S T U D I A N A D B E Z P I E C Z E Ń S T W E M

NR 2 ss. 163–173 ROK 2017

ISSN 2543–7321

Małgorzata Beskosty

Akademia Pomorska
Słupsk
menturia@gmail.com

ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI

INFORMATION SECURITY MANAGEMENT

***Zarys treści*:** Obecnie możemy zaobserwować dynamiczny rozwój przedsiębiorstw nie tylko ze względu na postępującą globalizację, ale także szeroko rozumiany dostęp do nowoczesnych technologii. Wraz z ciągłym rozpowszechnianiem się sieci informacyjnych i telekomunikacyjnych znacznie obniżył się koszt pozyskania informacji, co ma ogromny wpływ na przyspieszenie procesów gospodarczych[1]. Celem niniejszego artykułu jest analiza informacji jako zasobu, przedstawienie charakterystycznych cech systemu bezpieczeństwa informacji, wyjaśnienie takich pojęć, jak informacja, bezpieczeństwo oraz przedstawienie działań wspomagających ochronę informacji w przedsiębiorstwie.
***Słowa kluczowe*:** informacja, ochrona danych, system bezpieczeństwa informacji, zarządzanie
***Key words*:** information, data protection, security of information system, management

Wstęp

Aby sprostać rosnącym wyzwaniom współczesnej gospodarki, ważna jest ochrona i dbanie o jakość zasobów. Pragnę poruszyć więc problem ochrony zasobu, jaki stanowi informacja, co jest o tyle problematyczne, że informacja stale ewoluuje, dlatego, aby mieć nad nią kontrolę, należy wdrożyć w przedsiębiorstwie system ochrony jej bezpieczeństwa. Stanowi to jednak przedsięwzięcie kosztowne, dlatego poprawa ochrony informacji powinna być opłacalna przede wszystkim dla przedsiębiorstwa oraz umacniać bądź zwiększać jego konkurencyjność[2].

[1] Z. Olesiński, *Środowiskowe uwarunkowania zarządzania informacją w małych przedsiębiorstwach,* [w:] *Zarządzanie zasobami informacyjnymi w warunkach nowej gospodarki*, red. R. Borowiecki, J. Czekaj, Warszawa 2010, s. 91.
[2] A. Białas, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Warszawa 2006, s. 28.

Czym jest informacja?

Niewątpliwie informacja jest jednym z najważniejszych aktywów firmy. Ona właśnie czyni przedsiębiorstwo wyjątkowym, decyduje o jego wartości, a także o sukcesie lub porażce[3]. Informacją jest komunikat, wiadomość, przekaz lub wskazówka, przekazywane w sposób zrozumiały i płynny za pomocą kodu lub języka. Możemy podzielić informację na trzy typy:

- niezbędną dla funkcjonowania przedsiębiorstwa,
- taką, na której opiera się przewaga konkurencyjna na rynku,
- dotyczącą bezpieczeństwa informacji i ich kontroli[4].

W dzisiejszych czasach „informacja jest kluczem do sukcesu rynkowego i staje się głównym elementem rozwoju gospodarczego”[5]. Dzieje się tak dlatego, że to jedyny zasób, do którego dostęp zapewnia możliwość prognozowania procesów zachodzących na rynku, a także podejmowania odpowiednich działań i reagowania na nie, porównywania czy decyzje podjęte przez przedsiębiorców są właściwe, czy też nie oraz ich dopracowania, co stanowi ogromną wartość dla strategii firmy.

Obecnie przedsiębiorstwa cierpią z powodu natłoku informacji, które niekontrolowane lub niepoprawnie zarządzane mogą spowodować ogromne szkody. Aby prawidłowo zarządzać informacją, należy wiedzieć przede wszystkim, gdzie jej szukać. Podstawowym jej nośnikiem są systemy informatyczne, sprzęt komputerowy, dokumenty papierowe bądź w formie elektronicznej oraz ludzka pamięć. W każdym z tych przypadków mamy do czynienia z ryzykiem utracenia lub dostania się informacji w niepowołane ręce[6]. Informacja zmienia się nieustannie, tak naprawdę trudno jest zdefiniować dzisiaj, co nią nie jest. Rozwój technologii i telekomunikacji spowodował, że ogromne wyzwanie dla przedsiębiorstwa i niejako jego sukces stanowi zapanowanie nad ogromem przepływu informacji, nie mówiąc już o ich usystematyzowaniu, podporządkowaniu i zarządzaniu nimi. Informacja może być dostarczana z wielu źródeł, niekoniecznie wiarygodnych, a ponadto w czasie swojej „wędrówki” może ulegać wielu przekształceniom, a tym samym zmniejsza się jej wartość. Dlatego należy chronić takie atrybuty informacji, jak poufność, dokładność i dostępność[7].

Poufnością informacji nazywamy zdolność do dzielenia się informacją wyłącznie z tymi instytucjami lub grupami osób, którym jest to niezbędne oraz do odmowy dostępu do informacji tym osobom, które nie są do tego powołane. Natomiast dokładność przekłada się na wiarygodność informacji, tzn. mówi o tym, że informacja pochodzi z wiarygodnego i sprawdzonego źródła i wiąże się z jej integralnością, czyli pewnością, że z upływem czasu nie została ona zniekształcona bądź nie straciła swojej pierwotnej wartości wskutek modyfikacji. O dostępności mówimy zaś wtedy, gdy

---

[3] D.L. Pipkin, *Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa*, tłum. E. Andrukiewicz, Warszawa 2002, s. 15.
[4] T. Kifner, *Polityka bezpieczeństwa i ochrony informacji*, Gliwice 2013, s. 14.
[5] Z. Gródek, *Sieci informacyjne dla przedsiębiorczości – czynnik przewagi konkurencyjnej opartej na informacji*, [w:] *Zarządzanie zasobami informacyjnymi…*, s. 203.
[6] T. Kifner, *Polityka bezpieczeństwa…*, s. 15.
[7] D.L. Pipkin, *Bezpieczeństwo informacji…*, s. 16.

wszystkie osoby mające pozwolenie na dostęp do danej informacji korzystają z niej, ponieważ należy ona do zasobów informacyjnych przedsiębiorstwa[8].

Pierwszym krokiem zmierzającym do ochrony informacji jest zrozumienie, dlaczego zapewnienie jej bezpieczeństwa jest tak ważne dla całego przedsiębiorstwa. W dobie gospodarki rynkowej nieustannie walczy się o informacje stanowiące o „być albo nie być" firmy, a ujawnienie wrażliwych danych może pociągnąć za sobą poważne straty finansowe.

Polityka bezpieczeństwa w przedsiębiorstwie

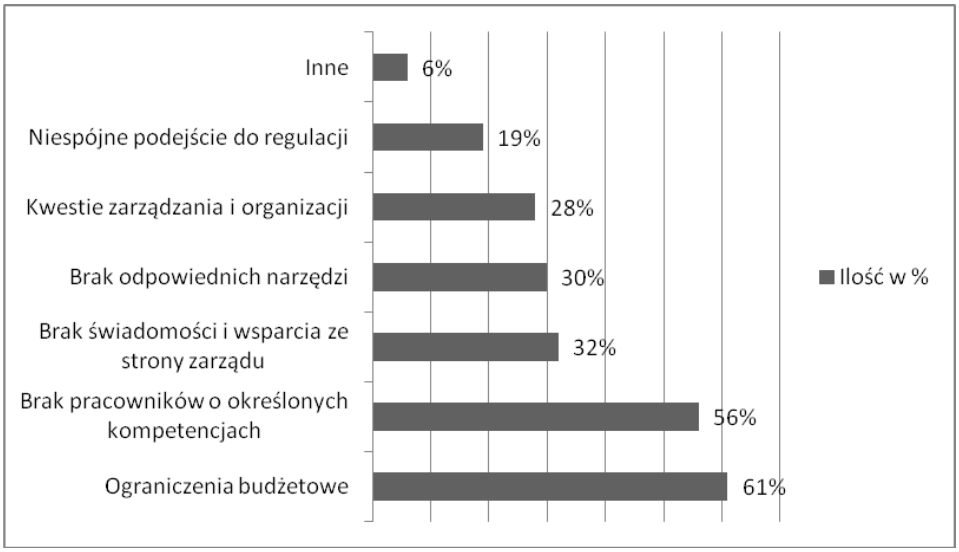
Mówiąc o bezpieczeństwie często mamy na myśli stan, w którym dane dobra są zabezpieczone, tzn. nie istnieje obawa ich utraty. W praktyce stan ten jest niemożliwy, ponieważ nigdy nie będziemy mieć stuprocentowej pewności, że zasoby, takie jak wiedza czy informacja, nie są narażone na ataki lub próby przejęcia. „Zapewnienie bezpieczeństwa jest procesem ograniczenia ryzyka lub prawdopodobieństwa szkody"[9], a, co się z tym wiąże, prowadzenie odpowiedniej polityki bezpieczeństwa służy jedynie stałemu zmniejszaniu bądź ograniczaniu stanu zagrożenia. Wynika więc z tego, że zagrożenie zawsze będzie istnieć. Wprowadzając jednak parę prostych zasad w przedsiębiorstwie, możemy zmniejszyć ryzyko ujawnienia cennych informacji.

Polityka bezpieczeństwa to system zarządzania nie tylko systemami informatycznymi, ale także organizacją i postępowaniem pracowników. To zapewnianie bezpieczeństwa informacji poprzez jasne zakomunikowanie i przedstawienie obowiązujących zasad i reguł pracownikom. Jest to świadome zarządzanie informacją i jej bezpieczeństwem za pomocą zaleceń i procedur, które w sposób klarowny opisują przepływ informacji w przedsiębiorstwie oraz między nim i jego kontrahentami[10]. Działania te powinny być sprecyzowane, przemyślane i skuteczne, a polityka bezpieczeństwa powinna dawać możliwość niezakłóconej pracy przedsiębiorstwa[11]. Podstawowy plan bezpieczeństwa informacji możemy podzielić na:

- analizę skutków finansowych określającą, które procesy w firmie można uznać za krytyczne, czyli niezbędne, aby instytucja przetrwała,
- analizę ryzyka przewidującą prawdopodobieństwo wystąpienia zagrożenia oraz wielkość przewidywanych szkód,
- planowanie działań w sytuacjach kryzysowych wskazujące, co należy zrobić, aby w jak najszybszy sposób przywrócić w przedsiębiorstwie stan sprzed incydentu,
- planowanie utrzymania ciągłości działania określające, co należy zrobić, aby pomimo sytuacji nadzwyczajnych oraz niezależnie od nich przedsiębiorstwo mogło dalej funkcjonować[12].

[8] Tamże, s. 16.
[9] Tamże, s. 17.
[10] T. Kifner, *Polityka bezpieczeństwa…*, s. 26.
[11] A. Białas, *Bezpieczeństwo informacji i usług…*, s. 34–35.
[12] D.L. Pipkin, *Bezpieczeństwo informacji…*, s. 19.

Bardzo ważne jest, aby dostrzec, że współczesna gospodarka i stopień zaawansowania technologii nie pozwalają na postrzeganie bezpieczeństwa jako możliwości, lecz jako niezbędnej konieczności, aby przedsiębiorstwo przetrwało. Bezpieczeństwo stanowi dzisiaj gwarancję gospodarczego postępu, dlatego plan bezpieczeństwa informacji powinien być ściśle związany z podstawowymi założeniami działania firmy oraz czynnościami kontrolnymi. Ważna jest również współpraca kadry zarządzającej. Powinna być ona świadoma zagrożeń oraz przygotowana na ewentualne reakcje niezbędne do ochrony zasobów.



Rys. 1. Główne przyczyny ograniczeń w zapewnianiu bezpieczeństwa informacji
Fig. 1. The main reasons of restrictions while providing information security

Źródło: *Raport* EY: Rośnie świadomość cyberzagrożeń, lecz firmom wciąż brakuje spójnego podejścia do bezpieczeństwa systemów informatycznych, EY, 13 stycznia 2017 www.ey.com/pl/pl/newsroom/news-releases/news-ey-20170113-swiatowe-badanie-bezpieczenstwa-informacji/ (dostęp: 14.03.2017).

Zarządzanie systemem bezpieczeństwa

Często bagatelizuje się wartość, jaką dla przedsiębiorstwa ma bezpieczeństwo, czego następstwem jest brak jakichkolwiek zabezpieczeń. Ten model „ochrony" może mieć wiele przyczyn, natomiast zazwyczaj wiąże się z brakiem finansów, czasu bądź po prostu z nieodpowiednim podejściem kadry zarządzającej. Prowadzi to do całkowitej bezczynności w sferze zabezpieczeń, gdyż przedsiębiorstwo, stanowiąc potencjalnie mało interesujący obiekt ataków, rezygnuje z jakichkolwiek form ochrony, wierząc, że bardziej zagrożone są firmy konkurencyjne. Ten model zabezpieczeń jest ryzykowny i w dłuższej perspektywie czasu nieopłacalny, gdyż straty, jakie ponosi się wskutek naruszenia dóbr firmy okazują się o wiele większe,

a przedsiębiorstwo może ponosić jego konsekwencje jeszcze długo po wyciszeniu sprawy[13].

Nieco lepszy jest model ochrony niektórych jednostek organizacyjnych, z punktu widzenia ekonomicznego bardziej opłacalny, natomiast niedający pewności, że dobra firmy nie zostaną utracone. Przedsiębiorstwo skupia się na zabezpieczeniu jedynie wybranych środków lub jednostek, stosując jednocześnie różne manewry mające na celu zmylenie potencjalnych włamywaczy, np. uwydatniając i wskazując najmocniejsze strony zabezpieczeń jako słabe[14].

Oczywiście, cel każdej firmy stanowi możliwość stworzenia ogólnego systemu zabezpieczeń obejmującego wszystkie sektory przedsiębiorstwa. Jest to niestety proces bardzo kosztowny, długotrwały i zawiły, w dzisiejszych czasach jednak konieczny[15].

Polityka bezpieczeństwa powinna obejmować stały dostęp do informacji i zarządzanie nią oraz przyczyniać się do ciągłego aktualizowania zmian i procedur systemu bezpieczeństwa. Nie bez znaczenia są także pracownicy, którzy powinni ponosić odpowiedzialność za wyznaczony im zakres bezpieczeństwa informacji. Polityka bezpieczeństwa każdego przedsiębiorstwa powinna charakteryzować się starannością w obsłudze sprzętu komputerowego, dbałością o miejsca pracy i ich zabezpieczanie, a także o możliwie jak największe zminimalizowanie błędów ludzkich. Te wszystkie elementy mają realny wpływ na politykę bezpieczeństwa, dlatego powinny podlegać uwadze kierownictwa przedsiębiorstwa i być wynikiem planowanych działań, a nie przypadku. Ponadto, aby uchronić dane wrażliwe firmy przed wypływem na zewnątrz, należy przechowywać je w sejfach lub miejscach pilnie strzeżonych. Aby firma mogła skutecznie chronić swoje zasoby, musi dokładnie zdawać sobie sprawę z ich wartości i ilości, dlatego należy na bieżąco prowadzić rejestr zakupionych urządzeń, sprzętu, oprogramowania i zaopatrzenia biurowego.

Ogólnie rzecz ujmując, możemy wyróżnić w planie bezpieczeństwa informacji pięć elementów. Pierwszym z nich jest inspekcja, czyli oszacowanie aktualnych zdolności przedsiębiorstwa, poziomu bezpieczeństwa i zależności występujących między zasobami a funkcjami firmy. Kolejny etap stanowi ochrona. Są to wszelkie działania zmierzające do zmniejszenie ryzyka utraty danych bądź przerwania ciągłości pracy firmy. Może to być tworzenie kopii zapasowych danych krytycznych firmy, kupno dodatkowego sprzętu lub oprogramowania, zwiększenie liczby dostawców. Na tym etapie podejmowane są decyzje, jakiej ochrony potrzeba, co należy chronić i jaki sposób wdrożyć planowany system bezpieczeństwa. Następne w kolejności jest wykrywanie, czyli monitorowanie zmian zachodzących w systemach i wyłapywanie tych uznanych za podejrzane. Może się jednak okazać, że system wykryje działania niepożądane lub dojdzie do próby włamania. Wtedy kluczowa okazuje się reakcja. To od niej zależy, czy przedsiębiorstwo przerwie pracę i na jak duże narazi się straty. W celu jak najszybszej reakcji opracowuje się plan awaryjny, w którym definiuje się, jaki powinien być odzew na zaistniały atak, dokumentuje się, a następnie testuje

[13] T. Kifner, *Polityka bezpieczeństwa…*, s. 31.
[14] Tamże.
[15] Tamże, s. 33.

daną odpowiedź, aby w czasie kryzysu nie budzić paniki i postępować według planu. Ostatnim etapem, nie mniej istotnym, jest refleksja. Po zażegnaniu niebezpieczeństwa przychodzi czas na podjęcie wszelkich kroków mogących udoskonalić plan ochrony informacji, ocenę dokonanych działań i dalszy rozwój. Dlatego tak ważne jest, aby opracować ogólny kierunek bezpieczeństwa i koordynować wszelkie procedury i zasady z nim związane[16].

Organizacja firmy

Przedsiębiorstwa, chcąc zaistnieć na rynku światowym i zapewnić sobie przewagę konkurencyjną, podejmują coraz to nowe wyzwania obejmujące gromadzenie wiedzy i umiejętne gospodarowanie nią[17]. Aby wdrażany system bezpieczeństwa był skuteczny, należy przede wszystkim opierać się na wiedzy ludzi, którzy są specjalistami w swoich dziedzinach. Trzeba jednak wziąć również pod uwagę, że zarządzanie wiedzą nie stanowi rozwiązania wszystkich problemów przedsiębiorstwa, jest natomiast idealnym instrumentem doskonalącym jego funkcjonowanie[18].

O ile zabezpieczenie papierowej dokumentacji czy też wydruków nie wymaga większych umiejętności, o tyle dobór optymalnego dla przedsiębiorstwa systemu informatycznego, oprogramowania czy systemu kodowania nie jest już rzeczą tak zwykłą i prostą. Jeśli zależy nam na całościowej ochronie informacji, niezbędne jest powierzenie tego zadania odpowiednim ludziom, którzy wezmą pełną odpowiedzialność za powzięte decyzje. Dlatego często zaleca się zorganizowanie w strukturze przedsiębiorstwa odrębnej komórki organizacyjnej, która zajmuje się bezpieczeństwem[19]. Nie bez znaczenia jest także oficjalne zatwierdzenie systemu oraz wprowadzanych w nim zmian. Ma to na celu nie tylko uświadomienie pracownikom wagi przedsięwzięcia, jakim jest ochrona informacji, ale także uniknięcie niepotrzebnych nieporozumień mogących się pojawić w przyszłości. Zatwierdzanie wszelkich działań przez zarząd podkreśla także ich znaczenie i zmusza do wywiązywania się z podjętych zadań. Bezwzględną koniecznością jest w takim wypadku powołanie komisji ds. bezpieczeństwa, której zadaniem byłaby kontrola przestrzegania wdrożonych procedur oraz konstruktywna krytyka zastanej sytuacji. Kontrole te powinny odbywać się systematycznie, aby zapewnić ciągłość systemu bezpieczeństwa i na bieżąco korygować zachowania odbiegające od pożądanych działań. Tylko w taki sposób zatwierdzony system ma szansę przetrwać i rozwijać się. Kontrola raportów i protokołów sporządzanych przez odpowiednich pracowników daje możliwość oceny realnej sytuacji i wprowadzenia ewentualnych poprawek. Równie niezbędny jest tu kontakt między komisją a kierownictwem kontrolowanego działu, który również

[16] D.L. Pipkin, *Bezpieczeństwo informacji…*, s. 20–21.
[17] W.M. Grudzewski, I. Hejduk, *Systemy zarządzania wiedzą warunkiem wzrostu wartości firmy*, [w:] *Współczesne źródła wartości przedsiębiorstwa*, red. B. Dobiegała-Korona, A. Herman, Warszawa 2006, s. 244.
[18] B. Siuta-Tokarska, *Zarządzanie wiedzą jako czynnik rozwoju współczesnej organizacji*, [w:] *Zarządzanie zasobami informacyjnymi…*, s. 108.
[19] T. Kifner, *Polityka bezpieczeństwa…*, s. 35.

podlegałby nadzorowi. Takie rozwiązanie daje poważną przewagę w samoorganizacji i zarządzaniu bezpieczeństwem i świadczy o zamiarze prowadzenia dalekosiężnej polityki.

Do obowiązków kadry zarządzającej należy także delegowanie uprawnień, czyli powierzanie podległym pracownikom zadań oraz odpowiedzialności za nie. Jest to warunek efektywnego zarządzania z tego względu, że pracownicy również wpływają na osobisty sukces kierowników. By zarząd mógł pełnić funkcje kierownicze, wymaga się od jego członków szerokiego zakresu wiedzy i kompetencji[20]. Obecnie zarządzanie jest raczej wyrazem ciągłego adaptowania się do postępujących zmian. Nie walczy się już o stabilność, lecz o rozwój i zmianę[21]. W związku z tym nieodzowna jest zarówno współpraca kierownictwa, jak i odpowiedni dobór kadry. Na kierownictwie ciąży obowiązek utrzymywania stabilności wprowadzonego systemu bezpieczeństwa oraz prognozowanie możliwych zmian technologicznych i strukturalnych mających wpływ na przedsiębiorstwo. Kierownictwo, wyrażając publicznie wolę przestrzegania procedur, informując o intencjach i wspierając pracowników w obowiązkach, pozwala im także przyzwyczaić się do nowych warunków, co znacznie usprawnia działanie przedsiębiorstwa. To również od kierownictwa zależy przepływ informacji. Powinno ono ustalić poziom dostępu do informacji poszczególnych działów firmy, aby zminimalizować ryzyko ujawnienia wrażliwych danych. Dotychczas często stosowano model pionowy, tzn. dostęp do informacji był taki sam dla przełożonych, jak i dla pracowników. Stwarza to ogromne ryzyko, gdyż osoby, które nie orientują się w informacjach, do których mają dostęp, nie są też w stanie zweryfikować ich wartości. Znacznie lepszym rozwiązaniem jest macierzowy dostęp do informacji, który charakteryzuje się dostępem do informacji szczegółowych, związanych bezpośrednio z wykonywaną pracą, zatem ograniczeniem przepływu informacji do minimum i ulepszeniem ochrony systemu informacyjnego[22].

Kolejne zagadnienie stanowi dobór kadry. Niezależnie od tego czy mówi się o kadrze zarządzającej czy o innych pracownikach, nie mogą być to ludzie przypadkowi. Zatrudnienie pracownika powinno wiązać się z przeprowadzeniem testów wiedzy czy doświadczenia lub badaniem skłonności psychicznych, zasad moralnych itd. W przedsiębiorstwie nastawionym na bezpieczeństwo informacji to od nich właśnie będzie zależeć poziom bezpieczeństwa, dlatego, obsadzając takie stanowiska, jak inspektor bezpieczeństwa czy administrator, szczególną uwagę powinniśmy zwrócić na wykształcenie. Innym problemem jest częste pomijanie pracownika jako integralnej części firmy. O wiele prostszym rozwiązaniem będzie przeszkolenie go w stosowaniu zasad bezpieczeństwa niż zakup skomplikowanego oprogramowania do gospodarowania dokumentami[23]. Istotą działania jest zaangażowanie pracownika w sprawy firmy poprzez zatrudnienie na umowę stałą, przeprowadzanie szkoleń, po-

[20] P. Bartkowiak, D. Sobczyński, B. Płokarz, *Zintegrowany system zarządzania a przepływ informacji*, [w:] *Zarządzanie zasobami informacyjnymi…*, s. 84.

[21] W.M. Grudzewski, I. Hejduk, *Kierunki zmian w systemie zarządzania*, [w:] *Wyzwania bezpieczeństwa cywilnego XXI wieku – inżynieria działań w obszarach nauki, dydaktyki i praktyki*, red. B. Kosowski, A. Włodarski, Warszawa 2007, s. 69.

[22] T. Kifner, *Polityka bezpieczeństwa…,* s. 37–38.

[23] Tamże, s. 40.

zwalających wyeliminować prawdopodobieństwo popełniania błędów. Informowanie o wchodzących zmianach w systemie czy zapoznanie z nowymi jego elementami z odpowiednim wyprzedzeniem pozwoli pracownikom oswoić się z nową sytuacją i przez to wpłynie na ich bardziej efektywną pracę. Ciągła edukacja pracowników, inwestowanie w ich rozwój jest także inwestycją w rozwój przedsiębiorstwa i gwarantem jego elastyczności i niepodzielności.

Zakończenie

Ochrona informacji w warunkach współczesnej gospodarki stanowi poważne wyzwanie dla rozwijających się przedsiębiorstw i powinna być zagadnieniem stale poruszanym przy omawianiu problematyki zmieniającego się rynku. Ogrom przepływu informacji między firmami, kontrahentami i światem zewnętrznym jest zjawiskiem powszechnym i pożądanym, ale także niebezpiecznym, jeżeli nie podejmuje się działań wspierających politykę bezpieczeństwa. Dany system bezpieczeństwa informacji obejmuje poza odpowiednim oprogramowaniem, sprzętem i zasobami materialnymi także pracowników, których przeszkolenie oraz przygotowanie w zakresie ochrony informacji znacznie zwiększa poziom bezpieczeństwa w przedsiębiorstwie.

Bibliografia

Bartkowiak P., Sobczyński D., Płokarz B., *Zintegrowany system zarządzania a przepływ informacji*, [w:] *Zarządzanie zasobami informacyjnymi w warunkach nowej gospodarki*, red. R. Borowiecki, J. Czekaj, Warszawa 2010.

Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Warszawa 2006.

Gródek Z., *Sieci informacyjne dla przedsiębiorczości – czynnik przewagi konkurencyjnej opartej na informacji*, [w:] *Zarządzanie zasobami informacyjnymi w warunkach nowej gospodarki*, red. R. Borowiecki, J. Czekaj, Warszawa 2010.

Grudzewski W.M., Hejduk I., *Kierunki zmian w systemie zarządzania*, [w:] *Wyzwania bezpieczeństwa cywilnego XXI wieku – inżynieria działań w obszarach nauki, dydaktyki i praktyki*, red. B. Kosowski, A. Włodarski, Warszawa 2007.

Grudzewski W.M., Hejduk I., *Systemy zarządzania wiedzą warunkiem wzrostu wartości firmy*, [w:] *Współczesne źródła wartości przedsiębiorstwa*, red. B. Dobiegała-Korona, A. Herman, Warszawa 2006.

Kifner T., *Polityka bezpieczeństwa i ochrony informacji*, Gliwice 2013.

Olesiński Z., *Środowiskowe uwarunkowania zarządzania informacją w małych przedsiębiorstwach*, [w:] *Zarządzanie zasobami informacyjnymi w warunkach nowej gospodarki*, red. R. Borowiecki, J. Czekaj, Warszawa 2010.

Pipkin D.L., *Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa*, tłum. E. Andrukiewicz, Warszawa 2002.

Siuta-Tokarska B., *Zarządzanie wiedzą jako czynnik rozwoju współczesnej organizacji*, [w:] *Zarządzanie zasobami informacyjnymi w warunkach nowej gospodarki*, red. R. Borowiecki, J. Czekaj, Warszawa 2010.

Raport EY: Rośnie świadomość cyberzagrożeń, lecz firmom wciąż brakuje spójnego podejścia do bezpieczeństwa systemów informatycznych, EY, 13 stycznia 2017 www.ey.com/pl/pl/newsroom/news-releases/news-ey-20170113-swiatowe-badanie-bezpieczenstwa-informacji/(dostęp: 14.3.2017).

Summary

The purpose of this article is to present the question of effective protection of information security management. The article begins with an explanation of the concept what the information is, its attributes and features. Moreover, the paper describes the models of security systems and the security policy in a company. Besides, the author shows what measures should be applied to manage information and what to do to implement security system which is both efficient and permanent.