ZESZYTY NAUKOWE 1/2019

Wywiad i kontrwywiad gospodarczy

Materiały z konferencji naukowych

pod redakcją
Hieronima Szafrana
i Jerzego Wojciecha Wójcika

WSZECHNICA POLSKA
Szkoła Wyższa w Warszawie

Recenzent
dr hab. Andrzej Czupryński
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach

Rdakcja naukowa
dr Hieronim Szafran, prof. dr hab. Jerzy Wojciech Wójcik

Redakcja wydawnicza
Bogumił Paszkiewicz

Projekt graficzny i typograficzny
Krystyna Bukowczyk

ISSN 2300-990X

Nakład 100 egz.

WSZECHNICA POLSKA
Szkoła Wyższa w Warszawie

Pałac Kultury i Nauki
00-901 Warszawa, pl. Defilad 1
rekrutacja@wszechnicapolska.edu.pl

www.wszechnicapolska.edu.pl

Spis treści

Wojciech Michalak

Wprowadzenie

Dwie konferencje naukowe na temat „Wywiad i kontrwywiad w teorii i praktyce biznesu" zorganizowała Wszechnica Polska Szkoła Wyższa w Warszawie i Fundacja Instytut Wywiadu Gospodarczego w Krakowie. Wybrany dorobek tych konferencji w syntetycznym ujęciu prezentuje właśnie niniejsze wydawnictwo.

Inspiracją do przygotowania pierwszej krajowej konferencji w 2017 roku była coraz bardziej widoczna bezwzględna rywalizacja i ekspansja międzynarodowych i krajowych podmiotów biznesowych (gospodarczych, finansowych i innych) dążących do opanowania rynku, wygrania konkurencji i wdrożenia innowacyjnych rozwiązań i działań. Przewaga informacyjna własnych podmiotów biznesowych, sprzyjającą także bezpieczeństwu ekonomicznemu państwa, mają m.in. zapewniać aktywne działania wywiadowcze i kontrwywiadowcze realizowane przez profesjonalnie przygotowane struktury (zespoły) na wszystkich poziomach działań biznesowych.

Wstępna analiza omawianego zjawiska wykazała, że praktyka funkcjonowania biznesu wymusiła różnorodne działania o charakterze wywiadowczym i przeciwdziałającym utracie wrażliwych informacji i rozwiązań własnych, nauka zaś nie zawsze podejmuje wszechstronne i pogłębione badania w tym zakresie. Ponadto, zwłaszcza z uwagi na dyskretność takich przedsięwzięć, część wyników badań i większość rozwiązań praktycznych stosowanych przez podmioty biznesowe ma charakter niejawny i nie podlega rozpowszechnianiu. Powoduje to rozproszenie prac naukowo-badawczych, ich fragmentaryczny opis czy też niesatysfakcjonujące usystematyzowanie wiedzy w zakresie praktyki biznesowej, natomiast częsta dezintegracja działań i swoista autarkia prowadzą do „odkrywania" lub powielania rozwiązań już stosowanych od pewnego czasu przez konkurencję. Dodatkowo dało się zauważyć, że kształcenie na poziomie wyższym omawianej problematyki nie należy do powszechnych; raczej można je zaliczyć do unikatowych specjalności lub przedmiotów nauczania przypisanych do niektórych kierunków kształcenia (jak np. bezpieczeństwo narodowe, bezpieczeństwo wewnętrzne, rachunkowość i finanse, ekonomia, informatyka, cyberbezpieczeństwo i inne).

W wyniku takiej oceny środowisko pracowników naukowo-dydaktycznych Wszechnicy Polskiej Szkoły Wyższej w Warszawie i Zarząd Instytutu Wywiadu Gospodarczego zainicjowały organizację ogólnopolskiego spotkania naukowego przeznaczonego dla pracowników naukowych (teoretyków) i praktyków biznesu, aby zidentyfikować przedmiot badań, usystematyzować podstawową wiedzę z zakresu wywiadu i kontrwywiadu w biznesie, poznać potrzeby (oczekiwania)

podmiotów gospodarczych i kształcenie z tej problematyki w naszych uczelniach oraz przeanalizować sposoby i metody działań stosowane w podmiotach biznesowych w przedmiotowym obszarze ich działalności.

Celem głównym spotkania była konfrontacja wyników badań prowadzonych przez przedstawicieli różnych dziedzin dyscyplin naukowych oraz interdyscyplinarna debata nad problemami wywiadu i kontrwywiadu gospodarczego w kontekście aktualnych i prognozowanych zmian w międzynarodowym i krajowym środowisku bezpieczeństwa biznesu.

Konferencja spotkała się z wyjątkowym zainteresowaniem, co dowodzi, że poruszana problematyka jest niezwykle ważna i aktualna nie tylko dla licznie reprezentowanego na konferencji świata nauki, biznesu i stowarzyszeń branżowych, ale i dla urzędników, funkcjonariuszy i pracowników administracji rządowej, służb i straży, a także doktorantów i młodzieży studenckiej z kilku uczelni.

Bardzo udanym zabiegiem organizacyjnym był wyraźny podział konferencji na panele plenarne (ogólne) i dyskusyjne. W panelach plenarnych zarówno pracownicy naukowi z kilku uczelni i instytutów naukowo-badawczych, jak i praktycy z instytucji (podmiotów) gospodarczych i innych koncentrowali swoje wystąpienia na teoretycznych aspektach prowadzenia wywiadu i kontrwywiadu w biznesie oraz przekazywaniu doświadczeń z pragmatycznej działalności różnych podmiotów w tym zakresie. Wskazywano różne propozycje poprawiające doraźne i długofalowe prowadzenie wywiadu oraz przeciwdziałanie temu zjawisku w świecie biznesu i gospodarki, a zatem i bezpieczeństwa narodowego (wewnętrznego, gospodarczego itp.). W czasie panelu dyskusyjnego poszukiwano odpowiedzi m.in. na takie problemy, jak: Jakie są oczekiwania biznesu ze strony własnego (i państwowego) wywiadu i kontrwywiadu? Jakie technologie, narzędzia i posoby działań wdrażać, aby zwiększyć konkurencyjność narodowych podmiotów biznesowych? Jakimi materiałami źródłowymi wzbogacać wiedzę zespołów odpowiedzialnych za wywiad i kontrwywiad w podmiotach biznesowych? Jaka jest potrzeba kształcenia w tym zakresie?

Zarówno w panelu plenarnym, jak i dyskusyjnym podnoszono problem wzrostu roli bezpieczeństwa, konieczności dokonywania analizy ryzyka, potrzebę kontrwywiadowczego zabezpieczenia inwestycji, niezbędność kształcenia z zakresu bezpieczeństwa biznesu czy też celowość pogłębienia współpracy uczelni z zainteresowanymi podmiotami gospodarczymi i innymi.

Przebieg konferencji potwierdził wagę i aktualność podjętej problematyki. Postanowiono wprowadzić roczną cykliczność ogólnopolskich konferencji dotyczących wywiadu i kontrwywiadu w teorii i praktyce biznesu, zintensyfikować kształcenie w tej tematyce oraz powołać przy Wszechnicy Polskiej swoiste centrum grupujące teoretyków i praktyków, którzy zajmą się pogłębionymi badaniami i przygotowaniem ekspertyz.

Kolejne spotkanie naukowe organizowane przez te same podmioty, co wcześniejsza konferencja (Wszechnicę Polską i Fundację Instytut Wywiadu Gospodar-

czego) odbyło się w 2018 roku. Zgromadziło ono kilkudziesięciu uczestników z różnych uczelni, instytucji badawczo-rozwojowych, podmiotów biznesowych, administracji publicznej i agencji centralnych. Znaczna część z nich uczestniczyła także w konferencji wcześniejszej. Założenia i przebieg omawianej konferencji nie odbiegały istotnie od tych zaprezentowanych wyżej. W panelach plenarnych koncentrowano wystąpienia na teoretyczno-badawczych wyzwaniach oraz uwarunkowaniach działalności wywiadowczej i kontrwywiadowczej w polskim biznesie i edukacji. Panel dyskusyjny zaś poświęcono przede wszystkim wyzwaniom pragmatycznym oraz problemom i propozycjom rozwiązań, które prezentowali głównie praktycy z podmiotów gospodarczych, usługowych i biznesowych.

Niemal dwudziestu referentów występujących w obu blokach panelowych eksponowało bardzo szerokie pola badawcze, obejmujące informacyjne funkcje wywiadu i kontrwywiadu gospodarczego, problemy bezpieczeństwa informacji, osobowe i analityczne (zespołowe) źródła pozyskiwania informacji, zasady zachowania tajemnicy przedsiębiorstwa, stosowane metody w wywiadzie i kontrwywiadzie biznesowym oraz inne zagadnienia. Obrazowały one niezwykle różnorodne i interdyscyplinarne obszary dociekań twórczych i rozwiązań praktycznych, które sprzyjają uzyskaniu przewagi konkurencyjnej w gospodarce. W wypowiedziach wskazywano ponadto na opóźnienia i trudności w prowadzeniu działalności wywiadowczej i kontrwywiadowczej w biznesie, zwłaszcza w małych podmiotach gospodarczych, opóźnienia w tworzeniu aktów normatywnych wobec dynamicznego postępu technologicznego czy też prowadzenia przedmiotowej działalności w zglobalizowanym świecie oraz w warunkach narastającej cyberprzestępczości i pojawiania się nowych rodzajów zagrożeń.

* * *

Niniejsze wydawnictwo zawiera zaledwie niewielką część z około czterdziestu wystąpień panelistów na obu konferencjach. Wybór materiałów do publikacji był podyktowany także tym, że większość referentów, wywodzących się zwłaszcza z podmiotów biznesowych nie oczekiwała publikacji ich wystąpień. Dotyczyło to szczególnie tych uczestników konferencji, którzy w swoich wypowiedziach sygnalizowali wrażliwe obszary działalności wywiadowczej i osłony kontrwywiadowczej w gospodarce i biznesie.

Prezentowane referaty potwierdzają bardzo szerokie pola badawcze lokowane w różnych dziedzinach i dyscyplinach naukowych i na styku wielu specjalności badawczych oraz różnorodne przedmioty i obiekty możliwych eksploracji, co czyni problematykę wywiadu i kontrwywiadu w biznesie trudną do opracowania teoretycznego i rozwiązań praktycznych. W tym kontekście trzeba zwrócić uwagę na materiał dr. Hieronima Szafrana, w którym zaprezentowano rozwiązania przyjęte w Wszechnicy Polskiej w zakresie kształcenia specjalistów wywiadu i kontrwywiadu gospodarczego wykorzystujące doświadczenia anglosaskie i holenderskie, czy też publikację Łukasza Wacławika o doświadczeniach fran-

cuskich w zakresie zarządzania strategicznego informacjami. Z opracowań tych wynika bowiem, że w innych państwach problematyka związana z wywiadem i osłoną kontrwywiadowczą w biznesie jest jednym z priorytetów działań państwa, szkół wyższych i podmiotów gospodarczych.

Problematyka ta jest także coraz bardziej eksponowana w naszym kraju, a dorobek polskich służb, administracji publicznej (gospodarczej), uczonych, przedsiębiorców i podmiotów biznesowych w przedmiotowej tematyce jest już znaczący. Potwierdzają to zawarte w niniejszym opracowaniu artykuły profesorów Mieczysława Kwiecińskiego i Jerzego Wojciecha Wójcika oraz Anny Nastuli i Pawła Pruszyńskiego, Agnieszki Latosińskiej, Teresy Przybyszewskiej i inne.

Wyrażamy nadzieję, że prezentowane wydawnictwo zainteresuje wszystkich, którym sukces polskich podmiotów biznesowych jest bliski, a bezpieczeństwo ekonomiczne państwa nie jest obojętne. Liczymy także, że zainspiruje ono Czytelników do aktywnego udziału w kolejnych edycjach konferencji Wywiad i kontrwywiad w teorii i praktyce biznesu.

Wojciech Michalak*

***prof. dr Wojciech Michalak, Wszechnica Polska Szkoła Wyższa w Warszawie**

Jerzy Wojciech Wójcik

Z problematyki bezpieczeństwa informacji i tajemnic zawodowych

Wprowadzenie

Minęły już czasy, w których fascynowano się kapitałem jako rzeczą najważniejszą, nie tylko w biznesie. Od dawna wiadomo, że informacja powstała wcześniej niż kapitał. Ponadto, już dawno rozpoznano, że w życiu społecznym nie ma nic bardziej wartościowego niż informacja. Podstawowym zasobem jest przede wszystkim posiadanie informacji i wiedzy, które przykładowo mogą w zasadny sposób doprowadzić do zgromadzenia kapitału.

Z przeprowadzonych badań wynika, że jeśli informacja jest dobrej jakości, to obecnie może być: towarem, podstawowym elementem procesów biznesowych, służyć do sterowania procesami w zautomatyzowanych procesach wytwórczych i usługowych o kluczowym znaczeniu dla gospodarki i społeczeństwa. Ponadto, informacja jest chroniona na mocy obowiązującego prawa lub zawartych umów.[1]

Warto zatem zwrócić uwagę na takie zagadnienia jak: informacja, wiedza, kapitał i prawo, gdyż mają one istotne związki z bezpieczeństwem biznesu. Nie ulega wątpliwości, że niejednokrotnie stają się przedmiotem penetracji ekspertów wywiadu gospodarczego, a nawet szpiegostwa gospodarczego.

Celem mojego referatu jest pobudzenie środowisk naukowych, zawodowych, biznesowych, a także studenckich do analizowania, badania i rozumienia znaczenia oraz potrzeby ochrony właściwych informacji i tajemnic zawodowych.

Definicja informacji

Informacja jest zjawiskiem starym jak świat i terminem interdyscyplinarnym. Najogólniej oznacza właściwość badanych obiektów, relację między elementami zbiorów obiektów, której istotą jest zmniejszanie niepewności (nieokreśloności)[2]. Wielość i różnorodność definicji skłania do wymienienia przynajmniej kilku, a przykładowo:

- informacja to wiadomość, nowina[3];
- informacja oznacza element wiedzy przekazywanej za pomocą języka lub innego kodu i stanowi czynnik zmniejszający stopień niewiedzy o jakimś zjawisku, umożliwiający człowiekowi polepszenie znajomości otoczenia i sprawniejsze przeprowadzenie celowego działania[4];

1 K. Liderman, *Bezpieczeństwo informacyjne. Nowe wyzwania*. PWN, Warszawa 2017, s. 15.
2 http://pl.wikipedia.org/wiki/Informacja(dostęp18.06.2010)
3 W. Kopaliński (red.) *Słownik języka polskieg*o, Warszawa 1985, s. 188.
4 B. Dunaj (red.) Słownik współczesny języka polskiego, Warszawa 1998, s. 320.

- informacją jest wiadomość lub określona suma wiadomości o sytuacjach, stanach rzeczy, wydarzeniach i osobach. Może być przedstawiona w formie pisemnej, fonicznej, wizualnej i każdej innej możliwej do odbioru przy pomocy zmysłów[5];
- informacja to: każdy czynnik, dzięki któremu człowiek lub urządzenia automatyczne mogą przeprowadzić bardziej sprawne, celowe działanie; powiadomienie o czymś, zakomunikowanie czegoś; wiadomość, pouczenie; komórka w urzędzie udzielająca informacji[6]. W języku potocznym informacja to wiadomość, komunikat, wskazówka, pouczenie[7].

Posługiwanie się informacją, jej przekaz czy wymiana są znane i niezbędne od najdawniejszych czasów. Ludzie pierwotni porozumiewali się za pomocą muzyki bębnów, czy pisma obrazkowego, a więc bez znajomości języków obcych[8]. Przekazywane informacje były zazwyczaj ważne, jak np.: nadciąga wróg, czy obiad przygotowany.

Prawna ochrona informacji

Prawna ochrona informacji związana jest przede wszystkim z obowiązkiem zachowania tajemnicy zawodowej. Sam termin *tajemnica* definiowany jest dość szeroko. Według *Słownika języka polskiego* jest to: „sekret czy nieujawnianie czegoś; wiadomość, której poznanie lub ujawnienie jest zakazane przez prawo; rzecz, której się nie rozumie lub nie umie wyjaśnić; najlepszy lub jedyny sposób na osiągnięcie czegoś”[9]. Według Wikipedii określany jest jako dane lub informacje, których ujawnienie osobom nieuprawnionym jest zakazane ze względu na normy prawne lub inne normy społeczne[10].

Dokonując podziału rodzaju informacji na jawne i poufne, a więc zawierające tajemnice zawodową lub inną prawnie chronioną, należy wspomnieć, że praktycznie w żadnym akcie prawnym nie jest zawarta pełna definicja tajemnicy zawodowej, mimo że niektóre ustawy posługują się tą terminologią.

Warto zatem podkreślić, że termin tajemnica zawodowa istnieje wówczas, gdy wiadomość nią objęta została uzyskana przez osobę reprezentującą określony zawód, z tytułu wykonywania którego było możliwe wejście w posiadanie cudzej tajemnicy czy sekretu[11]. Ustalenie obowiązku zachowania tajemnicy zawodowej może wynikać wprost z przepisów regulujących tryb i zasady wykonywania określonych zawodów bądź z przyjęcia na siebie zobowiązania, co do nieujawniania faktów poznanych w związku z wykonywaną pracą zawodową[12]. Źródłem obo-

5 B. Michalski, *Prawo dziennikarza do informacji*, Kraków 1974, s. 9-10.
6 Leksykon PWN, Warszawa 1972, s. 444.
7 M. Szymczak (red.), *Słownik języka polskieg*o, t. 1, Warszawa 1988, s. 788.
8 Warto przy tym zaznaczyć, że wymiana informacji za pomocą pisma obrazkowego stosowana jest do dzisiaj w analizie kryminalnej.
9 http://sjp.pwn.pl/lista/T;6.html(dostęp 22.9.2014)
10 http://pl.wikipedia.org/wiki/Tajemnica(dostęp12.12.2014)
11 W. Wróbel, *Niektóre problemy ochrony tajemnicy w projekcie kodeksu karnego*, Przegląd Prawa Karnego 1996, nr 14, 15.
12 Tamże.

wiązku zachowania dyskrecji w przypadku tajemnicy zawodowej nie muszą być wyraźne przepisy prawne, lecz także zasady etyki zawodowej.

Tajemnica zawodowa ma dwojaki charakter, tzn. może obejmować wiadomości, które dotyczą życia określonych osób, uzyskane w ramach dokonywania czynności zawodowych czy też pełnionych funkcji, oraz informacje dotyczące samego zawodu i sposobu jego wykonywania. Przykładem w tej mierze może być przepis art. 266 § 1 k.k.[13], który nie dotyczy jednak tylko tajemnicy zawodowej, ma bowiem zakres o wiele szerszy – obejmuje także każdą tajemnicę, poznaną w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową. Stąd też ten rodzaj tajemnicy określany jest także, jako tajemnica funkcyjna[14]. Pojęcie tajemnicy prywatnej natomiast używane być może ze względu na rodzaj informacji stanowiących przedmiot tajemnicy, tj. dotyczących prywatnej sfery życia dysponenta informacji[15].

Źródłem obowiązku zachowania tajemnicy zawodowej jest cytowany art. 266 § 1 k.k. bądź konkretny przepis prawa, czyli z określonej ustawy, bądź też umowa pomiędzy dysponentem informacji i depozytariuszem, której treścią jest przyjęcie zobowiązania dyskrecji[16]. Oczywista staje się zatem uwaga, że tajemnicą nie może być informacja powszechnie znana.

Przepisy prawa regulują rodzaje tajemnic, związanych najczęściej z pełnioną funkcją, wykonywanym zawodem, prowadzoną działalnością: sędziowską, prokuratorską, adwokacką, radcowską, notarialną i inną.

Kolejnym przykładem informacji, chronionej przepisami kodeksu karnego jest tajemnica korespondencji. Pojęcie to oznacza, iż wszystko, co jest przedmiotem przekazu od nadawcy do adresata, należy wyłącznie do tych osób, z wyjątkiem sytuacji, gdy wyrażą one zgodę na udostępnienie również innym osobom informacji, które między sobą przekazują. Ten rodzaj tajemnic jest istotną częścią składową prawa do poszanowania życia prywatnego, w tym również do poszanowania informacji, które mają pozostać w tajemnicy. Naruszenie tajemnicy korespondencji podlega karze z art. 267 § 1 k.k. W sytuacjach szczególnych (np. związanych ze ściganiem poważnych przestępstw) przepisy zezwalają na naruszenie tajemnicy korespondencji, jak to ma miejsce zgodnie z art. 15 ust. 1 pkt 5a ustawy z 6 kwietnia 1990 r. o Policji[17].

13 Art. 266. § 1. Kto, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Funkcjonariusz publiczny, który ujawnia osobie nieuprawnionej informację niejawną o klauzuli „zastrzeżone" lub „poufne" lub informację, którą uzyskał w związku z wykonywaniem czynności służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes, podlega karze pozbawienia wolności do lat 3.

14 Kunicka-Michalska, *Przestępstwa przeciwko tajemnicy państwowej i służbowej*, w: System Prawa Karnego 1989, s. 445, 446. Cyt. za M. Mozgawa, Kodeks karny. Komentarz, Warszawa 2014, s. 666.

15 Tamże.

16 T. Bojarski (red.), *Kodeks karny. Komentarz*, Warszawa 2011, s. 638.

17 Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz.U. 1990 nr 30, poz 179 z późn. zm.).

Szeroki zakres tematyki skłania do konieczności omówienia jedynie wybranych zagadnień tego interesującego zagadnienia. Koniecznie jednak należy wspomnieć, że: w przypadku postępowania karnego można przykładowo uchylić: tajemnicę korespondencji, rozmów telefonicznych czy przelewów bankowych.

Wybrane rodzaje tajemnic zawodowych

Mówiąc o problemach bezpieczeństwa informacji, najczęściej mamy na myśli tylko te elementy wiadomości, które są opatrzone klauzulą tajne czy poufne.

Znanych jest przynajmniej 58 różnych aktów prawnych, regulujących omawiane problemy; począwszy od Konstytucji RP i kodeksu postępowania karnego aż po prawo kanoniczne. Przepisy te regulują różnorodne rodzaje tajemnicy, nie tylko o charakterze strategicznym czy przemysłowym. Wszystkie one podlegają ochronie prawnej zgodnie z przepisami szczegółowymi, a ich ujawnienie może być ścigane według regulacji karnoprawnych[18].

Zagadnienie ochrony informacji zawodowych przejawia się w obowiązującym stanie prawnym. Można zatem wyróżnić szereg rodzajów tajemnic zawodowych prawnie chronionych[19], a przykładowo: tajemnica handlowa, ksiąg rachunkowych, bankowa, ubezpieczeniowa, publicznego obrotu papierami wartościowymi, doradcy podatkowego i biegłego rewidenta, tajemnice rzeczoznawców majątkowych, pośredników w obrocie nieruchomościami i zarządców nieruchomościami, adwokacka i radcowska, notarialna, komornika sądowego, funduszy inwestycyjnych, wynalazcza, skarbowa, statystyczna, dziennikarska, autorska, detektywistyczna, pomocy społecznej, spowiedzi[20], służby więziennej, wojskowa, geologiczna i geodezyjna, wolności sumienia i wyznania, akt stanu cywilnego, tajności głosowania w wyborach, ubezpieczeń społecznych, majątkowych i osobowych, postępowania administracyjnego, postępowania karnego, świadka koronnego, czynności operacyjno-rozpoznawczych gromadzenia, przetwarzania i przekazywania informacji kryminalnych i szereg innych.

W zasadzie tajemnice te chronione są właściwymi aktami prawnymi, a przykładowo:

- tajemnica lekarska – ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty[21],
- prokuratorska – ustawa z dnia 20 czerwca 1985 r. o prokuraturze[22],
- radcowska – ustawa z dnia 6 lipca 1982 r. o radcach prawnych[23],

18 Niektórzy autorzy dopatrują się około 200 tajemnic.

19 Szerzej R i M. Taradejna, *Ochrona informacji w działalności gospodarczej, społecznej i zawodowej oraz życiu prywatnym*, Warszawa 2004, s. 24-253.

20 Z aktu oskarżenia przeciwko zakonnikowi z Zakroczymia wynika, że do uwodzenia chłopców poniżej lat 15 duchowny miał wykorzystywać informacje zdobyte w konfesjonale, a więc w ramach tajemnicy spowiedzi. Szerzej: J. Bilikowska, *Prokuratura: cztery ofiary zakonnika pedofila*, Rzeczpospolita z 11 sierpnia 2014 r.

21 t.j. Dz. U. 1997 nr 28, poz. 152 z późn. zm.

22 t.j. Dz. U. 1985. nr 31, poz. 138 z późn. zm.

23 t.j. Dz. U. 1982 nr 19, poz. 145 z późn. zm.

- notarialna – ustawa z dnia 14 lutego 1991 r. - Prawo o notariacie[24],
- komornicza – ustawa z dnia 29 sierpnia 1997 r. o komornikach sądowych i egzekucji[25],
- dziennikarska – ustawa z dnia 26 stycznia 1984 r. - Prawo prasowe[26],
- pielęgniarska i położnicza – ustawa z dnia 15 lipca 2011 r. o zawodach pielęgniarki i położnej[27],
- psychiatryczna – ustawa z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego[28],
- psychologa – ustawa z dnia 8 czerwca 2001 r. o zawodzie psychologa i samorządzie zawodowym psychologów[29],
- przeszczepów – ustawa z dnia lipca 2005 r. o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów[30].

Należy mieć na uwadze indywidualną czy specyficzną wiedzę pracownika, która nie stanowi tajemnicy przedsiębiorstwa. Dotyczy to osobistych umiejętności, specyficznego zakresu wiedzy i doświadczeń pracownika, o ile nabytych informacji nie można utrwalić lub przekazać innemu podmiotowi w postaci opisu, planu, rysunku itp. W związku z tym zatrudnionemu wolno je swobodnie wykorzystywać w celach zawodowych. Przedsiębiorca może jednak ograniczyć posługiwanie się informacjami nabytymi mimo woli w związku z zajmowanym stanowiskiem poprzez wprowadzenie zakazu konkurencji. Stanowi to umowne ograniczenie pracownika w podejmowaniu działalności mogącej naruszyć interesy przedsiębiorcy. Zatem zakaz konkurencji stanowi dodatkowe narzędzie, które umożliwia pracodawcy zintensyfikowaną ochronę tajemnic firmy. Nie ulega wątpliwości, że jeśli pracownik podejmuje pracę u innego przedsiębiorcy, zwłaszcza na zbliżonym stanowisku, to z dużym prawdopodobieństwem będzie wykorzystywał informacje nabyte w pierwszej firmie. Jeżeli zatem szef wprowadzi pracownikowi zakaz konkurencji, to wyeliminuje lub ograniczy posługiwanie się przez niego informacjami poufnymi.

Mając na względzie działalność w ramach wywiadu czy kontrwywiadu gospodarczego warto zwrócić uwagę na fakt, że zakres przedmiotowy tajemnicy przedsiębiorstwa ujęty został przez ustawodawcę bardzo szeroko. Opisany w ustawie katalog informacji mogących stanowić tajemnice przedsiębiorstwa w zasadzie wyczerpuje zakres informacji, które mogą zostać wykorzystane przez przedsiębiorcę w związku z prowadzoną działalnością gospodarczą. Na podstawie doświadczeń orzecznictwa sądowego oraz doktryny przedmiotu można wskazać

24 t.j. Dz. U. 1991 nr 22, poz. 91 z późn. zm.
25 Dz. U. 1997 nr 133, poz. 882 z późn. zm.
26 Dz. U. 1984 nr 5, poz. 24 z późn. zm.
27 t.j. Dz. U. 2011 r. nr 174, poz. 1039 z późn. zm.
28 Dz. U. 1994 nr 111, poz. 535 z późn. zm.
29 Dz. U. 2001 nr 73, poz. 763 z późn. zm.
30 R. Bieda, *Zakres pojęcia „tajemnica przedsiębiorstwa" na gruncie ustawy o zwalczaniu nieuczciwej konkurencj*i, http://www.itlaw.pl, s. 4 (dostęp 23.09.2014).

pewien zakres typowych informacji mogących stanowić tajemnicę przedsiębiorstwa. Ponadto, we współczesnej literaturze prawniczej przyjmuje się, iż tajemnicę przedsiębiorstwa stanowić mogą między innymi:

1) nieopatentowane wynalazki,
2) plany techniczne, listy klientów,
3) wiedza i metody natury administracyjnej i organizacyjnej,
4) metody kontroli jakości, sposoby marketingu, organizacji pracy,
5) treść zawartych umów, porozumień, korespondencję handlową,
6) strategię funkcjonowania przedsiębiorstwa,
7) informacje dotyczące techniki czy sposobu produkcji,
8) informacje dotyczące struktury przedsiębiorstwa, przepływu dokumentów, sposobu kalkulacji cen, zabezpieczenia danych,
10) treść opinii prawnych udzielanych przedsiębiorcy, treść negocjacji czy prac nad nowymi rozwiązaniami[31].

Wszystkie powyższe tajemnice mogą stanowić istotne źródła informacji przydatnych dla wywiadu gospodarczego, a szczególnie dla celów szpiegostwa gospodarczego.

Z kolei w praktyce sądowej jako tajemnice przedsiębiorstwa uznane zostały między innymi:

- dane zawarte w sprawozdaniach podatkowych PIT-5 i F-01, gdyż obrazują one pasywa i aktywa oferentów, dochód i zyski, koszty działalności, straty, zobowiązania finansowe[32],
- dane obrazujące wielkość produkcji i sprzedaży, a także źródła zaopatrzenia i zbytu[33],
- informacje o planach wydawniczych[34],
- wyniki finansowe stowarzyszenia i regulamin repartycji wynagrodzeń autorskich[35].

Nie ulega wątpliwości, że przedsiębiorca może ustanowić tajemnicę przedsiębiorstwa dotyczącą również w zakresie danych o: klientach, dostawcach, metodach i procedurach szkolenia pracowników, planach inwestycyjnych i produkcyjnych, założeniach cenowych produktów, wynikach przeprowadzonych testów i badań marketingowych, a także o wynagrodzeniach pracowników.

31 R. Bieda, *Zakres pojęcia „tajemnica przedsiębiorstwa" na gruncie ustawy o zwalczaniu nieuczciwej konkurencji*, http://www.itlaw.pl, s. 2/8-6/8 (dostęp 23.09.2014).
32 Orzeczenie Sądu Antymonopolowego z 10.07.2002 r. XVII Am 78/01, Dz. Urz. UOKiK z 2002, Nr 5, poz. 224.
33 Postanowienie Sądu Antymonopolowego z 15.10.1997 r. XVII Ama 1/96, Wokanda 1997, Nr 10, poz. 55.
34 Wyrok Sądu Apelacyjnego w Krakowie z 11.06.2003 r. I A Ca 469/03, TPP 2004, Nr 1-2, s. 157.
35 Wyrok SN z 05.09.2001 r. I CKN 1159/00, OSNC 2002, Nr 5, poz. 67.

Manipulowanie informacją jako czyn nieuczciwej konkurencji

Jednym z kluczowych zagadnień w gospodarce narodowej jest działalność przedsiębiorców i tajemnica przedsiębiorstwa. Mają one oczywiste związki biznesowe z konkurencją, a niejednokrotnie z nieuczciwą konkurencją, a ponadto z manipulowaniem informacją czy z wywiadem gospodarczym lub szpiegostwem gospodarczym.

Konkurencja (z jęz. łacińskiego *concurrentia*), czyli współzawodnictwo, towarzyszy zachowaniu przedsiębiorców uczestniczącym w grze rynkowej. Wynikają z tego przynajmniej dwa wnioski: konkurencja jest zjawiskiem zupełnie naturalnym oraz możliwe jest jej występowanie tylko w ramach gospodarki wolnorynkowej. Można przyjąć o stwierdzenie że w sensie ekonomicznym konkurencja jest jednym z podstawowych elementów napędzających rozwój gospodarczy. Konkurencja to *dążenie wielu niezależnych przedsiębiorców na wspólnym dla nich rynku do osiągnięcia takiego samego celu gospodarczego, w szczególności prowadzenia interesów z dostawcami, odbiorcami i pracownikami*[36].

Czyny nieuczciwej konkurencji zostały określone w art. 3, 5, 6, 98 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (uznk.)[37]. Zgodnie z art. 3 tej ustawy czynem nieuczciwej konkurencji jest działanie sprzeczne z prawem lub obyczajami, zagrażające lub naruszające interesy innego przedsiębiorcy lub klienta. Oznacza to, że muszą być spełnione określone zachowania przedsiębiorcy, aby można było uznać, że są one czynem nieuczciwej konkurencji. Uzasadniony jest pogląd, że muszą wystąpić łącznie następujące przesłanki:

1) przedsiębiorca musi uczestniczyć w obrocie gospodarczym, tj. w ramach działalności gospodarczej;
2) działanie przedsiębiorcy musi być niezgodne z prawem lub dobrymi obyczajami;
3) czyn ten musi zagrażać lub też naruszać interes innego przedsiębiorcy lub klienta – w ramach interesu o charakterze gospodarczym[38].

Zachowania, które zawarto w regulacji ustawowej jako czyny nieuczciwej konkurencji zostały ujęte w artykułach od 3 do 17f uznk. Jako główne znamiona tych czynów w szczególności są:

1) wprowadzające w błąd oznaczenie przedsiębiorstwa (art. 5, 6 i 7);
2) fałszywe lub oszukańcze oznaczenie pochodzenia geograficznego towarów albo usług (art. 8, 9 i 10);
3) wprowadzające w błąd oznaczenie towarów lub usług, jeżeli może wprowadzić klientów w błąd co do tożsamości producenta lub produktu (art. 10 i 13);

36 J. Szwaja, *Ustawa o zwalczaniu nieuczciwej konkurencji*. Komentarz, Warszawa, 2006, s.42
37 Dz.U. 1993 nr 47, poz. 211 z późn. zm.
38 M. Mrzygłód, *Jak bronić się przed nieuczciwą konkurencją*, http://msp.money.pl/wiadomosci/prawo/artykul/jak;bronic;sie;przed;nieuczciwa;konkurencja,51,0,707379.html(3.03.2012).

4) naruszenie tajemnicy przedsiębiorstwa (art. 11) oraz szpiegostwo gospodarcze (art. 23 ust. 2 uznk);
5) nakłanianie do rozwiązania lub niewykonania umowy (art. 12);
6) naśladownictwo produktów (art. 13)
7) pomawianie lub nieuczciwe zachwalanie (art. 14);
8) utrudnianie dostępu do rynku, na przykład poprzez stosowanie cen dumpingowych (art. 15);
9) przekupstwo osoby pełniącej funkcję publiczną (art. 15a);
10) nieuczciwa lub zakazana reklama (art. 16);
11) organizowanie systemu sprzedaży lawinowej (art. 17a),
12) prowadzenie lub organizowanie działalności w systemie konsorcyjnym (17c i 17d).

Celem omawianej ustawy jest zabezpieczenie istnienia konkurencji. Dopiero działanie sprzeczne z prawem lub dobrymi obyczajami jest zabronione, jeżeli zagraża lub narusza interes innego przedsiębiorcy lub klienta. W różnych krajach występują różne formy obrony przed nieuczciwą konkurencją. W naszym kraju występuje również pojęcie dobrych obyczajów.

Czyny nieuczciwej konkurencji powodują wiele różnorodnych skutków oraz konsekwencji społecznych, ekonomicznych i prawnych. Przykładowo, zgodnie z art. 89 ust. 1 pkt 3 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych[39] zamawiający odrzuca ofertę, gdy jej złożenie stanowi czyn nieuczciwej konkurencji w rozumieniu przepisów tej ustawy

Naruszenie tajemnicy przedsiębiorstwa

Mając na względzie analizę informacji dotyczących obrotu gospodarczego, warto upowszechniać tezę, która brzmi: przedsiębiorstwo, które nie stosuje profesjonalnych zasad bezpieczeństwa, wkrótce zanotuje poważne straty. Bezpieczeństwo informacji prawnie chronionych jest podstawowym obowiązkiem związanym z bezpieczeństwem firmy i tajemnicą przedsiębiorstwa..

Regulacja prawna dotycząca naruszenia tajemnicy przedsiębiorstwa została zawarta w art. 11 ust. 4 uznk. Wynika z niej, że przez tajemnicę przedsiębiorstwa należy rozumieć nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności.

Zatem tajemnicę przedsiębiorcy należy traktować jako tajemnicę przedsiębiorstwa. Należy podkreślić, że o uznaniu konkretnej informacji za tajemnicę decyduje zawsze sam przedsiębiorca, podejmując działania w kierunku zachowania ich poufności. Zatem za czyn nieuczciwej konkurencji uznaje się: przekazanie, ujawnienie, wykorzystanie, nabycie od nieuprawnionego cudzych informacji, stanowiących tajemnicę przedsiębiorstwa.

39 Dz. U. 2004 nr 19, poz. 177 z późn. zm..

Definicje tego czynu stosuje się również do osoby, która świadczyła pracę na podstawie stosunku pracy lub innego stosunku prawnego – przez okres 3 lat od jego ustania, chyba, że umowa stanowi inaczej albo ustał stan tajemnicy[40].

Zdarza się, że skrzętnie ukrywane receptury, składniki czy technologie, nowatorskie przedsięwzięcia organizacyjne, a nawet dane obrazujące wielkość produkcji i sprzedaży, źródła zaopatrzenia i konkurencyjnego zbytu – mogą stanowić informacje, które przedostając się do konkurencyjnej firmy, mogą doprowadzić do poważnych perturbacji ekonomicznych, a nawet do upadłości dobrze do prosperującej firmy.

W zasadzie zarządy przedsiębiorstw zwracają istotną uwagę na ochronę zagadnień informacji i tajemnic, stanowiących niematerialne walory, a nawet majątek przedsiębiorstwa. Zazwyczaj są to zarówno techniczne, jak i organizacyjne *know-how*, wypracowane specjalistyczne systemy technologiczne oraz inne informacje poufne. Takie informacje najczęściej stanowią tajemnicę przedsiębiorstwa, która jest prawnie chroniona w myśl art. 11 uznk. Niejednokrotnie przedsiębiorcy wykonują wiele przedsięwzięć w celu ochrony tych danych, lecz nie zawsze skutecznie. Ujawnienie tego typu informacji nawet przez byłego pracownika stanowi czyn nieuczciwej konkurencji.

Zgodnie z art. 11 ust. 2 uznk były pracownik, który w ciągu trzech lat od ustania stosunku pracy dopuści się przekazania, ujawnienia lub wykorzystania informacji stanowiących tajemnicę byłej firmy, jeżeli zagraża to lub narusza jej interes – może być pociągnięty do odpowiedzialności.

Dokładne kwestie powinny być sprecyzowane w ramach umowy konkurencyjnej. Natomiast ujawnienie tajemnicy przedsiębiorstwa nie zostanie zakwalifikowane w ten sposób tylko wtedy, gdy zawarta między pracownikiem a ówczesnym pracodawcą umowa stanowi inaczej albo ustał stan tajemnicy, czyli upłynął czas ochrony lub tajemnice stały się jawne.

Były pracodawca nie będzie jednak miał gwarancji, że były pracownik nie podejmie zatrudnienia w konkurencyjnym przedsiębiorstwie. Jednakże nie upoważnia to do wykorzystywania informacji, które stanowiły tajemnicę byłego pracodawcy. Niezwykle ważne są walory praktyczne tego przepisu. Istotą jest bowiem, aby informacje podlegające ochronie nie mogły być pokazane do wiadomości publicznej. Zatem przedsiębiorca powinien zadbać, jeszcze w trakcie zatrudnienia, aby podejmować właściwe działania zmierzające do zachowania określonych informacji w należytej staranności co do ich poufności. Związane jest to przede wszystkim z poinformowaniem pracowników o poufnym charakterze określonych działań i wiadomości.

Tajemnice przedsiębiorstwa mogą występować w każdym obszarze działalności firmy. Z natury informacji podlegających ochronie jako tajemnica przedsiębiorstwa wynika, że ich lista jest nieograniczona i ma charakter otwarty. Pamię-

40 R. Blichniarz, J. Grabowski, M. Pawełczyk., K. Pokryszka , E. Przeszło, *Publiczne prawo gospodarcze*. Zarys wykładu pod red. J. Grabowskiego, Bydgoszcz-Katowice 2008, s.143.

tać należy, że nowoczesne technologie szeroko udostępniają informacje w systemach teleinformatycznych.

Poniższa, przykładowa lista, może okazać się pomocna przy analizie własnego przedsiębiorstwa pod kątem występowania w nim informacji, które warto objąć prawem tajemnicy przedsiębiorstwa. Przykładowo: w zakresie sprzedaży: lista klientów, informacje dotyczące osób decyzyjnych u klientów, ceny transakcyjne, poufne cenniki, terminy obowiązywania lub odnawiania umów, potrzeby klientów, np. w zakresie asortymentu, oprogramowania, obsługi itp. otrzymane zapytania ofertowe, złożone oferty, fakt prowadzenia negocjacji i ich przebieg.

W zakresie marketingu: prognozy i plany sprzedaży, informacje uzyskane podczas badania konkurencji, informacje uzyskane podczas badania klientów, wartość budżetów reklamowych, plany kampanii marketingowych lub reklamowych, dostawcy, podwykonawcy, pracownicy, informacje o dostawcach i stosowanych cenach, informacja o jakości dostaw lub usług poszczególnych dostawców, terminach realizacji, informacja o stosowanych zakazach konkurencji, informacje o wynagrodzeniach pracowników.

W zakresie kontroli jakości: informacje o wadliwościach poszczególnych produktów, zgłaszanych reklamacjach, dane statystyczne, procedury kontroli jakości. W zakresie produkcji: informacje koszt - cena. Ponadto, chronione powinny lub mogą być przykładowo: dane dotyczące dostawców, stosowane receptury, przepisy, metody produkcji, procedury, pozytywne i negatywne *know-how*; badania i rozwój, a w szczególności: plany i kierunki rozwoju, wynalazki przed zgłoszeniem wniosku patentowego, wyniki badań, wyniki poszukiwań nowych produktów lub usług, pozytywne *know-how* w zakresie badań i rozwoju, negatywne *know-how*, czyli informacje o niepowodzeniach i ślepych uliczkach. W zakresie informacji finansowych: wewnętrzne dokumenty finansowe, budżety, prognozy, raporty, nieujawniane rachunki zysków i strat, obowiązkowe sprawozdania finansowe przed ujawnieniem, wewnętrzne informacje o firmie.

Ponadto, chronione powinny być dane dotyczące sposobu i organizacji pracy, biznes plany oraz oprogramowanie stosowane przez firmę[41].

W praktyce pracodawca dla zastosowania skutecznych działań ochronnych powinien przedstawić każdemu z zatrudnionych na piśmie zakres danych objętych tajemnicą przedsiębiorstwa. Każdy z właściwych pracowników powinien potwierdzić ich otrzymanie. Powyższa procedura zapewnia dochodzenie roszczeń od byłego pracownika, który takie wiadomości ujawnił. Zatem należy:

1) określić chronione dane jako poufne, tuż po ich powstaniu,
2) powiadomić personel, że dane te nie mogą być ujawnione osobom nieupoważnionym,
3) zastosować ochronę fizyczną lub elektroniczną np.: monitoring, dozór fizyczny, kontrola dostępu do pomieszczeń,

41 https://tajemnica-przedsiebiorstwa.pl/tajemnica-przedsiebiorstwa/ (dostęp 22.05.2018).

5) zastosować środki prawne takie jak: wprowadzenie dodatkowych klauzul do umów o pracę, oddzielnych umów o poufności, czy zakazie konkurencji,
6) przedstawić każdemu z zatrudnionych na piśmie zakres danych objętych tajemnicą przedsiębiorstwa. Każdy z właściwych pracowników powinien potwierdzić ich otrzymanie. Taka procedura zapewnia dochodzenie roszczeń od byłego pracownika, o ile takie wiadomości ujawnił.

Interesujące jest w tej kwestii stanowisko Sądu Najwyższego, który orzekł, że jeżeli nawet szef nie zawrze z podwładnym na piśmie zakazu konkurencji po ustaniu stosunku pracy, nie zwalnia to byłego pracownika z obowiązku zachowania w tajemnicy informacji poufnych. Zatem zwolnienie byłych pracowników z zakazu konkurencji po ustaniu stosunku pracy nie jest równoznaczne z godzeniem się przez byłego pracodawcę na ujawnienie informacji stanowiących tajemnice przedsiębiorstwa przez pracowników lub na uczynienie z nich dowolnego użytku, zwłaszcza sprzecznego z interesem pracodawcy[42].

Na tle omawianego zagadnienia istotne jest określenie informacji nieujawnionej. Zatem informacja nieujawniona do wiadomości publicznej to dane, które są nieznane ogółowi lub osobom, które ze względu na wykonywany zawód są zainteresowane jej posiadaniem. Taka informacja mieści się w pojęciu „tajemnicy przedsiębiorstwa", w przypadku gdy przedsiębiorca wyraża (łatwo dostrzegalną) wolę, aby pozostała ona tajemnicą, zwłaszcza dla konkurencji[43].

Tym niezwykle ważnym zagadnieniem również zajął się Sąd Najwyższy, który zgodnie z wyrokiem z 3 października 2000 r., sygn. akt I CKN 304/00 orzekł, że wykorzystanie przez pracownika we własnej działalności gospodarczej informacji, co do których przedsiębiorca (pracodawca) nie podjął niezbędnych działań w celu zachowania ich poufności, należy traktować jako wykorzystanie powszechnej wiedzy, do której przedsiębiorca nie ma żadnych ustawowych uprawnień. Nie każda bowiem informacja (wiadomość) technologiczna i handlowa mieści się w pojęciu „tajemnicy przedsiębiorstwa". Istnieje różnica między wiadomościami odpowiadającymi treści pojęcia „tajemnica przedsiębiorstwa" a informacjami wchodzącymi w skład powszechnej, aczkolwiek specjalistycznej wiedzy zdobytej przez pracownika w wyniku własnej działalności zawodowej podczas zatrudnienia. Zatem tajemnica przedsiębiorstwa jest chroniona z mocy ustawy przez cały okres zatrudnienia oraz w ciągu 3 lat od jego ustania, chyba że umowa stanowi inaczej lub ustał stan tajemnicy. Natomiast wiedza, doświadczenia i umiejętności zdobyte przez pracownika podczas zatrudnienia nie korzystają z ustawowej ochrony na rzecz przedsiębiorstwa, choć – ze względu na zasadę swobody umów - dopuszcza się możliwość zawarcia przez strony (pracodawcę i pracownika) porozumienia zawierającego klauzulę ograniczającą posługiwanie się tą wiedzą w celach konkurencyjnych po ustaniu zatrudnienia.

42 Wyrok SN z 25 stycz¬nia 2007 r. nr I PK 207/06.
43 http://mojafirma.infor.pl/dzialalnosc-gospodarcza/56129,Ochrona-tajemnicy-przedsiebiorstwa.html (2.07.2012)

W podsumowaniu warto sprecyzować, że określona informacja stanowi tajemnicę przedsiębiorstwa, jeżeli spełnia łącznie trzy podstawowe warunki:

1. ma charakter techniczny, technologiczny, organizacyjny przedsiębiorstwa lub posiada wartość gospodarczą,
2. nie została ujawniona do wiadomości publicznej,
3. podjęto w stosunku do niej niezbędne działania w celu zachowania poufności.

Aktualna treść tej regulacji jest zgodna z przepisem art. 39 *Agreement on Trade – Related Aspects of Intellectual Property – TRIPS*, tj. Porozumieniem sporządzonym w Marakeszu w sprawie Handlowych Aspektów Własności Intelektualnej z dnia 15 kwietnia 1994 r. [44]. Oznacza to, że osoby fizyczne i prawne będą miały możliwość zapobiegania, aby informacje pozostające w sposób zgodny z prawem pod ich kontrolą nie zostały ujawnione, nabyte lub użyte bez ich zgody przez innych, w sposób sprzeczny z uczciwymi praktykami handlowymi, jak długo takie informacje:

1. są poufne w tym sensie, że jako całość lub w szczególnym zestawie i zespole ich elementów nie są ogólnie znane lub łatwo dostępne dla osób z kręgów, które normalnie zajmują się tym rodzajem informacji;
2. mają wartość handlową, dlatego że są poufne;
3. poddane zostały przez osobę, pod której legalną kontrolą informacje te pozostają rozsądnym, w danych okolicznościach, działaniem dla utrzymania ich poufności.

Zatem ochronie podlegają wyłącznie informacje pozyskane zgodnie z prawem (tzw. przesłanka legalności). Przesłanka ta nie została jednak wprowadzona do treści art. 11 ust. 4 uznk.

Powszechnie przyjmuje się, że informacja ma charakter technologiczny wówczas, gdy dotyczy najogólniej rozumianych sposobów wytwarzania, formuł chemicznych, wzorów i metod działania. Natomiast informacja handlowa obejmuje, całokształt doświadczeń i wiadomości przydatnych do prowadzenia przedsiębiorstwa, niezwiązanych bezpośrednio z cyklem produkcyjnym.

Informacja nie ujawniona do wiadomości publicznej to informacja nieznana ogółowi lub osobom, które ze względu na prowadzoną działalność są zainteresowane jej posiadaniem. Taka informacja staje się tajemnicą przedsiębiorstwa, kiedy przedsiębiorca chce, by pozostała ona tajemnicą dla pewnych kół odbiorców, konkurentów i jego wola dla innych osób jest oczywista. Bez takiej woli, choćby tylko domniemanej, informacja może być nieznana, ale nie będzie tajemnicą[45].

44 art. 39 Obwieszczenia Ministra Spraw Zagranicznych z dnia 12 lutego 1966 r. w sprawie publikacji załączników do Porozumienia ustanowiającego Światową Organizację Handlu (WTO) (Dz.U. 1996 nr 32, poz. 143 .

45 http://msp.money.pl/wiadomosci/prawo/artykul/tajemnica;przedsiebiorstwa;przy;starcie;w;przetargu,131,0,555651.html (2.07.2012).

Dobro zakładu pracy a tajemnica przedsiębiorstwa

Każdy pracownik ma obowiązek potwierdzenia faktu, że znane są mu przepisy dotyczące obowiązku poufności, a w szczególności art. 100 § 2 ustawy z dnia z dnia 26 czerwca 1974 r. kodeks pracy[46], który stanowi, że pracownik jest obowiązany w szczególności: dbać o dobro zakładu pracy, chronić jego mienie oraz zachować w tajemnicy informacje, których ujawnienie mogłoby narazić pracodawcę na szkodę; przestrzegać tajemnicy określonej w odrębnych przepisach, a także potwierdzić znajomość art. 11 uznk oraz sankcje związane z naruszeniem obowiązku zachowania tajemnicy. Ponieważ skutkiem ujawnienia informacji ma być szkoda, przyjąć należy, że obowiązek zachowania tajemnicy chronić ma informacje istotne z punktu widzenia interesów pracodawców.

Przestrzeganie tajemnicy przedsiębiorstwa ma istotne znaczenie strategiczne w związku z prowadzoną działalnością, a zatem ma charakter ekonomiczny. Podstawowym wskaźnikiem ekonomicznego znaczenia tajemnic handlowych jest częstotliwość naruszania chronionych informacji. Można nawet wnioskować, że liczba ataków na chronione dobro wyznacza w pewnym sensie jego gospodarcze znaczenie. W prowadzonych badaniach przez różne wyspecjalizowane firmy na temat przestępczości gospodarczej, wśród wielu przedsiębiorstw z różnych krajów świata, wykazano, że działania naruszające tajemnicę przedsiębiorstwa, stanowią poważne zagrożenia w stosunku do wszystkich przypadków przestępstw gospodarczych, z którymi stykali się przedsiębiorcy. Najwięcej zanotowano przypadków kradzieży mienia (60%). Jednakże, jak podkreślają autorzy raportu, takie dane są z pewnością konsekwencją faktu, że kradzież mienia jest stosunkowo łatwa do wykrycia, czego nie można na przykład powiedzieć o bezprawnym przywłaszczeniu tajemnic przedsiębiorstwa. Jeżeli jednak przyjrzymy się wysokości szkody, której doznało przedsiębiorstwo w wyniku naruszenia jego tajemnic, pomimo że tylko 7% przedsiębiorców zetknęło się z tym rodzajem naruszenia, wysokość strat wyniosła ponad 4 mln dolarów i była wyższa niż w przypadku np. fałszerstwa produktów, z którym zetknęło się aż 19% przedsiębiorców[47].

Powyższe dane potwierdzają przyjęte założenie o strategicznym znaczeniu pewnych informacji w działalności przedsiębiorstwa. Wyniki analiz naświetlają kilka interesujących faktów związanych z ochroną tajemnic przedsiębiorstwa, a mianowicie:

1) wskazują, że najczęściej przywłaszczane są tajemnice dotyczące procesu produkcyjnego i informacji o nowych rozwiązaniach technologicznych, co oznacza, że centralnym przedmiotem zamachu jest tradycyjnie rozumiane *know-how*, a dopiero w dalszej kolejności inne informacje, posiadające wartość gospodarczą;

46 Dz.U. 1974 nr 24, poz. 141 z późn. zm.

47 A. Michalak, *Ochrona tajemnicy przedsiębiorstwa. Zagadnienia cywilnoprawne*, Warszawa 2006, s. 22.

2) ujawniają bardzo ciekawy aspekt źródeł zagrożenia dla tajemnic przedsiębiorstwa. W tym zakresie przedsiębiorcy za największe zagrożenie dla swoich tajemnic w relacjach wewnętrznych uznają partnerów handlowych w postaci dostawców lub partnerów strategicznych;
3) doprowadzają do uzasadnionej obawy, że ujawnienie tajemnic przedsiębiorstwa następuje przez byłych i obecnych pracowników;
4) podmioty zewnętrzne, to duże zagrożenie powodowane przez konkurentów krajowych i zagranicznych[48];
5) hakerzy komputerowi, których działalność wskazuje na fakt, że rozwój informatyczny, który przyczynił się do zwiększenia roli informacji we współczesnym świecie, stał się jednocześnie zagrożeniem dla posiadanych przez przedsiębiorców tajemnic[49].

Co zatem jest istotne w ramach tajemnic, które może rozpoznać konkurencja. Przykładowo, pracownik może wynieść wiele cennych informacji, jak np.: bazy kontrahentów, informacje o cenach i upustach, którymi są przyciągani klienci, albo nowatorskie projekty czy receptury, nad którymi firma pracowała latami. Firma traci wówczas setki tysięcy a czasami nawet miliony złotych. Takie straty spowodowane wyciekiem informacji wiążą się często z utratą kluczowych klientów, ponieważ konkurencja, znając je, po prostu ich przejmuje, poprzez propozycje lepszych warunków.

W zapobieganiu działania nieuczciwych pracowników mogą pomagać właściwe procedury. Na każde kluczowe stanowiska, które się wyznacza - w zależności od branży – pisze się specjalne procedury zabezpieczeń, które udaremniają wyciek danych. Ścisła współpraca z firmą trwa do miesiąca i w znacznym stopniu eliminuje niebezpieczeństwo kradzieży tajemnic. Jeżeli wspomniana procedura jest weryfikowana (kontrolowana) co trzy miesiące, czyli jest robiony audyt, to można ujawnić zaistniałe nieprawidłowości[50].

Know-how a tajemnica przedsiębiorstwa

Z zagadnieniem tym związany jest *know-how,* termin pochodzący z jęz. angielskiego (*know* – „wiedzieć”, *how* – „jak”) określający konkretną wiedzę techniczną z danej dziedziny, umiejętność wykonania lub wyprodukowania czegoś, kompetencję, biegłość.

Definicja przyjęta przez Międzynarodową Izbę Handlową w Paryżu jako *know-how* określa całokształt wiadomości, czyli fachowej wiedzy oraz doświadczeń w zakresie technologii i procesu produkcyjnego dla określonego wyrobu.

W prawie europejskim definicja know-how zawarta jest w Rozporządzeniu nr 772/2004 z dnia 7 kwietnia 2004 r. w sprawie stosowania art. 81 ust. 3 Traktatu

48 M. Duszczyk, *Polskie firmy na celowniku szpiegów*, „Rzeczpospolita” z 16 października 2014 r. oraz tegoż Polski biznes rajem złodziei, tamże.

49 J.W. Wójcik, *Z problematyki ochrony informacji nie tylko w sytuacjach kryzysowych*, w: R. Częścik i inni: *Zarządzanie kryzysowe w administracj*i, Warszawa, Dęblin 2014, s. 4000-434.

50 G. Zawadka, *Rozmowa z detektywem Alicją Słowińską – Firmy oszczędzają na swoim bezpieczeństwie*, „Rzeczpospolita” z 16 października 2014 r.

do kategorii porozumień o transferze technologii51. Stanowi ona, iż *know-how* to pakiet nieopatentowanych informacji praktycznych, wynikających z doświadczenia i badań, które są:

1) niejawne, czyli nie są powszechnie znane lub łatwo dostępne,
2) istotne, czyli ważne i użyteczne z punktu widzenia wytwarzania produktów objętych umową oraz
3) zidentyfikowane, czyli opisane w wystarczająco zrozumiały sposób, aby można było sprawdzić, czy spełniają kryteria niejawności i istotności.

Na gruncie polskiego prawa cywilnego umowa know-how upoważnia do korzystania z określonych praw podmiotowych. Jedna ze stron (przekazujący, dostawca, udzielający) zobowią-zuje się do przekazania drugiej (zamawiającemu, odbiorcy) wiedzy technicznej lub organizacyjnej o charakterze poufnym lub tajnym, bezpośrednio użytecznej w działalności gospodarczej w zakresie określonym w umowie.

Jako cechy charakterystyczne tej umowy wymienia się, że:

1) przedmiotem umowy jest obrót wiedzą techniczną o poufnym charakterze,
2) dotyczy jedynie dóbr niematerialnych,
3) nie przenosi praw majątkowych,
4) w prawie polskim jest to umowa nienazwana – możliwość jej zawarcia wynika z zasady swobody umów według art. 353 k.c., jest umową odpłatną, wzajemną, dwustronnie zobowiązującą.

Dobrami chronionymi umową *know-how* mogą być np.: nieopatentowane wynalazki, niezarejestrowane wzory użytkowe, informacje techniczne dotyczące stosowania patentów lub wzorów użytkowych, doświadczenie administracyjne i organizacyjne związane z własnością przemysłową.

W związku z tym umowa ta może stanowić uzupełnienie ochrony przewidzianej prawem na dobrach niematerialnych (własność przemysłowa: patenty, wzory użytkowe, także takie, które nie posiadają zdolności patentowej)[52].

Zatem nazwa *know-how* oznacza poufną, odpowiednio ustaloną wiedzę lub doświadczenie o charakterze technicznym, handlowym, administracyjnym, finansowym lub innego rodzaju, które nadają się do stosowania w działalności danego przedsiębiorstwa albo do wykonywania określonego zawodu.

Szpiegostwo gospodarcze, czyli gra wywiadów

Powszechnie wiadomo, że nawet najlepsze systemy prawne nie przynoszą oczekiwanych rezultatów. Podobnie jest z prawną ochroną informacji. Bez względu na kraj czy narodowość, system gospodarczy i stan prawny daje się zaobserwować olbrzymie zainteresowanie informacją, a szczególnie informacją o charakterze przemysłowym. Zawsze była i jest ona związana ze szpiegostwem

51 Dz. U. UE L 123 z 27 kwietnia 2004, s. 11.
52 http://pl.wikipedia.org/wiki/Know-how (22.06.2012).

gospodarczym, określanym również innymi terminami, a przykładowo: jako wywiad technologiczny czy wywiad przemysłowy. Specjalne zainteresowania kierowane są w ramach działów określanych jako wywiad militarny czy polityczny, a także z innymi dziedzinami życia społecznego, z których warto wyróżnić ochronę danych osobowych.

Szpiegostwo gospodarcze ma bardzo długą historię. Często przyczyniało się do rozprzestrzeniania postępu cywilizacyjnego. Przykładem w tej kwestii może być informacja, że już w drugim tysiącleciu przed Chrystusem egipscy agenci starali się wykraść od Hetytów tajemnicę technologii produkcji żelaza, a w XVIII w. Europejczycy wykradali w Chinach sekrety produkcji porcelany. W XIX wieku fascynowano się wynikami wywiadu brytyjskiego. Obecnie analizujemy sukcesy wywiadu rosyjskiego i chińskiego. Ataki rosyjskich hakerów są powszechnie znane. Natomiast Chińczycy wykazują się wielką pomysłowością przy wykradaniu informacji. Przykładowo, brytyjska Służba Bezpieczeństwa MJ5 (ang. Security Service) ostrzegał biznesmenów m.in. przed przyjmowaniem pendrive'ów z danymi od chińskich przedsiębiorców, gdyż mogą zawierać *trojany*, które ułatwiają włamania do systemu informatycznego. Jednakże według 900 stronicowego raportu komisji Chrisa Coxa jako specjalnej komisji Kongresu USA Chiny bez przeszkód przez 20 lat zdobywały informacje o kluczowych tajemnicach militarnych[53].

Po podstępne metody sięgają również kraje, które głośno narzekają na to, jak obcy hakerzy naruszają ich proces demokratyzacji. Przykładem może być znany dość powszechnie fakt, iż np. w amerykańskim departamencie handlu istnieje mała ale bardzo ważna, komórka o nazwie Biuro Współpracy Wywiadu. Przekazuje ona dane pochodzące od organizacji wywiadowczych do zamawiających je firm amerykańskich.

Od połowy marca 2018 r. głośno jest o aferze Cambridge Analytica, która zakupiła dane użytkowników Facebooka. Podobno dane te pod pretekstem naukowego eksperymentu wydobył naukowiec Aleksandr Kogan. Dane te rzekomo zostały użyte do tworzenia profili psychologicznych potencjalnych wyborców. Skorzystał z nich sztab wyborczy Donalda Trumpa. Ponadto firma Cambridge Analytica była zaangażowana w wiele innych kampanii wyborczych na całym świecie. Niektóre z nich miały krwawy przebieg, a szczególnie w Kenii w latach 2013 i 2017.

Wprawdzie kilka dni po ujawnieniu transakcji z wyciekiem danych z Facebooka jego szef Mark Zuckerberg przemówił publicznie i przyznał się do błędów, ale ostrzegł też że społeczność złożona z dwóch miliardów ludzi nigdy nie będzie w pełni bezpieczna.

Sprawa wyszła na jaw w marcu 2018 r. gdy szczegółowo opowiedział o niej jeden z byłych pracowników Cambridge Analytica. Wspominał o 50 mln osób, na których danych w ten sposób urządzono „żniwa". Natomiast sam Zuckerberg

53 Metodę określono jako: z miliardów ziarenek piasku zebranego w USA, można ułożyć plażę w Chinach.

przyznał, że było ich jeszcze więcej – aż 87 mln.[54]. W rezultacie, jak twierdzą niektórzy publicyści, skutki takich zdarzeń to: Trump jest dziś prezydentem, a Cambridge Analytica synonimem manipulowania wyborcami. Natomiast Zuckerberg pomimo, że wziął na siebie całą odpowiedzialność za aferę, stał się tarczą strzelniczą dla całego świata. Nic dziwnego, że Parlament Europejski i władze wielu państw zażądały wyjaśnień. Natomiast akcje Facebooka spadły o 30 proc.

Wszelkie rekordy bije jednak podjęta jeszcze w ubiegłym wieku przez media szeroka akcja informacyjna o działalności amerykańskiej Agencji Bezpieczeństwa Narodowego (*National Security Agency – NSA*) i o prowadzonym przez nią ośrodku Echelon, zajmującym się totalnym podsłuchiwaniem. Działania tego typu prowadzone są za pomocą sieci około 120 satelitów szpiegowskich. Podsłuchiwane są wszelkiego rodzaju elektroniczne środki masowej komunikacji, tj. od rozmów telefonicznych, przez faksy, pagery, pocztę e-mail, sieć Internetu, łączność satelitarną i światłowodową, a kończąc na specjalnych połączeniach przy pomocy bardzo zaawansowanej technologii.

Sama idea szpiegowania na masową skalę pochodzi jeszcze z czasów II wojny światowej, a rozwinięto ją w latach 60. wraz z rozwojem Echelonu, tj. systemu globalnej sieci wywiadu elektronicznego, który powstał z inicjatywy USA, by wspólnie z sojusznikami, na masową skalę gromadzić i analizować rozmowy telefoniczne, faksy, e-maile i transfery plików[55]. Pierwsze informacje na ten temat pojawiły się już w 1988 r., a później temat wracał wraz z kolejnymi skandalami. Echelon miał być wykorzystany m.in. do podsłuchiwania ważnych osobistości jak np. księżnej Diany czy sekretarza generalnego ONZ. Prawdopodobnie dzięki informacjom zdobytym za pomocą tego systemu ujawniono korupcję podczas przetargu na samoloty dla Arabii Saudyjskiej, w efekcie czego kontrakt stracił europejski Airbus. W marcu 2000 r. James Woolsey Jr, już wtedy były dyrektor CIA, ironizował broniąc się przed zarzutami szpiegowania Europejczyków. Napisał wówczas w „The Wall Street Journal": „My musimy was kontrolować, bo bierzecie łapówki".

54 Według potwierdzonej informacji biura prasowego Facebooka wyciek danych może dotyczyć 57 tys. osób w Polsce.

55 Echelon to globalna sieć wywiadu elektronicznego. System powstał przy udziale Stanów Zjednoczonych, Wielkiej Brytanii, Kanady, Australii i Nowej Zelandii i jest zarządzany przez amerykańską służbę wywiadu NSA. Później dołą¬czyły inne państwa, głównie europejskie. Echelon posiada w całym świecie urządzenia techniczne do przechwytywania (podsłuch) wiadomości w kanałach telekomunikacji. System gromadzi ianalizuje transmisje fal elektromagnetycznych przez urządzenia elektroniczne z całego świata – urządzenia telekomunikacyjne, IT, faksy, e-maile, transfery plików, rozmowy telefoniczne, komputery, radary, satelitów rozpoznawczych, s. telekomunikacyjnych itp. System gromadzi i przetwarza miliardy przekazów elektronicznych na dobę. Jest to tylko niewielki ułamek całej komunikacji elektronicznej, gdyż jedynie w USA wykonuje się prawie 4 mld samych tylko rozmów telefonicznych na dobę. Zebrane lokalnie informacje z całego świata przesyłane są do centrali w Fort Meade, gdzie znajduje się główna siedziba NSA. Superkomputery dokonują analizy materiału, dostosowanej do regionu, tworzą słownik haseł, stanu materiału i algorytm szyfrowania. System Echelon był m.in. prawdopodobnie bezpośrednim źródłem informacji o korupcji przy wartym 6 miliardów dolarów przetargu na samoloty dla Arabii Saudyjskiej. W efekcie tej informacji NSA przetarg stracił europejski Airbus. http://pl.wikipedia.org/wiki/Echelon (12.03.2018).

Rola RODO w ochronie danych osobowych

Kolejny akt unijny ma na celu umocnienie bezpieczeństwa osób fizycznych. W dniu 27 kwietnia 2016 r. przyjęto Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 93/46/WE (ogolne rozporządzenie o ochronie danych[56] RODO, które weszło w życie 25 maja 2018 r. Nawiązuje doń ustawa z dnia 10 maja 2018 r. o ochroniee danych osobowych[57]. Istnieje przekonanie, że to rewolucja w zakresie ochrony danych osobowych.

Dane sensytywne czy, jak określane są w RODO „szczególne kategorie danych osobowych" to takie, które ujawniają specyficzne, prywatne informacje o nas; informacje którymi nie dzielimy się z przypadkowymi ludźmi. Należą do nich m.in. nasze pochodzenie rasowe i etniczne, przekonania religijne czy światopoglądowe, przynależność do związków zawodowych czy partii, poglądy polityczne, stan zdrowia, kod genetyczny, dane biometryczne czy te o naszej seksualności lub orientacji seksualnej. Nowa regulacja ma na celu zapewnienie swobodnego przepływu danych osobowych pomiędzy państwami członkowskimi, ale także wprowadzenie zasad, zgodnie z którymi przetwarzanie danych osobowych będzie ujednolicone na terenie całej Unii Europejskiej. Nowe zasady prawne dotyczą wszystkich firm, które gromadzą i wykorzystują dane dotyczące obywateli europejskich. Istnieje zatem prawny obowiązek przestrzegania zasad RODO.

Zakończenie

Praktyka dowodzi, że nawet najlepsza chroniona informacji i tajemnic nie dają gwaranccji ich bezpieczeństwa. Systemy prawne z zasady rozbudowują ochronę informacji i tajemnic zawodowych. Natomiast praktycy zarówno z dziedziny wywiadu gospodarczego, jak i szpiegostwa gospodarczego wszelkimi sposobami rozwijają systemy przeznaczone do zdobywania chronionych informacji.

Wśród wielu powodów wyróżnia się postęp technologiczny i dążność do zawładnięcia nowymi technologiami. Jednakże wśród wielu specjalistów, także ludzi nauki, uwidacznia się różnorodność poglądów na tle obecnych możliwości technicznych i metod badawczych. Jedni twierdzą, że jest to bardzo proste zagadnienie, inni zakładają, że jest ono niezwykle złożone.

Jerzy Wojciech Wójcik*

56 Dz. U. VEL 119/1 z 4 maja 2016 r.
57 Dz. U. 2018, poz. 1000.

***prof. dr hab. Jerzy Wojciech Wójcik, Wszechnica Polska Szkoła Wyższa w Warszawie**

Agnieszka Latosińska

Wywiad gospodarczy a bezpieczeństwo ekonomiczne państwa

Wprowadzenie

Zdobywanie informacji niejawnych zawsze miało znaczenie dla funkcjonowania państwa. Ten, kto wiedział więcej, miał przewagę nad konkurentem czy rywalem, zarówno na płaszczyźnie ekonomicznej, jak i w sferze bezpieczeństwa polityczno-militarnego. Niewielkie grupy osób, zaangażowanych w zdobywanie poufnych informacji o kluczowym znaczeniu dla państwa, z czasem urosły do rangi potężnych organizacji wywiadowczych, zatrudniających tysiące osób: agentów i informatorów, analityków i funkcjonariuszy operacyjnych, będących w posiadaniu najnowocześniejszego sprzętu, mających do dyspozycji wszystkie zdobycze technologiczne.

W ramach wywiadu państwowego istniał i nadal z powodzeniem funkcjonuje wywiad gospodarczy. Niejednokrotnie prowadzony jest przez byłych funkcjonariuszy wywiadu lub kontrwywiadu, często na zlecenie nie państwa, a przedsiębiorstw zainteresowanych dostępem do informacji na temat konkurentów biznesowych.

1. Pojęcie i istota wywiadu

Pojęcie wywiadu ma trzy znaczenia: w pierwszym jest to instytucja państwa, której zasadniczym celem jest uzyskanie dostępu do tajnych informacji dotyczących wojska, polityki i gospodarki innych państw. W drugim znaczeniu jest to sposób badań socjologicznych i psychologicznych, które polegają na zebraniu określonych informacji i badaniu opinii publicznej. Natomiast w znaczeniu trzecim wywiad jest postrzegany jako proces, którego integralnymi częściami są: planowanie działań wywiadowczych, gromadzenie, przetwarzanie, analiza i dystrybucja informacji wywiadowczych[1].

Można dokonać podziału wywiadu, w zależności od obszaru jego zainteresowania:

1) wywiad wszechstronny – nieustająco i w kompleksowy sposób monitorujący sytuację;
2) wywiad ukierunkowany – na jasno zdefiniowany cel do osiągnięcia[2].

1 http://centrum.vismagna.pl/index.php?site=wg&vm1=podstawy&vm2=piwg (dostęp: 21.05.2017).
2 http://wywiadgospodarczy.pl/pl-PL/article/artykuly/article/wywiad_gospodarczy/wywiad_gospodarczy_%E2%80%93_proba_definicji (dostęp: 21.05.2017).

Jeśli podziału dokonujemy w oparciu o sposoby uzyskiwania informacji, to wówczas wywiad można podzielić na:

1) wywiad biały – jest to legalny sposób pozyskiwania danych, w oparciu o ogólnodostępne źródła. Źródłami białego wywiadu są media, internet, rejestry państwowe (Krajowy Rejestr Sądowy czy Księgi Wieczyste), wszelkiego rodzaju źródła informacji politycznych (Instytut Pamięci Narodowej czy Archiwa Sejmu i Senatu RP);
2) wywiad czarny – wzbudzający największe kontrowersje, ponieważ jego głównym celem jest pozyskanie informacji tajnych, bez względu na środki do tego celu służące, często z ominięciem obowiązującego prawa;
3) wywiad szary – wykorzystuje zarówno legalne źródła informacji, jak i te zdobyte w nie do końca legalny sposób[3].

Wywiad gospodarczy jest to proces gromadzenia, przetwarzania, analizowania i dystrybucji informacji wywiadowczych w przedsiębiorstwie, prowadzony legalnymi metodami i środkami, którego celem jest (...) zdobycie, utrzymanie bądź powiększenie przewagi konkurencyjnej[4]. Wywiad gospodarczy można określić po prostu jako pozyskiwanie informacji gospodarczych albo takich, które mają znaczenie dla gospodarki.

Przedmiotem zainteresowań wywiadu gospodarczego są przede wszystkim:

- wszystkie dane dotyczące działalności konkurentów,
- rachunki bankowe,
- klienci, partnerzy i rodzaje zawieranych transakcji,
- wyniki badań technologicznych, wynalazki, itp.,
- prognozy i plany rozwoju[5].

Trudności gospodarcze w państwie sprzyjają wręcz rozwojowi wywiadu w korporacjach transnarodowych. Odsetek przedsiębiorstw międzynarodowych, korzystających z wywiadu gospodarczego w walce konkurencyjnej wzrósł z 63% w 2009 roku do 76% w 2011 roku. Okazało się również, że 35% przedsiębiorstw, które nie posiadały komórek wywiadowczych, zadeklarowało chęć ich stworzenia w przeciągu roku. Z kolei 93% badanych firm przyznało się do czerpania korzyści z wywiadu gospodarczego, natomiast aż 78% ujawniło, iż wkład włożony w wywiad gospodarczy przynosi korzyści.

Najwięcej, bo aż 85% przedsiębiorstw prowadzących zorganizowany wywiad, pochodzi z regionu Rosji i WNP, a tuż za nimi umiejscawia się przedsiębiorstwa z Ameryki Północnej (84%)[6].

3 http://rynekinformacji.pl/techniki-wywiadowcze-bialy-czarny-szary-wywiad-detektyw-zdobywa-informacje/ (dostęp: 21.05.2017).

4 http://centrum.vismagna.pl/index.php?site=wg&vm1=podstawy&vm2=piwg (dostęp: 21.05.2017)

5 R.Borowiecki, M.Kwieciński (red.), *Informacja w zarządzaniu przedsiębiorstwem. Pozyskiwanie, wykorzystanie i ochrona (Wybrane problemy teorii i praktyki),* Zakamycze 2003, s. 380-381

6 M.Ciecierski, *Wywiad ma się lepiej...,* [w:] http://www.wywiad-gospodarczy.pl/wywiad-ma-sie-lepiej.html.

Wywiad gospodarczy w Federacji Rosyjskiej, a także na terenach państw WNP nadal zakotwiczony jest w zasobach wywiadów wojskowego i cywilnego, mających kiedyś ogromny wpływ na życie polityczne, gospodarcze i społeczne w byłym ZSRR. Natomiast w korporacjach amerykańskich i kanadyjskich istotną rolę spełnia kultura informacyjna korporacji, od której zależy sposób zdobywania potrzebnych informacji. Z kolei w Północnej Europie 81% korporacji wykorzystuje do swoich celów wywiad gospodarczy, a najgorzej rozwinięty wywiad posiadają przedsiębiorstwa działające na terenach Afryki i Bliskiego Wschodu, bo tylko 50% z nich korzysta z informacji wywiadu gospodarczego[7].

Najwięcej środków na prowadzenie działalności wywiadowczej przeznaczono w Ameryce Północnej oraz w Zachodniej Europie, natomiast najmniej wydano w Federacji Rosyjskiej i krajach WNP, a także w Europie Środkowo-Wschodniej. Najwięcej wydano w sektorach samochodowym, farmaceutycznym i medycznym oraz sprzedaży detalicznej. Najmniej w usługach, logistyce i transporcie, energetyce, przemyśle wydobywczym[8]. Obecnie w dużych korporacjach uważa się, że znaczenie wywiadu będzie ciągle rosło, a to w związku z rosnącą dynamiką i globalizacją rynku. Zapotrzebowanie na wysoko kwalifikowaną i przetworzoną informację we wszystkich obszarach działalności przedsiębiorstwa będzie systematycznie rosło. Widać będzie również zwiększone zapotrzebowanie na wykorzystania nowych narzędzi IT, służących do przetwarzania i obiegu informacji. Pojawić się mają także nowe, wymyślne techniki informatyczne, do wykorzystania w służbie wywiadu[9].

2. Historia wywiadu

Wywiad gospodarczy prowadzony był od wielu wieków. Niektórzy badacze twierdzą, że najwcześniejszą informację na temat wywiadu gospodarczego można odnaleźć w greckiej mitologii, gdzie agent wywiadu gospodarczego, Prometeusz, ukradł bogom niedostępną zwykłym śmiertelnikom technologię, czyli ogień[10]. Jako drugi przykład może posłużyć kradzież Chińczykom tajemnicy produkcji jedwabiu, z polecenia cesarza Justyniana I[11]. Na rozkaz cesarza dwóch mnichów przemyciło w wydrążonych laskach gąsienice jedwabników, likwidując tym sposobem chiński monopol na produkcję jedwabiu[12]. Z kolei w Republice Weneckiej[13] rolę agentów wywiadu pełniły prostytutki, pozyskując dane wrażli-

7 Ibidem.

8 Ibidem.

9 M.Ciecierski, *Wywiad ma się lepiej...,* [w:] http://www.wywiad-gospodarczy.pl/wywiad-ma-sie-lepiej.html.

10 M.Karpiński, *Historia szpiegostwa,* Warszawa 2003, s. 11.

11 Justynian I Wielki (483-565) – cesarz bizantyjski od 1 sierpnia 527 do 13 listopada 565, święty Kościoła prawosławnego. Za jego czasów Cesarstwo Bizantyjskie osiągnęło największą świetność w swych dziejach.

12 M.Minkina, *Sztuka wywiadu w państwie współczesnym,* Bellona /Oficyna Wydawnicza RYTM, Warszawa 2014, s. 153.

13 Republika Wenecka – północnowłoska republika kupiecka, istniejąca od VIII wieku aż do

we od podróżnych, swoich klientów[14]. Jednym z najznamienitszych dzieł o sztuce wywiadowczej jest *Sztuka Wojny* Sun Tzu[15]: *Szpiegów dzieli się na: lokalnych, wewnętrznych, nawróconych, czyli podwójnych agentów, martwych, czyli spisanych na straty, oraz żywych. Jeżeli wszystkie te grupy współpracują ze sobą (…) dla władcy jest to istny skarb*[16].

Wojnę o porcelanę określa się jako jedną z największych wojen wywiadów gospodarczych. W 1712 roku o. François Xavier d'Entrecolles, francuski jezuita, wykradł Chińczykom sekrety produkcji porcelany. Udało mu się przesłać do Francji próbki kaolinu, surowca potrzebnego do jej produkcji. Wówczas nikt nie pomyślał nawet, że kilkaset lat później jego wyczyn będzie klasycznym przykładem szpiegostwa gospodarczego[17].

Pierwszym przedsiębiorcą wywiadu gospodarczego na skalę światową, handlującym informacjami na sprzedaż był, Lewis Tappan, założyciel firmy The Mercantile Agency w roku 1841. Głównym celem firmy była ocena zdolności kupców do regulowania ich zobowiązań finansowych. Również w 1841 roku niejaki Robert Dun założył podobną agencję. W 1859 roku zmienił nazwę firmy na R.G.Dun & Comapny, publikując jednocześnie książkę z ocenami ratingowymi. W 1933 roku dokonano fuzji obu firm. Nowa agencja została nazwana Dun & Bradstreet i uznawana jest za jedną z czołowych wywiadowni na świecie[18].

W pierwszej połowie dwudziestego wieku, z powodu mnogości konfliktów zbrojnych, jakie wówczas miały miejsce, państwowe służby specjalne różnych krajów zdominowały zarówno wywiad, jak i szpiegostwo gospodarcze. Druga połowa dwudziestego wieku przyniosła niesamowity postęp informacyjny. Wzrosło też zapotrzebowanie na różnego rodzaju informacje i dane technologiczne, co było powodem systematycznego udoskonalania metod zdobywania informacji tajnych. Przykładowo w połowie lat siedemdziesiątych w USA, w zakładach Coca Cola w Atlancie został upubliczniony przypadek zainstalowania fotokopiarki w niszczarce do dokumentów. Każdy skrawek papieru był oczywiście kopiowany przed zniszczeniem[19]. W ten sposób można było wejść w posiadanie każdej tajnej informacji, rzecz jasna ze szkodą dla firmy Coca Cola.

1797 roku. Najdłużej nieprzerwanie funkcjonujące państwo o ustroju republikańskim w historii. W średniowieczu jedna z największych potęg handlowych i politycznych w basenie Morza Śródziemnego i jedno z najbogatszych miast Europy.

14 M. Minkina, *op.cit.,* s. 163.

15 Sun Tzu (544 p.n.e.-469 p.n.e.) – chiński generał, uważany za jednego z największych myślicieli Wschodu, autor traktatu *Sztuka Wojny*, zbioru zaleceń i rad dla każdego, kto dowodzi ludźmi, stawia czoła wyzwaniom i walczy o pozycję dla siebie i swoich podwładnych.

16 Sun Tzu, *Sztuka Wojny,* Gliwice 2013, s. 92.

17 L.Korzeniowski, A.Pepłoński, *Wywiad gospodarczy, historia i współczesność,* Kraków 2005, s. 19. Por. L.Bajer, *Wywiad gospodarczy, wszystko o...,* Warszawa 1979, s. 12

18 http://www.wywiadgospodarczy.pl/pl-PL/article/artykuly/article/wywiad_gospodarczy/historia_wywiadu_gospodarczego_w_pigulce (dostęp: 22.05.2017).

19 Ibidem.

Przełom wieku XX i XXI, w tym transformacja ustrojowa w licznych krajach świata spowodowały daleko idące zmiany, istotne zarówno dla służb specjalnych państw, jak i dla wywiadu gospodarczego. Powstało szereg korporacji transnarodowych, które w znaczący sposób wpływają na gospodarkę wielu państw, można nawet powiedzieć – na gospodarkę światową. Oczywiście nie wyeliminowało to przypadków szpiegostwa gospodarczego. W latach dziewięćdziesiątych było kilka takich głośnych przypadków: w Niemczech przyłapano na szpiegostwie przemysłowym pochodzącego z Hiszpanii, byłego menadżera zakładów Opla i Volkswagena, z Francji wydalono dyplomatów amerykańskich, pod zarzutem szpiegostwa gospodarczego, w Korei Południowej za szpiegostwo gospodarczo-militarne zostały skazane cztery osoby: trzech Koreańczyków i Amerykanin, który był przedstawicielem firmy handlującej bronią[20].

W Krakowie na przełomie lat dziewięćdziesiątych i nowego milenium działała firma Classic Diamond, prowadzona przez pułkownika Specnazu i FSB, z siedzibą tuż obok klubu garnizonowego. Oficjalnie zajmowała się handlem diamentami, nieoficjalnie starała się uzyskać dostęp do danych technologicznych i wynalazków krakowskiej AGH. Niestety, po ukazaniu się artykułu na temat Classic Diamond polskie służby nie podjęły natychmiastowych działań, co pozwoliło firmie i zatrudnionym w niej ludziom na ucieczkę[21].

3. Szpiegostwo przemysłowe

Szpiegostwo przemysłowe są to działania wywiadowcze podejmowane w celach komercyjnych, co różni je od działań wywiadowczych prowadzonych przez państwa, te są bowiem prowadzone dla zabezpieczenia ich narodowych interesów. Kilka lat temu wybuchła wielka afera po tym, jak szwajcarskie władze oskarżyły byłego analityka działu IT (technologii informacyjnych) genewskiego oddziału bankowości prywatnej HSBC, Hervé Falciani, o szpiegostwo przemysłowe i udostępnianie tajnych informacji władzom innych państw. Prokuratura uważa, że złamał państwowe prawo dotyczące tajemnic informacyjnych. Falciani przekazał władzom Francji i Hiszpanii dane na temat tysięcy kont bankowych. Sam analityk tłumaczył się , że jego celem była realna pomoc Paryżowi i Madrytowi w ściganiu tych obywateli, którzy nie płacili podatków. Szwajcarska prokuratura dowodziła jednak, że były analityk czerpał zyski z prowadzonej przez siebie działalności. Oskarżył go też o chęć sprzedaży tajnych informacji bankom z Libanu. Nieuczciwe praktyki, które podejmował Falciani wyszły na jaw, kiedy w dniu 26 grudnia 2008 roku podał francuskim władzom podatkowym kilkadziesiąt gigabajtów tajnych informacji z danymi francuskich klientów HSBC z lat 2005-2006[22].

20 M.Taradejna, R.Taradejna, *Dostęp do informacji publicznej, a prawna ochrona informacji dotyczących działalności gospodarczej, społecznej i zawodowej oraz życia prywatnego,* Toruń 2003, s. 282-293

21 http://forum.echodnia.eu/polskie-sluzby-sa-zagrozeniem-dla-panstwa-sluzby-wojskowe-spenetrowane-przez-rosjan-t182980/ (dostęp: 22.05.2017)

22 http://www.forbes.pl/szwajcaria-oskarza-analityka-ktory-przekazal-dane-bankowe-

W wielu przypadkach kradzieże danych technologicznych są przeprowadzane przez szpiegów na usługach chińskiego rządu. W 2012 roku Amerykanie oskarżyli agentów chińskich firm o wykradzenie receptury produkcji białego barwnika firmy DuPont. Firma ta ma kontrolę 70 % rynku farb stosowanych do barwienia różnego rodzaju produktów – lodówek, iPodów, czy nawet papieru. Po latach wysiłków włożonych w zdobycie informacji, koncern z Syczuanu nielegalnie wszedł w jej posiadanie. Firma DuPont już wcześniej miała problemy ze szpiegowaniem tajemnic firmy. Michael Mitchell, pracownik, który został zwolniony z pracy z działu sprzedaży syntetycznych włókien kevlar, zaproponował sprzedaż posiadanych przez siebie informacji koreańskiemu koncernowi Kolon Industries Inc. Zdemaskowany w trakcie przekazywania nowemu pracodawcy – pocztą elektroniczną - tajnych informacji na temat produkcji kevlaru został aresztowany przez FBI i skazany na półtora roku więzienia oraz grzywnę w wysokości 180 tysięcy dolarów[23].

W chwili obecnej znacznie skuteczniejsze od szpiegów są specjalne programy komputerowe, określane przez znawców branży jako Zaawansowane Ustawiczne Zagrożenie, czyli APT (od *Advanced Persistent Threat*). Odkryty kilka lat temu w Peru wirus ACAD/Medre wykradał rysunki inżynierów i architektów zrobione w programie AutoCAD i dostarczał je pod określone adresy poczty elektronicznej, znajdujące się na chińskim serwerze[24]. Utrata ważnych informacji technologicznych może zachwiać bezpieczeństwem ekonomicznym państwa zwłaszcza, jeśli dotyczy wielkich koncernów, mających znaczące wpływy do budżetu państwa.

Biorąc pod uwagę geopolitykę polską, przyjęto założenie, że naszym państwem w szczególny sposób są zainteresowane wywiady służb specjalnych Federacji Rosyjskiej, Białorusi, Ukrainy oraz Chin i Indii. Najprawdopodobniej służby wywiadowcze naszych wschodnich sąsiadów są zainteresowane głównie kierunkami naszej polityki zagranicznej i polityką bezpieczeństwa, a także naszą gospodarką i infrastrukturą. Z kolei uwaga wywiadu państw azjatyckich może skupiać się wokół technologii, inwestycji i rynków zbytu[25]. Jako członek NATO i UE, Polska również może stać się obiektem zainteresowania obcych służb wywiadowczych. Z końcem kwietnia 2009 roku NATO wycofało akredytację dla dwóch rosyjskich dyplomatów, za prowadzenie działalności wywiadowczej. Pikanterii sprawie dodaje fakt, że jeden z wydalonych Rosjan był synem dyplomaty, będącego przedstawicielem FR przy Unii Europejski[26].

Jedną z największych afer związanych ze szpiegostwem przemysłowym ostatnich kilku lat jest sprawa zabójstwa w hotelu w mieście Chongqing w Chi-

francji,artykuly,187160,1,1.html (dostęp:23.05.2017)

23 http://www.newsweek.pl/biznes/wiadomosci-biznesowe/wywiad-gospodarczy--szpiedzy-na-miare-xxi-wieku,98099,1,1.html (dostęp: 23.05.2017)

24 Ibidem

25 M.Minkina, *op.cit.,* s. 313

26 Ibidem, s. 317

nach[27] pewnego brytyjskiego biznesmena, Neila Heywooda. Jego śmierć miała polityczne konsekwencje, ponieważ to doprowadziło do wybuchu afery, której konsekwencją było odsunięcie od władzy i upadek Bo Xilaia – sekretarza partii w Chongqing, silnego kandydata na nowego lidera chińskich komunistów.

W sierpniu 2012 roku winną zbrodni w hotelu w Chongqing uznana została żona sekretarza, Gu Kailai28. Skazano ją na karę śmierci w zawieszeniu, która w Chinach zazwyczaj jest zamieniana po dwóch latach na karę dożywocia29, wyszła bowiem na jaw korupcja na ogromną skalę, w którą zamieszany był sekretarz i jego małżonka. Chcieli oni wywieźć z Chin wielomiliardowe sumy pieniędzy. Niedawno okazało się, że sprawa zabójstwa Heywooda może mieć inny powód. Neil Heywood rzekomo współpracował z brytyjskim wywiadem MI6, przekazując różnorakie informacje, także na temat życia osobistego Bo Xilai[30], co miało przyczynić się do jego śmierci. Poza tym Heywood współpracował z jedną z dużych firm konsultingowych, która pomagała wielkim korporacjom w zdobywaniu cennych informacji. Zdaniem brytyjskich mediów był on osobowym źródłem informacji, dostarczał wiadomości na temat powiązań biznesu z polityką oraz o chińskich korporacjach, a jest to właśnie ten obszar, w którym dochodzi do najbardziej zaciętej rywalizacji pomiędzy współczesnymi agencjami wywiadowczymi świata[31].

4. Bezpieczeństwo ekonomiczne państwa

Nie ulega wątpliwości fakt, że bezpieczeństwo ekonomiczne państwa w znacznej mierze zależy od jakości i skuteczności własnych służb kontrwywiadowczych, choć nie jest to oczywiście warunek *sine qua non*. Definicje bezpieczeństwa ekonomicznego można podzielić na cztery grupy:

1) opierające się na zagrożeniu;

2) łączące zagrożenia i możliwości;

3) odwołujące się do zdolności państwa do funkcjonowania;

4) definicje jednostronne[32].

Według Krzysztofa Michała Księżopolskiego *bezpieczeństwo ekonomiczne to niezakłócone funkcjonowanie gospodarek, to znaczy utrzymanie podstawowych wskaźników rozwojowych oraz zapewnienie komparatywnej równowagi z go-*

27 Chongqing – jedno z czterech miast wydzielonych Chińskiej Republiki Ludowej. Powstało po wydzieleniu z terytorium prowincji Syczuan w 1997 roku.

28 http://www.theepochtimes.com/n3/1482874-british-businessman-neil-heywood-divulged-too-much/full/ (dostęp: 27.05.2017).

29 http://www.newsweek.pl/biznes/wiadomosci-biznesowe/wywiad-gospodarczy--szpiedzy-na-miare-xxi-wieku,98099,1,1.html (dostęp: 27.05.2017) Por. E.Javers, *Agent. Handlarz. Prawnik. Szpieg. Tajemniczy świat korporacyjnego szpiegostwa,* Kraków 2010.

30 Ibidem.

31 Ibidem.

32 K. M. Księżopolski, *Bezpieczeństwo ekonomiczne*, Warszawa 2011, s. 18-19.

spodarkami innych państw[33]. Podobną definicję przedstawił Paweł Dziekański: *Bezpieczeństwo ekonomiczne jest pojęciem bardzo szerokim. Jest to to taki stan rzeczywistości, w którym możliwy jest harmonijny rozwój gospodarki oraz zapewnienie odpowiedniego poziomu życia obywateli poprzez niezakłócony dostęp do surowców, rynków zbytu, kapitału, nowoczesnych technologii czy informacji (…) Bezpieczeństwo ekonomiczne jest to zdolność systemu gospodarczego państwa (grupy państw) do takiego wykorzystania wewnętrznych czynników rozwoju i międzynarodowej współzależności ekonomicznej, które będą gwarantowały jego nie zagrożony rozwój*[34].

Z treści pojęć takich, jak bezpieczeństwo państwa i bezpieczeństwo ekonomiczne można wyprowadzić definicje zagrożenia gospodarczego. Można przy tym zauważyć dwa stanowiska, dotyczące treści zagrożeń bezpieczeństwa ekonomicznego:

1) stanowisko koncentrujące się na określaniu zagrożeń przez negatywne skutki różnych oddziaływań na możliwość realizacji przez dany obiekt ważnych dla niego wartości;
2) stanowisko polegające na lokalizowaniu zagrożeń wśród konfliktów[35].

Zagrożenia bezpieczeństwa ekonomicznego są różnego rodzaju: podlegają zmiennym uwarunkowaniom, przybierają wiele form i dotyczą wielopoziomowych płaszczyzn. Biorąc jednak pod uwagę wpływ wywiadu gospodarczego na bezpieczeństwo ekonomiczne państwa trzeba wyraźnie podkreślić, że jest to jeden z tych czynników, które w znaczący sposób mogą zmniejszyć jego poziom.

Dzieląc bezpieczeństwo ekonomiczne z uwzględnieniem gospodarki, do której się ono odnosi, wyróżnić można:

- *bezpieczeństwo surowcowe (oznaczające zdolność gospodarki do zapewnienia niezbędnych do niezachwianego funkcjonowania surowców zarówno ze źródeł krajowych jak i pochodzących z importu, w sposób niezagrażający rozwojowi gospodarczemu państwa);*
- *bezpieczeństwo żywnościowe (oznaczające zdolność do wykorzystywania wewnętrznych czynników rozwoju, jak również wymiany i współpracy międzynarodowej w celu zapewnienia społeczeństwu zarówno fizycznej jak i ekonomicznej dostępności żywności, oraz jej odpowiedniej jakości, z drugiej zaś strony zapewnienia dogodnych warunków do rozwoju krajowej produkcji żywności);*
- *oraz bezpieczeństwo finansowe (zewnętrzne, oznaczające przede wszystkim brak zadłużenia zagranicznego i zdolność gospodarki do przeciwstawiania*

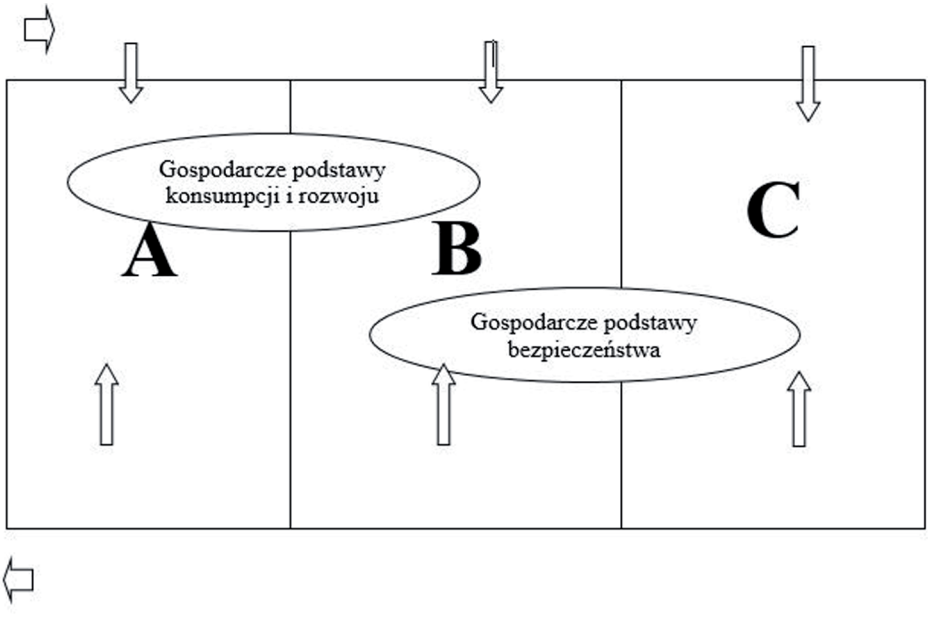
33 Ibidem, s. 30-31.

34 http://kultura-bezpieczenstwa.pl/wp-content/uploads/2015/07/P.-Dzieka%C5%84ski1-KB16.121-140.pdf (dostęp: 27.05.2017)
Por. E. Frejtag-Mika, Z. Kołodziejak, W. Putkiewicz, *Bezpieczeństwo ekonomiczne we współczesnym świecie,* Radom 1996/; K. Księżopolski, *Ekonomiczne zagrożenia bezpieczeństwa państw. Metody i środki przeciwdziałania,* Warszawa 2004.

35 *Bezpieczeństwo ekonomiczne Rzeczypospolitej Polskiej,* s. 72 [w:] http://adamkorcz.w.interiowo.pl/ekon.pdf (dostęp: 30.05.2017).

się kryzysom finansowym, oraz wewnętrzne, czyli zdolność systemu finansów publicznych do niezakłóconego finansowania gospodarki krajowej i zdolność instytucji finansowych do realizacji interesów narodowych)[36].

Rysunek 1
Gospodarcze podstawy bezpieczeństwa państwa w ujęciu narodowym



Źródło: S. Kurek, *Identyfikacja gospodarczych podstaw bezpieczeństwa państwa,* [w:] Z.Stachowiak (red.), *Podstawy, mechanizmy i procedury kształtowania bezpieczeństwa ekonomicznego polski z punktu widzenia narodowej i sojuszniczej strategii obronnej, cz.* I – *Metodologia i model badań bezpieczeństwa ekonomicznego kraju*, Wyd. AON, Warszawa 2001, s. 196, cyt. za: *Bezpieczeństwo ekonomiczne Rzeczypospolitej Polskiej*, s. 78 [w:] http://adamkorcz.w.interiowo.pl/ekon.pdf (dostęp: 12.06.2017).

36 https://www.researchgate.net/profile/Igor_Protasowicki/publication/263571152_Determinanty_bezpieczenstwa_ekonomicznego_Polski/links/02e7e53b41a652fa30000000.pdf s. 10 (dostęp: 12.06.2017).

Tabela 1. **Interpretacja treści wydzielonych obszarów gospodarki z punktu widzenia ich przydatności do zaspokajania zróżnicowanych potrzeb**

OBSZAR	EKONOMIA	EKONOMIKA OBRONY
A	Obszar służący zaspokajaniu potrzeb podstawowych	Obszar niedostępny lub nieprzydatny do zaspokajania potrzeb związanych z bezpieczeństwem
B	Obszar zaspokojenia potrzeb konsumpcyjnych wyższego rzędu i rozwojowych. Obszar racjonalnej transformacji	Obszar „podwójnego zastosowania”
C	Koszt alternatywny bezpieczeństwa w stosunku do innych potrzeb	Obszar służący wyłącznie bezpieczeństwu
A + B	Gospodarcze podstawy konsumpcji i rozwoju	
B + C		Gospodarcze podstawy bezpieczeństwa

Źródło: S. Kurek, *Identyfikacja gospodarczych podstaw bezpieczeństwa państwa,* [w:] Z.Stachowiak (red.), *Podstawy, mechanizmy i procedury kształtowania bezpieczeństwa ekonomicznego polski z punktu widzenia narodowej i sojuszniczej strategii obronnej, cz.* I – *Metodologia i model badań bezpieczeństwa ekonomicznego kraju*, Wyd. AON, Warszawa 2001, s. 196, cyt. za: *Bezpieczeństwo ekonomiczne Rzeczypospolitej Polskiej*, s. 79 [w:] http://adamkorcz.w.interiowo.pl/ekon.pdf (dostęp: 12.06.2017).

Podsumowanie

W burzliwym otoczeniu, w jakim obecnie funkcjonujemy, coraz większego i bardziej istotnego znaczenia nabierają służby wywiadowcze i kontrwywiadowcze. To, czy osiągniemy sukces w jakiejś dziedzinie (ekonomicznej czy militarnej) uzależnione jest od szybkiego i trafnego pozyskania wiarygodnych informacji, ich późniejszej dogłębnej i szczegółowej analizy oraz wydania rekomendacji.

Pamiętać należy tutaj o szerokim instrumentarium narzędzi, jakie służby mogą (czasami z powodzeniem) stosować – np. dezintegrację i dezinformację. W świetle rozważań na temat wywiadu gospodarczego i związanego z tym bezpieczeństwa ekonomicznego państwa są to kwestie o priorytetowym znaczeniu. Nie bez znaczenia pozostają także skutki procesów globalizacyjnych, często bowiem działalność gospodarcza prowadzona jest nie tylko w obrębie własnego państwa, ale również poza jego granicami, czy wręcz na różnych kontynentach. Szeroko rozwinięte powiązania gospodarcze z licznymi podmiotami zagranicznymi mogą mieć dwojakie znaczenie: z jednej strony dają dostęp do światowych rynków zbytu czy kapitału zagranicznego, z drugiej zaś strony, poprzez wiele złożonych czynników, mogą negatywnie wpłynąć na bezpieczeństwo ekonomiczne państwa. Sytuacja geopolityczna państwa również może zagrozić bezpieczeństwu, zarówno ekonomicznemu, jak i polityczno-militarnemu. Pozostaje mieć nadzieję, że w sytuacjach niekorzystnych czy trudnych, służby kontrwywiadowcze państwa będą tymi, które w polityczno-ekonomicznych rozgrywkach okażą się najskuteczniejsze.

Bibliografia

Bajer L., *Wywiad gospodarczy, wszystko o...,* Warszawa 1979.

Bezpieczeństwo ekonomiczne Rzeczypospolitej Polskiej, [w:] http://adamkorcz.w.interiowo.pl/ekon.pdf.

Borowiecki R., Kwieciński M. (red.), *Informacja w zarządzaniu przedsiębiorstwem. Pozyskiwanie, wykorzystanie i ochrona (Wybrane problemy teorii i praktyki),* Zakamycze 2003.

Ciecierski M., *Wywiad ma się lepiej...,* [w:] http://www.wywiad-gospodarczy.pl/wywiad-ma-sie-lepiej.html.

Frejtag-Mika E., Kołodziejak Z., Putkiewicz W., *Bezpieczeństwo ekonomiczne we współczesnym świecie,* Radom 1996.

Javers E., *Agent. Handlarz. Prawnik. Szpieg. Tajemniczy świat korporacyjnego szpiegostwa,* Kraków 2010.

Karpiński M., *Historia szpiegostwa,* Warszawa 2003.

Korzeniowski L., Pepłoński A., *Wywiad gospodarczy, historia i współczesność,* Kraków 2005.

Księżopolski K. M., *Bezpieczeństwo ekonomiczne*, Warszawa 2011.

Księżopolski K., *Ekonomiczne zagrożenia bezpieczeństwa państw. Metody i środki przeciwdziałania,* Warszawa 2004.

Kurek S., *Identyfikacja gospodarczych podstaw bezpieczeństwa państwa,* [w:] Stachowiak Z. (red.), *Podstawy, mechanizmy i procedury kształtowania bezpieczeństwa ekonomicznego polski z punktu widzenia narodowej i sojuszniczej strategii obronnej, cz.* I – *Metodologia i model badań bezpieczeństwa ekonomicznego kraju*, Warszawa 2001.

Minkina M., *Sztuka wywiadu w państwie współczesnym,* Warszawa 2014.

Sun Tzu, *Sztuka Wojny,* Gliwice 2013.

Taradejna M., Taradejna R., *Dostęp do informacji publicznej, a prawna ochrona informacji dotyczących działalności gospodarczej, społecznej i zawodowej oraz życia prywatnego,* Toruń 2003

http://centrum.vismagna.pl/index.php?site=wg&vm1=podstawy&vm2=piwg.

http://kultura-bezpieczenstwa.pl/wp-content/uploads/2015/07/P.-Dzieka%C5%84ski1--KB16.121-140.pdf.

http://wywiadgospodarczy.pl/pl-PL/article/artykuly/article/wywiad_gospodarczy/wywiad_gospodarczy_%E2%80%93_proba_definicji.

http://rynekinformacji.pl/techniki-wywiadowcze-bialy-czarny-szary-wywiad-detektyw-zdobywa-informacje/.

http://www.wywiadgospodarczy.pl/pl-PL/article/artykuly/article/wywiad_gospodarczy/historia_wywiadu_gospodarczego_w_pigulce.

http://forum.echodnia.eu/polskie-sluzby-sa-zagrozeniem-dla-panstwa-sluzby-wojskowe-spenetrowane-przez-rosjan-t182980/.

http://www.forbes.pl/szwajcaria-oskarza-analityka-ktory-przekazal-dane-bankowe-francji,artykuly,187160,1,1.html.

http://www.newsweek.pl/biznes/wiadomosci-biznesowe/wywiad-gospodarczy--szpiedzy--na-miare-xxi-wieku,98099,1,1.html.

http://www.theepochtimes.com/n3/1482874-british-businessman-neil-heywood-divulged-too-much/full/.

https://www.researchgate.net/profile/Igor_Protasowicki/publication/263571152_Determinanty_bezpieczenstwa_ekonomicznego_Polski/links/02e7e53b41a652fa30000000.pdf.

Agnieszka Latosińska*

*** Agnieszka Latosińska, Uniwersytet Ekonomiczny w Krakowie**

Łukasz Wacławik

Zarządzanie strategiczne informacjami we Francji w warunkach globalizacji. Ocena ewolucji pomocy instytucjonalnej

Wprowadzenie

Przełom lat 80. i 90. ubiegłego stulecie rozpoczął okres, w którym gospodarka światowa zaczęła mieć wymiar globalny. Proces globalizacji dotyczył zarówno handlu i produkcji, jak i badań i rozwoju. Dotychczasowe zasady rywalizacji ekonomicznej wymusiły na państwach i na przedsiębiorstwach zmodyfikowania swoich polityk bezpieczeństwa, tak w obszarze rywalizacji handlowej, jak i technologicznej. W przypadku firm wielonarodowych. tworzenie odpowiednich procedur i ich stosowanie było co prawda kosztowne, ale duże firmy dysponowały stosownymi zasobami.

W znacznie trudniejszej sytuacji znalazły się przedsiębiorstwa mniejsze, które nie tylko miały ograniczone możliwości ekspansji, ale też względu na koszty były bardziej narażone na nieuczciwe pozyskanie informacji wewnętrznych.

Celem referatu jest omówienie procesu współpracy Republiki Francuskiej z sektorem przedsiębiorstw w aspekcie pozyskiwania i ochrony informacji, istotnych dla strategicznej sytuacji przedsiębiorstw, jak i dla państwa. Politykę tę rozpoczął raport Martre'a, który bardzo szeroko przedstawił zagadnienia wywiadu ekonomicznego i strategii przedsiębiorstw wskazując przede wszystkim na obowiązki państwa w aktywnym rozwoju przedsiębiorstw. Kolejny raport Carayona zrewidował krytycznie założenia przyjęte przez Martre'a, zwracając zdecydowanie większą uwagę na zagadnienia bezpieczeństwa. Bez wątpienia ten aspekt zarządzania informacjami jest obecnie najważniejszy.

Polityki państwowe w zakresie zarządzania informacją w przedsiębiorstwie – pierwsze doświadczenia

Wielka Brytania i Szwecja najwcześniej jako pierwsze rozpoczęły tworzenie zasad bezpieczeństwa polityki konkurencyjnej: Pierwsze doświadczenia europejskie odwołują się do czasów rewolucji przemysłowej i polityki Wielkiej Brytanii, państwa, będącego prekursorem ochrony konkurencyjnej przemysłu tekstylnego (maszyna tkacka – kara ucięcia ręki za zdradę zasady działania), jak i w czasach już bardziej współczesnych np. chroniąc interesy brytyjskie w krajach Zatoki Perskiej. W Wielkiej Brytanii doszło do współpracy państwa, służb i przedsiębiorstw

naftowych, co skutecznie zabezpieczało pozycję gospodarczą Zjednoczonego Królestwa aż do czasu kryzysu naftowego.

Drugim państwem, które aktywnie prowadziło działalność zabezpieczającą konkurencyjność kraju była Szwecja. W przeciwieństwie do Wielkiej Brytanii, miała trudną sytuację geopolityczną, będąc krajem na styku wielkich sojuszy wojskowych XX wieku, z bardzo silnym wpływem Niemiec. W XX wieku Szwecja stała się dzięki polityce konkurencyjnej państwa przykładem kraju, którego produkty cechowały się wysokim poziomem technicznym i technologicznym, zaś społeczeństwo uznawano za jedno z najbardziej mobilnych, wykształconych i otwartych. W publikacjach często przywoływany jest przykład koncernu ABB, stworzonego pierwotnie na bazie przedsiębiorstwa szwedzkiego i szwajcarskiego, które jako jedno z pierwszych stosowało globalną strategię rozwoju. Szwecja prowadziła spójna strategię wsparcia eksportu i wspomagała rozwój techniki i technologii, dzięki czemu wytwarzano produkty konkurencyjne, o dużej wartości dodanej.

W literaturze przedmiotu należy zwrócić uwagę na przykłady Japonii, Niemiec czy Stanów Zjednoczonych, które to państwa próbowały stosować unikatowe strategie w działaniach prorozwojowych odnoszące się jednak raczej do dziedzictwa historycznego i kulturowego. Rozwój gospodarki japońskiej po II WŚ był rezultatem globalnego transferu technologii i działań długofalowych, rozpisanych na dziesięciolecia. Niemiecki patriotyzm gospodarczy faworyzuje kontakty pomiędzy niemieckimi firmami na całym świecie. Specyfika Stanów Zjednoczonych sprowadza się do skupienia się wyłącznie na rywalizacji wewnętrznej, ignorując konkurentów zagranicznych oraz działając w krótkim okresie.

Opisane skrótowo polityki państwowe posiadały swoje specyfiki, jednak w latach 90. nastąpił przełom w zarządzaniu informacjami. Tradycyjne sposoby pozyskiwania i przechowywania informacji, sprowadzające się do dość prostych narzędzi ich gromadzenia i ochrony, zostały ukierunkowano na pozyskiwanie informacji z wykorzystaniem Internetu.

Jednocześnie zjawisko globalizacji spowodowało umiędzynarodowienie rywalizacji gospodarczej na obszarze całej planety. Pojawiły się nieznane wcześniej szanse oraz zagrożenia.

Pierwsze doświadczenia francuskie w zakresie zarządzania strategicznego informacjami

Przypadek Francji jest szczególny. Po II WŚ Francja była głęboko osadzona w strukturach bezpieczeństwa NATO czy też była wśród założycieli dzisiejszej Unii Europejskiej, jednak posiadała zawsze silną odrębność wynikająca z ambicji państwa postkolonialnego. Jest jednym z pierwszych państw, które starały się pozyskiwać informacje ekonomiczne metodami wywiadowczymi (np. podsłuchy w samolotach), chronić swój dorobek technologiczny (np. ochrona firmy Michelin) czy też tworzyć unikatową technologię (SECAM, TGV).

W przeciwieństwie do innych państw, Internet nie był pierwszą siecią, dzięki której można było pozyskiwać informacje. W 1982 wspólna inicjatywa poczty i telekomunikacji francuskiej doprowadziła do powstania Minitela – urządzenia, które umożliwiało płatne pozyskiwania informacji, z początku była to książka telefoniczna, a z czasem informacji ekonomicznych, łącznie z dostępem do własnego konta w banku. Minitel, który działał równolegle z Internetem (do 2012), i doświadczenia wynikające z posiadania sieci i z udostępniania danych, miały istotny wpływ na percepcję zarządzania informacjami we Francji.

W literaturze francuskiej występują trzy pojęcia opisujące zagadnienia zarządzania strategicznego informacjami: *intelligence economique, veille strategique* oraz *intelligence strategique*. Pierwsze z pojęć jest najbliższe określenia wywiadu ekonomicznego, drugie strategii czuwania czy strategicznego śledzenia otoczenia konkurencyjnego, trzecie wywiadu strategicznego. Wywiad ekonomiczny to zespół skoordynowanych działań poszukiwania, przetwarzania i dystrybucji informacji użytecznych dla podmiotów gospodarczych. Aktywności te są równolegle chronione przed zagrożeniami zewnętrznymi. Strategiczne śledzenie otoczenia konkurencyjnego to działanie ciągłe i interaktywne ukierunkowane na aktywne monitorowanie otoczenia konkurencyjnego, technologicznego, handlowego, prawnego itd w celu antycypacji jego zmian. Wywiad strategiczny to definiowanie, zbieranie, obserwowanie, zatwierdzanie i interpretowanie informacji strategicznych. Trzy powyższe pojęcia są niekiedy traktowane jako synonimy.

Wywiad ekonomiczny, strategiczne śledzenie otoczenia konkurencyjnego i wywiad strategiczny są więc elementami strategii zarządzania informacjami w organizacji, a ich stosowanie może być skuteczne tylko wtedy, gdy wpisuje się w perspektywę strategiczną zarządzania informacjami. Organizacja musi więc podejmować niezbędne działania, by pozyskiwać informacje z otoczenia, faworyzując jej użyteczność, by stworzyć przedsiębiorstwo wiedzy.

Zarządzanie informacjami, wywiad gospodarczy czy śledzenie otoczenia konkurencyjnego wydają się kategoriami zarezerwowanymi dla sfery przedsiębiorstw. Należy więc postawić pytanie: dlaczego Francja zdecydowała się na prowadzenie polityki państwowej w tym zakresie? Informacja, zarządzanie informacjami staje się podstawą każdej organizacji, a przedsiębiorstwa doskonalą swoje polityki informacyjne i zarządzają wiedzą. W tym kontekście szczególnego znaczenia nabiera polityka państwa, które powinno skutecznie wspomagać przedsiębiorców w działaniach mających na celu zarządzanie zgromadzoną wiedzą[1].

Raport Henri Martre'a – podstawa debaty nad zarządzaniem informacjami

Po II WŚ specyfiką gospodarki Francji było centralne planowanie w wymiarze strategicznym. Państwo definiowało podstawowe cele strategiczne oraz określa-

1 Bergeron P., *Veille strategique et PME, Comparaison des politiques gouvernementales de soutien*, Presses de l'Universite du Quebec, 2000, s.5 i dalsze

ło problemy, które pojawią się w perspektywie kilkuletniej oraz proponowało politykę państwa związaną z pojawiającymi się szansami i zagrożeniami. Co 4-6 lat odbywano debaty i wyznaczano kierunki rozwoju kraju w oparciu o próbę określenia zmian zachodzących na świecie i priorytetów państwa. W 1992 roku, podczas przygotowań do wdrażania XI planu, w ramach grupy: informacja i konkurencyjność opracowano pod kierunkiem H. Martre'a raport: *Intelligence economique et strategie des enterprises* (Wywiad ekonomiczny i strategia przedsiębiorstw), będący punktem wyjścia do debaty nad rolą i znaczeniem zarządzania strategicznego informacjami we Francji.

Raport[2] został opracowany przez zespół badawczy, w skład którego wchodzili przedstawiciele państwa oraz przedsiębiorstw. W 30 najważniejszych firmach francuskich do pomocy przy jego realizacji oddelegowano pracowników począwszy od prezesów firm po kierowników zajmujących się pozyskiwaniem czy ochroną informacji.

W raporcie można wyróżnić 4 podstawowe elementy:

1) Perspektywa na poziomie centralnym i konieczne działania (określenie działań, które należy podjąć na szczeblu rządowym, identyfikacja podmiotów związanych z wywiadem, wskazanie znaczenia badań nad rozwojem zarządzania informacjami w wymiarze konkurencyjnym i kooperacyjnym, zaproponowanie środków wsparcia instytucjonalnego, promowanie francuskiej kultury wywiadu gospodarczego).
2) Pozyskiwanie informacji wywiadowczych poprzez bazy danych (określenie przedmiotu zainteresowania wywiadu gospodarczego, które będą użyteczne w definiowaniu i wdrażaniu strategii, określenie standardów produktów i usług informatycznych stosowanych w przemyśle).
3) Analiza porównawcza wywiadu gospodarczego na świecie (omówienie doświadczeń innych państw, przedstawienie typowych praktyk przedsiębiorstw-eksporterów, zgromadzenie podstawowych problemów stojących przed przedsiębiorstwami nowej ekonomii).
4) Promocja wiedzy z zakresu zarządzania informacjami strategicznymi (podniesienie poziomu świadomości i edukacji w zakresie zarządzania informacjami)

W toku prac określono 4 podstawowe przeszkody w rozwoju zarządzania strategicznego informacjami:

1) Rozproszenie zasobów i działań, które są podejmowane bez wzajemnej koordynacji, co powoduje niezadawalające wyniki. Brak koordynacji, brak priorytetów powoduje, że podejmowane działania często się dublują, a są niewystarczające w istotnych obszarach.
2) Brak koordynacji i współpracy między przedsiębiorstwami francuskimi na rynkach zagranicznych. Dotyczy to zarówno działań podejmowanych na rynkach zagranicznych jak i współpracy pomiędzy podmiotami francuskimi na rynkach obcych.

2 Elementy, przeszkody i wnioski opracowano na podstawie: *Rapport Martre 1994: Intelligence économique et stratégie des enterprises*, Commissariat General du Plan, La Documentation Francaise, 1994

3) Konflikty między poszczególnymi działami w przedsiębiorstwie. Bardzo częstą przyczyną porażek są konflikty i rywalizacja między pracownikami rożnych działów przedsiębiorstwa, co skutecznie utrudnia wdrażanie spójnych praktyk.
4) Problemy administracyjne utrudniające przepływ informacji. Problemy te wynikają zarówno z braku stosownych procedur, jak i braku świadomości znaczenia przepływu informacji w działaniach przedsiębiorstw.

W toku prac sformułowano 4 wnioski odnoszące się do rozwoju zarządzania strategicznego informacjami:

1) Rozszerzać stosowanie zarządzania strategicznego informacjami w przedsiębiorstwach: zobowiązać dyrekcję przedsiębiorstw do określenia polityki, potrzeb, osób zaangażowanych w zarządzanie informacjami, zorganizowanie sieci wewnętrznej, stworzenie funkcji wewnętrznego animatora, szkolenie specjalistów, wdrażanie standardów etycznych, stworzenie narzędzi ewaluacji wdrożonego sytemu, powołanie osoby odpowiedzialnej za stosowanie zarządzania strategicznego informacjami.
2) Poprawienie przepływu informacji między sektorem publicznym a prywatnym w celu zarządzania kolektywnego informacjami (określanie obszarów współpracy i eksperymentów, tworzenie jednolitych procedur, określenie potencjału sektorów, stworzenie powiązań wymiany informacji, inicjatywa państwa w zakresie stworzenia instytucji zajmującej się zarządzaniem strategicznym informacjami, stworzenie sieci powiązań między wspomaganiem innowacji oraz badań i rozwoju a organami administracji centralnej wspomagającymi badania naukowe, wdrożenie programu kształcenia dla specjalistów).
3) Projektowanie baz danych dostosowanych do potrzeb użytkowników (przygotowanie kadr, w tym średniego szczebla usługodawców, kształcenie specjalistów rozumiejących zależności między bazami danych a potrzebami informacyjnymi pracowników, podnoszenie świadomości znaczenia tych informacji.

Wzmocnienie edukacji w zakresie zarządzania informacjami (utworzenie studiów dla osób zajmujących się zarządzaniem strategicznym informacjami[3]).

Realizacja raportu H. Martre'a – norma XP X 50-053 i tworzenie instytucji

W kwietniu 1998 roku Francuskie Stowarzyszenie Normalizacyjne (Association Française de Normalisation – AFNOR) opublikował zasady wdrażania zarządzania strategicznego informacjami. Norma regulowała pojęcia i procedury z zakresu zarządzania strategicznego informacjami. Głównym celem normy było ułatwienie wzajemnych relacji między dostawcą wewnętrznym lub zewnętrznym a klientem poprzez stworzenie terminologii oraz wzajemnych relacji zawartych w kontrakcie. Służyło to ułatwieniu i zabezpieczeniu interesu zarówno firm korzystających z usług wywiadowczych, jak i firm oferujących takie usługi. AFNOR

3 W ramach działalności edukacyjnej powołano studia w Poitiers, równolegle prowadzono w Archamps (francuska część Genewy) studia doktoranckie w zakresie zarządzania strategicznego informacjami, będące wynikiem współpracy uczelni francuskich i szwajcarskich. Autor tekstu był ich uczestnikiem.

pragnął również poprawić jakość dostaw związanych z zarządzaniem strategicznym informacjami.

Norma regulowała pojęcia, które zostały stworzone w literaturze francuskiej na początku lat 90., ściśle związanych z pojęciami zarządzania strategicznego informacjami (antycypacja, poszukujący informacji, dezinformacja, informacja krytyczna, informacja strategiczna, informacja użyteczna, alert), omówiono proces śledzenia otoczenia konkurencyjnego wskazując na 8 kolejnych kroków:

1) Definiowanie obszaru tematycznego analizy (chodzi o opisanie i sprecyzowanie tematów, które interesują zamawiającego, tak by były adekwatne do wymagań technologicznych, prawnych, normatywnych ekonomicznych, konkurencyjnych, społecznych itp. oraz określenie ostatecznych oczekiwań zamawiającego co do zalecanej formy raportu).
2) Określenie rodzaju pożądanych informacji (określenie czy badanie ma mieć charakter ilościowy i/lub jakościowy. Czy raport ma się ograniczać do informacji pierwotnych, wtórnych czy do opinii ekspertów).
3) Identyfikacja i selekcja źródeł informacji (celem działań jest wybór spośród źródeł informacji tych, które zapewnią skuteczną realizację zamawiającego, tak pod względem czasu, poufności jak i kosztu ich pozyskania).
4) Zebranie i wybór informacji (informacje zbierane są albo regularnie albo dla jakiegoś czasu. Dostawca odpowiada za dostarczenie odpowiednio wyselekcjonowanych informacji związanych bezpośrednio lub pośrednio z badanym zagadnieniem).
5) Analiza zebranych informacji (Chodzi o przekształcenie zebranych informacji i ich pogrupowanie w taki sposób, by można było je wykorzystać – wyniki, klasyfikacja, synteza czy bibliografia).
6) Synteza w aspekcie obszaru tematycznego (chodzi o dokonanie syntezy zebranych informacji i zaproponowanie takiej ich formy, by mogły być użyteczne w podejmowanych decyzjach).
7) Przedstawienie wyników zlecającemu (wyniki analizy powinny być przedstawione w ściśle ustalonej formie. Mogą to być notatki, prezentacje, raporty, opracowania itp.).
8) Ocena i działania korygujące (omówienie wyników powinno służyć również uściśleniu dalszych poszukiwań dla kolejnego tematu czy kolejnego okresu).

W wyniku raportu Martre'a utworzono lub poszerzono kompetencje 6 instytucji, których zadania zostały powiązane z wywiadem ekonomicznym i strategią przedsiębiorstw:

1) Zgromadzenie francuskich izb handlowych i przemysłowych (franc. Assemblée des Chambres Francaises de Commerce et d'Industrie – ACFCI),
2) Agencja dyfuzji informacji technologicznych (franc. Aagence pour la Diffusion de l'Information Technologique – ADIT), której celem jest tworzenie polityki zarządzania informacją technologiczną, dokonywanie studiów przyszłej ewolucji nauki i techniki oraz przemysłu i próba oceny ich wpływu na sytuację

społeczną i ekonomiczną. Ciągła synteza bieżących zdarzeń z zakresu nauki, technologii czy techniki i ich wpływu na innowacje techniczne.

3) Agencja regionalna informacji naukowej i technologicznej (franc. Aagence Régionale d' Informations Scientifiques – ARIST),

4) Francuskie Centrum handlu zagranicznego (franc. Centre Français du Commerce Extéieur – CFCE),

5) Dyrekcja relacji ekonomicznych zewnętrznych (franc. Direction des Relations Economiques Extérieurs – DREE),

6) Dyrekcja działań regionalnych oraz małych i średnich przedsiębiorstw przemysłowych (DARPMI), której celem jest współuczestnictwo w programach mających ułatwić przedsiębiorstwom małym i średnim działania w zakresie samodzielnego pozyskiwania informacji strategicznych z otoczenia.

Raport Carayona – krytyczne spojrzenie na wyniki raportu Martre'a.

Dziesięć lat po raporcie opracowanym przez Martre'a pojawił się kolejny raport opracowany przez zespół Bernarda Carayona[4]. Celem raportu była próba odpowiedzi na trzy podstawowe pytania:

1) Jaki jest stan wywiadu ekonomicznego i jakie ma braki?

2) Co należy zrobić, by wzmocnić wywiad ekonomiczny?

3) W jaki sposób poprawić strategiczny wymiar wywiadu ekonomicznego.

Powyższe pytania wynikały wprost z krytyki raportu Martre'a, który co prawda stworzył administrację związana z wywiadem ekonomicznym, i doprowadził do uruchomienia procesu poprawy innowacyjności czy edukacji, jednak osiągnięte wyniki bardzo trudno było uznać za satysfakcjonujące.

Raport Carayona składa się z 38 postulatów zebranych w 6 rozdziałach.

1) Podmioty i obszar wywiadu gospodarczego, w którym zdefiniowano trzy podstawowe strony: państwo i samorządy, przedsiębiorstwa i obywateli.

2) Konkurencyjność Francji, konkurencyjność francuskich przedsiębiorstw francuskich, w którym omówiono dwa najważniejsze fundamenty konkurencyjności: badania i innowacje. W raporcie poddano krytyce podejście zaproponowane przez Martrea, istnienie bardzo wielu podmiotów, które albo koordynują albo współpracują w ramach zarządzania strategicznego informacjami, jednak powszechny jest brak współpracy oraz zdefiniowania założeń strategicznych. W raporcie zaproponowano stworzenie Krajowej Rady Konkurencyjności i bezpieczeństwa gospodarczego i wyznaczenie międzyresortowego delegata ds. konkurencyjności i bezpieczeństwa ekonomicznego. W sektorze małych i średnich przedsiębiorstw zaleca się wykorzystanie nowoutworzonej agencji UBIFRANCE do poszerzenia wsparcia sektora MSP.

3) Kolejny punkt to znaczenie potencjalnych zagrożeń dla przedsiębiorstw francuskich. By im sprostać należy wdrożyć kompleksową bezpieczeństwa ekono-

4 Opracowano na podstawie: *Rapport Carayon, Intelligence économique, compétitivité et cohésion sociale*, Base de Connaissance, 2003.

micznego, która wymaga adaptacji, wdrożenia przepisów wzmacniających rolę służb, wzmocnienie świadomości roli etyki i bezpieczeństwa w gospodarce.

4) Polityka wpływu. Zdaniem autora koniecznością jest poprawa wpływu polityki Francji na partnerów zagranicznych, w tym wzmocnienie roli kraju w strukturach unijnych. Zdaniem autora raportu jest to jeden z najbardziej zaniedbanych elementów zarządzania informacjami

5) Polityka kształcenia. Raport krytykuje francuski model kształcenia w zakresie wywiadu ekonomicznego, brakuje wzorców, programów, wymogów, procedur, kształceniem zajmują się przypadkowe osoby często bez doświadczenia. Nauka ma charakter teoretyczny, a weryfikacja wiedzy i jej użyteczność często niewielka. Ciekawą propozycją jest wprowadzenie programu stażowego dla urzędników, tak by mogli się zapoznać ze specyfiką pracy przedsiębiorców

6) Wywiad gospodarczy i regiony. Zdaniem autora wzmocnienia wymaga stosowanie regionalnych narzędzi wywiadu gospodarczego, który, dzięki zastosowaniu najlepszych praktyk ułatwi rozwiązywanie problemów lokalnych.

Jak widać, kolejny raport opisujący praktykę zarządzania strategicznego informacjami zwraca uwagę na brak korelacji między pierwotnymi założeniami przyjętymi w raporcie Martre'a a jego praktyką. Raport Carayona wykazał, że bardzo ambitne plany przyjęte pod koniec XX wieku nie wpłynęły pozytywnie na cele, dla których państwo francuskie postanowiło wspierać w formie instytucjonalnej zarządzanie strategiczne informacjami. Francja przez 10 lat wspierania rozwoju przedsiębiorstw nie wzmocniła swojej pozycji konkurencyjnej, ba pozycja ta pogarsza się do czasów współczesnych. Raport Carayona pokazuje więc, że co prawda problemy zarządzania strategicznego informacjami zostały poprawnie zdefiniowane przez zespół Martre'a, jednak praktyka działań i jej wyniki należy ocenić negatywnie. Istotnym elementem raportu Carayona jest zwrócenie uwagi na politykę bezpieczeństwa, czyli ochrony, i negacja dotychczasowych założeń polityki rozwoju przedsiębiorstw, w której zaangażowanie państwa powinno być mniejsze.

Percepcja zarządzania strategicznego informacjami w przedsiębiorstwach francuskich

Wśród przedsiębiorstw francuskich można wyróżnić trzy grupy, których charakterystykę zaproponował H. Lesca oceniając stosunek przedsiębiorstw do strategicznego podejścia do informacji. Wyróżnił on :

- korzystających z zarządzania strategicznego informacjami do tworzenia przewagi konkurencyjnej,
- wykorzystujących pewne narzędzia zarządzania strategicznego informacjami i zdających sobie sprawę z własnych niedoskonałości,
- ignorantów w sprawach zarządzania strategicznego informacjami.

Przenosząc ten klasyczny już podział w czasy współczesne, można zaproponować jego modyfikację i wyodrębnić następujące grupy przedsiębiorstw:

- tworzących stanowiska pracy wspomagane *outsourcingiem* w zakresie analizy wybranych elementów otoczenia, korzystających z *outsourcingu* w zakresie analizy otoczenia z niewielkim wkładem własnym,
- ignorantów, którzy nie chcą lub nie muszą śledzić zmian w otoczeniu. Przynależność do każdej z powyższych grup determinuje relacje z podmiotami, które zajmują się pozyskiwaniem informacji i sprzedawaniem jej innym partnerom.

Pierwszą grupę tworzą firmy działające w warunkach dużego postępu techniki, technologii czy innowacji. Firmy z tej grupy korzystają z wielu źródeł informacji, korzystają z pomocy państwa, wspomagając się wyspecjalizowanymi bazami danych, współpracują ze środowiskiem naukowym oraz kierują się raportami sektorowymi, opracowanymi m.in. przez wywiadownie gospodarcze. Raporty wywiadowni gospodarczych mają tu jednak przede wszystkim funkcje kontrolne, pozwalają stwierdzić *ex post* czy działania własnych komórek odpowiedzialnych za zbieranie informacji o charakterze strategicznym były właściwe. Druga grupa firm jest znacznie bardziej liczna niż to zakładał Lesca. Przedsiębiorstwa coraz chętniej korzystają z *outsourcingu* w poszukiwaniu danych gospodarczych czy technologicznych. W przypadku średnich firm takie rozwiązanie jest zdecydowanie najtańsze, co zapewne przekłada się na nietworzenie stanowisk pracy odpowiedzialnych za śledzenie otoczenia konkurencyjnego. Właściciele firm po prostu wolą zapłacić firmie zewnętrznej za ściśle zdefiniowane informacje, zamiast próbować je pozyskać samodzielnie. Ponadto dynamika zjawisk ekonomicznych wzrasta i niezwykle trudno wykształcić osobę, która będzie potrafiła prawidłowo ocenić tendencje w zakresie zmian w technice czy otoczeniu. Dlatego też przedsiębiorcy, mając do wyboru ponoszenie dużych kosztów na komórki poszukujące informacji, często zadowalają się raportem umożliwiającym ocenę konkurentów czy partnerów biznesowych tworzoną przez wywiadownie gospodarcze. Należy nadmienić, że znaczenie antycypacyjne informacji jest w przypadku tych firm zdecydowanie mniejsze. W tej grupie przedsiębiorstw obserwuje się powolny rozwój zastosowania narzędzi służących kontroli (a raczej rejestracji) procesów wewnętrznych. Jednak działania te mają przede wszystkim podłoże ekonomiczne. Wreszcie pozostaje ostatnia grupa przedsiębiorstw małych, których działania sprowadzają się co najwyżej do śledzenia konkurencji.

We Francji podobnie jak w Polsce trwają czynności wzmacniające bezpieczeństwo ekonomiczne i zabezpieczające przedsiębiorstwa przed narażeniem na utratę informacji strategicznych.

Wnioski

Polityka Francji w zakresie zarządzania strategicznego informacjami, czyli wywiadu ekonomicznego, strategicznego śledzenia otoczenia konkurencyjnego czy wywiadu strategicznego ulega ewolucji. Wdrażając pierwsze programy związane z zarządzaniem informacjami politycy francuscy skupili się na czynnikach rozwojowych, chcąc poprawić sytuację konkurencyjną kraju, umożliwić rozwój przemysłu i usług o wysokim poziomie wartości dodanej bazującej na innowa-

cjach technologicznych, z wykorzystanie współpracy pomiędzy sektorem publicznym a prywatnym; zakładano, że państwo będzie wspierać rozwój technologii przedsiębiorstw francuskich i unijnych pozwalających osiągnąć przewagę na rynku światowym, z zachowaniem kontroli produktów wrażliwych. Próby tej nie można uznać za udaną. Stworzono instytucje, wdrażano programy, jednak Francja nie poprawiła swojej pozycji konkurencyjnej.

Tymczasem zdecydowanie wzrosła świadomość potrzeby bezpieczeństwa ekonomicznego i ochrony własnych zasobów będących potencjalnymi źródłami przewagi konkurencyjnej przedsiębiorstw francuskich. I właśnie to zadanie staje się podstawowym dla wywiadu ekonomicznego: zarówno w obszarach wrażliwych jak i badań i rozwoju, który w przyszłości zaowocuje produktami o wysokiej wartości dodanej.

Bibliografia:

Bergeron P., *Veille stratégique et PME. Comparaison des politiques gouvernementales de soutien*, Presses de l'Universite du Quebec, 2000.

Moinet N., *Petite histoire de l'intelligence* économique*: une innovation «à la française*» Veille magazine – Janvier / Février 2012.

Lesca H.*, Pour un management stratégique de l'information*, Revue Française de Gestion 1992, n° 90.

Raporty:

Rapport Martre, *Intelligence* économique *et stratégie des enterprises*, Commissariat General du Plan, La Documentation Francaise, 1994 http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/074000410.pdf.

Rapport Carayon, *Intelligence économique, compétitivité et cohésion sociale*, 2003, Base de Connaissance.

https://portail-ie.fr/resource/textes-de-reference/658/rapport-carayon-2003- intelligence-economique-competitivite-et-cohesion-sociale.

Akty prawne i normy:

Décret n° 2013-759 du 22 août 2013 relatif au délégué interministériel à l'intelligence économique.

Décret n° 2016-66 du 29 janvier 2016 instituant un commissaire à l›information stratégique et à la sécurité économiques et portant création d›un service à compétence nationale dénommé «service de l'information stratégique et de la sécurité économiques».

Prestations de veille. Prestations de veille et prestations de mise en place d'un système de veille, norma XP X 50-053, AFNOR, 1998.

Łukasz Wacławik*

*** Łukasz Wacławik, Akademia Górniczo-Hutnicza w Krakowie.**

Krystian Kula

Iluzja pełnej informacji jako przestrzeń dla skutecznego działania wywiadu i kontrwywiadu w świecie fintechu

Wstęp

Informacja odgrywa kluczową rolę przy podejmowaniu decyzji. Do tej pory największym wyzwaniem było dostarczanie jak największej ilości danych, by optymalizować decyzje finansowe.

Trwająca współcześnie czwarta rewolucja przemysłowa wymusiła zmianę postrzegania problemu informacji. Zdobycie dostępu do pełnych danych jest obecnie możliwe bez wielkiego wysiłku. Problemem staje się więc nie tyle samo dostarczenie danych, a raczej ich analiza i właściwa hierarchizacja. Pozyskanie informacji, które są dobrze zdefiniowane, zgodne z tematem analizy oraz posiadają odpowiednią wagę staje się kluczowym zadaniem.

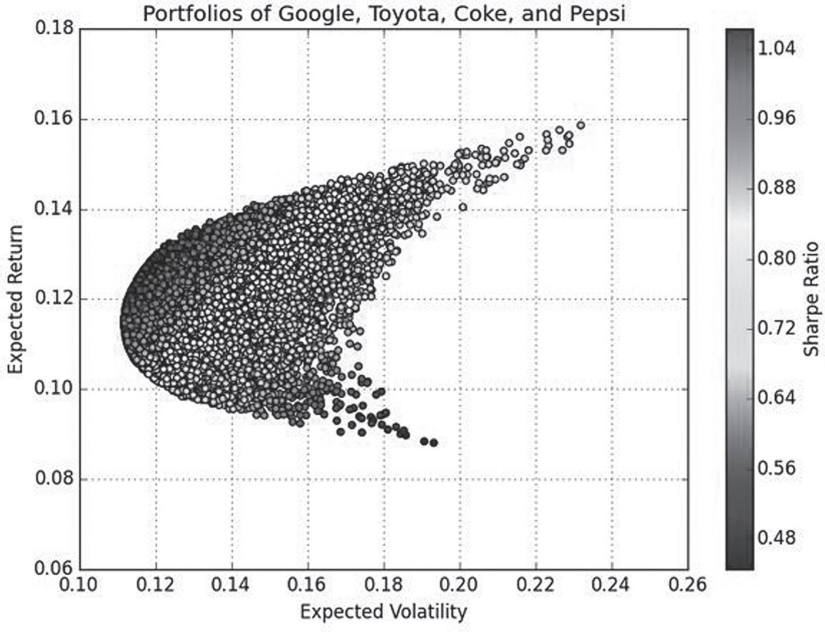
Modern Portfolio Theory

Podstawową zasadą w świecie finansów jest minimalizacja ryzyka przy jednoczesnej maksymalizacji zysków. Każdy racjonalny inwestor będzie preferował portfel o większym zysku przy zachowaniu tego samego ryzyka oraz portfel o mniejszym ryzyku przy zachowaniu tego samego zysku.

Powyższa zasada została po raz pierwszy ujęta w Teorii portfela (*Modern Portfolio Theory*, MPT). Harry Markowitz zaprezentował ją w artykule *Portfolio Selection* w czasopiśmie Journal of Finance (1952).

MPT pokazuje, że inwestor może skonstruować portfel składający się z wielu aktywów w celu maksymalizacji zysku przy danym poziomie ryzyka lub przy danym poziomie zysku skonstruować portfel mniej ryzykowny. Aby stworzyć taki portfel oprzeć się trzeba na danych statystycznych (odchylenie standardowe, kowariancja). Warto wspomnieć, że zakładamy, iż wszyscy inwestorzy mają równy i pełny dostęp do informacji.

Najlepiej tą teorię prezentuje jej graficzne przedstawienie zwane Markowitz Bullet (Efficient *Frontier*). Intuicyjnie oddaje ono intencje racjonalnego inwestora.



Rysunek 1. **Efficient Frontier,Github.com**

Ryzyko jest miarą odchylenia standardowego od prognozowanego zysku. Informuje ono inwestora, jak prawdopodobne jest niespełnienie założeń co do prognozowanego zysku. Inwestor prognozuje zysk i jest świadomy, iż jest kwantyfikowalne prawdopodobieństwo niespełnienia tego założenia.

Dla aktywa ryzyko definiowane jest jako:

$$S| = \sqrt[2]{\sum_{i=1}^{n} (R_i - E(R_i))^2 P_i}$$

R-zysk
E(R) – szacowany zysk
P – prawdopodobieństwo

MPT wprowadza korelację między aktywami. Korelacja pokazuje, czy ryzyko jednego aktywa występuje w tym samym czasie co innego. Jeżeli korelacja jest pozytywna i wynosi 1, to jeśli ryzyko zmaterializuje się w jednym aktywie, zmaterializuje się też w drugim. Łącząc aktywa (dywersyfikując) w portfel uzyskujemy mniejsze odchylenie od założonego zysku definiowane następująco:

$$S_{port} = \sqrt{\sum_{i=1}^{n} w_i^2 s_i^2 + \sum_{i=1}^{n} \sum_{\substack{j=1 \\ i \neq j}}^{n} w_i w_j Cov_{ij}}$$

w – udział aktywa w portfelu
Cov – kowariancja zysków miedzy aktywami numer 1 oraz numer 2 w portfelu.

Powstaje więc pytanie, co mogłoby skłonić inwestora do zaakceptowania niższego zysku przy takim samym ryzyku (wszyscy inwestorzy pod krzywą). Zakładamy, że pełna informacja jest dostępna, a punkty to tylko potencjalne portfele dla zobrazowania zależności miedzy ryzykiem, zyskiem a korelacją. W świecie rzeczywistym jednak istnieje wiele, różniących się od siebie, portfeli. Większość z inwestorów, działa w przekonaniu, że maksymalizuje zysk przy jednoczesnej minimalizacji ryzyka. Każdy z tych inwestorów działa logicznie, różni ich jedynie dostęp do informacji.

Powyższa analiza jest fundamentem obecnego świata inwestycji i przez jej pryzmat powinniśmy spojrzeć na kluczową rolę danych czy informacji.

Bat tunel effect

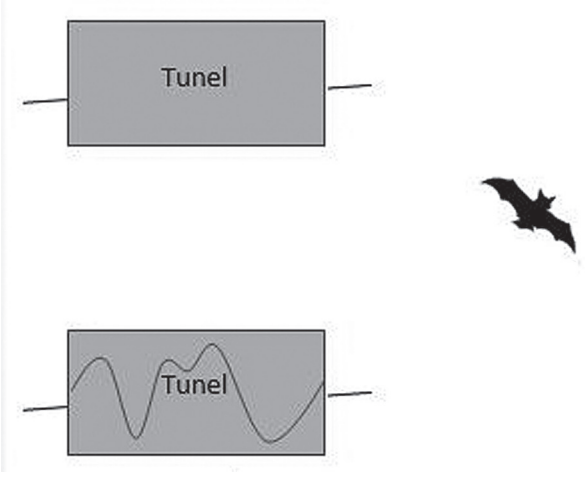
Podstawą każdej analizy są dane. Wywiad, rozumiany jako proces pozyskiwania informacji, dostarczający rzetelnych i dobrze opisanych danych jest jednym z kluczowych elementów opracowań. Dane dostarczone z pewnym opóźnieniem nie niosą już takiej samej wartości i mogą być nieprzydatne dla analityków.

Aby możliwe było porównanie różnych informacji, po procesie gromadzenia danych następuje ich standaryzacja, wymagająca wielokrotnych przeliczeń. Niestety w wyniku takich zabiegów ostateczny wynik może być obarczony błędami.

Spośród gromadzonych danych historycznych brane są pod uwagę jedynie jednostki obecnie istniejące. Pozostałe, czyli te które nie zostały zachowane nie są uwzględniane w populacji. Powoduje to zawyżenie zysku oraz zaniżenie ryzyka.

Innym problemem w porównywaniu danych jest zmieniające się środowisko. Informacje zebrane z poprzedniego okresu mogą już nie być przydatne w związku ze zmieniającym się otoczeniem prawno/ekonomicznym.

Istotny jest również problem braku lub ograniczonego dostępu do pełnego zakresu danych. Nasuwa się porównanie z lotem nietoperza w tunelu. W przypadku kiedy nie widzimy pełnej trajektorii lotu, uznajemy, iż ten lot był prosty, a więc bez znaczących odchyleń. Gdybyśmy jednak byli w stanie prześledzić każdą poszczególną pozycję w tunelu, zobaczylibyśmy, iż tak naprawdę nietoperz poruszał się w górę i w dół wielokrotnie. Tak więc jego trajektoria znacząco różniła się od prostej.



Rysunek 2. **Efekt Nietoperze, CFA Institute**

Blockchain

Obecnie dominuje technologia zcentralizowanych baz danych. Taka baza jest zlokalizowana, archiwizowana i przetrzymywana w jednym miejscu, najczęściej jest to serwer lub system bazy danych. Bardzo często taka baza jest używana przez jedną organizację lub instytucję. Użytkownicy korzystają z niej za pośrednictwem komputera z dostępem do głównego serwera, który ową bazę utrzymuje.

Blockchain to rozproszona baza danych w architekturze P2P (peer to peer) korzystająca z połączenia internetowego. Każdy użytkownik działa na zasadzie serwera, utrzymując i przechowując rejestry. Poszczególne transakcje lub zapisy zakodowane są za pomocą algorytmów kryptograficznych (np. SHA256) w następujących po sobie blokach danych. Mimo, iż wszystkie zapisy zakodowane są w ogólnodostępnych blokach, są one zaszyfrowane, tak więc pojedynczy użytkownik ma dostęp tylko do danych do których jest uprawniony. *Blockchain* został scharakteryzowany w następujący sposób (Iansiti i Lakhani, 2017):

1. Rozproszona baza danych:

Każdy uczestnik łańcucha bloków ma dostęp do całej bazy danych jak i do jej historii. Żaden pojedynczy użytkownik nie kontroluje bazy danych. Każdy użytkownik może sprawdzić transakcje z innym użytkownikiem, bez pośredniczenia centralnej bazy

2. P2P

Wymiana informacji następuje bezpośrednio między użytkownikami.

3. Transparentność i pseudonim

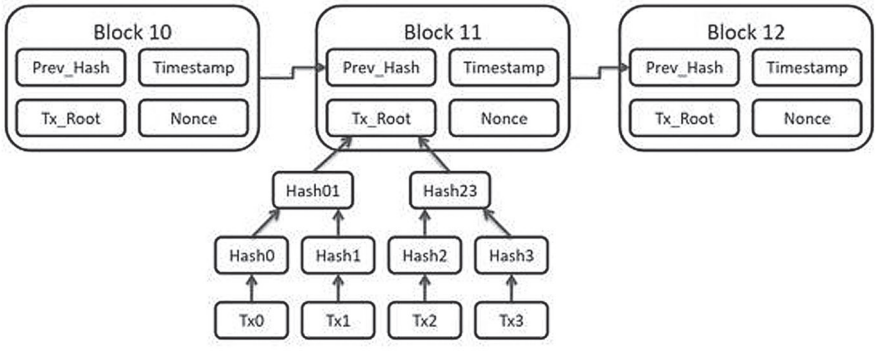
Każda transakcja i jej wartość są widoczne dla każdego z dostępem do systemu. Wszyscy użytkownicy mają swój unikalny trzydziestoznakowy adres identyfikujący, chociaż mogą pozostać anonimowi. Wymiana informacji dokonuje się poprzez adres blockchain.

4. Nieodwracalność

W momencie, kiedy transakcja jest wpisana do bazy danych i następuje synchronizacja rachunku, wpisu nie można już zmienić ponieważ jest on połączony z każdą poprzednią i kolejną transakcją.

5. Logika

Cyfrowa natura bazy danych powoduje, że można zastosować logikę komputerową. Użytkownicy mogą zbudować i wprowadzić algorytm i zasady, które zostaną automatycznie uruchomione w przypadku transakcji.



Rysunek 3. **Blockchain, Insiti i Laghani**

Technologia gwarantuje ciągłość transakcji, jest odporna na błędy ludzkie ale i błędy w obliczeniach. Ponieważ każda transakcja jest rejestrowana, prześledzenie historii nie stanowi problemu. Innymi słowy dokładnie wiadomo co się stało, kiedy i w którym miejscu od powstania rejestru.

Zalety tej technologii powodują, że może być ona wykorzystywania do prowadzenia rejestrów – od ksiąg głównych czy ksiąg wieczystych po transakcje przelewów.

Blockchain coin

Jednym z zastosowań technologii *Blockchain* jest tworzenie krypto walut. Najważniejszymi przedstawicielami są *Bitcoin* i *Ethereum*. W ciągu ostatnich kilku lat właśnie takie zastosowanie otrzymuje sporo uwagi, szczególnie w mediach społecznościowych. Nie bez znaczenia pozostaje fakt, iż Bitcoin (BTC) zanotował wzrost z poziomu około 1000 $ na początku 2017 roku do prawie 20 000 $ na koniec 2017 roku. A jeszcze 4 lata wcześniej, na początku 2013 roku cena kształtowała się na poziomie nieznacznie powyżej 10 $. Taki wzrost musi budzić emocje.

Bitcoin wprowadzono w 2009 roku przez osobę (bądź grupę osób) o pseudonimie Satoshi Nakamoto. Uważany jest on za główną kryptowalutę dominując ponad 1/3 rynku kryptowalut.

Obecnie dostępnych jest prawie 17 milionów Bitcoinów spośród 250 milionów adresów. Niemniej, jeśli choć trochę głębiej przyjrzymy się owym liczbom, zauważymy jak mało informacji one niosą.

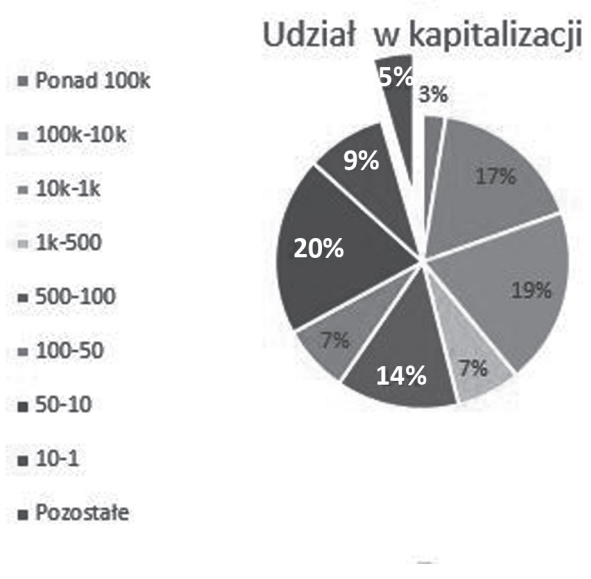
Spośród 250 milionów adresów, z pozytywnym bilansem jest jedynie 9% – 22 miliony. Analiza wartości poszczególnych adresów również ukazuje niepokojącą naturę bitcoina.

Jedynie 3 adresy mają więcej niż 100 tysięcy BTC stanowiących równowartość 3% wszystkich obecnie dostępnych.

Zaledwie 102 adresy posiadają więcej niż 10 tysięcy Bitcoinów, a kolejne 1 423 więcej niż 1 tysiąc BTC. Niemniej owe 1 528 adresów kontroluje prawie 40 procent całkowitej wartości.

Drobny wycinek z poniższego wykresu, przedstawiający 5% wszystkich Bitcoinów, jest kontrolowany przez ponad 97% adresów. Niecałe 3% adresów ma więcej niż choćby jednego Bitcoina.

Trudno jest również powiedzieć ile adresów jest przypisanych do jednej osoby, gdyż są one anonimowe.



Rysunek 4. **Udziały w Kapitalizacji Bitcoin, Własny**

Owe informacje pokazują, że rynek Bitcoina może być znacznie płytszy niż się zakłada oraz dużo bardziej podatny na gwałtowne zmiany.

Inną kryptowalutą, która wzbudza spore zainteresowanie jest Ethereum. W 2017 roku jego wartość wzrosła 130 krotnie.

W porównaniu do Bitcoina, Ethereum ma około dwukrotnie mniejszą kapitalizację , niemniej jest bardziej efektywny. Jeden blok generuje się co 15 sekund w porównaniu do 10 minut Bitcoina.

Środowisko Ethereum podaje, że technologią interesują się duże banki inwestycyjne, szczególnie w zagadnieniu MIFID II (*Markets in Financial Instruments Directive*) (Nation, 2017).

Etherum może być również wykorzystywany przy zagadnieniach finansowych, Internecie Rzeczy, przy dostawach i wycenie prądu, w zakładach bukmacherskich. Jest też wiodącą platformą do ICO (*Initial Coin Offering*) posiadając ponad 50% rynku.

Mimo większej efektywności Ethereum obecnie zmaga się z problemem przeciążenia.

W listopadzie 2017 roku przy liczbie użytkowników około 12 milionów wielkość księgi głównej wynosiła ok 16 GB. Miesiąc później, przy 13,4 milionach już 35 GB. Dla porównania Facebook posiada obecnie 3 miliardy użytkowników.

Ethereum zużywa 11 TWh rocznie, niewiele mniej niż województwo małopolskie (12 TWh).

Bitcoin, aby funkcjonować używa 0,13% energii konsumowanej na całym świecie, czyli około 29,05 TWh, podczas gdy jedna transakcja wymaga użycia 275 kWh (Jacobs, 2017). Gdyby Bitcoin był krajem, plasowałby się na 61 pozycji pod względem zużycia energii, niewiele dalej niż Hong Kong. Należy pamiętać, iż kapitalizacja Bitcoina jest na poziomie PKB Republiki Czeskiej.

Future Blockchain

Obecnie świat przechodzi kolejną, czwartą już, rewolucję przemysłową. Mimo wielkiego potencjału w rozwiązaniach zdecentralizowanych, naiwnie jest sądzić, że nie powstają nowe, bardziej efektywne narzędzia.

Jednym z takich przykładów jest *Holochain*, który ma być 10 tysięcy razy bardziej efektywny od *blockchaina*. *Holochain* jest agentocentrycznym, zdystrybuowanym systemem komputerowym, gdzie Użytkownicy nadal mogą tajnie brać udział w całym systemie mimo, iż nie są zobligowane do przechowywania pełnej informacji. (Harris-Brown, Luck i Bruck, 2018)

W dynamicznie rozwijającym się świecie, rzadko które rozwiązanie ma długoterminową technologiczną przewagę – a co za tym idzie wartość. Od tej zasady nie ma wyjątków, nawet jeśli weźmiemy pod uwagę najnowocześniejsze rozwiązania, zwłaszcza jeśli ich podstawą jest kod otwarty.

Podsumowanie

Aby dobrze skwantyfikować ryzyko potrzebne są pełne informacje. Braki w danych czy też pełne dane, ale nieodpowiadające już rzeczywistości poważnie wpływają na budowanie modelu opisującego rzeczywistość. Jeśli zbudowany model jest wadliwy, niepoprawne będą również prognozy, a co za tym idzie inwestycje będą realizowane w sposób mało efektywny.

Po trzeciej rewolucji przemysłowej rolą wywiadu było uzyskanie jak najpełniejszych danych poprzez pozyskiwanie ich z różnych źródeł. Kluczowym proble-

mem było zebranie właściwych danych na czas. Czwarta rewolucja przemysłowa stawia przed wywiadem całkiem inne wyzwania. Ilość informacji staje się obezwładniająca, a ich przetworzenie zaczyna być fizycznie niemożliwe. Z drugiej strony wśród ogromu danych ciężko wyłowić te najbardziej wartościowe. Przy braku możliwości filtracji i oceny istotności danych zaczyna się tworzyć wirtualna rzeczywistość, w której dominuje przekonanie o pełnej dostępności danych. Wyciągane wnioski wydają się logiczne, a decyzje podejmowane na ich podstawi słuszne. Wszyscy inwestorzy postępują podobnie, bo każdy przetwarza te same informacje – tworząc iluzję rynku.

Iluzja ma jednak to do siebie, że znika szybciej, niż się pojawia, pozostawiając po sobie realne straty.

Bibliografia

Calverley, J., Meder, CFA, A., & Singer, CFA, B. (2012). *Capital Market Expectations*. In C. Institute, CFA Program Curricullum (pp. 15-16). Pearson.

Darko, E. (n.d.). ICO Market Research: The Leading Blockchain Platforms Of 2017. Retrieved from icowatchlist.com: https://icowatchlist.com/blog/ico-market-research-leading-blockchain-platforms-2017/

Economist, T. (2015, Październik 31). *The great chain of being sure about things. The Economist Group Limited*.

Harris- Brown, E., Luck, N., & Bruck, A. (2018, Luty 15*). Holochain scalable agent-centric distributed computing DRAFT*.

Iansiti, M., & Lakhani, K. (2017, Styczen/Luty). *The Truth About Blockchain. Harvard Business Review, pp. 118-127.*

Jacobs, F. (2017, Grudzień 1). How Bitcoin consumes more energy than 159 individual countries. Retrieved from Bigthing.com: http://bigthink.com/strange-maps/bitcoin-consumes-more-energy-than-159-individual-countries

Markowitz, H. (1952, 7). *Portfolio Selection. Journal of Finance*, pp. 77–91.

Nation, J. (2017, Grudzień 11). Barclays, UBS, Credit Suisse Seek Ethereum Blockchain Solution For MiFID II Regulations. Retrieved from www.ethnews.com: https://www.ethnews.com/barclays-ubs-credit-suisse-seek-ethereum-blockchain-solution-for-mifid-ii-regulations

Krystian Kula*

*** mgr Krystian Kula, HSBC Servicr Delivery Polska Sp. z o.o.**

Paweł Pruszyński, Anna Nastuła

Wykorzystanie sieci TOR (*The Onion Router*) do pozyskania w sposób nielegalny danych na potrzeby szpiegostwa gospodarczego

Dynamiczny rozwój nowych technologii oraz międzynarodowy zasięg sieci informatycznej powodują wzrost znaczenia problematyki cyberprzestrzeni, a co za tym idzie i cyberprzestępczości. Innowacyjne możliwości korzystania z nowoczesnych technologii interaktywnych i mediów cyfrowych generują nowe, powszechne zagrożenia, które wynikają z działań w samej sieci jak również z inspiracji jej użytkowników. Czynności dnia codziennego coraz częściej powiązane są poprzez szereg udogodnień organizacyjno-technicznych z Internetem, co powoduje, iż człowiek *de facto* egzystuje w dwóch światach: w realnym i wirtualnym. Dodatkowo, często nieświadomie i bezwiednie, poprzez działania w sieci ujawnia swoje niekiedy nawet najskrytsze i intymne zachowania. Należy zaznaczyć, iż wszelkie działania w sieci zostawiają swój cyfrowy ślad, który w zależności od zestawienia z celem, może stać się atrakcyjnym towarem dla przestępców.

Jakże często mamy na to dowody, że właśnie takie działania ułatwiają a wręcz otwierają możliwość realizacji zadań przez osoby zajmujące się szpiegostwem gospodarczym. Szpiegostwo gospodarcze opiera się na uzyskiwaniu informacji, stanowiących największą wartość w rozwoju gospodarczym. Informacje te pozyskuje się nie tylko poprzez środki techniczne, ale przede wszystkich ze źródeł osobowych. W sieci TOR istnieją całe pokłady nielegalnie zdobytych informacji m.in. z dziedziny naukowo-technicznej, postępu (ang. *The Onion Router*) badań czy też sylwetek osób wpływających na rozwój tychże dziedzin. Naiwnością byłoby stwierdzenie, iż do tak atrakcyjnego rezerwuaru nie sięgną szpiedzy gospodarczy. Dlatego sieć TOR stała się obecnie podstawowym narzędziem w realizacji szeroko zakrojonych działań wywiadowczych.

Przyczyny popularności anonimowości w Internecie

Coraz częstsze wycieki danych ujawnione przy okazji m.in. ACTA czy ogólnoświatowego protestu hakerów *Anonymous* spowodowały, iż na plan pierwszy w międzynarodowych dyskusjach wysunął się temat prywatności w Internecie. Dodatkowo działania marketingowe dużych korporacji oraz niespotykany na taką skalę handel informacjami, pokazują, że jest to problem który należy rozpatrywać na płaszczyźnie prawnej, społecznej ale również ekonomicznej. Wzrost

świadomości użytkowników w tym zakresie generuje jednocześnie potrzebę zachowania coraz większej anonimowości w sieci, która jest często mylnie traktowana równoznacznie z prywatnością. Na tej płaszczyźnie obywatele stoją przed koniecznością odpowiedzi na pytanie o granice prywatności. Jednym z możliwych rozwiązań proponowanych przez część władz i służb specjalnych jest ograniczenie prywatności celem zachowania ładu, bezpieczeństwa oraz przeciwdziałaniu zagrożeniom. Osoby, które nie zgadzają się z takimi rozwiązaniami szukają innych sposobów i środków, dzięki którym mogą zachować anonimowość. Najpopularniejszym i najbardziej znanym obecnie narzędziem wśród innych rozwiązań dotyczących anonimowości w Internecie jest sieć TOR. Z sieci tej korzystają również osoby, które mając świadomość faktu, iż rozwój techniki spowodował wzrost możliwości cyfrowej inwigilacji, przeciwstawiają się temu zjawisku. Niestety ze względu na ogólnoświatowy charakter cyberprzestrzeni obce państwa mogą pod pretekstem np. walki z terroryzmem, szpiegować obywateli innych krajów. O ile sytuacja ograniczenia prywatności ze względu na dobra obywatelskie i bezpieczeństwo własnego kraju znajduje zwolenników, o tyle szpiegostwo innych krajów budzi sprzeciw.

Na podkreślenie zasługuje, iż wykorzystanie sieci TOR, jak każdego innego narzędzia, zależy wyłącznie od legalnych bądź nielegalnych intencji użytkownika.

Sieć TOR jest jednym z najważniejszych i prawdopodobnie najczęściej implementowanych narzędzi przez użytkowników dbających o swoją anonimowość na całym świecie. Istnieją również inne aplikacje tzw. technologie zwiększające bezpieczeństwo danych, które pomagają internautom zachować anonimowość wcyberprzestrzeni[1]. Klasyfikacja takich technologii może przybierać różne formy, ale zazwyczaj występują one w kategorii: serwerów pośredniczących (*proxy*), tunelowania oraz wirtualnych sieci prywatnych (VPN), obejścia blokady systemu nazw domenowych (DNS) oraz trasowania cebulowego[2]. Sieć TOR, implementująca trasowanie cebulowe trzeciej generacji, jest najbardziej popularnym narzędziem wykorzystywanym przez przestępców.

Struktura Internetu

Korzystając z sieci Internet użytkownicy, w swych codziennych aktywnościach takich jak wyszukiwanie i przeglądanie stron WWW, korzystanie z serwisów aukcyjnych, portali społeczności czy też poczty elektronicznej, przenikają jedynie do jej niewielkich zasobów. Ta część Internetu określana jako *Surface Web* (Internet powierzchniowy) lub clearnet stanowi jedynie czubek góry lodowej wielowarstwowej sieci. Natomiast jej pozostała, znacznie większa i jednocześnie niewidoczna dla użytkownika część znajduje się pod wirtualną linią wody. Jest to

1 I. Golberg, *Privacy Enhancing Technologies for the Internet III:Ten Years Later*, in Alessandro Acquisti, Stefanos Gritzalis, Costas Lambrinoudakis&Sabrina De Capitani di Vimercati, ed., Digital Privacy: *Theory, Technologies and Practices*, New York, London:Auerbach Publications 2007.

2 Cormac Callanan, Hein Dries -Ziekenheiner, Alberto Escudero-Pascual, Robert Guerra*, Lepaing Over the Firwall: A Review of Censorship Circumvention Tools*, Freedom House 2011

Deep Web czyli głęboka sieć zwana inaczej siecią ukrytą (Hiden Web). Określenie *Deep Web* wprowadził i spopularyzował w 2001 roku Mike Bergman, autor przełomowej pracy opublikowanej w Journal of Electronic Publishing[3]. Treści, które funkcjonują w obrębie sieci niewidzialnej, cechuje wysoka jakość informacji, rzetelność i profesjonalizm[4], z uwagi na fakt, iż często powstają one z inicjatywy ekspertów i specjalistów z danej dziedziny, którzy pod osłoną anonimowości z większą odwagą prezentuje swoje poglądy. Głęboki Internet zawiera strony nie indeksowane przez najpopularniejsze wyszukiwarki działające w *clearnet.* W jego zasobach odnajdziemy również konta chronione hasłami, serwisy archiwizujące stare wersje stron internetowych. Znajdują się tu również duże bazy danych, zbiory biblioteczne czy testrony Narodowej Agencji Aeronautyki i Przestrzeni Kosmicznej (ang. NASA).

Deep Web często mylony jest z *Darknetem* (ang. ciemnym internetem, czarnym internetem), który *de facto* stanowi jego najgłębszą część. *Darknet* to sieć anonimową, w której połączenia odbywają się wyłącznie pomiędzy zaufanymi osobami, czasami określanymi jako Przyjaciele (F2F). *Friend-to-Friend* to typ sieci *peer-to-peer*, w której użytkownicy dokonują bezpośrednich połączeń wyłącznie z osobami, które znają. W sieci mogą być stosowane uwierzytelnienia danego użytkownika za pomocą haseł lub podpisów cyfrowych. W ramach *Darknetu* funkcjonują zdecentralizowane anonimowe sieci takie jak I2P (*Invisible Internet Project*), *Freenet* czy najbardziej popularna wśród nich sieć TOR (*The Onion Router*). Ciemny Internet umożliwia tworzenie stron, portali, forów i społeczności w pełni zabezpieczonych przed dostępem z wyszukiwarek funkcjonujących w *clearnet*. Do tych treść mają dostęp wyłącznie osoby znające specyficzny adres szukanej strony (indywidualny alias *.onion*), posiadające odpowiednie oprogramowanie szyfrujące informacje oraz zainstalowaną przeglądarkę TOR. To właśnie w ukrytych serwisach w sieci TOR można znaleźć wszystko to co jest nielegalne, począwszy od dziecięcej pornografii, handlu ludzkimi organami, sklepów z narkotykami i bronią po obrót materiałami rozszczepialnymi.

Użytkownicy korzystając z Internetu nawet nie zdają sobie sprawy z tego, jak wiele elementów, z pozoru drobnych, po złożeniu ich w całość, pozwala na zbudowanie profilu osobowego. To tak jak malarz tworzący obraz mozaikowy układa go z drobnych dotknięć pędzla. Pojedyncze naniesienia nie znaczą nic i są nieciekawe, natomiast po złożeniu stanowią interesujący, pełny obraz. Tak właśnie działa Internet, a szczególnie sieć TOR wykorzystująca te drobne szczegóły do charakterystyki osoby, która nie mając nawet świadomości tworzy *de facto* swoją indywidualną wirtualną sylwetkę. Można stwierdzić z dużą dozą prawdopodobieństwa graniczącą z pewnością, że wykorzystana ona zostanie nielegalnie przeciwko użytkownikowi.

3 M. Bergman, *The Deep Web: Surfacing Hidden Value*, Journal of Electronic Publishing 2001.

4 J. Devine, F. Egger-Sider, Beyond Google: *The Invisible Web in the Academic Library*, The Journal of Academic Librarianship 2004, vol. 30, s. 265-269

Historia oraz zasady działania sieci TOR

Sieć TOR to wirtualna sieć komputerowa implementująca trasowanie cebulowe trzeciej generacji, która zapobiega analizie ruchu sieciowego i w konsekwencji zapewnia użytkownikom praktycznie anonimowy dostęp do zasobów Internetu. Sieć Tor została zaprojektowana w 2002 roku przez Laboratorium Badań Marynarki Wojennej Stanów Zjednoczonych w celu ochrony informacji w ramach agencji rządowych. Podstawowym celem projektu było zapewnienie bezpieczeństwa rządowej komunikacji. W pierwszym okresie jej działania serwery tworzące sieć były umiejscowione jedynie w Stanach Zjednoczonych oraz Niemczech. Projekt w latach 2004-2005 został oddany pod opiekę fundacji „Electronic Frontier Foundation", organizacji działająca na rzecz wolności obywatelskich[5]. Obecnie rozwojem sieci TOR zajmuje się organizacji non-profit „The TOR Project" o charakterze badawczo-naukowym, która sponsorowana jest m.in. przez rząd Stanów Zjednoczonych, amerykańskie instytucje badawcze, korporację Google oraz osoby prywatne[6]. Celem sieci TOR jest zapewnienie maksymalnej możliwej anonimowości jej użytkowników dzięki wielowarstwowemu szyfrowaniu danych i przesyłaniu ich przez szereg losowo wybranych węzłów sieciowych nazywanych routerami lub węzłami cebulowymi. Urządzenia te utrzymywane są przez osoby prywatne wspierające rozwój projektu TOR. Zabezpieczenie ruchu sieciowego w sieci TOR następuje w kilku etapach. Wejście do sieci rozpoczyna się od uruchomienia aplikacji TOR, której wygląd bazuje na popularnym programie Mozilla Firefox. Po jej uruchomieniu użytkownik pobiera listę węzłów wejściowych – z ang. *Entry Node* – z oficjalnego serwera. Pierwszy serwer proxy podmienia adres IP użytkownika na własny[7]. Router cebulowy w pierwszej kolejności usuwa jedną warstwę szyfru celem uzyskania dostępu do kolejnego celu danych i następnie przesyła dalej pakiet danych do innych, losowych węzłów cebulowych, zwanych również przekaźnikowymi – z ang. *Rely Node*. Gdy ostatnia warstwa zostaje odszyfrowana, pakiet danych dociera do serwera docelowego. Połączenie pomiędzy ostatnim węzłem sieciowym – z ang. *Exit Node* – zwanym węzłem wyjściowym jest jawne. Rysunek numer 1 przedstawia zasady połączeń w sieci TOR.

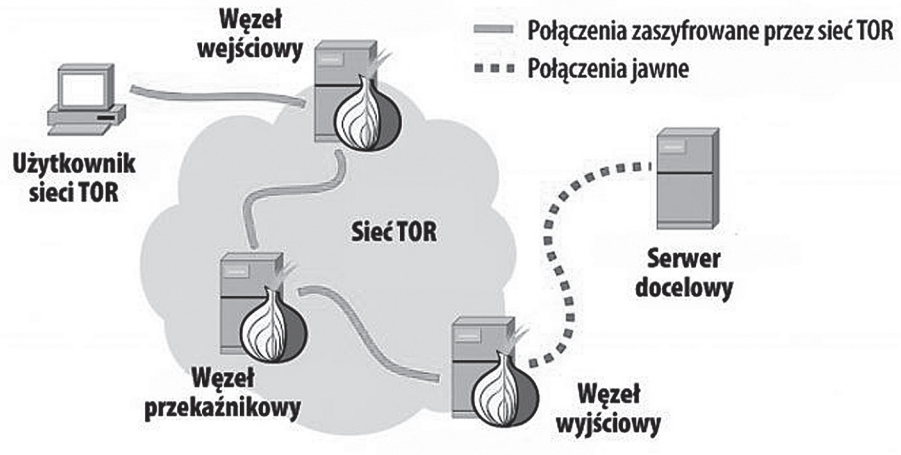
Tym sposobem nadawca pakietu danych pozostaje anonimowy, ponieważ każdy pośrednik zna tylko lokalizację bezpośrednio poprzedzających i następujących węzłów[8]. Taka budowa sieci TOR zapewnia anonimowość jej użytkowników, w tym usługodawcom czy twórcom stron internetowych jej dedykowanych. Sieć TOR nie szyfruje natomiast danych przesyłanych przez węzeł wyjściowy do zasobów sieciowych, dlatego każdy węzeł wyjściowy ma potencjalną możliwość przechwycenia dowolnych danych, które przezeń są przesyłane bez zabezpieczenia.

5 www.onion–router.net/History.html

6 https://www.torproject.org/about/sponsors.html.en

7 https://www.komputerswiat.pl/artykuly/redakcyjne/tor-wszystko-co-trzeba-wiedziec-o-sieci-cebulowej/lp69phy

8 Goldschlag D., Reed M., Syverson P. (1999.) *Onion Routing for Anonymous and Private Internet Connections*, Onion Router,



Rysunek 1. Zasady działania TOR (opracowanie własne na podstawie źródła)

Źródło : https://www.extremetech.com/internet/188095-portal-is-a-travel-router-that-offers-instant-anonymity-after-one-time-setup

Mechanizmy działania sieci TOR przeciwdziałają podstawowej formie inwigilacji internetowej, jaką jest analiza ruchu sieciowego (*ang. traffic analysis*). Jednym z zastosowań tejże analizy jest identyfikacja systemów i użytkowników korzystających z sieci publicznej. Wiedza o źródłach oraz celach ruchu sieciowego pozwala na śledzenie użytkowników, pozyskanie informacji o ich preferencjach i zainteresowaniach. W konsekwencji informacje te mogą mieć wpływ na kształtowanie się cen towarów i usług. Podmioty gospodarcze działające na rynku *e-commerce* mogą różnicować ceny np. w oparciu o miejsce zamieszkania klienta.

Bitcoin

Środkiem płatniczym, który służy do rozliczeń wszelkich transakcji w sieci TOR, są kryptowaluty, w tym najpopularniejsza z nich - Bitcoin. Za nielegalne usługi i towary można dokonać płatności również przy użyciu *paysafecard*. Nie ma jednoznacznych odpowiedzi co do genezy powstania waluty Bitcoin, przyjmuje się jednak, że osobą lub grupą osób, która stworzyła koncepcje algorytmu Bitcoin i jego wykorzystywania w pozagotówkowych transakcjach rozliczeniowych był Satoshi Nakamoto. Istnieje domniemanie, iż twórcą Bitcoina może być również Ross Ulbricht - właściciel największego i najpopularniejszego do tej pory serwisu w sieci TOR o nazwie „Silk Road" (z ang. Jedwabny Szlak). Bitcoin określany jest jako e-waluta drugiej generacji[9]. Nazwa odnosi się do systemu informatycznego umożliwiającego dokonywanie płatności oraz przelewów w tej walucie. Jest to algorytm składający się z kryptograficznego ciągu znaków po-

9 E. Chrabonszczewska, *Bitcoin - nowa wirtualna globalna waluta?*, Zeszyty Naukowe Kolegium Gospodarki Światowej SGH 2013, nr 40, s. 52.

siadający określoną wartość[10]. Bitcoin używa zdecentralizowanej, rozproszonej bazy danych, która jest rozprowadzana pomiędzy węzłami sieci *peer-to-peer* oraz przechowuje transakcję i jej historię. Określenie *peer-to-peer* opiera się na modelu komunikacji w sieci komputerowej, który zapewnia wszystkim hostom te same uprawnienia. Oznacza to, iż nie ma jednego centralnego punktu do emitowania pieniędzy czy monitorowania transakcji a poszczególne zadania są wykonywane kolektywnie przez sieć, do której waluta jest organicznie przywiązana. Prywatne klucze kryptograficzne których używa się do autoryzowania transakcji są zapisywane na komputerze osobistym w stworzonym do tego celu specjalnym oprogramowaniu zwanym plikiem portfela lub na zewnętrznym serwisie zajmującym się obsługą tego typu portfeli. Autoryzacja transakcji, zabezpieczenie przed podwójnym wydaniem tych samych monet czy cofnięciem transakcji odbywa się również w zdecentralizowanym środowisku wirtualnego systemu transakcyjnego. Bitcoin jest walutą tworzoną przez samych użytkowników bez pośrednictwa banku czy też innej instytucji, która występuje wyłącznie w Internecie. Ze względu na fakt światowej ogólnodostępności Internetu stosowany jest zarówno w krajach rozwiniętych jak i rozwijających się. Zakłada się, iż liczba Bitcoinów jest wartością skończoną na poziomie 21 milionów, a sam system emisji Bitcoina został wyposażony w specjalny kod, który uniemożliwia wzrost ich liczby. Wartość Bitcoina opiera się wyłącznie na popycie i podaży, jest niezależna od któregokolwiek z krajów, waluty, rządu czy instytucji. Jego siła oparta jest na koniunkturze m.in. reklamowej, która wytwarza potrzebę posiadania „modnej", szeroko komentowanej waluty. Fakt oderwania Bitcoina od wszelkich instytucji i państwowych organizacji jest często atrakcyjny dla młodych ludzi, dla których jest on wręcz ideologicznym środkiem w obrocie gospodarczym.

Posługiwanie się walutą Bitcoin generuje jednak szereg zagrożeń. Na płaszczyźnie technicznej są to ataki hakerskie oraz możliwość umieszczenia w dokonywanych transakcjach dodatkowych, nielegalnych plików m.in. pornograficznych. Należy również brać pod uwagę prawdopodobieństwo znalezienia potencjalnych błędów w samym systemie i wykorzystania ich przez zawodowych hakerów. Na płaszczyźnie ekonomicznej natomiast pojawiają się problemy związane ze spekulowaniem wartością czy nieodwracalnością transakcji oraz brakiem powiązania tejże waluty z wiarygodnością gospodarczą. Bitcoina nie można również ubezpieczyć, tak jak można to uczynić m.in. z gotówką przechowywaną w bankowym depozycie. Obrót wirtualnymi walutami obarczony jest również dużym ryzykiem. Wynika to z faktu, iż brak jest odpowiednich form nadzoru na emitowaną wirtualną walutą oraz jednolitych norm regulujących jej status prawny Wszystkie te cechy powodują jednak, iż dla osób oraz podmiotów gospodarczych, które nie mogą dokonywać transferów pieniężnych za pomocą tradycyjnych kont bankowych oraz chcą pozostać anonimowe jest to idealny środek do przeprowadzania nielegalnych transakcji. W połączeniu z technikami anonimizującymi, wynikającymi z

10 M. Szymankiewicz, *Bitcoin. Wirtualna waluta Internetu*, Warszawa 2014, s. 33.

mechanizmów działania sieci TOR, stanowi istotną ochronę wszelkiego rodzaju działalności przestępczej.

Różnice pomiędzy wywiadem gospodarczy a szpiegostwem gospodarczym

Konkurencyjność w gospodarce to obecnie wyścig z czasem o pozyskanie informacji, przy czym w ich bogactwie i różnorodności bardzo istotna jest systematyczność działań, odrzucenie elementów dezinformacyjnych oraz przygotowanie jasnej i syntetycznej analizy pozyskanych materiałów. Dlatego też przedsiębiorcy coraz częściej sięgają do nowoczesnych technologii i usług osób, często hakerów, posiadających specjalistyczną wiedzę w tej dziedzinie. Wywiad gospodarczy określany jest jako działalność, która ma na celu zaspokajanie potrzeb związanych z pozyskiwaniem, przetwarzaniem i udostępnianiem informacji o rynku, otoczeniu gospodarczym, obecnych i potencjalnych konkurentach, ich działaniach, a także zapobieganiu wypływowi strategicznych i istotnych dla danego podmiotu informacji. Wywiad gospodarczy narodził się w społeczeństwem informacyjnym, korzysta z dynamicznie działającego rynku informacji i wraz z postępem technologicznym stopniowo rozwija wachlarz swoich usług i możliwości[11]. Wywiad gospodarczy stanowi profesjonale i skuteczne narzędzie zarządzania strategicznego i w tym kontekście powinien być postrzegany. Sławomir Stępień zauważa, że umiejętne dostosowanie się przedsiębiorstw do zmieniających się warunków, a także wpływanie na otoczenie, stało się podstawową szansą i receptą na poprawę pozycji konkurencyjnych i wzmocnienie udziałów w rynku[12]. Pojęcie „wywiadu gospodarczego" budzi u niektórych osób złe skojarzenia związane z inwigilacją i szpiegostwem, przy jest to działalność legalna i etyczna. Nadal mała liczba menedżerów kojarzy to pojęcie z pozyskiwaniem, ochroną, przetwarzaniem i rozpowszechnianiem informacji. Dopóki w Polsce nie rozwinie się kompetentna edukacja oraz rozpowszechnianie informacji na temat skutecznych i etycznych metod wyszukiwania informacji, nadal te zjawiska mogą być postrzegane przez negatywny pryzmat.

Szpiegostwo gospodarcze to pozyskiwanie tajemnic handlowych firm, konkurentów biznesowych, przechwytywanie wykorzystywanych technologii produkcji, wzorów, formuł i procesów wytwórczych oraz zdobywanie badań i planów rozwoju produktów, a także planów ekspansji rynkowej[13]. Szpiegostwo przemysłowe jest najczęściej związane z nowymi branżami przynoszącymi bardzo wysokie zyski, jak branża IT, farmaceutyczna, kosmetyczna czy nawet samochodowa. Jest do działanie niejawne i spenalizowane przez polskie prawodawstwo. Szpiegostwo gospodarcze do osiągnięcia zamierzonych celów wykorzystuje osobowe źródła informacji, wywiad teleinformatyczny czy elektroniczny. W związku z faktem, iż konkurencja zwłaszcza w nowych technologiach polega na szybkości

11 Moryś A., *Geneza i ewolucja wywiadu gospodarczego. Część pierwsza,* [w:] iNFOTEZY Wol. 1, Nr 1 (2011).

12 Stępień, S. (2002), *Rola i sposoby pozyskiwania informacji marketingowej w zmieniającej się rzeczywistości funkcjonowania przedsiębiorstw na polskim rynku.* Materiały i Prace Instytutu Funkcjonowania Gospodarki Narodowej, T. 83, s. 89.

13 https://pl.wikipedia.org/wiki/Szpiegostwo_gospodarcze

działania i rozbudowanych pracach badawczo-rozwojowych prowadzonych w laboratoriach, co wiąże się ze znacznymi kosztami, coraz częściej w tych branżach sięga się do wykradania osiągnięć konkurencji. Dzięki takim działaniom, które są i niemoralne i niezgodne z prawem podmioty osiągają: przyspieszenie technologiczne, uzyskanie przewagi nad konkurencją oraz, chyba najważniejsze, znaczne obniżenie kosztów wprowadzenia najnowszych rozwiązań w poszczególnych branżach.

Szpiegostwa gospodarcze a atrakcyjność sieci TOR

Obecnie informacja jest elementem najważniejszym przy podejmowaniu decyzji o znaczeniu gospodarczym. Wynika to z faktu, iż jest ona wartościowa zarówno mentalnie, jak i materialnie. Dobra informacja przyczynia się do podwyższenia jakości podejmowanych decyzji i ma bezpośredni wpływ na rozwój przedsiębiorstwa. Odpowiednio opracowana kształtuje przyszłość przedsiębiorstwa, stopień jego aktywności i złożoność warunków działania[14].

Czarny Internet oprócz wywiadu gospodarczego, który jest legalną formą, roi się od oferentów, którzy zajmują się szpiegostwem gospodarczym. Forma ta jest naruszeniem wszelkich norm prawnych.

Już w 2013r. firma Kaspersky Lab w swym Biuletynie przedstawiła prognozy dotyczące cyberbezpieczeństwa, w których sygnalizowała, iż: „Firmy będą musiały uciekać się do cyberszpiegostwa biznesowego, aby mogły pozostać konkurencyjne, ponieważ ich rywale już teraz stosują szpiegostwo w celu uzyskania przewagi konkurencyjnej. Niektóre firmy mogą nawet szpiegować struktury rządowe, jak również własnych pracowników, partnerów i dostawców”[15]. Nie da się ukryć, iż w tym sformułowaniu było dużo racji, gdyż wywiadownie gospodarcze zaczynają się przeistaczać w centra szpiegostwa gospodarczego, co oczywiście jest nielegalne i niemoralne oraz narusza wiele norm prawnych. I tu ponownie pojawia się doskonale narzędzie dla szpiegów, jakim jest sieć TOR, która może bezpośrednio nie służy do wykradania informacji, ale buduje swoistą strukturę szpiegowską, która w pełni jest w stanie zrealizować wszelkie działania jednoznacznie wypełniające znamiona szpiegostwa gospodarczego. Ukryte serwisy w sieci TOR są idealnym miejsce do pozyskania interesujących informacji a dodatkowo system anonimowej płatności zapewnia bezimienność potencjalnych szpiegów.

Przykładowo w sieci TOR w serwisie „Satriale’s Forum”[16] można uzyskać informacje o spółkach, dzięki czemu ewentualna konkurencja ma ułatwione zadanie w rozpoznaniu sytuacji finansowej czy stabilność kadry danego podmiotu. Wraz z nowymi potrzebami społeczności czarnej sieci powstają również nowe rynki, na których użytkownicy dokonują transakcji kupna sprzedaży poufnych

14 Siemieniuk, N., Ignatowska, B. (1999), *Aspekty informacyjne wywiadu gospodarczego w przedsiębiorstwie*. Optimum, nr 2, s. 142–144.

15 https://www.securelist.pl/analysis/7263,kaspersky_security_bulletin_2013_prognozy.html

16 http://itcontent.eu/strony-tor/

informacji z korporacji. Tego typu oferty pojawiały się na nieaktywnym już forum internetowym o nazwie „Enigma". Handel produktami i cyfrowymi informacjami wydaję się mniej ryzykowny, dodatkowo mechanizmy anonimizujące, na których opiera się działanie sieci TOR powodują, iż nielojalni pracownicy motywowani chęcią zemsty czy zarobku coraz częściej wykradają informacje z firm, w których pracują[17]. Anonimowe fora przestępcze niemal powszechnie pomagają obniżyć bariery wejścia dla potencjalnych cyberprzestępców. Dodatkowo anonimowość kryptowaluty zwiększa dostęp nielegalnych towarów dla zwykłych ludzi, którzy często skuszeni prostotą uzyskania czegoś zakazanego stają się w świetle prawa przestępcami.

W sieci TOR funkcjonują też strony oferujące wyspecjalizowane usługi hakerskie. Można tu nabyć m.in. programy szpiegujące, konie trojańskie, maszynki do rozsyłania spamu oraz narzędzia do szyfrowania exploity 0-day, czyli dziury w popularnym oprogramowaniu i systemach, do których nie ma jeszcze łatek. Hakerzy oferują wykradanie informacji zarówno od osób fizycznych, jak i firm. Wykorzystują również pozyskane nielegalnie bazy danych do szantażu poszkodowanych osób i instytucji. Popularną usługą jest „Spear phishing", czyli w pełni spersonalizowana i poprzedzona wywiadem środowiskowym bardziej wyrafinowana forma standardowego ataku phishingowego. Celem tych ataków jest kradzież poufnych informacji oraz tajemnic handlowych[18].

Podsumowanie

Dynamiczne zmiany oraz rozwój nowych technologii powodują, iż kontrola działań w architekturze cyberprzestrzeni jest dużym wyzwaniem zarówno dla organów ścigania, jak i struktur legislacyjnych. Dlatego już dziś należy przeciwdziałać wszelkim patologiom tworzącym się i wykorzystującym sieć TOR. W przeciwnym razie to nie użytkownicy Internetu będą decydować o swoim losie, ale decyzje takie pozostawać będą w rękach przestępców. W zdrowym społeczeństwie odsetek zachowań kryminalnych powinien pozostać tylko marginesem w stosunku do zgodnego z prawem postępowania.

Paweł Pruszyński*, Anna Nastuła**

17 https://news.bitcoin.com/trading-corporate-secrets-darknet/

18 http://www.benchmark.pl/aktualnosci/spear-phishing-co-to-jest-ataki-coraz-popularniesze.html

*** gen. bryg. Paweł Pruszyński, b. zastępca Szefa Agencji Bezpieczeństwa Wewnętrznego**

**** mgr Anna Nastuła, doktorantka Uniwersytetu Opolskiego**

Maciej Karwas

Współczesny wymiar wywiadu i kontrwywiadu w świetle nielegalnego obrotu towarami i technologiami o znaczeniu strategicznym

Streszczenie

Materiał podejmuje oraz przybliża problematykę funkcjonowania wywiadu i kontrwywiadu w aspekcie rozpoznawania zagrożeń związanych z nielegalnym obrotem towarami i technologiami o znaczeniu strategicznym dla bezpieczeństwa z uwzględnieniem otoczenia biznesowego. Zawarte w artykule treści są okazją do szerszego poznania i zrozumienia roli cywilnych i wojskowych służb specjalnych, jaką w funkcjonowaniu państwa odgrywają służby specjalne zwłaszcza w obszarze monitorowania procesów gospodarczych związanych z obrotem towarami i technologiami o znaczeniu strategicznym dla bezpieczeństwa państwa. Rola wywiadu i kontrwywiadu w formułowaniu polityki gospodarczej jest również istotnym elementem współczesnych relacji otoczenia biznesowego w wymiarze krajowym i międzynarodowym z otoczeniem administracji publicznej. Stanowi on punkt wejścia do problematyki funkcjonowania służb wywiadu i kontrwywiadu, zarówno z punktu widzenia analityka, naukowca czy decydenta, będąc jednocześnie spójnym studium procesów wywiadowczych i kontrwywiadowczych w omawianym zakresie.

* * *

Problemy bezpieczeństwa międzynarodowego oraz zagrożeń dla stabilności pokoju oraz szeroko rozumianego rozwoju cywilizacyjnego pozostawały i nadal pozostają przedmiotem szczególnej uwagi polityków, naukowców, ekspertów w tym akademickich oraz społeczności międzynarodowej. Wśród wielu zagrożeń dla międzynarodowego pokoju i bezpieczeństwa w wymiarze zewnętrznym i wewnętrznym można identyfikować między innymi proliferację broni masowego rażenia i środków jej przenoszenia. Zjawisko proliferacji broni masowego rażenia i środków jej przenoszenia jest jednym z kluczowych instrumentów terroryzmu międzynarodowego wykorzystywanego przez państwa, a także przez podmioty niepaństwowe w osiąganiu swoich politycznych zamierzeń i celów. Materiał będzie próbą dokonania opisu problematyki i zagadnień związanych z proliferacją broni masowego rażenia i środków jej przenoszenia ze szczególnym uwzględ-

nieniem mechanizmów krajowego systemu kontroli towarów strategicznych jako elementu kształ**towania bezpieczeństwa państwa.** Istotą i nadrzędnym celem funkcjonowania wspomnianego sytemu w każdym jego sektorze jest uniemożliwienie bezprawnego pozyskiwania towarów i technologii strategicznych przez te podmioty, które dążą do wzmocnienia swojej pozycji międzynarodowej nie zawsze postępując zgodnie z *duchem pokoju międzynarodowego.*

Nielegalny obrót towarami i technologiami o znaczeniu strategicznym dla bezpieczeństwa państwa – definicja problemu

Na początku XXI wieku problemy bezpieczeństwa międzynarodowego oraz zagrożenia dla stabilności i szeroko rozumianego rozwoju cywilizacyjnego nadal pozostają przedmiotem szczególnej uwagi polityków, ekspertów oraz społeczności międzynarodowej. Wśród wielu zagrożeń dla międzynarodowego pokoju obok terroryzmu międzynarodowego należy identyfikować również proliferację broni masowego rażenia i środków jej przenoszenia, zwłaszcza w kontekście możliwości ich przechwycenia przez ugrupowania terrorystyczne.

Teza ta znalazła swoje odzwierciedlenie nie tylko w wielu aktach prawa międzynarodowego i krajowego, ale też w dokumentach strategicznych[1] dotyczących bezpieczeństwa Polski[2] i innych państw oraz takich organizacji, jak NATO czy UE[3].

Trzeba bowiem zauważyć, że koniec zimnej wojny spowodował multilateralizację stosunków międzynarodowych, która oprócz wszelkich swych pozytywnych efektów, ożywiła zamrożone dotychczas konflikty regionalne i sprzyjała kształtowaniu się warunków dogodnych do rozprzestrzeniania broni atomowej, biologicznej, chemicznej oraz środków jej przenoszenia (w tym towarów i technologii podwójnego zastosowania[4] wykorzystywanych przy produkcji broni BMR) z państw je posiadających do państw lub innych podmiotów międzynarodowych dążących do jej pozyskania.

Polska, jako sygnatariusz wielu umów międzynarodowych i konwencji dotyczących zapobiegania proliferacji broni masowego rażenia i kontroli towarów strategicznych, swoje zadania w tym obszarze realizuje głównie w oparciu o aktywność na forum Unii Europejskiej. Jako uczestnik procesów globalnych RP śledzi międzynarodową debatę w sferze rozbrojenia i nieproliferacji, szczególnie rozmowy rosyjsko-amerykańskie o redukcji zbrojeń strategicznych. Głębokie redukcje arsenałów państw posiadających największe zapasy broni jądrowej, mogą mieć bowiem duże znaczenie w doprowadzeniu do stopniowego rozbrojenia jądrowego, z udziałem wszystkich państw.

1 Strategia Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej, Warszawa 2014.

2 Strategia Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej 2007.

3 Bezpieczna Europa w Lepszym świecie – Europejska Strategia Bezpieczeństwa, 2003 r., Rada Europejska, Bruksela 2003

4 Towary i technologie podwójnego zastosowania zwane inaczej *dual-use* zostały zdefiniowane w ustawie z dnia 29.11.2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa; Dz.U. 2000, nr 119, poz. 1250 z późn. zm..

Współcześnie nie można sobie wyobrażać nowocześnie rozwijającego się kraju i społeczeństwa bez sprawnie działającego systemu bezpieczeństwa państwa, w którego tło wpisuje się kwestia zapobiegania proliferacji BMR uwzględniająca kontrolę towarów strategicznych.

Ta wieloaspektowość objawia się również w wymiarze międzynarodowym, w tym w ramach członkostwa w Unii Europejskiej, ONZ, NATO oraz innych organizacjach międzynarodowych.

W Polsce aktualnie istniejący system zapobiegania proliferacji BMR skoncentrowany jest wokół podsystemu wewnętrznego i zewnętrznego. Podsystem wewnętrzny to ustawowa działalność służb specjalnych (wywiadu i kontrwywiadu cywilnego i wojskowego) i instytucji zajmujących się zapobieganiem i przeciwdziałaniem proliferacji BMR.

Natomiast podsystem zewnętrzny to międzynarodowa wymiana informacji o monitorowaniu działalności podmiotów zaangażowanych w rozprzestrzenianie BMR. Ten aspekt polityki międzynarodowej w ostatnich latach nabrał istotnego znaczenia w związku z tendencjami wykorzystania BMR przez kraje tzw. podwyższonego ryzyka. Stąd też państwa położyły duży nacisk na wprowadzenie skutecznych mechanizmów kontroli obrotu, a przede wszystkim kontroli eksportu towarów strategicznych, warunkując tym samym dostęp do ich towarów i technologii. Zatem z punktu widzenia podstawowych interesów RP sprawnie działający system zapobiegania proliferacji BMR i środków jej przenoszenia wynika z trzech podstawowych przyczyn:

- pierwszą z nich jest zapewnienie bezpieczeństwa państwa, które w dużej mierze zależy od skuteczności funkcjonowania krajowego systemu kontroli towarów strategicznych, w konsekwencji zaś od jego współpracy w ramach międzynarodowych aktów prawnych, czy umów regulujących kwestie kontroli obrotu towarami strategicznymi. Współpraca ta ma wielki wpływ na ograniczenie rozprzestrzeniania BMR i przeciwdziałania gromadzeniu przez kraje ryzyka broni konwencjonalnych i niekonwencjonalnych, stanowiących zagrożenia dla społeczności międzynarodowej, a tym samym dla zewnętrznego bezpieczeństwa Polski. Ograniczenie możliwości niekontrolowanego transferu tego rodzaju materiałów przez i na terytorium RP, jako wynik funkcjonowania skutecznego sytemu kontroli eksportu może mieć znaczący wpływ na zwiększenie bezpieczeństwa wewnętrznego poprzez utrudnienie dostępu do tych materiałów przez nieformalne struktury funkcjonujące na terenie kraju;
- druga przyczyna jest konsekwencją integracji ze strukturami politycznymi i ekonomicznymi UE i NATO. Państwa tych organizacji stanowią trzon reżimów antyproliferacyjnych, mają wspólne uregulowania w dziedzinie kontroli eksportu, wymagają, aby kandydaci do przystąpienia do ich struktur dostosowali się do obowiązujących w tym zakresie standardów.
  Polska, dążąc do pełnej integracji, wdrożyła system kontroli i opublikowała ujednoliconą listę kontrolną towarów i technologii podwójnego zastosowania, co miało duże znaczenie w uzyskaniu statusu wiarygodnego partnera w zakresie międzynarodowego obrotu nowoczesnymi technologiami;

- trzecia przyczyna wynika z konieczności uzyskania swobodnego dostępu do nowoczesnych towarów i technologii, których wykorzystanie w działalności przemysłu krajowego będzie decydowało o możliwości zwiększenia konkurencyjności wytwarzanych przez niego wyrobów na rynkach międzynarodowych, stanowiąc w ten sposób istotny element decydujący o rozwoju ekonomicznym kraju.

Pomimo funkcjonującego obecnie sytemu nadal nie można wykluczyć zagrożenia RP terroryzmem międzynarodowym, którego aktorzy państwowi i pozapaństwowi mogą mieć realny dostęp do broni masowego rażenia, bądź do możliwości jej wytworzenia. Zatem działania nasze powinny być realizowane między innymi pod kątem udoskonalenia identyfikowania ewentualnych transferów uzbrojenia oraz obrotu towarów i technologii podwójnego zastosowania, które mogłyby posłużyć do bezpośrednio do działań terrorystycznych lub trafić do któregoś z ośrodków podejrzewanych o wspieranie międzynarodowego terroryzmu.

Powyższe tezy były między innymi głównym przedmiotem debaty międzynarodowej w trakcie Szczytu Nuklearnego w Waszyngtonie[5], w dniach 29 marca – 1 kwietnia br. w z udziałem Prezydenta RP Andrzeja Dudy. Celem uczestników Szczytu Nuklearnego, który odbył się z inicjatywy Prezydenta USA Baracka Obamy, było wypracowanie takich rozwiązań strategicznych na szczeblu politycznym, które zredukują potencjał światowego arsenału nuklearnego.

Między innymi koncepcja B. Obamy zakłada zwiększenie wysiłków społeczności międzynarodowej w celu wzmocnienia realnej kontroli nad proliferacją materiałów rozszczepialnych, które mogą dostać się w ręce ugrupowań terrorystycznych. Ponadto w ocenie Prezydenta USA zagrożenie dla światowego pokoju i międzynarodowej stabilności stanowi kalifat powstały na części terytorium Iraku i Syrii, który dąży do pozyskania materiałów rozczepianych celem wyprodukowania tzw. „brudnej bomby". Z danych przygotowanych na waszyngtoński szczyt wynika, iż w opracowanym rankingu, który szacuje bezpieczeństwo nuklearne w 24 atomowych krajach, Polska zajmuje wysokie czwarte miejsce – przed Niemcami, Francją czy nawet USA. Wynika to przede wszystkim z faktu, że Polska przerobiła swój jedyny reaktor atomowy w Świerku. Jeszcze do niedawna jego paliwem był wysoko wzbogacony uran, który można było wykorzystać do produkcji bomby atomowej. Teraz reaktor działa na nisko wzbogacony uran, zawierający poniżej 20 proc. rozszczepialnego izotopu U235 (do wyprodukowania bomby potrzeba powyżej 80 proc.) wykorzystywany w celach medycznych.

Najbardziej wymiernym efektem waszyngtońskiego szczytu była deklaracja, którą złożyli Prezydenci USA i Chin.

Po spotkaniu w Białym Domu Barack Obama i Xi Jinping ogłosili, że wspólnie będą próbować okiełznać Koreę Północną, która co jakiś czas przeprowadza próby atomowe lub urządza testy rakiet balistycznych. Podejmowane przeciwdziałania przynoszą – jak dotąs – połowiczne rezultaty.

5 Źródło: www.gazeta.pl. M. Zawadzki. *Rozbrojenie atomowe – marzenie Obamy z* 02.04.2016.

Warto dodać, iż na Szczycie Waszyngtońskim nie byli obecni przedstawiciele Rosji – mocarstwa atomowego; w obliczu znacznego potencjalnego wzrostu ryzyka wykorzystania przez ugrupowania terrorystyczne materiałów rozczepianych pochodzących z terenów byłego Związku Radzieckiego a nieobecność jest bardzo znamienna i wymowna.

Zagrożeniom opisanym powyżej można skutecznie przeciwstawić się jedynie stosując ciągle modyfikowane systemowe rozwiązania krajowe i sojusznicze. W przypadku antyprolioferacyjnej ochrony RP należy mówić o określonym typie systemu bezpieczeństwa, a dokładnie o Krajowym Systemie Kontroli Towarów Strategicznych, który na potrzeby niniejszego artykułu możemy roboczo nazwać Krajowym Systemem Zapobiegania Proliferacji BMR (KSZPBMR). System ten powinien składać się w pierwszej kolejności z systemów – wewnętrznego oraz zewnętrznego. Rozwiązanie takie pozwoliłoby w sposób bardziej sprawny organizować współpracę oraz współdziałanie poszczególnych podmiotów wchodzących w jego skład, czyli tych o charakterze militarnym, jak i niemilitarnym. Gwarancją skutecznego działania *KSZPBMR* byłby sprawnie działający podsystem zarządzania i kierowania [6], charakteryzujący się przede wszystkim odpowiednim przygotowaniem do reagowania i funkcjonowania w sytuacjach kryzysowych związanych z proliferacją BMR, a co za tym idzie z nielegalnym obrotem towarami o znaczeniu strategicznym.

Uwzględniając wymienione przesłanki trzeba zauważyć, że aktualnie istnieje pilna potrzeba pogłębiania wiedzy teoretycznej jak i praktycznej w zakresie problematyki bezpieczeństwa państwa związanej z kontrolą towarów strategicznych, której celem jest zapobieganie i przeciwdziałanie proliferacji broni masowego rażenia.

Oprócz publikacji Akademii Obrony Narodowej [7], książki Mieczysława Malca, Pawła Durysa i Piotra Pacholskiego [8] nie występują na polskim rynku księgarskim nowe pozycje poświęcone ściśle tej tematyce. Problematyka kontroli towarów strategicznych jest potraktowana jak widać dość fragmentarycznie i cząstkowo.

Ponadto, obserwując realizację określonych zadań w ramach antyproliferacyjnej ochrony kraju można zauważyć pewne braki zarówno w wiedzy, jak i praktyce działania poszczególnych podmiotów biorących w nich udział zwłaszcza w kontekście braku rozwiązań systemowych w zakresie antyproliferacyjnej ochrony państwa ze szczególnym uwzględnieniem działań i mechanizmów koordynujących w tym zakresie.

6 Podsystem zarządzania i kierowania KSZPBMR – to (próba definicji) - zintegrowany wewnętrznie oraz skoordynowany zbiór elementów mechanizmów, relacji oraz zasobów osobowych, prawnych i materiałowo – sprzętowych, funkcjonujący w celu organizowania procesu zarządzania i kierowania na wszystkich poziomach i obszarach KSZPBMR.

7 J. Borkowski. *Terroryzm, a broń masowego rażenia*. Zeszyt Naukowy nr 1(50) AON, Wyd. AON, Warszawa 2003.

8 M. Malec, P. Durys, P. Pacholski. *Proliferacja BMR i środki jej przenoszenia – aktualne wyzwania*. Wydawnictwo Adam Marszałek, Warszawa 2001.

Ze wstępnych badań wynika, że brak intensywnych eksploracji w przedmiotowym zakresie spowodowany jest również wyjątkową specyfiką i hermetycznością, jaką charakteryzują się poszczególne podmioty, zwłaszcza służby specjalne – wywiad i kontrwywiad cywilny i wojskowy, w omawianej sferze bezpieczeństwa państwa.

Wywiad i kontrwywiad jako podmioty bezpieczeństwa reagujące na współczesne zagrożenia.

Od lat społeczność międzynarodowa obserwuje z narastającym niepokojem dążenia niektórych krajów w różnych regionach świata do posiadania broni masowego rażenia, czy też gromadzenia arsenałów broni konwencjonalnych, w tym opartych o zaawansowane technologie militarne, które mogą zostać wykorzystane w regionalnych konfliktach zbrojnych.

Po 11 września 2001 r. zagadnienia nieproliferacji i kontroli eksportu stały się istotnym przedmiotem debaty międzynarodowej [9]. Problematyka ta podejmowana jest i dyskutowana na różnych forach międzynarodowych, takich jak NATO, UE, ONZ oraz OBWE. Jest także przedmiotem wielostronnych inicjatyw politycznych. Gromadzenie broni konwencjonalnych przez niektóre państwa, niekontrolowane transfery towarów i technologii podwójnego zastosowania powodujące zagrożenie regionalnego i globalnego pokoju i bezpieczeństwa oraz zagrożenie terroryzmem, spowodowały intensyfikację międzynarodowych wysiłków na rzecz ustanowienia bądź zaostrzenia istniejących reżimów nieproliferacyjnych kontrolujących międzynarodowy obrót bronią konwencjonalną oraz wybranymi kategoriami dóbr, urządzeń technologii tzw. podwójnego przeznaczenia, posiadającymi obok zastosowań cywilnych również zastosowania militarne i tym samym wiążącymi się z możliwością uzyskania zdolności wytwarzania nowoczesnych systemów broni, zwłaszcza masowego rażenia (jądrowej, chemicznej, biologicznej) oraz rakietowych środków jej przenoszenia.

Skuteczna, odpowiadająca standardom międzynarodowym, kontrola obrotu z zagranicą produkowanymi w kraju oraz importowanymi *„wrażliwymi"* towarami i technologiami skutkuje nieskrępowanym dostępem krajowych przedsiębiorstw do najnowocześniejszych towarów, technologii i myśli technicznej, którymi obrót na rynkach światowych objęty jest międzynarodową kontrolą. Posiadanie przez nasz kraj efektywnego systemu kontroli jest zatem jednym z elementów umożliwiających wejście do Polski zagranicznego kapitału, ważnego czynnika rozwoju gospodarczego.

Krajowy system kontroli jest też częścią polityki integracyjnej naszego kraju. Przystąpienie Polski do NATO i Unii Europejskiej wiązało się z przyjęciem przez nasz kraj standardów obowiązujących w tych organizacjach, również w zakresie kontroli eksportu, importu i tranzytu towarów i technologii objętych listami kontrolnymi międzynarodowych porozumień nieproliferacyjnych. Polska, jak więk-

9 M. Karwas. *Proliferacja broni masowego rażenia, a bezpieczeństwo ekonomiczne państwa – wybrane zagadnienia.* Collegium Civitas PAN, Warszawa 2012, s. 32.

szość państw, opiera na handlu zagranicznym i planuje wzmacnianie rozwoju swojej gospodarki.

Inicjowanych jest wiele programów służących rozwojowi przedsiębiorczości, dynamizujących rozwój małych i średnich przedsiębiorstw, wspomagających rozwój regionalny, zachęcających inwestorów zagranicznych do trwałej kooperacji z polskim przemysłem, także z przemysłem obronnym.

Zwłaszcza małe i średnie przedsiębiorstwa są motorem rozwoju naszej gospodarki. Są one głównym źródłem miejsc pracy i pomysłów związanych z działalnością handlową.

Jednakże wraz z rozwijającym się handlem międzynarodowym zwiększa się zagrożenie, że strategicznie ważne towary i technologie podwójnego zastosowania, uzbrojenie czy wyniki prac badawczych i wdrożeniowych, pozornie nie mające nic wspólnego z bronią, mogą dostać się w niepowołane ręce. Zamachy terrorystyczne w USA i innych krajach wskazują, że jest to możliwe. W przekonaniu Ministerstwa Rozwoju skala obrotu z zagranicą towarami o znaczeniu strategicznym jest w dużej mierze uzależniona od postawy polskich przedsiębiorców wobec wyzwań wynikających z międzynarodowej, wspólnej z państwami NATO i Unii Europejskiej polityki zagranicznej i wspólnej polityki bezpieczeństwa [10].

Niniejszy materiał jest wielostronną próbą dokonania opisu i diagnozy funkcjonowania Krajowego Systemu Kontroli Towarów Strategicznych w aspekcie zapobiegania i przeciwdziałania proliferacji broni masowego rażenia i środków jej przenoszenia jako szerszego zjawiska.

Kwestie zapobiegania terroryzmowi międzynarodowemu są szczególnie ważne w kontekście zagrożenia dla bezpieczeństwa państwa i utrzymania pokoju międzynarodowego na świecie. Jak wynika z przedstawionych treści wiele państw i organizacji w tym o charakterze terrorystycznym dąży i aspiruje do wzmocnienia swojej pozycji międzynarodowej, której celem jest realizacja własnych interesów nie zawsze zgodnych z duchem pokoju międzynarodowego. Działalność aktorów państwowych i nie państwowych może wpływać na bezpieczeństwo narodowe, które określa się często jako stan świadomości społecznej, w którym istniejący poziom zagrożeń, dzięki posiadanym zdolnościom obronnym, nie budzi obaw, lęku o zachowanie lub możliwość osiągania uznanych wartości . Ponadto ten stan świadomości niepodzielnie i nierozerwalnie jest powiązany z rozwojem państwa. W trosce o jego wysoki poziom, trwałe i skuteczne zapewnienie jego suwerenności kwestie te winny być elementarną powinnością wszystkich rządzących państwem i odpowiedzialnych za bezpieczeństwo kraju w każdym wymiarze. W tą politykę rządzących powinna się pojawić odpowiedź na pytanie i jego złożoność skłaniająca do refleksji: *Czy proliferacja broni masowego rażenia w odniesieniu do zagadnień terroryzmu międzynarodowego stanowi dziś realne zagrożenie dla utrzymania bezpieczeństwa i pokoju międzynarodowego na świecie i czy podejmowane środki i działania na rzecz poprawy bezpieczeństwa*

10 Z. Stachowiak, S. Kurek. Bezpieczeństwo ekonomiczne Rzeczypospolitej Polskiej. AON, Warszawa 2004, s. 87.

w tym zakresie przez państwo są wystarczające?. Należy stwierdzić, iż w chwili obecnej biorąc pod uwagę aktualną sytuację polityczno-ekonomiczną między innymi tzw. *„państw progowych"* wzrasta niebezpieczeństwo ataku terrorystycznego z użyciem broni masowego rażenia przez aktorów państwowych i pozapaństwowych. Zwłaszcza takie zagrożenie może się pojawić w przypadku rozwiązywania problemów w konfliktach regionalnych. Z drugiej zaś strony czynnikiem obniżającym ryzyko wystąpienia omawianego zagrożenia może być wciąż niski poziom zaawansowania technologicznego tzw. państw progowych w dziedzinie środków przenoszenia broni masowego rażenia, który aktualnie nie pozwala na stworzenie realnego zagrożenia między innymi atakami rakietowymi ze względu na ograniczony charakter programów rakietowych. Nie należy również zapominać o tym, że tak naprawdę poziom zagrożenia atakiem terrorystycznym z użyciem broni masowego rażenia jest mało weryfikowalny, a zabezpieczenie przed tego rodzaju działaniami znacznie utrudnione (pokazuje to sytuacja w Stanach Zjednoczonych w związku z odnotowanymi przypadkami terrorystycznego użycia wąglika, czy też północnokoreańskie próby rakietowe).

W związku z tym istnieje konieczność wzrostu nakładu środków finansowych na działania zabezpieczające przed proliferacją broni masowego rażenia i środków jej przenoszenia. Chodzi głównie o działania polegające na monitorowaniu poziomu omawianego zagrożenia i koordynacji działań zabezpieczających.

Z punktu widzenia interesów naszego państwa zagrożenie proliferacją broni masowego rażenia i środków jej przenoszenia ma ważne znaczenia dla interesów politycznych, militarnych i ekonomicznych naszego kraju. Obecnie funkcjonujące rozwiązania w tym zakresie zwłaszcza Krajowy System Kontroli Towarów Strategicznych wymaga podjęcia zdecydowanych zmian prawnych i legislacyjnych przez decydentów, gdyż w pełni nie zabezpiecza naszego kraju przed zagrożeniami, których zwalczanie i zapobieganie jest przedmiotem zaprojektowanych zmian systemowych. Obecne rozwiązania w tym zakresie nie pozwalają w pełni Polsce jako sygnatariuszowi wielu porozumień nieproliferacyjnych, w tym kontroli towarów strategicznych zapewnić właściwej realizacji ustawowych zadań służb specjalnych – wywiadu i kontrwywiadu oraz innych instytucji odpowiedzialnych za wykrywanie zagrożeń związanych z proliferacją bronią masowego rażenia i środków jej przenoszenia jako elementu przeciwdziałania zjawiskom terroryzmu międzynarodowemu. Ewentualne wprowadzenie zaproponowanych, zaprojektowanych zmian zdecydowanie poprawi jakość funkcjonowania w tym zakresie wszystkich organów i instytucji zapewniających właściwy, wysoki poziom bezpieczeństwa państwa i jego obywateli.

Reasumując wnioski wynikające z procesu badawczego można postawić tezę, że Krajowy System Kontroli Towarów Strategicznych odpowiednio zmodyfikowany i zarządzany może być w sposób profesjonalny i kompleksowy wykorzystany na rzecz bezpieczeństwa państwa i utrzymania pokoju międzynarodowego na świecie. Zawarta w artykule wiedza o systemie zapobiegania proliferacji broni

masowego rażenia i środkach jej przenoszenia jego wpływu na bezpieczeństwo państwa wskazuje jednak na możliwości i zadania, jakie muszą realizować podmioty Krajowego Systemu Kontroli Towarów Strategicznych na rzecz poprawy bezpieczeństwa państwa.

Z tego punktu widzenia niniejszy artykół może być traktowana jako baza do dalszych badań obszaru bezpieczeństwa w zakresie funkcjonowania KSKTS jako elementu tworzącego architekturę bezpieczeństwo państwa w kontekście wewnętrznym i międzynarodowym. Bowiem Świat coraz wyraźniej podlega podziałowi wynikającemu z poziomu cywilizacyjnego w znaczeniu technologicznym.

Stan zagrożenia skutkami użycia broni masowego rażenia stanowić będzie wypadkową zarówno stosunkowo wysokiej odporności państw, jak i rozumienia ich roli jako celu coraz powszechniej pożądanego. Brak konsekwencji w egzekwowaniu postanowień ograniczających proliferację napędza „koło strachu", które pod wpływem skrajnych zagrożeń może wymuszać drastyczne posunięcia likwidujące swobodę niezbędną do rozwoju cywilizacyjnego.

Bibliografia

Adamski J., *Nowe technologie w służbie terrorystów*, Wydawnictwo TRIO, Warszawa 2007.

Bolechów B. *Terroryzm w świecie poddwubiegunowym, przewartościowania i kontynuacje,* Toruń 2002.

Borkowski J. *Terroryzm, a broń masowego rażenia,* Zeszyt Naukowy nr 1(50) AON, Wyd. AON, Warszawa 2003.

Cost of the Afghanistan War By the Numbers. cnl.org.issues. *13 FEB13.2013.*

Durys P. *Inicjatywa PSI – Nowy wymiar zwalczania proliferacji,* MON Departament Polityki Obronnej, Warszawa 2006.

Dyrcz C. *Terroryzm XXI wieku jako zagrożenie bezpieczeństwa międzynarodowego i narodowego,* Gdynia 2005.

Dyrektywa 2009/43/WE z dnia 6 maja 2009 r. w sprawie uproszczenia Warunków transferów produktów związanych z obronnością we Wspólnocie (Dz. Urz. UE 2009 L 146/1).

Eksport uzbrojenia i sprzętu wojskowego z Polski. Raport za 2012, Departament Polityki Bezpieczeństwa MSZ, Warszawa 2013.

Europejska Strategia Bezpieczeństwa z grudnia 2003 r. www.msz.gov.pl

Kamiński A. *Metodologia, technika, procedura badawcza w pedagogice empirycznej.* Ossolineum, Wrocław 1974.

Karwas M. *Proliferacja broni masowego rażenia, a bezpieczeństwo ekonomiczne państwa – wybrane zagadnienia,* Zeszyty Doktoranckie WBN AON nr 1(6)/2013, Warszawa 2013.

Karwas M. *Proliferacja broni masowego rażenia, a bezpieczeństwo ekonomiczne państwa – wybrane zagadnieni,* Collegium Civitas PAN, Warszawa 2012.

Karwas M. *Proliferacja broni masowego rażenia, a zagrożenie terroryzmem międzynarodowym – wybrane zagadnienia,* Uniwersytet Warszawski, Warszawa 2009.

Karwas M. *Zapobieganie proliferacji broni masowego rażenia, jako element prewencyjny zarządzania kryzysowego – wybrane zagadnienia*, Wiedza Obronna, Kwartalnik Towarzystwa Wiedzy Obronnej 2-3/252/, Warszawa 2015.

Kitler W. *Bezpieczeństwo narodowe RP. Podstawowe kategorie. Uwarunkowania, System,* Warszawa 2011.

Maciej Karwas*

,

*** dr Maciej Karwas, Uniwersytet im. Kardynała Stefana Wyszyńskiego w Warszawie**

Alojzy Pilich

Rola i znaczenie wywiadu gospodarczego dla bezpieczeństwa biznesu

Streszczenie

Materiał dotyczy działań podejmowanych przez przedsiębiorstwa w celu ochrony zasobów informacyjnych przed zagrożeniem związanym z nielegalnym wywiadem gospodarczym. Autor podkreśla wagę, rolę i znaczenie wywiadu gospodarczego dla sektora gospodarki oraz eksponuje znaczenie informacji, która jest zasobem łatwym do wytworzenia i rozpowszechniania, lecz trudnym do ochrony i kontroli. W artykule wskazano istotne praktyki oraz standardy, które służą zarządzaniu i doskonaleniu systemu bezpieczeństwem informacji w przedsiębiorstwie. Ponadto wyjaśniono pojęcie „wywiadu gospodarczego" oraz opisano początki, role i znaczenie jego funkcjonowania. Zilustrowano przykładowe metody działań podmiotów zajmujących się pozyskiwaniem zasobów informacyjnych oraz określono rodzaje i charakter informacji, które mogą być przedmiotem zainteresowania podmiotów tzw. wywiadowni gospodarczych. Podjęto także próbę wyznaczenia granicy pomiędzy legalnym a nielegalnym wywiadem gospodarczym. Jak podkreśla autor nierzadko zdarza się, że podmioty realizujące zlecenie przeprowadzenia wywiadu gospodarczego sięgają po nielegalne metody. Przed takimi działaniami powinny chronić się nie tylko podmioty prawa handlowego, ale także inne podmioty prawa międzynarodowego również w wymiarze korporacyjnym.

Wstęp

Światowa sytuacja gospodarcza uwidacznia coraz bardziej uzależnienie od determinantów globalnej, coraz bardziej zaostrzającej się konkurencji, w której informacja jest postrzegana jako jedno z najważniejszych źródeł zdobycia przewagi konkurencyjnej. Jest tak głównie dlatego, że czynnikiem sukcesu są wieloaspektowe działania niekonwencjonalne, innowacyjne, róże od dotychczasowych praktyk biznesowych.

Muszą one być oparte na informacji, i to takiej, która jest trudno dostępna dla konkurentów. Aby informacja spełniła warunek niepowtarzalności, nie może być powszechnie dostępna. Tak jest przede wszystkim w przypadku wiedzy tworzonej w przedsiębiorstwach. Jeśli w danej firmie brakuje dostatecznie sprawnej organizacji, zdolnej w porę zapobiec nieuprawnionemu wyciekowi *know-how* i wszelkiego rodzaju innych niematerialnych aktywów, to cały system zarządzania informacją okaże się mało skuteczny przy tworzeniu trwałej przewagi konkurencyjnej.

Prowadzenie działalności gospodarczej nie jest możliwe bez informacji, która wspomaga podejmowanie strategicznych decyzji, planowanie czy zarządzanie wieloma obszarami przedsiębiorstwa. Informacja jest również narzędziem walki z konkurencją. Przedsiębiorstwa, które mają istotne dla swojej działalności informacje, zwiększają szanse na utrzymanie przewagi w danym sektorze działalności. Z kolei ich utrata może prowadzić do obniżenia pozycji ekonomicznej przedsiębiorstwa, a nawet do zakończenia jego działalności. Do najważniejszych skutków naruszenia bezpieczeństwa informacji zalicza się zmniejszenie dochodów oraz obniżenie konkurencyjności. Obecnie istnieje coraz więcej ośrodków dostarczających informacje przedsiębiorcom (tzw. dostawcy informacji); są to firmy, które wyspecjalizowały się w określonych produktach informacyjnych. Należą do nich m.in. wywiadownie gospodarcze, biura detektywistyczne oraz systemy informacji gospodarczej – na szczeblu regionalnym, krajowym i międzynarodowym.

Pozyskiwaniem informacji w sektorze gospodarczym zajmują się podmioty prawa handlowego:

- przedsiębiorstwa zbierające informacje na własne potrzeby, aby konkurować na rynku,
- podmioty, które pozyskują informacje i sprzedają je innym (dostawcy usług informacyjnych, pośrednicy, brokerzy itp.),
- organizacje pełniące misje społeczną.

Przedmiotem operacyjnego zainteresowania tych podmiotów mogą być takie informacje, jak np. sprawozdania finansowe przedsiębiorstw, rachunki bankowe czy wyniki badań marketingowych. Zdobywanie i analizowanie informacji o osiągnięciach technicznych, planowanych działaniach i pozycji ekonomicznej podmiotów funkcjonujących na regionalnym i globalnym rynku nazywa się wywiadem gospodarczym. W polskich opracowaniach (monografiach) można spotkać również takie określenia, jak: „wywiad konkurencyjny", „wywiad rynkowy", „wywiad biznesowy" oraz „analiza konkurencyjności". Najczęściej jednak posługują się one oryginalnym, angielskim terminem *competitive intelligence*, co oznacza, że jest to działalność, której celem jest głównie pozyskiwanie informacji o potencjalnych konkurentach i obszarach ich aktywności biznesowej. Niniejszy artykuł jest pisany z perspektywy przedsiębiorstw i potrzeb ochrony ich własnych informacji biznesowych.

Istotne aspekty funkcjonowania wywiadu gospodarczego – identyfikacja źródeł informacji

Początki wywiadu rozumianego jako pozyskiwanie informacji o kluczowym znaczeniu, można odnaleźć już w odległej przeszłości. Autorzy literatury przedmiotu często wskazują na czasy starożytne i na takie postacie, jak np. Mojżesz, Konfucjusz czy Sun Tzu (wspominają o nich np. L. Korzeniowski i A. Pepłoń-

ski oraz E. Cilecki). Istotne znaczenie dla wywiadu gospodarczego mają źródła informacji. Autorzy publikacji charakteryzują je w różny sposób, np. jako źródła wewnętrzne i zewnętrzne, źródła formalne i nieformalne, źródła pierwotne i wtórne.

Źródła zewnętrzne są potrzebne szczególnie małym i średnim przedsiębiorstwom, gdyż ocenia się, że (...) *w dużych przedsiębiorstwach 80 proc. potrzebnych informacji znajduje się na miejscu, a poszukiwania na zewnątrz obejmują tylko pozostałe 20 proc*. Źródłem informacji mogą być m.in. podwykonawcy, pracownicy konkurencji, dostawcy usług czy stażyści. Ponadto takie wydarzenia, jak np. kongresy, targi, szkolenia, spotkania okolicznościowe – organizowane głównie z myślą o ułatwieniu ich uczestnikom wymiany informacji – są także doskonałym miejscem zdobywania nowej wiedzy. W tej grupie źródeł zewnętrznych mogą znajdować się tzw. wewnętrzne źródła informacji. Jak podają B. Martinet i Y.M. Marti, przeprowadzone badania dowiodły, że z tych właśnie źródeł pochodzi trzy czwarte informacji mających wartość gospodarczą.

W dobie rozwoju nowych technologii oraz powszechnego dostępu do informacji wywiadownie gospodarcze zdobywają znaczną część wiedzy ze źródeł ogólnodostępnych (ten rodzaj źródeł nie jest wcześniej wymieniony). Jej uzyskanie nie wymaga zastosowania skomplikowanych metod, ponieważ są to informacje umieszczane w Internecie, prasie, książkach, oficjalnych publikacjach różnych instytucji oraz w dostępnych bazach danych itp. Wielu pracowników różnych firm ujawnia informacje służbowe na forach internetowych, portalach społecznościowych, ułatwiając tym samym pracę wywiadowniom. Nie wszystkie jednak informacje, które mają wartość dla przedsiębiorcy, są ogólnie dostępne, dlatego wywiadownie w celu ich zdobycia często wykorzystują powiązania personalne. Metoda dotarcia do informacji bazuje na kontaktach międzyludzkich. Według T. Aleksandrowicza cechą wyróżniającą tę grupę źródeł jest to, że dostęp do nich wymaga poniesienia określonych nakładów, np. w postaci uzyskania praw dostępu do potrzebnych baz danych.

Istota wywiadu a jego legitymizacja

Wywiad jest przedsięwzięciem legalnym, jeżeli działa w granicach prawa i na zasadach określonych przez unormowania prawne. Bardzo często zdarza się jednak, że osoby realizujące zlecenie przeprowadzenia wywiadu gospodarczego wykorzystują źródła w sposób bezprawny i sięgają po nielegalne metody, np. podsłuch, podgląd, wnikanie w cyberprzestrzeń bądź pozyskiwanie osobowych źródeł informacji. Osobowe źródła informacji są rekrutowane spośród byłych pracowników przedsiębiorstwa konkurencyjnego lub nowo przyjmowanych, przy założeniu, że stanowią oni najłatwiejszy cel. Nierzadko stosuje się bardziej wyrafinowaną praktykę, jaką jest zatrudnienie swojego pracownika w rozpracowywanym przedsiębiorstwie. Niekiedy próbuje się również pozyskać osobowe źródła informacji w postaci sfrustrowanych pracowników konkurencyjnej firmy,

niezadowolnych z wysokości zarobków, braku perspektyw awansu czy panujących stosunków międzyludzkich w miejscu ich pracy. W typowaniu kandydatów na informatorów uwzględnia się ich aktualny status majątkowy, nałogi i cechy charakterologiczne. Nielegalny wywiad gospodarczy stwarza szczególne i coraz powszechniejsze zagrożenie dla funkcjonowania przedsiębiorstw, nie tylko w Polsce, lecz także na świecie. Nie można bowiem wykluczyć, że przynajmniej część wywiadowni gospodarczych realizuje działania, które można określić jako szpiegostwo przemysłowe.

I chociaż ów rodzaj aktywności nie jest przedmiotem tego opracowania, to należy zauważyć, że zjawisko to występuje prawie we wszystkich dziedzinach gospodarki i nie ogranicza się jedynie do firm wdrażających zaawansowane technologie. Dotyczy praktycznie każdej działalności, która zapewnia osiągnięcie wymiernych korzyści ekonomicznych. Dawno już minęły czasy, gdy szpieg potrzebował dotrzeć do dokumentu, aby go wykraść, skopiować lub sfotografować. Nowoczesna technologia umożliwia globalny dostęp do zasobów informacji przetwarzanych chociażby przez systemy informatyczne. Bardzo często zdarza się, że kierownictwo przedsiębiorstwa nie zdaje sobie sprawy, że firma już padła ofiarą szpiegostwa przemysłowego. Dotyczy to zwłaszcza dużych koncernów przetwarzających strategiczne informacje, chronione na podstawie przepisów prawa, np. informacje niejawne, których ujawnienie mogłoby spowodować szkody dla ważnych interesów państwa (w 2013 r. w Stanach Zjednoczonych 3 tys. organizacji otrzymało od rządu oficjalne powiadomienie o ataku hakerskim). Przedsiębiorstwa powinny współpracować w tym zakresie z odpowiednimi organami, których zadaniem jest przeciwdziałanie szpiegostwu przemysłowemu, zwłaszcza jeśli jest ono dokonywane przez służby specjalne innych państw. Według FBI Rosja i Chiny regularnie od lat zajmują się wykradaniem tajemnic ekonomicznych i technologicznych w przedsiębiorstwach – szczególnie przez ich aktywną działalność w cyberprzestrzeni. Fakt agresywnego pozyskiwania informacji gospodarczych przez Chiny potwierdził przedstawiciel FBI w Polsce, która od lat współpracuje z przedsiębiorstwami w Stanach Zjednoczonych i Polsce w zakresie przeciwdziałania szpiegostwu gospodarczemu. Straty gospodarki amerykańskiej z tytułu szpiegostwa gospodarczego w 2011 r. wyniosły łącznie ponad 13 mld dolarów. W kolejnym, 2012 r., straty te zamknęły się już kwotą 19 mld dolarów. Okazuje się zatem, że pomimo działań podejmowanych przez służby specjalne Stanów Zjednoczonych, opisany proceder nie ulega zmniejszeniu, lecz wręcz przeciwnie, w ciągu dwóch lat zwiększył się on blisko o 50 proc. Niepokojąca w tym kontekście jest także wypowiedź Steve'a Durbina, wiceprezesa Forum Bezpieczeństwa Informacji, który zauważył, że (...) *wspierane przez państwo cyberszpiegostwo nie jest już ograniczone tylko i wyłącznie do Chin czy Korei Północnej, w pełnym zakresie zajmują się nim także państwa demokratyczne*. W tej sytuacji z dużą dozą prawdopodobieństwa, graniczącą z pewnością, można stwierdzić, że i polskie przedsiębiorstwa są narażone na takie działania. Według

Symantec w Polsce od 2011 r. działa grupa hakerów o nazwie „Dragonfly", która dokonuje ataków szpiegowskich na firmy z sektora energetycznego w różnych krajach na świecie. Na przykład w 2011 r. straty poniesione w wyniku cyberprzestępczości szacowano w USA na 1,52 mld dolarów, a w skali globu wyniosły one 221 mld dolarów.

W 2013 r. straty związane z cyberprzestępczością szacowano już w świecie na 445 mld dolarów. Przedstawione dane dowodzą, jak duży wpływ na gospodarkę, w tym na działalność przedsiębiorstw, mają wskazane zagrożenia. Według szacunków zawartych w raporcie *Center for Strategic and International Studies (CSIS)* globalne straty związane z cyberszpiegostwem okazują się niższe od podanych powyżej, ale i tak zawierają się w przedziale od 70 do 140 mld dolarów. Przedmiotem zainteresowania wywiadu gospodarczego są w dużej części tajemnice przedsiębiorstwa dotyczące nowych technologii, produkcji, patentów, praw własności, znaków towarowych i tajemnicy handlowej (*know-how*).

Tajemnica przedsiebiorstwa została zdefiniowana w art. 11 *Ustawy z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji* jako (...) *nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności*. Pozyskanie tajemnicy przedsiębiorstwa w sposób nieuprawniony, w myśl art. 3 tej ustawy, stanowi czyn nieuczciwej konkurencji, czyli działanie sprzeczne z prawem lub dobrymi obyczajami, jeżeli zagraża interesowi innego przedsiębiorcy lub klienta lub go narusza. Oznacza to, że zdobywanie informacji dotyczących np. produkcji prowadzonej przez konkurencyjny podmiot jest czynem nieuczciwej konkurencji. Polskie prawodawstwo nie reguluje działalności wywiadu gospodarczego, dlatego nie ma aktu prawnego, który określałby, jakiego rodzaju informacje mogą być pozyskiwane w ramach takiego wywiadu.

Wywiad gospodarczy jest coraz powszechniejszym działaniem realizowanym przez polskich przedsiębiorców, dlatego dziedzina ta wymaga uregulowania w drodze legislacyjnej. Prawo powinno określać, jakie działania są dozwolone w ramach prowadzonego wywiadu gospodarczego, a jakie stanowią czyn nieuczciwej konkurencji lub są już szpiegostwem gospodarczym.

Polskie przepisy prawne dokładnie regulują, w jaki sposób oraz kto może uzyskać dostęp do określonych rodzajów informacji, np. do danych osobowych, informacji niejawnych, tajemnicy bankowej. Zbieranie informacji o pracownikach konkretnego przedsiębiorstwa musi odbywać się zgodnie z przepisami prawa. Oznacza to, że dostęp do takich informacji mają określone podmioty, takie jak: organy ścigania i sądowe oraz służby specjalne a także niektóre organy administracji publicznej. Również kodeks pracy w art. 22^1 zawiera zamknięty katalog informacji, których pracodawca i tylko pracodawca może żądać od pracownika.

Istnieją także informacje, których pozyskiwanie wymaga przedstawienia in-

1 Dz.U. 1997 nr 98, poz. 60 z późn. zm.

teresu prawnego. Należą do nich m.in. dane z centralnej ewidencji pojazdów i centralnej ewidencji kierowców (art. 100 ah i art. 80c *Ustawy dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym*[2]), informacje z ewidencji gruntów i budynków (art. 24.2,2a,4,5 *Ustawy z dnia 17 maja 1989 r. – Prawo geodezyjne i kartograficzne*)[3]. Dotyczy to także rejestrów dłużników prowadzonych przez biura informacji gospodarczej, określonych na podstawie *Ustawy z dnia 9 kwietnia 2010 r. o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych*. Zgodnie z art. 26. ust. 2 tej ustawy *Podmiot, który otrzymał od biura informacje gospodarcze dotyczące dłużnika będącego konsumentem, nie może ich ujawnić innym osobom*. Nieuprawnione pozyskiwanie informacji może skutkować sankcjami karnymi oraz finansowymi nie tylko dla podmiotu realizującego taką usługę, lecz także dla zlecającego jej wykonanie.

Działania prewencyjne w zakresie przeciwdziałania utracie informacji

Produkt, jakim jest informacja, to zasób łatwy do wytworzenia i rozpowszechniania, lecz trudny do ochrony i kontroli. Nigdy nie można mieć pewności, że tajemnice są całkowicie chronione, można jednak podjąć działania, aby ryzyko ich utraty znacznie zminimalizować. Wdrożenie systemu bezpieczeństwa w przedsiębiorstwie wiąże się z wprowadzeniem ograniczeń w poszczególnych obszarach jego działalności, co może wydłużyć czas pracy niezbędny do osiągnięcia zamierzonych wyników. Brak odpowiedniej ochrony oraz nieprzestrzeganie wewnętrznych procedur dotyczących bezpieczeństwa mogą mieć nieodwracalne, negatywne dla przedsiębiorstwa skutki. Amerykański Ponemon Institute LLC przeprowadził badanie na temat kosztów przedsiębiorstw związanych z utratą informacji. Badanie przeprowadzono w dziewięciu państwach, w których dokonano analizy kosztów dotyczących naruszenia bezpieczeństwa i utraty informacji. Największe straty w wyniku wycieku informacji poniosły Niemcy i Stany Zjednoczone, odpowiednio: 199 dolarów i 188 dolarów za rekord baz danych. Łącznie Stany Zjednoczone poniosły 5,4 mld dolarów strat, a Niemcy 4,8 mld dolarów. Najmniejsze koszty poniesiono w Brazylii i Indiach (odpowiednio: 58 dolarów i 42 dolary za rekord). Brazylia poniosła straty w wysokości 1,3 mld dolarów, a Indie 1,1 mld dolarów. Przedstawione statystyki pokazują, jak wielkie straty ponosi gospodarka narodowa w wyniku utraty informacji przez przedsiębiorstwa.

Dlatego tak ważne są działania wyprzedzające podejmowane przez przedsiębiorstwa, a związane z wdrażaniem zabezpieczeń w celu ochrony zasobów informacyjnych. System bezpieczeństwa musi być dostosowany do specyfiki konkretnego podmiotu. Powinien przy tym uwzględniać wszelkie aspekty zabezpieczenia i ochrony informacji związane z przeciwdziałaniem utracie informacji spowodowanej zarówno przez aktywność obcych służb specjalnych, wywiadowni

2 Dz.U. 1989 nr 30, poz. 163 z późn. zm.
3 Dz.U. 2010 nr 81, poz. 530 z późn. zm.

gospodarczych, a także w sposób nieumyślny zawinione działania pracowników oraz przez nieprzewidziane oddziaływanie czynników pozaludzkich (tzn. takich zdarzeń losowych, jak pożar czy powódź). System bezpieczeństwa informacji wymaga spełnienia co najmniej trzech warunków, aby można było mówić o jego skuteczności. Są nimi:

- wysoka świadomość pracowników, poczynając od najwyższego kierownictwa,
- efektywne zarządzanie informacjami w taki sposób, aby zapewnić ich bezpieczeństwo,
- stworzenie odpowiednich rozwiązań technologicznych, które zapewniają realizację polityki bezpieczeństwa informacji.

W związku z powyższym kierownictwo spółek powinno kompleksowo zarządzać zasobami informacyjnymi, a wdrożony w przedsiębiorstwie system bezpieczeństwa musi zapewnić ich efektywną ochronę i obronę przed szpiegostwem, cyberatakami i przestępczością komputerową. Zarządzanie zasobami informacyjnymi należy rozumieć jako określony zestaw sposobów postępowania dotyczących tego, jak przedsiębiorstwo zdobywa, dystrybuuje i używa informacji oraz wiedzy. System bezpieczeństwa musi uwzględniać przede wszystkim kontrolę pozyskiwania, wytwarzania i przetwarzania informacji, ich bezpieczną dystrybucję oraz monitorowanie „ścieżki" obiegu informacji w strukturze danego przedsiębiorstwa. Zarządy spółek powinny przeprowadzać okresowe analizy ryzyka utraty informacji oraz sporządzać plany postępowania z tym ryzykiem. Działania, które trzeba podjąć, to rozpoznanie i natychmiastowe reagowanie na pojawiające się zagrożenia. Bardzo ważne jest też określenie i zidentyfikowanie, jakiego rodzaju informacje mają podlegać szczególnej ochronie, z czym wiąże się ograniczenie do nich dostępu. Oznacza to konieczność opracowania listy dokumentów, które wymagają ochrony w przedsiębiorstwie. Każdy pracownik powinien wiedzieć, które zasoby informacyjne i jak należy chronić. Przedsiębiorca powinien wprowadzić zasady organizacyjne dotyczące oznaczania, udostępniania, publikowania, kopiowania i niszczenia informacji, które są jego własnością. Główną rolę odgrywają również procedury kadrowe podczas weryfikacji i rekrutacji pracowników identyfikujące wewnętrzne zagrożenia, których źródłem może być np. niezadowolony pracownik.

Polskie przepisy prawa, w tym kodeks pracy, jasno precyzują, jakiego rodzaju informacji może zażądać pracodawca od pracownika. Oznacza to, że pracodawca ma, niestety, ograniczone możliwości dotarcia do informacji o przyszłym pracowniku podczas procesu rekrutacji.

Nie może np. żądać od kandydata do pracy (tak samo jak i od pracownika) oświadczenia o niekaralności, chyba, że przepisy szczególne na to pozwalają. Zarządy spółek powinny zatwierdzić i wdrożyć własną strategię działań ochronnych i opublikować ją pod nazwą *Polityka bezpieczeństwa informacji*. Jest to zbiór zasad i procedur dotyczących ochrony i zabezpieczenia informacji,

w którym powinny być uwzględnione cele, sposoby i środki ochrony informacji. Oprócz podjęcia środków ochrony o charakterze organizacyjnym istotne są zabezpieczenia techniczne i fizyczne. W systemie bezpieczeństwa w przedsiębiorstwie musi zostać uwzględniona ochrona systemu teleinformatycznego, uzależnienie od skomputeryzowanych systemów wszystkich aspektów działalności przedsiębiorstw zwiększa bowiem ryzyko utraty cennych informacji. Przedsiębiorstwa, opracowując system bezpieczeństwa, mogą posiłkować się „dobrymi praktykami" zawartymi w normie ISO/IEC 27001:2013, która umożliwia zarządzanie bezpieczeństwem informacji w sposób całościowy i usystematyzowany. Wskazana norma dotyczy całości funkcjonowania przedsiębiorstwa, ponieważ uwzględnia jego strukturę organizacyjną, politykę działania, zakres odpowiedzialności, praktyki, procedury, procesy i zasoby. Norma ta szczegółowo opisuje także wymaganą dokumentację i sposób jej prowadzenia. ISO/IEC 27001 jest normą zawierającą model systemu zarządzania bezpieczeństwem informacji, który może być zastosowany przez każdą organizację, niezależnie od specyfiki jej działalności, wielkości, realizowanych procesów, statusu prawnego i struktury organizacyjnej. Norma pozwala na ustanowienie, wprowadzenie, eksploatowanie, monitorowanie, przegląd i doskonalenie systemu. Wdrożenie systemu bezpieczeństwa informacji w przedsiębiorstwie musi uwzględniać przepisy szczególne, których przedsiębiorstwa – z uwagi na prowadzoną działalność – są zobowiązane przestrzegać. Przykładem mogą być przedsiębiorstwa energetyczne, które oprócz zastosowania się do przepisów dotyczących bezpieczeństwa informacji, takich jak np. *Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* czy *Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji*, są zobligowane do przestrzegania przepisów dotyczących bezpieczeństwa informacji określonych w *Ustawie z dnia 10 kwietnia 1997 r. – Prawo energetyczne*. Wprowadzenie systemu zarządzania bezpieczeństwem informacji powinno być postrzegane w przedsiębiorstwie jako decyzja strategiczna i powinny wypływać z potrzeb biznesowych.

Podsumowanie

Przedsiębiorcy niechętnie planują środki budżetowe na modernizację i rozbudowę systemów bezpieczeństwa. Przyczyną takiej postawy może być problem z prawidłowym oszacowaniem korzyści, jakie niosą z sobą tego typu inwestycje. Stosowanie kompleksowych strategii ochrony własnych zasobów informacyjnych może zwiększyć koszty prowadzenia działalności, jednak ryzyko utraty informacji na rzecz konkurencji wiąże się z nieporównywalnie większymi kosztami i stratami. Właściwa ochrona opisywanych zasobów ma istotne znaczenie dla sprostania wymaganiom prawnym i wywiązania się z biznesowych zobowiązań. Zarządy spółek muszą mieć świadomość znaczenia informacji, które są realnym wsparciem dla prowadzenia działalności gospodarczej i budowania silnej, konkurencyjnej marki w danej branży. Należy pamiętać, że nie tylko jedna strona

chce pozyskać informacje ułatwiające jej podejmowanie strategicznych decyzji. Firma konkurencyjna, kierując się pragnieniem uzyskania dostępu do cennych dla niej, lecz zastrzeżonych przez pierwszą firmę informacji, może sięgnąć po metody nielegalne, ze szpiegostwem gospodarczym włącznie. Przedsiębiorstwa, które zbyt lekkomyślnie kierują się zasadami otwartości, ignorując przestrzeganie zasad bezpieczeństwa w obiegu informacji chronionych, mogą narazić się na istotne, niepowetowane straty.

Biblografia

Aleksandrowicz T., *Analiza informacji w administracji i biznesie*, Warszawa 1999, Wyższa Szkoła Handlu i Prawa.

Ciecierski M., *Wywiad biznesowy w korporacjach transnarodowych: teoria i praktyka*, Toruń 2009, Adam Marszałek.

Ciecierski M., *Wywiad gospodarczy (rynkowy) – wybrane aspekty*, „Wiek XXI" 2003, nr 3.

Cilecki E., *Penetracja rynków zagranicznych: wywiad gospodarczy*, Warszawa 1997, PWSzBiA.

Cilecki E., *Penetracja rynku a metody uzyskiwania informacji gospodarczych ze źródeł zagranicznych*, [w] *System informacji strategicznej*, Borowiecki R., Romanowska M.(red.), Warszawa 2001, Difin.

Fleischer C.S., Blenkhorn D.L., *Managing Frontiers in Competitive Intelligence*, Westport 2001, Conn.

Identity Theft Cost Americans $1.52B in 2011 [online], Reuters 2012, 28 February 2012, www.huffingtonpost.com

Kaliski M., Mrozik P., *Tworzenie efektywnego systemu wywiadu gospodarczego* [w]: *Informacja w zarządzaniu przedsiębiorstwem: pozyskiwanie, wykorzystanie i ochrona. Wybrane problemy teorii i praktyki*,

Borowiecki R., Kwieciński M. (red.), Kraków 2003. Korzeniowski L., Pepłoński A., *Wywiad gospodarczy: historia i współczesność*, Kraków 2005, EAS.

Martinet B., Marti Y.M., *Wywiad gospodarczy: pozyskiwanie i ochrona informacji*, Warszawa 1999, Polskie Wydawnictwo Ekonomiczne.

Mashable, Jolie O'Dell, *How much does identity theft cost?*, 28 January 2011, www.mashable.com.

Surma, J., *Business Intelligence. Systemy wspomagania decyzji biznesowych*, Warszawa 2009, Wydawnictwo Naukowe PWN.

Szczepanik R., Krzyżowska O., *Nietypowe przypadki Public Relations*, Gliwice 2003, Onepress.

Alojzy Pilich*

***dr Alojzy Pilich, Państwowa Wyższa Szkoła Zawodowa w Skierniewicach**

Mirosław Kwieciński

Wykorzystanie analizy wywiadowczej i osłony kontrwywiadowczej w ocenie zagrożeń zagranicznej ekspansji przedsiębiorstwa

Streszczenie

Współczesne przedsiębiorstwo realizuje kluczową koncepcję własnego rozwoju poprzez ekspansję, głównie dla poszerzenia rynków zbytu i zwiększenia zysków. O wyborze kierunku zagranicznej ekspansji decydują częstokroć okazje. Wszelkie decyzje o podjęciu ekspansji wiążą się zdużym ryzykiem. Dlatego każde jego ograniczanie ma ogromne znaczenie w praktyce menedżerskiej.

W artykule przedstawiono, obok wsparcia instytucjonalnego ekspansji, różne narzędzia z teorii i praktyki wywiadu i kontrwywiadu gospodarczego. Dokonano charakterystyki wybranych technik analizy wywiadowczej, zawierającej bogactwo opisów czynników, trendów, hipotez, scenariuszy, rekomendacji i ocen. Przedstawiono także istotę, cele i funkcje działania osłony kontrwywiadowczej, sprowadzającej się do prowadzenia przemyślanej pracy z personelem.

Słowa kluczowe: ekspansja przedsiębiorstwa, bezpieczeństwo, zagrożenia bezpieczeństwa, osłona kontrwywiadowcza, analiza wywiadowcza.

Summary *(tłumaczenie Małgorzata Czyrnek)*

Today the companyimplements a keyconcept of itsown development through the expansion, mainly to expandthe markets and increaseownprofits.The approachingaccasionsoftendecide on the choice of the direction of internationalexpansion.Anydecision to proceed withanexpansioninvolves a high degree of risk.Therefore, anyreductionthereofis of greatimportance in the practice of management.

The articlepresents, in addition to institutionalsupportof the expansion, varioustools from the theory and practice of economicintelligence and counterintelligence. Characteristics of selectedintelligenceanalysistechniqueshavebeenmade, including a wealth of descriptions of factors, trends, hypotheses, scenarios, recommendations, and assessments. The articlealsoshows the nature, objectives and principles of action of counterintelligenceactivitiesprotection, brought to performing well-thoughtcooperation with staff.

Keywords:expansion of the enterprise, safety, safetythreats, counterintelligenceprotection, Intelligence analysis

Wstęp

Nauka o przedsiębiorstwie we współczesnym jej wydaniu ujmuje wiele obszarów jego funkcjonowania w gospodarce, m.in. opis zagadnień zarządzania przedsiębiorstwem. Dużo uwagi poświęca się również ocenie wyników finansowych i wartości przedsiębiorstwa. Wprawdzie nie brak także haseł dotyczących samej przedsiębiorczości i rozwoju przedsiębiorstwa, ale odczuwa się niedosyt w opisie samej problematyki ekspansji, która stanowi kluczowy przejaw funkcjonowania przedsiębiorstwa. Niezwykle istotnym zagadnieniem zwłaszcza wobec postępującej globalizacji, jawi się ocena zagrożeń związanych z zagraniczną ekspansją przedsiębiorstw.

Celem artykułu jest wskazanie na możliwości minimalizowania ryzyka w przypadku zagranicznej ekspansji przedsiębiorstw poprzez wykorzystanie narzędzi analizy wywiadowczej i osłony kontrwywiadowczej oraz zwrócenie uwagi na ich znaczenie w praktyce bezpieczeństwa biznesu, a także na potrzebę koniecznego kształcenia przyszłych menedżerów w tym zakresie. Problematyka ta jest ciągle nową i wymaga szerokiego upowszechniania dla potrzeb budowania kolejnej istotnej kompetencji kadry menedżerskiej. Artykuł w pierwszej części zawiera opis przesłanek wyboru kierunków zagranicznej ekspansji oraz narzędzi wsparcia decyzji w postaci technik analizy wywiadowczej. Mają one na celu wskazanie na możliwości uchwycenia istotnych zagrożeń oraz sposobów ich minimalizowania, także przy uwzględnieniu nie tylko trendów i procesów, ale również kontekstu osobowego. Samo podjęcie ekspansji oraz jej realizacja wymaga także budowania kolejnej kompetencji w postaci tworzenia osłony kontrwywiadowczej siłami organizacji przedsiębiorstwa. Ma ona na celu utrzymanie zdobytej przewagi konkurencyjnej i jej umocnienie. Kluczem do sukcesu w realizacji poczynań kontrwywiadowczych jest rozwój konceptualizacji, metod i działań związanych z ochroną depozytu informacji wśród personelu przedsiębiorstwa.

Zasadniczym przesłaniem artykułu jest zatem wizja holistycznego spojrzenia na zagadnienie ekspansji przedsiębiorstwa, szczególnie zagranicznej, która wiąże się z koniecznością podjęcia często dużego ryzyka. Jest to szczególnie istotne w dobie kończącej się ery zarządzania w warunkach konkurencji, na rzecz rozwijającej się dynamicznie ery zarządzania w warunkach konfrontacji, która zaczyna powoli dominować w globalnym biznesie. Nie od rzeczy jest również zwrócenie uwagi na konieczność zapewnienia bezpieczeństwa realizacji wszelkich kontraktów biznesowych opartych na częstokroć zawiłej literze prawa. Rozpoznanie wszelkich ryzyk wiąże się zatem także z potrzebą budowania potencjału osłony kontrwywiadowczej w ekspansji przedsiębiorstw. Wszelkie te konieczne do rozwijania kompetencje menedżerskie stają się dziś zatem niezbędne dla realizacji procesu rozwoju przedsiębiorstwa.

Przesłanki wyboru kierunku ekspansji przedsiębiorstw

Ekspansja ekonomiczna należy do tych współczesnych obszarów aktywności w sferze gospodarczej, która polega na rozszerzeniu sfery wpływów nie tylko w postaci poszerzania rynków zbytu, ale także wpływów politycznych. Sama ekspansja jest immanentną koncepcją działania przedsiębiorstwa, gdyż jest ono strukturą, która z natury rzeczy mocą woli inwestorów (właścicieli) dąży do stałego rozszerzania kręgu klientów (interesariuszy).

Do zasadniczych ogólnych motywów (przesłanek) współczesnej ekspansji przedsiębiorstwa, uwzględniając złożoność oraz dynamikę otoczenia, a także geograficzne rozszerzanie swoich wpływów, należy zaliczyć:

- zwiększanie zysku,
- rozszerzanie rynków zbytu,
- wynik oceny ryzyka związanego z podjęciem i realizacją współpracy gospodarczej.

Zasadniczym motywem podjęcia ekspansji przez przedsiębiorstwo jest potrzeba ciągłego zwiększania zysku. Jeden ze sposobów to wyjście z realizowaną działalnością poza granice kraju. Wskutek ekspansji zagranicznej przedsiębiorstwa mogą zwiększać swoje zyski w sposób nieosiągalny lub bardzo trudny do realizacji na rynku krajowym.

Decyzja o podjęciu ekspansji zagranicznej stanowi złożony proces. Motywy szczegółowe zagranicznej orientacji działalności przedsiębiorstw można podzielić na: ekonomiczne, rynkowe i prawne.[1] W przypadku pierwszym inwestor działa z zamiarem uzyskania maksymalizacji efektu. Dotyczy to zarówno zwiększenia rynku zbytu, jak i zmniejszenia kosztów produkcji. Motyw drugi wiąże się z praktyką lepszego postrzegania przedsiębiorstw silnie zinternalizowanych, o mocnej pozycji przetargowej uzyskanej m.in. dzięki stosowaniu nowoczesnych narzędzi marketingowych. W ramach trzeciego motywu dostrzec można protekcjonizm państwowy oraz łagodniejsze przepisy prawne, sprzyjające ekspansji.

W przypadku polskich przedsiębiorstw zasadniczym motywem ekspansji jest poszukiwanie perspektywicznego rynku zbytu. Niestety, problem bezpieczeństwa inwestycji oraz osobiste kontakty zajmują odległe miejsce w strukturze szczegółowych motywów ekspansji.

Rozpatrując formy zagranicznej ekspansji przedsiębiorstw można wyróżnić następujący podział:

1) ze względu na umiędzynarodowienie sfery wymiany:
   - eksport pośredni,
   - eksport bezpośredni,
2) ze względu na powiązania kooperacyjne:
   - licencje,

1 Wach K., *Działalność gospodarcza w Unii Europejskiej. Wybrane zagadnienia.* Katedra Przedsiębiorczości i Innowacji, Akademia Ekonomiczna w Krakowie, Kraków 2005, s. 47.

- kontrakty na dostawy,
- kontrakty menedżerskie,
- wspólne przedsięwzięcia *(joint venture),*

3) ze względu na samodzielną działalność zagraniczną:

- oddział,
- filia[2].

Wraz ze wzrostem poziomu zaangażowania rosną potencjalne korzyści w postaci potencjalnych zysków (renta od ryzyka). Wzrasta także poziom wiedzy izdobywanych doświadczeń. Nieuchronnie wzrasta także poziom ryzyka niepowodzenia przedsięwzięcia.

Wybór kierunku zagranicznej ekspansji przedsiębiorstw częstokroć podyktowany jest okolicznościami, jakie mogą determinować decyzję o podjęciu ekspansji i jej przebieg, a zwłaszcza korzystne sploty okoliczności o charakterze okazji.

Okazją w działalności przedsiębiorstwa nazywa się nieoczekiwane wydarzenie, sposobność czy zaskakujący, wyjątkowo korzystny splot okoliczności, który – dostrzeżony w porę – może przynieść przedsiębiorstwu pewne wymierne lub niewymierne korzyści gospodarcze. Okazja ujawnia się także w ramach ekspansji międzynarodowej[3].

Okazja identyfikowana jest na drodze intuicyjnego pojmowania, co implikuje problem jej niewymierności, a zatem na trudności z ilościową oceną wpływu, jaki ma wykorzystanie okazji na taki element, jak chociażby konkurencyjność przedsiębiorstwa na zagranicznym rynku. Można przyjąć, że im wyższa różnica pomiędzy wartością oczekiwaną transakcji uznanej za okazję a wartością oczekiwaną transakcji uznanej za standardową i godziwą w danych uwarunkowaniach, tym dana okazja może być uznana za bardziej atrakcyjną[4].

Przykładowo, jeśli rozważana jest ekspansja międzynarodowa przedsiębiorstwa drogą eksportu bezpośredniego, a okazją jest np. nieoczekiwane wygranie przetargu na rynku zagranicznym, to wartość oczekiwana okazji będzie równa wartości kontraktu oraz prawdopodobieństwa, że główny konkurent wycofa swoją ofertę. Taka definicja okazji zwraca uwagę na kilka jej cech, do których wypada zaliczyć: ponadprzeciętność, subiektywizm postrzegania oraz nagłość i krótki czas trwania[5].

Ponadprzeciętność okazji zaznacza się głównie dwiema cechami: z jednej strony okazja zaznacza w sobie cechy niezwykłości, a z drugiej strony – dzięki jej wykorzystaniu przedsiębiorstwo spodziewa się uzyskać pewne dodatkowe ko-

2 E. Dąbrowska, D. Cielecki, *Ekspansja międzynarodowa polskich przedsiębiorstw po przystąpieniu Polski do Unii Europejskie,* s. 125-126 [dostęp: 05.05.2017].

3 R. Mrówka, M. Pindelski, *Zobaczyć pewne okazje (1)*, „Personel i Zarządzanie" 2009, nr 3, s. 26–29.

4 Zob. R. Krupski, *Okazje w zarządzaniu strategicznym przedsiębiorstwa*, Komitet Nauk Organizacji i Zarządzania PAN , Szkoła Głowna Handlowa, „Organizacja i Kierowanie", 2011, nr 4 (147), s.12.

5 E Rakowska, *Okazje w ekspansji międzynarodowej przedsiębiorstwa*, w: *Ekspansja polskich firm na rynki międzynarodowe*, red.R. Sobiecki, J. W. Pietrewicz, Oficyna Wydawnicza SGH w Warszawie, Warszawa 2014, s. 142.

rzyści – ponadprzeciętny efekt. W tym wypadku oznacza on międzynarodową ekspansję, która w innych okolicznościach nie zostałaby podjęta.

Subiektywizm postrzegania okazji zaznacza się poziomem percepcji danego menedżera. Oznacza to, czy dana osoba dostrzeże okazję, czy uzna, że warto ją wykorzystać, jaką nada jej wartość oraz jaką decyzję podejmie w odniesieniu do jej wykorzystania na każdym etapie jej cyklu życia. Jest to z kolei pochodną podatności danej osoby na ryzyko, bowiem skutek wykorzystania okazji jest niepewny, zależy od uprawnień decyzyjnych, a także – postaw i wartości, jakie prezentuje.

Krótkotrwałość okazji oznacza pewien skończony czas, kiedy okazja może być wykorzystana. Wraz z upływem czasu może ona ulec dezaktualizacji lub koszty jej wykorzystania mogą znacznie wzrosnąć.

Jako realizację okazji wyłaniającej się należy uznać jako przykład pomoc techniczną udzielaną przez Narodowy Bank Polski (NBP) przedstawicielom banków centralnych krajów rozwijających się (zwanych dalej beneficjentami). Współpraca techniczna banków centralnych polega na międzynarodowej wymianie doświadczeń w rożnych obszarach działalności banku centralnego. Sprzyja to zawiązywaniu relacji międzynarodowych i promowaniu tą drogą rodzimych przedsiębiorstw, mogących dostarczać produkty i usługi na potrzeby sektora bankowości centralnej.

Współpraca techniczna z bankami centralnymi państw przechodzących transformację gospodarczą, niebędących państwami członkowskimi Unii Europejskiej (UE), które dzięki poznawaniu doświadczeń bardziej rozwiniętych krajów modyfikują swoją działalność w kierunku spełniania międzynarodowych standardów, stwarza szczególną okazję. Sytuację, w której beneficjent zgłasza potrzebę szkoleniową w wybranym obszarze bankowości centralnej NBP i w dowolnej formie, można uznać z perspektywy polskiego przedsiębiorstwa za okazję.

Udzielanie pomocy przez NBP dają rożne możliwości w zakresie kreowania okazji do międzynarodowej ekspansji:

- seminaria i warsztaty, w których uczestniczy średnio 10–30 przedstawicieli banków centralnych, sprzyjają wymianie doświadczeń w szerokim gronie uczestników. Jest to okazja, by zaprezentować produkty i/lub usługi w trakcie rozmów kuluarowych i wykładu,
- kilkudniowe wizyty studyjne oraz pobyty stażowe odbywają się w bardziej kameralnym gronie i stanowią źródło okazji do nawiązania relacji nieformalnych. Beneficjenci z krajów rozwijających się chętnie korzystają z przekazywanych doświadczeń oraz nawiązują podczas pobytu kontakty biznesowe,
- wyjazdy eksperckie pracowników NBP do banku beneficjenta w celu udzielenia konsultacji merytorycznych na miejscu stanowią okazję do podzielenia się doświadczeniem z zakresu współpracy z przedsiębiorstwami prywatnymi bezpośrednio z pracownikami wykorzystującymi podobne produkty i systemy w banku centralnym innego kraju[6].

6 Tamże, s. 151.

Podane powyżej formy pomocy spełniają kryteria uznania ich za okazję, ponieważ:

- przedsiębiorstwo współpracujące z NBP będzie w stanie szybko zaoferować sprofilowany na potrzeby innego banku centralnego produkt i/lub usługę, gdyż zna specyfikę tej szczególnej branży i to stanowi jego przewagę konkurencyjną. W przypadku krajów wschodnich współpraca biznesowa opiera się na kontakcie osobistym, dlatego okazja ta jest bardziej atrakcyjna, ponieważ wiąże się z możliwością praktycznie bezpłatnego i bezpośredniego nawiązania kontaktu,
- są niespodziewane – prośba o zorganizowanie szkolenia pojawia się z miesiąca na miesiąc, a w przypadku zaplanowanego wydarzenia – około pół roku, rok wcześniej. Okazja, jaką jest takie szkolenie, trwa bardzo krótko – od kilku dni do jednego, dwóch tygodni. Stanowi w istocie właściwie jedyną taką okazję, by nawiązać bezpośredni kontakt z przedstawicielami banku centralnego drugiego kraju,
- cechuje je subiektywizm postrzegania – nie każde przedsiębiorstwo będzie postrzegać okazje jako atrakcyjne i pożądane dla swojego rozwoju. Dla jednego bowiem decydenta może to stanowić okazję atrakcyjną z punktu widzenia perspektyw rozwoju, dla innego ryzyko ekspansji na rynki wschodnie może być zbyt duże[7].

Beneficjenci korzystający z pomocy technicznej NBP zawiązują nieformalne relacje, które jednocześnie wskazywane są jako jedno z kluczowych uwarunkowań podczas prowadzenia działalności gospodarczej na rynkach wschodnich.

I tak z ogólnej liczby wydarzeń pomocowych na rzecz banków centralnych poszczególnych krajów, zrealizowanych przez NBP w latach 2009–2011 dominowały:

- Ukraina 66 przypadków,
- Rosja 37 przypadków,
- Azerbejdżan i Białoruś po 31 przypadków,
- Serbia przypadków 29,
- Mołdawia przypadków 27[8].

Ryzyko nawiązywania kontaktów zagranicznych może być zwi**ązane** z czynnikami obiektywnymi, począwszy od:

- nieznajomości języka ewentualnego kontrahenta, poprzez
- brak wiedzy na temat zwyczajów handlowych obowiązujących na danym rynku,
- aż – co najważniejsze – po nieumiejętność stosowania przepisów prawa normujących w tym państwie obrót gospodarczy. Nie od rzeczy jest także znajomość praktyki biznesowej wynikającej z kontekstu osobowego i powiązań (układów) biznesowych.

7 Tamże, s. 152.
8 Tamże, s. 153.

Brak praktyki posługiwania się miejscowym kodeksem handlowym uniemożliwia wykrycie istniejących w nim luk prawnych, których znajomość od razu stawia potencjalnego partnera zagranicznego w uprzywilejowanej sytuacji.

Istnieje też czynnik czysto subiektywny, bardzo często pomijany przy dokonywaniu wstępnej analizy opłacalności przeprowadzenia transakcji handlowej z zagranicznym partnerem. Polscy przedsiębiorcy w większości przypadków nadal jeszcze nie przyjmują do wiadomości, że zagraniczny kontrahent – zwłaszcza jeśli działa na renomowanym, cieszącym się doskonałymi tradycjami rynku zbytu – może być zwyczajnym oszustem lub naciągaczem.

Tymczasem praktycy z firm windykacyjnych czy ubezpieczeniowych, zwłaszcza zajmujący się relacjami gospodarczymi zachodzącymi między firmami krajowymi a zagranicznymi, ostrzegają, iż sporo polskich firm obdarza zachodnich przedsiębiorców nieuzasadnionym zaufaniem, co niestety coraz częściej kończy się mniej lub bardziej dotkliwymi stratami.

Jest oczywiste, że w krajach, gdzie gospodarka rynkowa funkcjonuje od kilkudziesięciu, czy wręcz kilkuset lat, wypracowano skuteczniejsze niż w Polsce mechanizmy ochronne zapewniające bezpieczeństwo obrotu.

Ale nigdzie nie udało się – i nie uda – w pełni wyeliminować nieuczciwości!

Podobnie jak w przypadku oceny wiarygodności partnera krajowego, sprawdzanie kontrahenta zagranicznego można przeprowadzić w oparciu o wewnętrzne zasoby kadrowe i dokumentacyjne własnej firmy, bądź też zebranie informacji zlecić wyspecjalizowanemu przedsiębiorstwu.

Pierwszy sposób jest zdecydowanie tańszy, bo z reguły nie wiąże się z koniecznością ponoszenia dodatkowych nakładów finansowych, ale też w wielu konkretnych przypadkach okazać się może zawodny. Krajowa firma produkcyjna lub usługowa z reguły dysponuje ograniczona wiedzą na temat ryzyka kraju potencjalnego kontrahenta, panującej tam specyfiki zwyczajów płatniczych, czy też powiązań i układów personalnych.

Znacznie bardziej niż na miejscu ograniczone są możliwości korzystania z „poczty pantoflowej", a odległość od kraju potencjalnego partnera handlowego powoduje osłabienie sygnałów wczesnego ostrzegania, a tym samym ogranicza możliwość reakcji na pogarszający się standing zagranicznej firmy.

Oczywiście wskazane jest pozyskiwanie informacji poprzez prywatnych i biznesowych przyjaciół, stosowanie zabezpieczeń umownych, konsultowanie projektu podpisywanej umowy z prawnikami znającymi uwarunkowania rynku danego odbiorcy. Generalnie jednak warto sprawdzać przyszłych kontrahentów w wywiadowniach gospodarczych, głównie tych o międzynarodowym, a nie tylko lokalnym, zasięgu. Koszty takiego przedsięwzięcia nie wykraczają poza możliwości zdecydowanej większości podmiotów gospodarczych.

Skuteczności korzystania z usług wywiadowni w kontekście sprawdzania zagranicznych partnerów nie da się jednoznacznie określić. Pośrednio jednak potwierdza ją fakt, iż od czasu włączenia Polski do struktur Unii Europejskiej liczba

raportów o podmiotach zagranicznych, opracowywanych przez wywiadownie na zlecenie rodzimych biznesmenów, wzrosła o ponad 400 proc.

Rozwój międzynarodowej współpracy gospodarczej i liberalizacja światowego handlu sprawiają, że uczestniczy w nim coraz więcej firm. Są one bardzo różne – dobre i złe, respektujące swoje zobowiązania i działające w sposób nieuczciwy.

Uczestnicy obrotu międzynarodowego dobrze wiedzą, że można spotkać dobre przedsiębiorstwa w krajach uznawanych za ryzykowne i złe – w krajach uchodzących za bezpieczne do prowadzenia interesów. Z drugiej jednak strony muszą oni pamiętać, iż rzeczywiste ryzyko jest funkcją specyfiki konkretnego przedsiębiorstwa oraz kraju, w którym ono funkcjonuje. Z punktu widzenia zagranicznego kontrahenta rzeczą niezwykle ważną jest przeanalizowanie, w jakim stopniu sytuacja polityczna, gospodarcza i finansowa kraju wpływa na regulowanie zobowiązań finansowych miejscowych firm. Od tego bowiem w dużym stopniu zależy bezpieczeństwo transakcji zawieranych z firmami danego kraju.

Takie właśnie zadanie spełnia przygotowywany przez wywiadownię gospodarczą Coface system ocen przyznawanych poszczególnym krajom. Mierzy on przeciętny poziom ryzyka nieuregulowania płatności krótkoterminowych zobowiązań przez przedsiębiorstwa. Wskazuje też, w jakim stopniu na zobowiązania finansowe przedsiębiorstwa wpływają perspektywy ekonomiczne, finansowe i polityczne danego kraju.

Noty przyznawane 152 krajom świata opierają się na podwójnej ekspertyzie prowadzonej przez Coface. Są to:

- ekspertyza makroekonomiczna, biorąca pod uwagę ocenę ryzyka kraju z uwzględnieniem całego arsenału wskaźników makroekonomicznych, finansowych i politycznych,
- ekspertyza mikroekonomiczna, dokonywana na podstawie analizy płatności ponad 50 mln przedsiębiorstw z całego świata, znajdujących się w bazach danych Coface.

W ekspertyzach tych bierze się pod uwagę siedem ściśle zdefiniowanych rodzajów ryzyka:

- podatność na zmiany w koniunkturze,
- ryzyko wystąpienia w danym kraju kryzysu walutowego,
- poziom zadłużenia zagranicznego,
- stan finansów państwa,
- bezpieczeństwo systemu bankowego,
- sytuacja polityczna i pozycja rządu,
- postępowanie przedsiębiorstw w regulowaniu płatności

Ostateczna nota przyznawana jest każdemu ze 152 krajów świata w oparciu wymienionych wyżej 7 kryteriów. Skala ocen, w kolejności od najmniejszego do największego ryzyka składa się z 7 stopni: A1, A2, A3, A4, B, C i D.

Skala ocen ryzyka:

A1 – stabilna sytuacja ekonomiczna i polityczna w kraju, niewielkie ryzyko niewypłacalności

A2 – gorsza sytuacja ekonomiczna i polityczna w kraju, niewielkie ryzyko niewypłacalności

A3 – gorsza sytuacja ekonomiczna i polityczna w kraju, możliwe opóźnienia w płatnościach, niewielkie ryzyko niewypłacalności,

A4 – groźba pogorszenia sytuacji ekonomicznej i politycznej kraju, postępowanie firm w dziedzinie płatności – do przyjęcia, ryzyko niewypłacalności wyższe,

Skala ocen ryzyka:

B – niepewna sytuacja ekonomiczna i polityczna kraju, złe zachowania płatnicze firm, wysokie ryzyko niewypłacalności,

C – zła sytuacja ekonomiczna i polityczna kraju, zachowania płatnicze firm – złe i mogą się jeszcze pogorszyć, wysokie ryzyko niewypłacalności,

D – bardzo zła sytuacja ekonomiczna i polityczna kraju, bardzo wysokie ryzyko niewypłacalności.

Analiza wywiadowcza jako narzędzie wsparcia zarządzania ekspansją

Analiza wiąże się z procesem transformacji zebranych „surowych" informacji, danych, pogłosek itp. w ich konkretyzację w postaci opisów, wyjaśnień, interpretacji, hipotez, ocen, prognoz, konkluzji, scenariuszy, rekomendacji itp. czynionymi zgodnie z zaspokojeniem potrzeb informacyjnych decydentów. Narzędzie analizy w wywiadzie nie jest narzędziem doskonałym, m. in. ze względu na:

- wykorzystywanie ludzkiego mózgu jako swoistego narzędzia nie do końca dostosowanego do rozwiązywania problemów analitycznych. Zauważa się to szczególnie w ramach uproszczonego rozumowania opartego na modelach myślowych, co może prowadzić do niebezpiecznych błędów analitycznych. Konieczne jest zatem stosowanie tytułem wsparcia analizy zastosowań w postaci ustrukturyzowanych metodologii,
- wymaga przeprowadzenia oceny stanu zrozumienia wyników przeprowadzonych analiz przez samych decydentów, działających dodatkowo pod ogromną presją czasu,
- subiektywny charakter percepcji wszelkich uczestników procesu analizy, a także odbiorców jej wyników – konieczne pozyskanie maksimum wiedzy o samym decydencie,
- gwałtowność i nieprzewidywalność zmian otoczeniowych zdecydowanie wyprzedza założenia modeli myślowych, wymagających modyfikacji.[9]

Zasadnicze zastosowanie ma analiza jakościowa. Jest ona podstawowym narzędziem interpretacji informacji, nadającym się do zastosowań wobec zagad-

9 Zob. A. Bielska, *Wywiad biznesowy w działalności gospodarczej: podstawowe aspekty, które należy wziąć pod uwagę*, w: *Wywiad biznesowy. Praktyczne wprowadzenie.* Wydawnictwo Nieoczywiste, Warszawa 2017, s. 51 i nast.

nień trudno mierzalnych. Wybór metod analizy jest szeroki; obejmuje możliwości typowe dla wywiadu gospodarczego, ale także dla analizy strategicznej stosowanej w przedsiębiorstwie, aż po stosowane w analizie wywiadowczej w sektorze bezpieczeństwa narodowego oraz służbach policyjnych.

Dokonując przeglądu technik analizy wywiadowczej, dostępnych już w literaturze na polskim rynku księgarskim, można skłaniać się do wyboru bardziej ogólnych, niemniej bardzo wartościowych. Należą do nich:

- Skanowanie Środowiskowe i Analiza PESTLE, celem których jest identyfikacja i analiza czynników, a także trendów wpływających na zewnętrzne środowisko działania przedsiębiorstwa,
- Analiza Przyczyn Źródłowych, która pozwala na zidentyfikowanie sił i relacji, kształtujących czynniki i trendy wyznaczone za pomocą Analizy PESTLE,
- Analiza Trendów/Wpływu pozwalająca na identyfikację i ocenę wpływu, jaki wynika z działania różnego rodzaju trendów mogących zachować swój wpływ na funkcjonowanie przedsiębiorstwa, czy też branży, sektora, segmentu rynku i samego rynku,
- Analiza Kluczowych Założeń, mająca na celu identyfikację i krytyczną ocenę wprowadzanych założeń (twierdzeń, hipotez, opinii),
- Analiza Konkurencyjnych Hipotez, która pozwala na krytyczną ocenę alternatywnych hipotez,
- Analiza „Co, jeśli?", której celem jest rozważenie potencjalnego wpływu scenariuszy, wcześniej zupełnie nierozpatrywanych lub uznanych za mało prawdopodobne i w konsekwencji niepoddanych dalszej analizie.[10]

Techniki analizy wywiadowczej zawierają bogactwo opisów czynników, trendów, hipotez, scenariuszy, rekomendacji, ocen wykorzystujących na ogół informacje „twarde". Nie wyczerpuje to jednak opisu obrazu przedstawianego pod „hasłem jak jest", czy „jak może być". Opis taki wymaga wkomponowania informacji „miękkich", to znaczy zawierających osobową naturę sprawstwa zjawisk, trendów, hipotez itd. A zatem wymaga uzupełnienia opisu o pytanie „*who?*" Prowadzi to do uwzględnienia w analizach i ocenach wszelkich uwarunkowań i okoliczności „personalnego" tworzenia faktów i wiedzy o motywach i efektach działań przedsiębiorstw konkurenta, możliwych do wykorzystania z perspektywy zarządzania bezpieczeństwem. Zwraca jednak uwagę na ważkie czynniki:

- emocje,
- animozje,
- zażyłości,
- uprzedzenia osobiste, ale i sympatie,
- system podzielanych ideałów i wartości.

10 Zob. A. Bielska, *Analiza danych: techniki analizy jakościowej,* w: *Wywiad biznesowy. Praktyczne wprowadzenie.* Wydawnictwo Nieoczywiste, Warszawa 2017, s. 117 – 137.

Buduje to w efekcie bardzo złożony, ale dający się zidentyfikować obraz działań firmy konkurenta. Stwarza to także ogromny kapitał wiedzy, pozwalając na uruchomienie szerokich możliwości niezwykle subtelnych działań podejmowanych z korzyścią dla beneficjenta przetworzonych informacji, w tym dla potrzeb kształtowania bezpieczeństwa, zatem firmy organizującej skomplikowany aparat narzędziowy, program i strukturę wywiadu gospodarczego.

Osłona kontrwywiadowcza – istota, cele i funkcje działania

Konceptualizacja działań, organizacja i zadania kontrwywiadu gospodarczego w przedsiębiorstwie, dające podstawy osłony kontrwywiadowczej, stanowi swoiste *know how.* Kontrwywiad gospodarczy stanowi oryginalną, wyspecjalizowaną i posiadającą szeroką autonomię wewnętrzna strukturę informacyjno-analityczno-kontrolną przedsiębiorstwa. Zawiera także system działań, wypełniający zadania przewidywania, wczesnego wykrywania i neutralizacji zagrożeń dla bezpieczeństwa informacyjnego, pochodzących zarówno ze świata zewnętrznego firmy (wywiad konkurencyjny, wywiad polityczny i ekonomiczny, przestępczość, w tym szpiegostwo), jak i od strony destrukcyjnych działań podejmowanych w samej firmie. W istocie kontrwywiad gospodarczy stanowi przemyślany zespół idei, metod, motywów i sposobów (chociażby przez stawianie hipotez) rozumienia natury poczynań potencjalnych sprawców podejmowanych działań związanych z przejęciem ludzi/pracowników/menedżerów – głównie jako depozytariuszy informacji, a także procedur, praktyk, itp. podejmowanych zasadniczo przez konkurentów, oraz jako organizację i metody uruchamiania określonych skutecznych przeciwdziałań, w tym także ocenę ryzyka.

Szeroki zakres działań kontrwywiadu gospodarczego wyznaczony jest przez system celów o charakterystyce nadrzędnego i operacyjnego. Celem nadrzędnym kontrwywiadu gospodarczego jest niedopuszczenie do niekontrolowanego wyprowadzenia z firmy informacji stanowiących tajemnicę przedsiębiorstwa lub informacji niejawnych, mogących zagrozić jego pozycji rynkowej, zarówno w sytuacji bieżących działań, jak i w przyszłości. Jako cel operacyjny kontrwywiadu gospodarczego wyznacza się rozpoznawanie i zbieranie dowodów na nielojalność i przestępstwa popełniane przez pracowników, osoby zarządzające i właścicieli firmy oraz kooperantów działających na szkodę organizacji.

Kontrwywiad gospodarczy jest niezwykle wysublimowaną konstrukcją tworzoną przez zespół ludzi o wysokim poziomie profesjonalizmu, przygotowanych multidyscyplinarnie do podejmowanych działań, zespołu dochodzącego w dłuższym okresie do pełni swoich możliwości realizacji zadań. Stąd jego implementacja w przedsiębiorstwie wymagać będzie podjęcia wielu przemyślanych kroków.[11] O randze i znaczeniu prowadzonych analiz kontrwywiadowczych można wnioskować na podstawie następujących funkcji postępowania:

11 Szerzej o problematyce implementacji kontrwywiadu gospodarczego w przedsiębiorstwie zob.: M. Kwieciński, K. Passella, *Implementation of the business counterintelligence branch in enterprise structure.* [w:] *The Economic Security of Business Transactions.* Editet by K. Raczkowski and F. Schneider. Chartridge Books Oxford, Oxford 2013, s. 169 – 190, www.chartridgebooksoxford.com.

- spełnia rolę ostrzegawczą i bufora dla informacji wrażliwych, stanowiących unikalną wartość dla firmy,
- zwalcza metodami dopuszczonymi prawem wszelką działalność wywiadowczą, szpiegowską i przestępczą wobec firmy,
- potrafi wypracować hipotezy, znaleźć metody poprawy i dokonać wdrożenia, odnośnie eliminacji słabych punktów systemu ochrony działań przedsiębiorstwa,
- posiada zdolność zrozumienia i wychwycenia na bieżąco w otoczeniu firmy oraz jej wewnętrznych strukturach natury poczynań wywiadu konkurencyjnego i działalności przestępczej,
- identyfikuje i skutecznie odseparowuje potencjalnych sprawców przejęcia informacji, procedur, praktyk istotnych dla przetrwania i rozwoju firmy na konkurencyjnym rynku,
- stanowi wewnętrzną ucząca się organizację, doskonalącą metody skutecznego przeciwdziałania próbom naruszenia integralności i bezpieczeństwa informacyjnego firmy,
- stanowi również zespół potrafiący wypracować metody oceny ryzyka i przeprowadzić analizę sytuacji.

Uwzględniając powyższe można stwierdzić, że kontrwywiad gospodarczy jako wewnętrzna służba ochrony informacyjnej stanowi swoistą organizację w strukturze przedsiębiorstwa, o wyraźnie zaznaczonej wysokiej kulturze organizacyjnej, profesjonalizmie oraz zdolności do zapewnienia niezakłóconego jego funkcjonowania w twardej rzeczywistości konkurencyjnego rynku. Jako pion specjalnego znaczenia działa na rzecz potrzeby ochrony informacji jako kluczowego aktywu decydującego o konkurencyjności przedsiębiorstwa) poprzez postawienie na człowieka/pracownika/menedżera jako centrum – kluczowego podmiotu i depozytariusza informacji, który to powinien podlegać specjalnym zabiegom prowadzącym do zachowania niezbędnego poziomu bezpieczeństwa.

Praca z personelem jako sposób minimalizowania ryzyka personalnego

Zasadniczym celem wysiłków kontrwywiadowczych jest wykrywanie wrogiej działalności przeciwko przedsiębiorstwu poprzez pracę z członkami personelu, czy tym przypadku ze źródłami osobowymi. Obserwacja personelu zawierać powinna cały system działań zorganizowanych obejmujących:

- identyfikację czynników ryzyka osobowego,
- określenie miejsc potencjalnego ryzyka wycieku informacji w strukturze zarządzania przedsiębiorstwem,
- monitorowanie działań personelu pod kątem wykrywania alternatywnych sposobów wycieku informacji,
- działania analityczne prowadzące do wyłonienia typologii informatorów, ze wskazaniem na członków personelu mogących być nieświadomym źródłem informacji, bądź prowadzących zamierzoną dywersję.

- prowadzenie aktywnego postępowania poprzez przeprowadzanie długookresowej, wielowątkowej i drobiazgowej analizy konkretnych zachowań wskazujących na pracownika – źródło wycieku informacji (wskazanie na tzw. „kreta"),
- prowadzenie równoległego z powyżej określonym postępowania mającego na celu ujawnienie sieciowych powiązań informacyjnych pracownika – „kreta", budowanych za pomocą różnorodnych metod (w tym szantażu) werbunku osoby – depozytariusza informacji z grona współpracowników,
- identyfikację osób mogących mieć podejrzane kontakty zewnętrzne, zaangażowanych w szkodliwą dla przedsiębiorstwa działalność wywiadowczą lub szpiegowską.

Wewnętrzne źródła zagrożeń bezpieczeństwa działalności, w tym także bezpieczeństwa informacyjnego, tkwią wyraźnie po stronie ludzi, głównie menadżerów i pracowników. Intensyfikacja zagrożeń wywoływana jest niewłaściwymi postawami. I tak, jeżeli menadżerowie charakteryzują się nieetycznymi zachowaniami wobec pracowników, w szczególności stosując:

- mobbing wobec wybranych osób i grup,
- ciągłe zastraszanie utratą pracy, wskazywanie na niepewną przyszłość zatrudnionych,
- niejasne reguły wypłaty dodatkowych wynagrodzeń,
- wywyższanie się nad pracownikami swoim statusem majątkowym, koneksjami, wpływami na aparat lokalnej władzy,
- jako jedyny środek podniesienia rentowności nacisk psychiczny na zwiększenie zaangażowania pracowników, połączony z wulgarnym zachowaniem,
- jako normę niskie zarobki, sprowadzające egzystencję pracownika do roli finansowego niewolnika zakładu pracy, to wcześniej czy później staną się łatwym celem dla wywiadu gospodarczego konkurencji (legalnego) i szpiegostwa przemysłowego (nielegalnego) wspartego ruchami wewnętrznymi, odwetowymi pracowników, nieidentyfikujących się w takich przypadkach z zatrudniającym ich przedsiębiorstwem.

Jak można zatem przypuszczać zagrożenia wewnętrzne bezpieczeństwa działalności przedsiębiorstwa wynikają w decydującej mierze z przyjętych postaw, zarówno personelu zarządzającego, jak i wykonawczego. Wszelkie następne zagrożenia ujawniają się na skutek nierzetelności, lekceważenia obowiązków, braku nadzoru, braku orientacji na przyszłość we wszelkich poczynaniach itp. Wymienione postawy wskazują na niski poziom lojalności, zarówno wobec samego inwestora (właściciela kapitału) – organizatora działań przedsiębiorstwa, jak i wobec zatrudnionego w nim personelu.

Działalność osłony kontrwywiadowczej wiąże się zatem z jednej strony z organizacją różnorodnych specyficznych działań podejmowanych wobec członków personelu, ale także określaniem wytycznych dla całości polityki bezpieczeństwa przedsiębiorstwa. Bezpieczeństwo przedsiębiorstwa stało się bowiem

ważnym i nieodłącznym elementem całości koncepcji podejmowanego biznesu. Winna ona uwzględniać sięganie po niezwykle wysublimowane „miękkie" metody obserwacji personelu, realizowanej głównie podczas uczestnictwa w podejmowanych procesach biznesowych oraz reagowania na niepożądane postępowanie personelu przedsiębiorstwa.

Zakończenie

Bogactwo problematyki poruszanej w niniejszym artykule uprawnia do podjęcia intensywnych poszukiwań badawczych, jak i wysiłków dydaktycznych. Miałyby one na cele pogłębienie wiedzy na temat budowania potencjału bezpieczeństwa działalności przedsiębiorstw jako kluczowej kompetencji menedżerskiej. Niestety, obserwacja poczynań kształceniowych oraz budowania ofert w szkolnictwie wyższym w tym zakresie nie nastrają jak dotąd optymistycznie. Generalnie wychodzi się z założenia, że jak coś jawi się jako trudne, to najlepiej tego nie podejmować i jakoś się to samo rozwiąże. Tymczasem praktyka biznesowa wybiegła już daleko naprzód, co wymuszać będzie konieczność podejmowania kształcenia w opisywanej problematyce. Wykład monograficzny z warsztatami dotyczący kształcenia w zakresie zarządzania strategicznego przedsiębiorstwem nie zaspakaja absolutnie potrzeby w tym zakresie.

Potwierdzeniem istnienia ogromnego dystansu w zakresie kształcenia w ramach problematyki zarządzania bezpieczeństwem działalności przedsiębiorstwa jest fakt, iż w Europie Zachodniej już od dawna kształci się studentów w obszarze studiów nad wywiadem i studiów nad służbami specjalnymi. Rodzi to określone przewagi, także w ramach rozwoju kapitału intelektualnego, prowadzące do daleko bardziej skutecznej ekspansji zachodnioeuropejskich przedsiębiorstw, niż to czynią z nielicznymi wyjątkami polskie przedsiębiorstwa. Potwierdzeniem niedojrzałości biznesowej menedżerów polskich przedsiębiorstw w obszarze zagranicznej ekspansji są coraz liczniejsze obserwowane przypadki aresztowań członków zarządów spółek publicznych, którym zarzuca się brak kompetencji, niedopilnowanie obowiązków albo wręcz przyjęcie łapówek za podjęcie nieprzemyślanych kierunków ekspansji, które narażają Skarb Państwa na ogromne straty.

Jednym z kluczowych, a ciągle nie docenianych obszarów zarządzania w przedsiębiorstwie jest problematyka kształtowania i rozwijania lojalności personelu. Lojalność personelu przedsiębiorstwa należy rozpatrywać głównie z perspektywy oceny poziomu bezpieczeństwa, szczególnie w warunkach niezwykle ostrej rywalizacji na rynku. Prowadzone analizy kontrwywiadowcze (w tym badania poligraficzne) powinny dawać podstawy dla wiedzy o rosnącym, bądź obniżającym się poziomie lojalności. Stanowić mogą także doskonały barometr dotyczący oceny nastrojów zatrudnionego personelu. Wykrycie aktów braku lojalności informuje kierownictwo o pogarszającym się stanie klimatu dochowywania standardów, dając także dowody potwierdzające znaczenie działań wewnętrznych

pionów kontrwywiadowczych, jak również ma wpływ na konieczność szybkiego podjęcia przemyślanych działań naprawczych. Wymagać też będzie uruchomienia bardziej zdecydowanych kroków związanych z pracą nad personelem przy aktywnym udziale specjalistów kontrwywiadu gospodarczego.

Bibliografia

Dąbrowska E., Cielecki D., *Ekspansja międzynarodowa polskich przedsiębiorstw po przystąpieniu Polski do Unii Europejskiej.*

Krupski R., *Okazje w zarządzaniu strategicznym przedsiębiorstwa*, Komitet Nauk Organizacjii Zarządzania PAN, Szkoła Głowna Handlowa, „Organizacja i Kierowanie", 2011, nr 4 (147).

Kwieciński M., Passella K., *Implementation of the business counterintelligence branch in enterprise structure.* [w:] *The Economic Security of Business Transactions.* Editet by K. Raczkowski and
F. Schneider. Chartridge Books Oxford, Oxford 2013.

Mrówka R., Pindelski M., *Zobaczyć pewne okazje (1)*, „Personel i Zarządzanie" 2009, nr 3.

Rakowska E., *Okazje w ekspansji międzynarodowej przedsiębiorstwa*, w: *Ekspansja polskich firm na rynki międzynarodowe*, red. R. Sobiecki, J. W. Pietrewicz, Oficyna Wydawnicza SGH w Warszawie, Warszawa 2014.

Wach K., *Działalność gospodarcza w Unii Europejskiej. Wybrane zagadnienia.* Katedra Przedsiębiorczości i Innowacji, Akademia Ekonomiczna w Krakowie, Kraków 2005.

Wywiad biznesowy. Praktyczne wprowadzenie. Red. A. Bielska, Wydawnictwo Nieoczywiste, Warszawa 2017.

Mirosław Kwieciński*

***prof. dr hab. Mirosław Kwieciński,**
Krakowska Akademia im. Andrzeja Frycza Modrzewskiego

Teresa Przybyszewska

Tworzenie potencjału innowacyjnego zespołu wywiadowczego (kontrwywiadowczego) przedsiębiorstwa

Streszczenie

Market intelligence i *competitiveintelligence* to dyscypliny ukierunkowane na dostarczanie wysoko jakościowych informacji, wspierających decyzje w zakresie m.in. marketingu, sprzedaży czy też projektowania produktu. W niniejszym artykule dokonano krótkiego przeglądu literatury przedmiotu w zakresie kluczowych determinant warunkujących wdrożenie koncepcji wywiadu gospodarczego w organizacji. Wynikiem końcowym opisanych dociekań jest przedstawienie innowacyjnego zastosowania podejścia działań wywiadowczych przez przedsiębiorstwo w obszarze odpowiedzialnym za zrządzanie zasobami ludzkimi.

Słowa kluczowe: *competitiveintelligence*, *market intelligence*, proces wywiadowczy, krytyczne determinanty, wdrożenie wywiadu gospodarczego, zarządzanie zasobami ludzkimi

1. Cykl wywiadu gospodarczego jako podstawa uwarunkowań dla budowanego zespołu

Określenie niezbędnych zasobów kadrowych to podstawa dla działania komórki/zespołu zajmującego się wywiadem gospodarczym. W literaturze przedmiotu istnieje kilka koncepcji podpowiadającej jak podejść do problemu[1], jednak wskazuje się, że idealny zespół to taki, który posiada w swoich zasobach osoby pozyskujące informacje pierwotne, zajmujące się zbieraniem informacji wtórnych, analityków dokonujących m.in. syntezy informacji oraz koordynatora, który harmonizuje wszystkie te działania. Często jednak dochodzi do sytuacji, w której to tylko jedna osoba wykonuje wszystkie wymienione zadania ze względu na braki kadrowe. Mimo to, zakłada się organizowanie struktur wywiadowczych, które mocno osadzone są na tradycyjnym cyklu wywiadowczym, gdzie tworzyć go będą: szef-menedżer, dział planistyczno-organizacyjny, baza danych (archiwum), dział analityczny, dział dystrybucji[2].

Nawiązując do powyższej koncepcji, firma wdrażając wywiad gospodarczy nie musi skalować rozwiązań wywiadowczych, aż na poziom biura, działu bądź

1 A. Bielska Za: C. Kalb, J.P. Herring, *Selectingtherightcompetitive Intelligence organizationalmodel*, „Competitive Intelligence Magazine" 2012, 15,1, s. 22-36.

2 M. Ciecierski, Wywiad biznesowy w korporacjach transnarodowych: teoria i praktyka. Wydawnictwo Adam Marszałek, 2009, s.246.

obszaru. Może je przenieść na poziom zespołu w strategicznych obszarach, w którym to poszczególne zadania będą wykonywać pracownicy w ramach przypisanych ról lub wyznaczone do tego osoby zatrudnione na pełen etat.

Proces wywiadu gospodarczego jest postępowaniem ciągłym, gdzie wszystkie fazy cyklu są ze sobą powiązane. Efekt jednego z nich decyduje o sukcesie kolejnego, stąd też osoby dedykowane do jednej lub więcej faz, powinny posiadać niezbędny zestaw umiejętności, aby skutecznie i wydajnie pracować w zakresie powierzonych im zadań.

Etapem wstępnym, ustalającym niezbędne zasoby[3], ale także identyfikującym cel i wynik projektu bądź też całego procesu wywiadowczego jest etap planowania[4]. Wobec tego wśród praktyków zajmujących się wywiadem biznesowym, poszukiwaną na pierwszym miejscu cechą, będą umiejętności analityczne niezastąpione w identyfikacji luk informacyjnych, a w następstwie do określenia potrzeb wywiadowczych. Częstym przypadkiem występującym w przedsiębiorstwach jest zjawisko nadkonsumpcji informacji, czego konsekwencją jest trudność w jej analizowaniu oraz wykorzystaniu do podjęcia odpowiednich decyzji, co wiąże się z ponoszeniem kosztów. Dlatego też specjaliści zajmujący się wywiadem będą musieli współpracować z menedżerami, celem odkrycia ich niezaspokojonych potrzeb w odniesieniu do podjęcia decyzji w planowanych działaniach. W oparciu o powyższe potrzeby jak również te bezpośrednio niezidentyfikowane przez menedżerów, specjalista będzie musiał przełożyć je na kluczowe tematy wywiadowcze (Key Intelligence Topics – KITs) jak również pytania (Key Intelligence Questions – KIQs), ułatwiające wybór źródeł informacji. Umiejętności analityczne na tym poziomie zapewnią podstawę do kierowania kolejnej fazy – gromadzenia informacji. Dodatkowo pomocne na tym etapie, będą również świadomość specjalisty w zakresie podstawowych typów psychologicznych, jak również umiejętności związane z przeprowadzaniem wywiadów, które umożliwią właściwie zrozumienie potrzeb i wymagań klientów.

Kolejną fazą po fazie planowania jest zbieranie danych i informacji. Opiera się ona na identyfikacji potencjalnych źródeł informacji, zebraniu danych, a następnie ich uporządkowaniu i syntezie. Jedną z umiejętności poszukiwaną wśród osób odpowiedzialnych za tą fazę będą umiejętności badawcze. Aby etap ten był przeprowadzony pomyślenie, specjalista powinien wykazywać znajomość różnorodnych metod i technik uzyskiwania dostępu do źródeł danych i informacji, przy jednoczesnym zapewnieniu ich wiarygodności, a także spełniania norm etycznych. Ponadto praktycy wywiadu powinni cechować się znajomością odróżniania hipotez od otwartych założeń. Dobra znajomość sieci kontaktów interpersonalnych będzie tutaj atutem, także zdolność do jej budowania co bezpośrednio wiąże się z umiejętnościami sprawnego komunikowania. Profesjonalny wywia-

3 K. Sawka, The Death of CompetitiveIntelligence Professional, „Competitive Intelligence Magazine" April/ March 2010, vol.13, nr. 2.

4 J.P. Herring, Key Intelligence Topics: A Processtoidentyfityanddefine Intelligence meeds. „Competitiveintelligencereview", 1999, vol. 10, nr 2.

dowca powinien być jednocześnie dobrym mówcą, jak i słuchaczem. Wynika to z faktu, że nie wszystkie informacje można pozyskać z opublikowanych zasobów. Zazwyczaj najlepsze rezultaty w poszukiwaniu informacji można uzyskać dzięki interakcji z ludźmi. Tzw. *humanintelligence* nie tylko dostarczaistotnych danych, ale wyjaśnia znaczenia i implikacje. Dodatkowo, nawet gdy konkretne osoby nie są dostawcami poszukiwanych informacji, to stanowią doskonałe źródło wskazujące na to, kto jest depozytariuszem wiedzy. Nie mniej jednak umiejętności nawiązywania kontaktów a przez pozyskiwania informacji, muszą opierać się na zasadach etyki.

Faza analizy procesu wywiadowczego jest najistotniejszą i najtrudniejszą fazą w cyklu wywiadowczym, w związku z tym specjalista winien wyróżniać się dobrze rozwiniętymi umiejętnościami analitycznymi. Musi wykazywać się przy tym dużą dozą kreatywności, która będzie niezbędna w zakresie tworzenia syntezy informacji i koncepcji, przy jednoczesnej biegłej znajomości stosowania metod, technik, narzędzi badawczych, a także form analizy. Podczas formułowania spostrzeżeń oraz wniosków, analityk musi również wykazywać umiejętności krytycznej interpretacji oraz umieszczania informacji we właściwym kontekście. Odnosi się to do zdolności oceny sytuacji, podejścia do problemu z różnej perspektywy oraz do określenia kluczowych kwestii. Dodatkowo musi unikać stereotypowego, szablonowego myślenia, odrzucać ideologiczne przekonania, jednak nie może lekceważyć nowych przesłanek lub być podatnym na wpływy innych, bowiem wywiadowca nie opiera się jedynie na faktach, ale czerpie wartość z własnej intuicji i doświadczenia.

Końcowym etapem cyklu wywiadowczego jest efektywna komunikacja, bowiem w rzeczywistości nawet głęboka analiza jest bezwartościowa, jeżeli nie trafi do odpowiednich osób celem podjęcia określonych działań. Specjalista wywiadu gospodarczego musi skutecznie rozprowadzić rezultaty swojej pracy do konkretnego odbiorcy, dlatego też praktycy powinni posiadać kwalifikacje w zakresie stosowania odpowiednich mediów, umiejętności perswazji oraz zdolności dostarczania w sposób obiektywny rezultatu wywiadowczego. Umiejętności do asertywności i dyplomacji również okażą się cenne w tym zakresie[5].

Istotny wpływ w kształtowaniu potencjału zespołu wywiadowczego niewątpliwie ma sam menedżer zarządzający zespołem, który powinien być człowiekiem wysoko osadzonym w strukturze organizacyjnej; dobrze znającym specyfikę firmy i rozumiejącym potrzeby wywiadowcze różnych interesariuszy; wzbudzającym zaufanie, słuchającym i zadającym pytania. W tym aspekcie wysoko rozwinięte umiejętności miękkie będą szczególnie cenne, bowiem wywiadowca musi być postrzegany jako ekspert i doradca merytoryczny, z którym interesariusze lubią współpracować. Dodatkowo powinien posiadać zdolność wpływania na kulturę organizacji, w tym pracowników spoza zespołu mu podległego,

5 A.C.Strauss, A.S.A. du Toit, Competitiveintelligenceskillsneededtoenhance South Africa'scompetitiveness. „Aslibproceedings", 2010, vol. 62, nr 3, s. 302-320.

poprzez budowanie odpowiedniego rodzaju korporacyjnej mentalności, a także promowania działań wywiadowczych. Być osobą potrafiącą rozwijać sieć kontaktów w zespołach z różnych działów, które pomogą mu w zbieraniu, analizowaniu i wykorzystaniu danych rynkowych. Jego naturalne predyspozycje analityczne oraz kreatywnego tworzenia syntezy informacji i koncepcji, umożliwią mu współtworzenie efektu wywiadowczego w odniesieniu do wszystkich kluczowych procesów biznesowych. Ścisła współpraca z menedżerami i wyższym kierownictwem zapewni właściwe dostarczenie produktów wywiadowczych do odpowiednich decydentów i ich wykorzystanie w firmie. Również same kompetencje w zakresie przywództwa i zarządzania będą tutaj wysoko cenione, ze względu na prowadzenie kliku projektów w jednym czasie, przy ograniczonych zasobach nie tylko czasowych. Ważne jest przy tym bycie asertywnym, odpornym, ale i zorientowanym na cel. Pożądane też, aby menedżer wykazywał się wysoką inteligencją emocjonalną, która poprzez przywództwo pośrednio wpływa na przewagę konkurencyjna organizacji.

Ze względu na fakt, iż na rodzimym rynku nie ma tak wielu profesjonalistów, którzy specjalizują się w zakresie wywiadu gospodarczego, jednocześnie posiadają wachlarz wyżej wymienionych umiejętności i kompetencji przy jednoczesnej znajomości danej branży, w której działa organizacja, budując zespół wywiadowczy warto sięgnąć po zasoby wewnętrzne firmy. Warto również zoptymalizować te działania, przez przypisanie roli pracującym już pracownikom, jednak nie dłużej niż na okres 2-3 lata ze względu na niską późniejszą efektywność, jaką pracownik mógłby dostarczyć firmie. Dodatkowo w obliczu wejścia na rynek kolejnych pokoleń, oczekiwania stawiane pracodawcy spełniałyby te wymagania, ozwalają na permanentny rozwój pracownika, który wiązałby się z firmą na wiele lat.

Konstruując zespół wywiadowczy, praktycy wskazują, iż jego wielkość może być uzależniona od branży, w jakiej działa organizacja. Można spotkać się z globalnymi firmami, których zespoły liczą ponad 25 osób. W instytucjach finansowych liczba ta wynosi zwykle wielokrotnie więcej, natomiast dla firm produkcyjnych może wynieść zaledwie 5 osób. Rekomendowane jest jednak uzależnienie zasobów od złożoności organizacji, a także jej skłonności do zmian. Pomocne w tym zakresie może okazać się zastosowanie *benchmarku* względem liczby analityków i budżetu, jakie stosują firmy będące o podobnym profilu, szczególnie jeżeli chodzi o planowanie rozwoju w zakresie zespołu wywiadowczego[6].

6 HowtoBuild A Competitive Intelligence Team: Interview WithVarunChhabra, Microsoft: B2B Market Research podcast, Pobrane z: https://www.cascadeinsights.com/build-competitive-intelligence-team-interview-varun-chhabra-microsoft-competitive-intel-ep-91/, 2 luty 2018 roku.

2. Wyzwania dotyczące czynnika ludzkiego

Powyższy przegląd najważniejszych kompetencji, jakie powinny posiadać osoby odpowiedzialne za wywiad gospodarczy z podziałem na poszczególne fazy i role, nie stanowi jedynej determinanty prawidłowego jego funkcjonowania. Oprócz powyższych uwarunkowań, praktycy zwracają również uwagę na cechy związane z odbiorem jego aktywności przez interesariuszy i innych pracowników organizacji. W tym zakresie ważną rolę pełni kultura organizacyjna, która będzie zasadniczym powodem w kwestii postaw wobec wprowadzanych zmian i zarządzania informacją[7].

Największe niebezpieczeństwo podczas tworzenia komórki wywiadu gospodarczego kryje się w chęci posiadania informacji, która jednocześnie stanowi wyznacznik statusu w ramach organizacji, rozpatrywanej na wszystkich jej szczeblach hierarchii. Przekazanie informacji innym pracownikom, którzy by z niej korzystali, równoznaczne byłoby z dobrowolnym pozbyciem się dotychczasowej możliwości decydowania oraz działania. Z tego powodu powołanie zespołu wywiadu gospodarczego współpracującego z licznymi działami może wywołać sprzeciw, a nawet opór ze strony pozostałych członków organizacji[8]. W tym przypadku w ramach przedsiębiorstwa musi być wzmocniona kultura zdolna do promowania oraz wymiany informacji między osobami i działami. Zakłada się bowiem, iż wysoki poziom kultury informacyjnej implikuje dbałość o informację i wynikającą z nich wiedzę. Przedsiębiorstwa, które dostrzegły tę wartość cechuje traktowanie informacji jako dobra wspólnego, gotowość do dzielenia się nią, otwarty system informacyjny, stymulowanie komunikacji bezpośredniej, szybkie pozyskiwanie i przetwarzanie informacji, niwelowanie chaosu informacyjnego, korzystanie z wielu źródeł wiedzy, a przede wszystkim gromadzenie i rozpowszechniane wiedzy[9]. W tej kwestii ważne jest poparcie płynące z góry, które nadaje mu rangę decyzji strategicznej, obowiązującej wszystkich członków organizacji, przez co mogącej uzyskać zrozumienie i aprobatę ze strony wszystkich współpracowników. Jeżeli zarząd nie jest przekonany co do wartości, jaką daje wywiad gospodarczy, stworzenie kultury informacyjnej będzie prawie niemożliwe[10]. W przypadku, gdy w organizacji kontekst kultury informacyjnej jest głęboko zakorzeniony, istnieje większe prawdopodobieństwo, że działania wywiadowcze będą szeroko wspierane i wykorzystywane, a także że wszyscy pracownicy będą w nich uczestniczyć na poziomie przekazywania informacji oraz jej ochrony[11].

7 L. Fuld Za: D. Rouach; P. Santi, *Competitive Intelligence Adds Value: Five Intelligence Attitude*.European Management Journal, October 2001, vol. 19, nr 5, s. 552-559.

8 R. Borowiecki, M. Kwieciński, *Koncepcja wywiadu gospodarczego w przedsiębiorstwie przyszłości, kulturowe i organizacyjne uwarunkowania jej realizacji*. http://www.zti.com.pl/instytut/pp/referaty/ref35_full.html, 13kwietnia 2013roku.

9 K. Materska, *Informacja w organizacjach w organizacjach społeczeństwa wiedzy.* Wydawnictwo SBP, Warszawa 2007, s. 194.

10 R. Borowiecki, M. Kwieciński, *Koncepcja wywiadu gospodarczego w przedsiębiorstwie przyszłości, kulturowe i organizacyjne uwarunkowania jej realizacji*. http://www.zti.com.pl/instytut/pp/referaty/ref35_full.html,

11 A. Saayman, J. Pienaar, P. de Pelsmacker, W. Viviers, L. Cuyvers, M.L. Muller, M. Jegers, *Competitive intelligence:*

W procesie akceptacji wdrażania wywiadu gospodarczego i tym samym optymalnego wykorzystania jego potencjału, ważne miejsce zajmuje świadomość pracowników co do istoty działalności wywiadu gospodarczego. Zasadne jest mocne nakreślenie wizji, misji, a także wyjaśnienie celów i wartości, z zamiarem usunięcia negatywnych mitów z nim związanych[12].

Pomocne w tym zakresie mogą okazać się szkolenia, które wyeliminują błędne przekonania dotyczące wywiadu gospodarczego, przekażą niezbędną wiedzę, zmienią nastawienie do wywiadu gospodarczego, a przede wszystkim jasno określą role i pełnione funkcje przez pracowników[13].

Odpowiedzialność za realną funkcję wywiadu gospodarczego spoczywa na profesjonalistach zajmujących się tą działalnością, ale także na jego klientach. Dla decydentów oznacza to współpracę ze specjalistą wywiadu gospodarczego, celem zdefiniowania potrzeb, ale także podatność na dostarczone spostrzeżenia celem ich wykorzystania. W przypadku gdy użytkownik będzie traktować wywiad gospodarczy wyłącznie jako nowy środek spełniający funkcje informacyjne, to prawie na pewno nie będzie on w stanie sprostać ich oczekiwaniom. Menadżerowie muszą zrozumieć, że jest to cenne narzędzie, pomagające w podejmowaniu decyzji oraz realizacji strategii, celem zwiększenia konkurencyjności firmy. W związku z tym, nieakceptowana jest postawa, w której menedżer zgłosi zadanie badawcze jednostce wywiadowczej, a następnie nawet nie zapozna się z dostarczonym raportem. Wówczas wartość i realna funkcja wywiadu gospodarczego, nie zostanie spełniona. Zaangażowanie decydentów oprócz ukierunkowywania prac wywiadowczych spoczywa również na ocenie dostarczonych wyników. Gdy zespół wywiadowczy wypełni swoje zadania, menadżerowie muszą dopełnić cykl wywiadowczy poprzez analizę dostarczonych spostrzeżeń celem przyszłego udoskonalania realizowanych działań[14].

Również niemała wydaje się rola pozostałych pracowników przedsiębiorstwa, którzy stanowią cenne ogniwa w łańcuchu wykonawców zadań wywiadowczych. Ich rola jest decydującym czynnikiem możliwości wywiadowczych, szczególnie jeżeli chodzi o pozyskiwanie informacji pewnych i raczej trudno dostępnych[15].

Jednak to specjaliści wywiadu gospodarczego odgrywają zasadniczą rolę, stanowiąc podstawowy czynnik działalności wywiadowczej. Umożliwiają bowiem przedsiębiorstwu przejście z etapu prowadzenia wywiadu na własną rękę do sta-

construct exploration, validation and equivalence, Aslib Proceedings, 2008, vol. 60, nr 4, s. 383-411.

12 D.J. Kalinowski and G. D. Maag, ROCI®: *A Framework for Determining the Value of Competitive Intelligence*. Journal Of Competitive Intelligence And Management. January/March 2012, vol. 15, nr 1, s. 9-21.

13 M.L. Muller, *Managing Competitive Intelligence, Knowres Publishing*, Johannesburg Za: A.C. Strauss, A.S.A. du Toit, *Competitive intelligence skills needed to enhance South Africa's competitiveness*, Aslib Proceedings, 2010, vol. 62, nr 3, s. 302-320.

14 K. Sawka, *Your Company's New Foray into Competitive Intelligence: Factors for Success*. Competitive Intelligence Magazine. January-February 2009, Vol. 12 , nr 1.

15 M. Kwieciński, *Wywiad gospodarczy – narzędzie poszukiwania wiedzy czy synergia w organizacji*. [w:] M. Morawski (red.) *Zarządzanie wiedzą i informacją w społeczeństwie sieciowym*. Tom II, Wałbrzyska Wyższa Szkoła Zarządzania i Przedsiębiorczości, Wałbrzych 2003, s. 11-13.

dium zorganizowanego wywiadu, gdzie kwestią fundamentalną jest skoordynowanie działań, celem zwiększenia zysków przedsiębiorstwa[16].

3. Organizacja *Market Intelligence* HR w Polskim Koncernie Naftowym ORLEN S.A.

Pomimo, iż większość organizacji działa w warunkach wysokiej konkurencji, brak im jakiegokolwiek formalnego procesu wywiadowczego. Same działy *Human Resources* (dalej: HR) ewaluują i również muszą agresywnie reagować na zmiany zachodzące na rynku, dlatego odpowiedzią na coraz ważniejszy strategicznie charakter obszaru kadr w PKN ORLEN, stanowiącym integralną część procesów decyzyjnych, było podjęcie decyzji o wdrożeniu systemu *market intelligence* w tym obszarze. Zaproponowane działania są jedynie zalążkiem dla stworzenia światowej klasy rozwiązań wywiadowczych, obejmującym początkowo obszar kadr w PKN ORLEN, a z biegiem czasu w działach HR spółek Grupy ORLEN. Rekomendowane jednak będzie stworzenie globalnego rozwiązania, które swym zakresem obejmie istniejące biura, realizujące zadania związane z formalnym zrozumieniem konkurencji oraz dynamiki rynku, a także zaimplementowanie podobnych rozwiązań w innych potencjalnie strategicznych obszarach organizacji.

Pierwszym etapem podjętych działań mających na celu wypracowanie założeń dla wdrożenia rozwiązań *market intelligence* w obszarze HR, były spotkania z pracownikami poszczególnych biur. Na podstawie wcześniej sporządzonych kwestionariuszy pytań, przeprowadzono wywiady, dzięki którym zdefiniowano jaką funkcję oraz w jaki sposób powinien zostać zorganizowany system *market intelligence* w obszarze HR. Dodatkowo dokonano przeglądu stosowanych w organizacji rozwiązań w tym zakresie, pod kątem możliwości zastosowania w obszarze zarządzania zasobami ludzkimi.

Dotychczasowy stan prowadzonych działań wywiadowczych w obszarze HR był podstawowy i przybierał charakter nieformalny. Pozyskiwane informacje stanowiły jedynie podstawę do działań reaktywnych i odbiegały od potrzeb strategicznych i planistycznych. Obszar aktywności nie był jednoznacznie zidentyfikowany, rozpoznanie rynku przyjmowało wyłącznie funkcjonalny charakter, tzn. wspierało działania poszczególnych zespołów bez współpracy z innymi biurami. Formułowano potrzeby informacyjne, jednak nie zawsze przekładały się one na decyzje i działania. Istniał niski poziom koordynacji wiedzy w zasobach poszczególnych Biur obejmujących różnego rodzaju raporty, sprawozdania, a także analizy dotyczące procesów HR. Również produkty wywiadowcze wykorzystywane w innych obszarach nie były dzielone w sposób sformalizowany i spójny, a także nie były znane wszystkim pracownikom z obszaru kadr. Brak skoordynowanych rozwiązań w zakresie zarządzani wiedzą prowadziły do dublowania działań

16 B. Martinet, Y.M. Marti, *Wywiad gospodarczy: pozyskiwanie i ochrona informacji,* Polskie Wydawnictwo Ekonomiczne, Warszawa 1999, s. 263.

związanych z pozyskiwaniem i analizą informacji. Jednak największe wyzwanie zidentyfikowane podczas przeprowadzonych badań był brak należytego uznania wśród pracowników HR w zakresie wywiadu gospodarczego. Bez względu na istnienie wąskich gardeł, spółka wykazywała potencjał w zakresie kultury informacyjnej, gwarantującej wdrożenie programu *market intelligence* w obszarze HR. Wyrażone to było mi.in. w znajomości przyjętej strategii, stosowaniu nieformalnych praktyk dzielenia się wiedzą przez pracowników a także podjęciu inicjatyw mających na celu usprawnienie tego procesu. Pracownicy wskazywali na potencjał informacyjny istniejący w samej organizacji oraz potrzebę dostępu do wysoko jakościowych informacji i śledzenia rynku w zakresie zachodzących zmian jako fundamentu realizacji obowiązków służbowych.

Po przeprowadzonej analizie stanu obecnego, przygotowano i zaprezentowano najwyższemu kierownictwu w obszarze, projekt rozwiązań wdrożenia Market Intelligence HR. Po jego akceptacji dokonano komunikacji w obszarze oraz wyznaczono osoby, odpowiedzialne za realizację zadań w zakresie implementacji programu, a następnie procesu wywiadowczego.

Sprecyzowano, iż misją programu *Market Intelligence* w obszarze Kadr w PKN ORLEN SA będzie wsparcie realizacji strategii HR. Obszarem docelowym, na którym będzie się skupiać jest analiza potrzeb rozwojowych biznesu, poszukiwanie nowych rozwiązań oraz inspiracji do wdrażania innowacji w zakresie zarządzania zasobami ludzkimi poprzez monitorowanie trendów i najlepszych praktyk rynkowych.

Market Intelligence HR:

- jest narzędziem wspierającym zdobywanie wartościowych informacji oraz inspiracji w celu optymalizacji działań,
- to rzetelne i sprawdzone źródło aktualnych informacji, będących asumptem do podjęcia określonych działań,
- dostarcza kompleksowej wiedzy do podejmowania kluczowych decyzji,
- pozwala na inicjowanie nowych pomysłów, rozwiązań, procesów w zakresie HR,
- daje przestrzeń do inspiracji, dyskusji, dzielenia się wiedzą i dobrymi praktykami.

Przyjęta wizja zakładała wdrożenie systemu *market intelligence*, spełniającego normy światowej klasy rozwiązań wywiadowczych, systematycznie stosowanego i praktycznie wykorzystywanego w Grupie Kapitałowej ORLEN.

Market Intelligence HR w PKN ORLEN został zdefiniowany jako systematyczny proces pozyskiwania i analizy informacji o naszych kluczowych interesariuszach, a także zmianach zachodzących na rynku z zachowaniem zasad prawnych i norm etycznych. Znajomość rynku wymaga porównania danych/informacji z różnych źródeł, zarówno tych wewnętrznych jak i zewnętrznych, tak by mieć pełny ogląd, otoczenia, w którym funkcjonuje organizacja.

Proaktywne użycie *MI* w obszarze HR pomoże:

- zrozumieć potrzeby interesariuszy (tj. pracowników, szczególnie tych kluczowych oraz kandydatów) i na podstawie tego dostarczać odpowiednie usługi, produkty i rozwiązania;
- odróżnić się od innych, zdając sobie sprawę z tego, co jest oferowane przez pozostałych uczestników na rynku i przyjęcia rozpoznawalnej i spójnej pozycji na rynku (m.in. poprzez *EmployerBranding* i świadome kreowanie swojego otoczenia)
- zidentyfikować i rozwijać strategiczne sojusze z innymi organizacjami i podmiotami (m.in. przez identyfikację dostawców szkoleń czy też uczelni lub innych organizacji);

Do głównych celów dla nowo wdrażanego projektu, można zaliczyć:

- eliminację dublowania wydatków na czasopisma i raporty rynkowe przez przejęcie centralnej kontroli nabywania wiedzy (początkowo w obszarze HR),
- znaczne poprawienie dostępności informacji poprzez wielobranżowe wiadomości i artykuły, wiadomości ostrzegawcze (alerty) i inne kanały komunikacji,
- mnożenie wykorzystania właściwie przetworzonych informacji poprzez globalną dostępność do depozytariuszy wiedzy w oparciu o rzeczywiste potrzeby wywiadowcze,
- stworzenie światowej klasy sieci wymiany wiedzy fachowej, pomiędzy ekspertami, działającymi w różnych podmiotach Grupy ORLEN, dzielących się wiedzą o rynku globalnym, ale i lokalnym czy regionalnym.

Za projekt wdrożenia, a następnie realizację działań związanych z *market intelligence* było odpowiedzialne biuro, bezpośrednio ulokowane pod Dyrektorem Wykonawczym ds. Kadr. Do realizacji zadań w tym zakresie dedykowane były dwie osoby, a pozostali pracownicy z zespole pełnili funkcję wsparcia. Dodatkowo Dyrektor z każdego Biura, wyznaczył jednego koordynatora przewodniego systemu *Market Intelligence* HR oraz koordynatora powiązanego. Koordynatorzy pełnili funkcję wsparcia w zakresie wdrażania projektu oraz później prawidłowego funkcjonowania systemu wywiadowczego w obrębie biura. Koordynatorem przewodnim była osoba charakteryzująca się dużym doświadczeniem, znająca współpracowników i specyfikę zespołu w tym m.in. poszukiwanych informacji, dokumentów i materiałów istniejących w biurze, a przede wszystkim osób, które posiadają odpowiednią wiedzę. Koordynatorem powiązanym była natomiast osoba stosunkowo młoda, inspirująca i aktywizująca do działania w zakresie dzielenia się wiedzą. Zadania obu koordynatorów były podobne, jednak możliwości organizacyjne znacznie ograniczone. Koordynator przewodni posiadał większą moc decyzyjną.

Po ustaleniu osób dedykowanych do zespołu *Market Intelligence* HR, został przeprowadzony warsztat tematyczny w zakresie wywiadu gospodarczego oraz realizacji powierzonych im zadań. Dodatkowo wszystkim osobom w obsza-

rze, zostały przekazane materiały informacje dotyczące funkcji i zadań zespołu Market Intelligence HR. Zdecydowano, iż działania *market intelligence* będą podzielone na poziomy, w zależności od przyjętej perspektywy w procesie decyzyjnym. W aspekcie strategicznym będą wspierały decydentów poprzez analizę rozwiązań i czynników wpływających na rozwój strategii oraz wdrażania nowych możliwości, w tym identyfikacji szans i zagrożeń występujących na rynku. Na poziomie taktycznym, w zakresie zrozumienia średnioterminowych uwarunkowań i trendów kształtujących sytuację w sektorze oraz w celu reagowania na wyzwania pojawiające się w organizacji lub na rynku. Na poziomie operacyjnym *Market Intelligence* HR, miał monitorować bieżącą sytuację na rynku, a także w organizacji.

Jednym z pierwszych produktów wdrożenia programu *Market Intelligence* był cotygodniowy *newsletter*, wysyłany do wszystkich pracowników z obszaru HR. Zawierał on przegląd najważniejszych informacji dotyczących rynku pracy, innowacyjnych rozwiązań, wydarzeń, trendów HR, a także opublikowanych, polecanych raportów. Dodatkowo, odpowiedzią na istnienie biznesowej potrzeby w zakresie wdrożenia narzędzia wspierającego i usprawniającego system dzielenia się wiedzą, a także podejmowania decyzji na poziomie taktycznym i operacyjnym, było wdrożenie dedykowanej platformy informatycznej – Grupy Praktyków *Market Intelligence* HR. Dotychczasowo, informacje były rozporoszone i zgromadzone w plikach poszczególnych osób, zespołu lub też stanowiły indywidualną wiedzę pracowników, między którymi nie dochodziło do wymiany. Pomimo deklarowanej możliwości wymiany tej wiedzy, mała ona charakter nieformalny inieogólnodostępny. Niewiedza o depozytariuszach wiedzy równoznaczna była z brakiem poszukiwanej informacji. Dlatego też zdecydowano o wdrożeniu powyższego narzędzia, które miały na celu służyć jako dodatkowy kanał kontaktu, umożliwiający dzielenie się informacją, dające powód do podejmowania określonych działań. Dzięki aktywnemu wykorzystaniu możliwości platformy, każdy pracownik z obszaru kadr mógł stać się jednocześnie użytkownikiem i uczestnikiem w procesie gromadzenia informacji i jej analizowania (z zastrzeżeniem istnienia poziomów zabezpieczeń/widoczności do poszczególnych zasobów). Wprzyjętych założeniach, zasoby platformy posiadały aktualności rynkowe, dane makroekonomiczne, analizy, raporty rynkowe, prognozy, komentarze eksperckie, bazę największych graczy i ich charakterystykę, a także informacje i analizy dotyczące samej organizacji. Tematyka zamieszczanych informacji skupiała się na zidentyfikowanych wcześniej kluczowych potrzebach informacyjnych pozyskanych podczas wcześniejszych spotkań z Koordynatorami przewodnimi. Dedykowane narzędzie, było też rzetelnym źródłem informacji dotyczącym samej tematyki wywiadowczej oraz funkcji jaka została przypisana *market intelligence* w obszarze HR. Każdy użytkownik platformy znajdzie tam informacje dotyczy m.in. misji, wizji, założeń systemu market intelligence, a także osób odpowiedzialnych za program. Takie informacje niwelowały niewiedzę dotyczącą istoty *Market Intelligence* HR, a także

były wsparciem w przypadku przyjścia nowego pracownika do obszaru i przekazania mu założeń dotyczących funkcjonujących działań.

Do innych produktów wywiadowczych, na wyższym poziomie decyzyjności, należały zaplanowane cykliczne przeglądy kwartalne, dedykowane dyrektorom z poszczególnych biur. Miały one na celu przedstawienie podsumowania kwartalnego monitoringu rynku oraz przeprowadzonych analiz w zakresie aktualnych i przyszłych trendów, wyzwań, szans i zagrożeń występujących na rynku pracy, po których podejmowano adekwatne decyzje i działania.

Market Intelligence w obszarze HR w PKN ORLEN S.A.,wciąż stoi przed poważnymi wyzwaniami, do których zalicza się m.in. ograniczone działania w zakresie wywiadu i kontrwywiadu biznesowego. Mimo to, zmiany zachodzące na rynku, będą coraz to bardziej wymuszać na Spółce, stosowanie systemowego rozwiązania w zakresie pozyskiwania i analizowania informacji do podejmowania decyzji w perspektywie długo i krótkoterminowej. Przedstawiony przykład wdrożenia *market intelligence* ukazuje, że potrzebę tworzenia nieszablonowych rozwiązań wywiadowczych należy dostosowywać do charakteru potrzeb zgłaszanych przez interesariuszy. Jednak niezależnie od decyzji w zakresie ulokowania w strukturach organizacyjnych zespołu wywiadowczego, krytyczną determinantą decydującą o sukcesie, będzie niewątpliwie czynnik ludzki, który tak często wymieniany jest w literaturze przedmiotu. Brak poparcia ze strony najwyższej kadry i jednocześnie braki w świadomości samych pracowników w zakresie zrozumienia istotności i potencjału płynącego z formalnego wykorzystania wywiadu ikontrwywiadu gospodarczego, na każdym poziomie decyzyjności zakończy się fiaskiem. Dlatego też ważny jest rozbudowany proces komunikacji, zwłaszcza w początkowych etapach procesu wdrażania rozwiązań wywiadowczych, ale także w późniejszym czasie. Systematyczne szkolenia w zakresie skutecznych technik i narzędzi pozyskiwania i analizowania informacji, zapewnią wysoki poziom zaangażowania pracowników w działania wywiadowcze, niezależnie od zajmowanego stanowiska oraz przypisanych zadań.

Bibliografia:

Bielska A., Smółka P. (red.), *Wywiad biznesowy. Praktyczne wprowadzenie*, Wydawnictwo Nieoczywiste, Piaseczno, 2017.

Borowiecki R., Kwieciński M., *Koncepcja wywiadu gospodarczego w przedsiębiorstwie przyszłości, kulturowe i organizacyjne uwarunkowania jej realizacji*, http://www.zti.com.pl/instytut/pp/referaty/ref35_full.html, 13 kwietnia 2013 roku.

Ciecierski M., *Wywiad biznesowy w korporacjach transnarodowych: teoria i praktyka*, Wydawnictwo Adam Marszałek, Toruń 2009.

Herring J.P., *Key Intelligence Topics: A Processtoidentyfityanddefine Intelligence meeds.* Competitiveintelligencereview, 1999, vol. 10, nr 2.

HowtoBuild A *Competitive Intelligence Team: Interview WithVarunChhabra, Microsoft:*

B2B Market Research podcast, Pobrane z: https://www.cascadeinsights.com/build-competitive-intelligence-team-interview-varun-chhabra-microsoft-competitive-intel-ep-91/, 2 luty 2018 roku.

Kalinowski D. J. , Maag G. D., ROCI®: *A Framework for Determining the Value of Competitive Intelligence*. Journal Of Competitive Intelligence And Management. January/March 2012, vol. 15, nr 1.

Kwieciński M., *Wywiad gospodarczy – narzędzie poszukiwania wiedzy czy synergia w organizacji*. [w:] M. Morawski (red.) *Zarządzanie wiedzą i informacją w społeczeństwie sieciowym*. Tom II, Wałbrzyska Wyższa Szkoła Zarządzania i Przedsiębiorczości, Wałbrzych 2003.

Martinet B., Marti Y.M., *Wywiad gospodarczy: pozyskiwanie i ochrona informacji*, Polskie Wydawnictwo Ekonomiczne, Warszawa 1999.

Materska K., *Informacja w organizacjach w organizacjach społeczeństwa wiedzy*. Wydawnictwo SBP, Warszawa 2007.

Muller M.L., *Managing Competitive Intelligence*, *Knowres Publishing*, Johannesburg Za: A.C. Strauss, A.S.A. du Toit, *Competitive intelligence skills needed to enhance South Africa's competitiveness*, Aslib Proceedings, 2010, vol. 62, nr 3

RouachD., Santi P., *Competitive Intelligence Adds Value: Five Intelligence Attitude*.European Management Journal, October 2001, vol. 19, nr 5.

Saayman A, Pienaar J., de Pelsmacker P.,Viviers W., Cuyvers L., Muller M.L., Jegers M., *Competitive intelligence: construct exploration, validation and equivalence*, Aslib proceedings, 2008, vol. 60, nr 4.

Sawka K., *The Death of CompetitiveIntelligence Professional*, Competitive Intelligence Magazine April/March 2010, vol.13.

Sawka K., *Your Company's New Foray into Competitive Intelligence: Factors for Success*. Competitive Intelligence Magazine. January-February 2009, Vol. 12, nr 1.

Strauss A.C., du Toit A.S.A., *Competitiveintelligenceskillsneededtoenhance South Africa-'scompetitiveness*. Aslib proceedings, 2010, vol. 62, nr 3.

Teresa Przybyszewska*

***Teresa Przybyszewska, Polski Koncern Naftowy ORLEN Spółka Akcyjna**

Hieronim Szafran

Doświadczenia Wszechnicy Polskiej Szkoły Wyższej w Warszawie w zakresie kształcenia specjalistów wywiadu i kontrwywiadu gospodarczego

Wprowadzenie

Nasilająca się współcześnie konkurencja w biznesie, postęp technologiczny w walce informacyjnej oraz zmienne uwarunkowania zapewnienia bezpieczeństwa przedsiębiorstw, a także obserwowana zmiana pokoleniowa kadr wymagają doskonalenia procesu kształcenia nowych pracowników dla podmiotów zajmujących się wywiadem i kontrwywiadem gospodarczym.

W artykule poddano analizie i uogólniono doświadczenia Wszechnicy Polskiej Szkoły Wyższej w Warszawie, która od 2017 roku wdraża stopniowo specjalność Wywiad i kontrwywiad gospodarczy na prowadzonym w uczelni od 2007 roku kierunku studiów Bezpieczeństwo wewnętrzne.

Celem rozważań jest zebranie doświadczeń uczelni z rozproszonych źródeł, próba identyfikacji potrzeb w zakresie kształcenia i możliwych rozwiązań pod kątem zakładanych efektów kształcenia, treści programowych, metod i form nauczania i samokształcenia studentów.

Podjęto też próbę wyjaśnienia ważnych uwarunkowań procesu kształcenia – ustalenia dostępnej literatury, potrzebnej infrastruktury, koniecznej współpracy z krajowym (regionalnym) otoczeniem społecznym i gospodarczym oraz możliwej kooperacji międzynarodowej.

1. Przesłanki i założenia koncepcji kształcenia

Wszechnica Polska przygotowuje pracowników i kandydatów na funkcjonariuszy dla podmiotów sektora publicznego i prywatnego[1], ukierunkowanych na rozpoznawanie i przeciwdziałanie zagrożeniom bezpieczeństwa wewnętrznego państwa powodowanym przez siły natury lub działalność człowieka, godzącym w bezpieczeństwo publiczne i bezpieczeństwo powszechne, spokój, ład i porządek publiczny oraz bezpieczeństwo jednostki. Studia proponujemy osobom zainteresowanym podjęciem pracy w komórkach ds. bezpieczeństwa instytucji publicznych i przedsiębiorstw, w agencjach ochrony osób i mienia, biurach detektywistycznych, w wywiadowniach gospodarczych, firmach zajmujących się instalacją i prowadzeniem monitoringu, w strukturach zarządzania kryzysowe-

1 Wspieramy ponadto rozwój zawodowy funkcjonariuszy pozostających w służbie.

go administracji rządowej i samorządowej, a także w służbach mundurowych: Policji, Straży Miejskiej, Straży Granicznej, Straży Ochrony Kolei i innych o podobnym charakterze.

Inicjatywa kształcenia w uczelni specjalistów z zakresu wywiadu i kontrwywiadu gospodarczego jest pokłosiem I Konferencji z 25 maja 2017 r. Jej obrady podsumował panel dyskusyjny, którego uczestnicy dostrzegli występującą konieczność kształcenia profesjonalistów zajmujących się bezpieczeństwem biznesu. Podjęcie wysiłku realizacji postulatu jest przejawem nadążania przez uczelnię za dynamiką zmian w praktyce społecznej i nauce, nastawienia na gotowość do stałej modyfikacji specjalności, treści i metod kształcenia w ramach transformacji na profil praktyczny, powiązania dydaktyki z pracami rozwojowymi wspierającymi działalność zawodową i gospodarczą partnerów Wszechnicy Polskiej oraz doskonalenie trybu konsultacji z podmiotami zewnętrznymi. Służy zatem wymianie doświadczeń, otwarciu na potrzeby praktyki i gotowości do wdrażania nowych rozwiązań.

W Wszechnicy Polskiej prowadzimy kierunek studiów Bezpieczeństwo wewnętrzne wprowadzając stopniowo od 1.10.2016 r. praktyczny profil kształcenia. W roku akademickim 2017/2018 uruchomiliśmy na studiach I stopnia (licencjackich) specjalność Wywiad i kontrwywiad gospodarczy a na studiach II stopnia (magisterskich) możliwość wyboru przedmiotu obieralnego Bezpieczeństwo biznesu wspieranego przez treści pozostałych przedmiotów.

Specjalność przygotowuje studentów do zatrudnienia w charakterze rozpoczynającego pracę w zawodzie specjalisty ukierunkowanego na pozyskiwanie informacji przydatnych w walce konkurencyjnej oraz ochronę tajemnic własnych przedsiębiorstwa i przedsiębiorcy w oparciu o wiedzę wspólną dla wszystkich studentów kierunku. Bezpieczeństwo wewnętrzne. Studenci będą mieli okazję zapoznać się dodatkowo z takimi zagadnieniami specjalistycznymi, jak: etyczne prawne aspekty działalności wywiadowczej i kontrwywiadowczej w Polsce, zadania i struktura komórek bezpieczeństwa w biznesie, identyfikacja potrzeb wybór źródeł informacji, analiza i opracowanie danych, identyfikacja zagrożeń wewnętrznych i zewnętrznych, audyt bezpieczeństwa w firmie, określenie założeń polityki bezpieczeństwa przedsiębiorstwa, organizacja bezpieczeństwa osobowego, fizycznego i teleinformatycznego, planowanie działalności wywiadowczej i kontrwywiadowczej. Specjalizacja przeznaczona jest dla osób zainteresowanych pracą w komórkach bezpieczeństwa przedsiębiorstw, w wywiadowniach gospodarczych, w biurach detektywistycznych, w agencjach ochrony mienia i osób oraz dla kandydatów na funkcjonariuszy służb mundurowych i służb specjalnych.

Oferujemy studia, które dadzą solidne przygotowanie zawodowe do pracy w nstytucjach bezpieczeństwa wewnętrznego. Nasz oryginalny program, który wykorzystuje doświadczenia anglosaskie i holenderskie, proponuje szeroki zakres zajęć niezbędnych do zrozumienia politycznego, społecznego i ekono-

micznego kontekstu współczesnych zagrożeń oraz międzynarodowych i wewnętrznych uwarunkowań polityki bezpieczeństwa państwa, w tym roli prawa. Dzięki dużej liczbie zajęć praktycznych absolwenci umieją wskazywać i diagnozować obszary zagrożeń oraz szacować ryzyko w stanach zagrożenia, podejmować trafne decyzje, stosować właściwe taktyki i techniki interwencji i kryminalistyczne. Zaopatrzeni w profesjonalną wiedzę i umiejętności potrafią chronić dane i informacje niejawne, projektować ochronę osób, mienia, obiektów i obszarów, zabezpieczenie imprez masowych, akcje ratownicze, a w ramach interesującej nas specjalizacji – działania wywiadu i kontrwywiadu biznesowego.

Mamy świadomość, że zapewnienie bezpieczeństwa ludzi, państwa, infrastruktury i środowiska stanowi współcześnie coraz większe wyzwanie. Kluczowym zadaniem specjalisty bezpieczeństwa wewnętrznego jest zapewnienie koordynacji działań i komunikacji między współdziałającymi stronami, celowe łączenie środków, możliwości i wysiłków, a także wyniesienie interesów wspólnych ponad partykularne. Każda kwestia bezpieczeństwa jest częścią łańcucha przyczynowo-skutkowego. I nie wystarcza ustalić, jaki problem wystąpił. Równie ważne jest, aby wiedzieć, dlaczego i w jaki sposób powtarzające się wydarzenia i incydenty, powinny być postrzegane jako sprawiające problemy i jakie są lub mogą być ich następstwa.

Studenci posiądą podstawy wiedzy z zakresu teorii, metodologii i zapewnienia zintegrowanego bezpieczeństwa i ochrony życia, zdrowia, wolności, dóbr i odpowiednich warunków egzystencji (jakości życia) obywateli.

Doświadczenia wskazują, że wykorzystanie wiedzy w praktyce będzie wymagało równoległego opanowania w czasie studiów szerokiego zakresu umiejętności: współpracy ze specjalistami z różnych dziedzin i w środowisku wielokulturowym;

1) wyszukiwania kontaktów, budowania ich i utrzymywania;
2) pozyskiwania, opracowania i przekazywania przydatnych informacji;
3) przekazywania informacji i pomysłów w sposób precyzyjny i jasny z użyciem właściwej komunikacji, odpowiedniej do sytuacji lub celu, ustnej lub pisemnej, zobrazowanej w formie graficznej;
4) działania zgodnego z obowiązującymi normami i wartościami;
5) odróżniania kwestii głównych od pobocznych;
6) analitycznego myślenia;
7) analizowania problemów złożonych i struktur oraz proponowania w razie potrzeby koniecznych działań lub zmian w dotychczasowych rozwiązaniach;
8) przygotowania na podstawie dostępnych informacji użytecznych wniosków o alternatywnych wariantach rozwoju sytuacji i możliwościach przeciwdziałania zagrożeniom, przydatnych do podjęcia decyzji przez przełożonego;
9) zaplanowania działań własnych i współpracowników: ustalenia celów, określenia zadań, wyboru sposobów działania, ustalenia priorytetów, dokonania kalkulacji czasu, i ujęcia ich w typowych dokumentach stosowanych w działalności zawodowej;

11) działania w zespole: współdziałania z uczestnikami grupy zadaniowej lub projektowej, komunikowania się z nimi oraz bezkonfliktowej realizacji zadań;
12) inno wacyjnego podejścia do wykonywanych czynności;
13) efektywnego działania w warunkach presji czasu i natłoku informacji.

Należy zauważyć, że kształcenie specjalisty wywiadu i kontrwywiadu gospodarczego realizujemy na szerszej podbudowie wiedzy, umiejętności i kompetencji z zakresu bezpieczeństwa wewnętrznego w ogóle, „wmontowując" weń potrzeby specjalizacji. Dzięki temu zabiegowi absolwent zna kontekst i uwarunkowania osobistej działalności, rozumie własną rolę i zadania, a także potrzebę współdziałania z innymi podmiotami.

Oceny potrzeb rynku pracy dokonywane okresowo przez uczelnię we współpracy z partnerami wskazują, że środowisko zawodowe i przyszli pracodawcy oczekują, że absolwenci studiów I stopnia ze specjalizacją w zakresie wywiadu i kontrwywiadu gospodarczego będą realizować zadania w rolach doradcy, planisty, bezpośredniego organizatora pracy lub wykonawcy. Dla kończących studia II stopnia przewidywane są stanowiska starszych specjalistów i (z czasem) kierowników niższego i średniego szczebla.

Odpowiednio do zidentyfikowanych ról zawodowych absolwenta sformułowano efekty kształcenia. Zachowano przy tym spójność z obszarem kształcenia, poziomami studiów i profilem praktycznym, do którego kierunek (i specjalizacja) zostały przyporządkowane.

Na podstawie analizy oczekiwań zgłoszonych przez przyszłych pracodawców oraz badań nad doświadczeniami z kształcenia pracowników wywiadu i kontrwywiadu gospodarczego w kraju i za granicą założono, że absolwent ze specjalnością Wywiad i kontrwywiad gospodarczy powinien:

- posiadać podstawową wiedzę z zakresu działalności wywiadu i kontrwywiadu biznesowego oraz umieć wykorzystać ją w budowaniu systemu bezpieczeństwa biznesu;
- potrafić identyfikować zagrożenia tajemnicy przedsiębiorstwa oraz formułować sposoby praktycznego reagowania;
- dysponować wiedzą o różnych rodzajach zależności prawnych w prowadzeniu i przeciwdziałaniu wywiadowi gospodarczemu;
- orientować się w rodzajach organizacji wywiadu gospodarczego i znać ich metody działania;
- posiadać wiedzę o źródłach i technikach analizy danych w działalności wywiadu i kontrwywiadu biznesowego i wykorzystywać ją do rozwiązania zidentyfikowanych problemów praktycznych;
- potrafić identyfikować w raporcie zagrożenia bezpieczeństwa ze strony wywiadu i kontrwywiadu biznesowego oraz formułować sposoby praktycznego reagowania;

- potrafić diagnozować i prognozować procesy i zjawiska w zakresie wywiadu i kontrwywiadu biznesowego oraz generować i wdrażać rozwiązania konkretnych problemów w zakresie ochrony bezpieczeństwa biznesu;
- posiadać wiedzę i umiejętności niezbędne do planowania działań ukierunkowanych na rozpoznanie konkurencji w ramach białego i szarego wywiadu;
- Stosować zasady i normamy etyczne w podejmowanej działalności, dostrzegać i analizować dylematy etyczne.

Wydaje się, że założone efekty są możliwe do osiągnięcia i zweryfikowania. Uszczegóławiają efekty obszarowe i kierunkowe odnosząc je do dyscypliny naukowej i specjalności. Komunikują otoczeniu i studentom, czego uczelnia chce nauczyć. Określają tożsamość specjalności i pozwalają na ukierunkowanie kształcenia praktycznego i przygotowanie do potrzeb rynku i pracy zawodowej. W ocenie kierownictwa Instytutu i Katedry zaletą opracowanej koncepcji, która sprzyja efektywności kształcenia, jest wykorzystanie dotychczasowych doświadczeń uczelni z kształcenia na profilu ogólnoakademickim, osobistego dorobku i praktyki zawodowej nauczycieli oraz pomocy interesariuszy zewnętrznych. Jednocześnie doceniamy duże znaczenie śledzenia zmian uwarunkowań i potrzeb procesu dydaktycznego, a także przejawianie przez nauczycieli gotowości do wdrażania modyfikacji programowych.

Podsumowując, autorzy koncepcji kształcenia starali się, aby opracowany program charakteryzowały następujące cechy:

- nadążanie za dynamiką zmian w praktyce,
- nastawienie na gotowość do stałej modyfikacji specjalności, treści i metod kształcenia,
- profil praktyczny,
- powiązanie dydaktyki z pracami rozwojowymi służącymi wsparciu działalności zawodowej i gospodarczej naszych partnerów,
- odpowiedni tryb konsultacji z podmiotami zewnętrznymi, służący wymianie doświadczeń, inspirowaniu i ocenie nowych rozwiązań.

2. Treści i metody kształcenia

Program studiów w zakresie omawianej specjalności zachowuje wyraźnie akcentowany profil praktyczny.

Został opracowany w oparciu o doświadczenia Wszechnicy Polskiej Szkoły Wyższej w Warszawie z wcześniejszego kształcenia na kierunku Bezpieczeństwo wewnętrzne na studiach pierwszego i drugiego stopnia o profilu ogólnoakademickim.

Kształcenie w specjalności Wywiad i kontrwywiad gospodarczy realizowane jest na 5. i 6. semestrze studiów I stopnia. Poprzedzają je cztery semestry studiów prowadzone z ogółem studentów.

Całość przedmiotów zawartych w programie studiów została podzielona na przedmioty kształcenia teoretycznego i przedmioty kształcenia praktycznego. W pierwszej grupie znalazły się przedmioty, którym przypisano efekty kształcenia typu wiedza oraz niekiedy efekty typu umiejętności, jeśli odnosiły się do umiejętności samodzielnego sięgania po wiedzę i rozwijania własnych kompetencji poznawczych studenta. Przedmiotom tym nadano formę wykładów. Przedmiotom praktycznym zostały przypisane efekty typu umiejętności i kompetencje społeczne. Nadano im formę zajęć praktycznych, tj. ćwiczeń, konwersatoriów, seminariów i praktyk.

Nadając studiom profil praktyczny, w sposób szczególny skoncentrowano się na kształtowaniu na zajęciach praktycznych umiejętności i kompetencji bezpośrednio wymaganych na rynku pracy. Zajęcia modułu kształcenia językowego, większość zajęć modułów specjalnościowych oraz modułu przedmiotów wspólnych zaprogramowano jako zajęcia praktyczne przypisując im efekty kształcenia typu umiejętności oraz treści ściśle wiążąc z przyszłą aktywnością zawodową.

Dobór treści kształcenia został przeprowadzony przez przyjęcie:

1) przedmiotów wspólnych (dla studiów z obszaru nauk społecznych) w ogólnouczelnianym module kształcenia podstawowego i kierunkowego:
   a. na studiach pierwszego stopnia: Podstawy socjologii, Historia bezpieczeństwa wewnętrznego w Polsce, Wprowadzenie do teorii bezpieczeństwa wewnętrznego, Podstawy organizacji i zarządzania, Komunikacja interpersonalna – interakcje społeczne, Technologie informacyjne, Organizacja i metodyka studiowania, Podstawy przedsiębiorczości, BHP i ergonomia;
   b. na studiach drugiego stopnia: Współczesne trendy rozwoju informatyki, Współczesne problemy psychologii, Wprowadzenie do redakcji prac naukowych, Samorozwój i samokształcenie, Teoria bezpieczeństwa wewnętrznego państwa, Podstawy prawne bezpieczeństwa wewnętrznego, Administracja publiczna w systemie bezpieczeństwa wewnętrznego, Strategia bezpieczeństwa wewnętrznego, Język obcy.
2) kluczowych przedmiotów dla modułu przedmiotów kształcenia kierunkowego:
   a. studiach pierwszego stopnia: Podstawy prawa, Logika, Podstawy finansów, Nauka o państwie i prawie, System bezpieczeństwa wewnętrznego RP, Zwalczanie przestępczości, Etyka zawodowa funkcjonariuszy służb bezpieczeństwa publicznego, Kryminologia, Kryminalistyka, Zarządzanie w sytuacjach kryzysowych, Ochrona osób, mienia i infrastruktury, Podstawy obronności państwa, Ratownictwo i ochrona ludności, Warsztaty zarządzania kryzysowego, Podstawy przeciwdziałania terroryzmowi, Metodyka szkolenia służb bezpieczeństwa publicznego, Ochrona danych osobowych i informacji niejawnych, Podstawy metodyki badania bezpieczeństwa, Prawo administracyjne;
   b. na studiach drugiego stopnia: Przeciwdziałanie zagrożeniom terrorystycznym, Ochrona ludności i obrona cywilna, Zarządzanie strategiczne syste-

mami bezpieczeństwa wewnętrznego, Ewolucja Instytucji bezpieczeństwa wewnętrznego, Metodologia nauk o bezpieczeństwie, Współczesne koncepcje filozofii i etyki, Wybrane zagadnienia Unii Europejskiej, Podstawy zarządzania zasobami ludzkimi.

3) modułu przedmiotów do wyboru:
   a. na studiach pierwszego stopnia – modułu przedmiotów specjalnościowych, z dobranymi przedmiotami, ukierunkowanymi na kształcenie praktyczne i przygotowanie do rynku pracy i pracy w określonym zawodzie.
   W programie specjalności Wywiad i kontrwywiad gospodarczy uwzględniono następujące przedmioty: Wprowadzenie w teorię wywiadu gospodarczego, Podstawy prawne wywiadu gospodarczego, Organizacje wywiadu gospodarczego, Ochrona i osłona kontrwywiadowcza biznesu, Źródła i techniki analizy danych, Metodyka przygotowania raportu końcowego, Warsztaty z metod i technik bezpieczeństwa biznesu, Planowanie działań wywiadu i kontrwywiadu gospodarczego, Techniki interwencji i samoobrony, Warsztaty współpracy z mediami, Seminarium licencjackie, Praktyki zawodowe;
   b. na studiach drugiego stopnia w module przedmiotów obieralnych (do wyboru) przedmioty: Bezpieczeństwo biznesu, Przestępczość w cyberprzestrzeni, Bezpieczeństwo systemów informatycznych Planowanie ochrony osób, mienia i infrastruktury, Zarządzanie jakością w instytucjach bezpieczeństwa wewnętrznego, Kontrola i audyt w zakresie bezpieczeństwa wewnętrznego, – i doborze przedmiotów ukierunkowanych na kształcenie praktyczne i przygotowanie do rynku pracy zgodnie z kierunkiem kształcenia (Praktyki zawodowe, Seminarium magisterskie, Przygotowanie pracy magisterskiej).

Nadając studiom profil praktyczny w sposób szczególny skoncentrowano się na kształtowaniu praktycznych umiejętności i kompetencji bezpośrednio wymaganych na rynku pracy. Zajęcia modułu kształcenia językowego, większość zajęć modułów specjalnościowych, oraz modułu przedmiotów wspólnych zaprogramowano jako zajęcia praktyczne przypisując im efekty kształcenia typu umiejętności oraz treści ściśle wiążąc z przyszłą aktywnością zawodową.

Znaczącą część programu studiów 1. i 2. stopnia zajmują praktyki zawodowe, którym przypisano łącznie 18 punktów ECTS (10% programu na studiach 1. stopnia i 15% programu na studiach 2. stopnia). Wymiar ten odpowiada wymaganiom zapewnienia trzymiesięcznego wymiaru praktyk dla studentów studiów o profilu praktycznym. Na studiach 1. stopnia zajęciom praktycznym przypisano 113 punktów ECTS, co stanowi 63% ogólnej liczby punktów. Natomiast na studiach 2. stopnia zajęciom praktycznym przyporządkowano 67 punktów ECTS co stanowi 56% ogólnej liczby punktów.[2]

2 *Raport samooceny. Ocena programowa (profil praktyczny). Kierunek Bezpieczeństwo Wewnętrzne,* Wszechnica Polska Szkoła Wyższa w Warszawie, Warszawa 2017, s. 8.

Dużą uwagę uczelnia przywiązuje do wnikliwego i starannego doboru treści kształcenia w ramach poszczególnych przedmiotów.

Punktem wyjścia są założone efekty kształcenia, które powinny współgrać z przekazywanymi treściami, metodami kształcenia oraz sposobami weryfikacji efektów kształcenia (formą zaliczeń).

Studia I stopnia

Na przykład w ramach przedmiotu Wprowadzenie w teorię wywiadu gospodarczego prowadzonego w wymiarze 45 lub 24 jednostek (godzin) lekcyjnych realizowane są następujące tematy i zagadnienia:

1) Znaczenie informacji we współczesnych formach życia społecznego.
2) Definicja wywiadu i kontrwywiadu gospodarczego.
3) Prawne zagadnienia ochrony informacji, tajemnicy przedsiębiorstwa i innych tajemnic zawodowych oraz wywiadu gospodarczego.
4) Otwarte źródła informacji a tajemnica przedsiębiorstwa.
5) Historia i geneza działań wywiadowczych w ekspansji państw i przedsiębiorstw.
6) Teorie poprzedzające rozwój współczesnej koncepcji wywiadu gospodarczego.
7) Warunki sprzyjające rozwojowi wywiadu gospodarczego.
8) Rola wywiadowni gospodarczych.
9) Istota i granice wywiadu gospodarczego.
10) Wywiad gospodarczy a wywiad biznesowy.
11) Współcześni teoretycy wywiadu gospodarczego.
12) Wywiad gospodarczy jako organizacja i proces.
13) Cykl wywiadowczy oraz produkty wewnętrzne wywiadu gospodarczego.
14) Źródła pozyskania informacji w wywiadzie gospodarczym.
15) Problemy etyczne wywiadu gospodarczego.
16) Outsourcing wywiadu gospodarczego.

Przedmiot realizowany jest w formie ćwiczeń. I dlatego wykładowca wybrał do weryfikacji efektów kształcenia indywidualne zadania zaliczeniowe w ramach trzech prac grupowych: Ochrona informacji, Koncepcja ochrony tajemnicy przedsiębiorstwa, Plan działania w zakresie rozpoznawania przedsięwzięć konkurencji. Może też zastosować obserwację i ocenę wykonania zadania praktycznego (zadań).

Efekty kształcenia typu „wiedza" weryfikujemy stosując test wiedzy, ustny sprawdzian wiedzy, pracę pisemną, pracę pisemną z obroną, prezentację.

Z kolei w przypadku efektów kształcenia typu „kompetencje społeczne" ich osiągnięcie weryfikuje się przez rozwiązanie/wykonanie zadania praktycznego lub projektowego, za pomocą zadania zespołowego z indywidualną kontrolą osiągnięć, obserwację i ocenę wykonania zadania praktycznego, a także kontrolę i ocenę przebiegu praktyk zawodowych.[3]

3 Prof. dr hab. Jerzy Wojciech Wójcik, *Karta przedmiotu Wprowadzenie w teorię wywiadu gospodarczego*.

Realizowany w formie wykładów przedmiot Źródła i techniki analizy danych nauczyciel akademicki prowadzi w wymiarze 30 lub 16 jednostek (godzin) lekcyjnych obejmujących następujące tematy i zagadnienia:

1) Nowoczesne przedsiębiorstwa i nowa ekonomia. Przedsięwzięcia typu *Startup*. Małe i średnie przedsiębiorstwa. Korporacje międzynarodowe (transnarodowe). Informacja w działalności gospodarczej.
2) Pozyskiwanie informacji. Informacje i dane. Kanały przepływu informacji. Źródła informacji. Klasyfikacja informacji.
3) Eksploatacja źródeł informacji. Mocne i słabe strony otwartych źródeł informacji. Mocne i słabe strony osobowych źródeł informacji.
4) Proces pozyskiwania informacji. Proces wywiadowczy i miejsce oraz rola analizy. Interpretacje i hipotezy. Prognozy i rekomendacje.
5) Analiza informacji. Psychologia analizy. Myślenie krytyczne. Myślenie kreatywne i koncepcyjne. Błędy poznawcze.
6) Techniki analizy. Ilościowa analiza danych. Jakościowa analiza informacji. Ustrukturyzowana burza mózgów. Analiza „Co jeśli…". Analiza PESTLE. Analiza grup strategicznych. Metoda „Wargaming".

Do weryfikacji efektów kształcenia wykładowca wybrał formy: dłuższa wypowiedź ustna, udział w dyskusji, obserwacja i ocena wykonania zadania praktycznego (zastosowanie metod prezentowanych w wykładzie do rozwiązania problemów praktycznych), ustny sprawdzian wiedzy[4].

Ostatni przykład. *Przedmiot Planowanie działań wywiadu i kontrwywiadu gospodarczego p*rowadzony w formie ćwiczeń podsumowuje zajęcia w ramach specjalizacji, wykorzystuje i pogłębia przekazywaną wiedzę przez jej praktyczne zastosowanie. Obejmuje 60 lub 32 jednostki (godziny) lekcyjne wykorzystywane do przekazania następujących treści (tematów i zagadnień):

1. Podmioty uprawnione do korzystania z otwartych i chronionych źródeł informacji.
2. Potrzeby informacyjne związane z portfelem działalności przedsiębiorstwa.
3. Pozyskiwanie informacji gospodarczych pozyskiwanych podczas imprez handlowych i w rezultacie stosunków biznesowych.
4. Budowanie modelu systemu informacji strategicznej w przedsiębiorstwie.
5. Cykl wywiadu ekonomicznego, przetwarzanie i analiza informacji.
6. Informacyjne metody i środki ochrony zasobów informacyjnych przedsiębiorstwa.
7. Rozpoznawanie zagrożeń.

Weryfikację osiągniętych efektów kształcenia wykładowca przeprowadza w formie indywidualnych zadań zaliczeniowych w ramach trzech prac grupowych: Planowanie rozpoznania konkurencji, Wypracowanie koncepcji działania,

4 mgr Maciej Jankielewicz, *Karta przedmiotu Źródła i techniki analizy danych.*

„Opracowanie planu działania", a ponadto ocenia udział studentki/studenta w dyskusjach, dłuższe wypowiedzi ustne, pisemny sprawdzian wiedzy[5].

Studia II stopnia

Studenci, którzy wybrali specjalizację Wywiad i kontrwywiad gospodarczy realizują przede wszystkim przedmiot obieralny Bezpieczeństwo biznesu prowadzony w wymiarze 30 lub 16 godzin w formie ćwiczeń, który ukierunkowuje ich przygotowanie zawodowe. Kończąc przedmiot powinni osiągnąć następujące efekty kształcenia:

- znać i rozumieć ustawy dotyczące bezpieczeństwa informacji oraz przetwarzania i ochrony danych, potrafić korzystać z norm międzynarodowych i krajowych w zakresie bezpieczeństwa informacji i podmiotów gospodarczych oraz ochrony własności intelektualnej;
- rozumieć funkcje wywiadu i kontrwywiadu biznesowego w działalności gospodarczej oraz umieć wykorzystać je w budowaniu systemu bezpieczeństwa przedsiębiorstwa;
- rozumieć zagadnienia i problemy organizacyjne nowoczesnych przedsiębiorstw, potrafi uczestniczyć w komórkach odpowiedzialnych za bezpieczeństwo organizacji w roli członka grup projektowych i nieetatowych zespołów bezpieczeństwa biznesu opartego wywiad biznesowy;
- znać i rozumieć zagrożenia w działalności biznesowej, potrafić prawidłowo reagować na sytuacje wymagające zarządzania kryzysowego, umieć budować zespół i komórkę zadania i funkcje zadaniową, potrafi we właściwy sposób je przydzielać.

Treść omawianego przedmiotu obejmuje następujące tematy i zagadnienia:

1) Pozyskiwanie informacji. Klasyfikacja informacji. Źródła informacji. Eksploatacja źródeł informacji. Mocne i słabe strony otwartych źródeł informacji. Mocne i słabe strony osobowych źródeł informacji.
2) Kodeks spółek handlowych. Spółki osobowe i spółki kapitałowe. Działalność gospodarcza. Oszustwa w obrocie gospodarczym. Oszustwa podatkowe.
3) Nowoczesne przedsiębiorstwa i nowa ekonomia. Przedsięwzięcia typu Start-up. Małe i średnie przedsiębiorstwa. Korporacje międzynarodowe (transnarodowe). Informacja w działalności gospodarczej.
4) Bezpieczeństwo biznesu. Elementy bezpieczeństwa. Wrażliwość informacji i usług. System ochrony informacji. Polityka bezpieczeństwa podmiotu gospodarczego. System zarządzania bezpieczeństwem informacji.
5) Przepisy i normy. Tajemnica przedsiębiorstwa a informacje wrażliwe. Ustawowe sposoby ochrony tajemnicy przedsiębiorstwa. Normy międzynarodowe i krajowe. Ochrona informacji a bezpieczeństwo biznesu. Zarządzanie ryzykiem i zarządzanie kryzysowe.
6) Audyt. Zabezpieczenia fizyczne i techniczne. Zabezpieczenia programowe (IT). Bezpieczeństwo procedur i struktur organizacyjnych. Kontrwywiad biznesowy.

5 Prof. dr hab. Jerzy Wojciech Wójcik, *Karta przedmiotu Planowanie działań wywiadu i kontrwywiadu*.

6) Strategie biznesowe. Strategia rozwoju i konkurencji. Strategie funkcjonalne. Strategia a wywiad i kontrwywiad biznesowy.
7) Alianse i przejęcia. Walka konkurencyjna. *Due dilligence i benchmarking.* Badanie powiązań kapitałowych i osobowych. Ocena wiarygodności podmiotów i osób.

Wykładowca sprawdza efekty za pomocą obserwacji i oceny wykonania zadań praktycznych, zadań zespołowych z indywidualną kontrolą osiągnięć, testu wiedzy[6]. Wiedza, umiejętności i kompetencje kształtowane na zajęciach dydaktycznych realizowanych w formie wykładów i ćwiczeń są pogłębiane i uzupełniane z zastosowaniem pozostałych form nauczania i uczenia się wykorzystanych w programie studiów.

Niezwykle ważna rola w procesie kształcenia przypada praktykom zawodowym. Są one niezastępowalną formą rozwoju kompetencji niezbędnych w przygotowaniu specjalisty wywiadu i kontrwywiadu gospodarczego. To okazja do uzupełnienia wiedzy i umiejętności nabytych w uczelni, sprawdzenia umiejętności ich zastosowania w warunkach podmiotu gospodarczego, poznania mechanizmów jego funkcjonowania oraz atmosfery i specyfiki pracy z ludźmi.

Praktyki zawodowe realizowane są w komórkach ds. bezpieczeństwa instytucji publicznych i przedsiębiorstw, w agencjach ochrony osób i mienia, biurach detektywistycznych, w wywiadowniach gospodarczych, firmach zajmujących się instalowaniem i realizowaniem monitoringu, z którymi uczelnia podpisała umowy. Są one prowadzone przez opiekunów praktyk w organizacjach i przez nauczycieli akademickich, którzy w formie zajęć grupowych weryfikują osiąganie przez studentów efektów kształcenia przypisanych praktykom.

Opracowanie prac dyplomowych uznajemy – podobnie jak praktyki – za ważny etap i element składowy kształcenia praktycznego. Seminarium dyplomowe licencjackie lub magisterskie ma na celu kształtowanie i weryfikację umiejętności stosowania metod i narzędzi badawczych w rozwiązywaniu problemów zawodowych właściwych dla kierunku studiów i wybranej przez studenta specjalności.

Weryfikacja nabytych kompetencji przyjmuje postać pracy dyplomowej licencjackiej w jednej z dwóch form:

8. Realizacji projektu – pracy pisemnej dokumentującej wybór, opracowanie i realizację rozwiązania konkretnego problemu praktycznego (autorskiego lub polegającego na adaptacji istniejących rozwiązań opisanych w literaturze lub obecnych w praktyce zawodowej). To ustalenie metodyki opracowania i przygotowanie konkretnego dokumentu wykonywanego w praktyce wywiadu i kontrwywiadu gospodarczego uwzględniającego uwarunkowania realne lub określone przez kierownika pracy dyplomowej. Do opracowania i realizacji projektu można wykorzystać praktyki zawodowe.
9. Projektu – pracy pisemnej opisującej wybór i opracowanie rozwiązania problemu (autorskiego lub polegającego na adaptacji istniejących rozwiązań

6 mgr Maciej Jankielewicz, *Karta przedmiotu Bezpieczeństwo biznesu.*

opisanych w literaturze lub obecnych w praktyce zawodowej). Opis rozwiązania powinien zostać poprzedzony badaniami diagnostycznymi z zastosowaniem metod i technik przyjętych w praktyce wywiadu i kontrwywiadu gospodarczego bądź uzupełniony badaniami ewaluacyjnymi (opinią osób kompetentnych i zainteresowanych proponowanym rozwiązaniem). Do opracowania projektu i przeprowadzenia diagnozy lub ewaluacji można wykorzystać praktyki zawodowe.

Prace dyplomowe licencjackie mogą też dotyczyć bardziej złożonego problemu, który jest rozwiązywany przez kilkuosobowy zespół. W tym przypadku należy wyraźnie zaznaczyć odrębny wkład każdego studenta.

3. Infrastruktura dydaktyczna

Literatura i biblioteka

W procesie kształcenia wykorzystujemy literaturę dostępną na polskim rynku wydawniczym. Jako literaturę podstawową i uzupełniającą polecamy naszym studentom m.in. następujące pozycje:

Aleksandrowicz T.R., *Analiza informacji w administracji i biznesie*, Warszawa 1999.

Ciecierski M., Nogacki R., *Bezpieczeństwo współczesnej firmy. Wywiad, szpiegostwo, ochrona tajemnic*, STUDIO EMKA, Warszawa 2016.

Ciecierski M., *Wywiad biznesowy w korporacjach transnarodowych. Teoria i praktyka*, Wyd. Adam Marszałek, Toruń 2009.

Ciecierski M., *Wywiad gospodarczy w walce konkurencyjnej przedsiębiorstw*, PAT, Warszawa 2007.

Cilecki E., *Penetracja rynków zagranicznych. Wywiad gospodarczy,* Warszawa 1997.

Filipkowski W., Mądrzejowski M., *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, C.H. Beck, Warszawa 2012.

Herman M., *Potęga wywiadu*, Dom Wydawniczy Bellona, Warszawa 2002.

Konieczny J., *Wstęp do etyki biznesu*, Warszawa 1998.

Korzeniowski L., Pepłoński A., *Wywiad gospodarczy. Historia i współczesność*, Wydawnictwo EAS, Warszawa 2005.

Kotler P., Marketing. *Analiza, planowanie, kontrola i wdrażanie*, Gebethner & Spółka, Warszawa 1994.

Kwieciński M., *Wywiad gospodarczy w zarządzaniu przedsiębiorstwem*, Wydawnictwo Naukowe PWN SA, Warszawa-Kraków 1999.

Liedel K., Serafin T., *Otwarte źródła informacji w działalności wywiadowczej*, Difin, Warszawa 2011.

Martinet B., Marti Y., *Wywiad gospodarczy. Pozyskiwanie i ochrona informacji*, Polskie Wydawnictwo Ekonomiczne, Warszawa 1999.

Minkina M., *Sztuka wywiadu w państwie współczesnym*, Oficyna Wydawnicza Rytm, Warszawa 2014.

Monitorowanie otoczenia, przepływ i bezpieczeństwo informacji w stronę inteligencji przedsiębiorstwa, pr. zb. pod red. R. Borowieckiego, M. Kwiecińskiego, Kantor Wydawniczy Zakamycze, Zakamycze 2008.

Siemiątkowski Z., Zięba A., *Służby specjalne we współczesnym państwie*, ELIPSA. Warszawa 2016.

Surma J., *Business Intelligence. Systemy wspomagania decyzji*, Wydawnictwo Naukowe PWN SA, Warszawa 2009.

System informacji strategicznej. Wywiad gospodarczy a konkurencyjność przedsiębiorstwa, pr. zb. pod red. R. Borowieckiego, M. Romanowskiej, Wyd. Difin, Warszawa 2007.

Tardejna M., Tardejna R., *Dostęp do informacji publicznej a prawna ochrona informacji dotyczących działalności gospodarczej, społecznej i zawodowej oraz życia prywatnego*, Wyd. Adam Marszałek, Toruń 2003.

Turaliński K., *Wywiad gospodarczy i polityczny. Podręcznik dla specjalistów ds. bezpieczeństwa detektywów i doradców gospodarczych*, wyd.2, ARTEFAKT, Warszawa 2015.

Wójcik J.W., *Ochrona informacji a wywiad gospodarczy. Zagadnienia kryminalistyczne, kryminologiczne i prawne.* Towarzystwo Naukowe Powszechne, Warszawa 2016.

Wójcik J.W. *Wywiad i kontrwywiad gospodarczy*. Wszechnica Polska Szkoła Wyższa w Warszawie. Warszawa 2018.

Wywiad biznesowy. Praktyczne wprowadzenie, red. A. Bielska, P. Smółka, WYDawnictwo nieoczywiste, Warszawa 2017.

Biblioteka uczelni współpracuje z różnymi bibliotekami naukowymi w Warszawie umożliwiając wypożyczanie naszym czytelnikom książek ze zbiorów z tych bibliotek. Daje rewersy międzybiblioteczne np. do Biblioteki Sejmowej iwydziałowych/instytutowych bibliotek Uniwersytetu Warszawskiego. Studentom studiów zaocznych mieszkającym poza Warszawą, często również nauczyciele akademiccy dostarczają książki do Biblioteki i udostępniają je na zasadach uzgodnionych z czytelnikiem i biblioteką wypożyczającą.

Gromadzenie zbiorów Biblioteki jest obecnie ukierunkowane na powiększanie materiałów – w formie papierowej i elektronicznej, wykorzystywanych w praktycznym przygotowaniu zawodowym studentów.Należy podkreślić, że uczelnia konsekwentnie realizuje zaplanowane działania na rzecz adaptacji i rozbudowy posiadanej infrastruktury dydaktycznej służące poprawie warunków realizacji procesu edukacyjnego na kierunku Bezpieczeństwo wewnętrzne o profilu praktycznym, przydatnej także dla specjalności Wywiad i kontrwywiad gospodarczy.

Urządzono pracownię przeznaczoną do realizacji zajęć dydaktycznych służących opanowaniu umiejętności pracy indywidualnej i zespołowej w małych grupach zadaniowych planujących działania służb bezpieczeństwa publicznego. Służy ona zapoznaniu i obyciu studentów z wyposażeniem i organizacją przestrzeni w pomieszczeniach pracy zespołów sztabowych służb bezpieczeństwa publicznego w reagowaniu na sytuacje kryzysowe z wykorzystaniem zainstalowanych narzędzi w czasie realizacji cyklu podejmowania i wdrażania decyzji.

Odpowiednio do przedstawionego przeznaczenia Pracownia została wyposażona w tablicę interaktywną i ekran projekcyjny z projektorami multimedialnymi, sześć białych tablic sucho ścieralnych, tablicę ogłoszeniową i zegar.

Do dyspozycji są laptopy (w praktyce studenci wolą jednak korzystać z prywatnych) i sieć Wi-Fi. Dodatkowo studenci mogą korzystać z Pracowni Komputerowej.

Możliwe jest dowolne kształtowanie przestrzeni Pracowni i ustawianie stołów lekcyjnych w „wyspy" stosownie do potrzeb pracy organizowanych doraźnie grup roboczych.

Wewnątrz pracowni znajduje się dodatkowe pomieszczenie wykorzystane na Magazyn Pomocy Naukowych.

Najważniejszym elementem pracowni jest przygotowany i nadal rozbudowywany zestaw środków (pomocy) dydaktycznych w postaci fragmentów filmów, zbiorów dokumentów oraz programów informatycznych prezentujących symulację działań i przydatnych baz danych niezbędnych do realizacji programu kształcenia.

Jako pomoce dydaktyczne w Pracowni wykorzystuje się:

- akty prawne i dokumenty służbowe (zarządzenia, instrukcje, regulaminy, poradniki) różnych instytucji dotyczące szeroko rozumianej problematyki wywiadu i kontrwywiadu gospodarczego;
- zbiór planów i dokumentów z różnych podmiotów i poziomów zarządzania (w oparciu o wybrane organizowane są zajęcia dydaktyczne);
- dokumenty organizacyjne zespołów i grup funkcjonalnych, m.in. zarządzenia o powołaniu oraz regulaminy i plany pracy;
- plany,
- plany pracy, harmonogramy i grafiki (sporządzane także na ćwiczeniach przez studentów);
- protokoły posiedzeń zespołów i grup funkcjonalnych (sporządzane także na ćwiczeniach przez studentów);
- analizy, oceny i opinie, meldunki (sporządzane także na ćwiczeniu przez studentów);
- raporty bieżące i okresowe (przykłady);
- polecenia, zarządzenia, decyzje i meldunki;
- dokumenty graficzno-tekstowe (mapy, plany, szkice, itp.) z wykorzystaniem Zestawu zasadniczych znaków operacyjnych właściwych dla jednostek organizacyjnych resortu spraw wewnętrznych i administracji z 2008 roku;
- wydruki sytuacyjne i analizy w postaci dokumentów drukowanych oraz zapisanych na nośnikach optomagnetycznych;
- specjalistyczne oprzyrządowanie i oprogramowanie systemu, zapewniające możliwości multimedialnej prezentacji danych;

- mapy operacyjne standardowe i cyfrowe oraz prezentacje specjalistycznego oprogramowania prognostyczno-planistycznego wykorzystywanego w praktyce. (Z oprogramowaniem specjalistycznym studenci są zapoznawani dokładniej podczas praktyk zawodowych).

4. Współpraca z lokalnym środowiskiem społeczno-gospodarczym i współpraca międzynarodowa

Współpraca z otoczeniem społecznym i gospodarczym uczelni powinna zapewnić dostosowanie i powiązanie procesu kształcenia z potrzebami społecznymi i gospodarczymi regionu Mazowsza i pracodawców[7]. Skorzystaliśmy z niej także w celu zagwarantowania racjonalnego doboru treści programowych i przygotowania właściwej jakości procesu edukacyjnego dla uruchomienia specjalności Wywiad i kontrwywiad gospodarczy.

Pomocy udzielili specjaliści – przedstawiciele biznesu pracujący w Radzie Eksperckiej powołanej w Uczelni we wrześniu 2017 roku[8]. Funkcjonuje w niej Zespół ds. kierunku Bezpieczeństwo wewnętrzne, w którego skład wchodzą m.in.:

1. dr Marian Zalewski – Zastępca Dyrektora Zarządu Wykonawczego – Związku Ochotniczych Straży Pożarnych Rzeczypospolitej Polskiej w Warszawie – Przewodniczący Zespołu,
2. mgr Henryk Dąbrowski – Dyrektor Polskiej Izby Systemów Alarmowych w Warszawie, członek Zarządu,
3. mgr Maciej Jankielewicz – *Managing Partner*, członek komitetu sterującego – BWB Consulting sp. z o. o w Warszawie,
4. mgr Zdzisław Mazurski – *Perfekt Business Consulting* w Warszawie.

Kompetencji Rady i Zespołu obejmują m.in.:

1. wymianę doświadczeń oraz informacji pomiędzy uczelnią a członkami Rady reprezentującymi instytucje i organizacje funkcjonujące w otoczeniu społeczno-gospodarczym Wszechnicy Polskiej,
2. sygnalizowanie uczelni potrzeb programowych i kadrowych pojawiających się w związku ze zmianami w otoczeniu gospodarczym,
3. udzielanie rad w zakresie kształtowania i doskonalenia planów i programów kształcenia oraz ich opiniowanie pod kątem przydatności do potrzeb rynku pracy,
4. wskazywanie tematyki prac etapowych i dyplomowych z możliwością ich wykorzystania w macierzystych instytucjach,
5. możliwość realizacji praktyk zawodowych przez studentów w reprezentowanych instytucjach,
6. informowanie o aktualnych tendencjach na rynku pracy.[9]

7 Założenia Programowe i Koncepcja Funkcjonowania Rady Eksperckiej we Wszechnicy Polskiej Szkole Wyższej w Warszawie na lata 2018-2020, Warszawa 3 lipca 2018 r., s. 2.

8 Zarządzenie nr 26/2017 Rektora Wszechnicy Polskiej Szkoły Wyższej w Warszawie z dnia 26.09.2017 r.

9 Założenia Programowe i Koncepcja…, *op. cit*., s. 3.

Projekt programu kształcenia dla specjalności Wywiad i kontrwywiad gospodarczy i jego poprawioną wersję wdrożeniową skonsultowano z Radą w dniach 18 listopada 2017 r. i 3 lipca 2018 r.[10] Poprzedzały je okazjonalne zebrania przedstawicieli Zespołu oraz Katedry Nauk o Bezpieczeństwie realizowane w trybie roboczym.

Spotkania cechowała szczerość, dążenie do uzyskania praktycznych efektów satysfakcjonujących obie strony, otwarcie na krytykę i posługiwanie się w dyskusji argumentami.

Potwierdzenie znajdujemy w protokołach.

Na przykład uczestnicy spotkania w dniu 18 listopada 2017 roku podkreślali w dyskusji dostrzegane praktyczne aspekty działalności Zespołu, możliwe do zastosowania formy współpracy i kontaktów. Stwierdzili, że bezpośrednie kontakty z katedrami, w tym z Katedrą Nauk o Bezpieczeństwie istniały przed zawiązaniem Zespołu i dość dobrze służyły zbliżeniu środowiska przedstawicieli pracodawców i otoczenia społeczno-gospodarczego z uczelnią.

Mgr Maciej Jankielewicz – *Managing Partner*, członek komitetu BWB Consulting sp. z o. o w Warszawie, poinformował zebranych o udziale w pracach nad przygotowaniem i oceną programów kształcenia na kierunku Bezpieczeństwo wewnętrzne o profilu praktycznym.

Jego wypowiedź dotyczyła takiego profilowania kierunków, które pozwoli na współpracę z firmami zewnętrznymi jako uczestnikami procesu kształcenia. Jednocześnie będą oni (przedstawiciele firm) już w trakcie studiów prowadzili własne zajęcia, które pozwolą studentom na uzyskanie dodatkowych uprawnień niezbędnych do późniejszego zatrudnienia. Takie zajęcia może też prowadzić obecna kadra dydaktyczna w porozumieniu z firmą co do programu. Może to być przykładowo uzyskanie uprawnień kwalifikowanego pracownika ochrony podczas studiów licencjackich z dodatkowymi uprawnieniami, które pozwolą takim absolwentom objąć stanowisko kierownika zmiany w portach lotniczych (firm ACS). Inne przykłady to współpraca Związku Banków Polskich w programie studiów związanych z finansami lub z Krajową Administracją Skarbową. Mówił także o rozwijaniu nowych kierunków jak wywiad biznesowy (gospodarczy), ale w oparciu o nowe trendy, które szerzy międzynarodowe stowarzyszenie *Strategic and Competitive Intelligence Professionals*. Na takim kierunku musi być dużo o strategiach biznesowych, ale także o nowych technologiach, *start up'* ach, monitorowaniu i analizie źródeł dostępnych w Internecie, w tym także w tzw. Dark-Necie. Jednocześnie studenci powinni w trakcie studiów uzyskiwać uprawnienia detektywa i rzetelną wiedzę w tym zakresie – jest to bardzo pomocne w polskich warunkach, a nawet niezbędne w przypadku chęci prowadzenia profesjonalnego wywiadu biznesowego, również w dużych korporacjach i strukturach administracji państwowej.

10 Protokół z konsultacji z przedstawicielami otoczenia społeczno-gospodarczego w dniu 18 listopada 2017 r.; Protokoł z posiedzenia Rady Eksperckiej Wszechnicy Polskiej w Warszawie w dniu 3 lipca 2018 r.

Na zakończenie dodał, że współpracuje z Katedrą Nauk o Bezpieczeństwie od blisko roku nad takimi zmianami, jednak jest to skomplikowany i długotrwały proces ze względu na dostrzeganą potrzebę przeprowadzenia wielu niezbędnych zmian w całym programie i poszczególnych przedmiotach. Zmiany te muszą dobrze ze sobą korelować i uzupełniać się w całej ścieżce studiów.

Równie szeroki zakres oczekiwań, uwag i propozycji do pracy zespołu sprecyzował przedstawiciel Polskiej Izby Ochrony mgr Henryk Dąbrowski.

Zgłoszono sugestie dotyczące:

1) formalizacji i usystematyzowania działalności Zespołu Eksperckiego, dostrzeżono potrzebę sformalizowania i usystematyzowania pracy Zespołu, zwłaszcza wypracowania programu jego działania mającego charakter dokumentu strategicznego oraz zebrania propozycji przydatnych do opracowania planu działania Zespołu;
2) jakości kształcenia – jedno ze spotkań kierunkowych poświęcić kwestii odbywania praktyk. Zweryfikować treści i miejsca ich odbywania, stosowane sposoby ewaluacji;
3) kierunkowych efektów kształcenia – przyjęte i obecnie realizowane poddać ponownej analizie na spotkaniu kierunkowym w szerszym składzie członków Zespołu i nauczycieli akademickich pod koniec bieżącego roku akademickiego;
4) programu studiów – zebrać doświadczenia nauczycieli z realizacji najważniejszych zrealizowanych dotąd przedmiotów praktycznych i przedyskutować treści i wskazówki metodyczne zawarte w Kartach przedmiotów z ekspertami. Powinniśmy zapraszać ekspertów do współudziału w hospitowaniu zajęć. Zaprosić ekspertów z poszczególnych kierunków do dyskusji nad tematyką i sposobem realizacji prac dyplomowych.

Kolejna uwaga: bardziej wnikliwie przygotowywać spotkania z ekspertami, poprzedzać je wcześniejszymi konsultacjami.

Podsumowując, dotychczasowe doświadczenia Wszechnicy Polskiej Szkoły Wyższej w Warszawie pozwalają sformułować opinię, że posiedzenia i spotkania Rady i Zespołu stanowią interesującą i wartościową formułę współpracy partnerów, umożliwiają wymianę doświadczeń i informacji zawierających duży potencjał poznawczy, dydaktyczny i społeczny (zawodowy). Na pewno należy współpracę kontynuować i pogłębiać.

6. Współpraca międzynarodowa

W ramach funkcjonowania kierunku Bezpieczeństwo wewnętrzne Wszechnica Polska podpisała umowy międzyinstytucjonalne Erasmus z HU *University of Applied Sciences* (Utrecht, Holandia) oraz U*niversitat Autònoma de Barcelona* (Barcelona, Hiszpania) umożliwiające wymianę studentów oraz kadry. Uczelnia podtrzymuje ponadto kontakty z uczelniami: *Vysoká Škola Bezpečnostného Manažérstva v Košiciach* (Republika Słowacka), Akademią „Koksze" z siedzibą w Kokszetau (Kazachstan) oraz Akademią Bezpieczeństwa Pożarowego im. Bohaterów Czarnobyla z siedzibą w Czerkasach (Ukraina).

W roku akademickim 2015/16 Wszechnica Polska Szkoła Wyższa w Warszawie jako jedyna polska uczelnia stała się członkiem międzynarodowej sieci CONRIS – ang. *Cooperation Network for Risk, Safety and Security Studies*, zrzeszającej między innymi uczelnie z Niemiec, Danii, Holandii, Austrii, Finlandii, Wielkiej Brytanii, Belgii, oferujące studia na kierunku Bezpieczeństwo.

Udział w sieci umożliwia tworzenie wspólnych ścieżek badawczych, wspólnych programów studiów, wyjazdy studentów do szkół letnich organizowanych przez uczelnie należące do sieci Conris. Członkostwo pozwala pracownikom naukowo-dydaktycznym na prowadzenie wykładów we współpracujących uczelniach.

W roku akademickim 2015/16 dwóch pracowników naukowo-dydaktycznych Wszechnicy z kierunku Bezpieczeństwo wewnętrzne zrealizowało wykłady w ramach mobilności STA na uczelni partnerskiej Erasmus: HU *University of Applied Sciences* oraz uczestniczyło w *International Week* organizowanym przez tę instytucję. Przedstawiciele partnerskich uczelni goszcząc w Wszechnicy spotykają się ze studentami kierunku w ramach wykładów gościnnych. W roku akademickim 2016/2017 zajęcia w formie konwersacji ze studentami Wszechnicy przeprowadzili dr Marcel M.J. Paschedag CPO i docent Michiel Spoor z *Saxion University of Applied Sciences* z miasta Enschede w Holandii.

W roku akademickim 2017/2018 Uczelnia rozwijała współpracę międzynarodową z siecią CONRIS. W dniach 1-2 marca 2018 r. w Wszechnicy Polskiej Szkole Wyższej w Warszawie odbyła się pierwsza w Polsce Międzynarodowa Konferencja sieci CONRIS.

Spotkanie rozpoczął referat gospodarzy prezentujący naszą Uczelnię i jej dokonania. Przedstawiono tradycje, dzieje i strukturę szkoły. Gros uwagi poświęcono kwestiom dotyczącym kształcenia na kierunku Bezpieczeństwo wewnętrzne. Wyjaśniono specyfikę i uwarunkowania procesu kształcenia. Scharakteryzowano studentów, a także oczekiwania ich oraz potencjalnych pracodawców. Szczegółowo opisano nasze programy studiów I i II stopnia. Przekazano charakterystykę kadry dydaktycznej. Poinformowano o zamiarach i planach Wszechnicy i Katedry na przyszłość, a także o oczekiwaniach Uczelni wobec sieci CONRIS. Referat wywołał dyskusję – gospodarze odpowiadali na interesujące i dociekliwe pytania świadczące o wysokich kompetencjach zawodowych interlokutorów spośród naszych gości.

Dwudniowe obrady dotyczyły spraw organizacyjnych i planów współpracy międzynarodowej uczestników sieci w kwestiach naukowych i dydaktycznych, w tym także udziału Wszechnicy Polskiej w jej pracach.

Udział przedstawicieli Wszechnicy w Konferencji, w tym Kierownika Katedry Nauk o Bezpieczeństwie, uznajemy za wyjątkową okazję do pogłębienia znajomości aktualnych problemów i stanu rozwoju wiedzy o bezpieczeństwie wewnętrznym w krajach anglosaskich oraz kierunków rozwoju kształcenia przyszłych specjalistów, w tym dostrzeganych wyzwań, przekazywanych treści, stosowanych form i metod nauczania oraz podejmowanych inicjatyw. Zgromadzono ma-

teriał porównawczy przydatny do samooceny dokonań własnych naszej Uczelni i ukierunkowania rozwoju wizytowanego kierunku w warstwach organizacyjnej, programowej, dydaktycznej i badawczej.

Za równie udany i owocny uważamy udział przedstawiciela Wszechnicy Polskiej – dr. Andrzeja Nikołajczuka (wykładowcy na kierunku Bezpieczeństwo wewnętrzne) w zajęciach Szkoły Letniej CONRIS (ang. *The 2018 CONRIS Summer School*) przeprowadzonych w dniach 1-6 lipca 2018 r. przez *University of Portsmouth* w Plymouth, Wielka Brytania. Wsparcia imprezie udzielił program Unii Europejskiej Erasmus +.

To coroczne wydarzenie gromadzi studentów i nauczycieli akademickich z całej Europy oraz współpracowników z kluczowych agencji bezpieczeństwa z kraju goszczącego. Uczestnicy mieli okazję przeanalizować szereg współczesnych wyzwań związanych z bezpieczeństwem i sposobów ich rozwiązywania, poznać powiązania międzykulturowe na studiowanym kierunku i zdobyć kolejne umiejętności zawodowe przy wsparciu różnych specjalistów ds. bezpieczeństwa z innych krajów.

Temat spotkania – „Od spraw globalnych do lokalnych: dostarczanie bezpieczeństwa w niepewnych czasach" (ang. *From Global to Local: Delivering Security in Uncertain Times),* zwrócił uwagę na wybrane zagrożenia charakterystyczne dla dzisiejszego niepewnego i wzajemnie połączonego świata. Uczestników zapoznano z aktualnymi podejściami do nowych wyzwań bezpieczeństwa możliwymi do zastosowania w sektorze publicznym lub prywatnym, a także na różnych poziomach: międzynarodowym, krajowym, lokalnym lub organizacji. Stworzono okazje do rozmów, ćwiczeń, dyskusji i wizyt w wybranych miejscowych instytucjach zajmujących się bezpieczeństwem, pozwalających zapoznać się z kluczowymi zagadnieniami i pomysłami na rozwiązywanie problemów, metodami i taktykami przydatnymi dla oceny i zarządzania ryzykiem bezpieczeństwa w różnych kontekstach.

W czasie zajęć przedstawiono m.in. charakterystykę i różne aspekty zastosowania metody analizy rodzajów i skutków możliwych błędów (ang. *Failure mode and effects analysis* – FMEA). Z ocenami współczesnych ryzyk z perspektywy rządu zapoznali uczestników przedstawiciele brytyjskiego Centrum Ochrony Infrastruktury Narodowej. Zasady bezpieczeństwa w Międzynarodowym Porcie w Portsmouth przybliżył miejscowy funkcjonariusz ds. bezpieczeństwa portu. Scharakteryzowane zostały także zasady bezpieczeństwa obowiązujące w kampusie Uniwersytetu w Portsmouth (przez Greame'a Dysona, szefa ochrony Uniwersytetu). Z kolei procedury bezpieczeństwa stosowane w centrum handlowym *Gunwharf Quays* wyjaśniał Bob Ralph, kierownik ochrony centrum.

Referat programowy „Opis ryzyk bezpieczeństwa i ochrony w czasie organizowanych wydarzeń w niepewnych czasach" wygłosił Kaci Bourdache z Uniwersyteut Laurea, Finlandia. Ciekawe kwestie dotyczące „Etyki w zarządzaniu ryzykiem" omówił Joaquin Rodriguez z Uniwersytet w Barcelonie, Hiszpania.

Przedstawiciel Wszechnicy Polskiej – dr Andrzej Nikołajczuk – przedstawił referat nt. „Wywiad i kontrwywiad gospodarczy w przedsiębiorstwie".

Ponadto prezentowane były referaty wykładowców i doktorantów z uczelni w Ni

W naszej ocenie – aktywność w sieci CONRIS oraz udział w Europejskiej Szkole Letniej CONRIS ma dla Wszechnicy Polskiej duże znaczenie poznawcze. Umożliwia rozeznanie aktualnych problemów kształcenia w kierunku Bezpieczeństwa wewnętrznego w uczelniach różnych państw. Jest przydatne dla właściwego nastawienia rozwoju kierunku bezpieczeństwo wewnętrzne i prowadzonych w jego ramach specjalizacji. Pozwala wzbogacić treści kształcenia i doskonalić nasz warsztat dydaktyczny.

7. Podsumowanie

Wszechnica Polska wprowadza stopniowo od 1.10.2016 r. na kierunku studiów Bezpieczeństwo wewnętrzne praktyczny profil kształcenia. W roku akademickim 2017/2018 uruchomiła na studiach I stopnia (licencjackich) specjalność Wywiad i kontrwywiad gospodarczy a na studiach II stopnia (magisterskich) możliwość wyboru przedmiotu obieralnego Bezpieczeństwo biznesu wspieranego przez treści pozostałych przedmiotów. Specjalizacja przeznaczona jest dla osób zainteresowanych pracą w komórkach bezpieczeństwa przedsiębiorstw, w wywiadowniach gospodarczych, w biurach detektywistycznych, w agencjach ochrony mienia i osób oraz dla kandydatów na funkcjonariuszy służb mundurowych i służb specjalnych.

Kształcenie specjalisty wywiadu i kontrwywiadu gospodarczego realizuje na szerszej podbudowie wiedzy, umiejętności i kompetencji z zakresu bezpieczeństwa wewnętrznego w ogóle, „wmontowując" weń potrzeby specjalizacji. Dzięki temu zabiegowi absolwent zna kontekst i uwarunkowania osobistej działalności, rozumie własną rolę i zadania, a także potrzebę współdziałania z innymi podmiotami.

Oceny potrzeb rynku pracy dokonywane okresowo przez uczelnię we współpracy z partnerami wskazują, że środowisko zawodowe i przyszli pracodawcy oczekują, że absolwenci studiów I stopnia ze specjalizacją w zakresie wywiadu i kontrwywiadu gospodarczego będą realizować zadania w rolach doradcy, planisty, bezpośredniego organizatora pracy lub wykonawcy. Dla kończących studia II stopnia przewidywane są stanowiska starszych specjalistów i (z czasem) kierowników niższego i średniego szczebla.

Odpowiedni do zidentyfikowanych ról zawodowych absolwenta sformułowano efekty kształcenia.

Kształcenie w specjalności Wywiad i kontrwywiad gospodarczy realizowane jest na 5. i 6. semestrze studiów I stopnia. Poprzedzają je cztery semestry studiów prowadzone z ogółem studentów.

Nadając studiom profil praktyczny w sposób szczególny skoncentrowano się na kształtowaniu praktycznych umiejętności i kompetencji bezpośrednio wymaganych na rynku pracy.

Dużą uwagę uczelnia przywiązuje do wnikliwego i starannego doboru treści kształcenia w ramach poszczególnych przedmiotów. Punktem wyjścia są założone efekty kształcenia, które powinny współgrać z przekazywanymi treściami, metodami kształcenia oraz sposobami weryfikacji efektów kształcenia (formą zaliczeń).

Wiedza, umiejętności i kompetencje kształtowane na zajęciach dydaktycznych realizowanych w formie wykładów i ćwiczeń są pogłębiane i uzupełniane z zastosowaniem pozostałych form nauczania i uczenia się wykorzystanych w programie studiów.

Niezwykle ważna rola w procesie kształcenia przypada praktykom zawodowym. Są one niezastępowalną formą rozwoju kompetencji niezbędnych w przygotowaniu specjalisty wywiadu i kontrwywiadu gospodarczego. To okazja do uzupełnienia wiedzy i umiejętności nabytych w uczelni, sprawdzenia umiejętności ich zastosowania w warunkach podmiotu gospodarczego, poznania mechanizmów jego funkcjonowania oraz atmosfery i specyfiki pracy z ludźmi.

Opracowanie prac dyplomowych uznano – podobnie jak praktyki – za ważny etap i element składowy kształcenia praktycznego. Seminarium dyplomowe licencjackie lub magisterskie ma na celu kształtowanie i weryfikację umiejętności stosowania metod i narzędzi badawczych w rozwiązywaniu problemów zawodowych właściwych dla kierunku studiów i wybranej przez studenta specjalności.

Pomocy w uruchomieniu specjalności Wywiad i kontrwywiad gospodarczy udzielili specjaliści – przedstawiciele biznesu pracujący w składzie Rady Eksperckiej powołanej w Uczelni. Funkcjonuje w niej Zespół ds. kierunku Bezpieczeństwo wewnętrzne.

Także współpraca międzynarodowa ma dla Wszechnicy Polskiej duże znaczenie poznawcze. Umożliwia rozeznanie aktualnych problemów kształcenia w kierunku Bezpieczeństwa wewnętrznego w uczelniach innych państw. Jest przydatna dla właściwego nastawienia rozwoju kierunku bezpieczeństwo wewnętrzne i prowadzonych w jego ramach specjalizacji. Pozwala wzbogacić treści kształcenia i doskonalić uczelniany „warsztat" dydaktyczny.

Hieronim Szafran*

***dr Hieronim Szafran, Wszechnica Polska Szkoła Wyższa w Warszawie**

Artur Kryst

Ochrona tajemnicy przedsiębiorstwa przed cyberwywiadem biznesowym

Wprowadzenie

Ochrona tajemnicy przedsiębiorstwa i przedsiębiorcy stała się współcześnie bardzo ważnym problemem, gdyż gwałtowny rozwój globalizacji i społeczeństwa informacyjnego spowodowały, że informacja stała się podstawą handlu. Pozyskanie informacji jest kluczowym aspektem przetrwania przedsiębiorcy zarówno na rynku krajowym jak i międzynarodowym. Poznanie tajemnic przedsiębiorstwa, przeciwnika, konkurenta oraz ochrona informacji własnych, w sposób skuteczny może przyczynić się do zwycięstwa jak i do porażki w biznesie[1]. Wypada jednak zauważyć, że samo pozyskanie kluczowych informacji nie wystarczy do sukcesu firmy, ale stanowi jedynie punkt wyjścia do podejmowania istotnych decyzji strategicznych w przedsiębiorstwie[2].

Zainspirowany przez wykładowców Uczelni, przedstawiam w artykule syntezę wyników badań zrealizowanych przez kilkuosobową grupę studentów Wszechnicy Polskiej Szkoły Wyższej w Warszawie w ramach przygotowań do jednego z ćwiczeń zrealizowanych w ramach przedmiotu Bezpieczeństwo biznesu.

Zadaniem studentów (celem badań) była identyfikacja i wyjaśnienie istoty zagrożeń cyberwywiadem biznesowym polskich przedsiębiorstw oraz stanu rozwoju metod przeciwdziałania zjawisku przez państwo oraz przedsiębiorstwa. Mieliśmy rozwiązać problem zawarty w pytaniu: jak państwo polskie i przedsiębiorstwa chronią tajemnice przedsiębiorcy przed nieprzyjaznym cyberwywiadem biznesowym? Przygotowane rozwiązania były następnie obiektem kilkugodzinnej dyskusji naszej grupy studenckiej[3].

Do poszukiwania odpowiedzi – jako studenci – wykorzystaliśmy metody badawcze: *desk research*, analizę i krytykę piśmiennictwa, badanie dokumentów. Stosowaliśmy również metody teoretyczne poznania. Źródła wiedzy stanowiły międzynarodowe i krajowe normy prawne, literatura przedmiotu, dokumenty wewnętrzne instytucji, artykuły prasowe oraz publikacje pochodzące z Internetu, w tym dane z ankiet i raportów, które zostały wtórnie wykorzystane.

1 L. Korzeniowski, A. Pepłoński, *Wywiad gospodarczy: historia i współczesność*, Wydawnictwo European Association for Security, Kraków 2005, s. 119.

2 M. Ciecierski, *Wywiad biznesowy w korporacjach transnarodowych. Teoria i praktyka*, Wyd. Adam Marszałek, Toruń 2009, s. 107.

3 Poszerzył je i rozwinął kolega Sylwester Tomasz Woźniak, który pobudzony udziałem w ćwiczeniu przygotował i obronił pół roku później pracę magisterską. Dziękuję mu za zgodę na jej wykorzystanie w przygotowaniu niniejszego artykułu.

Artykuł proszę traktować jako przykład dydaktyczny – ilustrację zakresu igłębi merytorycznej treści kształcenia, a także specyfiki zastosowanych form i metod nauczania i uczenia się.

1. Istota walki informacyjnej na tle konkurencji gospodarczej

Informacja w przedsiębiorstwie jest bardzo ważnym aspektem wiedzy zgromadzonej w organizacji, jej kapitałem. A zatem powinna być odpowiednio chroniona z uwzględnieniem metod działania potencjalnych konkurentów, w sposób skuteczny od strony prawnej (przez egzekwowanie regulacji ustawowych) i fizycznie (przez ochronę i kontrwywiad przedsiębiorstwa), w celu wyeliminowania zagrożeń – jej utracenia, zniszczenia lub ujawnienia osobie trzeciej. W przeciwnym razie może po upływie pewnego czasu nastąpić utrata przewagi konkurencyjnej na rynku wewnętrznym i międzynarodowym oraz powolna degradacja przedsiębiorstwa.

Walka informacyjna prowadzona jest w sposób skryty, aby zainteresowane podmioty nie odkryły prawdziwych intencji gracza – konkurenta. Jej celem jest osiągnięcie korzyści gospodarczych, niekiedy politycznych, jak również promowanie własnego przedsiębiorstwa. Państwo powinno odpowiednio stosować regulacje prawne, finansowe i kapitałowe, a także stwarzać różnego rodzaju fundusze i programy pomocowe dla polskich przedsiębiorstw, aby je chronić na agresywnym rynku wewnętrznym i międzynarodowym, w tym unijnym. Gwałtowny rozwój technologiczny stymuluje szybki rozwój wywiadu państwowego i niepaństwowego, powodując liczne zagrożenia dla przedsiębiorcy i przedsiębiorstwa, a tym samym wymusza konieczność lepszego zgłębienia mechanizmów działania wywiadu gospodarczego i biznesowego oraz zagrożeń, na które może się natknąć firma, w tym z wrogim wykorzystaniem nowych technologii w cyberprzestrzeni.

Pod pojęciem aktorów konfliktu informacyjnego rozumie się między innymi:

1) instytucje państwowe, w tym związane ze służbami specjalnymi a także z problematyką komunikacji i informacji;
2) organizacje prywatne, których działalność opiera się na zysku. Najważniejszą rolę odgrywają w tym przypadku firmy *Public Relations* (PR) różnej wielkości i skali działania, determinującej obszar i zakres funkcjonowania, jak również grupy przestępcze wykorzystujące okazję;
3) organizacje społeczne, których zasadnicza działalność opiera się na realizacji szczytnych celów, są najczęściej określane, jako *non-profit* lub humanitarne, ze względu na sposób finansowania[4].

Naruszenie bezpieczeństwa gospodarczego (ekonomicznego) państwa, może być działaniem celowym. Może przyjąć postać agresji ekonomicznej zmierzają-

4 P. Daniluk, *Współczesne wymiary konfrontacji informacji*, „Rocznik Bezpieczeństwa Międzynarodowego" 2014, vol. 8, nr 2, http://www.rocznikbezpieczenstwa.dsw.edu.pl/rocznik-bezpieczenstwa-miedzynarodowego/numery/2014-vol-8-nr-2/, (17.05.2017).

cej do destabilizacji gospodarki popraez manipulacje wskaźnikami ekonomicznych (osłabienie kursu waluty państwa – spowodowane walką informacjami, polegającej na manipulacji percepcji z użyciem działań psychologicznych). Może być również formą uzależnienia gospodarki poprzez zwiększenie wpływu na firmy eksportujące i importujące, w zakresie technologii czy własnych zasobów, co może skutkować dalszym uzależnieniem sektora finansowego państwa od obcego kapitału, a tym samym może przekładać się na decyzje ekonomiczne, polityczne i wojskowe państwa. Może znacznie ograniczać sskuteczność państwa oraz przedsiębiorstw znajdujących się w nim na globalnym rynku konkurencji gospodarczej[5].

Dlatego przedsiębiorca, w myśl ustawy o zwalczaniu nieuczciwej konkurencji[6], powinien opracować i wdrożyć procedury administracyjno-organizacyjne ochrony tajemnicy przedsiębiorstwa, oparte na pięciu filarach:

1) sporządzenie wykazu (katalogu dokumentów) informacji stanowiących tajemnicę przedsiębiorstwa;
2) sporządzenie listy osób uprawnionych do zapoznania się z tajemnicą przedsiębiorstwa, z racji wykonywania obowiązków służbowych i zawodowych;
3) stworzenie instrukcji lub regulaminu ochrony tajemnicy przedsiębiorcy;
4) zebranie oświadczeń od kluczowych pracowników, zobowiązujących ich do zachowania tajemnicy;
5) przeszkolenie pracowników z zakresu ochrony tajemnicy przedsiębiorstwa[7].

Zagrożenia dla przedsiębiorstwa działającego w cyberprzestrzeni są jeszcze większe i jakościowo inne, ponieważ organizują je i prowadzą specjaliści wywiadu biznesowego lub gospodarczego, stosując specyficzne metody i środki pozyskiwania informacji o przedsiębiorstwie.

2. Zagrożenia cyberwywiadowcze ze strony konkurencji

Zagrożenia dla przedsiębiorstw działających w cyberprzestrzeni wynikają z dużej wrażliwości Internetu na akty cyberszpiegostwa, a to z racji jego unikalnych właściwości. Jest on obecnie kopalnią wiedzy dla wywiadu biznesowego korzystającego ze wsparcia narzędzi informatycznych. Należy podkreślić, że państwowe służby specjalne straciły monopol działalności wywiadowczej w cyberprzestrzeni. Obecnie głównymi aktorami zajmującym się wywiadem biznesowym są konkurencyjne przedsiębiorstwa, instytuty badawcze, uniwersytety, wywiadownie gospodarcze, agencje ratingowe, jak również pojedyncze osoby

5 A. Żebrowski, *Ewolucja polskich służb specjalnych. Wybrane obszary walki informacyjnej (wywiad i kontrwywiad w latach 1989 -2003)*, Wyd. Oficyna Wydawnicza ABRYS, Kraków 2005, s. 256.

6 Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. 1993 nr 47, poz. 211, t.j. Dz. U. z 2018 r. poz. 419, 1637.).

7 K. Ślusarczyk, *Tajemnica przedsiębiorstwa, handlowa, giełdowa – filary bezpieczeństwa biznesowego i rozwoju gospodarczego kraju,* [w:] *Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały X kongresu*, red. J. Sobczak, M. Gajos-Grżetic, Wyd. Krajowe Stowarzyszenie Ochrony Informacji Niejawnych, Katowice 2014, s. 103.

wynajęte do konkretnego zlecenia, np. hakerzy do sprawdzenia szczelności własnego systemu[8].

Na gwałtowny rozwoju działalności wywiadu w cyberprzestrzeni oraz rolę informacji w biznesie miało wpływ kilka czynników:

1) stale powiększające się tempo operacji biznesowych;
2) nadmierne nagromadzenie informacji w przedsiębiorstwie (tzw. szum informacyjny);
3) globalizacja rynków, a tym samym wzrost agresywności konkurencji (walka o utrzymanie rynku zbytu);
4) wpływ zmian politycznych na działalność przedsiębiorstw;
5) postęp technologiczny i funkcjonowanie społeczeństwa informacyjnego[9].

Wynika stąd szereg zagrożeń z cyberprzestrzeni groźnych dla bezpieczeństwa informacji w przedsiębiorstwie. W literaturze wyróżnia się:

1) zagrożenia losowe – do których należą wszelkiego rodzaju klęski żywiołowe, awarie techniczne, które mogą zniszczyć nośniki informacji np.: pęknięta rura z wodą i zalane serwery w piwnicy;
2) tradycyjne zagrożenia informacyjne – do takich należy zaliczyć szpiegostwo, sabotaż, działania walki konkurencyjnej o charakterze ofensywnym i dezinformacyjnym prowadzonym przez osoby, podmioty lub organizacje;
3) zagrożenia technologiczne – związane z pozyskaniem, przechowywaniem, analizą, i przekazaniem wytworzonej wiedzy w sieciach teleinformatycznych (chmura). Do tych zagrożeń należy zaliczyć przestępstwa komputerowe, cyberterroryzm, walkę informacyjną;
4) zagrożenia związane z nieodpowiednimi rozwiązaniami organizacyjno-strukturalnymi (małe i średnie przedsiębiorstwa mają słabo rozwiniętą politykę bezpieczeństwa lub nawet jej brak, co wiąże się z przełożeniem na odpowiednie procedury ochrony)[10].

Z punktu widzenia lokalizacji zagrożenia w cyberprzestrzeni możemy podzielić na:

1) źródła wewnętrzne – powstałe wewnątrz firmy, mające charakter uszkodzenia danych z powodu błędu lub przypadkiem. Również utrata lub uszkodzenie danych celowe spowodowane przez przekupionego pracownika;
2) źródła zewnętrzne – powstałe poza strukturą przedsiębiorstwa, mające na celu utratę, uszkodzenie lub pozbawienie danych, powstałe przy pomocy osób trzecich w sposób celowy lub przypadkowy dla sieci lub systemu przedsiębiorstwa;

8 http://www.wywiad-gospodarczy.pl/cyberprzestrzen.html (17.03.2017).
9 K. Lidel, T. Serafin, *Otwarte źródła informacji w działalności wywiadowczej*, Wyd. Difin, Warszawa 2011, s. 128.
10 M. Jabłońska, M Mielus, *Zagrożenia bezpieczeństwa informacji w organizacji gospodarczej,* [w:] *Bezpieczeństwo informacji i biznesu. Zagadnienia wybrane,* red. M. Kwieciński, Wyd. Krakowskie Towarzystwo Edukacyjne, Kraków 2010, s. 28.

3) źródła fizyczne – są to wszystkiego rodzaju katastrofy, awarie, wypadki związane z nieprzewidzianymi zdarzeniami mogące uszkodzić systemy informatyczne lub urządzenia sieciowe[11].

Taki podział wskazuje, z jakiej strony może przyjść zagrożenie np. cyberszpiegostwa. Może ono mieć charakter wewnętrzny – w postaci przekupionego pracownika, zatrudnionego agenta, lub charakter zewnętrzny – w postaci włamania i kradzieży, jako tańsza alternatywa tradycyjnego szpiegostwa.

Niestety, w cyberszpiegostwie przemysłowym, które napędzane jest potrzebami rozwojowymi oraz wyścigiem technologicznym gospodarek narodowych, jak również korporacji międzynarodowych i przedsiębiorstw, nie liczą się żadne sojusze, decydują jedynie interesy gospodarcze, a co za tym idzie narodowy dobrobyt oraz rozwój rodzimych przedsiębiorstw[12]. Istnieje kilka przesłanek, które spowodowały aż tak duży rozwój cyberszpiegostwa przemysłowego:

1) bardzo trudne wykrycie sprawców operacji szpiegowskich spowodowanych eksterytorialnością (duża odległość od miejsca czynu) oraz podobieństwem narzędzi, taktyki i techniki popełnienia przestępstw, co uniemożliwia identyfikację osób odpowiedzialnych za włamania komputerowe;
2) sprawcą kradzieży informacji w cyberprzestrzeni może być każdy, poczynając od słabego państwa poprzez niewielkie przedsiębiorstwo, których zasób finansowy pozwala na wynajęcie zdolnego hakera (*craker*), który wykradnie wrażliwe informacje;
3) w cyberprzestrzeni trudno ustalić motyw działania sprawców, ponieważ zaciera się różnica pomiędzy cyberprzestępstwem (w szerokim rozumieniu) a gromadzeniem informacji gospodarczych i technologicznych przez podmioty państwowe i niepaństwowe;
4) cyberprzestrzeń oferuje bezpieczeństwo sprawcom np.: pracownik organizacji „wtyczka lub zdrajca", który w ten sposób może sprzedać wiedzę bez fizycznego spotkania, co znacznie utrudnia wykrycie;
5) cyberszpiegostwo jest tanią i szybką alternatywą dla szpiegostwa tradycyjnego, gdzie bardzo duża ilość informacji może być zgromadzona na niewielkim nośniku danych i szybko przesłana za pomocą Internetu bez żmudnego i czasochłonnego kopiowania i gromadzenia pojedynczych stron dokumentacji[13];
6) brak monopolu państw na wywiad gospodarczy, a co za tym idzie przejście części specjalistów wywiadu państwowego do sektora prywatnego.

Powyższe czynniki znacznie przyczyniły się do rozwoju cyberszpiegostwa, jak również są przyczyną ignorowania zagrożeń ze strony małych i średnich przedsiębiorstw w Polsce. Niska świadomość zagrożeń oraz brak inwestycji odnośnie do bezpieczeństwa informacji we własnych systemach informatycznych spowodowana jest błędnym założeniem, że taka inwestycja w bezpieczeństwo systemu ochrony jest bardzo droga.

11 Tamże.

12 http://www.wywiad-gospodarczy.pl/cyberprzestrzen.html (7.05.2017).

13 Tamże, (17.04.2017).

Niestety, takie podejście spowodowało, że według danych z raportu firmy Kroll Ontrack z 2012 r., opartego na dużej grupie przebadanych przedsiębiorstw w Polsce, aż 25% poniosło straty z tytułu utraty informacji. Natomiast w Europie, według raportu PwC, aż 93% badanych małych i średnich przedsiębiorstw utraciło informacje wrażliwe[14].

Przedstawiciele średnich i małych firm często błędnie uważają, że nie przetwarzają żadnych danych osobowych, a tym samym bagatelizują problem związany z zagrożeniami płynącymi z cyberprzestrzeni i rozpoznania konkurencyjnego prowadzonego przez wywiad biznesowy z zasobów Internetu, jak również nielegalnymi metodami szpiegostwa i kradzieży danych. Obecnie widoczna jest raczej bardzo niska świadomość kierownictwa firm w powyższym zakresie, chociaż widać wzrost świadomości zagrożeń i chęci dokonania zmian w tym obszarze. Przyczyn tego należy upatrywać w dużych stratach ekonomicznych dla firmy; w roku 2013 aż 40% firm traci dane ze środowisk wirtualnych (chmura – BIG DATA), przy 65% w 2011 roku[15]. Wiąże się to z bardzo dużymi kosztami odzyskania ich (jeżeli nie mamy kopii zapasowych), ponieważ brak jakichkolwiek zabezpieczeń na początku wiąże się z większymi wydatkami w chwili zaistnienia potrzeby i stworzenia wszystkiego od zera.

W roku 2015 wszystkie pięć prawdopodobnych zagrożeń było związane z działalnością przedsiębiorstwa i były to: *Phishing* z wykorzystaniem poczty elektronicznej, atak DDoS na podmioty komercyjne, zagrożenia dla platformy Android, wyciek danych zawierających dane osobowe, APT – atak ukierunkowany na organizacje.

Z naszych rozważań wynika wniosek, że w dobie dynamicznie rozwijającej się gospodarki cyfrowej i społeczeństwa informacyjnego niezbędne są nowe, kolejne, doskonalsze narzędzia i rozwiązania (prawne i techniczne), które zapewnią bezpieczeństwo danych, jak również przesyłu oraz sieci i urządzeń mobilnych dla przedsiębiorstw i konsumentów. Konieczne są również wzmożone szkolenia i kampanie edukacyjne, które mogą znacznie poprawić świadomość firm i obywateli w stosunku do zagrożeń i możliwości ochrony danych w cyberprzestrzeni[16].

14 J. Sobczak, *Wybrane zagadnienia bezpieczeństwa informacji w małych i średnich przedsiębiorstwach*, [w:] *Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały X kongresu*, Red. J. Sobczak, M. Gajos-Gržetic, Wyd. Krajowe Stowarzyszenie Ochrony Informacji Niejawnych, Katowice 2014, s. 41.

15 http://media.ontrack.pl/pr/255055/niemal-polowa-firm-traci-dane-ze-srodowisk-wirtualnych, (18.04.2017).).

16 https://www.cybsecurity.org/najwieksze-zagrozenia-dla-bezpieczenstwa-w-internecie-w-roku-2014-glos-polskich-eksper tow, (8.05.2017).

3. Instytucjonalne formy ochrony tajemnic przedsiębiorstw przed wywiadem biznesowym w sferze polskiej cyberprzestrzeni. Rola państwa i analiza przyjętych w kraju środków normatywnych ochrony

Państwo organizuje i utrzymuje odpowiedni arsenał instrumentów do ochrony własnych interesów. Wypracowuje odpowiednią politykę przeciwdziałania szpiegostwu gospodarczemu. Głównym elementem przeciwdziałania wywiadowi jest system ochrony informacji niejawnych, zarządzany za pośrednictwem instytucji ABW i SKW, które nadzorują funkcjonowanie systemu ochrony informacji niejawnych w podległych jednostkach organizacyjnych oraz przedsiębiorstwach. Wskazane służby:

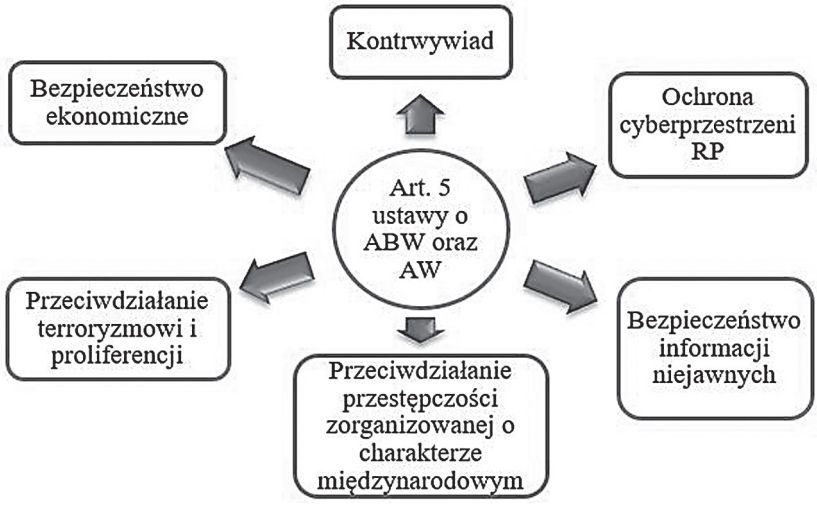
1. „przeprowadzają kontrolę ochrony informacji niejawnych oraz przestrzegania przepisów w tym zakresie;
2. realizują zadania w zakresie bezpieczeństwa systemów teleinformatycznych;
3. przeprowadzają postępowania sprawdzające, kontrolne oraz postępowania bezpieczeństwa przemysłowego;
4. zapewniają ochronę wymiany informacji niejawnych między Rzeczpospolitą Polską, a innym państwem, organizacją, przedsiębiorstwem;
5. prowadzą szkolenia i doradztwo w zakresie ochrony informacji niejawnych, również dla przedsiębiorców[17]".

Do głównych zadań ochrony kontrwywiadowczej kraju została utworzona Agencja Bezpieczeństwa Wewnętrznego, która odpowiada za ochronę podmiotów mogących znaleźć się w zainteresowaniu innych służb wywiadowczych oraz za monitorowanie ich działań na terytorium RP, w celu wykrycia i zneutralizowania nielegalnych prób pozyskania informacji prawnie chronionych. System ochrony ABW jest skoncentrowany na urzędach administracji centralnej i terenowej, na podmiotach gospodarczych istotnych dla interesów państwa oraz na ochronie ośrodków naukowych i technicznych, zajmujących się technologiami podwójnego zastosowania[18]. Na rys. 1 wskazano ustawowy obszar zagrożeń dla państwa, w którym Agencja Bezpieczeństwa Wewnętrznego realizuje zadania ochronne.

17 http://www.iniejawna.pl/pomoce/przyc_pom/4_organizacja_in.html, (18.05.2017).

18 https://www.abw.gov.pl/pl/zadania/kontrwywiad/ochrona-kontrwywiadowc/40,Ochrona-kontrwywiadowcza-kraju.html, (28.05.2015).

Rysunek 1. Obszar zadań ochronnych realizowanych przez Agencję Bezpieczeństwa Wewnętrznego



Źródło: *Raport z działalności Agencji Bezpieczeństwa Wewnętrznego w 2009 r.*, Wyd. Agencja Bezpieczeństwa Wewnętrznego, Warszawa 2010, s. 10.

Nowym obszarem wyzwań w dziedzinie bezpieczeństwa dla państwa stała się cyberprzestrzeń i płynące z niej zagrożenia dla infrastruktury krytycznej państwa, która w znacznym stopniu jest oparta na nowych technologiach informatycznych i informacyjnych, przy czym znaczna część tej infrastruktury znajduje się w dyspozycji podmiotów pozapaństwowych[19]. Wynika stąd potrzeba współpracy instytucji państwa i podmiotów gospodarczych mu niepodlegających w zakresie ochrony cyberprzestrzeni RP.

Taka jest geneza dwóch rządowych programów: ochrony cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2009-2011 oraz jego kontynuacji w latach 2011-2016, w których ukazano główne cele strategiczne i szczegółowe oraz adresatów programów. Programy dotyczą działań podejmowanych w czterech obszarach, a mianowicie: legislacyjnym, proceduralno-organizacyjnym, edukacyjnym i technicznym. Dzięki nim świadomość obywateli związana z bezpieczeństwem cybernetycznym państwa jest ciągle rozwijana. Również firmy poszerzają specjalistyczną wiedzę i i usprawniają systemy zabezpieczeń.

Podejście państwa polskiego do ochrony cyberprzestrzeni wypada uznać za zasadne. Natomiast można by się zastanowić nad potrzebą rozszerzenie ochrony również poza obszar terytorium Polski – nie tylko dla jednostek państwa, ale także dla podmiotów prywatnych. Zakres ochrony mógłby obejmować firmy,

19 T. R. Aleksandrowicz, K. Liedel, *Społeczeństwo informacyjne – sieć – cyberprzestrzeń. Nowe zagrożenia*, [w:] *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, red. K. Liedel, P. Piasecka, T. R. Aleksandrowicz, Wyd. Difin, Warszawa 2014, s. 11.

zarejestrowane w Polsce, ale część ich systemów teleinformatycznych ze względu na otworzoną w innym państwie filię firmy lub inny podmiot prywatny pracuje w cyberprzestrzeni innego państwa.

Ustanowiony system trójpoziomowego reagowania na incydenty komputerowe w cyberprzestrzeni zapewnia szybką wymianę informacji pomiędzy zespołami CERT administracji publicznej, militarnej oraz sektora prywatnego (CERT Polska, CERT ORANGE Polska, PIONIERCERT).

Przyjęta polityka zakłada współpracę z przedsiębiorcami z sektorów zaopatrzenia w energię, łączności, sieci teleinformatycznych, finansów i transportu, którzy posiadają własną infrastrukturę o podobnym charakterze jak infrastruktura teleinformatyczna cyberprzestrzeni Rzeczpospolitej Polskiej lub się do niej zalicza i jest narażona na różnego rodzaju podobne metody ataków. Współpraca z przedsiębiorcami zapewnia możliwość powoływania zespołów do wewnętrznej ochrony infrastruktury firmy, jak również do wymiany informacji i doświadczeń w zakresie bezpieczeństwa z zespołami CERT administracji publicznej[20]. Również w zakresie zagrożeń płynących z cyberprzestrzeni, do czego zostały powołane w strukturach ABW i SKW już scharakteryzowane zespoły CERT.GOV.PL i MIL-CERT. Koordynują one współpracę poszczególnych zespołów CERT w poszczególnych ministerstwach i jednostkach administracji rządowej, jak również w firmach prywatnych, z którymi współdziałanie na płaszczyźnie monitorowania, diagnozowania i reagowania na różnego rodzaju incydenty w cyberprzestrzeni.

Podsumowując rozważania o instytucjonalnych formach ochrony informacji przed wywiadem biznesowym w polskiej cyberprzestrzeni pragniemy podkreślić wiodącą i organizatorską rolę państwa w ochronie przedsiębiorstw przed zagrożeniami wywiadowczymi z zewnątrz państwa, nie tylko ze strony innych państw, ale także ze strony korporacji międzynarodowych, dużych firm oraz grup przestępczych, które to zagrożenia należy rozpatrywać w kontekście ekonomicznym, społecznym, politycznym i zjawisk globalizacji. Dlatego państwo i jego instytucje muszą prowadzić uniwersalne (multidyscyplinarne) działania ochronne przed wywiadem biznesowym, we wszystkich sferach, działach, gałęziach i branżach funkcjonowania państwa.

Podstawą ochrony przed wywiadem biznesowym w polskiej cyberprzestrzeni jest prawo krajowe oraz normy prawa międzynarodowego. Jeżeli te dwa elementy ze sobą nie współgrają oraz nie mają jednakowych celów i rozwiązań prawnych w postaci definicji, zakazów, norm prawnych i sankcji karnych, to cały aparat bezpieczeństwa państwa nie będzie w stanie sprostać wyzwaniu ochrony tajemnicy przedsiębiorstw przed wywiadem i szpiegostwem. Dlatego tak bardzo konieczna i zasadna wydaje się praca nad doskonaleniem istniejących rozwiązań prawnych, które znacznie wyprzedzą postęp technologiczny i tym samym mogą przyczynić się do skuteczniejszego przeciwdziałania cyberwywiadowi i wzmocnić ochronę tajemnic przedsiębiorstw w warunkach współczesnych, przy czym

20 Tamże, s.19.

należy mieć na uwadze procesy globalizacji, ale także integracji w ramach Unii Europejskiej. Analiza treści ustaw dowodzi szerokiego zakresu działań instrumentów bezpieczeństwa państwa w kwestii ochrony przed wywiadem państwowym i niepaństwowym.

Nasz zespół wyciągnął z badań wniosek, że tworzony przez państwo i egzekwowany przez jego instytucje racjonalny system prawa zabezpieczającego tajemnice przedsiębiorstw przed wywiadem i szpiegostwem stanowi pierwszą linię obrony.

Funkcjonujący w Polsce system rozwiązań prawnych jest uważany przez międzynarodowych ekspertów za wartościowy i adekwatny do aktualnych zagrożeń. Jednak skala przestępstw godzących w tajemnice przedsiębiorstw budzi niepokój i świadczy, że występuje potrzeba poszukiwania nowych rozwiązań.

W minionych latach nacisk w programach rządowych kładziono na edukację w dziedzinie bezpieczeństwa cybernetycznego. Może dobrym rozwiązaniem byłoby zacieśnienie współpracy zespołów CERT.GOV.PL z innymi podmiotami – nieobjętymi dotąd strukturami monitorowania cyberprzestrzeni. Rozwój tych zespołów może w przyszłości przynieść korzyści, ponieważ zwiększy prawdopodobieństwo wykrycia groźnych incydentów – nie tylko w administracji publicznej, ale również w podmiotach prywatnych, także w gospodarczych. Tym samym pozwoli na uniknięcie dużych strat związanych z nieuprawnionym dostępem do informacji prawnie chronionych i stanowiących tajemnicę przedsiębiorstwa.

Informacja jest współcześnie czymś bardzo ważnym i może posiadać określoną (niekiedy nawet bardzo dużą) cenę, więc i ochrona jej niestety jest skomplikowana i kosztowna, ponieważ większość chroniących ją zabezpieczeń trzeba czasami dublować, organizując np. programy ochronne i monitorujące informatyczną sieć wewnętrzną i zewnętrzną, zabezpieczenia fizyczne w postaci ochrony fizycznej oraz kontroli dostępu na drzwiach czy czytnikach kart w komputerach, a także odpowiednie procedury bezpieczeństwa w postaci zmiany haseł dostępu czy szyfrowanie dysków z ważnymi informacjami. Tego rodzaju przedsięwzięcia będą przedmiotem rozważań w dalszej części artykułu. Natomiast nie mniej ważnym elementem ochrony tajemnic jest sama polityka bezpieczeństwa informatycznego przedsiębiorstwa, która jest pewnego rodzaju drugą linią obrony przed zagrożeniami wywiadowczymi i cybernetycznymi w nowoczesnej firmie.

Warto również zwrócić uwagę na fakt, że jeżeli pracownicy firmy nie dbają o bezpieczeństwo, to pomimo najlepszych rozwiązań prawnych i działań państwowych instytucji bezpieczeństwa z wysoko wyspecjalizowanym aparatem monitorującym i zwalczającym zagrożenia, przedsiębiorstwo same naraża siebie na zagrożenie wywiadowcze i przestępcze. Dlatego koniecznym i zasadnym wydaje się samodzielne wdrażanie własnych rozwiązań bezpieczeństwa w firmach, równolegle i niezależnie od działań podejmowanych przez państwo, z eliminacją negatywnych zachowań pracowników i ich niechęci do utrudniania sobie pracy.

4. Przeciwdziałanie wywiadowi gospodarczemu przez przedsiębiorstwo. Doświadczenia i wnioski

W badaniach staraliśmy się zidentyfikować struktury i wyjaśnić, w jaki sposób przeciwdziałają zagrożeniu przedsiębiorstwa cyberwywiadem biznesowym.

Dążyliśmy do ustalenia wymaganych procedur ochrony i bezpieczeństwa informacji oraz scharakteryzowania odpowiednich struktur komórek zajmujących się ochroną przedsiębiorstwa. Niezbędna była również identyfikacja metod ochrony, które można podzielić na ochronę fizyczną i stosowanie technicznych środków zabezpieczenia, jak również konieczność wykonania audytu bezpieczeństwa, który pomaga weryfikować możliwe niebezpieczeństwa oraz wykrywać luki i błędy w systemie ochrony informacji firmy.

Nasze poszukiwania koncentrowały się na funkcjonowaniu ochrony w dużych firmach oraz w korporacjach międzynarodowych, ponieważ w ich strukturach występują zazwyczaj duże piony ochrony, które wdrażają wypracowaną politykę ochrony firmy.

Średnich i małych firm nie stać na rozbudowę drogich systemów zabezpieczeń, zatem powierzchowna jest ich ochrona i współpraca z wyspecjalizowanymi organami państwa. Przeważnie ograniczają się do prostych zabezpieczeń administracyjnych, fizycznych i elektronicznych w zakresie sieci komputerowych i baz danych.

Naszą uwagę zwrócił pogląd P. Tomaszewskiego, że te małe i średnie firmy nie mają dużej świadomości zagrożeń oraz potrzeby ochrony, i bagatelizują problem. Dlatego państwo powinno podejmować właściwe działania profilaktyczne, szczególnie wobec małych firm uczestniczących w produkcji związanej z wysoko rozwiniętą technologią[21].

Struktury ochrony przedsiębiorstwa są ściśle powiązane z jego zakresem działania i specyfiką. Pion ochrony zawsze podporządkowany jest kierownictwu firmy. W małych firmavh zazwyczaj ochrona fizyczna jest wynajęta. Zarządza nią inspektor ochrony, który podlega właścicielowi firmy i informuje go o zagrożeniach, nieprawidłowościach, możliwych sposobach przeciwdziałania. Taka prosta struktura przynosi wiele korzyści, ale niestety – w przypadku firmy dużej, a do tego działającej w cyberprzestrzeni – jest niewystarczająca. W firmach dużych, w korporacjach i organizacjach, występuje pion ochrony z szefem bezpieczeństwa firmy, do którego spływają informacje z podległych oddziałów i od lokalnych inspektorów ochrony, a dodatkowo jeszcze od Administratorów Bezpieczeństwa Informacji (rys. 1 i 2).

Jak wspomniałem, struktura ochrony wynika ze zdefiniowanych przez przedsiębiorstwo potrzeb bezpieczeństwa i wiąże się z koniecznością opracowania odpowiedniej polityki bezpieczeństwa[22].

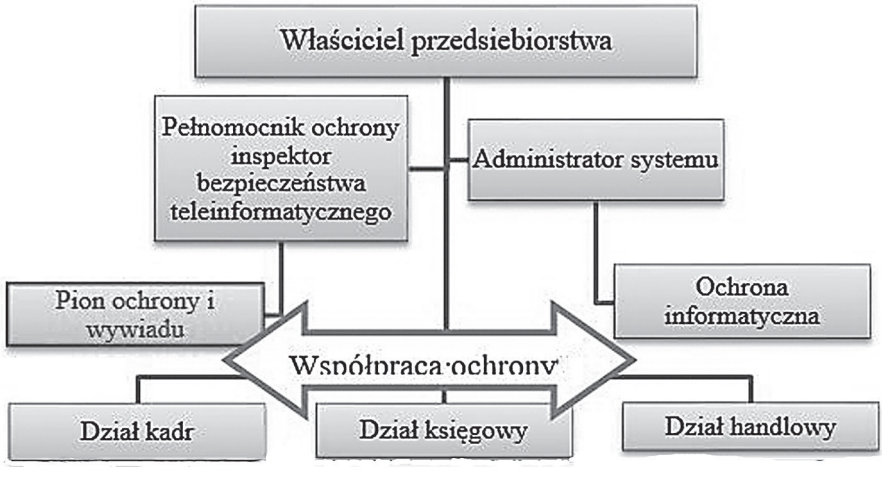
21 Tamże.

22 http://www.log24.pl/artykuly/na-strazy-bezpieczenstwa,432, (11.05.2017).

Rysunek 2. Przykładowa struktura ochrony pionu bezpieczeństwa – wg ustawy o ochronie informacji niejawnych (z umiejscowieniem pionu wywiadu w przedsiebiorstwie)

Źródło: opracowanie własne na podstawie . http://www.zegarbiznesu.pl/wiedza_dla_biznesu/ praktyczne_poradniki_card.xhtml?usecaseid=110, (15.05.2017)

Rysunek 3. Przykładowa struktura ochrony pionu bezpieczeństwa – wg ustawy o ochronie danych osobowych (z umiejscowieniem pionu wywiadu w przedsiębiorstwie)



Źródło: opracowanie własne na podstawie http://www.zegarbiznesu.pl/wiedza_dla_biznesu/ praktyczne_poradniki_card.xhtml?usecaseid=110, (05.06.2015).

Na rys. 4 przedstawiono ustalone w badaniach zasadnicze etapy procesu opracowania i wdrożenia polityki bezpieczeństwa w przedsiębiorstwie ustalone i scharakteryzowane w literaturze.

Rysunek 4. Proces opracowania i wdrożenia polityki bezpieczeństwa w przedsiębiorstwie

Źródło: opracowanie własne na podstawie http://www.zegarbiznesu.pl/wiedza_dla_biznesu/praktyczne_ poradniki_card.xhtml?usecaseid=110, (11.05.2017).

W zależności od skali, rodzaju i charakteru posiadanych informacji w przedsiębiorstwie stosuje się odpowiednie zasady i procedury ochrony, określone w stosownych dokumentach. Jeżeli w przedsiębiorstwie są przechowywane dokumenty o charakterze niejawnym, to pełniący obowiązki pełnomocnik ochrony powinien stworzyć dokument „Plan ochrony informacji niejawnych" – zgodnie z wymaganiami, które narzuca ustawa o ochronie informacji niejawnych. Jeżeli przedsiębiorstwo posiada w swoich zbiorach informacje mające charakter danych osobowych, powinno zastosować się do wymogów i przepisów określonych w ustawie o ochronie danych osobowych oraz do odpowiednich rozporządzeń dotyczących wykonania regulacji zawartych w ustawie. Wskazana ustawa stanowi o konieczności sprecyzowania środków ochrony danych osobowych

i odpowiedniej ochronie systemów teleinformatycznych, w którym takie dane są gromadzone.

Zatem przedsiębiorca chcąc chronić tajemnice firmy powinien stworzyć odpowiedni dokument zwany polityką bezpieczeństwa, w którym będą uregulowane odpowiednie procedury związane z ochroną danych osobowych, dokumentów (tajemnic przedsiębiorstwa) i praw autorskich[23].

Dokument formułujący politykę bezpieczeństwa zawiera elementy ochrony zewnętrznej, wewnętrznej i szyfrowania informacji[24], a jego treść określa procedury bezpieczeństwa dla całego przedsiębiorstwa. Należą do nich:

1) informacje ogólne – powinny zawierać ogólny charakter polityki związany z bezpieczeństwem informacji;
2) administracja i organizacja bezpieczeństwa – kto sprawuje ochronę i jak wygląda jej struktura (zadania);
3) bezpieczeństwo osobowe – procedury ochrony związane z pracownikami;
4) bezpieczeństwo fizyczne – elementy ochrony obiektu i zabezpieczeń technicznych obiektu (procedury)
5) bezpieczeństwo dokumentu – obieg dokumentów, nadanie klauzuli i sposoby ich ochrony;
6) bezpieczeństwo sprzętu i oprogramowania – procedury związane z wgrywaniem oprogramowania i użytkowaniem firmowego sprzętu (np.: zakaz podłączania sprzętu niefirmowego, możliwość wgrywania oprogramowania tylko z pozycji administratora systemu);
7) bezpieczeństwo łączności – połączenia szyfrowane, wewnętrzna sieć połączeniowa (Intranet), ochrona elektromagnetyczna i transmisji danych;
8) monitorowanie bezpieczeństwa i kontrolowanie – obserwacja przez administratora sieci ruchu sieci za pomocą oprogramowania typu IPS lub IDS;
9) konserwacja i naprawy – odpowiedni serwis mogący naprawić, odzyskać dane z nośników czy też je definitywnie zniszczyć bez możliwości odzyskania danych;
10) plany awaryjne i zapobiegawcze – sposoby odzyskiwania utraconych danych, sprzętu lub na wypadek innych zagrożeń podczas użytkowania (pożar, przegrzanie serwerów, zalanie serwerowni, zanik napięcia)
11) polityka antywirusowa – odpowiednie zabezpieczenia, które chronią przed zagrożeniami zewnątrz sieci i podsłuchami[25].

Wszystkie procedury bezpieczeństwa powinny opierać się na czterech podsta-

23 A. Hernas, *Bezpieczeństwo informacji, bezpieczeństwo teleinformatyczne i polityka bezpieczeństwa – trzy wymiary ochrony informacji i danych osobowych,* [w] *Bezpieczeństwo informacji i biznesu. Zagadnienia wybrane,* red. M. Kwieciński, Wyd. Krakowskie Towarzystwo Edukacyjne, Kraków 2010, s. 15.

24 A. Żebrowski, *Bezpieczeństwo wiedzy – nowy atrybut działalności przedsiębiorstwa,* [w:] *Informacja i wiedza w zintegrowanym systemie zarządzania*, red. R.Borowiecki, M. Kwieciński, Wyd. Zakamycze, Kraków 2004, s. 439.

25 A. Żebrowski, *Bezpieczeństwo wiedzy – nowy…*, s. 443.

wowych filarach bezpieczeństwa, którymi są:

1) właściwe osoby, które dadzą rękojmię zachowania tajemnicy przedsiębiorstwa;
2) właściwe zabezpieczenia fizyczne, które mogą uchronić od włamania i nieautoryzowanego dostępu do informacji;
3) właściwa organizacja, która polega na odpowiednim obiegu informacji w przedsiębiorstwie;
4) właściwe zabezpieczenia teleinformatyczne, które mogą uchronić przed inwigilacją z cyberprzestrzeni[26].

Wdrożenie w przedsiębiorstwie odpowiednich dokumentów opisujących kształt systemu bezpieczeństwa jest tylko pierwszym etapem w tworzeniu systemu bezpieczeństwa informacyjnego, do którego zalicza się dwa przedsięwzięcia:

1) wprowadzenie do użytku odpowiedniego dokumentu opisującego politykę bezpieczeństwa oraz procedury jemu towarzyszące;
2) przeprowadzenie odpowiednich serii szkoleń personelu przedsiębiorstwa (na podstawie polityki bezpieczeństwa) – wykształcenie świadomości kierownictwa i personelu firmy pod kątem kluczowych elementów ochrony i bezpieczeństwa informacji[27].

Ważnym ogniwem ochrony informacji w firmie jest ochrona fizyczna, gdyż nawet mimo najlepszych systemów teleinformatycznych może znaleźć się przestępca, który zdoła wejść do pomieszczeń niechronionych i wykraść nośniki danych w postaci papierowej lub elektronicznej. Ochrona fizyczna jest w przedsiębiorstwie „przednim skrajem linii ochrony informacji", a jej głównym celem – zgodnie z normą *ISO/IEC 27002 (wcześniej: ISO/IEC 17799), wersja polska: PN-ISO/IEC 27002:2014-12* – jest *„zapobieganie nieuprawnionemu dostępowi, uszkodzeniom i ingerencji w pomieszczenia instytucji i jej informacje"*[28].

System ochrony fizycznej przedsiębiorstwa powinien obejmować następujące elementy:

1) odpowiednią organizację – zasady, sposób i dobór środków ochrony (realizowanej przez wynajętą firmę zewnętrzną lub własną formację ochronną przedsiębiorstwa);
2) mechaniczno-budowlane – urządzenia (systemy) ochrony (SKD, CCTV, SWiN, dyspozytora kluczy, instalację wideofonową – domofonową, system ppoż. — m.in. oddymiania oraz inne systemy);
3) elektroniczne systemy sygnalizacji zagrożeń – centrum monitoringu ochrony fizycznej, podgląd kamer i sygnalizację wykorzystującą różne czujniki (sensory);
4) osobowe środki ochrony – pracowników ochrony odpowiedzialnych za stały nadzór nad systemami ochrony i dostępu (raportowanie, monitorowanie)[29].

26 http://nf.pl/manager/informacja-8211-strategiczny-zasob-przedsiebiorstwa,,7954,276, (12.05. 2017).
27 K. Liderman, *Bezpieczeństwo informacyjne,* Wyd. PWN, Warszawa 2010, s. 127.
28 http://ochronainformacji.pl/index.php?option=com_content&view=article&id=18:ochrona-fizyczna-zasobow-it&catid=10: bezpieczestwo-w-it&Itemid=12, (12.05.2017).
29 http://ochronainformacji.pl/index.php?option=com_content&view=article&id=18:ochrona-

System ochrony fizycznej przedsiębiorstwa powinien spełniać następujące wymogi: efektywności (koszt zabezpieczeń powinien być adekwatny do kosztów ochrony), racjonalności (system jest akceptowany przez użytkownika), kompleksowości (wzajemnie uzupełniające się rodzaje i metody ochrony: organizacyjne; zabezpieczenia – budowlane, mechaniczne, elektroniczne; prawne; ochrona fizyczna).

Niestety, najsłabszym ogniwem we wszystkich systemach ochrony jest nadal czynnik ludzki i należy pamiętać o tym na etapie projektowania, rekrutacji i zatrudnienia pracowników firmy. Dobrym rozwiązaniem w polepszaniu bezpieczeństwa są częste niezapowiedziane kontrole ochrony, jak i audyty bezpieczeństwa, które kompleksowo badają na rozwiązania zabezpieczeń i aktualny stan systemów firmy.

Podsumowanie

Przedsiębiorstwo w warunkach globalizacji gospodarek i rynku konkurencyjnego zostało niejako rzucone na głęboką wodę i wyjęte spod ochrony państwa przed nieprzyjaznymi działaniami wywiadowczymi. Jedynie niektóre przedsiębiorstwa cieszą się pełną ochroną państwa przed działaniami wywiadowczymi ze strony obcych podmiotów, a spowodowane to jest istotnymi interesami państwa o znaczeniu gospodarczym, finansowym, militarnym i naukowym, m.in. w gałęziach energetycznej i transportu.

Państwo sprawuje z mocy prawa ochronę przedsiębiorstw przed wywiadem oraz szpiegostwem poprzez odpowiednie instytucje, które są zobowiązane do monitorowania, wykrywania i przeciwdziałania zagrożeniom o charakterze szpiegowskim, wywiadowczym, terrorystycznym i przestępczym – związanych z kradzieżą i niszczeniem wszelkich danych. W obliczu nowych zagrożeń przedsiębiorstwa, niestety, muszą radzić sobie same i są zmuszone do tworzenia odpowiednich systemów i struktur ochrony, zgodnie z rozwiązaniami prawa krajowego. Muszą inwestować w odpowiednie systemy zabezpieczeń, które czasami są droższe niż informacje, jakie firma chce chronić.

Dlatego w określonych uwarunkowaniach warto zainwestować w pomoc dobrych wywiadowców, którzy przy użyciu legalnych źródeł są w stanie przewidzieć posunięcia konkurentów firmy i tym samym przeciwdziałać ich poczynaniom, neutralizować działania konkurencji.

Zasadne jest tworzenie odpowiednich struktur ochronnych, których zadaniem jest szkolenie pracowników w kwestiach dotyczących wywiadu i kontrwywiadu, ochrony oraz analizy informacji i jej dystrybucji. Działania prewencyjne traktowane na początku nawet jako zbędne, w przyszłości mogą okazać się prorocze i korzystne.

Stworzenie idealnego systemu ochrony połączonego z systemem *Business Inteligence* (BIGDATA) przedsiębiorstwa jest przedsięwzięciem bardzo trudnym bo

fizyczna-zasobow-it&catid=10: bezpieczestwo-w-it&Itemid=12, (12.05.2017)

– jak pokazują doświadczenia – zazwyczaj udaje się to jedynie 15% firm, w których taki system był wdrażany, w 70% przypadków kończy się fiaskiem już na starcie, a kolejne 15% inicjatyw przestaje funkcjonować po roku działalności[30].

Dlatego ważna jest racjonalna identyfikacja potrzeb ochrony i rozwiązań wspomagających działalność biznesową w przedsiębiorstwach opartych na wiedzy i rozwiązaniach IT, które obecnie przynoszą duże zyski, a tempo ich rozwoju wynosi około 5% rocznie. Nie dziwi więc że ostro konkurują, a ochrona ukrywanych w tajemnicy ich aktywów stanowi prawdziwe wyzwanie[31].

Artur Kryst*

30 http://it-manager.pl/nowa-twarz-business-intelligence/, (12.05.2017).
31 Tamże.

***Artur Kryst, student Wszechnicy Polskiej Szkoły Wyższej w Warszawie**

Michał Kurzaj

Zagrożenia wynikające z użytkowania i utraty mobilnych urządzeń komunikacyjnych, czyli „technologia w cuglach”

Wstęp

Prezentowane opracowanie dotyczy problemu zagrożeń powiązanych z użytkowaniem mobilnych urządzeń komunikacyjnych, a przede wszystkim utraty danych zawartych w tych urządzeniach. Szczególny nacisk położono na problematykę techniczną tego zagadnienia. Przedstawiono też metodykę pozyskania danych ze smartfonów oraz wskazano czas, jaki potrzebny jest do uzyskania danych, w tym także danych systemowo czy aplikacyjnie ukrytych.

Przykładem w tej kwestii może być MK MY DATA, która jest profesjonalną firmą zajmującą się, między innymi, odzyskiwaniem i dogłębną analizą utraconych danych, oferującą swe usługi zarówno osobom prywatnym, jak również firmom. Wieloletnie doświadczenie wykwalifikowanego personelu oraz dysponowanie najnowocześniejszym zapleczem technicznym pozwala twierdzić, iż jest to jedna z najbardziej doświadczonych i profesjonalnych firm działających na polskim rynku, zajmująca się przedmiotowymi zagadnieniami. Należy nadmienić, iż personel firmy legitymuje się uprawnieniami do sporządzania opinii na potrzeby służb oraz sądów, a także pełni funkcję biegłego sądowego przy Sądzie Okręgowym w Warszawie w dziedzinie informatyki.

Znacząca część komunikacji prowadzonej między osobami, zarówno na płaszczyźnie prywatnej, jak i służbowej, odbywa się dziś poprzez użytkowanie smartfonów, a wymiana istotnych informacji biznesowych, w tym również dotyczących szeroko rozumianego bezpieczeństwa, odbywa się z wykorzystywaniem mobilnych urządzeń komunikacyjnych, niezwykle istotnym zatem jest poddanie analizie metod pozyskiwania danych zawartych w tych urządzeniach.

Dzisiejsze czasy to era globalnej cyfryzacji. Prawie każdy z nas jest posiadaczem urządzenia mobilnego, czy to w postaci telefonu komórkowego, tabletu, czy smartwatcha. Za pomocą tych urządzeń wymieniamy pomiędzy sobą informacje, począwszy od tych mało istotnych, zabawnych, osobistych, kończąc na treściach dotyczących naszej pracy, życia zawodowego, finansów, zdrowia czy tajemnic służbowych. Telefon jest naszym biurem, placem zabaw, oknem na świat, nadzorujemy nim nasze finanse i bankowość, komunikujemy się ze

znajomymi lub współpracownikami zarówno głosowo jak również przez pisanie wiadomości tekstowych czy korespondencję mailową. Urządzenia mobilne towarzyszą nam często przez całą dobę, nosimy je przy sobie, przenosząc w nich ogrom informacji. Informacji, o gromadzeniu których przez użytkowane przez nas urządzenia nie zawsze jesteśmy świadomi. Mało kto zdaje sobie sprawę, że systemy operacyjne i aplikacje mieszczące się w naszym sprzęcie, zbierają i przechowują mnóstwo informacji na nasz temat, na temat naszego stylu życia, upodobań czy preferencji. W wielu przypadkach zainstalowane na urządzeniu aplikacje wysyłają mnóstwo prywatnych treści na serwery w sieci i tak naprawdę nie wiadomo co się z nimi dzieje, kto ma do nich dostęp i jak są wykorzystywane.

W niniejszym opracowaniu naświetlimy niebezpieczeństwa wynikające z fizycznej utraty kontroli nad urządzeniami mobilnymi. Omówimy zakres i rodzaje danych, jakie magazynują nasze urządzenia. Przybliżymy w sposób przystępny i klarowny jakimi sposobami osoby trzecie mogą przejąć nasze dane oraz informacje magazynowane w naszym sprzęcie oraz w jaki sposób mogą je wykorzystać. Na przykładzie kilkunastu modeli telefonów komórkowych oraz tabletów pokażemy, jakie informacje można ekstrahować z takich urządzeń. Pokażemy także, że w wielu przypadkach standardowe zabezpieczenie, w postaci szyfrowania telefonu, zabezpieczenia go blokadą w formie pinu, tzw. „wzorku", czy też odcisku palca, nie jest do końca bezpieczne i nie chroni nas w stu procentach przed wyciekiem naszych prywatnych informacji. Przedstawimy w jaki sposób należy się zabezpieczyć dodatkowo, by podnieść poziom bezpieczeństwa swoich danych. Omówimy najpopularniejsze aplikacje, tzw. komunikatory i udowodnimy, że nie wszystkie są tak bezpieczne, jak nam się do tej pory zdawało. Omówimy rodzaje szyfrowania stosowane w komunikatorach, jak również wskażemy te komunikatory, którym, naszym zdaniem, można powierzyć swoją prywatność, bo gwarantują najwyższy poziom bezpieczeństwa. W tym miejscu należy podkreślić, że w obecnym czasie najbezpieczniejszym medium do wymiany korespondencji są komunikatory, które oferują szyfrowanie, przez co w niektórych przypadkach potrafią zapewnić praktycznie całkowicie naszą anonimowość. Oczywiście przy zachowaniu z naszej strony zasad tzw. bhp pracy z urządzeniami mobilnymi.

Warto również zwrócić uwagę na kilka aktualnie stosowanych rozwiązań kryptograficznych służących do zabezpieczania danych w tzw. kontenerach, czy sejfach, które uważane są za najsilniejszy środek zapobiegawczy, dający gwarancję możliwie najwyższego poziomu bezpieczeństwa.

Utrata fizyczna urządzenia mobilnego

Szczególnie niebezpiecznym rodzajem wycieku naszych prywatnych danych jest fizyczna utrata urządzenia lub brak kontroli czasowej nad nim. Jest to najbardziej popularny przypadek wycieku naszych poufnych danych, w wyniku którego osoby niepowołane mogą uzyskać najwięcej istotnych informacji na temat naszego życia prywatnego i zawodowego.

Często oprócz widocznych danych takich jak treści rozmów, poczty, czy multimediów osoby trzecie mają możliwość wykonania kopii binarnej kości pamięci, a co za tym idzie dostają możliwość odzyskania skasowanych wcześniej przez użytkownika treści.

Występujące najczęściej rodzaje utraty urządzenia czy braku kontroli nad nim to:

- kradzież urządzenia,
- zagubienie,
- wyrzucenie urządzenia po wyeksploatowaniu lub urządzenia niesprawnego,
- oddanie do serwisu,
- pozostawienie bez nadzoru, np. w miejscu pracy czy w lokalu.

W takich przypadkach zastosowane zabezpieczenie lub zaszyfrowanie urządzenia nie będzie stanowiło dostatecznej blokady dostępu do danych i bez większych problemów nastąpi rozszyfrowanie lub złamanie blokady dostępu do nich. Osoby niepowołane będą dysponować dostateczną ilością czasu na to, by „popracować" z konkretnym modelem urządzenia i wydobyć z niego jak najwięcej istotnych informacji .

Częstymi przypadkami nieautoryzowanego uzyskania danych przez osoby trzecie są kontakty w serwisach telefonów komórkowych. To tam nierzadko osoby niepowołane uzyskują dostęp do naszych danych.

Zajmujemy się sposobami zminimalizowania tego rodzaju niebezpieczeństwa, a nawet wyeliminowania go w możliwie najlepszy sposób.

Wyrzucenie do śmieci urządzenia, w przekonaniu, że nie stanowi wartości, bo jest zepsute, martwe i bezużyteczne, a jego utrata nie stanowi już zagrożenia często okazuje się złudne, gdyż dla osób, których celem jest pozyskać dotyczące nas poufne informacje może to być jedna z najlepszych okazji, aby uzyskać dostęp do naszych prywatnych lub służbowych danych. Osoby mające zlecenie na tzw. „profilowanie" naszej osoby będą nas pilnować w celu wygenerowania sprzyjającej okazji na pozyskanie naszego sprzętu. A w wielu przypadkach nasz śmietnik stanowić będzie miejsce służące budowie naszego pokaźnego portfolio. Warto pamiętać, że jeżeli zamierzamy wyrzucić nasze wyeksploatowane urządzenie to uprzednio należy je zniszczyć mechanicznie, w taki sposób, by zniszczyć zawarty w nim chip pamięci. Oczywiście nie każdy dysponuje wiedzą techniczną i umiejętnościami manualnymi pozwalającymi na permanentne zniszczenie takiego urządzenia. Istnieją jednakże znacznie prostsze i równie skuteczne sposoby, o których wspomnimy w dalszej części przedmiotowego opracowania.

Po co komu nasze dane?

Jako użytkownicy urządzeń mobilnych często w swoich aparatach przechowujemy mnóstwo służbowych i prywatnych informacji. Będą to między innymi nasze kontakty, wiadomości, smsy i mms wymieniane ze znajomymi, współpracownikami czy przyjaciółmi. Będzie to korespondencja z komunikatorów na tematy prywatne i służbowe. Będą to także nasze prywatne zdjęcia, notatki i wpisy w kalendarzu, wszelkiego rodzaju informacje w formie multimedialnej, korespondencja pocztowa itp.

Wszystkie te informacje mogą posłużyć osobom trzecim i być przez nie bardzo skutecznie wykorzystane. Prywatne treści mogą posłużyć do szantażowania nas, do wywarcia na nas presji lub przymuszenia nas do zmiany powziętych wcześniej decyzji w wielu różnych dziedzinach. Informacje prywatne dotyczące naszych haseł, adresów portfeli, kont bankowych mogą w prosty sposób przyczynić się do uszczuplenia naszego zasobu finansowego, wyczyszczenia portfela elektronicznego lub konta bankowego.

Często zdjęcia naszych czy służbowych dokumentów oraz skany przechowywane są w sposób niezabezpieczony w pamięci urządzenia, po prostu w galerii wraz z innymi zdjęciami. Taka niefrasobliwość może skutkować pobraniem pożyczki czy kredytu z wykorzystaniem naszych danych osobowych. W tym miejscu należy podkreślić, że w dzisiejszych czasach nie jest problemem założenie przez Internet konta bankowego z wykorzystaniem danych skradzionych z naszego urządzenia, często wystarczy adres mailowy, czy dane z dostępnych dokumentów i można bez problemu pobrać, np. tzw. „chwilówkę" lub spowodować, że staniemy się twz. słupem w olbrzymich transakcjach finansowych przechodzących przez nasze „nowe konto", oczywiście bez naszej wiedzy.

Kolejnym istotnym aspektem jest wykorzystanie danych z naszego urządzenia mobilnego do przeprowadzenia ataku na strukturę teleinformacyjną firmy lub placówki, w której pracujemy lub piastujemy ważną funkcję. W naszych telefonach, tabletach, przechowujemy bezwiednie wiele informacji, które mogą stworzyć olbrzymie możliwości cyberprzestępcy. Zdarza się, że w telefonach zapisujemy hasła do sieci WiFi firmy lub placówki, w której pracujemy. Przechowujemy maile służbowe i informacje służbowe, które mogą pomóc przestępcy w zbudowaniu fałszywych adresów internetowych, stron WWW, które mogą posłużyć do ataku socjotechnicznego na pracowników firmy i umożliwią przełamanie jej zabezpieczeń teleinformatycznych. Informacje z naszego urządzenia mogą pomóc przestępcy poznać strukturę działania naszej firmy, ustalić panującą w niej hierarchię oraz rozkład dnia pracowników itp. Wszystkie te informacje mogą przyczynić się bezpośrednio do udanego ataku na placówkę, w której pracujemy, a co za tym idzie umożliwić pozyskanie dostępu do jej poufnych informacji biznesowych objętych tajemnicą państwową, a także dać możliwość wyrządzenia szkód na tle finansowym, wizerunkowym lub ekonomicznym.

Pozyskanie dostępu do korespondencji, która znajduje się w użytkowanych przez nas darmowych komunikatorach zainstalowanych w naszym urządzeniu, również nie stanowi dużego problemu dla cyberprzestępcy. To właśnie w tego rodzaju korespondencji pozwalamy sobie na wiele więcej swobody niż przy korzystaniu z poczty elektronicznej czy sms-ów. Korzystając z popularnych i darmowych komunikatorów mamy poczucie wysokiego bezpieczeństwa.

Dane przechowywane na urządzeniach mobilnych

Poniżej wymienione zostały najbardziej popularne informacje magazynowane przez nasze smartfony i tablety oraz inne urządzenia mobilne. Są to:

- kontakty,
- historia połączeń i aktywności użytkownika,
- notatki,
- zdjęcia,
- wiadomości sms i mms,
- korespondencje z komunikatorów,
- poczta elektroniczna,
- pozycje GPS, stacje BTS,
- hasła,
- sieci WiFi,
- dokumenty, publikacje, prezentacje,
- nagrania głosowe czy obrazowe,
- wszelkie zdefiniowane aplikacje z dostępem do danych w sieci czy np. monitoringu domu, firmy, mieszkania.

Warto zaznaczyć, że wymieniono tu tylko te najbardziej popularne i istotne informacje, jakie potencjalny cyberprzestępca może pozyskać z naszego urządzenia. Całość tych danych odpowiednio przeanalizowana i usystematyzowana może dać ogromną wiedzę osobom, które przejęły nasze urządzenie. Wiedza ta może być wykorzystana w celu popełnienia wielu przestępstw i nadużyć, jak również posłużyć do ośmieszenia nas lub zdyskredytowania w oczach znajomych, współpracowników, wspólników lub społeczeństwa.

Rodzaje ingerencji w urzadzenia mobilne

Ingerencję w urządzenia mobilne podzielić można na dwa następujące sposoby: ingerencję inwazyjną oraz ingerencjaę bezinwazyjną.

Na rynku dostępnych jest kilka rozwiązań hardwerowo – *Software-wych, w tym: UFED, Xray, Oxygen Forensic oraz Mobileedit.*

Rozwiązania te wykorzystywane są do ekstrakcji danych z urządzeń mobilnych. Używa się ich najczęściej do bezinwazyjnej ekstrakcji pamięci urządzenia. Z ich pomocą można również przeanalizować i ekstrahować obrazy pamięci, które wykonane są metodami inwazyjnymi.

Metody bezinwazyjne pozyskiwania danych

Z bezinwazyjną metodą ekstrakcji pamięci urządzenia mamy do czynienia wówczas, gdy nie rozkładamy i nie rozbieramy oraz nie modyfikujemy urządzenia od strony jego elektroniki, a jedyne czynności wykonywane z urządzeniem to podłączenie go do komputera z oprogramowaniem lub specjalnego urządzenia przenośnego za pomocą właściwych kabli serwisowych oraz adapterów pośredniczących. W ten sposób następuje dokonywanie zrzutu pamięci urządzenia. W kolejnym etapie ma miejsce analiza zrzutu pamięci i ekstrahowanie z niej pożądanych informacji, danych i treści. Metoda ta nie zostawia żadnych śladów jej przeprowadzania na „badanym" urządzeniu mobilnym. Czas takiej ekstrakcji jest różny i zależny od rodzaju urządzenia, jego modelu, marki, wersji systemu operacyjnego, a także rodzaju zabezpieczenia tego urządzenia. Nie wszystkie modele telefonów czy tabletów są możliwe do obsłużenia tą metodą. Producenci ww. rozwiązań do akwizycji danych dosyć szybko reagują na zmiany w rynku urządzeń mobilnych i cały czas aktualizują swoje urządzenia, aby nadążyły za nowo dystrybuowanymi na rynek sprzętu mobilnego urządzeniami. Metoda bezinwazyjna znakomicie nadaje się do zrzucenia pamięci urządzenia, niekiedy w czasie nieprzekraczającym godziny. Właśnie z tego powodu ważne jest dla bezpieczeństwa naszych poufnych informacji zwracanie uwagi na sprzęt, w którym są przechowywane i w miarę możliwości nietracenie nad nim fizycznej kontroli. Często pozostawienie telefonu, np. w szatni podczas treningu albo wizyty na basenie w zupełności wystarczy do wykonania jego kopii. Wykreowanie sytuacji, które nasi przeciwnicy mogą wykorzystać często zależne jest od naszego trybu życia.

Omawiając wykonanie zrzutów pamięci urządzeń mobilnych należy wspomnieć o rodzajach ekstrakcji danych i krótko je scharakteryzować. W opisie tych metod nie będziemy zagłębiać się w arkana techniczne, a jedynie w prosty sposób opiszemy ich rodzaje tak, aby czytelnik umiał je odróżnić i był w stanie dostrzec najbardziej istotne różnice. Omówione zostaną dwa rodzaje najczęściej wykorzystywanych.

Wszystkie rozwiązania bazują na dwóch podstawowych rodzajach zrzutu zawartości pamięci, tj. logicznym i fizycznym. Oto ich charakterystyka:

1. Logicznym zrzutem pamięci nazwiemy kopię danych logicznych, czyli odzwierciedlenie istniejących struktur katalogów i plików systemu operacyjnego urządzenia. Wszystkie pliki i katalogi będą skopiowane w takiej formie w jakiej aktualnie znajdują się w pamięci urządzenia, np. telefonu. Pozyskanie logiczne oznacza wykonanie kopii logicznej obiektów (np. plików czy katalogów) znajdujących się w przestrzeni logicznej urządzenia (np. na partycji systemowej). Przy zastosowaniu ekstrakcji logicznej o wiele łatwiej jest analizować dane, jak również je przeglądać. Wyodrębnienie logiczne struktury pamięci oraz jej synchronizację i interpretację wykonuje się przy użyciu specjalistycznego oprogramowania. Pozyskanie logiczne jest dość prostą metodą i również najszybszą do wykonania.

2. Fizycznym zrzutem pamięci nazwiemy dokładną (sektor po sektorze) kopię całego fizycznego nośnika danych, w naszym przypadku pamięci eMMC lub UFS. Metoda ta jest analogiczna, tak jak w przypadku badania tradycyjnych komputerów. Na kopii fizycznej można zbadać pozostałości usuniętych danych czy plików. Uzyskanie kopii fizycznej pamięci urządzenia jest dużo trudniejsze i wymaga wielu zabiegów oraz doświadczenia, gdyż producenci sprzętu zwykle zabezpieczają go przed bezpośrednim dostępem do pamięci. Dlatego też urządzenie może być zablokowane, a dostęp do niego możliwy tylko dla konkretnego producenta. W tym celu urządzenia służące do ekstrakcji danych mają cały wachlarz komend serwisowych i innych metod, między innymi swój własny *boot loader*, czyli program służący do rozruchu, dający, np. urządzeniu UFED dostęp do pamięci urządzenia mobilnego. Tworzenie kopii fizycznej można podzielić w przypadku urządzeń mobilnych na dwie fazy: fazę tworzenia zrzutu pamięci oraz na fazę dekodowania i wyodrębniania danych.

Metody inwazyjne pozyskiwania danych

Metody inwazyjne stosuje się w przypadku uszkodzenia lub częściowego zniszczenia badanego urządzenia, jak również w sytuacji, gdy metody bezinwazyjne nie dają pożądanego efektu.

Wiele osób jest błędnie przekonanych, że skoro ich urządzenie uległo zniszczeniu, jest połamane lub po prostu nie działa to nie istnieją już możliwości odzyskania z niego danych. Dodatkowo fakt, że było zabezpieczone pinem lub wzorkiem jeszcze bardziej utwierdza użytkownika takiego urządzenia w przekonaniu, że może spokojnie się go pozbyć, bo i tak nic z niego nie da się odzyskać. Niekiedy użytkownicy nie mają świadomości i nawet nie biorą pod uwagę faktu, że ich dane narażone są na nieautoryzowany dostęp. Niestety, nic bardziej mylnego. W wielu przypadkach udaje się odzyskać dane w całości lub w części. Wszytko zależy od tego jakiego rodzaju dane są szukane i czy przystąpiono do procesu odzyskiwania w sposób profesjonalny. Nieumiejętne postępowanie z pamięcią urządzenia mobilnego może skutkować jej uszkodzeniem i spowodować całkowitą utratę możliwości pozyskania danych.

Metody inwazyjne można podzielić na dwa następujące sposoby: Jtag i Chipoff

W obu przypadkach następuje odczyt fizyczny urządzenia polegający na zgraniu pełnej kopii pamięci wewnętrznej urządzenia sektor po sektorze. Stosując tą metodę omijamy wymagany w metodzie bezinwazyjnej dostęp do chronionych obszarów systemu, dzięki czemu nie jesteśmy zależni od producenta urządzenia i wersji systemu operacyjnego. Ponadto dostęp do danych często jest utrudniony poprzez zastosowane zabezpieczenia, takie jak PIN, hasło bądź symbol, które najpierw należy złamać. W metodzie Jtag oraz Chipoff pomijamy te aspekty.

Wspomniane metody, wymagają ingerencji do wnętrza urządzenia. W przypadku podłączenia się do płyty głównej urządzenie (metoda Jtag) pozostanie ono sprawne, natomiast w przypadku zastosowania metody Chipoff istnieje

ryzyko, że urządzenie nie wystartuje. W takiej sytuacji można ponownie wlutować pamięć poprzez technikę zwaną rebalingiem. Proces ten jest długi i czasochłonny, wymaga też użycia specjalistycznego sprzętu. Metodę JTag stosuje się często w urządzeniach, które po wykonaniu odczytu danych mają być ponownie złożone i funkcjonalne.

JTag w praktyce składa się z 5 etapów.

Etap I . Rozłożenie telefonu w celu uzyskania dostępu do płyty głównej.

Etap II. Lokalizacja pinów technicznych i ocena stanu uszkodzeń. Czynność wykonuje się pod mikroskopem technicznym. Następuje wlutowanie w zlokalizowane przewody celem podpięcia interfejsu czytnika. Najczęściej stosuje się tzw. boxy serwisowe.

Etap III. Podłączenie adapteru czytnika do boxu serwisowego w celu dokonania ekstrakcji danych.

Etap IV. Odczyt kości pamięci (wykonujemy jej obraz fizyczny).

Etap V. Po wykonaniu zrzutu pamięci istnieje możliwość otwarcia pliku z kopią w programie do analizy i wykonania ekstrakcji interesujących nas danych użytkownika.

ChipOff w praktyce na przykładzie telefonu Samsung S7 oraz Nokia LUMIA 720.

Etap I. Rozbieranie telefonu. Telefon po wypadku drogowym. Całkowicie zniszczony.

Etap II. Wylutowywanie kości pamięci z płyty głównej telefonu. W tym przypadku pracuje się z wykorzystaniem stacji lutowniczej na gorące powietrze oraz specjalistycznej chemii w postaci preparatów typu Flux oraz preparatów czyszczących. Istotnym jest, aby zastosować schemat temperaturowy dla danej kości pamięci. Należy dobrać taki zakres temperatur przy wylutowywaniu, aby nie uszkodzić delikatnych chipów.

Etap III. Oczyszczanie pinów kości pamięci.

Po ekstrakcji kości pamięci należy dokładnie wyczyścić chip z resztek spoiwa oraz past i chemikaliów. Czyszczenie odbywa się pod mikroskopem. Należy zachować szczególną ostrożność, by nie uszkodzić żadnych pinów układu scalonego.

Etap IV. Sczytywanie danych z kości pamięci.

Karty rozszerzenia pamięci

Omawiając urządzenia mobilne należy wspomnieć również o pamięci dodatkowej, którą można powiększyć w formie karty microsd. Na tego rodzaju nośnikach najczęściej magazynujemy filmy, fotografie czy muzykę. Często taki nośnik służy nam również jako pamięć przenośna, na której migrujemy nasze dane między komputerem, a urządzeniami mobilnymi. Na tej pamięci często robimy backupy swoich danych z telefonu, tabletu itp., a co za tym idzie archiwizujemy czaty, smsy, mms, maile itp. Dostęp do tego rodzaju nośników pamięci nie powoduję większych problemów technicznych. W wielu przypadkach takie karty mogą się stać łatwym celem dla osób niepowołanych, którym może zależeć na pozyskaniu naszych danych. Często też myślimy błędnie, że uszkodzona karta, do której nie mamy z jakiegoś powodu dostępu, nie stanowi zagrożenia, a zapisywane i gromadzone tam informację nie są do pozyskania. Należy podkreślić, że nawet z mechanicznie (fizycznie) uszkodzonej karty często udaje się odzyskać dane. Wszystko zależy w jakim stopniu jest uszkodzona, i czy np. podczas jej nadłamania czy nawet złamania lub ukruszenia, nie uszkodziła się tzw. pamięć NAND znajdująca się w monolicie. Do odzyskiwania danych z takich kart można skorzystać z istniejących na rynku specjalistycznych rozwiązań takich jak czytniki i programatory pamięci NAND. Opracowanie niniejsze ma jedynie naświetlić w prosty sposób omawiane zagadnienia.

Przykładowe dane pochodzące z ekstrakcji telefonów i krótka charakterystyka uzyskanych z nich informacji

Omawiane przykłady zostały przygotowane przy użyciu rozwiązania UFED marki Cellebrite. Po wykonaniu zrzutu pamięci dane są analizowane i dekodowane za pomocą modułu UFED Physical Analyzer 7. W wyniku przetwarzania uzyskuje się przejrzysty interfejs do swobodnego poruszania się po informacjach zdekodowanych z urządzenia mobilnego, w tym przypadku jest to telefon marki SAMSUNG. Dane znajdują się w zakładce zawierającej podsumowanie ekstrakcji. Są to wszystkie podstawowe i zaawansowane informacje na temat badanego urządzenia, takie jak: numery IMEI, IMSI, wersja systemu, model, nazwa itp. Po prawej stronie znajduje się menu, z którego można wybierać interesujące dane. Liczby koloru białego przy każdej pozycji określają ilość odnalezionych artefaktów z danej kategorii. Natomiast cyfry koloru czerwonego informują, jaka liczba elementów z danej kategorii została odzyskana. Poruszanie się po poszczególnych kategoriach jest proste i przejrzyste, a dla uproszczenia wyszukiwania można używać filtrów pomagających zawęzić zakres interesujących nas danych.

Kolejne dane, jakie można uzyskać z zabezpieczonego i sklonowanego urządzenia to m.in.: wiadomości SMS, wiadomości MMS, rozmowy z czatów i komunikatorów, hasła, historia przeglądarek i lokalizacji. Oczywiście zakres kategorii danych dekodowanych z obrazu pamięci badanych urządzeń jest bardzo szeroki, co daje wiele możliwości, form i rodzajów zastosowań.

Urządzenia typu UFED i Xray znakomicie radzą sobie z ekstrakcją z urządzeń mobilnych wszelkiego rodzaju haseł zapamiętanych przez system operacyjny urządzenia. Można w ten sposób uzyskać hasła do wszelkiego rodzaju kont na stronach WWW, poczty elektronicznej, zapamiętanych i używanych sieci WiFi, zarówno tych domowych jak i firmowych. W tym miejscu należy podkreślić i przypomnieć, że dane te są bardzo często jednymi z najbardziej istotnych informacji dla osób niepowołanych, które między innymi przygotowują atak na zasoby firmy.

Warto podkreślić, że uzyskanie dostępu do historii przeglądania z przeglądarek internetowych używanych w urządzeniu mobilnym również nie stanowi dużego wyzwania. Możliwość przejrzenia i zapoznania się z treściami przeglądanymi przez użytkownika telefonu daje olbrzymią wiedzę osobom niepowołanym (rozkład dnia, zainteresowania, preferencje, problemy finansowe, kłopoty zdrowotne), która może być bezwzględnie wykorzystana przeciwko właścicielowi urządzenia.

Kolejnymi danymi pożądanymi przez osoby trzecie jest historia naszych lokalizacji, czyli gdzie się udajemy, chodzimy, jeździmy, gdzie mieszkamy itp.

Dane lokalizacyjne zawierają bardzo istotne informacje. Dzielą się na lokalizację po danych GPS oraz na lokalizację po stacjach bazowych (BTS) należących do poszczególnych operatorów telefonii komórkowych. Przy pozycji GPS zazwyczaj znamy dokładne współrzędne geograficzne, natomiast przy danych ze stacji BTS możemy określić ich położenie za pomocą CID i LAC, które są znacznikami poszczególnych stacji bazowych i w ten sposób zlokalizować je na mapie, np. za pomocą portalu www.btsearch.pl

Kolejnym istotnym zagadnieniem są dane dotyczące treści wszelkiego rodzaju komunikatorów.

Komunikatory mobilne – zasady działania

W niniejszym pracowaniu wzięto pod uwagę najbardziej popularne, szeroko stosowane przez użytkowników aplikacje mobilne, takie jak: WhatsApp, Signal, Facebook Messenger, Viber, Hangauts, Message oraz Usecrypt .

Należy zaznaczyć, że na rynku istnieje cała gama różnego rodzaju aplikacji mobilnych służących do wymiany korespondencji, jednakże postanowiliśmy skupić się na tych komunikatorach, z którymi nasza firma styka się najczęściej podczas wykonywanych zleceń czy ekspertyz, a także zadań związanych z ekstrakcją informacji z urządzeń mobilnych.

Na wstępie warto zaznaczyć, że większość popularnych komunikatorów korzysta z podobnych rozwiązań zabezpieczających, w tym także metody szyfrowania tzw. *end-to-end.* Posiadają one zbliżony poziom funkcjonalności począwszy od wysyłania wiadomości tekstowych, głosowych, wszelkiego rodzaju wiadomości multimedialnych, a kończąc na rozmowach głosowych, tj. telefonicznych. Dodatkowo dają możliwość tworzenia czatów grupowych, co w dzisiejszych cza-

sach jest opcją niezwykle pożądaną, wykorzystywaną często do zarządzania grupami zasobów ludzkich w granicach firmy lub instytucji. Często służą do celów grupowej wymiany informacji, np. w ramach grupy tematycznej czy grupy znajomych. Reasumując z aplikacji tych korzysta większość z nas celem przesyłania informacji do swoich współpracowników lub znajomych. W wielu przypadkach treści przesyłane tą drogą nie są szczególnie istotne czy poufne, a przejęcie ich przez osoby trzecie nie spowoduje dotkliwych dla użytkownika skutków. Kłopoty mogą pojawić się kiedy korzystając z tych aplikacji prześlemy treści szczególnie dla nas ważne, czy o niejawnym charakterze. Świadomość użytkowników komunikatorów wzrasta w momencie zdania sobie sprawy z faktu, iż przejęcie przesyłanych przez nich danych może wiązać się z olbrzymim zagrożeniem. Wówczas rozpoczyna się poszukiwanie skutecznych i bezpiecznych rozwiązań stosowanych w mobilnej łączności. Jak już wcześniej wspomniano większość z topowych komunikatorów ma zastosowane podobne mechanizmy szyfrowania. Co istotne, większość z nich to aplikacje darmowe.

Podejmując decyzję o wyborze komunikatora warto przemyśleć do jakich celów będziemy go użytkować. Jeżeli większą cześć naszej konwersacji będą zajmowały śmieszne zdjęcia i filmy, a przesyłane treści nie będą poufne, lepiej zdecydować się na któryś z oferowanych darmowych komunikatorów. Natomiast przy korespondowaniu na tematy wrażliwe, firmowe, wysokiej rangi, objęte wszelkiego rodzaju tajemnicą należy zdecydowanie wybrać rozwiązanie profesjonalne.

Firma MY DATA zebrała szereg doświadczeń zdobytych podczas wyodrębnienia i odzyskiwania treści z przejętych urządzeń mobilnych. Warto zaznaczyć, że większość dostępnych komunikatorów oferuje podwyższony poziom bezpieczeństwa wymiany informacji za pomocą szyfrowania metodą *end-to-end*. Aplikacja ta wyposażona jest w standardowy wachlarz funkcji, w tym wiadomości tekstowe, multimedialne, czy bezpieczne rozmowy głosowe.

Komunikatory to produkty różnych marek. Mają one jedną wspólną cechę, która dotyczy nieskomplikowanej procedury pozyskiwania treści korespondencji z urządzeń mobilnych, w których są zainstalowane. Posiadając fizycznie telefon lub tablet użytkownika tych aplikacji, możemy uzyskać dostęp do jego kompletnej, pełnej korespondencji, łącznie z elementami, które usunięto. Po pozyskaniu takiego urządzenia i wykonaniu jego kopii fizycznej jesteśmy w stanie odczytać kompletną korespondencję właściciela urządzenia.

Podsumowanie

Bezpieczeństwo jest wartością bezcenną, pożądaną przez wszystkich, bez wyjątku. Informacja jest narzędziem, które to poczucie bezpieczeństwa może zburzyć, a nawet zupełnie zniweczyć. Dlatego też potrzeba zabezpieczenia anonimowości przepływu informacji staje się w dzisiejszych czasach priorytetowa.

Tekst, wiadomość głosowa, multimedia, nasze prywatne dane, informacje dotyczące bliskich, kont bankowych czy tajemnic służbowych, w tym również

tych najbardziej wrażliwych, poufnych i tajnych, to dane szczególnejnie możemy pozwolić na ich niekontrolowaną utratę. Chcemy je chronić, choć nagminnie przesyłamy za pośrednictwem dostępnych komunikatorów czy innych rozwiązań komunikacji instalowanych na wszechobecnych urządzeniach mobilnych. To skutkuje potrzebą wprowadzenia zabezpieczeń tych urządzeń. Blokujemy więc dostęp do urządzeń poprzez hasło lub blokadę ekranu. Co prawda często łatwe do przełamania. W niektórych jednak urządzeniach wręcz niemożliwe bez wysoce laboratoryjnych badań. Zawsze jednak jakikolwiek stopień zabezpieczenia stwarza problemy dla osób, które w nieuprawniony sposób chcą wejść w posiadanie naszych danych.

My, jako firma MK MY DATA, zalecamy szyfrowanie telefonu. Zabieg taki pozwala osiągnąć bardzo wysoki poziom bezpieczeństwa. Jednak należy pamiętać, że gdy osoby trzecie wejdą w posiadanie klucza szyfrującego lub hasła do telefonu – nie będą mieć problemu ze zrobieniem kopii urządzenia. Dobrym nawykiem jest co jakiś czas zmieniać hasła lub wzorki zabezpieczające. To tak niewiele, a w wielu przypadkach może uchronić przed pozyskaniem z naszego urządzenia mobilnego ważnych informacji.

Radzimy także, by nie szyfrować kart rozszerzenia pamięci, bo istnieje ryzyko, że stracą właściwość nośnika zewnętrznego służącego do migracji danych między komputerem, a np. telefonem. Zdecydowanie korzystniej zakładać szyfrowane „kontenery" lub eksportować kopie i ważne dane. Nie należy też robić tzw. pamięci wewnętrznej z kart microsd, bo dość często ulegają awarii co skutkuje problemem z odzyskiem zawartych na nich danych.

Sugerujemy, by rozsądnie korzystać z wachlarza obecnych na rynku aplikacji służących do zabezpieczenia danych na urządzeniach mobilnych. Nie zawsze aplikacja bezpłatna jest dobrym wyborem, choć często może być po prostu wystarczająca. Zawsze przed dokonaniem wyboru należy przeanalizować potencjalne zyski i straty, które mogą towarzyszyć utracie danych.

Niezmiennie i w każdej sytuacji wskazane jest zachowanie kontroli nad użytkowanym sprzętem oraz rozsądne przekazywanie dotyczących nas treści, ze świadomością ich wagi i wartości, jaką dla nas stanowią. Ważne też, by beztrosko nie wyrzucać wyeksploatowanego sprzętu, bez uprzedniego profesjonalnego zniszczenia jego zawartości.

Istotnym jest zgłębianie własnej wiedzy na przedmiotowy temat, jak również przeprowadzanie stosownych szkoleń wśród współpracowników czy podległych pracowników. Pozyskane informacje, a co za tym idzie wprowadzenie stosownych rozwiązań, będą skutkować podniesieniem standardów bezpieczeństwa przesyłanych danych. Zdecydowanie lepiej zapobiegać, niż ponosić skutki korzystania z niezabezpieczonych urządzeń mobilnych

Michał Kurzaj

*** Michał Kurzaj, MK MY DATA, *ekspert data recovery*, biegły sądowy, informatyk śledczy**

Jerzy Wojciech Wójcik, Czesław Marcinkowski

Podsumowanie

Niniejsza publikacja Wszechnicy Polskiej Szkoły Wyższej w Warszawie jest wynikiem dwóch naukowych spotkań ekspertów zajmujących się wciąż mało nagłośnioną i stosunkowo mało znaną problematyką – wywiadem i kontrwywiadem w biznesie. W spotkaniach i ich organizacji istotną rolę odegrali członkowie Fundacji Instytutu Wywiadu Gospodarczego z Krakowa. Eksperci uczestniczący w obu spotkaniach są teoretykami oraz praktykami, głęboko obeznanymi z prezentowanym zagadnieniami.

Tytuł publikacji *Wywiad i kontrwywiad w teorii i praktyce biznesu* jest identyczny z obszarem rozważań zakreślonych w idei spotkań oraz zrealizowanej dyskusji. Został uznany za merytorycznie poprawnie odpowiadający problematyce dyskusji w czasie obu konferencji. Jest również adekwatny do prezentowanej treści, jednakże stanowi jedynie wybrane fragmenty rozważań i dyskusji uczestników.

Sesje plenarne konferencji pod wspólnym tytułem *Wywiad i kontrwywiad w teorii i praktyce biznesu* odbyły się w dniach 25 maja 2017 roku i 24 maja 2018 roku i skupiały się na takich zagadnieniach jak:

- Teoria i praktyka działalności rozpoznawczo – informacyjnej w gospodarce.
- Wywiad i kontrwywiad w teorii i praktyce biznesu.
- Wyzwania, uwarunkowania oraz stan działalności wywiadowczej i kontrwywiadowczej w biznesie.
- Funkcjonowanie wywiadu i kontrwywiadu gospodarczego. Doświadczenia i propozycje.
- Jakie są oczekiwania od wywiadu gospodarczego ze strony biznesu?
- Jaka jest przyszłość kształcenia w tym zakresie?

Uczestnikami i referentami na konferencjach byli naukowcy oraz praktycy, a przykładowo: prof. dr hab. Jerzy Konieczny z Uniwersytetu w Opolu, który wygłosił referat pt.: *Zagrożenia cybernetyczne i ich analiza*. Na uwagę zasługuje fakt, że uczestnikami konferencji było liczne grono studentów Wszechnicy Polskiej Szkoły Wyższej w Warszawie z kierunku Bezpieczeństwo wewnętrzne.

Ogólnie ujmując, wywiad jest szeroką formą aktywności nie tylko państwowej, prowadzonej przez specjalnie powołane instytucje do zdobywania niejawnych informacji zarówno z obszaru politycznego czy militarnego, a przede wszystkim gospodarczego innych podmiotów czy państw. Jest również formą aktywności różnych wyspecjalizowanych podmiotów. Treścią tej publikacji są więc problemy aktywności wywiadu gospodarczego i jednocześnie niektóre aspekty przeciwdziałania tej aktywności przez wyspecjalizowane podmioty.

Obecnie gromadzenie informacji gospodarczych jest równie ważne zarówno ze sfery politycznej czy militarnej, lecz przede wszystkim ze sfery gospodarczej. Taka forma znana jest od niepamiętnych czasów. W okresie globalizacji współczesnego świata nie utraciła nic ze swego znaczenia, lecz wprost przeciwnie nasila się. Przykładem jest pojawienie się na rynku instytucjonalnym różnego rodzaju profesjonalnych wywiadowni gospodarczych. Nastawione są one na poszukiwanie i zbieranie informacji z różnych dziedzin życia gospodarczego (wynalazczego, przemysłowego w tym technologicznego, finansowego itp.), a przede wszystkim analizowanie osiągnięć firm konkurencyjnych. Istotą wywiadu gospodarczego jest udostępnianie osiągnięć technicznych, rodzących się nowych koncepcji strukturalnych, czy też powiązań biznesowo-finansowych.

Dzisiejszy wywiad gospodarczy niekoniecznie opiera się na działalności agentów działających pod przykryciem. To jest już historią. Współczesna informatyzacja (cyfryzacja) właściwie całych obszarów życia jest faktem dokonanym. Za tym procesem ułatwiającym w wielu przypadkach biznes poprzez Internet – kryją się ogromne zagrożenia, które tylko częściowo zasygnalizowano w niniejszej publikacji.

Współczesne zarządzanie instytucjami, współpracą gospodarczą oraz bankową odbywa się głównie w cyberprzestrzeni. Możliwości prawie natychmiastowego porozumienia się z konkretnym kontrahentem w dowolnym punkcie świata jest bezcenne. Niemniej jest doskonałą okazją do włamań w systemy informatyczne i wykradania różnorodnych informacji, przede wszystkim tych poufnych i prawnie chronionych.

Zarówno obydwie konferencje, jak i szereg spotkań naukowych przed konferencjami i nadal organizowanych spotkań zainteresowanych ekspertów, można określić w kilku węzłowych zagadnieniach obejmujących szeroki zakres wiedzy, a w szczególności:

- teoretyczno-badawcze wyzwania oraz uwarunkowania działalności wywiadowczej i kontrwywiadowczej w polskim biznesie i edukacji;
- teoria i praktyka działalności rozpoznawczo-informacyjnej w gospodarc;
- wyzwania, problemy oraz propozycje rozwiązań.

Na treść publikacji składają się opracowania poświęcone wielu teoretycznym, badawczym i praktycznym aspektom aktywności wywiadu i kontrwywiadu w sferze biznesu. Zasygnalizować warto przynajmniej kilka tytułów wygłoszonych referatów, a przykładowo:

- z problematyki bezpieczeństwa informacji i tajemnic zawodowych (J.W. Wójcik);
- iluzja pełnej informacji jako przestrzeni do skutecznego działania wywiadu i kontrwywiadu (K. Kula);
- przedsięwzięcia w zakresie tworzenia potencjału innowacyjnego zespołu wywiadowczego (kontrwywiadowczego) przedsiębiorstwa (T. Przybyszewska);

- wykorzystywanie różnorodnych sieci czy zespołów do pozyskiwania w sposób niejawny danych na potrzeby wywiadu gospodarczego (A. Nastula, P. Pruszyński);
- wykorzystanie analizy wywiadowczej i osłony kontrwywiadowczej w ocenie zagrożeń zagranicznej ekspansji działalności przedsiębiorstwa (M. Kwieciński).

Warto podkreślić znaczący referat i prezentację Michała Kurzaja informatyka śledczego, którego praca pt. *Zagrożenia wynikające z użytkowania i utraty mobilnych urządzeń komunikacyjnych, czyli „technologia w cuglach"*, wskazuje na potrzebę racjonalnego obchodzenia się z uszkodzonymi czy zniszczonymi urządzeniami teleinformatycznymi, z których można jednak odczytać szereg informacji.

Na uwagę zasługuj fakt, że wśród uczestników konferencji był również student Wszechnicy Polskiej Szkoły Wyższej w Warszawie z kierunku Bezpieczeństwo wewnętrzne Artur Kryst, który wygłosił referat pt. *Ochrona tajemnicy przedsiębiorstwa przed cyberwywiadem biznesowym*.

Równie interesujące są pozostałe opracowania i warto wyrazić przekonanie, że publikacja spełni zarówno oczekiwania, jak i zainteresowania poznawcze czy zawodowe wszystkich zainteresowanych omawianymi problemami.

Jerzy Wojciech Wójcik*, Czesław Marcinkowski**

*** prof. dr hab. Jerzy Wojciech Wójcik, Wszechnica Polska Szkoła Wyższa w Warszawie**
****dr Czesław Marcinkowski, Wszechnica Polska Szkoła Wyższa w Warszawie**