej i jej obywateli.

Bibliografia

Aleksandrowicz T.R. (2011). *Bezpieczeństwo w Unii Europejskiej.* Warszawa.

Balicki J., Stalker P. (2006). *Polityka imigracyjna i azylowa. Wyzwania i dylematy*. Warszawa.

Kozłowski P. (2004). *Gospodarka nieformalna w Polsce*. Warszawa.

Krajniak O. (2011). *Zorganizowane grupy przestępcze*. Warszawa.

Kryminologia. Repetytorium (2013). Wydanie 3. Warszawa.

Kubiak M., Minkina M. (red. nauk.), (2011). *Współczesne bezpieczeństwo narodowe i międzynarodowe. Uwarunkowania, relacje, zależności*. Siedlce.

Mądrzejowski W. (2008). *Przestępczość zorganizowana, system zwalczania*. Warszawa.

Mierzejewski D.J. (2011). *Bezpieczeństwo europejskie w warunkach przemian globalizacyjnych*. Toruń.

Pokruszyński W. (2010). *Teoretyczne aspekty bezpieczeństwa*. Józefów.

Problems and Dangers Posed by Organised Transnational Crime in the Various Regions of the Word, dokument NZ, E/CONF.88/2, 18 sierpnia 1994, s. 8.

Raczyński R. (2015). *Wpływ migracji międzynarodowych na bezpieczeństwo wewnętrzne państwa*, „Bezpieczeństwo. Teoria i Praktyka", nr 2.

Sztumski J. (1996). *Elity nowoczesnych państw*, [w:] *Z zagadnień socjologii polityki*, t. 1, L.W. Zacher (red.). UMCS, Lublin.

Świniarski J. (2001). *Bezpieczeństwo w perspektywie socjologicznej*. Rzeszów – Tyczyn.

Źródła internetowe

Kryzys migracyjny zagrożeniem dla systemu obronnego Polski, http://www.defence24.pl/278545,kryzys-migracyjny-zagrozeniem-dla-systemu-obronnego-polski [data dostępu: 10.11.2016].

Mala-Europa: globalna, bogata i nieagresywna mafia europejska, http://www.cafebabel.pl/polityka/artykul/mala-europa-globalna-bogata-i-nieagresywna-mafia-europejska.html [data dostępu: 02.11.2016].

Piasecki R., *Procesy globalizacji a interesy państw narodowych. Konsekwencje dla Polski*, http://www.kulturaswiecka.pl/node/74 [data dostępu: 25.02.2016].

Studzińska M., *Nielegalna imigracja – nowe wyzwania dla bezpieczeństwa europejskiego*, http://www.rocznikbezpieczenstwa.dsw.edu.pl/fileadmin/user_upload/wydawnictwo/RBM/RBM_artykuly/2006_18.pdf [data dostępu: 02.11.2016].

Wołejko P., *Globalizacja a bezpieczeństwo*, http://www.politykaglobalna.pl/2010/03/globalizacja-a-bezpieczenstwo/ [data dostępu: 16.03.2016].

Wpływ globalizacji i regionalizacji na bezpieczeństwo międzynarodowe, http://stosunki-miedzynarodowe.pl/bezpieczenstwo/1089-wplyw-globalizacji-i-regionalizacji-na-bezpieczenstwo-miedzynarodowe [data dostępu: 25.10.2016].

ALEKSANDER OLEJNIK
Wydział Mechatroniki i Lotnictwa
Wojskowa Akademia Techniczna
im. Jarosława Dąbrowskiego
aleksander.olejnik@wat.edu.pl

EDWARD KOŁODZIŃSKI
Wydział Mechatroniki i Lotnictwa
Wojskowa Akademia Techniczna
im. Jarosława Dąbrowskiego
edward.kolodzinski@wat.edu.pl

ROBERT ROGÓLSKI
Wydział Mechatroniki i Lotnictwa
Wojskowa Akademia Techniczna
im. Jarosława Dąbrowskiego
robert.rogulski@wat.edu.pl

ŁUKASZ KISZKOWIAK
Wydział Mechatroniki i Lotnictwa
Wojskowa Akademia Techniczna
im. Jarosława Dąbrowskiego
lukasz.kiszkowiak@wat.edu.pl

TOMASZ ŁĄCKI
Wydział Mechatroniki i Lotnictwa
Wojskowa Akademia Techniczna
im. Jarosława Dąbrowskiego
tomasz.lacki@wat.edu.pl

IRENEUSZ KRAMARSKI
Hornet

WYBRANE PROBLEMY PROTOTYPOWANIA BEZZAŁOGOWEGO STATKU POWIETRZNEGO KLASY MINI

SOME PROBLEMS OF MINIATURE UNMANNED AIRCRAFT VEHICLE PROTOTYPING

ABSTRACT

In the paper some fundamental problems concerning miniature Unmanned Aerial Vehicle (miniUAV) prototyping were presented. As a result of undertaking analysis and designing the proper aerodynamic and structural layout was fixed. The geometric 3-dimensional model was developed in advanced CAD environment. Then the cycle of some technological techniques was presented to show the manufacturing process prescribed for miniUAV airframe parts. The main subsystems of on-board equipment were described and the essence of the whole avionic system integration was explained too. A methodology of UAV flight quantities validation was presented due to the technical features of applied control system. The complete system set was specified at the end.

Keywords: *miniature unmanned aerial vehicle (miniUAV), aircraft design and manufacturing, on-board systems integration, UAV camera system*

STRESZCZENIE

W artykule zaprezentowano wybrane problemy związane z prototypowaniem bezzałogowego statku powietrznego klasy mini (mini-BSP). W ramach prac analityczno-projektowych uzgodniono układ aerodynamiczno-konstrukcyjny minisamolotu i opracowano jego model geometryczny w środowisku CAD. Zaprezentowano cykl czynności technologicznych uruchomionych w procesie wytwarzania elementów konstrukcji płatowca. Pokrótce opisano zasadnicze podsystemy wyposażenia pokładowego oraz wyjaśniono istotę integracji systemu awionicznego. Przedstawiono metodykę walidacji własności lotnych minisamolotu w kontekście możliwości zastosowanego układu automatycznego sterowania. Określono ostateczną kompletację gotowego demonstratora systemowego.

Słowa kluczowe: *bezzałogowy statek powietrzny klasy mini (mini-BSP), projektowanie i wytwarzanie samolotów, integracja systemów pokładowych, miniaturowe kamery pokładowe*

WPROWADZENIE

W ciągu ostatnich kilkunastu lat badania w zakresie projektowania, automatyzacji i niezawodności eksploatacyjnej bezzałogowych statków powietrznych (BSP, ang. UAV) zostały znacząco zintensyfikowane. Własne projekty badawcze w tej dziedzinie lotnictwa prowadzą zarówno kraje mocno rozwinięte (USA, Izrael, Wielka Brytania), jak i te o znacznie skromniejszych budżetach i mniejszym potencjale naukowo-technologicznym (Grecja, Turcja, Jordania). Do grona producentów bezzałogowych aparatów latających należą także państwa azjatyckie, z racji położenia, wielkości i zaludnienia aspirujące do roli światowych mocarstw (Chiny, Indie, Pakistan, Iran). W 2010 roku zidentyfikowano prawie 1200 projektów różnego rodzaju aparatów bezzałogowych, przy czym liczba ta dotyczyła zarówno obiektów w fazie badawczej, jak i już wdrożonych do eksploatacji („UAS: The Global Perspective", s. 165).

W związku z różnorodnością i wielozadaniowością bezzałogowych aparatów funkcjonuje pewna klasyfikacja tych obiektów. Najczęściej klasyfikuje się je ze względu na:

- wielkość i osiągi – uwzględniając takie parametry, jak: masa, zasięg, długotrwałość lotu, osiągalny pułap, obciążenie skrzydła, typ napędu,
- funkcjonalność misyjną – rozróżniając aparaty: obserwacyjne, bojowe, wielozadaniowe, pionowego startu i lądowania, komunikacyjno-przekaźnikowe, transportowe (Arjomandi, 2006).

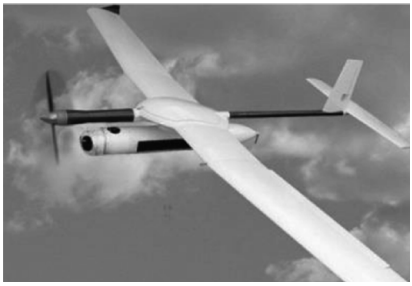
Organizacja UVS International rozróżnia statki bezzałogowe taktyczne, strategiczne oraz specjalnego przeznaczenia („UAV/UAS classification", 2010). Aparaty taktyczne, czyli przeznaczone do lotów rozpoznawczych w zakresie troposfery, sklasyfikowane są ze względu na wielkość i osiągi w dziesięciu kategoriach (μ, mini, CR, SR, MR, MRE, LADP, LALE, MALE, HALE).

Platformy klasy mini są zaszeregowane jako jedne z najmniejszych, jednakże ilościowo stanowią około 30% liczby wszystkich aktualnie realizowanych projektów BSP. W kontekście powyższego podziału przypisywane im cechy kryterialne to:

- zasięg – do około 12 km,
- pułap praktyczny – 300–400 m,
- długotrwałość lotu – do około 2 h,
- masa startowa – nie większa niż 25 kg (zazwyczaj jednak w granicach 4–7 kg).

Ilustracja 1.
Samoloty klasy mini będące pierwowzorem dla koncepcji płatowca mini-BSP Rybitwa: a) Skylark II – Elbit Systems, b) Skyblade III – ST Aerospace1, c) Kiwit – AT Group

a)



b)

c)

Źródła: Elbit Systems – Skylark® I LE – mini UAS, ST Aerospace – Skyblade III, Kiwit – Mini Unmanned Arborne System

Samoloty bezzałogowe tego typu ze względu na „modelarskie" gabaryty i małą masę użyteczną (*payload*) są niezbyt drogim asortymentem w globalnej skali produktów przemysłu lotniczego. Niezbyt wysokie wymagania technologiczne, ogólna dostępność komponentów konstrukcyjnych, napędowych i wyposażeniowych, niewysoka cena pozyskania zarówno elementów składowych, jak i produktu finalnego – wszystkie te powody sprawiają, iż wykorzystanie mini-BSP w różnych dziedzinach działalności staje się coraz bardziej powszechne i oczywiste. W zastosowaniach militarnych minisamolot wyposażony w kamerę TV i cichy napęd elektryczny to doskonały instrument rozpoznania dla pododdziału szczebla plutonu/kompanii bądź też samodzielnej grupy specjalnej. Istnieje wiele aparatów dedykowanych do tego typu misji, zróżnicowanych ze względu na układ aerodynamiczno-konstrukcyjny, rodzaj i konfigurację zespołu napędowego czy sposób montażu wyposażenia misyjnego.

Oprócz zastosowań stricte wojskowych mini-BSP są coraz częściej wykorzystywane w przedsięwzięciach cywilnych związanych z działalnością zarówno instytucji państwowych, jak i prywatnych przedsiębiorstw. Do potrzeb związanych z działalnością cywilną można zaliczyć m.in.:

- monitorowanie obszarów dotkniętych klęskami żywiołowymi (pożarem, powodzią, suszą),
- dozorowanie obszarów leśnych i areałów uprawnych,
- dozorowanie dużych zbiorowisk ludzkich w trakcie plenerowych wydarzeń okolicznościowych,
- monitoring turystycznych akwenów w okresie wzmożonej rekreacji,
- obserwacja fragmentów infrastruktury lądowej o szczególnym znaczeniu strategicznym celem lokalizacji i identyfikacji ewentualnych katastrof technicznych (zakłady przemysłowe, elektrownie, porty, platformy wiertnicze, rurociągi itp.),
- dozorowanie lądowych szlaków i węzłów komunikacyjnych,
- patrolowanie obszarów przygranicznych (pod kątem przemytu ludzi i towarów).

Wymienione wyżej, a także inne miejsca i sytuacje mogą być związane z wystąpieniem różnego typu zagrożeń, takich jak skażenie chemiczne, zagrożenie pożarowe, wypadki komunikacyjne, utonięcia lub nawet skrajne zagrożenia działaniami sabotażowymi i terrorystycznymi. W takich właśnie

okolicznościach wykorzystanie mini-BSP jako dyskretnego i nieinwazyjnego środka pozyskania informacji wydaje się celowe i jak najbardziej uzasadnione.

W artykule zaprezentowano wybrane problemy związane z opracowaniem autorskiej koncepcji systemu rozpoznawczego opartego na miniaturowym samolocie bezzałogowym. Prace realizowano w Instytucie Techniki Lotniczej WAT w latach 2010–2012 w ramach projektu badawczego rozwojowego. Docelowe zadanie polegało na zaprojektowaniu i zbudowaniu demonstratora systemu zdolnego do realizacji misji rozpoznawczych w lotach autonomicznych na korzyść administracyjnych instytucji państwowych, takich jak Policja, Straż Pożarna, Straż Graniczna, Straż Leśna.

PROTOTYPOWANIE W KONTEKŚCIE WYMAGAŃ MAŁYCH APARATÓW BEZZAŁOGOWYCH

Proces opracowania prototypu miniaturowego samolotu bezzałogowego musi uwzględniać dość specyficzne wymagania stawiane małym obiektom latającym, wynikające zarówno z ograniczeń konstrukcyjnych, jak i dedykowanych zadań misyjnych. Celem procesu ma być zbudowanie struktury nośnej niewielkich rozmiarów, spełniającej wymagania aerodynamiczne, wytrzymałościowe oraz standardowe kryteria stateczności i sterowności. Ze względu na rozmiar docelowej platformy nośnej zadanie wydaje się dość banalne i mogłoby stanowić wyzwanie dla przeciętnego modelarza. W zasadzie wielkość samolotu, stosowane materiały konstrukcyjne, rozwiązania układu sterowania w dużej mierze bazują tu na doświadczeniach modelarskich. Jednak ze względu na kosztowne urządzenia awioniczne instalowane na pokładzie oraz przeznaczenie systemu do lotów na dość sporych odległościach, także nad terenami zurbanizowanymi, konieczne są dodatkowe zabiegi i starania gwarantujące niezawodność funkcjonowania i bezpieczeństwo lotu.

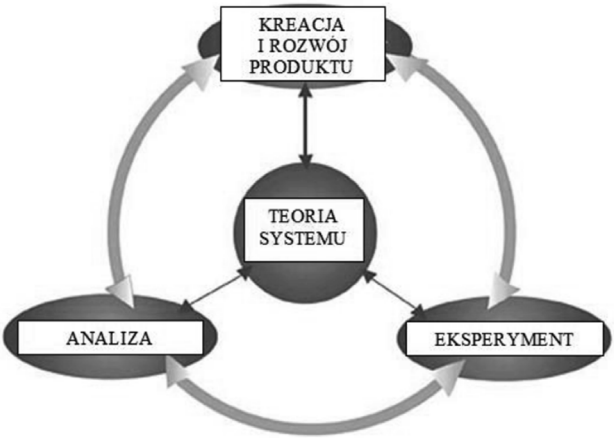
Płatowce minisamolotów bezzałogowych muszą spełniać pewne określone z góry wymagania, umożliwiające ich użytkowanie w warunkach zmiennych i różnorodnych obciążeń aeromechanicznych, zróżnicowanych oddziaływań atmosferycznych oraz cykliczności procesów eksploatacyjnych (pakowanie i rozwijanie systemu, starty, lądowania, montaże i demontaże elementów). Do wymagań najistotniejszych z punktu widzenia użytkownika można zaliczyć:

- odporność na obciążenia w locie (aerodynamiczne, masowe),

- odpowiednie sztywności zespołów płatowcowych wykluczające wystąpienie zjawisk aerosprężystych,
- odporność na chwilowo występujące gwałtowne przeciążenia w fazach lądowania (wyhamowanie spadochronowe, przyziemienie),
- odporność elementów na obciążenia związane z brutalną obsługą (przypadkowe szarpnięcia, uderzenia, naciski na powierzchnie pokryciowe),
- sztywność i powtarzalność niepogorszonego funkcjonowania połączeń montażowych (w szczególności brak tendencji do wyrabiania luzów).

Przyjmuje się, że płatowiec bezzałogowego samolotu klasy mini powinien być zdatny do użytkowania w cyklu kilkuset (zwykle od 100 do 400) startów i lądowań.

Rysunek 1.
Diagram powiązań przyczynowo-skutkowych determinujących kreację nowego produktu technicznego



TEORIA SYSTEMU – założenia, modele, parametry, ograniczenia;

ANALIZA – zdefiniowanie obszaru poszukiwań, studium przypadku, przegląd możliwych rozwiązań, projekt, obliczenia, symulacje;

EKSPERYMENT – pomiary fizyczne, próby i testy wg wytyczonych programów i procedur;

KREACJA I ROZWÓJ PRODUKTU – **prototypowanie**, transfer technologii, wytwarzanie, ocena ekspercka, metodyka eksploatacji, modernizacja

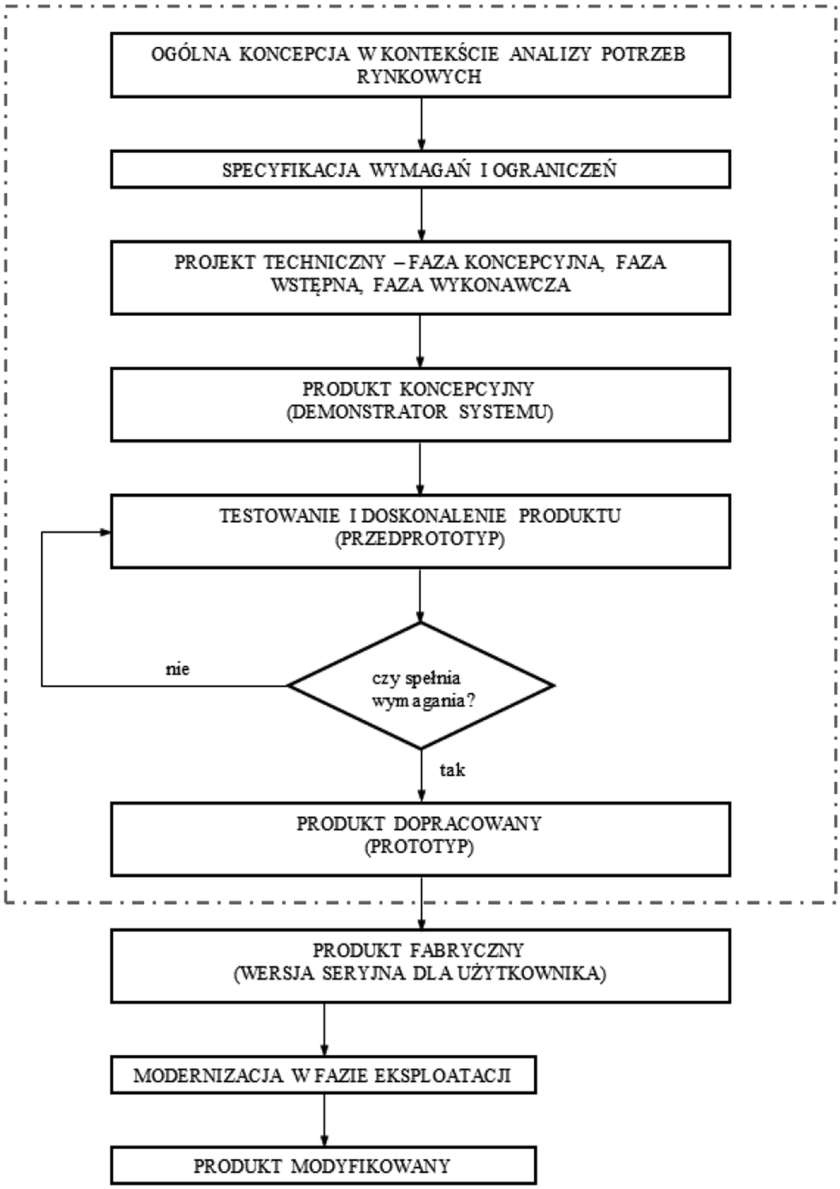
Źródło: Na podstawie „Center for the Management of Information (CMI) – The University of Arizona", 2002

Prototypowanie jest procesem budowy urządzenia, systemu lub konstrukcji w oparciu o koncepcję sformułowaną w projekcie i udokumentowaną stosownymi obliczeniami, badaniami modelowymi i doświadczalnymi. W odniesieniu do prototypowania przytoczyć można zmodyfikowany nieco schemat obrazujący cykl powstawiania produktu („Aircraft Design", 2001). W oparciu o wiedzę teoretyczną, przy uwzględnieniu informacji nabytych w trakcie analiz obliczeniowych i symulacyjnych oraz badań doświadczalnych następuje kreacja i doskonalenie cech wytwarzanego produktu finalnego. W tym mechanizmie prototypowanie jest pierwszym procesem etapu kreacyjno-rozwojowego, stanowiącego skutek sprzężenia bazowej wiedzy teoretycznej z wiedzą pozyskaną w konsekwencji wykonanych prognoz, obliczeń i badań.

W kontekście doskonalenia cech kreowanego produktu prototypowanie jest procesem iteracyjnym. W trakcie określania wymagań gromadzone są informacje o systemie pozyskiwane poprzez analizy, obserwacje i eksperymenty. W wyniku porównania cech pożądanych, sprecyzowanych w założeniach z cechami faktycznymi zaobserwowanymi w sprawdzanym produkcie modelowym (prototypie) dokonywana jest ocena pod kątem takich własności, jak zgodność parametrów, funkcjonalność, jakość, podatność obsługowa. Jeśli któraś z tych własności nie spełnia stosowanego w ocenie kryterium, zespół wprowadza domniemaną poprawkę, a zmodyfikowany produkt – kolejny prototyp – poddawany jest nowej serii sprawdzeń. Użytkowanie produktu finalnego przez docelowego odbiorcę może być konsekwencją niejako dwóch ścieżek – wdrożenia produktu podstawowego lub modernizacji produktu wdrożonego pod kątem poprawy jego własności funkcjonalnych, estetycznych lub też eksploatacyjnych. Uwzględniono to w schemacie blokowym wykreowania produktu technicznego (rysunek 2.) opracowanym na bazie diagramu tradycyjnego prototypowania.

Projekt systemu rozpoznawczego z bezzałogowym minisamolotem dopracowany został do poziomu demonstratora technologii. W odniesieniu do samolotu wykazane w schemacie fazy prototypowania można scharakteryzować nieco bardziej szczegółowo (rysunek 2).

Rysunek 2.
Schemat blokowy kreowania produktu technicznego; fazy identyfikowane w ramach procesu tradycyjnego prototypowania zakreślone przerywaną obwiednią



Źródło: Opracowanie własne w ramach publikacji „Wybrane aspekty prototypowania płatowca…", 2010

Ogólna koncepcja – typ statku powietrznego – stałopłat (samolot), klasyczny układ aerodynamiczny – proste skrzydło wolnonośne, tradycyjne usterzenie ogonowe ze sterem kierunku i wysokości, podwieszany zasobnik ładunkowy (gondola), typ napędu – elektryczny ze śmigłem ciągnącym, podział technologiczny – możliwość szybkiego montażu i demontażu.

Specyfikacja wymagań i ograniczeń (wstępne założenia taktyczno-techniczne) – maksymalna masa startowa – 10 kg; orientacyjne prędkości charakterystyczne (minimalna, przelotowa, maksymalna) – 40, 70, 120 km/h; maksymalny promień działania – 10 km; długotrwałość lotu – 90 min; pułap praktyczny – 100–400 m, maksymalne wymiary gabarytowe (rozpiętość, długość) – 3,0, 2,0 m; pożądany zakres wartości ciągu statycznego – 6–17 N, metoda startu – wyrzut z ręki, metoda lądowania – klasyczna lub ze spadochronem, podział technologiczny umożliwiający szybki montaż i demontaż, przechowywanie – mobilny kontener.

Projekt techniczny – zapis konstrukcji, obliczenia, analizy, symulacje, dobór technologii, opracowanie dokumentacji (z poziomem zaawansowania adekwatnym do realizowanej fazy projektu).

Demonstrator technologii – pierwsza postać fizyczna samolotu gotowego do podjęcia misji demonstrująca kluczowe cechy i funkcjonalności.

Doskonalenie produktu – badania przedprototypów w locie pod kątem funkcjonalności podsystemów, własności lotnych, osiągów, wpływu czynników eksploatacyjnych.

Prototyp – ostatecznie dopracowany samolot posiadający pożądane cechy i spełniający wymogi wstępnych założeń taktyczno-technicznych, gotowy do produkcji seryjnej.

ZADANIA W ZAKRESIE ZAPROJEKTOWANIA PŁATOWCA I ZESPOŁU NAPĘDOWEGO

Projekt koncepcyjny, czyli pierwsze przybliżenie formy płatowca dla małego systemu bezzałogowego, to efekt analizy najczęściej stosowanych w tej dziedzinie rozwiązań. Istnieje wiele układów aerodynamiczno-konstrukcyjnych aplikowanych z powodzeniem w ramach wstępnych założeń definiowanych dla minisamolotów. Najczęściej spotykanym w mini-BSP rozwiązaniem jest górnopłat ze skrzydłem prostym (często z dodatnio wzniesionymi

końcówkami) i klasycznym usterzeniem ogonowym. Obszar ładunkowy przeznaczony dla urządzeń misyjnych znajduje się zazwyczaj w przedniej części kadłuba lub podwieszanej gondoli.

Własną koncepcję płatowca minisamolotu (określanego jako mini-BSP Rybitwa) wzorowano zasadniczo na konstrukcjach klasycznych z podwieszanym centralnie zasobnikiem ładunkowym ((ilustracja 1). Przyjęto konfigurację z prostym skrzydłem wolnonośnym oraz klasycznym usterzeniem ogonowym typu T. Argumenty sprzyjające podjęciu decyzji o takiej właśnie formie to m.in.:

- prostota czynności obsługowych użytkownika w początkowej fazie eksploatacji,
- przewidywalność dużej doskonałości aerodynamicznej,
- warunki zrównoważenia aerodynamicznego odpowiadające naturalnej stateczności statycznej.

Tabela 1.
Podstawowe parametry geometryczne i masowe minisamolotów w konfiguracji z podwieszanym zasobnikiem

Mini-BSP	Długość całkowita l [m]	Rozpiętość płata s [m]	s/l	Długość zasobnika l_z [m]	Masa użyteczna m_u [kg]	Masa całkowita m [kg]	Wskaźnik udziału m_u m_u/m
Skylark 1	2,2	2,4	1,09	0,93	0,65	5,5	0,12
Skylark 1LE	2,2	2,9	1,32	0,95	1,15	7,3	0,16
Skyblade III	1,4	2,6	1,86	---	1,00	5,4	0,18
Kiwit v.2	1,2	2,5	2,08	---	0,95	4,0	0,24

Źródło: „Elbit Systems", „ST Aerospace", „Kiwit – Mini UAS"

Wymiary gabarytowe płatowca oraz masę startową i użytkową przyjęto do założeń projektowych, sugerując się danymi analitycznymi zebranymi dla istniejących już konstrukcji podobnych (tabela 1). Przewidując nieco większy udźwig na wypadek konieczności montażu wielosensorowej głowicy, założono ostatecznie masę maksymalną nie większą niż 10 kg oraz rozpiętość płata nośnego rzędu 3 m. Orientacyjny wymiar cięciwy skrzydła określono wg formuły Reynoldsa:

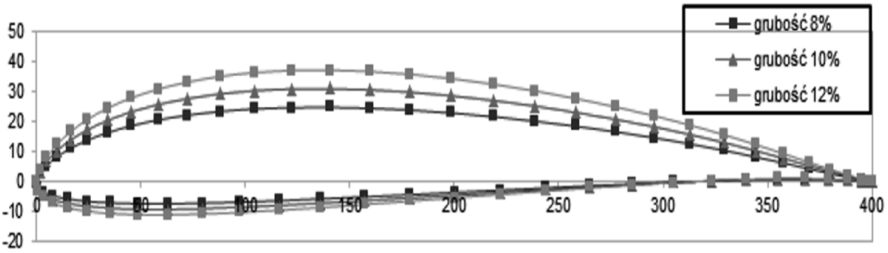
$$\mathrm{Re} = \frac{V \cdot l}{\nu} \tag{1}$$

gdzie:
V – prędkość lotu,
l – charakterystyczny wymiar linowy (tutaj cięciwa skrzydła c),
v – lepkość kinematyczna. Zakładając minimalną prędkość lotu $V_{min} = 12$ m/s oraz przyjmując lepkość powietrza v = 17,08 μPa·s, można wyznaczyć minimalną cięciwę skrzydła dobraną tak, aby opływ odpowiadał korzystnemu zakresowi liczby Reynoldsa (powyżej $2*10^5$). Wykorzystując przekształcony wzór (1):

$$c_{\min} \approx \frac{\mathrm{Re} \cdot \nu}{V_{\min}} \tag{2}$$

można oszacować wystarczającą długość cięciwy skrzydła na c_{min} = 240 mm. Na podstawie dostępnych albumów profili lotniczych (Abbot, 1958; „Airfoil Database", 2010; „UIUC Airfoil Database", 2010) ustalono wstępnie profile skrzydła i usterzeń. W skrzydłach zastosowano profil SD 7037 o grubości 8% z powodzeniem stosowany w szybowcach. Jest to profil dwuwypukły, turbulentny gwarantujący niski opór aerodynamiczny i dobrze sprawdzający się w zakresie małych liczb Reynoldsa. Skrzydła modyfikowanych później wersji Rybitwy miały ten sam profil, jednak o stopniowo większych grubościach – 10% i 12%.

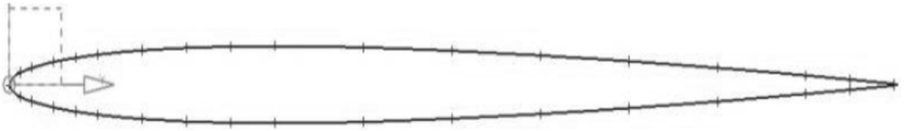
Rysunek 3.
Modyfikacje profilu SD 7037 uwzględniające zmianę grubości w kolejnych wersjach



Źródło: Badania własne w ramach projektu „Autonomiczne bezzałogowe statki powietrzne...", 2013

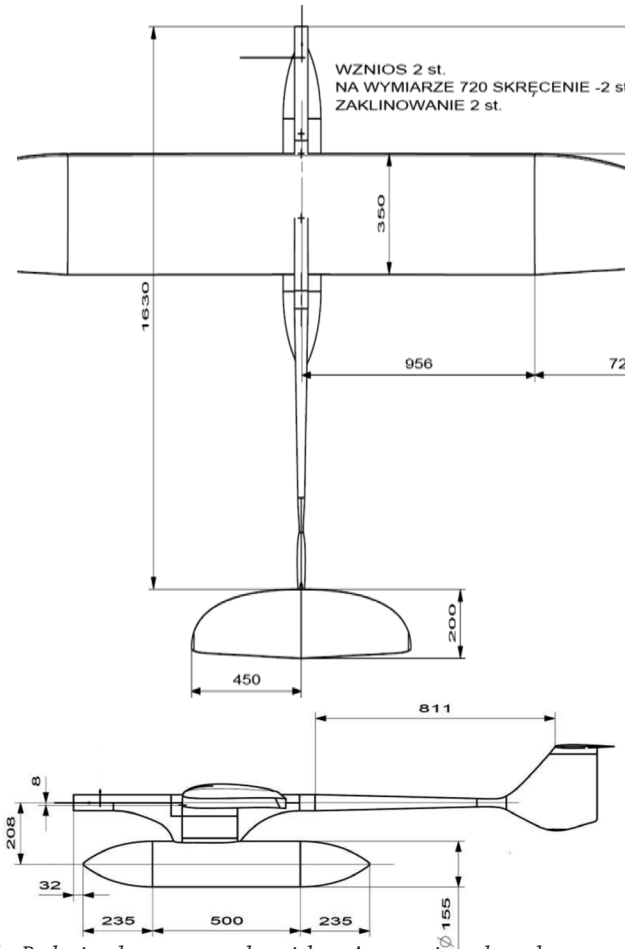
W usterzeniu poziomym i pionowym zastosowano profil symetryczny – odpowiednio NACA 0006 i NACA 0008. Profil ten zapewnia minimalny opór usterzenia ogonowego oraz pożądaną symetrię aerodynamiczną (identyczne, lecz przeciwne co do wartości przyrosty siły nośnej i momentu pochylającego przy dodatnich bądź ujemnych kątach natarcia).

Rysunek 4.
Profil symetryczny NACA 0006



Źródło: Badania własne w ramach projektu „Autonomiczne bezzałogowe statki powietrzne…", 2013

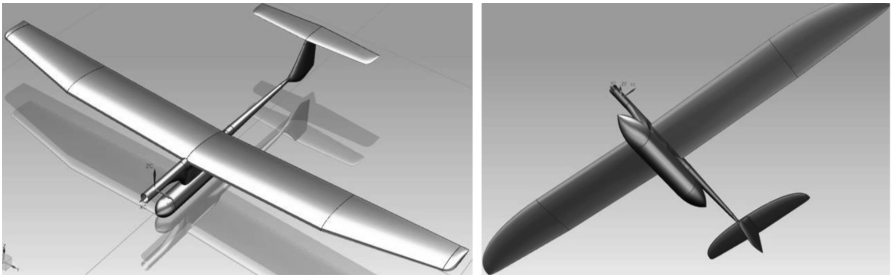
Rysunek 5.
Szkic geometrii ogólnej płatowca mini-BSP w wersji z największym zasobnikiem



Źródło: Badania własne w ramach projektu „Autonomiczne bezzałogowe statki powietrzne…", 2013

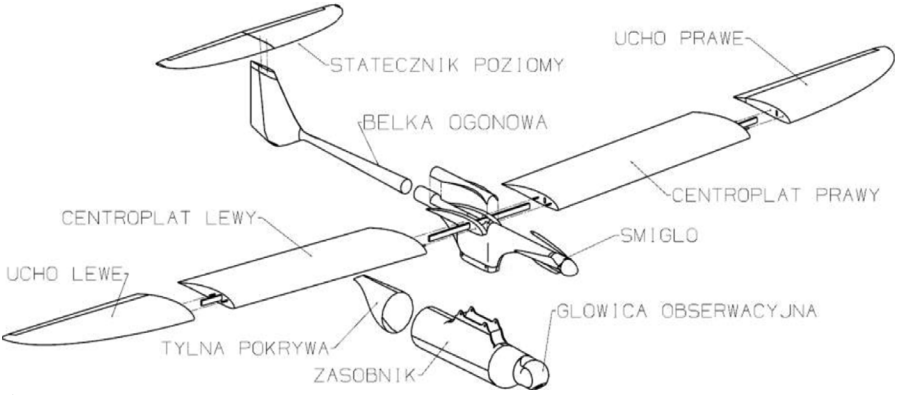
Podział konstrukcyjno-technologiczny płatowca uwzględnia takie elementy, jak: płat nośny, kadłub, belka ogonowa z usterzeniem pionowym, usterzenie poziome, zespół napędowy, podwieszany zasobnik ładunkowy (gondola). Bryłę geometryczną płatowca opracowano w systemie CAD Semens NX. Statecznik poziomy ma kształt trapezowy z zaokrąglonymi końcami krawędzi natarcia. Usterzenie pionowe stanowi integralną część skorupy kadłuba. W zasobniku przewidziano umieszczenie źródeł zasilania i większości wyposażenia awionicznego. Poniżej zamieszczono grafiki demonstrujące geometrię płatowca w rzutach oraz w widoku przestrzennym.

Ilustracja 2.
Modele CAD płatowca mini-BSP w kolejnych wersjach rozwojowych – zmiany dotyczyły zasadniczo kształtu i wielkości zasobnika oraz obrysu i rozpiętości płata nośnego



Źródło: Badania własne w ramach projektu „Autonomiczne bezzałogowe statki powietrzne...", 2013

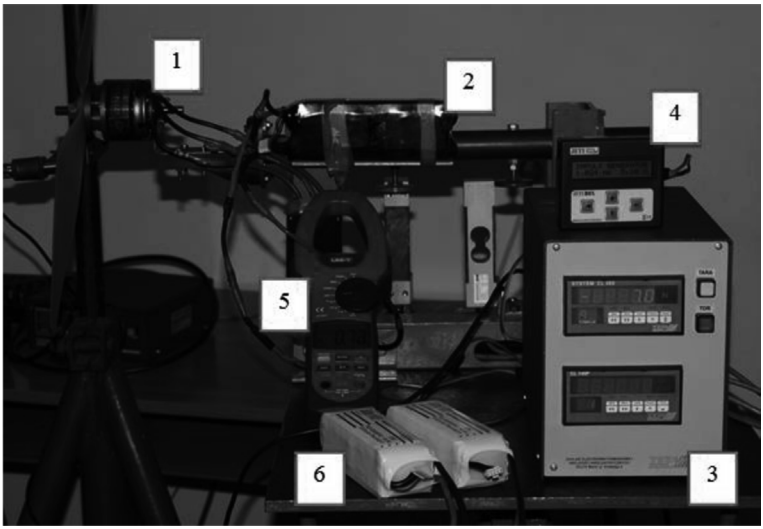
Rysunek 6.
Schemat podziału technologiczno-montażowego samolotu



Źródło: Badania własne w ramach projektu „Autonomiczne bezzałogowe statki powietrzne...", 2013

W bezzałogowych statkach powietrznych klasy mini wykorzystywane są zespoły napędowe wytwarzające ciąg za pomocą śmigieł napędzanych silnikami elektrycznymi lub spalinowymi. W skład zespołu napędowego z silnikiem elektrycznym wchodzą: śmigło, silnik prądu stałego, regulator obrotów, źródło zasilania (pakiet akumulatorowy), przewody zasilające i sterujące. Wyboru napędu dokonano na drodze testów wybranych kilku wariantów silnik-śmigło przeprowadzonych na stanowisku laboratoryjnym do hamowania miniaturowych napędów. Przeprowadzono pomiary parametrów elektrycznych w obwodzie zasilania badanych silników (napięcie, natężenie) oraz sił reakcyjnych (wzdłużnej i obwodowej) w warunkach statycznych. Sporządzając charakterystyki zależności parametrów mechanicznych (ciągu, momentu obrotowego) od prędkości obrotowej i pobieranego prądu, ustalono konfiguracje napędu optymalne dla przyjętego projektu.

Ilustracja 3.
Stanowisko do badań miniaturowych napędów śmigłowych



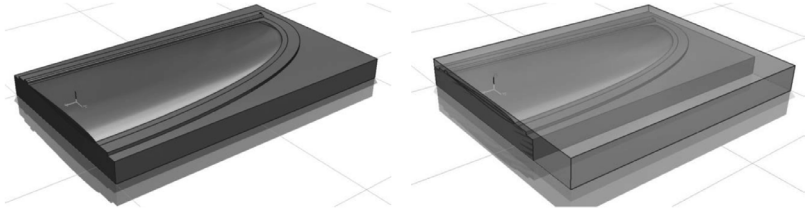
1 – zespół napędowy,
2 – pakiet akumulatorowy do zasilania silnika,
3 – układ do pomiaru sił reakcji,
4 – generator sygnału PWM,
5 – miernik prądowy (z opcjonalnym rejestratorem),
6 – pakiet akumulatorowy przygotowany do kolejnego wariantu.

Źródło: Badania własne w ramach projektu „Autonomiczne bezzałogowe statki powietrzne…", 2013.

TECHNIKI WYTWARZANIA ZASTOSOWANE W BUDOWIE PŁATOWCA

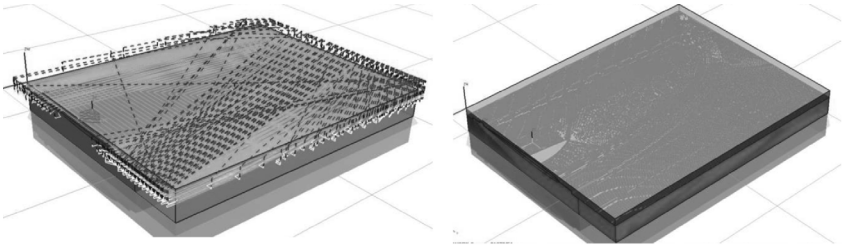
Fragmenty struktury płatowcowej, pokazane jako technologicznie odrębne elementy na rysunku 2, wykonano w technologii laminowania. Na potrzeby przygotowania foremników zaprojektowano formy pozytywowe odwzorowujące rzeczywiste kształty zewnętrzne elementów oraz opracowano technologię ich wykonania. Trójwymiarowe modele geometryczne elementów posłużyły jako podstawa do zaprojektowania form. Jako materiału na formy użyto pianki poliuretanowej firmy AXON – Prolab 65. Płyta została zamodelowana w oprogramowaniu CAM jako przygotówka do wycięcia docelowej matrycy. Proces definiowania operacji obróbkowych wykonano w module *Manufacturing* systemu Siemens NX. Kolejne fazy skrawania zdefiniowane w preprocesorze dla wirtualnego modelu płyty zapisywano w pliku tekstowym. Przygotowane w ten sposób kody maszynowe (tabela 1) wykorzystywano następnie jako dane sterujące maszyną skrawającą w procesach obróbkowych kolejno wykrawanych form.

Ilustracja 4.
Model formy docelowej oraz płyty bazowej z przygotówką (Siemens NX)



Źródło: Badania własne w ramach projektu „Autonomiczne bezzałogowe statki powietrzne...", 2013

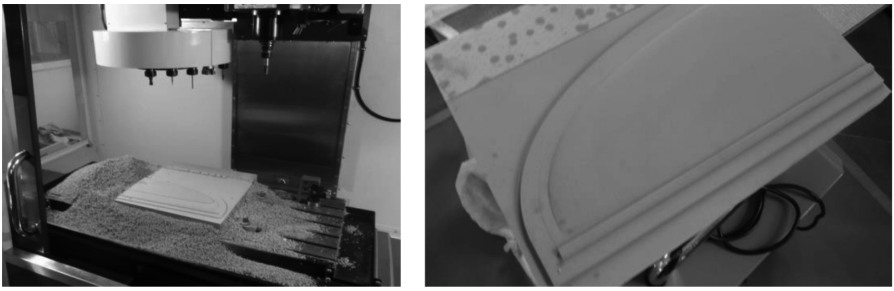
Ilustracja 5.
Symulowane ścieżki narzędzia skrawającego i wizualizacja płyty po symulacji obróbki



Źródło: Badania własne w ramach projektu „Autonomiczne bezzałogowe statki powietrzne...", 2013

Formy wykonano na frezarce trójosiowej Haas VF4. Dzięki wykorzystaniu obrabiarki sterowanej numerycznie możliwe stało się precyzyjne odwzorowanie powierzchni skrzydła, przede wszystkim kształtu profilu, co przełożyło się na uzyskanie osiągów modelu zgodnych z oczekiwanymi. Wykorzystanie obrabiarki CNC numerycznie pozwala wykonać powierzchnię o dowolnym stopniu komplikacji, dzięki temu projekt płatowca nie jest ograniczany technologicznymi barierami.

Ilustracja 6.
Obrabiarka Haas VF4 – wgląd w komorę roboczą w toku frezowania oraz efekt końcowy – wyrzeźbiona forma pozytywowa usterzenia poziomego jako baza do wylaminowania foremnika

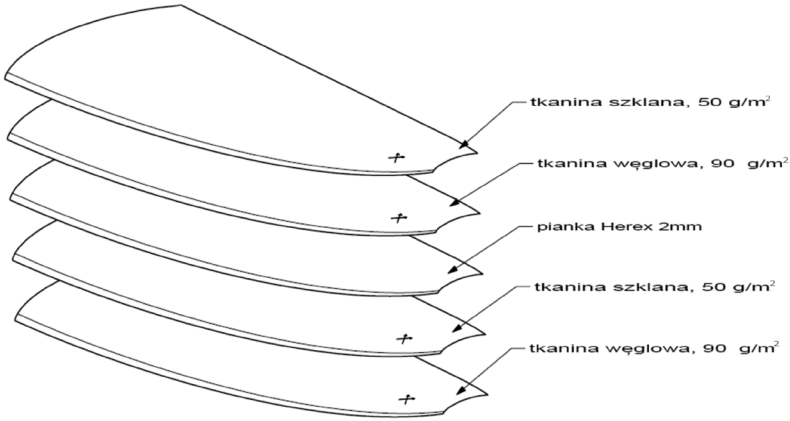


Źródło: Badania własne w ramach projektu „Autonomiczne bezzałogowe statki powietrzne...", 2013

W przypadku kadłuba, steru kierunku i zasobnika formy wykonano techniką modelarską, wykorzystując dostępne elementy, np. rury z tworzywa sztucznego (kształt zasobnika), sklejkę modelarską, styrodur, gips, jak również: tkaniny szklane i żywice epoksydowe. Opracowane formy szpachlowano, szlifowano papierem ściernym o różnych granulacjach oraz zabezpieczano lakierem.

Struktury płatowcowe zostały wylaminowane według wcześniej przygotowanych planów nakładania poszczególnych warstw z uwzględnieniem zalecanej metodyki (Rzepczyńska, 2006) i własnych doświadczeń. Laminowane kompozycje (głównie tkaninowo-żywicowe lub przekładkowe) zostały zaprojektowane w toku przeprowadzonych wcześniej sprawdzających obliczeń wytrzymałościowych. Zastosowano tkaninę węglową i szklaną o różnych gramaturach, wypełniacz piankowy typu Herex oraz pasma rowingu węglowego w szczególnie wytężonych strefach konstrukcji. Jako dodatki konstrukcyjne wykorzystano również drobne elementy metalowe, drewniane lub balsowe.

Rysunek 7.
Przykładowy plan laminowania – warstwy struktury pokryciowej ucha skrzydłowego



Źródło: Badania własne w ramach projektu „Autonomiczne bezzałogowe statki powietrzne...", 2013

Ilustracja 7.
Technologia próżniowa w zastosowaniu do laminowania struktury usterzenia poziomego oraz komplet laminatowych elementów płatowcowych

Źródło: Badania własne w ramach projektu „Autonomiczne bezzałogowe statki powietrzne...", 2013

INTEGRACJA PODSYSTEMÓW WYPOSAŻENIA POKŁADOWEGO

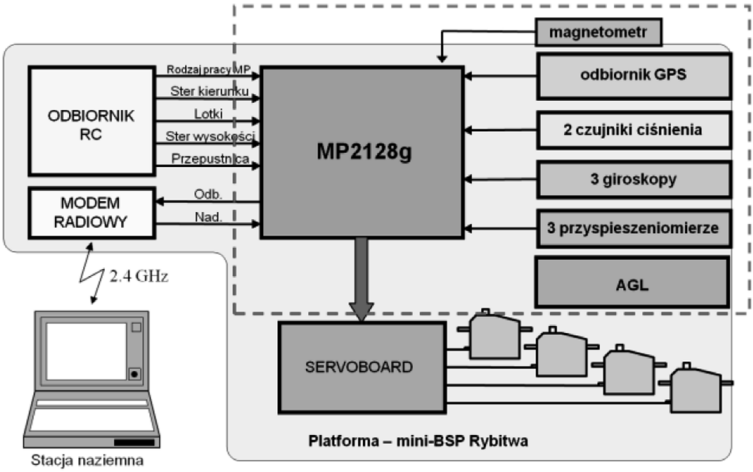
Pokładowy system awioniczny minisamolotu obejmuje zintegrowane ze sobą układy wykazujące określone dla systemu funkcjonalności. Komponenty wyodrębnione w ramach specjalizowanych funkcji podsystemowych to: układ automatycznego sterowania, układ zasilania elektrycznego, układ rozpoznania wizyjnego, podsystem łączności.

Podsystem sterowania bazuje na autopilocie MP2128g. Autopilot ten jest profesjonalnym, mikroprocesorowym układem automatycznego sterowania

lotem przeznaczonym dla obiektów bezpilotowych. Dzięki zastosowaniu półprzewodnikowych czujników przyspieszeń liniowych, piezoelektrycznych żyroskopów prędkościowych, półprzewodnikowych czujników ciśnienia statycznego i dynamicznego, system ma zdolność stabilizacji prędkości lotu względem prędkości powietrza, stabilizacji wysokości lotu oraz umożliwia wykonanie zakrętu skoordynowanego. Ponadto wykorzystując informację z odbiornika GPS i wysokościomierza ultradźwiękowego, pozwala na wykonywanie automatycznego startu, zaprogramowanego lotu oraz autonomicznego lądowania. Dodatkowo podczas lotu autopilot za pośrednictwem modemu radiowego współpracuje z naziemną stacją bazową, realizując szereg dodatkowych funkcji, takich jak: ostrzeganie o zużyciu baterii, automatyczne przełączenie na program lotu awaryjnego, umożliwiający w przypadku zaniku sygnału z aparatury radiowej powrót obiektu do miejsca startu.

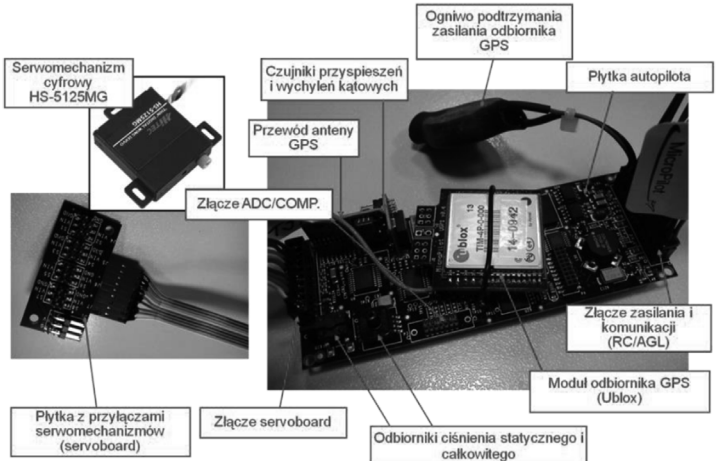
Bardzo ważną i przydatną funkcją autopilota, szczególnie na etapie badań, jest obszerna rejestracja danych, możliwość planowania i symulacji misji, sprawdzanie i strojenie wzmocnień w torach sprzężeń zwrotnych regulatorów PID oraz wstępne konfigurowanie czujników i serwonapędów. W przypadku mini-BSP Rybitwa autopilot za pomocą sygnałów PWM (sterownika modulacji impulsów) steruje czterema serwomechanizmami w kanałach: przepustnicy silnika, lotek, steru wysokości i steru kierunku.

Rysunek 8.
Schemat blokowy integracji komponentów układu automatycznego sterowania



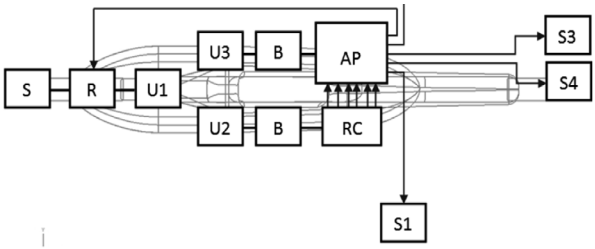
Źródło: Badania własne w ramach projektu „Autonomiczne bezzałogowe statki powietrzne...", 2013

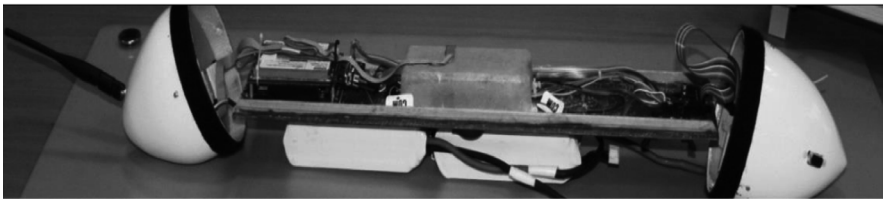
Ilustracja 8.
Komponenty układu automatycznego sterowania z autopilotem MP2128g



Źródło: Badania własne w ramach projektu „Autonomiczne bezzałogowe statki powietrzne...", 2013

Ilustracja 9.
Schemat blokowy powiązania elementów awionicznych oraz widok wybranych elementów zamontowanych w zasobniku w wariancie do lotu sterowanego półautomatycznie





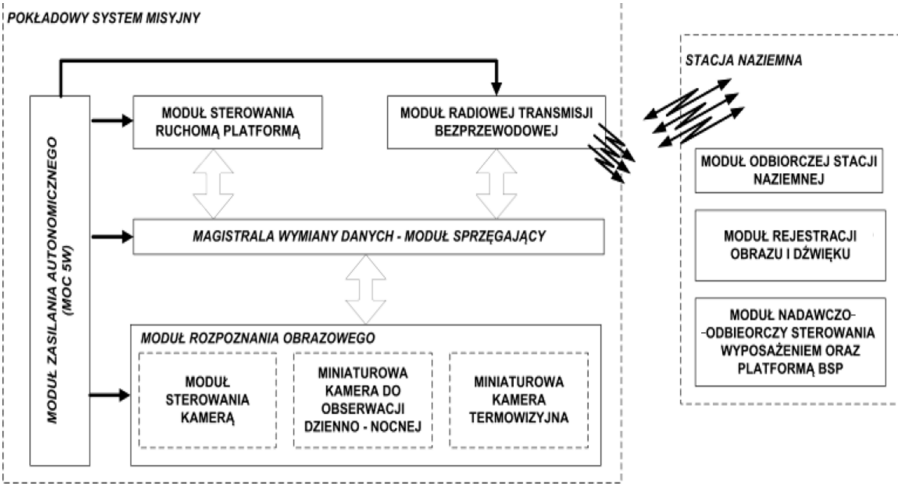
Oznaczenia:
S – silnik elektryczny,
R – regulator napięcia,
U1 – źródło zasilania głównego,
U2 – źródło zasilania odbiornikowego,
B – stabilizator impulsowy typu BEC,
RC – odbiornik radiowy sygnałów zdalnego sterowania,
U3 – źródło zasilania autopilota,
AP – autopilot,
S1, S2, S3, S4 – serwomechanizmy lotek i sterów.

Źródło: Badania własne w ramach projektu „Autonomiczne bezzałogowe statki powietrzne...", 2013

Na schemacie (ilustracja 9) zademonstrowano konfigurację wyposażenia pokładowego minisamolotu do próbw w locie w trybie manualnym (sterowanie poprzez odbiornik RC) oraz półautomatycznym (sterowanie z udziałem autopilota). Układ AP poprzedzony jest układem odbiornika aparatury zdalnego sterowania RC, który w trybie awaryjnym staje się priorytetowym układem kontroli lotu.

W strukturze podsystemu misyjnego przedstawionego na rysunku 9 można wyróżnić część pokładową i część naziemną. W ramach misyjnej instalacji pokładowej wyróżnić można moduł rozpoznania obrazowego (głowica z miniaturową kamerą TV/IR), modułem sterowania platformą, moduł radiowej transmisji bezprzewodowej i moduł zasilania autonomicznego. W części naziemnej występuje moduł odbiorczy sygnału obrazowego, moduł rejestracji danych oraz nadawczo-odbiorczy moduł sterowania. Magistrala wymiany danych zabezpiecza komunikację pomiędzy układami modułowymi. Z kolei moduł radiowy zapewnia transmisję obrazu i sygnałów sterujących.

Rysunek 9.
Ogólna koncepcja powiązań funkcjonalnych elementów wyposażenia misyjnego mini-BSP



Źródło: Badania własne w ramach projektu „Autonomiczne bezzałogowe statki powietrzne...", 2013

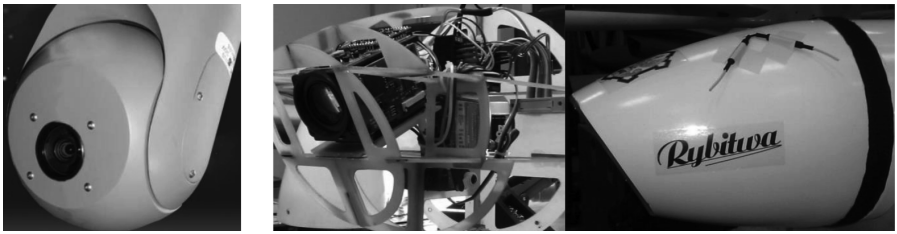
Zadaniem realizowanym przez pokładowy system misyjny jest obserwacja i rozpoznanie wizyjne. Centralnym elementem modułu rozpoznania obrazowego jest kamera do obserwacji dziennej oraz kamera termowizyj-

na. Z kolei zadaniem stacji naziemnej jest zapewnienie możliwości odbioru i projekcji danych obrazowych i telemetrycznych, jak również zapewnienie możliwości ich rejestrowania. Dodatkowy kanał łączności musi zapewnić możliwość swobodnej manipulacji położeniem ruchomej platformy głowicy oraz regulacji nastaw optycznych sensora.

Rozwiązaniem wybranym dla minisamolotu jest głowica MP-Dayview z dzienną kamerą TV firmy MicroPilot. Urządzenie może również występować w wersji nocnej (MP-Nightview). Kamera dzienna oferuje obraz w rozdzielczości 800 kpikseli z 25-krotnym powiększeniem. Główną zaletą MP-Dayview – poza niewielkimi wymiarami i masą (< 1 kg) oraz niskim poborem energii – jest możliwość współpracy z dedykowanym autopilotem MicroPilot przewidzianym do zastosowania w projekcie.

Ilustracja 10.
Sensory zastosowane w podsystemie rozpoznania wizyjnego mini-BSP Rybitwa: a) głowica MP-Dayview/Nightview, b) kamera Sony FCB-EX20D/P zabudowana w głowicy własnej konstrukcji

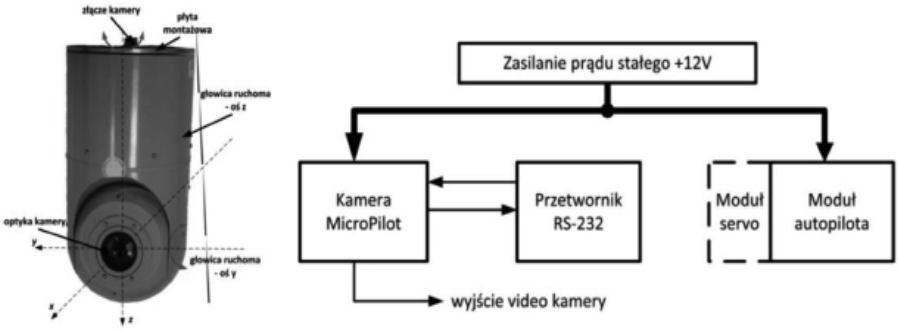
a) b)



Źródło: Badania własne w ramach projektu „Autonomiczne bezzałogowe statki powietrzne...", 2013

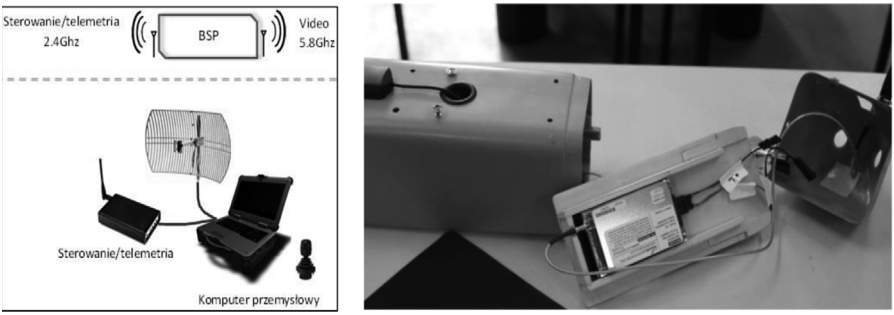
Kamery firmy MicroPilot są montowane na ruchomej i sterowanej głowicy. W układzie tym znajdują się dwa połączenia ruchome: połączenie wewnętrzne, które steruje blokiem kamery, i połączenie zewnętrzne zawierające mikrokontroler sterujący wszystkimi funkcjami optycznymi. Wszystkie opcje sterowania i regulacji obsługiwane są przez mikrokontroler, który przetwarza otrzymane komendy oraz przesyła bieżące parametry poprzez dwukierunkowy port transmisji RS-232.

Ilustracja 11.
Głowica MP-Dayview i schemat jej połączenia z pokładowym systemem awionicznym



Źródło: Badania własne w ramach projektu „Autonomiczne bezzałogowe statki powietrzne...", 2013

Ilustracja 12.
Schemat funkcjonalny dwutorowego podsystemu łączności (transmisja telemetrii – 2,4 GHz, transmisja TV – 5,8 GHz) oraz przykładowe rozwiązanie montażowe z anteną i modemem telemetrycznym



Źródło: Badania własne w ramach projektu „Autonomiczne bezzałogowe statki powietrzne...", 2013

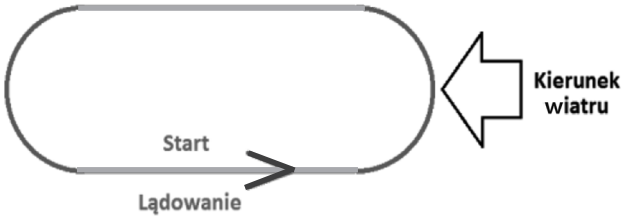
Podsystem łączności powinien zapewniać ciągłą transmisję obrazu wideo i danych telemetrycznych z obiektu latającego poruszającego się w dowolnych warunkach pogodowych i przy eksploatacyjnie przewidzianych parametrach nawigacyjnych (prędkości, lokalizacji, kursie, kątach położenia przestrzennego). Jakość identyfikowanego obrazu determinuje zastosowana kamera, której pole obserwacji decyduje o możliwościach zaprojektowanego systemu. System przesyłania obrazu obejmuje elementy umieszczone na pokładzie statku powietrznego i elementy umieszczone w stacji naziemnej. Na pokładzie statku powietrznego oprócz kamery umieszczony jest nadajnik wraz z anteną. Stacja naziemna wyposażona jest

w terminal antenowy z odbiornikiem oraz urządzenie do wyświetlania lub zapisu obrazu. Podsystem łączności proponowany w ramach rozwijanego systemu bezzałogowego zabezpiecza transmisję dwutorową – oddzielnie dla danych z rozpoznania obrazowego i danych pilotażowo-nawigacyjnych (telemetrycznych).

TESTY W LOCIE FUNKCJONALNOŚCI PODSYSTEMU AUTOMATYCZNEGO STEROWANIA

Wykazanie pełnej funkcjonalności systemu rozpoznawczego opartego na bezzałogowej platformie latającej wymaga realizacji programu prób opartego na lotach testowych w różnych konfiguracjach misyjnych oraz warunkach pogodowych. Po zainstalowaniu elementów systemu awionicznego oraz przeprowadzeniu czynności kontrolnych pod kątem osiągnięcia wymaganej integracji systemowej (zdatność, funkcjonalność, powtarzalność) przeprowadzono serię lotów doświadczalnych z różnymi wariantami wyposażenia. Zadaniem priorytetowym było sprawdzenie jakości i niezawodności działania podsystemu automatycznego sterowania bazującego na autopilocie MP2128g.

Rysunek 10.
Schemat trasy lotu testowego z odcinkami realizacji różnych trybów sterowania



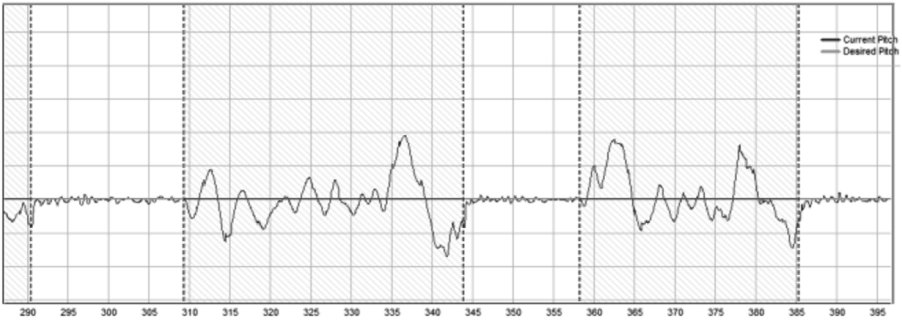
Źródło: Badania własne w ramach projektu „Autonomiczne bezzałogowe statki powietrzne...", 2013

Wstępne loty odbywały się w oparciu o klasyczny krąg nadlotniskowy. Kolorem czerwonym zaznaczono nawroty wykonywane w trybie operatorskim PIC (*Pilot-In-Command*). Z kolei kolor niebieski przedstawia tryb lotu CIC (*Computer-In-Command*), gdzie autopilot uruchamiany jest do pracy w trybie automatycznym, sterując BSP za pomocą określonych przez operatora pętli sterowania. Na tym etapie regulowane są parametry trzech podstawowych pętli sterujących, mających kluczowe znaczenie podczas prowadzenia lotów w trybie automatycznym. Wykonane wcześniej testy symulacyjne pozwalają na wstępne ustawienie parametrów regulacji układu.

Podczas pierwszych lotów sprawdzana jest poprawność działania wszystkich czujników autopilota. Przeprowadzany jest test działania odbiornika ciśnień oraz jakości wibroizolacji platformy montażowej układu. Wstępnie autopilot pracuje w trybie rejestratora parametrów lotu z fizycznie wykonanym obejściem sygnałów sterujących, umożliwiającym sterowanie w trybie PIC.

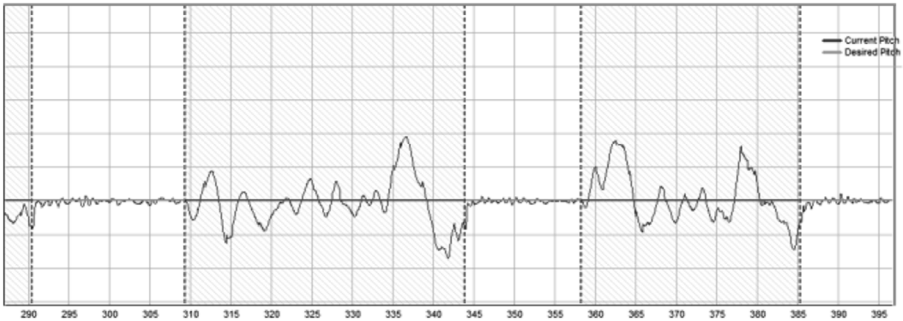
Na kolejnych dwóch wykresach przedstawiono czasowe przebiegi wartości kątów pochylenia i przechylenia regulowanych w trybie CIC podczas wykonywania lotu ustalonego. Wartość zadana obu wielkości na poziomie 0^0 jest utrzymywana przez układ stabilizacji z oscylacjami nieprzekraczającymi 3^0. Podczas wykonywania zakrętów autopilot pracuje w trybie PIC, gdzie wielkości przechylenia i pochylenia uzyskują duże wartości.

Rysunek 11.
Przebiegi rzeczywistych wartości kąta pochylenia na tle pochylenia zadanego



Źródło: Badania własne w ramach projektu „Autonomiczne bezzałogowe statki powietrzne...", 2013

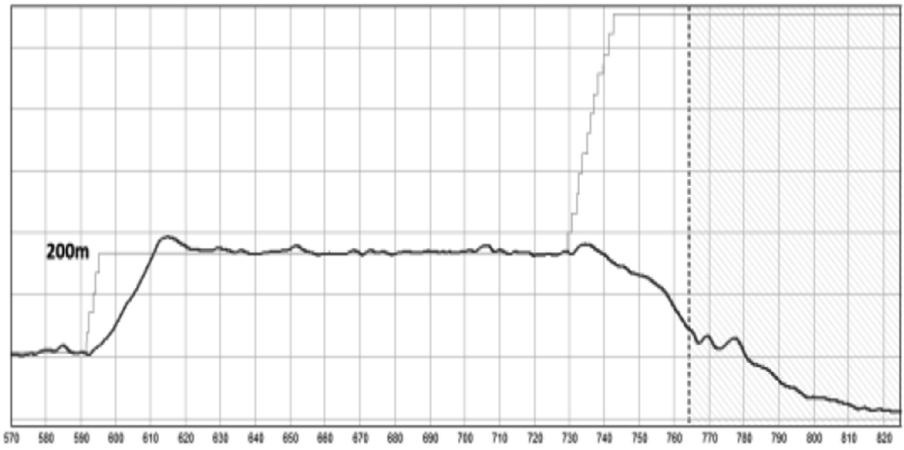
Rysunek 12.
Przebieg rzeczywistych wartości kąta przechylenia na tle przechylenia zadanego



Źródło: Badania własne w ramach projektu „Autonomiczne bezzałogowe statki powietrzne...", 2013

Kolejny etap integracji autopilota to dostrajanie pętli odpowiadających za utrzymywanie i zmianę wysokości. Poniższy wykres uwidacznia jakość utrzymywania wysokości lotu zdefiniowanej jako 200 m. W dalszej fazie lotu zwiększono wartość zadaną wysokości, jednak niski poziom naładowania akumulatorów uniemożliwił wznoszenie, co wymusiło przeprowadzenie lądowania. Oszacowane na podstawie odczytów z centrali aerometrycznej oscylacje wysokości nie przekraczały 6 m.

Rysunek 13.
Przebieg rzeczywistych wartości wysokości bieżącej na tle zadanej wysokości ustalonej

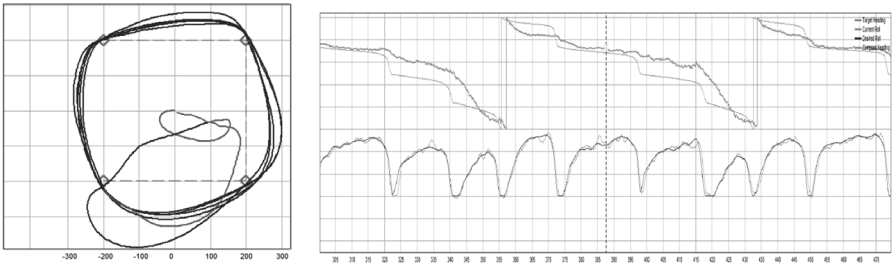


Źródło: Badania własne w ramach projektu „Autonomiczne bezzałogowe statki powietrzne...", 2013

Ostateczny dobór parametrów pętli nawigacyjnych odpowiadających za utrzymywanie zadanej ścieżki lotu oraz wykonywanie zakrętów przeprowadzono według planu lotu opierającego sięna czterech punktach nawigacyjnych. Lot ten wykonany w większości w trybie automatycznym potwierdza zdatność zabudowanego autopilota do wykonywania lotów według zaplanowanej przez użytkownika trasy. Do wykonywania lotów w pełnym trybie automatycznym należy dopracować manewr lądowania BSP przy użyciu spadochronu.

Dobrane w fazie lotów symulacyjnych parametry sterowania okazały się zbliżone do tych, które osiągnięto podczas serii lotów rzeczywistych. Oba testowane autopiloty wykazały się pełną funkcjonalnością w zakresie stabilizacji i sterowania minisamolotem.

Rysunek 14.
Zarejestrowana ścieżka lotu wg punktów nawigacyjnych i czasowe przebiegi wartości bieżącej oraz zadanej kursu i kąta przechylenia



Źródło: Badania własne w ramach projektu „Autonomiczne bezzałogowe statki powietrzne...", 2013

KOMPLETACJA DEMONSTRATORA SYSTEMU

Opracowany miniaturowy bezzałogowy samolot stanowi wraz z naziemną stacją kontroli i akcesoriami kompletny mobilny system obserwacji. W ramach systemu można wyodrębnić następujące komponenty:

- miniaturowy samolot z wyposażeniem misyjnym i spadochronowym układem odzyskiwania,
- naziemną stację kontroli lotów (NSKL) z jednostką sterującą (komputer przenośny z konsolą operatorską) oraz urządzeniami łączności,
- wyposażenie dodatkowe – kontener transportowy, ładowarka pakietów akumulatorowych, agregat zewnętrznego zasilania elektrycznego, zestaw akcesoriów obsługowo-naprawczych.

System, którego głównym elementem jest miniaturowy samolot, może wykonywać misje według zróżnicowanych trybów sterowania:

- Lot według pola obserwacji – minisamolot dokonuje oblotu nad obszarem pozostającym w zasięgu kamery; operator, sterując położeniem kątowym głowicy obserwacyjnej, wprowadza pośrednio parametry definiujące „widzianą" trasę oblotu.
- Lot po wyznaczonej trasie – do pamięci autopilota minisamolotu zapisywany jest plan lotu zdefiniowany na podstawie zdefiniowanych punktów nawigacyjnych.
- Lot nad określonym obszarem obserwacji – minisamolot wykonuje lot nad zadanym obszarem zdefiniowanym poprzez koordynaty zakreślające pole stałej obserwacji; lot odbywa się zwykle po okręgu bądź tzw. ósemce.

- Lot powrotny do punktu startu (tryb *fly home*) – minisamolot powraca do punktu startu, wykonując lądowanie w sposób zdefiniowany przez operatora.

System spadochronowy instalowany jest w zasobniku kadłubowym poprzez zamocowanie linek nośnych do trzech węzłów znajdujących się wewnątrz kadłuba. Czasza główna spadochronu zajmuje większą część komory za dźwigarem. W części przedniej (przed dźwigarem) zapakowany jest pilocik ze sprężyną wyrzucającą.

Ilustracja 13.
Główne komponenty systemu oraz sposób pakowania elementów minisamolotu do transportu

Źródło: Badania własne w ramach projektu „Autonomiczne bezzałogowe statki powietrzne...", 2013

Ilustracja 14.
Komora kadłubowa z zamontowanym spadochronem

Źródło: Badania własne w ramach projektu „Autonomiczne bezzałogowe statki powietrzne...", 2013

Minisamolot po wykonaniu lotów jest rozmontowywany i umieszczany w dobranej do tego celu mobilnej skrzyni ładunkowej. Każdy z elementów powierzchniowych struktury nośnej wkładany jest do oddzielnego pokrowca transportowego, chroniącego przed ewentualnymi uszkodzeniami w czasie transportu. Kadłub osadzony jest w stojaku ułatwiającym montaż płatowca oraz przewidziane obsługi przed lotem i po nim.

Start miniaturowego samolotu realizowany poprzez wyrzut z ręki zaprezentowany został na sekwencyjnej ilustracji (ilustracja 15). Moc startowa napędu elektrycznego umożliwia bezpieczny manewr przy kącie ustawienia kadłuba w granicach 20–30°. Do startu automatycznie wychylane są klapy. Po wzniesieniu się na wysokość około 15 m moc startowa jest redukowana i BSP kontynuuje wznoszenie przy mniejszych wydatkach prądowych. Wykonywanie każdego lotu kończone jest poprzez przeprowadzenie procedury lądowania. Zapoczątkowanie tej fazy determinowane jest poprzez naciśnięcie przycisku lądowania na pulpicie NSKL. Proces lądowania polega na wyhamowaniu samolotu do odpowiednio niskiej prędkości, otwarciu klap i uruchomieniu układu spadochronowego na pożądanej wysokości. W efekcie zapewnione jest powolne opadanie i miękkie przyziemienie dolną powierzchnią zasobnika.

Ilustracja 15.
Fazy startu mini-BSP Rybitwa

Źródło: Badania własne w ramach projektu „Autonomiczne bezzałogowe statki powietrzne...", 2013

PODSUMOWANIE

Zadaniem docelowym w ramach wysiłków projektowo-badawczych podjętych w Instytucie Techniki Lotniczej WML WAT było opracowanie demonstratora technologii systemu rozpoznawczego z miniaturową platformą latającą, który to system byłby w pełni funkcjonalną i konkurencyjną alternatywą dla aktualnie oferowanych rozwiązań światowych. Własna idea małego aparatu bezzałogowego w pełni dopracowana pod względem konstrukcyjnym, technologicznym i użytkowym może stanowić interesującą i niedrogą propozycję – w szczególności dedykowaną państwowym służbom publicznym. Jednakże aby osiągnąć poziom rozwoju systemu umożliwiający jego w pełni użyteczne wdrożenie, niezbędne jest przeprowadzenie bardziej zaawansowanych testów i sprawdzeń, które powinny się odbywać w toku co najmniej kilkumiesięcznej ciągłej eksploatacji doświadczalnej.

Niniejsze opracowanie powstało na podstawie wyników prac projektowych i badań przeprowadzonych w ramach projektu badawczego rozwojowego pt. „Autonomiczne bezzałogowe statki powietrzne wyposażone w środki monitorowania i nadzorowania wspomagające działania policji i straży pożarnej". Projekt został zrealizowany w latach 2010–2013 przez konsorcjum AGH WIMiR Katedra Robotyki i Mechatroniki – WAT WML Instytut Techniki Lotniczej – EC Engineering Sp. z o.o.

Bibliografia

Abbott I.H., von Doehnoff A.E. (1958). *Theory of Wing Sections Including a Summary of Airfoil Data*. Dover Publication, Inc. New York.

Arjomandi M., *Classification of Unmanned Aerial Vehicles*. Mechanical Enginnering 3016 – The University of Adelaide.

Olejnik A., Rogólski R., Chachurski R., Frant M., *Wybrane aspekty prototypowania płatowca bezzałogowego statku powietrznego klasy mini*. XIV Szkoła Komputerowego Wspomagania Projektowania Wytwarzania i Eksploatacji – Jurata 10–14 maja 2010 (materiały konferencyjne).

Rao P.N., Tewari N.K., Kundra T.K. (1993). *Computer Aided Manufacturing*. Tata McGraw-Hill Publishing Company Limited.

UAS: The Global Perspective. UAS Yearbook 2009/2010. 7th Edition, June 2009, Copyright Blyenburgh & Co.

Źródła internetowe

Aircraft Design: Synthesis and Analysis. Version 0.99, January 2001. DesktopAeronautcs, Inc., http://adg.stanford.edu/aa241/AircraftDesign.html [data dostępu: 28.08.2013].

Airfoil Tools, http://airfoiltools.com/ [data dostępu: 14.05.2010].

Center for the Management of Information (CMI) – The University of Arizona, http://www.nsf.gov/pubs/2002/nsf01168/nsf01168w.htm [data dostępu: 28.08.2013].

Elbit Systems – Skylark® I LE - mini UAS, http://www.elbitsystems.com/elbitmain/areain2.asp?parent=-3&num=279&num2=279 [data dostępu: 31.12.2012].

Kiwit – Mini Unmanned Arborne System, https://www.uvsr.org/Documentatie%20UVS/Documen-tatie%20uav/UAVEmirate/ATE_SA_Kiwit_20110227.pdf [data dostępu: 23.09.2015].

Rzepczyńska K., *Podstawowe informacje dotyczące materiałów i procesu laminowania – konspekt szkoleniowy,* http://stamodra.za.pl/wp-content/uploads/2013/03/instrukcja_kon_lam.pdf [data dostępu: 05.05.2013].

Skylark 1 LE Mini Unmanned Aerial Vehicle (Mini-UAV), http://defenseupdate.com/products/s/skylark1-uav.htm#more [data dostępu: 30.06.2009].

ST Aerospace – Skyblade III. https://www.staero.aero/staero/upload/20150723153136_2411.pdf [data dostępu: 23.09.2015].

UAV/UAS classification, www.unmanned-aerial-system.com/classification.html [data dostępu: 12.07.2010].

UIUC Airfoil Coordinates Database, http://m-selig.ae.illinois.edu/ads/coord_database.html [data dostępu: 14.05.2010].

BRONISŁAW SITEK
Wyższa Szkoła Gospodarki Euroregionalnej
im. Alcide de Gasperi w Józefowie
bronislaw.sitek@gmail.com

ZASADY ETYCZNE STOSOWANE W CYBERPRZESTRZENI

ETHICAL PRINCIPLES APPLIED IN CYBERSPACE

ABSTRACT

Cyberspace is a global phenomenon and is not controlled by any country or international body. The lack of control does not mean anarchy. Hence, the Internet regulations as well as the ethical principles adapted to cyberspace, which is composed of the technologies and network, are developed. For each of these areas similarly, although a different ethical principles were constructed. The codes of ethics were developed for information technology. And for the networks, that means for ordinary users, a specific ethical Decalogue were created. The construction of ethical norms for cyberspace is an important task that requires deep thought.

Keywords: *information technology, networks, Internet law, ethics, cyberspace*

STRESZCZENIE

Cyberprzestrzeń ma charakter globalny i nie jest kontrolowana przez jakiekolwiek państwo bądź instytucję międzynarodową. Brak kontroli nie oznacza jednak anarchii. Stąd rozwija się prawo internetowe, a także zasady etyczne dostosowane do cyberprzestrzeni, na którą składają się technologie i sieci informatyczne. Dla każdego z tych obszarów zbudowano podobne, chociaż też różniące się zasady etyczne. Dla technologii informacyjnych stworzono kodeksy etyczne. Z kolei dla sieci informatycznych, czyli dla zwykłych użytkowników, stworzono swoisty dekalog etyczny. Budowa norm etycznych dla cyberprzestrzeni jest ważnym zadaniem, wymagającym głębokiego przemyślenia.

Słowa kluczowe: *technologie informatyczne, sieci informatyczne, prawo internetowe, etyka, cyberprzestrzeń*

WPROWADZENIE

Rozwój nowych technologii, zwłaszcza w obszarze informatycznym, wymaga dość pogłębionej refleksji nad celami nowych badań, a także nad granicą, której człowiek nie powinien przekraczać. Ta wstępna uwaga ma swój sens w świetle tego, że współczesne badania w dużej mierze są inspirowane (i finansowane) potrzebami ekonomicznymi czy po prostu inwestycjami kapitałowymi, które chcą w ten sposób zwiększyć swój stan posiadania. Jeszcze 100 lat temu badania naukowe były inspirowane głównie potrzebą rozwiązania istotnych problemów człowieka bądź społeczeństwa. W tym właśnie duchu należy widzieć badania takich naukowców, jak L. Pasteur (wynalazca szczepionki na wściekliznę), A. Fleming oraz H.W. Florey i E.B. Chain (odkrycie penicyliny) oraz F.G. Banting (odkrycie insuliny). Człowiek czuł się odtwórcą czy badaczem praw, które istniały w naturze, przykładem czego jest I. Newton, który odkrył – a nie stworzył – zasady dynamiki, oraz A. Einstein, który zbudował słynną teorię względności. Naukowcy aż do przełomu XIX i XX wieku starali się naturę odkrywać bądź poprawiać, zwłaszcza w obszarze zdrowia człowieka, nie zaś tworzyć nową rzeczywistość.

Wyniki badań naukowych tamtego okresu najczęściej nie wzbudzały obaw społecznych co do ich zgodności z moralnością czy szeroko rozumianą etyką. To nastawienie do badań naukowych, postępu i rozwoju nowych technologii oraz technik zmieniło się wraz z technologiami zaawansowanymi. Człowiek nie zajmuje się już odkrywaniem praw natury bądź też jej poprawianiem, lecz tworzeniem nowej rzeczywistości. Kończy się pewna epoka oparta na biblijnym nakazie czynienia sobie ziemi poddaną (Rdz. 1,28). W tej koncepcji człowiek miał być tylko użytkownikiem ziemi, miał prawo do korzystania z niej i pobierania pożytków. Nie jest jednak kreatorem, jest nim bowiem Bóg. Nowa epoka charakteryzuje się tym, że człowiek przechodzi od roli użytkownika do roli twórcy. Taka zmiana podejścia człowieka do materii ożywionej i nieożywionej jest możliwa właśnie dzięki zaawansowanym technologiom, zwłaszcza w obszarze technologii informatycznych. Pozwalają one na stworzenie nowej wirtualnej rzeczywistości, która z jednej strony głęboko przenika dotychczasowe życie jednostki i społeczeństwa, z drugiej zaś daje nowe, dotychczas niespotykane możliwości.

Przedmiotem niniejszego opracowania jest analiza treści zasad etycznych, jakie już funkcjonują w cyberprzestrzeni. Jest to bowiem rzeczywi-

stość globalna i rozproszona jednocześnie, trudna do skontrolowania. Chociaż podejmowane są w tym zakresie liczne próby. Między innymi Rosja, Chiny, a także ostatnio i Unia Europejska ustami komisarz E. Bieńkowskiej zapowiedziały stworzenie własnych systemów satelitarnych (GPS). Poza zapowiedziami, jak na razie nie udało się żadnemu państwu wprowadzić kontroli nad funkcjonowaniem cyberprzestrzeni.

W tej perspektywie jawi się jedyna możliwość, tj. formułowanie zasad odpowiedzialnej etyki, którą winni posługiwać się tak twórcy poszczególnych elementów cyberprzestrzeni, jak i użytkownicy poszczególnych instrumentów cyberprzestrzeni. Można powiedzieć, że normy etyczne są jednym z instrumentów, które pozwolą na jej uporządkowanie.

POJĘCIE CYBERPRZESTRZENI

Jednym z pojęć, które w ostatnich czasach zdobyło największą popularność, jest słowo „cyberprzestrzeń". Jednocześnie dla przeciętnego człowieka to pojęcie owiane jest nimbem tajemniczości. Niewiele osób zapytanych na ulicy o jego znaczenie byłoby w stanie je zdefiniować. Tymczasem można zaleźć liczne definicje tego pojęcia w profesjonalnym piśmiennictwie, w politykach sektorowych poszczególnych państw, korporacji oraz organizacji międzynarodowych, a także w aktach normatywnych krajowych, unijnych i międzynarodowych.

Twórcą pojęcia „cyberprzestrzeń" (*cyberspace*) jest William Gibson, który w 1982 roku użył go po raz pierwszy w powieści pt. „Burning Chrom". W powieści pt. „Neuromancer" zaprosił czytelników do cyberprzestrzeni, którą określał jako halucynacja doświadczana każdego dnia przez miliardy uczestników we wszystkich krajach. Cyberprzestrzeń według niego to graficzne odwzorowanie danych pobieranych z dysków wszystkich komputerów świata (zob. J. Wasilewski, s. 226).

Pojęcie „cyberprzestrzeń" jest pochodną wcześniej używanego terminu „cybernetyka" (*cybernetics*). Po raz pierwszy termin ten został sformułowany przez Norberta Wienera w 1948 roku. Według niego zadaniem cybernetyki było zbudowanie komunikacji pomiędzy światem ożywionym, zwłaszcza zwierząt, do których zaliczał człowieka, a światem maszyn. W ten sposób powstało nowe środowisko składające się z inteligentnych istot żywych i maszyn. Oba światy wzajemnie się przenikają i nie są rozdzielne (zob. J. Wasilewski, s. 226).

Dalszy rozwój koncepcji cyberprzestrzeni powiązany był z progresem technologii teleinformatycznych, służących do zwiększenia efektywności komunikacji w wielu obszarach życia, zwłaszcza w wojsku, w służbach specjalnych, w administracji publicznej oraz w wielkich korporacjach. Powstałe urządzenia teleinformatyczne stały się częścią państwowej, a także korporacyjnej infrastruktury krytycznej. Istotnym elementem tej infrastruktury stały się komputery i sieci, które służyły nie tylko do przekazywania informacji, ale również do zawierania czynności cywilnoprawnych, podejmowania decyzji administracyjnych, gromadzenia bądź archiwizowania danych (bazy danych). Negatywną stroną nowej przestrzeni aktywności człowieka było stworzenie nowych form przestępczości (zob. J. Wasilewski, s. 226; odnośnie do cyberprzestępczości zob. J. Wójcik, s. 99–116).

Według K. Dobrzenieckiego cyberprzestrzeń jest rodzajem kontrolowanego chaosu. Nie ma właściciela ani jednego centralnego ośrodka decyzyjnego. Pomimo tych ujemnych cech rzeczywistość ta funkcjonuje i szybko się rozwija. Próba podporządkowania cyberprzestrzeni przepisom praw napotyka opór wirtualnej społeczności oraz przeszkody natury technicznej, raczej trudne do przezwyciężenia. Stąd rodzą się pytania, w szczególności o relację twórców i użytkowników wirtualnej rzeczywistości do przepisów prawa, zasad etycznych czy obyczajności. Rodzi się bowiem nowy wymiar wolności i praw jednostki, który wymyka się spod klasycznych ograniczeń, jakie istnieją w świecie realnym (K. Dobrzeniecki, s. 15 i nast.).

Pojęcie „cyberprzestrzeń" definiowane jest w licznych dokumentach zawierających wytyczne dla polityki państwa. I tak, w „Rządowym programie Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016"[1] pojęcie to zostało zdefiniowane w następujący sposób: „Cyberprzestrzeń – cyfrowa przestrzeń przetwarzania i wymiany informacji tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami". Dodatkowo zaś zostało zdefiniowane pojęcie „cyberprzestrzeń RP", przez które rozumie się „cyberprzestrzeń w obrębie terytorium państwa Polskiego i w lokalizacjach poza terytorium, gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe)".

[1] Tekst Programu znajduje się na stronie internetowej: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf [data dostępu: 3.11.2016].

Z kolei w ekspertyzie dotyczącej rekomendowanego, optymalnego strategicznego modelu organizacji systemu bezpieczeństwa cyberprzestrzeni w Polsce, opracowanej przez NASK na zlecenie Ministerstwa Administracji i Cyfryzacji, przez cyberprzestrzeń rozumie się przestrzeń, którą tworzą urządzenia i programy informatyczne komunikujące się pomiędzy sobą i z użytkownikami[2].

W kolejnym dokumencie – „Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej" – przyjętym przez rząd Polski w 2015 roku cyberprzestrzeń zdefiniowano jako „przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci) wraz z powiązaniami między nimi oraz relacjami z użytkownikami"[3].

Ustawowa zaś definicja cyberprzestrzeni znajduje się w art. 2.1b ustawy z 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U. 2002 nr 156 poz. 1301). Według tej ustawy przez cyberprzestrzeń „[...] rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2014 r. poz. 1114), wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami".

Polskie definicje nie obiegają od tych, które stosuje się w doktrynie bądź polityce chociażby USA. Departament Obrony USA tak zdefiniował pojęcie „cyberprzestrzeń": jest to „globalna domena środowiska informacyjnego składająca się z współzależnych sieci tworzonych przez infrastrukturę

[2] Tekst ekspertyzy pt. *System bezpieczeństwa cyberprzestrzeni RP*, Warszawa, wrzesień 2015, znajduje się pod adresem internetowym: https://mac.gov.pl/files/nask_rekomendacja.pdf [data dostępu: 3.11.2016].

[3] Dokument znajduje się na stronie internetowej BBN pod adresem: https://www.bbn.gov.pl/pl/prace-biura/publikacje/6818,Doktryna-cyberbezpieczenstwa-RP.html [data dostępu: 4.11.2016].

technologii informacyjnej (IT) oraz zawartych w nich danych, włączając Internet, sieci telekomunikacyjne, systemy komputerowe, a także osadzone w nich procesory oraz kontrolery" (zob. J. Wasileski, s. 227).

Ciekawostką jest to, że pojęcie „cyberprzestrzeń" nie zostało zdefiniowane w „Strategii bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń" z 2013 roku[4]. Komisja przyjmuje znaczenie tego pojęcia jako coś oczywistego.

Słusznie stawia się akcent w powyższych dokumentach na bezpieczeństwo w cyberprzestrzeni, jednak głównie z zastosowaniem przepisów prawa, polityk okołounijnych bądź też poprzez rozbudowę zasobów przemysłowych i technologicznych wykorzystywanych na potrzeby bezpieczeństwa cybernetycznego. Nie ulega wątpliwości, że są to ważne i konieczne działania. Nie można jednak wszystkich zdarzeń, jakie mają miejsce w cyberprzestrzeni, uregulować przepisami prawa lub też rozwiązaniami technologicznymi. Konieczne jest również zdefiniowanie norm etycznych, które mogą być stosowane tam, gdzie nie dostaje prawo lub nowe technologie.

CZY W CYBERPRZESTRZENI JEST POTRZEBNA ETYKA?

Inspirowany przez biznes, a także potrzeby polityczne dynamiczny rozwój cyberprzestrzeni wymusza stosowanie nie tylko instrumentów prawnych, technicznych, ale i pozanormatywnych, tzw. miękkich (*soft law*). Już na samym początku należy zauważyć, że nieco inne treści będzie zawierała etyka dotycząca obszaru technologii informacyjnych (IT – *Information Technology*), a inaczej będą one wyglądały w systemach informacyjnych (IS – *Information System*). Pogłębiona analiza zasad etycznych winna obejmować również kwestie związane z problematyką rygoryzmu moralnego vs. relatywizm moralny, uniwersalizm vs. indywidualizm, oraz monizm vs. pluralizm, np. wielokulturowość. Tych kwestii jednak nie da się rozstrzygnąć w tak krótkim opracowaniu (zob. X. Wu, S. Rogerson, N.B. Fairweather).

Normy etyczne są niezbędne do zbudowania etosu zachowań akceptowanych w sieci. Wydaje się, że konieczne jest nawet zbudowanie swoistego dekalogu norm moralnych czy etycznych dla uczestników cyberprzestrzeni, w tym dla programistów. Właśnie te normy etyczne powinny być też elementem składowym procesu edukacji nowych pokoleń informatyków.

[4] JOIN(2013) 1 final.

Specyfiką tejże etyki jest to, że normy etyczne są definiowane już nie przez religię, ośrodki polityczne, kulturę, lecz przez uczestników cyberprzestrzeni, do których należy zaliczyć:

- projektantów,
- programistów,
- użytkowników,
- administratorów sieci komputerowych, baz danych i opiekunów komputerowych,
- a przede wszystkim wielkie korporacje działające na rynku elektronicznym.

Etyka dla IT

Technologie informatyczne tworzone są przez profesjonalistów. Dla ich użytku tworzone są akty wewnętrzne korporacji oraz przedsiębiorstw w formie kodeksów. Wzorcowe kodeksy etyczne, będące zbiorem zasad postępowania dla twórców narzędzi wykorzystywanych w cyberprzestrzeni, powstały przede wszystkim w USA, zwłaszcza w wielkich korporacjach przemysłu elektronicznego. Najbardziej znany jest kodeks IEEE – Institute of Electrical and Electronics Engineers, który jest częścią Strategii Rozwoju tejże firmy. Upływ czasu oraz pojawianie się nowych technologii IT sprawia, że jest on ciągle aktualizowany. Ostatnia jego wersja jest datowana na 2 lipca 2016 roku.

Podstawowym przesłaniem kodeksu etycznego IEEE jest to, aby pracownicy zobowiązali się do zachowywania najwyższych standardów etycznych oraz profesjonalnych. Do najważniejszych zasad etycznych tego kodeksu należą takie normy, jak:

- pracownicy firmy winni składać oświadczenia, że są świadomi znaczenia technologii w podnoszeniu jakości życia na świecie oraz że akceptują zobowiązania, jakie płyną z wykonywanego zawodu. W ten sposób pracownicy zobowiązują się do akceptowania odpowiedzialności za nowe produkty przez nich wytwarzane. Mogą one bowiem zagrażać bezpieczeństwu, zdrowiu, dobru publicznemu albo środowisku naturalnemu,
- pracownicy firmy zobowiązują się do unikania realnych lub możliwych konfliktów, a powstałe już konflikty zobowiązują się rozwiązywać bezpośrednio z osobami, między którymi ten konflikt powstał,
- pracownicy firmy winni cechować się takimi wartościami, jak uczciwość i profesjonalizm w obchodzeniu się z bazami danych,

- pracownicy tej firmy powinni odrzucać wszelkie formy nieuczciwości, winni podnosić swój poziom wiedzy i kompetencji dotyczących nowych technologii, aplikacji, ale też winni się uczyć o negatywnych i pozytywnych skutkach programów oraz aplikacji,
- pracownicy akceptują rzeczową krytykę współpracowników i przełożonych o swojej pracy; uznają i poprawiają własne błędy,
- pracownicy zobowiązują się do równego traktowania uczestników cyberprzestrzeni, niezależnie od rasy, religii, płci, niepełnosprawności, wieku czy narodowości,
- pracownicy unikają świadomego wyrządzania szkód innym osobom, ich własności czy reputacji,
- pracownicy mają być solidarni, a więc winni pomagać kolegom w ich profesjonalnym rozwoju oraz w przestrzeganiu norm prawnych i zasad etyki,
- pracownicy nie mogą używać komputera w celu szkodzenia innym użytkownikom cyberprzestrzeni oraz nie mogą zakłócać innym pracy na komputerze.

Typowo polski jest Kodeks Etyki z 2011 roku, który został zredagowany i przyjęty przez Polskie Stowarzyszenie Informatyków. Jest to kodeks skierowany do pracowników i osób przynależących do Stowarzyszenia. W pkt 1 podkreślono rolę służebną informatyków wobec klientów. W pkt 3 jest mowa o obowiązku doskonalenia wiedzy przez informatyków. W pkt 6 zobowiązani są do zachowania integralności systemów komputerowych, które obsługują. Stąd też muszą swojemu klientowi przedstawiać rzetelną informację o tym, co robią, i muszą zrobić tak, aby system informacyjny działał sprawnie. Informatycy skupieni w Polskim Stowarzyszeniu Informatyków nie mogą też naruszać zasad uczciwej konkurencji, czyli nie mogą np. podejmować pracy w firmach, które ze sobą konkurują[5].

Etyka dla SI

Etyka dla użytkowników systemów informacyjnych musi mieć charakter ogólny, nie tak jak to jest w przypadku etyki korporacyjnej bądź zawodowej. Najbardziej znany obecnie zbiór takich zasad powstał w 1992 roku w Wa-

[5] Tekst Kodeksu Etyki Polskiego Stowarzyszenia Informatyków znajduje się na stronie internetowej pod adresem: http://www.pti.org.pl/index.php/KZI-Kodeks-zawodowy-informatykow-PTI-29-maja-2011-r2 [data dostępu: 4.11.2016].

szyngtonie i został utworzony przez Instytut Etyki Komputerowej (*Computer Ethics Institute*). Instytut ten powstał w 1985 roku, wydał on 10 przykazań, jakimi powinni posługiwać się użytkownicy komputerów czy cyberprzestrzeni. Układ przykazań nie jest przypadkowy, bowiem wzorowany jest na biblijnym Dekalogu, zresztą jak również niektóre treści. Przykazania te były później przyjmowane w piśmiennictwie, niekiedy też były krytykowane.

Te 10 przykazań zostało zdefiniowane od strony negatywnej, tak jak Dekalog. Są to następujące przykazania[6]:

1. Nie używaj komputera w celu szkodzenia innym. Zakaz ten nie ogranicza się do szkód fizycznych, ale dotyczy głównie szkód wyrządzonych innym użytkownikom komputerów poprzez uszkodzenie ich plików, napisanie aplikacji, która będzie wykradała dane z innych komputerów, nieuprawnione kopiowanie danych, wejście w komputer bez zgody właściciela. Do tej kategorii zachowań nieetycznych zalicza się również zaangażowanie w hakerstwo, spamowanie, wyłudzanie informacji, cyberprzemoc.
2. Nie zakłócaj pracy innym na komputerze. Takie działanie materializuje się m.in. poprzez używanie komputera lub oprogramowania w taki sposób, aby zakłócać prace innych. Przykładem może być wpuszczanie do sieci wirusów komputerowych, które zaburzają normalną pracę innych użytkowników cyberprzestrzeni. Takie zaburzenia mogą przybierać różną formę. Może to być zablokowanie pamięci operacyjnej, przez co komputery zainfekowane nie mogą normalnie pracować lub pracują powoli, może to być też użycie programów normalnie funkcjonujących, ale są też wykorzystywane do przeprowadzenia ataku na inne komputery bądź na systemy informatyczne instytucji publicznych lub nawet państwa.
3. Nie podglądaj treści na komputerze innych ludzi. Nie jest moralnie i prawnie dopuszczalne czytanie cudzych listów, w tym maili oraz SMS-ów. Jest to też naruszenie praw człowieka do prywatności. Ograniczeniem tego przykazania będzie kontrola komputera i jego zawartości przez uprawnione do tego służby, w razie nadużycia stosowania urządzeń elektronicznych, np. gromadzenie na dysku pornografii dzie-

[6] Wykaz tych przykazań oraz objaśnienia ich znaczeń w dużej mierze zostały opracowane na podstawie hasła *Ten Commandments of Computer Ethics,* [w:] en.wikipedia.org. Adres: https://en.wikipedia.org/wiki/Ten_Commandments_of_Computer_Ethics [data dostępu: 4.11.2016].

cięcej. Zajmują się tym wyspecjalizowane instytucje śledzące aktywność użytkowników cyberprzestrzeni, którzy dopuszczają się czynów o charakterze kryminalnym lub terrorystycznym. Także pracodawca jest uprawniony do kontroli zawartości komputerów, na których pracują pracownicy w jego firmie.

4. Nie używaj komputera do kradzieży informacji wrażliwych lub poufnych. Chodzi o informacje, które dotyczą pracowników, pracodawcy, pacjentów ze szpitala lub tym podobnych. Podobnie należy traktować włamanie się do banku danych bądź też nielegalny transfer danych. Praktyki te są coraz częstsze z powodu postępu technologicznego.
5. Nie używaj komputera do tworzenia lub rozpowszechniania fałszywych informacji przez Internet lub maile. Nieetyczne jest zatem uczestniczenie w procesie rozpowszechniania fałszywych i zniesławiających informacji dotyczących osób lub firm. Dość częstą praktyką w Internecie jest rozpowszechnianie fałszywych informacji o odkryciach naukowych oraz o produktach (nieprawdziwa reklama). Niektóre państwa celowo tworzą fałszywe opisy wydarzeń historycznych tylko po to, aby zmienić historiografię. Do realizacji tego celu wykorzystuje się fakt, że prawdziwe zdarzenia są opisane w publikacjach drukowanych, do których, zwłaszcza młode pokolenie, już nie sięga. Czytane czy wręcz kopiowane są informacje znajdujące się w Internecie, często zmanipulowane czy wręcz nieprawdziwe. Brak konfrontacji tekstów drukowanych z wirtualnymi sprawia, że młode pokolenie wychowywane jest już na bazie informacji nieprawdziwych i zmanipulowanych, które przyjmuje jako prawdziwe.
6. Nie kopiuj ani nie używaj oprogramowania, za które nie zapłaciłeś. Każdy programista ma prawa autorskie do programu, który napisał. Podobnie zresztą jak twórca innego dzieła intelektualnego. Respektowane też muszą być prawa własności intelektualnej zakładu pracy, w którym programista pracuje i dla którego tworzy oprogramowania. Stąd nielegalne używanie kopii programów komputerowych jest uznawane za bezprawne i nieetyczne.
7. Nie korzystaj z zasobów komputera innych bez ich zgody lub bez adekwatnej zapłaty. Za nieetyczny uznaje się nieuprawniony dostęp do cudzego komputera, jego zasobów lub udostępnianie danych nielegalnie uzyskanych innym użytkownikom sieci. Jest to forma naruszenia

ich prawa do prywatności. Takie zachowanie materializuje się poprzez nieuprawnione wejście w posiadanie hasła do cudzego komputera lub jego poszczególnych zasobów. Nieetyczne jest również uprawnione korzystanie z zasobów cudzego komputera lub baz danych, ale bez zapłaty. Przykładem może być korzystanie z prywatnych zasobów naukowych, do których jest otwarty dostęp, ale za odpłatnością. Niespełnienie tego wymogu jest również działaniem nieetycznym.

8. Nie zawłaszczaj cudzej własności intelektualnej. Program jest własnością jego wytwórcy lub organizacji, dla której wytwórca pracuje. Zatem kopiowanie programu i rozprowadzenie go w formie odpłatnej lub nieodpłatnej pod własnym imieniem uznawane jest za zachowanie nieetyczne.
9. Nie zapominaj o skutkach społecznych programu, który napisałeś, lub programu, który zaprojektowałeś. Programy komputerowe są używane przez miliony użytkowników w różnym wieku, poczynając od małych dzieci, a kończąc na osobach starszych. Są to w szczególności gry komputerowe, animacje, programy edukacyjne, które mają znaczący wpływ na ich użytkowników. Stąd twórcy programów komputerowych winni czuć się moralnie odpowiedzialni za konsekwencje społeczne, jakie swoim działaniem mogą wywołać. Programiści zatem powinni uwzględniać specyfikę grupy docelowych odbiorców ich produktów nie tylko pod względem treści, możliwości percepcyjnych, ale również pod kątem ich systemu wartości i wrażliwości. Świadome pisanie programów negatywnie oddziaływających na odbiorców jest uważane za nieetyczne, podobnie zresztą jak to jest w przypadku reklam.
10. Zawsze używaj komputera w taki sposób, aby zapewnić respektowanie praw innych użytkowników. Obecnie komputer stał się podstawowym narzędziem komunikowania się w cyberprzestrzeni. Do tego służy nie tylko poczta elektroniczna, ale również portale społecznościowe czy czat. Normy etyczne obowiązujące w tego rodzaju komunikacji w cyberprzestrzeni w dużej mierze są takie same, jakie obowiązują w komunikacji, która ma miejsce w realnym świecie. Zatem komunikujący się ze sobą, niezależnie od środka, winni: nie stosować języka wulgarnego, nie umieszczać nieodpowiedzialnie negatywnych znaków obok nazwiska innych osób, np. negatywnych emotikonów, nie naruszać prawa innych do prywatności poprzez rozpowszech-

nianie informacji prawdziwych, ale zniesławiających, np. informacji o romansie, w końcu nie należy składać fałszywych deklaracji, np. dotyczących statusu cywilnego czy wykształcenia. Komunikacja przez Internet powinna też respektować czas innych użytkowników.

Etyka a prawo komputerowe

Jedną z szybciej rozwijających się gałęzi prawa jest prawo komputerowe. Jego zadaniem jest regulacja zasad korzystania z własności programów oraz danych znajdujących się w bazach danych. Kluczową zatem kwestią jest własność, która odpowiada nowemu rodzajowi przedmiotów niematerialnych tworzonych i funkcjonujących w cyberprzestrzeni. Ponadto prawo komputerowe tworzy zasady bezpieczeństwa, zwłaszcza chroni prawo do prywatności i integralności. Określa zasady dostępu do komputera, sieci informatycznej oraz usług informatycznych.

W przepisach prawa przewiduje się ochronę, w szczególności reguluje zachowanie ludzi, którzy używają komputerów i sieci. Przepisy prawa dotyczą zwłaszcza:

- ochrony praw autorskich dotyczących programów bądź projektów programów,
- ochrony komputera i sieci przed działaniami kryminalnymi,
- ochrony haseł i danych zawartych w komputerach,
- ochrony dostępu do programów i usług internetowych,
- ochrony baz danych zawierających dane o osobach, dane technologiczne czy inne (zob. A. Junker, M. Benecke, s. 35 i nast.).

Prawo określa tylko ogólne zasady poruszania się w cyberprzestrzeni, stąd nie zawsze w sposób odpowiedni może zagwarantować należyty poziom kontroli działań w komputerze i w Internecie. Ponadto prawo komputerowe rozwija się dość powoli i nie nadąża za postępem technicznym w tej dziedzinie i rozwojem cyberspołeczności.

Nie jest tajemnicą, że sędziowie, prawnicy, politycy, pracownicy administracji publicznej lub policjanci nie zawsze rozumieją zasady korzystania z urządzeń technicznych związanych z cyberprzestrzenią, nierzadko nie rozumieją poleceń komputerowych. Wielu użytkowników cyberprzestrzeni nie rozumie, w jaki sposób komputer i korzystanie z niego może podlegać przepisom prawnym. Należy dysponować specjalną wiedzą. Na jej

zdobycie konieczne jest dużo czasu. Wszyscy musimy mieć czas na adoptowanie się do nowej sytuacji i powstanie kultury bycia w cyberprzestrzeni. Pomocne w tym są właśnie zasady etyki, które tworzone są przez samą cyberspołeczność.

PODSUMOWANIE

Postęp techniczny w ostatnich 30 latach nabrał tempa dotąd niespotykanego w dziejach ludzkości. Jednym z obszarów prawie całkowicie nowych, stworzonych przez człowieka jest cyberprzestrzeń. Ma ona charakter globalny i nie jest kontrolowana przez jakiekolwiek państwo. Tworzy się nowa społeczność, do niedawna jeszcze określana jako wirtualna. Brak kontroli nie oznacza anarchii. Stąd dość dynamicznie rozwija się prawo internetowe, a także zasady etyczne typowe dla cyberprzestrzeni.

Na cyberprzestrzeń składają się technologie i sieci informatyczne. Dla każdego z tych obszarów zbudowano podobne, ale jednak znacząco różniące się zasady etyczne. Dla technologii informacyjnych tworzone są kodeksy etyczne. Wzorcowe kodeksy etyczne dla informatyków powstały w USA. Z tych wzorców czerpią również polscy informatycy skupieni w Polskim Towarzystwie Informatyków. Z kolei dla sieci informatycznych, czyli dla zwykłych użytkowników, stworzono swoisty dekalog etyczny.

Budowa norm etycznych dla cyberprzestrzeni jest ważnym zadaniem, wymagającym przemyślenia. Niemniej jednak można powiedzieć, że nie odbiegają one zasadniczo od norm etycznych stosowanych w świecie realnym. Czymże jest bowiem zakaz kradzieży dóbr intelektualnych, zakaz zniesławiania w sieci, zatrudnianie profesjonalistów, czymże jest uczciwość i szacunek dla drugiej osoby, jak nie wartościami często przytaczanymi z prawa rzymskiego i nauki katolickiej.

Bibliografia

Dobrzeniecki K. (2004). *Prawo a etos cyberprzestrzeni*. Toruń.

Junker A., Benecke M. (2000). *Computerrecht*. Baden-Baden 2000.

Wasilewski J. (2013). *Zarys definicji cyberprzestrzeni*. „Przegląd Bezpieczeństwa Wewnętrznego", 5/9/2013.

Wójcik J. (2009). *Cyberprzestrzeń i jej główne zagrożenia: cyberprzestępczość i cyberterroryzm*, [w:] Lisiecki M. i in., *Bezpieczeństwo wewnętrzne Rzeczpospolitej Polskiej na tle innych państw Unii Europejskiej*. Józefów.

Źródła internetowe

http://www.pti.org.pl/index.php/KZI-Kodeks-zawodowy-informatykow-PTI-29-maja-2011-r2 [data dostępu: 4.11.2016].

https://en.wikipedia.org/wiki/Ten_Commandments_of_Computer_Ethics [data dostępu: 4.11.2016].

https://mac.gov.pl/files/nask_rekomendacja.pdf [data dostępu: 3.11.2016].

https://www.bbn.gov.pl/pl/prace-biura/publikacje/6818,Doktryna-cyberbezpieczenstwa-RP.html [data dostępu: 4.11.2016].

https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf [data dostępu: 3.11.2016].

Wu X., Rogerson S., Fairweather N.B., *Ethical Considerations on Information System Development: Perspectives on a Practical Moral Framework*, http://rccs.southernct.edu/category/ethicomp-99/ [data dostępu: 4.11.2016].

MAGDALENA EL GHAMARI
Uniwersytet w Białymstoku
Zakład Bezpieczeństwa Międzynarodowego
elghamari@op.pl

NOWOCZESNE NARZĘDZIA INFORMATYCZNE W WALCE Z EKSTREMIZMEM ISLAMSKIM

MODERN TOOLS IN THE FIGHT AGAINST ISLAMIC EXTREMISM

Piraci komputerowi rozsyłają w świat wirusa, który otwiera na twardym dysku „tylne drzwi", umożliwiające terrorystom zdalne kontrolowanie komputerów elektrowni atomowych, banków, linii lotniczych, laboratoriów farmaceutycznych, wodociągów. Cyfrowa epidemia paraliżuje cały świat[1]

ABSTRACT

Combating terrorism information has become not only an important matter of policy, but also, and perhaps above all, the problem of economic nature. Cyberterrorist can also adjust their activities in order to maximize the positive outcome for themselves. In addition, cyberterrorism does not require physical training or high security logistics. There also requires travel. Cyberterrorism is not a separate or specific type of terrorism because of ideology. It serves exactly the same purpose as bombings, kidnapping or hostage taking. There are only a form – using computer hardware and software.

Cyberattacks do not pose a risk of death or physical injury, reduce the need for so risking life – attacks on the network do not require for suicide attacks. To carry out such an attack, you do not need to have virtually no skill – you can rent a cracker who broke security (often without realizing the consequences of his actions) money will carry out a terrorist attack.

Past examples of cyber crimes show how a large number of people may be affected by the consequences of such action; this is due to the global nature of computerization. Thus one of the essential objectives of terrorists – mediality attack – is huge. A separate issue is the use of the Internet and computers

[1] Meyer E., Kerdellant Ch., *Cyfrowa katastrofa*.

by terrorists for purposes other than direct attacks. Computer systems are a great collection and exchange of information and communication. They provide anonymity, allow coding or hiding information. Transfers can be hidden do not raise suspicions text files or graphics.

Keywords: *extremism, radicalization, modern technology, cyberterrorism*

STRESZCZENIE

Zwalczanie terroryzmu informatycznego stało się nie tylko ważnym zagadnieniem natury politycznej, ale również, a może przede wszystkim, problemem natury ekonomicznej. Cyberterroryści mogą również dostosować swoje działania tak, aby zmaksymalizować pozytywny dla siebie wynik. Ponadto cyberterroryzm nie wymaga treningu fizycznego ani dużego zabezpieczenia logistycznego. Nie wymaga również podróżowania. Cyberterroryzm nie jest odrębnym lub specyficznym rodzajem terroryzmu ze względu na ideologię. Służy dokładnie tym samym celom co zamachy bombowe, porwania oraz branie zakładników. Wyróżnia się tylko formą – zastosowaniem sprzętu i oprogramowania komputerowego.

Ataki w cyberprzestrzeni nie stwarzają ryzyka poniesienia śmierci lub obrażeń fizycznych, ograniczają więc konieczność narażania życia – zamachy w sieci nie wymagają bowiem ataków samobójczych. Aby przeprowadzić taki atak, nie potrzeba posiadać praktycznie żadnych umiejętności – można wynająć crackerów, którzy łamiąc zabezpieczenia (często nie zdając sobie sprawy ze skutków swojego działania), za pieniądze przeprowadzą atak terrorystyczny.

Dotychczasowe przykłady przestępstw informatycznych pokazują, jak wielka liczba ludzi może być dotknięta skutkami takiego działania; wynika to z globalnego charakteru informatyzacji. Tym samym jeden z zasadniczych celów terrorystów – medialność ataku – jest przeogromny. Odrębną kwestią jest wykorzystanie Internetu i komputerów przez terrorystów w celach innych niż bezpośrednie zamachy. Systemy komputerowe są doskonałym środkiem zbierania i wymiany informacji oraz łączności. Zapewniają anonimowość, pozwalają na kodowanie lub ukrywanie informacji. Przekazy mogą być ukryte w niebudzących podejrzeń plikach tekstowych czy graficznych.

Słowa kluczowe: *ekstremizm, radykalizacja, nowoczesna technologia, cyberterroryzm*

WPROWADZENIE

Do podstawowych zasad rządzących współczesnym światem należą: zmienność, ekspansywność oraz z pewnością żywotność. Jedna sekunda w sieci 3 października 2016 roku w skali światowej oznaczała:

- 7363 wysłane nowe tweety,

- 744 nowe zdjęcia na Instagramie,
- 1164 nowe posty na Tumblr,
- 2294 rozmowy prowadzone za pomocą komunikatora Skype,
- 38 456 GB nowych danych,
- 56 538 wyszukiwań fraz oraz słów w wyszukiwarce Google,
- 132 412 obejrzanych filmów na YouTubie,
- 2 528 192 wysłanych maili[2].

Jak pokazuje to krótkie doświadczenie, dostęp do tej kompleksowej sieci wymiany doświadczeń oraz wiedzy staje się przymusem w obecnym świecie. Chcąc nadążać za współczesnym światem i jednocześnie nowymi technologiami, nie mamy wyboru – musimy płynąć z nurtem wiedzy zanurzonej w technologii. Świat, jaki powstaje poprzez fundamentalne zmiany, które nastąpiły wraz z rozwojem Internetu, ciągle wywołuje transformację, której efektów nie jesteśmy w stanie przewidzieć. Zmiana społeczna, kulturowa, ekonomiczna, nowa jakość zagrożeń. To wszystko to jedynie początek tego, co przyniosła nam rewolucja technologiczna XXI wieku – kultura cyberprzestrzeni, wirtualne społeczności, nowy język sieci, owe wzory interakcji międzyludzkich. Wszystko to warunkuje stwierdzenie, że funkcjonujemy w obszarze czterech społeczności etnicznych w sieci: społeczeństwo wirtualne, gdzie ludzie kontaktują się wyłącznie przez Internet; społeczeństwo obywatelskie, którego celem jest rozpowszechnianie informacji dotyczącej danej grupy oraz działania systemu demokratycznego; społeczeństwo dyskusyjne – jego członkowie skupiają się wokół wybranego problemu, forum dyskusyjnego, zainteresowań, oraz społeczeństwo wspomagające, gdzie ludzie kontaktują się zarówno przez Internet, jak i w świecie rzeczywistym.

CYBERTERRORYZM

Po raz pierwszy termin „cyberterroryzm" użyty został w 1979 roku przez szwedzkie Ministerstwo Obrony w raporcie o zagrożeniach komputerowych. Cyberterroryzm, zwany również hi-terroryzmem albo terroryzmem informacyjnym, jest połączeniem dwóch słów: cyberprzestrzeni i terroryzmu. Czym jest cyberprzestrzeń? To przestrzeń komunikacyjna tworzona przez system powiązań internetowych. Jeśli chodzi o sam

[2] http://www.internetlivestats.com/one-second/ [data dostępu: 3.10.2016].

terroryzm, terminów i definicji jest wiele. Ogólnie rzecz biorąc, jest to fakt dokonywania aktów terroru z pobudek politycznych, powodujących ogromne straty i wywołujących powszechne poczucie strachu. W cyberterroryzmie broń zastąpiona zostaje komputerem podłączonym do sieci, a atak wymierzony jest w system informatyczny państwa i znajdujące się w nim dane. Przeważnie atak taki skutkować ma uniemożliwieniem efektywnego wykorzystania najważniejszych gałęzi gospodarki państwa, takich jak infrastruktura bankowa, transport, energetyka czy instytucje państwowe (E. Aronson, A. Pratkanis, 2004, s. 41).

Tezą niniejszego artykułu, poddaną wnikliwej analizie, jest stwierdzenie, że każde państwo może być zagrożone atakiem cyberterrorystów. Niestety, ze szkodami tym większymi, im bardziej skomputeryzowana jest gospodarka danego kraju. Co więcej, każde państwo może dokonać ataku cybernetycznego, jeżeli tylko znajdą się w nim profesjonalni hakerzy, zdolni, zmotywowani i gotowi do jego przeprowadzenia.

Termin „cyberterroryzm" poruszył Barry Collin z Institute for Security and Intelligence w Kalifornii (J. Adamski, 2007, s. 56). Stworzył termin „cyberterroryzm" jako pojęcie zbieżne dla przestrzeni cybernetycznej i terroryzmu. Natomiast Mark Pollit, agent FBI, zaproponował definicję roboczą: „Cyberterroryzm to zamierzony, motywowany politycznie atak na informację, system komputerowy, programy komputerowe i dane, którego skutkiem jest użycie przemocy wobec celów niewalczących przez grupy ponadnarodowe bądź tajnych agentów" (M. Pollit, październik 1997, s. 285–289).

Później pojawiały się kolejne definicje starające się uzupełnić ciągle ewoluujący termin. Według US Federal Bureau of Investigation: „(...) jest to obmyślony, politycznie umotywowany akt przemocy wymierzony przeciwko informacjom, programom, systemom komputerowym lub bazom danych, który mając charakter niemilitarny, przeprowadzony jest przez ponadnarodowe lub narodowe grupy terrorystyczne", zaś Dorothy Denning stwierdza, że jest to „(...) groźba lub bezprawny atak wymierzony w system informatyczny lub zgromadzone dane, w celu zastraszenia czy wymuszenia na władzach państwowych lub jej przedstawicielach ustępstw lub oczekiwanych zachowań, w celu wsparcia określonych celów (np. politycznych). Aby działania takie zostały zakwalifikowane jako terroryzm informacyjny, atak powinien powodować znaczne straty lub takie skutki, które wywołu-

ją powszechne poczucie strachu". Inny badacz, James Lewis, konkluduje, iż cyberterroryzm to: „wykorzystanie sieci komputerowych jako narzędzia do sparaliżowania lub poważnego ograniczenia możliwości efektywnego wykorzystania struktur narodowych (takich jak energetyka, transport, instytucje rządowe itp.) bądź też do zastraszenia czy wymuszenia na rządzie lub populacji określonych działań". Według US National Infrastructure Protection Centre jest to: „akt kryminalny popełniony przy użyciu komputera i możliwości telekomunikacyjnych, powodujący użycie siły, zniszczenie i/lub przerwanie świadczenia usług dla wywołania strachu, poprzez wprowadzanie zamieszania lub niepewności w danej populacji, w celu wpływania na rządy, ludność tak, aby wykorzystać ich reakcje dla osiągnięcia określonych celów politycznych, społecznych, ideologicznych lub głoszonego przez terrorystów programu" (R. Kosta, 2007, s. 27). Analiza przedstawionych definicji pozwala zaobserwować pojawiające się w nich dwa zasadnicze wyróżniki. Definicje cyberterroryzmu uzupełniają się i uwzględniają to, że istnieje możliwość wykorzystania systemów komputerowych lub telekomunikacyjnych do przeprowadzenia ataku cybernetycznego. Ponadto powyższe definicje zawierają określenie, że komputery i systemy informacyjne są celem takiego ataku. Problematyczne staje się to, iż wielokrotnie cyberterroryzm i cyberatak są traktowane jako elementy równoważne, co w konsekwencji prowadzi do nieporozumień. D. Denning uważa, że politycznie umotywowany cyberatak, który prowadzi do śmierci, ofiar lub uszkodzeń ciała, eksplozji bądź poważnych strat materialnych, może być przykładem cyberterroryzmu[3]. Takim działaniem nie jest przypadek ataku, który jedynie zakłóca przyjęty porządek prawny lub ekonomiczny lub taki, który nie pociąga za sobą zasadniczych zakłóceń lub strat. Opierając się na wybranych wskaźnikach i wybiórczym traktowaniu przedstawionych definicji, należy stwierdzić, że do tej pory nie było przypadku cyberterroryzmu (D. Denning, 2002, s. 77). Jeśli zaś zastosuje się kryteria kwalifikacyjne, okazuje się, że zdarzyło się kilka przypadków takich działań. Nie były one jednak poparte motywacją polityczną lub inną, która kwalifikowałaby je jako przypadki terroryzmu[4].

[3] D. Denning, *Cyberterrorism*, http://www.cs.georgetown.edu/ ~denning/infosec/cyberterror-GD.doc [data dostępu: 24.08.2000].

[4] L. Garrison., M. Grand, *Cyberterrorism: An evolving concept, NIPC Highlights*, http://www.nipc.gov/publications/highlights/2001/ highlight-01-06.htm 6.

Efekty działań zagrożeń cyberterrorystycznych można sklasyfikować za pomocą poniższego podziału:

- małe skutki ekonomiczne zakłócenia systemu informatycznego,
- małe skutki ekonomiczne zakłócenia systemu informatycznego połączone z ofiarami,
- poważne skutki ekonomiczne zakłócenia systemu informatycznego,
- poważne skutki ekonomiczne zakłócenia systemu informatycznego połączone z ofiarami,
- działania stanowiące zagrożenie dla bezpieczeństwa narodowego[5].

Charakter działań cyberterrorystów można podzielić na: działania bezprawne, hakerstwo, szpiegostwo, cyberterroryzm i cyberagre. Ponadto na działalność cyberterrorystyczną składa się wiele technik. Część z nich może być stosowana praktycznie przez każdego członka organizacji, natomiast pozostałe wymagają dużych umiejętności praktycznych oraz właściwego przygotowania teoretycznego. Jedną z technik jest tzw. *web sit-in*, czyli okupowanie sieci przez dużą liczbę użytkowników w tym samym czasie, powodując przez to utrudnienie lub brak możliwości wywołania strony (D. Verton, 2004, s. 133). Takie zdarzenie miało miejsce chociażby w listopadzie 2000 roku po wybuchu powstania palestyńskiego, gdy witrynę IDF okupowało tygodniowo blisko 130 tys. osób, podczas gdy przed wybuchem zamieszek stronę odwiedzało około 7 tys. internautów. Skuteczność kolejnej techniki zwanej *flooding* przedstawia atak separatystów tamilskich na serwery ambasad Sri Lanki w 1998 roku. Polegał on na wysyłaniu około 1 tys. e-maili przez okres dwóch tygodni z oświadczeniem kwestii roszczeń niepodległościowych, zakończonych informacją mówiącą o celowości działań. Atak całkowicie sparaliżował komputerowy system łączności MSZ Sri Lanki oraz systemy informatyczne kilku ambasad tego państwa. W ostatnim okresie wśród zwolenników radykalnych islamistów można zaobserwować zjawisko postępującej koordynacji ataków tego typu. Przygotowania do nich są zapowiadane z wyprzedzeniem na internetowych forach dyskusyjnych. Koordynaty oraz termin i czas ataków podaje się dopiero około 30 minut przed ich dokonaniem. Czę-

[5] L. Staten Clark, zeznanie przed Subcommitte of Technology, Terrorism and Government Information, U.S. Senate Judiciary Committee [data dostępu: 24.02.1998].

sto dołączane jest również specjalistyczne oprogramowanie opracowane przez islamistyczne grupy hakerskie, np. Al-Jihad czy Dorach War Engine (M.F. Gawrycki, 2003, s. 166–167).

Najnowsze wersje programów opracowywanych przez radykalnych islamistów umożliwiają zdalne ładowanie obiektów ataków ze stron ich administratorów oraz synchronizowanie akcji z innymi uczestnikami. W atakach uczestniczy zwykle kilka tysięcy osób. Mimo że skuteczność takich działań jest obecnie niewielka, zagrożenia nie można lekceważyć, ponieważ islamiści nie rezygnują z prowadzenia takich akcji i stale udoskonalają wykorzystywane oprogramowanie. O wysokich ambicjach ich działań świadczy planowany zmasowany atak przeciw serwerom wybranych banków amerykańskich w grudniu 2006 roku pod nazwą „The Electronic Guantanamo Raid". Ostatecznie został on jednak odwołany najprawdopodobniej z powodu dekonspiracji[6].

Kolejne zagrożenie wiązało się z możliwością wprowadzenia do systemów szkodliwego oprogramowania. Rozpowszechnione i łatwo dostępne w Internecie automatyczne generatory są w stanie utworzyć nieskomplikowane wirusy i robaki. Takie oprogramowanie usiłował nabyć pod koniec 1998 roku Khalid Ibrahim, członek powiązanego z Al-Kaidą separatystycznego ugrupowania Hakat-ul-Ansar, działającego w Indiach. Opierając się na amerykańskich źródłach, z pełną odpowiedzialnością można stwierdzić, że organizacje terrorystyczne mają już specjalistów zdolnych do tworzenia szkodliwego oprogramowania. Agencja Bezpieczeństwa Narodowego Stanów Zjednoczonych (NSA) wskazuje, że tylko do końca 2001 roku około 60% dyplomów ukończenia studiów uniwersyteckich przez studentów zagranicznych w USA na kierunkach związanych z informatyką uzyskali obywatele państw muzułmańskich. Wynika z tego, że Amerykanie sami szkolą swoich potencjalnych wrogów, a także wrogów całej cybernetyki. Sytuacja jest o tyle groźna, że duża część grupy absolwentów nie wróciła do swoich państw, lecz została w USA (K. Kerr, 2003, s. 29).

Pewną klasyfikację osób dokonujących ataków w cyberprzestrzeni (ze względu na motywacje polityczne) podaje Dorothy E. Denning. Wyróżnia ona (oprócz hakerów) także: aktywistów, haktywistów i cyberterrorystów. Ponadto wyróżnia się grupy zorganizowane i cyberterrorystów indywidualnych.

[6] I. Bunsch., J. Świątkowska, *Cyberterroryzm – Nowa forma zagrożenia bezpieczeństwa międzynarodowego w XXI wieku*, s. 17, http://ik.org.pl/pl/ publikacja/nr/4298/ [data dostępu 15.06.2012].

Wszystkie organizacje terrorystyczne, które korzystają z sieci, charakteryzują się pewnymi cechami. Są to przede wszystkim:

- budowanie i zmienianie komunikacji oraz koordynacji stosownie do zadań,
- nieformalne powiązania o różnym stopniu intensywności (zależnie od potrzeb),
- brak biurokratycznego zarządzania, lecz więzy wewnętrzne i zewnętrzne umożliwiające podzielanie wspólnych norm i wartości oraz wzajemne zaufanie,
- uzupełnianie wewnętrznych sieci przez łączność z osobami niezwiązanymi z organizacją (możliwość wychodzenia poza granice państw) (por. B. Adkins, 2001, s. 51).

Systemy informatyczne, które mogą być zaatakowane, to między innymi:

- systemy, które wspomagają zarządzanie transportem (szczególnie kolejowym) oraz ruchem powietrznym,
- systemy, które wykorzystywane są w instytucjach państwowych, a których działanie opiera się na sprawnym funkcjonowaniu baz danych,
- systemy powiadamiania służb ratowniczych i reagowania antykryzysowego,
- systemy, które pracują w różnych sektorach – np. bankowości – oraz stosowane są przy produkcji i dystrybucji dóbr o strategicznym znaczeniu (energia elektryczna, woda, gaz, ropa) (zob. P. Monge, F. Janet, [w:] Shaping G. Desanctis, J. Fulk, 1999 s. 58–61).

Ataki te mogłyby zniszczyć lub przerwać działanie infrastruktury krytycznej państwa poprzez wykorzystanie słabości komputerowych. Do głównych elementów tej infrastruktury zalicza się:

- telekomunikację: linie telefoniczne, satelity, sieci komputerowe, komercyjne, wojskowe, akademickie,
- system energetyczny: produkcja, przemysł i dystrybucja energii oraz transport i magazynowanie surowców niezbędnych do jej produkcji,
- produkcję, magazynowanie i transport gazu ziemnego i ropy naftowej: cały proces wydobycia ropy naftowej i gazu ziemnego,
- przetwarzanie, magazynowanie i transportu za pomocą statków, rurociągów, transportem kolejowym i kołowym,

- system bankowy i finansowy: system przepływu kapitałów,
- transport: lotniczy, kolejowy, morski, rzeczny, drogowy osób i towarów oraz system wsparcia logistycznego,
- system zaopatrzenia w wodę: ujęcia wody, zbiorniki wodne, wodociągi, systemy filtrowania i oczyszczania wody, dostarczania jej dla rolnictwa, przemysłu, straży pożarnych i indywidualnych odbiorców,
- służby ratownicze: komunikacja ze służbą zdrowia, strażą pożarną i policją,
- ciągłość funkcjonowania władzy i służb publicznych.

Wśród obiektów infrastruktury krytycznej należy wymienić również tzw. krytyczną infrastrukturę teleinformatyczną, na której działaniu opiera się większość systemów odpowiedzialnych za prawidłowe funkcjonowanie większości instytucji i przedsiębiorstw w państwie. Działanie tej infrastruktury oparte jest na prawidłowym działaniu wielu systemów na nią złożonych.

Obecnie można wyróżnić trzy poziomy zagrożenia związanego z cyberterroryzmem. Pierwszym z nich jest tzw. *simple-unstructured*. Polega on na dokonaniu przez cyberterrorystów prostych włamań do indywidualnych systemów informacyjnych poprzez wykorzystanie narzędzi internetowych skonstruowanych przez inną osobę. Zgodnie z tym organizacje terrorystyczne nie mają zdolności analizy celów, które będą przedmiotem ataku, a także dowodzenia, kontroli czy uczenia się nowych metod atakowania w cyberprzestrzeni. Drugim poziomem zagrożenia jest tzw. *advanced-structured*. W poziomie tym cyberterroryści dokonują bardziej skomplikowanych ataków przeciw złożonym sieciom komputerowym i systemom. Mają możliwość tworzenia lub modyfikacji własnych narzędzi, które służą do atakowania w cyberprzestrzeni, mają zdolność analizy celów, które będą przedmiotem ataku, a także dowodzenia, kontroli i uczenia się nowych metod atakowania. Ostatnim – najpoważniejszym – poziomem zagrożenia jest tzw. *complex-coordinated*. Cyberterroryści dokonują tu skoordynowanych ataków mających na celu totalną destrukcję zintegrowanego systemu obronnego, mają możliwość tworzenia skomplikowanych narzędzi, które służą do niszczenia celów w cyberprzestrzeni, a także analizy celów będących przedmiotem ataku. Mogą dowodzić, kontrolować, jak również samodoskonalić się (zob. S. Serwiak, [w:] E. Pływaczewski, 2005, s. 589–613).

Niezwykle istotne jest podkreślenie, że organizacje terrorystyczne, które posługują się nowymi technikami, można (zdaniem A. Rathmella) podzielić na trzy kategorie:

- kategoria I, która obejmuje nowe techniki używane przez terrorystów do prowadzenia tradycyjnej działalności. Internet wykorzystuje się tutaj do zbierania informacji, komunikacji, zdobywania środków finansowych i komunikacyjnych,
- kategoria II, w której wykorzystywane są stare techniki do nowej działalności. Używana jest tutaj siła fizyczna, która ma na celu zniszczenie systemu informacyjnego,
- kategoria III, w której używa się nowe techniki do nowych działań – jest to atak w cyberprzestrzeni na system informacyjny (H. Münkler, 2004, s. 21).

Należy również pamiętać, że nie da się z działalności w sieci wykluczyć wszystkich agresorów. Richard Clarke w wywiadzie dla autora Dana Vertona twierdzi również: „załóżmy dla przykładu, że następny atak jest planowany przez Al-Kaidę. Nawet gdyby udało się dobrać im do skóry i wyeliminować całkowicie albo zmniejszyć do pozbawionej znaczenia grupki, nie wyeliminuje to całkowicie zagrożenia w cyberprzestrzeni. Ktoś inny wyszuka słabe punkty naszych systemów i wykorzysta je do ataków. Nie ma co zgadywać, kto będzie następnym atakującym, nawet gdyby w końcu udało się go wyśledzić i zrobić z nim, co należy. Trzeba zająć się słabościami, które umożliwiają ataki. Dopóki sobie z nimi nie poradzimy, dopóty będziemy narażeni na ryzyko ataków". Działalność cyberterrorystów w sieci jest bardzo poważnym problemem, gdyż ich poczynania są ukryte. Z uwagi na łatwość maskowania tożsamości można mówić o relatywnej anonimowości atakujących, którzy bez obaw, że zostaną wykryci, przeprowadzają za pomocą sieci wrogie działania. Wynika stąd kolejny problem – skala potencjalnych strat, zarówno pod względem finansowym, jak i bezpieczeństwa, jest trudna do oszacowania.

KLASYFIKACJA ATAKÓW

Pierwszą zaprezentowaną metodą klasyfikacji jest lista siedmiu kategorii działań w cyberprzestrzeni, opracowana przez S. Bellovina i W. Cheswicka:

- *stealing passwords* (kradzież haseł) – metoda polegająca na uzyskaniu haseł dostępu do sieci,

- *social engineering* (inżynieria społeczna) – wykorzystanie niekompetencji osób mających dostęp do systemu,
- *bugs and backdoors* (błędy i tylne drzwi) – używanie oprogramowania z nielegalnych źródeł lub korzystanie z systemu bez specjalnych zezwoleń,
- authentication failures (błędy uwierzytelniania) – zniszczenie lub uszkodzenie procedur mechanizmu autoryzacji,
- *protocol failures* (błędy protokołu) – wykorzystywanie luk w zbiorze reguł, które sterują wymianą informacji pomiędzy dwoma lub wieloma niezależnymi urządzeniami bądź procesami,
- *information leakage* (wyciek informacji) – uzyskanie informacji dostępnych tylko administratorowi, które niezbędne są do poprawnego funkcjonowania sieci,
- *denial of services* (odmowa usługi) – uniemożliwienie użytkownikom korzystania z systemu (D.E. Denning, [w:] J. Arquilla, D. Ronfeldt, 2001, s. 239–262).

F. Cohen, mając na uwadze powyższą listę kategorii, stworzył własną kategoryzację, która uwzględniała przede wszystkim rezultat ataku w cyberprzestrzeni. Rozpatrywane kategorie to:

- *corruption* – nieuprawniona zmiana informacji,
- *leakage* – informacja znalazła się w niewłaściwym miejscu,
- *denial* – kiedy komputer lub sieć nie nadają się do użytkowania (A. Bogdół-Brzezińska, M.F. Gawrycki, 2003, s. 73).

Warto zauważyć, że wielu specjalistów (w tym J. Howard i T. Longstaff) podkreśla, iż działania w sferze cyberprzestrzeni nie da się zakwalifikować tylko do jednej kategorii. Często są to akcje mieszczące się w wielu kategoriach. W efekcie takiego ujęcia P. Neumann i D. Parker zaproponowali następujący podział, który opiera się na dostępnych danych empirycznych:

- *external information theft* – przeglądanie oraz kradzież informacji przez osobę spoza systemu,
- *external abuse of resources* – zniszczenie twardego dysku,
- *masquerading* – podawanie się za kogoś innego,
- *pest programs* – zainstalowanie złośliwego programu,
- *bypassins authentication or authority* – złamanie haseł,
- *authority abuse* – fałszowanie danych,

- *abuse through inaction* – celowe prowadzenie złego zarządzania,
- *indirect abuse* – używanie innych systemów do stworzenia „złośliwych" programów (M. Zanini, S.J.A. Edwards, [w:] J. Arquilla, D. Ronfeldt, 2001, s. 29–60).

Atakujący dokonują uderzenia w niecodziennych sytuacjach. Wynika stąd, że działań w sferze cyberprzestrzeni nie da się zakwalifikować wyłącznie do jednej kategorii.

Klasyfikacja oparta na działaniu polega na czterech rodzajach ataków zdefiniowanych przez W. Stallingsa. Ma jednak ona ograniczoną możliwość zastosowania, gdyż dotyczy jedynie ataków traktowanych jako seria działań. Są to:

- *interruption* (przerwanie) – nie można zastosować zabezpieczenia systemu lub zostało ono zniszczone,
- *interception* (przechwytywanie) – dostęp do istniejących zabezpieczeń zdobyła nieuprawniona osoba,
- *modification* (modyfikacja) – nieuprawniona osoba zdobyła dostęp, a także manipulowała zabezpieczeniem,
- *fabrication* (produkcja) – przez nieuprawnioną osobę do systemu wprowadzony został sfałszowany obiekt (B. Hoffman, 1998, s. 131–134).

Początki pierwszych ataków. Pierwsze wzmianki o niebezpieczeństwie zamachów terrorystycznych przy użyciu systemów komputerowych pojawiły się w 1979 roku w raporcie szwedzkiego ministerstwa obrony na temat zagrożeń społecznych związanych z komputeryzacją. W wypowiedziach amerykańskich specjalistów w dziedzinie wywiadu wojskowego samo słowo „cyberterroryzm" zaczęło być używane już w latach 80. O tej nowej formie terroryzmu zaczęto mówić coraz częściej (S. Reeve, 1999). Na przełomie lat 80. i 90. XX wieku medialną gwiazdą został Kevin Mitnick. Na liście poszukiwanych przez FBI oszustów komputerowych zajmował pierwsze miejsce. Został schwytany w 1995 roku i skazany wyrokiem sądu na wieloletnie pozbawienie wolności uzasadnieniem: „uzbrojony w klawiaturę, jest groźny dla społeczeństwa". Był znakomitym hakerem, włamał się m.in. do komputerów Pentagonu, laboratorium Digital Equipment Corporation, banków i sieci telefonicznej Pacific Bell, z których wykradał tajne dane. Po odbyciu wyroku został konsultantem firmy zabezpieczającej komputery, a narzędzia, których

używał w czasie włamań, zostały wykorzystane w systemach zabezpieczeń wielu krajów. Zbieranie informacji oraz operacje psychologiczne i manipulowanie percepcją w wojnie informacyjnej stosowali również terroryści. Niektóre grupy w swoich działaniach wykorzystywały Internet do propagandy i zbierały informacje z różnych bezpośrednio przyłączonych źródeł. Clark Staten, dyrektor ENRI (Emergency Response & Research Institute – Instytut Badania Nagłych Sytuacji i Reagowania) w lutym 1998 roku zeznał przed podkomisją senatu amerykańskiego, że „nawet małe grupy terrorystyczne korzystają teraz z Internetu do nadawania komunikatów i jednoczesnego wprowadzania w błąd ludności wielu krajów". Przekazał on również kopie komunikatów z propagandą antyamerykańską i antyizraelską oraz groźbami, gdzie szeroko było rozpowszechniane hasło ekstremistów wzywające do „dżihadu" przeciw Ameryce i Wielkiej Brytanii. W czerwcu tego samego roku w US News & World Report podano, że z 30 grup terrorystycznych (które umieszczone są na liście amerykańskiego Departamentu Stanu) 12 znajduje się w Internecie i nie można zmusić ich do opuszczenia sieci (zob. M. Whine, 1999).

W 1997 roku amerykański nastolatek unieruchomił główną kampanię telefoniczną obsługującą mały port lotniczy w Worcester (Massachusetts) na sześć godzin. W tym czasie wieża kontrolna nie miała możliwości świadczenia usług normalnymi kanałami. Bezpieczeństwo lotów zapewniono dzięki informacjom przekazywanym samolotom przez inne porty lotnicze drogą radiową. Jak wielkie zagrożenie stanowią takie ataki, można sobie uświadomić, analizując dane dotyczące ataków informatycznych, które wykonywane są na pozawojskowe systemy informatyczne. W 2003 roku szacunkowe straty wywołane takimi atakami wyniosły 82 mld dolarów. Na świecie ich liczba systematycznie wzrasta.

W lutym 1998 roku to, co było tematem Eligible Receiver, stało się rzeczywistością – dokonano kilkuset ataków na serwery Departamentu Obrony. Zastępca sekretarza obrony John Hamre określił to jako „najlepiej zorganizowany atak w historii" i przyznał, że jeszcze nigdy nie był atakowany w tak systematyczny sposób. Początkowo sądzono, że atak ten był sponsorowany przez Irak, a celem było uniemożliwienie wysłania sprzętu i posiłków na Zatokę Perską. Okazało się jednak, że atakującymi byli 18-latek z Izraela i dwóch 16-latków z Kalifornii. Hakerzy, po dostaniu się do komputerów, zainstalowali program do przeszukiwania danych, dzięki czemu mogli zdobyć hasła do komputerów wojskowych i rządowych. Mieli też dostęp do serwerów

z kontami osobistymi. Strony rządowe, tak jak i prywatne, są bardzo podatne na tego typu ataki. Wskutek działań hakerów bardzo szybko można narobić sporego zamieszania. Ważne jest, aby pamiętać, iż jeśli nie zadbamy o bezpieczeństwo, ataki w przyszłości będą się stawały coraz groźniejsze.

W 2000 roku hakerzy należący do Pakistan Hackerz Club skradli numery kart kredytowych około 700 członków i fundatorów proizraelskiej organizacji Amerykańsko-Izraelskiego Komitetu Spraw Publicznych, działającego na terenie Stanów Zjednoczonych. Kolejnym sposobem pozyskania w nielegalny sposób środków finansowych jest wykorzystanie grup hakerskich do ataków wymierzonych w systemy informatyczne instytucji finansowych. Jesienią 2000 roku, działając na zlecenie Hezbollahu, podczas tzw. drugiej intifady, hakerzy spenetrowali systemy informatyczne zarządzane przez Bank Izraela i giełdę w Tel Awiwie. Dane dotyczące liczby ataków nie są w tym przypadku znane, powodem jest oczywiście dbałość o renomę instytucji oferujących usługi w sektorze finansowo-bankowym. Każdy ujawniony atak to potencjalnie mniej klientów obawiających się o bezpieczeństwo swoich oszczędności (J. Stern, 2000, s. 115–126).

Al-Kaida, chcąc wzbudzić nieufność obywateli państw zachodnich do oficjalnej polityki informacyjnej, podejmuje próby prostowania lub dementowania informacji podawanych przez oficjalne ogólnoświatowe serwisy informacyjne. W artykule „Świadectwo Talibanu" z 2002 roku na stronie Al Neda oskarżono „zachodnie i wschodnie" media o demonizowanie i pozbawienie czci talibów, poprzez opisywanie ich w wulgarny sposób, jako wrogo usposobionych fanatyków, którzy prześladują kobiety i mniejszości narodowe. Przykładem operacji nakierowanej na dążenie do wywierania presji na władze poprzez wywołanie poczucia zagrożenia wśród obywateli była kampania psychologiczna prowadzona przez Al-Kaidę w październiku i listopadzie 2001 roku (zob. Organised Crime Situation Report 2004, Focus on the Threat of Cybercrime, 2003, s. 125). Terroryści w Pakistanie dążyli do wywołania fali demonstracji i zamieszek przeciwko udziałowi tego państwa w koalicji antyterrorystycznej oraz wspieraniu operacji wojskowej w Afganistanie. Przedstawiciele Al-Kaidy wydali ostrzeżenia za pośrednictwem prasy i Internetu, że w przypadku amerykańskiego ataku na Afganistan przeprowadzą szereg zamachów na terenie Pakistanu z wykorzystaniem broni jądrowej. Było to niedługo po atakach na World Trade Center w 2001 roku, dlatego też opinia publiczna traktowała groźby z pełną

powagą. Pakistan uległ groźbom i ograniczył swoją pomoc do pozornej kontroli na granicy z Afganistanem. Następnym krokiem był apel przywódcy talibów mułły Omara, z dnia 23 października 2006 roku, aby państwa Organizacji Traktatu Północnoatlantyckiego wycofały swoje wojska z Republiki Afganistanu i zaprzestały tym samym poświęcać życie swoich żołnierzy dla realizacji interesów Stanów Zjednoczonych. Al-Kaida stale prowadzi kampanię psychologiczną skierowaną w stronę ludności państw zachodnich. Takim przykładem była wypowiedź przedstawiciela tej organizacji, Sulaimana Abu Ghaithema, że w kolejnych zamachach na Amerykę ucierpi około 4 mln obywateli tego kraju w wyniku użycia broni chemicznej i biologicznej. Specjalnością talibów w zakresie zastraszania stało się również publikowanie egzekucji pojmanych zakładników. Ponieważ wszystkie stacje telewizyjne odmówiły emisji materiałów wideo, z uwagi na makabryczną zawartość, przedstawiających śmierć niewinnych ludzi poprzez odcięcie głowy, zapisy z egzekucji są publikowane w Internecie. Martwi fakt ogromnego zainteresowania takimi filmami zwłaszcza przez internautów z państw zachodnich. Ugrupowania terrorystyczne zamieszczają także na swoich stronach pliki wideo zachęcające do wstępowania w ich szeregi. W przypadku Al-Kaidy były to między innymi wystąpienia nagrane w Finsbury Park w Londynie i umieszczone na stronie Haganah. Jak to możliwe, że w stolicy Anglii zostały nagrane takie materiały. Otóż w tym czasie Finsbury Park w Londynie był zarządzany przez radykalnego islamistę Abu Hanza al-Masri powiązanego z Al-Kaidą, zanim został aresztowany 27 maja 2004 roku.

W listopadzie 2001 roku w Australii Vitek Boden został skazany na dwa lata więzienia za wykorzystanie Internetu, radia i ukradzionego oprogramowania do wypuszczenia miliona litrów ścieków do rzeki i wód przybrzeżnych Maroochydore w Queensland w Australii. Skazany był konsultantem przy opracowywaniu projektu wodnego. Opisany atak przeprowadził w marcu 2000 roku, po tym jak odrzucono jego kandydaturę na pracownika władz hrabstwa Maroochy. W efekcie jego działań na akwenie objętym wyciekiem zamarło życie biologiczne, a mieszkańcy tego rejonu ze względu na panujące warunki musieli na wiele tygodni opuścić miejsce zamieszkania.

Rosnące zagrożenie cyberterrorystyczne zauważono także w 2002 roku, kiedy CIA w liście przesłanym do przewodniczącego Senackiej Komisji specjalnej do spraw wywiadu – senatora Boba Grahama – stwierdza, że „(...) Al-Kaida i różne sunnickie grupy ekstremistyczne popierające działania

antyamerykańskie prawdopodobnie spróbują dokonać w przyszłości ataku cybernetycznego. Jest to zgodne zarówno z ich intencjami, jak i z żądzą rozwijania umiejętności hackerskich i informatycznych potrzeb do stworzenia efektywnego modus operandi, nieodzownego do dokonywania skutecznych cyberataków (...). Przeprowadzenie cyberataków na systemy staje się coraz bardziej możliwe dla terrorystów – w miarę zapoznawania się przez nich z celami ataków i technologiami potrzebnymi do ich przeprowadzenia. Różne grupy terrorystyczne, łącznie z Al-Kaidą i Hezbollahem, coraz skuteczniej posługują się technologiami internetowymi i komputerowymi – FBI odnotowuje rosnącą liczbę zagrożeń" (R. Borkowski, 2006, s. 51).

W 2008 roku również doszło do ataków cybernetycznych. Miały one miejsce w Gruzji, a odbyły się równolegle do konwencjonalnych działań wojennych. Doszło wtedy do zmasowanych ataków na gruzińskie strony internetowe, a zniekształcone zostały najważniejsze strony państwowe. Dziś o te ataki podejrzewa się głównie obywateli Rosji, a w szczególności organizację Russian Business Network. Wynika to z faktu, iż na rosyjskich serwisach internetowych podczas rozpoczęcia działań zbrojnych zaczęły się pojawiać narzędzia i ogólnodostępne instrukcje do przeprowadzania ataków wraz z listą celów.

Szokującą informacją dla świata była również wiadomość na temat ataku cybernetycznego z października 2010 roku, wskutek którego zainfekowane zostały irańskie systemy obsługujące niemal całą infrastrukturę państwa – od sieci elektrowni, przez rurociągi ropy naftowej, aż po systemy wojskowe. Przypuszcza się, że celem ataku było zniszczenie, uszkodzenie bądź zlikwidowanie reaktora jądrowego Iranu. Nie wyklucza się, że trojan, którego użyto – Stuxnet – został wprowadzony do irańskiego systemu przez pracownika jednej z rosyjskich firm podwykonawczych zaangażowanych w budowę elektrowni. Trojan ten skutecznie sparaliżował irański system komputerowy, który nadzorował pracę podziemnego ośrodka wzbogacania uranu w Natanz, opóźniając uruchomienie elektrowni jądrowej w Buszerze o dwa miesiące. O skali ataku świadczyć może fakt, że w Iranie zainfekowanych zostało blisko 30 tys. komputerów (D. Doroziński, 2001; M.F. Gawrycki, 2003, s. 50–65).

W Polsce zjawisko cyberterroryzmu zaczęto poważnie traktować również dopiero z początkiem XXI wieku. Obecnie nasz kraj znajduje się na piątym miejscu pod względem ataków internetowych pochodzących z urządzeń mobilnych (A. Bógdał-Brzezińska, M. Gawrycki, 2003, s. 63). Dane na ten temat opracowała amerykańska firma Akamai, która jest jedną z naj-

większych firm na świecie zajmujących się zarządzaniem ruchu sieciowego. Fakt, że Polska stoi tak wysoko w zestawieniu państw, w których najczęściej dochodzi do ataków pochodzących z sieci, wynika z kilku przyczyn. Jedną z najważniejszych jest to, że nasz kraj nie nadąża z rozwojem mechanizmów i procedur bezpieczeństwa w stosunku do tempa rozwoju technologii informacyjnych. Ponadto Polacy nie zdają sobie sprawy z zagrożeń, jakie mogą wynikać z coraz powszechniejszego informatyzowania wielu dziedzin życia[7]. Co więcej, do niedawna zagrożenia pochodzące z cyberprzestrzeni bagatelizowano. Dopiero na początku 2012 roku zauważono, że Polska również może być zagrożona cyberterroryzmem. Zaatakowane zostały wtedy strony rządowe, czego powodem był sprzeciw w sprawie podpisania porozumienia ACTA. Protesty związane z tymi wydarzeniami pokazały, że serwisy rządowe są niezwykle słabo zabezpieczone w Internecie. Ataki hakerów dobitnie udowodniły, że realne jest zagrożenie[8].

Daesh, czyli tak zwane Państwo Islamskie, czy też wcześniej Al-Kaida, w swej aktywności nigdy nie stroniły od używania najnowszych technologii teleinformatycznych. Wykorzystywane są one zarówno do promowania swoich poglądów wśród rozsianych na całym świecie zwolenników, jak i do szerzenia przekazów propagandowych, skierowanych do nowych, potencjalnych odbiorców. Tym samym Internet, dotychczas postrzegany jako narzędzie Zachodu w zakresie promocji własnego obrazu świata, zyskał nowy wymiar i stał się bronią przeciwników Zachodu (M. El Ghamari, 2016, s. 47–90).

Jednocześnie cały czas cyberprzestrzeń jest polem znaczącej aktywności służb specjalnych niemal wszystkich państw świata, zarówno w obrębie pozyskiwania danych o rywalach, jak i sojusznikach. Nie chodzi przy tym o samo pozyskiwanie danych, ale również ich odpowiednie pozycjonowanie, nie mówiąc o tworzeniu specjalnych przekazów w celu wprowadzenia w błąd przeciwnika i wywołania u niego zamierzonej reakcji. Jest to o tyle istotne, że wraz z pojawieniem się nowej fali mediów, opierających się o przekaz publikowany w sieci, można bardzo łatwo docierać do społeczeństw czy wybranych jednostek bez czasochłonnego lokowania własnych aktywów operacyjnych w klasycznych mediach.

[7] Zob. http://technologie.gazeta.pl/ internet/1,104530,9036923,Mobilny_Internet_na_swiecie___Polacy_na_ni echlubnym.html [data dostępu: 15.06.2012].

[8] Zob. http://next.gazeta.pl/internet/1,104530,90369,Mobilny_Internet_na_swieciePolacynaniechlubnym.html.

W ostatnich latach znaczną siłą stały się media społecznościowe, gdzie jakże trudno jest wielokrotnie uchwycić jednolitą strukturę decyzyjną oraz proces powstawania informacji.

Wystarczy przytoczyć przykład tak zwanych arabskich rewolucji z 2011 roku. Fala protestów, zainicjowana często na portalach społecznościowych zmieniła oblicze regionu MENA – Bliski Wschód i Afryka Północna. Jej niezaprzeczalnym elementem były komunikatory sieciowe i różnorakie media społecznościowe. To dzięki nim możliwe było organizowanie się w grupy przez demonstrujących, omijanie przez nich kordonów policji oraz sił bezpieczeństwa, a przede wszystkim pokazywanie światu własnego obrazu wydarzeń bez pośredników. Nie było to jednak działanie jednostronne, ale zostało przejęte przez wszystkie strony różnych konfliktów społecznych, politycznych itp.

W ten sposób bez zrozumienia nowego obiegu danych nie jest możliwe ustalenie wielu aspektów w zakresie taktycznej oceny wydarzeń, a tym bardziej prób wnioskowania na płaszczyźnie strategicznej. Lecz i ich czas nieubłaganie się kończy. Twitter w ciągu ostatnich sześciu miesięcy zawiesił 235 tys. kont za promowanie terroryzmu – podaje portal money.cnn.com. W sumie od połowy 2015 roku Twitter zawiesił już 360 tys. kont. Wiele z nich powiązanych jest z Państwem Islamskim (IS), które szczególnie aktywnie na Twitterze i innych portalach społecznościowych szerzy propagandę i przyciąga nowych rekrutów. Jak informuje amerykański portal, zarówno Facebook, jak i YouTube również w ostatnich miesiącach podjęły kroki, które doprowadziły do zawieszenia kont lub zablokowania treści udostępnionej przez zwolenników IS. Zwolennicy IS, w reakcji na blokady kont, posunęli się tak daleko, że zaczęli nawet grozić założycielom Twittera i Facebooka[9].

Na podstawie przeprowadzonych badań można stwierdzić, iż nowe techniki komunikacji i komputeryzacji nadają sieci trojakie cechy:

- zredukowanie czasu transmisji, które umożliwia rozproszonym organizacjom (grupom) porozumiewanie się i koordynowanie zadań,
- znaczne zmniejszenie kosztów komunikacji, które sprzyja rozproszeniu organizacji przez decentralizację,
- zwiększenie zakresu i kompleksowości informacji.

[9] Zob. http://niezalezna.pl/84940-twitter-na-wojnie-z-terroryzmem.

Takie innowacje, jak telekonferencje czy czaty internetowe, pozwalają uczestnikom na szeroką wymianę informacji bez względu na odległość. Posługiwanie się Internetem przyspiesza mobilizację członków grup terrorystycznych, umożliwia dialog między nimi i zwiększa elastyczność organizacji przez możliwość zmiany taktyki w razie potrzeby. Członkowie grup terrorystycznych mogą dzielić się na podgrupy, ustalać miejsca spotkania, przeprowadzać operacje terrorystyczne, po czym szybko przerywać swoje powiązania i się rozpraszać.

Zgodnie z raportami osób, które były w górskiej kwaterze Ibn Ladina w Afganistanie, ten koordynator i finansista terroryzmu dysponuje nowoczesnym komputerem i sprzętem telekomunikacyjnym, a nawet wykorzystuje telefonię satelitarną do koordynacji działań rozproszonych grup. Dysponuje też urządzeniami dającymi mu bezpieczeństwo, gdy korzysta z systemów komunikacji. Najczęściej dyktuje on polecenia asystentowi, który przekazuje je telefonicznie z różnych miejsc. Funkcjonariusze Ibn Ladina używają dysków CD-ROM do zapisu i rozpowszechniania informacji dotyczących rekrutacji członków, produkcji bomb, ciężkiej broni i operacji terrorystycznych. Amerykańskie agencje wywiadowcze otrzymały ostatnio kopie dysków komputerowych zawierających podręczniki szkoleniowe używane przez Ibn Ladina podczas szkolenia rekrutów (S.M. Lawson, 2002, s. 16–37).

Egipscy eksperci komputerowi, którzy walczyli w Afganistanie, opracowali dla Ibn Ladina sieć komunikacyjną na bazie internetowej i e-mailowej. W latach 90. w operacjach antyterrorystycznych przeciw bazom algierskiej GIA skonfiskowano komputery i dyskietki z instrukcjami dotyczącymi konstrukcji bomb (Organised Crime Situation Report 2004, Focus on the Threat of Cybercrime, 2003, s. 125).

Bojowa grupa islamska Hamas również posługuje się Internetem w przekazywaniu operacyjnych informacji. W Stanach Zjednoczonych aktywiści Hamasu wykorzystują kanały dyskusyjne, czyli chatrooms, podczas planowania i realizacji operacji. Agenci Hamasu posługują się także pocztą elektroniczną w koordynowaniu akcji w Gazie, na Zachodnim Brzegu Jordanu i w Libanie. Zauważyli oni, że informacje mogą być przekazywane względnie bezpiecznie przez Internet, gdyż wywiad kontrterrorystyczny nie jest w stanie ściśle monitorować całego ich przepływu i treści. Ponadto sieci terrorystyczne mogą chronić przepływ informacji dostępnymi technikami, np. programami kodującymi. Nowe programy

kodujące są tak wyrafinowane, że kody zabezpieczające pocztę elektroniczną niezwykle trudno jest złamać. Prawdopodobnie izraelskim siłom nie udało się złamać kodów używanych przez Hamas do przesyłania przez Internet instrukcji terrorystycznych ataków. Terroryści mogą posługiwać się też steganografią, tj. metodą ukrywania tajnych danych w innych informacjach, w tym w plikach graficznych. Mogą także kodować transmisje realizowane przez telefony komórkowe, kraść numery takich telefonów i przeprogramowywać je albo używać opłaconych z góry kart telefonicznych sprzedawanych anonimowo. Te ostatnie techniki komunikowania się umożliwiają terrorystom operowanie z prawie każdego zakątka świata przy dostępie do niezbędnej infrastruktury IT. Analitycy twierdzą, że terroryści mający możność kodowania informacji są niezależni od sponsorów oraz pomocy państwa i mogą zapewnić sobie większy stopień bezpieczeństwa. Inni wskazują, że grupy terrorystyczne mogą zdobywać pieniądze, wykorzystując sieć. Z Pakistanu jest znany przypadek podjęcia tak dużych sum z kont wahhabitów z Arabii Saudyjskiej, że terroryści planowali utworzenie na ich bazie własnego banku. Dzięki Internetowi informacje o zamachach bombowych mogą małym kosztem przedostać się bezpośrednio ze stron internetowych do prasy – o ile życzą sobie tego terroryści (zob. E. Aronson, A. Pratkanis, 2004, s. 4). Terroryści mający bezpośrednią kontrolę treści informacyjnych mogą dokonywać manipulacji obrazami, stosować specjalne efekty i oszustwa (por. R. Borkowski, 2006, s. 16).

Internet jest korzystny także ze względu na możliwość mobilizacji czasowej cyberterrorystów (*parttime cyberterrorists*), tj. osób niezwiązanych bezpośrednio i na stałe z ugrupowaniami terrorystycznymi, ale wspierających ich działania. Na przykład zarówno rząd Palestyny, jak i rząd Izraela zachęcały prywatne osoby do przesyłania danych z komputerów w związku z konfliktem dotyczącym świątyni Al-Aksa i późniejszą intifadą.

Cyberterroryści mogą wykorzystywać IT do ataków elektronicznych, które wpływają negatywnie na wolę walki przeciwników. Destrukcyjne ataki obejmują także dławienie systemów komputerowych (*choking*) za pomocą takich metod i narzędzi, jak e-bomby, masowe rozsyłanie wiadomości elektronicznych (*fax-spamming*) i włamania hakerów w celu zniekształcenia stron internetowych. Liczba tych destrukcyjnych ataków ma tendencję wzrostową (zob. J. Adamski, 2002, s. 12–21).

NARZĘDZIA DO WALKI Z CYBERTERRORYZMEM?

Ciekawym przypadkiem jest modułowy system informatyczny CSI. Jego autorzy skupili swoją uwagę na dualnej strukturze wykrywania i analizy potencjalnych zagrożeń, obejmujących zarówno te fizyczne, jak i wirtualne. Narzędzie ma charakteryzować się uniwersalnością i można je stosować, zgodnie z założeniami twórców, do całego spektrum współczesnych wyzwań – od terroryzmu po lokalne zamieszki bądź działania coraz groźniejszych hakerów. Oprogramowanie tego rodzaju daje możliwość monitorowania różnych źródeł generujących istotne informacje, tj. komentarzy zamieszczanych w sieci, forów internetowych, portali informacyjnych, aż do mediów społecznościowych włącznie. Według producenta analityk jest w stanie dzięki temu sprawnie i szybko dokonywać określenia chociażby najbardziej zagrożonych miejsc – począwszy od potencjalnych celów dla terrorystów po możliwe działania osób dążących do wszczęcia zamieszek lub innego rodzaju prób naruszenia porządku publicznego. Oczywiście, w myśl zasady, że wszelkie działania w sieci pozostawiają ślady, które zastosowanie narzędzi pokroju Comarch CSI pozwala odpowiednio odnajdywać i układać w większą całość.

W dobie ciągłego zagrożenia terrorystycznego ewidentnie nowego znaczenia nabiera skuteczna analiza działań różnych organizacji terrorystycznych, chociażby tzw. Państwa Islamskiego w sieci. Jak już niejednokrotnie pokazały dokładne, szczegółowe dochodzenia, rozpoczęte po konkretnych zamachach terrorystycznych, kluczowe w tworzeniu systemu zapobiegania jest wyszukiwanie i śledzenie wszelkich informacji pozwalających na wyznaczenie potencjalnych kierunków działań terrorystów. Niezwykle istotna jest możliwość monitorowania komunikacji związanej z ugrupowaniami terrorystycznymi, jak również wykorzystania zdobytych informacji do lokalizowania miejsc działań ekstremistów.

Do kolejnych pomocnych narzędzi przy analizie zagrożeń o charakterze terrorystycznym należą:

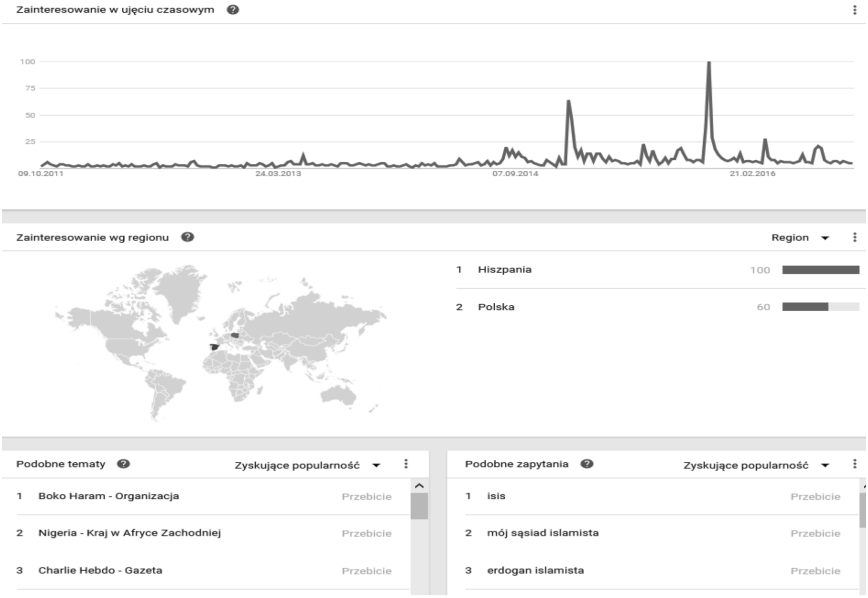
- platforma Quintly – narzędzie badające treści i jej przepływy w Internecie. Badania wykazują, że najbardziej popularne, atrakcyjne są grupy fundamentalistyczne, zmierzające ku idei nacjonalizmu. Przykładem jest: Pegida (wskaźnik polubień – algorytm)[10],

[10] Zob. https://www.quintly.com/.

- platforma Google Trends (wskaźnikiem jest kraj i 24-godz. popoularność wiadomości w danym kraju),
- platforma IceRocket,
- platforma Keyhole.

W kontekście portali społecznościowych niezwykle ważny jest tak zwany feedback, czyli informacja zwrotna. Reakcja zwrotna. Jej skutek można zaobserwować poprzez stosowanie przez użytkowników tak zwanego przycisku polubień. Co ciekawe, w przypadku Pegidy przycisk „lubię to" zastosowało około 300 tys. osób, zaś grupy Emisco jedynie 90 razy. Podobny wyraz mają komentarze i udostępnianie. Pegida osiągnęła poziom 80 tys. komentarzy, a jej artykuły zostały udostępnione ponad 70 tys. razy, zaś Emisco uzyskało jedynie 8 komentarzy i 33 udostępnienia. Platforma analityczna Quintly udowadnia za pomocą wskaźników zależności pomiędzy badanymi stronami użytkowników.

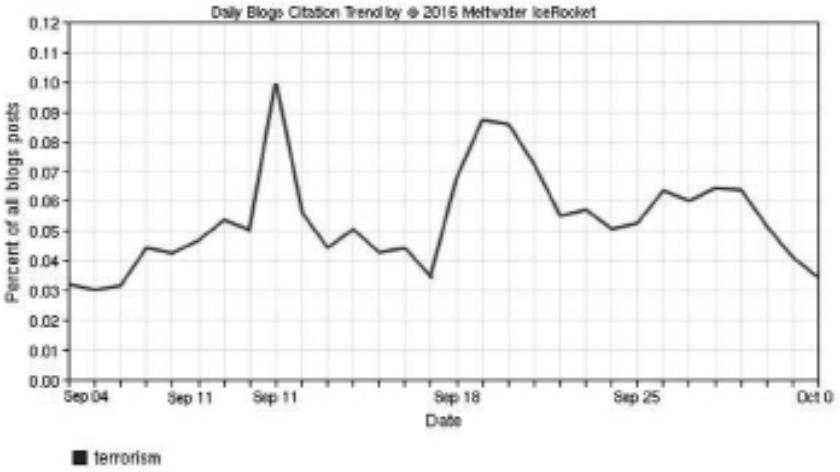
Schemat 1.
Zainteresowanie hasłem „islamista" – w ujęciu czasowym (ostatnie 5 lat) oraz regionalnym (cały świat)



Źródło: Opracowanie własne na podstawie https://www.google.pl/trends/explore?q=islamista [dostęp 04.10.2016]

Platforma Google Trends analizuje współzależności pomiędzy poszczególnymi hasłami i wykazuje ich składowe. Na przykładzie ataku we Francji można wskazać pewne zależności pojawiające się w hasłach, wiadomościach, nagłówkach, komunikatorach i tytułach artykułów, blogach itd. Korzystając z możliwości Google Trends, można porównać zależność pomiędzy hasłami „muzułmanin" czy „islamista" a odsetkami społeczeństw imigracyjnych w społecznościach rdzennych, które wyszukiwały to hasło. Im wyższy odsetek imigrantów w regionie, tym więcej wyszukiwania i jednostkowego pojawiania się samego hasła (schematy 1, 2).

Schemat 2.
Popularność hasła „Daesh" w wybranym czasie



Źródło: http://www.icerocket.com/trend?query1=ISIS&days=30 [dostęp: 03.10.2016]

W celu monitorowania mediów społecznościowych wypracowano gotowe narzędzia, z których można skorzystać, aby dokonać analizy i syntezy danych:

- Buzzsumo – umożliwi wgląd w treści szybko zyskujące popularność oraz użytkowników, którzy chętnie je między sobą współdzielą (szczególnie przydatne przy analizie danych z: Twittera, Facebooka, LinkedIn, Google+ oraz Pinteresta).
- Social Mention – to wyszukiwarka danych dotyczących mediów społecznościowych. Aplikacja ma ponad 100 funkcji wyszukiwania dla takich portali, jak Twitter, Facebook, YouTube, Digg oraz Google.

- Mention – dostępna w aż 42 językach, umożliwia analizowanie danych z mediów społecznościowych, portali informacyjnych, blogów oraz stron firmowych.
- HowSociable – umożliwia szybkie oszacowanie widoczności i rozpoznawalności danego hasła w mediach społecznościowych.
- Addict-o-matic – gromadzi dane poprzez skanowanie plików RSS witryn informacyjnych oraz silników wyszukiwania, m.in.: Google, Yahoo, Technorati, Ask, YouTube, Truveo, Flickr, Blinkx, IceRocket, Digg, Topix, Newsvine oraz Tweetscan.
- Topsy – umożliwia wyszukiwanie działające w czasie rzeczywistym dedykowanym mediom społecznościowym. Indeksuje oraz ocenia wyniki wyszukiwania w oparciu o najpopularniejsze konwersacje prowadzone przez miliony użytkowników na dany temat, przykładowo – o danej stronie, domenie czy zagadnieniu.
- SumAll – umożliwia dostęp do wszystkich danych portali społecznościowych: Facebook, Instagram, Twitter, LinkedIn i Google Analytics z poziomu jednej aplikacji. Pozwala na śledzenie statystyk ponad 30 kont.
- Sprout Social – pozwala na monitorowanie oraz zarządzanie działaniami prowadzonymi w mediach społecznościowych.
- WhosTalkin – jest narzędziem do przeszukiwania zawartości mediów społecznościowych zorientowanym na wyszukiwanie konwersacji prowadzonych na określony temat. Dane zbierane są z 60 najpopularniejszych źródeł.
- Pluggio – to aplikacja do zarządzania kontami prowadzonymi na platformach Twitter oraz Facebook. Pluggio automatycznie śledzi oraz generuje wykresy dla nawet kilku kont, a więc możliwe jest określenie wydajności prowadzonej kampanii oraz oszacowanie wzrostu bazy klientów. Opcjonalna integracja z witryną Bit.ly daje użytkownikowi szansę analizy liczby odwiedzin współdzielonych linków – pozwala to na dokładną ocenę popularności publikowanych postów.
- SharedCount – usługa sprawdzająca liczbę udostępnień danego adresu URL w głównych mediach społecznościowych, takich jak: Facebook, Twitter, Pinterest, LinkedIn, Google+ oraz StumbleUpon.
- Social Searcher – ułatwia przeszukiwanie oraz analizę kanałów społecznościowych w czasie rzeczywistym. Gromadzi informacje bez konieczności logowania się na portale, takie jak: Twitter, Google+ bądź Facebook. Zapisuje wyniki wyszukiwania oraz ustaw powiadomienia dla konta.

- Edgerank Checker – aplikacja analizująca oraz oceniająca jakość prowadzonej strony na platformie Facebook. Sprawdzi, kiedy twoi fani są online, aby lepiej oszacować najlepszy moment publikacji materiałów promocyjnych. Sprawdza wydajność dla określonych dat, aby sprawdzić, kiedy użytkownicy byli najbardziej zainteresowani twoją stroną.
- Aplikacja Followerwonk – pozwala na pozyskanie zaawansowanych danych statystycznych dotyczących portalu Twitter.
- NutshellMail – zbiera informacje o najnowszych wydarzeniach na kontach założonych na różnych portalach społecznościowych, a następnie przesyła podsumowanie mailem.

PODSUMOWANIE

Zwalczanie terroryzmu informatycznego stało się nie tylko ważnym zagadnieniem natury politycznej, ale również, a może przede wszystkim, problemem natury ekonomicznej. Cyberterroryści mogą również dostosować swoje działania tak, aby zmaksymalizować pozytywny dla siebie wynik. Ponadto cyberterroryzm nie wymaga treningu fizycznego ani dużego zabezpieczenia logistycznego. Nie wymaga poza tym podróżowania. Ataki w cyberprzestrzeni nie stwarzają ryzyka poniesienia śmierci lub obrażeń fizycznych, ograniczają więc konieczność narażania życia – zamachy w sieci nie wymagają bowiem ataków samobójczych[11]. Aby przeprowadzić taki atak, nie potrzeba posiadać praktycznie żadnych umiejętności – można wynająć crackerów, którzy łamiąc zabezpieczenia (często nie zdając sobie sprawy ze skutków swojego działania), za pieniądze przeprowadzą atak terrorystyczny.

Dotychczasowe przykłady przestępstw informatycznych pokazują, jak wielka liczba ludzi może być dotknięta skutkami takiego działania; wynika to z globalnego charakteru informatyzacji. Tym samym jeden z zasadniczych celów terrorystów – medialność ataku – jest przeogromna[12].

Terroryści zdają sobie również sprawę, iż walka z cyberterroryzmem wymaga o wiele większej koordynacji działań niż w przypadku klasyczne-

[11] National Research Council, Computer at Risk, Washington, DC, 1991, s. 36.

[12] Devost M.G., Brian K.H., Neal A.P., *Information terrorism: Can you trust your toaster?*, [w:] *San Tzu and Information Warfare*, Washington, DC, 1997, s. 51.

go ataku. Dysponując różnymi możliwościami zastosowania sankcji – nie wiadomo, w jaki sposób odpowiedzieć na taki atak. W konsekwencji można stwierdzić, że cyberterrorystą może zostać każdy, dlatego kwestia cyberterroryzmu może stanowić kluczowy problem bezpieczeństwa międzynarodowego w XXI wieku. Ryzyko cyberterroryzmu będzie wzrastać w społeczeństwie wraz ze wzrostem znaczenia Internetu w naszym życiu. Cyberwojnę już dziś można prowadzić niezależnie od konfliktu na lądzie i morzu, w dodatku mniejszym nakładem kosztów. Systemy informacji w podstawowych dziedzinach gospodarki – bankowości, finansach, telekomunikacji, handlu – już dziś stały się nadrzędne, dlatego dostęp do nich lub ich blokada mogłyby skutecznie sparaliżować działanie instytucji i państwa. Wiele racji miał zatem sekretarz generalny NATO Jaap de Hoop Scheffer, mówiąc, że „cyberataki nie wymagają użycia ani jednego żołnierza czy naruszenia granic – mogą jednak sparaliżować działanie państwa".

Strach informatyczny jest zjawiskiem coraz powszechniejszym, jednak jest on wyolbrzymiony. Pomimo faktu, że pozaprawne ataki informatyczne na newralgiczne składniki narodowej infrastruktury informatycznej stają się coraz powszechniejsze, to nie są one, jak dotychczas, przeprowadzane przez terrorystów. Poziom ich niszczycielskiej siły nie jest ponadto na tyle znaczny, by można go zakwalifikować jako terroryzm informatyczny. Jakkolwiek strach przed tym zagrożeniem jest przesadzony, to nie może być lekceważony czy ignorowany.

Bibliografia

Adamski J. (2007). *Nowe technologie w służbie terrorystów*. Warszawa.

Adamski A. (2002). *Cyberterroryzm*, [w:] Materiały z konferencji na temat terroryzmu, 11.04.2002 r. Wydział Prawa UMK Toruń.

Adkins B. (2001). *The spectrum of cyber conflikt from hacking to information warfare: What is law enforcament's role?* Maxwell AFB, Alabama.

Aronson E., Pratkanis A. (2004). *Wiek propagandy*. Warszawa.

Barnas R. (2001). *Terroryzm. Od Asasynów do Osamy bin Laden*. Wrocław.

Białek T. (2005). *Terroryzm – manipulacja strachem*. Warszawa.

Borkowski R. (2006). *Terroryzm ponowoczesny*. Toruń.

Bógdał-Brzezińska A., Gawrycki M. (2003). *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*. ASPRA-JR. Warszawa.

Denning D. (2002). *Wojna informacyjna i bezpieczeństwo informacji*. Wydawnictwa Naukowo-Techniczne. Warszawa.

Denning D.E. (2001). *Activism, hacktivism and cyberterrorism: The Internet as a tool for influencing foreign policy*, [w:] J. Arquilla, D. Ronfeldt, Networks and Netwars, Santa Monica.

Doroziński D. (2001). *Hakerzy. Technoanarchiści cyberprzestrzeni*. Helion.

El Ghamari M. (2016). *Cool Jihad*. Wydawnictwo Difin.

Gawrycki M.F. (2003). *Cyberterroryzm*. Fundacja Studiów Międzynarodowych. Warszawa.

Kerr K. (2003). *Putting cyberterrorism into contex*. AusCERT.

Kosta R. (2007). *Terroryzm jako zagrożenie dla bezpieczeństwa cywilizacji zachodniej w XXI wieku*. Toruń.

Lawson S.M. (2002). *Information Warfare: An Analysis of the Threat of Cyberterrorism Towards the US Critical Infrastructure*. SANS Institute.

Monge P., Janet F., *Communication technology for global network organizations*, [w:] Shaping Organizational Form: Communication, Connection and Community, red. G. Desanctis, J. Fulk, Thousand Oaks, Calif., 1999.

Pollitt M., Cyberterrorism: Fact or Fancy? Proceedings of 20-th National Information Systems Security Conference, październik 1997.

Münkler H., *Terrorismusheute. Die Asymmetrisierung des Krieges*, „Internationale Politik", nr 2, 2004.

Organised Crime Situation Report 2004, *Focus on the Threat of Cybercrime*, Council of Europe, Strasburg, 23.12.2003.

Reeve S. (1999). *The New Jackals: Ramzi Yousef, Osama Ben Laden and the Future of Terrorism*. Mass, Boston.

Serwiak S. (2005). *Cyberprzestrzeń jako źródło zagrożenia terroryzmem*, [w:] E. Pływaczewski, *Przestępczość zorganizowana*. Kraków.

Staten C. (24.02.1998). *Subcommitte of Technology*. Terrorism and Government Information, U.S. Senate Judiciary Committee.

Stern J. (listopad/grudzień 2000). *Pakistan's Jihad Culture*.„Foreign Affairs".

Verton D. (2004). *Black Ice. Niewidzialna groźba cyberterroryzmu*. Helion..

Whine M., *Islamist organizations on the Internet*, „Terrorism and Political Violence", t. 11, nr 1, 1999.

Zanini M., Edwards S.J.A. *(2001). The networking of terror in the information age,* [w]:
J. Arquilla, D. Ronfeldt, Networks and Netwars. Santa Monica.

Źródła internetowe

Garrison J., Grand M., *Cyberterrorism: An evolving concept*, NIPC Highlights, http://www.nipc.gov/publications/highlights/2001/ highlight-01-06.html [data dostępu: 15.06.2012].

http://niezalezna.pl/84940-twitter-na-wojnie-z-terroryzmem.

http://technologie.gazeta.pl/ internet/1,104530,9036923,Mobilny_Internet_na_swiecie___Polacy_na_ni echlubnym.html [data dostępu: 15.06.2012].

https://www.quintly.com/.

WALDEMAR ZUBRZYCKI
Wyższa Szkoła Policji w Szczytnie
boa.01@wp.pl

CENTRUM ANTYTERRORYSTYCZNE ABW JAKO NARZĘDZIE W PRZECIWDZIAŁANIU ZAGROŻENIOM TERRORYSTYCZNYM W POLSCE[1]

ANTI-TERRORIST CENTRE OF THE INTERNAL SECURITY AGENCY AS A TOOL IN COUNTERING TERRORIST THREAT IN POLAND

ABSTRACT

Anti-terrorist Centre of the Internal Security Agency is one of the most important tools of the Polish state to recognize terrorist threats. The essence of its operation is to coordinate the exchange of information between entities of the system of anti-terrorist protection of Poland. The free flow of information between the services of security of the state and other institutions is possible thanks to the work of this unit. It is also involved in supporting decision-making in cases of real emergency. Characteristics of the Centre, the history of its origin, the nature, purpose and conducted domestic and international cooperation, is presented in this paper on the background of the system of counteracting terrorist threats in Poland and the involvement of special services of Poland in this system – with emphasis on the leading role of the Internal Security Agency.

Keywords: *terrorism, the Internal Security Agency, Anti-terrorist Centre, the exchange of information*

[1] Inspiracją do stworzenia niniejszego opracowania stało się częste błędne identyfikowanie Centrum Antyterrorystycznego ABW jako ośrodka odpowiedzialnego za całokształt przedsięwzięć w zakresie walki z terroryzmem realizowanych w Polsce, co wynika – prawdopodobnie – z intuicyjnej interpretacji jego nazwy.

STRESZCZENIE

Centrum Antyterrorystyczne ABW to jedno z najważniejszych narzędzi państwa polskiego w zakresie rozpoznawania zagrożeń terrorystycznych. Istotą jego funkcjonowania jest koordynacja procesu wymiany informacji pomiędzy podmiotami systemu ochrony antyterrorystycznej RP. Dzięki pracy tej jednostki możliwy jest swobodny przepływ informacji pomiędzy służbami odpowiadającymi za bezpieczeństwo państwa a innymi instytucjami. Bierze ona również udział we wspomaganiu procesów decyzyjnych w przypadkach realnego zagrożenia. Charakterystyka Centrum, historia jego powstania, specyfika, przeznaczenie oraz prowadzona współpraca krajowa i międzynarodowa przedstawiona została w niniejszym opracowaniu na tle systemu przeciwdziałania zagrożeniom terrorystycznym w Polsce oraz udziału służb specjalnych RP w tym systemie – z podkreśleniem wiodącej roli Agencji Bezpieczeństwa Wewnętrznego.

Słowa kluczowe: *terroryzm, Agencja Bezpieczeństwa Wewnętrznego, Centrum Antyterrorystyczne, wymiana informacji*

WPROWADZENIE

Współczesny wymiar zagrożenia bezpieczeństwa terroryzmem powoduje, że różnorodność służb i instytucji zajmujących się przeciwdziałaniem i walką z nim jest ogromna. Wynika to ze złożoności charakteru współczesnego terroryzmu i wykorzystywania przez niego w swej działalności instrumentów nie tylko związanych z użyciem siły, ale także finansowych, w tym m.in. legalizacja środków na działalność terrorystyczną czy systemów powszechnej wymiany informacji.

Drugiego lipca 2016 roku weszła w życie Ustawa z dnia 10 czerwca 2016 roku o działaniach antyterrorystycznych (Dz.U. 2016 poz. 904). Podstawowym jej celem jest podniesienie efektywności polskiego systemu antyterrorystycznego, a tym samym zwiększenie bezpieczeństwa wszystkich obywateli RP, poprzez:

- wzmocnienie mechanizmów koordynacji działań,
- doprecyzowanie zadań i obszarów odpowiedzialności poszczególnych służb i organów oraz zasad współpracy między nimi,
- zapewnienie możliwości skutecznych działań w przypadku podejrzenia przestępstwa o charakterze terrorystycznym, w tym w zakresie postępowania przygotowawczego,
- zapewnienie mechanizmów reagowania adekwatnych do rodzaju występujących zagrożeń,

- dostosowanie przepisów karnych do nowych typów działań o charakterze terrorystycznym.

W ustawie dokonano jasnego przypisania odpowiedzialności za zapobieganie terroryzmowi szefowi Agencji Bezpieczeństwa Wewnętrznego. W związku z przypisanymi kompetencjami zapewniono temu organowi narzędzia prawno-organizacyjne mające w założeniu umożliwić skuteczną realizację ww. zadania[2].

AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO WŚRÓD SŁUŻB SPECJALNYCH RP

Służby specjalne, często mylone z siłami specjalnymi – ale temu poświęcić należy odrębne opracowanie – to zbiorcze określenie wszystkich służb wywiadowczych cywilnych i wojskowych oraz innych służb bezpieczeństwa, których działalność odbiega od zwykłej praktyki policyjnej („Encyklopedia szpiegostwa", s. 234). Tradycyjny podział służb specjalnych klasyfikuje je na wywiad i kontrwywiad. Ogólne zadania wywiadu w walce z zagrożeniami terrorystycznymi i przeciwdziałaniu im można określić jako:

- rozpoznawanie środowisk i organizacji terrorystycznych poza granicami kraju,
- analizowanie potencjalnego i realnego zagrożenia terrorystycznego państwa terroryzmem zewnętrznym,
- wyprzedzające reagowanie na realną możliwość zagrożenia terrorystycznego państwa przez organizacje terrorystyczne spoza kraju,
- prowadzenie działalności analitycznej dotyczącej stanu obecnego i ewentualnych przyszłych kierunków rozwoju zagrożenia terroryzmem zewnętrznym państwa,
- współpraca wywiadowcza z innymi państwami w zakresie zapobiegania i zwalczania terroryzmu (B. Hołyst, 2009, s. 1116).

Wśród zadań kontrwywiadu we wskazanym obszarze należy wymienić:

- rozpoznawanie środowisk i organizacji terrorystycznych na terytorium kraju,

[2] http://www.antyterroryzm.gov.pl/CAT/ochrona-antyterrorysty/ustawa-o-dzialaniach-an/1273,USTAWA-O-DZIALANIACH-ANTYTERRORYSTYCZNYCH.html.

- analizowanie potencjalnego i realnego zagrożenia terrorystycznego państwa terroryzmem wewnętrznym,
- reagowanie wyprzedzające na realną możliwość zagrożenia terrorystycznego państwa przez organizacje terrorystyczne w kraju,
- aresztowanie członków organizacji terrorystycznych,
- prowadzenie działalności analitycznej dotyczącej stanu obecnego i ewentualnych przyszłych kierunków rozwoju zagrożenia terroryzmem wewnętrznym państwa,
- współpracę kontrwywiadowczą z innymi państwami w zakresie zapobiegania terroryzmowi i jego zwalczania (B. Hołyst, 2009, s. 1117).

Rzeczpospolita Polska dysponuje służbami specjalnymi – cywilnymi i wojskowymi – których rodowód sięga okresu tuż po transformacji ustrojowej. Powołano je w 1990 roku, w miejsce funkcjonującej w poprzednim ustroju Służby Bezpieczeństwa podległej Ministerstwu Spraw Wewnętrznych oraz w miejsce Wywiadu Wojskowego podległego Ministerstwu Obrony Narodowej. Służbami specjalnymi RP do 2002 roku był Urząd Ochrony Państwa (UOP) oraz do 2006 roku – Wojskowe Służby Informacyjne (WSI). Obie organizacje działały z mocy ustaw, które regulowały ich zakres zainteresowania i kompetencje. Realizowały one zarówno zadania wywiadowcze, jak i kontrwywiadowcze, a UOP miał dodatkowo w swych strukturach pion śledczy. Do 1996 roku Urząd Ochrony Państwa stanowił integralną część Ministerstwa Spraw Wewnętrznych, po czym w tym samym roku został wyodrębniony z MSW, stając się centralnym urzędem administracji rządowej (M. Wierzbowski, 2006, s. 345).

W 2002 roku dokonano reformy służb specjalnych. Jej głównym zadaniem było utworzenie dwóch podstawowych segmentów: wywiadowczego i kontrwywiadowczego. Pierwszy zorientowany jest na zdobycie informacji poza granicami kraju, drugi ma za zadanie zapewnienie wewnętrznego bezpieczeństwa. W miejsce Urzędu Ochrony Państwa powołano dwie Agencje: Wywiadu oraz Bezpieczeństwa Wewnętrznego.

Wojskowe służby specjalne poddano reorganizacji w 2006 roku. Nastąpiło rozwiązanie istniejących do tej pory Wojskowych Służb Informacyjnych. W ich miejsce powstała: Służba Kontrwywiadu Wojskowego (SKW) oraz Służba Wywiadu Wojskowego (SWW) (M. Wierzbowski, 2006, s. 246).

Agencja Bezpieczeństwa Wewnętrznego (ABW) jest instytucją rządową działającą na rzecz bezpieczeństwa Rzeczypospolitej Polskiej i jej obywateli. Status służby specjalnej, jaki posiada ABW, oraz wynikające z tego obowiązki i uprawnienia, zostały uregulowane ustawą z dnia 24 maja 2002 roku o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. 2002 nr 74 poz. 676 ze zm.). Agencja Bezpieczeństwa Wewnętrznego jest właściwą agencją w sprawach ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego.

Do jej zadań należą:

- rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, a w szczególności w suwerenność i międzynarodową pozycję, niepodległość i nienaruszalność jego terytorium, a także obronność państwa,
- rozpoznawanie, zapobieganie i wykrywanie przestępstw:
  - szpiegostwa, terroryzmu, naruszania tajemnicy państwowej i innych przestępstw godzących w bezpieczeństwo państwa,
  - godzących w podstawy ekonomiczne państwa,
  - korupcji osób pełniących funkcje publiczne, (...) jeśli może to godzić w bezpieczeństwo państwa, w zakresie produkcji i obrotu towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa,
  - nielegalnego wytwarzania, posiadania i obrotu bronią, amunicją i materiałami wybuchowymi, bronią masowej zagłady oraz środkami odurzającymi i substancjami psychotropowymi, w obrocie międzynarodowym

  oraz ściganie ich sprawców,
- realizowanie, w granicach swojej właściwości, zadań służby ochrony państwa oraz wykonywanie funkcji krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych,
- uzyskiwanie, analizowanie, przetwarzanie i przekazywanie informacji, które mogą mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego,
- podejmowanie innych działań określonych w odrębnych ustawach międzynarodowych (art. 5.1. ustawy z dnia 24 maja 2002 roku o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu).

Na czele tej instytucji stoi szef ABW, jako centralny organ administracji rządowej. Podlega bezpośrednio prezesowi Rady Ministrów, a jego działalność – kontroli Sejmu. Powołuje go i odwołuje prezes Rady Ministrów, po zasięgnięciu opinii prezydenta Rzeczypospolitej Polskiej, Kolegium do Spraw Służb Specjalnych oraz sejmowej Komisji do Spraw Służb Specjalnych. Prezes Rady Ministrów, na wniosek szefa ABW, powołuje i odwołuje zastępców szefa ABW, po zasięgnięciu opinii sejmowej Komisji do Spraw Służb Specjalnych.

W skład ABW wchodzą jednostki organizacyjne – departamenty i biura: Departament Kontrwywiadu, Departament Przeciwdziałania Korupcji i Przestępczości Zorganizowanej, Departament Przeciwdziałania Terroryzmowi, Departament Postępowań Karnych, Departament Zabezpieczenia Technicznego, Departament Ochrony Informacji Niejawnych, Departament Bezpieczeństwa Teleinformatycznego, Biuro Ewidencji i Archiwum, a także: Biuro Prawne, Biuro Finansów, Biuro Kadr, Biuro Administracyjno-Gospodarcze. Jednostkami organizacyjnymi są delegatury. W skład delegatur mogą wchodzić wydziały zamiejscowe (M. Bożek, M. Czuryk, M. Karpiuk, J. Kostrubiec, 2014, s. 123). Kadra ABW to absolwenci elitarnych szkół wyższych, wyróżniający się odpowiednimi standardami etycznymi do realizowania istotnych dla bezpieczeństwa państwa zadań (M. Bożek, M. Czuryk, M. Karpiuk, J. Kostrubiec, 2014, s. 124). Służbę w ABW może pełnić osoba mająca wyłącznie obywatelstwo polskie, korzystająca w pełni z praw publicznych, wykazująca się nieskazitelną postawą moralną, obywatelską i patriotyczną, dająca rękojmię zachowania tajemnicy stosownie do wymogów określonych w przepisach o ochronie informacji niejawnych, mająca co najmniej średnie wykształcenie i określone kwalifikacje zawodowe oraz zdolność fizyczną i psychiczną do służby w formacjach uzbrojonych, wymagających szczególnej dyscypliny służbowej, której gotowa jest się podporządkować (art. 44 ustawy z dnia 24 maja 2002 roku o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu).

Funkcjonariusze Agencji Bezpieczeństwa Wewnętrznego wykonują czynności operacyjno-rozpoznawcze i dochodzeniowo-śledcze w celu rozpoznawania, zapobiegania i wykrywania przestępstw oraz ścigania ich sprawców, a także czynności na polecenie sądu lub prokuratora w zakresie określonym w Kodeksie karnym wykonawczym (M. Bożek, M. Czuryk, M. Karpiuk, J. Kostrubiec, 2014, s. 124). Realizując swoje służbowe obowiązki, mają oni prawo do:

- wydawania osobom poleceń określonego zachowania się,
- legitymowania osób w celu ustalenia ich tożsamości,
- zatrzymywania osób,
- przeszukiwania osób i pomieszczeń,
- dokonywania kontroli osobistej,
- przeglądania zawartości bagaży oraz sprawdzania ładunku w środkach transportu lądowego, powietrznego i wodnego, w razie istnienia uzasadnionego podejrzenia popełnienia czynu zabronionego pod groźbą kary,
- obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych oraz dźwięku towarzyszącego tym zdarzeniom w trakcie wykonywania czynności operacyjno-rozpoznawczych,
- żądania niezbędnej pomocy od instytucji państwowych, organów administracji rządowej i samorządu terytorialnego oraz przedsiębiorców prowadzących działalność w zakresie użyteczności publicznej,
- zwracania się o niezbędną pomoc do innych przedsiębiorców, jednostek organizacyjnych i organizacji społecznych, jak również zwracania się w nagłych wypadkach do każdej osoby o udzielenie doraźnej pomocy (art. 23.1. ustawy z dnia 24 maja 2002 roku o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu).

W razie niepodporządkowania się wydanym na podstawie prawa poleceniom funkcjonariusze ABW mogą stosować fizyczne, techniczne i chemiczne środki przymusu bezpośredniego, służące do obezwładniania lub konwojowania osób oraz do zatrzymywania pojazdów. Jeżeli środki te okazałyby się niewystarczające lub ich użycie, ze względu na okoliczności danego zdarzenia, nie byłoby możliwe, funkcjonariusz ABW ma prawo do użycia broni palnej przy spełnieniu warunków określonych przez przepisy prawa. Ma on również prawo prowadzić kontrolę operacyjną oraz niejawne nadzorowanie wytwarzania, przemieszczania, przechowywania i obrotu przedmiotami przestępstwa, jeżeli nie stworzy to zagrożenia dla życia lub zdrowia ludzkiego.

Misją Agencji jest posiadanie wiedzy – możliwie wcześnie i możliwie najpełniejszej – aby skutecznie neutralizować zagrożenia dla bezpieczeństwa państwa. Doświadczenie w kompletowaniu i analizowaniu informacji, istotnych z punktu widzenia tego bezpieczeństwa, pozwala jej skutecznie realizować delegowane ustawowo zadania.

CENTRUM ANTYTERRORYSTYCZNE W SYSTEMIE PRZECIWDZIAŁANIA ZAGROŻENIOM TERRORYSTYCZNYM RP

Przeciwdziałanie zagrożeniom terrorystycznym w naszym kraju dotyka wielu obszarów działalności, od ochrony granicy państwowej, poprzez odpowiednie konstrukcje prawne oraz zagadnienia związane z sądownictwem i prokuraturami, neutralizację skutków zamachów, aż po umiejętne zapobieganie finansowaniu tego zjawiska. Odbywa się to w ramach zbudowanego w tym celu systemu funkcjonującego na trzech poziomach:

- strategicznym – realizowanym przez prezesa Rady Ministrów i Międzyresortowy Zespół do Spraw Zagrożeń Terrorystycznych,
- operacyjnym – realizowanym przez krajowe służby w zakresie działań operacyjno-rozpoznawczych oraz Centrum Antyterrorystyczne ABW (CAT),
- taktycznym – wykonywanym przez służby i instytucje, w których zakresie właściwości pozostaje antyterrorystyczna ochrona kraju (m.in. ABW, AW, Policja, Straż Graniczna, GIIF) (W. Zubrzycki, „Organy administracji państwowej RP w przeciwdziałaniu zjawisku terroryzmu", [w:] Z. Piątek, A. Letkiewicz, 2010, s. 190–191).

Poziom operacyjny służy stałemu, szybkiemu i syntetycznemu informowaniu kierownictwa państwa o zagrożeniach oraz działaniach podejmowanych przez służby państwowe. Na tym poziomie – na płaszczyźnie analityczno-informacyjnej – odbywa się również koordynacja działań służących identyfikacji i przeciwdziałaniu zagrożeniom terrorystycznym, prowadzonych przez krajowe służby i instytucje (A. Makarski, 2010, s. 103).

Przeprowadzona pod koniec 2007 roku analiza porównawcza rozwiązań systemowych w państwach Unii Europejskiej – realnie zagrożonych atakiem terrorystycznym – z funkcjonującą wówczas w Polsce strukturą wykazała, że w wielu krajach Wspólnoty istnieją rozwiązania pozwalające na koordynację działalności służb i instytucji państwowych w zakresie przeciwdziałania terroryzmowi. W zależności od zastosowanych systemów, działanie rozwiązań systemowych dotyczy sfery analityczno-informacyjnej, czynności operacyjno-rozpoznawczych, prewencyjnych lub reagowania po dokonaniu zamachu terrorystycznego. Jednocześnie uplasowanie struktur

i osób koordynujących działania jest różnorodne[3] – niejednokrotnie są to członkowie rad ministrów, jednostki organizacyjne ministerstw spraw wewnętrznych albo podmioty funkcjonujące w lub przy wewnętrznych służbach specjalnych. Pomimo rekomendacji Wspólnoty oraz wcześniejszych prób opracowania rozwiązań systemowych w tym zakresie, w Polsce brak było struktury, która koordynowałaby działalność krajowych służb i instytucji w zakresie zwalczania terroryzmu. W zakresie czterech filarów UE, zajmujących się przeciwdziałaniem terroryzmowi[4], funkcjonowały liczne organy państwowe, podległe prezesowi Rady Ministrów, ministrom spraw wewnętrznych i administracji, finansów, obrony narodowej, spraw zagranicznych oraz infrastruktury, ale ich działania nie były w pełni koordynowane, zaś efektem tego stanu były różne – niejednokrotnie skrajnie rozbieżne – oceny poziomu zagrożenia terrorystycznego RP oraz identyfikacji czynników oddziałujących na ten stan. W związku z taką diagnozą stworzona została koncepcja rozdziału zadań – wynikających ze strategii UE dotyczącej zwalczania terroryzmu – pomiędzy instytucje państwowe oraz pomysł powołania struktury o charakterze operacyjnym, czyli Centrum Antyterro-

[3] Przykłady ulokowania międzyinstytucjonalnych jednostek administracji państwowej odpowiedzialnych za koordynację zwalczania zagrożeń o charakterze terrorystycznym w wybranych krajach UE: Wielka Brytania – *Joint Terrorism Analysis Centre* (*JTAC*) – organizacja ustanowiona przy MI5 (*The Security Service*), jej dyrektor podlega dyrektorowi naczelnemu MI5, który z kolei odpowiada przed ministrem spraw wewnętrznych; Hiszpania – *Centro Nacional de Coordinación Antiterrorista* (*CNCA*) – funkcjonuje w ramach Ministerstwa Spraw Wewnętrznych i z poziomu tego resortu koordynuje wszelkie działania antyterrorystyczne w kraju; Niemcy – *Gemeinsames Terrorismusabwehrzentrum* (*GTAT*) – operuje w Departamencie Bezpieczeństwa Państwa służby specjalnej BKA (*Bundeskriminalamt*); Włochy – *Comitato Analisi Strategica Antiterrorismo* (*CASA*) – działa w ramach Centralnej Dyrekcji Policji Prewencyjnej w Departamencie Bezpieczeństwa Publicznego Ministerstwa Spraw Wewnętrznych, podlega szefowi Policji, który pełni funkcję dyrektora generalnego ds. bezpieczeństwa publicznego; Francja – *Antiterrorist Struggle Coordination Unit* (*UCLAT*) – jednostka podporządkowana bezpośrednio dyrektorowi generalnemu Policji Narodowej, odpowiada za zbieranie informacji pochodzących z instytucji podległych resortowi właściwemu do spraw wewnętrznych, obrony, finansów, gospodarki i sprawiedliwości; Holandia – *De Nationaal Coördinator Terrorismebestrijding* (*NCTb*) – w ramach Urzędu Krajowego Koordynatora ds. Przeciwdziałania Terroryzmowi funkcjonuje Departament Ekspertyz i Analiz, holenderski koordynator ds. antyterroryzmu podlega jednocześnie według właściwości zarówno ministrowi sprawiedliwości, jak i ministrowi spraw wewnętrznych; Dania – *Centre for Terror Analyse* (*CTA*) – operuje w strukturze służby specjalnej PET (*Politiets Efterretningstjeneste*) i podlega bezpośrednio jej dyrektorowi naczelnemu.

[4] Zapobieganie, ochrona, ściganie i reagowanie.

rystycznego ABW. Projekt ten przedstawiony został członkom Międzyresortowego Zespołu ds. Zagrożeń Terrorystycznych[5], którzy poparli zawarte w nim idee, dotyczące przede wszystkim rozdziału kompetencji i wskazania podmiotów koordynujących realizację zadań na terenie Polski oraz struktury krajowego systemu zwalczania terroryzmu (A. Makarski, 2010, s. 102). Konieczność zorganizowania takiej instytucji wynikała z potrzeby usprawnienia realizacji zadań wynikających z ustawy o ABW oraz AW z dnia 24 maja 2002 roku, jak również realizacji zaleceń Parlamentu Europejskiego z 2005 roku[6]. Według założeń, w świetle zbliżającej się prezydencji Polski w Unii Europejskiej w 2011 roku oraz konieczności zabezpieczenia imprez masowych – mistrzostw Europy w piłce siatkowej kobiet i w koszykówce mężczyzn w 2009 roku oraz mistrzostw Europy w piłce nożnej w 2012 roku, CAT miał być kluczowym elementem systemu ochrony i koordynacji działań antyterrorystycznych w Polsce.

Centrum Antyterrorystyczne Agencji Bezpieczeństwa Wewnętrznego powołano na mocy Zarządzenia Prezesa Rady Ministrów nr 102 z dnia 17 września 2008 roku zmieniającego zarządzenie w sprawie nadania statutu Agencji Bezpieczeństwa Wewnętrznego (M.P. 2008 nr 69 poz. 622). Bezpośrednie prace związane z utworzeniem CAT trwały przez dziewięć miesięcy; w styczniu 2008 roku minister spraw wewnętrznych i administracji oraz szef Agencji Bezpieczeństwa Wewnętrznego podpisali wspólną koncepcję powołania Centrum. W dniu 1 października 2008 roku CAT faktycznie rozpoczął swoje funkcjonowanie.

---

[5] Przewodniczący – minister spraw wewnętrznych i administracji, zastępcy przewodniczącego: minister spraw zagranicznych, minister finansów, minister obrony narodowej, minister sprawiedliwości oraz minister – członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych. Pozostałymi członkami Zespołu są sekretarze lub podsekretarze stanu w MSWiA, sprawujący nadzór nad prowadzeniem spraw objętych działem administracji rządowej, sekretarz Kolegium ds. Służb Specjalnych, szef Obrony Cywilnej Kraju, szef Agencji Bezpieczeństwa Wewnętrznego, szef Agencji Wywiadu, szef Biura Ochrony Rządu, komendant główny Policji, komendant główny Straży Granicznej, komendant główny Państwowej Straży Pożarnej, szef Służby Wywiadu Wojskowego, szef Służby Kontrwywiadu Wojskowego, komendant główny Żandarmerii Wojskowej, Generalny Inspektor Kontroli Skarbowej, Generalny Inspektor Informacji Finansowej, szef Służby Celnej i dyrektor Rządowego Centrum Bezpieczeństwa.

[6] Zob. P6_TA(2005)0220 *Ataki terrorystyczne: zapobieganie, przygotowanie i odpowiedź*. Zalecenie Parlamentu Europejskiego dla Rady Europejskiej i Rady w sprawie zapobiegania, przygotowania i odpowiedzi na ataki terrorystyczne, 2005/2043(INI), Dziennik Urzędowy Unii Europejskiej 25.5.2006.

Centrum zajmuje się koordynacją działań operacyjno-rozpoznawczych zmierzających do weryfikacji informacji o potencjalnych zagrożeniach, bierze udział we wspomaganiu procesów decyzyjnych w przypadkach realnego zagrożenia, poprzez przekazywanie wszelkich danych umożliwiających przygotowanie i zabezpieczenie sił i środków niezbędnych do prawidłowego reagowania w sytuacji kryzysowej. W ramach pracy analityczno-informacyjnej sporządza dla kierownictwa państwa, Międzyresortowego Zespołu ds. Zagrożeń Terrorystycznych i Rządowego Centrum Bezpieczeństwa[7] informacje na temat aktualnego poziomu zagrożenia terrorystycznego kraju i działań podejmowanych przez służby i instytucje państwowe w celu likwidacji niebezpieczeństw („Raport z działalności Agencji Bezpieczeństwa Wewnętrznego w 2009 r.", s. 23). Do zadań CAT należą[8]:

- wspomaganie procesów decyzyjnych w przypadku realnego zagrożenia atakiem terrorystycznym – CAT niezwłocznie po uzyskaniu wiedzy o możliwym zamachu przekazuje m.in. prezesowi Rady Ministrów, ministrowi spraw wewnętrznych i administracji oraz dyrektorowi Rządowego Centrum Bezpieczeństwa wszelkie dane pozwalające na przygotowanie i zabezpieczenie sił i środków niezbędnych do prawidłowego reagowania kryzysowego,
- koordynacja współdziałania służb odpowiedzialnych za zwalczanie terroryzmu w zakresie działań operacyjno-rozpoznawczych, realizowana przez:
  - cykliczne lub doraźne narady osób szczebla decyzyjnego, w trakcie których określane są zadania do realizacji w ramach rozpoznawanych zagrożeń oraz wytyczane perspektywiczne kierunki i obszary aktywności służb i instytucji państwowych,
  - stałe przekazywanie sygnałów o potencjalnych zagrożeniach dla kierownictw instytucji współpracujących z CAT celem podejmowania na bieżąco działań, zgodnie z algorytmami reagowania w sytuacjach zagrożenia,

[7] Państwowa jednostka budżetowa, podległa prezesowi Rady Ministrów, porządkująca funkcjonowanie zespołów właściwych w sprawach zarządzania kryzysowego, poprzez dokonywanie pełnej analizy zagrożeń, opracowywanie optymalnych rozwiązań pojawiających się sytuacji kryzysowych oraz koordynowanie przepływu informacji o zagrożeniach (na podstawie: http://rcb.gov.pl/o-rcb/, data dostępu: 26.08.2016).

[8] http://www.abw.gov.pl/pl/zadania/zwalczanie-terroryzmu/centrum-antyterrorysty/zadania/331,Zadania.html [data dostępu: 26.08.2016].

- monitoring aktywności organizacji terrorystycznych i ich członków oraz struktur wspierających,
- monitoring poziomu bezpieczeństwa obiektów mogących stanowić potencjalne cele dla ataku terrorystycznego,

➲ wykonywanie czynności analityczno-informacyjnych, m.in. w zakresie sporządzania:
- aktualnych, syntetycznych i całościowych informacji dla kierownictwa państwa (prezydenta RP, prezesa Rady Ministrów) na temat poziomu zagrożenia terrorystycznego kraju oraz działań podejmowanych przez służby i instytucje państwowe w celu zniwelowania niebezpieczeństw,
- prognoz długo- i krótkookresowych na temat poziomu zagrożenia terrorystycznego Polski,
- analiz zagrożenia terrorystycznego w innych państwach, w kontekście bezpieczeństwa strategicznych interesów i obywateli RP,
- ocen funkcjonowania systemów ochrony elementów infrastruktury krytycznej kraju, pod kątem usunięcia ewentualnych nieprawidłowości,

➲ udział w opracowywaniu i nowelizowaniu procedur reagowania kryzysowego na wypadek ataku oraz sporządzanie algorytmów działań przed zamachem, poprzez uczestnictwo w działaniach weryfikujących skuteczność aktualnie wykorzystywanych schematów postępowania w sytuacjach kryzysowych, a także wykrywanie i analizowanie słabych punktów zarządzania kryzysowego przy jednoczesnym wskazaniu potencjalnych strategii i kierunków dalszych działań,

➲ monitoring zagranicznych mediów sympatyzujących z terrorystami,

➲ wspomaganie, po ewentualnym zamachu terrorystycznym, działań służb i instytucji uczestniczących w akcji antyterrorystycznej w Polsce; CAT kontynuuje działalność koordynacyjną w zakresie analityczno-informacyjnym także po wystąpieniu sytuacji kryzysowej, jaką jest zamach terrorystyczny – zgodnie z ustawą z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym (Dz.U. 2007 nr 89 poz. 590), szef ABW uczestniczy w realizacji czynności z zakresu likwidacji skutków zdarzeń o charakterze terrorystycznym; ponadto w centrali ABW funkcjonuje zespół reagowania podejmujący działania w przypadku uzyskania informacji o wystąpieniu lub możliwości wystąpienia zdarzenia o takim charakterze,

- współpraca z partnerami zagranicznymi, prowadzona na płaszczyźnie dwu- i wielostronnej; obejmuje ona przede wszystkim wymianę informacji, wspólną analizę globalnych zagrożeń oraz dzielenie się doświadczeniami i wiedzą.

W zakresie realizowania tego ostatniego zadania priorytet stanowi nawiązywanie i rozwój relacji z podobnymi strukturami w innych krajach. Warunkiem skuteczności europejskiego systemu ochrony antyterrorystycznej jest szybkość wymiany danych pomiędzy podmiotami odpowiadającymi za bezpieczeństwo państw członkowskich przed terroryzmem. W związku z tym CAT kładzie szczególny nacisk na uruchamianie i utrzymywanie bezpośredniej, bezpiecznej łączności z centrami antyterrorystycznymi na świecie. Wśród partnerów Centrum znajdują się m.in.: brytyjski Joint Terrorism Analysis Centre (JTAC), amerykański National Counterterrorism Center (NCTC), niemiecki Gemeinsames Terrorismus-abwehrzentrum (GTAZ) czy duński Centre for Terrorism Analysis (CTA). Szczególną rolę wśród partnerów CAT, z uwagi na wspólne zabezpieczanie mistrzostw Europy w piłce nożnej Euro 2012, zajmuje jego ukraiński odpowiednik – Anti-Terrorist Center (ATC), funkcjonujący przy Służbie Bezpieczeństwa Ukrainy.

Polska, jako członek Unii Europejskiej, jest zobowiązana do realizacji unijnej Strategii w zakresie zwalczana terroryzmu[9]. Działania w tym zakresie CAT realizuje poprzez udział w pracach grupy roboczej ds. terroryzmu w ramach współpracy policyjnej i sądowej w sprawach karnych. Na forum tego gremium państwa członkowskie wymieniają się informacjami dotyczące terroryzmu oraz podejmują inicjatywy zmierzające do poprawy współpracy europejskiej w zakresie zwalczanie tego zjawiska. Ponadto Centrum Antyterrorystyczne – jako jednostka organizacyjna Agencji Bezpieczeństwa Wewnętrznego – uczestniczy w pracach grup skupiających służby wywiadu i bezpieczeństwa państw europejskich, takich jak Klub Berneński[10] oraz The Counter Terrorist Group[11] (CTG). Centrum Antyterrorystyczne ABW jest

[9] Przyjęta przez Radę UE w dniach 1–2 grudnia 2005 roku.

[10] Skupia służby wywiadu i bezpieczeństwa państw członkowskich UE oraz Norwegii i Szwajcarii.

[11] Międzynarodowa, nieformalna grupa, utworzona przez Klub Berneński, która koncentruje się na terroryzmie międzynarodowym.

też aktywnym członkiem organu konsultatywnego dla służb bezpieczeństwa państw członkowskich NATO[12].

Przy tworzeniu koncepcji polskiego Centrum Antyterrorystycznego skorzystano z doświadczeń innych państw, m.in. z brytyjskich rozwiązań (JTAC) przeniesiono w polskie realia sferę działań w zakresie pracy analityczno-informacyjnej; na podstawie rozwiązań niemieckich (GTAZ) stworzono system koordynacji działań operacyjno-rozpoznawczych; korzystając z wzorców brytyjskiego (JTAC) oraz ukraińskiego (ATC), polski CAT ulokowano przy wewnętrznej służbie specjalnej, jaką jest Agencja Bezpieczeństwa Wewnętrznego (A. Makarski, 2010, s. 109). Własnym, wyłącznie polskim wkładem do koncepcji działań CAT są zastosowane założenia teleinformatyczne, które – jak niejednokrotnie stwierdzali przedstawiciele zagranicznych centrów – spowodowały, że w polskim Centrum Antyterrorystycznym wdrożone zostały rozwiązania na miarę XXI wieku. Osiągniętą przez CAT funkcjonalność docenił również koordynator UE ds. zwalczania terroryzmu, Gilles de Kerchove, który w jednym ze swoich raportów wskazał, że analogiczne rozwiązania należałoby wdrożyć w innych państwach Wspólnoty (A. Makarski, 2010, s. 110). Jednym z elementów tych założeń są stałe, bezpieczne połączenia (on-line) z najważniejszymi instytucjami państwowymi (Kancelarią Prezydenta RP, Kancelarią Prezesa Rady Ministrów, MSWiA, MON), najważniejszymi instytucjami i podmiotami oraz krajowymi służbami uczestniczącymi w systemie antyterrorystycznej ochrony kraju, a także partnerami zagranicznymi.

Istotą funkcjonowania CAT jest koordynacja procesu wymiany informacji między uczestnikami systemu ochrony antyterrorystycznej, umożliwiająca wdrażanie wspólnych procedur reagowania w przypadku zaistnienia jednej z czterech kategorii zdefiniowanego zagrożenia:

- zdarzenia terrorystycznego zaistniałego poza granicami Polski, mającego wpływ na bezpieczeństwo RP i jej obywateli,
- zdarzenia terrorystycznego zaistniałego na terenie Polski, mającego wpływ na bezpieczeństwo RP i jej obywateli,
- uzyskania informacji o potencjalnych zagrożeniach mogących wystąpić na terenie Polski i poza granicami RP,

[12] http://www.abw.gov.pl/pl/zadania/zwalczanie-terroryzmu/centrum-antyterrorysty/wspolpraca-zagraniczna/355,Wspolpraca-zagraniczna-CAT.html [data dostępu: 26.08.2016].

- uzyskania informacji dotyczących prania pieniędzy lub transferów środków finansowych mogących świadczyć o finansowaniu działalności terrorystycznej[13].

Centrum Antyterrorystyczne ABW funkcjonuje w systemie całodobowym, przez siedem dni w tygodniu. Oprócz funkcjonariuszy ABW służbę w nim pełnią oddelegowani funkcjonariusze, żołnierze i pracownicy m.in. Policji, Straży Granicznej, Biura Ochrony Rządu, Agencji Wywiadu, Służby Wywiadu Wojskowego, Służby Kontrwywiadu Wojskowego oraz Służby Celnej. Realizują oni zadania w ramach kompetencji instytucji, którą reprezentują. Ponadto z Centrum Antyterrorystycznym ABW aktywnie współpracują inne podmioty uczestniczące w systemie ochrony antyterrorystycznej RP, takie jak: Ministerstwo Spraw Wewnętrznych i Administracji, Ministerstwo Spraw Zagranicznych, Państwowa Straż Pożarna, Generalny Inspektor Informacji Finansowej, Sztab Generalny Wojska Polskiego, Żandarmeria Wojskowa, Urząd Lotnictwa Cywilnego, Państwowa Agencja Atomistyki, Rządowe Centrum Bezpieczeństwa itp. (A. Makarski, 2010, s. 106–107).

Mając na uwadze, że wszystkie służby i instytucje biorące udział w pracach CAT przekazują do niego znajdujące się w ich posiadaniu niezbędne informacje służące prowadzeniu bieżącego rozpoznawania czy przeciwdziałaniu zagrożeniom terrorystycznym, posiada on najpełniejszy obraz rzeczywistych zagrożeń, bieżących trendów w zakresie terroryzmu oraz ma możliwość sporządzania najbardziej przekrojowych prognoz w opisywanym zakresie. Dlatego do zadań CAT należy również bieżące określanie poziomu i charakteru zagrożenia terrorystycznego oraz rekomendowanie podwyższenia, obniżenia lub utrzymania stopnia zagrożenia takim atakiem[14].

Służby i instytucje uczestniczące w systemie ochrony antyterrorystycznej RP przekazują do Centrum Antyterrorystycznego informacje na podstawie „Otwartego katalogu incydentów i zdarzeń zgłaszanych do Centrum Antyterrorystycznego Agencji Bezpieczeństwa Wewnętrznego". Dokument ten, sporządzony w 2008 roku przez Międzyresortowy Zespół do Spraw Za-

[13] http://www.antyterroryzm.gov.pl/CAT/ochrona-antyterrorysty/centrum-antyterrorysty/518,CENTRUM-ANTYTERRORYSTYCZNE-CAT.html [data dostępu: 26.08.2016].

[14] Każdorazowo posiedzenia Międzyresortowego Zespołu ds. Zagrożeń Terrorystycznych rozpoczynają się właśnie od relacji dyrektora CAT na temat bieżących wydarzeń i rekomendowanego poziomu zagrożenia RP terroryzmem.

grożeń Terrorystycznych, został znowelizowany 24 maja 2013 roku i przyjęty przez to gremium w formie Uchwały nr 1/2013. Obecnie katalog ten zawiera szczegółowy wykaz 108 zdarzeń i incydentów, które są pogrupowane w 15 kategorii.

Dzięki przyjętym rozwiązaniom, informacje przekazywane do CAT mogą być wykorzystywane przez wszystkie podmioty rozpoznające i zwalczające zjawisko terroryzmu oraz w pełni służyć skutecznemu działaniu całego systemu ochrony antyterrorystycznej RP. Bazy danych oraz systemy łączności Centrum umożliwiają natychmiastowe pozyskiwanie informacji, ich weryfikowanie i dzielenie się nabytą w ten sposób wiedzą z partnerami w kraju i za granicą. Nowoczesne rozwiązania techniczne w zakresie zarządzania informacjami i łącznością pozwalają skrócić do niezbędnego minimum czas wymiany tych informacji między podmiotami (M. Obuchowicz, 2014, s. 277). Na podstawie informacji przekazywanych przez służby i instytucje uczestniczące w pracach CAT, w Centrum sporządzane są również bieżące informacje odnoszące się do odnotowanych incydentów mogących mieć wpływ na zagrożenie bezpieczeństwa państwa w zakresie terroryzmu. Raporty te mają przedstawiać działania realizowane przez poszczególne jednostki organizacyjne współdziałające w ramach CAT w odniesieniu do konkretnych zagrożeń.

Z aktualnego rozpoznania Agencji Bezpieczeństwa Wewnętrznego wynika, że zagrożenie podjęcia na terytorium naszego kraju bezpośrednich działań terrorystycznych jest niskie i ma raczej charakter potencjalny. Jak dotąd nie odnotowano próby ataku terrorystycznego skierowanego przeciwko obiektom rządu polskiego, polskim instytucjom państwowym.

PODSUMOWANIE

Spośród aktualnych zagrożeń RP nadrzędną rolę odgrywają zagrożenia o charakterze politycznym, ponieważ mogą one być impulsem wyzwalającym wystąpienie innego rodzaju zagrożeń, szczególnie ekonomicznych, militarnych i społecznych. W skomplikowanej rzeczywistości stosunków międzynarodowych zagrożenia mogą się wzajemnie przenikać, występować pojedynczo lub kompleksowo, a niekiedy przybrać formę zagrożenia innego typu. Procesy globalizacji powodują poszerzenie przedmiotowego zakresu bezpieczeństwa państwa. Pojawiły się też nowe rodzaje zagrożeń, czego przykładem może być zagrożenie dla bezpieczeństwa systemów informacyjnych. W obecnych czasach zmalała rola zagrożeń militarnych, w tym ze stro-

ny sąsiadów Polski. Zmienił się również charakter zagrożeń, choćby z tego powodu, że nośnikiem siły mogą być podmioty ponadpaństwowe bądź pozapaństwowe oraz dlatego, że pojawił się nowy typ przemocy wewnątrz państwa. W dobie globalizacji coraz więcej zagrożeń ma charakter transgraniczny. Są to np. zagrożenia ekonomiczne, wynikające z oddziaływania rynków kapitałowych, kapitału spekulacyjnego i międzynarodowych korporacji, oraz zagrożenia ekologiczne. Jednocześnie następuje poszerzenie zakresu podmiotów będących nośnikami określonych zagrożeń, np. zagrożenia o charakterze społecznym są powodowane przez podmioty niepaństwowe, takie jak międzynarodowe struktury i grupy przestępcze oraz terrorystyczne. Zwłaszcza w ostatnich latach następuje intensyfikacja zagrożeń z ich strony. Cechą niektórych zagrożeń bezpieczeństwa narodowego jest ich międzyterytorialny zasięg. Funkcjonujące w transnarodowej przestrzeni społecznej są oderwane od jakiejkolwiek lokalizacji. Do takich zagrożeń zaliczyć można terroryzm międzynarodowy, dotyczący również bezpieczeństwa narodowego Rzeczypospolitej Polskiej (R. Olszewski, 2005, s. 79).

Wzrost znaczenia terroryzmu jako czynnika wpływającego na rozwój stosunków międzynarodowych spowodował zmiany w koncepcjach jego zwalczania. Początkowo była to domena policji i sił porządkowych, by w krótkim czasie stać się zadaniem policji politycznych i służb specjalnych. Ten model posłużył do budowy prawnego, międzynarodowego modelu zwalczania terroryzmu, który opiera się na uznaniu obowiązków państw w zakresie ścigania terrorystów przy udziale międzynarodowej pomocy prawnej. Model ten rozwija się nadal w różnych kierunkach. Ponadto zwalczanie terroryzmu w ramach tego rozwiązania obejmuje już nie tylko ściganie sprawców aktów terrorystycznych, ale także zapobieganie finansowaniu, rekrutacji, szkoleniu bądź propagowaniu działań terrorystycznych.

Najważniejszym elementem krajowego systemu ochrony antyterrorystycznej jest Centrum Antyterrorystyczne ABW (M. Obuchowicz, 2014, s. 275). Podstawowym zadaniem CAT ABW jest koordynowanie procesu wymiany informacji pomiędzy uczestnikami systemu ochrony antyterrorystycznej oraz wdrażanie we właściwym czasie wspólnych procedur reagowania w przypadku wystąpienia zdarzenia terrorystycznego w kraju bądź za granicą, mającego wpływ na bezpieczeństwo RP i jej obywateli (M. Obuchowicz, 2014, s. 277). Dzięki pracy tej jednostki jest możliwy swobodny przepływ informacji pomiędzy służbami odpowiadającymi za bezpieczeństwo

państwa a innymi instytucjami. Informacje uzyskane przez CAT od krajowych oraz zagranicznych służb i instytucji liczone są w dziesiątkach tysięcy, jednocześnie Centrum pełni funkcję jednostki analitycznej i wspiera działania podmiotów właściwych w zakresie zwalczania terroryzmu. W swojej historii Centrum Antyterrorystyczne monitorowało wiele incydentów, rozpoznając je pod kątem ewentualnych zagrożeń terrorystycznych dla Polski lub jej obywateli. Z punktu widzenia ich bezpieczeństwa ważny jest fakt, że wielopłaszczyznowa współpraca CAT z instytucjami aktywnymi w zakresie zapobiegania terroryzmowi w Polsce i za granicą stale się rozwija, a jej zakres nieustannie się poszerza.

Bibliografia

Bożek M., Czuryk M., Karpiuk M., Kostrubiec J. (2014). *Służby specjalne w strukturze władz publicznych. Zagadnienia prawnoustrojowe*. Wydawnictwo Wolters Kluwer. Warszawa.

Encyklopedia szpiegostwa (1995). PWN. Warszawa.

Hołyst B. (2009). *Terroryzm,* t. 2. LexisNexis. Warszawa.

Makarski A. (2010). *Centrum Antyterrorystyczne Agencji Bezpieczeństwa Wewnętrznego. Geneza, zasady działania oraz doświadczenia po pierwszym roku funkcjonowani*., „Przegląd Bezpieczeństwa Wewnętrznego", nr 2/10. ABW. Warszawa.

Obuchowicz M. (2014). *Pięć lat funkcjonowania Centrum Antyterrorystycznego ABW (2008–2013)*. „Przegląd Bezpieczeństwa Wewnętrznego", nr 10/14. ABW. Warszawa.

Olszewski R. (2005). *Bezpieczeństwo współczesnego świata*. Wydawnictwo Adam Marszałek. Toruń.

Piątek Z., Letkiewicz A. (red.), (2010). *Terroryzm a infrastruktura krytyczna państwa – zewnętrznego kraju Unii Europejskiej*. Szczytno.

Raport z działalności Agencji Bezpieczeństwa Wewnętrznego w 2009 r. ABW. Warszawa 2010.

Wierzbowski M. (2006). *Prawo administracyjne*. Wydawnictwo Wolters Kluwer. Warszawa.

Źródła prawa

Ustawa z dnia 24 maja 2002 roku o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. 2002 nr 74 poz. 676 ze zm.).

Ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym (Dz.U. 2007 nr 89 poz. 590).

Ustawa z dnia 10 czerwca 2016 roku o działaniach antyterrorystycznych (Dz.U. 2016 poz. 904).

Zarządzenie nr 102 Prezesa Rady Ministrów z dnia 17 września 2008 roku zmieniające zarządzenie w sprawie nadania statutu Agencji Bezpieczeństwa Wewnętrznego (M.P. 2008 nr 69 poz. 622).

Źródła internetowe

http://rcb.gov.pl

http://www.abw.gov.pl

http://www.antyterroryzm.gov.pl

KONRAD ŚWIRSKI
Politechnika Warszawska
konrad.swirski@itc.pw.edu.pl

ISSUES OF CRITICAL INFRASTRUCTURE CYBER SECURITY IN THE POWER SECTOR

ABSTRACT

The article presents the problem of modern threats to critical IT infrastructure in the power sector (ICS – Industrial Control Systems) and the current status of global solutions, norms, standards and procedures and shows typical control systems protection strategies employed in the power sector. The emergence of advanced cyber-attacks against power control and distribution systems indicates a growing possibility of military attacks and malware prepared as a new forms of offensive weapons. Taking into consideration the possibility of using advanced techniques in cyber-attacks, most of the existing, commercial protection systems may be insufficient. It is necessary for critical infrastructure in the power sector to isolate systems from the outside world, which in turn could be inconvenient because it limits the possibility of remote process observation. In addition, solutions for the secure data communication are constantly developed and evaluated and this article presents in detail a secure communication solution for acquiring data from industrial DCS automation systems (power generation).

Keywords: *cyber security, critical infrastructure, IT OT, ICS, control systems*

STRESZCZENIE

Artykuł przedstawia problem cyberbezpieczeństwa infrastruktury krytycznej w energetyce (ICS – Industrial Control Systems) poprzez pryzmat możliwych zagrożeń, światowych rozwiązań, norm, standardów i procedur oraz pokazuje typowe strategie ochrony systemów sterowania w energetyce. Pojawianie się coraz bardziej zaawansowanych form ataków cybernetycznych na systemy stero-

wania związane z wytwarzaniem i przesyłem energii wskazuje na zwiększającą się możliwość ataków militarnych i malware przygotowanych jako nowa forma broni ofensywnej. Wobec możliwości wykorzystania bardzo zaawansowanych technik, większość obecnych, komercyjnych systemów ochrony może być niewystarczająca. Dla systemów infrastruktury krytycznej energetyki koniecznością staje się ścisła ich izolacja od świata zewnętrznego, co z kolei jest niewygodne, gdyż ogranicza możliwość zdalnej obserwacji procesu. Opracowywane i testowane są więc rozwiązania bezpiecznego sposobu przesyłania danych, a w niniejszym artykule zaprezentowane jest rozwiązanie bezpiecznej komunikacji dla pozyskania danych z przemysłowych systemów automatyki DCS.

Słowa kluczowe: *cyberbezpieczeństwo, infrastruktura krytyczna, IT OT, ICS, systemy sterowania*

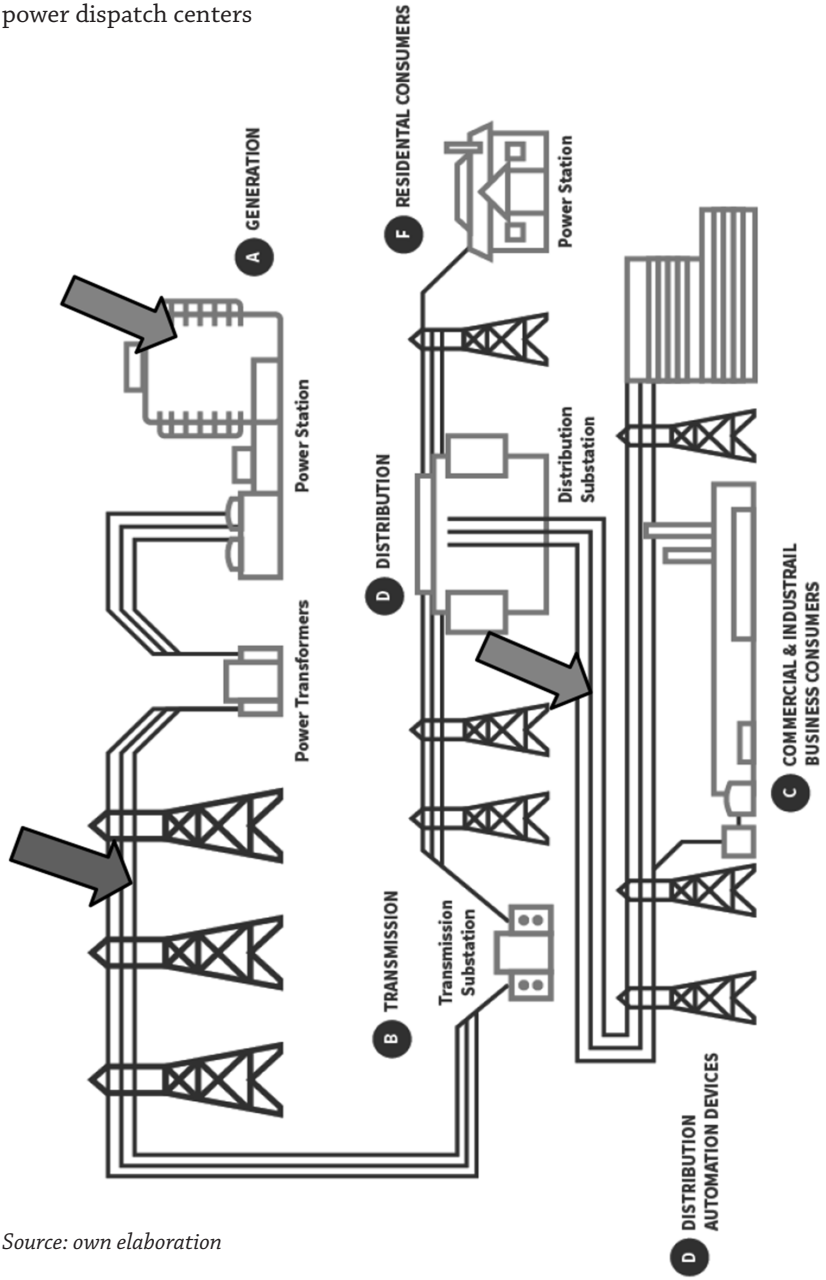
INTRODUCTION

Development of IT technologies and practically complete take-over of industrial process control by advanced automation systems has also been recognized by military doctrine. The ability to take down critical infrastructure of the enemy (which includes the electricity supply system, as the key element of the infrastructure) has been considered the top-priority defensive option as well as a new form of attack. Not surprisingly considerable resources were employed to develop sophisticated "cyber warfare", which was accompanied with increasing activity of criminal groups utilizing IT systems and the Internet for data theft or extortions. With time and with increasing dissemination of digital control systems in power plants, invisible components of the new cyber warfare, such as malware used to attack control system and to bring down the infrastructure, have become even more severe danger than conventional attacks. The year 2010 with Stuxnet attack, that is the attack on the Iranian control systems of uranium enrichment centrifuges, marked the start of a new era – the era of IT wars. Now power systems are facing more severe threats than bombs. Today, malware is perceived as one of the fundamental industrial problems and one of the most severe military threats [Bayar 2016] [Clarke, Knake 2012] and the cost of protection as well as the scale of potential damages caused by malware has been exponentially growing.

THE POWER SECTOR CRITICAL INFRASTRUCTURE AND DIGITAL CONTROL SYSTEMS – SCADA, DCS

The critical infrastructure spans a broad group of systems which are required by a modern state to function. Power sector holds one of the key

Figure 1.
Diagram of the power system with its key threats: of the Transmission System Operator (including National Power Dispatch Center), major power plants, regional power dispatch centers



Source: own elaboration

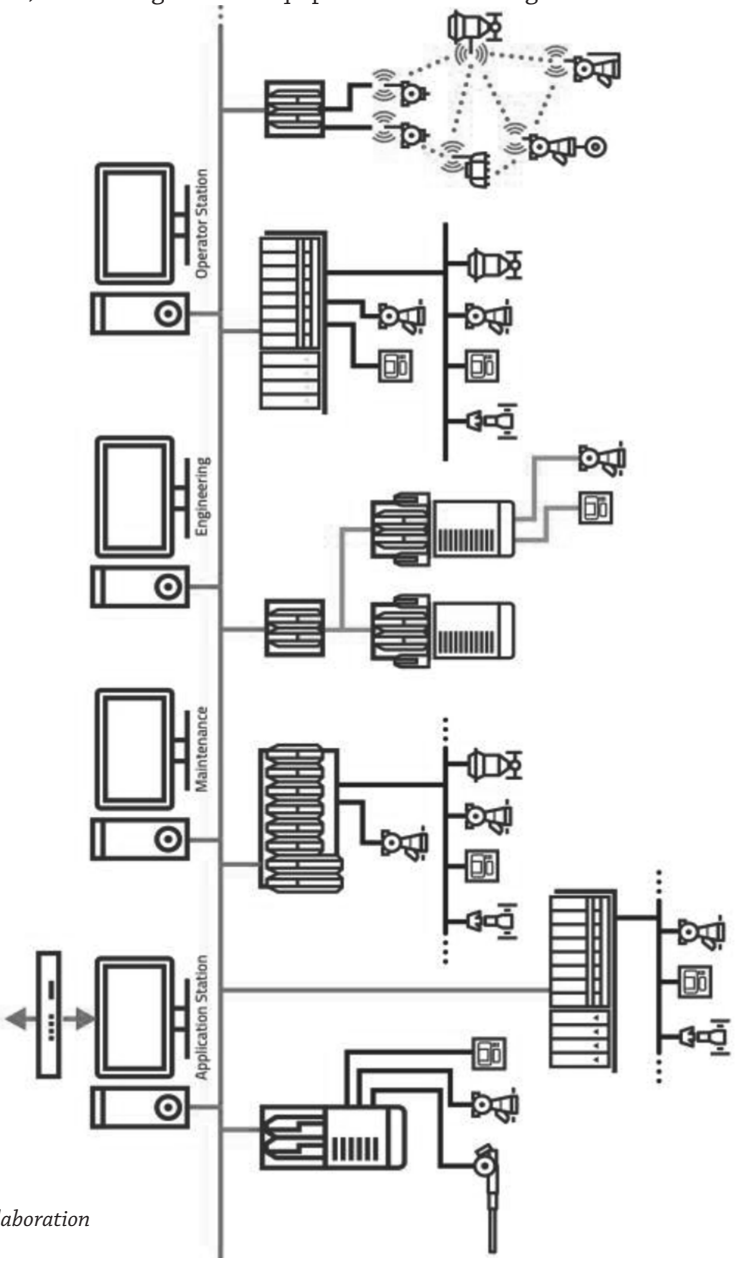
places in this group. From the perspective of system classes, it utilizes digital process control systems, usually referred to in governmental documents as SCADA, or named more accurately in the automation engineering nomenclature Supervisory Data Acquisition and Control (SCADA) systems or Distributed Control Systems (DCS) and is intended to automatically control or supervise various technological processes. According to the act on crisis management, automation systems and IT systems of this kind are responsible for supplying power, energy resources (gas) or water for industrial production (chemical production as well as in other sectors) and transmission pipelines (including oil, gas pipelines as well as industrial pipelines used for transporting hazardous substances). These systems are usually referred to in general as Industrial Control Systems (ICS) or Operational Technology (OT). However, the power sector plays a key role – the power supply system is centralized and practically lacks any energy storage capability. Consequently, potential attacks may result with total, uncontrollable loss of power supply capability over a wide area, i.e. a blackout. Other activities of control systems are limited to local monitoring of processes in specific industrial plants or networks and therefore potential threats affecting them (although with potentially severe financial consequences or life-threatening) have no such global impact. Power supply also affects operation of other critical infrastructure sectors (such as transport, telecommunication, health care, food distribution etc.) and the effect is instantaneous – and as such it may be considered a particularly attractive target in a offensive doctrine and in military plans. The key components in the electric power system, which in turn can cause threats, are the Transmission System Operator Infrastructure (supervision of transmission network, National Power Dispatch Center and power market organization), key centers of Distribution System Operators and of course DCSs of largest power units or central control room systems build in many power plants.

In process management systems of this type, it is important to understand the overall protection issues in terms of "safety" – that is ensuring protection for the proper execution of processes in contrast to less important in this case "security" – that is data security (as, for example, in the financial sector). The role of SCADA and DCS systems is to correctly regulate and to protect technological processes. Thus, the fact that these systems could be used "against own facilities" and that it is possible to intentionally damage the equipment using infected control systems shall

be considered a serious threat in the case of cyber attacks. It is therefore necessary to anticipate other types of attacks and potential threats than in other critical infrastructure sectors (e.g. financial sector) – which has been clearly proven by Stuxnet and other types of malware.

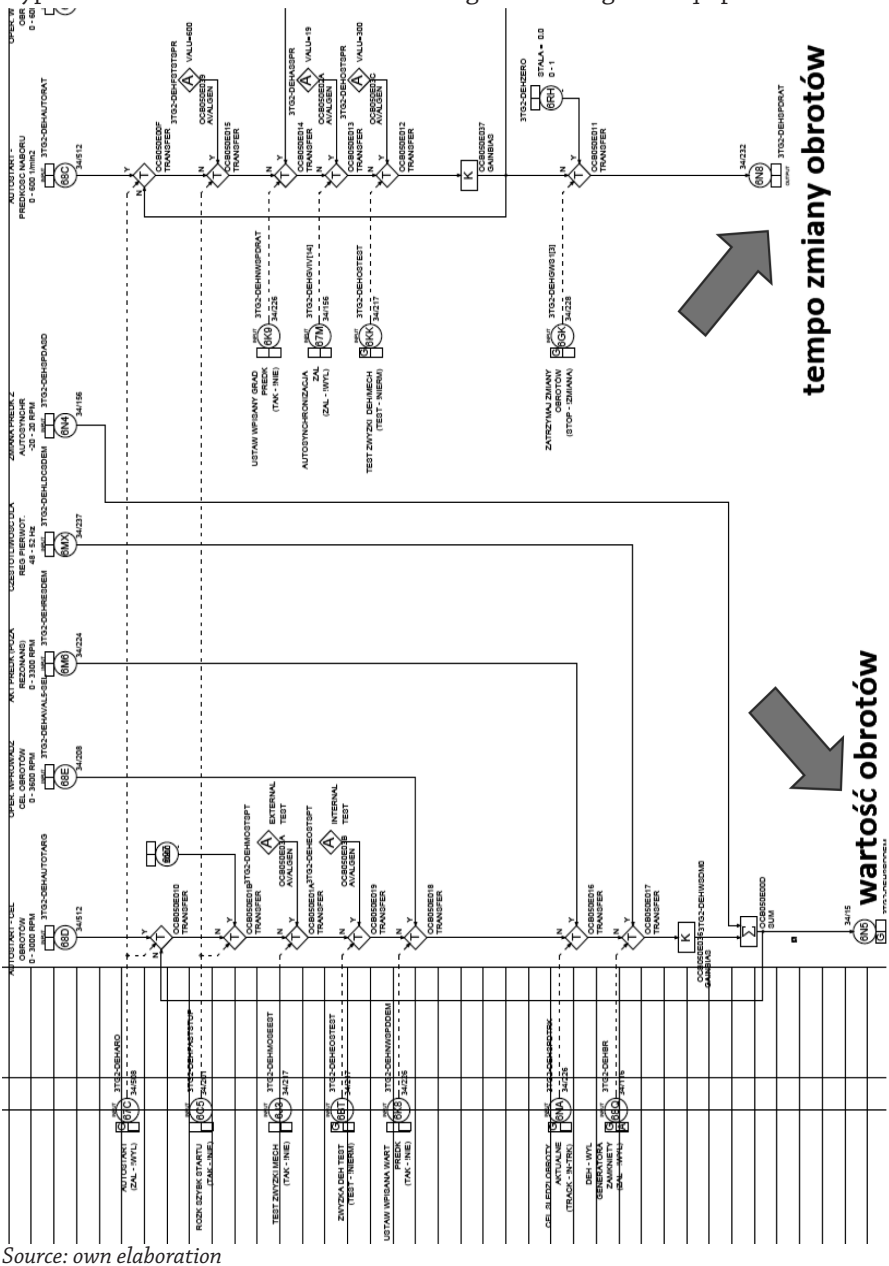
Systems, which are currently being commonly used to control the whole industrial and power infrastructure, appeared at the onset of the computer revolution. In 1970, Yokogawa and Honeywell concurrently developed first so-called Distributed Control Systems (DCS) which become the standard in on-line control systems. During the following years these DCSs were evolving and growing stronger. Today, they practically replaced power plant operators (the whole process from the start of a power unit, through its normal operation, up to its control in emergency situations is now handled automatically). At the same time, Programmable Logic Controllers (so-called PLCs) have been continuously developing and upgraded in terms of functionality. These are freely configurable controllers, that is electronic circuits, which control individual pieces of equipment used mostly in the industry and in discrete processes. In further stages of technological development these systems were connected with SCADA (Supervisory Data Acquisition and Control) systems. This abbreviation has also become a synonym for systems which collect data from distributed and remote locations, e.g. from the power grid. Currently, along with the pressure on costs reduction and on product standardization (e.g. utilization of standard components and operating environments, such as Microsoft Windows), differences between DCS, PLC and SCADA have been becoming less visible and apparent only for automation experts. For an outsider it all looks quite similar – that is as a some sort of an IT system which controls the equipment operation. System operation is also analogous – engineers are designing and developing so-called control algorithms (which describe how processes are to be controlled), they are using engineering computers running specialized, proprietary software, and algorithms are being then translated to computer programs, which are installed in controllers (control computers). The controllers then read process data (measurements from signals), process the data, supervise controlled process and by executing the control algorithm send settings to various actuators (valves dampers, etc.). It is essential for the physical equipment to operate within safe limits and that is ensured by protections and process interlocks – i.e. also computer programs which constantly check whether acceptable values have not been exceeded.

Figure 2.
Functional diagram of a DCS – controllers connected with a network (bus) and master operator workstations and engineering workstations; in some solutions a network (bus) connecting the field equipment is also distinguished



Source: own elaboration

Figure 3.
An example of a steam turbine rotational speed control algorithm (second pic.). Hypothetical malware could alter its settings and damage the equipment



Source: own elaboration

Today, the majority of controllers and engineering computers are in practice machines similar to desktop computers and running standard Windows operating systems (only some of the controllers use real-time operating systems), whereas the network interconnecting these computers to form DCS is almost exclusively classic Ethernet. Thus, access to the hardware is now possible for anyone knowledgeable in IT technology. And this is just one step away from a cyber attack, which may involve modification of actuators' settings (valves opening, altering engine rotation speeds, flap positions etc.) in a completely different way than under control algorithm supervision. We can therefore imagine a situation in which a control system, instead of supervising the power generation or transmission process may be used for a completely different purpose – that is to abort power generation, or even worse, to intentionally damage the generating equipment, bypassing its software interlocks and limit protections which finally may be sufficient sufficient to bring the power system down and cause potential blackout [Hadji-Janev, Bogdanoski, 2015].

CYBER SECURITY OF THE POWER SECTOR CRITICAL INFRASTRUCTURE

Until 2010 cyber security of power systems has not been very frequently considered a real threat but everything changed in 2010, after the Stuxnet incidents (malware which attacked and damaged the Iranian centrifuges used for uranium enrichment). The Stuxnet attack has been very well diagnosed and is described, for example, in [Hadji-Janev, Bogdanoski, 2015]. Stuxnet worked by gradually and covertly infecting digital systems of Siemens PLCs (Simatic S7 PLCs, which were programmed with Step 7 language and which utilized WinCC visualization systems – as that was the equipment used to control the Iranian centrifuges) and by continuously propagating onto successive controllers and engineering computers. Stuxnet exploited unknown vulnerabilities in Microsoft operating system and blocked its detection by typical anti-virus software. Having reached its target (engineering computers used to program Simatic PLCs), it detected relevant control algorithms and modified rotational speed settings of centrifuges in these algorithms – it re-programmed centrifuges spin up so as to damage them. Naturally, it also bypassed software protections preventing rotation speed from exceeding maxima and managed to accomplish that

in a way invisible to process engineers. It activated in a specific moment – i.e. it commanded execution of the modified algorithm, which resulted with mechanical damage to centrifuges which simply broke apart due to excessive rotational speeds.

Hence, Stuxnet was the first "cyber warfare" and marked the beginning of the new era [Farwell, Rogozinski, 2012] [Wilson, 2014], even if some authors are finding traces of first military attacks in attempts to paralyze public IT infrastructure undertaken several years before [Kaiser, 2015].

During following years information appeared about evolution of malware and detection of other threats with catchy names such as Duqu, Gauss or Flame. In 2015, energy supply in the Ukrainian distribution grid was aborted in consequence of attacks conducted using BlackEnergy software (which subsequently downloaded and activated KillDIsk). However, in that case the malware infection was caused by employees opening mislabeled files attached to e-mail messages and the attack was less elaborate than in the case of Stuxnet, as it only involved deletion of data from computer disks (which combined with likely incorrect configuration of the Ukrainian systems caused the described consequences). Today, attacks on computer systems of energy companies are occurring on daily basis [8]; however, all publicized cases were non-military actions or actions which just wanted to be perceived as such. Proliferation of the malware codes and means of attack from the military sector to the civilian sector has significantly facilitated this task for persons and groups trying to penetrate the power sector IT systems, although classic protections and separation of key systems seems to fulfill its protective task quite well. Unfortunately, today the most serious threat remains invisible as it is being developed by large teams developing offensive military systems utilizing new, unknown security vulnerabilities and combining the IT knowledge with the engineering knowledge.

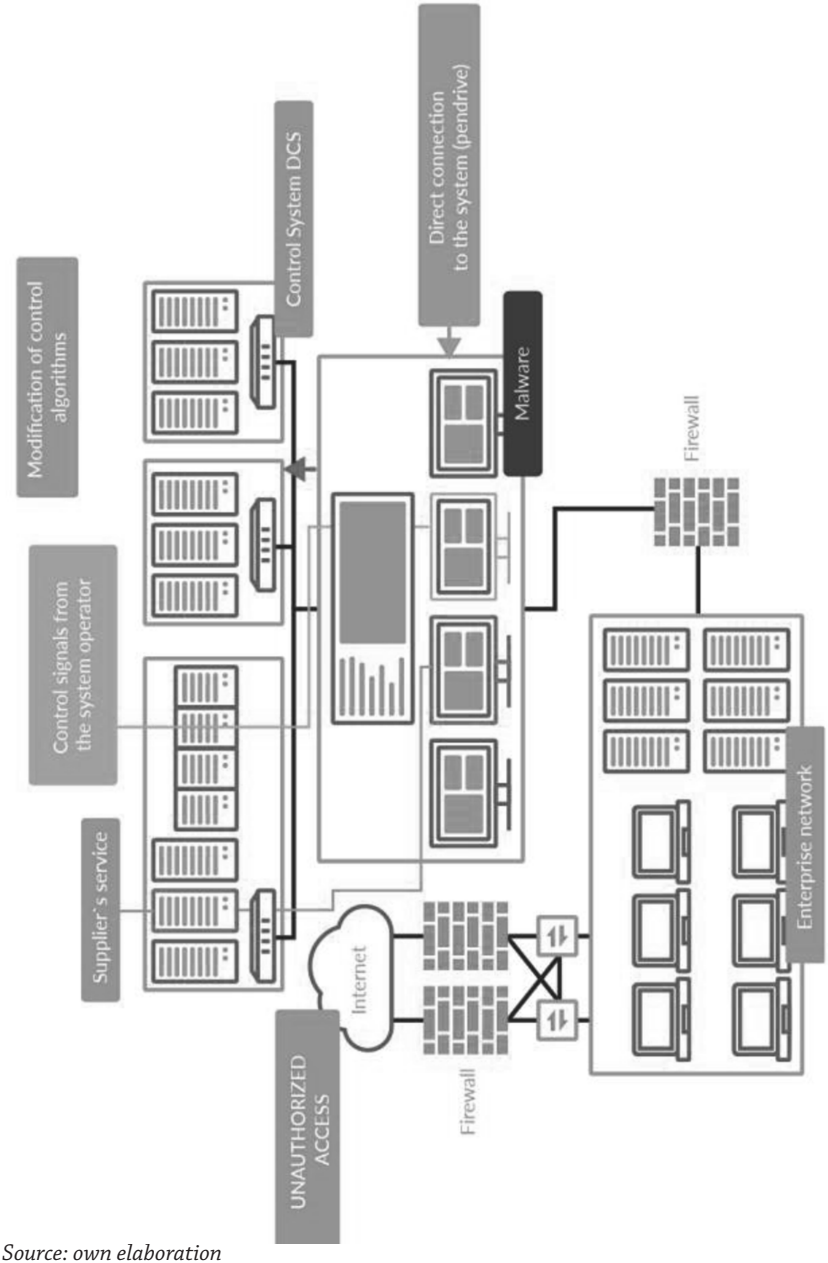
We may expect not only the increased intensity of attacks from varying origins (conducted by amateurs, professional private groups, professional private groups commissioned by businesses and by foreign states or by military IT organizations of other states or a combination of all of the above) either in daily system penetration testing practice or in the case of real conflicts and we should treat this as the first element of the hybrid war [Kaiser, 2015], [Wilson, 2014].

PROTECTION OF CRITICAL INFRASTRUCTURE IN THE ENERGY SECTOR

Since the beginning of industrial control systems implementation, and certainly since the emergence of threats such as Stuxnet, the basic strategy for information protection (ICS – Industrial Control Systems) has been to reduce the possibility of access and separate the control systems from computer networks and Internet access points [The NIS Directive..., 2016], as well as the use of specialized security platforms, in network management systems. In the case of DCS (power plants), the infection of control systems with malicious software can be carried out through direct physical access to the system (e.g. by connecting an engineering workstation to the PLC network or entering malware from a pendrive or other data carrier directly connected to the control system computers) or via contact points with external information systems. The first threat – physical access – has been gradually eliminated by the new system solutions, featuring for instance the inability to connect devices or external storage devices and by increasingly rigorous security policies for physical access to systems (procedures regulating who and how is allowed to use the system). As for the latter case, connection to other systems is eliminated or limited to specific communication methods. As a principle, the control system can operate autonomously (without any connection to the outside world), whilst the few information exchange points with other systems should be carefully controlled [GE Power Digital..., 2016].

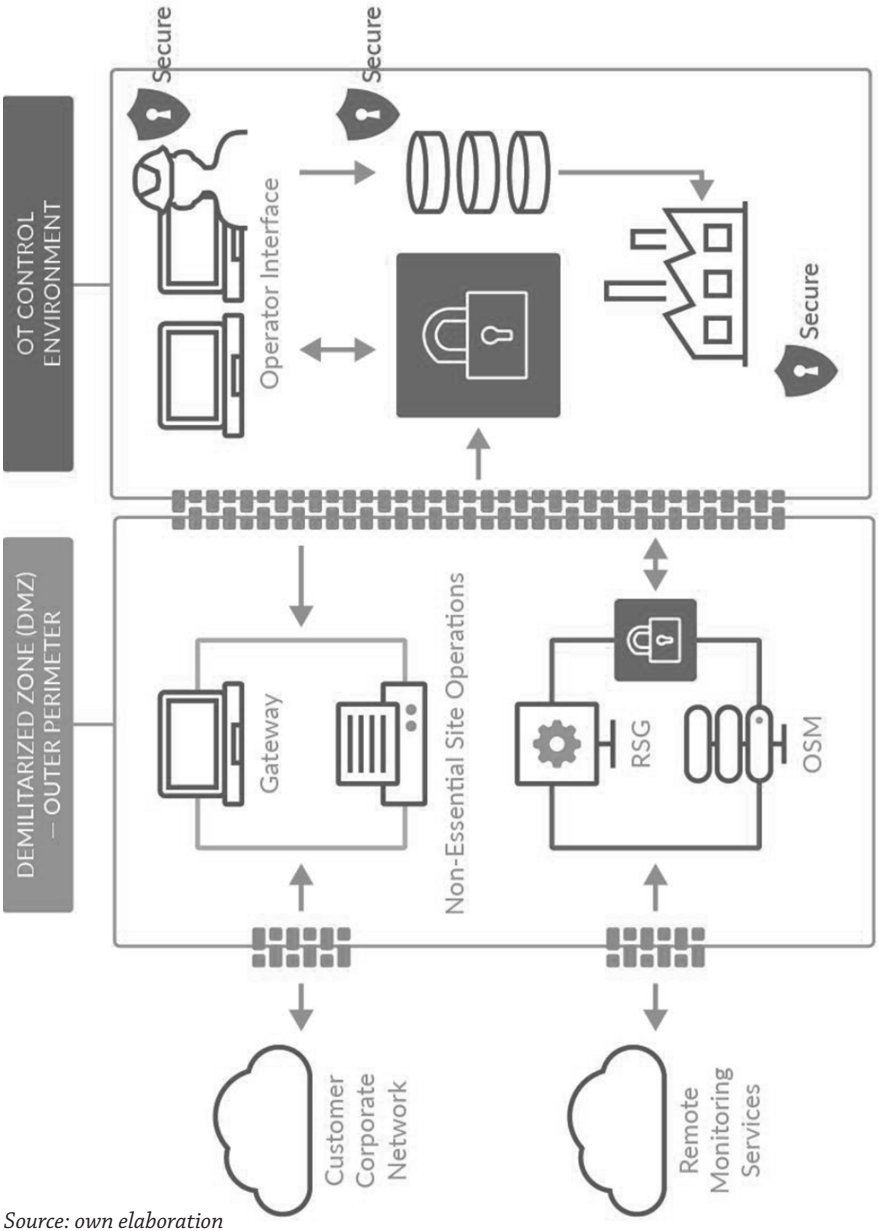
Therefore, in the case of well-supervised IT systems being a part of critical energy infrastructure there should be no possibility of uncontrolled connection between the technical networks (ICS) and other systems. In reality, this is not entirely feasible – DCS or SCADA systems must have a dedicated connection to the national management centers (e.g. in the case of power plants, with a Transmission System Operator for power units operating in ARCM (automatic regulation of frequency and power) systems, from which they receive special control signals controlling the desired operation level), in addition, there are service connections with automation system providers and connections used for process information transfer used by operation control or maintenance departments for diagnostic purposes or for global data analysis. Whilst the former information transfer points are specialized and dedicated networks and use dedicated communication

Figure 4.
DCS and potential attack routes



Source: own elaboration

Figure 5.
A typical mandatory model for separation of automation systems from external environment



Source: own elaboration

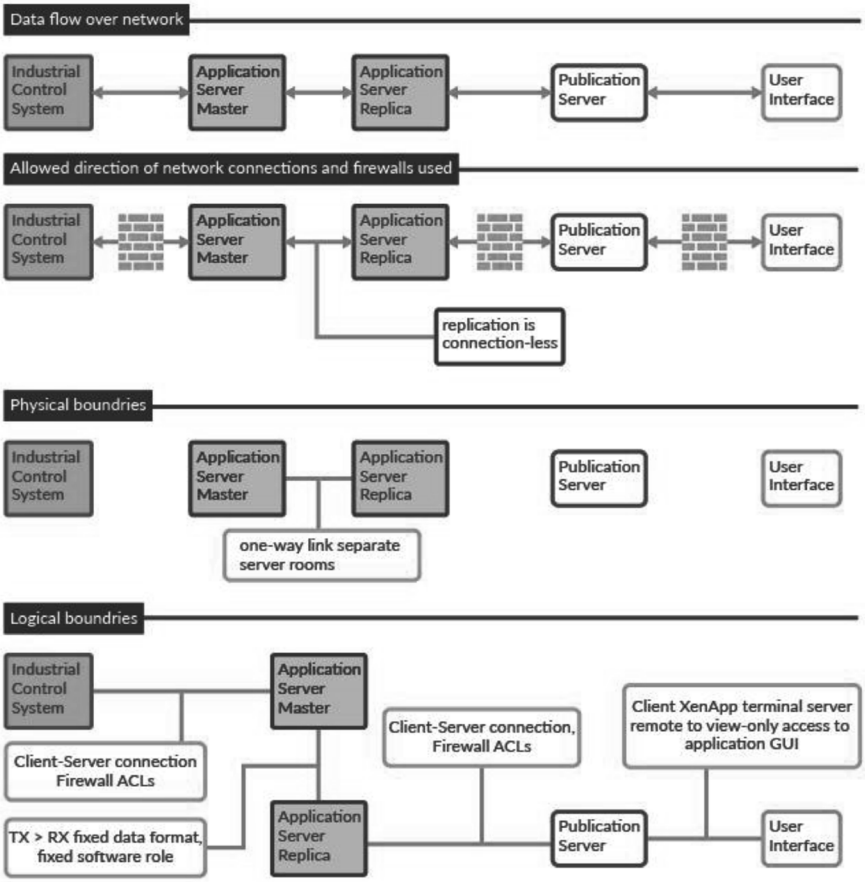
protocols or special authorization methods, the usual policy for information transfer from automation systems to local site (plant and corporate) networks typically does not comply with appropriate safety standards. It is that last integration element that is often the Achilles heel of security. Connections between the automation system and site networks are usually a "gray zone of responsibility" – between the supervision by the Department of Automation and IT Department of the company (therefore uncontrolled) and often utilizing standard, low protection data acquisition protocols (OPC), or even involve undocumented connections by local IT teams. As a result, the critical infrastructure element has many gaps and contains potential routes for security breach, perhaps not posing much danger in the case of common hacking attacks, but being extremely dangerous for potential advanced military threats. As a consequence, the key issue here is to allow process data access whilst isolating automation systems.

Nowadays, it is hard to imagine industrial installations without data access. The number of local area network users processing data at day-to-day work is constantly growing (process engineers, maintenance departments, operation control departments), the possibilities for business intelligence with the use of large data sets are increasing. The use of universal protocols (OPC UA, REST, SOAP) is growing, which, combined with the standardization of architecture of the control systems, increasingly relying on commercial hardware and software leads to the disappearance of previously present barriers (specific protocols and communication media and operating systems). Processing data with the use of mobile devices has also become a standard.

Data acquisition is therefore necessary, but this has to be combined with appropriate cyber-security solutions. It can be achieved with a comprehensive security protection application and industrial data security system, making use of:

- Real-time data replication from the control system with unidirectional connections
- Archive data replication from the control system with unidirectional connections
- Access application isolation with VDI processes (application/user's work environment virtualization)
- No local copies of data or software on user's workstations

Figure 6.
Main components and data flow in proposed solution (EDS Vault)



Source: own elaboration

Figure 6 above presents a detailed solution used by Transition Technologies SA (TT) for projects implemented in Poland and worldwide, mainly for power plants and industrial facilities equipped with Emerson Process Management OVATION control systems and TT proprietary EDS software. In order to ensure the operational security and information safety a multi-layer solution was developed, aimed at eliminating, whenever possible, threats relating to the security of control systems and at minimizing the risk of losing control over sensitive information. The schematic diagram below presents the solution's architecture.

Solution for ensuring the safety of control systems: The control system and the master application server are components of critical significance. The master application server is located in the DMZ of the control system network and dedicated to connect the control network with external systems in a controlled manner. All data from the control system network published within any lower security level network are transferred by the master application server – there is no other connection between the control system network and external networks of lower security levels. Communication between the master application server and lower security level networks is facilitated in an unidirectional connectionless mode. This means that there is no physical possibility to send a data packet from a lower security level network to the DMZ of the control system.

The unidirectional connection is ensured by a hardware solution or hardware connection, as well as the configuration of network layer. Among the supported solutions that ensure unidirectional communication, we can distinguish the so-called Data LEDs, unidirectional network adapters for passive listening or modified UTP network cables. The programming for the unidirectional communication channel includes ACL rules and/or SPAN operation mode of one of the ports, limiting the role of the port to copying packets from another port without the possibility to send. Hardware and configuration elements of unidirectional communication can be combined in order to eliminate certain possibilities for unauthorized change to bidirectional communication (e.g. by bypassing devices or changing the ACL rules). Unidirectional communication is used to replicate live and archive data between the master application server and its replica on the lower security level network side. The method to ensure information security: data is made available to end users with the use of VDI, which means that users use applications which do not run on their workstations, but run remotely, on an application virtualization server. The server used for application virtualization is Citrix XenApp, connected to the domain controller (the element not included in the diagrams), which is used to manage both the access rights for shared applications and the configuration of systems from which the end users access the shared applications. The end user host does not launch any access applications locally. The host for industrial data processing does not establish connection with the replica application server or any other network component of higher security level (i.e. control system network or DMZ subnet).

The industrial data processing/presenting application runs locally on publishing server, and only the user interface of the application is transmitted to the host operated by the user. The data acquired by the application running on the publishing server cannot be sent to the user's system via the channel used to share the application interface. Each application publication session is associated with the user's domain account in order to trace activity and to have the possibility to use access control policies, based on the role, time and place of access. In addition, integration with the domain controller allows the use of multi-factor user authentication mechanisms without affecting the structure of the solution. A domain controller (e.g. Microsoft Active Directory) manages access to the application server. Only devices managed by the domain controller (and devices of appropriate local security level – e.g. restricting the possibility of USB drive use, etc.) are able to access the application publishing interface (e.g. Citrix XenApp).

Despite the use of multiple hardware and software layers the solution maintains a low data transfer latency. Current values (measurements, alarms) are available in the EDS Terminal client application with a delay of approximately 1 second, compared to the data available on operator terminals of the control system. Therefore, this solution may be consider as a one of examples of modern data acquisition software architecture and is accepted and successfully tested according to the advanced international cybersecurity standards.

NORMS AND STANDARDS FOR CYBERSECURITY IN THE ENERGY SECTOR AND THE FUTURE

With the advent of computer threats, we witness the emergence of appropriate standards, procedures or recommendations. International experience shows that all countries are struggling to find the solution for structural problems connected to the development of optimal operational procedures. When analyzing the different approaches, it is worth to look at the following standards: NERC CIP V5 and NEI CIP (USA), CPNI SCADA (UK), CIGRE, JWG D2/B3/C2-01 (France) or VGB R175 (Germany). Apart from the diversity of both the systematics and the detailed norms (for energy) in each country, we also observe the efforts for unification by applying standards pertaining to particular devices (the European

industrial standards level) but here, however, it has been exclusively limited to selected issues of cybersecurity. Accordingly, European industrial standards for selected technology sectors such as IEC 62351 are being introduced in parallel with attempts to develop an industry-wide standard for automation (ISA99 Industrial Automation and Control Security) and the corresponding European IEC 62443 standard ("security for industrial measurement and control").

When analyzing the approach of particular countries to the problem of energy sector cybersecurity, the American procedures seem to be particularly interesting. The analysis of initial experiences on the market indicated the failure of the "voluntary" approach – a system of voluntary compliance with standards. Accordingly, given the expected scale of threats, it has been decided to move to a system of compulsory standard compliance. Supervision of energy (within the scope of cyber-security) under "The Energy Independence and Security Act of 2007 (EISA)" was submitted to the FERC (Federal Energy Regulatory Commission), and the organization in turn commissioned the development of a comprehensive system of procedures and standards of conduct to the North American Electric Reliability Corporation (NERC) NERC's Critical Infrastructure Protection Committee (CIPC). At the moment, the energy sector – utility power generation and transmission branches, with the exception of nuclear power sector, regulated by a separate set of standards – is subject to compulsory adherence to the so-called NERC CIP Ver.5 [North Amercan Electric ..., 2016] enforced by a system of financial penalties. Therefore, the energy sector is obliged to adhere to the cyber security requirements from their own resources, and under pain of financial penalties. It should be noted, however, that the procedures are relatively well developed and precise, and the compliance requirements rightfully relate in the first place to major facilities or installations having the greatest impact on the energy infrastructure and security (in the American nomenclature referred to as BES – Bulk Energy Systems, regulated by the appropriate NERC CIP 002). Today, the entire NERC CIP compilation comprehensively regulates the issue, relating to the definitions, the requirements of the industry and the nature of present risks and protection, both in terms of physical access and IT risks, to staff training and reporting incidents, and undergoes constant updating. The latest version of the standards is NERC

CIP 5, with its further modifications under way. The relevant procedures are CIP-002-5.1 BES Cyber SystemCategorization, CIP-003-6 Security Management Controls, CIP-004-6 Personnel & Training, CIP-005-5 Electronic Security Perimeter, CIP-006-6 Physical Security of BES Cyber Systems, CIP-007-6 Security Management System, CIP-008-5 Incident Reporting and Response Planning, CIP-009-6 Recovery Plans for BES Cyber Systems, CIP-010-2 Configuration Change Management and Vulnerability Assessments, CIP-011-2 Information Protection, CIP-014-2 Physical Security where, as evident, the CIP 7-11 procedures represent the typical problems addressed by IT operations (as with ISO 27000 standards), but the whole issue of security is treated more holistically.

The American solutions constitute a relatively coherent system, which involves the collaboration of the disciplinary CERT, the regulator and the organization responsible for issuing procedures. It seems that this is one of the best models to follow and possibly apply in Polish conditions.

Nevertheless, it should be noted that even the United States are far from complete consistency, because, for instance, cyber security at nuclear power plants is regulated by the relevant provisions of NEI (organizations associated with nuclear power) and for the recently relevant cyber-security issue of ”smart grid” FERC issued the NIST document (“Guidelines for Smart Grid Cybersecurity”). These procedures and standards also apply exclusively to electric power industry, as the gas industry for instance is subject to conditions as set out by the American Gas Association (AGA): Series of AGA12 reports, with the chemical industry being regulated by a yet different set of regulations. To sum up – even in the US it is being discussed whether the current system of organization and operation of the relevant services is appropriate and adequate for the risks and whether the critical infrastructure is secure against cyberattacks.

The newly adapted (July 2016) NIS Directive of the European Parliament and of the EU Council 2016/1148 dated July 6, 2016 – on measures to promote high common level of security of networks and information systems in the European Union should become an impulse (in Europe and Poland) for further development of a comprehensive information protection system for the energy sector. However, this is a “high level” directive – referring to the holistic view on the problem of cybersecurity and all sectors. From the perspective of energy sector it describes elements

that define the so-called "critical service provider" and includes enterprises *defined as in Art. 2, Item 35 of the Directive of the European Parliament and Council 2009/72/EC (1), which execute the function of "delivery" as defined in Art. 2, Item 19 of the directive*

- distribution system operators as defined in Art. 2, Item 6 of Directive 2009/72/EC
- transmission system operators as defined in Art. 2, Item 4 of Directive 2009/72/EC.

To sum up, the European experience today is based on a system of recommendations, the detail level of which varies depending on particular country. Procedures are created for particular devices, SCADA systems as well as particular sectors. The signaled desire for unification based on a single European procedure is probably the reason for lack of detail in the procedures as well as their substantially general scope – which contributes to difficulties in their practical application. Recommendations are still not mandatory and not regulated by any coherent system.

Comparing the international approach, it seems that European countries are at a stage that the US and Israel have long left behind – of noticing the great problem and the numerous threats connected to cybersecurity, but also the expectation that the issue will be resolved by manufacturers and users by voluntary complying to the standards. Therefore the recommendations in place are general and usually issued too late in order to respond to the market situation. It seems probable that one day the European countries will adapt the compulsory system, robustly formalized for each subarea of critical infrastructure. The key Polish IT systems for energy and gas supply are not protected against contemporary threats. In practice, only the "classical" and commercial security measures of relatively low proceduralization level are implemented – there are no standards of conduct, and if so, they are applied exclusively by particular businesses or constitute general practices, such as set out in ISO/IEC 27000 standards. In most cases, the industrial corporations' security policies focus on the safety of "information" and not the "process" and here also only standard practices are followed.

Looking pessimistically, considering the technology of power plant control and energy distribution, the systems nowadays in Poland are full of

gaps – related for instance to multiple connections to master systems (for data transfer). The landscape for other systems such as water or gas supply systems presents itself even worse. The entire set of practices for system changes does not live up to contemporary standards. The current approach (although changing) entails protection against common network threats and the use of modern but only commercial solutions for protection, omitting the importance of military threats (in the case of actual military conflict). As a result, the IT systems for critical installations are vulnerable in case of a modern conflict with the use of modern cyber warfare. Meanwhile, this issue is considered to be absolutely crucial in the security doctrines of the US, where well-developed standards are already in place. While this has not been a problem yet, as we have no reported incidents of control systems activation or successful cyber-attacks in Poland, it does not mean that the problem does not exist. Conversely, it seems that this is the final call before the rising tide of both criminal and military threats. Obviously, there have been first signs indicating that the cybersecurity problem exists and relevant systems must be secured. Energy industry organization have created appropriate bodies for their Information security management. In some cases their work is in accordance with the actual needs, however some of them limit exclusively to security audits. Some IT compliance departments of energy corporations are urgently seeking a specialized set of industry standards, which would allow to improve the security better than the general ISO procedures for IT.

The issue is evident in selected tender specifications by references made to foreign standards and documentation. Finally, we see the emergence of integrated security plans and models that aim at ensuring the continuity of the process by the use of backup and recovery. Recent months have shown a growing awareness of the major energy companies that sign agreements with the leading suppliers of audit and protection services, or even appoint their own CERT units. Unfortunately, the IT management is affected by constant personnel changes, and, as a consequence, changes or discontinuity regarding IT policies for particular businesses. In the absence of a global security strategy for critical infrastructure or any detailed industry standards for critical infrastructure of the energy sector, the strategy undertaken is a sum of actions by individual enterprises, without any comprehensive plan.

CONCLUSION

It seems that the adoption of the NIS [13] and the new revisions of cybersecurity strategies for the Republic of Poland [15], the revised version of the National Critical Infrastructure Protection Program [Rządowe Centrum ..., 2016] are subsequent steps that must lead to a further fundamental change in policy towards the protection of critical infrastructure in the energy sector. The appointment of National CERT must also result in the construction of a specialized "disciplinary" CERT – dedicated specifically to information systems for controlling the supply of gas, water, etc., as well as the adoption of some form of copy of the prescriptive American system, with robust standards for energy sector. Yet another step will be the necessary investments in which the energy sector companies will have to embrace the new standards under the pain of financial penalties We need to accept that predictable next (even hypothetical) military conflict will be a cyber clash with the use of software and advanced security systems.

Literature

Bayar T. (2016). *Cybersecurity in the power sector.* Power Engineering International.

Clarke R., Knake K. (2012). *Cyber War; The Next Threat to National Security and What to Do About It*. NY Ecco HarperCollins Publishers.

Falliere N., Murchu L.; W32.Sruxnet.Dossier, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf [data dostępu: 16.09.2016].

Farwell J., Rogozinski R. (2012). *Stuxnet and the Future of Cyber War*. Survival 54.

GE Power Digital Solutions, 5 Security Imperatives for Power Executives, https://www.ge.com/digital/products/cyber- [data dostępu: 16.09.2016].

Hadji-Janev M., Bogdanoski M. (2015). *Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare.* JVG Books LLC.

Kaiser R. (2015). *The birth of cyberwar.* Political Geography.

Kyung-bok L., Jong-in L. (2016). *The Reality and Response of Cyber Threats to Critical Infrastructure: A Case Study of the Cyber-terror Attack on the Korea Hydro & Nuclear Power Co., Ltd*. KSII Transactions on Internet and Information Systems Vol. 10.

North Amercan Electric Realiability Corporation CIP Standards, http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx [data dostępu: 16.09.2016].

Rządowe Centrum Bezpieczeństwa Narodowy Program Infrastruktury Krytycznej, http://rcb.gov.pl/wp-content/uploads/NPOIK-dokument-g%C5%82%C3%B3wny.pdf [data dostępu: 16.09.2016].

Takebe T. (2014). *Trends in Industry Standards and International Standards for Industrial Automation Control System Security*. Yokogawa Technical Report English Edition Vol. 57 No. 2.

The NIS Directive of the European Parliament, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013PC0048 [data dostępu: 16.09.2016].

Wilson C. (2014). *Cyber Threats to Critical Information Infrastructure, chapter un Cyberterrorism: Understanding, Assessment, and Response, Chapter: Cyber Threats to Critical Information Infrastructure*. Springer-Swansea University.

Zespół międzyresortowy Ministerstwa Cyfryzacji, Założenia Strategii Cyberbezpieczeństwa dla Rzeczpospolitej Polskiej, https://mc.gov.pl/files/zalozenia_strategii_cyberbezpieczenstwa_v_final_z_dnia_22-02-2016.pdf [data dostępu: 16.09.2016].

JAROSŁAW MOSZCZYŃSKI

Katedra Kryminalistyki i Medycyny Sądowej
Wydział Prawa i Administracji
Uniwersytet Warmińsko-Mazurski w Olsztynie
jaroslaw_moszczynski@go2.pl

POLSKIE DAKTYLOSKOPIJNE I GENETYCZNE BAZY DANYCH – PROBLEM PODSTAW PRAWNYCH

POLISH DACTYLOSCOPIC AND GENETIC DATABASES – THE PROBLEM OF THE LEGAL BASIS

ABSTRACT

Forensic databases, especially computerized fingerprint and genetic databases, are very valuable tools in the fight against crime, as long as they are big enough and up to date.

They allow to compare in a short time, dactyloscopic and biological traces developed at the scenes of crimes, against large collections of fingerprints and genetic profiles, which enables the detection of offenders. They are also used to determine the identity of the persons and bodies. For this reason, they are widely used not only in the individual countries, but also in international cooperation. The basic condition for a positive outcome of search of the database is the presence of a suitable reference material in it – fingerprints or DNA profiles of the potential offenders. This means that the identification of the perpetrator can be made only in the cases of recidivism. There is currently a problem in Poland with the relevant legal bases for forensic registration, which leads to obsolescence of databases.

Keywords: *fingerprints, DNA profiles, databases, forensic registration, legal basis*

STRESZCZENIE

Kryminalistyczne bazy danych, a zwłaszcza skomputeryzowane bazy daktyloskopijne i genetyczne to bardzo wartościowe narzędzia w walce z przestępczością, o ile są one odpowiednio duże i aktualne. Pozwalają one na porównywanie w krótkim czasie śladów daktyloskopijnych i biologicznych, zabezpieczonych na miejscach zdarzeń, z dużymi zbiorami odbitek linii papilarnych oraz profili genetycznych, co umożliwia wykrywanie sprawców przestępstw. Służą one także do ustalania

tożsamości osób i zwłok. Z tego względu są one szeroko wykorzystywane nie tylko na potrzeby poszczególnych państw, ale także we współpracy międzynarodowej. Podstawowym warunkiem uzyskania pozytywnego rezultatu przeszukania bazy jest obecność w niej odpowiedniego materiału porównawczego – odbitek linii papilarnych bądź profili DNA potencjalnych sprawców. Oznacza to, że identyfikacji sprawcy można dokonać tylko w przypadkach powrotu do przestępstwa. W Polsce istnieje aktualnie problem z odpowiednimi podstawami prawnymi rejestracji kryminalistycznej, co przekłada się na dezaktualizację baz danych.

Słowa kluczowe: *odciski palców, profile DNA, bazy danych, rejestracja kryminalistyczna, podstawy prawne*

WPROWADZENIE

Polska Policja dysponuje nowoczesnymi kryminalistycznymi bazami danych w postaci systemu automatycznej identyfikacji daktyloskopijnej – AFIS (J. Moszczyński, 1997, s. 198–214) oraz skomputeryzowanej bazy danych DNA (M. Goc, H. Dąbrowska, 2002, s. 5–7; A. Filewicz, I. Sołtyszewski, 2003, s. 5–12). Obydwie bazy mogą być bardzo skutecznymi narzędziami w walce z przestępczością (K. Krassowski, 2007, [w:] I. Sołtyszewski, s. 111–128), jeśli zawierają odpowiednio duże i aktualne zasoby informacji w postaci odbitek linii papilarnych oraz profili DNA sprawców przestępstw.

W 2006 roku miała miejsce nowelizacja art. 20 ustawy o Policji, w ramach której przyjęto, iż danych dotyczących DNA, odcisków linii papilarnych i innych informacji nie pobiera się w przypadku, gdy nie mają one przydatności wykrywczej, dowodowej lub identyfikacyjnej w prowadzonym postępowaniu. Interpretacja tego przepisu jest następująca: jeśli na miejscu zdarzenia nie ujawniono śladów daktyloskopijnych bądź biologicznych, to podejrzanych nie daktyloskopuje się ani nie pobiera się od nich wymazów śliny w celu oznaczenia profilu DNA. Rozwiązanie takie będzie prowadziło, zdaniem autora, do dezaktualizacji oraz spowolnienia budowy obydwu kryminalistycznych baz danych. Naturalną konsekwencją takiego stanu rzeczy będą coraz mniejsze możliwości wykrywania sprawców przestępstw w oparciu o ślady ujawniane na miejscach zdarzeń.

W opracowaniu został przedstawiony m.in. przegląd podstaw prawnych rejestracji kryminalistycznej w ujęciu historycznym oraz ich wpływ na funkcjonowanie zbiorów daktyloskopijnych i genetycznych, co zostało zobrazowane za pomocą odpowiednich analiz statystycznych.

RYS HISTORYCZNY POLSKICH ZBIORÓW DAKTYLOSKOPIJNYCH

Po odzyskaniu niepodległości przez Polskę, komendant główny Policji Państwowej podpisał w dniu 24 grudnia 1919 roku pierwszą polską instrukcję daktyloskopijną, na mocy której jednostki Policji były zobowiązane do przesyłania jednego egzemplarza karty daktyloskopijnej do Wydziału IV KG PP w Warszawie. Zgodnie z tą instrukcją daktyloskopowaniu podlegały następujące osoby (zob.: W. Brzęk, 1980, s. 510–523; J. Misztal, 2008, s. 63–71; D. Buras, 2004, s. 56–61; D. Buras, 2009, [w:] P. Rybicki, T. Tomaszewski, s. 71–82):

- aresztowani oraz podejrzani, którzy należeli do kategorii zawodowych zbrodniarzy podlegających dozorowi policyjnemu,
- aresztowani, którzy ze względu na swoje wcześniejsze życie, rodzaj oraz sposób popełnienia czynów karygodnych są szkodliwi dla państwa, mienia i życia obywateli, a którym za popełnienie czynu karygodnego grozi kara ciężkiego więzienia,
- międzynarodowi zbrodniarze i włóczędzy wszelkiego rodzaju,
- wydaleni z kraju wyrokami sądowymi lub orzeczeniami administracyjnymi,
- podający fałszywe nazwisko oraz legitymujący się fałszywymi dowodami osobistymi, jak też osoby, co do których zachodzi uzasadnione podejrzenie, że starają się wprowadzić w błąd urzędy państwowe,
- Cyganie obojga płci, bez względu na wiek i przynależność państwową,
- osoby aresztowane lub podejrzane o szpiegostwo oraz inne działanie mające na celu wyrządzenie szkody państwu,
- osoby nieznane w okolicy, przetrzymywane z jakichkolwiek powodów, głuchoniemi, umysłowo chorzy itp., celem stwierdzenia ich tożsamości,
- osoby, których zdjęcia daktyloskopijnego zażądał sąd lub inne władze do tego powołane,
- zwłoki zamordowanych, a nieznanych w okolicy, jak też osób, które przypadkowo poniosły śmierć.

Na podstawie rozkazu nr 165 komendanta głównego Policji Państwowej z 20 marca 1922 roku w ekspozyturach śledczych działających w większych miastach zorganizowano biura rejestracyjne, w skład których wchodziły m.in. registratury daktyloskopijne. W 1927 roku prowadzenie registratur

powierzono urzędom śledczym, które w tym roku utworzono przy komendach wojewódzkich Policji Państwowej. W 1928 roku opublikowano instrukcję dla urzędów śledczych, nakładającą obowiązek daktyloskopowania następujących kategorii osób:

- znani Policji przestępcy zawodowi recydywiści, bez względu na rodzaj i kwalifikacje popełnianych przez nich przestępstw,
- osoby aresztowane, względnie zatrzymane pod zarzutem popełnienia przestępstw zagrożonych karą śmierci lub ciężkim więzieniem,
- osoby aresztowane za dopuszczenie się takich przestępstw, które z reguły popełniane są zawodowo, np.: kradzież kieszonkowa, kradzież sklepowa, kradzież jarmarczna, kradzież z włamaniem, kradzież z podkopem, fałszerstwo banknotów, monet i papierów wartościowych, oszustwa z użyciem fałszywych brylantów, bezwartościowych przedmiotów i materiałów, uprawianie gry hazardowej w pociągach i inne,
- osoby przytrzymane pod zarzutem jakichkolwiek wykroczeń przeciwko prawu i porządkowi, jeśli bezsprzeczne stwierdzenie ich tożsamości nastręcza trudności danemu urzędowi policyjnemu,
- osoby zwolnione po odbyciu kary co najmniej więzienia za przestępstwa kryminalne, jeżeli przedtem nie były daktyloskopowane,
- osoby aresztowane za przestępstwa skierowane przeciwko państwu,
- osoby wydalone z kraju na mocy wyroków sądowych, względnie orzeczeń władz administracyjnych, jak również osoby deportowane do kraju przez zagraniczne władze ze względu na ich szkodliwość dla bezpiecznego życia i mienia,
- Cyganie obojga płci, od 14 roku życia począwszy, bez względu na przynależność państwową,
- nieznani, a przytrzymani z jakichkolwiek powodów prawnych osobnicy niewiadomego pochodzenia, np. głuchoniemi, umysłowo chorzy itp., celem ustalenia ich tożsamości,
- osoby, których daktyloskopowanie zostało zarządzone przez władze sądowe, administracyjne lub wojskowe,
- zwłoki nieznanych osobników zamordowanych oraz osób niewiadomego pochodzenia, które poniosły śmierć przypadkowo, np. skutkiem katastrof, przejechania, utonięcia, zostały zabite w czasie pościgu policyjnego lub które popełniły samobójstwo.

W latach 1944–1949 utworzono Sekcję Naukowo-Techniczną Ekspertyz w Komendzie Głównej Milicji Obywatelskiej oraz laboratoria foto-daktyloskopijne w komendach wojewódzkich. Podjęto prace nad tworzeniem powiatowych kartotek znanych przestępców, wojewódzkich registratur daktyloskopijnych (dziesięciopalcowych), albumów fotograficznych przestępców oraz registratur monodaktyloskopijnych. Niestety, w 1949 roku zlikwidowano Sekcję Naukowo-Techniczną Ekspertyz KG MO. W 1954 roku przystąpiono do organizacji Zakładu Kryminalistyki KG MO i wojewódzkich laboratoriów kryminalistycznych. Na mocy rozkazu nr 8/54 KG MO z 22 października 1954 roku wprowadzona została instrukcja o zasadach stosowania i wykorzystania rejestracji daktyloskopijnej przez jednostki MO. Zgodnie z nią prowadzenie Centralnej Registratury Daktyloskopijnej (CRD) powierzono Zakładowi Kryminalistyki KGMO. Centralna Registratura Daktyloskopijna składała się z trzech działów: registratury dziesięciopalcowej, registratury monodaktyloskopijnej oraz centralnego zbioru śladów linii papilarnych nieustalonych przestępców.

W późniejszym okresie zasady rejestracji daktyloskopijnej regulowała instrukcja nr 1/77 Dyrektora Zakładu Kryminalistyki KG MO z 10 stycznia 1977 roku o zasadach i sposobie postępowania w sprawach rejestracji daktyloskopijnej, łusek, pocisków, broni utraconej oraz dokumentów anonimowych, wydana na podstawie zarządzenia nr 101/72 Ministra Spraw Wewnętrznych z 25 września 1972 roku. Zgodnie z powyższą instrukcją rejestracji daktyloskopijnej podlegały następujące osoby:

- podejrzani, którym przedstawiono zarzuty, oraz osoby, które przesłuchano w charakterze podejrzanego,
- osoby zatrzymane, które odmawiały podania swoich danych personalnych, oraz osoby, co do których zachodziło podejrzenie, że posługują się fałszywymi danymi personalnymi,
- nieletni, podejrzani o popełnienie zbrodni przeciwko życiu, zbrodni zgwałcenia, rozboju lub zbrodni przeciw bezpieczeństwu powszechnemu albo umyślne spowodowanie ciężkiego uszkodzenia ciała lub ciężkiego rozstroju zdrowia, a także o dokonanie poważniejszych kradzieży, szantażu lub takich przestępstw, których sposób popełnienia wskazuje na daleko posunięty proces deprawacji lub nabycie kwalifikacji przestępczych.

Kolejne zmiany w zakresie podstaw prawnych rejestracji daktyloskopijnej zaprezentowane są w dalszej części opracowania.

MOŻLIWOŚCI USTALEŃ W OPARCIU O KLASYCZNE ZBIORY DAKTYLOSKOPIJNE

Zbiory kart daktyloskopijnych zorganizowane wg dziesięciopalcowej formuły daktyloskopijnej (P. Horoszowski, 1958, s. 381–400) umożliwiały ustalanie tożsamości (lub jej weryfikację) osób podejrzanych o popełnianie przestępstw, a także zwłok. Oczywiście warunkiem koniecznym do dokonania takich ustaleń była wcześniejsza rejestracja daktyloskopijna danej osoby.

Wywiady daktyloskopijne były prowadzone poprzez dostarczenie karty daktyloskopijnej do CRD lub przez telefon (D. Raczyński, Z. Skopiński, 1961). W tym drugim przypadku eksperci daktyloskopii lub technicy łączyli się telefonicznie z CRD i przekazywali informacje o podstawowych elementach budowy wzorów linii papilarnych na karcie daktyloskopijnej. Pracownicy CRD szkicowali na czystej karcie zarysy wzorów i na tej podstawie wyprowadzali formuły daktyloskopijne, co wymagało nie tylko perfekcyjnej znajomości zasad klasyfikacji kart daktyloskopijnych i wielkiego doświadczenia, ale także dużej wyobraźni. Następnie wyszukiwali w zbiorach kart o analogicznych formułach i przekazywali zainteresowanej jednostce dane osobowe ze znalezionych kart. Pomimo dużej precyzji takich ustaleń, każdy wywiad daktyloskopijny przez telefon wymagał potwierdzenia poprzez przesłanie karty daktyloskopijnej do CRD. O dużej potrzebie korzystania z usług CRD świadczą np. dane z 1990 roku, kiedy to przeprowadzono 2067 wywiadów daktyloskopijnych, w ramach których ustalono tożsamość 906 osób i 208 zwłok.

Pod koniec 1991 roku zainstalowano w polskiej Policji sieć telefaksów, które bardzo szybko znalazły zastosowanie w wywiadach daktyloskopijnych (J. Moszczyński, 1993, s. 15–21), co znacznie usprawniło dokonywanie szybkich ustaleń tożsamości osób i zwłok. Na przykład w 1995 roku liczba wywiadów daktyloskopijnych wzrosła do 6277, w ramach których ustalono lub zweryfikowano tożsamość 1784 osób i 275 zwłok.

Zbiory CRD, podobnie jak wszystkie klasyczne registratury daktyloskopijne, były – niestety – niemal zupełnie nieprzydatne do wykrywania sprawców przestępstw na podstawie śladów z miejsc zdarzeń, ponieważ ślady pojedynczych czy nawet kilku palców nie pozwalały na wyprowadzanie dziesięciopalcowej formuły daktyloskopijnej. Tylko w wyjątkowych przypadkach, kiedy to sprawca pozostawił na miejscu zdarzenia ślady większości palców, można było wyprowadzić szereg formuł prawdopodobnych

(J. Moszczyński, 1988), co wymagało przeszukiwania znacznie większych podzbiorów CRD niż w przypadku formuł jednoznacznych. Dlatego od 1926 roku w Wydziale IV Komendy Głównej Policji Państwowej rozpoczęto prowadzenie dodatkowo registratury monodaktyloskopijnej (P. Horoszowski, 1958, s. 400–410), w ramach której wzory linii papilarnych na poszczególnych palcach klasyfikowano oddzielnie. Dzięki niej pierwsze pozytywne rezultaty uzyskano w latach 30., i tak w 1931 roku wykryto 59 sprawców, natomiast w 1938 roku liczba wykrytych w ten sposób przestępców wzrosła do 176 (A. Misiuk, A. Pepłoński, 1994, s. 218). Prowadzenie registratury monodaktyloskopijnej było jednak bardzo pracochłonne, a poszczególne formuły szybko się przepełniały, tzn. wiele wzorów linii papilarnych miało taką samą formułę. Dlatego zbiory monodaktyloskopijne, prowadzone do lat 70., nie mogły być zbyt liczne i obejmowały jedynie odbitki linii papilarnych najbardziej aktywnych przestępców.

Na przełomie lat 80. i 90. eksperci z laboratoriów wojewódzkich mieli obowiązek prowadzenia zbiorów śladów N.N. Gromadzono w nich fotogramy śladów z miejsc zdarzeń, które spełniały odpowiednie wymagania jakościowe i pozostawały niezidentyfikowane po badaniach eliminacyjnych. Ślady te należało porównywać z kartami daktyloskopijnymi, nadsyłanymi w ramach kolejnych ekspertyz[1]. Wielka pracochłonność tego przedsięwzięcia także nie dawała oczekiwanych rezultatów.

Pewien postęp w wykorzystaniu zbiorów monodaktyloskopijnych przyniosły systemy półautomatyczne, których działanie polegało na „ręcznym" kodowaniu śladów i odbitek z kart daktyloskopijnych, wprowadzaniu kodów do odpowiednio zaprogramowanego komputera i automatycznego porównywania kodów. Systemy takie funkcjonowały w policjach niektórych państw. W Polsce także powstało kilka projektów tego rodzaju rozwiązań (W. Kozłowski, T. Pietrzykowski, 1960, s. 5–10; W. Kozłowski, 1962, s. 621–629; Cz. Grzeszyk, S. Grzegórski, 1973, s. 627–635; A. Szota-Koziczak, 1985, s. 635–641; M. Owoc, 1986, s. 213–220). W 1988 roku w Wydziale Daktyloskopii CLK KGP uruchomiony został pilotażowy

[1] W większości przypadków, kiedy na miejscu zdarzenia zostały ujawnione ślady linii papilarnych i nie było osób podejrzanych, prowadzący postępowania zlecali ekspertyzy, załączając do nich po kilkadziesiąt „kart z szuflady" osób, które pozostawały w zainteresowaniu Milicji (Policji). W ten sposób wykazywano aktywność w prowadzeniu postępowań, a przy okazji istniała jakaś szansa na przypadkowe wykrycie sprawcy.

system półautomatyczny, oparty na opracowaniu autora (J. Moszczyński, 1986, s. 23–27). Po kilku miesiącach pracy w czteroosobowym zespole uzyskano pierwsze rezultaty w postaci identyfikacji kilkunastu sprawców kradzieży z włamaniem. Wkrótce jednak, po roku 1989, kiedy to autor[2] miał możliwość zapoznania się z systemami AFIS, funkcjonującymi od lat 70. w USA oraz państwach Europy Zachodniej, zmienił się kierunek dalszego rozwoju polskiej daktyloskopii. Zdobywana za granicą wiedza była sukcesywnie przenoszona na polski grunt (np.: J. Moszczyński, 1991a, s. 20–25; J. Moszczyński, 1991, s. 3–6; J. Moszczyński, 1992a, s. 19–28; J. Moszczyński, 1997).

WDROŻENIE SYSTEMU AFIS

Po uzyskaniu niezbędnych środków finansowych z unijnego funduszu PHARE przystąpiono do przygotowań zakupu i wdrożenia systemu AFIS do praktyki polskiej Policji[3]. Należało m.in. dokonać adaptacji pomieszczeń, zwiększyć obsadę kadrową, przeprowadzić szkolenia, uzyskać dostęp do policyjnych łączy teleinformatycznych i zaprojektować krajową sieć systemu AFIS. W drodze przetargu wyłoniono w 1998 roku zwycięską firmę Sagem (Morpho). Wielkiego wysiłku wymagało przygotowanie kart daktyloskopijnych do konwersji (skanowanie i wprowadzanie do systemu), którą w ciągu kilku miesięcy wykonał dostawca systemu w swoim centrum konwersji, zlokalizowanym w USA. Bardzo poważnym problemem, z jakim musieliśmy sobie także poradzić, było odbudowanie, prawie zanikłej na początku lat 90., rejestracji daktyloskopijnej, o czym będzie mowa w dalszej części opracowania.

W roku 2000 został zainstalowany centralny system AFIS, zawierający bazę danych, zespół urządzeń kodujących i porównujących oraz 10 stanowisk roboczych, a w dwa lata później uruchomiono sieć krajową, obejmującą 28 stanowisk roboczych, zainstalowanych w laboratoriach wojewódzkich, oraz 58 urządzeń Morpho-Touch do szybkiej identyfikacji osób, wykorzystywanych w jednostkach policyjnych niższego szczebla. Wdrożenie systemu AFIS pozwoliło już wkrótce na uzyskanie bardzo dobrych rezultatów.

[2] W latach 1988–2003 autor był kolejno, ekspertem, naczelnikiem Wydziału Daktyloskopii oraz zastępcą dyrektora Centralnego Laboratorium Kryminalistycznego KGP.

[3] Koordynację wdrożenia systemu AFIS powierzył komendant główny Policji autorowi.

Liczba pozytywnych identyfikacji śladów z miejsc zdarzeń (wykryć sprawców przestępstw) w latach 2002–2007 wynosiła kolejno: 3443, 5435, 4544, 4028, 4527, 3963. Ponadto w ciągu każdego roku ustalano tożsamość średnio około 15 000 osób i 500 zwłok. AFIS spotkał się z entuzjastycznym przyjęciem ze strony polskich ekspertów daktyloskopii.

Równocześnie z wdrożeniem systemu AFIS powstała także w Wydziale Daktyloskopii CLK KGP pracownia wizualizacji, wyposażona w najnowocześniejszy sprzęt i technologie służące do skutecznego ujawniania śladów linii papilarnych na różnych podłożach. Stała się ona wzorem i inspiracją dla laboratoriów wojewódzkich.

System AFIS jest stale rozwijany – aktualizowane jest oprogramowanie, poszerzana jest sieć stanowisk roboczych w postaci urządzeń do elektronicznego daktyloskopowania (LiveScan) oraz urządzeń do szybkiej identyfikacji (MorphoRapID) (E. Kot, K. Tomaszycki, 2015, [w:] E.W. Pływaczewski, W. Filipkowski, Z. Rau, s. 332–348).

Wdrożenie do praktyki systemu AFIS, wspartego nowoczesnymi metodami wizualizacji śladów linii papilarnych, było niewątpliwym przełomem w polskiej daktyloskopii, pozwalającym na skuteczniejszy udział kryminalistyki w zwalczaniu przestępczości.

POWSTANIE POLSKIEJ BAZY DNA

Kryminalistyczna identyfikacja genetyczna osób[4] ma znacznie krótszą historię niż identyfikacja daktyloskopijna – dzieli je cały wiek. Z tego względu, o ile w momencie uruchamiania systemu AFIS istniał duży zbiór kart daktyloskopijnych, które wprowadzono do bazy tego systemu, to budowanie bazy profili DNA należało rozpocząć od zera. Decyzją Rady Unii Europejskiej z 9 czerwca 1997 roku (97/C 193/02) państwa członkowskie Unii, a także państwa ubiegające się o taki status, zostały zainspirowane do tworzenia krajowych baz danych DNA. Miały one przyczynić się do skuteczniejszego zwalczania przestępczości zarówno krajowej, jak i transgranicznej, dzięki wymianie danych pomiędzy krajowymi bazami. Pierwsza i największa europejska baza genetyczna powstała w Wielkiej Brytanii już w 1995 roku. Wkrótce zaczęto organizować podobne bazy w innych

[4] Naukowe podstawy tej identyfikacji oparte są na opracowaniu przez A. Jeffreysa w 1985 roku metody nazywanej *DNA-fingerprinting*.

krajach europejskich (A. Filewicz, I. Sołtyszewski, 2003). W Polsce przygotowania do utworzenia bazy DNA rozpoczęto w Centralnym Laboratorium Kryminalistycznym KGP na przełomie lat 1998/1999. Polegały one m.in. na opracowaniu stosownych podstaw prawnych[5], przeszkoleniu ekspertów w Forensic Science Service, gdzie wówczas prowadzona była brytyjska baza danych DNA, przygotowaniu odpowiedniej infrastruktury oraz wyposażeniu policyjnych laboratoriów genetycznych w nowoczesną aparaturę (M. Goc, H. Dąbrowska, 2002). Szacowano wówczas, iż do bazy DNA w ciągu roku będzie trafiało około 200 tys. profili DNA osób podejrzanych oraz 30 tys. profili DNA oznaczanych na podstawie śladów biologicznych z miejsc zdarzeń.

Ostatecznie polska baza danych DNA, po perturbacjach z zakupem odczynników oraz problemami z oprogramowaniem CODIS (T. Noszczyński, lipiec 2006, s. 28–29), została uruchomiona w roku 2007. Gromadzi się w niej i przetwarza profile genetyczne:

- osób wymienionych w art. 74 i 192a k.p.k., tj. oskarżonych i podejrzanych,
- osób o nieustalonej tożsamości oraz osób usiłujących ukryć swoją tożsamość,
- zwłok ludzkich o nieustalonej tożsamości,
- osób stwarzających zagrożenie, o których mowa w ustawie z dnia 22 listopada 2013 roku o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających zagrożenie życia, zdrowia lub wolności seksualnej innych osób,
- śladów nieznanych sprawców przestępstw, np. śladów znalezionych na miejscu przestępstwa, gdy ich pochodzenia nie można przypisać do konkretnej osoby,
- osób zaginionych,
- osób spokrewnionych z osobami zaginionymi.

Aktualny stan polskiej bazy danych DNA na dzień przedstawiony jest w tabeli 1.

[5] Nowelizacja ustawy o Policji – art. 20 ust. 2, podpisanej przez Prezydenta RP 24 sierpnia 2001 roku.

Tabela 1.
Liczba profili DNA zarejestrowanych w polskiej bazie danych DNA – stan na dzień 30 września 2016 roku

Kategoria profilu	Liczba profili DNA
Podejrzani	52 444
Ślady nieznanych sprawców przestępstw	7 131
Zwłoki o nieustalonej tożsamości	1 035
Osoby o nieustalonej tożsamości lub ukrywające tożsamość	30
Osoby zaginione	338
Krewni osób zaginionych	1 782
Suma	62 760

Źródło: Centralne Laboratorium Kryminalistyczne Policji

WYMIANA DANYCH DAKTYLOSKOPIJNYCH I GENETYCZNYCH W RAMACH DECYZJI PRÜM

Zamach terrorystyczny w Madrycie (11 marca 2004 roku) zdopingował niektóre państwa członkowskie do podjęcia nowych inicjatyw w celu podniesienia skuteczności zapobiegania i zwalczania terroryzmu i groźnej przestępczości międzynarodowej (A. Gruszczak, 2009, s. 194–200). Ministrowie sprawiedliwości i spraw wewnętrznych Austrii, Belgii, Holandii, Luksemburga i Niemiec podpisali 28 maja 2004 roku deklarację o wzmocnieniu współpracy transgranicznej w zakresie walki z terroryzmem, przestępczością transgraniczną i nielegalną imigracją. Do piątki sygnatariuszy dołączyły także Francja i Hiszpania. Polityczna decyzja o zawarciu traktatu, otwartego również dla innych państw, zapadła podczas posiedzenia Rady Unii Europejskiej na szczeblu ministrów spraw wewnętrznych i sprawiedliwości 14 kwietnia 2005 roku. Wkrótce po tym, bo 27 maja 2005 roku, siedem wymienionych państw podpisało traktat o pogłębianiu współpracy transgranicznej, w szczególności w zakresie zwalczania terroryzmu, przestępczości transgranicznej i nielegalnej migracji, zwany traktatem z Prüm, który wszedł w życie 1 listopada 2006 roku. Przyjęto m.in., że w ramach współpracy transgranicznej będą udostępniane dane z krajowych zbiorów daktyloskopijnych oraz profili DNA. W celu przeniesienia

niektórych postanowień traktatu do uregulowań wspólnotowych, w dniu 13 czerwca 2007 roku Rada Ministrów Spraw Wewnętrznych Unii Europejskiej podjęła decyzję nr 11896/07 w sprawie wzmocnienia współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej, której konsekwencją była analogiczna decyzja Rady Europy z 23 czerwca 2008 roku. Przyjęto, że ostateczny termin uruchomienia nowego narzędzia wymiany danych daktyloskopijnych i genetycznych upływa w dniu 6 sierpnia 2011 roku.

Tabela 2.

Liczba identyfikacji uzyskanych w wyniku międzynarodowej wymiany danych z polską bazą DNA – od stycznia 2013 do 31 maja 2016 roku

	Ślad (PL) / osoba (UE)	**Ślad (PL) / ślad (UE)**	**Osoba (PL) / ślad (UE)**	**Osoba (PL) / osoba (UE)**	**Suma**
Austria	43	40	78	149	310
Cypr	0	0	0	0	0
Czechy	18	12	17	78	125
Estonia	2	0	1	0	3
Finlandia	2	1	5	4	12
Francja	56	17	71	57	201
Hiszpania	11	7	6	14	38
Holandia	20	28	71	78	197
Litwa	4	3	6	28	41
Łotwa	0	0	0	1	1
Malta	0	0	0	0	0
Niemcy	112	123	489	668	1 392
Rumunia	2	1	0	5	8
Słowacja	10	8	12	20	50
Słowenia	5	0	2	8	15
Szwecja	12	3	28	48	91
Węgry	0	0	2	0	2
SUMA	297	243	788	1 158	2 486

Źródło: Centralne Laboratorium Kryminalistyczne Policji

W styczniu 2013 roku w Zakładzie Biologii CLKP uruchomiony został Krajowy Punkt Kontaktowy (KPK) ds. automatycznej wymiany danych DNA z państwami członkowskimi UE (J. Mondzelewski, 2015, [w:] E.W. Pływaczewski, W. Filipkowski, Z. Rau, s. 485–502). Do jego głównych zadań należą: zapewnienie całodobowego dostępu punktom innych państw do wykonywania sprawdzeń profili DNA w zbiorach polskiej Bazy Danych DNA udostępnianych przez pozostałe kraje oraz weryfikacja pozytywnych identyfikacji. Obecnie KPK prowadzi wzajemną wymianę danych DNA z: Austrią, Cyprem, Czechami, Estonią, Finlandią, Francją, Hiszpanią, Holandią, Litwą, Łotwą, Maltą, Niemcami, Rumunią, Słowacją, Słowenią, Szwecją i Węgrami. Rezultaty tej wymiany przedstawiono w tabeli 2.

W ramach porównań ślad/osoba oraz osoba/ślad uzyskano łącznie 1085 identyfikacji, co odzwierciedla skalę wykryć sprawców przestępstw. W 1158 przypadkach ustalono bądź zweryfikowano tożsamość osób (porównania osoba/osoba), zaś w 243 przypadkach skojarzono miejsca zdarzeń, na których działali ci sami sprawcy (porównania ślad/ślad).

Wymianę danych daktyloskopijnych w ramach UE uruchomiono dopiero w listopadzie 2015 roku i nie uzyskano jeszcze znaczących rezultatów.

PROBLEMY Z PODSTAWAMI PRAWNYMI REJESTRACJI KRYMINALISTYCZNEJ

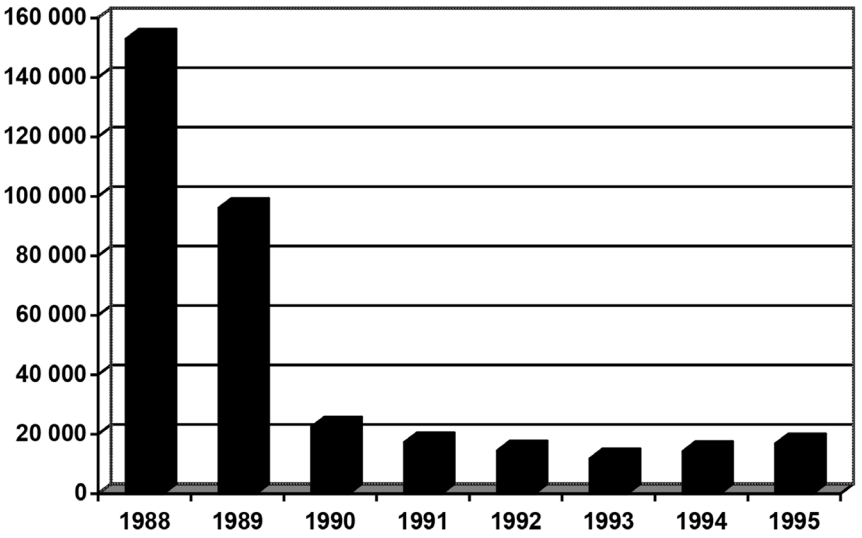
W roku 1989 wspomniana wcześniej instrukcja nr 1/77 została uchylona w części dotyczącej rejestracji daktyloskopijnej, na wniosek Prokuratora Generalnego, który w piśmie z dnia 24 kwietnia 1989 roku, l. dz. 94/89/1-d, do Ministra Spraw Wewnętrznych stwierdził m.in.: „Prokuratura Generalna otrzymuje informacje, że niektóre przypadki pobierania odcisków linii papilarnych (daktyloskopowania) prowadzonego przez organa resortu spraw wewnętrznych są sprzeczne z zasadami ochrony praw obywatelskich, wynikających z art. 87 ust. 1 Konstytucji PRL. (...) Pozbawienie obywatela wolności może nastąpić tylko w przypadkach określonych ustawą. Jedyną podstawą prawną dla naruszenia wolności w zakresie dysponowania liniami papilarnymi jest art. 65 § 1 pkt 1 k.p.k., który zobowiązuje oskarżonego (podejrzanego), gdy jest to potrzebne dla celów dowodowych danego postępowania karnego, do poddania się pobraniu odcisków. (...) Kodeks postępowania karnego nie upoważnia do daktyloskopowania oskarżonych (podejrzanych) wyłącznie do celów ewidencyjnych”. Podobne stanowisko

zostało zaprezentowane w piśmie Rzecznika Praw Obywatelskich z dnia 24 sierpnia 1989 roku, l. dz. RPO 46208/89/II/HK, do wiceministra spraw wewnętrznych (J. Moszczyński, 1992, s. 3–9).

Stan zawieszenia podstaw prawnych rejestracji daktyloskopijnej, pomimo usilnych starań ze strony przedstawicieli kryminalistyki (np. J. Moszczyński, 1992b, s. 55–58), trwał aż do 2005 roku, kiedy to została znowelizowana ustawa o Policji z dnia 6 kwietnia 1990 roku i zgodnie z art. 20 Policja uzyskała prawo do pobierania, gromadzenia, przetwarzania i wykorzystywania w celach wykrywczych i identyfikacyjnych odcisków linii papilarnych, zdjęć oraz innych danych o osobach podejrzanych o popełnienie przestępstw umyślnych, ściganych z oskarżenia publicznego, nieletnich dopuszczających się czynów zabronionych przez ustawę jako przestępstwa ścigane z oskarżenia publicznego, a także o osobach o nieustalonej tożsamości lub usiłujących ukryć swoją tożsamość oraz o osobach poszukiwanych.

Brak podstaw prawnych rejestracji daktyloskopijnej w latach 1989–2005 spowodował gwałtowny spadek pobierania odcisków palców od osób podejrzanych o popełnienie przestępstw (wykres 1).

Wykres 1.
Rejestracja kart daktyloskopijnych w CRD w latach 1988–1995



Źródło: Centralne Laboratorium Kryminalistyczne KGP

W latach 1988–1995 zarejestrowano w CRD następujące liczby kart daktyloskopijnych: w 1988 roku – 152 929 kart, 1989 – 96 056, 1990 – 22 473, 1991 – 17 225, 1992 – 14 450, 1993 – 11 738, 1994 – 14 211, 1995 – 16 817.

Dezaktualizacja zbiorów CRD miała bardzo niekorzystny wpływ na wykorzystanie identyfikacji daktyloskopijnej w procesie zwalczania przestępczości, tym bardziej że w roku 2000 został uruchomiony system AFIS, który dawał możliwości wykrywania sprawców przestępstw, ale jego skuteczność w oczywisty sposób zależy od wielkości i aktualności bazy danych. Pojawienie się w 1995 roku podstaw prawnych rejestracji daktyloskopijnej wcale nie spowodowało radykalnego wzrostu wpływu kart daktyloskopijnych do CRD i wymagało długofalowych działań, polegających na rygorystycznym egzekwowaniu od policjantów daktyloskopowania sprawców przestępstw.

Kolejne załamanie rejestracji daktyloskopijnej nastąpiło po 2005 roku, kiedy to Trybunał Konstytucyjny, uwzględniając wniosek Rzecznika Praw Obywatelskich, wydał orzeczenie z dnia 12 grudnia 2005 roku (sygn. K 32/04), w którym zakwestionował przepisy ustawy o Policji dotyczące rejestracji daktyloskopijnej, stwierdzając między innymi, iż art. 20 ust. 2 ustawy o Policji jest niezgodny z art. 51 ust. 2 w związku z art. 31 ust. 3 Konstytucji przez to, że nie precyzuje, w jakich sytuacjach można gromadzić informacje o osobach podejrzanych o popełnienie przestępstwa ściganego z urzędu, i nie określa rodzajów tych informacji w sposób wyczerpujący. W związku z powyższym w 2006 roku art. 20 ustawy o Policji został znowelizowany między innymi w ten sposób, że w ust. 2c. zapisano: „Informacji, o których mowa w ust. 2a nie pobiera się w przypadku, gdy nie mają one przydatności wykrywczej, dowodowej lub identyfikacyjnej w prowadzonym postępowaniu".

Przepis ten jest interpretowany w taki sposób, że jeśli na miejscu zdarzenia nie zostaną ujawnione ślady linii papilarnych, to osób podejrzanych nie daktyloskopuje się. Analogiczna procedura została przyjęta w odniesieniu do rejestracji profili DNA. W rezultacie od 2006 roku nastąpił znaczny spadek wpływu kart daktyloskopijnych do bazy AFIS oraz pozytywnych identyfikacji w ramach przeszukań typu karta/karta (tabela 3 oraz wykres 2).

Tabela 3.

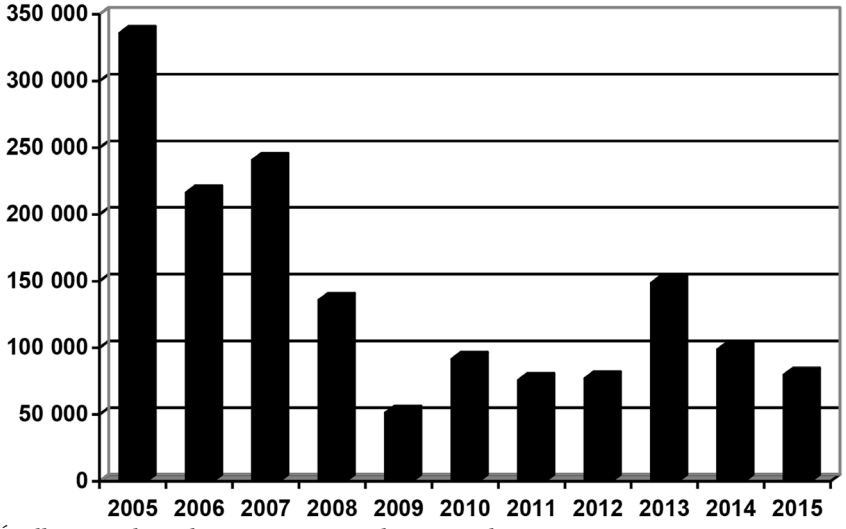
Wpływ kart daktyloskopijnych do bazy AFIS oraz wyniki przeszukań typu karta w latach 2005–2015

Rok	Liczba kart daktyloskopijnych	Przeszukania karta/karta	Pozytywny wynik karta/karta
2005	335 806	485 866	140 504
2006	216 394	354 277	125 993
2007	240 548	328 736	79 183
2008	135 852	212 933	69 198
2009	51 350	113 455	52 737
2010	91 741	117 954	27 906
2011	75 660	82 849	20 556
2012	76 968	97 057	22 434
2013	148 649	158 767	30 095
2014	98 860	111 916	28 071
2015	79 816	99 946	21 857

Źródło: Centralne Laboratorium Kryminalistyczne Policji

Wykres 2.

Wpływ kart daktyloskopijnych do systemu AFIS w latach 2005–2015



Źródło: Centralne Laboratorium Kryminalistyczne Policji

Polska baza DNA od momentu jej uruchomienia funkcjonuje w warunkach obowiązujących od 2006 roku podstaw prawnych rejestracji kryminalistycznej, co sprawia, że jej rozbudowa przebiega w bardzo wolnym tempie. Wielkości baz danych DNA w wybranych państwach europejskich zaprezentowane są w tabeli 4.

Tabela 4.
Wielkości baz danych DNA w wybranych państwach europejskich – stan na rok 2015

Państwo	Liczba profili DNA osób (w tys.)	% populacji
Wielka Brytania	6 000	10
Francja	3 100	6
Niemcy	850	1
Hiszpania	313	0,7
Holandia	225	1,3
Austria	197	2,5
Czechy	174	1,7
Finlandia	157	3
Szwecja	148	1,5
Węgry	138	1,4
Litwa	90	2,3
Słowacja	55	1
Estonia	48	3,2
Polska	45	0,1

Źródło: Opracowano na podstawie danych Rady Unii Europejskiej[6]

[6] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border-crime, Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border-crime („Prüm Decisions") - statistics and reports on automated data exchange for 2015, [data dostępu: 24.11.2016]. http://statewatch.org/news/2016/apr/eu-council-prum-statistics-2015-dna-fingerprints-vrd-05129-16.pdf

Według danych Rady Unii Europejskiej za rok 2015 w polskiej bazie DNA znajdowały się 44 553 profile DNA sprawców przestępstw, co sytuuje ją wśród najmniejszych europejskich baz genetycznych, natomiast w odniesieniu do liczby mieszkańców poszczególnych państw – na samym końcu.

PODSUMOWANIE

Baza danych nowoczesnego i kosztownego systemu AFIS dezaktualizuje się, natomiast baza danych DNA należy do najmniejszych w Europie, czego naturalną konsekwencją jest ograniczenie potencjalnych możliwości wykrywczych. Przyczyną tego niekorzystnego stanu rzeczy są aktualnie obowiązujące podstawy prawne rejestracji kryminalistycznej, uzależnione de facto od ujawnienia śladów na miejscach zdarzeń. Są one zaprzeczeniem sensu prowadzenia kryminalistycznych baz danych. Sprawców przestępstw powinno się daktyloskopować oraz pobierać od nich wymazy śliny na potrzeby oznaczania profilu DNA, nie tylko w celu wykonania ekspertyz w prowadzonych postępowaniach, lecz także w celu umożliwienia wykrywania ewentualnych przestępstw popełnionych w okresie wcześniejszym lub późniejszym. Właśnie do tego służą kryminalistyczne bazy danych, stale rozwijane w innych państwach. Prezentowany problem był już przedmiotem alarmujących doniesień prasowych (A. Krawczyńska, kwiecień 2013), s. 12–13; T. Noszczyński, kwiecień 2013, s. 13–14), jednak sytuacja pozostaje bez zmian.

Bibliografia

Brzęk W. (1980). *Daktyloskopia w Polsce okresu międzywojennego,* „Problemy Kryminalistyki", nr 145–146.

Buras D. (2004). *Wykorzystanie daktyloskopii przez Policję Państwową w Drugiej Rzeczypospolitej.* „Problemy Kryminalistyki", nr 246, s. 56–61.

Buras D. (2009). *Daktyloskopia na ziemiach polskich i w Polsce w latach 1909–1939,* [w:] P. Rybicki, T. Tomaszewski (red.), *Daktyloskopia. 100 lat na ziemiach polskich*. Wydawnictwo Stowarzyszenie Absolwentów Wydziału Prawa i Administracji Uniwersytetu Warszawskiego. Warszawa, s. 71–82.

Filewicz A, Sołtyszewski I. (2003). *Bazy DNA w Europie – rozwiązania legislacyjne.* „Problemy Kryminalistyki", nr 241, s. 5–12.

Goc M., Dąbrowska H. (2002). *Polska baza DNA dziś i jutro,* „Problemy Kryminalistyki", nr 237, s. 5–7.

Gruszczak A. (2009). *Współpraca policyjna w Unii Europejskiej w wymiarze transgranicznym. Aspekty polityczne i prawne.* Wydawnictwo Uniwersytetu Jagiellońskiego. Kraków, s. 194–200.

Grzeszyk Cz., Grzegórski S. (1973). *Metody automatycznej identyfikacji daktyloskopijnej,* „Problemy Kryminalistyki", nr 105, s. 627–635.

Horoszowski P. (1958). *Kryminalistyka.* Wydawnictwo PWN. Warszawa.

Kot E., Tomaszycki K. (2015). *Funkcjonowanie automatycznego systemu identyfikacji daktyloskopijnej AFIS,* [w:] E.W. Pływaczewski, W. Filipkowski, Z. Rau (red.), *Przestępczość w XXI wieku. Zapobieganie i zwalczanie. Problemy technologiczno-informatyczne*. Wydawnictwo Wolters Kluwer. Warszawa, s. 332–348.

Kozłowski W. (1962). *System automatycznej registratury daktyloskopijnej*, „Problemy Kryminalistyki", nr 40, s. 621–629.

Kozłowski W., Pietrzykowski T. (1960). *Zastosowanie cyfrowych maszyn elektronowych w kryminalistyce.* „Problemy Kryminalistyki", nr 23, s. 5–10.

Krassowski K. (2007). *Bazy danych – wspomaganie procesu wykrywczego,* [w:] I. Sołtyszewski (red.), *Badania kryminalistyczne (wybrane aspekty)*. Wydawnictwo Uniwersytetu Warmińsko-Mazurskiego w Olsztynie. Olsztyn, s. 111–128.

Krawczyńska A. (kwiecień 2013), *AFIS, czyli baza skromnie wykorzystywana*. „Policja 997", nr 4(97), s. 12–13.

Misiuk A., Pepłoński A. (1994). *Organizacja instytucji policyjnych w II Rzeczypospolitej 1918–1926.* Wydawnictwo Wyższej Szkoły Policji w Szczytnie. Szczytno.

Misztal J. (2008). *Daktyloskopia w Polsce w XX wieku.* „Problemy Kryminalistyki", nr 262, s. 63–71.

Mondzelewski J. (2015). *Problematyka międzynarodowej automatycznej wymiany danych DNA prowadzonej w ramach postanowień decyzji Prüm*, [w:] E.W. Pływaczewski, W. Filipkowski, Z. Rau (red.), *Przestępczość w XXI wieku. Zapobieganie i zwalczanie. Problemy technologiczno-informatyczne.* Wydawnictwo Wolters Kluwer. Warszawa, s. 485–502.

Moszczyński J. (1986). *Możliwości kodowania śladów linii papilarnych zabezpieczonych na miejscu zdarzenia.* „Problemy Kryminalistyki", nr 171, s. 23–27.

Moszczyński J. (1988). *Najbardziej prawdopodobne formuły daktyloskopijne.* Wydawnictwo Zakładu Kryminalistyki KG MO. Warszawa.

Moszczyński J. (1991). *O potrzebie automatyzacji identyfikacji daktyloskopijnej w Polsce.* „Problemy Kryminalistyki", nr 191–192, s. 3–6.

Moszczyński J. (1991a). *Wykorzystanie identyfikacji daktyloskopijnej przez policję londyńską.* „ Biuletyn Informacyjny", nr 3–4, s. 20–25.

Moszczyński J. (1992). *Aktualne problemy rejestracji daktyloskopijnej – propozycje nowych rozwiązań*. „Problemy Kryminalistyki", nr 197–198, s. 3–9.

Moszczyński J. (1992a). *Materiały i sprzęt daktyloskopijny – oferta firm zachodnich*. „Biuletyn Informacyjny", nr 85–86, s. 19–28.

Moszczyński J. (1992b). *Pilny problem powstania podstaw prawnych kryminalistycznej rejestracji daktyloskopijnej*. „Biuletyn Informacyjny", nr 85–86, s. 55–58.

Moszczyński J. (1993). *Wywiad daktyloskopijny za pomocą telefaksu*. „Biuletyn Informacyjny", nr 90, s. 15–21.

Moszczyński J. (1997). *Daktyloskopia. Zarys teorii i praktyki*. Wydawnictwo Centralnego Laboratorium Kryminalistycznego KGP. Warszawa.

Noszczyński T. (lipiec 2006). *Kody do szuflady*. „ Policja 997", nr 7(16), s. 28–29.

Noszczyński T. (kwiecień 2013), *Prawo kontra DNA*, „Policja 997", nr 4(97), s. 13–14.

Owoc M. (1986), *Wirtualna registratura monodaktyloskopijna*. „Problemy Kryminalistyki", nr 172, s. 213–220.

Raczyński D., Skopiński Z. (1961). *Wywiad daktyloskopijny przez telefon*. Wydawnictwo Zakładu Kryminalistyki KG MO. Warszawa.

Szota-Koziczak A. (1985). *Skomputeryzowana registratura monodaktyloskopijna – propozycja badania odcisku palca wzdłuż biegu linii naturalnych*. „Problemy Kryminalistyki", nr 170, s. 635–641.

Źródła internetowe

Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border-crime, Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border-crime („Prüm Decisions") – statistics and reports on automated data exchange for 2015, http://statewatch.org/news/2016/apr/eu-council-prum-statistics-2015-dna-fingerprints-vrd-05129-16.pdf [data dostępu: 24.11.2016].

KRZYSZTOF CYGAŃCZUK

Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej
im. Józefa Tuliszkowskiego – Państwowy Instytut Badawczy
w Józefowie k. Otwocka

kcyganczuk@cnbop.pl

WYKORZYSTANIE BEZZAŁOGOWYCH STATKÓW POWIETRZNYCH JAKO SKŁADNIKÓW MOBILNEGO SYSTEMU MONITOROWANIA I PRZECIWDZIAŁANIA ZAGROŻENIOM POŻAROWYM W LASACH

USAGE OF UNMANNED AERIAL VEHICLES AS A MOBILE MONITORING COMPONENTS OF FIRE HAZARD IN THE FORESTS

ABSTRACT

This paper describes the concept of mobile system for observation of land in order to detect fire outbreaks. The primary function of this system meets the unmanned aerial vehicle equipped with a specialized television cameras and thermal imaging indicating the presence of areas with elevated temperatures, which may be identified as a fire. The system has the possibility of two-way radio communication with the position of command and after minor modifications, can be used to monitor events related to the protection of persons and property as well as ensuring security in conditions of vulnerability to natural disasters and terrorism. Due to the low altitude limit regulations will include a signaling system risks arising from the approximation of the overhead high voltage lines, which will help them bypass the collision.

Keywords: *UAV – Unmanned Aerial Vehicle, UAS – Unmanned Aerial Systems, crisis management, terrorism, rescue operations, monitoring areas*

STRESZCZENIE

W artykule opisano możliwość wykorzystania mobilnego systemu do obserwacji obszarów w celu wykrywania ognisk pożarów. Podstawową rolę w tym systemie spełnia bezzałogowy statek powietrzny (BSP), wyposażony w wyso-

kiej jakości kamery światła dziennego i termowizyjne sygnalizujące obecność obszarów o podwyższonej temperaturze, które mogą zostać zidentyfikowane jako ogniska pożaru. System ma możliwość dwukierunkowej komunikacji drogą radiową ze stanowiskiem dowodzenia i po drobnych modyfikacjach może być wykorzystany do monitorowania zdarzeń związanych z ochroną ludzi i mienia, a także z zapewnieniem bezpieczeństwa w warunkach zagrożenia klęskami żywiołowymi i terroryzmem. Ze względu na ograniczenia dopuszczalne przepisami wysokości lotu, wykorzystany został układ sygnalizujący zagrożenie wynikające ze zbliżania się do napowietrznych linii wysokiego napięcia, który ułatwi bezkolizyjne ich ominięcie[1].

Słowa kluczowe: *dron, bezzałogowce, pożary, klęski żywiołowe*

WPROWADZENIE

Pożary należą do największych zagrożeń trwałości ekosystemów lądowych. Czynią zniszczenie we wszystkich formacjach roślinnych porastających powierzchnię ziemi. Szacuje się, że około 40% zasobów leśnych świata jest potencjalnie zagrożonych pożarami. W Europie udział ekosystemów zagrożonych pożarami sięga do 65%, a w Polsce aż do około 80%. W naszym kraju, w latach suchych, pożary lasów stanowią średnio 10–12% wszystkich powstających pożarów, choć w niektórych powiatach udział ich sięga 50%. Pożar lasu to ogromne niebezpieczeństwo, przede wszystkim ze względu na tempo rozprzestrzeniania. Zawsze stanowi zagrożenie dla ludzkich osad, które są w pobliżu. Zwykle czas jest wyłącznie na ewakuację, ale już nie zawsze na ratowanie mienia. To, co znika w wyniku pożarów, jest praktycznie nie do odzyskania. Zagładzie ulega roślinność i zwierzęta, w tym bardzo często gatunki wpisane do Czerwonej Księgi Gatunków Zagrożonych. Zniszczeniu ulegają lasy wokół aglomeracji i na wiele lat zmniejsza się mieszkalna i rekreacyjna atrakcyjność terenów w tych rejonach. Zgodnie z prawem Unii Europejskiej, las jest obszarem z pokrywą korony drzew (lub równoważnym poziomem pni drzew) na ponad 10% i o powierzchni większej niż 0,5 ha. Drzewa powinny w nim osiągać wysokość przynajmniej 5 m w stanie dojrzałym. Może on tworzyć formacje zamknięte, gdzie drzewa różnych

[1] Artykuł został opracowany na podstawie referatu prezentowanego podczas IX Międzynarodowej Konferencji Uzbrojeniowej nt. „Naukowe aspekty techniki uzbrojenia i bezpieczeństwa", Pułtusk, 25–28 września 2012 r.

poziomów i podszycia leśnego pokrywają znaczną część powierzchni, lub formacje otwarte z pokrywą o stałej wegetacji, stanowiącą ponad 10% powierzchni gruntu. Lasy w Polsce zajmują powierzchnię około 9,14 mln ha, co stanowi niemal 30% powierzchni kraju. Większość z nich to własność Skarbu Państwa, zarządzana przez Państwowe Gospodarstwo Leśne Lasy Państwowe oraz przez parki narodowe. Lasy prywatne stanowią około 17% ogólnego areału lasów. Udział poszczególnych własności ze względów historycznych jest bardzo zróżnicowany (najmniej lasów prywatnej własności spotykamy w Polsce zachodniej i północnej).

Zgodnie z definicją obowiązującą w Unii Europejskiej, pożar lasu to taki, który wybucha i rozprzestrzenia się w lesie i na innych obszarach zalesionych lub który wybucha na innym terenie i rozprzestrzenia się na las i inne obszary zalesione. Jednostki ochrony przeciwpożarowej, a w szczególności jednostki organizacyjne Państwowej Straży Pożarnej, wypełniają ustawowy cel ochrony przeciwpożarowej, którym jest realizacja przedsięwzięć chroniących życie i zdrowie ludzi oraz zwierząt, a także mienie i środowisko naturalne(przyrodnicze) przed pożarem lub innym miejscowym zdarzeniem wynikającym z rozwoju cywilizacyjnego i naturalnych praw przyrody poprzez działania profilaktyczne zapobiegające powstawaniu i rozprzestrzenianiu się pożaru lub innego miejscowego zdarzenia, poprzez zapewnienie sił ratowniczych (ludzi i zwierząt wykorzystywanych w działaniach ratowniczych) oraz zapewnienie środków ratowniczych pod postacią sprzętu i pojazdów ratowniczych do prowadzenia działań ratowniczych podczas pożarów lub innych miejscowych zdarzeń, które w niektórych sytuacjach i okolicznościach mogą przybrać rozmiary klęski żywiołowej. Aby kierujący działaniami ratowniczymi mógł szybko i trafnie podjąć decyzję o metodach, wariantach i formach prowadzenia działań ratowniczych i aby te działania były szybko, sprawnie, skutecznie i bezpiecznie realizowane, musi posiadać bardzo dużo informacji nie tylko o siłach i środkach ratowniczych, ale w szczególności o istniejącej sytuacji zdarzenia, aby móc także przewidywać prognozowany jego rozwój i rozprzestrzenianie. Obecna technika i wiedza pożarnicza pozwala dość dobrze radzić sobie z takimi niebezpiecznymi zdarzeniami, ale często niepełna lub opóźniona informacja o istniejącym zdarzeniu potęguje niekontrolowane rozmiary zdarzenia, podnosząc koszty działań ratowniczych oraz straty w mieniu i środowisku, a niekiedy doprowadzając do utraty

życia lub zdrowia poszkodowanych bądź nawet samych ratujących. Podczas wielu niebezpiecznych zdarzeń prowadzenie rozpoznania w czasie działań ratowniczych najczęściej sprowadza się do rozpoznania naziemnego, które ograniczane jest m.in. dużą powierzchnią strefy zagrożenia, wysokim oddziaływaniem promieniowania cieplnego lub wysokim skażeniem tej strefy nawet dla samych ratujących, terenem trudno dostępnym bądź warunkami nocnymi lub zadymieniem.

W nielicznych przypadkach niebezpiecznych zdarzeń siły ratownicze wspomagane są prowadzeniem rozpoznania z powietrza za pomocą tradycyjnych statków latających (samoloty lub śmigłowce) nienależących do Państwowej Straży Pożarnej.

Lasy to miejsce, do którego wstęp ma każdy z nas i w którym każdy może spędzić czas, uprawiając sport i odpoczywając. Aby lasu starczyło dla wszystkich, trzeba się o niego troszczyć. W trosce o nasze tereny zielone pomóc mogą najnowsze zdobycze technologii. Jedną z takich zdobyczy są bezzałogowe statki powietrzne (BSP) – drony. Dzięki nim można przeprowadzać inspekcje drzewostanu, szacować straty wyrządzone przez szkodniki oraz wykonywać wiele innych czynności i zabiegów pielęgnacyjnych. Za pomocą bezzałogowych statków powietrznych można szybciej i efektywniej obserwować tereny leśne o zdecydowanie większej powierzchni niż tradycyjnymi sposobami. Bezzałogowe statki powietrzne mogą przyczynić się także do znacznej redukcji kosztów niektórych operacji. Obecnie inspekcje lasów przeprowadzane z powietrza wiążą się z wynajęciem samolotu wraz z załogą lub z wynajęciem motolotniarza. Korzystając z bezzałogowych statków powietrznych, można takie inspekcje przeprowadzać samodzielnie, nie będąc zależnym od innych osób bądź firm. Koncepcja zastosowania w ratownictwie BSP do prowadzenia rozpoznania jest już znana na świecie i przynosi ogromne efekty w postaci znacznego ograniczania strat spowodowanych narażeniem ludzkiego życia w wyniku wystąpienia niebezpiecznego zdarzenia. Bezzałogowy statek powietrzny na potrzeby leśnictwa powinien charakteryzować się przede wszystkim:

- możliwością bezpośredniej transmisji obrazu,
- kamerą wysokiej rozdzielczości z dużym zoomem optycznym umożliwiającą także wykonywanie zdjęć,
- możliwością wykonywania lotów autonomicznych,
- jak najdłuższym czasem lotu na jednym akumulatorze.

Tabela 1.
Wymagania techniczne i eksploatacyjne bezzałogowych statków powietrznych do zastosowania w działaniach Państwowej Straży Pożarnej

Lp.	Parametr	Wartość	Uzasadnienie wartości
1.	Udźwig	5 kg	GPS, kamera światła dziennego i termowizyjna, czujnik temperatury, czujnik promieniowania jonizacyjnego, wykrywacz pola elektromagnetycznego (linie wysokiego napięcia), zasilanie, transmisja.
2.	Długotrwałość lotu	4 h	Średni czas patrolowania.
3.	Zasięg energetyczny	200 km	Obszar patrolowania lasów i powodzi.
4.	Zasięg radiowy	25 km	Obszar patrolowania powiatu.
5.	Pułap operacyjny	200–1000 m	W zależności od potrzeb (istnieje możliwość lotu na wysokościach do 3000 m).
6.	Prędkość przelotowa	0–120 km/h	Najmniejsza wartość możliwa do uzyskania, obserwacja obrazu z kamer.
Zmienne parametryczne			
7.	Liczba operatorów	2–3	Przepisy bhp, odpowiedzialność za sprzęt.
8.	Czas przygotowania do pierwszej misji	10 min	Szybkie podjęcie działań.
9.	Wymiary po demontażu	dł. 2,5 m szer. 1,5 m wys. 1,5 m	Możliwość transportu skrzyni na samochodzie do 3,5 t.
10.	Sposób startu	start pionowy	Szybkie podjęcie działań.
11.	Sposób lądowania	lądowanie pionowe	Bezpieczne lądowanie.

Monitorując dany teren, BSP powinien bardzo długo móc pracować (utrzymywać się) w powietrzu, mieć długi zasięg lotu, dużą wysokość lotu, posiadać kamerę wizyjną i kamerę termowizyjną wykorzystywaną w wa-

runkach słabej widoczności (noc, mgła) oraz podczas spalania bezpłomieniowego, mieć możliwość sterowania bezprzewodowego przez człowieka z ziemi, jak też działać samodzielnie zgodnie z programem z możliwością przeprogramowania lotu i sensorów pomiarowych w trakcie lotu, mieć wysoką odporność na zakłócenia sterowania parametrami lotu podyktowanymi obcą emisją radiową lub warunkami meteorologicznymi, mieć możliwość transmisji obrazu i danych w czasie rzeczywistym do naziemnego stanowiska dowodzenia, mieć zamontowane urządzenia startu i lądowania naziemnego oraz lądowania awaryjnego na ziemi i wodzie w przypadku utraty kontroli nad maszyną, mieć możliwość przesyłania obrazu w trójwymiarze, wykrywania promieniowania radioaktywnego, a także możliwość zaznaczania trasy lotu. Założone podstawowe wymagania techniczne i eksploatacyjne bezzałogowych statków powietrznych do zastosowania w działaniach Państwowej Straży Pożarnej zostały przedstawione w tabeli 1.

Budowa BSP powinna być modułowa. W zależności od potrzeb bezzałogowy statek powietrzny będzie uzbrajany w odpowiednie urządzenia. Do jego zadań należałaby obserwacja obszaru: powodzi, wypadku albo objętego pożarem. Dron pracowałby w dwóch trybach: patrol i akcja. Praktycznym zastosowaniem BSP byłaby działalność prewencyjna w okresie zagrożenia pożarowego łąk i lasów, a także możliwość poszukiwania ludzi np. w czasie powodzi lub zaginięcia.

ZASTOSOWANIE BEZZAŁOGOWYCH STATKÓW POWIETRZNYCH W OCHRONIE PRZECIWPOŻAROWEJ LASÓW

Bezzałogowy statek powietrzny w wielu państwach na świecie znalazł już zastosowanie zarówno w obszarze militarnym, jak i cywilnym, w tym związanym z ochroną lasów przed pożarami oraz obszarem czysto ratowniczym związanym z prowadzeniem rozpoznania podczas gaszenia pożarów lasu. Pierwszy z obszarów, w którym BSP znalazłby w Polsce zastosowanie, to rozpoznawanie zagrożeń, czyli działania związane z patrolowaniem obszarów leśnych w celu wczesnego wykrycia pożaru, zawiadomienia o jego powstaniu, a także podjęcia działań ratowniczych. W Polsce zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 7 czerwca 2010 roku w sprawie ochrony przeciwpożarowej budynków, innych

obiektów budowlanych i terenów (Dz.U. nr 109 poz. 719): „Właściciele, zarządcy lub użytkownicy lasów, których lasy samoistnie lub wspólnie tworzą kompleks leśny o powierzchni ponad 300 ha, organizują obserwację i patrolowanie lasów w celu wykrywania pożarów oraz alarmowania o ich powstaniu, zgodnie z przepisami o zabezpieczeniu przeciwpożarowym lasów". Kolejne rozporządzenie – rozporządzenie Ministra Środowiska z dnia 22 marca 2006 roku w sprawie szczegółowych zasad zabezpieczenia przeciwpożarowego lasów (Dz.U. nr 58 poz. 405 z późn. zm.) – doprecyzowuje wyżej wymieniony zapis prawny w taki sposób, że „W lasach o powierzchni powyżej 300 ha zaliczonych do I lub II kategorii zagrożenia pożarowego, w okresach oznaczonego dla tych lasów 1., 2. lub 3. stopnia zagrożenia pożarowego lasów, jest wymagane prowadzenie obserwacji mającej na celu wczesne wykrycie pożaru, zawiadomienie o jego powstaniu, a także podjęcie działań ratowniczych". Dalej to samo rozporządzenie wymienia trzy sposoby obserwacji lasów w celu wczesnego wykrycia pożaru lasu:
1) ze stałych punktów obserwacji naziemnej,
2) przez naziemne patrole przeciwpożarowe,
3) przez patrole lotnicze.

Jednym z tych trzech sposobów obserwacji jest patrolowanie lotnicze. Jeżeli obserwacja lasu jest prowadzona np. przez patrole lotnicze, wówczas nie jest wymagane prowadzenie obserwacji ze stałych punktów obserwacji naziemnej lub przez naziemne patrole przeciwpożarowe dla kompleksów leśnych o powierzchni do:
1) 1000 ha – zaliczonych do I kategorii zagrożenia pożarowego,
2) 2000 ha – zaliczonych do II kategorii zagrożenia pożarowego.

Prowadzenie obserwacji nie jest również wykluczone w lasach zaliczonych do III kategorii zagrożenia pożarowego. Rozporządzenie Ministra Środowiska z dnia 22 marca 2006 roku w sprawie szczegółowych zasad zabezpieczenia przeciwpożarowego lasów mówi, że w uzasadnionych wypadkach w lasach zaliczonych do III kategorii zagrożenia pożarowego prowadzi się obserwację przez naziemne patrole przeciwpożarowe lub przez patrole lotnicze, które zostały uzgodnione z właściwym miejscowo komendantem wojewódzkim Państwowej Straży Pożarnej. W odniesieniu do lasów użytkowanych przez jednostki organizacyjne podległe albo nadzorowane przez

ministra obrony narodowej – powiadamia się Wojskową Ochronę Przeciwpożarową (WOP). Patrolowanie lotnicze w Polsce obecnie realizuje wyłącznie Państwowe Gospodarstwo Leśne Lasy Państwowe (PGL LP) w stosunku do lasów przez siebie zarządzanych, czyli lasów stanowiących własność Skarbu Państwa. Do tego celu PGL LP co roku angażuje około 10 samolotów i śmigłowców patrolowych rozlokowanych w prawie 30 leśnych bazach lotniczych występujących na terenie większości regionalnych dyrekcji Lasów Państwowych. Koszt poniesiony przez PGL LP na prowadzenie lotów patrolowych i gaśniczych wynosi co roku około 15 mln zł.

Ilustracja 1.
Rozpoznanie z powietrza łąk i pastwisk w trakcie ich wypalania

Źródło: Państwowa Straż Pożarna

Na świecie co roku ubywa około 0,5% całkowitej powierzchni lasów, z czego połowa za przyczyną pożarów. W ostatnich dwóch dekadach notuje się wzrost liczby pożarów lasów, zarówno na świecie, jak i w Polsce. Obszary leśne w naszym kraju są zagrożone pożarami w około 80%.

W Polsce średnia roczna liczba pożarów lasów wynosi 9900 i według statystyk unijnych zajmujemy pod tym względem trzecie miejsce za Portugalią i Hiszpanią, a ósme pod względem średniej rocznej powierzchni spalonych drzewostanów (6816 ha). Patrole lotnicze wykrywają w Polsce około 2,5% ogólnej liczby pożarów. Bezzałogowy statek powietrzny jest alternatywą dużo tańszą w stosunku do tradycyjnego patrolowania lotniczego, bardziej niezawodną i bezpieczną, a także możliwą do zastosowania w patrolowaniu lasów niestanowiących własności Skarbu Państwa, czyli lasów osób fizycznych, lasów osób prawnych, lasów gminnych czy komunalnych występujących bardzo często w sąsiedztwie z lasami Skarbu Państwa w tych samych kompleksach leśnych. W Polsce aż około 60% pożarów lasów powstaje w lasach prywatnych właścicieli – spaleniu ulega aż około 80% ich powierzchni. Drugim z obszarów ratownictwa, w którym BSP znalazłby w Polsce zastosowanie, jest prowadzenie rozpoznania z powietrza podczas już istniejących pożarów lasów. Prowadzenie rozpoznania z powietrza podczas takich zdarzeń jak pożar lasu, w szczególności przy dużych jego powierzchniach, daje kierującemu działaniami ratowniczymi olbrzymią przewagę nad tradycyjnym prowadzeniem rozpoznania za pomocą sił naziemnych.

Prowadzenie rozpoznania z powietrza za pomocą BSP wyposażonego w kamerę światła dziennego i kamerę termowizyjną pozwala kierującemu działaniami ratowniczymi na bardzo szybką ocenę sytuacji pożarowej nawet w przypadku pożarów podpowierzchniowych oraz przy bardzo dużym zadymieniu lub też w porze nocnej, nie narażając na niebezpieczeństwo strażaków prowadzących tradycyjne rozpoznanie naziemne. Zastosowanie BSP podczas pożarów lasu wyklucza angażowanie wielu strażaków do prowadzenia rozpoznania naziemnego, którzy w tym samym czasie mogą prowadzić działania gaśnicze.

Zamontowanie w BSP dodatkowego oprzyrządowania pozwalającego na śledzenie strażaków podczas pożaru lasu podnosi w sposób bardzo znaczący poziom ich bezpieczeństwa, a jednocześnie pozwala kierującemu działaniami ratowniczymi śledzić rozprzestrzenianie się pożaru, które ma wpływ na dyslokację sił ratowniczych na tę część obwodu pożaru lub w miejsce nowych ognisk pożaru powstałych od ogni lotnych, które wymagają większego zaangażowania sił gaśniczych. Bieżący sygnał z BSP, poza przekazywaniem go do odpowiedniego stanowiska dowodze-

nia opartego na samochodzie operacyjnym lub samochodzie dowodzenia i łączności, może być również skierowany do właściwego miejscowo powiatowego (miejskiego) stanowiska kierowania komendanta powiatowego (miejskiego) Państwowej Straży Pożarnej lub stanowisk innych podmiotów. Bezzałogowy statek powietrzny, poza możliwością przewozu go na miejsce działań na platformie samochodowej, mógłby startować z wyznaczonego stanowiska zlokalizowanego na terenie wybranej jednostki ratowniczo-gaśniczej komendy powiatowej (miejskiej) Państwowej Straży Pożarnej, będąc sterowany i kierowany na miejsce przyszłych działań gaśniczych. Na początek BSP wszedłby na wyposażenie tej komendy powiatowej (miejskiej) Państwowej Straży Pożarnej w Polsce, która w swoim rejonie operacyjnym (na terenie powiatu) posiada największą powierzchnię leśną zaliczoną do I kategorii zagrożenia pożarowego, czyli zagrożenia dużego w porównaniu z innymi powiatami. Co prawda w treści rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 września 2000 roku w sprawie szczegółowych zasad wyposażenia jednostek organizacyjnych Państwowej Straży Pożarnej (Dz.U. nr 93 poz. 1035) przewidziano śmigłowce ratownicze – co najmniej jeden na 20 000 km^2 w ramach minimalnego wyposażenia Państwowej Straży Pożarnej w sprzęt, pojazdy i środki do działań związanych m.in. ze zwalczaniem pożarów, to jak na razie jest to mało realne.

W związku z powyższym, do czasu wyposażenia Państwowej Straży Pożarnej w odpowiednią liczbę śmigłowców ratowniczych, BSP wypełniałby w znaczącej części ich zadania związane z prowadzeniem rozpoznania z powietrza podczas wszelkich działań ratowniczych, nie tylko gaśniczych.

OKREŚLENIE TYPÓW I DOBÓR SENSORÓW OBSERWACYJNYCH W BEZPILOTOWYCH STATKACH POWIETRZNYCH PRZEZNACZONYCH DLA PSP

Zastosowanie kamer termowizyjnych ma kluczowe znaczenie podczas prowadzenia akcji ratowniczych, poszukiwania osób oraz prowadzenia akcji gaszenia pożarów i lokalizacji miejsc niedogaszonych. Kamery termowizyjne stosowane są również w diagnostyce i wyszukiwaniu uszkodzeń obiektów technicznych. Kamery umożliwiają nieinwazyjną lokalizację wszelkich nieprawidłowości. Każdy człowiek emituje ciepło, ponieważ

jego temperatura ciała jest najczęściej wyższa od temperatury otoczenia. Przeszukując teren leśny, gęstą łąkę lub pole uprawne, uwadze obserwatorów i operatora może umknąć poszukiwana osoba. Kamera termowizyjna umożliwia dostrzeżenie osób w lesie albo w gęsto zarośniętym polu lub na łące. Ponieważ człowiek ma wyższą temperaturę niż otoczenie, kamera termowizyjna od razu to zauważy i będzie można łatwiej zidentyfikować poszukiwanego. W ramach potrzeb PSP wybór kamery pod względem przydatności użycia w bezzałogowym statku powietrznym dokonuje się w trzech głównych obszarach zastosowań:

- obserwacja pożarów lasów i łąk,
- poszukiwanie zaginionych osób,
- pomiar temperatury.

Z uwagi na fakt specyficznego środowiska pracy, kamera musi umożliwiać pracę w szerokim zakresie temperatur (–40 do +80°C), tak aby zmiany podczas startu, lotu i lądowania w różnych warunkach meteorologicznych nie wpływały na pracę kamery. Zakres widmowy powinien być zawarty w przedziale największej emisji ciała ludzkiego (7,5–13 μm). Należy dokonać również doboru optymalnych parametrów obiektywów i sposobu regulacji ostrości (automatyczna lub obiektyw z dużą głębią ostrości). Z tego powodu kamera powinna mieć możliwość wymiany obiektywów. Rozdzielczość obrazu kamery powinna umożliwiać dokładną lokalizację zwierząt i ludzi z wysokości kilkudziesięciu metrów i na odległość kilkuset metrów. Ponieważ aparat będzie w ciągłym ruchu, uniemożliwi to wykonywanie ujęć statycznych. Aby zapewnić ostry obraz dobrej jakości, wymagane jest, żeby czas ekspozycji pojedynczej ramki obrazu był możliwie krótki, co również będzie brane pod uwagę przy dobieraniu kamery. Równolegle z torem obrazu termowizyjnego pozyskiwany będzie obraz w paśmie światła widzialnego. Pod względem wymagań środowiska pracy, kamera światła widzialnego powinna mieć zbliżone parametry jak kamera termowizyjna. Ocenia się, że największy udział masy w obciążeniu przypadnie na kamery i system ich sterowania, dlatego masa całkowita obu kamer musi być możliwie najmniejsza.

Należy używać sterowania kamerami, które powinno umożliwiać zdalną zmianę położenia w płaszczyźnie poziomej i pionowej względem aparatu latającego. Platforma, do której będą przytwierdzone kamery, powinna mieć

automatyczną stabilizację żyroskopową oraz uchwyty umożliwiające szybką wymianę przymocowanego sprzętu. Kluczową cechą zestawu przeznaczonego na potrzeby leśnictwa jest możliwość zastosowania zoomu optycznego. Wykonując przelot nad kompleksem leśnym na dużej wysokości, można obserwować obszar o sporej powierzchni. Gdy na trasie przelotu znajdzie się szczegół godny zainteresowania, nie ma potrzeby obniżania lotu, by go dostrzec. Jeśli dron jest wyposażony w kamerę z zoomem optycznym, wystarczy zbliżyć wzrok kamery na interesujący nas szczegół i dokładnie go obejrzeć. Zastosowanie kamer z zoomem optycznym daje możliwość uzyskania wysokiej jakości obrazu z dużej odległości. Przybliżanie w tym przypadku nie powoduje zmniejszenia rozdzielczości obrazu – w przeciwieństwie do zoomu cyfrowego, w którym to zbliżanie powoduje spadek rozdzielczości kadru.

W przypadku lotów inspekcyjnych, im większy zoom optyczny, tym lepiej. Jednym z najczęściej spotykanych rozwiązań jest kamera V18 producenta Yuneec, która oferuje 18-krotne zbliżenie optyczne. Otwiera to przed Służbą Leśną niespotykane dotąd możliwości dokładnego filmowania koron drzew z powietrza. Obok wiodącej pod względem możliwości zoomowania kamery V18, możliwość optycznego zbliżania dają też kamery Yuneec CGO4 oraz Sony RX100. Maksymalne zbliżenie optyczne oferowane przez te kamery to nieco ponad 3 razy, przy innych dodatkowych atutach możliwości konfiguracji ustawień, z dużym rozmiarem matrycy i wymiennymi jasnymi obiektywami, co wpływa dodatnio na jakość obrazu. Korzystając z kamery oferującej trzykrotny zoom, znajdując się kilkanaście metrów od drzewa lub nad drzewem, można obserwować je tak samo jak z odległości kilku metrów. Przy zastosowaniu urządzenia oferującego osiemnastokrotny zoom, przy tej samej odległości od drzewa można obserwować je tak, jakby znajdowało się kilkadziesiąt centymetrów od obiektywu. Dzięki temu pojawiła się możliwość wnikliwej inspekcji drzewostanu z powietrza. Dlatego najważniejszym elementem zestawu przeznaczonego dla leśnictwa jest wysokiej klasy kamera wideo umożliwiająca podgląd obrazu oraz jego nagrywanie.

Kamera do drona powinna też mieć możliwość objęcia jak największego obszaru i sfotografowania go w wysokiej rozdzielczości. Zebrane dane będą służyły do późniejszej analizy. Stabilność obrazu powinien zapewnić gimbal, czyli specjalne urządzenie składające się ze sterowni-

ka i dwóch lub trzech silników, które odpowiadają za utrzymanie pozycji kamery w czasie lotu. Nie bez znaczenia jest też możliwość optycznego zoomowania w czasie lotu. Taką opcję oferują m.in. kamery: CGO4, Sony RX100 oraz Yuneec V18.

Aby lasu starczyło dla wszystkich, trzeba się o niego troszczyć. Pomóc mogą w tym najnowsze zdobycze technologii. Jedną z takich nich są drony. Dzięki nim można przeprowadzać inspekcje drzewostanu, szacować straty wyrządzone przez szkodniki oraz wykonywać wiele innych czynności i zabiegów pielęgnacyjnych. Z uwagi na fakt udziału aparatu w wielkoobszarowych akcjach gaśniczych, istotnym parametrem, który powinien podlegać rejestracji, jest temperatura najbliższego otoczenia. Dron wyposażony w czujnik temperatury przekazujący informacje do systemu sterowania o nadmiernej temperaturze otoczenia może przekroczyć znamionową temperaturę jego pracy.

Ilustracja 2.
Powietrzna inspekcja drzewostanu – szacowanie strat wyrządzonych przez choroby i szkodniki

Źródło: Państwowa Straż Pożarna

Poza czujnikiem temperatury, należy wyposażyć BSP w czujnik promieniowania jonizacyjnego, który może być przydatny przy monitorowaniu promieniowania w okolicach ośrodków potencjalnie niebezpiecznych, takich jak granice sąsiadujące z elektrowniami jądrowymi i ośrodki badawcze wykorzystujące materiały radioaktywne, a także teren przygraniczny. Głównymi kryteriami doboru detektorów będą: masa, warunki pracy i czułość. Ponadto na pokładzie aparatu latającego nieodzowne jest zainstalowanie czujnika pola elektrycznego, który będzie wykorzystywany do wykrywania przeszkód na drodze w postaci linii wysokiego napięcia. Konstrukcja detektora pola elektrycznego przewidziana jest w ten sposób, aby sygnalizował on kierunek – zbliżanie się lub oddalanie od przeszkody. Istotnym rejestrowanym parametrem dodatkowym będzie pozycja współrzędnych geograficznych pobierana z zainstalowanego odbiornika GPS. Dane telemetryczne będą przekazywane w dodatkowym kanale transmisji cyfrowej aparat – operator. Rejestracji będą podlegać prędkość, długość i szerokość geograficzna oraz wysokość lotu. Określony zostanie zbiór sensorów obserwacyjnych, które będą wykorzystywane w opracowywanym systemie. Przewiduje się rozważenie następującego zakresu czujników:

- kamery światła dziennego,
- kamery termowizyjne,
- urządzenia zdalnego pomiaru temperatury – np. pirometry,
- systemy detekcji skażeń,
- systemy detekcji promieniowania radiologicznego,
- sensory środowiskowe (temperatura, wilgotność).

Oprócz wymienionych czujników, system będzie wyposażony w wiele różnorodnych sensorów niezbędnych dla awioniki pokładowej BSP (żyroskopy, akcelerometry, magnetometry, czujniki ciśnienia, odbiorniki nawigacji satelitarnej).

LOTY AUTONOMICZNE

Im dany BSP może dłużej latać, tym jego wydajność liczona względem inspekcjonowanej powierzchni w jednostce czasu oraz względem jednego akumulatora jest większa. Im dłuższy czas lotu, tym potrzebnych jest mniej akumulatorów oraz tym rzadziej trzeba wymieniać zasilanie w trakcie lotu.

Przykładowo, jeśli bezzałogowy statek powietrzny może wykonywać lot bez międzylądowania, który trwa 35 do 40 minut, w ciągu godziny będzie lądował tylko raz. Bezzałogowy statek powietrzny, który może latać 15–20 minut na jednym ładowaniu, będzie musiał wykonać co najmniej 3 starty i lądowania, a to w pewnym stopniu obniża wydajność pracy. Leśnictwo, jak żadna inna branża, wymaga cierpliwości i powtarzalności. Wykonanie przelotu dokładnie po takiej samej trasie kilkakrotnie jest właściwie niemożliwe bez udziału narzędzia do planowania trasy przelotu. Loty autonomiczne to olbrzymie ułatwienie w pilotowaniu bezzałogowych platform latających. Dzięki tej funkcji możliwe jest zaplanowanie konkretnej trasy przelotu, zapisanie jej i wykorzystanie zawsze wtedy, gdy będzie taka potrzeba. W trybie lotów autonomicznych bezzałogowy statek powietrzny samodzielnie startuje, wykonuje przelot po zaplanowanej trasie, a następnie ląduje w zaplanowanym miejscu. To wszystko odbywa się między innymi poprzez użycie Globalnego Systemu Pozycjonowania (GPS).

GPS to system nawigacyjny zbudowany przez Departament Obrony USA w latach 1982–1994 i zarządzany przez Agencję Kartograficzną oraz Dowództwo Sił Powietrznych USA. Pierwotnie opracowany był na potrzeby nawigacji amerykańskich łodzi podwodnych. Obecnie jest ogólnodostępny i dostarcza użytkownikom we wszystkich zakątkach świata, przez całą dobę, dokładnych informacji o czasie, położeniu oraz prędkości satelitów obsługujących system. GPS umożliwia określenie pozycji w jednolitym, trójwymiarowym układzie współrzędnych WGS-84 w każdych warunkach atmosferycznych. Zasadniczą częścią systemu są 24 satelity poruszające się po sześciu stacjonarnych orbitach kołowych, na wysokości 20 000 km nad Ziemią. Wszystkie one transmitują sygnał o częstotliwości 1575,42 MHz, używając niezależnych kodów do rozróżnienia sygnałów. Odbiorniki użytkowników systemu GPS mierzą odległość od satelitów przez pomiar czasu, jaki potrzebny jest na przesłanie sygnału do anteny odbiornika. Sygnał z satelity zawiera dane o statusie, tzw. efemerydę – dane orbitalne oraz charakterystyki zegarów. Na podstawie danych z efemerydy możliwe jest określenie położenia satelity w momencie transmisji, natomiast położenie odbiornika w przestrzeni trójwymiarowej jest obliczane przez triangulację – na podstawie pomiarów odległości do kilku (w zasadzie trzech) satelitów. Czwarty, dodatkowy, pomiar odległości umożliwia likwidację błędu zegara odbiornika.

Ilustracja 3.
Przykład wyznaczonej trasy lotu, tzw. wielokrotnego powtarzania lotu

Źródło: Youtube.com

System GPS tworzy nową, rewolucyjną jakość orientacji w terenie, nawigacji oraz określania miejsca położenia, wzbogacając znajdujące się dotychczas w powszechnym użyciu narzędzia, takie jak mapa topograficzna, kompas oraz sekstans. Należy przyjąć, że w najbliższym czasie użycie tego narzędzia będzie tak powszechne, jak samochodu, kalkulatora czy Internetu. Dzięki osiągnięciom elektroniki oferowane są coraz mniejsze i tańsze odbiorniki GPS. System już dzisiaj pozwala zaspokoić potrzebę natychmiastowego poznania swego położenia oraz odpowiedzieć na pytanie, gdzie znajduje się poszukiwany przez nas adres.

Po zakończeniu misji autonomicznej i wykonaniu serii zdjęć bądź nagrania wideo w wysokiej rozdzielczości do dyspozycji pozostaje duża ilość materiałów, które można przeanalizować. Lot autonomiczny podobnie jak manualny daje obserwatorom możliwość podglądu obrazu przesyłanego z pokładu BSP w czasie rzeczywistym.

SYSTEM ZAPOBIEGAJĄCY KOLIZJI Z LINIAMI ENERGETYCZNYMI

Zaletą bezzałogowych statków powietrznych jest znaczna prędkość przemieszczania się oraz możliwość prowadzenia działań w terenie trudno dostępnym. Istniejące ograniczenia natury prawnej oraz prowadzenie skutecznych działań rozpoznawczych wymagają lotów na niewielkiej wysokości, nieprzekraczającej kilkudziesięciu metrów. Sytuacja taka wiąże się jednak z ryzykiem kolizji z różnymi obiektami, a zwłaszcza z napowietrznymi liniami przesyłowymi wysokiego napięcia. Ryzyko kolizji z budowlami i wysokimi drzewami jest stosunkowo niewielkie, ponieważ ich wymiary geometryczne są znaczne i spostrzeżenie ich przez operatora systemu jest stosunkowo łatwe.

Ilustracja 4.
Lokalizacja przeszkody terenowej poprzez detektor sygnału częstotliwości

Źródło: Państwowa Straż Pożarna

Charakterystyczne dla współczesnej cywilizacji wielkie zapotrzebowanie na energię elektryczną spowodowało, że napowietrzne linie przesyłowe wysokiego napięcia są obecne niemal wszędzie w zasięgu wzroku. Stosunkowo dobrze widoczne są kratowe konstrukcje słupów, w mniejszym stopniu rozpoznawalne są słupy rurowe, same zaś przewody są bardzo słabo widoczne w warunkach obserwacji terenu przez operatora systemu za pomocą

kamery. Prędkość poruszania się bezzałogowych statków powietrznych nie przekracza na ogół 50 m/s, w związku z czym należy przyjąć, że wykrycie i lokalizacja przeszkody powinny nastąpić z odległości przynajmniej 500 m przed nią. Stanowi to wytyczną do konstrukcji układu wykrywającego i lokalizującego linię napowietrzną. Wykrycie linii przesyłowej następuje, gdy odebrany zostanie sygnał częstotliwości 50 Hz, do pełnej lokalizacji położenia kątowego linii potrzebna jest znajomość kierunku, z którego pochodzi sygnał emitowany przez linię oraz znajomość jej odległości od systemu monitorującego. Z punktu widzenia bezpieczeństwa lotów w aspekcie możliwej kolizji obiektu latającego, napowietrzne linie przesyłowe są instalacjami o zróżnicowanych wymiarach geometrycznych, z których największe znaczenie mają wysokość zawieszenia linii, wysokość słupów, a także ich konstrukcja i odległości między nimi. Wykrywanie i lokalizacja linii wysokiego napięcia możliwe są dzięki temu, że są one źródłem promieniowania elektromagnetycznego niskiej częstotliwości (w Polsce 50 Hz). Realizacja celu obarczona jest wieloma trudnościami; podstawowym utrudnieniem jest fakt, że natężenie pola elektromagnetycznego bardzo szybko maleje w miarę oddalania się od osi linii. Ponadto badania wykazały, że sygnał użyteczny jest bardzo silnie tłumiony przez różne zakłócenia, głównie niskiej częstotliwości, które są indukowane na skutek poruszania się układu pomiarowego w ziemskim polu magnetycznym.

W systemach stosuje się magnetometry typu fluxgate lub magnetoinductive oraz ich aplikacje umożliwiające wykrycie linii przesyłowej. Czujnikiem jest uzwojenie nawinięte na rdzeniu ferromagnetycznym, który zmienia swą przenikalność magnetyczną pod wpływem zmian ziemskiego pola magnetycznego.

Zazwyczaj wysokość słupów wysokiego napięcia jest proporcjonalna do wartości napięcia linii i na ogół mieści się w granicach 30–65 m, przy czym większe wysokości dotyczą linii najwyższych napięć. Wyznaczenie odległości linii wymaga znajomości napięcia, pod którym się ona znajduje, zakładając jednak, że istotnym zagrożeniem dla lotu rozważanego obiektu są linie wysokie (powyżej 30 m), wstępne prace i obliczenia można ograniczyć do linii 220 lub nawet 400 kV, przyjmując, że każdy manewr uniknięcia kolizji powinien doprowadzić do zwiększenia wysokości lotu powyżej przyjętej maksymalnej przewidywanej wysokości linii, czyli około 65 m. Przy tak przyjętym założeniu wystarczająca jest znajomość kierunku, na którym

znajduje się przeszkoda, rozpoczęcie manewru omijania następuje po sygnale układu potwierdzającego znalezienie się obiektu latającego w pobliżu rozpatrywanej instalacji.

W przypadku linii wysokich (najwyższych napięć) celowe może się okazać rozważenie manewru polegającego na przelocie obiektu latającego poniżej przewodów linii stanowiącej przeszkodę. Przeznaczony do monitoringu terenu w aspekcie zagrożeń pożarowych bezzałogowy statek powietrzny wraz z zainstalowanymi na pokładzie kamerami jest częścią wielowymiarowego, najczęściej nieautonomicznego układu regulacji. Ze względu na zasygnalizowane w poprzednim punkcie zagrożenia kolizją z linią przesyłową, zadaniem znajdującego się na jego pokładzie układu pomiarowego jest wykrycie będącej pod napięciem i przewodzącej prąd linii, przeprowadzenie lokalizacji jej położenia oraz poinformowanie operatora systemu lub spowodowanie stosownych działań autopilota w celu uniknięcia kolizji. Rozwiązanie przedstawionego problemu wymaga znajomości właściwości dynamicznych bezzałogowego statku powietrznego, doboru właściwego układu pomiarów i regulacji oraz możliwości wykrycia celu i lokalizacji jego położenia kątowego. Należy przeprowadzić analizę dynamiki bezzałogowego statku powietrznego, której efektem będzie opracowanie dla niego odpowiedniej strategii działania i układów automatycznej regulacji dla autopilota dla stanu obserwacji i zagrożenia kolizją. W dalszej kolejności konieczne jest przeprowadzenie badań symulacyjnych pracy BSP wraz z opracowanym układem regulacji. Analiza przeprowadzonych badań zmierzać będzie do oceny jakości pracy BSP wyposażonego w zaprojektowane układy pomiarów i regulacji zgodnie z kryteriami obowiązującymi w teorii sterowania.

WIEŻA CZY DRON?

W 2013 roku doszło do 126 406 pożarów, z czego 3,77% przypada na pożary lasu – podaje Komenda Główna Państwowej Straży Pożarnej (KG PSP)[2]. Paliła się głównie ściółka leśna, ale strażacy odnotowali również kilkaset pożarów pojedynczych drzew. Każda akcja gaśnicza wymaga zaangażowania odpowiednich sił i środków, w zależności od okoliczności wybuchu pożaru. Inaczej gasi się pole torfowe, inaczej las z przewagą drzew

[2] Dane statystyczne KG PSP: www.kgpsp.gov.pl.

iglastych. Bardzo pomocne okazują się wówczas zintegrowane systemy wspierania zarządzania kryzysowego. Siłą systemu jest jednak mechanizm automatycznego wykrywania pożarów na obszarach otwartych i leśnych. Wysokiej klasy kamery ulokowane na wieżach obserwacyjnych przesyłają obraz do systemu centralnego.

Ilustracja 5.
Przykład betonowych wież obserwacyjnych

Źródło: Lasy Państwowe

Tam wykrywane są typowe objawy pożarowe, np. dym. Biorąc pod uwagę położenie poszczególnych wież oraz kąt, pod którym widać dym, system określa miejsce pożaru. To jest, owszem, metoda prosta i skuteczna, ale droga. Wymaga wszak budowy betonowej wieży w środku leśnej głuszy, o masie fundamentu porównywalnej z masą samej wieży, do której trzeba doprowadzić prąd lub zadbać o oszczędny agregat prądotwórczy. Wie-

ża zmienia też krajobraz okolicy i nie można jej posadowić w rezerwatach przyrody. W Polsce leśnicy postawili również na budowę betonowych wież obserwacyjnych o wysokości od 35 do 60 m. Przy dobrych warunkach widoczność z tych wysokości sięga nawet 20 km. Jeśli przyjmiemy, że każde nadleśnictwo (430 w Polsce) stawia po dwie lub trzy takie wieże, to winniśmy z czasem doczekać się od 860 do 1290 budowli górujących nad lasami (z wyłączeniem parków narodowych i ścisłych rezerwatów przyrody). Na razie dominuje model zlecania monitorowania sytuacji pożarowej tzw. Zakładom Usług Leśnych, które oddelegowują do pracy na wieżach swoich pracowników. Zaczyna się też stawiać wieże całkowicie zautomatyzowane, wyposażone w kamery i radiolinie, umożliwiające przesyłanie obrazu z kamer bezpośrednio do nadleśnictwa. Na takie rozwiązanie zdecydowało się m.in. Nadleśnictwo Biłgoraj[3]. Obraz z masztu w Rogóźniance przesyłany jest do wieży na ul. Zamojskiej, a następnie do Nadleśnictwa. Obserwatorzy nie będą już musieli siedzieć na wieżach. Jedynie w przypadku awarii kamery. Inwestycja kosztowała 1,26 mln zł. Z prostego rachunku wynika, że 1000 takich wież kosztowałoby fundusz leśny, gromadzony z zysków Lasów Państwowych, oraz poszczególne nadleśnictwa ok. 126 mln zł! Nawet jeśli te obsługiwane przez człowieka zostaną w pełni zautomatyzowane i tym samym odpadną koszty budowy nowych wież, to koszty i tak przekraczają możliwości finansowe Państwowego Gospodarstwa Leśnego Lasy Państwowe. Już nie mówiąc o czasie, ponieważ zanim PGL LP dostawiłoby do tej sieci ostatnią wieżę, musiałoby wymieniać zużyty sprzęt z tych najstarszych. Rozwiązanie nasuwa się samo.

Należy zaufać szybkiemu rozwojowi techniki i zaprząc do kompleksowej ochrony przeciwpożarowej lasów obserwację satelitarną oraz sieci czujników posadowione na różnego rodzaju robotach, w tym dronach. Być może na pierwszy ogień (nomen omen) winny pójść parki narodowe, akurat pozostające poza jurysdykcją PGL LP, w których nie można budować betonowych wież. Wyobraźmy sobie sytuację, w której nad połaciami Kampinoskiego Parku Narodowego albo nad Puszczą Białowieską w czasie letnich upałów unoszą się drony wyposażone w odpowiednie kamery. Ich lot śledzą obserwatorzy w centrum koordynacyjnym służb, korzystający

[3] http://www.bilgorajska.pl/aktualnosc,7481,0,0,0,Nowe-wieze-do-obserwacji-lasu.html.

dodatkowo ze zobrazowań satelitarnych. System informatyczny na bieżąco wykrywa zmiany w obrazach zarejestrowanych przez satelity i BSP. Tak oto znacznie wzrasta zdolność do wykrycia zarzewia ognia. Skraca się czas podjęcia akcji. W konsekwencji zamiast gasić pożar lasu, mielibyśmy do czynienia z akcją gaszenia np. traw. Koszty finansowe i społeczne, jak też przyrodnicze zdecydowanie niższe od betonowych wież.

PODSUMOWANIE

Za pomocą bezzałogowych statków powietrznych można szybciej i efektywniej obserwować tereny leśne o zdecydowanie większej powierzchni niż tradycyjnymi sposobami. Drony mogą przyczynić się także do znacznej redukcji kosztów niektórych operacji. Obecnie inspekcje lasów przeprowadzane z powietrza wiążą się z wynajęciem samolotu wraz z załogą lub z wynajęciem motolotniarza. Korzystając z BSP, można takie inspekcje przeprowadzać samodzielnie, nie będąc zależnym od innych osób oraz firm. Bezzałogowy statek powietrzny ma możliwość przesyłania obrazu w czasie rzeczywistym, tak więc idealnie nadaje się do monitorowania zagrożenia pożarowego obszarów trudno dostępnych, takich jak lasy, torfowiska, tereny bagienne. Zaletą systemu jest możliwość szybkiego przemieszczania się z pominięciem tras komunikacyjnych.

Ważną cechą dronów przeznaczonych dla leśnictwa jest czas trwania lotu na jednym akumulatorze. Zgodnie z tym, o czym było już wspomniane w niniejszej publikacji, dłuższy czas lotu poprawia zdolności operacyjne BSP i umożliwia szybszą oraz bardziej wydajną inspekcję. Nie bez znaczenia jest też liczba akumulatorów zapasowych. W przypadku BSP użytkowanych w lasach, rozsądne minimum to 3 dodatkowe komplety akumulatorów. Przy założeniu, że w miejscu lotów dostępna jest ładowarka, zapewnienie takiej liczby akumulatorów umożliwia właściwie ciągłą pracę. Monitorowanie zagrożeń pożarowych dzieli się na dwa elementy: wykrywanie i lokalizację ognisk spalania (wielogodzinne patrolowanie obszarów zagrożonych pożarem) oraz przesyłanie informacji w czasie rzeczywistym do stanowiska pracy operatora. Informacja obrazowa z kamer pokładowych TV lub IR służy do bardzo szybkiego i precyzyjnego określenia sytuacji pożarowej (dym, spalanie płomieniowe i bezpłomieniowe) oraz miejsca pożaru (aktualna pozycja punktu obserwowanego przez głowicę optoelektroniczną BSP jest przesyłana do stacji kierowania i kontroli).

Pożary lasów mają dużą tendencję do szybkiego rozprzestrzeniania się. W sytuacji takiej ważną rolę odgrywają systemy BSP, które mogą być używane do przesyłania informacji obrazowych z przebiegu i postępu akcji gaszenia pożaru. Zdolność oceny sytuacji pożarowej przez kierującego działaniami ratowniczymi jest dość ograniczona ze względu na bliskość drzew, natomiast podgląd na trójwymiarowo przedstawiony obraz z powietrza umożliwia bardziej efektywne podejmowanie decyzji, jak również rozplanowanie użycia sił i środków gaśniczych do gaszenia pożaru. Rzeczywisty obraz może być przesyłany do dowódców poszczególnych odcinków gaśniczych (bojowych), co zwiększa komfort pracy oraz bezpieczeństwo ratowników i osób postronnych. System BSP ma zastosowanie również w monitorowaniu stanu poziomu wód (rzek, jezior, rozlewisk) oraz terenów zagrożonych powodzią i podtopieniami. Za pomocą kamer znajdujących się na pokładzie BSP można sprawdzać poziom wody w akwenach (zbliżenie i obraz skali wodowskazu), stan wałów przeciwpowodziowych oraz rozwój sytuacji, a w tym prędkość i kierunek przemieszczania się fali powodziowej. Bezzałogowe statki powietrzne znajdują zastosowanie przy kierowaniu działaniami ratowniczymi i prewencyjnymi. Za pomocą przesyłanych współrzędnych lokalizuje się osoby poszkodowane lub zagrożone. Posiadanie takiego systemu pozwoliłoby na uniknięcie wielu katastrof i zmniejszenie skutków klęsk żywiołowych. Budowa mobilnego systemu monitorowania zagrożeń pożarowych na terytorium Polski w oparciu o bezzałogowe statki powietrzne wymaga pilnego zrealizowania m.in. opracowania cyfrowej mapy zagrożenia pożarowego lasów na podstawie danych satelitarnych oraz opracowania scenariuszy i algorytmów realizowania misji za pomocą bezzałogowych statków powietrznych.

Źródła prawa

Rozporządzenie Ministra Infrastruktury i Budownictwa z dnia 8 sierpnia 2016 roku zmieniające rozporządzenie w sprawie wyłączenia zastosowania niektórych przepisów ustawy – Prawo lotnicze do niektórych rodzajów statków powietrznych oraz określenia warunków i wymagań dotyczących używania tych statków (Dz.U. poz. 1317).

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 7 czerwca 2010 roku w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz.U. nr 109 poz. 719).

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 września 2000 roku w sprawie szczegółowych zasad wyposażenia jednostek organizacyjnych Państwowej Straży Pożarnej (Dz.U. nr 93 poz. 1035).

Rozporządzenie Ministra Środowiska z dnia 22 marca 2006 roku w sprawie szczegółowych zasad zabezpieczenia przeciwpożarowego lasów (Dz.U. nr 58 poz. 405 z późn. zm.).

WACŁAW BRZĘK
Wyższa Szkoła Gospodarki Euroregionalnej
im. Alcide De Gasperi w Józefowie
waclawbrzek@gmail.com

BEZPIECZEŃSTWO KOSMETYKÓW W ŚWIETLE PRAWA POLSKIEGO ORAZ UNIJNEGO

THE SAFETY OF COSMETICS IN LIGHT OF POLISH AND EUROPEAN UNION LAW

ABSTRACT

Cosmetics have become the objects of a common use. Their manufacturing is also a great and profitable branch of production. Hence, the great importance of the issue concerned with their use, in light of health safety of the potential user. It is impossible to discuss in a single elaboration all aspects (technical, organizational and legal) related to the safety of cosmetics. Therefore, an attempt to present only the legal conditions based on the provisions of Polish law and EU law was taken. The first part presents the definition of cosmetic (cosmetic product) in Polish and EU law, as well as the US one. It turns out that under this term lies – in the case of Polish and the European Union regulations – as many as 20 groups of different products. The second part discusses the legal regulations related to the safety of cosmetics, addressed directly to the manufacturer. For it is the manufacturer who in the first place is responsible for the marketing of safe cosmetic (cosmetic product). In the final part of the elaboration, legal regulations related to the functioning of the supervisory authorities (State Sanitary Inspection) and to labeling, falsification and regularities of cosmetics' trading (Trade Inspection) were presented.

Keywords: *cosmetics, cosmetic product, cosmetic law, Poland, the European Union*

STRESZCZENIE

Dawno już kosmetyki stały się przedmiotami powszechnego użytku. Ich wytwarzanie to również wielka i dochodowa gałąź produkcji. Stąd też niebagatelnego znaczenia nabiera problem ich bezpieczeństwa dla zdrowia potencjalne-

go użytkownika. W jednym opracowaniu nie sposób jest omówić wszystkich aspektów (technicznych, organizacyjnych czy prawnych) związanych z bezpieczeństwem kosmetyków. Dlatego podjęto w nim próbę przedstawienia jedynie prawnych uwarunkowań bezpieczeństwa kosmetyków w oparciu o przepisy prawa polskiego oraz unijnego. W pierwszej części przedstawiona została definicja kosmetyku (produktu kosmetycznego) w prawie polskim i unijnym, a także w USA. Okazuje się, że pod tym pojęciem kryje się – w przypadku przepisów polskich oraz Unii Europejskiej – aż 20 grup różnorodnych produktów. W części drugiej omówione zostały prawne regulacje związane z bezpieczeństwem kosmetyków skierowane bezpośrednio do producenta. Bowiem to producent w pierwszej kolejności jest odpowiedzialny za wprowadzenie do obrotu bezpiecznego kosmetyku (produktu kosmetycznego). Wreszcie – w części końcowej – przedstawiono regulacje prawne związane z funkcjonowaniem organów nadzoru nad bezpieczeństwem produkcji (Państwowa Inspekcja Sanitarna) oraz w zakresie znakowania, zafałszowań i prawidłowości obrotu kosmetyków (Inspekcja Handlowa).

Słowa kluczowe: *kosmetyk, produkt kosmetyczny, prawo kosmetyczne, Polska, Unia Europejska*

WPROWADZENIE

W ostatnich latach wartość produkcji i sprzedaży kosmetyków w Polsce rośnie, licząc rok do roku, zwykle o kilkanaście procent. Prognozy branżowe na lata 2013–2016 zakładały wzrost wartości polskiego rynku kosmetycznego z 20 do 26 mld zł. Jeśli chodzi o wielkość, polski rynek kosmetyków plasowany jest na szóstym miejscu w Europie pod względem wartości sprzedaży, a także eksportu (M. Kasprzak, 2016). Polskie kosmetyki dostępne są już w 130 krajach. Około 60% polskich produktów kosmetycznych eksportowanych jest do krajów Unii Europejskiej. Kolejne 23% sprzedawane jest w krajach Europy Środkowej i Wschodniej. Głównym ich importerem pozostaje Rosja, w której polskie produkty znane są konsumentom od wielu lat. Polskie produkty dostępne są nie tylko w Europie, ale również w drogeriach i perfumeriach m.in. takich krajów, jak Trynidad i Tobago, Nowa Zelandia, Chile czy emiratu Dubaj (K. Bochner, K. 2013).

Z kolei w UE każdego roku około 25% produktów kosmetycznych będących w obrocie to nowości. Europa jest światowym liderem w branży kosmetycznej, a jej rynek detaliczny ma wartość 77 mld euro. Europa eksportuje jedną trzecią wszystkich produktów kosmetycznych sprzedawanych na

całym świecie [Sprawozdanie Komisji dla parlamentu z dnia 19.9.2016 roku COM(2016) 580 final, s. 1]. Szacuje się, że przy produkcji oraz dystrybucji kosmetyków w Europie zatrudnionych jest ponad pół miliona osób (M. Borkowski, 2015, s. 13).

Produkty kosmetyczne są również wprowadzane przez producentów z krajów trzecich na rynek europejski, w tym i rynek polski. Część z nich wprowadzana jest nielegalnie. Z danych opublikowanych w 2015 roku wynika, że służby celne UE zatrzymały podróbki produktów kosmetycznych o wartości ponad 42 mln euro. Produkty te pochodziły głównie z Chin, Malezji, Turcji, Singapuru oraz Hongkongu (Report on EU customs... 2015, passim).

Rodzi się więc w tym miejscu pytanie o bezpieczeństwo kosmetyków. Jakie są europejskie oraz polskie unormowania prawne w tym zakresie? Antycypując szczegółowe rozważania na ten temat, wypada w tym miejscu stwierdzić, że obecnie w sensie normatywnym bezpieczeństwo kosmetyków na terenie UE opiera się na rozwiązaniach prawnych, których celem nadrzędnym jest zapewnienie, aby każdy kosmetyk, który trafia na rynek, był bezpieczny dla zdrowia ludzi.

W dalszych częściach opracowania przedstawiony zostanie przegląd polskich oraz unijnych regulacji prawnych związanych z bezpieczeństwem kosmetyków (jak chce polski ustawodawca) czy też produktów kosmetycznych (jak to określa prawodawca unijny).

DEFINICJE KOSMETYKU W PRAWIE POLSKIM I WSPÓLNOTOWYM

W literaturze przyjmuje się, że słowo „kosmetyk" wywodzi się od greckiego *kosmetikos* oznaczającego sztukę upiększania (K. Szewczyk, J. Młynarczyk, 2015, s. 61). Natomiast w sensie językowym rzeczownik „kosmetyk" to środek kosmetyczny służący do upiększania i pielęgnowania ciała (Słownik języka polskiego, 1978, t. 1, s. 1021). Z kolei przymiotnik „kosmetyczny" to: dotyczący kosmetyki, kosmetyków; służący do pielęgnowania ciała i urody; upiększający (Słownik języka polskiego, 1978, t. 1, s. 1021).

W prawodawstwie polskim pierwszym aktem prawa dotyczącym kosmetyków było rozporządzenie Prezydenta RP z dnia 22 marca 1928 roku o dozorze nad artykułami żywności i przedmiotami użytku. Nie definiowało ono, czym jest kosmetyk. W zamian posługiwało się określeniem „środek kosmetyczny". Określenie to również nie zostało zdefiniowane. Natomiast

akt ten m.in. stanowił, w jakich przypadkach należy uznać, że środek kosmetyczny jest szkodliwy (art. 2), zepsuty (art. 3), podrobiony (art. 4), sfałszowany (art. 5) bądź fałszywie oznaczony (art. 6).

Po raz pierwszy pojęcie „środek kosmetyczny" w prawie polskim zostało zdefiniowane w rozporządzeniu Ministra Opieki Zdrowotnej z dnia 25 czerwca 1934 roku wydanym w porozumieniu z Ministrem Przemysłu i Handlu o dozorze nad wyrobem i obiegiem środków kosmetycznych. Zgodnie z brzmieniem § 1 wspomnianego rozporządzenia: „środki kosmetyczne (...) są to środki do oczyszczania, barwienia i pielęgnowania skóry, włosów, paznokci oraz jamy ustnej i zębów". Zostały one – zgodnie z § 2 cytowanego rozporządzenia – podzielone na trzy grupy:

1) środki kosmetyczne do skóry (kremy, mydła toaletowe i mydła do golenia, pudry, środki przeciw poceniu się, szminki, środki do masażu i do nacierania, środki do pielęgnowania paznokci, dodatki do kąpieli z wyjątkiem środków leczniczych),
2) środki kosmetyczne do włosów (mydła do mycia włosów i głowy, płyny do włosów, olejki, brylantyny, pomady, środki do barwienia włosów, środki na odwłosienie),
3) środki kosmetyczne do jamy ustnej i zębów (płyny i tabletki do płukania ust i zębów, proszki, pasty i mydełka do zębów, ołówki, pomadki i płyny do warg).

Listę powyższych środków kosmetycznych rozszerzyło rozporządzenie Ministra Opieki Społecznej z dnia 18 stycznia 1939 roku wydane w porozumieniu z Ministrem Przemysłu i Handlu o dozorze nad wyrobem i obiegiem środków kosmetycznych. Utrzymano w nim podział na trzy grupy produktów kosmetycznych, ale zmieniono ich nazwy oraz dodano w poszczególnych grupach nowe produkty. Stąd, zgodnie z brzmieniem § 2 wspomnianego rozporządzenia, do grupy środków kosmetycznych do skóry i paznokci zaliczano: mydła toaletowe oraz mydła, proszki, kremy i pasty do golenia, kremy, pasty, emulsje, galaretki, olejki i balsamy, pudry (stałe i w płynie), szminki (barwiczki), maski, plastry, papiery kosmetyczne, masy plastyczne i emalie, środki przeciw poceniu się, płyny i octy toaletowe, środki do masażu i do nacierania, sole i dodatki do kąpieli (z wyjątkiem leczniczych), środki na odciski, środki do pielęgnowania, polerowania, barwienia paznokci, lakiery, pomadki oraz środki do zmywania lakierów i pomadek.

Do grupy środków kosmetycznych do włosów zaliczono: mydła i szampony do włosów i głowy, płyny do włosów i skóry głowy, olejki, brylantyny i pomady, środki do barwienia włosów, środki na odwłosienie, środki do trwałej ondulacji.

Do grupy środków kosmetycznych do jamy ustnej i zębów zaliczono zaś: płyny i tabletki do płukania jamy ustnej i zębów, proszki, pasty i mydełka do zębów oraz ołówki, pomadki i płyny do warg.

Unormowania te przetrwały do 12 maja 2002 roku, kiedy to weszła w życie ustawa z dnia 30 marca 2001 roku o kosmetykach. Jej celem było dostosowanie polskich rozwiązań prawnych odnoszących się do wytwarzania i obrotu kosmetyków do wymagań jednolitego rynku Unii Europejskiej (Uzasadnienie do rządowego projektu ustawy o kosmetykach, s. 13).

Wedle wspomnianej ustawy kosmetykiem jest każda substancja chemiczna lub mieszanina przeznaczone do zewnętrznego kontaktu z ciałem człowieka: skórą, włosami, wargami, paznokciami, zewnętrznymi narządami płciowymi, zębami i błonami śluzowymi jamy ustnej, których wyłącznym lub podstawowym celem jest utrzymanie ich w czystości, pielęgnowanie, ochrona, perfumowanie, zmiana wyglądu ciała lub ulepszenie jego zapachu (art. 2 ust. 1).

Definicja ta nie różniła się prawie wcale od definicji kosmetyku zawartej w dyrektywie Rady (76/768/EWG) z dnia 27 lipca 1976 roku w sprawie zbliżenia ustawodawstwa państw członkowskich dotyczących kosmetyków. Zgodnie z art. 1 ust. 1 wspomnianej dyrektywy kosmetyk oznacza każdy produkt przeznaczony do kontaktu z zewnętrznymi częściami ciała ludzkiego (skórą, owłosieniem, paznokciami, wargami i zewnętrznymi narządami płciowymi) lub zębami i błonami śluzowymi jamy ustnej, którego wyłącznym lub głównym zadaniem jest ich czyszczenie, perfumowanie lub ochranianie, aby utrzymywać je w dobrym stanie, zmieniać ich wygląd lub poprawiać zapachy ciała.

Nie różni się ona zasadniczo także od późniejszej definicji produktu kosmetycznego zawartej w przepisach prawa wspólnotowego, konkretnie w rozporządzeniu Parlamentu Europejskiego i Rady (WE) nr 1223/2009 z dnia 30 listopada 2009 roku dotyczącym produktów kosmetycznych. Zgodnie z unormowaniami tego rozporządzenia: „produkt kosmetyczny oznacza każdą substancję lub mieszaninę przeznaczoną do kontaktu z zewnętrznymi częściami ciała ludzkiego (naskórkiem, owłosieniem, paznokciami, wargami

oraz zewnętrznymi narządami płciowymi) lub z zębami oraz błonami śluzowymi jamy ustnej, którego wyłącznym lub głównym celem jest utrzymywanie ich w czystości, perfumowanie, zmiana ich wyglądu, ochrona, utrzymywanie w dobrej kondycji lub korygowanie zapachu ciała" (art. 2 ust. 1 lit. a). Jednak w cytowanym rozporządzeniu wprowadzono wyraźne zastrzeżenie, że nie jest uznawana za produkt kosmetyczny substancja lub mieszanina przeznaczona do spożycia, wdychania, wstrzykiwania lub wszczepiania do ciała ludzkiego (art. 2 ust. 2). Czyli kosmetykiem jest produkt w postaci określonych w przepisach prawa substancji bądź ich mieszanin, który oddziałuje wyłącznie poprzez zewnętrzny kontakt z ciałem człowieka.

Polska czy wspólnotowa definicje normatywne kosmetyku (produktu kosmetycznego) to jedne z wielu funkcjonujących w obiegu międzynarodowym. Zdecydowana większość państw we własnym zakresie definiuje w odpowiednich aktach prawnych to pojęcie. Na przykład w USA definicja kosmetyku jest węższa. Zgodnie z ustawą o żywności, lekach i kosmetykach (Federal Food, Drug, and Cosmetic Act) z 1938 roku kosmetykiem jest produkt przeznaczony do wcierania, spryskiwania, rozpylania, wprowadzania do wnętrza lub innego aplikowania do ciała ludzkiego lub jego części, w celu czyszczenia, upiększenia, zwiększenia atrakcyjności bądź zmiany wyglądu (D. Dąbrowska, J. Kaniewski, s. 54). Stąd może na pierwszy rzut oka budzić zdziwienie fakt, że szereg współczesnych produktów kosmetycznych produkowanych i oferowanych konsumentom unijnym traktowanych jest przez administrację Stanów Zjednoczonych jako leki OTC (*over-the-counter drugs*), czyli leki bez recepty. To rodzi określone skutki w sferze prawnej, organizacyjnej i w zarządzaniu dla firm kosmetycznych mających siedzibę w państwie na terenie UE, a chcących eksportować swoje produkty do Stanów Zjednoczonych.

Warto w tym miejscu zaznaczyć, że polski ustawodawca zdawał sobie od początku sprawę, że tak określona normatywna definicja kosmetyku obejmuje bardzo szeroką gamę produktów. Dlatego też zobowiązał w art. 2 ust. 2 wspomnianej wyżej ustawy ministra właściwego do spraw zdrowia do określenia, drogą rozporządzenia, najczęściej występujących kategorii produktów będących kosmetykami. Minister zdrowia wywiązał się z nałożonego nań obowiązku, wydając w dniu 16 czerwca 2003 roku rozporządzenie w sprawie określenia kategorii produktów będących kosmetykami. Rozporządzenie to określa 20 grup kosmetyków najczęściej występujących na rynku.

Zgodnie z brzmieniem § 2 wspomnianego rozporządzenia są to: kremy, emulsje, płyny, żele i oliwki oraz balsamy do skóry, maseczki do twarzy, z wyjątkiem maseczek służących do peelingu chemicznego, podkłady barwiące, pudry do makijażu, pudry po kąpieli, pudry higieniczne, mydła toaletowe, a także mydła dezodoryzujące, perfumy, wody toaletowe i kolońskie, środki do kąpieli i pod prysznic, środki do depilacji, dezodoranty i środki przeciw poceniu, środki do pielęgnacji włosów, w tym środki do barwienia i rozjaśniania, do trwałej ondulacji, do prostowania i utrwalania, do układania, do mycia, odżywki, do utrwalania fryzury, środki do golenia, środki do makijażu i demakijażu, środki przeznaczone do pielęgnacji i malowania ust, środki do pielęgnacji zębów i jamy ustnej, środki do pielęgnacji i malowania paznokci, środki do higieny zewnętrznych narządów płciowych, środki do opalania i chroniące przed promieniowaniem ultrafioletowym, środki do samoopalania, środki do rozjaśniania skóry oraz środki przeciw zmarszczkom.

Powyższy wykaz obejmuje jedynie najczęściej występujące grupy kosmetyków. Nie da się więc z góry wykluczyć, że w przyszłości mogą być do niego dołączone kolejne, o ile będą spełniać wymogi określone w art. 2 ust. 1 ustawy o kosmetykach. Co więcej, kosmetykiem będzie też każdy produkt, niewymieniony w przedstawionym wykazie, o ile tylko będzie spełniał wymogi cytowanej ustawy.

Podobnie postąpiono w prawodawstwie unijnym. Wspomniana wcześniej dyrektywa Rady z 1976 roku nie stworzyła zamkniętej raz na zawsze definicji kosmetyku. W art. 1 ust. 1 wyraźnie zaznaczono, że za kosmetyki w rozumieniu definicji zawartej w tym artykule uważane są w szczególności produkty wymienione w załączniku 1. Załącznik ten, zatytułowany „Przykładowy wykaz kosmetyków według kategorii", zawierał 20 grup produktów. Porównanie tekstu rozporządzenia Ministra Zdrowia z dnia 16 czerwca 2003 roku w sprawie określenia kategorii produktów będących kosmetykami ze wspomnianym załącznikiem 1 do dyrektywy Rady z 1976 roku pozwala wyciągnąć wniosek o identyczności treści § 2 polskiego rozporządzenia z owym załącznikiem. Taki stan rzeczy był wynikiem dostosowywania prawa polskiego do prawa unijnego w przededniu wstąpienia Polski do UE. Obecnie obowiązujące rozporządzenie PE i Rady (WE) nr 1223/2009 nie zawiera już takiego osobnego wykazu. Jedynie w pkt 7 preambuły rozporządzenia wymienione są grupy produktów, którym można przypisać miano produktów kosmetycznych.

Warto w tym miejscu nadmienić, że prócz wspomnianych wyżej wykazów na terenie UE funkcjonują także i inne klasyfikacje kategorii kosmetyków, czy jak chce unijny prawodawca – produktów kosmetycznych. Przykładem może być Wspólna Taryfa Celna obowiązująca w UE. Posługuje się ona określeniami „preparaty perfumeryjne, kosmetyczne lub toaletowe" oraz „mydła". Zgodnie z logiką konstrukcji owej taryfy oraz nomenklatury taryfowej i statystycznej w sekcji VI, dziale 33, umieszczono: olejki eteryczne i rezinoidy, preparaty perfumeryjne, kosmetyczne lub toaletowe. Dział ten podzielono m.in. na poddziały: preparaty kosmetyczne lub upiększające oraz preparaty do pielęgnacji skóry (inne niż leki), włącznie z preparatami przeciwsłonecznymi lub do opalania, preparaty do manicure lub pedicure; preparaty do włosów; preparaty do higieny zębów lub jamy ustnej, włącznie z pastami i proszkami do przytwierdzania protez, nici dentystyczne do czyszczenia międzyzębowego; preparaty stosowane przed goleniem, do golenia lub po goleniu, dezodoranty osobiste, preparaty do kąpieli, depilatory i pozostałe preparaty perfumeryjne, kosmetyczne lub toaletowe, gotowe odświeżacze pomieszczeń. Natomiast mydła umieszczono w dziale 34 (rozporządzenie wykonawcze Komisji UE 2015/1754 z dnia 6 października 2015 roku).

Nie jest to zamknięta lista produktów kosmetycznych. W każdej chwili można, po wyczerpaniu drogi legislacyjnej, dołączyć do niej kolejny produkt.

W literaturze światowej, już od lat 70. ubiegłego stulecia, pojawiły się propozycje, aby wyraźnie wydzielić osobną grupę produktów kosmetycznych zwanych potocznie dermokosmetykami bądź kosmeceutykami. Wedle definicji zaproponowanej przez amerykańskiego dermatologa A.M. Kligsmana kosmeceutyki to produkty kosmetyczne zawierające aktywne składniki, które mogą wpływać na procesy fizjologiczne zachodzące w skórze człowieka. Oprócz działania pielęgnacyjnego wykazują one działanie lecznicze lub wspomagające leczenie. Są to kosmetyki o podwójnym działaniu – pielęgnacyjnym i leczniczym. Czyli „kosmeceutyk" to kosmetyk wpływający na procesy fizjologiczne skóry i wspomagający leczenie chorób skóry (S.Z. Rzeźnik, K. Kordus, R. Śpiewak, 2012, s. 101). Jak dotąd żadne z państw na świecie nie wyodrębniło kosmeceutyków w sensie normatywnym. Z punktu widzenia prawa polskiego i unijnego taki produkt jest albo produktem kosmetycznym (o ile jego głównym zadaniem jest utrzymanie w czystości, pielęgnowanie, ochrona, perfumowanie, zmiana

wyglądu ciała lub ulepszenie jego zapachu), albo produktem leczniczym, którego definicja, zgodnie z art. 2 pkt 32 ustawy z dnia 6 września 2001 roku – Prawo farmaceutyczne, brzmi następująco: jest to „substancja lub mieszanina substancji, przedstawiana jako posiadająca właściwości zapobiegania lub leczenia chorób występujących u ludzi lub zwierząt lub podawana w celu postawienia diagnozy lub w celu przywrócenia, poprawienia lub modyfikacji fizjologicznych funkcji organizmu poprzez działanie farmakologiczne, immunologiczne lub metaboliczne". Ustawa ta – od nowelizacji w 2007 roku – reguluje również sytuację, gdy dany produkt spełnia jednocześnie kryteria leku i np. kosmetyku. Wówczas to, zgodnie z art. 3a ustawy – Prawo farmaceutyczne, stosuje się do niego właśnie przepisy tej ustawy. Przepis ten stanowi wyraźnie, że do produktu spełniającego jednocześnie kryteria produktu leczniczego oraz kryteria innego rodzaju produktu, w szczególności suplementu diety, kosmetyku lub wyrobu medycznego, określone odrębnymi przepisami, stosuje się przepisy niniejszej ustawy. Dlatego też zgodzić się wypada z poglądem, że kosmeceutyki bądź dermokosmetyki to terminy z zakresu raczej marketingu niż nauki (S.Z. Rzeźnik, K. Kordus, R. Śpiewak, 2012, s. 103).

W warunkach polskich, w kontekście art. 3a ustawy – Prawo farmaceutyczne, warto zwrócić uwagę na wyrok NSA z dnia 19 maja 2009 roku sygn. II GSK 899/08, w którym stwierdzono, że oczywiste jest, iż w razie poważnych wątpliwości co do charakteru tego produktu, czy aby nie jest on środkiem leczniczym, jedyny dowód rozstrzygający wszelkie wątpliwości powinna stanowić opinia biegłego odpowiedniego instytutu naukowego (D. Wąsik, s. 23).

Warto też zaznaczyć, że ustawodawca przewidział w art. 86 ust. 8 ustawy – Prawo farmaceutyczne możliwość sprzedaży produktów kosmetycznych w ogólnodostępnych aptekach, ale z wyłączeniem kosmetyków przeznaczonych do perfumowania lub upiększania oraz pod warunkiem, że ich przechowywanie i sprzedaż nie będą przeszkadzać podstawowej działalności apteki.

BEZPIECZEŃSTWO KOSMETYKÓW

Każdy produkt występujący na rynku winien być bezpieczny. W warunkach polskich kwestię bezpieczeństwa produktów reguluje w pierwszej kolejności ustawa z dnia 12 grudnia 2003 roku o ogólnym bezpieczeństwie produktów (Dz.U. z 2015 r., poz. 322 z późn. zm.). Z treści art. 10 ust. 1

wspomnianej ustawy wynika, że producent zobowiązany jest wprowadzać na rynek polski wyłącznie produkty bezpieczne. Ustawa ta w art. 4 ust. 1 przyjmuje, że „produktem bezpiecznym jest produkt, który w zwykłych lub w innych, dających się w sposób uzasadniony przewidzieć, warunkach jego używania, z uwzględnieniem czasu korzystania z produktu, a także, w zależności od rodzaju produktu, sposobu uruchomienia oraz wymogów instalacji i konserwacji, nie stwarza żadnego zagrożenia dla konsumentów lub stwarza znikome zagrożenie, dające się pogodzić z jego zwykłym używaniem i uwzględniające wysoki poziom wymagań dotyczących ochrony zdrowia i życia ludzkiego".

Ustawa o kosmetykach nie określa wprost definicji bezpiecznego kosmetyku. Zastrzega jedynie w art. 4 ust. 1, że kosmetyk wprowadzony do obrotu nie może zagrażać zdrowiu ludzi, o ile używany jest w zwykłych lub w innych dających się przewidzieć warunkach, z uwzględnieniem w szczególności jego wyglądu lub prezentacji, oznakowania, wszystkich instrukcji użycia oraz innych wskazówek lub informacji pochodzących od producenta.

W podobny sposób kwestię tę reguluje rozporządzenie PE i Rady (WE) nr 1223/2009 dotyczące produktów kosmetycznych. Otóż w art. 3 ust. 1 tego rozporządzenia stwierdzono wyraźnie, że „produkt kosmetyczny udostępniany na rynku powinien być bezpieczny dla zdrowia ludzi w normalnych lub dających się przewidzieć warunkach stosowania (...)". Nadto w pkt 9 preambuły wspomnianego rozporządzenia znajduje się stwierdzenie, że „produkty kosmetyczne powinny być bezpieczne w normalnych lub dających się racjonalnie przewidzieć warunkach stosowania. W szczególności analiza ryzyka i korzyści nie powinna uzasadniać występowania ryzyka dla zdrowia ludzi".

Z przepisów tych wynika więc zasada bezwzględnego bezpieczeństwa kosmetyków. Nigdy więc ryzyko stosowania kosmetyku nie może przewyższyć korzyści z jego stosowania. W warunkach polskich za bezpieczeństwo kosmetyku odpowiada jego producent.

Zgodnie z art. 3 ust. 1 ustawy o kosmetykach za producenta uważa się:

a) przedsiębiorcę, który wytwarza i wprowadza kosmetyk do obrotu,
b) przedsiębiorcę, który wprowadza kosmetyk do obrotu,
c) przedstawiciela przedsiębiorcy,
d) każdą osobę, która występuje jako wytwórca, umieszczając na produkcie lub dołączając do niego swoją firmę, znak towarowy lub inne odróżniające oznaczenie,

e) importera wprowadzającego do obrotu kosmetyk spoza państwa, w którym ma swoją siedzibę.

Odmiennie postąpił prawodawca unijny. W rozporządzeniu PE i Rady (WE) nr 1223/2009 osobno uregulował pojęcia producenta (art. 2 ust. 1 lit. d), dystrybutora (art. 2 ust. 1 lit. e) oraz importera (art. 2 ust. 1 lit. i). Definicje te łączy jeden element; wprowadzenie (udostępnienie) produktu kosmetycznego na rynku Wspólnoty. Nie ma tu znaczenia, czy produkt kosmetyczny został wytworzony na terenie UE, czy też pochodzi z kraju trzeciego. Podmioty te odpowiedzialne są za bezpieczeństwo kosmetyków (art. 3).

W warunkach polskich – w art. 4 ust. 2 i 3 ustawy o kosmetykach – wprowadzone zostały ograniczenia polegające na tym, że producent w kosmetykach nie może stosować materiałów pochodzących z ciała ludzkiego oraz nie wolno mu stosować substancji rakotwórczych, mutagennych, a także działających szkodliwie na rozrodczość.

Kolejnym ograniczeniem jest zakaz prowadzenia testów kosmetyków bądź poszczególnych ich składników na zwierzętach. Zakaz ten wynika z treści art. 4a wspomnianej ustawy.

Z kolei w art. 5 ustawy o kosmetykach sformułowany został zakaz wprowadzenia do obrotu kosmetyków zawierających niedozwolone substancje. Te ostatnie ustawa podzieliła na trzy grupy:

a) substancje niedozwolone do stosowania w kosmetykach,
b) substancje dozwolone do stosowania w kosmetykach wyłącznie w ograniczonych ilościach, zakresie i warunkach stosowania, o ile wymagania te zostały przekroczone,
c) barwniki, substancje konserwujące, substancje promieniochronne dozwolone w kosmetykach wyłącznie w ograniczonych ilościach, zakresie i warunkach stosowania, o ile wymagania te zostały przekroczone.

Jednocześnie ustawodawca w art. 5 ust. 3 wspomnianej ustawy zobowiązał ministra właściwego do spraw zdrowia do wydania rozporządzenia zawierającego m.in. listę substancji niedozwolonych do stosowania w kosmetykach, listę substancji dozwolonych do stosowania w kosmetykach wyłącznie w ograniczonych ilościach, zakresie i warunkach stosowania, a także listy dozwolonych do stosowania barwników, substancji konserwujących i substancji promieniochronnych – z podaniem ich ilości, zakresu

i warunków stosowania. Obecnie listy te zawiera rozporządzenie Ministra Zdrowia z dnia 30 marca 2005 roku w sprawie list substancji niedozwolonych lub dozwolonych z ograniczeniami do stosowania w kosmetykach oraz znaków graficznych umieszczanych na opakowaniach kosmetyków (Dz.U. nr 72 poz. 642).

Lista zawierająca wykaz substancji niedozwolonych w kosmetykach znajduje się w załączniku nr 1 do wspomnianego rozporządzenia i zawiera 1132 pozycje. Załącznik nr 2 zawiera listę 158 substancji dozwolonych do stosowania w kosmetykach wyłącznie w ograniczonych ilościach, zakresie i warunkach stosowania. Załącznik nr 3 to z kolei nienumerowana lista barwników dozwolonych do stosowania w kosmetykach, a załącznik nr 4 to lista substancji konserwujących dozwolonych do stosowania w kosmetykach obejmująca 55 pozycji. Wreszcie załącznik nr 5 do wspomnianego wyżej rozporządzenia zawiera listę obejmującą 26 substancji promieniochronnych dopuszczonych do stosowania w kosmetykach. Powyższe listy są aktualizowane na bieżąco i zgodne są z prawodawstwem unijnym.

W Unii Europejskiej nad bezpieczeństwem składników stosowanych m.in. w produktach kosmetycznych czuwa Komitet Naukowy ds. Bezpieczeństwa Konsumentów (Scientific Committee on Consumer Safety – SCCS), którego siedziba mieści się w Luksemburgu. Jest on organem doradczym Komisji Europejskiej. Komitet opracowuje opinie na temat zagrożeń (chemicznych, biologicznych, mechanicznych i innych zagrożeń fizycznych) dla zdrowia i bezpieczeństwa produktów nieżywnościowych (np. produktów kosmetycznych i ich składników, zabawek, odzieży i artykułów gospodarstwa domowego), a także usług (np. tatuowanie, sztuczne opalanie). Jego zadaniem jest m.in. ocena bezpieczeństwa każdego składnika kosmetyku, co do którego pojawiają się jakiekolwiek doniesienia o potencjalnej szkodliwości. Komitet, przygotowując swe opinie, bierze pod uwagę także wszelkie dostępne dane naukowe w postaci m.in. wyników badań, publikacji naukowych i na ich podstawie przygotowuje szczegółową analizę bezpieczeństwa i opinię dla danego składnika. Jeśli opinia Komitetu jest negatywna, wówczas Komisja Europejska podejmuje kroki prawne w celu zakazania stosowania takiego składnika w produktach kosmetycznych bądź ograniczenia jego ilości do bezpiecznej dla zdrowia ludzi.

Warto w tym miejscu podkreślić, że prawodawca unijny dopuszcza możliwość występowania w produktach kosmetycznych śladowych substancji

niedozwolonych. Otóż zgodnie z art. 17 rozporządzenia PE i Rady (WE) 1223/2009 dopuszczalna jest niezamierzona obecność małej ilości substancji niedozwolonej, pochodzącej z zanieczyszczeń składników naturalnych lub syntetycznych, procesu wytwarzania, przechowywania, migracji z opakowania, która przy zastosowaniu zasad dobrej praktyki produkcji jest ze względów technologicznych nie do uniknięcia, pod warunkiem że obecność ta nie powoduje, że kosmetyk staje się niebezpieczny dla zdrowia.

Polska ustawa o kosmetykach zobowiązuje producenta także do widocznego i czytelnego oznakowania opakowania kosmetyku metodami uniemożliwiającymi łatwe usunięcie oznakowania (art. 6 ust. 1). Oznakowanie opakowania jednostkowego i opakowania zewnętrznego powinno zawierać – co do zasady – osiem precyzyjnie określonych w art. 6 ust. 2 ustawy informacji, m.in. funkcję kosmetyku, jeżeli nie wynika ona jednocześnie z jego prezentacji, oraz wykaz składników określonych zgodnie z nazwami przyjętymi w Międzynarodowym Nazewnictwie Składników Kosmetycznych (INCI). W tym ostatnim przypadku producent może, ze względu na tajemnicę przedsiębiorstwa, zwrócić się do Głównego Inspektora Sanitarnego o wyrażenie zgody na nieujawnianie na opakowaniu jednostkowym nazw jednego bądź kilku składników kosmetyku. W przypadku wydania zgody w postaci decyzji Główny Inspektor Sanitarny nadaje stosowny numer zastępujący nazwę składnika kosmetyku. Decyzję taką wydaje się na 5 lat. Wydanie decyzji odmownej uzasadnione może być względami bezpieczeństwa zdrowia ludzi (art. 7 ust. 1–6).

Kolejnym obowiązkiem ustawowym nałożonym na producenta było przekazanie informacji o wprowadzanym do obrotu kosmetyku do utworzonego na podstawie art. 8 ustawy o kosmetykach krajowego systemu informowania o kosmetykach wprowadzonych do obrotu. W systemie tym gromadzone miały być dane o kosmetykach oraz informacje o przypadkach zachorowań spowodowanych użyciem tych kosmetyków (art. 8 ust. 1–3). Informacje zawarte w tym systemie udostępniane miały być organom Państwowej Inspekcji Sanitarnej, a także lekarzom. Tym ostatnim w szczególności, gdy zachodziła potrzeba podjęcia natychmiastowego i właściwego leczenia, a zachodziło podejrzenie, że zastosowanie kosmetyku było przyczyną zachorowania (art. 10 ust. 2).

Producent został więc zobowiązany przed dniem wprowadzenia kosmetyku do obrotu do przekazania do tego systemu danych obejmujących na-

zwę handlową kosmetyku i jego kategorię, imię i nazwisko lub nazwę i adres producenta zgłaszającego kosmetyk, a także adres miejsca udostępniania dokumentów zawierających informacje o kosmetyku (art. 8 ust. 4). Nadto producent został obowiązany zgłaszać do krajowego systemu wszelkie zmiany danych w odniesieniu do kosmetyku znajdującego się już w obrocie (art. 8 ust. 5).

Do prowadzenia wspomnianego systemu zobowiązany został Główny Inspektor Sanitarny bądź upoważniona przez niego jednostka organizacyjna (art. 9 ustawy). Główny Inspektor Sanitarny skorzystał z tego upoważnienia i przekazał prowadzenie tego systemu Instytutowi Medycyny Pracy im. prof. J. Nofera w Łodzi. Ten system na wspomnianych zasadach funkcjonował do dnia 11 lipca 2013 roku, kiedy to weszło w życie rozporządzenie PE i Rady (WE) 1223/2009. Od tego czasu kosmetyki nie są już w nim rejestrowane, a system będzie funkcjonował i udzielał – jak dotąd – stosownych informacji do dnia 11 lipca 2020 roku (art. 38 przywołanego wcześniej rozporządzenia). W zamian za to producent został zobowiązany do zgłoszenia kosmetyku w Portalu Zgłaszania Produktów Kosmetycznych (Cosmetic Product Notification Portal – CPNP) utworzonego na podstawie art. 13 wspomnianego rozporządzenia 2223/2009. Jest to jedyna baza rejestracji kosmetyków dla UE.

Natomiast w cytowanym już po wielokroć rozrządzeniu przyjęto zasadę, że do obrotu na terenie UE mogą być wprowadzone tylko te produkty kosmetyczne, dla których na terenie Wspólnoty jest wyznaczona „osoba odpowiedzialna", która może być osobą prawną lub fizyczną. Najczęściej są to producenci mający swoje siedziby na terenie UE. Mogą oni wyznaczyć pisemnie jako osobę odpowiedzialną inną osobę mającą swą siedzibę na terenie Wspólnoty (art. 4 ust. 1 oraz 3–4 rozporządzenia). Osoba odpowiedzialna ma gwarantować, że spełnione zostały wszystkie obowiązki określone w rozporządzeniu przez każdy wprowadzany do obrotu produkt kosmetyczny (art. 4 ust. 2 rozporządzenia). Jest to szczególnie ważne, gdy producent ma swoją siedzibę poza terytorium Wspólnoty.

Do jednych z najważniejszych zadań stojących przed osobą odpowiedzialną należy zapewnienie przeprowadzenia oceny bezpieczeństwa produktu kosmetycznego oraz sporządzenia raportu bezpieczeństwa takiego produktu zgodnie z treścią załącznika I do rozporządzenia (art. 10 ust. 1 rozporządzenia), a także przechowanie przez 10 lat dokumentacji produk-

tu kosmetycznego od momentu wprowadzenia do obrotu ostatniej partii danego kosmetyku (art. 11 ust. 1 rozporządzenia). Dokumentacja ta musi zawierać:

a) opis produktu kosmetycznego umożliwiający łatwe przyporządkowanie dokumentacji produktu do danego produktu kosmetycznego,
b) raport bezpieczeństwa produktu kosmetycznego,
c) opis metod produkcji i oświadczenie o zgodności z dobrą praktyką produkcji,
d) jeżeli jest to uzasadnione ze względu na rodzaj produktu kosmetycznego lub efekt jego działania, dowód deklarowanego działania,
e) dane dotyczące wszelkich testów na zwierzętach, przeprowadzonych przez producenta, jego przedstawicieli lub dostawców w trakcie opracowania lub oceny bezpieczeństwa produktu kosmetycznego lub jego składników, w tym testów na zwierzętach przeprowadzanych w celu spełnienia wymogów przepisów ustawowych lub wykonawczych obowiązujących w krajach trzecich (art. 11 ust. 2 rozporządzenia).

Ocenę bezpieczeństwa produktu kosmetycznego przeprowadza osoba legitymująca się dyplomem bądź innym dowodem posiadanych kwalifikacji formalnych. Zazwyczaj jest to dyplom ukończenia studiów w dziedzinie farmacji, toksykologii, medycyny lub innej podobnej dyscypliny, bądź kursu uznawanego przez dane państwo członkowskie za równorzędny (art. 10 ust. 2 rozporządzenia). Jest to tzw. *safety assess*or (w wolnym tłumaczeniu: specjalista ds. oceny bezpieczeństwa kosmetyków). W sensie formalnym nie ma on odpowiednika w języku polskim. .Nie występuje on także w załączniku – klasyfikacja zawodów i specjalności na potrzeby rynku pracy do rozporządzenia Ministra Pracy i Polityki Społecznej z dnia 7 sierpnia 2014 roku w sprawie klasyfikacji zawodów i specjalności na potrzeby rynku pracy oraz zakresu jej stosowania (Dz.U. z 2014 r., poz. 1145). Można więc przyjąć, że z formalnego punktu widzenia specjalność taka w Polsce nie występuje.

Do jego zadań należy, jak już wcześniej stwierdzono, przeprowadzenie oceny bezpieczeństwa kosmetyku na podstawie wszelkich istniejących danych. Takimi danymi mogą być przede wszystkim informacje otrzymane od producenta kosmetyku. Najważniejszymi będą te, które dotyczą składu produktu, specyfikacji dla poszczególnych składników, a także wyniki

badań gotowego produktu. Osoba ta wykorzystuje także całą dostępną literaturę, bazy danych, dane uzyskane na potrzeby oceny bezpieczeństwa innych produktów, np. leków, żywności itd.

Na ocenę bezpieczeństwa kosmetyku sporządzaną przez specjalistę ds. oceny bezpieczeństwa kosmetyków składają się następujące czynności:

1) ocena zgodności składu produktu z przepisami prawa,
2) ocena toksykologiczna składników kosmetyku,
3) ocena ekspozycji lub inaczej ocena narażenia,
4) ocena ryzyka dla składników kosmetyku,
5) ocena wyników badań gotowego kosmetyku,
6) ocena przypadków niepożądanego działania,
7) przygotowanie raportu z oceny bezpieczeństwa kosmetyku (Jak się ocenia...).

Aby kosmetyk przeszedł pozytywnie procedurę oceny bezpieczeństwa, producent powinien w procesie produkcji stosować tzw. zasady dobrej praktyki produkcji (Good Manufacturing Practices – GMP). Wyraźnie o tym stanowi art. 8 rozporządzenia PE i Rady (WE) 1223/2009. W przypadku produktów kosmetycznych dobre praktyki produkcji wskazane są w normie ISO GMP 22716, która w szczególności określa wytyczne w zakresie produkcji, kontroli, magazynowania oraz transportu produktów kosmetycznych. W warunkach polskich zastosowanie ma zharmonizowana norma europejska przetłumaczona na język polski: PN-EN ISO 22716:2007 Kosmetyki – Przewodnik GMP.

Ponieważ w prawodawstwie unijnym związanym z produktami kosmetycznymi nie istnieje zasada wstępnej kontroli takiego produktu przez organy poszczególnych państw przed wprowadzeniem go do obrotu, stąd – po zebraniu stosownej dokumentacji – osoba odpowiedzialna dokonuje drogą elektroniczną zgłoszenia wyrobu kosmetycznego zgodnie z regułami określonymi w art. 13 cytowanego rozporządzenia. Zgłoszenia produktu kosmetycznego dokonuje się na stronach Portalu Zgłaszania Produktów Kosmetycznych, o którym wspomniano wcześniej. Gdy produkt został zgłoszony w CPNP, nie ma potrzeby stosowania dodatkowego zgłoszenia na szczeblu krajowym w ramach UE. Warto w tym miejscu zwrócić uwagę na fakt, iż pewne informacje przekazane przy zgłoszeniu produktu kosmetycznego udostępniane są drogą elektroniczną właściwym organom (do celów

nadzoru i analizy rynku, oceny i informowania konsumentów), a także do celów terapeutycznych ośrodkom zatruć lub podobnym jednostkom ustanowionym przez państwa członkowskie UE.

NADZÓR NAD RYNKIEM PRODUKTÓW KOSMETYCZNYCH I ICH BEZPIECZEŃSTWEM

Przyjęcie zgłoszenia, a tym samym zarejestrowanie produktu kosmetycznego za pośrednictwem Portalu Zgłaszania Produktów Kosmetycznych i wprowadzenia go do obrotu nie zwalnia producenta od ciągłego monitorowania bezpieczeństwa swojego produktu znajdującego się na rynku. Musi on też reagować na informacje konsumentów o działaniach niepożądanych i podjąć czynności w tym zakresie (art. 23 rozporządzenia).

Rozporządzenie PE i Rady (WE) 1223/2009 w art. 22 zobowiązuje państwa członkowskie do monitorowania zgodności występujących na rynku produktów kosmetycznych z jego przepisami. W tym celu powinny przeprowadzać kontrolę produktów kosmetycznych i podmiotów gospodarczych, wykorzystując dokumentację takiego produktu. Innym zalecanym przez wspomniane rozporządzenia typem kontroli jest kontrola fizyczna oraz badania laboratoryjne. Państwa członkowskie mają również obowiązek monitorowania przestrzegania zasad dobrych praktyk. Muszą też raz na cztery lata dokonać przeglądu i ocen przebiegu działań nadzorczych i poinformować o nich pozostałe państwa członkowskie.

Z kolei ustawa o kosmetykach w art. 13 ust. 1 stanowi, że nadzór nad przestrzeganiem jej przepisów sprawuje:

a) Państwowa Inspekcja Sanitarna na zasadach i w trybie określonym w odrębnych przepisach,
b) Inspekcja Handlowa w zakresie znakowania, zafałszowań oraz prawidłowości obrotu.

Nadzór w tym zakresie, zgodnie z art. 13 ust. 2 wspomnianej ustawy, obejmuje wykonywanie czynności i stosowanie środków określonych w ustawie oraz w odrębnych przepisach, a w szczególności kontrolę, pobieranie próbek kosmetyku oraz przeprowadzanie badań laboratoryjnych w zakresie bezpieczeństwa zdrowia ludzi.

Państwowa Inspekcja Sanitarna realizuje zadania nadzorcze w oparciu o przepisy ustawy z dnia 14 marca 1985 roku o Państwowej Inspekcji Sani-

tarnej (Dz.U. z 2015 r., poz. 1412). Zgodnie z art. 4 ust. 1 pkt 4 wspomnianej ustawy do zakresu działania Państwowej Inspekcji Sanitarnej w dziedzinie bieżącego nadzoru sanitarnego należy kontrola przestrzegania przepisów określających wymagania higieniczne i zdrowotne, w szczególności dotyczących: „warunków zdrowotnych produkcji i obrotu (...) kosmetykami (...)".

Z § 19 regulaminu organizacyjnego Głównego Inspektoratu Sanitarnego będącego załącznikiem do zarządzenia 108/15 Głównego Inspektora Sanitarnego z dnia 13 maja 2015 roku w sprawie ustalenia regulaminu organizacyjnego Głównego Inspektoratu Sanitarnego wynika, że sprawami związanymi z kosmetykami zajmuje się Departament Bezpieczeństwa Żywności i Żywienia. Do niego należy bowiem m.in.:

a) ustalanie priorytetów i kierunków działania Państwowej Inspekcji Sanitarnej w zakresie bezpieczeństwa żywności, żywienia, kosmetyków oraz materiałów i wyrobów przeznaczonych do kontaktu z żywnością,
b) koordynowanie i nadzór realizacji przepisów o produktach kosmetycznych.

Jednocześnie warto w tym miejscu podkreślić, że zgodnie z art. 27c ustawy o Państwowej Inspekcji Sanitarnej, właściwy państwowy inspektor sanitarny:

a) „w przypadku uzasadnionego podejrzenia, że produkt stwarza zagrożenie życia lub zdrowia ludzi (...), wstrzymuje, w drodze decyzji, jego wytwarzanie lub wprowadzanie do obrotu lub nakazuje wycofanie produktu z obrotu na czas niezbędny do przeprowadzenia oceny i badań jego bezpieczeństwa, nie dłuższy jednak niż 18 miesięcy". W przypadku wydania takiej decyzji właściwy państwowy inspektor sanitarny zatrzymuje produkt i „nakazuje zaprzestania prowadzenia działalności w pomieszczeniach lub obiektach służących wytwarzaniu lub wprowadzaniu produktu do obrotu na czas niezbędny do usunięcia zagrożenia, nie dłuższy niż 3 miesiące",
b) „w przypadku stwierdzenia, że produkt stwarza zagrożenie życia lub zdrowia ludzi, zakazuje, w drodze decyzji, wytwarzania produktu lub wprowadzania produktu do obrotu, a także nakazuje wycofanie produktu z obrotu oraz jego zniszczenie na koszt strony postępowania".

Natomiast organizację oraz prawa i obowiązki Inspekcji Handlowej reguluje ustawa z dnia 15 grudnia 2000 roku o Inspekcji Handlowej (t.j. Dz.U.

z 2016 r., poz. 1059 z późn. zm.). W ramach Inspekcji Handlowej bezpieczeństwem produktów kosmetycznych zajmuje się Departament Ochrony Interesów Konsumentów w Urzędzie Ochrony Konkurencji i Konsumentów. Do jego zadań należy przede wszystkim monitorowanie rynku w celu eliminowania z niego produktów niebezpiecznych oraz wyrobów konsumenckich niespełniających zasadniczych wymagań. Nadto departament ten zobowiązany jest do ewidencjonowania produktów niebezpiecznych, a także zbierania na ich temat informacji, które przekazywane są następnie właściwym organom. Gromadzi on także powiadomienia przekazywane przez producentów i dystrybutorów o wprowadzonych na rynek wyrobach niespełniających wymagań bezpieczeństwa.

Urząd Ochrony Konkurencji i Konsumentów jest także Krajowym Punktem Kontaktowym systemu RAPEX (The Rapid Exchange of Information System – Wspólnotowy System Szybkiej Informacji). Zgodnie z art. 10 dyrektywy 2001/95/WE Parlamentu Europejskiego i Rady z dnia 3 grudnia 2001 roku w sprawie ogólnego bezpieczeństwa produktów system ten ma za zadanie w szczególności ułatwić:

a) wymianę informacji dotyczących oceny ryzyka, produktów niebezpiecznych, metod badawczych i wyników, najnowszych odkryć naukowych oraz innych aspektów dotyczących czynności kontrolnych,
b) ustanowienie i wykonanie wspólnych projektów nadzoru i badań,
c) wymianę wiedzy specjalistycznej i wiedzy na temat rzetelnych praktyk oraz współpracę w zakresie szkoleń,
d) lepszą współpracę na szczeblu Wspólnoty w odniesieniu do czynności związanych z wykrywaniem, wycofywaniem i działaniami w celu odzyskania niebezpiecznych produktów od konsumentów.

System ten nie obejmuje informacji dotyczących środków farmaceutycznych, wyrobów medycznych, pasz oraz żywności. Jest on dostępny w postaci elektronicznej dla każdego konsumenta.

Prezes UOKiK, występując jako punkt kontaktowy RAPEX, dysponuje prawem do wprowadzania, zatwierdzania i przesyłania notyfikacji do Komisji Europejskiej. Notyfikacje zamieszczane w systemie tworzone są na podstawie informacji otrzymywanych zarówno od przedsiębiorców w formie dobrowolnych powiadomień, jak i z innych krajowych organów nadzoru rynku. Organy te przekazują do polskiego punktu kontaktowe-

go RAPEX (PPK RAPEX) informacje z kontroli. PPK RAPEX koordynuje działanie systemu na poziomie krajowym, zlecając kontrole właściwym organom nadzoru rynku w przypadku informacji o wystąpieniu niebezpiecznego produktu na terenie Polski (Krajowy program nadzoru rynku. UOKiK, 2016, s. 9).

PODSUMOWANIE

Bezpieczeństwo kosmetyków (produktów kosmetycznych) od ubiegłego stulecia znajduje się w sferze coraz większego zainteresowania ustawodawstw poszczególnych państw.

Również w literaturze coraz częściej zaczęto podnosić kwestie związane z zarządzaniem bezpieczeństwem kosmetykami. W przypadku Unii Europejskiej zagadnienie to nabrało szczególnego znaczenia z chwilą wejścia w życie w 2013 roku rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1223/2009 z dnia 30 listopada 2009 roku dotyczącego produktów kosmetycznych. Zdefiniowało ono bowiem na nowo szereg terminów i pojęć, a także zmieniło dotychczasowy zakres obowiązków producentów kosmetyków oraz ich dystrybutorów i importerów (A. Budzowski, 2012, s. 23). Polska ustawa z dnia 30 marca 2001 roku o kosmetykach nie odpowiada już w pełni unijnym regulacjom prawnym. Stąd też do wykazu prac legislacyjnych i programowych Rady Ministrów zostało wprowadzone zgłoszenie o przygotowywaniu projektu ustawy o produktach kosmetycznych, który ma być gotowy i przyjęty przez Radę Ministrów w I kwartale 2017 roku. Celem proponowanego projektu jest określenie obowiązków podmiotów i właściwości organów w zakresie wykonywania obowiązków i zadań administracyjnych wynikających z rozporządzenia PE i Rady (WE) nr 1223.

Nie oznacza to jednak, że bezpieczeństwo kosmetyków w Polsce drastycznie spadło. Wręcz przeciwnie. Z danych ogłaszanych przez Państwową Inspekcję Sanitarną w corocznych publikacjach na temat stanu sanitarnego kraju wynika, że w latach 2013–2015 zdyskwalifikowano tylko średnio 1,35% przebadanych próbek kosmetyków. W tej grupie kosmetyki polskie stanowiły 1,57%, z Unii Europejskiej – 0,61%, zaś z krajów trzecich – 3,81%.

Bibliografia

Borkowski M. (2015). *Prawo kosmetyczne. Zarys prawa polskiego i europejskiego*. Wydawnictwo Gdańskiej Szkoły Wyższej, Gdańsk.

Budzowski A. (2012). *Zarządzanie bezpieczeństwem produktów kosmetycznych w świetle nowych przepisów unijnych*. „Bezpieczeństwo. Teoria i Praktyka", nr 4, s. 23–39.

Dąbrowska D., Kaniewski J. (2006). *Ochrona konsumenta przed szkodą wynikłą z użycia kosmetyku w prawie polskim i amerykańskim*. Zeszyty Naukowe Akademii Ekonomicznej w Krakowie, s. 49–64.

Kosmetyk. *Słownik języka polskiego,* red. M. Szymczak (1978). Warszawa, PWN.

Report on EU customs enforcement of intellectual property rights – results at the EU border 2015, EU Publication Office, Luxembourg 2015.

Rzeźnik S.Z., Kordus K., Śpiewak R. (2012). *„Kosmeceutyki" i „dermokosmetyki" – unikalna kategoria produktów do pielęgnacji skóry czy zwykły chwyt marketingowy?,* „Estetologia Medyczna i Kosmetologia" 2 (4), s. 101–103.

Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady na temat oświadczeń o produktach sporządzanych na podstawie wspólnych kryteriów w branży kosmetycznej, Bruksela, dnia 19.09.2016 r. COM (2016) 580 final.

Szewczyk K., Młynarczyk J. (2015). *Historia kosmetyków kolorowych*. „Zeszyty naukowe – Wyższa Szkoła Przedsiębiorczości w Warszawie" nr 2(1) s. 61–67.

Wąsik D. (2016). *Ustawa o kosmetykach – komentarz*. Wolters Kluwer, Warszawa.

Źródła internetowe

Bochner K. (2013). Made in Poland. *Wiadomości kosmetyczne,* http://www.wiadomoscikosmetyczne.pl/kosmetycznybiznes/7859-made-in-poland [data dostępu: 25.09.2016].

Jak się ocenia bezpieczeństwo kosmetyków?, http://www.kosmopedia.org/bezpieczenstwo_kosmetykow/jak_sie_ocenia_bezpieczenstwo_/ [data dostępu: 10.09.2016].

Kasprzak M. (2016). *Polski rynek kosmetyczny*. „Analiza Rynku", http://analizarynku.eu/polski-rynek-kosmetyczny Pozyskano [data dostępu: : 27.09.2016].

Krajowy program nadzoru rynku. UOKiK, 2016, https://uokik.gov.pl/download.php?id=1400 [data dostępu: 10.09.2016].

Uzasadnienie do rządowego projektu ustawy o kosmetykach, Sejm III kadencji, druk 2281 z dnia 16 października 2000 r., http://orka.sejm.gov.pl/Rejestrd.nsf/wgdruku/2281/$file/2281.pdf [data dostępu: 25.09. 2016].

Źródła prawa

Dyrektywa Rady (76/768/EWG) z dnia 27 lipca 1976 roku w sprawie zbliżenia ustawodawstw Państw Członkowskich dotyczących kosmetyków (Dz. Urz. WE L 262, s. 169 i nast.).

Dyrektywa 2001/95/WE Parlamentu Europejskiego i Rady z dnia 3 grudnia 2001 roku w sprawie ogólnego bezpieczeństwa produktów (Dz. Urz. L 11/4, s. 447 i nast.).

Rozporządzenie Prezydenta RP z dnia 22 marca 1928 roku o dozorze nad artykułami żywności i przedmiotami użytku (Dz.U. nr 36, poz. 343).

Rozporządzenie Ministra Opieki Zdrowotnej z dnia 25 czerwca 1934 roku wydane w porozumieniu z Ministrem Przemysłu i Handlu o dozorze nad wyrobem i obiegiem środków kosmetycznych (Dz.U. nr 62, poz. 523).

Rozporządzenie Ministra Opieki Społecznej z dnia 18 stycznia 1939 roku wydane w porozumieniu z Ministrem Przemysłu i Handlu o dozorze nad wyrobem i obiegiem środków kosmetycznych (Dz.U. nr 13, poz. 72).

Rozporządzenie Ministra Zdrowia z dnia 16 czerwca 2003 roku w sprawie określenia kategorii produktów będących kosmetykami (Dz.U. nr 125, poz. 1168).

Rozporządzenie Ministra Zdrowia z dnia 30 marca 2005 roku w sprawie list substancji niedozwolonych lub dozwolonych z ograniczeniami do stosowania w kosmetykach oraz znaków graficznych umieszczanych na opakowaniach kosmetyków (Dz.U. nr 72, poz. 642).

Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1223/2009 z dnia 30 listopada 2009 roku dotyczące produktów kosmetycznych (Dz.U. L 342 z 22.12.2009, s. 59–209).

Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 7 sierpnia 2014 roku w sprawie klasyfikacji zawodów i specjalności na potrzeby rynku pracy oraz zakresu jej stosowania (Dz.U. z 2014 r., poz. 1145).

Rozporządzenie wykonawcze Komisji (UE) 2015/1754 z dnia 6 października 2015 roku zmieniające załącznik 1 do rozporządzenia Rady (EWG) nr 2658/87 w sprawie nomenklatury taryfowej i statystycznej oraz w sprawie Wspólnej Taryfy Celnej (Dz. Urz. UE L 285, tom 58, z dnia 30 października 2015 r.).

Ustawa z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej (t.j. Dz.U. z 2015 r., poz. 1412).

Ustawa z dnia 15 grudnia 2000 r. o Inspekcji Handlowej (t.j. Dz.U. z 2016 r., poz. 1059 z późn. zm.).

Ustawa z dnia 30 marca 2001 r. o kosmetykach (t.j. Dz.U. z 2013 r., poz. 475).

Ustawa z dnia 6 września 2001 r. – Prawo farmaceutyczne (Dz.U. z 2008 r., nr 45, poz. 271 z późn. zm.).

Ustawa z dnia 12 grudnia 2003 r. o ogólnym bezpieczeństwie produktów (t.j. Dz.U. z 2015 r., poz. 322 z późn. zm.).

Orzecznictwo sądowe

Wyrok NSA z dnia 19 maja 2009 roku sygn. II GSK 899/08. Centralna Baza Orzeczeń Sądów Administracyjnych, http://orzeczenia.nsa.gov.pl/doc/1034539D82 [data dostępu: 28.09. 2016].

KRZYSZTOF KRAKOWSKI
Państwowa Wyższa Szkoła Zawodowa
w Ciechanowie
k.krakowski@aon.edu.pl

ANATOMIA BEZPIECZEŃSTWA WEDŁUG NATO W PERSPEKTYWIE 2030

ANATOMY OF SECURITY ACCORDING TO NATO IN 2030

ABSTRACT

The process of change in the international security environment has resulted in the need for adjustments in the current security policy of NATO. As the key to Alliance security are indicated blended threats, and Russia's desire to strengthen its position in the international arena through a return to dominance in the former Soviet Union. NATO sees the need to take measures to combat the aggressive Russian policy. NATO Summit in Newport and in Warsaw shows that efforts are adequate to the immanent danger of security. As the challenges for NATO are indicated: maintaining the transatlantic link, growing in strength and importance of China, India, Brazil, decreasing importance of international security organizations and internal destabilization in the EU.

Keywords: *international security environment, security threats, the ability of NATO, NATO Summit*

STRESZCZENIE

Proces zmian w międzynarodowym środowisku bezpieczeństwa zaowocował potrzebą korekt w dotychczasowej polityce bezpieczeństwa NATO. Jako kluczowe dla bezpieczeństwa Sojuszu wskazywane są zagrożenia hybrydowe i dążenie Rosji do wzmocnienia swojej pozycji na arenie międzynarodowej poprzez

powrót do dominacji w państwach byłego ZSRR. NATO dostrzega konieczność podejmowania działań przeciwdziałających agresywnej polityce Rosji. Szczyt NATO w Newport i w Warszawie wskazuje, że podejmowane są działania adekwatne do zaistniałego zagrożenia bezpieczeństwa. Jako wyzwania dla NATO wskazywane są: podtrzymywanie więzi transatlantyckiej, rosnące w siłę i znaczenie Chiny, Indie, Brazylia, malejące znaczenie międzynarodowych organizacji bezpieczeństwa i wewnętrzna destabilizacja w UE.

Słowa kluczowe: *międzynarodowe środowisko bezpieczeństwa, zagrożenia bezpieczeństwa, zdolności NATO, szczyt NATO*

WPROWADZENIE

Proces zmian w architekturze bezpieczeństwa europejskiego (bezprawna w świetle prawa międzynarodowego aneksja Krymu, konflikt rosyjsko-ukraiński w Donbasie, ekspansja militarystycznej polityki zagranicznej Federacji Rosyjskiej, kryzys w obrębie spójności Unii Europejskiej, kryzys migracyjny, zagrożenie terroryzmem) spowodował rozchwianie ukształtowanego po okresie zimnej wojny ładu międzynarodowego w regionie Europy i Bliskiego Wschodu.

Silne do tej pory struktury państw stały się podatne na destabilizujące działania sił wewnętrznych wspieranych często przez zewnętrzne podmioty państwowe. Wyzwaniem dla NATO stała się nie tylko polityka Rosji i dążenie do odbudowy stref wpływu w Europie i Azji, ale i ekspansja ideologiczna oraz terytorialna Państwa Islamskiego.

Jak zauważył prof. Jarosław Gryz w trakcie wykładu inaugurującego rok akademicki w AON (2015/2016), zmianie uległ stosunek sił politycznych w Europie, a sam kontynent stał się areną wewnętrznej, europejskiej, ale i euroatlantyckiej gry interesów. Podejmowane przez polityków europejskich próby zażegnania kryzysów w kluczowych dla bezpieczeństwa regionach świata nie kończą się sukcesem, a jedynie „zamrażają" je w stanie umożliwiającym ich ponowną erupcję w każdej chwili. Strach przed rozbudzeniem konfliktu stał się skutecznym narzędziem w rękach polityków rosyjskich. Przykładem destabilizujących działań stała się nie tylko sama ingerencja bezpośrednia lub pośrednia Rosji w Naddniestrzu, Górskim Karabachu, Osetii Południowej, Abchazji, ale i wzmacnianie zaczepnego potencjału militarnego w obwodzie kaliningradzkim, Zachodnim Okręgu Wojskowym. Polityka Rosji ukierunkowana została na zmniejszenie woli

państw członkowskich NATO do wdrażania postanowień art. 5 Traktatu Północnoatlantyckiego, zaakceptowanie bezprawnych działań na Ukrainie (aneksja Krymu) oraz zniesienie wprowadzonych przez Unię Europejską sankcji, a jednocześnie rozszerzenie swojej strefy wpływów do tej sprzed 2000 roku.

Marginalizowane w polityce instytucje międzynarodowe i stosowane przez nie instrumenty polityki bezpieczeństwa nie są w stanie utrzymać stałego ładu międzynarodowego. Wobec tych zmian kluczowymi dla bezpieczeństwa europejskich podmiotów wydają się wyzwania związane z redefinicją miejsca i roli Stanów Zjednoczonych w NATO i dla bezpieczeństwa całej Unii Europejskiej.

Ustalenia szczytu w Newport wobec eskalacji konfliktu na Ukrainie zaowocowały trwającą reorientacją Stanów Zjednoczonych i całego NATO na bezpieczeństwo w regionie Europy. Zmiany w polityce obronnej Sojuszu i pogłębienie więzi transatlantyckiej pozwoliło na:

- podkreślenie, że głównym celem istnienia i zadaniem NATO jest obrona terytorium państw członkowskich,
- zwiększenie możliwości reakcji Sojuszu na zagrożenie dla któregokolwiek z państw członkowskich. W ramach Sił Odpowiedzi NATO wyodrębniono kilkutysięczny rotacyjny kontyngent, pozostający w stałej gotowości, zdolny do przerzutu w zagrożony obszar w ciągu 2–5 dni,
- podwyższenie stopnia gotowości dowództwa i oddziałów Wielonarodowego Korpusu Północno-Wschodniego z niższej (Forces at Lower Readiness – FLR) do wysokiej (High Readiness Forces – HRF),
- przeprowadzanie licznych ćwiczeń wojskowych – na terenie państw Europy Środkowo-Wschodniej jako akcentowanie obecności NATO w regionie Europy Wschodniej,
- uzgodnienie, że zbiorowa obrona obejmie też przeciwdziałanie zagrożeniom cybernetycznym,
- uzyskanie zapewnień USA na rozlokowanie na terenie Polski i innych państw Europy Środkowo-Wschodniej ciężkiego sprzętu,
- stopniowe zwiększanie budżetów obronnych państw członkowskich do poziomu dwóch procent w ciągu dekady[1],

[1] Postanowienia szczytu NATO w Newport, https://www.msz.gov.pl/pl/polityka_zagraniczna/szczyt_nato_2016/dokumenty_nato_1/deklaracja_szczytu_nato_w_walii_w_2014 [data dostępu: 12.09.2016].

- uruchomienie procesu przygotowania planów stopniowej odpowiedzi na zagrożenia bezpieczeństwa w Europie.

Niemniej jednak wobec nagłych, trudnych do wcześniejszych prognoz zmian środowiska bezpieczeństwa międzynarodowego analitycy wojskowych i polityczno-militarnych struktur NATO stali się bezbronni. Opracowywany co cztery lata raport Allied Command Transformation (ACT) pod nazwą Strategic Foresight Analysis (SFA) zawierający prognozę zmian w środowisku bezpieczeństwa międzynarodowego w perspektywie 30 lat, a w tym trendy i implikacje dla przyszłego środowiska bezpieczeństwa oraz potencjalne wyzwania i możliwości w kontekście strategicznym, przestał być już po roku aktualny[2]. Aktualizacja raportu skierowała uwagę na przyspieszenie tempa zmian w międzynarodowym środowisku bezpieczeństwa i tworzenie skumulowanych skutków na innych niż oczekiwane aspektach polityki międzynarodowej. Ryzyko kryzysu finansowego, odrodzony duch mocarstwowy Rosji, nuklearny wyścig zbrojeń, konflikty międzypaństwowe o kurczące się zasoby to niektóre z niebezpieczeństw nadchodzących czasów. Złożoność i niepewność wynikająca z natury globalnie ujmowanego świata pozwala na dostrzeganie narastania zmian w sferze bezpieczeństwa międzynarodowego, w dziedzinie gospodarki, technologii, źródeł energii i życia społecznego. Jak zauważają autorzy raportu, zmiany te to wyzwanie dla decydentów oraz planistów i wymagają one od nich kreowania nowych strategii i taktyki działań. Pomimo globalizacji i rozwoju technologii komunikacji, transportu i handlu rosnące odradzanie się świadomości, tożsamości państw narodowych jest faktem. Zdefiniowany w raporcie z 2013 roku policentryczny świat, ponad- i pozanarodowy staje się zagrożeniem dla istniejącego porządku międzynarodowego, a rosnąca współzależność państw nie jest wspierana przez instytucje porządku międzynarodowego. Powojenny system międzynarodowy stanął pod presją[3]. Te i inne aspekty rozwoju stosunków międzynarodowych wpłynęły na postrzeganie przyszłości w kategorii transferu pozycji i znaczenia państw z regionu do regionu.

[2] SFA Raport 2013, www.act.nato.int/futures-ws-1 [data dostępu: 13.02.2016].

[3] http://www.act.nato.int/images/stories/events/2012/fc_ipr/sfa2017_interim_update_coord_draft.pdf [data dostępu: 12.09.2016].

Znamienne jest, że od kryzysu gospodarczego w 2008 roku większość państw członkowskich NATO cięła wydatki obronne, kilka nawet o ponad 10%. Wydatki obronne w Azji, zwłaszcza w Azji Południowo-Wschodniej, rosły wykładniczo w ciągu ostatnich dwóch dekad. Od 2000 roku wydatki na obronność europejską wzrosły tylko o 14%, natomiast w Azji i Oceanii wydatki obronne wzrosła o 101%[4] .

Ciąg następujących równolegle bądź kolejno zdarzeń umożliwia ośrodkom analitycznym NATO – nadzorowanym przez ACT – Center of Excellence oraz Joint Warfare Centre podjęcie badań i konceptualizację założeń do przyszłych operacji Sojuszu.

Podjęte w 2015 roku działania zaowocowały identyfikacją nowych trendów rozwoju międzynarodowego środowiska bezpieczeństwa[5].

W obszarze politycznym następuje przeniesienie swoistego środka ciężkości z Zachodu do innych regionów:

- Wzrośnie znaczenie Chin i Indii jako największych gospodarek świata.
- Zmaleje znaczenie strefy europejskiej (tempo wzrostu będzie mieć wartość w granicach 1,2%), zmaleje tempo wzrostu gospodarki amerykańskiej od 2,4 do 1,7%.
- Wydatki obronne USA maleją (spadek o 36% w latach 2004–2013), natomiast Chiny wydają na zbrojenia średnio o 9,7% więcej co roku.
- W lipcu 2014 roku Brazylia, Rosja, Indie, Chiny i RPA uruchomiły nowy Bank Rozwoju – nazywany BRICS Bank – który łączy w sobie cechy Banku Światowego i Międzynarodowego Funduszu Walutowego. Chiny zaproponowały powołanie Azjatyckiego Banku Inwestycji Infrastrukturalnych: Asian Infrastructure Investment Bank, który wspierałby inwestycje infrastrukturalne w regionie Azji. Niezależne instytucje finansowe stanowią nowe mechanizmy współpracy w regionie i będą go integrować.
- Dalsze zaangażowanie Stanów Zjednoczonych w politykę bezpieczeństwa i obrony Europy i Bliskiego Wschodu nie będzie szło w parze z podtrzymywaniem wiodącej roli gwaranta bezpieczeństwa w regionie Afryki.
- Oczekuje się zmiany w możliwościach podtrzymywania zdolności Zachodu do wpływania globalnie na politykę państw.

[4] Tamże, s. 6. https://www.sipri.org/sites/default/files/SIPRI-Milex-data-1988-2015.xlsx [data dostępu: 12.10.2016].

[5] http://www.act.nato.int/images/stories/events/2012/fc_ipr/sfa2017_interim_update_coord_draft.pdf [data dostępu: 12.09.2016].

- Przyjęta przez Rosję strategia działań hybrydowych odniosła sukces i należy oczekiwać jej stosowania w polityce, jako narzędzia i środka osiągania celów politycznych, tym bardziej że gama stosowanych narzędzi w wojnie (polityce) hybrydowej może być bardzo szeroka, a poszukiwanie strategii odpowiedzi długotrwałe.
- Należy oczekiwać pojawiających się trudności w rozwiązywaniu problemów globalnych – finansowych, ekologicznych, gospodarczych, w sferze bezpieczeństwa i obrony – których współpraca międzynarodowa może nie rozwiązywać z wystarczającą determinacją.
- Osiągnięcia Arabskiej Wiosny nie spowodują zmian w najbliższym czasie co do bardziej demokratycznego modelu sprawowania rządów w Libii, Egipcie, Jemenie i legitymizacji działań sił rządzących.
- Także w przestrzeni państw posowieckich nie należy oczekiwać adopcji wartości wolności demokratycznych, do czego wydatnie przyczyni się Rosja i jej polityka.
- Policentryzm i współzależność to cechy współczesnego środowiska bezpieczeństwa.
- W polityce dużo większą rolę niż dotychczas zaczną odgrywać podmioty niepaństwowe (grupy interesów, ruchy społeczne, organizacje i osobowości indywidualne).
- W ocenie analityków w państwach demokratycznych rosnąć będzie niezadowolenie z demokracji jako formy sprawowania władzy i podziału dóbr[6].

W czasie szczytu NATO w Warszawie podjęto decyzje z jednej strony o wzmacnianiu aktywności Sojuszu w obszarach, w których już prowadzi działania, a z drugiej podjęcia ich tam, gdzie praktycznie go nie było. Stąd też do kluczowych decyzji w zakresie wzmacniania bezpieczeństwa i obrony w regionie należy:

- przedłużenie misji Resolute Support w Afganistanie ponad 2016 rok,
- wsparcie sił zbrojnych i bezpieczeństwa Afganistanu kwotą 1 mld dolarów rocznie przez NATO i państwa członkowskie co najmniej do 2020 roku,
- dalsze szkolenie żołnierzy i funkcjonariuszy służby bezpieczeństwa Afganistanu,

[6] Tamże.

- zwiększenie zaangażowania NATO w walce z ISIS poprzez: szkolenie wojsk irackich (kontynuację szkoleń irackich oficerów w Jordanii i rozpoczęcie szkoleń w samym Iraku), powstanie centrum wywiadowczego w Tunezji, udostępnienie samolotów wczesnego ostrzegania i rozpoznania AWACS koalicji,
- w dalszej kolejności przekształcenie misji Active Endeaour na Morzu Śródziemnym w misję Sea Guardian,
- wzmocnienie współpracy z Unią Europejską, której celem jest zwiększenie zdolności Europy Zachodniej do odpowiedzi na zagrożenia hybrydowe (NATO i UE podpisało porozumienie o wzajemnej współpracy w dziedzinie bezpieczeństwa, m.in. w kwestii zagrożeń hybrydowych i ataków cybernetycznych ze strony Rosji),
- uznanie cyberprzestrzeni i mediów społecznościowych jako nowy obszar operacyjny,
- ogłoszenie wstępnej gotowości operacyjnej tarczy antyrakietowej,
- zobowiązanie się przez wszystkie kraje NATO do zwiększenia zdolności obronnych poprzez m.in. utrzymanie ustalonego w czasie szczytu w Newport poziomu wydatków na obronność,
- wzmocnienie Sojuszu poprzez otwarcie na przyjęcie nowych członków – Ukrainy, Czarnogóry i Gruzji,
- wzmocnienie obecności sił Sojuszu na jego wschodniej flance – rotacyjna obecność batalionowych grup bojowych w Polsce, na Łotwie, Litwie i w Estonii[7],
- rozmieszczenie w Polsce dowództwa amerykańskiej brygady pancernej i dowództwa komponentów dywizyjnych,
- zapewnienie przez NATO o swoim „zaangażowaniu" w dbanie o potencjał broni konwencjonalnej oraz broni nuklearnej.

Przedstawione wizje zmian w środowisku bezpieczeństwa międzynarodowego pozwalają na planowanie rozwoju zdolności NATO w perspektywie najbliższych lat. W założeniach do przyszłych operacji Sojuszu (Framework for Future Alliance Operations)[8] wskazano, że środowisko bezpieczeństwa

[7] https://www.wprost.pl/szczyt-nato/10014425/Postanowienia-szczytu-NATO-w-Warszawie-to-nie-tylko-wschodnia-flanka.html [data dostępu: 12.09.2016].

[8] Framework for Future Alliance Operations – FFAO (2015), http://www.act.nato.int/images/stories/media/doclibrary/160121sfa.pdf [data dostępu: 18.03.2016].

2030 jest coraz bardziej skomplikowane i niepewne. **Przeciwnikiem** staną się podmioty zarówno państwowe, jak i niepaństwowe, które mogą działać w porozumieniu przeciwko Sojuszowi. Państwa mogą wykorzystywać podmiot niepaństwowy, ukrywając za nim swoje intencje i działania. Ocenia się, że przyszłe działania państw i „niepaństw" łączyć będą formy konwencjonalnej walki zbrojnej, działań nieregularnych i wojny w cyberprzestrzeni. Nie uniknie się aktów przemocy lub terroru. Takie działania prowadzone będą w rejonach niezarządzanych, w dużych aglomeracjach miejskich, w terenie trudno dostępnym, w miejscu występowania zasobów naturalnych.

Dostrzega się, że działanie przeciwnika może zmierzać do rozerwania spójności Sojuszu. W trakcie IV konferencji Center for Security and Strategic Research pt. „Strategic implications of multipolarity for European security" w Akademii Obrony Narodowej Republiki Łotwy[9] jej uczestnicy wskazali na konieczność integracji państw europejskich w aspekcie przeciwdziałania narastaniu wewnętrznych nacjonalizmów, przeciwdziałania propagandzie i dezinformacji ze strony mediów kontrolowanych przez Rosję, a potępiających NATO i UE. Nie ulega wątpliwości, że Rosja dysponuje obecnie największym potencjałem obronnym od końca zimnej wojny i ukierunkowała swoje strategie na operacje daleko poza granicami kraju (czego przykładem jest chociażby Syria). Działania Rosji zmierzają również do dyskredytacji tych jej przeciwników, którzy w sposób stanowczy sprzeciwiają się jej wpływowi na państwa pozostające do końca XX wieku pod jej oddziaływaniem.

Przyszłe konflikty zbrojne łączyć będą: działania specjalne, działania sił nieregularnych (najemnicy, terroryści, przestępcy), działania psychologiczne, działania w cyberprzestrzeni i mediach społecznościowych. Wykorzystywane będą każde nowe technologie, ich funkcje i metody użycia.

Sojusz określił pięć obszarów tematycznych, wokół których budował będzie swoje zdolności do przeciwstawienia się zagrożeniom konwencjonalnym i hybrydowym.

Pierwszym obszarem jest **sprawność organizacyjna** umożliwiająca siłom zbrojnym większą elastyczność, zwiększająca szybkość reakcji i adaptacji. Obszar drugi – obejmuje budowanie zdolności i możliwości oddziaływania w zakresie bezpieczeństwa poprzez **współpracę w obszarze bezpieczeństwa** szczególnie poprzez partnerstwo pozasojusznicze. Obszarem

[9] http://www.naa.mil.lv/Petnieciba/DSPC_konference.aspx [data dostępu: 12.11.2016].

trzecim jest **zdolność do utrzymania elastyczności działań.** Obejmuje potrzebę utrzymania i zwiększenia potencjału w celu zachowania odpowiednich sił do operacji. Obszar czwarty – obejmuje **świadomość strategiczną**, czyli zdolność do poznania i zrozumienia sytuacji oraz oceny możliwych zagrożeń. Ostatni obszar – **komunikacja strategiczna** – obejmuje przekaz informacyjny, upowszechnianie informacji.

W perspektywie kolejnych 15 lat uważa się, że NATO będzie musiało przeciwstawić się nowego rodzaju zagrożeniom. W tych działaniach nie będzie starało się być osamotnione, ale poprzez wzmocnienie relacji z wszystkimi członkami UE będzie budowało silniejszą pozycję jako przeciwwagę dla słabnących więzi transatlantyckich. Ta prognoza dotyczy scenariusza, w którym USA zaangażują się bardziej w podtrzymywanie swojej strefy wpływów na Bliskim i Dalekim Wschodzie wobec rosnącej roli Chin, Indii i Iranu. Przeniesienie ciężaru wysiłku politycznego nie odbędzie się gwałtownie, ale będzie on przesuwany stopniowo poprzez wpływanie na tych partnerów, którzy są zainteresowani pogłębianiem relacji dwustronnych ze Stanami Zjednoczonymi. W najbliższym okresie należy oczekiwać raczej, że USA zaangażują się tak jak to deklarowały we wzmacnianie swojej obecności w państwach Europy Środkowo-Wschodniej, ale będzie to się odbywało w trybie rotacji w ramach sił stacjonujących w Europie Zachodniej.

Kolejną strategiczną kwestią dla kształtowania miejsca i roli NATO jako filaru bezpieczeństwa w Europie i w regionie Eurazji jest rozszerzenie Sojuszu o nowych członków. Należy oczekiwać, że wobec podtrzymywania polityki destabilizacji przez Rosję wstąpienia do NATO domagać się zaczną jeszcze bardziej społeczeństwa państw skandynawskich – Szwecji i Finlandii, dla których polityka Rosji może stać się szczególnym zagrożeniem. W najbliższej perspektywie po Czarnogórze i Gruzji do członkostwa w NATO przygotowywać się będą kraje skandynawskie. Rozszerzenia Sojuszu o Ukrainę pomimo tworzenia specjalnych dla niej warunków, w zapowiedziach polityków, trudno raczej oczekiwać w najbliższej perspektywie.

Powodzenie utrzymania przewagi Sojuszu w przyszłych operacjach możliwe będzie poprzez pozyskiwanie nowych zdolności sił zbrojnych poszczególnych państw członkowskich, jak i synergicznych zdolności wydzielonych komponentów. Przewaga militarna nie stanowi podstawowego warunku osiągnięcia powodzenia w perspektywicznym konflikcie. Szybkość prowadzenia działań, przewaga informacyjna, działania ofen-

sywne w cyberprzestrzeni i determinacja w osiąganiu celów militarnych to tylko niektóre z warunków sukcesu. Otwarte pozostaje też pytanie: czy Sojusz jest przygotowany na hipotetyczny otwarty konflikt z Rosją, co prognozują ostatnio amerykańscy generałowie i dziennikarze mainstreamowi? To pytanie będzie kolejnym problemem do rozwiązania, a odpowiedź na nie tekstem następnego komunikatu.

PODSUMOWANIE

1. Sojusz będzie dążył do utrzymania przewagi technologicznej i organizacyjnej w zakresie elastyczności swoich struktur organizacyjnych i wzmacniania woli wszystkich członków do podejmowania działań adekwatnych do zagrożeń.
2. Zdolność i sprawność operacyjna Sojuszu do przeciwstawienia się nowego rodzaju zagrożeniom będzie zapewniona przez rozszerzanie działań odstraszających, których szczególnym objawem jest obecność sił Sojuszu w najbardziej wysuniętych państwach – członkach Sojuszu. Wzmocnienie wschodniej i południowo-wschodniej flanki NATO, podnoszenie gotowości dowództwa WKPW, pozyskiwanie nowych zdolności w zakresie skrócenia cyklu podejmowania decyzji o użyciu sił NATO to działania budujące strategiczny potencjał odstraszania NATO.
3. Sojusz zostanie poddany presji poszukiwania nowych koncepcji kształtowania bezpieczeństwa w swoim bliskim i dalszym otoczeniu. W chwili obecnej działania te są raczej reakcją na działania podejmowane przez Rosję, Daesh czy talibów.
4. NATO musi przygotować się do działań w środowisku cyberprzestrzeni aktywniej niż do tej pory. Sojusz musi być przygotowany do ciągłych działań w cyberprzestrzeni zarówno defensywnych, jak i ofensywnych.

Źródła internetowe

https://www.msz.gov.pl/pl/polityka_zagraniczna/szczyt_nato_2016/dokumenty_nato_1/deklaracja_szczytu_nato_w_walii_w_2014 [data dostępu: 12.09.2016].

https://www.wprost.pl/szczyt-nato/10014425/Postanowienia-szczytu-NATO-w-Warszawie-to-nie-tylko-wschodnia-flanka.html [data dostępu: 12.09.2016].

Framework for Future Alliance Operations – FFAO (2015), w: http://www.act.nato.int/images/stories/media/doclibrary/160121sfa.pdf [data dostępu: 18.03.2016].

http://www.act.nato.int/images/stories/events/2012/fc_ipr/sfa2017_interim_update_coord_draft.pdf [data dostępu: 12.09.2016].

http://www.act.nato.int/images/stories/events/2012/fc_ipr/sfa2017_interim_update_coord_draft.pdf [data dostępu: 12.09.2016].

https://www.sipri.org/sites/default/files/SIPRI-Milex-data-1988-2015.xlsx [data dostępu: 12.10.2016].

SFA Raport 2013, www.act.nato.int/futures-ws-1 [data dostępu: 13.02.2016].

http://www.naa.mil.lv/Petnieciba/DSPC_konference.aspx [data dostępu: 12.11.2016].

MAGDALENA SITEK
Wyższa Szkoła Gospodarki Euroregionalnej
im. Alcide De Gasperi
ms@wsge.edu.pl

PRAWO DO PRYWATNOŚCI W DOBIE PERMANENTNEJ INWIGILACJI WSPIERANEJ TECHNIKAMI ELEKTRONICZNYMI

THE RIGHT TO PRIVACY IN THE ERA OF PERMANENT SURVEILLANCE SUPPORTED BY THE ELECTRONIC TECHNIQUES

ABSTRACT

The right to privacy is one of the fundamental human rights and it is an expression of the need to protect the individual's dignity. Rapid technological progress, particularly in the area of information, opens the way to a fairly deep penetration into the human's privacy. Additionally, there is a process of globalization, which initiated the era of post-modernity. This era is characterized by changes in axiology, polycentricism and the loss of faith in the progress with the simultaneous acceleration of innovation. It is necessary to redefine the concepts of privacy and to build a system, based on good law, to protect the human right to privacy.

Keywords: *privacy, the Constitution of the Republic of Poland, European law, globalization, media, consumer*

STRESZCZENIE

Prawo do prywatności jest jednym z podstawowych praw człowieka i wyrazem potrzeby ochrony godności jednostki. Szybki postęp technologiczny i techniczny, w szczególności w obszarze informatyki, otwiera drogę do dość głębokiej penetracji prywatności człowieka. Do tego dochodzi jeszcze globalizacja, która zapoczątkowała epokę ponowoczesności. Epoka ta charakteryzuje się zmianami w aksjologii, policentrycznością, utratą wiary w postęp z jednoczesnym przyspieszeniem innowacyjności. Konieczne jest ponowne zdefiniowanie pojęcia prywatności oraz zbudowanie systemu jej ochrony na bazie dobrego prawa.

Słowa kluczowe: *prywatność, Konstytucja RP, prawo europejskie, globalizacja, media, konsument*

WPROWADZENIE

Prawo do prywatności należy do podstawowych praw człowieka, a jednocześnie jest fundamentalną jego potrzebą, zwłaszcza w kulturze Zachodu. Prawo to jest wyrazem wolności człowieka do decydowania o zakresie dostępu do informacji o nim samym. M. Pryciak zauważa, że sfera prywatności jest dość szeroka i obejmuje dane dotyczące samej osoby jako takiej, a także przestrzeni, w której się porusza i żyje, jak chociażby pomieszczeń, w których żyje (zob. M. Pryciak, s. 212). Autor ten wykazał, że namiastek tego prawa należy szukać już w przekazie biblijnym. Koncepcyjnie prawo to jednak było rozwijane dopiero pod koniec XIX wieku (zob. M. Pryciak, s. 213), między innymi dzięki takim badaczom, jak V. Brandeis i E. Warren (zob. S.D. Warren, L. Brandeis, 1890, s. 193–220).

Według M. Safjana prywatność jest sferą wolności człowieka, która podlega jego wyłącznej kontroli (zob. M. Safjan, 2006, s. 211 i nast.; L. Leszczyński, B. Liżewski, 2008, s. 88). Prywatność jest dobrem i prawem osobistym przynależnym każdemu człowiekowi, niezależnie od jego stanu fizycznego, psychicznego, stadium rozwoju, a także płci, wyznania bądź rasy. Podlega też ochronie prawnej. Prawo do prywatności jest sferą zamkniętą przed dociekliwością innych. Może jednak doznawać pewnych ograniczeń na podstawie szczególnych przepisów prawa, zwłaszcza dotyczących bezpieczeństwa publicznego, jak np. przeciwdziałanie wszelkim formom terroryzmu. Do tego konieczne jest niejednokrotne ingerowanie w sferę prywatności przez ustawowo uprawnione do tego służby specjalne.

Prawo do prywatności rozumiane jako sfera prywatności jest jednocześnie potrzebą każdego człowieka. Potrzeba ta jednak może być różnie rozumiana w różnych kręgach kulturowych bądź nawet grupach społecznych tej samej kultury. Inna jest granica tej sfery w przypadku naturystów, a inna w przypadku przeciwników publicznego obnażania swojej cielesności, chociaż przedstawiciele obu grup przynależą do tej samej rodziny kulturowej. Dlatego to człowiek ma wyłączne uprawnienie do decydowania o tym, jakie informacje dotyczące jego mogą być publicznie ujawnione, a które podlegają wyłączeniu i są zachowywane tylko do wiadomości samego zainteresowanego lub osób, którym te informacje ujawnił. Tak rozumiane prawo do prywatności pozwala na obronę człowieka przed nieuprawnionymi nadużyciami, np. ośmieszaniem go albo redukcjonizmem, np. sprowadzenie go do poziomu tylko konsumenta lub narzędzia do promocji samochodu – ten ostatni przypadek może dotyczyć w szczególności kobiety (zob. M. Sitek, 2016, s. 181).

Przedmiotem niniejszego opracowania jest analiza i ukazanie wpływu rozwoju współczesnych technik informatycznych na prawa człowieka, zwłaszcza w obszarze prawa do prywatności. Rozwój nowych technologii powoduje zagrożenie dla takich danych, jak: kontakty, tożsamość osoby, tożsamość telefonu, w tym jego numer, lokalizacja, historia przeglądania, e-maile, SMS-y, dane biometryczne (odciski palców, twarz), informacje pozwalające na uwierzytelnienie w usługach społecznościowych lub karta kredytowa i dane dotyczące płatności.

Już na samym początku można postawić hipotezę badawczą, że współczesne narzędzia informatyczne, takie jak portale społecznościowe, bazy danych, programy do współdzielenia dokumentów, budowane są z wykorzystaniem elementów psychologii człowieka, jego potrzeb, zwłaszcza zaspokojenia wiadomości o życiu innych, a także potrzeby dzielenia się z innymi swoimi sekretami, sukcesami, porażkami bądź uczuciami. Ta potrzeba rośnie proporcjonalnie do narastania zjawiska samotności w społeczeństwie masowym, wielokulturowym. Ludzie szukają przyjaźni coraz częściej właśnie w Internecie, nie zaś w świecie realnym (zob. J. Zawisza, s. 403–415). Praca ma być odpowiedzią na podstawowe obecnie pytanie, a mianowicie: na ile rozwój technik informatycznych ogranicza tradycyjnie rozumiane prawo prywatności? Drugim pytaniem jest: czy można mówić dzisiaj o prywatności w świetle postępu technologicznego umożliwiającego właściwie bezgraniczną ingerencję w sferę prywatności człowieka?

TECHNOLOGIA ELEKTRONICZNA ZAGROŻENIEM DLA PRAWA DO PRYWATNOŚCI?

W kulturze Zachodu prawo do prywatności jest jednym z tych praw człowieka, które obok prawa do życia są najczęściej naruszane nie tylko przez media, ale również przez organy państwowe, instytucje biznesowe bądź też przez portale społecznościowe.

Media

Tempo współczesnego postępu technologicznego najlepiej uwidacznia się w obszarze mediów. Polega on na odchodzeniu od mediów tradycyjnych, czyli gazety, a nawet telewizji. Ich miejsce zajmuje Internet i urządzenia mobilne, zwłaszcza telefon. Zmienia się też filozofia komunikowania i formy zagrożeń. Dodaną wartością tych przemian jest łatwość komunikowania

się, wymiany informacji, większa aktywizacja społeczeństwa, podniesienie poziomu kultury ogólnej i zaspokojenie w większym stopniu niż dotychczas potrzeby informacji.

Różne formy funkcjonowania mediów można sprowadzić do tych, które zalicza się do mediów tradycyjnych i tych, które zalicza się do mediów interaktywnych. Co do zasady, oba rodzaje mediów spełniają te same funkcje, tj. przekazywanie różnorakich informacji. Zasadnicza jednak różnica między nimi koncentruje się na roli czytelnika. W mediach tradycyjnych jest on biernym odbiorcą informacji wytwarzanych przez określone centra opiniotwórcze, nierzadko skoncentrowane w ręku kilku potentatów prasowych. Z klei w mediach interaktywnych odbiorca staje się jednocześnie odbiorcą i aktorem, który nie tylko czyta, ogląda, ale i tworzy. Do tego służą możliwości komentowania artykułów zamieszczanych w mediach elektronicznych, tworzenie blogów bądź też własnych storn internetowych (zob. Ł. Kołodziejczyk, 2014).

W konsekwencji codziennie dostarczane są informacje ze świata polityki, gospodarki, sportu, kultury, nauki, ale też ważne miejsce zajmują informacje dotyczące życia prywatnego gwiazd filmowych, polityków lub innych osób publicznych. Społeczna potrzeba sensacji popycha dziennikarzy do łamania coraz to nowych granic tabu, dostarczając szczegółów pochodzących ze sfery prywatności albo nawet sfery intymnej, o istnieniu których przeciętny człowiek nie ma pojęcia (zob. M. Puwalski, 2003, s. 11). Jedną z najbardziej negatywnych grup dziennikarzy są wszechobecni paparazzi, dla których nie ma żadnych granic moralnych ani etycznych.

Media interaktywne stworzyły nieograniczone możliwości nie tylko odbioru, ale i produkcji oraz dystrybucji, a także rozpowszechniania informacji pozytywnych i negatywnych. Przykładem może być rozpowszechnianie treści pornograficznych, ale też np. rasistowskich. W mediach tradycyjnych odbiorca był biernym uczestnikiem rynku pornograficznego. Obecnie jest nie tylko odbiorcą, ale też może sam dostarczać materiału, chociażby w postaci zdjęć zrobionych samemu sobie i umieszczonych w sieci, a które następnie są powielane najczęściej już bez jego zgody czy wiedzy (zob. D. Boyd, 2007). Media interaktywne pozwalają również na szerzenie agresji lub też wyrządzanie szkody na poszczególnych dobrach osobistych człowieka, o których jest mowa w art. 23 kc (zob. J. Pyżalski, 2012, s. 92). W szczególności zagrożone bądź naruszane jest dobro, jakim jest atak na dobre imię innych

osób poprzez zniesławienie, czyli ujawnianie prawdziwych i nieprawdziwych informacji o charakterze intymnym albo prywatnym. Raz ujawnione w ten sposób zniesławiające informacje i zamieszczone w tzw. chmurze, są nie do usunięcia. Wprawdzie wprowadzone zostało prawo do zapomnienia, czyli możliwość usunięcia z sieci danych wrażliwych, w praktyce jednak jest to prawie niemożliwe. Wpisy te są chronione domniemaniem, że posiadają one znaczenie dla społeczeństwa.

Można powiedzieć, że chociaż rozwój interaktywnych mediów ma niewątpliwie pozytywny wkład w rozwój naszej cywilizacji, to jednak należy brać pod uwagę również i zagrożenia dla właśnie prywatności jednostki.

Służby specjalne

We wzroście poziomu działań ograniczających sferę prywatności mają swój udział również organy państwa, a zwłaszcza jego służby korzystające z coraz to nowszych urządzeń inwigilujących. Do tego wykorzystywane są urządzenia tak mobilne (telefony mobilne, chipy w telefonach, gniazdkach do prądu, żyrandolach itp.), jak i stałe (np. kamery). Z jednej strony społeczeństwo masowe wymusza, a nawet żąda i akceptuje zwiększenie poziomu kontroli w celu zapewnienia bezpieczeństwa w wymiarze jednostkowym i wspólnotowym. Z drugiej jednak strony narasta coraz większy społeczny niepokój wobec permanentnej inwigilacji prowadzonej prawie że już na wzór orwellowskiego Wielkiego Brata z książki pt. „Rok 1984".

W państwie prawa służby zobowiązane są do podejmowania działań na podstawie prawa i w zakresie swoich kompetencji określonych ustawami. Tak to ustawodawca zapisał w art. 5 ust. 1 pkt 3 ustawy z 9 czerwca 2006 roku o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (t.j. Dz.U. 2016 poz. 1318). Działania wszystkich służb winny przestrzegać postanowień ustawy z 5 sierpnia 2010 roku o ochronie informacji niejawnej (t.j. Dz.U. 2016 poz. 1167).

Nie zawsze jednak działania służb bezpieczeństwa są uzasadnione, a nawet często motywowane są imperatywami o charakterze politycznym w celu np. dyskredytacji oponenta bądź oponentów politycznych. Gromadzone dane przez funkcjonariuszy mogą być potem wykorzystywane do szantażowania albo politycznej eliminacji danej osoby. Służby dzięki takim informacjom mogą mieć realny wpływ na wydarzenia polityczne. Przykładem wybory w USA, kiedy to FBI stopniowo ujawniała maile pochodzące

z komputera Hillary Clinton. W efekcie przegrała ona wybory. Do dzisiaj nie zostały wyjaśnione motywy, ani tym bardziej to, kim byli prawdziwi protektorzy nagrań członków rządu PO-PSL, jakie miały miejsce w 2013 roku w restauracji „Sawa i Przyjaciele". Doszło wówczas do ujawnienia szeregu informacji należących do sfery prywatności, nawet osób publicznych. Widocznym efektem tych działań były przegrane w 2015 roku wybory przez ówczesne elity rządzące.

Specyfika służb oraz możliwości techniczne sprawiają, że istniejące normatywne ograniczenia, chociażby w znowelizowanej w 2016 roku ustawie w sprawie zasad inwigilacji, nie ograniczają wykraczania służb poza te granice. Każdy motyw – prawdziwy bądź nieprawdziwy – jest dobry dla działań ludzi zatrudnionych we wszelkiego rodzaju agencjach. We wspomnianej noweli kontrola operacyjna nie może trwać dłużej niż 18 miesięcy. Może za to polegać na podsłuchu, poglądzie osób w pomieszczeniach, środkach transportu, kontroli korespondencji, w tym elektronicznej, kontroli przesyłek, kontroli informatycznych nośników danych systemów informatycznych i teleinformatycznych. Służby mogą inwigilować za pomocą nadajnika GPS i z wykorzystaniem dronów. Obowiązek przechowywania bilingów został utrzymany na wcześniejszym poziomie, tj. 12 miesięcy. Nad tymi działaniami pozostaje właściwie tylko kontrola sądowa.

Biznes

Trzecią grupą podmiotów gromadzących dane o jednostce i jej funkcjonowaniu w społeczeństwie są instytucje biznesowe, jak banki, sieci sklepów, pizzerii, dealerzy samochodów, sklepy internetowe itp. Dane dotyczące prywatności gromadzone są za pomocą kart płatniczych, kart lojalnościowych, poprzez używanie wielu aplikacji na telefon oraz komputer. Nieuczciwe aplikacje są w stanie przesłać na zdalny serwis informacje z książki adresowej, informacje na temat sieci albo samego urządzenia, ustalić lokalizację urządzenia, a tym samym i jego posiadacza. Ponadto ściągnięte aplikacje mogą uzyskiwać dostęp do wielu funkcjonalności urządzenia. W konsekwencji ze zdalnego komputera mogą być wysłane na rachunek posiadacza urządzenia SMS-y albo maile. Można w ten sposób przejmować zdjęcia. Media co jakiś czas donoszą, że zostały skradzione intymne zdjęcia z komputera znanych aktorek. Nie zawsze twórcy aplikacji informują użytkowników o rodzaju i celu gromadzenia informacji. Większość z uzyskanych w ten sposób da-

nych przekazywana jest osobom trzecim dla przeprowadzenia analizy. To wszystko jest robione w celu pozyskania, a następnie zbudowania obrazu potrzeb potencjalnego klienta (zob. L. Pułka, 2010).

Przykładem działań powyżej opisanych może być informacja, jaka ukazała się na portalu auto-swiat.pl. Znamienny jest już sam tytuł artykułu, a mianowicie „Uważaj: Twoje auto to szpieg"[1]. Autor artykułu opisał sposób gromadzenia informacji producenta samochodów o ich użytkownikach. Zamontowane urządzenia w najnowszych typach samochodów zbierają takie dane, jak: położenie, przebieg kilometrów, zużycie paliwa, stan paliwa w zbiorniku oraz błędy odnotowane przez układy diagnostyczne. Ponadto monitorowany jest styl jazdy, brak zamknięcia drzwi w czasie parkowania, a także przekroczenie dozwolonej liczby obrotów silnika, czyli bardzo szybka jazda samochodem. Takie systemy do monitorowania pracy samochodu, ale też i użytkownika montują już w najnowszych modelach BMW i Volvo. Systemy te pozwalają na wyciągnięcie korzyści dla obu stron, tj. użytkownika i producenta. Zebrane dane pozwalają bowiem na usprawnienie funkcjonowania samochodów i poszczególnych jego elementów, usprawnienie ruchu na drodze, zwiększają bezpieczeństwo użytkowania. Z drugiej jednak strony gromadzone dane są poddawane analizie, najczęściej w firmach zewnętrznych dla producentów. Działania te są podejmowane w celu zbudowania sylwetki użytkownika dla potrzeb marketingu bądź też dla innych celów. W tym kontekście konieczne jest zastanowienie się nad bezpieczeństwem danych gromadzonych przez producenta samochodów. Co robi z danymi firma analityczna? Na ile te dane są tam bezpieczne, a nie są np. przedmiotem handlu? Dalej, na ile te dane są wrażliwe i pozwalają na identyfikację użytkownika? Jaka jest podstawa prawna dla takiego działania? Na te pytania bez drobiazgowej analizy sposobów gromadzenia oraz wykorzystywanych urządzeń do gromadzenia odpowiedź jest prawie niemożliwa.

Portale społecznościowe

Odrębną grupą narzędzi wykorzystywanych do gromadzenia danych należących do sfery prywatności są portale społecznościowe, np. Facebook, Instagram, Nasza Klasa, które zostały stworzone w oparciu o jedną

[1] http://www.auto-swiat.pl/eksploatacja/uwazaj-twoje-auto-to-szpieg-wyjasniamy-po-co-producentom-dane-o-autach-i-kierowcach/4e0b6d [data dostępu: 29.11.2016].

z największych słabości człowieka, a mianowicie potrzebę chwalenia się zdjęciami, podróżą lub innymi zdarzeniami z życia osobistego. Tak informatycznie i psychologicznie skonstruowane narzędzia wywołują brak autokontroli u wielu użytkowników tych portali. Oni sami dokonują samoobnażania się, zdradzając miejsca pobytu, zamieszczając zdjęcia z wakacji, nierzadko intymne. Do tej samej kategorii narzędzi należy zaliczyć iCloud lub iCloud Drive. W obu przypadkach jest to tzw. chmura, w której można przechować zdjęcia, dokumenty, apki, notatki, kontakty, a także dokumenty prywatne, naukowe albo służbowe.

Jednym z przykładów portali społecznościowych są portale randkowe oraz matrymonialne. Chociaż inne mają one cele niż FB oraz Instagram, to jednak ich funkcjonowanie opiera się na podobnych zasadach. Na portalach randkowych oraz społecznościowych spotykają się osoby, które chcą realizować swoje potrzeby o charakterze matrymonialnym bądź tylko towarzyskim, o charakterze krótkotrwałym. Portale tego rodzaju stosują różne techniki gromadzenia informacji o różnym charakterze. Bez wątpienia chodzi jednak nierzadko o dane wrażliwe, zaliczane do dóbr osobistych wchodzących w skład sfery prywatności. Są to takie dane, jak światopogląd, stosunek do religii, orientacja i preferencje seksualne. Dane te są gromadzone w celu lepszego doboru partnerów.

Jednak z funkcjonowaniem tych portali wiąże się wiele wątpliwości i pytań natury technicznej i prawnej. Przede wszystkim rodzi się pytanie o to, czy klienci są poprawnie informowani o tym, co dzieje się z ich danymi, nierzadko wyjątkowo drażliwymi. Jaka jest gwarancja, że osoba przeglądająca opis w celu poszukiwania partnera zachowa w tajemnicy uzyskane dane wrażliwe? Kto ponosi odpowiedzialność prawną za ujawnienie tych danych w sieci lub w środowisku rodzinnym, zawodowym bądź małych społeczności? Problem nie jest łatwy ani z punktu widzenia technicznego, ani prawnego, a to z tego względu, że już ponad 3 mln Polaków odwiedza takie portale[2]. W USA jedno na sześć zawartych małżeństw ma swoje początki w korzystaniu z portali matrymonialnych.

Korzystanie z portali matrymonialnych albo randkowych rodzi też problemy natury prawnej i finansowej, jak np. odpłatność za korzystanie

[2] *Oto najpopularniejsze serwisy randkowe w Europie*, http://interaktywnie.com/biznes/artykuly/portale/oto-najpopularniejsze-serwisy-randkowe-w-europie-250222 [data dostępu: 29.11.2016].

z nich. Co do zasady nieodpłatne korzystanie z tych portali jest czasowe, zwykle do 6 miesięcy. Użytkownicy najczęściej nie czytają treści umowy, w której nierzadko zapisane jest, że przed upływem okresu darmowego korzystania z portalu należy umowę wypowiedzieć. Zaniedbanie tego obowiązku skutkuje naliczaniem opłat. Do tego w przypadku sporu najczęściej stosuje się prawo niemieckie i sądy niemieckie, chociaż portale są pisane w języku angielskim albo polskim. Takie rozwiązanie powoduje, że dochodzenie roszczeń jest bardzo utrudnione. Portale te często nie mają jasno zbudowanych polityk prywatności. Te mechanizmy stosowane są również w innych rodzajach portali.

Badania naukowe

Kolejnym obszarem możliwego naruszenia prawa do prywatności jest przechowywanie próbek i profili DNA. W jednym z wyroków Europejskiego Trybunału Praw Człowieka odnotowano, że odciski palców, próbki i profile DNA zawierają wiele wrażliwych i osobistych informacji o osobie, wliczając w to dane o stanie zdrowia. Istnienie niepowtarzalnego kodu genetycznego umożliwia identyfikację osoby, a także jej bliskich. Tym samym gromadzenie tych danych może być naruszeniem art. 8 i 14 Europejskiej Konwencji Praw Człowieka, co zostało zarzucone rządowi Wielkiej Brytanii. W wyroku ETPCz z 4 grudnia 2008 roku 3056/04 (S. i Marper przeciwko Wielkiej Brytanii) stwierdzono, że tylko termin „prywatność" i „życie prywatne" jest szerokim terminem, niemającym wyczerpującej definicji i kryje się pod nim psychiczna i fizyczna integralność osoby. Trybunał orzekł, że samo gromadzenie tych danych nie narusza postanowień ETPC, dopiero charakter i ilość informacji zawartych w próbkach oraz ich przechowywanie bez wyraźnego powodu musi zostać uznane za naruszające prawo do poszanowania prywatności osób, których sprawa dotyczy.

Ponadto Trybunał zauważył, że nie można tak samo traktować przechowywania próbek biologicznych i profili DNA, jak i przechowywania odcisków palców, a to ze względu na ilość danych zgromadzonych w materiale DNA. Nie oznacza to, że przechowywanie odcisków palców bez zgody osób zainteresowanych jest bez znaczenia.

Innym przykładem może być wprowadzenie e-mediacji nowelizacją kpc, jaka weszła w życie z dniem 8 września 2016 roku. Mediacja rodzinna dotyczy zawsze danych wrażliwych o różnym charakterze. Dotyczy

więc wspólnej historii życia dwóch osób, ale też zdarzeń jednej lub drugiej strony uczestniczącej w mediacji. W zamyśle ustawodawcy było ułatwienie prowadzenia mediacji pomiędzy osobami zamieszkującymi w znacznej od siebie odległości, oszczędzenie środków na przejazd i po prostu uniknięcie kolejnego konfliktu między stronami przy okazji fizycznego spotkania. Komunikacja między stronami i mediatorem odbywa się za pomocą komunikatorów Gadu-Gadu, Facebooka i innych. Wątpliwości jednak, jakie tu są wskazywane przez doktrynę dotyczą bezpieczeństwa transmisji przekazu podczas mediacji. W przypadku komunikatorów pisemnych: w jaki sposób tekst zapisany jest chroniony? Najczęściej mediator korzysta z komunikatorów powszechnie dostępnych i łatwych do przechwycenia przez osoby niepożądane (zob. A. Arkuszewska, M. Bosak, 2008, s. 166; M. Bobrowicz, 2008, s. 27–28).

OCHRONA PRAWNA PRZED NARUSZENIEM PRYWATNOŚCI

Zdobyte w ten sposób informacje o jednostce, grupie społecznej, np. klasie, a także o grupie zawodowej, sąsiedzkiej itp. są nie tylko gromadzone, ale przede wszystkim przetwarzane. Pomimo zapewnień o uczciwości czy istnienia kodeksów etyki informatyka, w wielu przypadkach dane te są przetwarzane nielegalnie. Istniej rynek danych zgromadzonych w ten sposób o jednostce czy jakiejś grupie społecznej. Takie działania nie tylko mogą budzić moralny sprzeciw, etyczną odrazę, ale mogą być również najnormalniej w świecie bezprawne. Jakie zatem jest lub powinno być remedium na tego rodzaju przypadki? W jaki sposób chronić prywatność zwłaszcza jednostki? Niewątpliwie takim narzędziem do ograniczenia, a przynajmniej rzetelnej kontroli nad gromadzonymi bazami danych jest dobre ustawodawstwo. Czyli nadążające za zmianami nie tylko mentalnościowymi, które są coraz szybsze, ale również, a może przede wszystkim, za rewolucją technologiczną.

Najszersze spektrum narzędzi prawnych służących do ochrony prywatności stworzyła Unia Europejska. Wystarczy tylko wyliczyć akty normatywne wydane głównie dla ochrony danych osobowych, a w konsekwencji i dóbr osobistych. Do najważniejszych z nich należy zaliczyć:

- dyrektywę 2002/58/WE z dnia 12 lipca 2002 roku w sprawie przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (Dz.Urz. WE L 201 z 31.07.2002),

- dyrektywę 2002/21/WE z dnia 7 marca 2002 roku w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (Dz.Urz. WE L 108 z 24.04.2002),
- dyrektywę 2002/20/WE z dnia 7 marca 2002 roku w sprawie zezwoleń na udostępnienie sieci i usługi łączności elektronicznej (Dz.Urz. WE L 108 z 24.04.2002),
- dyrektywę 2002/19/WE z dnia 7 marca 2002 roku w sprawie dostępu do sieci łączności elektronicznej i urządzeń towarzyszących oraz ich łączenia (Dz.Urz. WE L 108 z 24.04.2002),
- dyrektywę 2002/22/WE z dnia 7 marca 2002 roku w sprawie usługi powszechnej i praw użytkowników odnoszących się do sieci i usług łączności elektronicznej (Dz.Urz. WE L 108 z 24.04.2002),
- dyrektywę 2002/58/WE z dnia 12 lipca 2002 roku w sprawie przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (Dz.Urz. WE L 201 z 31.07.2002),
- dyrektywę 2002/77/WE z dnia 16 września 2002 roku w sprawie konkurencji na rynkach sieci i usług łączności elektronicznej (Dz.Urz. WE L 249 z 17.09.2002),
- dyrektywę 2014/53/UE z dnia 16 kwietnia 2014 roku w sprawie harmonizacji ustawodawstw państw członkowskich dotyczących udostępniania na rynku urządzeń radiowych i uchylającej dyrektywę 1999/5/UE (Dz.Urz. UE L 153 z 22.05.2014, str. 62);
- dyrektywę 89/336/EWG z dnia 3 maja 1989 roku o zbliżeniu praw państw członkowskich dotyczących kompatybilności elektromagnetycznej (Dz.Urz. L 139 z 23.05.89).

Analiza powyższych przepisów prawa pozwala na stwierdzenie, że współczesne społeczeństwo informacyjne, w szczególności poszanowanie życia prywatnego i ochrona danych osobowych – są ważnym obszarem działania Unii Europejskiej. Między innymi poprzez Europejską Agendę Cyfrową, Komisja Europejska podkreśliła kluczową rolę ICT, w szczególności Internetu, który stanowi „ważny środek działalności gospodarczej i społecznej: służy on pracy, zabawie, komunikacji oraz pozwala na swobodne wyrażanie poglądów[3].

[3] Unijny plan bezpieczeństwa cybernetycznego na rzecz ochrony otwartego Internetu oraz wolności i możliwości w Internecie, http://europa.eu/rapid/press-release_IP-13-94_pl.htm [data dostępu: 2.12.2016].

Podkreśla się potrzebę wzmocnienia zaufania i bezpieczeństwa w sieci oraz zagwarantowanie dostępu do różnych informacji, źródeł i poglądów. Można to osiągnąć poprzez zajęcie się problematyką praw podstawowych w cyberprzestrzeni, w szczególności poprzez wzmocnienie polityki na rzecz ochrony i poprawy wolności i pluralizmu mediów, wspierania umiejętności korzystania z mediów, wspierania ochrony prywatności i danych osobowych oraz zwalczania cyberprzestępczości (zob. A. Mednis, 2006). Na poziomie UE podjęto konkretne inicjatywy, takie jak dyrektywa w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, strategia UE w zakresie cyberprzestępczości, uruchomienie w ramach Europolu Europejskiego Centrum ds. Walki z Cyberprzestępczością, dyrektywa w sprawie zapobiegania handlowi ludźmi oraz nowe ramy prawne UE dotyczące ochrony danych. Prawa podstawowe w Internecie są także ważnym elementem zarządzania Internetem[4].

W prawie polskim podstawę ochrony prawa do prywatności stanowi art. 47 ust. 2 Konstytucji RP gwarantujący ochronę prawa każdego człowieka do poszanowania życia rodzinnego, czci, dobrego imienia oraz decydowania o swoim życiu. Ponadto w art. 49 Konstytucji RP ustrojodawca gwarantuje swobodę i tajemnicę komunikowania się, w art. 50 nienaruszalność mieszkania, a w art. 50 ust. 1 gwarantowana jest ochrona informacji dotyczących danej osoby.

Prawo do prywatności wymaga również ochrony informacji o aktywności człowieka na rynku konsumenckim. Karty kredytowe, przedpłatnicze (pre-paid), debetowe, bankomatowe bądź karty lojalnościowe pozwalają nie tylko na identyfikację konsumenta, ale przede wszystkim na odtworzenie jego osobowości. Uzyskane w ten sposób dane mogą być następnie wykorzystywane do marketingu, a także dla dokonywania czynów przestępczych. Wytworzony na podstawie karty płatniczej profil konsumenta może posłużyć do sprofilowania przesyłanej mu oferty. W konsekwencji konsument może być nękany ofertami poprzez maile, telefony albo oferty przesyłane pocztą. Stąd w art. 76 Konstytucji RP zapisano zobowiązanie władz publicznych do stworzenia systemu normatywnego i instytucjonal-

[4] Decyzja Rady ustanawiająca wieloletnie ramy prac dla Agencji Praw Podstawowych Unii Europejskiej na lata 2018–2022. COM(2016) 442 final.

nego w celu ochrony konsumentów oraz użytkowników i najemców przed naruszeniem ich prywatności i nieuczciwymi praktykami rynkowymi, w tym poprzez handel danymi w celu oferowania produktów lub usług w porze obiadowej. Wypełnienie tego konstytucyjnego zadania ustawodawca spełnił poprzez wprowadzenie art. 22.1 do Kodeksu cywilnego, w którym zdefiniowano pojęcie konsumenta, oraz poprzez art. 66.1 kc, w którym ustawodawca wprowadził regulacje dotyczące wymogów, jakie musi spełniać oferta elektroniczna.

Prawo do prywatności jest kwalifikowane jako dobro osobiste chronione na podstawie art. 23 Kodeksu cywilnego. Nie jest ono *expressis verbis* wymienione w tekście przepisu, jednak *opinio communis* oraz orzecznictwo wyraźnie wskazują na interpretację rozszerzającą art. 23 kc. Ochrona prawa do prywatności może być realizowana nie tylko na drodze cywilnej (art. 23 kc), ale również i karnej (art. 212–217 kk). Podstawowym jednak aktem prawnym służącym do ochrony prywatności jest ustawa z 29 sierpnia 1997 roku o ochronie danych osobowych. Według art. 1 ust. 1 tejże ustawy ochronie podlegają wszelkie dane osobowe, które mogłyby doprowadzić do zidentyfikowania lub nawet stworzenia możliwości zidentyfikowania osoby fizycznej.

W art. 1 ust. 1 pkt 7 ustawy z dnia 16 lipca 2005 roku prawo telekomunikacyjne (t.j. Dz.U. z 2016 r. poz. 1489; dalej: PrTel) ustawodawca postanowił, że tym aktem prawnym określa m.in. warunki ochrony użytkowników usług, w szczególności w zakresie prawa do prywatności i poufności. Ochrona ta jest realizowana głównie przepisami działu VII, ale nie tylko. W art. 56 PrTel ustawodawca określił formę i treść umowy telekomunikacyjnej z odbiorcą końcowym. Zgodnie z art. 56 ust. 3 pkt 19 PrTel w takiej umowie należy określić „sposób przekazywania abonentowi informacji o zagrożeniach związanych ze świadczoną usługą, w tym o sposobach ochrony bezpieczeństwa, prywatności i danych osobowych". Według S. Piątka w przepisie tym ustawodawca zobowiązał dostawcę usługi do przekazywania informacji abonentowi o sposobach ochrony bezpieczeństwa, prywatności i danych osobowych. Obowiązek przygotowania strategii bezpieczeństwa nałożył na prezesa UKE (zob. S. Piątek, 2013, Legalis). Filozofia ochrony prywatności w PrTel opiera się na zapewnieniu bezpieczeństwa i integralności sieci, usług oraz przekazu komunikatów w związku ze świadczonymi usługami integralności.

PODSUMOWANIE

Prawo do prywatności, dość dobrze dookreślone w XX wieku, ulega daleko idącym zmianom. Powodowane są one szybkim postępem technologicznym i technicznym, w szczególności w obszarze informatyki. Do tego dochodzi jeszcze globalizacja, która zapoczątkowała epokę ponowoczesności. Epoka ta charakteryzuje się zmianami w aksjologii, policentrycznością, utratą wiary w postęp z jednoczesnym przyspieszeniem innowacyjności.

Najważniejszą jednak cechą obecnej epoki jest postęp techniczny. Pozwala on na niezwykle głębokie wchodzenie w życie człowieka, a właściwie na jego permanentne „podglądanie" i „podsłuchiwanie". Możliwości technologiczne pozwalają na gromadzenie ogromnej ilości danych przez służby, organy administracji państwowej i samorządowej oraz przez prywatne firmy. To sprawia, że sfera prywatności, a nawet intymności podlega ciągłemu kurczeniu się. Konieczne zatem jest ponowne zdefiniowanie pojęcia prywatności oraz budowanie jej ochrony na dobrym prawie. Chodzi tutaj nie tylko o dobre prawo od strony legislacyjnej, ale takie, które dostosowane będzie do potrzeb nowych technologii i człowieka posługującego się najnowszymi wynalazkami technologicznymi. Tym bardziej że użytkownik nie zawsze jest świadomy możliwości urządzeń, którymi się posługuje, i sam udostępnia liczne informacje o sobie, najczęściej nieświadomie. Ponadto prawna ochrona prywatności aby była skuteczna – winna mieć charakter międzynarodowy.

Bibliografia

Arkuszewska A., Bosak M. (2008). *Mediacja jako metoda rozwiązywania indywidualnych i zbiorowych sporów z zakresu prawa pracy*, [w:] J. Olszewski (red.), *Sądy polubowne i mediacja*. Warszawa.

Bobrowicz M. (2008). *Mediacja. Jestem za*. Warszawa.

Boyd D. (2007). *Why youth (heart) social network sites: The role of networked publics in teenage social life*, [w:] D. Buckingham (ed.). *Mc Arthur Foundation on Digital Learning – youth, identity, and digital media volume*. Cambridge.

Decyzja Rady ustanawiająca wieloletnie ramy prac dla Agencji Praw Podstawowych Unii Europejskiej na lata 2018–2022. COM(2016) 442 final.

Kołodziejczyk Ł. (2014). *Prywatność w Internecie*. Warszawa.

Leszczyński L., Liżewski B. (2008). *Ochrona praw człowieka w Europie – szkic zagadnień podstawowych*. Lublin.

Mednis A. (2006). *Prawo do prywatności a interes publiczny*. Warszawa.

Piątek S. (2013). *Prawo telekomunikacyjne. Komentarz*. Warszawa.

Pryciak M. (2010). *Prawo do prywatności*. „Studia Erasmiana Wratislaviensia", nr 4.

Pułka L. (2010). *Utracona prywatność: u progu XX-wiecznej ekspansji mediów: studia antropologiczne*. Wrocław.

Puwalski M. (2003). *Prawo do prywatności osób publicznych*. Toruń.

Pyżalski J. (2012). *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży*. Kraków.

Safjan M. (2006). *Prawo do ochrony życia prywatnego*, [w:] *Szkoła Praw Człowieka, Helsińska Fundacja Praw Człowieka*. Warszawa, s. 211 i nast.

Sitek M. (2016). *Prawa (potrzeby) człowieka w ponowoczesności*. Warszawa.

Warren S.D., Brandeis L. (December 1890). *The Right to Privacy*. Harvard Law Review, vol. IV.

Zawisza J., *Cyberprzestrzeń jako zagrożenie bezpieczeństwa państwa*, JoMS 4/27/2015.

Źródła internetowe

http://www.auto-swiat.pl/eksploatacja/uwazaj-twoje-auto-to-szpieg-wyjasniamy-po-co-producentom-dane-o-autach-i-kierowcach/4e0b6d [data dostępu: 29 11 2016].

Oto najpopularniejsze serwisy randkowe w Europie, http://interaktywnie.com/biznes/artykuly/portale/oto-najpopularniejsze-serwisy-randkowe-w-europie-250222 [data dostępu: 29.11.2016].

Unijny plan bezpieczeństwa cybernetycznego na rzecz ochrony otwartego Internetu oraz wolności i możliwości w Internecie, http://europa.eu/rapid/press-release_IP-13-94_pl.htm [data dostępu: 2.12.2016].

Źródła prawa

Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 23 sierpnia 2016 roku w sprawie ogłoszenia jednolitego tekstu ustawy – Prawo telekomunikacyjne (Dz.U. 2016 poz. 1489).

Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 28 lipca 2016 roku w sprawie ogłoszenia jednolitego tekstu ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz.U. 2016 poz. 1318).

Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 6 lipca 2016 roku w sprawie ogłoszenia jednolitego tekstu ustawy o ochronie informacji niejawnych (Dz.U. 2016 poz. 1167).

RYSZARD GROSSET
Szkoła Główna Służby Pożarniczej
ryszard.grosset@gmail.com

MAŁGORZATA CIUKA-WITRYLAK
Szkoła Główna Służby Pożarniczej
gosiaciuka@gmail.com

KARINA JAROSŁAWSKA-KOLMAN
Szkoła Główna Służby Pożarniczej
karina.kolman@gmail.com

WOJCIECH JAROSZ
Szkoła Główna Służby Pożarniczej
wjarosz@sgsp.edu.pl

MARCIN ŁAPICZ
Szkoła Główna Służby Pożarniczej
marcinlapicz@gmail.com

KONCEPCJA SYSTEMU EWAKUACJI I RATOWANIA POSZKODOWANYCH EVACOPNET PODCZAS KLĘSK ŻYWIOŁOWYCH Z WYKORZYSTANIEM NOWYCH TECHNOLOGII

THE CONCEPT OF EVACUATION AND RESCUE OF VICTIMS EVACOPNET DURING NATURAL DISASTERS USING THE NEW TECHNOLOGY

ABSTRACT

Saving lives and health of the people is the most important of the tasks imposed on National Firefighting and Rescue System (NFRS) and is an integral part of any kind of emergency. For the health and lives of people in the danger zone they correspond to the rescuers, mostly firefighters. Their chief mission is to master the threat, and in terms of qualified first aid and emergency medical evacuation of vulnerable people out of dangerous area. In some cases it is necessary to conduct an effective triage, which is a big challenge for emergency services. According to the idea rescue the most important aspect of the fight against natural disasters and civilization is to minimize human and material losses. Currently implemented are warning systems and broad public education on the prevention and mitigation of disasters and behavior of their occurrence. The missing link in the chain of survival, which would improve the conduct of activities in the areas covered by large-scale disaster is to implement a monitoring system for the victims and rescue teams in the zone of influence.

Keywords: *evacuation, system monitoring, triage, medical emergency, chain of survival, new technology, NFRS*

STRESZCZENIE

Ratowanie życia i zdrowia poszkodowanych jest integralną częścią każdego zagrożenia oraz głównym założeniem Krajowego Systemu Ratowniczo-Gaśniczego (KSRG). Za zdrowie i życie ludzi, którzy znaleźli się w strefie niebezpiecznej, odpowiadają ratownicy, głównie strażacy. Nadrzędnym celem ich działania jest opanowanie zagrożenia, ewakuacja osób z zagrożonej strefy oraz udzielenie niezbędnej kwalifikowanej pierwszej pomocy. W przypadku zdarzeń masowych lub mnogich konieczne jest przeprowadzenie triage'u, który zawsze jest wyzwaniem dla służb ratunkowych. Zgodnie z ideą ratownictwa najważniejszym aspektem w zwalczaniu klęsk żywiołowych i cywilizacyjnych jest zminimalizowanie strat ludzkich i materialnych. Obecnie wdrażane są systemy oraz szeroka edukacja społeczeństwa w zakresie zapobiegania i łagodzenia skutków katastrof, a także ostrzeżenia o ich wystąpieniu. Brakującym ogniwem w łańcuchu przeżycia, które mogłoby poprawić prowadzenie działalności w obszarach objętych katastrofą na wielką skalę, jest wdrożenie systemu monitoringu dla ofiar i zespołów ratowniczych w strefie oddziaływania.

Słowa kluczowe: *ewakuacja, system monitoringu, triage, ratownictwo medyczne, łańcuch przeżycia, nowe technologie, KSRG*

WPROWADZENIE

Zgodnie z ideą ratownictwa najważniejszym elementem walki z katastrofami naturalnymi i cywilizacyjnymi jest zminimalizowanie strat ludzkich i materialnych. Obecnie zarówno w kraju, jak i na świecie duży nacisk kładzie się na edukację społeczeństwa polegającą na wdrożeniu prawidłowego postępowania podczas wystąpienia katastrof. Niestety, element ten jest niewystarczający do realizacji wszystkich założeń stawianych przed ratownikami. Brakującym modułem, który usprawniłby prowadzenie działań, byłoby wdrożenie systemu monitorowania poszkodowanych, jak i zespołów ratowniczych przebywających w strefie oddziaływania.

Kierując się tą dewizą, Szkoła Główna Służby Pożarniczej, jako lider, postawiła przed sobą trudne zadanie stworzenia założeń do opracowania systemu ewakuacji poszkodowanych oraz zdalnego pomiaru parametrów życiowych. Projekt systemu ewakuacji i ratowania poszkodowanych podczas klęsk żywiołowych – EvaCopNet – realizowany jest w ramach Programu Badań Stosowanych PBS3 i współfinansowany ze środków Narodowego Centrum Badań i Rozwoju (PBS3/B9/37/2015). System składałby się z dwóch głównych elementów:

- bezzałogowego systemu powietrznego (unmannedaerial system, UAS) – zbierającego dane,
- detektorów osobistych wykonanych np. w formie opasek na nadgarstek monitorujących parametry życiowe, takie jak tętno, ciepłota ciała, saturacja, oraz umożliwiających lokalizację poszczególnych osób.

Pierwszym etapem działań zmierzających do realizacji postawionych celów było rozpoznanie stanu techniki, potencjału aplikacyjnego, analizy aktualnych rozwiązań, analizy zdarzeń historycznych i przyszłych scenariuszy determinujących potencjalne obszary wykorzystania technologii oraz integracja poszczególnych bloków funkcjonalnych systemu, a także określenie możliwości wykorzystania EvaCopNet w działaniach operacyjnych. W ramach tego zadania zrealizowano dwa podzadania:

- Opracowanie i analiza scenariuszy determinujących potencjalne obszary wykorzystania technologii zdalnego pomiaru parametrów życiowych.
- Analiza danych zawartych w programach ewidencji zdarzeń PSP pod kątem sytuacji, w których liczba osób poszkodowanych znacznie przewyższała możliwości zadysponowanego potencjału ratowniczego.

ANALIZA POTENCJALNYCH ZAGROŻEŃ

Wszystkie zagrożenia czyhające we współczesnym świecie można podzielić na dwie główne grupy. Ze względu na źródło pochodzenia wyróżnić należy katastrofy nieantropogeniczne, czyli naturalne, wywołane przez czynniki niezależne od człowieka, oraz katastrofy antropogeniczne, wywołane przez czynnik ludzki (A. Szymańska, 2013). Do katastrof nieantropogenicznych (naturalnych) zalicza się:

- powodzie,
- susze,
- cyklony,
- trzęsienia ziemi,
- wybuchy wulkanów,
- tsunami,
- lawiny,
- osuwiska,
- pożary lasów,
- silne, długotrwałe mrozy,

- silny wiatr,
- lokalnie rozwój szkodników i pasożytów.

Najczęstszymi katastrofami antropogenicznymi są:
- katastrofy komunikacyjne,
- katastrofy budowlane,
- katastrofy przemysłowe (chemiczne, biologiczne, radiologiczne, nuklearne i wybuchowe – CBRNE),
- pożary i wybuchy w aglomeracjach.

Prócz ogólnego podziału na dużą uwagę zasługuje nowy rodzaj katastrof, uznawanych obecnie za najczęściej występujące na całym świecie, tj. katastrofy synergiczne zwane również katastrofami cywilizacyjno-środowiskowymi, cywilizacyjno-ekologicznymi lub naturalno-technicznymi. Istotą katastrof synergicznych jest jednoczesne wystąpienie katastrofy naturalnej i antropogenicznej. Taki stan rzeczy wywołany jest w głównej mierze ekspansywną działalnością człowieka, która stanowi nieodłączną część szybkiego rozwoju gospodarczo-społecznego (H. Lorent, 2012). Wśród przykładów można wyróżnić:
- trzęsienia ziemi powodujące zniszczenie obiektów przemysłowych i emisję toksycznych cieczy lub gazów,
- zalania wodami powodziowymi składowisk odpadów albo oczyszczalni ścieków,
- wystąpienie niekorzystnych warunków naturalnych, jak huragany, śnieżyce,
- silny wiatr powodujący uszkodzenia w budownictwie, przemyśle, energetyce.

Niezależnie od rodzaju i przyczyn źródła zagrożenia cechą wspólną opisywanych zdarzeń jest duży obszar oddziaływania oraz duża liczba osób zagrożonych wymagających pomocy w formie ewakuacji lub hospitalizacji. Dużym problemem dla ratowników jest sytuacja, w której osoby potencjalnie zagrożone nie wyrażają zgody na opuszczenie miejsca zamieszkania lub gdy na miejscu zdarzenia występuje brak możliwości przeprowadzenia natychmiastowej ewakuacji. Kolejnym czynnikiem determinującym jest zaangażowanie znacznego potencjału ratowniczego. W przypadku wystąpienia

katastrofy pierwszymi ratownikami wysyłanymi na miejsce są ratownicy Państwowej Straży Pożarnej (PSP) lub Ochotniczej Straży Pożarnej (OSP). Krajowy System Ratowniczo-Gaśniczy skonstruowany jest w taki sposób, aby najbliższa jednostka ratownicza dotarła na miejsce zdarzenia w możliwie najkrótszym czasie, tj. maksymalnie w ciągu 15 minut od momentu otrzymania zgłoszenia, do najdalej oddalonego punktu swojego terenu chronionego. Takie rozwiązanie pozwala na dotarcie ratowników pierwszego rzutu do poszkodowanych w czasie umożliwiającym udzielenie skutecznej pomocy w ramach kwalifikowanej pierwszej pomocy i przekłada się bezpośrednio na zwiększenie prawdopodobieństwa przeżycia ratowanych po przekazaniu ich jednostkom Państwowego Ratownictwa Medycznego (PRM).

W zdarzeniach, w których uczestniczy znaczna liczba osób poszkodowanych lub obszar działania jest bardzo duży, siły pierwszego rzutu są zwykle niewystarczające. Zadysponowanie i dotarcie większego potencjału nie stwarza dla PSP większego kłopotu, jednak wiąże się z czasem potrzebnym na dojazd oddalonych jednostek KSRG. W tym przypadku kompetencje ratowników pierwszego rzutu polegają głównie na określeniu niezbędnego potencjału ratowniczego (ilu ratowników jest potrzebnych do realizacji działań, ilu poszkodowanych) oraz rozpoczęciu triage'u (segregacji poszkodowanych). Ze względu na deficyt ratowników w pierwszych minutach akcji, ten etap zaliczany jest do jednego z najtrudniejszych. Obecnie ratowników PSP obowiązuje system START, według którego poszkodowani dzieleni są na cztery grupy. W zależności od oceny stanu zdrowia poszkodowanemu przyporządkowuje się jeden z kolorów (zielony, żółty, czerwony, biało-czarny), który jest równoznaczny z priorytetem ewakuacji i kolejnością udzielania pomocy. Największą trudnością jest, już po dokonaniu triage'u, ciągła kontrola parametrów życiowych. Należy pamiętać, że jedną z głównych przyczyn zgonów (A. Zawadzki, 2015) jest zbyt późno udzielona pomoc na miejscu zdarzenia oraz niewłaściwy transport poszkodowanych. Wychodząc naprzeciw tym problemom, w celu usprawnienia procesu ratowniczego powstał pomysł opracowania koncepcji systemu monitoringu stanu zdrowia. Odczyt i szybka analiza danych byłyby ważnym elementem działań ratowniczych podczas zdarzeń wielkoobszarowych oraz zdarzeń z dużą liczbą osób poszkodowanych. Detektor osobisty stanowiłby element wspomagania systemu segregacji – triage'u, umożliwiając szybkie lokalizowanie i ewakuację osób znajdujących się w stanie bezpośredniego zagro-

żenia życia. Dane sczytywane byłyby w trybie on-line bezpośrednio lub za pośrednictwem UAV i przekazywane do kierującego działaniem ratowniczym. Każda zmiana parametrów życiowych wpływających na zmniejszenie szansy przeżycia byłaby od razu przekazywana do dowodzącego. System ten oprócz usprawnienia samego procesu dowodzenia wpłynąłby na ograniczenie liczby ratowników potrzebnych do obserwacji stanu zdrowia poszkodowanych i równocześnie miałby bezpośredni wpływ na zwiększenie szans uratowania większej liczby poszkodowanych.

ANALIZA DANYCH STATYSTYCZNYCH PSP Z LAT 1995–2016

Krajowy System Ratowniczo-Gaśniczy powstał w celu usprawnienia i ujednolicenia działań o charakterze ratowniczym. Mowa tu o czynnościach podejmowanych przez Państwową Straż Pożarną oraz inne podmioty ratownicze, głównie Ochotnicze Straże Pożarne. Jednym z elementów monitorujących zakres czynności ratowniczych jest sporządzanie meldunków z prowadzonych działań. Meldunki z całego kraju gromadzone są w centralnym rejestrze ewidencji zdarzeń należącym do Systemu Wspomagania Decyzji SWD – ST w Komendzie Głównej Państwowej Straży Pożarnej. W meldunkach znajdują się najpotrzebniejsze informacje dotyczące rodzaju, wielkości i przyczyn zdarzenia, zaangażowanego potencjału ratowniczego, zarówno z KSRG, jak i spoza KSRG, liczby poszkodowanych, rodzaju udzielonej pomocy, rodzaju wykorzystanego sprzętu oraz opisu prowadzonych działań. Na tej podstawie, na potrzeby realizacji projektu, przeprowadzono analizę statystyczną meldunków za lata 1995–2015. Dodatkowo uwzględniono okres pierwszego kwartału 2016 roku. Dane zostały przefiltrowane na podstawie parametrów przyjętego algorytmu:

Parametr 1. użyto sprzętu do udrażniania dróg oddechowych
i/lub
Parametr 2. użyto zestawu opatrunkowego
i/lub
Parametr 3. użyto sprzętu do tlenoterapii 100% tlenem
i/lub
Parametr 4. użyto sprzętu ratowniczego ludzi (nosze typu deska-ewakuacja)
Parametr 5. liczba rannych równa lub powyżej 4.

Głównym determinantem była liczba osób, które pozostawały w stanie potencjalnego bądź rzeczywistego zagrożenia życia albo zdrowia ze względu na zbyt małą ilość sił i środków pierwszego rzutu lub pozostających w warunkach rozproszenia z brakiem możliwości dotarcia tradycyjnych środków transportu kołowego. Analizowano wyłącznie zdarzenia zaliczane do miejscowych zagrożeń, podczas których ratownicy udzielali pomocy minimum czterem poszkodowanym w zakresie kwalifikowanej pierwszej pomocy.

Potrzebne informacje statystyczne uzyskano poprzez wprowadzenie algorytmu do programu SWD – ST i przefiltrowanie w wybranych stałych tabelach zestawieniowych, tj.:

- zdarzenia wg rodzaju i wielkości w rozbiciu na jednostkę podziału administracyjnego,
- wypadki z ludźmi podczas miejscowych zagrożeń w rozbiciu na jednostkę podziału administracyjnego,
- rodzaj miejscowego zagrożenia w rozbiciu na jednostkę podziału administracyjnego.

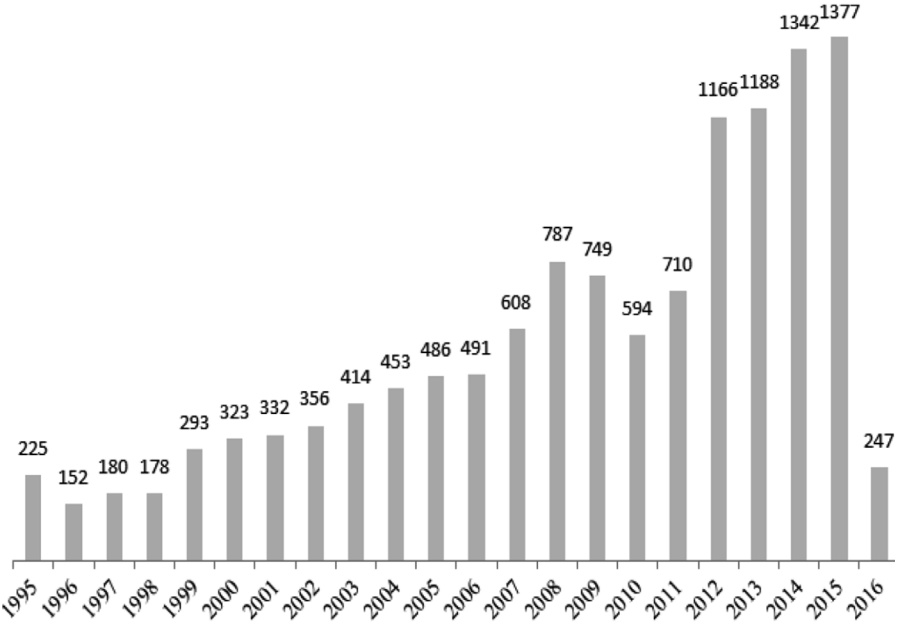
Na podstawie otrzymanych danych została opracowana wizualizacja danych historycznych dotyczących zdarzeń mnogich i masowych oraz katastrof wielkoobszarowych.

Analizowane dane zobrazowano na wykresach obejmujących następujące zależności:

- Zestawienie sumaryczne liczby zdarzeń ze względu na wielkość miejscowego zagrożenia (wykres 1).
- Liczba zdarzeń ze względu na wielkość miejscowego zagrożenia w rozbiciu na poszczególne lata (wykresy 2–9).
- Zestawienie liczby zdarzeń ze względu na rodzaj miejscowego zagrożenia (wykres 10).
- Liczba zdarzeń ze względu na rodzaj miejscowego zagrożenia w rozbiciu na poszczególne lata (wykresy 11 i 12).
- Liczba osób poszkodowanych podczas miejscowych zagrożeń w rozbiciu na poszczególne lata (wykresy 13 i 14).
- Ilość udzielanej pomocy podczas miejscowych zagrożeń, bez uwzględnienia parametrów algorytmu w rozbiciu na poszczególne lata – tło (wykresy 15 i 16).

Na podstawie otrzymanych statystyk możliwe było określenie trendu w rozpatrywanych obszarach. W przeciągu 20 lat liczba zdarzeń ze względu na wielkość miejscowego zagrożenia wzrosła ponad sześciokrotnie – z 225 w 1995 roku do 1377 w 2015 roku. Należy zwrócić uwagę na fakt, że w I kwartale 2016 roku liczba zdarzeń była wyższa niż w całym 1995 roku.

Wykres 1.
Zestawienie liczby zdarzeń ze względu na wielkość miejscowego zagrożenia

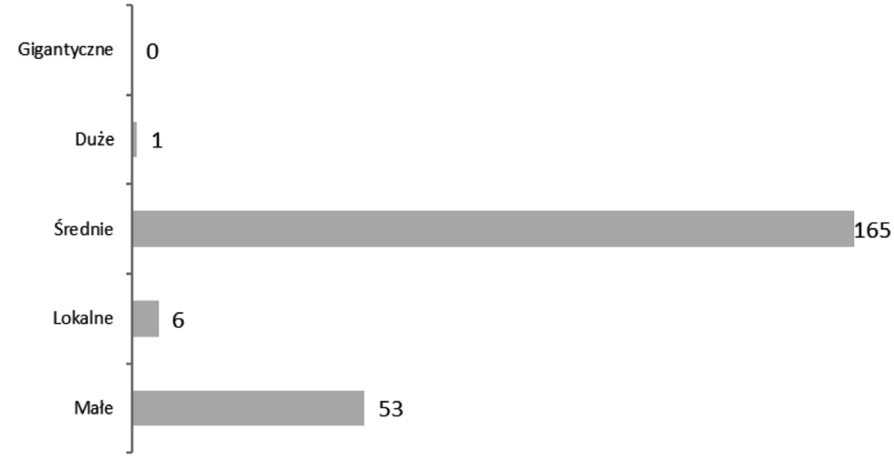


Źródło: Opracowanie własne

Rozpatrując liczbę zdarzeń ze względu na wielkość miejscowego zagrożenia w rozbiciu na poszczególne lata, można zauważyć, że w latach 1995–1998 przeważały zdarzenia zaliczane do średnich (powyżej 100) i małych (około 50).

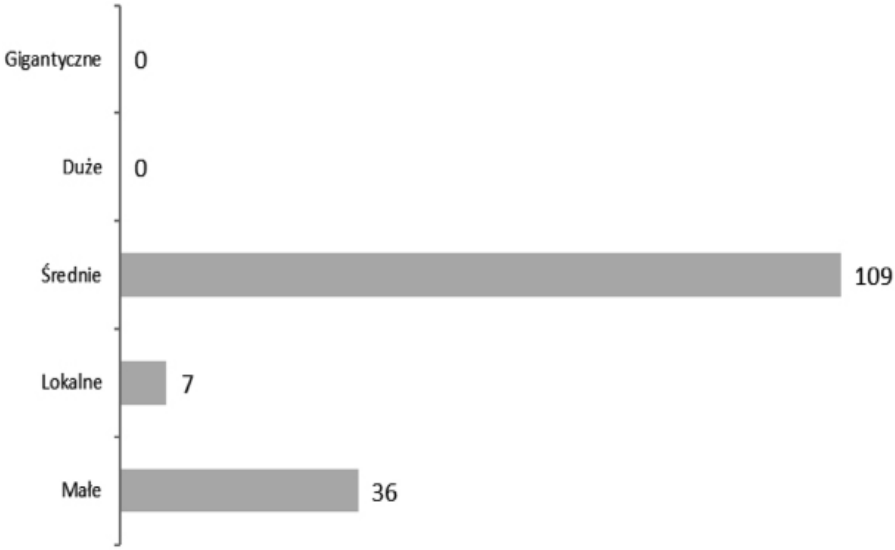
W kolejnych dwóch latach większość stanowiły zdarzenia małe (powyżej 130) i lokalne (powyżej 90). Od 2001 roku obserwuje się trend rosnący zdarzeń zaliczanych do lokalnych – od 135 w 2001 roku do 834 w 2015 roku.

Wykres 2.
Liczba zdarzeń ze względu na wielkość miejscowego zagrożenia w 1995 roku



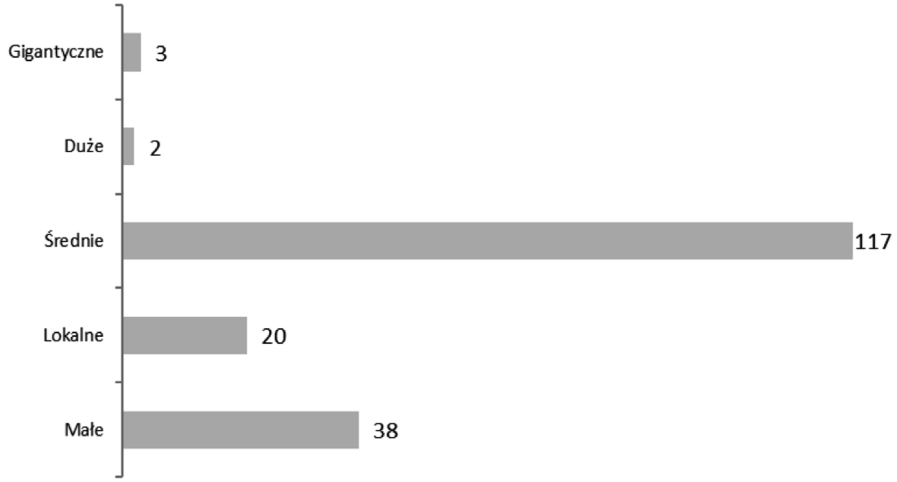
Źródło: Opracowanie własne

Wykres 3.
Liczba zdarzeń ze względu na wielkość miejscowego zagrożenia w 1996 roku



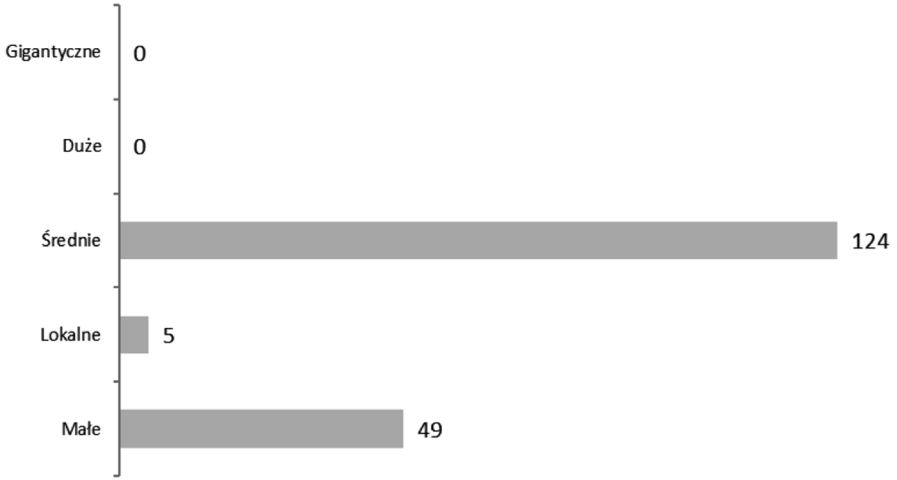
Źródło: Opracowanie własne

Wykres 4.
Liczba zdarzeń ze względu na wielkość miejscowego zagrożenia w 1997 roku



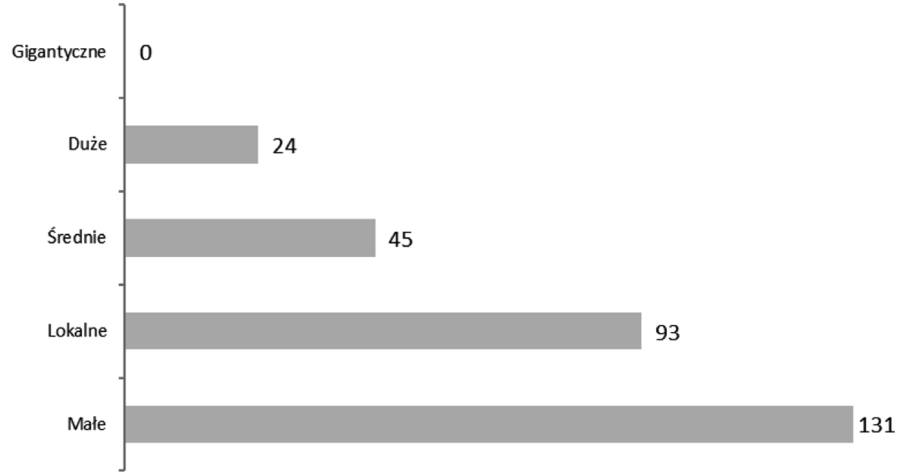
Źródło: Opracowanie własne

Wykres 5.
Liczba zdarzeń ze względu na wielkość miejscowego zagrożenia w 1998 roku



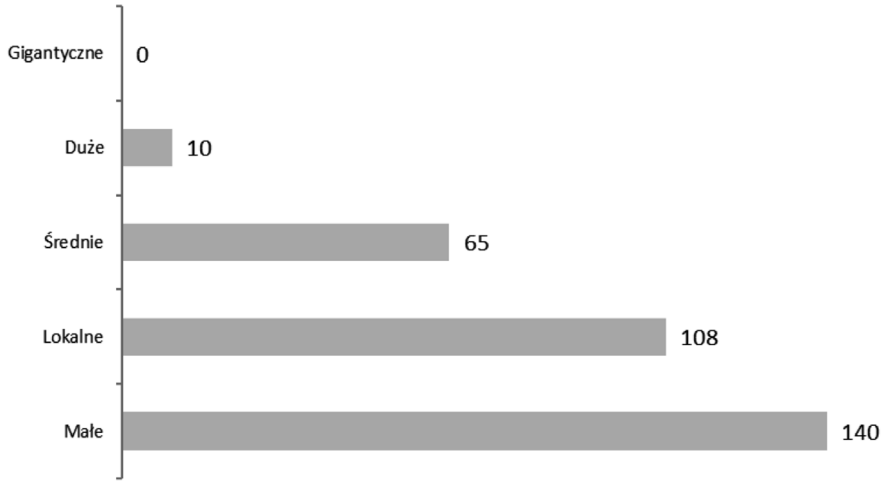
Źródło: Opracowanie własne

Wykres 6.
Liczba zdarzeń ze względu na wielkość miejscowego zagrożenia w 1999 roku



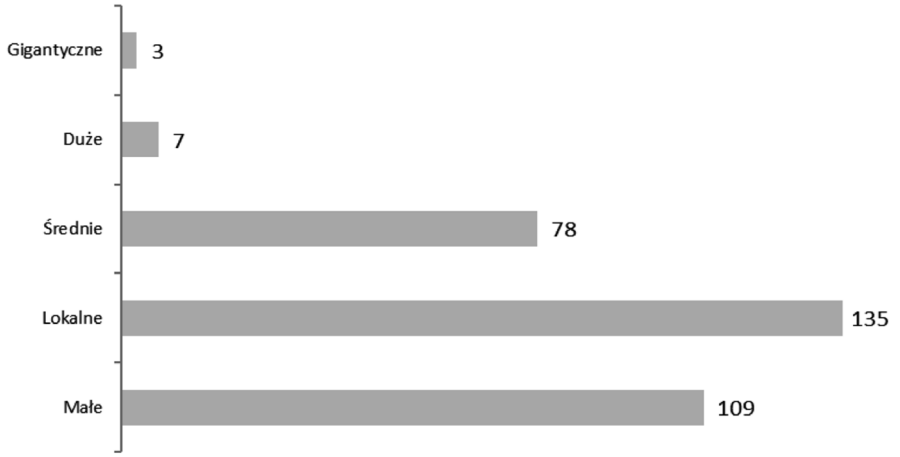
Źródło: Opracowanie własne

Wykres 7.
Liczba zdarzeń ze względu na wielkość miejscowego zagrożenia w 2000 roku



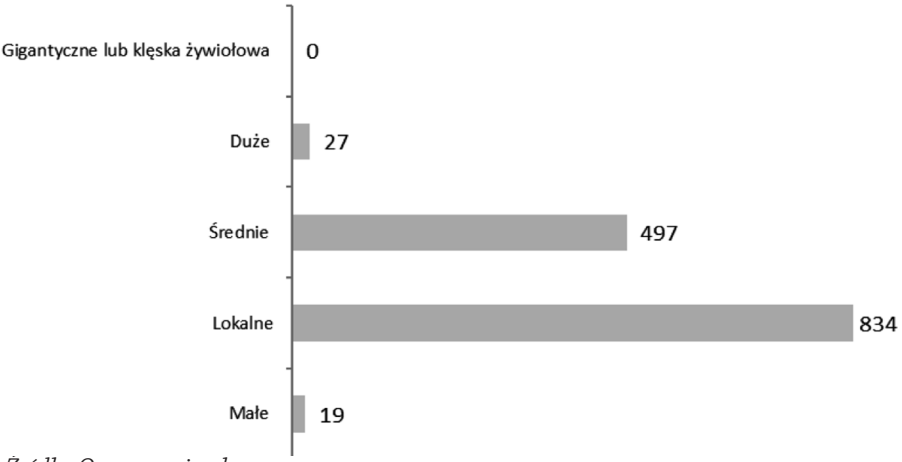
Źródło: Opracowanie własne

Wykres 8.
Liczba zdarzeń ze względu na wielkość miejscowego zagrożenia w 2001 roku



Źródło: Opracowanie własne

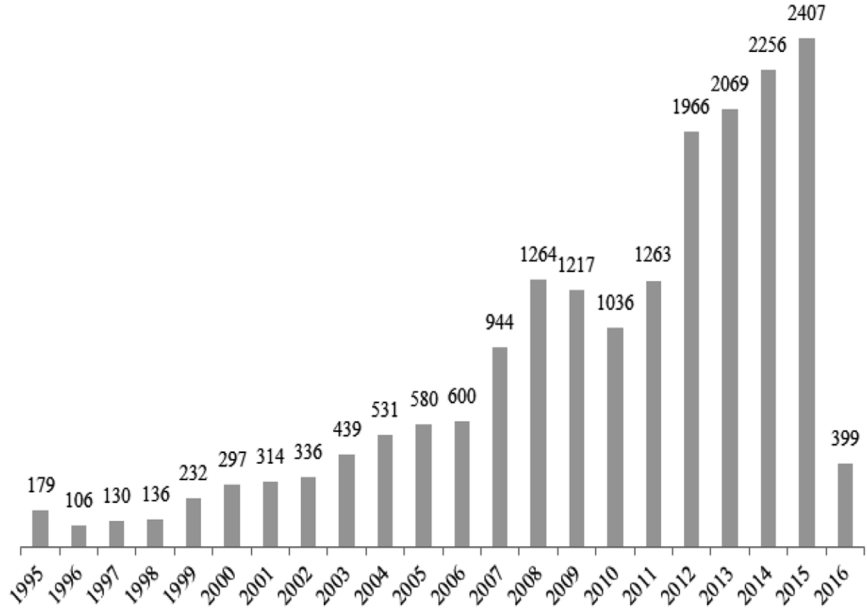
Wykres 9.
Liczba zdarzeń ze względu na wielkość miejscowego zagrożenia w 2015 roku



Źródło: Opracowanie własne

W przypadku zestawienia liczby zdarzeń ze względu na rodzaj miejscowego zagrożenia, podobnie jak w poprzednim przypadku obserwuje się corocznie zwiększającą się liczbę zdarzeń: od 179 w 1995 roku do 2407 w 2015 roku.

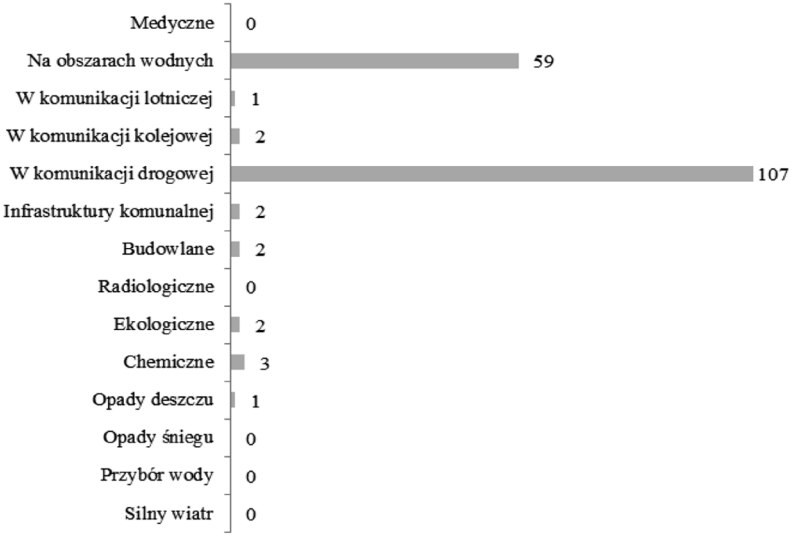
Wykres 10.
Zestawienie liczby zdarzeń ze względu na rodzaj miejscowego zagrożenia



Źródło: Opracowanie własne

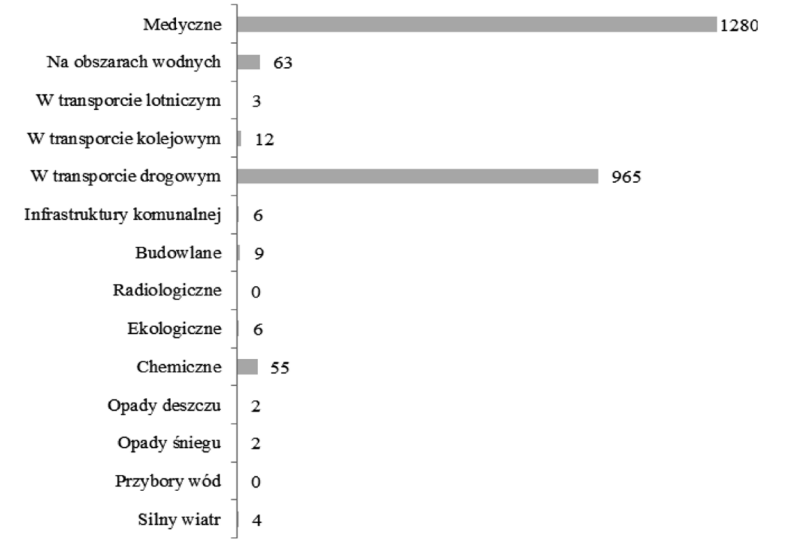
W latach 1995–1998 najwięcej zdarzeń spełniających założone warunki było podczas zdarzeń w komunikacji drogowej (średnio 90). Na drugim miejscu uplasowały się zdarzenia prowadzone na obszarach wodnych (średnio 40). Od 1999 roku zaczęto odnotowywać rosnącą liczbę zdarzeń medycznych.

Wykres 11.
Liczba zdarzeń ze względu na rodzaj miejscowego zagrożenia w 1995 roku



Źródło: Opracowanie własne

Wykres 12.
Liczba zdarzeń ze względu na rodzaj miejscowego zagrożenia w 2015 roku

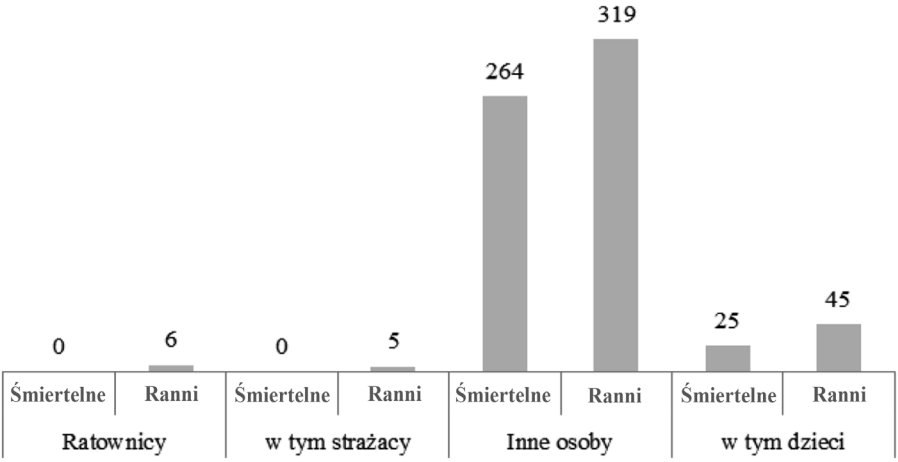


Źródło: Opracowanie własne

Spowodowane było to wprowadzeniem ratownictwa medycznego w struktury Państwowej Straży Pożarnej oraz włączeniem do sprawozdawczości tego rodzaju zdarzeń. Opracowano również standardy szkoleniowe i sprzętowe zawarte w „Wytycznych do organizacji ratownictwa medycznego w Krajowym Systemie Ratowniczo-Gaśniczym" z dnia 17 marca 1999 roku. Wytyczne opracowano w celu ujednolicenia zasad udzielania pomocy medycznej osobom będącym w nagłym stanie zagrożenia życia i zdrowia przez ratowników KSRG i podmiotów współpracujących na mocy stosownych porozumień oraz zapewnienia właściwego nadzoru nad poziomem ich wyszkolenia.

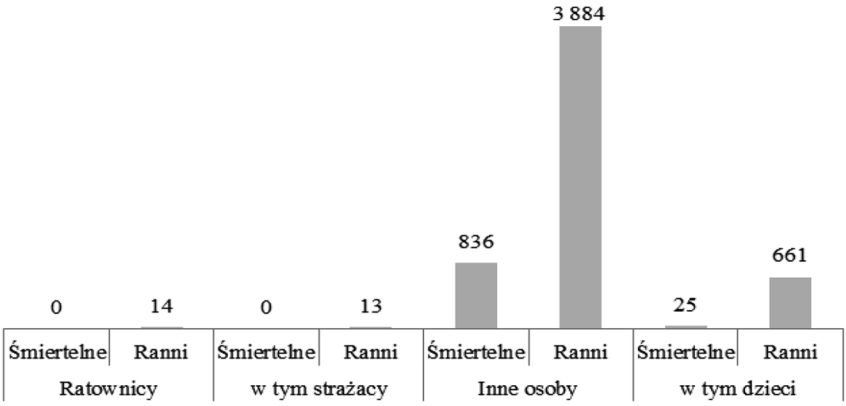
W latach 2007–2008 liczba zdarzeń medycznych i w komunikacji drogowej była praktycznie taka sama (oscylowała w okolicy 500). Od 2009 roku zdarzenia medyczne stały się czynnościami priorytetowymi, co spowodowało, że w 2015 roku liczba zdarzeń medycznych osiągnęła wartość 1280. Obserwuje się również tendencję wzrostową liczby osób poszkodowanych biorących udział w zdarzeniach. W 1997 roku odnotowano 264 ofiary śmiertelne oraz 319 rannych, zaś w 2015 roku odpowiednio 836 i 3884. Liczba ofiar śmiertelnych wzrosła zaledwie trzykrotnie, w porównaniu z ponaddwunastokrotnym wzrostem liczby osób rannych.

Wykres 13.
Liczba osób poszkodowanych podczas miejscowych zagrożeń w 1995 roku



Źródło: Opracowanie własne

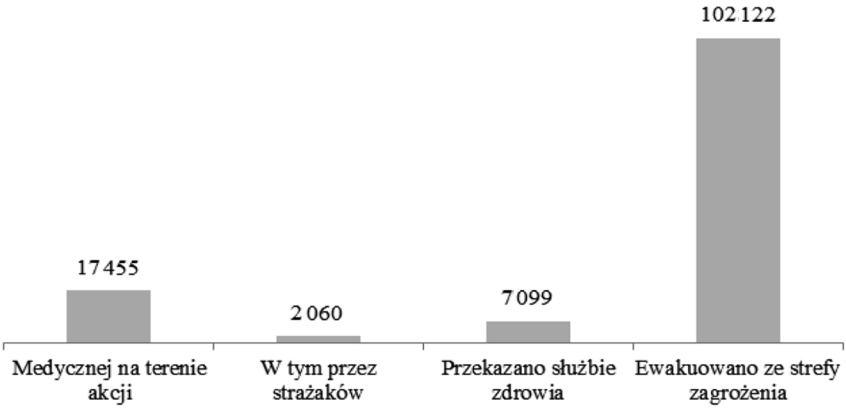
Wykres 14.
Liczba osób poszkodowanych podczas miejscowych zagrożeń w 2015 roku



Źródło: Opracowanie własne

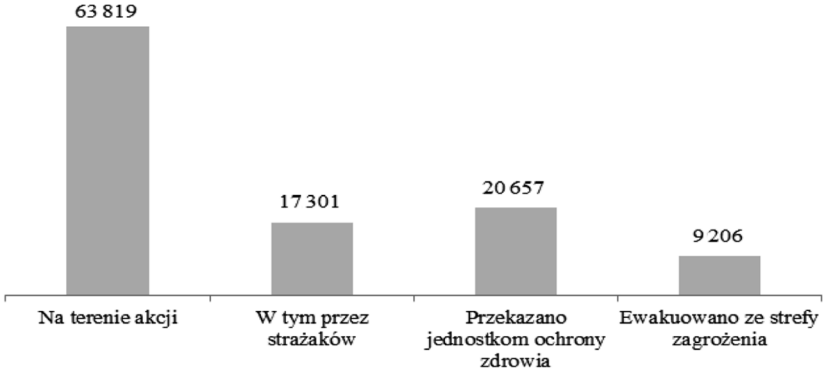
Jako tło przedstawiono dane ilustrujące ogólną liczbę zdarzeń miejscowych, podczas których ratownicy PSP i OSP udzielali kwalifikowanej pierwszej pomocy (bez uwzględnienia założonego algorytmu). W 1999 roku pomocy udzielano 17 455 razy – w tym przez strażaków 2060 razy, natomiast w 2015 roku – 63 819 razy, w tym przez strażaków 17 301 razy.

Wykres 15.
Ilość udzielanej pomocy podczas miejscowych zagrożeń w 1995 roku



Źródło: Opracowanie własne

Wykres 16.
Ilość udzielanej pomocy podczas miejscowych zagrożeń w 2015 roku



Źródło: Opracowanie własne

Analiza powyższych danych potwierdziła potrzebę kontynuacji prac zmierzających do stworzenia koncepcji systemu monitoringu stanu zdrowia poszkodowanych i ratowników.

OPRACOWANIE SCENARIUSZY DETERMINUJĄCYCH POTENCJALNE OBSZARY WYKORZYSTANIA TECHNOLOGII ZDALNEGO POMIARU PARAMETRÓW ŻYCIOWYCH

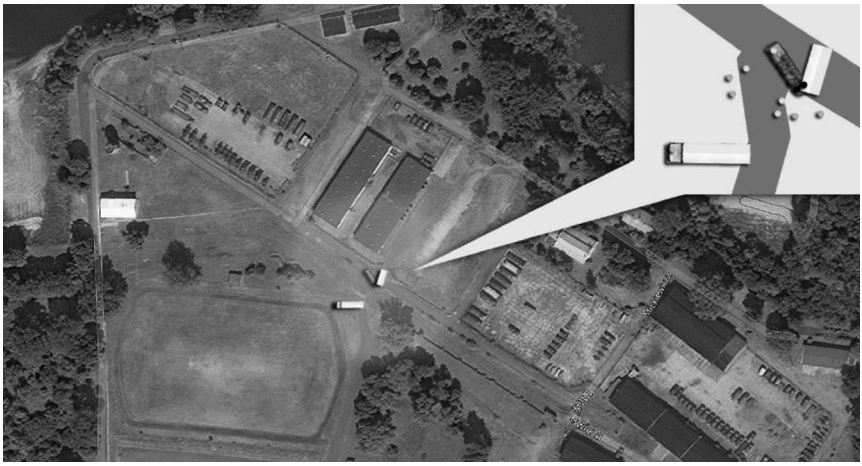
Na podstawie opracowanych danych historycznych oraz danych statystycznych opracowano scenariusze ćwiczeń, które umożliwią przygotowanie i przeprowadzenie testów poligonowych sprawdzających sprawność założeń systemu oraz potwierdzających obszary możliwości wykorzystania. Do badań wytypowano dwa poligony należące do Szkoły Głównej Służby Pożarniczej. Pierwszy – Baza przeciwpożarowa w Zamczysku Nowym, w którym planowane są testy sprawdzające kompatybilność poszczególnych podzespołów systemu wraz ze sprawdzeniem prawidłowości funkcjonowania w trudnych warunkach. Drugi to Kompleks poligonowy w Nowym Dworze Mazowieckim usytuowany nad zbiegiem rzek Wisły i Narwi. Kompleks ma rozbudowaną infrastrukturę rozmieszczoną na powierzchni 24 ha, co w pełni umożliwia realizację testów na podstawie opracowanych scenariuszy. W toku analiz wytypowano dwa reprezentatywne zdarzenia spełniające wymogi założeń systemu EvaCopNet. Koncepcja scenariuszy została opracowana w taki sposób,

aby zawierała początkowe założenia oraz związana była z urozmaiconymi warunkami terenowymi. Scenariusz pierwszy dotyczy wypadku masowego, natomiast drugi dotyczy przeciwdziałaniu skutkom powodzi. Poniżej przedstawiono wstępne założenia do reprezentatywnych zdarzeń.

Scenariusz 1. Wypadek masowy

Na skrzyżowaniu doszło do poważnego wypadku, w którym uczestniczył autokar oraz samochód ciężarowy z przyczepą. Kierowca ciężarówki, skręcając w drogę podporządkowaną, nie ustąpił pierwszeństwa przejazdu, w wyniku czego doszło do zderzenia z autobusem. Wypadek spowodował całkowite zablokowanie drogi. Siła uderzenia spowodowała wypięcie się przyczepy, która wbiła się w lewą, przednią część autokaru. Samochód ciężarowy zepchnięty został na skraj drogi, kierowca pozostał w kabinie. Kierowca autokaru został zakleszczony wewnątrz pojazdu. We wraku autokaru oprócz kierowcy znajdowało się 9 poszkodowanych osób, uwięzionych pomiędzy siedzeniami.

Ilustracja 1.
Szkic sytuacyjny scenariusza z wypadku masowego



Źródło: Opracowanie własne

Poszkodowanych przypisano do następujących grup:

- Grupa 1 – czerwona (pomoc medyczna i transport w pierwszej kolejności).
- Grupa 2 – żółta (pomoc medyczna konieczna, jednak jej opóźnienie nie powoduje zagrożenia życia).

- Grupa 3 – zielona (osoby, które przeżyją niezależnie od rodzaju udzielanej pomocy).
- Grupa 4 – biało-czarna (nie do uratowania w warunkach katastrofy).

Scenariusz 2. Przeciwdziałanie skutkom powodzi

Gwałtowne opady atmosferyczne połączone z burzami występujące na terenie Polski spowodowały lokalne wezbrania wód w strumieniach i rzekach, stwarzając zagrożenie powodziowe. W konsekwencji takiej sytuacji hydrometeorologicznej nastąpił niebezpieczny przyrost poziomu wody w zbiornikach retencyjnych, zmuszający służby techniczne do szybkiego, ale kontrolowanego zrzutu jej nadmiaru. Okoliczności te sprawiły, iż rzeki Wisła i Narew wystąpiły z brzegów. Nastąpiły lokalne przekroczenia stanów alarmowych, przerwanie wałów przeciwpowodziowych, uszkodzenie mostów i przepustów. W założeniu woda zajmuje 80% powierzchni kompleksu poligonowego w Nowym Dworze Mazowieckim. Na obszarze ok. 19 ha pozostaje bez możliwości samodzielnej ewakuacji 20 osób zagrożonych lub poszkodowanych przez falę powodziową.

Ilustracja 2.
Szkic sytuacyjny scenariusza z przeciwdziałania skutkom powodzi

Źródło: Opracowanie własne

Przeprowadzenie kompleksowych badań poligonowych umożliwi pełną ocenę założeń do projektu, pozwoli określić efekty wykorzystania systemu w odniesieniu do efektywności prowadzenia działań oraz da możliwość zebrania, np. w formie ankiety, ocen ewentualnych użytkowników końcowych.

PODSUMOWANIE

Analizując otrzymane dane statystyczne, wyraźnie widoczny jest wzrost liczby zdarzeń zaliczanych do miejscowych zagrożeń. Rośnie również stale liczba osób poszkodowanych wymagających udzielenia kwalifikowanej pierwszej pomocy na miejscu zdarzenia. Rozpatrywane przypadki zaliczane są do zdarzeń masowych ze względu na niewystarczające siły i środki pierwszego rzutu oraz zdarzeń występujących na rozległych obszarach, na których utrudnione jest dotarcie do poszkodowanych. W wielu przypadkach dochodzi jeszcze problem skutecznego monitorowania stanu zdrowia poszkodowanych oraz osób, których natychmiastowa ewakuacja z różnych przyczyn nie jest możliwa. Powołując się na zasady ratownictwa, należy pamiętać, że zarówno ewakuacja, jak i kontrola parametrów życiowych poszkodowanych jest jednym z priorytetów działań ratowniczych. Efektywna kontrola stanu ratowanych w znaczny sposób usprawnia proces dowodzenia oraz przekłada się na liczbę osób uratowanych.

Opisane powyżej scenariusze zdarzeń oraz reakcja związana z przeciwdziałaniem i minimalizacją ich skutków mogą opierać się na rozwiązaniu organizacyjno-technicznym, jakim jest system ewakuacji. Mając na uwadze powyższe analizy, można stwierdzić, że postawione cele i oczekiwane efekty projektowanego systemu EvaCopNet znajdują potwierdzenie w danych historycznych zawartych w programie ewidencji zdarzeń Państwowej Straży Pożarnej oraz danych pochodzących z innych krajów.

Mając powyższe na względzie, jeszcze silniej dowiedziona jest potrzeba prowadzenia dalszych prac badawczych i rozwojowych nad organizacją oraz optymalizacją działań ratowniczych i medycznych podczas zdarzeń masowych z wykorzystaniem nowych technologii.

Bibliografia

Grosset R., Jarosz W., Ciuka-Witryak M., Jarosławska-Kolman K., Łapicz M., Smolarkiewicz M. (2016). *Rozpoznanie stanu techniki, potencjału aplikacyjnego i analiza aktualnych rozwiązań, analiza zdarzeń historycznych i przyszłych scenariuszy determinujących potencjalne obszary wykorzystania technologii, integracja poszczególnych bloków funkcjonalnych systemu oraz określenie możliwości wykorzystania EvaCopNet w działaniach operacyjnych*. Sprawozdanie z realizacji zadania 1 projektu „Systemu ewakuacji i ratowania poszkodowanych podczas klęsk żywiołowych – EvaCopNet" realizowanego w ramach Programu Badań Stosowanych PBS3, współfinansowanego ze środków Narodowego Centrum Badań i Rozwoju (PBS3/B9/37/2015).

Zawadzki A. (red.) (2015), *Medycyna ratunkowa i katastrof*, Warszawa: Wydawnictwo Lekarskie PZWL.

Źródła internetowe

Lorent H. (red.) (2012), *Klęski żywiołowe a bezpieczeństwo wewnętrzne kraju, projekt „Wpływ zmian klimatu na środowisko, gospodarkę i społeczeństwo (zmiany, skutki i sposoby ich ograniczania, wnioski dla nauki, praktyki inżynierskiej i planowania gospodarczego)"*, realizowanego na podstawie umowy o dofinansowanie nr POIG.01.03.01-14-011/08 – 00 z dnia 1 grudnia 2008 roku w ramach Programu Operacyjnego Innowacyjna Gospodarka, IMiGW, Warszawa, http://klimat.imgw.pl/wp-content/uploads/2013/01/tom3.pdf [data dostępu: 2.12.2016]. Ratownictwo chemiczne – Katastrofy i zagrożenia, http://www.ratownictwo.chem.pl/ [data dostępu: 2.12.2016].

Szymańska A. (styczeń – luty 2013). *Katastrofy ekologiczne i obszary zagrożone klęskami żywiołowymi – Polska i świat*. „Ekologia i Środowisko", nr 53, http://rme.cbr.net.pl/index.php/archiwum-rme/148-styczen-luty-nr-53/ekologia-i-srodowisko/326-katastrofy-ekologiczne-i-obszary-zagrozone-kleskami-zywiolowymi-polska-i-swiat [data dostępu: 2.12.2016].

Akty prawne

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 lutego 2011 roku w sprawie szczegółowych zasad organizacji krajowego systemu ratowniczo-gaśniczego (Dz.U. 2011 nr 46 poz. 239).

Zasady Organizacji Ratownictwa Medycznego w Krajowym Systemie Ratowniczo-Gaśniczym (2013). KG PSP, KCKRiOL, Warszawa.

JÓZEF PIOTR KNAP
Warszawski Uniwersytet Medyczny – Zakład Epidemiologii
i Komenda Główna Straży Granicznej
panknap1@gmail.com

ARKADIUSZ KOSOWSKI
Centrala Narodowego Funduszu Zdrowia
Departament ds. Służb Mundurowych
AK.gabi@o2.pl

CYBERATAK KONTRA MEDYCYNA
CYBERATTACK CONTRA MEDICINE

ABSTRACT

The „new" and growing problem of cybersecurity in the field (areas) of modern medicine *sensu largo* – is described. Authors stressed theoretical, practical (including: clinical) and legal problems of cyberattacks and bioterrorist attacks against medicine (e.g. contra patents, medical devices and hospital/outpatients clinic networks). Actual worldwide situation of cybersecurity in this issue is discussed.

Keywords: *cybersecurity, cyberattacks, cyberterrorism, medical devices*

STRESZCZENIE

W opracowaniu przedstawiono „nowy" i narastający problem zagrożeń cyberbezpieczeństwa w obszarze najszerzej pojętej współczesnej medycyny. Rozważono teoretyczne, praktyczne i legislacyjne skutki cyberataków i działań cyberterroru jako zagrożenia: dla konkretnych chorych, dla urządzeń medycznych, dla teleinformatycznych sieci w służbie zdrowia, dla potencjalnych działań ratowniczych. Ukazano aktualną sytuację cyberbezpieczeństwa w medycynie światowej, z zaakcentowaniem Polski.

Słowa kluczowe: *cyberbezpieczeństwo, cyberataki, cyberterroryzm, urządzenia medyczne*

WPROWADZENIE

Cyberatak jest zawsze uderzeniem w informację. Także w informację będącą podstawą każdego działania diagnostycznego, leczniczego i organizacyjnego w służbie zdrowia. Cyberatak jest więc – różnego rodzaju – zakłóceniem wytwarzania, przechowywania, przesyłania i wykorzystywania informacji, a także uderzeniem w jej dokładność, sprawdzalność i wiarygodność, czyli – prawdziwość.

Przybliżmy pojęcia do niedawna – jeszcze na przełomie wieków – mało znane i całkiem abstrakcyjne, zwłaszcza w aspekcie bezpośrednich zagrożeń dla medycyny. Klaryfikacja taka wydaje się konieczna, gdyż jest to pierwsze w polskim piśmiennictwie opracowanie dotyczące – szeroko pojętych – aspektów medycznych cyberbezpieczeństwa. Przytoczymy, w klasycznym ujęciu, zarówno pojęcia ogólne (podstawowe), jak i nowe, obowiązujące definicje zawarte w aktach normatywnych. Wciąż całkowicie nowe – i co więcej: całkiem obce w swej pozornej nierzeczywistości i wirtualnej abstrakcji – są bowiem same pojęcia „cyberprzestrzeni" i „cyberataku". Z trudnością uświadamiamy sobie i przyjmujemy bowiem zarówno wzajemne przenikanie się tego, co rzeczywiste, namacalne, z tym, co wirtualne. „Wirtualne" – a więc stworzone w umyśle ludzkim, ale istniejące w rzeczywistości lub mogące zaistnieć. Co więcej, zaskakuje nas, że cyberprzestrzeń, postrzegana wielokroć jako odrębny świat, mało konkretny i jakby nierzeczywisty, ma tak przemożny wpływ na codzienne realne bytowanie. W nowych, zaskakujących odsłonach powracają tu odwieczne problemy filozoficzne, wraz ze sporem o uniwersalia, w którym problem cyberprzestrzeni kontruje stanowisko nominalistów negujących rzeczywiste istnienie powszechników. Słynne tezy: „1.13. Światem są fakty w przestrzeni logicznej" czy „5.61. Logika wypełnia świat; granice świata są też jej granicami. W logice nie można zatem powiedzieć: to a to w świecie jest, a tamtego nie ma (...)", zawarte w „Tractatus logico-philosophicus" Ludwiga Wittgensteina (1889–1951) z roku 1922 (Wittgenstein, 2011), ukazywały całkiem nowe pojęcie „przestrzeni logicznej", i wraz z pracami największych polskich logików (Łukasiewicza, Leśniewskiego, Tarskiego, Ajdukiewicza i innych) tego okresu dawały asumpt do powstania pojęć wirtualnego cyberświata, wypełnionego jednak nad wyraz realnymi strukturami informacji i jej transferu. Należy ponadto przypomnieć, że jeśli – w swych założeniach ogólnych, ale i w praktyce codzienności – informacja powinna być przekazem **prawdy, to cyberatak**

uderza też w prawdę, także w kategoriach etycznych, powodując **dezinformację** również i w wymiarze aksjologicznym.

Pomijając, z konieczności, ale i z braku wystarczających kompetencji, genezę i kształtowanie się ontycznych i metodologicznych poglądów w omawianej kwestii, analizowaną zresztą przez polskich autorów (Berdel-Dudzińska, 2001; Sienkiewicz, 2015), nie można pominąć tu wielkiego wkładu znakomitego polskiego pisarza – futurologa, ale i wybitnego filozofa, lekarza z wykształcenia, Stanisława Lema (Jastrzębski, 2003; Okołowski, 2005). Idee odnośnie do styku informatyki, przestrzeni wirtualnych i filozofii zostały przezeń potężnie sformułowane już na początku lat 60. XX wieku, głównie w dziele „Summa technologiae", ale i w późniejszych, jak „Filozofia przypadku", „Golem XIV", „Bomba megabitowa", „Okamgnienie" i „Rasa drapieżców. Teksty ostatnie". W 1984 roku pisarz kanadyjski William Gibson użył po raz pierwszy określenia „cyberprzestrzeń" w kultowej dziś powieści „Neuromancer". W okresie tym zaczęto również podnosić aspekty socjologiczne („społeczności wirtualne", „społeczeństwo informatyczne") omawianego problemu i rozpatrywać jego wymiar światowy – w ścisłej łączności semantycznej i tematycznej z globalizacją (Szponar, 2004).

Warto jednak pamiętać, że omawiane tu zjawiska narodziły się, choć w niepomiernie węższym zakresie i daleko mniejszej złożoności, już wraz z pojawieniem się przed niemal 100 laty radia. Wiadomości przenoszone, jak to wówczas mówiono „na falach eteru", miały także potężną moc rażenia. Słynna audycja radiowa Orsona Wellesa (1915–1985) z 1938 roku o lądowaniu Marsjan, której rzekomy autentyzm wywołał w USA panikę – jest takiego wpływu pierwszym donośnym sygnałem (przykładem).

„Informacja (łac. *informatio* – przedstawienie, wizerunek; *informare* – kształtować, przedstawiać) – treść komunikatu, sens przekazywanej wiadomości. Potocznie: wiadomość, komunikat (ujęcie przedmiotowe), ale także: powiadomienie o czymś, zakomunikowanie czegoś, przekazanie wiadomości dotyczącej czegoś indywidualnemu lub zbiorowemu odbiorcy (ujęcie czynnościowe)" (Błasiak i Koszowy, 2003). Twórcą klasycznej ilościowej teorii informacji (1949) jest Claude Elwood Shannon (1916–2001). Ze zbitki pojęć „informacja" i „automatyka" w latach 70. XX wieku powstało określenie **informatyki**, ściśle związane z gromadzeniem, przechowywaniem, przetwarzaniem i przesyłaniem (transferowaniem) informacji za pomocą sprzętu komputerowego (telekomunikacja) – i później – sieci informatycznych (tele-

informatyka), które (coraz bardziej złożone i powszechne) zaczęły od połowy lat 90. XX wieku prowadzić do powstania „społeczeństwa informatycznego". Są to zagadnienia już bezpośrednio związane z treścią tego artykułu. Z kolei pojęcia z przedrostkiem „cyber" – mają swój źródłosłów w terminie „cybernetyka" wprowadzonym przez Norberta Wienera (1894–1964) w 1947 roku.

„Cybernetyka (gr. *he kybernetike* – sztuka sterowania, kierowania) – nauka o procesach sterowania i łączności w maszynach i organizmach żywych (abstrahująca od materialnego podłoża tych zjawisk) oraz o sposobach przekazywania informacji między częściami układu i między układami; jest działem matematyki stosowanej" (Lubański, Szymański, Zięba, 2001). Cybernetyka jest więc nauką o procesach informacyjnych (Tadeusiewicz, 2009) i stanowiła, jak to określał jeden z jej współtwórców, zarazem wybitny neurolog i psychiatra, W. Ross Ashby (1903–1972), nowe podejście do szeregu zjawisk oraz umożliwiła **wykrycie** pewnych mechanizmów kontroli w systemach żywych (i nie tylko), jak na przykład „sprzężenie zwrotne" (*feedback*), „sieci neuronowe", „algorytmy genetyczne" czy „sztuczna inteligencja", które okazały się niezbędne w zrozumieniu mechanizmów automatyki, informatyki, telekomunikacji, a i w samym tworzeniu tych pojęć (Ashby, 1963; Tadeusiewicz, 2009).

Pojęcie **cyberprzestrzeni** zostało wprowadzone do polskiego systemu prawnego w 2011 roku (Dz.U. 2011, nr 222 poz. 1323). We wprowadzeniu do tej ustawy napisano: „działalność w cyberprzestrzeni staje się nieodzownym warunkiem funkcjonowania państwa i społeczeństwa". W roku 2013 Rada Ministrów przyjęła Politykę Ochronną Cyberprzestrzeni.

- W listopadzie 2015 roku Rada Ministrów RP (uchwała 210/2015) przyjęła zaktualizowany „Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK)". Uchwała zawiera rozbudowany załącznik „Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje".
- W roku 2015 ogłoszona została „Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej", w której zrekapitulowano poszczególne pojęcia i definicje (podane skrótowo powyżej) oraz podano przesłanki – strategiczne kierunki działań – na rzecz stworzenia zintegrowanego systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej.
- Przywódcy krajów NATO, zebrani na szczycie natowskim dnia 8 lipca 2016 roku w Warszawie, uznali cyberbezpieczeństwo za nową strefę działań operacyjnych, taką jak przestrzeń powietrzna, morze i ląd.

REGULACJE PRAWNE ODNOŚNIE DO CYBERBEZPIECZEŃSTWA W MEDYCYNIE

Wśród licznych już polskich aktów prawnych i dokumentów związanych z cyberbezpieczeństwem jedynie dwa odnoszą się bezpośrednio do zagrożeń cyberatakiem obszaru działań medycznych:

A. Ustawa z dnia 17 lutego 2005 roku o informatyzacji, działalności podmiotów realizujących zadania publiczne (Dz.U. 2005, nr 64 poz. 565; tekst jednolity: Dz.U. 2014, poz. 114). Zgodnie z jej art. 2.1. przepisy ustawy stosuje się (z pewnymi zastrzeżeniami) między innymi do:
   - samodzielnych publicznych zakładów opieki zdrowotnej,
   - ZUS i KRUS,
   - Narodowego Funduszu Zdrowia itd.

B. Rozporządzenie Ministra Zdrowia z dnia 9 listopada 2015 roku w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. 2015, poz. 2069, z 8 grudnia 2015 r.). Rozporządzenie to należy traktować jako akt wykonawczy w stosunku do:
   - ustawy z dnia 15 kwietnia 2011 roku o działalności leczniczej (Dz.U. 2011, nr 112 poz. 654) – z późniejszymi zmianami,
   - ustawy z dnia 28 kwietnia 2011 roku o systemie informacji w ochronie zdrowia (Dz.U. 2011, nr 113 poz. 657). Ustawa ta nakłada na placówki ochrony zdrowia obowiązek informatyzacji dokumentacji medycznej; tak więc wszystkie podmioty prowadzące działalność leczniczą powinny wdrażać system **Elektronicznej Dokumentacji Medycznej (EDM**), co – w założeniu – ma znacznie usprawnić funkcjonowanie systemu ochrony zdrowia. Zgodnie z art. 5 cytowanej ustawy z dnia 28 kwietnia 2011 roku, System Informacji w ochronie zdrowia obejmuje bazy danych funkcjonujące w ramach:
     1. Systemu Informacji Medycznej (SIM).
     2. Dziedzinowych systemów teleinformatycznych, np.:
        - Systemu Rejestru Usług Medycznych NFZ („RUM -NFZ”),
        - Systemu Statystyki w Ochronie Zdrowia,
        - Systemu Ewidencji Zasobów w Ochronie Zdrowia,
        - systemu wspomagania Ratownictwa Medycznego,
        - Systemu Monitorowania Zagrożeń itd.

Wyobraźmy sobie skutki zmasowanego ataku na wymienione struktury, który ponadto przebiegać może z całkowitą utratą danych zawartych w ww. systemach.

C. Pośrednio, problemu medycznego (katastrofy) dotyczy także art. 3, ust. 1, pkt 4 ustawy z dnia 3 sierpnia 2011 roku o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych, mówiący: „katastrofę naturalną lub awarię techniczną mogą wywołać również zdarzenia w cyberprzestrzeni oraz działania o charakterze terrorystycznym".

Cytowana ustawa z dnia 17 lutego 2005 roku definiuje dwa ważne pojęcia. Są to:

- **Interoperacyjność** – „zdolność różnych podmiotów oraz używanych przez nie systemów teleinformatycznych i rejestrów publicznych do współdziałania na rzecz osiągnięcia wzajemnie korzystnych i uzgodnionych celów, z uwzględnieniem współdzielenia informacji i wiedzy (...)".
- **Krajowe Ramy Interoperacyjności (KRI)** – „zestaw wymagań semantycznych, organizacyjnych i technologicznych dotyczących interoperacyjności systemów teleinformatycznych i rejestrów publicznych". Podstawowe w tym zakresie jest rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 roku, znowelizowane i podane w postaci tekstu jednolitego jako obwieszczenie Prezesa Rady Ministrów z dnia 14 stycznia 2016 roku w sprawie ogłoszenia jednolitego tekstu rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2016, poz. 113).

W rozporządzeniu tym wprowadzono też dalsze definicje w omawianym temacie; przytoczymy cztery z nich:

- obiekt przestrzenny – w rozumieniu przepisów ustawy z dnia 4 marca 2010 roku o infrastrukturze informacji przestrzennej (Dz.U. 2016, poz. 113),
- podatność systemu teleinformatycznego – właściwość systemu teleinformatycznego, która może być wykorzystana przez co najmniej jedno zagrożenie,

- polityka bezpieczeństwa informacji – zestaw efektywnych, udokumentowanych zasad i procedur bezpieczeństwa wraz z planem ich wdrożenia i egzekwowania,
- zagrożenia systemu teleinformatycznego – potencjalna przyczyna niepożądanego zdarzenia, które może wywołać szkodę w systemie teleinformatycznym.

System zarządzania bezpieczeństwem informacji jest w Polsce oparty o Polską Normę PN-ISO/IEC 27001 [wprowadza ISO/IEC 27001: 2013 (E) (E)]. Tam też zawarte są definicje, jak np.:

- bezpieczeństwo informacji,
- zdarzenie związane z bezpieczeństwem informacji,
- incydent związany z bezpieczeństwem informacji,
- system zarządzania bezpieczeństwem informacji.

Z kolei ustawa z dnia 6 listopada 2008 roku o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. 2008, nr 52 poz. 417, z późn. zm.) porusza zagadnienia praw chorego, które mogą być naruszone wskutek cyberataku (np. bezprawne ujawnienie danych osobowych).

METODYCZNE I REALNE PROBLEMY CYBERATAKÓW W MEDYCYNIE

Ten nieco zawiły wstęp usprawiedliwia autorów o tyle tylko, że ukazuje z jednej strony już istniejący spis aktów prawnych, dotyczący jednak głównie tezauryzacji, przekazywania i ochrony danych teleinformatycznych, z drugiej zaś – zderza niejako istniejącą już w polskim prawodawstwie legislaturę z niezmierną złożonością wieloaspektowego oraz interdyscyplinarnego problemu określonego przez nas najogólniej: „cyberatak kontra medycyna".

Anglosaskie pojęcie **urządzeń medycznych – *Medical Devices* (MD)** jest zdefiniowane bardzo szeroko i precyzyjnie zarazem: „**Medical Devices:** An instruments, apparatus, implement, machine, contrivance, implant, in vitro reagent, or rather similar or related article, including a component part, or accessory (...) intended for use in the diagnosis of disease or other conditions, or in the cure, mitigations, treatment or prevention of disease (...)" (Williams i Woodward, 2015). Sądzimy, że definicja powinna być szeroko przyjęta. Całokształt zagadnień związanych z MD (także

więc ich cyberbezpieczeństwa) stał się przedmiotem, wydanej ostatnio, obszernej monografii (Fiedler, 2016). W cytowanej, metodycznej i źródłowej pracy Williams i Woodward rozwinęli również charakterystykę pojęcia „cyberbezpieczeństwa" (*cybersecurity*), właśnie w odniesieniu do *Medical Devices* i szpitalnych (zakładowych) sieci (*network*) tych urządzeń. Za właściwą dla zastosowania odnośnie do medycyny uważają oni następującą, również ostatnio podaną, definicję (Craigen i Diakun-Thibault, 2014): **„Cybersecurity** entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption".

Precyzyjną charakterystykę cyberataków na urządzenia medyczne (*Medical Devices*) i szpitalne sieci informatyczne (*hospital networks*) oraz ich konsekwencje medyczne i prawne przedstawiła Katherine B. Wellington z Uniwersytetu Yale, USA (Wellington, 2013). W zależności od celu, na który ukierunkowany jest cyberatak, wyróżniła:

1. Cyberatak na indywidualną aparaturę medyczną (*C. on Individual Medical Devices*).
2. Cyberatak na szpitalne sieci informatyczne (*C. on Hospital Networks*).
3. Cyberatak nakierowany na kradzież informacji medycznych.

Cele 1, 2, 3 – mogą się na siebie wzajemnie nakładać i zazębiać pojęciowo, co dotyczy zarówno sieci generatorów danych (dane kliniczne i laboratoryjne chorych, ceny i stany składowe leków itd.), jak i ich przesyłu i właściwego odbioru.

Cyberatak na indywidualną aparaturę medyczną (*C. on Individual Medical Devices*) może doraźnie zagrażać życiu i zdrowiu chorego. Zatrzymanie lub zbrodnicze przeprogramowanie pracy urządzenia monitorującego i/lub kontrolującego funkcje życiowego organizmu chorego człowieka może doprowadzić do zgonu (i to zgonu, którego ustalenie przyczyny może być bardzo trudne). Narażeni będą więc pacjenci pozostający na oddechu kontrolowanym lub wspomaganym (respiratory), poddawani zabiegom nerkozastępczym (hemodializy – „sztuczne nerki"), detoksykacyjnym (hemofiltracja, plazmafereza, separatory komórkowe itd.), noworodki przedwcześnie urodzone pozostające w tzw. inkubatorach, chorzy poddawani terapii hiperbarycznej, pacjenci poddawani precyzyjnym zabiegom operacyjnym za pomocą urządzeń stereotaktycznych (neurochirurgia) i robotów chirurgicz-

nych oraz poddawani różnego rodzaju radioterapii z powodu nowotworów, bardzo liczni już dziś w rozwiniętych społeczeństwach chorzy z wszczepionymi stymulatorami pracy serca i defibrylatorami, czy wreszcie diabetycy korzystający z pomp insulinowych. Zwłaszcza trzy ostatnio wymienione urządzenia, niejako bezpośredniego stałego wsparcia chorego organizmu, są szczególnie narażone na atak indywidualny (Halperin i wsp., 2008; Nathanel i wsp., 2011). Oto na przykład przeprogramowanie pompy insulinowej, tak by sygnalizowała zbyt wysoki poziom glukozy w organizmie (hiperglikemia), spowoduje wyrzut zbytecznej w istocie dawki insuliny, co prowadzić może do gwałtownego zgonu w mechanizmie ostrego niedocukrzenia (hipoglikemii) (Nathanel i wsp., 2011). Oceniono w 2008 roku, że wobec potencjalnych aktów cyberterroru skierowanych przeciw wszczepionym stymulatorom pracy serca i defibrylatorom nie dysponujemy praktycznie żadną skuteczną obroną („software radio attack and zero-power defenses") (Halperin i wsp., 2008). Po filmie fabularnym „Homeland", obrazującym skuteczny cyberatak na stymulator serca prezydenta USA, były wiceprezydent USA Dick Chenay ujawnił, że jego wszczepiony defibrylator został zmodyfikowany w obawie przed cyberatakiem.

Obecnie trwają na świecie wielokierunkowe, interdyscyplinarne i wręcz gorączkowe prace nad „uszczelnieniem" cyberbezpieczeństwa urządzeń teleinformatycznych stosowanych w służbie zdrowia. W 2015 roku wielka rządowa Agencja do Spraw Żywności i Leków (FDA – *Food and Drug Administration*) wdrożyła oficjalne działania dotyczące cyberbezpieczeństwa w zakresie swej odpowiedzialności ustawowej (FDA, 2014, także FDA, 2016).

Jeśli chodzi o cyberatak na szpitalne sieci informatyczne (*C. on Hospital Networks*) oraz cyberatak nakierowany na kradzież informacji medycznych, akty cyberterroru uderzają zarazem w oba punkty, rozróżnione przez Wellington, jedynie w celach dydaktycznych i klasyfikacyjnej poprawności. Wytworzony chaos (opisany poniżej) zagraża, zarówno bezpośrednio, jak i pośrednio, zdrowiu i życiu chorych, generuje wielkie straty ekonomiczne i może dezorganizować pracę służby zdrowia na wielkich obszarach, a nawet na terenie całego kraju (np. USA).

Określone przez Katherine Wellington zasadnicze kierunki i rodzaje cyberataków nie wyczerpują możliwości i zasięgu uderzenia w struktury bezpośrednio i pośrednio związane z medycyną: zdrowiem publicznym, bezpieczeństwem zdrowotnym, nadzorem epidemiologicznym – najogól-

niej – w **infrastrukturę krytyczną** w rozumieniu art. 5 pkt 7 ustawy o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 roku. W pewnym uproszczeniu infrastrukturę krytyczną można określić jako rzeczywiste i cybernetyczne systemy, niezbędne do minimalnego funkcjonowania państwa. Wymieńmy tu przykładowo uderzenie w Państwowe Ratownictwo Medyczne, określone ustawą z dnia 8 września 2006 roku (Dz.U. 2006, nr 191 poz. 1410 z późn. zm.) – wraz z systemem wspomagania Ratownictwa Medycznego (Dz.U. 2011, nr 113 poz. 657), w system zaopatrzenia w leki i sprzęt medyczny i ich ogólnokrajową dystrybucję, w system tezauryzacji danych medycznych zbieranych w celach statystycznych, demograficznych i epidemiologicznych, nieraz przez dziesiątki lat. Zwłaszcza precyzyjne cyberataki przeciwko działaniom ratowniczym podejmowanym w stosunku do katastrof, zarówno naturalnych, jak i wywołanych przez człowieka (także intencjonalnie – właśnie jako akt cyberterroru), mogą być atakami na infrastrukturę krytyczną konkretnego państwa o potencjalnie trudnych nawet do wyobrażenia, tragicznych następstwach. Z zasygnalizowaną tu jedynie problematyką cyberbezpieczeństwa muszą być więc dogłębnie zaznajomione struktury obrony i ochrony państwa i przedstawiciele wszystkich służb czuwających, a więc ludzie tworzący tzw. grupy supozycyjne (Maciejewski, 2014), w tym oczywiście – służb medycznych i ratunkowych.

Jak częstym zjawiskiem są cyberataki na MD? Precyzyjna odpowiedź nie jest możliwa poza ogólnymi stwierdzeniami o wybitnym zróżnicowaniu pomiędzy poszczególnymi państwami i kontynentami oraz niewątpliwym narastaniu rozmiaru zjawiska w skali globu. Stany Zjednoczone Ameryki Północnej są niewątpliwie państwem, w którym zjawisko to występuje najczęściej i na największą skalę, lecz dane o cyberatakach kontra medycyna pochodzą już także z innych kontynentów i krajów (np. Chiny, Australia).

Oto niekompletna lista przykładów:

- W latach 2009–2013 odnotowano 804 włamania do zastrzeżonych informacji medycznych, naruszając 29 276 385 zapisów (*records*) dotyczących pacjentów. Tylko w 2013 roku nastąpiły włamania do danych o 7 095 145 pacjentach. W 2012 roku nastąpił wzrost naruszonych danych pacjentów o 137,7%.
- W latach 2013–2014 przeprowadzono w USA dwa cyberataki na sieć Beecher's Hospital, dezorganizując prace i wręcz powodując chaos w 20 szpitalach o 31 000 łóżek w 29 stanach.

- W pojedynczym największym ataku hakerskim na Community Health Systems (CHS) wykradziono 4 029 530 danych (*records*) dotyczących chorych z 206 szpitali w 29 stanach USA.
- Atak na US Department of Veteran Affairs doprowadził do wykradzenia około 50 tysięcy danych.
- Rok 2016. Zaatakowano system MedStar Washington Hospital Centre: 10 szpitali i 250 przychodni. Chorzy leczeni byli bez wyników badań laboratoryjnych, co obrazuje dowodnie, że ataki tego typu są przykładem cyberterroru skierowanego bezpośrednio przeciwko życiu i zdrowiu ludzi.
- Jedyny w swoim rodzaju cyberatak *a rebours* przeprowadziła 15 marca 2003 roku w USA rządowa amerykańska Agencja do spraw Walki z Narkotykami (DEA – *Drug Enforcement Administration*). Po raz pierwszy w historii DEA przeprowadziła oficjalny atak przeciwko sklepom sprzedającym narkotyki, dopalacze i fajki wodne. Chociaż cyberatak był „łagodny", miał charakter głównie prewencyjny: osoby wchodzące na witrynę internetową tych sklepów wchodziły w istocie na stronę agencji DEA, która wyświetla treści ostrzegające przed zakupami, spotkał się z nasiloną polemiką.

W Polsce, z krakowskiego szpitala przekazano blisko 500 tysięcy złotych na konto oszusta, który podszywając się pod dostawcę leków, poinformował w e-mailu o zmianie konta bankowego.

Powyższe dane są nie tylko przykładowe, ale i z pewnością niepełne odnośnie do rozeznania rzeczywistej skali „cyberataków kontra medycyna" w USA, jak i ich kosztów finansowych, pomijając – jakże istotne – imponderabilia związane ze skutkami w postaci śmierci i dodatkowych schorzeń pacjentów, wynikających z aktów bioterroru przeciwko, najszerzej pojętym, strukturom medycznym. Zachodzą tu bowiem dwa znane w epidemiologii, a nakładające się zjawiska dotyczące ich rzeczywistej częstości. Jednym jest niepełne ich zgłaszanie (*underestimation*), drugim – dalece niepełne rozpoznanie (*underdiagnosed*) hakerskich cyberataków na urządzenia i infrastrukturę medyczną. Ponadto prominentne ofiary cyberataków (wielkie sieci szpitali, centrale dystrybucji leków, korporacje farmaceutyczne, systemy ubezpieczeniowe) niechętnie przyznają się – jako świadczeniodawcy „usług" medycznych, do braku ich bezpieczeństwa. Część danych jest także z pewnością utajnionych. Ponadto w Polsce cyberataki na struktury me-

dyczne mogą być z pewnością nierozpoznane i przypisywane (jak często?) „zwykłym" awariom sprzętu i omyłkom operatorów.

We wszystkich państwach rozwiniętych postępuje coraz powszechniejsze stosowanie – wprowadzonych już w poprzednich latach – technologii informacyjnych w służbie zdrowia. Jedna z zasadniczych (flagowych) inicjatyw Unii Europejskiej: „Strategia Europy 2020" – wprowadza pojęcie Agendy Cyfrowej, której celem ma być „maksymalizacja społecznego i ekonomicznego potencjału technologii informacyjnych i telekomunikacyjnych (ICT)", w tym ich wprowadzenie do wszystkich „usług medycznych", jak żargonowo i pozbawiając ich personalistycznego nazywania, określa się całokształt działań profilaktycznych, diagnostycznych i leczniczych współczesnej medycyny. W dosłownie każdym dokumencie oficjalnym, publikacji czy dyskusji na temat poprawy wydajności ochrony zdrowia publicznego pojawiają się pojęcia „E-health" lub „e-zdrowie". Pojawiły się oficjalne inicjatywy interoperacyjności i telemedycyny, np.: „Calliope" (interoperacyjność w e-zdrowiu), „epSOS" (platforma e-usług dla pacjentów europejskich), „Renewing Health", „eHealth for Regions for Regions. Integrated Structures in the Baltic Sea Area". Opisany proces postępuje od kilku lat również w Polsce, np. wprowadzony system „Ewuś". Awaryjność rozwiązań sieciowych znamy z codziennej praktyki („system się zawiesił", „awaria systemu"); jednak skala zagrożeń cyberatakami (a nawet sama ich możliwość) nie jest jeszcze u nas, odnośnie do ochrony zdrowia, brana poważnie pod uwagę (poza pierwszymi sygnałami ze strony prywatnych właścicieli sieci laboratoriów diagnostycznych). Paradoksalnie, pewnym atutem jest w Polsce niewątpliwe zapóźnienie w procesach informatyzacji służby zdrowia i struktur pokrewnych. Oczekiwać należy, że informatyzacja – także w służbie zdrowia – postępować będzie u nas równolegle z tworzeniem systemów zabezpieczających: niezwykle złożonych, drogich i nadal nie w pełni skutecznych. Interdyscyplinarne i międzyresortowe wypracowanie takich zabezpieczeń systemowych nie jest zadaniem łatwym ani tanim. Prace takie zostały już podjęte wspólnie z Ministerstwem Cyfryzacji, między innymi w ramach działań tworzenia „e-państwa" i Narodowego Operatora Sieci Strategicznych (Burgemeister, 2016; Ruman, 2016).

Podsumowaniem realności zagrożenia cyberatakami cyberterroryzmem mogą być słowa prezydenta USA Baracka Obamy, wypowiedziane 12 lutego 2013 roku: „America must also face the rapidly growing threat from

cyber-attacks… We cannot look back years from now and Wonder with we did nothing in the face of real threats to our security and our economy".

A może należy postawić półżartem obrazoburczą tezę, że najbardziej zacofani (opóźnieni w informatyzacji) są najbardziej bezpieczni?

WNIOSKI

1. Realne i pojawiające się już zagrożenie za strony cyberataków (cyberterroryzmu) wymierzonego we wszystkie struktury najszerzej pojętej współczesnej medycyny jest nowym, ale gwałtownie narastającym wyzwaniem nie tylko dla decydentów służby zdrowia, ale i dla władz wszystkich cywilizowanych państw świata.
2. Wymóg zapewnienia cyberbezpieczeństwa w stosunku do działalności medycznej (chorych, aparatury medycznej, sieci teleinformatycznej służby zdrowia, farmakoekonomiki) staje się jednym z najważniejszych globalnych wyzwań stających przed medycyną obecnej doby.
3. Szacowanie ryzyka takich cyberataków (wraz z oceną ich źródeł, metod, szkodliwości) oraz systemowe i interdyscyplinarne wdrażanie działań zaradczych (wraz z oceną ich realnej skuteczności i efektywności – także „cost-benefit analysis") wymaga natychmiastowych działań, podjętych już zresztą w wielu krajach świata (USA, Australia, Nowa Zelandia, Chiny i inne), a zapoczątkowanych ostatnio także w Polsce.

Bibliografia

Ashby W.R. (1963). *Wstęp do cybernetyki*. Państwowe Wydawnictwa Naukowe. Warszawa.

Błasiak Z.A., Koszowy M. (2003). *Informacja*, [w:] A.M. Krąpiec, A. Lobato, P. Jaroszyński, H. Kiereś, Z.J. Zdybicka (red. nauk.). *Powszechna Encyklopedia Filozofii*. Tom 4 (Go-Iq). Wyd. PTTA – SITA. Lublin. s. 824–829.

Bógdał-Brzezińska A., Gawrycki M.F. (2003). *Cyberterroryzm i problemy bezpieczeństwa narodowego we współczesnym świecie*. ASPA-JR. Warszawa.

Burgemeister S. (14 czerwca 2016 r.). Realizacja okresowego audytu wewnętrznego w zakresie bezpieczeństwa teleinformatycznego. Przykłady dobrych praktyk. MSWiA. Pierwsza Konferencja szkoleniowa audytorów wewnętrznych w resorcie spraw wewnętrznych i administracji. MSWiA. Warszawa. Materiały e-mailowe, s. 24–58.

Craigen D., Diakun-Thibault N., Purse R. (2014). *Defining Cybersecurity*. „Technology Innovation Management Review", nr 4 (10), s. 13–21.

Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej. Biuro Bezpieczeństwa Narodowego. Warszawa 2015.

Fiedler B.A. (red.) (2016). *Managing Medical Devices within a Regulatory Framework*. Elsevier. Amsterdam.

Halperin D., Heydt-Benjamin T.S., Ransford B., Clark S.S., Defen B. et al. (2008). *Implantable Cardiac Deffibrillations: Software Radio Attack and Zero-Power Defenses*, [w:] *Security and Prevency*. SP 2008 IEEE Symposium. Oakland, California, USA. May 18–22, 2008, s. 129.

Jastrzębski J. (2003). *Chaos na cenzurowanym, późna eseistyka Lema*. „Zagadnienia Filozofii w Nauce", XXXIII, s. 47–63.

Kowalewski J., Kowalewski M. (2014). *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa*. „Telekomunikacja i Techniki Informacyjne", nr 1–2, s. 24 –32.

Kramer D.B., Baker M., Ransford B., Molina-Markham A., Stewart Q., Fu K., Reynolds M.R. (2012). *Security and Privacy Qualities on Medical Devices: An Analysis of FDA Postmarket Surveillance*. PLoS One. 7(7), e40200.

Lubański M., Szymański A., Zięba S. (2001). *Cybernetyka*, [w:] A.M. Krąpiec, A. Lobato, P. Jaroszyński, H. Kiereś, Z.J. Zdybicka (red. nauk.). *Powszechna Encyklopedia Filozofii*. Tom 1 (A-C). Wyd. PTTA – SITA. Lublin, s. 326–329.

Maciejewski J. (2014). *Grupy dyspozycyjne. Analiza socjologiczna*. Wydanie II. Wydawnictwo Uniwersytetu Wrocławskiego. Wrocław.

Mider D. (2013). *Analiza pojęcia cyberterroryzmu. Próba uporządkowania chaosu*. Annales Universitatis Mariae Curie-Skłodowska. Lublin – Polonia. Sectio K., XX, 2, s. 81–114.

Okolowski P. (2005). *Stanisław Lem*, [w:] W. Mackiewicz (red.), *Polska filozofia powojenna*. AW Witmark. Warszawa, Tom III, s. 179–204.

Patelak A. (2005). *Cyberterroryzm a bezpieczeństwo Rzeczypospolitej.* II. *Problem cyberterroryzmu w polityce ONZ, UE, NATO, USA i Rosji*. „Biuletyn Centralnego Ośrodka Szkolenia Straży Granicznej", 34 (3), s. 81–95.

Ruman S. (22–28 sierpnia 2016). *Powołajmy narodowego operatora sieci strategicznych*. „W Sieci".

Sienkiewicz P. (2015). *Ontologia cyberprzestrzeni*. „Zeszyty Naukowe Wyższej Szkoły Informatyki", nr 13, s. 89–102.

Szpunar M. (2004). *Społeczności wirtualne jako społeczności – próba ujęcia socjologicznego*, [w:] M. Radochoński, B. Przywara (red.) *Jednostka – grupa – cybersieć. Psychologiczne, społeczno-kulturowe i edukacyjne aspekty społeczeństwa informacyjnego*. WSiZ. Rzeszów , s. 157–184.

Tadeusiewicz R. (red.), (2009). *Neurocybernetyka teoretyczna*. Wydawnictwa Uniwersytetu Warszawskiego. Warszawa.

Talbot D. (2012, October 17). *Computer Viruses are "Rampant" an Medical Devices in Hospitals*. Massachussets Institute of Technology (MIT). Technology Review.

US Food and Drug Administration (FDA). *Content of Premarket Submision for Management of Cybersecurity in Medical Devices*. US FDA, 2014 [Accessed June 9, 2015].

Wellington K.B. (2013). *Cyberattacks on medical devices and hospital networks: legal gaps and regulatory solutions*. „Santa Clara High Technology Law Journal", 30, 2, s. 138–200.

Williams P.A.H., Woodward A.J. (2015). *Cybersecurity vulnerabilities in medical devices: a complex environmental and multifaceted problem*. Medical Devices (Auckland). 8, s. 305–316.

Wittgenstein L.: *Tractatus logico-philosphicus*. Tłum. B. Wolniewicz. PWN. Warszawa 2011.

Źródła internetowe

Berdel-Dudzińska M. (bez daty, po 2011). *Pojęcie cyberprzestrzeni we współczesnym polskim porządku prawnym*. Profinfo.pl.