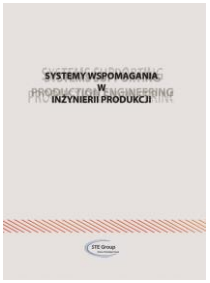
Po co przedsiębiorcy tajemnica przedsiębiorstwa?

Data wpłynięcia do Redakcji: 03/2022
Data akceptacji przez Redakcję do publikacji: 06/2022

2022, volume 11, issue 1, pp. 1-9



Marzena Smolarska
FAMUR S.A. **Polska**

Streszczenie: W artykule przedstawiono jak należy rozumieć tajemnicę przedsiębiorstwa i jakie korzyści płyną z jej wdrożenia. Jakie wymogi musi spełniać informacja żeby mogła być chroniona tajemnicą przedsiębiorstwa. Zdefiniowano również główne obszary, które musi wziąć pod uwagę przedsiębiorca decydując się na rozwiązania związane z bezpieczeństwem informacji. Jak istotny jest człowiek w procesie oraz monitoring wdrożonych rozwiązań prawnych, organizacyjnych i technicznych. Przedstawiono również kierunki prawidłowego zarządzania informacjami szczególnie ważnymi dla organizacji. Wskazano obszary monitoringu wdrożonych rozwiązań takich jak audyt, klasyfikacja informacji czy analiza ryzyka. W artykule przedstawiono również obszary które warto objąć wewnętrznymi regulacjami tajemnicy przedsiębiorstwa. Przeanalizowano co przede wszystkim stanowi o bezpieczeństwie aktywów w przedsiębiorstwie. Zwrócono również uwagę na konieczność odpowiedniego zarządzania informacjami stanowiącymi tajemnicę przedsiębiorstwa i co to oznacza w praktyce funkcjonowania organizacji. Jak ogromne znaczenie ma ciągły monitoring zastosowanych środków bezpieczeństwa poprzez cykliczne audyty i analizę ryzyka.

Słowa kluczowe: audyt, analiza ryzyka, bezpieczeństwo, informacja, integralność, dostępność, poufność, przedsiębiorca, tajemnica przedsiębiorstwa

WPROWADZENIE

Informacje stanowią dla firmy szczególną wartość, dlatego prowadząc działalność gospodarczą, wymieniając się informacjami, czy to wewnątrz firmy jak i udostępniając informacje na zewnątrz dostrzec należy konieczność zapewnienia im maksymalnej ochrony. Odpowiednie zabezpieczenie informacji ważnych dla przedsiębiorstwa wiążących się z technologią, techniką czy organizacją ma kluczowe znaczenie dla działalności biznesowej i utrzymania przewagi nad konkurencją. Nie każda informacja może być zaliczana do tajemnicy przedsiębiorstwa, chociaż byłaby bardzo cenna. Jej cechy określa ustawa z dnia 16 kwietnia 1993 roku o zwalczaniu nieuczciwej konkurencji, a dokładnie art. 11 ust. 2 tej ustawy. Warto podkreślić, że definicja, która znana była do tej pory w polskim porządku prawnym uległa zmianie ze względu na przeprowadzoną implementację Dyrektywy Parlamentu Europejskiego i Rady UE nr 2016/943 z dnia 8 czerwca 2016 roku w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem,

Contact address: msmolarska@famur.com

wykorzystywaniem i ujawnianiem [1]. Od 4 września 2018 roku mamy nową definicję tajemnicy przedsiębiorstwa.

I tak zgodnie z treścią artykułu 11 ust. 2 ustawy o zwalczaniu nieuczciwej konkurencji przez tajemnice przedsiębiorstwa należy rozumieć informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje, które to mają wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są one łatwo dostępne dla takich osób, o ile osoba uprawniona do korzystania z informacji lub rozporządzania nimi podjęła, przy zachowaniu należytej staranności, działania w celu utrzymania tych informacji w poufności [2].

Informacja, którą można objąć tajemnicą, musi mieć określoną wartość dla przedsiębiorstwa i spełniać wszystkie ustawowe wymogi, czyli: jest to informacja techniczna, technologiczna, organizacyjna przedsiębiorstwa, posiadająca wartość gospodarczą, ekonomiczną,

- nie może być powszechnie znana, jak również oczywista dla osób pracujących w tej samej branży, czy mających kontakt z tego typu informacjami na co dzień [1],
- przedsiębiorca podjął niezbędne działania, które pozwolą mu utrzymać daną informacje w tajemnicy.

Jeżeli te cechy nie są spełnione łącznie, dana informacja nie może stanowić tajemnicy przedsiębiorstwa i każdy może z niej korzystać. W dobrze pojętym interesie przedsiębiorcy jest ustalenie, jakiego rodzaju informacje mogłyby stanowić tajemnicę przedsiębiorstwa, doprowadzenie tej informacji do pracowników w formie oświadczenia woli, stworzenia systemu nadzoru i kontroli przez przedsiębiorcę i w końcu – pełna kontrola, czy tajemnica przedsiębiorstwa w jednostce jest przestrzegana. Przestrzeganie tajemnicy przedsiębiorstwa jest ważne nie tylko na niwie samej firmy, ale także, a może przede wszystkim w kontaktach zewnętrznych pracowników z innymi podmiotami, kontrahentami, zleceniodawcami.

CZŁOWIEK – NAJWAŻNIEJSZE AKTYWO, NAJSŁABSZE OGNIWO

Najsłabszym ogniwem, a jednocześnie najważniejszym jest człowiek. To on tworzy różnego rodzaju zabezpieczenia, systemy ochrony, bez niego nic się nie dzieje. A dlaczego słabym? Posiadł określoną wiedzę, umie ją wykorzystać. Ma informacje na temat mankamentów i niedociągnięć systemu, gdzie znajdują się cenne zbiory informacyjne przedsiębiorstwa. Zmieniając pracę może tą wiedzą dowolnie dysponować. Dlatego tak ważna jest kontrola i wnikliwy dobór pracowników. Pracowników, którzy daliby „rękojmię zachowania tajemnicy". Polskie prawo zwraca na to uwagę w ustawie o ochronie informacji niejawnych (Dz. U. 1999 Nr 11 z późn. zmianami). Reasumując, każdy kto posiadł tajemnicę przedsiębiorstwa, zobowiązany jest zachować ją w poufności. Istotnym bowiem jest, aby wola przedsiębiorcy, co do zachowania informacji w poufności została sprecyzowana w

sposób jednoznaczny. Bardzo ważne jest, aby pracownik miał świadomość powagi sytuacji i ciążącej na nim odpowiedzialności za ochronę informacji stanowiących tajemnicę przedsiębiorstwa w firmie, której pracuje. Niezbędna tez jest wiedza, że ciężkim naruszeniem podstawowych obowiązków pracowniczych może być czyn nieuczciwej konkurencji, związany z nieuprawnionym ujawnieniem tajemnicy przedsiębiorstwa lub nieuprawnionym wykorzystaniem informacji biznesowych, a także sprowadzenie realnego niebezpieczeństwa takiego zdarzenia.

Wartość rynkowa przedsiębiorstwa uzależniona jest w dużej mierze od wartości znajdujących posiadanych przez firmę informacji, które wykorzystywane są w działalności produkcyjnej, usługowej, marketingowej, badawczo–rozwojowej, ekonomicznej. Ważnym więc jest, aby te wszystkie newralgiczne informacje odpowiednio zabezpieczyć i chronić [3]. Tajemnica przedsiębiorstwa może ustrzec zarządzających przedsiębiorstwem przed ewentualnymi nadużyciami lub naruszeniami, a przede wszystkim przed szkodami finansowymi. Bezpieczeństwo informacji jest integralnym elementem procesu zarządzania organizacją. Zarządzanie bezpieczeństwem informacji powinno być dla kierownictwa zagadnieniem strategicznym, priorytetowym [3].

Wobec zaostrzającej się walki konkurencyjnej w niemal wszystkich dziedzinach działalności gospodarczej, problem ochrony informacji nabiera szczególnego znaczenia [4]. Dlatego tak ważną wydaje się być problematyka określenia, jakie informacje mogłyby wejść do kanonu informacji szczególnie wrażliwych, spełniających wymogi informacji stanowiących tajemnicę przedsiębiorstwa. Jakie obszary warto objąć wewnętrznym prawem tajemnicy przedsiębiorstwa?

- sprzedaż – baza klientów, informacje dotyczące osób decyzyjnych u klientów, ceny transakcyjne, cenniki, terminy obowiązywania lub odnawiania umów, potrzeby klientów, np. w zakresie asortymentu, oprogramowania, obsługi itp., otrzymane zapytania ofertowe, złożone oferty, prowadzenia negocjacji i ich przebieg, procedury i instrukcje sprzedażowe, realizacja sprzedaży, informacje w procesie przetargowym w postepowaniu nie objętym ustawa o zamówieniach publicznych;
- marketing – 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, informacje o wynagrodzeniach pracowników;
- kontrola – informacje o wadliwościach poszczególnych produktów, zgłaszanych reklamacjach, procedury kontroli jakości;
- produkcja – informacja koszt-cena, dane dotyczące dostawców, stosowane receptury, przepisy, metody produkcji, procedury, know-how, procesy technologiczne, dokumentacja konstrukcyjna, innowacyjne projekty

strategiczne, parametry technologii, uzyskane wyniki doświadczeń (prototypy), statystyki jakościowe;
- badania i rozwój – plany rozwoju, kierunki rozwoju, wynalazki przed zgłoszeniem wniosku patentowego, wyniki badań, wyniki poszukiwań nowych produktów lub usług, know-how w zakresie badań i rozwoju;
- informacje finansowe – wewnętrzne dokumenty finansowe, budżety realizowanych kontraktów, prognozy, raporty, nieujawniane rachunki zysków i strat, sprawozdania finansowe, dokumentacja księgowa;
- zakupy i logistyka – zbieranie i analiza ofert, reklamacje, wskaźniki dotyczące jakości kupowanego sprzedawanego towaru;
- relacje inwestorskie – obowiązkowe sprawozdania finansowe przed ujawnieniem;
- wewnętrzne informacje o firmie – sposób organizacji pracy, biznes plany, plany strategiczne, dokumenty korporacyjne;
- IT – oprogramowanie stosowane przez firmę, informacje związane z technologicznymi i technicznymi aspektami realizacji usługi IT, rozwój systemów informatycznych, repozytoria danych uwierzytelniających.

Informacje stanowiące tajemnice przedsiębiorstwa mogą występować w każdym obszarze działalności firmy a ich lista jest nieograniczona i ma charakter otwarty.

MĄDRY PRZEDSIĘBIORCA PO SZKODZIE

Do właściwego zabezpieczenia tajemnicy przedsiębiorstwa przekonuje się coraz więcej firm. Bardzo często po powstaniu szkody. Istotnym jest, by przekonać przedsiębiorcę, że nakłady na ochronę informacji są zawsze opłacalne. Nie tylko chronią przed niekontrolowanym wypływem informacji, ale podnoszą wartość przedsiębiorstwa i skuteczność dochodzenia ewentualnych roszczeń czy odszkodowań [5].

Tajemnica przedsiębiorstwa to sposób na ochronę informacji, które nie podlegają ochronie prawa własności przemysłowej. Patenty i znaki towarowe powodują rodzaj ochrony, który nie wymaga utrzymania rozwiązań w poufności. Czyli tajemnica przedsiębiorstwa jest to zbiór informacji, które przedsiębiorca chcąc chronić – musi samodzielnie podjąć środki techniczne i organizacyjne celem zachowania poufności, bo tylko poufność pozwoli na ochronę tej wiedzy. Należy zwrócić uwagę, że bezpieczeństwo informacji powinno zapewnić przetwarzanym informacjom nie tylko poufność ale i integralność oraz dostępność informacji.

O poufności informacji mówimy wtedy gdy jest ona dostępna tylko tym użytkownikom, którzy otrzymali odpowiednie uprawnienia. Integralność informacji to jej kompletność i wiarygodność oraz zapewnienie, że informacja nie została zmieniona w sposób niekontrolowany. Dostępność to swobodny dostęp do informacji wtedy kiedy jest potrzebna.

Wdrażając wewnętrzne regulacje chroniące informacje przedsiębiorca zabezpiecza realizację istotnych procesów w organizacji, minimalizuje straty finansowe oraz ryzyko utraty reputacji i zaufania u klientów. Tajemnica

przedsiębiorstwa pomaga poukładać procesy w firmie i ograniczyć koszty związane z przerwami w działalności oraz zabezpieczyć ciągłości działania organizacji.

Bezpieczeństwo aktywów informacyjnych w przedsiębiorstwie to przede wszystkim:

- ludzie, czyli kim jesteśmy – akcjonariusze, właściciele, kadra zarządzająca, pracownicy, dostawcy usług, kontrahenci, prawnicy, współpracownicy;
- procesy, czyli co robimy – system pomocy dla użytkowników (Help Desk), zarządzanie dostępem do usług, raportowanie incydentów i zarządzanie nimi, zarządzanie dostępem, zarządzanie tożsamością, kontrola spełnienia wymagań prawnych, szkolenia;
- technologie, czyli czego używamy w tym – oprogramowanie, systemy operacyjne, programy komunikacyjne, użytkowe;
- urządzenia dostępowe – komputery PC, Notebooki, Smarfony, terminale, stacje sieciowe, stacje WWW, infokioski aparaty cyfrowe, drukarki, skanery, kopiarki;
- zabezpieczenia fizyczne – elektroniczne systemy dostępu, klucze, karty, czytniki biometryczne, kamery monitorujące;
- zabezpieczenia środowiskowe – systemy p-poż, wentylacja, klimatyzacja, zasilanie awaryjne/.

Aktualnie w podmiotach gospodarczych, jak i w skali całej gospodarki, zaobserwować można zjawisko nadawania większej rangi problemom związanym z tworzeniem efektywnych systemów zarządzania bezpieczeństwem informacji. Jedna z podstawowych zasad leżących u podstaw budowy systemu zarządzania bezpieczeństwa informacji jest zasada podporządkowania środków ochrony wartości informacji. To wartość informacji decyduje, czy i jakie powinny być stosowane środki jej ochrony. Im wyższa wartość informacji, tym wyższa powinna być skuteczność środków ochrony [3]. W przypadku, gdy przedsiębiorca zdecyduje, że firma, którą kieruje, posiada informacje stanowiące tajemnicę przedsiębiorstwa, koniecznym staje się wprowadzić pewne regulacje.

W tym momencie należy zwrócić uwagę na jeszcze jeden ważny aspekt zachowania tajemnicy przedsiębiorstwa, a mianowicie na pouczenie pracownika lub osoby współpracującej o poufnym charakterze informacji dotyczących, np. zasad obsługi urządzenia, struktury organizacyjnej spółki, organizacji rynków zbytu itp. i odebrania od zatrudnionych oświadczeń o zachowaniu poufności. Istotnym bowiem jest, aby wola przedsiębiorcy, co do zachowania tych wiadomości w poufności została sprecyzowana w sposób jednoznaczny. Bardzo ważne jest, aby pracownik miał świadomość powagi sytuacji i ciążącej na nim odpowiedzialności za ochronę informacji stanowiących tajemnicę przedsiębiorstwa w firmie, której pracuje. Niezbędna też jest wiedza, że ciężkim naruszeniem podstawowych obowiązków pracowniczych może być czyn nieuczciwej konkurencji, związany z nieuprawnionym ujawnieniem tajemnicy przedsiębiorstwa lub nieuprawnionym wykorzystaniem informacji biznesowych, a także sprowadzenie realnego

niebezpieczeństwa takiego zdarzenia. Zasadnym więc jest podpisanie oświadczenia przez pracownika, w którym udokumentowane jest, że nie przestrzeganie tajemnicy przedsiębiorstwa jest ciężkim naruszeniem podstawowych obowiązków pracowniczych i grozi za to odpowiedzialność karna. Odpowiednie zabezpieczenie informacji stanowiących tajemnicę przedsiębiorstwa obliguje przedsiębiorcę do precyzyjnego określenia i przestrzegania procedur dotyczących organizacji ochrony tych informacji, zwłaszcza osób odpowiedzialnych za przedmiotowe zagadnienia, dopuszczanie pracowników do informacji chronionych po uprzednim przeszkoleniu i podpisaniu stosownych oświadczeń poufności, zminimalizowaniu liczby osób mających dostęp do poszczególnych informacji, właściwej organizacji obiegu dokumentów, rejestrowania i uważnej dekretacji korespondencji, wykonywania kopii dokumentów oraz ich dystrybucji, archiwizacji i niszczenia. Niezwykle istotne jest określenie zasad postępowania w przypadku wystąpienia incydentów bezpieczeństwa informacji spowodowanych utratą dokumentów lub ujawnienia informacji chronionych. Najistotniejszym elementem ochrony informacji i wdrożonych zabezpieczeń wydaje się być cykliczne szkole pracowników i kontrola wewnętrzna wdrożonych zabezpieczeń.

MONITORING I DOSKONALENIE OCHRONY

Żaden system ochrony informacji nie działa efektywnie, jeżeli nie jest na bieżąco sprawdzany i monitorowany. Zachowanie poufności, integralności i dostępności informacji coraz częściej zaczyna odgrywać strategiczną rolę w funkcjonowaniu organizacji. Dlatego ogromnie ważne stają się dobrze opracowane procedury bezpieczeństwa, które są niezbędne do prawidłowego funkcjonowania firmy, a tym samym ułatwiające stały proces monitoringu i kontroli. Istotnym elementem jest również odpowiednie zarządzanie informacjami stanowiącymi tajemnicę przedsiębiorstwa, co w praktyce oznacza:

- identyfikowanie oraz ochronę zasobów informacyjnych przedsiębiorstwa oraz środków służących do ich przetwarzania;
- zapewnienie bezpieczeństwa i ciągłości działania przetwarzanych informacji;
- zarządzanie ryzykiem obowiązującym w przedsiębiorstwie poprzez identyfikacje zasobów informacyjnych, zagrożeń z nimi związanych i wyborem działań zabezpieczających informacje stanowiące tajemnicę przedsiębiorstwa;
- analizę wprowadzonych zmian i ich wpływu na bezpieczeństwo informacji w firmie.

Główny ciężar nadzoru nad prawidłową ochrona tajemnicy przedsiębiorstwa nałożony jest na kadrę kierowniczą wewnętrznych komórek organizacyjnych przedsiębiorstwa, której obowiązkiem nadzorczym jest dopilnowanie, by podlegli jej pracownicy działali zgodnie z zasadami bezpieczeństwa informacji, jakie zostały przyjęte w firmie. Kadra ta zobowiązana jest również podejmować działania dyscyplinujące, organizacyjne i szkoleniowe, ukierunkowane na eliminowanie

pojawiania się naruszeń przez podległych pracowników zasad ochrony informacji stanowiących tajemnicę przedsiębiorstwa [6].

Formą działania monitoringu ochrony informacji stanowiących tajemnicę przedsiębiorstwa jest audyt. Wyniki audytu powinny być przedstawione zarządowi danej spółki. W przypadku nieuprawnionego ujawnienia bądź naruszenia tajemnicy przedsiębiorstwa, czy też sprowadzenie realnego niebezpieczeństwa takiego ujawnienia warto powołać zespół, który ocenia, jak owo zdarzenie wyczerpuje znamiona ciężkiego naruszenia obowiązków pracowniczych, czy też nie. Zespół sporządza notatkę, która przedstawia ocenę zdarzenia wraz z wnioskiem dotyczącym dalszego postępowania. Ma to na celu wyeliminować tego rodzaju zdarzenia w przyszłości. Notatkę przedstawia się zarządowi, który podejmuje decyzję o zastosowaniu trybu rozwiązania stosunku pracy lub nie. Wydaje decyzję modernizacji systemu ochrony przedsiębiorstwa, która ma wyeliminować pojawienie się tego typu zdarzeń.

W monitoringu i doskonaleniu tajemnicy przedsiębiorstwa ważna jest również okresowa weryfikacja wykazu rodzajów informacji stanowiących tajemnicę przedsiębiorstwa i zgłoszenie ewentualnych zmian do prezesa zarządu. Prawidłowa weryfikacja i analiza informacji wymaga wprowadzenia procedury, która definiuje cel i zakres stosowania, określa role i zadania w procesie klasyfikacji informacji oraz reguluje opis postępowania. Zastosowanie odpowiedniego narzędzia spowoduje że klasyfikacja informacji stanie się procesem powtarzalnym i ustandaryzowanym w przedsiębiorstwie. Ponadto należy pamiętać, że celem klasyfikacji informacji jest przeanalizowanie wszystkich zidentyfikowanych i przetwarzanych informacji w firmie pod względem poufności, integralności i dostępności dla zastosowania właściwych mechanizmów ochrony, adekwatnych do potrzeb biznesowych przedsiębiorstwa.

Monitoring tajemnicy przedsiębiorstwa w obszarze adekwatnych zabezpieczeń prawnych, organizacyjnych i technicznych nie może odbywać się bez analizy ryzyka, której celem jest:

- zapewnienie, iż wszystkie informacje oraz istotne ryzyka bezpieczeństwa tych informacji identyfikowane i analizowane są na bieżąco;
- zapewnienie, iż w miarę potrzeb są opracowywane i wdrażane odpowiednie plany działań wobec ryzyka bezpieczeństwa informacji;
- zapewnienie powtarzalności i porównywalności wyników oceny analizy ryzyka bezpieczeństwa informacji;
- uwzględnienie funkcjonujących mechanizmów kontrolnych, przy ocenie ryzyka bezpieczeństwa informacji;
- precyzyjne określenie odpowiedzialności związanych z zarządzaniem poszczególnymi obszarami ryzyka bezpieczeństwa informacji.

W analizie ryzyka należy przede wszystkim zidentyfikować aktywa i ustanowić kontekst w jakim działa organizacja. Ponadto koniecznym jest wyszukanie i rozpoznanie ryzyk które zagrażałyby bezpieczeństwu informacji oraz zidentyfikowanie szans, czyli pozytywnych zjawisk i tendencji w otoczeniu firmy,

które jeżeli zostaną właściwie wykorzystane, wspomogą rozwój organizacji lub osłabią zagrożenia.

PODSUMOWANIE

Powszechność informacji, które mogą stanowić tajemnicę przedsiębiorstwa, dowodzi doniosłości tej problematyki. Każda jednostka organizacyjna w swojej strukturze, działalności i kierunkach rozwoju posiada informacje, które stanowią jej tajemnice. Jeżeli nie są one odpowiednio chronione, może dojść do ich ujawnienia [3]. Jeżeli przedsiębiorstwo nie potrafi chronić własnych aktywów informacyjnych, jakim niewątpliwie jest tajemnica przedsiębiorstwa, to pojawia się wątpliwość, czy będzie mogło skuteczne chronić informacje niejawne lub inne, które mogą być powierzone mu przez potencjalnych partnerów biznesowych. Przedsiębiorca powinien mieć świadomość powagi sytuacji i móc efektywnie dochodzić swoich roszczeń w razie niekompetencji pracownika, co do nieprawnego ujawnienia przez niego informacji stanowiących tajemnice przedsiębiorstwa.

Postępowanie przed sądami w sprawach o naruszenie tajemnicy przedsiębiorstwa jest długotrwałe i kosztowne. Nasuwa się pewna konkluzja: przedsiębiorcy, żeby nie tracić czasu ani pieniędzy na długoletnie procesy, powinni zrobić wszystko, co możliwe i konieczne, by ochronić tajemnicę przedsiębiorstwa, którym kierują i tym samym uniknąć udowadniania swoich racji przed sądem. Tym samym cała procedura przygotowania i wdrożenia dokumentacji dotyczącej ustanowienia w firmie tajemnicy przedsiębiorstwa staje się priorytetem i przynieść może zauważalne korzyści.

LITERATURA

[1] https://marketingibiznes.pl/prawo-w-biznesie/tajemnica-przedsiebiorstwa/
[2] Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. 2020r. poz. 1913)
[3] Wiluś J., Praktyczne aspekty wdrażania procedur bezpieczeństwa informacji biznesowych. [w:] Ochrona informacji niejawnych i biznesowych. Materiały III Kongresu. Katowice 2007
[4] Zybała T., Ryszkowski M., Etyczne problemy działań w przedsiębiorstwie w zakresie ochrony informacji niejawnych. [w:] Ochrona informacji niejawnych i biznesowych. Materiały IV Kongresu. Katowice 2008
[5] Glonek A., Prawo – Organizacyjne aspekty ochrony tajemnicy przedsiębiorstwa. [w:] Ochrona informacji niejawnych i biznesowych. Materiały III Kongresu. Katowice 2007
[6] Ryszkowski M., Ochrona aktywów informacyjnych przedsiębiorstwa. [w:] Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały V Kongresu. Katowice 2009

Why entrepreneurs need a trade secret?

Abstract: The article presents how to understand a trade secret and what are the benefits of its implementation. The main areas that an entrepreneur must take into account when deciding on solutions related to information security have also been defined. How important is the human being in the process and monitoring of implemented legal, organizational and technical solutions. What requirements must the information meet in order to be protected by a trade secret. The directions for proper information management of particular importance to the organization were also presented. The areas of monitoring the implemented solutions, such as audit, information classification or risk analysis, were indicated. The article also presents the areas that should be covered by internal regulations of trade secrets. It was analyzed what primarily determines the security of assets in the enterprise. Attention was also drawn to the need of proper management of information constituting a trade secret, as it has a crucial meaning in the practical functioning of the organization.

Keywords: audit, risk analysis, security, information, integrity, availability, confidentiality, entrepreneur, business secret

mgr Marzena Smolarska
FAMUR S.A.
ul. Armii Krajowej 51
40-698 Katowice, Polska
tel.: +48 781 550 418
e-mail: msmolarska@famur.com