AUTOR
mgr Piotr Idrian
pj-id56@o2.pl

ISTOTA, MIEJSCE I ROLA BEZPIECZEŃSTWA PRZEMYSŁOWEGO W SYSTEMIE OCHRONY INFORMACJI NIEJAWNYCH W POLSCE

Rozważania podjęte w niniejszym artykule na temat: *istoty, miejsca i roli bezpieczeństwa przemysłowego w systemie ochrony informacji niejawnych w Polsce*, oparte zostały na wiadomościach udostępnionych przez służby specjalne zajmujące się tą tematyka (Agencja Bezpieczeństwa Wewnętrznego i Służba Kontrwywiadu Wojskowego) z racji swojego powołania i poszczególnych przepisów zapisanych w ustawie. Podstawowym źródłem informacji były odpowiednie artykuły *Ustawy z dnia 5.08.2010 r. o ochronie informacji niejawnych* – głównego aktu prawnego traktującego o ochronie informacji niejawnych w aspekcie bezpieczeństwa przemysłowego. Dodatkowym wsparciem okazały się informacje zawarte w artykułach branżowych na stronach internetowych o podobnej tematyce.

Tematyka znaczenia informacji w aspekcie bezpieczeństwa przemysłowego jest sprawą istotną i ważną we współczesnym świecie. Sektor przemysłowy jest bardzo ważną dziedziną gospodarki każdego państwa, ponieważ jest on w dużej mierze podstawą danej gospodarki. Dlatego też organy państwa muszą chronić same strategiczne informacje w tej sferze i dostępu do nich przez niepowołane osoby. Wobec tego niektóre z tych informacji są chronione poprzez nadanie im odpowiednich klauzul poufności. Szczególnie wydarzenia ostatnich miesięcy dotyczące kryzysu ukraińskiego pokazały jak ważne jest bezpieczeństwo ekonomiczne oraz jak ono wpływa na stan bezpieczeństwa narodowego. Może bowiem powstać niebezpieczna sytuacja, w której ważne informacje dotyczące przemysłu zostaną wykorzystane jako bardzo poważne narzędzie w polityce międzynarodowej, co może powodować znaczne problemy w realizacji interesów narodowych przez dane państwo. W dzisiejszych czasach okazuje się, że równie silnym orężem w polityce międzynarodowej jest nie tylko potencjał militarny, lecz także przemysłowy, którego znaczenie cały czas wzrasta.

Rozpoczynając rozważania na wspomniany temat, należy na samym początku zdefiniować podstawowe pojęcia dotyczące istoty, miejsca i roli bezpieczeństwa przemysłowego w systemie ochrony informacji niejawnych w Polsce. Pojęciami tymi będą w pierwszej kolejności, „informacje niejawne" oraz „bezpieczeństwo przemysłowe".

Dla zapewnienia bezpieczeństwa każdego państwa jednym z pierwszych niezbędnych działań jest objęcie pewnych istotnych i ważnych dla funkcjonowania państwa informacji ograniczeniem dostępu i szczególnym nadzorem. W tym celu odpowiednie służby w państwie odpowiedzialne są za nadzór nad stworzonym systemem ochrony informacji niedostępnych dla każdego obywatela. Głównym aktem prawnym, który określa zasady i organizację systemu ochrony informacji niejawnych w Polsce jest ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, zwana dalej „ustawą", która zastąpiła regulację o takiej samej nazwie z 1999 roku.

Ustawa z dnia 5.08.2010 r. o ochronie informacji niejawnych definiuje **informacje niejawne** jako *informacje, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania*[1]. Wspomniana ustawa klasyfikuje te informacje według 4 rodzajów klauzul tajności. Klauzule te zaczynając od tych najbardziej poufnych to[2]:

- ściśle tajne;
- tajne;
- poufne;
- zastrzeżone.

Dostęp do wspomnianych informacji w zależności od ich klauzuli tajności obarczony jest pewnymi obostrzeniami. Obostrzenia te wyszczególnione są dokładnie w ustawie, natomiast z racji tego, że nie są przedmiotem tego artykułu nie będą omawiane.

Drugim podstawowym pojęciem, o którym wspomniano jest **bezpieczeństwo przemysłowe**. Rozdział 9. wspomnianej Ustawy poświecony jest w całości temu zagadnieniu. Jak możemy się dowiedzieć *bezpieczeństwo przemysłowe to wszelkie działania związane z zapewnieniem ochrony informacji niejawnych udostępnianych przedsiębiorcy w związku z umową lub zadaniem wykonywanym na podstawie przepisów prawa*[3]. Na koniec warto również wspomnieć o pojęciu przedsiębiorcy, ponieważ to do jego osoby kierowane jest świadectwo bezpieczeństwa, o którym będzie mowa później. Przedsiębiorcą – *jest przedsiębiorca w rozumieniu art. 4 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz. U. z 2007 r. Nr 155, poz. 1095, z póz. zm.) lub każda inna jednostka organizacyjna, niezależnie od formy własności, którzy w ramach prowadzonej działalności gospodarczej zamierzają realizować lub realizują związane z dostępem do informacji niejawnych umowy lub zadania wynikające*

[1] Ustawa z dnia 5.08.2010r. o ochronie informacji niejawnych, art. 1, ust. 1, (Dz. U. 2010. 182.1228).

[2] Por., tamże, art. 1, ust. 1-5.

[3] www.bip.abw.gov.pl/palm/bip/73/148/BEZPIECZENSTWO_PRZEMYSLOWE.html, [dostęp: 22.05.2013].

z przepisów prawa[4]. Jak wynika z powyższych informacji, to właśnie przedsiębiorcy są adresatami działań związanych z bezpieczeństwem przemysłowym, ponieważ to przedsiębiorcy prowadzący określone działania biznesowe mogą działać w branżach, w których pewne informacje mogą być istotne z punktu widzenia bezpieczeństwa państwa. Warto zaznaczyć, że oprócz osób fizycznych mogą to być także osoby prawne[5].

Podstawowym dokumentem umożliwiającym dostęp przedsiębiorcy do informacji niejawnych z obszaru przemysłu jest **świadectwo bezpieczeństwa przemysłowego**. Daje ono dostęp do informacji o klauzuli „poufne" lub wyższej. Świadectwo takie wydawane jest na wniosek przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego, po wykonaniu odpowiedniego postępowania. Ważne jest, że każdy ubiegający się musi obligatoryjnie *mieć zdolność do ochrony informacji niejawnych*[6]. W zależności od stopnia klauzuli poufności wydawane są świadectwa odpowiedniego stopnia[7]:

- pierwszego stopnia – potwierdzające pełną zdolność przedsiębiorcy do ochrony tych informacji;
- drugiego stopnia – potwierdzające zdolność przedsiębiorcy do ochrony tych informacji, z wyłączeniem możliwości ich przetwarzania we własnych systemach teleinformatycznych;
- trzeciego stopnia – potwierdzające zdolność przedsiębiorcy do ochrony tych informacji, z wyłączeniem możliwości ich przetwarzania w użytkowanych przez niego obiektach.

Świadectwa potwierdzające zdolność do ochrony informacji niejawnych wydawane są na odpowiedni czas ważności tego zezwolenia w zależności od stopnia klauzuli poufności, o którą występuje wnioskodawca. Podział ten został zaprezentowany w tabeli 1.

Wygaśnięcie ważności świadectwa następuje w przypadku, kiedy: upłynął okres jego ważności (por. tabela 1.); przedsiębiorca zrzekł się uprawnień określonych w świadectwie; przedsiębiorca został przejęty przez inny podmiot lub zlikwidowany[8].

[4] Ustawa…, wyd. cyt., art. 2, ust. 13.
[5] Por., tamże, art. 2, ust. 14, pojecie kierownika przedsiębiorcy.
[6] Tamże, art. 54, ust. 1.
[7] Tamże, art. 55, ust. 1.
[8] Por., definicja przedsiębiorcy.

Tabela 1.

Świadectwo potwierdzające zdolność do ochrony informacji niejawnych

Klauzula	Czas trwania
„Ściśle tajne"	„ściśle tajne" – przez okres 5 lat od daty wystawienia „tajne" – przez okres 7 lat od daty wystawienia „poufne" – przez okres 10 lat od daty wystawienia
„Tajne"	„tajne" – przez okres 7 lat od daty wystawienia „poufne" – przez okres 10 lat od daty wystawienia
„Poufne"	„poufne" – okres 10 lat od daty wystawienia

Źródło: Opracowane własne na podstawie: art. 2, ust. 3, (Dz.U.2010.182.1228).

Postępowanie rozpoczyna się na wniosek wnioskodawcy i, co istotne, wniosek ten nie musi być uzasadniony. Natomiast musi zawierać stopień świadectwa oraz klauzulę tajności informacji niejawnych, których zdolność do ochrony ma potwierdzać świadectwo. Do wniosku dołącza się też odpowiedni kwestionariusz, tzw. kwestionariusz bezpieczeństwa przemysłowego, oraz ankiety lub kopie poświadczeń bezpieczeństwa osób (kierownika przedsiębiorcy, pełnomocnika ochrony i jego zastępcy, osób zatrudnionych w pionie ochrony administratora systemu teleinformatycznego oraz pozostałych osób, które powinny mieć dostęp do informacji niejawnych). Służby ABW i SKW sprawdzają w dostępnych sobie źródłach informacji wszelkie dane niezbędne do ustalenia kwestii związanych z[9]:

- strukturą kapitału oraz powiązaniami kapitałowymi przedsiębiorcy, źródłami pochodzenia środków finansowych i sytuacją finansową;
- strukturą organizacyjną;
- systemem ochrony informacji niejawnych, w tym środkami bezpieczeństwa fizycznego;
- wszystkimi osobami wchodzącymi w skład organów zarządzających, kontrolnych oraz osobami działającymi z ich upoważnienia.

Służby kontrolne mają za zadanie w ciągu 6 miesięcy od dnia dostarczenia wszystkich wymaganych dokumentów zakończyć postępowania. *Postępowanie bezpieczeństwa przemysłowego kończy się wydaniem przez ABW albo SKW świadectwa zgodnie z wnioskiem przedsiębiorcy albo decyzją o odmowie wydania świadectwa lub decyzją o umorzeniu postępowania bezpieczeństwa przemysłowego*[10]*.* W przypadku stwierdzenia braku zdolności do ochrony informacji niejawnych AWB lub SKW zawiadamia o odmownym i negatywnym przebiegu postępowania. Dzieje się tak, gdy weryfikatorzy stwierdzą, że osoby, które zajmują stanowisko kierownika przedsiębiorcy, nie mogą otrzymać poświadczenia bezpieczeństwa; nie można ustalić struktury kapitałowej i źródeł pochodzenia środków

[9] Tamże, art. 57, ust. 2.
[10] Tamże, art. 64, ust. 1.

finansowych; wnioskodawca nie zorganizował w ciągu 6 miesięcy systemu ochrony informacji niejawnych; gdy zatajono dane w kwestionariuszu lub podano nieprawdziwe informacje o zmianach danych zawartych w kwestionariuszu. Brak wydania świadectwa może zdarzyć się także w momencie niewyeliminowania nieprawidłowości w toku postępowania sprawdzającego.

Wielce istotną rzeczą jest też fakt, że przedsiębiorca w trakcie otrzymywania świadectwa bezpieczeństwa przemysłowego oraz po jego otrzymaniu ma obowiązek informowania w terminie 30 dni ograny o powstałych zmianach związanych z[11]:

- zmianą danych zawartych w kwestionariuszu, ogłoszeniu upadłości, likwidacji lub rozwiązaniu jednostki organizacyjnej albo innej formie zakończenia przez nią działalności, wypowiedzeniu umowy oraz zakończeniu wykonywania umowy;
- zawarciem umowy związanej z dostępem do informacji niejawnych o klauzuli „poufne" lub wyższej;
- zawarciem umowy z podwykonawcą, związanej z dostępem do informacji niejawnych o klauzuli „poufne" lub wyższej, wypowiedzeniu tej umowy;
- zmianami w systemie ochrony informacji niejawnych;
- zmianami osób wykonujących umowę;
- potrzebą zawarcia z podwykonawcą umowy związanej z dostępem do informacji niejawnych.

Wspomniany wcześniej 6 miesięczny okres na wprowadzenie systemu ochrony informacji niejawnych wiąże się ze sporządzeniem instrukcji bezpieczeństwa przemysłowego. Zadanie to jest kolejnym obowiązkiem wnioskodawcy, a sama instrukcja powinna zawierać szczegółowe wymagania dotyczące ochrony informacji niejawnych o klauzuli „poufne" lub wyższej, które zostaną przekazane przedsiębiorcy w związku z wykonywaniem umowy, a także skutki oraz zakres odpowiedzialności wykonawcy umowy z tytułu niewykonania lub nienależytego wykonania obowiązków wynikających z niniejszej ustawy i nieprzestrzegania wymagań określonych w instrukcji bezpieczeństwa przemysłowego. Instrukcja bezpieczeństwa przemysłowego powinna określać w szczególności: klauzule tajności poszczególnych materiałów lub rodzajów materiałów, które zostaną wytworzone przez przedsiębiorcę w związku z wykonywaniem umowy i sposób postępowania z materiałami niejawnymi, które zostaną przekazane przedsiębiorcy lub przez niego wytworzone w związku z wykonywaniem umowy.

Jak można stwierdzić, wnioskodawca ubiegający się o wydanie świadectwa bezpieczeństwa przemysłowego musi spełnić wiele, często rygorystycznych warunków. Nawet po otrzymaniu świadectwa obowiązki te nie

[11] Por., tamże, art. 70, ust, 1-2.

zmniejszają się. Nie trzeba się temu dziwić, ponieważ delikatność i ranga informacji niejawnych o charakterze przemysłowym ma duże znaczenie dla bezpieczeństwa gospodarczo-ekonomicznego państwa. Przedsiębiorcy (jednostki), które ubiegają się o taki dostęp muszą być tutaj w 100% wiarygodni i pewni, a informacje im powierzone – szczelnie chronione przed dostaniem się w niepowołane ręce.

Po dokonaniu analizy trybu otrzymywania świadectwa bezpieczeństwa przemysłowego można stwierdzić, że świadectwo bezpieczeństwa przemysłowego jest dokumentem potwierdzającym zdolność przedsiębiorcy do zapewnienia ochrony informacji niejawnych przed nieuprawnionym ujawnieniem w związku z realizacją umów lub zadań[12]. Jeżeli więc przedsiębiorca chce wykonywać jakieś prace na rzecz państwa (np. ministerstw, policji), a praca związana jest z dostępem do informacji niejawnych oznaczonych klauzulą „poufne", „tajne" lub „ściśle tajne", przedsiębiorca zobligowany jest posiadać odpowiednie świadectwo bezpieczeństwa przemysłowego. Nie dotyczy to jednak osób fizycznych, które prowadzą działalność gospodarczą jednoosobowo i osobiście, osobom takim wystarcza jedynie posiadanie odpowiedniego poświadczenia bezpieczeństwa. Wszędzie tam, gdzie istnieje styczność z informacjami niejawnymi, pojawia się konieczność posiadania świadectwa bezpieczeństwa. Zasada ta odnosi się zarówno dla umów kontraktów krajowych, jak i zagranicznych, (np. na rzecz NATO lub Unii Europejskiej). Z racji tego, że umowy te są z reguły wysoko dochodowe i prestiżowe, to w gestii przedsiębiorcy leży decyzja, czy warto podejmować ryzyko poddania swojej firmy gruntownemu prześwietleniu przez służby ochrony państwa i poniesienia kosztów związanych z przystosowaniem do przetwarzania informacji niejawnych. Przedsiębiorca – to ktoś, kto wykorzystuje najlepiej to, czego wszyscy mają po równo, czyli czas.

Przedstawiona w niniejszym artykule tematyka miała za zadanie określić istotę bezpieczeństwa przemysłowego, określić jej miejsce i rolę w systemie ochrony informacji niejawnych. Jak wynika z analizy przytoczonych treści aspekty bezpieczeństwa przemysłowego odgrywają istotną rolę w systemie ochrony informacji niejawnych. W dzisiejszej gospodarce przedsiębiorstwa prywatne są bardzo istotnymi podmiotami na rynku. Czasy, kiedy przemysłem zajmowały się przedsiębiorstwa państwowe już dawno minęły, a ich miejsce zajęły podmioty prywatne. Otrzymały tym samym dostęp do wrażliwych informacji z sektorów, w których prowadzą swoją działalność gospodarczą. Dlatego też ochrona informacji niejawnych polega na strzeżeniu, aby istotne dla państwa informacje nie dostały się w niepowołane ręce. Toteż przedsiębiorstwa świadczące usługi na rzecz

[12] www.bezpieczneit.com/dane_osobowe_informacje_niejawne/swiadectwo-bezpieczenstwa-przemyslowego-jak-uzyskac/, [dostęp: 22.03.2014].

państwa muszą być pod szczególną ochroną i być w pełni wiarygodne. Tam gdzie dokonują się interesy państwa, zaczyna się też chęć poznania, niekiedy strategicznych działań Polski przez inne państwa i ich służby specjalne. Restrykcyjny proces pozwalający na uczestniczenie w działalności gospodarczo − przemysłowej innym przedsiębiorcom jest jak najbardziej zasadny. Dlatego umiejscowienie pozycji bezpieczeństwa przemysłowego i aspektów z tym związanych w *Ustawie o ochronie informacji niejawnych*[13] jest bez wątpienia bardzo dobrym krokiem do polepszenia bezpieczeństwa państwa jako całości.

Według klasyka wojnę definiowano jako narzędzie realizacji polityki państwa. Można zatem użyć (być może zbyt śmiałego) stwierdzenia, że jak kiedyś narzędziem takiej polityki były czołgi i armaty, tak teraz są to surowce i energia.

Bibliografia

1. Ustawa z dnia 5.08.2010 r. o ochronie informacji niejawnych, (Dz.U. 2010.182.1228).
2. www.abw.gov.pl.
3. www.bezpieczneit.com.
4. www.bossg.eu.
5. www.iniejawna.pl.
6. www.ochronainformacji.com.pl.
7. www.skw.gov.pl.

ABSTRACT
ESSENCE, PLACE AND ROLE OF INDUSTRIAL SAFETY AND SECURITY IN THE SYSTEM OF CLASSIFIED INFORMATION PROTECTION IN POLAND

The subject matter presented in the article is to define the essence of industrial security and safety, its place and role in the system of classified information protection. The author's analysis shows that industrial security and safety aspects play a vital role in the system of classified information protection. In a modern economy, private companies are very important entities on the market. The times when only state companies dealt with industry are gone and they have been replaced by private companies who,

[13] Rozdział 9, art. 54-71 Ustawy z dnia 5.08.2010 r. o ochronie informacji niejawnych, (Dz.U.2010.182.1228).

in this way, gained access to sensitive information in industries where they have placed their business. Therefore, classified information protection consists in guarding so as essential information for the state would not be intercepted by unauthorized persons. Thus companies rendering services for the state should be specially protected and be fully reliable.