Mirosław Ryba*

OPARTA NA KONCEPCJI RYWALIZACJI METODA ANALIZY RYZYKA SYSTEMÓW INFORMATYCZNYCH

Publikacja prezentuje opracowaną przez autora metodę oceny poziomu ryzyka informatycznego z perspektywy ludzkich zachowań. Stanowi ona alternatywę dla powszechnie stosowanych podejść do analizy ryzyka, polegających na identyfikacji podatności i zagrożeń oraz szacowaniu prawdopodobieństw ich wystąpienia. Metoda ta uwzględnia wpływ na ryzyko systemu informatycznego takich czynników, jak kwalifikacje administratorów i użytkowników tego systemu, wiedzę i determinację atakującego czy zastosowane przez niego techniki ataku. Kluczowym elementem metody analizy ryzyka, proponowanej w niniejszej pracy, jest formuła matematyczna pozwalająca na ilościowe określenie poziomu tego ryzyka.

Słowa kluczowe: *ryzyko informatyczne, metody oceny ryzyka oparte na rywalizacji*

COMPETITIVE APPROACH TO INFORMATION SYSTEM RISK ANALYSES

This article presents the method of IT risk assessment from human behaviour perspective, developed by the author. It is an alternative for the commonly used approaches to risk assessment, based on vulnerability and threat identification and the probability estimation of their occurrence. The authors method applies to risk calculation factors such as administrators or users skills, attackers knowledge and determination, or attack method used. The key element of the proposed risk analysis competitive method is a mathematical formula which allows for risk level quantification.

Keywords: *IT system risk analyses, competitive methods*

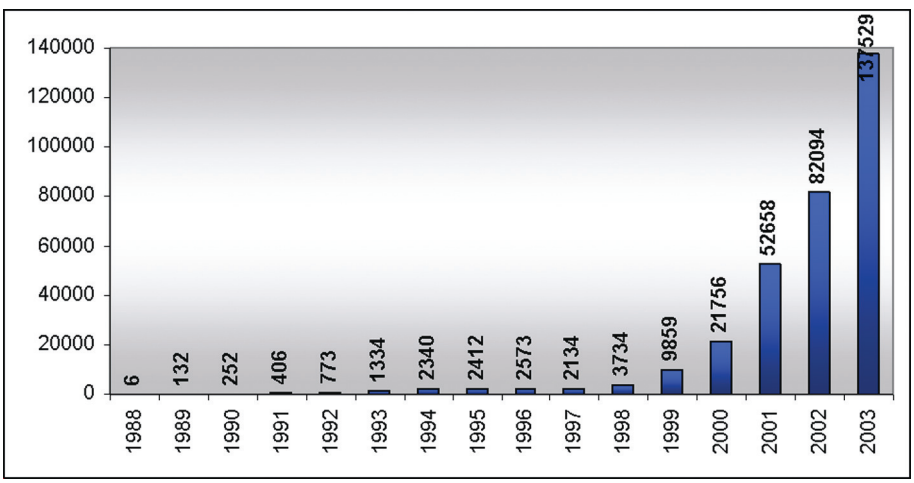
1. Wprowadzenie

W dobie powszechnej informatyzacji, systemy informatyczne zaczynają odgrywać coraz bardziej znaczącą rolę w funkcjonowaniu firm. Systemy te wiążą się jednak z pewnymi zagrożeniami, których wyznaczenie staje się obecnie jednym z kluczowych elementów analizy ryzyka działalności.

*Doświadczony konsultant w Dziale Zarządzania Ryzykiem Informatycznym w polskim oddziale firmy audytorsko-doradczej Ernst & Young, Miroslaw.Ryba@pl.ey.com

Obecnie stosowanych jest wiele podejść mających na celu wyznaczenia poziomu ryzyka systemów informatycznych. Większość tych metod opiera się na podobnym schemacie polegającym na określeniu wielkości potencjalnych strat, jakie mogą zostać spowodowane przez zidentyfikowane zagrożenia i szacowaniu prawdopodobieństw ich wystąpienia [11, 14, 15]. Podstawową wadą większości stosowanych obecnie metod oceny poziomu ryzyka jest nieuwzględnianie czynnika ludzkiego w procesie analizy ryzyka [1].

Istotność tej wady potwierdzają oficjalne statystyki prezentujące poziom zagrożeń dla systemów informatycznych wynikających z działać ludzkich. Statystyki publikowane przez CERT/CC, pokazane na wykresie (rys. 1) podają, że liczba odnotowanych unikalnych incydentów wzrosła z 252 w roku 1990 do 21 756 w roku 2000, 82 094 w roku 2002 i 137 529 w roku 2003. Incydent definiowany jest przy tym jako grupa niepożądanych zdarzeń posiadających wspólną przyczynę – może on zatem swoim zakresem obejmować zarówno jedną, jak i setki lokalizacji, i być zdarzeniem jednorazowym bądź długotrwałym procesem związanych z bezpieczeństwem funkcjonowania systemów informatycznych [4].



Rys. 1. Liczba incydentów zgłoszonych do CERT/CC w latach 1988–2003

Jeśli zatem w latach 90 XX w. zagrożenia wynikające z działań ludzkich były pomijalne, to ich gwałtowny wzrost na początku XXI wieku świadczy o konieczności ich uwzględnienia w ocenie poziomu bezpieczeństwa systemów informatycznych funkcjonujących w firmach. Próbą uzależnienia wynikowej wielkości ryzyka informatycznego od zachowań i predyspozycji ludzkich jest koncepcja metod opartych na rywalizacji (*Competitive Methods*).

Celem niniejszego artykułu jest prezentacja opracowanej przez autora metody oceny poziomu ryzyka związanego z systemami informatycznymi z perspektywy ludzkich zachowań, ich wiedzy i kompetencji.

2. Istniejące podejścia

Jednym z funkcjonujących obecnie podejść do analizy ryzyka, opartych na idei rywalizacji, jest metodyka Operations Security (OPSEC) opublikowana w USA w postaci dyrektywy National Security Decision Directive NSDD 298 z dnia 22 stycznia 1988 roku [5, 10].

Metodyka OPSEC definiuje pięcioetapowy proces prowadzący do oszacowania poziomu ryzyka, który według OPSEC przebiegać powinien według następującego schematu [3]:

1. identyfikacja informacji i zasobów mogących być potencjalnym celem stron atakujących,
2. analiza zagrożeń – identyfikacja stron atakujących, celów ich działań, intencji, wiedzy i możliwości,
3. analiza podatności – badanie czynników jakie mogą doprowadzić do przełamania zabezpieczeń systemu informatycznego poprzez wykorzystanie jego słabości,
4. szacowanie ryzyka – wycena efektów potencjalnego wykorzystania podatności systemu oraz przeprowadzenie analizy nakładów i wyników (*cost-benefit analysis*) możliwych działań zapobiegawczych i naprawczych,
5. identyfikacja i wdrożenie stosownych zabezpieczeń.

Bardziej sformalizowanym podejściem, opartym wyłącznie na rywalizacji jest model kalkulacji ryzyka opublikowany w 1993 roku przez Angelo Marcello [7]. W swoim podejściu Marcello rozważa następujące czynniki mające jego zdaniem wpływ na końcowe ryzyko systemów informatycznych:

- poziom wiedzy atakującego o atakowanym systemie,
- gotowość do podjęcia przez atakującego ryzykownych działań mających na celu przełamanie zabezpieczeń systemu,
- przewidywalność narzędzi wykorzystywanych przez stronę przeciwną.

Ostatecznie Marcello proponuje przedstawiony poniżej wzór pozwalający na wyznaczenie poziomu ryzyka dla systemu informatycznego zaproponowaną przez niego metodą [6]:

$$R = \theta^2 \psi \frac{1}{t^2} F \tag{1}$$

gdzie:

θ – poziom wiedzy atakującego o atakowanym systemie,

ψ – stosunek otwartości na ryzyko strony broniącej do otwartości na ryzyko strony atakującej,

t – poziom nieznajomości systemu przez atakującego,

F – poziom przekonania o sukcesie strony atakującej.

3. Metoda oceny konkurencyjności

Przedstawione podejście zaproponowane przez Marcello stanowi nowatorską próbę ilościowego wyrażenia poziomu ryzyka związanego z zachowaniami ludzkimi. Jednak zdaniem autora niniejszego opracowania, podejście Marcello jest niekompletne. Wprawdzie bierze ono pod uwagę poziom wiedzy atakującego o atakowanym systemie informatycznym, nie uwzględnia jednak na przykład takich czynników, jak kompetencje użytkowników i administratorów tego systemu. Dodatkowo, podejście to w zbyt uproszczony sposób opisuje wpływ zidentyfikowanych przez Marcello czynników bezpieczeństwa na ogólny poziom ryzyka związanego z danym systemem informatycznym.

W związku z wymienionymi brakami w podejściu Marcello, w niniejszym opracowaniu proponowane jest wprowadzenie nowego miernika określającego poziom zagrożeń dla systemu informatycznego wynikających z działań ludzkich.

Należy podkreślić, że podejście zaproponowane w niniejszym opracowaniu w żadnym stopniu nie odcina się od obserwacji i wniosków poczynionych przez Marcello. W obliczu jednak wspomnianych niedoskonałości tamtej metody, wprowadza nowe elementy analizy ryzyka systemów informatycznych wykorzystując jej ideę matematycznej prezentacji wielkości wpływu poszczególnych czynników na wielkość ryzyka systemu informatycznego związanego z czynnikiem ludzkim.

W podejściu przedstawionym w niniejszym opracowaniu, wielkość ryzyka systemu informatycznego związanego z czynnikiem ludzkim określana będzie pojęciem konkurencyjności systemu informatycznego, ponieważ wynika ono wprost z zainteresowania hakerów przełamaniem zabezpieczeń danego systemu. W związku z powyższym, konkurencyjnością systemu informatycznego nazywana będzie podatność systemu informatycznego na zagrożenia pochodzące od wszystkich zidentyfikowanych stron nieuprawnionych, a jej miarą będzie wskaźnik konkurencyjności systemu informatycznego. Wskaźnik konkurencyjności określony dla pewnego systemu informatycznego S_i oznaczany będzie jako κ_{S_i}.

W niniejszym opracowaniu proponuje się uwzględnienie przedstawionych dalej czynników wpływających zdaniem autora na wskaźnik konkurencyjności systemu informatycznego.

3.1. Stopień pewności strony nieuprawnionej o sukcesie ataku

Stopień pewności strony nieuprawnionej o sukcesie ataku na system informatyczny S_i (oznaczany dalej $\tau^j_{S_i}$) wyraża determinację atakującego w dążeniu do przełamania zabezpieczeń atakowanego systemu. O istotności tego czynnika świadczy fakt, iż pojawia się on już w podejściu Marcello. Jednak według Marcello jego wpływ na końcowy poziom ryzyka systemu informatycznego jest liniowy, co świadczy o proporcjonalności pomiędzy stopniem pewności strony nieuprawnionej o sukcesie ataku na system informatyczny a poziomem konkurencyjności tego systemu. W podejściu proponowanym w niniejszej pracy stopień pewności strony nieuprawnionej o sukcesie ataku wpływa wykładniczo na wskaźnik konkurencyjności atakowanego systemu informatycznego.

Tak silny wpływ tej wielkości wynika z uwzględnienia czynników psychologicznych. Jeżeli dla danej strony kompromitacja pewnego systemu informatycznego będzie sprawą priorytetową i prestiżową, to dołoży ona wszelkich starań, aby osiągnąć zamierzony rezultat.

W związku z powyższym, zdaniem autora, wpływ stopnia pewności strony nieuprawnionej o sukcesie ataku na wskaźnik konkurencyjności systemu informatycznego S_i będzie miał charakter wykładniczy:

$$\kappa_{S_i} \sim 2^{\tau_{S_i}^j} \tag{2}$$

Wykładnik $\tau_{S_i}^j$ w zależności (2) może przyjmować wartości ze zbioru $\tau_{S_i}^j \in \{0, 1, 2, 3\}$, przy czym:

0 – oznacza brak wiary strony atakującej j w sukces ataku,

3 – oznacza determinację i pełne przeświadczenie strony atakującej j o powodzeniu ataku.

3.2. Poziom wiedzy oraz kwalifikacji administratorów i użytkowników systemu

Czynnikiem, którego Marcello nie wziął pod uwagę w swoim podejściu, są kompetencje zarówno administratorów systemu, jak i jego indywidualnych użytkowników. Istotność tych czynników podkreślał już Mitnick [8], twierdząc, że nawet najlepsze zabezpieczenia nie są w stanie zapewnić bezpieczeństwa systemu informatycznego, jeżeli nie istnieje wystarczająca świadomość personelu mającego dostęp do tego systemu. Twierdzenie to adresują również prawidłowo skonstruowane polityki bezpieczeństwa informacji, które jednoznacznie powinny, zgodnie z wytycznymi standardu brytyjskiego BS 7799 [2, 9, 13], definiować konieczność wprowadzenia właściwego poziomu świadomości bezpieczeństwa w organizacji. Świadomość bezpieczeństwa jest również jednym z kluczowych czynników analizowanych podczas audytów bezpieczeństwa oraz podczas audytów certyfikacyjnych ISO 17799 [12].

Widać zatem, że odpowiednio wysoki poziom kompetencji administratorów i użytkowników systemu może istotnie zwiększyć bezpieczeństwo systemu, zmniejszając automatycznie jego wskaźnik konkurencyjności. Z drugiej strony niski poziom wiedzy o systemie wśród administratorów i niski poziom świadomości informatycznej oraz świadomości bezpieczeństwa wśród użytkowników mogą drastycznie zmniejszyć poziom bezpieczeństwa systemu, czego odzwierciedleniem będzie wzrost poziomu wskaźnika konkurencyjności dla danego systemu informatycznego.

Na potrzeby wyrażenia wpływu kompetencji personelu firmy na wskaźnik konkurencyjności systemu przyjmijmy następujące oznaczenia:

$k_{S_i}^a$ – poziom wiedzy i kwalifikacji administratorów systemu informatycznego S_i,

$k_{S_i}^u$ – poziom wiedzy i kwalifikacji użytkowników danego systemu informatycznego S_i.

W celu oszacowania wielkości wpływu kompetencji personelu firmy na wskaźnik konkurencyjności systemu, a jednocześnie uwzględnienia faktu, że wskaźniki poziomu wiedzy i kwalifikacji administratorów oraz użytkowników mogą zarówno zwiększać, jak i obniżać wskaźnik konkurencyjności systemu, proponuje się wykładniczy charakter wpływu tych składowych na wskaźnik konkurencyjności postaci:

$$\kappa_{S_i} \sim 3^{(2-k^a_{S_i}-k^u_{S_i})} \tag{3}$$

Dla tak określonego wpływu kompetencji na wskaźnik konkurencyjności proponuje się następujące zbiory dopuszczalnych wartości dla poszczególnych współczynników:

- poziom wiedzy i kwalifikacji administratorów $k^a_{S_i} \in \{0, 1, 2, 3\}$, gdzie 0 oznacza brak kompetencji, a 3 określa profesjonalizm administratorów systemu S_i,
- poziom wiedzy i kwalifikacji użytkowników $k^u_{S_i} \in \{0, 1, 2\}$, gdzie 0 oznacza brak kompetencji, a 2 określa profesjonalizm użytkowników systemu S_i.

Przedstawiony dobór zbiorów wartości dla $k^a_{S_i}$ i $k^u_{S_i}$, a w szczególności brak wartości 3 w zbiorze wartości dla $k^u_{S_i}$, wynika z faktu, że kompetentni administratorzy systemu mają znacznie większy wpływ na zwiększenie bezpieczeństwa systemu informatycznego niż kompetentni użytkownicy tego systemu. Z kolei niekompetentni użytkownicy praktycznie w równym stopniu mogą obniżyć poziom bezpieczeństwa systemu, co niekompetentni administratorzy, stąd w obydwu zbiorach wartości 0 oznaczają niekompetencję kadry.

Jednocześnie zwrócić należy uwagę na postać proporcjonalności zawartej we wzorze (3). Zapewnia ona, że niskie kompetencje administratorów i użytkowników będą istotnie zwiększały wartość wskaźnika konkurencyjności systemu informatycznego, a wysokie będą zmniejszały jego wartość.

3.3. Poziom wiedzy strony nieuprawnionej o systemie

Poziom wiedzy strony nieuprawnionej o systemie (oznaczany dalej $q^j_{S_i}$) określa jak dogłębną i szczegółową wiedzą o atakowanym systemie (S_i) dysponuje atakujący. Istotność tej składowej w stosunku do pozostałych podkreśla wzór:

$$\kappa_{S_i} \sim q^{j^2}_{S_i} \tag{4}$$

Wskaźnik poziomu wiedzy strony nieuprawnionej o systemie został bezpośrednio zaczerpnięty z metody Marcello. Również charakter jej wpływu na wskaźnik konkurencyjności systemu informatycznego pochodzi z podejścia przedstawionego przez Marcello.

W proponowanym modelu, współczynnik $q^j_{S_i}$ może przyjmować wartości ze zbioru $\{1, 2, 3, 4, 5\}$, przy czym:

1 – oznacza szczątkową wiedzę strony nieuprawnionej j o atakowanym systemie informatycznym,

5 – oznacza wiedzę ekspercką strony nieuprawnionej j o atakowanym systemie informatycznym.

3.4. Poziom niewiedzy strony nieuprawnionej o zabezpieczeniach systemu

Poziom niewiedzy strony nieuprawnionej o zabezpieczeniach systemu informatycznego S_i (oznaczany dalej $\hat{q}^j_{S_i}$) jest miarą pewności organizacji, że atakujący nie zdaje sobie sprawy z istnienia pewnych zabezpieczeń atakowanego systemu.

Wpływ poziomu niewiedzy strony nieuprawnionej $\hat{q}^j_{S_i}$ na wskaźnik konkurencyjności jest odwrotnie proporcjonalny do jego wartości:

$$\kappa_{S_i} \sim \frac{1}{\hat{q}^j_{S_i}} \tag{5}$$

Wielkość wpływu poziomu niewiedzy strony nieuprawnionej na wskaźnik konkurencyjności jest kolejną różnicą prezentowanego tutaj podejścia do modelu Marcello, gdzie wielkość poziomu niewiedzy strony nieuprawnionej wpływa na wskaźnik konkurencyjności odwrotnie proporcjonalnie kwadratem swojej wartości. O ile przyjęcie ukwadratowionego wpływu poziomu wiedzy strony nieuprawnionej o systemie na wskaźnik konkurencyjności jest jak najbardziej zrozumiałe, gdyż wiedza ta daje atakującemu przewagę i istotnie ułatwia kompromitację systemu, o tyle poziom niewiedzy strony nieuprawnionej o jego zabezpieczeniach, który dodatkowo wyraża jedynie przeświadczenie organizacji o niewiedzy atakującego, a nie jest jej bezpośrednio weryfikowalnym miernikiem, zdaniem autora, nie ma aż tak wielkiego przełożenia na bezpieczeństwo systemu, żeby należało go ukwadratawiać.

W niniejszym opracowaniu modelu współczynnik $\hat{q}^j_{S_i}$ może przyjmować wartości $\{1, 2, 3, 4, 5\}$, przy czym:

1 – oznacza pełną wiedzę strony nieuprawnionej j o wszelkich zastosowanych zabezpieczeniach atakowanego systemu informatycznego,

5 – oznacza całkowity brak wiedzy strony nieuprawnionej j o zastosowanych zabezpieczeniach atakowanego systemu informatycznego.

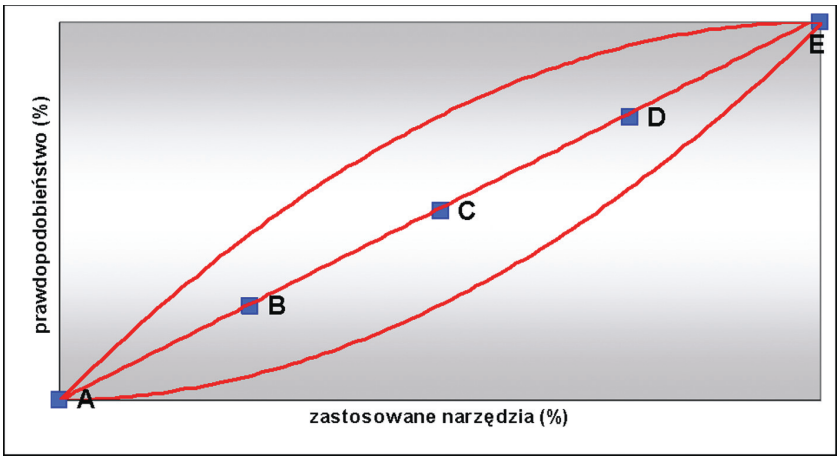
3.5. Skłonność strony nieuprawnionej do ryzyka podczas ataku na system

Skłonność strony nieuprawnionej do ryzyka podczas ataku na system określa jej poziom akceptacji ryzyka przy wyborze metod i narzędzi wykorzystywanych do ataku na dany system informatyczny.

Aby właściwie zinterpretować tę składową, rozważmy rodzinę krzywych (oznaczaną dalej $\hat{\Psi}$) zależności prawdopodobieństwa wykrycia ataku od narzędzi zastosowanych przez atakującego, rozumianych zarówno jako typy ataków, jak również jako stosowne oprogramowanie i technologia. Poglądowe krzywe z rodziny $\hat{\Psi}$ prezentuje wykres (rys. 2).

Z rysunku 2 wynika, że użycie większej ilości lub bardziej wyrafinowanych technik ataków, co zwiększa szanse na powodzenie ataku na system, wiąże się ze wzrostem prawdopodobieństwa wykrycia strony atakującej.

Kształt konkretnej krzywej z przedstawionej na rysunku 2 rodziny krzywych $\hat{\Psi}$ jest różny dla różnych konfiguracji „system – atakujący", gdyż zależy zarówno od zabezpieczeń systemu, jak i od wiedzy atakującego.



Rys. 2. Rodzina krzywych zależności prawdopodobieństwa wykrycia ataku od zastosowanych narzędzi

Dla uproszenia modelu i dalszych rozważań, zdaniem autora można przyjąć, że zależność prawdopodobieństwa wykrycia ataku od zastosowanych narzędzi jest liniowa. Również wpływ czynnika związanego ze skłonnością danej strony nieuprawnionej do ryzyka podczas ataku na system informacyjny S_i (oznaczanego dalej $r^j_{S_i}$) na wskaźnik konkurencyjności systemu ma, zdaniem autora, charakter liniowy:

$$\kappa_{S_i} \sim r^j_{S_i} \tag{6}$$

Dla uproszczenia modelu uznaje się, że współczynnik $r^j_{S_i}$ może przyjmować wartości z przedziału $\{1, 2, 3, 4, 5\}$, przy czym:

1 – oznacza pełną awersję strony atakującej j do ryzyka względem systemu informatycznego S_i,

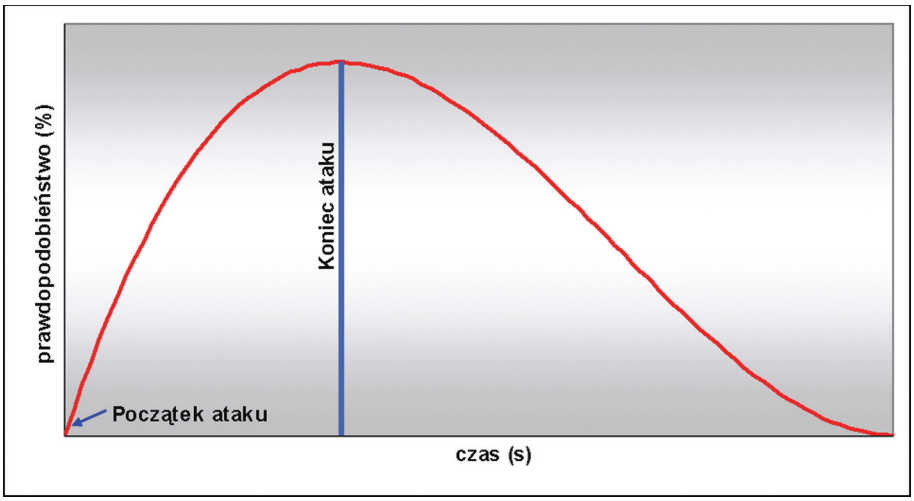
5 – oznacza pełną otwartość strony atakującej j na ryzyko względem systemu informatycznego S_i.

Wartości te w przybliżeniu odpowiadają kolejno punktom A, B, C, D i E na rysunku 2.

3.6. Awersja organizacji do ryzyka względem systemu

Awersja organizacji do ryzyka względem systemu informatycznego S_i (oznaczana dalej $\hat{r}_{S_i}$) precyzuje, jaką wagę przywiązuje organizacja do bezpieczeństwa danego systemu informatycznego. Może ona wynikać zarówno z poufności danych przechowywanych i przetwarzanych przez ten system, jak i jego istotności z perspektywy funkcjonowania organizacji oraz poziomu świadomości kadry zarządzającej.

Aby przedstawić ten czynnik, należy rozważyć, jak zmienia się prawdopodobieństwo wykrycia ataku na system w czasie. Rozkład ten prezentuje krzywa na rysunku 3.



Rys. 3. Krzywa zależności prawdopodobieństwa wykrycia ataku od czasu

Z rysunku 3 wynika, że po upływie dostatecznie długiego czasu wartość prawdopodobieństwa wykrycia zaistniałego nadużycia w systemie informatycznym zmierza do zera. Wynikać to może na przykład z faktu, że rejestry zdarzeń zostaną nadpisane, czy też zdarzenie nie zostało w porę wykryte, a logi systemowe starsze niż pewien standardowo przyjęty w danej organizacji okres czasu nie będą już podlegały analizie.

Przejawem awersji organizacji do ryzyka względem systemu informatycznego jest niedopuszczenie do sytuacji, w których następuje obniżenie poziomu bezpieczeństwa, a w szczególności wzrasta szansa atakującego na niewykrycie jego działań. Sytuacjami takimi mogą być na przykład niedobór administratorów, brak logowania zdarzeń w systemie lub brak osób odpowiedzialnych za przeglądanie i analizę logów systemowych czy też pozostawienie domyślnych parametrów bezpieczeństwa w systemie.

Zatem im większa wartość awersji organizacji do ryzyka względem danego systemu informatycznego, tym system ten jest lepiej zabezpieczony, a zatem wskaźnik konkurencyjności dla tego systemu jest odwrotnie proporcjonalny do wartości składowej awersji organizacji do ryzyka:

$$\kappa_{S_i} \sim \frac{1}{\hat{r}_{S_i}} \tag{7}$$

W modelu proponowanym w niniejszym opracowaniu współczynnik $\hat{r}_{S_i}$ może przyjmować wartości z przedziału $\{1, 2, 3, 4, 5\}$, gdzie:

1 – oznacza pełną otwartość organizacji na ryzyko względem danego systemu informatycznego S_i,

5 – oznacza pełną awersję organizacji do ryzyka względem danego systemu informatycznego S_i.

3.7. Udział zagrożeń pochodzących od strony nieuprawnionej

Ostatnim elementem, który należy uwzględnić przy ocenie ryzyka systemu informatycznego związanego z zachowaniami ludzkimi, jest fakt, iż system informatyczny jest celem nie jednej, lecz wielu stron nieuprawnionych. Dodatkowo każda ze stron ma różną motywację, wiedzę, kwalifikacje, doświadczenie i inne czynniki, które wprowadzają konieczność rozróżnienia poszczególnych atakujących oraz oszacowania i przypisania im wielkości potencjalnego wpływu na bezpieczeństwo danego systemu informatycznego.

Dla wszystkich zidentyfikowanych stron nieuprawnionych w odniesieniu do danego systemu informatycznego należy określić wielkość udziału zagrożeń pochodzących od danej strony nieuprawnionej wśród wszystkich zagrożeń pochodzących od wszystkich zidentyfikowanych stron nieuprawnionych. Wielkość ta w modelu przedstawionym w niniejszym opracowaniu oznaczana będzie jako υ_j, gdzie j jest numerem kolejnej zidentyfikowanej strony nieuprawnionej.

Przy tak określonym parametrze υ_j, dla każdego systemu informatycznego (w szczególności systemu S_i) musi zachodzić równość:

$$\sum_{j=1}^{J} \upsilon_{S_i}^{j} = 1 \tag{8}$$

gdzie J – jest ilością zidentyfikowanych stron nieuprawnionych w stosunku do systemów informatycznych danej organizacji.

4. Wskaźnik konkurencyjności

Ostatecznie, na podstawie przedstawionych powyżej elementów składowych, wskaźnikiem konkurencyjności dowolnego systemu informatycznego S_i jest suma:

$$\kappa_{S_i} = \sum_{j=1}^{J} \left(2^{\tau_{S_i}^{j}} \cdot 3^{(2-k_{S_i}^{a}-k_{S_i}^{u})} \cdot \frac{(q_{S_i}^{j})^2}{\hat{q}_{S_i}^{j}} \cdot r_{S_i}^{j} \cdot \frac{1}{\hat{r}_{S_i}} \cdot \upsilon_{S_i}^{j} \right) \tag{9}$$

gdzie:

$\tau_{S_i}^{j}$ – stopień pewności strony nieuprawnionej j o sukcesie ataku na system S_i,

$k_{S_i}^{a}$ – poziom wiedzy i kwalifikacji administratorów systemu S_i,

$k_{S_i}^{u}$ – poziom wiedzy i kwalifikacji użytkowników systemu S_i,

$q_{S_i}^{j}$ – poziom wiedzy strony nieuprawnionej j o systemie S_i,

$\hat{q}_{S_i}^{j}$ – poziom niewiedzy strony nieuprawnionej j o zabezpieczeniach systemu S_i,

$r_{S_i}^{j}$ – skłonność strony nieuprawnionej j do ryzyka podczas ataku na system S_i,

$\hat{r}_{S_i}$ – awersja organizacji do ryzyka względem systemu S_i,

$\upsilon^j_{S_i}$ – udział zagrożeń dla systemu informatycznego S_i pochodzących od strony nieuprawnionej j wśród wszystkich zagrożeń pochodzących od zidentyfikowanych stron nieuprawnionych.

Tak określony wskaźnik dla systemu informatycznego S_i pozwala na wyznaczenie szacowanego poziomu zagrożeń wynikających z działań osób trzecich mających na celu przełamanie zabezpieczeń tego systemu. Jednocześnie uwzględnia on wszystkie czynniki, które, zdaniem autora niniejszego opracowania, mają istotny wpływ na ryzyko systemu informatycznego rozpatrywane z perspektywy zachowań ludzkich.

5. Wnioski

Należy zaznaczyć, że metody oparte na rywalizacji, pomimo iż stanowią pewną alternatywę dla metod bazujących na kalkulacji prawdopodobieństw, nie odrzucają całkowicie koncepcji szacowania prawdopodobieństw wystąpienia zdarzeń wpływających na ryzyko systemów informatycznych.

Każda z metod szacowania ryzyka, włączając w to również metody oparte na rywalizacji, bazując na tak trudno mierzalnych czynnikach jak awersja do ryzyka, motywacja, dostępne narzędzia, wiedza czy doświadczenie zaangażowanych stron, wymaga na pewnym etapie dokonania, na podstawie doświadczenia i przyjętych kryteriów, kwantyfikacji i oceny wpływu tych czynników na ostateczne ryzyko systemu informatycznego. Dlatego przedstawiona w niniejszym opracowaniu koncepcja oceny ryzyka systemu informatycznego opierająca się na ocenie zagrożeń wynikających z działań ludzkich nie stanowi alternatywy dla metod opartych o szacowanie wielkości strat i ich prawdopodobieństwa, lecz może być ich skutecznym dopełnieniem.

Literatura

[1] Baskerville R.: *Information Systems Security Design Methods: Implications for Information Systems Development*. Computing Surveys 25 (4), grudzień 1994

[2] British Standard BS 7799–1:1999: *Information security management – Part 1: Code of practice for information security management*. Londyn BSI, 1999

[3] Cameron D.: *Information Control in the Information Age*. 3rd ed. OPSEC Journal, Frederick MD 1996

[4] `http://www.cert.org/stats/cert_stats.html`

[5] Jelen G. F.: *The Nature of OPSEC*. 1st ed. OPSEC Journal, Frederick MD 1993

[6] Manunta G.: *Security and Methodology*. Swindon, The Royal Military College of Science, Cranfield Security Centre Cranfield University 2000

[7] Marcello A.: *La Moderna Gestione Dei Rischi A ziendali*. Milan, Masson 1993

[8] Mitnick K., Simon W. L.: *Sztuka podstępu*. Warszawa, Wydawnictwo Helion 2003

[9] Mukund B.: *BS 7799 (ISO 17799) – Information Security Management System*. Express Computer – 6th May 2002, Indie

[10] *9. National Operations Security Program*. National Security Decision Directive 298, USA, 1988

[11] Parker D. B.: *Computer Security Management*. Reston, Reston Publishing Company 1981

[12] PN-ISO/IEC 17799:2003: *Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji*

[13] Restell P.: *BS 7799: How it works*. Quality World, luty 2002

[14] Stoneburner G., Goguen A., Feringa A.: *Risk Management Guide for Information Technology Systems – Recommendations of the National Institute of Standards and Technology*. National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, Special Publication 800–30

[15] U.S. Department of Commerce, National Bureau of Standards: *Federal Information Processing Standards Publication 65: Guideline For Automatic Data Processing Risk Analysis*. 1 sierpnia 1979