MODEL ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI W PRZEDSIĘBIORSTWIE
THE INFORMATION SECURITY MANAGEMENT MODEL IN THE ENTERPRISE

Lech KOŚCIELECKI

Lech.koscielecki@wat.edu.pl

Karolina DORAN

Wojskowa Akademia Techniczna

Wydział Logistyki

Streszczenie: W artykule podjęto problem modelu systemu zarządzania bezpieczeństwem informacji, który wymaga dużego zaangażowania kierownictwa organizacji. Bez niego nie będzie efektywny. Systemowe zarządzanie bezpieczeństwem informacji daje najlepsze rezultaty, ponieważ jest traktowane jako całość wszystkich procesów zachodzących w organizacji i jest z nimi spójne. Przy wdrożeniu systemu zarządzania bezpieczeństwem informacji najważniejsze jest opieranie się na najlepszych praktykach, zaś rodzaje wprowadzanych zabezpieczeń muszą być wybierane w taki sposób, aby minimalizowały ryzyko wystąpienia zagrożeń, jednocześnie nie utrudniając funkcjonowania przedsiębiorstwa.

Abstract The article addresses the issue of a model for an information security management system that requires a great deal of management involvement. Without it, it will not be effective. Systematic information security management gives the best results because it is treated as a whole and is consistent with all processes in the organization. When implementing an information security management system, the best thing to do is to build on best practices, and the types of security you have to put in place must be chosen in such a way that they minimize the risk, while not hindering your business.

Słowa kluczowe: zarządzanie, bezpieczeństwo, informacje.

Keywords: management, security, information

1.Wprowadzenie

Wszechobecna współcześnie rewolucja informacyjna, powiązana z rosnącym znaczeniem konkurencyjności, wiedzy i własności intelektualnej, legła u podstaw pojawienia się terminu „nowa gospodarka” (new economy). Stała się ona, w sposób naturalny, kolejnym etapem historycznego rozwoju gospodarek - po rewolucji przemysłowej i rewolucji naukowo-technicznej. Wkroczenie w erę nowej gospodarki oznacza zarazem początek tworzenia nowego ładu opartego na wiedzy, kreatywności, kapitale intelektualnym, postępie w zakresie telekomunikacji i informatyzacji.

O walorach współczesnego, skutecznie działającego przedsiębiorstwa, a zwłaszcza o jego sukcesie decydują takie czynniki jak: otwarty system informacyjny, kultura organizacyjna, charakterystyczna dla organizacji uczącej się, konstruktywny krytycyzm i konfrontacja, czyli gotowość do podważania stereotypów i efektywnego wykorzystania tego, co popularnie nazywamy synergią, a co jest rezultatem szeroko rozumianego łączenia sił i możliwości wewnątrz podmiotu gospodarczego z możliwościami znajdującymi się na zewnątrz (alianci, partnerzy biznesowi).

Współczesne zarządzanie przedsiębiorstwem jest zgoła odmienne od tradycyjnego. Mówi się o nowym informacyjnym paradygmacie zarządzania przedsiębiorstwem w XXI wieku. Informacyjny wzorzec działalności przedsiębiorstwa wymaga totalnego zaangażowania kadry w zdobywanie informacji, w „słuchanie otoczenia".

Informacje, jak odpowiednie zarządzanie nimi oraz umiejętnie wykorzystywana technika informatyczna przyczyniają się do szybkich i ciągłych zmian warunków działania każdego przedsiębiorstwa. Dysponowanie przez przedsiębiorstwo odpowiednim zasobem informacyjnym i infrastrukturą przetwarzającą te zasoby wpływa na jego konkurencyjność i sukces rynkowy. Menadżerowie, dysponując odpowiednimi informacjami, mogą swoje decyzje opierać na konkretach i realiach rynkowych, a nie na domysłach lub błędnych przesłankach.

Czym zatem jest bezpieczeństwo informacji w przedsiębiorstwie? Oznacza ono ochronę informacji przed szerokim spektrum zagrożeń w celu zapewnienia ciągłości działania, minimalizacji ryzyka i maksymalizacji zwrotu z inwestycji oraz możliwości biznesowych. Można je osiągnąć, wdrażając odpowiedni zestaw zabezpieczeń, którymi mogą być polityki, procesy, procedury, struktury organizacyjne, oraz funkcje oprogramowania i sprzętu. Od właściwego zrozumienia takich problemów, jak wartość aktywów informacyjnych i ich wpływu na określenie poziomu ochrony, znaczenia podatności i zagrożeń dla bezpieczeństwa informacji, bardzo często zależy, czy system bezpieczeństwa będzie efektywny, a także ekonomicznie uzasadniony, czy przedsiębiorstwo może bezpiecznie operować na rynku**.**

2. Propozycja rozwiązania problemu zarzadzania bezpieczeństwem informacji na szczeblu podmiotu gospodarczego

Prezentowana w artykule propozycja modelu zarządzania bezpieczeństwem informacji w przedsiębiorstwie odnosi się do uniwersalnego podmiotu i odzwierciedla aspekty jego działalności. Filozofia podejścia do rozważanego tematu i szczegóły rozstrzygnięć na poszczególnych etapach budowania modelu prezentowane były we wcześniejszych publikacjach autorów. Przyjęty w rozważaniach schemat działań wspomagający działalność przedsiębiorstwa w zakresie zarządzania bezpieczeństwem informacji powinien – w opinii autorów - kreować nowe dziedziny i sposoby działania przedsiębiorstwa (schemat 1.).

Cele, które przedsiębiorstwo ma w ten sposób osiągnąć, będą pochodną planowego działania proponowanego rozwiązania. Wymierną korzyścią płynącą z wprowadzenia proponowanego modelu będzie wzrost zysków.

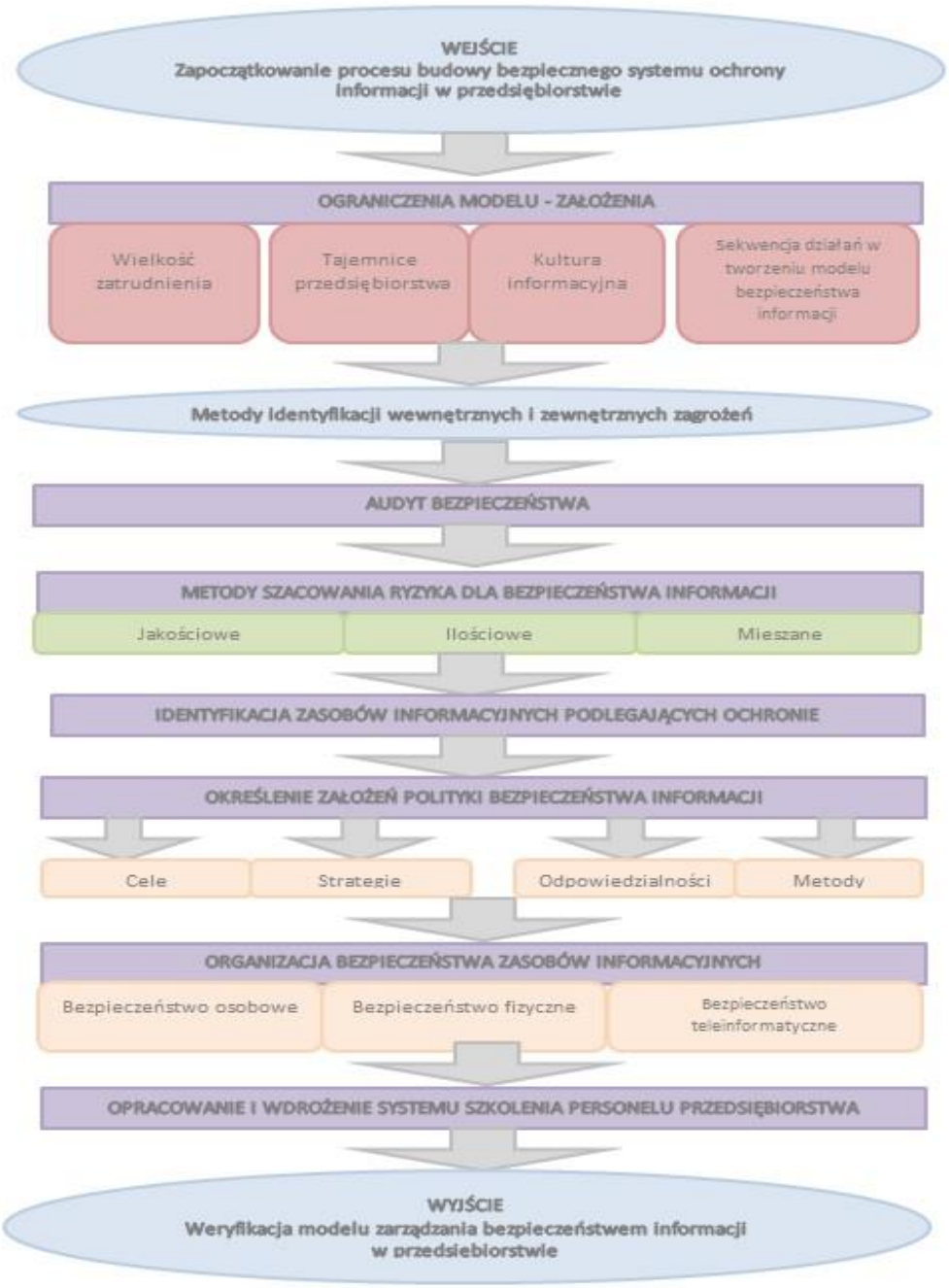
2.1. Ograniczenia modelu

Proponowany model zarządzania bezpieczeństwem informacji w przedsiębiorstwie oparto na kilku założeniach, które determinują i uzasadniają dalsze postulowane rozwiązania i ich zakres.

Założenie pierwsze. Propozycja dotyczy co najmniej średnich przedsiębiorstw, a więc zatrudniających nie mniej niż 50 osób, a nie więcej niż 250 osób, a ich roczny obrót nie przekracza 50 milionów euro lub roczna suma bilansowa nie przekracza 43 milionów euro.

Oczywiście proponowany model jest także rozwiązaniem dla wszystkich przedsiębiorstw większych, przekraczających wskazane bariery zatrudnieniowe i finansowe.

Schemat 1. Model zarzadzania bezpieczeństwem informacji w podmiocie gospodarczym



Źródło: opracowanie własne

W takich przedsiębiorstwach mamy do czynienia z jasno wyodrębnioną strukturą, podziałem zadań, pionami funkcjonalnymi, które to elementy nie są tak oczywiste ani konieczne

w przedsiębiorstwach mniejszych, np. w mikroprzedsiębiorstwach. Nie ma znaczenia dla podjętych rozważań forma własności, typ działalności, aktywność zagraniczna

(przedsiębiorstwo międzynarodowe), chociaż z punktu widzenia samego przedsiębiorstwa są to kwestie ogromnie istotne.

Założenie drugie. Proponowany model zarządzania bezpieczeństwem informacji dotyczy przedsiębiorstw, które posiadają (wytwarzają, przetwarzają, dystrybuują) informacje stanowiące tajemnicę przedsiębiorstwa w ustawowym rozumieniu tego pojęcia. W ustawie z dnia 16 kwietnia 1993 roku o zwalczaniu nieuczciwej konkurencji - 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. Tajemnicą przedsiębiorstwa jest zatem jedynie taka informacja, która kumulatywnie spełnia trzy przesłanki. Jest to informacja techniczna, technologiczna, organizacyjna przedsiębiorstwa lub inna posiadająca wartość gospodarczą, nieujawniona do wiadomości publicznej, co do której przedsiębiorca podjął niezbędne działania w celu zachowania jej poufności. Niespełnienie którejkolwiek przesłanki powoduje, że informacja jest ogólnie dostępna i każdy może z niej korzystać.

Założenie trzecie to warunek określonego poziomu kultury informacyjnej w przedsiębiorstwie. Jest to kategoria nieostra, chociaż niektórzy teoretycy uważają, iż kultura informacyjna może być obiektywnie mierzona oraz jest determinowana przez szereg zmiennych, takich jak misja, historia, przywództwo, osobiste doświadczenia pracowników, sektor, kultura narodowa i inne. Istnieje też pogląd, iż kultura informacyjna nie jest fragmentem kultury organizacyjnej, ale jej specyficzną odmianą. W takim ujęciu kultura informacyjna to „*kultura, która rozumie wartość i użyteczność informacji w osiąganiu sukcesu operacyjnego i strategicznego, w której informacja stanowi podstawę podejmowania decyzji zaś Technologia Informacyjna jest wykorzystywana jako czynnik umożliwiający działanie Systemów Informacyjnych*". Zaproponowana w tym ujęciu konceptualizacja kultury informacyjnej opiera się na wskazaniu siedmiu najistotniejszych komponentów, umożliwiających dokonanie oceny kultury informacyjnej organizacji:

- komunikacja,
- współpraca pomiędzy wydziałami funkcjonalnymi,
- docenianie wartości informacji,
- zarządzanie systemami informacyjnymi,
- środowisko wewnętrzne,
- zarzadzanie informacją,

- profesjonalizacja.

Należy przyjąć, iż kultura informacyjna przedsiębiorstwa stanowi o jakości wymiany oraz ochrony informacji i jej zabezpieczenia, stanowiących w istocie ochronę jego dorobku konkurencyjnego. Zasadniczym przesłaniem kultury informacyjnej przedsiębiorstwa jest niekrępowanie gromadzenia informacji, przetwarzania i rozpowszechniania przydatnych informacji przesadnymi lub niedostosowanymi środkami bezpieczeństwa. Informacja stanowi bowiem nieodłączny zasób przedsiębiorstwa. Ważnym jest zatem, aby mimo realnych zagrożeń wynikających z działań konkurencji, unikać swoistej „demonizacji" oraz przesadnej skłonności do zabezpieczania wszystkiego, wszędzie i bez przerwy. Obieg informacji w przedsiębiorstwie musi być zachowany, by mogło ono skutecznie realizować swoje działania na rynku, a jego siła tkwi w sprzyjaniu zachowania klimatu i kultury organizacyjnej korzystnych dla obiegu informacji oraz jej gromadzenia i wykorzystania.

Informacja może odegrać właściwą rolę wtedy, gdy zachowana jest możliwość dzielenia się nią jako zasobami służącymi przedsiębiorstwu, a wprowadzenie powszechnie znanego i akceptowanego systemu jej ochrony stanowi istotny czynnik spójności przedsiębiorstwa.

Dla potrzeb przyjętych rozwiązań można założyć więc, iż na kulturę informacyjną składają się wszystkie elementy kultury organizacyjnej, które wpływają na zarządzanie informacją i jej wykorzystanie. Tym samym kultura informacyjna ma odwzorowanie w wartościach, normach i praktykach organizacji, które odnoszą się do sposobu, w jaki informacja jest postrzegana, tworzona i wykorzystywana. Ważne w kontekście powyższych rozważań wydaje się znalezienie równowagi między dwiema filozofiami postępowania z informacją: filozofią otwartości (need to share), a filozofia niezbędnego dostępu do informacji (need to know).

W założeniu czwartym istotnym wydaje się przyjęcie określonej sekwencji działań w ramach tworzenia optymalnego modelu bezpieczeństwa informacji. Możliwe oraz akceptowalne dla większości ekspertów i samych przedsiębiorstw, byłoby przyjęcie następujących etapów budowy bezpiecznego systemu ochrony informacji:

1) identyfikacja wewnętrznych i zewnętrznych zagrożeń bezpieczeństwa informacji,
2) identyfikacja wewnętrznych zasobów informacyjnych podlegających ochronie,
3) opracowanie założeń polityki bezpieczeństwa informacji w formie dokumentu,

4) organizacja osobowego, fizycznego i teleinformatycznego bezpieczeństwa zasobów informacyjnych,
5) opracowanie i wdrożenie systemu szkolenia personelu przedsiębiorstwa.

Według takiej sekwencji działań podjęto próbę nakreślenia optymalnego modelu zarządzania bezpieczeństwem informacji.

2.2. Metody identyfikacji wewnętrznych i zewnętrznych zagrożeń

2.2.1. Audyt bezpieczeństwa w firmie

Audyt bezpieczeństwa informacyjnego w przedsiębiorstwie jest przedsięwzięciem postulowanym we wszystkich teoretycznych rozważaniach dotyczących zarządzania bezpieczeństwem. Jest częścią międzynarodowej normy ISO 27001:2007, programów wywiadu gospodarczego oraz innych autorskich rozwiązań. Jawi się jako niekwestionowany pierwszy krok w budowie optymalnego modelu bezpieczeństwa firmy, w zasadzie jest jedynym narzędziem pozwalającym rzetelnie ocenić poziom bezpieczeństwa informacji.

Audyt bezpieczeństwa informacji to podstawowa i kompleksowa forma dokonania analizy, systematyzacji i oceny istniejącego stanu ochrony informacji przetwarzanych w organizacji. Profesjonalnie przeprowadzony audyt pozwala przygotować dla kierownictwa raport ilustrujący stan faktyczny zasobów informacyjnych i ich poziom bezpieczeństwa.

Realizacja czynności audytorskich może być organizowana w dwóch formach: audytu wewnętrznego i zewnętrznego. W pierwszym przypadku audyt przeprowadzany jest przez zespół pracowników przedsiębiorstwa, wyznaczony do tych czynności decyzją zarządu, w drugim zaś audyt zlecony jest zewnętrznej wyspecjalizowanej instytucji konsultingowej lub grupie niezależnych ekspertów. W Polsce coraz więcej firm decyduje się na umieszczenie w swej strukturze organizacyjnej audytu wewnętrznego. Na zachodzie Europy i Stanach Zjednoczonych Ameryki Północnej jest to już standard. Audyt wewnętrzny winien być niezależny i obiektywny. Celem audytu wewnętrznego jest usprawnienie działań w organizacji oraz właściwy nadzór nad wykorzystywanymi zasobami. Audyt pomaga organizacji w osiąganiu jej celów poprzez systematyczne i zdyscyplinowane podejście do oceny i doskonalenia skuteczności procesów zarządzania ryzykiem oraz kontroli procesów nadzoru właścicielskiego.

Z uwagi na zakres, szczegółowość prowadzonych badań, audyt bezpieczeństwa informacji można podzielić na „zerowy" i główny. Pierwszy z nich jest formą podstawową, sygnalną. Ma on wyłącznie za zadanie dać odpowiedź, czy organizacja zapewnia niezbędny, akceptowalny poziom ochrony informacji, bez oceny poszczególnych elementów systemu. Drugi rodzaj jest kompleksową i szczegółową analizą wszystkich elementów bezpieczeństwa informacyjnego.

Dla sprawniejszego prowadzenia badań, a następnie dla efektywnej analizy wyników zasadnym jest stosowanie w procesie audytu jednolitych arkuszy ocen, a przede wszystkim jasno sprecyzowanego progu akceptowalności (tolerancji) zagrożeń.

Prawidłowy, profesjonalnie przygotowany i przeprowadzony audyt bezpieczeństwa informacyjnego powinien zakończyć się opracowaniem raportu – dokumentu przeznaczonego dla zarządu przedsiębiorstwa, w którym nakreślony winien być obraz faktycznego stanu zasobów informacyjnych i poziom ich bezpieczeństwa. zalecenia kluczowe.

2.2.2.Audyt według normy ISO 27001:2007

Audyty wewnętrzne są wymaganym i niezbędnym elementem systemowego zarządzania bezpieczeństwem informacji, a także jednym z ważniejszych elementów zapewniających utrzymanie i ciągłe doskonalenie systemu. Z tego powodu audyty są stałym elementem znormalizowanych systemów zarządzania.

Audyt to systematyczny, niezależny i udokumentowany proces uzyskiwania wniosków z audytu oraz jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu.

Audyt stał się skutecznym narzędziem stosowanym jako metoda kwalifikacji i ciągłej oceny dostawców. W praktyce jest to metoda kosztowna, ale jednocześnie bardzo skuteczna, pozwalająca nie tylko na ocenę, ale też prowadząca do doskonalenia zarządzania u dostawcy. Coraz częściej spotykany jest audyt dostawcy lub potencjalnego dostawcy pod kątem zarządzania bezpieczeństwem informacji.

Formalnym uwieńczeniem prac wdrożeniowych znormalizowanych systemów zarządzania bezpieczeństwem dotyczącym informacji, jakości, środowiska, BHP i innych jest audyt certyfikacyjny, dzięki któremu organizacja uzyskuje certyfikat poświadczający zgodność wdrożonego i funkcjonującego systemu zarządzania z wymaganiami normy.

Audyt jest bardzo cennym narzędziem zarówno w trakcie wdrażania, jak i na etapie doskonalenia systemu zarządzania. Trudno wyobrazić sobie właściwe utrzymanie i rozwój systemu bez ciągłego doskonalenia procesu audytu wewnętrznego, realizowanego w ramach tzw. zarządzania programami audytów.

Wykorzystanie metody audytu pozwala na ocenę, czy organizacja prezentuje wystarczający poziom zarządzania, aby można było uznać, że system:

- spełnia zaplanowane ustalenia;
- spełnia wymagania normy międzynarodowej PN-ISO/IEC 2700l:2007 oraz inne wymagania systemu zarządzania bezpieczeństwem informacji ustanowione przez organizację;
- jest skutecznie wdrożony i utrzymywany.

Audyt jest koniecznym elementem stosowanym także w innych systemach kształtowania jakości. Aby w pełni wykorzystać możliwości, jakie daje przeprowadzanie audytu, konieczna jest znajomość podstaw metody audytu oraz wymagań normy zarządzania bezpieczeństwem informacji, a także wymagań określonych w normie stanowiącej wytyczne do audytowania, tj. ISO 19011:2002.

Wyróżnia się trzy podstawowe typy audytów:

- audyt pierwszej strony, gdzie audytujemy własny system organizacji w celu sprawdzenia zgodności jego założeń i funkcjonowania z wymaganiami normy;
- audyt drugiej strony, w ramach którego audytowany jest system zarządzania naszego dostawcy;
- audyt trzeciej strony, podczas którego system zarządzania w organizacji jest audytowany przez jednostkę certyfikującą.

Norma ISO/IEC 27001 wymaga, aby kierownictwo przedsiębiorstwa zapewniło ustanowienie efektywnego i sprawnego procesu audytów wewnętrznych dla dokonywania systematycznej oceny mocnych i słabych stron SZBI. Audyty przeprowadzane są przez zespół audytorów, któremu przewodzi audytor wiodący. Audytor wiodący ponosi ostateczną odpowiedzialność za wszystkie fazy audytu, w związku z tym powinien posiadać umiejętności i doświadczenie w kierowaniu audytami oraz uprawnienia do podejmowania ostatecznych decyzji dotyczących wszystkich działań audytowych.

2.3. Szacowanie ryzyka dla bezpieczeństwa informacji

Pojęcie ryzyka ma wiele znaczeń. Najogólniej ujmując, jest to możliwość lub prawdopodobieństwo wystąpienia niekorzystnego w skutkach zdarzenia.

Znaczenie zarządzania ryzykiem informacji podnosi fakt, iż w nowej ustawie z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych pełnomocnikowi do spraw ochrony informacji niejawnych przypisano nowe zadanie, a mianowicie: *„zarządzanie ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowanie ryzyka”.* Dokonano jednocześnie próby definicji tego pojęcia, a mianowicie ryzykiem jest kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji. Szacowanie ryzyka to - według zapisów ustawy - całościowy proces analizy i oceny ryzyka, natomiast zarządzaniem ryzykiem są skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji, z uwzględnieniem ryzyka.

Podobną treść tych definicji przedstawiono w Polskiej Normie PN-ISO/IEC 27001:2007 – „Technika informatyczna - Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania”. Szacowanie ryzyka to całościowy proces analizy i oceny ryzyka. Analiza ryzyka to systematyczne wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka. Ocena ryzyka jawi się jako proces porównywania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka.

W teorii i praktyce stosowanych jest kilkadziesiąt metod szacowania i oceny ryzyka bezpieczeństwa informacji. Ogólnie dzieli się je na trzy grupy:

- metody jakościowe,
- metody ilościowe,
- metody mieszane.

Jakościowe szacowanie ryzyka opiera się najczęściej na subiektywnej ocenie, mającej swe podłoże w dobrych praktykach i doświadczeniu. W wyniku takiego szacowania powstają listy zagrożeń wraz z relatywnym rankingowaniem ryzyka (niskie, średnie, wysokie). Zaletą tych metod jest ich elastyczność i możliwość stosowania wszelkich możliwych modyfikacji. Dzięki temu w sposób kosztowo efektywny dostarczają organizacji wyników w zakresie identyfikacji zagrożeń i stosowania zabezpieczeń. Elastyczność tych metod sprawia jednocześnie, że zakres i koszt szacowania może być bardzo różny, dlatego zakres szacowania ryzyka może być zmienny w czasie w zależności od dostępnego budżetu.

Pozytywne aspekty stosowania metod jakościowych:

- proste i zrozumiałe kalkulacje i obliczenia (jeżeli występują);
- niekonieczna w większości wypadków wycena informacji (jej dostępności, poufności, integralności);
- niekonieczne ilościowe określenie skutków i częstotliwości wystąpienia zagrożeń;
- niekonieczne szacowanie kosztów rekomendowanych sposobów postępowania z ryzykiem i wyliczania potencjalnego zysku (straty);
- szerokie wskazanie znaczących obszarów ryzyka, na które konieczne jest zwrócenie uwagi;
- możliwość rozpatrywania i analizy przy szacowaniu takich elementów, jak wizerunek firmy, kultura organizacyjna, itd.;
- możliwość stosowania w sytuacji braku konkretnych informacji na temat zasobów czy danych ilościowych potrzebnych przy posłużeniu się metodami ilościowymi.

Dla podejścia ilościowego szacowania ryzyka kluczowe jest określenie dwóch podstawowych parametrów: wartości skutku i prawdopodobieństwa wystąpienia danego ryzyka. Konsekwencje jego wystąpienia mogą być wyrażane w różnych kategoriach, np.: pieniężnie, technicznie, operacyjnie, w zasobach ludzkich. Jakość i skuteczność analizy wykorzystującej podejście ilościowe jest uzależniona od dokładności wskazanych wartości i statystycznej walidacji użytego modelu.

Korzystne aspekty stosowania metod ilościowych to:

- szacowanie i wyniki są obiektywne, a dzięki temu porównywalne;
- wartość poszczególnych atrybutów informacji, czyli dostępności, integralności, poufności wyrażana jest w konkretnej kwocie;
- wyniki szacowania ryzyka mają swój wymiar finansowy i procentowy dzięki określaniu ich w ustalonej strukturze.

Do stron ujemnych metod ilościowych można zaliczyć:

- kalkulacje są wykonywane całościowo, w sytuacji braku ich wytłumaczenia i zrozumienia kierownictwo może nie ufać wynikom z szacowania ryzyka;
- metody ilościowe są niepraktyczne i nieefektywne, jeżeli nie stosuje się zautomatyzowanych narzędzi czy aplikacji informatycznych;
- niezbędne jest zbieranie wymiernych informacji na temat środowiska IT, zabezpieczeń, zasobów.

Zarówno metody ilościowe, jak i metody jakościowe mają swoje niedoskonałości: niedokładnie identyfikują wszelkie potrzeby, są zbyt ogólne, nie dostarczają informacji na temat analizy kosztowej w zakresie wprowadzenia nowych zabezpieczeń. Powoduje to stosowanie przez wiele przedsiębiorstw kombinacji tych dwóch rozwiązań. Przeprowadza się analizy jakościowe do identyfikowania wszystkich obszarów ryzyka i ich skutków przy jednoczesnym użyciu ilościowej analizy do określenia kosztów skutków wystąpienia ryzyka. Dzięki temu zwiększa się wiedza na temat procesów realizowanych w organizacji i poziom uświadomienia sobie przez managerów potencjalnego ryzyka.

Ocena ryzyka jest związana z modelowaniem zdarzeń. Pojawienie się rozważanego niekorzystnego zdarzenia o zależy często od wielu rzadko występujących zdarzeń cząstkowych, dla których należy zbadać:

- prawdopodobieństwo ich wystąpienia;
- znajomość związków przyczynowo skutkowych zachodzących między nimi.

Informacje o prawdopodobieństwie wystąpienia zdarzeń cząstkowych można czerpać z różnych źródeł, ale najczęściej są to dane statystyczne gromadzone przez instytucje rządowe, organizacje zajmujące się daną problematyką, szacunki ekspertów itp.

Drugim problemem jest wypracowanie modelu określania związków przyczynowo skutkowych, jakie łączą zdarzenia cząstkowe. Według A. Białasa szeroki wachlarz metod oceny ryzyka można podzielić na dwie zasadnicze grupy:

- metody zstępujące, od ogółu do szczegółu, cechujące się dedukcyjnym badaniem przyczyn znanych skutków;
- metody wstępujące, od szczegółu do ogółu, polegające na indukcyjnym wnioskowaniu o możliwych skutkach znanych przyczyn.

Pojęcie ryzyka – według niego – wiąże możliwość (prawdopodobieństwo, częstość) wystąpienia zdarzenia z wielkością strat, które może ono powodować (konsekwencja zdarzenia). Potrzebna jest w tym wypadku ogólna ocena sytuacji i możliwość porównywania zjawisk rzadkich, ale dotkliwych, z częstymi, ale mniej groźnymi w skutkach. Ocena sytuacji pozwala wyznaczyć obszar ryzyka istotnego, podlegającego redukcji. Problem ryzyka bezpieczeństwa informacji w działalności przedsiębiorstwa należy postrzegać w szerszym kontekście zarzadzania ryzykiem gospodarczym (biznesowym), które w języku angielskim określane jest jako Industry Risk Management.

Ryzyko gospodarcze dotyczy wszystkich rodzajów zagrożeń, w obliczu których stoi lub może stanąć przedsiębiorstwo, a więc ryzyko bezpieczeństwa informacji jest tylko jednym z zagrożonych obszarów. Zagrożenia gospodarcze przedsiębiorstwa generowane są przez zmiany w krajobrazie gospodarczym, które w literaturze określane są zmianami strukturalnymi. Źródłem zmian strukturalnych mogą być zmieniające się potrzeby klientów, zmiany strategii konkurentów, nowe wejścia i alianse, gwałtowny wzrost pozycji dostawców czy nowa polityka rządowa. Identyfikacja tych zagrożeń wymaga specjalnego paradygmatu - systemu wczesnego ostrzegania. Zarządzanie kryzysowe to wypracowanie takich działań, które przygotują przedsiębiorstwa do odpowiedniej reakcji na dokonujące się zmiany. Obejmuje ono koordynację i kierowanie wszystkimi mechanizmami przedsiębiorstwa, na wszystkich szczeblach zarządzania. Polityka bezpieczeństwa informacji jest naturalnie ważnym elementem podejmowanych działań.

Proces zarządzania ryzykiem gospodarczym obejmuje dwa etapy: identyfikację zagrożenia oraz jego minimalizację.

Identyfikacja zagrożeń gospodarczych następuje poprzez strategiczny system wczesnego ostrzegania SSWO (ang. SEWS – Strategic Early Warning System). Jego budowa winna obejmować następujące etapy:

- **Sporządzenie mapy obszarów wysokiego ryzyka** – stosując narzędzia jakościowe (takie jak gry wojenne, opracowywanie symulacji) lub bardziej ilościowe podejścia, zwłaszcza w finansach (tabele przewidywanych strat), specjaliści winni dokonać podziału aktualnych działań w przedsiębiorstwie i branży na kategorie z niskim, średnim i wysokim ryzykiem; stosując wybór „*czarnego*" scenariusza będą mogli ocenić możliwe straty przedsiębiorstwa wpływające na jego aktualną pozycję konkurencyjną.
- **Budowa wskaźników ostrzegawczych** – obszary wysokiego ryzyka winny być objęte wczesnym ostrzeganiem poprzez wskaźniki zarówno ilościowe, jak i jakościowe; wskaźniki winny być budowane w połączeniu z odpowiednimi segmentami i do nich się odnosić (np. zarządzanie przedsiębiorstwem, zarządzanie produktem, zarządzanie funkcjonalne).
- **Monitorowanie wskaźników** – opracowany powinien być plan monitoringu identyfikującego źródła (zarówno osobowe, jak i publikowane, wewnętrzni i zewnętrzni eksperci), który może dostarczyć danych wyjściowych do budowy wskaźników; wczesne ostrzeganie i działanie we właściwym czasie jest kwestią podstawową.

- **Uruchamianie alarmów** – alarm jest uruchamiany, kiedy dany wskaźnik przekracza przyjęty próg ryzyka, próg krytyczny; kalkulacja tych progów winna być oparta na danych, projektach lub na podstawie konsensusu ekspertów.

Drugim etapem w zarządzaniu ryzykiem jest kierowanie akcją mającą na celu zapobieganie stratom lub zminimalizowanie szkód. Zmniejszanie zagrożenia zwykle przejawia się w podjęciu jednej z czterech kategorii działań (w drastycznych przypadkach czterech naraz):

- rewizja strategii marketingowej,
- rewizja strategii operacyjnej,
- reakcja w obszarze rozwijania biznesu,
- przyspieszanie/opóźnianie prac badawczo-rozwojowych.

Ostateczna decyzja strategiczna spoczywa na zarządzie firmy, który alarm otrzymał, ale rola wywiadu nie powinna się na alarmowaniu kończyć. Śledzenie i koordynowanie działań zapobiegawczych oraz ich dozbrajanie w efektywne „*narzędzia*" winny być naturalną i poszerzoną funkcją zarządzania ryzykiem.

Minimalizacja ryzyka w obszarze bezpieczeństwa informacyjnego jest realizowana w postaci szeregu zabezpieczeń, które mają na celu ograniczenie ryzyka do akceptowalnego poziomu. Będą one szerzej omawiane w trakcie budowy modelu bezpieczeństwa informacyjnego firmy, ale już w tym miejscu warto wspomnieć – w ślad za Donaldem L. Pipkinem – iż zabezpieczania te mogą mieć charakter zapobiegawczy (proaktywny), chroniąc informacje, zanim zdarzy się incydent, lub reaktywny, stanowiąc odpowiedź na wykrycie incydentu. W obu przypadkach zabezpieczania winny być spójne, kompletne i efektywne kosztowo.

2.4. Identyfikacja zasobów informacyjnych podlegających ochronie

Należy przyjąć, iż w „klasycznym" przedsiębiorstwie przetwarzane są dwa rodzaje informacji podlegających z mocy prawa ochronie:

- dane osobowe,
- informacje stanowiące tajemnice przedsiębiorstwa.

Dodatkowo, przedsiębiorstwa na podstawie zawartych kontraktów mogą przetwarzać informacje niejawne, ale w tym przypadku zobowiązane są uzyskać świadectwa bezpieczeństwa przemysłowego i stworzyć systemy bezpieczeństwa certyfikowane przez odpowiednie służby specjalne państwa.

Należy, dla klarowności dalszego wywodu przypomnieć, iż 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. Nie każda informacja posiadająca wartość gospodarczą, nieujawniona do informacji publicznej, stanowi tajemnicę przedsiębiorstwa. Staje się ona nią wtedy, gdy przedsiębiorca podejmie „niezbędne działania" w celu zachowania jej w poufności. To przedsiębiorca decyduje o utajnieniu informacji nieujawnionej publicznie, a zatem o uznaniu jej za tajemnicę przedsiębiorstwa.

Tajemnica przedsiębiorstwa powstaje zatem z woli przedsiębiorcy. Informacja nieujawniona do wiadomości publicznej podpada pod pojęcie „tajemnicy", kiedy przedsiębiorca ma wolę, by pozostała ona tajemnicą dla pewnych kół odbiorców i konkurentów. Wola ta dla innych osób musi być rozpoznawalna. Bez takiej woli, choćby tylko dorozumianej, informacja może być nieznana, ale nie będzie tajemnicą.

W literaturze przyjęła się szeroka interpretacja ustawowego określenia „informacje techniczne, technologiczne, handlowe lub organizacyjne przedsiębiorstwa". Przez informacje chronione uważa się m.in.:

- patenty lub nieopatentowane wynalazki, wzory użytkowe lub zdobnicze,
- plany techniczne,
- sposoby zbierania informacji,
- listy klientów,
- metody kontroli jakości i usług,
- sposoby prowadzenia marketingu,
- sposoby organizacji pracy,
- informacje przydatne w pracy naukowo-badawczej i rozwojowej,
- know-how,
- wyniki prób i badań (także te, które nie nadają się do praktycznego wykorzystania),
- informacje o ujemnych skutkach stosowania leku lub środka ochrony roślin,
- wstępne projekty rozwiązań technologicznych wymagające dalszych prac rozwojowych,
- przedmioty własności intelektualnej chronione przepisami prawa autorskiego.

Powyższy katalog jest otwarty, w różnych przedsiębiorstwach do informacji stanowiących tajemnicę przedsiębiorstwa można zaliczyć zgoła inne kategorie i rodzaje informacji.

W każdym przedsiębiorstwie winien być stworzony dokument pod roboczą nazwą „Wykaz informacji stanowiących tajemnicę przedsiębiorstwa firmy X.", przyjęty na podstawie uchwały zarządu przedsiębiorstwa.

Informacje tam zebrane winny, dla celów praktycznych, być podzielone na grupy na podstawie następujących czynników:

- znaczenia informacji dla interesów przedsiębiorstwa,
- zasad przetwarzania informacji,
- podziału organizacyjnego przedsiębiorstwa,
- zasad ochrony informacji,
- dostępu do informacji i zakresu tego dostępu,
- systemów przetwarzania informacji.

Biorąc te kwestie pod uwagę, można zaproponować wyodrębnienie następujących grup informacji podlegających ochronie:

- sprawy ogólne,
- organizacja i zarządzanie przedsiębiorstwem,
- informacje ekonomiczne i finansowe,
- sprawy pracownicze,
- działalność handlowa,
- infrastruktura teleinformatyczna,
- bezpieczeństwo,
- prace rozwojowe.

Powyższy podział nie jest podziałem absolutnym, powinien odzwierciedlać aktualne uwarunkowania i podlegać zmianom na podstawie decyzji zarządu spółki lub wyznaczonego głównego administratora informacji. W każdej z tych grup następuje podział na podgrupy informacji, w zależności od potrzeb i specyfiki przedsiębiorstwa,

Jest to propozycja, która może być adoptowana w wielu zmodyfikowanych formach, w zależności od rozmiaru przedsiębiorstwa, jego struktury, profilu, wartości chronionych informacji i wielu innych czynników wpływających na powodzenie biznesowe.

2.4. Określenie założeń polityki bezpieczeństwa informacji

Polityka bezpieczeństwa tworzy bazę do opracowania i wdrożenia akceptowanych koncepcji bezpieczeństwa. Jest podstawowym, długoterminowym dokumentem, w którym przedstawiono cele, strategie, odpowiedzialność i metody oraz ich wzajemnie powiązania gwarantujące osiągnięcie założonego poziomu bezpieczeństwa.

Cele, strategie oraz polityka powinny być rozwijane w przedsiębiorstwie hierarchicznie z najwyższego szczebla zarządzania do poziomu operacyjnego. Zadaniem polityki bezpieczeństwa informacji jest określenie wszystkich aspektów bezpieczeństwa i ochrony procesów przetwarzania informacji w przedsiębiorstwie.

Polityka bezpieczeństwa powinna:

- stanowić dokument w formie pisemnej,
- zawierać ogólne wytyczne bezpieczeństwa,
- być dokumentem przyjętym oficjalnie przez zarząd przedsiębiorstwa.

Przykładowy układ dokumentu „Polityka bezpieczeństwa w przedsiębiorstwie X" przedstawiono na schemacie 2.2.

Schemat 2.2. Zawartość dokumentu „Polityka bezpieczeństwa przedsiębiorstwa"

1. Definicje
2. Opis sytuacji bezpieczeństwa w przedsiębiorstwie
3. Cele polityki bezpieczeństwa
4. Zakres polityki bezpieczeństwa
5. Dokumenty polityki bezpieczeństwa
6. Główne założenia
7. Identyfikacja zasobów
8. Zasady dostępu do informacji
9. Zasady zarządzania informacjami
10. Zasady przetwarzania i ochrony informacji
11. Wymagania dla systemów przetwarzania informacji
12. Sytuacje kryzysowe
13. Kontrola wewnętrzna stanu bezpieczeństwa informacji stanowiących tajemnicę
14. Doskonalenie systemu bezpieczeństwa informacji
15. Zmiany
16. Załączniki

Źródło: opracowanie własne

2.4.1. Cele i strategie

Przy tworzeniu polityki bezpieczeństwa muszą być uwzględnione cele przedsiębiorstwa, którym polityka bezpieczeństwa ma służyć. Takimi celami mogą być m.in.:

- zagwarantowanie prawnych wymagań ochrony informacji (np. danych osobowych, informacji niejawnych),
- zagwarantowanie zaufania publicznego i prestiżu przedsiębiorstwa,
- bezpieczeństwo ciągłości funkcjonowania przedsiębiorstwa,
- redukcja wzrostu kosztów.

Głównym celem ustanowienia w przedsiębiorstwie polityki bezpieczeństwa informacji jest stworzenie podstaw do zapewnienia właściwej ochrony przetwarzanych informacji stanowiących tajemnicę przedsiębiorstwa, których upublicznienie mogłoby zagrozić jego bezpieczeństwu i jego interesariuszy. Powyższy cel realizowany jest poprzez osiągnięcie celów szczegółowych:

- zapewnienie, że informacje stanowiące tajemnicę przedsiębiorstwa zachowają poufność, integralność, dostępność, autentyczność, rozliczalność, niezaprzeczalność,
- zidentyfikowanie zagrożeń i świadome zarządzanie ryzykiem,
- ustanowienie struktury organizacyjnej zarządzania bezpieczeństwem informacji stanowiących tajemnicę przedsiębiorstwa oraz uprawnień i odpowiedzialności osób uczestniczących w procesie przetwarzania tych informacji,
- zapewnienie bezpieczeństwa systemów, w których odbywa się proces przetwarzania informacji stanowiących tajemnicę przedsiębiorstwa,
- zapewnienie ciągłego podnoszenia stanu bezpieczeństwa informacji stanowiących tajemnicę przedsiębiorstwa poprzez aktualizację mechanizmów ochrony oraz podnoszenie kwalifikacji pracowników w zakresie bezpieczeństwa informacji.

Osiągnięcie tak zdefiniowanych celów polityki bezpieczeństwa możliwe jest dzięki wypracowaniu określonej strategii. Polityka bezpieczeństwa powinna te strategie formułować na dość ogólnym poziomie. Dokładne opisy powinny być dokonane na poziomie grupy chronionych informacji, systemu informacji i systemów przetwarzania informacji. Do obszarów, dla których powinny być opracowane strategie, można zaliczyć[1]:

- metody osiągania wymaganego poziomu bezpieczeństwa,

[1] L. Kiełtyka, Ochrona i bezpieczeństwo informacji…, s. 233.

- przyporządkowanie ról i odpowiedzialności w procesie budowania bezpieczeństwa,
- zarzadzanie poprzez system jakości,
- rozwój polityk bezpieczeństwa dla każdej grupy informacji i dla każdego systemu przetwarzania,
- bezpieczna wymiana informacji.

2.4.2. Zakres polityki bezpieczeństwa informacji

Polityka bezpieczeństwa informacji powinna mieć zastosowanie do:

- wszystkich informacji określonych w „Wykazie informacji stanowiących tajemnicę przedsiębiorstwa" bez względu na ich formę oraz system, w którym następuje ich przetwarzanie;
- wszystkich pracowników przedsiębiorstwa, którzy posiadają uprawnienia do przetwarzania informacji stanowiących tajemnicę przedsiębiorstwa;
- wszystkich istniejących systemów przetwarzania informacji stanowiących tajemnicę przedsiębiorstwa,
- wszystkich miejsc, bez względu na ich lokalizację, w których następuje przetwarzanie informacji stanowiących tajemnicę przedsiębiorstwa,
- klientów przedsiębiorstwa oraz osób współpracujących z nim na podstawie odrębnych umów określających ich zakres, formę i czas współpracy.

Tak sformułowana polityka bezpieczeństwa informacji nie ma zastosowania do przetwarzania informacji zawierających dane osobowe, które podlegają ochronie z mocy ustawy o ochronie danych osobowych. Obszar ten należy uregulować odrębnie w oparciu o takie dokumenty, jak: Polityka bezpieczeństwa danych osobowych, Instrukcja zarządzania systemami informatycznymi oraz na innych dokumentach, które powinny być wydane w tym celu przez organ zarządzający przedsiębiorstwem.

5.5. Organizacja bezpieczeństwa osobowego, fizycznego i teleinformatycznego zasobów informacyjnych

5.5.1. Bezpieczeństwo osobowe

Pierwszym działaniem w zakresie zapewnienia bezpieczeństwa zasobów informacyjnych winno być precyzyjne określenie odpowiedzialności personalnej za

przetwarzanie i bezpieczeństwo informacji oraz - w konsekwencji - wyznaczenie osób funkcyjnych odpowiedzialnych za ten obszar.

Biorąc pod uwagę to, że w przedsiębiorstwie zidentyfikowano zasoby informacyjne stanowiące tajemnicę przedsiębiorstwa i dokonano ich klasyfikacji w grupy informacji oraz określono systemy przetwarzania informacji, wydaje się, iż optymalnym rozwiązaniem byłoby wyznaczenie następujących osób funkcyjnych:

1) główny administrator informacji,
2) główny administrator bezpieczeństwa informacji,
3) administrator grupy informacji,
4) administrator bezpieczeństwa grupy informacji,
5) administrator sytemu,
6) administrator bezpieczeństwa systemu.

Jak wynika z podziału kompetencji, zasady dostępu do informacji stanowiących tajemnicę przedsiębiorstwa ustala główny administrator informacji. Zgodnie z założeniami przyjętymi w dokumencie głównym „*Polityka bezpieczeństwa informacji stanowiących tajemnice przedsiębiorstwa*" dostępu do tego rodzaju informacji udziela się:

- właścicielom (udziałowcom) przedsiębiorstwa,
- członkom zarządu,
- członkom organu nadzorczego – jeżeli zostanie powołany,
- pracownikom przedsiębiorstwa,
- osobom lub firmom wykonującym zlecenia lub zadania na rzecz przedsiębiorstwa na podstawie umowy,
- partnerom biznesowym na podstawie stosownych umów o współpracy,

w zakresie i na czas niezbędny do realizacji zadań wynikających z pełnionej funkcji lub wykonania umowy, zgodnie z zasadą „wiedzy koniecznej" (need to know).

Szczegółowy zakres dostępu do informacji dla poszczególnych grup użytkowników w ramach grup informacji określa się indywidualnie w procesie nadawania uprawnień dostępowych. Udzielenie użytkownikowi dostępu do informacji stanowiących tajemnicę przedsiębiorstwa następuje po spełnieniu przez niego następujących warunków:

- użytkownik został zapoznany z „Wykazem informacji stanowiących tajemnicę przedsiębiorstwa",
- został zapoznany z regulaminem ochrony informacji,

- złożył pisemne oświadczenie o znajomości ww. wykazu oraz regulaminu,
- złożył pisemne zobowiązanie do zachowania tajemnicy przedsiębiorstwa.

Decyzję w sprawie udzielenia dostępu do informacji stanowiących tajemnicę przedsiębiorstwa, z jednoczesnym określeniem zakresu informacji, wydaje administrator grupy informacji (główny administrator informacji). Wszyscy użytkownicy, którzy uzyskali taki dostęp, podlegają ewidencji w stosownym wykazie prowadzonym przez głównego administratora bezpieczeństwa informacji. Użytkownicy informacji mogą stracić wszelkie prawa do dostępu do tych informacji, gdy informacja stanowiąca tajemnicę przedsiębiorstwa nie będzie im więcej potrzebna lub w przypadku naruszenia zasad polityki bezpieczeństwa informacji. Decyzję o cofnięciu praw dostępu do informacji stanowiących tajemnicę wydaje główny administrator informacji na wniosek głównego administratora bezpieczeństwa informacji, z zastrzeżeniem, że nie mogą być cofnięte uprawnienia dostępu do informacji właścicielom (udziałowcom) przedsiębiorstwa oraz członkom organu nadzorczego, wynikające z zakresu informacji określonego w stosownych przepisach prawa, w tym szczególnie w kodeksie spółek handlowych.

Kwestie dostępu do informacji są odmiennie regulowane w różnych systemach przetwarzania informacji. Należy przyjąć, iż w „klasycznym" przedsiębiorstwie funkcjonują trzy systemy przetwarzania informacji:

- system tradycyjny - oparty na przetwarzaniu informacji stanowiących tajemnicę przedsiębiorstwa zawartych w dokumentach papierowych oraz zarejestrowanych na innych trwałych nośnikach nieelektronicznych,
- system informatyczny - przetwarzający informacje stanowiące tajemnicę przedsiębiorstwa zarejestrowane jako pliki cyfrowe,
- system poczty elektronicznej (e-mail) - przetwarzane informacje stanowiące tajemnicę przedsiębiorstwa mają postać wiadomości i plików cyfrowych.

W tradycyjnym systemie stały dostęp do niego oraz prawo do wykorzystywania jego elementów do przetwarzania informacji przysługuje wyłącznie pracownikom przedsiębiorstwa posiadającym upoważnienie do przetwarzania takich informacji. Ponadto dostęp mogą mieć członkowie rady nadzorczej, zgodnie z posiadanym zakresem dostępu, po nadaniu im uprawnień przez administratora bezpieczeństwa systemu.

W przypadku systemu informatycznego udzielenie dostępu wiąże się z ustanowieniem dostępu do następujących elementów:

- sieci Wi-Fi (jeśli taka funkcjonuje),
- stanowiska komputerowego (stacjonarnego i/lub mobilnego) – logowanie do systemu operacyjnego,
- wydzielonej, zaszyfrowanej partycji na dysku w przydzielonym sprzęcie komputerowym,
- przydzielonego, zabezpieczonego zewnętrznego nośnika danych.

Stały dostęp do systemu oraz możliwość wykorzystywania jego elementów do przetwarzania informacji stanowiących tajemnicę przedsiębiorstwa mogą mieć wyłącznie pracownicy posiadający upoważnienie do przetwarzania takich informacji oraz - zgodnie z posiadanym zakresem dostępu, po nadaniu im uprawnień dostępowych przez administratora bezpieczeństwa systemu - członkowie zarządu i rady nadzorczej. Warunkowy dostęp do systemu mogą uzyskać przedstawiciele administracji państwowej, na zasadach określonych w przepisach prawa.

W systemie poczty elektronicznej (e-mail) stały dostęp do systemu oraz wykorzystywania jego elementów do przetwarzania informacji stanowiących tajemnicę przedsiębiorstwa mogą posiadać wyłącznie pracownicy.

Dostęp do systemu poczty e-mail przez uprawnionych użytkowników może być realizowany:

- przy użyciu urządzeń dopuszczonych do przetwarzania informacji stanowiących tajemnicę przedsiębiorstwa w formie plików cyfrowych;
- przy użyciu aplikacji „klienta pocztowego” zapewniającej: możliwość szyfrowania połączenia (SSL), logowania z użyciem ustanowionego loginu i hasła, zapisywania wiadomości wyłącznie na serwerze pocztowym, dopuszczonej do eksploatacji w systemie przez administratora bezpieczeństwa systemu.

Kontrolę dostępu do systemu poczty e-mail winno się zapewnić poprzez zastosowanie mechanizmów uwierzytelniania (logowanie) do urządzeń, do kont pocztowych oraz rejestracji na serwerze pocztowym raportów z logowania.

Hasło dostępu do konta pocztowego winno stanowić tajemnicę przedsiębiorstwa i podlegać szczególnej ochronie. Zabrania się ujawniania hasła dostępu do konta pocztowego wszystkim innym osobom niż użytkownik konta, do którego hasło jest przypisane. Hasło dostępu (logowania) do konta pocztowego powinno podlegać cyklicznym zmianom.

5.5.2. Bezpieczeństwo fizyczne

Organizując modelowe rozwiązania w zakresie bezpieczeństwa fizycznego informacji stanowiących tajemnice przedsiębiorstwa warto odwołać się i brać wzorce z istniejących rozwiązań prawnych (ale też praktycznych), jakie stworzono do ochrony informacji niejawnych.

Przyjąć należy, iż system ochrony fizycznej informacji stanowiących tajemnicę przedsiębiorstwa powinien być szczegółowo opisany w dokumencie stanowiącym załącznik do „Polityki bezpieczeństwa informacji" (np. jako plan ochrony fizycznej), a przyjęte środki bezpieczeństwa fizycznego powinny być konsekwencją oceny istniejących zagrożeń. Ponadto należy uznać, iż nie ma rozwiązań uniwersalnych i że każdorazowo to przedsiębiorca decyduje, jaki wdroży wachlarz środków bezpieczeństwa fizycznego.

Z rozwiązań proponowanych dla zapewnienia fizycznego bezpieczeństwa informacji niejawnych można na grunt przedsiębiorstwa, które w sposób skuteczny chce chronić tajemnice, przenieść następujące elementy:

- metodykę oceny zagrożeń,
- system środków bezpieczeństwa fizycznego,
- organizację stref ochronnych,
- organizację systemu kancelaryjnego.

5.5.3. Bezpieczeństwo teleinformatyczne

Informacje w formie elektronicznej, jak założono w przypadku modelowego rozwiązania, są przetwarzane w dwóch systemach:

- systemie informatycznym,
- systemie poczty e-mail.

Systemy te winy spełniać następujące wymogi:

- posiadają własną „politykę bezpieczeństwa" w formie zatwierdzonego dokumentu,
- wyznaczono osoby funkcyjne: administratora systemu oraz administratora bezpieczeństwa systemu,
- posiadają procedury przyznawania praw dostępu,
- składają się wyłącznie z elementów dopuszczonych do przetwarzania informacji stanowiących tajemnicę przedsiębiorstwa, stosownie oznaczonych, podlegających

kontroli przez cały czas eksploatacji i posiadają mechanizmy zabezpieczające informację przed nieautoryzowanym zniszczeniem lub przed kradzieżą,

- uniemożliwiają w istotny sposób nieautoryzowany dostęp do informacji,
- posiadają mechanizmy pozwalające wykrywać próby nieautoryzowanego dostępu do informacji,
- zapewniają możliwość prowadzenia kontroli dostępu do informacji:
- posiadają mechanizmy pozwalające wykryć próby nieautoryzowanego dostępu do informacji,
- posiadają mechanizmy bezpowrotnego niszczenia informacji.

Typowy system informatyczny w przedsiębiorstwie składa się z automatycznych stanowisk komputerowych, stacjonarnych i mobilnych (komputery, laptopy, tablety), z urządzeń peryferyjnych (drukarki), serwerów zewnętrznych oraz zewnętrznych nośników danych. W polityce bezpieczeństwa teleinformatycznego należy przestrzegać następujących zasad:

- w ramach przedsiębiorstwa nie jest wykorzystywana sieć wewnętrzna pozwalająca na bezpośrednie połączenia i transmisję danych między poszczególnymi stanowiskami komputerowymi, wszelka transmisja danych w postaci plików cyfrowych odbywa się poprzez Internet (poczta e-mail),
- serwery zewnętrzne przedsiębiorstwa nie są wykorzystywane do przetwarzania informacji stanowiących tajemnicę przedsiębiorstwa,
- każde stanowisko komputerowe (stacjonarne i mobilne) posiada wydzieloną, zaszyfrowaną partycję dyskową przeznaczoną do przechowywania plików zawierających informacje stanowiące tajemnicę przedsiębiorstwa, a do każdego stanowiska komputerowego przydzielony jest zewnętrzny nośnik danych, z mechanizmem zabezpieczenia plików (szyfrowanie), przeznaczony do wykonywania kopii zapasowych,
- każdemu użytkownikowi systemu przydziela się zewnętrzny nośnik danych, z mechanizmem zabezpieczenia plików (szyfrowanie), przeznaczony do doraźnego przechowywania plików lub do umożliwienia przekazywania plików między uprawnionymi użytkownikami,
- każdy komputer mobilny posiada aktywny program antywirusowy,
- urządzenia wchodzące w skład systemu (komputery, tablety, drukarki, router, firewall) podlegają ewidencji i oznaczeniu.

5.6. Wdrażanie systemu szkolenia personelu przedsiębiorstwa

Szkolenia w zakresie bezpieczeństwa informacji winny mieścić się w szerszym procesie doskonalenia bezpieczeństwa obejmującym stałą analizę zagrożeń dla bezpieczeństwa informacji, modernizację technicznych środków bezpieczeństwa – technicznych systemów zabezpieczających – na podstawie analizy zmian wynikających z rozwoju technologicznego oraz analizy zagrożeń, aktualizację oprogramowania służącego do przetwarzania i ochrony informacji w systemach elektronicznych, prowadzenie okresowych zewnętrznych audytów bezpieczeństwa w zakresie oceny stosowanych rozwiązań, prowadzenie rocznych i doraźnych kontroli wewnętrznych stanu bezpieczeństwa tajemnicy przedsiębiorstwa oraz prowadzenie cyklicznych szkoleń dla pracowników upoważnionych do przetwarzania informacji stanowiących tajemnicę przedsiębiorstwa.

System szkolenia personelu przedsiębiorstwa w zakresie bezpieczeństwa informacji winien być precyzyjnie określony w dokumencie „Polityka bezpieczeństwa informacji stanowiących tajemnicę przedsiębiorstwa". Chodzi o rodzaje szkoleń, cele, zakres oraz częstotliwość. Podobnie jak w przypadku innych kwestii związanych z bezpieczeństwem, tak i w zakresie szkoleń to przedsiębiorca decyduje o tym, w jaki sposób ma być doskonalona wiedza i świadomość bezpieczeństwa podległych pracowników.

Zakres tematyki szkoleń i ich szczegółowość zależą od wielu czynników, ale przede wszystkim od znaczenia problematyki bezpieczeństwa w przedsiębiorstwie. Powinny być one zróżnicowane według szczebla i charakteru stanowiska pracy, czyli roli odgrywanej w systemie bezpieczeństwa przedsiębiorstwa. Rola ta określa zasady dostępu do określonej informacji.

System szkolenia w zakresie bezpieczeństwa informacji w przedsiębiorstwie można oprzeć również na wzorcu, który jest wypracowany i stosowany w zakresie ochrony informacji niejawnych. Można w związku z tym przewidzieć w przedsiębiorstwie następujące rodzaje szkoleń:

- podstawowe,
- uzupełniające,
- specjalistyczne

Szkolenie podstawowe byłoby pierwszym szkoleniem na stanowisku pracy, dopuszczającym do pełnienia obowiązków związanych z przetwarzaniem informacji stanowiących tajemnicę przedsiębiorstwa. Szkolenie takie prowadziłby główny administrator

bezpieczeństwa informacji, a po jego zakończeniu pracownik pisemnie oświadczyłby, iż zapoznał się z zasadami ochrony tajemnicy przedsiębiorstwa oraz podpisałby zobowiązanie do zachowania tej kategorii informacji w poufności.

Szkoleniem uzupełniającym objęte byłyby wszystkie osoby mające dostęp do informacji stanowiących tajemnicę przedsiębiorstwa. Można je organizować cyklicznie 1-2 razy w roku.

Celem tego szkolenia byłoby pogłębienie wiedzy uzyskanej podczas szkolenia podstawowego. Byłoby ono okazją do omówienia wszelkich nieprawidłowości występujących w pracy z wykorzystaniem materiałów zawierających tajemnice przedsiębiorstwa, jak również do przedstawienia prawidłowych rozwiązań. Powinno ono być wykorzystywane do wymiany doświadczeń i wyjaśniania niejasności w pragmatyce działania poszczególnych grup informacji, systemów przetwarzania i osób. Szkolenie to organizowaliby administratorzy bezpieczeństwa grupy informacji i administratorzy bezpieczeństwa systemów.

Szkoleniu specjalistycznemu podlegałyby osoby pełniące funkcje związane z bezpieczeństwem informacji w przedsiębiorstwie. Szkolenie byłoby prowadzone przez specjalistów zewnętrznych. Celem tego szkolenia byłoby przygotowanie osób do pełnienia specjalistycznych funkcji w pionie bezpieczeństwa przedsiębiorstwa.

PODSUMOWANIE

Przedstawiona w artykule propozycja modelu zarządzania bezpieczeństwem informacji w przedsiębiorstwie nie jest teoretycznym projektem, ponieważ czerpie szereg wzorców i rozwiązań znajdujących już praktyczne zastosowanie w praktyce biznesu. Propozycje te obejmują wprawdzie szereg zagadnień ujętych w różnych, mniej lub bardziej oficjalnych materiałach normatywnych, dokumentach firmowych oraz publikacjach naukowych, ale nade wszystko odwołują się do rozwiązań praktycznych wdrażanych w przedsiębiorstwach. Kreując ten model, starano się pokazać, jak korzystać z aktualnie dostępnego dorobku w zarządzaniu bezpieczeństwem informacji. Proponowany model, bazując na dotychczasowym dorobku w zarządzaniu bezpieczeństwem informacji, wnosi:

1) nowatorskie rozwiązania polegające na uwzględnieniu i umiejętnej kompilacji najlepszych rozwiązań polskich i międzynarodowych w zarzadzaniu bezpieczeństwem informacji;
2) wzorcowe praktyki działania w obszarze zarzadzania bezpieczeństwem informacji w podmiocie gospodarczym;
3) bezwzględne dążenie do zapewnienia uniknięcia niekontrolowanego wypływu informacji z przedsiębiorstwa.

W artykule podjęto zatem próbę prezentacji rozwiązań najprostszych i najtańszych, a jednocześnie skutecznych. Pokazano wzorcowe praktyki działania, na podstawie których zarządza się bezpieczeństwem informacji, ogranicza ryzyko szkód, ale tak naprawdę bez gwarancji osiągnięcia sukcesu w sensie mierzalnym. Proponowane rozwiązania systemowe są przykładem tak zwanych „działań w dobrej wierze". Oznacza to, iż są zgodne z przepisami normatywnymi, zgodne z zasadami sztuki i najlepszymi praktykami, ale nie są w stanie zagwarantować pełnego sukcesu – całkowitej szczelności informacyjnej przedsiębiorstwa.

BIBLIOGRAFIA

1. A. Białas, *Bezpieczeństwo informacji I usług w nowoczesnej instytucji i firmie*, Wydawnictwo Naukowo-Techniczne, Warszawa 2007, s. 75.
2. M. Ciecierski, Wywiad biznesowy…, s. 77.
3. K. Doran: *Zarządzanie bezpieczeństwem informacji we współczesnym przedsiębiorstwie,* AON Warszawa 2015.
4. P. Jedynak (red.), *Audyt* w *zarządzaniu przedsiębiorstwem,* Księgarnia Akademicka, Kraków 2004.
5. L. Kiełtyka, Ochrona i bezpieczeństwo informacji…, s. 233.
6. Ł. Kister, *Audyt jako narzędzie oceny bezpieczeństwa informacji w organizacji* [w:] *Ochrona informacji niejawnych, biznesowych i danych osobowych*, Materiały VI Kongresu KSOIN Katowice 2010, s. 58.
7. L. Kościelecki: *Finanse w zarzadzaniu gospodarką. Bezpieczeństwo finansowe w okresie kryzysu*, AON Warszawa 2013, *Finanse-ich istota i funkcje. Pieniądz atrybutem finansów* [w] *Propedeutyka finansów*, AON, Warszawa 2014.

8. J. Łuczak, M. Tyburski, *Systemowe Zarządzanie bezpieczeństwem informacji ISO/IEC 27001*, Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu, Poznań 2010.
9. W. Ozier, *Risk analysis and assessment*, CRC Press LLC 2004.
10. D.L. Pipkin, Bezpieczeństwo informacji…, s. 93.
11. M.E. Porter, *Strategia konkurencji. Analiza sektora i konkurentów*, PWE, Warszawa 1992.
12. Risk management: implementation principles and Inventories for risk management/risk assessment methods and tools, European Network and Information Security Agency (ENISA) 2006.
13. M. Sumiński, *Kultura informacyjna: przegląd teorii oraz potencjalne problemy badawcze*
    [w:] *Wyzwania i perspektywy współczesnego zarządzania. Innowacje, kryzys, przedsiębiorczość,* pod. red. K. Łukasika, Politechnika Częstochowska, Częstochowa 2013.
14. D. Wealleans, *The quality audit for ISO 9001: 2000. Apractical guide*, Gower 2005.
15. ISO 19011:2002 *Guidelines for quality and/or environmental management systems auditing.*
16. ISO/IEC Guide 73:2002.
17. ISO 9000:2005 *Quality management systems – Fundamentals and vocabulary*.

Ustawy

1. Art. 15 ust. 1 pkt 3 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2010 r. Nr 182, poz. 1228, z późn. zm.).
2. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r. Nr 182, poz. 1228, z późn. zm.).
3. Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. U z 2012 r. poz. 683).