Rafał Leszczyna[1]

Metoda szacowania kosztu zarządzania bezpieczeństwem informacji i przykład jej zastosowania w zakładzie opieki zdrowotnej

1. Wstęp

Wraz z rosnącym wykorzystaniem technologii informatycznych oraz Internetu przez jednostki administracji publicznej oraz służbę zdrowia wzrosło narażenie tych jednostek na cyberzagrożenia. Według „Raportu o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 roku"[2], opublikowanego przez Rządowy Zespół Reagowania na Incydenty Komputerowe cert.gov.pl, każdego roku rośnie liczba incydentów związanych z cyberbezpieczeństwem administracji publicznej i stają się one coraz groźniejsze. Największą grupę stanowią ataki wykonywane przez tzw. botnety, czyli sieci komputerów zainfekowanych przez złośliwe oprogramowanie, których zadaniem jest wykonywanie rozkazów cyberprzestępców. W 2015 r. odnotowano aż 4284 takich ataków. Rok ten okazał się też rekordowy pod względem liczby zgłoszonych incydentów związanych z nieprawidłową konfiguracją systemów funkcjonujących w instytucjach administracji państwowej[2].

Konsekwencje tego typu incydentów mogą mieć różną skalę – od zakłócenia działalności instytucji i utrudnień w pracy, przez „wycieki" poufnych informacji, do katastrof ekologicznych i zagrożenia zdrowia oraz życia tysięcy osób, w przypadku instytucji wchodzących w skład tzw. infrastruktury krytycznej, do których należą m.in. jednostki służby zdrowia. Dla przykładu na początku 2015 r. dokonano dedykowanego ataku na Urząd Miejski w Jaworznie. W wyniku ataku z konta urzędu skradziono ponad 940 tysięcy złotych. Do ataku wykorzystano tzw. konia trojańskiego, który podczas przelewu dokonywał zmiany konta odbiorcy. Ofiarami podobnych ataków stały się też Urzędy Gminy Gidle i Rząśnia.

---

[1] Politechnika Gdańska, Wydział Zarządzania i Ekonomii.

[2] *Raport O Stanie Bezpieczeństwa Cyberprzestrzeni RP W 2015 Roku*, http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/910, Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2015-roku.html (10.09.2017).

Cybernetycznego wyłudzenia dokonano w Podlaskim Zarządzie Dróg Wojewódzkich, gdzie po starannie przeprowadzonym rekonesansie informatycznym, przestępcy przygotowali i wysłali fałszywe pismo informujące o zmianie numeru konta wykonawcy. W rezultacie Zarząd przelał na ich rachunek 3,7 mln złotych.

Stąd jednym z kluczowych aspektów współczesnego zarządzania instytucjami administracji publicznej staje się zarządzanie bezpieczeństwem systemów informatycznych. Stosowane zabezpieczenia mogą mieć charakter podstawowy, jak na przykład zainstalowanie oprogramowania antywirusowego, bardziej złożony, chociażby korzystanie z kilku rodzajów zabezpieczeń, i wreszcie bardzo zaawansowany – strategie ochrony, które oprócz zróżnicowanych rozwiązań technicznych wykorzystują także środki administracyjne i operacyjne. Z wdrożeniem i utrzymaniem każdego z tych środków powiązany jest koszt, który w przypadku rozwiązań kompleksowych może stać się znaczącą częścią kosztów operacyjnych instytucji. Kadra kierownicza jednostek administracji publicznej staje więc przed trudną decyzją dotyczącą skali inwestycji w zabezpieczenia systemów informatycznych. Zbyt wysokie wydatki spowodują znaczące niedofinansowanie innych obszarów działalności instytucji. Z drugiej strony niedostateczna ochrona może doprowadzić do poważnych strat.

W artykule przedstawiono metodę, której zadaniem jest wsparcie decydentów w podejmowaniu tego typu decyzji przez wskazanie kosztu, jaki dana instytucja będzie musiała ponieść na działania zapewniające skuteczny poziom ochrony. Koszty te są najczęściej niejawne, a przez to trudne do zidentyfikowania. Opisywana metoda pozwala je oszacować na podstawie niewielkiej liczby parametrów określających takich zmienne, jak liczba pracowników, wskaźniki fluktuacji czy wysokości wynagrodzeń. Prace nad metodą obejmowały analizę uznanych metod analizy kosztów działalności przedsiębiorstw, a następnie wybranie tej, która najlepiej odnosi się do dziedziny zarządzania bezpieczeństwem informacji. Następnie zaproponowano modyfikacje, służące dopasowaniu do specyfiki zagadnienia (rozdział 2). Praca obejmowała również identyfikację wszelkich działań związanych z zarządzaniem bezpieczeństwem IT, wybór oraz przyporządkowanie nośników kosztów oraz określenie minimalnego zbioru danych wejściowych, które pozwolą uzyskać zadowalające rezultaty oszacowań (rozdział 3 i 4). W rozdziale 5 przedstawiono natomiast studium przypadku zastosowania metody do oszacowania kosztu zarządzania bezpieczeństwem informacji w przychodni zdrowia.

2. Wybór i adaptacja metody kalkulacji kosztów

W wyniku przeprowadzonej analizy uznanych metod kalkulacji kosztów w przedsiębiorstwie za najbardziej odpowiednie do określenia kosztów związanych z zarządzaniem bezpieczeństwa IT w organizacji uznano rachunek kosztów działań (ang. *Activity-Based Costing* – ABC) oraz rachunek kosztów działań sterowany czasem (ang. *Time-Driven Activity-Based Costing* – TDABC).

Tradycyjne metody kosztów są zorientowane na wyznaczenie kosztu jednostkowego produktu przy znajomości kosztów bezpośrednich i ogólnozakładowych przedsiębiorstwa[3]. Istotą tych metod jest odpowiedni podział i przyporządkowanie kosztu do produktów. Tymczasem w analizowanym problemie to właśnie te koszty bezpośrednie i pośrednie nie są znane, i to je należy oszacować. Nie występuje tu także problem określania kosztu jednostkowego.

Metody ABC i TDABC koncentrują się na działaniach jako podstawowych obiektach związanych z kosztami w przedsiębiorstwie[4]. W tym sensie stają się przydatne, gdyż proponują podejście do oszacowania czynnościowego (w przeciwieństwie do rzeczowego – związanego z zasobami rzeczowymi) kosztu wdrażania bezpieczeństwa IT w organizacji, bazując na określeniu wszystkich działań związanych z tym przedsięwzięciem. Tak samo w przypadku rachunku kosztów działań oraz rachunku kosztów działań sterowanego czasem, każde z działań zostanie powiązane z odpowiednimi obiektami kosztów za pomocą nośników kosztów, a następnie zostanie określony koszt działań[6].

Wybranym nośnikiem kosztów zasobów jest nośnik *czasu trwania*. Ponieważ zasoby mają charakter przede wszystkim osobowy, najbardziej naturalnym wyborem nośnika kosztów zasobów jest *czas pracy* personelu wyrażany w godzinach. O ile jednak w przypadku metody ABC i TDABC działania przyporządkowywane są różnym obiektom kosztów, o tyle w przypadku analizowanego problemu zostaną one wszystkie zagregowane, gdyż wspólnie wpływają na koszt przedsięwzięcia. Druga istotna różnica związana jest z faktem, że w ABC i TDABC, podobnie jak w metodach tradycyjnych, koszty działań znane są w organizacji i otrzymuje się je głównie w drodze ankietowania albo przepytywania

[3] K. Cooper, R.S. Kaplan, *Zarządzanie kosztami i efektywnością*, Dom Wydawniczy ABC, Kraków 2000.

[4] R.S. Kaplan, S.R. Anderson, P. Mućko, A. Mućko, *Rachunek kosztów działań sterowany czasem – TDABC Time-Driven Activity-Based Costing: prostsza i bardziej skuteczna droga do większych zysków*, Wydawnictwo Naukowe PWN, Warszawa 2012.

pracowników. Natomiast w odniesieniu do analizowanego zagadnienia wszystkie koszty działań należy oszacować.

3. Identyfikacja listy działań

W celu zdefiniowania listy działań dokonano analizy standardów i powszechnie uznanych monografii dotyczących zarządzania bezpieczeństwem systemów informatycznych. Z uwagi na poszukiwaną uniwersalność działań (a przy tym powszechną stosowalność) byłoby wskazane, aby lista działań bazowała na standardzie. W wyniku analiz literatury[5, 6, 7, 8, 9, 10] za podstawę do opracowania listy działań przyjęto standard NIST SP 800–53 „Recommended Security Controls for Federal Information Systems and Organizations"[7], zawierający wytyczne do wybierania i definiowania mechanizmów bezpieczeństwa (ang. *security controls*) dla systemów informatycznych w agencjach federalnych Stanów Zjednoczonych. Wytyczne dotyczą wszystkich komponentów systemów informatycznych, które przetwarzają, przechowują albo transmitują informację federalną.

Wyboru normy dokonano ze względu na jej następujące cechy:

- Będąc powszechnie zaakceptowaną normą, posiada wymagane cechy uniwersalności i powszechności.
- Przedstawiono w niej wyczerpującą listę komponentów bezpieczeństwa IT, obejmującą wszelkie obszary zarządzania bezpieczeństwem systemu informatycznego organizacji.
- Dedykowana dla agencji federalnych bardzo racjonalnie odnosi się do zagadnień bezpieczeństwa: proponowane wymagania nie są wygórowane,

[5] National Institute of Standards and Technology (NIST), *NIST SP 800–53 Rev. 3 Recommended Security Controls for Federal Information Systems and Organizations*, U.S. Government Printing Office 2009.

[6] R. Lusignan, O. Steudler, J. Allison, *Managing Cisco Network Security: Building Rock-Solid Networks*, Syngress 2000.

[7] J. Ramachandran, *Designing Security Architecture Solutions*, Wiley 2002.

[8] T.R. Peltier, *Information Security Policies and Procedures: A Practitioner's Reference, Second Edition*, Auerbach Publications, Boston 2004.

[9] H.F. Tipton, M.K. Nozaki, *Information Security Management Handbook*, vol. 4, 6th ed., Auerbach Publications, Boston 2010.

[10] S. Purser, *A Practical Guide to Managing Information Security (Artech House Technology Management Library)*, Artech House, Inc., Norwood 2004.

a jednocześnie ich spełnienie prowadzi do zapewnienia dobrego poziomu bezpieczeństwa organizacji.

- Jest w pełni zgodna z najważniejszym standardem zarządzania bezpieczeństwem – ISO/IEC 27001[11]. W tabeli H-1, Załącznika H do normy NIST SP 800–53 przedstawiono jednoznaczne odwzorowanie pomiędzy obiema normami[7].

Standard NIST 800–53 definiuje zabezpieczenia techniczne, organizacyjne i administracyjne dla trzech poziomów odpowiadających systemom i instytucjom o niskim, umiarkowanym oraz wysokim oddziaływaniu[12]. Opracowując metodę szacowania kosztu zarządzania bezpieczeństwem informacji, wykorzystano listę zabezpieczeń poziomu pierwszego, czyli zapewniającego podstawowy, ale wyczerpujący poziom bezpieczeństwa w organizacji, obejmujący kompleksowo wszystkie obszary zabezpieczeń. W rezultacie utworzono listę działań obejmującą takie obszary zarządzania bezpieczeństwem organizacji, jak m.in. kontrola dostępu do zasobów systemu informatycznego, szkolenia dotyczące bezpieczeństwa systemu IT, ochrona fizyczna, bezpieczeństwo personelu czy ocena ryzyka.

4. Określenie danych wejściowych i wyjściowych, przyporządkowanie nośników kosztów

Następnie dla poszczególnych działań oszacowano czasy ich wykonywania oraz przyporządkowano zasoby. Każdemu działaniu przyporządkowano cztery rodzaje oszacowań czasu wykonania. *Minimalny czas wykonania* jest to najkrótszy możliwy czas wymagany dla zapewnienia i utrzymania danego elementu bezpieczeństwa. Konsekwentnie *czas maksymalny* to ilość czasu potrzebna na wykonanie działania, która w normalnych warunkach nie powinna być przekroczona przez organizację. *Czas średni* jest wielkością otrzymywaną przez obliczenie średniej arytmetycznej z dwóch wcześniejszych wartości. Natomiast *przeciętny czas wykonania* odpowiada czasowi uzyskanemu z obserwacji praktyki organizacji. Jest to czas określający, ile organizacje w praktyce przeciętnie poświęcają czasu na skuteczne wykonanie danego działania.

[11] Polski Komitet Normalizacyjny, PN-ISO/IEC 27001:2007: Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania, 2007.

[12] NIST. FIPS PUB 199. *Standards for Security Categorization of Federal Information and Information Systems*, 02.2004,

Jako zasoby przyjęto grupy pracowników odpowiedzialnych za wykonanie bądź biorące udział w wykonywaniu działań według stanowisk. W tym na przykład: pracowników bezpieczeństwa IT, administratorów IT, pracowników działu zarządzania kadrami, kierowników lub członków zarządu, pracowników ochrony czy pracowników jednostki budżetowania i kontroli finansów (tabela 2). Następnie każdemu działaniu przyporządkowano nośniki kosztu zasobów oraz oszacowania czasu trwania.

W celu dokonania oszacowań całkowitego kosztu związanego z działaniami wdrażania i utrzymania bezpieczeństwa konieczne jest podanie informacji dotyczących analizowanej organizacji. I tak należy określić:

- liczbę użytkowników – liczbę pracowników organizacji korzystających z urządzeń komputerowych,
- liczbę pracowników bezpieczeństwa IT – planowaną liczbę pracowników organizacji odpowiedzialnych za bezpieczeństwo systemu informatycznego,
- w_{przyj} – wskaźnik przyjęć – wartość przeciętna stosunku liczby pracowników przyjętych do wszystkich pracowników organizacji w ciągu roku,
- w_{fl} – wskaźnik odejść – wartość przeciętna stosunku liczby pracowników odchodzących do wszystkich pracowników organizacji w ciągu roku,
- w_{przen} – wskaźnik przeniesień – wartość przeciętna stosunku liczby pracowników zmieniających stanowisko w organizacji do wszystkich pracowników organizacji w ciągu roku,
- w_{mob} – wskaźnik wykorzystania urządzeń mobilnych – wartość przeciętna stosunku liczby pracowników korzystających z mobilnych urządzeń komputerowych w organizacji do wszystkich pracowników organizacji w ciągu roku,
- szacunkową liczbę osób spoza organizacji mających dostęp do systemu (wskaźnik nieobowiązkowy),
- oraz przeciętne stawki godzinnych wynagrodzenia pracowników odpowiadających wymienionym wcześniej stanowiskom.

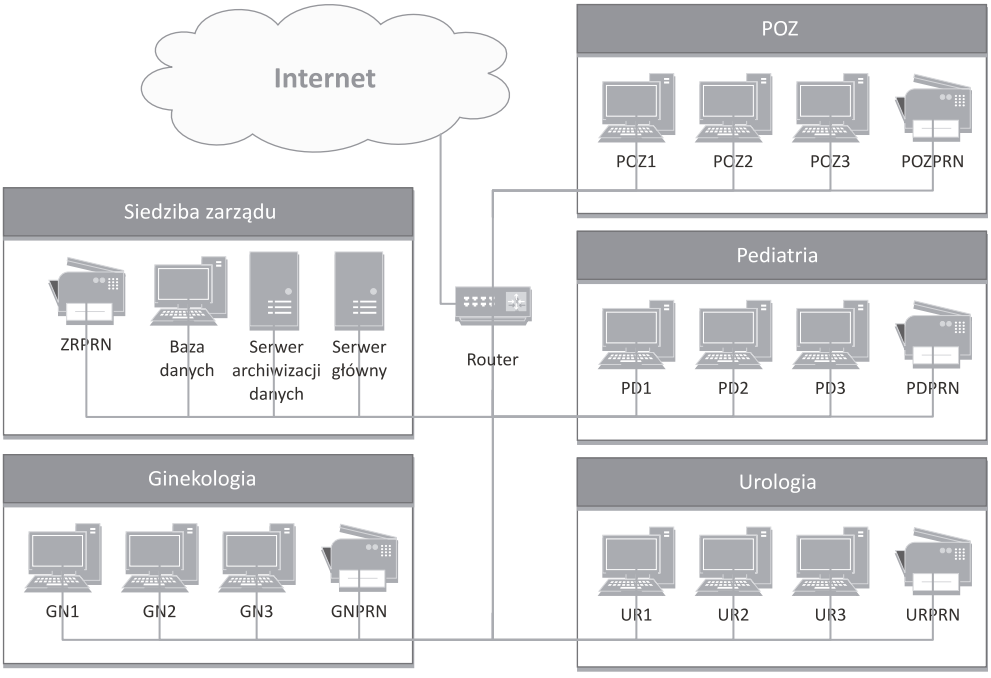
Na podstawie powyższych danych wejściowych metoda pozwala oszacować:

- szacunkowy koszt całkowity działań związanych z zarządzaniem bezpieczeństwem IT, obejmujący koszt działań wszystkich zaangażowanych pracowników,
- szacunkowy koszt całkowity działań wykonywanych wyłącznie przez pracowników bezpieczeństwa IT,
- liczbę wymaganych godzin pracy pracowników bezpieczeństwa IT,
- liczbę wymaganych etatów dla pracowników bezpieczeństwa IT.

5. Studium przypadku

W ramach studium przypadku dokonano oszacowania rocznych kosztów działań związanych z zarządzaniem bezpieczeństwem informacji w zakładzie opieki zdrowotnej posiadającej cztery oddziały – podstawowej opieki zdrowotnej, pediatrii, ginekologii i urologii. Jednostka zatrudnia 17 pracowników medycznych, w tym 12 lekarzy i 5 pielęgniarek, oraz 3-osobowy personel administracyjny.

W skład systemu informatycznego przychodni (rysunek 1) wchodzi podsieć oddziału podstawowej opieki medycznej (POZ), podsieć oddziału ginekologii, podsieć oddziału pediatrii, podsieć oddziału urologii oraz podsieć administracyjna. Każda z podsieci jest połączona z Internetem, podsiecią administracyjną oraz z serwerem baz danych. Archiwizacja danych przesyłanych z oddziałów oraz rejestracja pacjentów przychodni odbywa się na urządzeniach znajdujących się w podsieci administracyjnej.



Rysunek 1. Diagram systemu informatycznego analizowanego zakładu opieki zdrowotnej

Źródło: opracowanie własne.

W ramach systemu są przechowywane i przetwarzane m.in. następujące zasoby informacyjne: karty pacjentów, dane pracowników i kontrahentów, rejestr wizyt, wyniki badań diagnostycznych (dołączane do kart pacjentów) oraz recepty, zwolnienia, skierowania. Większość z tych zasobów dotyczy danych osobowych lub danych sensytywnych, które w Polsce podlegają szczególnej ochronie.

W celu oszacowania rocznego kosztu należy podać liczbę pracowników korzystających z urządzeń komputerowych. W przypadku analizowanej przychodni liczba ta wynosi 17. Pozostałe dane wymagane do oszacowania kosztu działań związanych z wdrożeniem i utrzymaniem systemu bezpieczeństwa zestawione są w tabelach 1 i 2.

Tabela 1. Dane dotyczące analizowanej przychodni potrzebne do oszacowania kosztu działań związanych z zarządzaniem bezpieczeństwem informacji

Wskaźnik przyjęć – w_{przyj}	5%
Wskaźnik odejść – $w_{od.}$	5%
Wskaźnik przeniesień – w_{przen}	5%
Wskaźnik wykorzystania urządzeń mobilnych – w_{mob}	20%
Szacunkowa liczba osób spoza organizacji mających dostęp do systemu	0

Źródło: opracowanie własne.

Tabela 2. Dane potrzebne do oszacowania – stawki wynagrodzeń pracowników

Stanowisko	Przybliżona przeciętna stawka godzinna wynagrodzenia brutto [zł]
Pracownik bezpieczeństwa IT	13,63
Administrator IT	13,63
Pracownik działu zarządzania kadrami	20,41
Pracownik organizacji obsługujący komputer (użytkownik)	17,41
Kierownik lub członek zarządu	21,97
Pracownik ochrony	10,66
Pracownik ochrony – strażnik	10,56
Pracownik jednostki budżetowania i kontroli finansów	20,41

Źródło: opracowanie własne na podstawie Rozporządzenia Ministra Zdrowia z dnia 3.03.2016, zmieniające rozporządzenie w sprawie warunków wynagradzania za pracę pracowników podmiotów leczniczych działających w formie jednostki budżetowej (DzU 2016, poz. 305).

Wyniki oszacowań kosztu oraz przewidywane zapotrzebowanie na pracowników bezpieczeństwa przedstawiono w tabelach 3–6.

Tabela 3. Wyniki oszacowania całkowitego kosztu działań związanych z zarządzaniem bezpieczeństwem IT w przychodni, obejmującego koszt działań wszystkich zaangażowanych pracowników

Koszt całkowity [zł]			
Minimalny	Maksymalny	Średni	Przeciętny
53275,73	638195,59	345735,66	80662,92

Źródło: opracowanie własne

Tabela nr 4. Wyniki oszacowania kosztu działań wykonywanych wyłącznie przez pracowników bezpieczeństwa IT

Koszt działań wykonywanych przez pracowników bezpieczeństwa IT [zł]			
Minimalny	Maksymalny	Średni	Przeciętny
9517,83	66473,51	37995,67	25331,36

Źródło: opracowanie własne.

Tabela nr 5. Oszacowana liczba wymaganych godzin pracy pracowników bezpieczeństwa IT

Liczba wymaganych godzin pracy pracowników bezpieczeństwa IT			
Minimalny	Maksymalny	Średni	Przeciętny
698,30	4877,00	2787,65	1858,50

Źródło: opracowanie własne.

Tabela 6. Oszacowane zapotrzebowanie na liczbę wymaganych etatów dla pracowników bezpieczeństwa IT

Liczba wymaganych etatów dla pracowników bezpieczeństwa IT			
Minimalny	Maksymalny	Średni	Przeciętny
0,5	2,5	1,5	1,0

Źródło: opracowanie własne.

Otrzymane oszacowania wskazują, że przeciętny roczny koszt działań związanych z zarządzaniem bezpieczeństwem informatycznym, zapewniających podstawowy, ale wyczerpujący poziomu bezpieczeństwa w analizowanym zakładzie opieki zdrowotnej, wynosi blisko 81 tys. zł. Jest to kwota możliwa do zaakceptowania, jeśli uwzględni się straty, jakie jednostka może ponieść w razie wystąpienia skutecznego ataku na jej system komputerowy. Dodatkowo należy uwzględnić to, że znaczącym komponentem całkowitego rocznego kosztu zarządzania bezpieczeństwem jest koszt związany z ochroną fizyczną zasobów informatycznych przychodni wymagającej ciągłej, 24-godzinnej obecności przynajmniej jednego

strażnika. Koszt ten to 50 356 zł i stanowi aż 62% całkowitego kosztu zarządzania bezpieczeństwem informacji. Należy jednak zauważyć, że zapewnienie fizycznej ochrony zasobów informatycznych przez zatrudnienie pracowników ochrony przekłada się na bezpieczeństwo wszystkich zasobów fizycznych zakładu opieki zdrowotnej, w tym sprzętu medycznego. Można również rozważyć inny scenariusz zapewnienia ochrony fizycznej np. przez zlecenie jej firmie zewnętrznej. Z takiej formy ochrony przychodnia korzysta w chwili obecnej – zainstalowany jest system alarmowy połączony z centralą telefoniczną firmy zajmującej się ochroną osób i mienia, gotowej w krótkim czasie od momentu wystąpienia alarmu dojechać na miejsce. Jeśli tę formę ochrony zasobów informatycznych systemu uzna się za wystarczającą, to całkowity roczny koszt pozostałych działań związanych z zarządzaniem bezpieczeństwem informacji wyniesie niecałe 31 tys. zł.

Wyniki oszacowania potwierdzają również intuicję dotyczącą liczby wymaganych etatów dla pracowników bezpieczeństwa IT. Do zapewnienia bezpieczeństwa IT systemu obejmującego około 20 stanowisk komputerowych, wystarczy zatrudnienie jednego pracownika bezpieczeństwa IT.

6. Podsumowanie i kierunki dalszych badań

W artykule opisano metodę szacowania kosztu działań związanych z zarządzaniem bezpieczeństwem informacji w organizacji oraz przedstawiono studium przypadku jej zastosowania do określenia kosztu w zakładzie opieki zdrowotnej. Metoda pozwala ocenić koszt związany z całościowym procesem zarządzania bezpieczeństwem informatycznym zapewniającym podstawowy poziom ochrony. W ramach prac nad metodą dokonano wyboru systemu kalkulacji kosztów i jego przystosowania do dziedziny problemowej, zaproponowano listę działań związanych z ochroną zasobów informacyjnych, wyspecyfikowano powiązane z nimi zasoby oraz określono podstawowe charakterystyki organizacji kluczowe z punktu widzenia szacowania całkowitego kosztu zarządzania bezpieczeństwem.

Dalsze badania będą obejmowały:

- rozszerzenie zakresu oszacowań o działania związane z zapewnieniem umiarkowanego i wysokiego poziomu bezpieczeństwa według klasyfikacji NIST;
- wzbogacenie metody przez moduł pozwalający określać koszty sprzętu i oprogramowania wykorzystywanego w procesie zarządzania bezpieczeństwem informacji;

- rozwinięcie komplementarnych metod bazujących na innych standardach zarządzania bezpieczeństwem informacji (np. ISO/IEC 27001).

Bibliografia

Cooper R., Kaplan R.S., *Zarządzanie kosztami i efektywnością*, Dom Wydawniczy ABC, Warszawa 2000.

Kaplan R.S., Anderson S.R., Mućko P., Mućko A., *Rachunek kosztów działań sterowany czasem – TDABC Time-Driven Activity-Based Costing: prostsza i bardziej skuteczna droga do większych zysków*, Wydawnictwo Naukowe PWN, Warszawa 2012.

Lusignan R., Steudler O., Allison J., *Managing Cisco Network Security: Building Rock-Solid Networks*, ed. F. Parent. Syngress 2000.

Polski Komitet Normalizacyjny, PN-ISO/IEC 27001:2007, *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*, 2007.

Peltier T.R., *Information Security Policies and Procedures: a Practitioner's Reference*, 2nd ed., Auerbach Publications, Boston 2004.

Purser S., *A Practical Guide to Managing Information Security (Artech House Technology Management Library)*, Artech House, Inc., Norwood 2004.

Ramachandran J., *Designing Security Architecture Solutions*, ed. C. Long C, Wiley 2002.

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 roku, http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/910, Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2015-roku.html (10.09.2017).

Recommended Security Controls for Federal Information Systems and Organizations, National Institute of Standards and Technology (NIST). *NIST SP 800–53 Rev. 3*, U.S. Government Printing Office, Washington 2009.

Standards for Security Categorization of Federal Information and Information Systems, NIST. FIPS PUB 199, *Fips*. 2004;199, 02.2004.

Tipton H.F., Nozaki M.K., *Information Security Management Handbook*, 6th ed., vol. 4, Auerbach Publications, Boston 2010.

* * *

Information Security Cost Estimation Method and its Application in a Health Centre

Abstract

Each year the number of computer attacks on public institutions is increasing. To protect themselves, organisations should invest in effective protection measures. The article presents a method which supports decision-making on these investments by estimating the cost of activities that ensure the appropriate security level. A case study of applying the method to estimate the cost of information security management in a health centre is described.

Keywords: information security, cost estimation, public administration, health care, case study