Nr 4 (170) 2013

WYKORZYSTANIE ANALIZY RYZYKA ORAZ SCENARIUSZY PRZEBIEGU INCYDENTÓW W SYSTEMIE ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI GROMADZONEJ, PRZETWARZANEJ I PRZESYŁANEJ W SYSTEMACH TELEINFORMATYCZNYCH INSTYTUCJI

Artur SZLESZYŃSKI[*], Marek WITKOWSKI[**]

[*] *Wydział Zarządzania, Wyższa Szkoła Oficerska Wojsk Lądowych*
e-mail: a.szleszynski@wso.wroc.pl
[**] *Instytut Dowodzenia, Wyższa Szkoła Oficerska Wojsk Lądowych*
e-mail: m.witkowski@wso.wroc.pl

Artykuł wpłynął do redakcji 29.05.2013 r., Zweryfikowaną i poprawioną wersję po recenzjach i korekcie otrzymano w listopadzie 2013 r.

W pracy przedstawiono wykorzystanie analizy ryzyka oraz scenariuszy przebiegu incydentów w systemie teleinformatycznym do oceny wpływu incydentów na bezpieczeństwo gromadzonej i przetwarzanej w systemie informacji. Dokonano przeglądu literatury przedmiotu, a następnie zaprezentowano związki pomiędzy analizą ryzyka a scenariuszami. Scenariusz w sposób opisowy ma pokazać, jakie mogą być skutki incydentów dla bezpieczeństwa systemu teleinformatycznego oraz dla znajdującej się w nim informacji. Przedstawiono wyniki badań dotyczące znajomości zagadnień związanych z analizą ryzyka. Wykonanie analizy ryzyka jest wymaganiem ustawowym.

Słowa kluczowe: *bezpieczeństwo informacji, analiza ryzyka, scenariusze przebiegu incydentów systemy teleinformatyczne*

WSTĘP

We współczesnej organizacji[1] zasoby informacyjne są tak samo ważne, jak posiadane zasoby finansowe, ludzkie czy materialne. Wkład informacji w koszcie wytwarzania produktu lub usługi rośnie od 5% w XIX wieku do 60% w XXI wieku [9]. Nie chronienie zasobu tak cennego i mającego znaczny wpływ na koszt wyrobu lub usługi jest nieracjonalne. Gdyby zapytać kadrę zarządzającą przedsiębiorstwem o motywację do ochrony zasobów informacyjnych, większość pytanych wskazałaby ustawę o ochronie danych osobowych jako podstawowy czynnik wymuszający podjęcie przedstawionych działań. Nie wiadomo, czy groźba sankcji, jaką może być pozbawienie wolności

[1] Przez pojęcie organizacji rozumie się przedsiębiorstwo komercyjne, instytucje rządowe i samorządowe oraz organizacje pożytku publicznego.

lub kara finansowa, jest większym czynnikiem motywującym do ochrony zasobów informacyjnych [14].

Abstrahując od kwestii motywacji do ochrony zasobów informacyjnych, należy odnieść się do kwestii związanych z systemem ochrony informacji wewnątrz organizacji. Przyjęte w tytule artykułu ograniczenie do zasobów, które są gromadzone i przetwarzane w systemach teleinformatycznych wynika z rozpowszechnienia środków elektronicznej obróbki informacji wykorzystywanych w organizacjach.

Środki te umożliwiają obróbkę dużych zbiorów danych[2] oraz wygodną, dla odbiorcy, prezentację wyników obróbki. Wygoda odbiorcy, oprócz walorów estetycznych wynikających z graficznej formy prezentacji wyników przetwarzania, posiada również wymiar utylitarny. Oznacza on, że użytkownik przetworzonych informacji właściwie ocenia sytuację oraz podejmuje adekwatne decyzje.

Dąży się zatem do zmniejszenia wartości entropii informacji do zera, co jednocześnie ogranicza niepewność decyzyjną. Należy ją rozumieć jako ryzyko związane z możliwością wystąpienia niewłaściwie podjętej decyzji oraz jej konsekwencjami. Oba warunki można wyrazić przy pomocy wzorów (1) i (2).

$$H(x) = -\sum_{i=1}^{n} x_i \cdot lgx_i \rightarrow 0, \tag{1}$$

gdzie:

H(x) – entropia informacji,

x_i – prawdopodobieństwo wystąpienia informacji i-tej,

$$Z(i) \rightarrow Z_{min}, \tag{2}$$

gdzie:

Z(i) – niepewność decyzyjna związana z wykorzystaniem informacji i-tej,

Zmin – akceptowana niepewność lub minimalne ryzyko decyzyjne związane z wykorzystaniem informacji i-tej.

Mówiąc o bezpieczeństwie informacji, znajdującej się w systemie teleinformatycznym, należy uściślić pojęcie bezpieczeństwa informacji. Definicja, którą można znaleźć w literaturze przedmiotu stwierdza, że bezpieczeństwo *„jest to brak poczucia obecności zagrożenia”* [2]. Przedstawiona definicja jest filozoficzna i odnosi się do stanu psychicznego osoby, która odczuwa lub nie obecność zagrożeń dla swojej egzystencji. Próba zbudowania systemu chroniącego bezpieczeństwo informacji na podstawie subiektywnego kryterium, takiego jak brak obecności zagrożeń, jest nie możliwa. Dlatego bezpieczeństwo informacji będzie rozumiane jako *„zachowanie atrybutów bezpieczeństwa informacji, takich jak: poufność, integralność i dostępność”* [5]. Rozwinięte definicje poszczególnych atrybutów zawarte są w normie PN ISO/IEC-17799:2007, dlatego znaczenie atrybutów nie będzie wyjaśniane.

Konieczność ochrony zasobów informacyjnych organizacji jest wymaganiem zawartym w aktach prawnych takich jak np.: ustawa o ochronie danych osobowych czy

[2] Pod pojęciem dużego zbioru danych rozumie się pliki o rozmiarze od dziesiątek MB do TB. W przypadku baz danych są bazy zawierające powyżej 10000 rekordów.

ustawa o ochronie informacji niejawnych [15]. Wymienione ustawy nie są jedynymi aktami prawnymi regulującymi kwestie ochrony zasobów informacyjnych[3], jakie występują w polskim systemie prawnym. Nieprzestrzeganie przez organizację zapisów ustaw wiąże się z sankcjami karnymi w postaci grzywny lub kary pozbawienia wolności [14]. Z zaniechaniem ochrony zasobów informacyjnych związane są konsekwencje niematerialne, takie jak utrata pozytywnego wizerunku czy odejście grupy klientów danej organizacji. Niematerialność związana jest z brakiem możliwości dokładnego określenia rozmiaru strat. Do ich określenia można posłużyć się jedynie szacunkami wykorzystującymi dane historyczne, które dotyczą podobnych przypadków.

Ochrona zasobów informacyjnych organizacji motywowana tylko konsekwencjami karnymi, które mogą zostać nałożone na podmiot przetwarzający dane – nie jest wystarczająco silnym argumentem. Silniejszym argumentem, przemawiającym za ochroną zasobów informacyjnych jest konieczność ich wykorzystania w działalności bieżącej organizacji. Jeżeli bez posiadanych zasobów informacyjnych dana organizacja jest w stanie funkcjonować bez zakłóceń, to oznacza to, że zasoby informacyjne nie były jej potrzebne. Jeżeli z brakiem zasobów informacyjnych związane są problemy w funkcjonowaniu organizacji lub jest ono niemożliwe, wówczas ochrona zasobów informacyjnych jest zadaniem o wysokim priorytecie.

Celem artykułu jest zaprezentowanie roli analizy ryzyka oraz scenariuszy przebiegu incydentów w bezpieczeństwie funkcjonowania systemu teleinformatycznego w procesie tworzenia lub utrzymania wewnętrznego systemu ochrony zasobów informacyjnych. Oba przedsięwzięcia powinny być realizowane w ramach wewnętrznego systemu ochrony zasobów informacyjnych. Jednakże czynności te nie są wykonywane poprawnie, dzieje się tak, ponieważ wymagają one opracowania dokumentów. Z dokumentami tymi powinny się zapoznać osoby odpowiedzialne za zasoby informacyjne. Dokumentacja ta będzie okresowo aktualizowana, co wynika ze zmiany zagrożeń pojawiających się dla zasobów informacyjnych. Zmiany te będą spowodowane wdrożeniem zabezpieczeń, które będą eliminować lub zmniejszać potencjalne negatywne skutki wystąpienia zagrożeń [1]. Dokumenty te opracowuje się w celu wskazania oczekiwanych działań w stosunku do komórek organizacyjnych instytucji, które są odpowiedzialne za ochronę zasobów informacyjnych.

1. WEWNĘTRZNY SYSTEM OCHRONY ZASOBÓW INFORMACYJNYCH INSTYTUCJI

Wymienione we wstępie akty prawne nie mówią, jak należy zorganizować wewnętrzny system ochrony zasobów informacyjnych. Wskazują czynności początkowe, jakie należy wykonać w trakcie organizacji systemu ochrony informacji. W rozporządzeniu Ministra Spraw Wewnętrznych i Administracji do ustawy o ochronie danych osobowych mówi się o poziomach ochrony, jakie muszą posiadać systemy teleinformatyczne przetwarzające dane osobowe [12,14]. Odwołanie się do systemów teleinformatycznych oznacza, że ustawodawca dostrzega kluczową rolę środków informatycznych w działalności organizacji. Obecnie prawie każda instytucja wykorzystuje narzędzia informatyczne do prowadzenia własnej działalności.

[3] W polskim systemie prawnym obowiązują 64 akty prawne dotyczące ochrony zasobów informacyjnych. Do grupy chronionych zasobów informacyjnych należą: informacje dotyczące stanu zdrowia, operacji bankowych, umów handlowych itp.

Informacje, których nie znajdzie się w aktach prawnych, dotyczą kwestii organizacji wewnątrz instytucji systemu ochrony zasobów informacyjnych gromadzonych i przetwarzanych w systemach teleinformatycznych. Zalecenia dotyczące sposobu organizacji wewnętrznego systemu ochrony zasobów informacyjnych znajdują się w normach oraz w literaturze przedmiotu.

Przy organizowaniu wewnętrznego systemu ochrony zasobów informacyjnych, zaleca się powołanie zespołu, który określany jest jako System Zarządzania Bezpieczeństwem Informacji [10]. W skład systemu powinni wejść wszyscy przedstawiciele komórek organizacyjnych instytucji [2]. W zespole powinien znaleźć się przedstawiciel zarządu lub dyrekcji instytucji posiadający odpowiednie uprawnienia do wydawania poleceń i egzekwowania ich wykonania. Obecność osoby z zarządu jest niezbędna, gdyż będzie ona podejmować decyzje, nakazujące wykonanie prac przez różne komórki wewnątrz instytucji. Decyzje te będą się wiązać z koniecznością przydzielenia środków finansowych niezbędnych do ich wykonania. Osoba posiadająca uprawnienia do podejmowania decyzji finansowych jest niezbędna do zapewnienia właściwego funkcjonowania systemu zarządzania bezpieczeństwem informacji w instytucji.

2. ANALIZA RYZYKA W PROCESIE TWORZENIA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI W INSTYTUCJI

Pracując nad zbiorem informacji, które z punktu widzenia działalności bieżącej instytucji posiadają największą istotność, należy je wstępnie zidentyfikować, a następnie ocenić ich wartość. Ocena wartości zasobów informacyjnych będzie wynikała z możliwych strat, jakie mogą powstać, kiedy zasób informacyjny nie będzie dostępny. W tym celu przeprowadza się analizę ryzyka dla bezpieczeństwa informacji gromadzonych i przetwarzanych w systemie teleinformatycznym instytucji. Należy zwrócić uwagę, że ryzyko nie jest tylko możliwością wystąpienia zdarzenia negatywnego, ale oznacza ono możliwość wystąpienia zdarzenia negatywnego oraz jego konsekwencje dla funkcjonowania instytucji [2,10,16]. Zatem jest ono wyrażane przy pomocy zależności (3).

$$r_i = m_{wst} \cdot k_{wst}, \tag{3}$$

gdzie:

ri – ryzyko dla i-tego zasobu informacyjnego,

mwst – możliwość wystąpienia zdarzenia negatywnego dla i-tego zasobu informacyjnego,

kwst – konsekwencje wystąpienia zdarzenia negatywnego dla i-tego zasobu informacyjnego.

Możliwość wystąpienia zdarzenia negatywnego oraz jego konsekwencje można oszacować na podstawie danych historycznych, pochodzących z innych systemów lub systemu ocenianego. Należy pamiętać, że wdrożenie zabezpieczeń zmienia stan rozwiązania, co sprawia, że dane historyczne mają wartość szacunkową, a nie dokładną wartość liczbową [1,17]. Wykonując analizę ryzyka, należy uwzględnić fakt, że możliwość wystąpienia zdarzenia negatywnego oraz jego konsekwencje są wartościami zmiennymi. Są one subiektywnie szacowane przez wykonawcę lub wykonawców analiz na potrzeby danej oceny. Korektę przyjętych wartości przeprowadza się na podstawie obserwacji systemu lub audytu.

Dlaczego należy przeprowadzić analizę ryzyka? Odpowiedź na powyższe pytanie wynika z:

- konieczności określenia zasobów informacyjnych o dużej wrażliwości[4] dla instytucji. Nie jest możliwa ochrona wszystkich zasobów informacyjnych;
- ustalenia granic systemu, który zostanie objęty ochroną w ramach wewnętrznego systemu ochrony informacji;
- ekonomicznego uzasadnienia konieczności ochrony wybranego zbioru zasobów informacyjnych;
- oszacowania czynności oraz czasu potrzebnego do wdrożenia zabezpieczeń;
- przygotowania zbioru kryteriów oceny skutków wdrożonych środków zabezpieczeń.

Z przedstawionego wcześniej zestawienia wynika konieczność zaangażowania pracowników oraz środków materiałowych i finansowych do ochrony wrażliwych zasobów informacyjnych.

Na podstawie badań przeprowadzonych przez autorów wynika, że w instytucjach odpowiedzialność za kwestie związane z ochroną zasobów informacyjnych, znajdujących się w systemach teleinformatycznych, przenosi się na komórki informatyki znajdujące się w strukturze instytucji. W ankiecie badawczej zadano pytania, grupie 41 respondentów, dotyczące analizy ryzyka. Uczestników badania podzielono na dwie grupy 20 osobowe i 21 osobowe.

Pierwszą grupę – stanowiły osoby niezwiązane zawodowo z komórkami informatyki i telekomunikacji w instytucji. Do drugiej grupy zakwalifikowano pracowników komórek informatyki i telekomunikacji, występujących w strukturze organizacji. Obie grupy ankietowanych pracowników, przeszły szkolenie z zakresu ochrony zasobów informacyjnych. Ponieważ analiza ryzyka stanowi jeden z pierwszych elementów systemu ochrony zasobów informacyjnych, w pierwszym pytaniu zapytano o to, czym zajmuje się analiza ryzyka. Badani mieli możliwość wybrania spośród czterech odpowiedzi oznaczonych literami *A, B, C* lub *D*.

W wyniku przeprowadzenia analizy odpowiedzi udzielonych przez respondentów, uzyskano następujące wyniki przedstawione w tabeli 1.

Tabela 1. Rozkład odpowiedzi udzielonych na pytanie 1

Odpowiedź	**A**	**B**	**C**	**D**
Grupa 1	9	0	0	11
Grupa 2	5	1	0	15
Razem	14	1	0	26

Źródło: Opracowanie własne

[4] Wrażliwość zasobu informacyjnego oznacza jego znaczenie dla niezakłóconego funkcjonowania instytucji.

Poprawną odpowiedzią była odpowiedź *D*, która stwierdzała, że „*analiza ryzyka zajmuje się identyfikacją zagrożeń dla zasobów informacyjnych oraz oceną skutków ich wystąpienia”*. 63% ankietowanych wybrało odpowiedź *D* jako poprawną definicję pojęcia analiza ryzyka. Pozostałe odpowiedzi zawierały cząstkowy opis funkcji analizy ryzyka i zostały wybrane przez 37% ankietowanych. Wśród odpowiedzi zawierających niekompletne definicje analizy ryzyka najczęściej wybierana była odpowiedź *A* (34% ankietowanych) i odpowiedź *B* (3% ankietowanych).

Najczęściej wybieraną przez respondentów opcją była odpowiedź *D*, najrzadziej odpowiedź *B*. Jeżeli uwzględni się odpowiedzi udzielone w pytaniu nr 2, wówczas liczba poprawnych odpowiedzi powinna być zaskoczeniem.

W pytaniu nr 2 ankietowani zostali zapytani o to, czy w trakcie szkoleń z zakresu ochrony informacji byli zapoznawani z zasadami procesu analizy ryzyka. Respondenci wybierali jedną odpowiedź z czterech dostępnych. Odpowiedzi *A, B* i *C* potwierdzały, że respondent był zapoznany z zasadami przeprowadzania analizy ryzyka, jednak zakres przekazywanej wiedzy był różny. W odpowiedzi *A* przekazana wiedza była ogólna, w odpowiedzi *B* przekazana wiedza była szczegółowa, odpowiedź *C* oznaczała, że szkolony nie zrozumiał, w jakim celu oraz jak przeprowadza się analizę ryzyka dla zasobów informacyjnych. Odpowiedź *D* oznaczała brak szkolenia dotyczącego analizy ryzyka. Rozkład udzielonych odpowiedzi przedstawia tabela 2.

Tabela 2. Rozkład odpowiedzi udzielonych na pytanie nr 2

Odpowiedź	**A**	**B**	**C**	**D**
Grupa 1	4	2	0	14
Grupa 2	10	1	0	10
Razem	14	3	0	24

Źródło: Opracowanie własne

Jeżeli ankietowani udzielili najwięcej poprawnych odpowiedzi dotyczących istoty analizy ryzyka, a nie byli szkoleni lub szkolenie (w ich odczuciu) było bardzo ogólne, to można przypuszczać, że przedstawiona definicja analizy ryzyka z pytania nr 1 była zgodna z intuicyjnym pojmowaniem analizy ryzyka przez respondentów.

Wyniki odpowiedzi na pytania nr 1 i 2 świadczą, iż respondenci domyślają się, co jest celem analizy ryzyka, ale brakuje im wiedzy, która mogłaby to intuicyjne rozumienie potwierdzić, dodatkowo wyjaśniając czym jest analiza ryzyka i jaki jest jej wpływ na bezpieczeństwo informacji gromadzonych, przetwarzanych i przesyłanych w systemie teleinformatycznym.

Interesująco wygląda kwestia związku pomiędzy odpowiedziami udzielanymi przez ankietowanych w pytaniach nr 1 i 2. Wyniki przedstawiono w tabeli 3.

Tabela 3. Związek pomiędzy liczbą wybranych odpowiedzi A,B,C lub D udzielonych w pytaniach nr 1 i nr 2

Wybrana odpowiedź w pytaniu nr 1	**Wybrana odpowiedź w pytaniu nr 2**							
	A		**B**		**C**		**D**	
	Grupa 1	**Grupa 2**	**Grupa 1**	**Grupa 2**	**Grupa 1**	**Grupa 2**	**Grupa 1**	**Grupa 2**
A	3	1	0	1	0	0	3	6
B	3	0	0	0	0	0	0	0
C	0	0	0	0	0	0	0	0
D	5	4	1	1	0	0	8	7

Źródło: Opracowanie własne

Na podstawie danych przedstawionych w tabeli nr 3 można stwierdzić, że ankietowanym brakowało wiedzy na temat analizy ryzyka. Skutkiem opisanego wcześniej braku była niemożność praktycznego wykorzystania posiadanej wiedzy. Potwierdzeniem przedstawionej tezy są wyniki odpowiedzi udzielonych na pytanie nr 3, które dotyczyło praktycznego wykonywania analizy ryzyka przez respondentów. Ankietowani mieli do wyboru trzy odpowiedzi. Odpowiedź *A* stwierdzała, że respondent samodzielnie wykonał analizę ryzyka lub uczestniczył w pracach zespołu oceniającego zagrożenia. Odpowiedź *B* oznaczała wykonanie analizy ryzyka, ale z pomocą osoby posiadającej większe doświadczenie niż ankietowany. Odpowiedź *C* stwierdzała, że respondent nie wykonywał analizy ryzyka. Rozkład udzielonych odpowiedzi przedstawia tabela 4.

Na podstawie analizy przedstawionych danych można stwierdzić, że umiejętność wykonania analizy ryzyka jest słaba. Zaledwie 17% ankietowanych samodzielnie wykonywało analizę ryzyka. Pozostałe 83% ankietowanych nie wykonywało tej czynności ani razu, co potwierdzają dane przedstawione w tabeli 4.

Tabela 4. Rozkład odpowiedzi udzielonych na pytanie nr 3

Odpowiedź	**A**	**B**	**C**
Grupa 1	3	0	17
Grupa 2	3	0	18
Razem	6	0	35

Źródło: Opracowanie własne

Zatem wiedza teoretyczna nie ma odwzorowania lub nieznana jest umiejętność jej zastosowania przez ankietowanych. Oznacza to, że dokument analizy ryzyka może zostać źle opracowany, a ponieważ wyszczególnia on zasoby informacyjne o wysokiej

wrażliwości, to można się spodziewać, iż nie będą one chronione w sposób właściwy. Fakt ten może posiadać dwa potencjalne skutki:

- pierwszy – analiza musi zostać powtórzona. Zaleca się w takim przypadku włączenie do zespołu doradcy posiadającego doświadczenie w prowadzeniu analiz ryzyka;
- drugi – powstanie dokument, który nie będzie należycie opisywał zasobów informacyjnych organizacji oraz zagrożeń i ich konsekwencji. System ochrony zasobów informacyjnych funkcjonujący na podstawie takiej analizy nie będzie rozwiązaniem efektywnym.

Wynikiem poprawnie przeprowadzonej analizy ryzyka będzie zbiór ryzyk dla poszczególnych zasobów informacyjnych wykazanych jako zasoby wrażliwe dla danej organizacji. Wartości ryzyk dla poszczególnych elementów systemu teleinformatycznego obliczane są według wzoru (3). Zbiór ryzyk dla elementów systemu teleinformatycznego przedstawiono przy pomocy wektora (4).

$$R = \{r_1, r_2, .., r_i\}, \tag{4}$$

gdzie:

R – zbiór ryzyk dla zasobów informacyjnych od 1-ego do j-tego,

r_j – ryzyka dla zasobów informacyjnych systemu teleinformatycznego instytucji oraz $j \in <1,i>$.

Jeżeli użytkownicy systemów teleinformatycznych, przetwarzających wrażliwe zasoby informacyjne, nie posiadają wiedzy na temat roli analizy ryzyka oraz umiejętności jej wykonania, to nie należy oczekiwać, że zasoby informacyjne w ich instytucjach będą chronione na podstawie przypadkowych decyzji. Opisana sytuacja jest sprzeczna z celem, dla którego organizuje się system ochrony informacji, a którym jest eliminowanie lub ograniczanie wpływu zdarzeń przypadkowych na bezpieczeństwo informacji znajdujących się wewnątrz systemu teleinformatycznego organizacji.

Na podstawie wyników badania ankietowego można przyjąć, że w stanie początkowym, wewnętrzny system zarządzania bezpieczeństwem informacyjnym będzie działał chaotycznie. Stan chaosu jest wynikiem braku wiedzy i doświadczenia osób odpowiedzialnych za organizację wewnętrznego systemu zarządzania bezpieczeństwem informacji. Z upływem czasu rozwiązanie to zacznie ewoluować od działań chaotycznych do działań zorganizowanych i powtarzalnych. Ewolucja ta będzie zgodna z zaleceniami normy PN ISO/IEC 27001 [11]. Norma określa zarządzanie bezpieczeństwem informacji znajdującej się w systemach teleinformatycznych jako ciąg działań powtarzanych w regularnych odstępach czasu, których celem jest podniesienie lub utrzymanie założonego poziomu bezpieczeństwa zasobów informacyjnych [11].

Pytaniem, na które – a priori – nie jest znana odpowiedź jest kwestia strat, jakie powstaną do momentu usprawnienia wadliwie działającego rozwiązania. Wielkość strat, powstałych w wyniku wykorzystania podatności w systemie, może być wyrażana szacunkowo. W przypadku zasobów informacyjnych dokładne określenie strat, w niektórych przypadkach, jest niemożliwe.

Wynikiem analizy ryzyka jest wektor ryzyk dla poszczególnych zasobów informacyjnych. Na podstawie wektora ryzyk wybierane są zasoby informacyjne, które będą

podlegały ochronie. Przykładowe procedury wyboru zasobów informacyjnych, podlegających ochronie na podstawie wartości ryzyka wyznaczonego dla niego, przedstawiono w pracach autorstwa K. Lidermana oraz L. Wolaniuka i A. Szleszyńskiego [8,16]. Wybór obiektów chronionych jest decyzją wielokryterialną, w której wyszukanie suboptymalnych rozwiązań może być wykonane przy pomocy metody Bellingera [4]. Metoda ta jest prosta w wykorzystaniu, a wyniki optymalizacji uzyskane dzięki jej zastosowaniu pokrywają się z innymi metodami wyboru wielokryterialnego [4].

Zasobami informacyjnymi gromadzonymi i przetwarzanymi przez systemy teleinformatyczne organizacji są dane oraz wiadomości umieszczone w bazach danych, zbiory dokumentów, zawartość serwera poczty elektronicznej instytucji itp.

Analiza ryzyka nie jest jedyną czynnością wykonywaną przez zespół stanowiący wewnętrzny system zarządzania bezpieczeństwem informacji. Analiza wskazuje zasoby wrażliwe oraz możliwe konsekwencje będące wynikiem braku właściwej ochrony zasobów informacyjnych. Korzystając z wyników analizy ryzyka – należy opracować plan działań, dotyczących redukcji możliwości wystąpienia incydentów w bezpieczeństwie zasobów informacyjnych, gromadzonych w systemie teleinformatycznym instytucji.

3. SCENARIUSZE PRZEBIEGU INCYDENTÓW W BEZPIECZEŃSTWIE INFORMACJI GROMADZONEJ I PRZETWARZANEJ W SYSTEMIE TELEINFORMATYCZNYM

Scenariusz ma za zadanie opisać przebieg incydentu, który pojawia się w trakcie funkcjonowania systemu informatycznego. Opisana w punkcie 2 procedura analizy ryzyka nie przedstawia powiązań pomiędzy zasobami informacyjnymi. W swojej najprostszej postaci analiza ryzyka ocenia zasoby informacyjne jako obiekty niezależne od siebie. Taka sytuacja w przypadku rzeczywistych systemów teleinformatycznych nie istnieje. Korzystając z relacyjnego lub obiektowo-relacyjnego modelu danych, stosowana jest dekompozycja danych na mniejsze fragmenty.

Celem dekompozycji jest przechowywanie zbiorów danych, dotyczących podobnych cech obiektu, np. dane osobowe, informacje o wyposażeniu pojazdu itp. Korzystając z algebry relacyjnej lub manipulacji na wskaźnikach, można dokonać agregacji zbiorów informacji o danym obiekcie. Rozkład danych pozwala rozmieszczać fragmenty informacji w różnych lokalizacjach fizycznych.

Zatem uszkodzenie lub uniemożliwienie dostępu do jednego z fragmentów bazy danych – ogranicza jej funkcjonalność lub czyni ją bezużyteczną dla użytkownika. Rolą scenariusza jest zagregowanie wiadomości o zasobach informacyjnych, ich wzajemnych relacjach, a następnie opisanie możliwych skutków wystąpienia zdarzenia negatywnego, jakim jest incydent.

Scenariusz będzie przedstawiał ścieżkę propagacji zagrożeń, jaka występuje w systemie teleinformatycznym instytucji.

Scenariusz adresowany jest do:

– zarządu organizacji, gdyż informuje go w sposób opisowy i przy wykorzystaniu języka potocznego o zdarzeniach, jakie mogą wystąpić oraz ich konsekwencjach dla funkcjonowania systemu teleinformatycznego i eksploatującej go instytucji;

- wewnętrznego zespołu zarządzania bezpieczeństwem informacyjnym, w składzie którego są osoby nie będące specjalistami z dziedziny technologii informatycznych. Zatem, mogą mieć problem ze zrozumieniem potencjalnych rozmiarów strat gdyby one wystąpiły;
- działu informatyki organizacji. Opracowując taki dokument należy wykonać analizę zależności występujących pomiędzy urządzeniami składującymi i przetwarzającymi wiadomości oraz pomiędzy zasobami informacyjnymi. Szczególną uwagę należy poświęcić zasobom informacyjnym zaklasyfikowanym do zbioru zasobów wrażliwych. W wyniku analizy można odkryć punkty wejścia do systemów przetwarzających dane wrażliwe, które nie były wcześniej brane pod uwagę.

Sam dokument nie powinien być zbyt obszerny objętościowo. Wymaganie to jest istotne, ponieważ ma się z nim zapoznawać zarząd danej instytucji. Również dla członków zespołu zarządzającego bezpieczeństwem informacyjnym instytucji, czytanie obszernego opracowania nie będzie zajęciem łatwym, kiedy uwzględni się konieczność łączenia terminologii prawniczej z techniczną. Rolą dokumentu jest informowanie: co jest zagrożone, co się stanie jeśli, podatność zostanie wykorzystana i jakie będą skutki takiego zdarzenia.

Analizując dostępną literaturę przedmiotu, znaleziono metodę oceny zagrożeń, opracowaną przez pracowników firmy Microsoft. Metoda przeznaczona jest do modelowania zagrożeń dla nowo opracowywanych systemów informatycznych. Koncentruje się ona na zagrożeniach dla oprogramowania, które stanowi kluczowy element systemu. Metoda oceny zagrożeń, przedstawiona w pracy F. Swiderskiego i W. Snydera, posługuje się scenariuszem użycia do opisu sposobu użytkowania systemu informatycznego [13].

Scenariusze użycia dzielone są na dwie kategorie:

- obsługiwane, czyli zgodne z przewidywanymi zasadami wykorzystania rozwiązania. Należą do nich typowe działania użytkowników, takie jak: uwierzytelnienie w systemie, uzyskanie dostępu do przydzielonych zasobów;
- nieobsługiwane, dotyczą zdarzeń nieprzewidzianych w trakcie tworzenia rozwiązania. Należą do nich: próby penetracji z wewnątrz systemu, ataki z zewnątrz systemu, awarie, sytuacje szczególne itp.

Wadą opisanej metody jest konieczność opracowania obszernej dokumentacji. Obszerność wynika z konieczności uwzględnienia różnych perspektyw rozwiązania. Wielość perspektyw związana jest z grupami odbiorców dokumentacji. Do wymienionych grup należą: kierownicy projektu ze strony: zamawiającego oraz wykonawcy, osoby odpowiedzialne za bezpieczeństwo informacyjne u zamawiającego, projektanci i programiści u wykonawcy, testerzy rozwiązania, osoby odpowiedzialne za opracowanie dokumentacji systemu itd.

Zatem opisana metoda jest skuteczna w opisie zagrożeń oraz prezentacji jej wyników, ale jest sprzeczna z przyjętym wymaganiem, jakim jest możliwie najmniejsza objętość. Dodatkowo tak rozbudowany system dokumentowania podatności w systemie będzie wymagał osoby lub osób odpowiedzialnych za uaktualnianie dokumentacji.

W literaturze przedmiotu można znaleźć metodę oceny niezawodności systemów nazywaną FMEA (ang. Failure Mode Effects Analysis). W metodzie tej system poddaje się dekompozycji na możliwie najmniejsze elementy, a następnie ocenia się wpływ uszkodzenia na funkcjonowanie modułu, w którym jest zamontowany, a także wpływ uszkodzenia na działanie całego systemu [17]. Użytecznym narzędziem wykorzystanym w metodzie FMEA jest drzewo uszkodzeń, które przedstawia związki pomiędzy zdarzeniami (awariami lub uszkodzeniami) a skutkami tych zdarzeń dla poprawnego działania systemu.

Metoda ta koncentruje się na analizie niezawodności systemu, a nie na przebiegu incydentu. Jest ona przeznaczona do wykorzystania przez personel techniczny, gdyż wymaga ona dekompozycji ocenianego rozwiązania na mniejsze części (podsystemy lub elementy). Zaletą metody jest możliwość wskazania ścieżki krytycznej, zawierającej najmniejszą liczbę elementów systemów, które uszkodzone doprowadzą do przerwania działania systemu [17]. Wyniki analiz, prowadzonych z wykorzystaniem metody FMEA, służą do planowania czynności diagnostycznych i obsługowych eksploatowanego rozwiązania. Nie jest to funkcja informacyjna, szczególnie dla osób, które nie zajmują się kwestiami niezawodności, obsługi technicznej sprzętu oraz oprogramowania.

W inżynierii oprogramowania wykorzystywana jest metoda oceny architektury danego rozwiązania. Zatem celem architektury systemu informatycznego jest przedstawienie opracowywanego rozwiązania z różnych perspektyw. Zależą one od funkcji, jakie będą wykonywane w systemie przez poszczególne jego elementy. Takie podejście do procesu tworzenia lub modyfikacji rozwiązania, umożliwia skupienie się na wybranych perspektywach systemu, co pozwala na ocenę ich użyteczności [3].

Według C. Larmana analiza architektury oprogramowania jest odmianą analizy wymagań, gdzie następuje skoncentrowanie na tych wymaganiach, które mają wpływ na tworzone rozwiązanie [7]. Takim przykładem może być opracowanie bezpiecznego lub wydajnego systemu informatycznego. Autor stwierdza, że najważniejszym elementem analizy architektonicznej jest identyfikacja czynników wpływających na funkcjonowanie systemu, poznanie ich priorytetów, stopnia zmienności oraz przedstawienie sposobów ich obsługi [7].

Jednakże ocena architektury systemu nie udziela informacji o tym, jak będzie przebiegał incydent w bezpieczeństwie informacji w systemie teleinformatycznym. Ocena architektury wskaże te elementy, które będą wpływały na bezpieczeństwo systemu jako całości. Jednak ocena architektury systemu nie udzieli informacji, jak taki proces będzie przebiegał oraz jakie negatywne skutki wywoła. Można stwierdzić, że skutki incydentów zawarte są w analizie ryzyka, która była prowadzona przy założeniu, że zasoby są niezależne od siebie. Sytuacja taka nie występuje w rzeczywistych systemach teleinformatycznych, co opisano na początku paragrafu.

Można stwierdzić, że w chwili obecnej nie ma metody, która pozwoliłaby na opracowanie scenariuszy przebiegu incydentów w bezpieczeństwie systemu teleinformatycznego. Istnieje oczywiście możliwość adaptacji jednej z przedstawionych metod, jednak działanie to będzie wymagało dużego nakładu pracy. Jest jednak możliwość opracowania rozwiązania autorskiego, co jest realizowane w ramach pracy naukowo-badawczej prowadzonej w Wyższej Szkole Oficerskiej Wojsk Lądowych.

PODSUMOWANIE

Na podstawie przeprowadzonych badań można stwierdzić, że proces szkolenia z zakresu ochrony zasobów informacyjnych nie przedstawia znaczenia analizy ryzyka w systemie ochrony zasobów informacyjnych wewnątrz instytucji. Należy pamiętać, że osoby które, mogą znaleźć się w składzie wewnętrznego systemu zarządzania bezpieczeństwem informacji w instytucji i będą zobligowane do przeprowadzenia pewnej części analizy ryzyka. Brak wiedzy może spowodować, że ocena częstości występowania oraz potencjalnych skutków może być przeszacowana lub niedoszacowana, co w konsekwencji spowoduje niewłaściwą ochronę zasobów informacyjnych.

Wyniki badań prowadzonych przez firmę IDG, w jednostkach rządowych i samorządowych, wykazały bardzo różne podejście urzędów do kwestii ochrony zasobów informacyjnych [6]. W jednym z pytań ponad 50% ankietowanych stwierdziło, że nie zgłaszają oni organom ścigania incydentów w bezpieczeństwie systemu, z powodu niskiej wykrywalności sprawców tych przestępstw [6].

Zatem szkolenie i utrzymanie systemu ochrony zasobów informacyjnych jest nadal jednym z kluczowych zadań kierownictwa instytucji. Jeżeli utrata lub uszkodzenie zasobów informacyjnych będzie skutkować brakiem możliwości realizacji zadań biznesowych przez instytucję, to kwestia ochrony zasobów informacyjnych nie będzie już przedmiotem dyskusji. Szkolenie z tematyki bezpieczeństwa informacji należy traktować jako inwestycję w przyszłość instytucji. Zaniedbania w tym obszarze mogą nieść bardzo poważne konsekwencje dla działalności instytucji.

LITERATURA

1. Aven T., *Foundation of risk analysis. A Knowledge and Decision – Oriented Perspective*, John Wiley & Sons Ltd, Chichester, West Sussex 2003.
2. Białas A., *Bezpieczeństwo informacji i usług we współczesnej firmie lub organizacji*, WNT, Warszawa 2006.
3. Clements P., Kazman R., Klein M., *Architektura oprogramowania. Metody oceny oraz analiza przypadków*, Wydawnictwo Helion, Gliwice 2003.
4. Górny P., *Elementy analizy decyzyjnej*, AON, Warszawa 2004.
5. International Standard ISO/IEC-15408 part 1., *Information security techniques, International Standardization Organization*, Geneva 2005.
6. Jóźwiak I., Szleszyński A., *Rola oraz bezpieczeństwo informacji w uczelni publicznej i niepublicznej*, [w:] „Zeszyty Naukowe WSOWL", nr 4/2011, Wrocław 2011.
7. Larman C., *UML i wzorce projektowe. Analiza i projektowanie obiektowe oraz iteracyjny model wytwarzania aplikacji*, Helion, Gliwice 2011.
8. Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych*, PWN, Warszawa 2008.
9. Michalski A., *Dostępność informacji w organizacji gospodarczej*, Wydawnictwo Politechniki Śląskiej, Gliwice 2007.
10. Polska Norma PN ISO/IEC 17799:2007, Technika informatyczna. Techniki bezpie-

czeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji, PKN, Warszawa 2007.

11. Polska Norma PN ISO/IEC 27001:2010, Technika informatyczna. Techniki bezpieczeństwa. System zarządzania bezpieczeństwem informacji. Wymagania, PKN, Warszawa 2010.
12. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).
13. Swiderski F., Snyder W., *Modelowanie zagrożeń*, Promise, Warszawa 2005.
14. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, (Dz. U. z 1997 r. Nr 133, poz. 883, z późn. zm.).
15. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r. Nr 182, poz. 1228, z późn. zm.).
16. Wolaniuk L., Szleszyński A., *Metodyka szacowania ryzyka bezpieczeństwa informacji wojskowego polowego systemu teleinformatycznego. Etap I: Wykorzystanie drzewa użyteczności do analizy ryzyka dla bezpieczeństwa informacji w wojskowym polowym systemie teleinformatycznym*, WSOWL, Wrocław 2010.
17. Zio E., *An Introduction To The Basics Of Reliability And Risk Analysis*, World Scientific, Singapore 2010.

USE OF RISK ANALYSIS AND INCIDENT SCENARIOS IN SYSTEMS MANAGING SECURITY OF INFORMATION COLLATED, PROCESSED AND TRANSMITTED IN INFORMATION AND COMMUNICATION TECHNOLOGY SYSTEMS

Summary

In the paper the use of risk analysis and incident scenarios in Information and Communication Technology (ICT) systems is presented. An evaluation of the incidents affecting the security of information stored and processed in an ICT system is made. In the first part of the paper an analysis of the current state is made. Next a correlation between risk analysis and incident scenarios developed for information security is shown. In Tables 1, 2, 3 and 4 the result of the survey conducted by the authors on the body of knowledge related to risk analysis methods is shown. The survey shows that potential analysis users who would have to do it sometime in the future have decent theoretical knowledge about risk analysis. However, as they indicated in their responses, they were not ready to make it themselves.

Keywords: *information security, risk analysis, incident scenarios, information and communication technology systems*

NOTY BIOGRAFICZNE

mgr inż. Artur SZLESZYŃSKI – wykładowca Katedry Inżynierii Systemów Wydziału Zarządzania Wyższej Szkoły Oficerskiej Wojsk Lądowych imienia generała Tadeusza Kościuszki. W pracy naukowej skupia się na zagadnieniach technicznego bezpieczeństwa systemów teleinformatycznych.

dr inż. Marek WITKOWSKI – adiunkt w Instytucie Dowodzenia Wyższej Szkoły Oficerskiej Wojsk Lądowych imienia generała Tadeusza Kościuszki. W pracy naukowej skupia się na zagadnieniach dotyczących bezpieczeństwa teleinformatycznego w systemie kierowania bezpieczeństwem narodowym.