Zeszyty Naukowe nr 865 2011
Uniwersytetu Ekonomicznego w Krakowie

Jan Madej
Katedra Informatyki

Wydatki na bezpieczeństwo systemów informatycznych. Inwestycja czy koszt funkcjonowania systemu?

Streszczenie. Artykuł poświęcony jest rozważaniom na temat tego czy wydatki na bezpieczeństwo systemu informatycznego są inwestycją, czy kosztem funkcjonowania systemu. W artykule przedstawione zostały najważniejsze czynniki, które należy uwzględnić, aby ustalić czy wydatki te są kosztem czy inwestycją, m.in. trudności pomiaru poziomu bezpieczeństwa, wielkość wydatków na bezpieczeństwo a jego poziom oraz zmiana poziomu bezpieczeństwa w czasie.

Słowa kluczowe: bezpieczeństwo systemów informatycznych, wydatki na bezpieczeństwo SI, koszty bezpieczeństwa, inwestycje w bezpieczeństwo.

1. Wprowadzenie

Obecnie technologia informatyczna (TI) osiągnęła we wszystkich niemal sferach życia człowieka tak duże znaczenie, że praktycznie można mówić o uzależnieniu od niej. Wiele obszarów działalności gospodarczej, społecznej, a nawet kulturalnej nie mogłoby bez niej funkcjonować. Dbałość o bezpieczeństwo systemów informatycznych (SI) w przedsiębiorstwach stała się koniecznością. Jednym z przejawów dbania o bezpieczeństwo SI jest ponoszenie wydatków na zakup nowych zabezpieczeń (sprzętowych i programowych), szkolenia pracowników, czy wdrażanie nowych rozwiązań organizacyjnych. Wydatki na bezpieczeństwo systemów informatycznych są niezbędne, a od kilku już lat można zaobserwować w publikacjach (branżowych i naukowych), ofertach firm TI, reklamach, wypowiedziach specjalistów i zwykłych użytkowników, że wydatki na bezpieczeństwo SI

stanowią inwestycję przedsiębiorstwa. Czy takie traktowanie tych wydatków jest uzasadnione, czy stanowi swoistego rodzaju nadużycie wykorzystywane np. w celu marketingowym, w celu uzasadnienia zbyt dużych kosztów, czy w celu poprawienia wizerunku przedsiębiorstwa w opinii akcjonariuszy lub kontrahentów? Stosowanie terminu „inwestycja" przez firmy zajmujące się świadczeniem usług w zakresie bezpieczeństwa systemów informatycznych jest, z oczywistych powodów, zrozumiałe. Jednak w przypadkach innych przedsiębiorstw często wynika to wyłącznie z chęci wywarcia pozytywnego, ale nie zawsze uzasadnionego wrażenia[1].

Celem artykułu jest próba uzyskania odpowiedzi na pytanie, czy wydatki na bezpieczeństwo systemów informatycznych można traktować jako inwestycję, czy pozostają one tylko i wyłącznie kosztem funkcjonowania systemu. Cel ten ma charakter dyskusyjny, gdyż bazuje na różnym postrzeganiu terminu „inwestycja"[2]. Ważne wydaje się wskazanie przyczyn, które sprawiają, że wydatki te powinny być traktowane jako inwestycje. Właśnie głównym zamiarem autora jest zwrócenie uwagi na to, jak złożonym zagadnieniem jest bezpieczeństwo systemów informatycznych, jak dużą zmiennością i nieprzewidywalnością się charakteryzuje i jak trudno dokonać odpowiednich pomiarów i szacunków oraz zrealizować założone plany dotyczące zakresu działań, terminów i wydatków.

Należy dodać, że celem artykułu nie jest analiza wielkości, struktury i celowości tych wydatków[3], chociaż jest to zagadnienie bardzo ważne tak w wypadku zarządzania bezpieczeństwem, jak i funkcjonowania całego przedsiębiorstwa.

---

[1] Przykładowo przedsiębiorstwo, które nie miało odpowiednio funkcjonującej sieci komputerowej i zostało w końcu zmuszone (np. wyciekami danych, atakami z zewnątrz, zarażeniem wirusami, awariami itp.) do poniesienia wydatków na przywrócenie normalnego funkcjonowania sieci, raczej nie powinno mówić o inwestycjach tylko o poniesionych kosztach.

[2] Należy zaznaczyć, że samo pojęcie inwestycji ma szerokie znaczenie. Mówi się o inwestowaniu „w bezpieczeństwo", „w naukę", „w pracowników", „w wychowanie dzieci", „w zdrowie". Chociaż wszystkie te zwroty oddają ideę inwestowania, to w artykule chodzi o bardziej formalne znaczenie tego słowa, tak jak jest ono rozumiane w obszarze zarządzaniu przedsiębiorstwem, czy w rachunkowości.

[3] Na rynku europejskim, wydatki na bezpieczeństwo systemów informatycznych przedsiębiorstwa stanowią około 5% ogólnej kwoty przeznaczonej na technologię informatyczną [*Bezpieczeństwo systemów…* 2000]. Na rynku amerykańskim udział tych wydatków jest nieznacznie większy. Przeprowadzone badania wykazały, że wynosi on około 7% [Augustyniak 2002]. Taki poziom wydatków na bezpieczeństwo nie jest wystarczający. Według tych samych badań, większość ankietowanych (63%) twierdzi, że potrzebne są w ich przedsiębiorstwie dalsze wydatki na ten cel, 32% uważa je za odpowiednie, a tylko 5% sądzi, że wydatki na bezpieczeństwo można obniżyć. Podobnych wyników dostarczyły badania przeprowadzone przez firmę Ernst & Young [*Światowe badania…* 2003]. Według nich, brak wystarczających środków finansowych stanowi największą przeszkodę w osiągnięciu zadowalającego poziomu bezpieczeństwa. W dodatku, największy wpływ na te wydatki ma poziom zysków osiąganych przez przedsiębiorstwo. Oznacza to, że pogarszanie się wyników finansowych przedsiębiorstwa bezpośrednio odbija się na poziomie wydatków na bezpieczeństwo SI.

2. Bezpieczeństwo systemu informatycznego

W celu lepszego zrozumienia problematyki należy najpierw przedstawić najważniejsze zagadnienia dotyczące bezpieczeństwa SI. Obecnie według standardów polskich i międzynarodowych pod pojęciem bezpieczeństwa systemu informatycznego rozumiane są wszystkie aspekty związane z definiowaniem, osiąganiem i utrzymywaniem tzw. atrybutów bezpieczeństwa, czyli poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności systemu [PN-I-13335-1: 1999]. Proces realizowany w celu osiągnięcia i utrzymania odpowiedniego poziomu atrybutów bezpieczeństwa określany jest mianem zarządzania bezpieczeństwem systemu informatycznego.

Punktem wyjścia w rozważaniach na temat bezpieczeństwa systemu informatycznego są zasoby[4] występujące w systemie, posiadające określoną wartość i związane z nią wymagania ochronne. Ponadto na rzeczywisty poziom bezpieczeństwa systemu i jego zasobów wpływają jeszcze inne elementy, takie jak [PN-I-13335-1: 1999]:

– zagrożenie, czyli potencjalna przyczyna niepożądanego incydentu, którego skutkiem może być szkoda dla systemu. Niektóre zagrożenia mogą mieć wpływ na większą liczbę zasobów i powodować różne skutki w zależności od tego, których zasobów dotknęły;

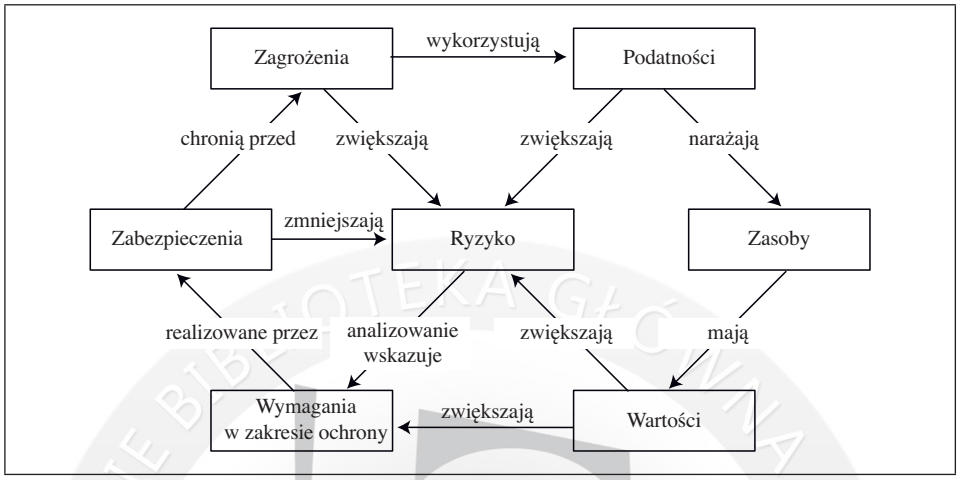
– podatność jest to słabość zasobu lub grupy zasobów, która może być wykorzystana przez zagrożenie. Podatność zasobów oznacza ich pewną słabość, ale sama w sobie nie powoduje szkody. Jest jedynie warunkiem (zbiorem warunków), które mogą umożliwić zagrożeniu oddziaływanie na zasoby;

– ryzyko jest to prawdopodobieństwo, że określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów, aby spowodować ich zniszczenie lub straty.

Wszystkie te elementy tworzą system wzajemnych relacji określany także mianem modelu zarządzania ryzykiem (rys. 1).

Według S. Augustyniaka [2002] struktura wydatków przedstawia się następująco: zabezpieczenia techniczne – 36%, wynagrodzenie specjalistów – 23%, konsulting – 11%, opracowanie strategii – 9%, szkolenia – 9%. Badania firmy Ernst & Young dowodzą również, że największe nakłady ponoszone są na zakup nowych technologii oraz narzędzi informatycznych.

[4] W celu ich identyfikacji najczęściej przyjmuje się, że „zasoby, to wszystko to, co ma dla instytucji wartość" [PN-I-13335-1: 1999]. Kryterium wartości jest powszechnie przyjęte i trafiające do przekonania, gdyż sprowadza się do zasady, że należy chronić wszystko to, co przedstawia dla przedsiębiorstwa wartość. Należy jednak pamiętać, że nie wszystkie zasoby mają postać materialną, a ich wartość nie zawsze można jednoznacznie określić.



Rys. 1. Zależności pomiędzy podstawowymi elementami wpływającymi na bezpieczeństwo SI

Źródło: opracowanie własne na podstawie [PN-I-13335-1: 1999].

Zależności pomiędzy tymi elementami wskazują jak wieloaspektowym zagadnieniem jest bezpieczeństwo systemu informatycznego. Występujące elementy są ze sobą ściśle powiązane i wszystkie mają wpływ na bezpieczeństwo systemu. Liczne zależności pomiędzy przedstawionymi elementami nie stanowią jedynej trudności w problematyce bezpieczeństwa SI, najważniejsze z nich zostały przedstawione poniżej. Warto zatem podkreślić, że wydatki na bezpieczeństwo SI są kierowane tylko na zakup (wdrożenie) zabezpieczeń lub na zmniejszanie podatności zasobów.

3. Charakter wydatków na bezpieczeństwo SI

Podstawowym argumentem osób traktujących wydatki na bezpieczeństwo SI jako inwestycje, jest twierdzenie, że pozwalają one uniknąć w przyszłości strat spowodowanych następstwami zagrożeń, które mogą wystąpić. Taką opinię wyrażają zarówno specjaliści, jak i przedstawiciele firm świadczących usługi bezpieczeństwa lub wytwarzających urządzenia i oprogramowanie zabezpieczające. Konieczność wdrażania zabezpieczeń i korzyści z tego płynące są bezsporne. Wątpliwość budzi, to, czy wydatki te można traktować jako inwestycje (w pełnym tego słowa znaczeniu), czy są to tylko koszty związane z prowadzeniem bieżącej działalności przedsiębiorstwa.

Stosowana w rachunkowości (por. np. [Burzym 1971]) klasyczna definicja kosztu zakłada, że jest to niezbędne (gospodarczo i społecznie uzasadnione) zuży-

cie środków, usług lub wykorzystanie pracy, które jest związane z efektem użytecznym, powstałym w danym okresie na jakimkolwiek odcinku działalności przedsiębiorstwa. Zgodnie z tą definicją, wydatki na bezpieczeństwo systemu można uznać niewątpliwie za koszty. Są one niezbędne i przynoszą użyteczny efekt. Tymczasem inwestowanie to proces określania, planowania, oceny i finansowania projektów inwestycyjnych przedsiębiorstwa. Inwestycje cechują się: ogromymi ponoszonymi nakładami, długotrwałością procesu, wpływami na przyszły stan przedsiębiorstwa, dlatego wymagają szczególnie ostrożnych, systematycznych analiz, które pozwalają m.in. na [Dobija 1997]:

– określenie potrzeb przedsiębiorstwa, których zaspokojenie wymaga zastosowania procesu inwestycyjnego,

– określenie metod oceny projektów inwestycyjnych,

– dokonanie obliczeń przy zastosowaniu wybranych metod rachunku.

Efektem procesu inwestycyjnego mają być korzyści przedsiębiorstwa w zakresie technicznym i finansowym w kolejnych latach (zob. [Drury 1995]). Bezpieczeństwo systemów informatycznych jest jednak problemem tak złożonym, zmiennym, nieprzewidywalnym oraz niedającym się zwymiarować, że określanie potrzeb, ocenianie i dokonywanie obliczeń jest bardzo trudne, a czasami wręcz niemożliwe. Do podstawowych czynników, które wykluczają możliwość traktowania wydatków na bezpieczeństwo jako inwestycji, należy:

– brak możliwości pomiaru poziomu bezpieczeństwa (zarówno obecnego, jak i przyszłego),

– ściśle nieokreślona zależność pomiędzy wielkością wydatków na bezpieczeństwo a poziomem uzyskanego bezpieczeństwa,

– nieprzewidywalny spadek poziomu bezpieczeństwa w czasie.

Traktowanie wydatków na bezpieczeństwo jako inwestycji wymaga uzasadnienia wydatków i wykazania ich opłacalności, ale najczęściej wykorzystywany miernik efektywności inwestycji – wskaźnik zwrotu z inwestycji ROI (*Return on Investment*) – nie spełnia swojego zadania, przede wszystkim ze względu na trudną do oszacowania wartość zysku, jaką przyniesie wdrożenie zabezpieczeń[5]. Według badań firmy Ernst & Young [*Światowe badania…* 2003], około 60% przedsiębiorstw nie próbuje nawet obliczać ROI dla „inwestycji" dotyczących bezpieczeństwa informacji lub robi to bardzo rzadko. Z powodu nieprzydatności tego wskaźnika opracowano nowy wskaźnik o nazwie zwrot z inwestycji w bezpieczeństwo – ROSI[6] (*Return on Security Investment*). Jednak także w wypadku

[5] Wskaźnik ROI oblicza się, dzieląc osiągnięty zysk przez zainwestowany kapitał.

[6] Zwrot inwestycji w bezpieczeństwo wyrażony jest wzorem [Edwards 2002]: ROSI = R – (ALE), gdzie: R – roczne koszty odzyskania poniesionych strat, ALE (Annual Loss Expectancy) – roczne spodziewane straty, ALE = T + (R – E), gdzie: T – koszt zabezpieczeń (koszt inwestycji), E – oszczędności wynikające z prewencji.

tego wskaźnika kwantyfikacja niektórych składowych wpływających na jego wartość jest bardzo trudna lub wręcz niemożliwa (np. spodziewane straty wynikające z utraty zaufania kontrahentów), dlatego nawet twórcy wskaźnika zaznaczają, że otrzymywane wyniki mają charakter orientacyjny.

4. Trudności pomiaru poziomu bezpieczeństwa SI

W potocznym języku istnieje sformułowanie „w 100% bezpieczne, jako określenie całkowitego bezpieczeństwa. Takie „procentowe" przedstawienie poziomu bezpieczeństwa jest zgodne z ogólnym wyobrażeniem o tym zjawisku i łatwe do zaakceptowania. Wydaje się również, że można je łatwo zinterpretować. Tymczasem w praktyce pomiary poziomu bezpieczeństwa realizowane są głównie na skalach porządkowych, a osoby zajmujące się zagadnieniami bezpieczeństwa systemów informatycznych od dawna poszukują metody pomiaru, która pozwalałaby dokładnie wyrazić poziom bezpieczeństwa w skali interwałowej lub ilorazowej. Taki pomiar posiadałby wiele zalet, umożliwiłby np.:

– dokładne porównywanie poziomu bezpieczeństwa różnych systemów,

– określenie skuteczności poszczególnych zabezpieczeń, dzięki możliwości zbadania zmian poziomu bezpieczeństwa wywołanych wprowadzeniem lub usunięciem zabezpieczenia,

– dokładne obliczenie kosztów, jakie należy ponieść, aby zwiększyć poziom bezpieczeństwa systemu o określoną wartość,

– bieżące i dokładne monitorowanie poziomu bezpieczeństwa, a tym samym szybkie reagowanie na jego spadki.

Niejednorodny charakter systemów informatycznych sprawia, że opracowanie użytecznej metody pomiaru bezpieczeństwa w skali interwałowej lub ilorazowej jest bardzo trudne. W przeszłości podejmowanych było wiele prób opracowania tego typu metod pomiaru[7]. Ich twórcy w większości przypadków sami zwracali uwagę na pewne słabości prezentowanych metod, wyrażając jednocześnie nadzieję, że dalsze badania, a przede wszystkim postępujący rozwój technologii informatycznej pozwoli je udoskonalić. Rozwój TI, wbrew przypuszczeniom, spowodował, że praktyczne wykorzystanie tych metod stało się jeszcze bardziej ograniczone. Do zasadniczych przyczyn tego stanu należy m.in.:

[7] Wspomnieć można chociażby o takich metodach pomiaru, jak: metoda oceny „najsłabszego ogniwa", pomiar poziomu bezpieczeństwa z użyciem ocen bezpieczeństwa, pomiar poziomu bezpieczeństwa z wykorzystaniem wartości rozmytych czy pomiar poziomu bezpieczeństwa przy użyciu list kontrolnych.

– złożony i niejednorodny charakter systemów informatycznych[8],
– brak standardowych rozwiązań w zakresie budowy i ochrony SI,
– duża dynamika rozwoju i zmienność SI,
– trudny do przewidzenia spadek poziomu bezpieczeństwa SI w czasie,
– brak metod pozwalających na wyznaczenie ryzyka, podatności i zagrożeń zasobów,
– brak danych empirycznych (na temat występowania zagrożeń, podatności i ryzyka),
– nieprzewidywalny charakter błędów i luk w programach, systemach operacyjnych, zabezpieczeniach itd.,
– trudności z wyznaczeniem wartości zasobu i wpływu jego uszkodzenia lub zniszczenia na poziom bezpieczeństwa systemu.

Należy mieć nadzieję, że wprowadzenie wspólnych zasad i standardów dotyczących budowy i funkcjonowania systemów informatycznych oraz tworzenie systemów zintegrowanych i posiadających wbudowane zabezpieczenia pozwoli w przyszłości na dokładne zmierzenie poziomu ich bezpieczeństwa. Na razie jednak nie jest możliwe uzyskanie jakichkolwiek rzetelnych pomiarów i obliczeń związanych z inwestowaniem w bezpieczeństwo SI (np. zmierzenie istniejącego poziomu bezpieczeństwa i założenie uzyskania – po inwestycji – poziomu dwukrotnie wyższego).

5. Wielkość wydatków na bezpieczeństwo a jego poziom

Brak możliwości zmierzenia poziomu bezpieczeństwa wyklucza możliwość ustalenia dokładnej zależności pomiędzy wydatkami a uzyskanym poziomem bezpieczeństwa. Nie znaczy to jednak, że nie jest znana ogólna zależność pomiędzy nimi. Specjaliści z zakresu bezpieczeństwa informatycznego są zgodni, że zależność między poziomem osiągniętego bezpieczeństwa a przeznaczonymi na nie wydatkami nie jest liniowa. Rys. 2 przedstawia główne relacje między osiągniętym poziomem bezpieczeństwa a wydatkami, jak np.[9]:

[8] Wspomniane metody pomiaru poziomu bezpieczeństwa SI (z użyciem ocen bezpieczeństwa, list kontrolnych itd.) działają w sposób syntetyczny. Zakładają, że jeśli uda się zmierzyć poziom bezpieczeństwa fragmentów systemu informatycznego (np. zasobów), to na tej podstawie ustali się bezpieczeństwo całego systemu. Jednak, jak dowodzi praktyka, złożony charakter systemu informatycznego sprawia, że wiele zagrożeń występuje „na granicy" różnych jego fragmentów, wtedy to współdziałające ze sobą elementy należące do różnych części systemu mają większy poziom podatności na zagrożenia i osłabiają cały system.

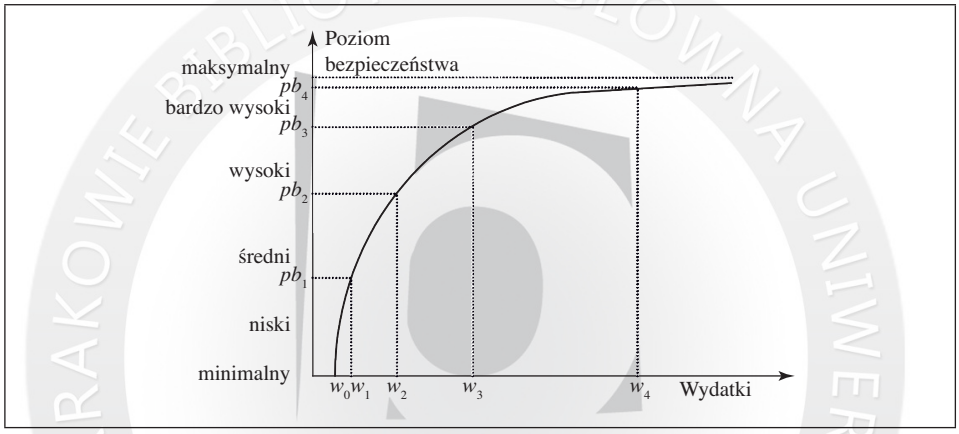
[9] Należy zaznaczyć, że zależność ta ma miejsce wtedy, kiedy ponoszone przez przedsiębiorstwo wydatki są celowe.

– osiągnięcie nawet minimalnego poziomu bezpieczeństwa wymaga poniesienia pewnych wydatków (w_0),

w systemie o niskim poziomie bezpieczeństwa nawet niewielkie zwiększenie wydatków (z w_1 do w_2) znacznie podnosi ten poziom (z pb_1 do pb_2),

– w systemie o wysokim poziomie bezpieczeństwa nawet duże zwiększenie wydatków (z w_3 do w_4) w niewielkim stopniu podnosi poziom bezpieczeństwa (z pb_3 do pb_4),

– maksymalny poziom bezpieczeństwa jest w praktyce nieosiągalny.



Rys. 2. Zależność między poziomem bezpieczeństwa a wydatkami na bezpieczeństwo
Źródło: opracowanie własne.

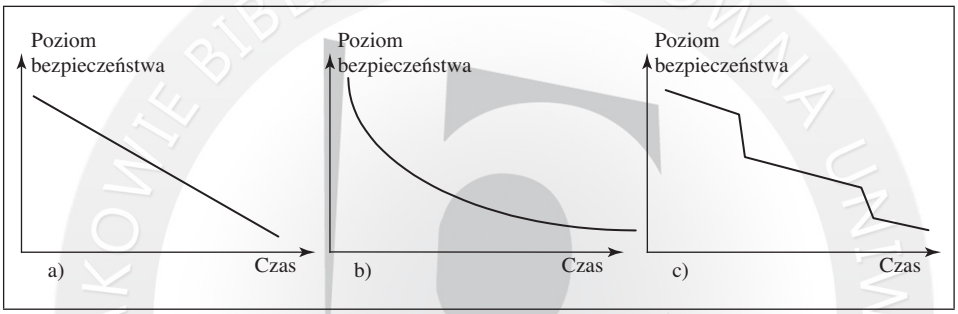
Traktując te wydatki jako inwestycje, niemożliwe jest osiągnięcie całkowitego poziomu bezpieczeństwa, także w systemie o wysokim poziomie bezpieczeństwa nawet znaczne zwiększenie wydatków w niewielkim stopniu podnosi poziom bezpieczeństwa. Te ograniczenia mają zdecydowany wpływ na niechęć kierownictwa do ponoszenia wydatków w tym zakresie.

6. Zmiana poziomu bezpieczeństwa w czasie

Kolejnym elementem, który należy uwzględnić podczas planowania wydatków na bezpieczeństwo systemu informatycznego, w szczególności kiedy wydatki te traktowane są jako inwestycja, jest czas. Technologia informatyczna charakteryzuje się dużą zmiennością w czasie. Jej szybki i dynamiczny rozwój sprawia, że zmienia się system informatyczny i jego otoczenie, a także pojawiają się nowe zagrożenia.

Ogólną zależność pomiędzy czasem a poziomem bezpieczeństwa można wyrazić następująco: jeżeli w systemie informatycznym nie są dokonywane żadne

zmiany mające na celu utrzymanie poziomu bezpieczeństwa (czyli wydatki na bezpieczeństwo nie są ponoszone), to poziom bezpieczeństwa maleje wraz z upływem czasu. Jednak dokładny przebieg tego zjawiska jest trudny do określenia, zależny od wielu czynników i może mieć różny charakter (rys. 3). Najbardziej odpowiadająca rzeczywistości jest sytuacja, w której stale zmniejszający się poziom bezpieczeństwa jest dodatkowo obniżany z powodu np. wykrycia błędów i luk w systemie ochrony lub wprowadzenia nowej technologii pozwalającej na pokonanie zabezpieczeń[10] (rys. 3c). Tego typu spadki poziomu bezpieczeństwa mają nieprzewidywalny charakter, co sprawia, że ich uwzględnienie jest bardzo trudne.



Rys. 3. Przykładowe zmiany poziomu bezpieczeństwa w czasie
Źródło: opracowanie własne.

Nieprzewidywalny spadek poziomu bezpieczeństwa w czasie w dużym stopniu utrudnia zarządzanie bezpieczeństwem SI i tym samym traktowanie wydatków na bezpieczeństwo jako inwestycji. Jakiekolwiek założenia dotyczące planowanego osiągnięcia poziomu bezpieczeństwa czy wielkości poniesionych wydatków w tej sytuacji są bardzo trudne.

7. Zakończenie

Celem artykułu była próba uzasadnienia, że wydatków na bezpieczeństwo SI nie powinno się traktować jako inwestycji, ale jako koszt funkcjonowania systemu głównie ze względu na dużą zmienność i nieprzewidywalność zjawiska bezpieczeństwa oraz brak możliwości dokonania odpowiednich pomiarów i szacunków pozwalających zrealizować założone plany działań, terminów i wydatków.

Porównania wydatków na bezpieczeństwo do ubezpieczeń od zdarzeń losowych są interesujące i często wykazują podobieństwa, szczególnie w zakresie

[10] Np. wzrost szybkości działania komputerów pozwolił na przełamanie niektórych algorytmów kryptograficznych, uchodzących jeszcze kilka lat temu za bezpieczne.

ponoszenia kosztów bez gwarancji czy w jakiś sposób one się zwrócą i czy w związku z tym jest potrzeba ich ponoszenia[11]. Jednak charakter różnych zabezpieczeń jest często inny i w większym zakresie oddziałuje na funkcjonowanie SI[12].

Należy zaznaczyć, że brak informacji zwrotnej o skuteczności wdrożonych zabezpieczeń (a tym samych wydanych środków) jest dużym problemem wydatkowania środków na zabezpieczenia (bez względu na to czy są one traktowane jako koszty, inwestycje, czy ubezpieczenia). Oznacza to, że jeżeli przedsiębiorstwo zakupi i wdroży jakieś zabezpieczenie SI i w ciągu roku nie wydarzy się żadne następstwo zagrożeń, to i tak najczęściej nie będzie wiadomo, czy „nic się nie stało", dlatego że system był zabezpieczony, czy dlatego że żadnego zagrożenia nie było.

Literatura

Augustyniak S. [2002], *Specjaliści od bezpieczeństwa*, CXO – Magazyn kadry zarządzającej, serwis internetowy, http://www.cxo.pl/.

Bezpieczeństwo systemów komputerowych [2000], red. A. Grzywak, Wydawnictwo Pracowni Komputerowej Jacka Skalmierskiego, Gliwice.

Burzym E. [1971], *Pomiar i ocena rentowności przedsiębiorstw przemysłowych*, PWE, Warszawa.

Dobija M. [1997], *Rachunkowość zarządcza i controlling*, Wydawnictwo Naukowe PWN, Warszawa 1997.

Drury C. [1995], *Rachunek kosztów. Wprowadzenie*, Wydawnictwo Naukowe PWN, Warszawa 1995.

Edwards M.J. [2002], *Intrusion Cleanup: What's the Cost?*, http://www.ntsecurity.net/Articles/.

Polska Norma PN-I-13335-1 [1999], [PN-I-13335-1], *Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych*, Polski Komitet Normalizacyjny, Warszawa.

Światowe badania dotyczące bezpieczeństwa informacji [2003], Ernst & Young, Ernst & Young www.

[11] Przykładowo fakt, że przedsiębiorstwo wykupiło ubezpieczenie przed zniszczeniami spowodowanymi przez wichurę nie ma wpływu na to, czy wichura wystąpi czy nie wystąpi i czy „warto było" to ubezpieczenie wykupić. Podobnie fakt, że przedsiębiorstwo zakupiło urządzenia do tworzenia kopii danych, też nie ma żadnego wpływu na to, czy wystąpi awaria nośników danych w systemie informatycznym.

[12] Np. zależność między wydatkami na szkolenia administratora a wystąpieniem zagrożeń wywołanych nieodpowiednim zarządzaniem siecią można już bezpośrednio wykazać.

Expenses for Computer Systems Security – an Investment or a Cost of System Operation?

The paper considers the issue, whether expenses for a computer system security should be regarded as an investment or as a cost of system functioning. The article also submits most important factors that should be taken into account in the problem, among others difficulties in security level measurement, extent of expenses for security in relation to its level, and change of a security level in time.

Key words: computer systems security, expenses for computer system security, cost of security, investments in security.