Grzegorz Mikrut[*]
Wojciech Jarek

Ochrona informacji w przedsiębiorstwie turystycznym

1. Wstęp

Zarządzanie bezpieczeństwem informacji to dziedzina stosunkowo nowa i rozległa, mieszcząca się na styku trzech nauk: zarządzania, prawa[1] i informatyki. Oczywiście w tym momencie najbardziej interesuje nas sfera między prawem i zarządzaniem. Potrzeba ochrony informacji w przedsiębiorstwach jest coraz większa, ze względu na wymagania rynkowe jak i prawne. Większość publikacji dotyczących tej tematyki odnosi się jedynie do fizycznych, technicznych i organizacyjnych środków ochrony informacji, pomijając prawne środki, które nie tylko są wymagane przez obecny porządek prawny, ale dają także możliwość ochrony ekonomicznego interesu przedsiębiorcy. Prezentowany artykuł w szczególności odnosi się do przedsiębiorstw turystycznych i jest próbą oceny konieczności przenoszenia innych regulacji z zakresu ochrony informacji do turystycznej części porządku prawnego.

Przyczyną podjęcia próby głębszej analizy „ochrony informacji w przedsiębiorstwie turystycznym" były wyniki badań ankietowych przeprowadzonych w latach 2006/2007 w katowickich biurach podróży. Badania te zostały ukierunkowane na zebranie podstawowych informacji odnoszących się do specyfiki funkcjonowania podmiotów na rynku turystycznym w Polsce. Dodatkowo postawionym celem było uzyskanie wiedzy na temat aktualnych rozwiązań w zakresie zarządzania bezpieczeństwem informacji stosowanych w biurach podróży, jak i oceny stanu świadomości oraz deklarowanych potrzeb w tym zakresie przez badane podmioty. Pytania kwestionariusza miały przyczynić się do wyjaśnienia procesu tworzenia, jak również środków realizacji polityki bezpieczeństwa informacji oraz trudności z tym związane. Ponadto kwestionariusz zawierał pytania otwarte pozwalające zaprezentować własny stosunek przedsiębiorców do kwestii doświadczeń związanych z sytuacjami zagrażającymi bezpieczeństwu informacji. Wyniki tychże badań zostaną zaprezentowane na końcu niniejszego opracowania.

2. Informacje w turystyce

Działalność każdego przedsiębiorstwa oparta jest na zasobach ludzkich, rzeczowych, finansowych oraz informacyjnych. Ważne są jednak nieustanne poszukiwanie czynników sukcesu oraz formułowanie i realizacja strategii konkurencyjnej. Wyznacznikiem skuteczności działania w tych zmaganiach jest pozycja, jaką przedsiębiorstwa zdołają osiągnąć w danej dziedzinie[2]. Informacja jest zasobem ekonomicz-

[*] Dr Grzegorz Mikrut, Wojciech Jarek - AWF Katowice.

[1] Problematyka ochrony informacji w przedsiębiorstwie posiada bogatą literaturę, w szczególności na uwagę zasługuje monografia autorstwa A. Michalaka *Ochrona tajemnicy przedsiębiorstwa. Zagadnienia cywilnoprawne* (Kraków 2006). W niniejszym materiale przedstawiony jest jedynie wycinek tegoż zagadnienia tytułem wstępu do prezentacji przeprowadzonych badań ankietowych.

[2] J. Czekaj, *Metody zarządzania informacją w przedsiębiorstwie*, Kraków 2000, s. 11.

nym i pełni obok ziemi, pracy oraz kapitału rolę czynnika produkcji. Z jednej strony stanowi ona szczególne dobro gospodarcze, niezbędne dla funkcjonowania przedsiębiorstwa, a z drugiej jest czynnikiem zmniejszającym niepewność w procesie podejmowania decyzji. Jak każdy zasób ekonomiczny wymaga pewnych kosztów, reprezentuje określoną wartość, wpływając również na wartość wyrobów lub usług[3]. Turystykę, jak każdą inną branżę, wyróżniają specyficzne informacje potrzebne do prowadzenia działalności gospodarczej. Niezbędna jest wiedza i znajomość jakości świadczonych usług zarówno kooperantów jak i konkurencji. Trzeba wiedzieć jacy przewoźnicy, hotelarze i gastronomicy są nieuczciwi lub świadczą usługi niewystarczającej jakości. Należy sprawdzić miejsca oferowane klientom. Potrzebna jest znajomość rzeczywistych standardów hoteli, gdyż deklarowane w ofertach handlowych mogą odbiegać od stanu rzeczywistego. W turystyce wykorzystuje się także informacje o tendencjach i modzie na rynku turystycznym. Duże przedsiębiorstwa opierają się na badaniach rynku, ukazujących preferencje klientów. Wachlarz informacji znajdujących się w dyspozycji przeciętnego biura jest niezwykle szeroki. Począwszy od tych odnoszących się do posiadanych zasobów, realizowanych zadań, planów, strategii rozwoju, akcji promocyjnych etc., poprzez dane klientów w zakresie danych osobowych, czy też dotychczas świadczonych im usługach (czasie, miejscu, towarzystwie) oraz planowanych na przyszłość. Istotna jest więc ocena wartości posiadanych informacji, a zarazem dostosowanie do niej właściwego systemu ochrony. Czy przeciętny kierownik biura podróży zastanawia się nad tym aby zabezpieczyć taką informację przed konkurencją? Z tym bywa różnie.

Zdobywanie wiedzy o rynku, a zwłaszcza o konkurencji, ma miejsce od dawna. Od wieków poszukiwano informacji, nie tylko o towarach i usługach, ale także nowin o wojnie i pokoju oraz o polityce i gospodarce. Uzyskanie wiadomości z odległych krajów, a także plotek z dworów i banków, mogło powodować zawarcie korzystniejszej transakcji i ubiegnięcie konkurentów. Każdy z domów bankowych dysponował własną służbą informacyjną, co nawiasem mówiąc dało początek pierwszym gazetom. Znajomość rynku i stosunków handlowych była coraz wyżej ceniona wraz z rozwojem gospodarki kapitalistycznej[4].

Działania wywiadu gospodarczego oraz wszelkie działania związane z informacją w przedsiębiorstwie, muszą być prowadzone zgodnie z obowiązującymi przepisami prawa. Chcąc prowadzić wywiad gospodarczy należy mieć świadomość granic nałożonych przez dany porządek prawny. Przepisy prawa analizowane z punktu widzenia przedsiębiorcy nakładają na niego obowiązki dotyczące zabezpieczenia pewnych informacji.

Informacje chronione, znajdujące się w posiadaniu biura podróży, podzielić można z punktu widzenia obowiązujących norm na dwie grupy:

1) informacje, których ochrony wymaga ekonomiczny interes biura – a których nieuprawnione naruszenie chronione jest przez normy prawa, np.: tajemnica przedsiębiorstwa, tajemnica pracodawcy etc.;

[3] J. Czekaj, *Metody zarządzania informacją...*, s. 40-41.
[4] S. Kaczmarczyk, *Badania marketingowe – Metody i techniki*, Warszawa 2002, s. 11.

2) informacje, których ochrony wymagają normy prawa, np.: dane osobowe, informacje niejawne, tajemnica lekarska etc.

3. Informacje, których ochrony wymaga interes ekonomiczny biura

Ochrona tajemnicy oznacza zespół różnych działań, zwłaszcza o charakterze prawnym, organizacyjnym, administracyjnym i fizycznym, które mają na celu zabezpieczenie informacji przed ich udostępnieniem osobom nieuprawnionym.

Z tego punktu widzenia należy przede wszystkim wskazać na ochronę tajemnicy przedsiębiorstwa przewidzianą w ustawie z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji[5]. Według jej art. 11 ust.1, przekazanie, ujawnienie lub wykorzystanie cudzych informacji stanowiących tajemnicę przedsiębiorstwa albo ich nabycie od osoby nieuprawnionej, jeżeli zagraża lub narusza interes przedsiębiorcy, jest czynem nieuczciwej konkurencji. W myśl ust. 4 tego artykułu przez tajemnicę przedsiębiorstwa rozumie się 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.

Zgodnie z interpretacją Sądu Najwyższego dokonaną wyroku z 3 października 2000 r.[6] informacje, co do których przedsiębiorca (pracodawca) nie podjął niezbędnych działań w celu zachowania ich poufności, należy traktować jako wiedzę powszechną, do której przedsiębiorca nie ma żadnych ustawowych uprawnień. Nie każda informacja technologiczna i handlowa zawiera się w pojęciu „tajemnicy przedsiębiorstwa". Istnieje bowiem różnica między informacjami odpowiadającymi treści pojęcia „tajemnica przedsiębiorstwa" a informacjami wchodzącymi w skład powszechnej, aczkolwiek specjalistycznej wiedzy zdobytej przez pracownika w wyniku własnej działalności zawodowej podczas zatrudnienia. Tajemnica przedsiębiorstwa jest chroniona z mocy ustawy przez cały okres zatrudnienia oraz w ciągu trzech lat od jego ustania, chyba że umowa stanowi inaczej lub ustał stan tajemnicy. Wiedza, doświadczenie i umiejętności zdobyte przez pracownika podczas zatrudnienia nie korzystają z ustawowej ochrony na rzecz przedsiębiorstwa. Jednak ze względu na zasadę swobody umów, należy dopuścić możliwość zawarcia przez strony (pracodawcę i pracownika) porozumienia zawierającego klauzulę ograniczającą posługiwanie się tą wiedzą w celach konkurencyjnych po ustaniu zatrudnienia. Jak trafnie zauważył Sąd Najwyższy w powołanym wyroku, granica między informacjami objętymi pojęciem „tajemnicy przedsiębiorstwa" a pojęciem powszechnej, aczkolwiek specjalistycznej wiedzy, jest niewątpliwie nieostra. Odnosi się to do każdej dziedziny życia, branży, w tym również do turystyki.

Jak widać, najważniejsze jest określenie, co należy rozumieć przez pojęcie „niezbędnych działań". Informacja staje się tajemnicą przedsiębiorstwa, kiedy przedsiębiorca ma wolę, by pozostała ona tajemnicą dla pewnych kręgów odbiorców (np. konkurentów) i wola ta dla innych osób musi być rozpoznawalna. Bez takiej woli, choćby tylko dorozumianej, informacja może być nieznana, ale nie będzie tajemnicą.

---

[5] T. jedn. Dz. U. z 2003 r., Nr 153, poz. 1503 ze zm.

[6] Orzeczenie SN z 3 października 2000, I CKN 304/00, OSNC 2001, Nr 4, poz. 59.

Działania jakie może podjąć przedsiębiorca to m.in. ograniczenie personalne. Informowanie, iż pewne informacje nie powinny być ujawnione osobom, które nie zostały w jakiś sposób uprawnione do ich posiadania – zarówno w drodze umowy, jak i przepisów ustawy. Opatrzenie informacji odpowiednim komentarzem – poufne, do użytku wewnętrznego itp. Zawężenie dostępu do pewnych informacji jedynie do części personelu przez opatrzenie plików zawierających informacje poufnymi hasłami. Takie działania dość jasno świadczą o chęci nieujawniania informacji wobec szerokiego grona odbiorców[7]. Informacja nieujawniona do wiadomości publicznej traci ochronę prawną, gdy inny przedsiębiorca (konkurent) może się o niej dowiedzieć zwykłą i dozwoloną drogą, a więc np. gdy pewna wiadomość jest przedstawiana w pismach fachowych lub gdy z towaru wystawionego na widok publiczny każdy fachowiec poznać może, jaką metodę produkcji zastosowano. Jednocześnie „tajemnica" nie traci swego charakteru przez to, że wie o niej pewne ograniczone grono osób, zobowiązanych do dyskrecji w tej sprawie, jak pracownicy przedsiębiorstwa lub inne osoby, którym przedsiębiorca powierza informację. Podjęcie niezbędnych działań w celu zachowania poufności informacji powinno prowadzić do sytuacji, w której chroniona informacja nie może dotrzeć do wiadomości osób trzecich w normalnym toku zdarzeń, bez żadnych specjalnych starań z ich strony[8].

Istotnym wsparciem dla ochrony tajemnicy przedsiębiorstwa są także przepisy o tajemnicy pracodawcy zawarte w kodeksie pracy[9]. Zgodnie z art. 100 §1 tej ustawy, „pracownik jest obowiązany wykonywać pracę sumiennie i starannie oraz stosować się do poleceń przełożonych, które dotyczą pracy, jeżeli nie są one sprzeczne z przepisami prawa lub umową o pracę". Ponadto według §2 tego artykułu pracownik jest obowiązany w szczególności do dbania o dobro zakładu pracy, chronienia jego mienia oraz zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę i przestrzegać tajemnicy określonej w odrębnych przepisach (pkt 4 i 5). W zakres informacji chronionych tajemnicą pracodawcy wchodzą informacje nie objęte ochroną na zasadach przepisów odrębnych. Informacje chronione tajemnicą pracodawcy muszą się wiązać z działalnością (choćby uboczną) danego pracodawcy. Brak jest natomiast przesłanek pozwalających na objęcie zakresem tych informacji wyłącznie takich, które związane są interesem gospodarczym, grą konkurencyjną, czy rywalizacją rynkową. Nie powinny być zaliczane do informacji objętych tajemnicą pracodawcy te, które stanowią element wiedzy ogólnej, wykształcenia czy kwalifikacji pracownika lub jego naturalnych umiejętności albo uzdolnień, stanowiących swoisty wkład wnoszony przez niego do powstającego stosunku pracy. Tajemnica pracodawcy powinna raczej być łączona z konkretnymi specyficznymi informacjami tworzącymi różnicę pomiędzy tym konkretnym pracodawcą, a innymi pracodawcami o podobnym zakresie działania. W ocenie konkretnego przypadku należy brać pod uwagę to, czy dany pracownik może być zakwalifikowany jako ten, który ma dostęp do zastrzeżonych informacji z racji wykonywa-

[7] M. Jabłoński, K. Wygoda, *Dostęp do informacji i jego granice. Wolność informacji, prawo dostępu do informacji publicznej i ochrona danych osobowych*, Wrocław 2002, s. 85.
[8] Orzeczenie SN z 3 października 2000, I CKN 304/00, OSNC 2001, Nr 4, poz. 59.
[9] Ustawa z dnia 26 czerwca 1974 r. - Kodeks pracy (t. jedn. Dz. U. z 1998 r., Nr 21, poz. 94 ze zm.).

nej pracy, czy też styka się z taką informacją przypadkowo, okazjonalnie. Takie rozróżnienie jest uprawnione zwłaszcza w świetle przepisu art. 101^2 §1 kodeksu pracy, zawierającego określenie „pracownik mający dostęp do szczególnie ważnych informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę". We wspomnianym orzeczeniu Sąd Najwyższy trafnie zwrócił także uwagę, że w każdej sytuacji pojawić się może trudny problem określenia i udowodnienia motywów działania pracownika, których charakter winien rzutować na ocenę konkretnego przypadku.

4. Informacje, których ochrony wymagają normy prawa

Przetwarzanie danych osobowych stanowi integralną część funkcjonowania większości podmiotów sfery publicznej, jak i prywatnej. Działalność przedsiębiorstw wiąże się z gromadzeniem i przetwarzaniem danych osobowych. W sektorze turystycznym oczywiście także mamy do czynienia z tą problematyką. Osoby podają swoje dane osobowe w celu skorzystania z oferty turystycznej, ale też w celach marketingowych.

Ochronę danych osobowych należy traktować jako element szeroko rozumianego prawa do prywatności. Samo prawo do ochrony danych osobowych zaczęło się kształtować w drugiej połowie zeszłego wieku, kiedy to dostrzeżono, że wraz rozwojem technologii informatycznej, a co za tym idzie automatyzacji przetwarzania danych, zaczęły pojawiać się różnorodne wynaturzenia w relacjach pomiędzy podmiotami stosunku informacyjnego[10].

W Polsce prawo do ochrony danych osobowych do 1997 roku znajdowało się w „legislacyjnej próżni"[11]. Dopiero przepisy Konstytucji[12] wprowadziły szereg postanowień dotyczących zarówno ochrony prywatności, jak również niektórych jej aspektów, podlegających ochronie prawnej. Ustrojodawca w art. 47 Konstytucji zagwarantował obywatelom prawo do prywatności, a w art. 51 każdej osobie, prawo do ochrony dotyczących jej informacji. Pozwoliło to na odejście od praktyki wywodzenia tych praw z art. 23 i 24 k.c. Mimo to, dane osobowe są w dalszym ciągu chronione dzięki przepisom dotyczącym cywilnoprawnej ochrony dóbr osobistych niezależnie od ochrony przewidzianej w innych przepisach oraz marginalnie przez karnoprawne normy dotyczące ochrony czci i dobrego imienia (rozdział XXVII kodeksu karnego[13] - przestępstwa przeciwko czci i nietykalności cielesnej)[14].

Zasady ochrony danych ustanowione dyrektywą 95/46/WE[15] wprowadzone zostały do polskiego porządku prawnego ustawą z dnia 29 sierpnia 1997 r. o ochronie

[10] M. Jabłoński, K. Wygoda, *Dostęp do informacji*..., s. 208.

[11] Nie mamy tu na myśli „próżni absolutnej" zasadniczo nie występującej w naturze, a jedynie stan do niej zmierzający, nazywany „próżnią", który charakteryzuje się niewielką, bliską zeru ilością materiału w wyodrębnionej przestrzeni.

[12] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78 poz. 483 ze zm.).

[13] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. Nr 88, poz. 553, ze zm.).

[14] W. Kwiatkowski, *Bezpieczeństwo informacji III Rzeczpospolitej*, Kraków 2000, s. 218.

[15] Dyrektywa 95/46/WE Parlamentu Europejskiego I Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. L 281 z 23.11.1995, s. 31).

danych osobowych[16]. Ustawa ta wprowadziła szczegółowe normy służące ochronie danych osobowych, a do dnia 1 maja 2004 r., czyli wstąpienia Polski do Unii Europejskiej, przeniosła do polskiego porządku prawnego wszystkie zasady określone we wspomnianej dyrektywie. Przepisy ustawy weszły w życie w dniu 30 kwietnia 1998 r.

Ustawa o ochronie danych osobowych określiła prawne ramy obrotu danymi osobowymi, a także zasady, jakie należy stosować przy przetwarzaniu danych osobowych. Unormowała też prawa i obowiązki organów, instytucji i osób prowadzących zbiory danych osobowych oraz prawa osób, których dane dotyczą, w taki sposób, aby zagwarantować maksymalną ochronę praw i wolności każdej osobie fizycznej oraz poszanowania jej życia prywatnego. W jej art. 1 ust. 1 zagwarantowano każdemu prawo do ochrony dotyczących go danych osobowych.

Świadcząc usługi drogą elektroniczną przedsiębiorstwo musi spełniać także wymogi ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[17]. Szczególnie ważnymi rozdziałami związanymi z informacjami jest rozdział czwarty tej ustawy – zasady ochrony danych osobowych w związku ze świadczeniem usług drogą elektroniczną oraz rozdział drugi – obowiązki usługodawcy świadczącego usługi drogą elektroniczną.

Wymagania ustawy muszą spełniać osoby fizyczne, osoby prawne albo jednostki organizacyjne nieposiadające osobowości prawnej, które prowadząc, chociażby ubocznie, działalność zarobkową lub zawodową, świadczą usługi drogą elektroniczną.

Powyżej opisane regulacje w zakresie wyodrębnionych prawnie chronionych tajemnic oraz innych informacji mogą zostać uzupełnione dodatkowymi działaniami proponowanymi przez normy o typowo fakultatywnym charakterze.

5. Fakultatywna ochrona informacji

Pod pojęciem bezpieczeństwa informacji rozumieć należy zachowanie poufności, integralności i dostępności informacji, a więc zapewnienie, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom (poufność), zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania (integralność) oraz dostępność i użyteczność informacji wraz ze związanymi z nią aktywami, na żądanie upoważnionego podmiotu (dostępność).

Informacje mające konkretną wartość są narażone na różne zagrożenia, zarówno z zewnątrz jak i wewnątrz przedsiębiorstwa. Źródłem takich incydentów związanych z bezpieczeństwem informacji, to jest zdarzeń lub serii niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji, mogą być zarówno ludzie jak i zdarzenia losowe[18]. Bezpieczne zarządzanie informacją wymaga więc zastosowania zabezpieczeń w obszarach zaso-

[16] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. jedn. Dz. U. z 2002 r., Nr 101, poz. 926, ze zm.).
[17] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1204, ze zm.).
[18] D. Dziembek, *Wybrane problemy bezpieczeństwa danych*, [w:] *Wstęp do systemów informacyjnych zarządzania w przedsiębiorstwie*, red. A. Nowacki, Częstochowa 2005, s. 179-180.

bów przedsiębiorstwa takich jak: otoczenie fizyczne, otoczenie techniczne, personel, administracja. Zabezpieczenia spełniają funkcje wykrywania, poprawiania, odtwarzania, monitorowania, uświadamiania[19].

Najczęściej zapewnienie bezpieczeństwa informacji, sprowadza się do stałych działań intuicyjnych lub podjętych w konsekwencji wystąpienia negatywnych skutków następstw. Skuteczne zarządzanie bezpieczeństwem informacji wymaga jednak całościowych rozwiązań opartych na przewidywaniu zagrożeń. Dobrym rozwiązaniem jest korzystanie z doświadczeń innych przedsiębiorstw.

Wiodące światowe przedsiębiorstwa już dawno zaczęły wprowadzać własne standardy zarządzania bezpieczeństwem informacji. Postanowiono wykorzystać te doświadczenia i stworzyć nową normę. Brytyjskie organizacje zainteresowane e-biznesem, skupione w strukturze BSI–DISC komitet BDD/2 Information Security Management, opracowały dwuczęściową normę BS 7799:2002. Pierwsza część – BS 7799-1:2002, to standardowy kodeks praktyk i zagadnień, które należy realizować dla potrzeb bezpieczeństwa informacji. Zawiera 12 kategorii zabezpieczeń, które są potrzebne przy tworzeniu systemu zarządzania bezpieczeństwem informacji. Druga cześć normy – BS 7799-2:2002, zawiera specyfikację i wytyczne dla systemów zarządzania bezpieczeństwem informacji. Część ta pozwala zaprojektować, wdrożyć i poddać certyfikacji system zarządzania bezpieczeństwem informacji (Information Security Management System). Polską wersję drugiej części brytyjskiej normy opracował Polski Komitet Normalizacyjny jako Polska Norma PN-I-07799-2:2005 „Systemy zarządzania bezpieczeństwem informacji – Część 2: Specyfikacja i wytyczne do stosowania".

Brytyjska norma BS 7799 stała się podstawą dla międzynarodowego standardu zarządzania bezpieczeństwem informacji ISO/IEC 27001:2005, przygotowanego przez Międzynarodową Organizację Normalizacyjną i Międzynarodową Komisję Elektrotechniczną, które tworzą wyspecjalizowany system światowej normalizacji. Polska wersja tej normy, mająca ten sam status co wersja oficjalna, została przetłumaczona przez Polski Komitet Normalizacyjny i opublikowana w styczniu 2007 roku jako PN-ISO/IEC 27001:2007 „Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania". Tym samym zastąpiła ona normę PN-I-07799-2005. Stała się więc normą, na zgodność z którą będą wydawane certyfikaty. Zainteresowanie wdrażaniem systemów zarządzania bezpieczeństwem informacji jest coraz większe, dlatego przygotowywana jest rodzina standardów bezpieczeństwa:

- ISO/IEC 27000 - słownictwo i terminologia,
- ISO/IEC 27002 - zasady zarządzania bezpieczeństwem informacji,
- ISO/IEC 27003 - porady i wskazówki dotyczące implementacji systemu zarządzania bezpieczeństwem informacji (ISMS),
- ISO/IEC 27004 - wskaźniki i pomiar efektywności zarządzania bezpieczeństwem informacji,

[19] R. Borowiecki, M. Kwieciński, *Informacja w zarządzaniu przedsiębiorstwem, pozyskiwanie, wykorzystanie i ochrona (wybrane problemy teorii i praktyki)*, Kraków 2003, s. 124-128.

- ISO/IEC 27005 (obecnie BS 7799-3) - zarządzanie ryzykiem bezpieczeństwa informacji.

W tym miejscu warto skupić uwagę na normie ISO/IEC 27001, na podstawie której można certyfikować system zarządzania bezpieczeństwem informacji (SZBI)[20]. Rozwiązania w niej zawarte są ogólne i z powodzeniem mogą być stosowane we wszystkich organizacjach. Wprowadzenie SZBI powinno być decyzją strategiczną. System ma za zadanie zapewnić ochronę aktywów informacyjnych spełniając postawione przez organizację wymagania, jak i oczekiwania ze strony klientów. Pozwala na zwiększenie konkurencyjności, zyskowności, zgodności z przepisami prawa i umacnianie dobrego wizerunku handlowego. Norma pokazuje model efektywnie działającego SZBI, który powinien być dostosowany do konkretnej organizacji. Przy projektowaniu i wdrażaniu systemu uwzględnia się potrzeby i cele biznesowe, wymagania bezpieczeństwa, realizowane procesy oraz wielkość i strukturę organizacji. Jest to bardzo ważne, gdyż osoby zainteresowane wdrażaniem w swoich przedsiębiorstwach SZBI mogą odnieść wrażenie, że normy te są potrzebne tylko w dużych przedsiębiorstwach. Mali przedsiębiorcy obawiają się dużej liczby zabezpieczeń i ogromnych środków, kiedy tak naprawdę proste sytuacje wymagają prostych rozwiązań. SZBI powinien więc zostać zaprojektowany tak, aby zapewnić adekwatne i proporcjonalne zabezpieczenia, które odpowiednio chronią aktywa informacyjne, oraz tak, aby uzyskać zaufanie zainteresowanych stron. Każdy system jest dostosowany do potrzeb organizacji i można chyba powiedzieć, że nie ma dwóch identycznych SZBI.

Norma przedstawia podejście procesowe do zagadnienia zarządzania bezpieczeństwem informacji. Chcąc osiągnąć wartość wyjściową procesu, to znaczy bezpieczeństwo informacji, należy do całej struktury procesów SZBI stosować model PDCA: Planuj – Wykonuj – Sprawdzaj – Działaj[21].

Planowanie odnosi się do procesu ustanowienia SZBI, który należy rozpocząć od zdefiniowania polityki bezpieczeństwa informacji, jako podstawowego długoterminowego dokumentu, w którym przedstawia się cele, strategie, odpowiedzialność i metody ich wzajemnych powiązań gwarantujące osiągnięcie założonego poziomu bezpieczeństwa. Jest to baza do opracowania i wprowadzenia akceptowanych koncepcji bezpieczeństwa. Cele i strategie polityki powinny być rozwijane w przedsiębiorstwie hierarchicznie z poziomu najwyższego szczebla zarządzania do poziomu operacyjnego. Zaangażowanie kierownictwa jest potrzebne na każdym etapie modelu PDCA. To kierownictwo musi zapewnić odpowiednie zasoby, określić role i zakresy odpowiedzialności, podjąć decyzje dotyczące kryteriów akceptacji ryzyka oraz dbać o ciągłe doskonalenie SZBI. Wdrożenie i eksploatacja nie kończą procesów SZBI. Przedsiębiorstwo egzystuje w powiązaniu ze zmiennym otoczeniem. Sama organizacja też jest dynamiczna i zmienia się w czasie.

Wskazana powyżej norma, a wraz z nią System Zarządzania Bezpieczeństwem Informacji w przedsiębiorstwie, stanowić może uzupełnienie wymogów ustawowych w zakresie informacji i danych chronionych. Regulacje te nie stoją w sprzeczności,

[20] Funkcjonuje także oryginalny skrót ISMS – *information security management system*.
[21] Skrót PDCA od: *Plan – Do – Check – Act*.

a tym samym nie wykluczają się. Równoległe przyczyny w postaci wymogów ustawowych wraz z dbałością o ekonomiczny interes przedsiębiorstwa stanowić mogą źródło dla opracowania, a następnie wdrożenia, jednolitego oraz spójnego systemu zarządzania bezpieczeństwem informacji.

6. Wyniki badań ankietowych

Podsumowując przedmiotową analizę, w tym miejscu zaprezentujemy wyniki przeprowadzonych badań ankietowych. Formularz ankiety został rozdany w biurach podróży na terenie Katowic. Miasto to zostało wybrane, ze względu na usytuowanie wielu filii biur podróży działających w całej Polsce, jak również siedziby lokalnych biur podróży. W badaniach uwzględniono jedynie wypełnione ankiety. Formularz ankiety wypełniony został w 20 biurach podróży.

6.1. Szczebel na którym opracowywane są założenia polityki bezpieczeństwa informacji

Polityka bezpieczeństwa informacji to podstawowe zasady obowiązujące użytkowników informacji, które mają na celu zapewnienie bezpieczeństwa informacji. Powinna być ona określana hierarchicznie, tak aby każdy niższy szczebel stosował te same zasady. Zgodnie z wynikami badań: przedsiębiorcy stosują tę zasadę, gdyż 56,3% odpowiedzi wskazuje na opracowywanie założeń polityki na szczeblu kierownictwa lub w centrali przedsiębiorstw posiadających filie (37,5%). Tylko 6,3% opracowuje założenia w dziale informatyki, żadne natomiast z biur nie korzysta z usług przedsiębiorstw zewnętrznych.

6.2. Perspektywa czasowa polityki bezpieczeństwa informacji

Polityka bezpieczeństwa informacji musi uwzględniać czynnik czasu, aby precyzyjnie określić jej cele, środki i koszty. Według badań: ponad połowa (55,6%) biur określa reguły bezpieczeństwa na bieżąco, a 5,6% deklaruje brak prowadzenia polityki w tym zakresie. Można więc przypuszczać, że w większości przypadków działania w zakresie bezpieczeństwa informacji sprowadzają się w praktyce jedynie do reagowania na pojawiające się problemy. Brak więc przewidywania zagrożeń i planowania odpowiednich środków zaradczych.

Perspektywa czasowa	%
Długookresowa (3 lata i więcej)	16,7
Średniookresowa	16,7
Roczna	5,6
Określana na bieżąco	55,6
Brak polityki	5,6

Źródło: opracowanie własne.

6.3. Sposób przeprowadzania analizy ryzyka

Potwierdzeniem złego przygotowywania polityki bezpieczeństwa informacji, są wyniki dotyczące analizy ryzyka. Analiza taka powinna być podstawą opracowania

polityki, gdyż dopiero wtedy wiadomo przed czym i w jakim wymiarze należy chronić informacje. W przypadku badanych biur 75% nie prowadzi analizy. Można więc spodziewać się, iż większość biur nie ma także żadnego dokumentu określającego całościowo zasady polityki bezpieczeństwa.

Sposób	%
Pracownicy przedsiębiorstwa	25
Przedsiębiorstwo zewnętrzne	0
Brak analizy ryzyka	75

Źródło: opracowanie własne.

6.4. Odpowiedzialność za realizację przyjętej polityki bezpieczeństwa informacji

Respondenci mieli także odpowiedzieć, kto jest odpowiedzialny za realizację polityki bezpieczeństwa informacji. Spośród nich 70,6% wskazało osobę ze szczebla kierowniczego, 23,5% dział informatyki, a co ciekawe 5,9% uznało przedsiębiorstwo zewnętrzne, mimo iż według wcześniejszych wyników nie uczestniczy ono w formułowaniu polityki, ani w analizie ryzyka.

6.5. Ocena ochrony przed zagrożeniami z wnętrza oraz z zewnątrz przedsiębiorstwa

Ankieta dała możliwość oceny ochrony przed zagrożeniami z wnętrza przedsiębiorstwa oraz zagrożeniami spoza przedsiębiorstwa. Oceny w obu przypadkach są bardzo zbliżone i większości system ochrony oceniany jest dobrze lub bardzo dobrze.

6.6. Ocena poszczególnych środków ochrony informacji

Jak wynika z pozyskanych danych przedsiębiorcy przede wszystkim za najważniejsze środki realizacji polityki bezpieczeństwa uznają środki fizyczne (alarmy, zamki, monitoring), następnie kontrolę antywirusową oraz dublowanie danych zawartych na dyskach. Za ważne uważane są zasady postępowania z niepotrzebnymi wydrukami, dokumentami i nośnikami danych oraz tworzenie kopii zapasowych.

6.7. Trudności w realizacji polityki bezpieczeństwa informacji

Ostatnim pytaniem odnoszącym się do polityki bezpieczeństwa informacji było określenie trudności w jej realizacji. Nie stwierdza żadnych trudności 26,1%, a 21,7% uważa za największy problem brak specjalistów w tej dziedzinie. Co ciekawe największym problemem nie są środki finansowe (13%). Warto również zauważyć, że niechęć do realizacji polityki wśród pracowników jest taka sama jak wśród kierownictwa.

Kategoria	%
Nie występują żadne trudności	26,1
Brak założeń polityki bezpieczeństwa informacji	0
Brak informacji o nowych zagrożeniach	17,4
Brak specjalistów w danej dziedzinie	21,7
Niewystarczające środki finansowe	13
Niechęć pracowników do realizacji polityki bezpieczeństwa	8,7
Niechęć kierownictwa do realizacji polityki bezpieczeństwa	8,7
Brak danych	4,3

Źródło: opracowanie własne.

Odpowiedzi na pozostałe pytania ankiety wskazują na to, iż większości (80%) respondentów nie utrudnia pracy przestrzeganie zasad bezpieczeństwa i jest uważane za normalny obowiązek. Jest to sytuacja bardzo dobra, gdyż niechęć pracowników i kierownictwa do ochrony informacji może być przyczyną występowania zagrożeń w tym zakresie. Otwartość ta pozwala na implementację nowych rozwiązań.

W pytaniu ankiety: *Które informacje powinny być szczególnie chronione?*, aż 73,3% udziela odpowiedzi, że powinny to być dane osobowe klientów. Najczęściej było to motywowane wymaganiami wynikającymi z ustawy o ochronie danych osobowych. Pytani udzielali także odpowiedzi, że powinny być chronione szczegóły umów z kontrahentami oraz dane księgowe. Pozostałe pojedyncze odpowiedzi to: informacje o kalkulacji cen imprez, hasła dostępu do aplikacji, plany działań przedsiębiorstwa, strategia oraz informacje o sprzedaży. Jak widać, katalog informacji, które powinny być chronione, jest szeroki i uwzględnia poza informacjami, które znajdują się w każdym przedsiębiorstwie, także specyficzne informacje, które są charakterystyczne dla tej branży, jak chociażby kalkulacja cen imprez.

Co prawda większość przedsiębiorców nie spotkała się z sytuacją naruszenia systemu bezpieczeństwa informacji, to jednak 33,3% miało takie doświadczenia. Wskazane zostały przypadki kradzieży komputerów z twardymi dyskami zawierającymi wszystkie informacje, kradzieży bazy danych klientów, skasowania oferty biura z serwera, ingerencji i modyfikacji danych przez jednego pracownika w wewnętrznym systemie rezerwacji, czy nawet przypadki naruszenia ochrony danych osobowych przez kooperującego operatora sieci komórkowej. Przypadki takich zdarzeń, w świetle wcześniejszych ocen, mogą sugerować, że dla większości biur zaistnienie takich okoliczności może być bardzo poważnym utrudnieniem lub uniemożliwić dalsze funkcjonowanie. Mimo tego, że sytuacje naruszenia systemu bezpieczeństwa miały miejsce w niektórych biurach, odsetek ocen bardzo dobrych i dobrych systemu był bardzo wysoki. Może to wskazywać na niechęć ankietowanych do przyznawania się do błędów i ukrywanie przez nich niewystarczającej ochrony.

Jak wynika z badań, 60% przedsiębiorców szkoli swoich pracowników w zakresie bezpieczeństwa zasobów informacyjnych. Można w tym miejscu zastanowić się,

czy szkolenia te mają charakter kompleksowy, czy są to może szkolenia przeprowadzane przy okazji wdrażania nowego pracownika do przedsiębiorstwa, jako jeden z jego elementów. Ciekawe jest też to, kto przeprowadza takie szkolenia? Jak wcześniej wskazano, żadne biuro nie wskazywało korzystania z usług zewnętrznych przedsiębiorstw specjalistycznych, a za największy problem uznano brak specjalistów w tej dziedzinie. Problem ten wymaga dalszego badania.

Tylko jedno biuro podróży poddało standaryzacji zarządzanie bezpieczeństwem zasobów informacyjnych. Niestety nie została wymieniona nazwa normy, która została wdrożona. Pozostałe 93,3% nie wprowadziło żadnej normy. Jak wcześniej wskazano, norma ISO 17799:2000 jest znacznym ułatwieniem w zarządzaniu bezpieczeństwem informacji. Oparta na wieloletnich doświadczeniach zachodnich przedsiębiorstw w pełni odpowiada potrzebom dzisiejszych czasów. Wprowadzone standardy mogą też okazać się sporym atutem w walce konkurencyjnej o klienta, który coraz częściej zwraca uwagę także na aspekt bezpieczeństwa. Tak słaby wynik wśród polskich biur podróży jest prawdopodobnie spowodowany niską znajomością treści tej normy.

Ataki na systemy bezpieczeństwa informacji często pochodzą od konkurencji, dlatego postawiono pytanie, jakie informacje chcieliby przedsiębiorcy turystyczni uzyskać na temat konkurentów. Najczęściej odpowiadali oni, że chcieliby wiedzieć o planowanych kampaniach promocyjnych, promocjach cenowych, polityce rabatów. Chcieliby również mieć bazy danych klientów swoich konkurentów oraz ich liczbę, informacje o nowych produktach, programy imprez. Co ciekawe, większość z wymienianych tu informacji odnosi się do działań marketingowych przedsiębiorstwa. Jednak w pytaniu o to, które z informacji powinny być szczególnie chronione nie zostały one wymienione. Zgodnie jednak odpowiadają, że chętnie znaliby dane osobowe klientów i ich ochronę uznają za najważniejszą. Potwierdza to potrzebę znajomości ustawy o ochronie danych osobowych i właściwego jej wypełniania. Tylko 14,3% pytanych przedsiębiorców chciałoby pozyskać te informacje, zastrzegając jednak, że jedynie w sposób zgodny z prawem.

W związku z powyższym sytuacje zagrożenia zasobów informacyjnych mogą mieć fatalne skutki dla biura podróży. Oprócz spadku zaufania klientów i kooperantów, biuro podróży może nawet całkowicie zaprzestać działalności. Stąd tak istotne opracowanie polityki bezpieczeństwa informacji, szkolenia pracowników i co najważniejsze próba dopasowania się do obowiązujących w tej dziedzinie standardów światowych. Ważne jest więc zatrudnianie odpowiednich specjalistów, którzy w sposób kompetentny wspomogą w tym zakresie kierownictwo przedsiębiorstwa.

Powyższe rozważania wskazują na różnorodne możliwości wykorzystania norm obowiązującego prawa w zakresie zapewnienia ochrony informacji znajdujących się w dyspozycji przedsiębiorstwa turystycznego. W związku z powyższym brak jest uzasadnienia dla ewentualnych prób rozszerzenia zakresu regulacji w sferze świadczenia usług turystycznych o element ochrony informacji. Obserwowana praktyka wskazuje na potrzebę edukacji oraz uświadamiania funkcjonujących w turystyce podmiotów co do faktu istnienia oraz skuteczności światowych standardów ochrony informacji. Zaakceptowanie, przyjęcie oraz wdrożenie tychże norm stanowić może pierwszy krok do sukcesu w postaci bezpieczeństwa informacji. Działania te winny

być poparte stałą weryfikacją wprowadzonego systemu, połączoną z cyklem szkoleń realizowanych przez wyspecjalizowane osoby bądź instytucje. Teoria i praktyka ochrony informacji znajduje więc swoje szczególne miejsce również w sferze turystyki, przy odpowiednim dostosowaniu poszczególnych elementów do potrzeb tegoż środowiska. Istotnym jest by konstruowany system ochrony odpowiadał oczekiwanemu poziomowi bezpieczeństwa oraz uwzględniał potencjalne zagrożenia.