OCENA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI W PRZEDSIĘBIORSTWIE W ŚWIETLE PRZEPROWADZONYCH BADAŃ

Michał PAŁĘGA, Marcin KNAPIŃSKI, Wiesław KULMA

Streszczenie: W artykule przedstawiono istotę i znaczenie bezpieczeństwa informacji w działalności gospodarczej współczesnego przedsiębiorstwa. Zaprezentowano także wyniki badań empirycznych przeprowadzonych w oparciu o metodę ankietowania, a dotyczące oceny systemu zarządzania bezpieczeństwem informacji w przedsiębiorstwie. Celem ich było poznanie opinii respondentów na temat wartości informacji i jej bezpieczeństwa w biznesie, występujących źródeł zagrożeń wycieku bądź utraty informacji oraz stopnia stosowanych w przedsiębiorstwie zabezpieczeń gwarantujących racjonalny poziomu ich bezpieczeństwa.

Słowa kluczowe: zarządzanie, informacje, bezpieczeństwo informacji, System Zarządzania Bezpieczeństwem Informacji (SZBI), zagrożenia bezpieczeństwa informacji.

1. Wstęp

Postęp w zakresie technologii informatycznej i komunikacyjnej spowodował, iż informacja stała się jednym z elementarnych czynników stymulujących rozwój współczesnej gospodarki, doprowadzając również do transformacji społeczeństwa z industrialnego w informacyjne. W tego rodzaju społeczeństwie aktywność wszystkich instytucji rządowych, organizacji, podmiotów gospodarczych, a nawet poszczególnych jednostek społecznych wiąże się szybkim, niezawodnym i bezpiecznym przetwarzaniem ogromnych ilości zasobów informacyjnych. Ich strategiczne znaczenie wynika z faktu, iż rzetelne oraz dostępne w pożądanym czasie mogą stanowić kluczowy czynnik sukcesu rynkowego, z kolei ich brak może stać się przyczyną wielu klęsk i niepowodzeń. Wobec powyższego istnieje konieczność troski o tak strategiczne aktywa, jakimi są dane i informacje, gdyż to one determinują przewagę nad innymi jednostkami i podmiotami gospodarczymi [1, 3, 4].

Odpowiedzią na tę potrzebę jest stosunkowo młody obszar nauki z pogranicza prawa, technologii informatycznej, organizacji i zarządzania oraz inżynierii produkcji, określany mianem *zarządzania bezpieczeństwem informacji*. Ukierunkowane jest ono na utworzenie i utrzymanie optymalnego poziomu bezpieczeństwa informacji w organizacji, czyli zagwarantowanie jej właściwej jakości oraz zapewnienie jej dostępności tylko dla wybranych jednostek i podmiotów, w odpowiednim czasie. Jak podaje specjalistyczna literatura, przez jakość informacji należy rozumieć ogół ich właściwości, które umożliwiają zaspokojenie aktualnych bądź przyszłych potrzeb jej użytkowników. Wobec tego bezpieczeństwo informacyjne to z jednej strony możliwość pozyskania dobrej informacji, z drugiej zaś ochrona posiadanych zasobów informacyjnych przed ich utratą (zniszczeniem, zmianą, wyciekiem, kradzieżą itp.) [2, 5].

W literaturze przedmiotu problematyka zagrożeń informacyjnych prezentowana jest w bardzo szerokim ujęciu. Postęp technologii komputerowej, niepohamowany rozwój sieci Internet oraz politechnizacja życia sprzyjają powstawaniu nowych form zagrożeń oraz intensyfikują już istniejące. Nie wnikając w szczegółowe rozważania można zidentyfikować następujące obszary zagrożeń [3, 6]:

- zagrożenia losowe – wszelkiego rodzaju klęski żywiołowe, katastrofy i wypadki, które wpływają na stan bezpieczeństwa informacji (np. pożar budynku, w którym znajdują się nośniki danych);
- tradycyjne zagrożenia informacyjne – szpiegostwo, działalność dywersyfikacyjna bądź sabotażowa (ukierunkowana na zdobycie informacji lub ofensywną dezinformację prowadzoną przez inne osoby, podmioty i organizacje);
- zagrożenia technologiczne – zagrożenia związane z gromadzeniem, przechowywaniem i przetwarzaniem informacji w sieciach i systemach teleinformatycznych (np. przestępstwa komputerowe, cyberterroryzm, walka informacyjna) oraz zagrożenia będące następstwem niedostatecznych rozwiązań strukturalnych i organizacyjnych.

Zagrożenia informacyjne można również podzielić ze względu na lokalizację ich źródła powstawania, wówczas wyróżnia się zagrożenia [7]:

- wewnętrzne – powstające wewnątrz organizacji; zagrożenia utratą, modyfikacją bądź uszkodzeniem mogą nastąpić w wyniku niezamierzonego (błędu lub przypadku) bądź celowego działania nieuczciwych pracowników (użytkowników);
- zewnętrzne – generowane poza instytucją; zagrożenia utratą, uszkodzeniem lub uniemożliwieniem wykonywania na zbiorach danych podstawowych operacji może skutkować zamierzonym bądź przypadkowym działaniem osób trzecich względem systemu czy sieci teleinformatycznej;
- fizyczne – bezpieczeństwo informacyjne zakłócone zostaje w wyniku wystąpienia awarii, katastrofy bądź innych nieoczekiwanych sytuacji ingerujących w system teleinformatyczny czy urządzenia sieciowe.

2. Materiał badawczy i metodyka badań

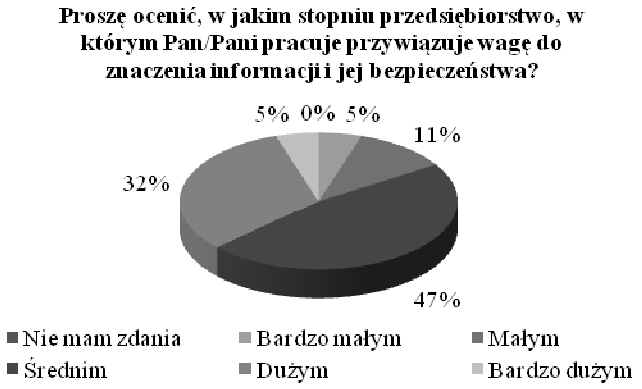
Przygotowane i przeprowadzone badania empiryczne miały na celu poznanie opinii respondentów na temat wybranych zagadnień związanych z organizacją systemu bezpieczeństwa informacji w przedsiębiorstwie. Szczególną uwagę zwrócono na trzy podstawowe aspekty, a mianowicie na: znaczenie bezpieczeństwa informacji dla badanych organizacji (sektor MŚP), identyfikację źródeł zagrożeń z uwzględnieniem nadrzędnej roli czynnika ludzkiego oraz poziom stosowanych zabezpieczeń w przedsiębiorstwie.

Kwestionariusz ankiety składał się z pytań zamkniętych (z dobraną listą odpowiedzi w oparciu o studium literaturowe) jedno- i wielokrotnego wyboru. Dobór próby badawczej miał charakter celowy, co umożliwiło wybór respondentów o określonych cechach (wykształcenie, stanowisko, staż pracy). Ankieta stanowiła cenne źródło informacji, wzbogaciła wiedzę na temat zagadnień poruszanych w niniejszej publikacji, a jej wyniki są doskonałym dopełnieniem rozważań teoretycznych.

3. Omówienie wyników badań empirycznych

Pierwszym etapem przeprowadzonych badań było poznanie opinii respondentów na temat znaczenia informacji oraz bezpieczeństwa ich pozyskiwania, gromadzenia i

przetwarzania dla prowadzonej działalności gospodarczej. Dane empiryczne pokazują, iż zdaniem 47% ankietowanych, badane organizacje w stopniu średnim przywiązują wagę do znaczenia i bezpieczeństwa informacji, natomiast w opinii 32% respondentów bezpieczeństwo informacji w posiadaniu, których jest konkretna jednostka gospodarcza ma duże znaczenie w realizowanej przez nią strategii działania. Na podkreślenie zasługuje również fakt, iż jedynie 5% ankietowanych uznaje, że przedsiębiorstwo, w którym pracują przywiązuje bardzo małą wagę do znaczenia informacji i jej bezpieczeństwa. Ponadto należy zaznaczyć, że tylko 5% respondentów wskazuje, iż badane przedsiębiorstwa uważają bezpieczeństwo informacji za coś bardzo ważnego. Rozkład odpowiedzi respondentów na pytanie prezentuje rys.1.



Rys. 1. Znaczenie informacji i jej bezpieczeństwa w przedsiębiorstwie
Źródło: opracowanie własne na podstawie wyników badań ankietowych

Dla zdiagnozowania poziomu świadomości wartości informacji ankietowani poproszeni zostali również o udzielenie odpowiedzi na pytanie: *Jakiego rodzaju straty Pana/Pani zdaniem powoduje wyciek (utrata) informacji z przedsiębiorstwa"*? Analiza uzyskanych danych wskazuje, iż pomimo znaczących trudności w ustaleniu materialnej wartości gromadzonych zasobów informacyjnych, dla blisko połowy ankietowanych (47%) utrata poufnych danych wiąże się konkretnymi stratami finansowymi ponoszonymi przez przedsiębiorstwo. Ponadto do negatywnych konsekwencji wycieku poufnych informacji ankietowani zaliczyli: brak zaufania klientów i kontrahentów (28%) oraz utratę reputacji/dobrego wizerunku firmy (25%).

Wobec powyższego, można stwierdzić, iż przeprowadzone badania zdają się potwierdzać zawartą w niniejszej pracy myśl, że informacje stanowią jedną z najwyżej cenionych wartości w biznesie. Uwzględniając również fakt, iż zarządzanie bezpieczeństwem informacji jest stosunkowo młodym obszarem zainteresowań, można przyjąć z dużym prawdopodobieństwem, iż świadomość organizacji (kierowników i pracowników) w zakresie uznawania informacji i jej bezpieczeństwa za priorytet w prowadzonej działalności gospodarczej będzie systematycznie wzrastać.

Drugim poruszanym w badaniach aspektem było zidentyfikowanie źródeł możliwych do wystąpienia zagrożeń bezpieczeństwa informacji, z uwzględnieniem wpływu czynnika ludzkiego.

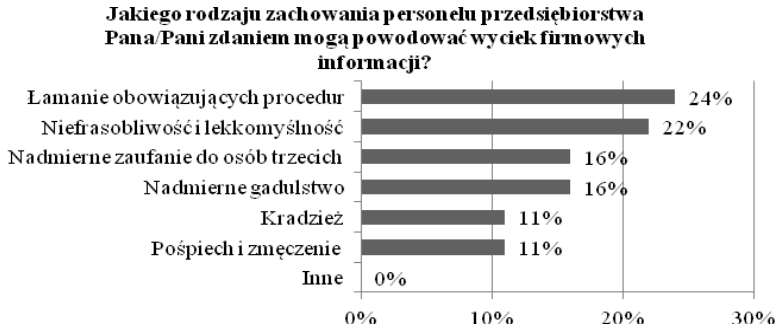
Zagrożenia związane z bezpieczeństwem informacji można podzielić na trzy zasadnicze grupy: zagrożenia zewnętrzne i wewnętrzne dla organizacji oraz zagrożenia fizyczne.

W opinii respondentów najważniejszą rolę w przedsiębiorstwie odgrywają wewnętrzne (42%) oraz zewnętrzne (37%) źródła zagrożeń. Z kolei zdaniem 21% ankietowanych to fizyczne źródła zagrożeń, takie jak katastrofy czy inne sytuacje kryzysowe w największym stopniu mogą determinować utratę bezpieczeństwa informacji. Rozkład odpowiedzi na zawarte w ankiecie pytanie prezentuje rys.2.

Rys. 2. Źródła zagrożeń bezpieczeństwa informacji
Źródło: opracowanie własne na podstawie wyników z badań ankietowych

W świetle przeprowadzonych badań można stwierdzić, iż badane organizacje świadome są tego, że to właśnie czynnik ludzki (zamierzone bądź celowe działania człowieka) stanowi najsłabsze ogniowo w procesie utworzenia, utrzymania i doskonalenia procesów związanych z zagwarantowaniem racjonalnego poziomu bezpieczeństwa. Niezbędne jest, zatem budowanie oraz wzmacnianie wśród personelu poczucia odpowiedzialności za przetwarzane dane i informacje, a także przestrzeganie ich przed rosnącą falą ataków na sieć bądź system teleinformatyczny przedsiębiorstwa lub za pośrednictwem zabiegów socjotechnicznych.

Kolejne pytanie dotyczyło rodzaju zachowań personelu przedsiębiorstwa, które mogą powodować wyciek firmowych danych. Przeprowadzona ankieta dostarczyła następujących wyników. Z zebranych danych wynika, że wśród najbardziej niepożądanych zjawisk związanych z niewłaściwym postępowaniem pracowników dominuje łamanie obowiązujących procedur (24%), niefrasobliwość oraz lekkomyślność (22%), nadmierne zaufanie do osób trzecich (16%), a także nadmierne gadulstwo (16%). Z kolei do najrzadziej wskazywanych przez ankietowanych czynników determinujących wyciek poufnych informacji z firmy należą kradzież i zmęczenie (po 11%). Rozkład udzielonych przez respondentów odpowiedzi przedstawiono na rys. 3.



Rys. 3. Zachowania personelu przedsiębiorstwa, które mogą powodować wyciek formowych informacji
Źródło: opracowanie własne na podstawie wyników z badań ankietowych

W tabeli 1 przedstawiono procentowy rozkład odpowiedzi respondentów na pytanie, w jakim stopniu poszczególne źródła wycieku informacji związane z czynnikiem ludzkim wpływają na poziom bezpieczeństwa informacji.

Tab. 1. Wpływ poszczególnych źródeł wycieku informacji na poziom bezpieczeństwa

	Niezadowolenie z zarobków	Niezadowolenie z warunków pracy	Odmowa awansu	Odmowa podwyżki	Różnice światopoglądowe	Pośpiech i zmęczenie	Monotonia wykonywanych zadań	Stres	Podatność na wpływ osób trzecich
Nie mam zdania	5%	11%	11%	21%	11%	11%	11%	16%	11%
Bardzo małym	5%	11%	11%	5%	21%	11%	42%	11%	11%
Małym	16%	47%	21%	16%	42%	37%	37%	26%	5%
Średnim	53%	21%	32%	37%	16%	26%	5%	32%	37%
Dużym	21%	11%	26%	11%	11%	16%	5%	11%	26%
Bardzo dużym	0%	0%	0%	0%	0%	0%	0%	5%	11%

Źródło: opracowanie własne na podstawie wyników z badań ankietowych

W celu oszacowania intensywności wpływu poszczególnych źródeł wycieku informacji na system bezpieczeństwa ustalono iloczyn stopnia wpływu i procentowego rozkładu udzielonej odpowiedzi. Stopień wpływu określono według następującego klucza: nie mam zdania – 0, bardzo mały – 1, mały – 2, średni – 3, duży – 4, bardzo duży – 5. Zestawienie otrzymanych wyników przedstawiono w tab. 2.

Tab. 2. Punktowa ocena wpływu poszczególnych źródeł wycieku informacji na poziom bezpieczeństwa

	Niezadowolenie z zarobków	Niezadowolenie z warunków pracy	Odmowa awansu	Odmowa podwyżki	Różnice światopoglądowe	Pośpiech i zmęczenie	Monotonia wykonywanych zadań	Stres	Podatność na wpływ osób trzecich
Nie mam zdania	0	0	0	0	0	0	0	0	0
Bardzo małym	0,05	0,11	0,11	0,05	0,21	0,11	0,42	0,11	0,11
Małym	0,32	0,94	0,42	0,32	0,84	0,74	0,74	0,52	0,1
Średnim	1,59	0,63	0,96	1,11	0,48	0,78	0,15	0,96	1,11
Dużym	0,84	0,44	1,04	0,44	0,44	0,65	0,2	0,44	1,04
Bardzo dużym	0	0	0	0	0	0	0	0,25	0,55
Razem	**2,8**	**2,12**	**2,53**	**1,92**	**1,97**	**2,27**	**1,51**	**2,28**	**2,91**

Źródło: opracowanie własne na podstawie wyników z badań ankietowych

Analiza danych zawartych w tab. 2 wskazuje, że największym zagrożeniem związanym z wyciekiem informacji jest podatność na wpływ osób trzecich (2,91). Równie istotnymi czynnikami są: niezadowolenie z zarobków (2,8), czy też odmowa awansu (2,53). Przeciętny poziom wpływu na bezpieczeństwo oszacowano dla stresu (2,8), pośpiechu i zmęczenia (2,27), niezadowolenia z warunków pracy (2,12), różnic światopoglądowych (1,97) oraz odmowy podwyżki (1,92). Z kolei według ankietowanych najmniej istotnym źródłem zagrożeń bezpieczeństwa informacji jest monotonia wykonywanych zadań (1,51).

Kolejną kwestią poruszaną podczas badań było określenie poziomu zabezpieczeń redukujących ryzyko wystąpienia niebezpieczeństwa związanego z utratą informacji.

Ankietowanych poproszono o wskazanie, ich zdaniem osoby odpowiedzialnej w przedsiębiorstwie za bezpieczeństwo posiadanych i przetwarzanych przez nie zasobów informacyjnych. Największy odsetek respondentów (54%) wskazywał na głównego informatyka firmy, z kolei jednie 8% badanych wybrało specjalistę ds. bezpieczeństwa. Negatywnym zjawiskiem są te opinie respondentów, które wyrażają braki personelu w strukturze organizacyjnej przedsiębiorstwa zajmującego się bezpieczeństwem informacji. Rozkład udzielonych odpowiedzi przedstawiono na rys.4.

Analiza danych empirycznych potwierdza przekonanie, jakie dominuje w wielu organizacjach, że bezpieczeństwo informacji równoznaczne jest z brakiem zagrożeń w infrastrukturze informatycznej przedsiębiorstwa, a odpowiedzialną za nie osobą zostaje wówczas administrator sieci. Niestety, z punktu widzenia zakresu kompetencji specjalisty ds. bezpieczeństwa jest to sytuacja wielce niepożądana. Do jego podstawowych obowiązków należy projektowanie systemu obiegu informacji (co nie ma związku

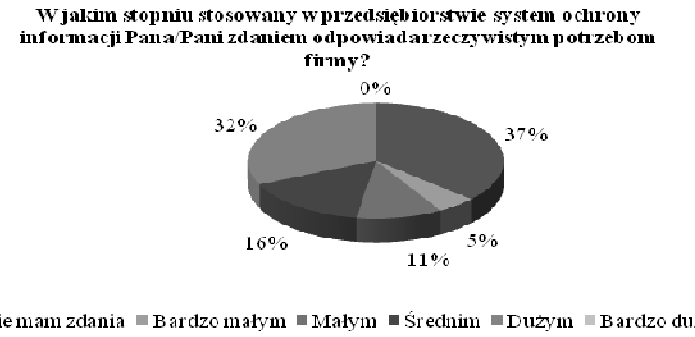
z technologią), klasyfikacja informacji, konsultacje z użytkownikami informacji i ich szkolenie, audyt wykonywania zaleceń i procedur, a także raportowanie stanu bezpieczeństwa zarządowi firmy.

Rys.4. Struktura personelu przedsiębiorstwa odpowiedzialnego za bezpieczeństwo informacji
Źródło: opracowanie własne na podstawie wyników z badań ankietowych

Do respondentów zostało również skierowane pytanie o poziom adekwatności wdrożonych w przedsiębiorstwie zabezpieczeń do jego realnych potrzeb. Zdaniem 32% ankietowanych stosowane zabezpieczenia gwarantują wysoki (duży) poziom bezpieczeństwa. Według 16% respondentów przyjęty w przedsiębiorstwie system ochrony informacji odpowiada rzeczywistym potrzebom w średnim stopniu, dla 11% - w stopniu małym, a dla 5% - bardzo małym. Rozkład odpowiedzi udzielonych przez wszystkich respondentów prezentuje rys. 5.

Na podstawie danych zaprezentowanych na rys. 5 można wysnuć wniosek, iż w świadomości pracowników stosowane w organizacji zabezpieczenia są niewystarczające do możliwości wystąpienia potencjalnych zagrożeń. Zdaniem autorów niniejszej pracy jest to pozytywne zjawisko. Po pierwsze, uświadomienie sobie przez organizację luk i braków w jej systemie bezpieczeństwa stanowi podstawę do przyjęcia strategii ukierunkowanej na ciągłe jego doskonalenie. Po drugie, świadomi zagrożeń pracownicy są bardziej ostrożni i wyczuleni na jakiekolwiek nielegalne próby wyłudzenia informacji. Nadmierne, złudne poczucie bezpieczeństwa może nie raz prowadzić do uśpienia czujności personelu organizacji i stwarzać zagrożenie chociażby w postaci udanego ataku socjotechnicznego.

System bezpieczeństwa informacji tworzą zabezpieczenia fizyczne, techniczne (informatyczne) oraz organizacyjno – proceduralne. Podczas ankietowana poproszono respondentów o wyrażenie opinii na temat wpływu poszczególnych zabezpieczeń fizycznych na stan bezpieczeństwa informacji w przedsiębiorstwie. Rozkład odpowiedzi udzielonych przez ankietowanych prezentuje tab.3.



Rys. 5. Stopień, w jakim stosowany w przedsiębiorstwie system ochrony informacji odpowiada rzeczywistym potrzebom firmy
Źródło: opracowanie własne na podstawie wyników z badań ankietowych

Tab. 3.Wpływ zabezpieczeń fizycznych na poziom bezpieczeństwa informacji

	System alarmowy	System włamania i napadu	System przeciw-pożarowy	System kontroli dostępu	System telewizji dozorowej
Nie mam zdania	16%	16%	11%	16%	16%
Bardzo mały	0%	0%	5%	0%	5%
Mały	0%	11%	16%	0%	16%
Średni	42%	26%	16%	26%	32%
Duży	26%	37%	32%	42%	32%
Bardzo duży	16%	11%	21%	16%	0%

Źródło: opracowanie własne na podstawie wyników z badań ankietowych

Celem określenia wielkości wpływu poszczególnych zabezpieczeń na poziom bezpieczeństwa dokonano ilościowej ich oceny za pomocą iloczynu stopnia wpływu i procentowego rozkładu udzielonej odpowiedzi. Stopień wpływu określono według następującego klucza: nie mam zdania – 0, bardzo mały – 1, mały – 2, średni – 3, duży – 4, bardzo duży – 5. Zestawienie otrzymanych wyników przedstawiono w tab. 4.

Na podstawie danych zamieszczonych w tab. 4 można stwierdzić, że wszystkie zastosowane w przedsiębiorstwie zabezpieczenia fizyczne, zdaniem ankietowanych mają znaczący wpływ na utworzenie i utrzymanie optymalnego poziomu bezpieczeństwa informacji. Największe znaczenie przypisano systemowi kontroli dostępu (3,26), następnie systemowi przeciwpożarowemu (3,18), systemowi alarmowemu (3,1), a także systemowi włamania i napadu. Zdaniem badanych system telewizji dozorowej (2,61) w porównaniu do pozostałych instalacji został oceniony najniżej pod względem funkcji ochronnych przed zagrożeniami związanymi z utratą firmowych danych.

Tab. 4. Punktowa ocena wpływu zabezpieczeń fizycznych na poziom bezpieczeństwa informacji

	System alarmowy	System włamania i napadu	System przeciw-pożarowy	System kontroli dostępu	System telewizji dozorowej
Nie mam zdania	0	0	0	0	0
Bardzo małym	0	0	0,05	0	0,05
Małym	0	0,22	0,32	0	0,32
Średnim	1,26	0,78	0,48	0,78	0,96
Dużym	1,04	1,48	1,28	1,68	1,28
Bardzo dużym	0,8	0,55	1,05	0,8	0
Razem	**3,1**	**3,03**	**3,18**	**3,26**	**2,61**

Źródło: opracowanie własne na podstawie wyników z badań ankietowych

4. Podsumowanie i wnioski

Informacje bez względu na to czy są drukowane na papierze, wypowiadane w trakcie rozmowy, przechowywane w formie elektronicznej czy też transmitowane za pomocą nowoczesnej technologii komputerowej stanowią cenny zasób każdej organizacji. Ogromna rola informacji wiąże się z licznymi zagrożeniami utraty jej bezpieczeństwa, do których można zaliczyć: uszkodzenie, ujawnienie, nieautoryzowaną modyfikację, utratę, a także kradzież. Wobec tego, kierownicy organizacji zobligowani są do bacznego przyglądania się problematyce bezpieczeństwa informacji w swojej jednostce oraz zorganizowania należytego systemu ochrony.

Opracowanie, utworzenie, utrzymanie i doskonalenie właściwego systemu ochrony informacji gwarantującego wysoki poziom jej bezpieczeństwa wymaga szerokie spektrum działań. Obok inwestycji w najnowocześniejsze dostępne na rynku rozwiązania techniczne bardzo ważne są również kwestie organizacyjne oraz świadomość całego personelu. Bezpieczeństwo informacji nie koncentruje się tylko i wyłącznie na zabezpieczeniach informatycznych czy fizycznych, ale przede wszystkim na odpowiednio przeszkolonych i świadomych pracownikach, jasno określonych zasadach i sposobach postępowania, odpowiednio przygotowanych umowach z klientami, dostawcami i innymi podmiotami, a także sformalizowanych i przetestowanych planach ciągłości działania.

Poprowadzone badania ankietowe pozwalają wnioskować, że organizacje świadome są wartości informacji, potrzeby zagwarantowania jej bezpieczeństwa oraz negatywnych skutków ich wycieku z firmy. Zdaniem badanych pracowników zasoby informacyjne, podobnie jak każdego rodzaju aktywa, posiadają określony wymiar materialny, a ich utarta wiąże się z rzeczywistymi stratami finansowymi.

W świetle przeprowadzonych badań empirycznych potwierdza się teza, iż najsłabszym ogniwem w systemie bezpieczeństwa informacji jest czynnik ludzki. W większości przypadków ankietowani wskazywali na wewnętrzne bądź zewnętrzne źródła zagrożeń, które wiążą się z różnorodną aktywnością człowieka. Wśród typowych zachowań personelu

determinujących wyciek informacji z firmy ankietowani wskazywali: łamanie obowiązujących procedur, niefrasobliwość oraz lekkomyślność, nadmierne zaufanie do osób trzecich, a także nadmierne gadulstwo. Istotny wpływ czynnika ludzkiego na system bezpieczeństwa informacji potwierdziła przeprowadzona w pracy analiza statystyczna otrzymanych wyników badań. Najistotniejszym źródłem wycieku informacji okazała się również podatność na wpływ osób trzecich.

Badania ankietowe obejmowały swoim zakresem również poziom stosowanego w przedsiębiorstwie systemu zabezpieczeń. Niepożądanym zjawiskiem jest fakt, iż aż 21 % badanych nie potrafi wskazać osoby odpowiedzialnej za bezpieczeństwo informacji w jednostce organizacyjnej. Z kolei dla ponad połowy badanych funkcję tę pełni główny informatyk firmy. Respondenci zapytani o to, w jakim stopniu stosowany w przedsiębiorstwie system ochrony informacji odpowiada rzeczywistym potrzebom, w większości przypadków wstrzymywali się od udzielenia merytorycznej odpowiedzi i wybierali opcję „Nie mam zdania". Analizując pozostałe informacje od respondentów można stwierdzić, iż ich zdaniem eksploatowany w przedsiębiorstwie system ochrony jest niewystarczający. Tego rodzaju opinia nie jest wynikiem poważnych uchybień po stronie firmy, ale świadomością personelu w zakresie pojawiania się coraz to nowszych form zagrożeń i w pozytywny sposób może przełożyć się na ich czujność wobec intruzów próbujących wyłudzić poufne dane organizacji. Biorąc pod uwagę system zabezpieczeń fizycznych w opinii badanych największe znaczenie przypisano systemom kontroli dostępu oraz przeciwpożarowemu, natomiast najmniejsze telewizji przemysłowej, powszechnie nazywanej monitoringiem.

Literatura

1. Bączek P., Zagrożenia informacyjne a bezpieczeństwo państwa polskiego, Adam Marszałek, Toruń 2005.
2. Calder A., A business guide to information security, Kogan Page, 2006.
3. Egan M., Mather T., The executive guide to information security. Threats, Challenges and Solutions, Addison-Wesley, Indianapolis 2005.
4. Janczak J, Nowak A., Bezpieczeństwo informacyjne. Wybrane problemy, AON, Warszawa 2013.
5. Korzeniowski L.F., Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych, EAS, Kraków 2008.
6. Wrzosek M., Nowak A., Identyfikacja zagrożeń determinujących zmiany w systemie bezpieczeństwa społeczeństwa informacyjnego, AON, Warszawa 2009.
7. Żebrowski A., Kwiatkowski M., Bezpieczeństwo informacyjne III Rzeczypospolitej, Oficyna Wydawnicza Abrys, Kraków 2000.

Mgr inż. Michał Pałęga
Dr hab. inż. Marcin Knapiński, prof. PCz.
Dr Wiesław Kulma
Instytut Przeróbki Plastycznej i Inżynierii Bezpieczeństwa
Politechnika Częstochowska
42 – 201 Częstochowa, Dąbrowskiego 69
tel./fax: (0-34) 325 07 90
e-mail: mpalega@wip.pcz.pl
knap@wip.pcz.pl
wkulma@wip.pcz.pl