Nr 2 (2013) ISSN 2084-2279

Katarzyna GŁOWANIA[1]

Pod merytoryczną opieką płk. dr. hab. Henryka SPUSTKA

WYWIAD I SZPIEGOSTWO GOSPODARCZE

Abstrakt: *Niniejszy artykuł objaśnia krótko problematykę związaną z wywiadem i szpiegostwem gospodarczym. Poruszono w nim przede wszystkim terminologię, katalog metod zdobywania informacji, propozycję przeciwdziałania ,,wyciekom" tajemnic oraz regulacje problemu szpiegostwa zawarte w aktach prawnych. Artykuł ten jest materiałem pokonferencyjnym Konferencji naukowej z dnia 16 maja 2013 roku na temat „Bezpieczeństwo personalne a bezpieczeństwo strukturalne państwa. Wolność i bezpieczeństwo obywatela."*

Słowa kluczowe: *tajemnica przedsiębiorstwa, wywiad gospodarczy, szpiegostwo gospodarcze, metody i środki pozyskiwania tajemnic przedsiębiorstwa, minimalizacja ryzyka, ustawa o zwalczaniu nieuczciwej konkurencji*

WSTĘP

Po zakończeniu Zimnej Wojny mogłoby się wydawać, że fach szpiegowski traci na znaczeniu. Dzisiejszy coraz bardziej konkurencyjny i wymagający rynek udowadnia, że szpiegostwo jako profesja istnieje nadal, rozwijając się, udoskonalając swoje metody i techniki. Jednak współcześnie, w sytuacji pokoju, kiedy legalne i formalne sposoby uzyskiwania informacji w sektorze gospodarczym stają się niewystarczające, często dochodzi do sytuacji, gdy rywalizujące ze sobą podmioty gospodarcze sięgają po sposoby niejawne - działania szpiegowskie. W dzisiejszych czasach żadna firma nie może być pewna bezpieczeństwa swoich tejemnic. Czasem jeden ,,wyciek" informacji może zadecydować o upadku przedsiębiorstwa lub o jego zmniejszonych zyskach. Niniejszy artykuł jest próbą zbadania tego zjawiska, jego analizy oraz propozycji przeciwdziałania szpiegostwu gospodarczemu.

1. SZPIEGOSTWO W DZIEJACH

Szpiegostwo towarzyszy ludzkości od zarania dziejów, o czym możemy się przekonać wczytując się w Stary Testament. Przeczytać możemy o Dalili, której zadaniem, w zamian za korzyść materialną, było zdobycie informacji na temat tego, co decyduje o sile Samsona. Dzięki swojemu urokowi, sprytowi i rozbudowanej technice manipulacji zdobyła tak potrzebną Filistenom informację, za którą Samson przypłacił kalectwem i niewolą. Sięgając do notatek XV-wiecznego arabskiego urzędnika dowiadujemy się, że królowie wysyłali swoich ambasadorów nie tylko w celach, jak by się wydawało dyplomatycznych, ale przede wszystkim w celach szpiegowskich. Ich zadaniem było pozyskanie informacji dotyczących m.in. stanu dróg, położenia przełęczy, rzek i żyznych pastwisk, danych o liczebności i uzbrojeniu armii[2].

[1] Katarzyna GŁOWANIA – studentka I roku, studiów I stopnia kierunku Bezpieczeństwo Wewnętrzne Uniwersytet Opolski.

[2] M. P. Ryszkowski, M. U. Ryszkowska, M. H. Ryszkowska, *O wybranych tajemnicach- bez tajemnic*, Katowice 2011, s. 9.

Informacje te były wówczas podstawą do planowania ewentualnych wojen czy przymierzy.

O sztuce szpiegostwa - jednego z najstarszych zawodów świata - możemy również dowiedzieć się sięgając po „Sztukę Wojny" autorstwa chińskiego teoretyka wojny Sun Tzu. W pochodzącym z VI w p.n.e. traktacie podkreślono wartość wywiadu dla prowadzenia wojny i funkcjonowania państwa. Sun Tzu nazywa szpiegów Doskonałą Siecią, znajdującą się pod szczególną opieką władcy[3]. Dokonuje także aktualnej do dziś klasyfikacji przedstawicieli tego fachu[4]. Od zawsze informacje znaczące dla jednych są w centrum zainteresowania drugich. Ich zdobycie pozwala na pewien element zaskoczenia, co pozwala na zdobycie przewagi nad drugą stroną. Wraz z rozwojem cywilizacji szpiegostwo zdobywało coraz większe uznanie, aż stało się jednym z najbardziej użytecznych narzędzi walki z konkurencją. Historia pokazuje, że szpiedzy na usługach swoich władców nie raz wpłynęli na zmianę dziejów.

2. WARTOŚĆ INFORMACJI

Obecnie zdobywanie tajnych informacji, istotnych dla bezpieczeństwa i obronności państwa, nadal jest pożądane. Agenci wciąż udoskonalają swoje techniki, by obejść zabezpieczenia, oszukać system ochrony i wykraść tajemnicę. W dzisiejszych czasach informacja ma niezwykle wielką wartość - jest towarem, i jak każdy towar ma swoją cenę. XXI wiek został już okrzyknięty wiekiem informacji - posiadając informację, posiadamy bowiem władzę. Potrzebna informacja, dostępna w odpowiednim czasie, staje się towarem strategicznym. Dlatego należy ją odpowiednio chronić przed nieuprawnionym ujawnieniem[5].

W tym miejscu należałoby wyjaśnić, co oznacza termin informacja. Według Kopalińskiego „(…) jest to wiadomość, wieść, nowina, rzecz zakomunikowana, zawiadomienie, komunikat, pouczenie, powiadomienie, zakomunikowanie o czymś; dane, pokój, okienko, stanowisko, gdzie się udziela informacji"[6].

Z nieco innym rozumieniem tego pojęcia spotykamy się w „Leksykonie Zarządzania". „ Informacja to przeanalizowana i przetworzona do postaci zrozumiałej dla odbiorcy wiadomość (dana, sygnał), która powiadamia go o sytuacji i ma dla niego wartość w procesie decyzyjnym. Informacja jest pojęciem węższym, niż dana. Zawiera bowiem tylko te fakty i liczby, które są przedstawione w formie zrozumiałej dla odbiorcy, dotyczą obszaru zainteresowań odbiorcy, posiadają wartość dla odbiorcy"[7].

Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji wprowadza pojęcie tajemnicy przedsiębiorstwa. Zgodnie z ustawą tajemnicą przedsiębiorstwa są nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość

[3] Sun Tzu, *Sztuka wojny*, Gliwice 2004, s.79-81.

[4] *Ibidem*, autor w rozdziale trzynastym pt. „Użycie szpiegów" wyszczególnia pięć typów tajnych agentów: agenci narodowi, wewnętrzni, podwójni, straceni oraz powracający. Agenci narodowi to ci spośród ludności wroga, którzy przeszli na naszą służbę. Agenci wewnętrzni rekrutują się spośród urzędników wroga, których udaje nam się pozyskać. Agenci podwójni to szpiedzy obcych państw, których udaje nam się. pozyskać. Agenci straceni, to ci, którzy rozpowszechniają, rozmyślnie sfałszowane informacje. Agenci powracający to ci, którzy po spełnieniu swojej misji w państwie wroga powracają do ojczyzny z odpowiednimi informacjami.

[5] B. Iwaszko, *Ochrona informacji niejawnych w praktyce*, Wrocław 2012 s. 13.

[6] W. Kopaliński, *Słownik wyrazów obcych i zwrotów obcojęzycznych*, Warszawa 1975, s. 429.

[7] M. Adamska, *Leksykon zarządzania*, Warszawa 2004, s. 165.

gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności[8].

Dziś walka o informację nie dotyczy jedynie wyspecjalizowanych tajnych służb wywiadowczych, lecz coraz częściej także podmiotów gospodarczych. Wiąże się to z faktem, że informacje stały się głównym zasobem przedsiębiorstw, który często decyduje o „byciu albo niebyciu" na coraz bardziej konkurencyjnym rynku.

3. WYWIAD A SZPIEGOSTWO GOSPODARCZE

Powyższe terminy są niesłusznie ze sobą utożsamiane, chociaż wgłębiając się w terminologię możemy dostrzec, jak wiele dzieli oba te pojęcia. Termin ,,wywiad gospodarczy" pojawił się na początku lat 80. XX wieku w USA, gdzie stał się nazwą przedmiotu akademickiego. Wywiad gospodarczy to ,,profesjonalne zdobywanie i analizowanie informacji o określonych segmentach rynku, funkcjonujących na tych rynkach podmiotach, ich osiągnięciach technicznych, projektach działań i pozycji ekonomicznej"[9]. Inną jego definicję odnajdujemy w „Systemie informacji strategicznej". „Jest to zespół działań polegających na poszukiwaniu, przetwarzaniu i rozpowszechnianiu (w celu jej wykorzystania) informacji przydatnej podmiotom gospodarczym"[10].

Wywiad działa w sposób jawny, zgodnie z obowiązującym prawem i zasadami etyki. Pozyskane przy jego pomocy informacje nie są objęte klauzulą poufności. To właśnie jednoznacznie odróżnia go od szpiegostwa. Wprawdzie oba terminy mają wspólny rodowód i niegdyś były pojęciami tożsamymi, to jednak dziś błędem byłoby ich nie rozróżniać.

,,Zgodnie z art. 23. Ustawy z dnia 15.04.1993 r. o zwalczaniu nieuczciwej konkurencji, szpiegostwo to fakt bezprawnego uzyskania informacji stanowiącej tajemnice przedsiębiorstwa, ujawnienie jej innej osobie lub wykorzystanie we własnych działalności gospodarczej"[11]. Szpiegostwem określa się także próbę uzyskania dostępu do tajnych informacji przy użyciu niedozwolonych środków[12].

Szpiegostwo różni się od wywiadu działaniem z ukrycia (często noszącym znamiona przestępstwa), metodami i środkami pozaprawnymi, które powodują bezpośrednią szkodę innego podmiotu gospodarczego. Działanie szpiegów polega na pozyskiwaniu informacji poprzez ich wykradanie (np. kradzież dokumentacji, przekupienie pracowników, stosowanie podsłuchu), gromadzenie, przetwarzanie, przechowywanie oraz wykorzystanie w celu zdobycia przewagi nad konkurencją.

Podsumowując, wywiad i szpiegostwo gospodarcze, różnią się:

- legalnością działania - metody i techniki zgodne lub niezgodne z prawem,
- charakterem i treścią informacji,
- celem uzyskania informacji.

W 1986 roku w Stanach Zjednoczonych powstało pierwsze stowarzyszenie profesjonalnych wywiadowców gospodarczych - Society of Competitor Intelligence

[8] *Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji* (Dz.U. 2003 Nr 153 poz. 1503), dalej: *Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji*.

[9] M. Gajos, *Ochrona informacji niejawnych, biznesowych i danych osobowych*, Katowice 2011, s. 102.

[10] M. Kwieciński, *Wywiad gospodarczy a konkurencyjność przedsiębiorstwa,* [w:] *System informacji strategicznej*, R. Borowiecki, M. Romanowska, Warszawa 2001, s.107.

[11](b.a.), *Wywiad a szpiegostwo gospodarcze*, http://www.ipo.pl/ubezpieczenia_biznesowe/artykuly/wywiad_a__szpiegostwo_gospodarcze_592648.html, dostęp z dnia 7.05.2013.

[12] (b.a.), *Zagrożenia ze strony szpiegostwa gospodarczego,* http://www.iniejawna.pl/pomoce/szpieg.html, dostęp z dnia 7.05.2013.

Professionals. Skupiało ono osoby, które wywiadem zajmowały się zawodowo i nie chciały być utożsamiane z szpiegostwem.

Dziś nadal istnieje tendencja do mylenia wywiadu i szpiegostwa (określanego często mianem czarnego wywiadu). Wynika ona z nieznajomości zakresu pojęć. Zarówno wywiad, jak i szpiegostwo kojarzą się społeczeństwu ze zjawiskami pejoratywnymi. Prawdopodobnie dlatego społeczeństwo nie oddczuwa potrzeby precyzyjnego nazywania tych zjawisk.

4. SZPIEGOSTWO - SPOSOBY POZYSKIWANIA INFORMACJI POUFNYCH

Zaprezentowane poniżej sposoby nie są katalogiem zamkniętym, są to jednak najczęściej stosowane techniki.

Jednym ze sposobów pozyskiwania informacji poufnych jest wykorzystanie potencjału ludzkiego, a mówiąc precyzyjniej, pracownika konkurencji. To właśnie ludzie są najlepszym źródłem informacji. Trzeba uświadomić sobie istotę szpiega, który działa w danej firmie. Ponieważ pracuje on w tajemnicy, może być nim praktycznie każdy. Niedoceniani, mało zarabiający, sfrustrowani pracownicy mogą posłużyć za fundamentalne źródło „wycieku" tajemnic. Mogą to być zarówno osoby bezpośrednio zaangażowane w daną tajemnicę przedsiębiorstwa, jak i osoby pośrednie, np. pion ochrony czy konsewatorzy komputerów, którzy rozpoczynają swoją pracę, kiedy kończy ją wykwalifikowany personel. Konkurencja może „przekupić" pracownika danego przedsiębiorstwa, a tym samym zapewnić sobie idealne źródło informacji.

Naczelną rolę w szpiegostwie gospodarczym (i nie tylko) odgrywają najnowsze technologie. Warte uwagi są programy pozwalające na włamanie się do zabezpieczonych baz danych, wszelkiego rodzaju mikrourządzenia, służące do podsłuchiwania i podglądania, które są bardzo skuteczne, a jednocześnie bardzo dyskretne. Są to np. mikrokamery ukryte pod guzikiem, w długopisie czy breloczku, nadajniki ukryte w różnego rodzaju przedmiotach. Praktycznie każdy przedmiot znajdujący się w biurze czy kancelarii może być przydatny przy operacji wykradania tajemnicy przedsiębiorstwa. Godny uwagi jest KeyKatch. To małe urządzenie instalowane pomiędzy klawiaturą a portem USB, które daje nieograniczony dostęp do wszystkich znaków wprowadzanych za pomocą klawiatury komputerowej[13]. Uzyskane w ten sposób dane po analizie mogą dostarczyć wprowadzane do komputera hasła i innych informacje.

Dla celów szpiegowskich wykorzystywane są również linie telefoniczne, na których instalowane są podsłuchy, mikronadajniki radiowe, nadajniki transmitujące przez sieć zasilającą, mikrofony bezprzewodowe, podsłuchy w przewodach wentylacyjnych. Można wykorzystać również powierzchniowy mikrofon akustyczny, lokowany przy rurach wodociągowych lub gazowych. Istnieją także środki operacyjne, które nie wymagają dużych nakładów finansowych, jednak ich stosowanie nie jest możliwe przez dłuższy okres czasu ze względu na nikłą dyskrecję. Są to m.in. mikrofony kierunkowe, stetoskopy, kamery, aparaty fotograficzne, lornetki - wymagają one większego zaangażowania oraz niosą za sobą ryzyko dekonspiracji.

5. ZAPOBIEGANIA - MINIMALIZACJA RYZYKA WYCIEKU

Żadne przedsiębiorstwo nie może być pewne tego, że jego tajemnice są bezpieczne i wolne od zagrożenia, jakim jest szpiegostwo gospodarcze. Katalog środków zapobiegających jest katologiem otwartym. Ustawa o zwalczaniu nieuczciwej konkurencji nie określa działań, jakie możemy przedsięwziąć w celu obrony naszych

[13]P. Piejko, *Gadżety szpiegowskie dla każdego – TOP 10*, http://www.gadzetomania.pl/2010/09/17/gadzety-szpiegowskie-dla-kazdego/keylogger-czyli-keykatch-usb/top, dostęp z dnia 8.05.2013.

informacji poufnych. Każde przedsiębiorstwo ma inne (często ograniczone) środki, warunki i indywidualne potrzeby. Zatem lista sposobów chronienia danych jest bardzo zróżnocowana i długa. Oto kilka strategii pomocnych w podwyższeniu bezpieczeństwa firmy:

a) **Ogranizacja** - aby poufne, pilnie strzeżone informacje nie zostały przechwycone przez konkurencję należy przede wszystkim skupić się na organizacji bezpieczeństwa. Analiza dotychczasowego stanu bezpieczeństwa powinna stanowić punkt wyjścia dla dalszych działań zapobiegawczych.
b) **Edukacja** - ważne dla bezpieczeństwa naszych tejemnic jest przeszkolenie pracowników, począwszy od ogólnej edukacji wszystkich pracowników (np. poprzez szkolenia z zakresu potencjalnych zagrożeń), po edukację specjalistyczną (dotyczącą węższego kręgu kadry, np. personel techniczny). Pogłębienie wiedzy oraz świadomości personelu to kluczowy punkt w projektowaniu systemu bezpieczeństwa informacji poufnych. W wielu przypadkach to właśnie pracownicy nieświadomie stają się narzędziem konkurencji, np. poprzez:
   - pozostawienie ważnych dokumentów bez należytej ostrożności;
   - niewylogowanie się z systemów po skończeniu pracy;
   - nieautoryzowane dorabianie firmowych kluczy;
   - zapisywanie ważnych haseł w widocznych lub oczywistych miejscach, np. w kalendarzu, hasła łatwe do złamania np. „1234", imię i nazwisko, „0000";
   - niekorzystanie z niszczarek;
   - składowanie ważnych dokumentów w miejscach do tego nie przystosowanych.
c) **Działalność specjalistyczna** - warto zatrudnić specjalistów do spraw informacji niejawnych oraz utworzyć w firmach specjalne kancelarie, w których magazynowane oraz przetwarzane mogłyby być dokumenty – zgodnie z zachowaniem zasad bezpieczeństwa oraz hermetyczności.
d) **Weryfikacja** - ważna jest także weryfikacja potencjalnego pracownika oraz okresowa ocena wiarygodności obecnego personelu. Czynności te trzeba przeprowadzać z uwzględnieniem praw pracownika, ochrony danych osobowych oraz innych regulacji prawnych. Warto też pamiętać, że dobra atmosfera panujaca w firmie oraz godziwe warunki zatrudnienia minimalizują ryzyko zdrady wśród personelu. Jak pokazuje praktyka, zdrady dopuszczają się najczęściej osoby, które źle czują się w swoim miejscu pracy, narzekają na złe warunki i niską płacę oraz deklarują niechęć do swojego przełożonego.
e) **Zabezpieczenie techniczne** – to wprowadzenie technologii wspomagającej ochronę i bezpieczeństwo, jak np. firewalle, wykrywanie włamań, szyfrowanie i mechanizmy służące identyfikacji[14]. Można także zainstalować urządzenia zakłócające podsłuchy i kamery. Warto też co jakiś czas weryfikować pomieszczenia w firmie na obecność podsłuchów - w razie wykrycia ingerencji osób trzecich, fakt ten należy zgłosić do prokuratury.
f) **Ochrona fizyczna** - zabezpieczająca firmę zarówno w godzinach pracy, jak i po opuszczeniu jej przez personel.

[14] (b.a.), *Szpieg w firmie*, http://www.mojafirma.infor.pl/e-firma/programy-dla-firm/214924,Szpieg-w-firmie.html, dostęp z dnia 8.05.2013.

6. REGULACJE PRAWNE

W przypadku wywiadu i szpiegostwa gospodarczego, nie możemy mówić o pełnej regulacji prawnej. Owszem, istnieją pomocne akty prawne, jednak jak dotąd nie powstał taki, który w całości poświęcony byłby tym zagadnieniom. Dlatego też można z całą pewnością stwierdzić, że wywiad gospodarczy coraz częściej działa na zasadzie: wszystko co nie jest zabronione, jest legalne. Praktyki wywiadowcze to najczęściej stąpanie po bardzo cienkiej linii między legalnością działania, a łamaniem prawa. Najważniejszym aktem prawnym, jest ustawa o zwalczaniu nieuczciwej konkurencji z 16 kwietnia 1993 r. Nie tylko definiuje kluczowe pojęcie, jakim jest ,,tajemnica przedsiębiorstwa" (art. 11 ust. 1), lecz także przewiduje pewne sankcje karne.

Artykuł 23 pkt. 1 ustawy stanowi: ,,Kto, wbrew ciążącemu na nim obowiązkowi w stosunku do przedsiębiorcy, ujawnia formację stanowiącą tajemnicę przedsiębiorstwa, jeżeli wyrządza to poważną szkodę przedsiębiorcy, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2"[15]. Zgodnie z pkt. 2 „(…) tej samej karze podlega, kto, uzyskawszy bezprawnie informację stanowiącą tajemnicę przedsiębiorstwa, ujawnia ją innej osobie lub wykorzystuje we własnej działalności gospodarczej"[16].

Niestety, orzecznictwo w tych kwestiach jest skomplikowane i niejasne. Praktyka wskazuje na sprzeczności występujące w naszym prawie, np. instytucje żądające od przedsiębiorstw informacji na temat dochodów, zysków, strat czy też zobowiązań finansowych, żądają danych, które z całą pewnością są tajemnicami przedsiębiorstwa. Ich wyjście poza mury firmy może stać się w rękach konkurencji poważną bronią.

Ważny dla sprawy jest także wyrok Sądu Najwyższego z 2001 roku. SN uznaje w nim, że materiały uzyskane na zwykłej, dozwolonej drodze nie są objęte tajemnicą przedsiębiorstwa.

Warto wspomnieć też o ustawie z 29 grudnia 1997 roku o prawie bankowym. Artykuł 104 niniejszego aktu stanowi o zachowaniu tajemnicy bankowej, jej wyłączeniu oraz o penalizacji za naruszenie owej tajemnicy.

Trzeba również pamiętać, że państwo także jest uczestnikiem obrotu gospodarczego, dlatego wyróżnić możemy dane znaczące zarówno dla gospodarki jak i państwa. W ustawie o ochronie informacji niejawnych (art. 2 pkt. 1, 2) ustawodawca nakreśla nam wyjaśnienie pojęć takich jak: tajemnica państwowa oraz tajemnica służbowa.

Na koniec rozważań nad prawną regulacją wywiadu i szpiegostwa gospodarczego warto zwrócić uwagą na rozdział XXXIII Kodeksu Karnego z 6 czerwca 1997 r. Rozdział ten, poświęcony przestępstwom przeciwko ochronie informacji, przewiduje następujące sankcje karne:

Art. 265. § 1. Kto ujawnia lub wbrew przepisom ustawy wykorzystuje informacje stanowiące tajemnicę państwową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 2. Jeżeli informację określoną w § 1 ujawniono osobie działającej w imieniu lub na rzecz podmiotu zagranicznego, sprawca podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 3. Kto nieumyślnie ujawnia informację określoną w § 1, z którą zapoznał się w związku z pełnieniem funkcji publicznej lub otrzymanym upoważnieniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

[15] *Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji.*
[16] *Ibidem.*

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 stanowiącą tajemnicę służbową 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.

§ 3. Ściganie przestępstwa określonego w § 1 następuje na wniosek pokrzywdzonego. Art. 267. §1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. § 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.

§ 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

§ 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1-3 ujawnia innej osobie. § 5. Ściganie przestępstwa określonego w § 1-4 następuje na wniosek pokrzywdzonego[17].

PODSUMOWANIE

Posiadając przedsiębiorstwo należy pamiętać o zagrożeniu, jakim jest szpiegostwo gospodarcze. Warto już na początku działalności projektować system bezpieczeństwa. Nigdy jednak nie osiągniemy 100% pewności, ponieważ metody i techniki wykorzystywane przez agencje szpiegowskie wciąż ulegają zmianom.

Zagrożeniem dla naszych informacji poufnych są nie tylko nowoczesne technologię. Od zawsze głównym ogniwem działalności szpiegowskich jest człowiek. Nawet przy zastosowaniu najlepszych, najdroższych zabezpieczeń możemy stać się ofiarami szpiegostwa. Aby uzyskać interesujące informacje konkurencyjny podmiot jest w stanie wytypować, w jego przekonaniu, najsłabsze ogniwo w naszej firmie: począwszy od pracownika, po stojącą na biurku, nie wzbudzającą podejrzeń popielniczkę, w której ktoś umiesza podsłuch. Informacja w XXI wieku pojmowana jest jako towar, wart tyle, na ile jest przydatny. Agresywny i wymagający rynek powoduje, że coraz częściej podmioty gospodarcze funkcjonują na zasadzie: cel uświęca środki. Pomimo deklarowania uczciwej i etycznej konkurencji przeciwnik nie zawaha się, by zdobyć tajemnicę naszego przedsiębiorstwa.

[17] *Ustawa z dnia 6 czerwca 1997 r. Kodeks Karny* (Dz. U. 1997 Nr 88, poz. 553 ze zmianami).

BIBLIOGRAFIA:

1. Adamska M., *Leksykon zarządzania*, wyd. Difin, Warszawa 2004.
2. Gajos M., *Ochrona informacji niejawnych, biznesowych i danych osobowych*, Wolters Kluwer Polska-Lex, Katowice 2011.
3. Iwaszko B., *Ochrona informacji niejawnych w praktyce*, Prescom Sp. z o.o., Wrocław 2012
4. Kopaliński W., *Słownik wyrazów obcych i zwrotów obcojęzycznych*, Wiedza Powszechna, Warszawa 1975.
5. Kwieciński M., *Wywiad gospodarczy a konkurencyjność przedsiębiorstwa,* [w:] *System informacji strategicznej*, R. Borowiecki, M. Romanowska, wyd. Difin, Warszawa 2001.
6. Ryszkowski M. P., Ryszkowska M. U., Ryszkowska M. H., *O wybranych tajemnicach-bez tajemnic*, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych, Katowice 2011.
7. Sun Tzu, *Sztuka wojny*, wyd. Helion, Gliwice 2004.

Akty normatywne:

1. Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, Dz.U. 2003 Nr 153 poz. 1503.
2. Ustawa z dnia 6 czerwca 1997 r. Kodeks Karny, Dz. U. 1997 Nr 88, poz. 553 ze zmianami.

Orzecznictwo:

1. Wyrok NS z dn. 5 września 2001r., I CKN 1159/00.

Źródła internetowe:

1. (b.a.), *Wywiad a szpiegostwo gospodarcze* http://www.ipo.pl/ubezpieczenia_biznesowe/artykuly/wywiad_a__szpiegostwo_gospodarcze_592648.htm .
2. (b.a.), *Zagrożenia ze strony szpiegostwa gospodarczego,* http://www.iniejawna.pl/pomoce/szpieg.html.
3. P. Piejko, *Gadżety szpiegowskie dla każdego – TOP 10 http://*www.gadzetomania.pl/2010/09/17/gadzety-szpiegowskie-dlakazdego/keylogger-czyli-keykatch-usb/top [dostęp dn. 8.05.2013].
4. (b.a.), *Szpieg w firmie*, http:// www.mojafirma.infor.pl/e-firma/programy-dla-firm/214924,Szpieg-w-firmie.html.