NAUKI O ZARZĄDZANIU MANAGEMENT SCIENCES 1(26) • 2016

ISSN 2080-6000
e-ISSN 2449-9803

Robert Walasek
Uniwersytet Łódzki
e-mail: rwalasek@uni.lodz.pl

SYSTEMY BEZPIECZEŃSTWA INFORMACJI W PRZEDSIĘBIORSTWACH LOGISTYCZNYCH – WYNIKI BADANIA

INFORMATION SECURITY SYSTEMS IN LOGISTICS ENTERPRISES – RESEARCH RESULTS

DOI: 10.15611/noz.2016.1.13

Streszczenie: W kontekście malejącego znaczenia zasobów materialnych warunkiem osiągania przez przedsiębiorstwo przewagi konkurencyjnej jest odkrywanie i wykorzystywanie własnych, wyróżniających kompetencji oraz kreowanie cennych wartości niematerialnych. Wartości niematerialne, takie jak: wiedza, doświadczenie czy umiejętności, pozwalają przedsiębiorstwu na uruchamianie skutecznych instrumentów konkurowania, m.in. przez tworzenie niepowtarzalnych i unikatowych relacji partnerskich, które stanowią najważniejsze ogniwo w walce konkurencyjnej. Jednak aby te relacje były skuteczne, muszą się cechować wzajemnym zaufaniem. Kluczowym elementem tworzenia wiarygodności przedsiębiorstwa na rynku jest wdrożony system zarządzania bezpieczeństwem informacji. Powyższe rozważania stały się podstawą do podjęcia tematyki związanej z wdrożeniem nowoczesnych rozwiązań w zakresie ochrony i bezpieczeństwa informacji w funkcjonujących w regionie łódzkim przedsiębiorstwach logistycznych. Podjęte rozważania oraz wnioski z badań mogą przyczynić się do wskazania kluczowych obszarów, w których przedsiębiorstwa, wykorzystując odpowiednie narzędzia zarządzania bezpieczeństwem informacji, mogą osiągać wymierne korzyści oraz tworzyć przewagę rynkową nad innymi podmiotami.

Słowa kluczowe: bezpieczeństwo, informacja, zarządzanie, klient, konkurencja.

Summary: In the context of decreasing importance of the material resources provided by the company achieving competitive advantage it is to discover and use their distinctive competencies and creating valuable intangible assets. Intangible assets such as knowledge, experience or skills, enable the company to run effective instruments of competition, including by creating unique partnerships, which are the most important link in the competitive struggle. However, to be effective, these relations must be characterized by mutual trust. A key part of creating the credibility of the company in the market is implemented information security management system. These considerations were the basis to take issues related to the implementation of innovative solutions for the protection and security of information in the logistics companies operating in the region of Lodz. The reflections and conclusions of the research can help to identify key areas where companies using the tools of information security management can achieve measurable benefits and create a competitive advantage in relation to other entities.

Keywords: safety, information, management, customer, competition.

1. Wstęp

Nowoczesnych rozwiązań w zakresie funkcjonowania organizacji poszukuje coraz więcej firm, w tym również firmy logistyczne. W związku z panującymi na całym świecie globalnymi tendencjami, takimi jak: skracanie czasu rozwoju oraz cyklu życia produktu, redukcja szczebli wytwarzania, dostosowywanie produktu do klienta czy też wzrost nacisku na koszty, ważne dla każdego przedsiębiorstwa logistycznego jest ciągłe doskonalenie procesu zarządzania oraz wprowadzanie różnego rodzaju udoskonaleń dotyczących bezpieczeństwa funkcjonowania całej organizacji. Największą zachętą do ich wdrażania jest możliwość pozytywnego wpływu na szybkość, pewność i bezpieczeństwo procesu decyzyjnego w oparciu o unikatowe informacje niedostępne dla konkurentów. Zasadniczym problemem jest natomiast wybór obszaru i podejścia do nowoczesnych rozwiązań, a także zespołu odpowiedzialnego za ich wdrażanie [Tylżanowski 2013]. Dlatego współcześnie, aby przedsiębiorstwo mogło je wdrażać, zobowiązane jest do zapewnienia dostępu do ich źródła i przygotowania informacji o dotychczasowych rozwiązaniach i możliwościach ich wykorzystania. Wobec takich wyzwań przedsiębiorstwa zobligowane są do poszukiwania i wdrażania nowych rozwiązań, które chociaż na krótki czas pozwolą im uzyskać przewagę konkurencyjną na rynku. By nowe pomysły przyniosły pożądany efekt, muszą zostać dokładnie zdefiniowane, zanalizowane i dopasowane do potrzeb organizacji. Takie działania mają szczególne znaczenie przy wprowadzaniu nowoczesnych metod i narzędzi mających na celu zapewnienie bezpieczeństwa informacji stanowiących podstawę do budowania zaufania wszystkich podmiotów wchodzących w kooperację biznesową. Częste zmiany technologii oraz wyposażenia informatycznego zmuszają do aktualizacji przyjętych rozwiązań w celu pełnej zgodności między poziomem ich zaawansowania a wymaganiami podmiotów korzystających ze wspólnych zasobów i baz danych. Dla poprawnego działania całego przedsiębiorstwa poziom automatyzacji i informatyzacji ma ogromne znaczenie. Dlatego obecnie zasoby informacyjne, które stanowią podstawę działalności przedsiębiorstw, są najpilniej strzeżoną tajemnicą każdego z nich. Informacje w postaci różnego rodzaju baz danych są gromadzone, przechowywane, a następnie przetwarzane i przesyłane [Zając 2010]. Liczba generowanych informacji z roku na rok zdecydowanie wzrasta. Powodem tego jest coraz większa aplikacyjność systemów informatycznych, dzięki którym przedsiębiorstwa mogą tworzyć różnego rodzaju procedury i schematy postępowania na każdym etapie funkcjonowania. Warto zwrócić uwagę na to, iż sprzęt komputerowy, jako narzędzie, nie podlega tak wielkiej ochronie, jak informacja w nim zawarta. Dlatego też wszelkie działania z zakresu bezpieczeństwa skierowane są przede wszystkim na ochronę informacji. Trudno jednak wyobrazić sobie efektywne korzystanie z informacji bez dobrze funkcjonujących systemów i sieci komputerowych. Zatem tworzy się efekt synergii. Otaczając ochroną sieć, systemy i narzędzia informatyczne, jednocześnie zabezpiecza się informacje oraz dane w nich zawarte. Są one w sposób szczególny chronione przed utratą, zniszczeniem, mody-

fikacją, dostępem osób nieupoważnionych itp. [Papińska-Kacperek (red.) 2008]. Jednak współczesne zabezpieczenia nie są wolne od wad. Obecnie dodatkowym zagrożeniem stał się powszechny dostęp do sieci Internet, bo kradzieże tożsamości czy włamania do internetowych kont bankowych są domeną współczesnego hakerstwa. Zagrożenia te mogą narazić przedsiębiorstwo na utratę wiarygodności, zasobów, pozytywnego wizerunku, środków finansowych czy nawet klientów.

Biorąc to pod uwagę, zasadne wydało się przeprowadzenie badania empirycznego i zaprezentowanie jego wyników w niniejszym referacie. Głównym celem referatu jest próba określenia innowacyjnych rozwiązań w zakresie bezpieczeństwa informacji stosowanych w przedsiębiorstwach logistycznych oraz wskazania korzyści, które sprzyjają tworzeniu ich konkurencyjności rynkowej. Takie sformułowanie celu wynika z faktu, iż obecnie postępujący systematycznie proces umiędzynarodowienia działalności gospodarczej podnosi problem konkurencji i konkurencyjności w odniesieniu do praktycznie wszystkich przedsiębiorstw funkcjonujących na rynku. Dla przedsiębiorstw najważniejszym zadaniem jest poszukiwanie nowych, a zarazem odrębnych dróg konkurowania, które pozwolą im na sprawne funkcjonowanie we współczesnych realiach rynkowych. Praktyka gospodarcza pokazuje, że firmy, aby być konkurencyjne, uciekają się do różnych metod osiągania tego celu: od tych najbardziej praworządnych, do tych nastawionych na kradzież i kopiowanie informacji i danych od konkurentów. Dlatego tak istotną kwestią jest zabezpieczanie się przedsiębiorstw przed działaniem nieuczciwej konkurencji i ochrona swojego strategicznego zasobu, jakim jest informacja.

2. Bezpieczeństwo informacji w przedsiębiorstwach logistycznych

Większość współczesnych przedsiębiorstw, aby uchronić się przed utratą newralgicznych informacji lub danych, stosuje tzw. politykę bezpieczeństwa informacji, inaczej nazywaną polityką bezpieczeństwa instytucji. Jest to plan działania mający na celu ochronę zasobów organizacji. Uwzględnia on wszystkie istotne kryteria, takie jak posiadane zasoby finansowe, typy posiadanych informacji, normy prawne i inne akty narzucone instytucji, zastosowane rozwiązania z dziedziny bezpieczeństwa czy też świadomość zatrudnionego personelu. Zatem polityka bezpieczeństwa to plan lub sposób działania przyjęty w celu zapewnienia bezpieczeństwa systemów i ochrony danych [Papińska-Kacperek (red.) 2008]. Głównym celem jej stosowania może być [Kiełtyka 2002]:

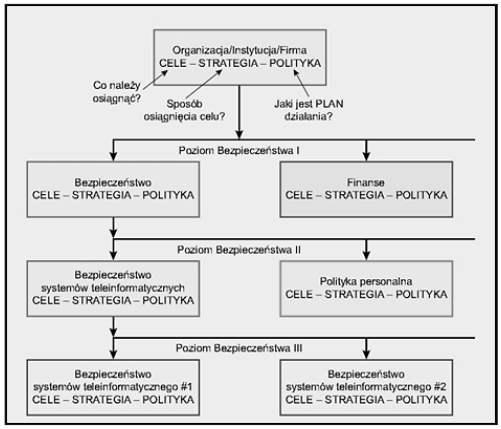
- zagwarantowanie prawnych wymagań ochrony informacji,
- zagwarantowanie poufności, integralności i dostępności przetwarzanej informacji,
- bezpieczeństwo informacji strategicznych,
- zagwarantowanie zaufania publicznego i prestiżu organizacji,
- bezpieczeństwo procesu ciągłości funkcjonowania organizacji,
- redukcja kosztów.

Stosowanie polityki bezpieczeństwa informacji wynika z faktu, że informacja stanowi kluczowy zasób przedsiębiorstwa i jest jego strategiczną wartością. Zatem każde przedsiębiorstwo zobowiązane jest do jej ochrony. Informacja stanowi element procesów biznesowych, a działanie przedsiębiorstw uzależnione jest od prawidłowego jej obiegu zarówno wewnątrz, jak i na zewnątrz. Ochrona informacji wynika również z obowiązujących przepisów prawa lub umów. Bowiem bezpieczeństwo informacyjne w Polsce to poziom ochrony informacji i narzędzi służących do jej opracowania, przechowywania i transmisji przed losowymi lub celowymi zniekształceniami sztucznego lub naturalnego pochodzenia, które mogą przynieść szkodę właścicielom lub użytkownikom informacji i narzędzi [Urbanowicz (red.) 2004].

W celu zapewnienia bezpieczeństwa informacji przedsiębiorstwa wdrażają i użytkują różnego rodzaju systemy mające na celu zapobieżenie zniszczeniu informacji i danych. To dzięki nim przedsiębiorstwo ogranicza ryzyko występowania zagrożeń związanych z utratą informacji. Stosowane zabezpieczenia systemowe mogą występować jako elementy osobowe, techniczne, programowe lub organizacyjne, wykorzystywane w procesach ochrony działań, których celem jest zapewnienie odpowiedniego poziomu ochrony logicznej i fizycznej informacji oraz elementów systemu teleinformatycznego [Krawczyk 2011]. Jednym z takich systemów jest System Zarządzania Bezpieczeństwem Informacji (SZBI) − *Information Security Management System* (ISMS), który stanowi element systemu zarządzania, oparty na podejściu wynikającym z ryzyka biznesowego, odnoszącego się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacyjnego (zgodnie z normą PN-I-07799-2:2005) [Molski, Łacheta 2009]. Pośród wielu modeli zarządzania bezpieczeństwem informacji powszechnie stosowanymi są dwa, mianowicie:

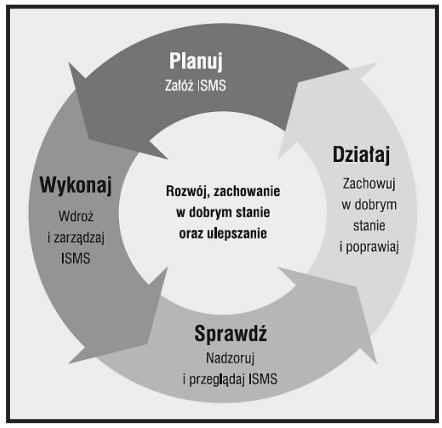
- trójpoziomowy model bezpieczeństwa, który wskazuje, co konkretnie powinno zostać zrealizowane i jakie zasady powinny być przestrzegane w polityce bezpieczeństwa przedsiębiorstwa i sieci, aby cel został osiągnięty (por. rys. 1);
- model PCDA − „planuj – wykonaj – sprawdź − działaj"; cykl ten jest stosowany do całej struktury procesów Systemu Zarządzania Bezpieczeństwem Informacji; model ten określa wymagania bezpieczeństwa informacji oraz oczekiwania zainteresowanych stron jako wartość wejściową, a przez niezbędne działania i procesy dostarcza wartości wyjściowych bezpieczeństwa informacji, które spełniają te warunki (por. rys. 2).

Głównym zadaniem modeli bezpieczeństwa jest ochrona informacji strategicznych przed różnego rodzaju zagrożeniami (por. tab. 1), które mogą spowodować ich ujawnienie lub zniszczenie. Wśród ogólnie dostępnych zagrożeń najczęściej występującymi zagrożeniami dla procesu przetwarzania, przesyłania i magazynowania informacji w systemach informatycznych są potencjalne działania człowieka, działania sił wyższych, awarie elementów sprzętowych różnorodnych systemów informatycznych, wady eksploatowanego w nich oprogramowania powodujące utratę tajności, integralności lub dostępności [Zaskórski 2011].



Rys. 1. Trójpoziomowy model bezpieczeństwa

Źródło: [Wójcik 2008].



Rys. 2. Model PDCA

Źródło: [Blim 2007].

Tabela 1. Typy zagrożeń ich skutki oraz sprzyjające warunki

Typy zagrożeń	Skutki	Sprzyjające warunki
Awarie: • systemu zasilania • komputera głównego • sprzętu transmisyjnego	• unieruchomienie systemu • zniszczenie sprzętu	• niewłaściwe warunki eksploatacji sprzętu • brak właściwej obsługi • niska jakość urządzeń
Żywioły i wypadki: • pożar • woda • trzęsienie ziemi	• zniszczenie sytemu • zniszczenie kopii archiwalnej	• nieprzestrzeganie przepisów przeciwpożarowych • brak przeciwpożarowej instalacji alarmowej • ludzka nieuwaga • niewłaściwa lokalizacja centrum przetwarzania • brak stałego nadzoru nad pracą sprzętu
Działania przestępcze: • szpiegostwo • kradzież • sabotaż • dywersja • podsłuch • terroryzm	• ujawnienie danych osobom nieupoważnionym • kradzież danych • zniszczenie danych • zniszczenie sprzętu • modyfikacja oprogramowania • niedozwolona modyfikacja danych	• brak właściwego systemu bezpieczeństwa osobowego, fizycznego systemów i sieci teleinformatycznych • brak właściwych zabezpieczeń • bark odpowiednich warunków przechowywania kopii danych • dostęp do głównych zasobów systemu osób nieupoważnionych • niski poziom administracji systemu • brak narzędzi administracyjnego nadzoru nad pracą systemu • ujawnione hasło • zła atmosfera w pracy, niezadowolony pracownik • brak nadzoru nad pracą serwisu • brak wdrożenia polityki antywirusowej
Działania w dobrej wierze: • pomyłki pracowników	• zniszczenie zasobów informacyjnych • brak poprawnych kopii danych • błędne dane	• brak systematycznych szkoleń • zbyt duże uprawnienia • brak fachowej pomocy w pracy i kontroli jej wykonania • wymuszona złymi stosunkami samodzielność pracowników

Źródło: [Borowiecki, Czekaj 2011].

Aby chronić informacje przed zagrożeniami, istotne jest również to, aby uwzględniały one ochronę w czterech obszarach:

- informatycznym − to wszelkiego rodzaju oprogramowania stosowane w systemach informatycznych,
- organizacyjnym − na tym obszarze ustanawiana jest polityka bezpieczeństwa informacji, w której określone są zasady postępowania oraz uprawnienia związane z dostępem do niej,
- prawnym − to wszelkiego rodzaju normy, przepisy, ustawy dotyczące ochrony danych,
- materialnym − ochrona budynku i pomieszczeń oraz systemy mające na celu informowanie o pojawiającym się zagrożeniu.

Ochrona w tych czerech, podstawowych obszarach wymusza na przedsiębiorstwach stosowanie wielu zabezpieczeń jednocześnie. Zabezpieczenia te wzajemnie się uzupełniają i tworzą sieć zabezpieczeń utrudniających czy wręcz uniemożliwiających niepowołanym osobom lub instytucjom ich pokonanie. Do nowoczesnych mechanizmów ochrony informacji stosowanych w przedsiębiorstwach logistycznych zaliczamy [Bilski 2005]:

- ograniczenie fizycznego dostępu do systemu informatycznego,
- uwierzytelnianie użytkowników,
- ograniczanie uprawnień użytkowników,
- mechanizmy kryptograficzne,
- monitorowanie,
- ochrona antywirusowa,
- ochrona sieci lokalnej przed dostępem do sieci rozległej,
- ochrona przed wpływem czynników zewnętrznych,
- wykonywanie zapasowych kopii danych.

Jednym z przykładów unikatowości w systemach bezpieczeństwa informacji jest ściana ognia (*firewall*). Jest to system programowy, sprzętowy lub sprzętowo-programowy, mający na celu ochronę danych przed atakami z sieci Internet. Podstawowym jego zadaniem jest kontrolowanie przepływu informacji pomiędzy lokalną siecią a globalnym Internetem. Protokoły dostępowe na każdej stacji roboczej lub głównym serwerze przedsiębiorstwa określają zasady korzystania użytkowników zewnętrznych z zasobów sieciowych oraz decydują, do jakich zasobów internetowych mogą mieć dostęp pracownicy. Ściana ognia zawiera również mechanizmy umożliwiające monitorowanie pracy sieci w przypadku włamania lub próby włamania. W takiej sytuacji administrator sieci natychmiast jest informowany o zagrożeniu. Kolejnym przykładem nowoczesnych rozwiązań w zapewnianiu bezpieczeństwa informacji jest szyfrowanie. Dzięki niemu istnieje możliwość kodowania informacji przy pomocy specjalistycznych narzędzi kodujących tak, aby zawarty w nich przekaz był niemożliwy do odczytania przez osoby nieupoważnione. Obecnie uwierzytelnianie danych stanowi kolejne z innowacyjnych rozwiązań w zakresie bezpieczeństwa informacji. Jest to proces weryfikacji tożsamości użytkownika zacho-

dzący we wstępnym etapie dostępu do zasobów systemu informatycznego. Występuje on często pod postacią logowania systemowego. Użytkownik logujący się w systemie operacyjnym lub sieciowym podaje swój identyfikator. Zgodnie z założeniem tylko uprawnieni użytkownicy, którzy pozytywnie przeszli proces uwierzytelniania, uzyskują dostęp do zasobów systemu informatycznego. System uwierzytelniania jest najczęściej zintegrowany z innymi elementami systemu komputerowego, takimi jak: oprogramowanie specjalistyczne, aplikacje pracownicze czy system zarządzania bazą danych.

Niestety większość przedsiębiorstw nie docenia bezpieczeństwa informacji, co wiąże się z niskim poziomem zabezpieczeń stosowanych do ich ochrony. Przykładem może być raport bezpieczeństwa informacji opracowany przez firmę Ernst& Young (*Fighting to Close the Gap 2013*). Ponad 75% badanych firm oceniło, iż zagrożenie atakami zewnętrznymi wzrosło, zaś prawie połowa z nich dostrzega wzrost zagrożeń wewnętrznych. Co trzecia badana firma doświadczyła w ostatnich dwóch latach incydentów naruszających jej bezpieczeństwo, ale ponad 60% z nich nie ma wdrożonej systemowej polityki bezpieczeństwa. Jedynie nieco ponad 15% badanych deklarowało, iż ich polityka bezpieczeństwa spełnia wszelkie wymogi i oczekiwania partnerów biznesowych. Prawie jedna trzecia firm postrzega swój system bezpieczeństwa jako zagrożony lub bezbronny, a świadomość ta wzrosła najbardziej w ciągu ostatnich dwunastu miesięcy [Nogacki 2015]. Biorąc pod uwagę wnioski z wielu badań oraz opinie menedżerów firm logistycznych, można stwierdzić, że głównymi barierami wdrożenia polityki bezpieczeństwa informacji są przede wszystkim: niska świadomość użytkowników systemów, niski budżet przeznaczony na ochronę zasobów informacyjnych oraz brak urządzeń, które byłyby odpowiedzialne za bezpieczeństwo. Dodatkowo ograniczenia w dostępie do wyspecjalizowanej kadry w zakresie ochrony informacji powodują, że przedsiębiorstwa powierzają zadania ich ochrony własnym pracownikom (nie w pełni kompetentnym) lub zlecają podmiotom zewnętrznym. Kolejną barierą w skutecznym stosowaniu systemów bezpieczeństwa jest brak wsparcia najwyższego kierownictwa, a co za tym idzie, brak podstawowych szkoleń z zakresu bezpieczeństwa informacji.

3. Innowacyjność systemów bezpieczeństwa – wyniki badania

Obecnie sytuacja rynkowa wymusza na przedsiębiorstwach absorpcję nowoczesnych metod szczególnie w obszarze wiedzy i unikatowych rozwiązań technologicznych. Podyktowane jest to przede wszystkim dużym stopniem zróżnicowania klientów, ich wymagań i oczekiwań w stosunku do nabywanych produktów. Coraz mniejsza lojalność klientów powoduje, iż przedsiębiorstwa starają się ich utrzymać przez oferowanie nowych udoskonalonych produktów, jednocześnie szukając źródeł konkurencyjności oraz sposobów ochrony swoich strategicznych zasobów przed ich utratą. Działania związane z zastosowaniem współczesnych technologii i rozwiązań w zakresie bezpieczeństwa zasobów informacyjnych pozwalają przedsiębiorstwom

na oferowanie klientom najbardziej aktualnych, nieskopiowanych produktów. Dają również możliwość szybkiego reagowania na zmiany rynkowe poprzez podejmowanie ważnych decyzji w oparciu o bieżące, często kluczowe informacje. Taka sytuacja ma miejsce również wśród przedsiębiorstw logistycznych, które z racji dynamizacji rozwoju całej gałęzi muszą decydować się na wdrażanie nowych technologii i ochrony informacji przed konkurencją. Widać to szczególnie na przykładzie przedsiębiorstw funkcjonujących w województwie łódzkim, postrzeganym jako wysoko konkurencyjny i atrakcyjny inwestycyjnie obszar Polski. Dlatego zasadne wydało się zaprezentowanie wyników badania empirycznego przeprowadzonego w Katedrze Logistyki Wydziału Zarządzania UŁ. Głównym celem badania była próba określenia poziomu wdrożenia i wykorzystania systemów bezpieczeństwa informacji w wybranych obszarach działalności logistycznej. Nacisk położono przede wszystkim na identyfikację głównych zagrożeń związanych z utratą informacji, określenie metod ochrony informacji oraz korzyści uzyskiwanych dzięki wdrożeniu polityki bezpieczeństwa informacji.

Dobór próby do badania miał charakter doboru celowego. Badaniem objęte zostały 93 przedsiębiorstwa logistyczne z regionu łódzkiego, które deklarowały stosowanie nowoczesnych systemów i narzędzi bezpieczeństwa informacji. W badaniu zastosowano technikę ankietową, której narzędziem badawczym był kwestionariusz badawczy. Przeprowadzono je wśród prywatnych przedsiębiorstw (małych, średnich i dużych) z uwzględnieniem ich kapitału oraz okresu ich funkcjonowania na rynku. Badaniu poddano przedsiębiorstwa o charakterze usługowym, handlowym oraz produkcyjnym. Badanie ankietowe zostało przeprowadzone na przełomie października i listopada 2014 r. metodą wywiadów bezpośrednich przez przeszkolonych ankieterów.

Strukturę próby w przekroju cech przedsiębiorstwa (okres funkcjonowania na rynku, pochodzenie kapitału, charakter prowadzonej działalności oraz liczbę zatrudnionych osób) przedstawia tab. 2.

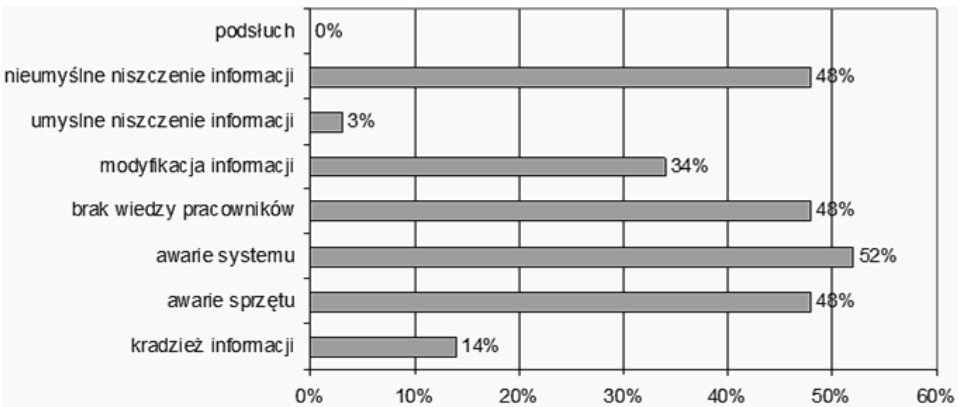
Tabela 2. Struktura próby w przekroju badanych cech przedsiębiorstw

Okres funkcjonowania na rynku*		Kapitał przedsiębiorstwa	
Poniżej 5 lat	23%	zagraniczny	22%
5-8 lat	19%	polski	**59%**
Powyżej 8 lat	**58%**	mieszany	19%
Charakter działalności przedsiębiorstwa		Liczba zatrudnionych osób	
Handlowa	**42%**	poniżej 50	**60%**
Usługowa	33%	50-250	32%
Produkcyjna	25%	powyżej 250	8%

* Ze względu na asymetryczny rozkład przedsiębiorstw z punktu widzenia tej zmiennej w dalszych analizach zastosowano podział na dwie kategorie: okres funkcjonowania do 8 lat oraz powyżej 8 lat.

Źródło: opracowanie własne.

Przedsiębiorstwa funkcjonujące na zmiennym i dynamicznym rynku, aby być konkurencyjne, muszą chronić swoje unikatowe i trudne do powielenia zasoby. Generalnie większość z nich skupia się na ochronie informacji jako zasobie, który bardzo łatwo stracić. Dlatego też przedsiębiorstwa, wdrażając politykę bezpieczeństwa informacji, w pierwszej kolejności starają się identyfikować zagrożenia dotyczące utraty informacji (por. rys. 3). Wielokanałowość pozyskiwania informacji, a z drugiej strony ich utraty powoduje, że przedsiębiorstwa w swoich działaniach starają się eliminować lub ograniczać w maksymalnym stopniu ryzyko związane z możliwością ujawnienia strategicznych danych osobom niepowołanym.

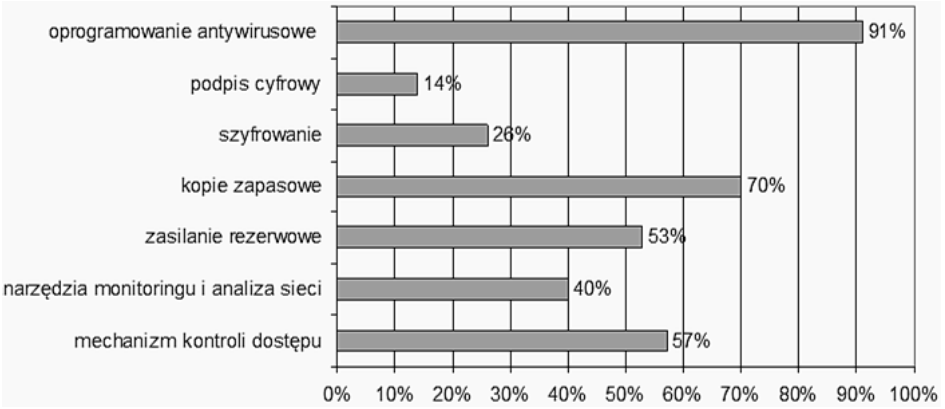


Rys. 3. Zagrożenia związane z utratą informacji w przedsiębiorstwie

Źródło: opracowanie własne.

Połowa ankietowanych stwierdziła, iż najczęściej utrata informacji następuje poprzez awarię systemu lub sprzętu. Również do utraty informacji przyczyniają się braki w kompetencjach pracowników oraz nieumyślne kasowanie informacji z dysku lub sieci. Ta ostatnia z odpowiedzi przeczy ogólnie przyjętej tezie, że największym zagrożeniem dla zasobów informacyjnych są ataki z zewnątrz na systemy bazodanowe. Takich odpowiedzi udzielały w większości przypadków przedsiębiorstwa handlowe i produkcyjne z kapitałem polskim, o krótkim stażu rynkowym. Tylko niecałe 15% badanych firm, przede wszystkim handlowych, z dłuższym stażem rynkowym, bez względu na kapitał, twierdziło, że było kiedykolwiek ofiarą kradzieży informacji. Jeżeli takie zdarzenia już miały miejsce, to dotyczyły w większości przypadków baz danych zawierających kluczowe informacje o klientach. Żadne z badanych przedsiębiorstw logistycznych nie stwierdziło, że było kiedykolwiek podsłuchiwane w celu pozyskania informacji przez osoby trzecie, chociaż wielu autorów jasno stwierdza, że podsłuch jest podstawowym atakiem mającym na celu ujawnienie informacji.

Kolejnym elementem w polityce bezpieczeństwa informacji, po identyfikacji zagrożeń, jest zastosowanie innowacyjnych narzędzi mających na celu ochronę zasobów informacyjnych przedsiębiorstwa (por. rys. 4). Duży wpływ na wybór rodzaju sposobu zabezpieczeń ma rodzaj i charakter kanału, którym informacja jest pozyskiwana. Należy brać pod uwagę to, że dla każdego przedsiębiorstwa wybierane zabezpieczenia mogą być inne. Uwarunkowane jest to poziomem ważności informacji oraz możliwościami techniczno-kapitałowymi danego przedsiębiorstwa. Jednak odpowiedni dobór innowacyjnych zabezpieczeń w celu ochrony informacji ma kluczowe znaczenie w funkcjonowaniu organizacji i budowaniu konkurencyjności rynkowej.



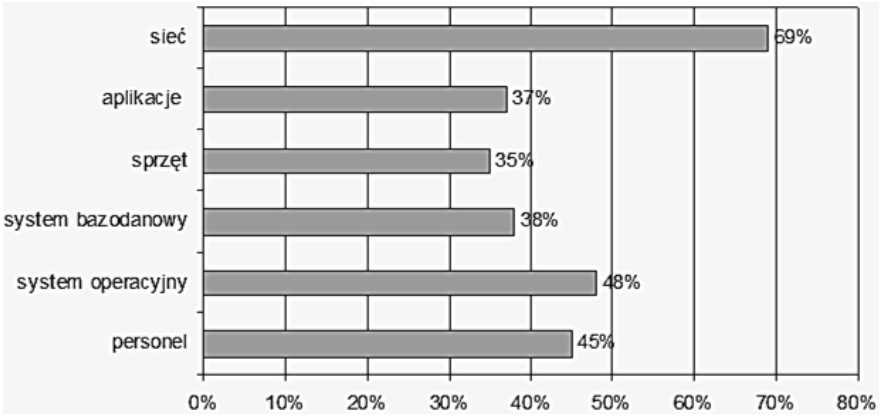
Rys. 4. Zabezpieczenia wykorzystywane w celu ochrony informacji

Źródło: opracowanie własne.

Prawie wszyscy ankietowani wskazali, że najczęściej stosowanym narzędziem ochrony informacji jest nowoczesne oprogramowanie antywirusowe. Obecnie stanowi ono podstawę systemu bezpieczeństwa informacyjnego każdego przedsiębiorstwa. Dzieje się tak dlatego, iż statystycznie największym zagrożeniem dla bezpieczeństwa informacyjnego są ataki hakerskie z sieci Internet w postaci różnego rodzaju wirusów, które po zainstalowaniu na komputerze zaczynają potajemnie przesyłać informacje z jego dysków. Nowoczesne oprogramowanie antywirusowe pozwala na skuteczną eliminację tych zagrożeń poprzez kontrolowanie wszystkich plików przychodzących i wyłapywanie tych, które są podejrzane i stanowią potencjalne niebezpieczeństwo. Nowoczesne programy antywirusowe identyfikują i aktualizują również nowo pojawiające się zagrożenia. Kolejnym narzędziem ochrony informacji według ¾ badanych jest tworzenie kopii zapasowych danych. Tendencja taka panowała wśród wszystkich przedsiębiorstw, jednak częściej takiej odpowiedzi udzielały przedsiębiorstwa handlowe i usługowe z kapitałem mieszanym i zagranicznym. Natomiast większość przedsiębiorstw produkcyjnych (z prawie 60% an-

kietowanych) uważała, że stosowanie kontroli dostępu stanowiskowego lub sieciowego to bardzo skuteczna metoda ochrony danych. Tylko niecałe 15% korzysta z innowacyjnego rozwiązania, jakim jest podpis cyfrowy. Nie jest to zaskoczeniem, ponieważ stosowanie podpisu cyfrowego wymaga dopełnienia odpowiednich procedur, a nie wszystkie przedsiębiorstwa są w stanie je stosować.

Współcześnie niemal każde przedsiębiorstwo zmuszone jest monitorować sieć, systemy oraz własnych pracowników (por. rys. 5). Dzieje się tak dlatego, iż przedsiębiorstwa we współczesnym otoczeniu narażone są na szereg niebezpieczeństw związanych z ich deprecjacją rynkową. Dlatego też systematyczne monitorowanie wybranych obszarów zagrożonych wystąpieniem niepożądanego zdarzenia pozwala firmom na szybką reakcję i eliminację tego zdarzenia.



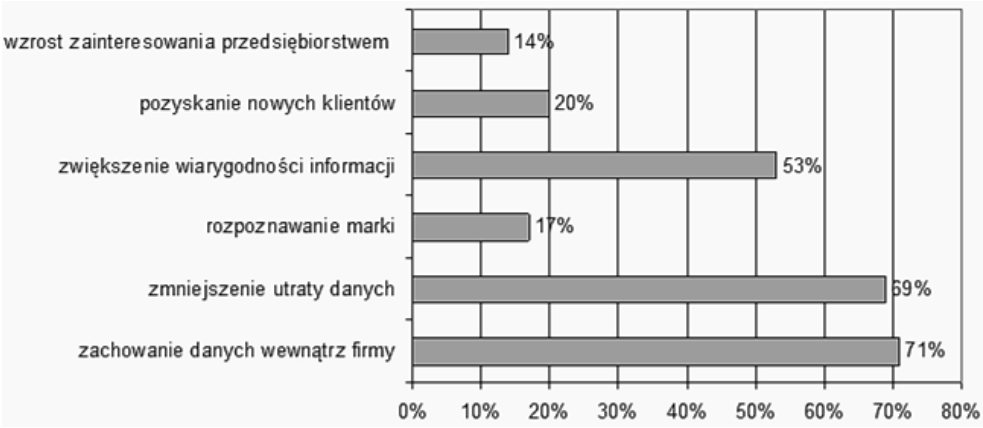
Rys. 5. Przedmioty podlegające kontroli w przedsiębiorstwie

Źródło: opracowanie własne.

Według prawie 70% ankietowanych najczęściej monitorowanym przez nowoczesne narzędzia jest obszar sieci (Internet) oraz systemy operacyjne (prawie połowa ankietowanych wskazała tę odpowiedź). Wraz ze wzrastającą świadomością dotyczącą ochrony danych prawie połowa badanych przedsiębiorstw coraz częściej decydowała się na monitorowanie własnego personelu. Takich odpowiedzi udzielały przede wszystkim przedsiębiorstwa sektora MSP, z kapitałem zagranicznym, bez względu na charakter działalności. Wyniki te wskazują, że wzrastająca świadomość przedsiębiorstw co do zagrożeń utraty informacji wymusza na nich stosowanie kontroli nie tylko zewnętrznych czynników ryzyka, ale również wewnętrznych, związanych z błędami pracowników, ich nieuczciwością czy też niekompetencją.

Wszystkie wymienione działania, stosowane przez przedsiębiorstwa w celu zapewnienia bezpieczeństwa informacji, są bardzo istotne z punktu widzenia bezpieczeństwa teleinformatycznego przedsiębiorstwa. Bezpieczeństwo to wpływa na budowę wizerunku firmy oraz zaufania ze strony partnerów biznesowych, w tym

szczególnie klientów, zatem stosowanie ochrony danych nie tylko podnosi poziom bezpieczeństwa funkcjonowania rynkowego organizacji, ale wpływa na uzyskiwanie wielu korzyści (por. rys. 6), które warunkują tworzenie partnerskich relacji z podmiotami rynkowymi.



Rys. 6. Korzyści związane z ochroną informacji

Źródło: opracowanie własne.

Zasadniczą korzyścią uzyskiwaną przez przedsiębiorstwa stosujące innowacyjne rozwiązania i narzędzia ochrony informacji jest zachowanie strategicznych danych wewnątrz organizacji. Ochrona wewnątrzzakładowa informacji warunkuje również kolejną korzyść, jaką jest ograniczenie ryzyka ich utraty. Takiej odpowiedzi udzieliło ponad ¾ średnich i dużych przedsiębiorstw zajmujących się handlem i usługami, bez względu na źródło pochodzenia kapitału. Te odpowiedzi nie dziwią, ponieważ zachowanie danych dotyczących klientów, dostawców czy kooperantów to być albo nie być dla wielu organizacji. Dla badanych firm pozyskanie nowych klientów (20% ankietowanych wskazało tę odpowiedź), zwiększenie rozpoznawalności marki (nieco ponad 15% ankietowanych wskazało tę odpowiedź) i wzrost zainteresowania przedsiębiorstwem (niecałe 15% ankietowanych wskazało tę odpowiedź) stanowiły najmniejsze korzyści uzyskiwane dzięki stosowaniu nowoczesnych narzędzi ochrony informacji. Wydawać by się mogło, iż w tych właśnie obszarach przedsiębiorstwo powinno odnotowywać największe korzyści. Według autora wynikać to może z przeświadczenia podmiotów zewnętrznych wchodzących w interakcję z przedsiębiorstwem, że stosowanie innowacyjnych rozwiązań w zakresie bezpieczeństwa i ochrony danych jest standardem, a jako standard powszechnie stosowany, zasadniczo nie wpływa na sposób postrzegania przedsiębiorstwa przez pryzmat jego wiarygodności i zaufania.

4. Zakończenie

Współczesne przedsiębiorstwa logistyczne, aby być konkurencyjne na rynku, muszą ciągle i systematycznie angażować się w proces doskonalenia biznesowego, który wiąże się z sukcesywnym wdrażaniem i ze stosowaniem innowacji we wszystkich obszarach działalności. Szczególnie jest to istotne w obszarze ochrony i bezpieczeństwa informacji jako strategicznego zasobu warunkującego rozwój rynkowy. Stosowanie innowacyjnych rozwiązań w tym obszarze działalności korzystnie wpływa na poprawę funkcjonowania przedsiębiorstw, przynosząc im szereg wymiernych korzyści, będących podstawą do budowania ich przewagi konkurencyjnej. W celu podniesienia konkurencyjności przedsiębiorstwa ważne jest odpowiednie zidentyfikowanie zagrożeń, wdrożenie, utrzymanie oraz doskonalenie systemów bezpieczeństwa informacji. Działania te mają istotny wpływ na płynność finansową, zyskowność oraz działalność zgodną z wymogami prawa. Bezpieczeństwo informacji pozwala również budować wizerunek organizacji i tworzyć długookresowe relacje z wszystkimi podmiotami funkcjonującymi na rynku. Dodatkowym czynnikiem wpływającym na poziom bezpieczeństwa informacji w przedsiębiorstwach jest stosowanie nowoczesnych zabezpieczeń, takich jak: oprogramowanie antywirusowe czy ściana ognia w ich najnowszych wydaniach. Jak wskazują międzynarodowe badania, z roku na rok wzrasta świadomość użytkowników systemów co do poziomu i skali zagrożeń płynących zarówno z wnętrza organizacji, jak i z zewnątrz. Dlatego też coraz częściej decydują się oni na stosowanie różnorodnych zabezpieczeń, które w sposób skuteczny mają chronić ich zasoby. Zdają sobie sprawę z tego, iż zapewniając ochronę informacji w przedsiębiorstwie, wpływają na poziom jego funkcjonowania oraz tworzenie konkurencyjności poprzez oferowanie unikatowych i trudnych do powielenia produktów. Większość badanych przedsiębiorstw logistycznych deklarowała, że stosuje nowoczesne rozwiązania w zakresie polityki bezpieczeństwa informacji. Jednak w dużej mierze ta innowacyjność systemowa polega na stosowaniu najnowszego oprogramowania służącego do monitoringu zasobów sieciowych i personalnych organizacji. Narzędzia kontroli są podobne u wszystkich, czyli: oprogramowanie antywirusowe, *firewall*, kopie zapasowe czy inne. I tu należałoby się zastanowić, czy świadomość rosnącego zagrożenia ze strony dynamicznie zmieniającego się otoczenia nie wymusza na przedsiębiorstwach poszukania innych, alternatywnych sposobów zabezpieczania informacji, takich, które są mało znane. Coś, co jest powszechnie stosowane, z reguły jest możliwe do obejścia, a tego przede wszystkim wystrzegają się współczesne przedsiębiorstwa logistyczne.

Literatura

Bilski T., 2005, *Wprowadzenie do ochrony danych,* Wydawnictwo Wyższej Szkoły Komunikacji i Zarządzania w Poznaniu, Poznań.

Blim M., 2007, *Teoria ochrony informacji cz. 2,* Zabezpieczenia, nr 4.

Borowiecki R., Czekaj J., 2011, *Zasoby Informacyjne w ograniczaniu ryzyka gospodarczego,* Wydawnictwo Dom Organizatora, Toruń.

Kiełtyka L., 2002, *Komunikacja w zarządzaniu, Techniki, narzędzia i formy przekazu informacji*, Wydawnictwo Placet, Warszawa.

Krawczyk S., 2011, *Logistyka. Teoria i praktyka cz. 2*, Wydawnictwo Difin, Warszawa.

Molski M., Łacheta M., 2009, *Bezpieczeństwo i audyt systemów informatycznych,* Wydawnictwo WSG Bydgoszcz, Bydgoszcz.

Nogacki R. (red.), 2015, *Firmy nie doceniają bezpieczeństwa informacji*, http://nf.pl/manager/firmy-nie-doceniaja-bezpieczenstwa-informacji,,43287,276.

Papińska- Kacperek J. (red.), 2008, *Społeczeństwo informacyjne*, PWN, Warszawa.

Tylżanowski R., 2013, *Innowacyjne rozwiązania logistyczne w przedsiębiorstwach*, [w:] *Studia i Prace Wydziału Nauk Ekonomicznych i Zarządzania nr 34*, red. B. Kryk, T. Wiśniewski, Wydawnictwo Uniwersytetu Szczecińskiego, Szczecin.

Urbanowicz P. (red.), 2004, *Ochrona informacji w sieciach komputerowych*, Wydawnictwo KUL, Lublin.

Wójcik A., 2008, *System Zarządzania Bezpieczeństwem Informacji zgodny z ISO/IEC 27001. Cz. 1. Wprowadzenie,* Zabezpieczenia, nr 2.

Zając P., 2010, *Elektroniczna wymiana danych w systemach logistycznych,* Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław.

Zaskórski P., 2011, *Zarządzanie organizacją w warunkach ryzyka utraty informacyjnej ciągłości działania,* Wojskowa Akademia Techniczna w Warszawie, Warszawa.