STUDIA I PRACE
Kolegium Zarządzania i Finansów
ZESZYT NAUKOWY 157

157/2017
s. 89–105

Szkoła Główna Handlowa w Warszawie
Oficyna Wydawnicza SGH
kolegia.sgh.waw.pl

Beata Dratwińska-Kania
Uniwersytet Ekonomiczny w Katowicach

Koszty cyberprzestępczości – perspektywa rachunkowości

Streszczenie

Z uwagi na postępującą informatyzację w różnych aspektach działalności przedsiębiorstwa, określenie, czym dokładnie są cyberprzestrzeń i koszty cyberprzestępczości, jest kluczowe dla późniejszych rozwiązań rachunkowości. Celem artykułu jest wyjaśnienie i analiza problemów rachunkowości związanych z kosztami cyberprzestępczości, w szczególności:

- dokonanie klasyfikacji kosztów cyberprzestępczości, przydatnej z punktu widzenia rachunkowości,
- omówienie zasad ujmowania kosztów cyberprzestępczości w księgach rachunkowych,
- analiza problemów zarządzania kosztami cyberprzestępczości, w szczególności opracowanie etapów wdrożenia procesu zarządzania zmianą w odniesieniu do kosztów cyberprzestępczości.

W wyniku podjętych rozważań zidentyfikowano koszty cyberprzestępczości w klasyfikacji rodzajowej i procesowej, dostosowane do warunków rachunku kosztów działań, który można zastosować do analizy i zarządzania tymi kosztami. Ponadto artykuł porusza problemy rachunkowości zarządczej, związanej z kosztami cyberprzestępczości oraz zarządzania ryzykiem operacyjnym. Zaproponowano schemat (etapy) wdrożenia procesu zarządzania zmianą w odniesieniu do kosztów cyberprzestępczości, posiłkując się zintegrowanym podejściem do zarządzania zmianą, obejmującym nurt systemowy i behawioralny. Metodami badawczymi

są analiza literatury oraz badania ankietowe. Posłużono się także techniką zwaną rejestr cech (ang. *selective listing*, *atribute listing*), zaliczaną jako odmiana techniki Gordona.

Słowa kluczowe: cyberkoszty, koszty cyberprzestępczości, zarządzanie ryzykiem cyberprzestępczości
Kod klasyfikacji JEL: M

1. Wprowadzenie

Koszty cyberprzestępczości to te z kosztów, które zaistniały w cyberprzestrzeni albo powstały w podmiocie gospodarczym w związku z jej istnieniem. Cyberprzestrzeń jest pojęciem definiowanym w dokumentach, opracowaniach naukowych, beletrystyce i regulacjach prawnych, co zostało podsumowane w tabeli 1.

Do pojęć bliskoznacznych, czasem stosowanych zamiennie do cyberprzestrzeni, należą przestrzeń wirtualna, świat wirtualny, rzeczywistość elektroniczna, świat cyfrowy, świat elektroniczny czy nawet wirtualizacja rzeczywistości. Wszystkie z tych zjawisk są tworzone przez człowieka, bo to przecież człowiek tworzy rzeczywistość, czasami nieświadomie. Ponadto charakteryzuje je pewna abstrakcja i potencjalizacja (zgodnie ze *Słownikiem wyrazów obcych* W. Kopalińskiego, „wirtualny" oznacza możliwy, mogący zaistnieć[1]), charakterystyczna dla współczesności, co można poprzeć stwierdzeniem wybitnego polskiego psychiatry A. Kępińskiego, który napisał, że człowiek, aby przetrwać, musi pogodzić dwie przeciwstawne postawy: kosmonauty i artysty[2]. Kosmonauta oczywiście w znaczeniu gotowości i otwartości na nowe we wszechświecie, artysta w kontekście opisu.

Istnieją także poglądy, że rzeczywistość wirtualna to ta, w której właśnie funkcjonujemy, której złożoności do końca jeszcze nie poznaliśmy, którą badają odrębnie różne dyscypliny nauki, takie jak fizyka, chemia, nauki biologiczne i inne, z każdym nowym odkryciem ujawnia się jej piękno i nie przestaje zaskakiwać. Niektórzy za Z. Baumanem uważają, że: „pojęcia, którymi się posługujemy, ukształtowały się w warunkach, które już nie istnieją. Używanie ich ma charakter metaforyczny.

[1] W. Kopaliński, *Słownik wyrazów obcych i zwrotów obcojęzycznych z almanachem*, Wydawnictwo Naukowe PWN, Warszawa 2000.

[2] M. Berdel-Dudzińska, *Pojęcie cyberprzestrzeni we współczesnym polskim porządku prawnym*, http://www.aplikanci.profinfo.pl/gfx/lexisnexis/userfiles/files/Pojecie-cyberprzestrzeni-we-wspolczesnym-polskim-porzadku-prawnym.pdf, dostęp 11.11.2016.

Staramy się uchwycić nowe zjawiska, wtłaczając je w stare ramy"[3]. Bauman wyraża również pogląd, że z socjologicznego punktu widzenia przestrzeń wirtualna jest potężnym narzędziem uniezależniania się nowej globalnej władzy od lokalnych, fizycznych ograniczeń.

Tabela 1. Definicje cyberprzestrzeni

Lp.	Źródło	Definicja
1	W. Gibson, *Burning Chrome, Neuromancer*	„Konsensualna halucynacja doświadczana każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach, przez dzieci nauczane pojęć matematycznych (...) Graficzne odwzorowanie danych pobieranych z banków wszystkich komputerów świata. Niewyobrażalna złożoność... świetlne linie przebiegały bezprzestrzeń umysłu, skupiska i konstelacje danych"*
2	Komisja Europejska, *Słownik pojęć z zakresu społeczeństwa informacyjnego***	Wirtualna przestrzeń, w której krążą elektroniczne dane przetwarzane przez komputery PC z całego świata
3	Ministerstwo Administracji i Cyfryzacji, *Polityka ochrony cyberprzestrzeni Rzeczpospolitej Polskiej****	Przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami
4	*Rządowy Program Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011–2016*****	Cyberprzestrzeń – cyfrowa przestrzeń przetwarzania i wymiany informacji tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami. Cyberprzestrzeń RP – cyberprzestrzeń w obrębie terytoriom państwa Polskiego i w lokalizacjach poza terytorium, gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe)

* Fragment książki w tłumaczeniu P. Cholewy. W. Gibson, *Neuromancer*, Katowice 2009, Książnica, s. 59; cyt. za: J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-fad9287e-d6f2-4713-ad9e-472717378ab4/c/Janusz_Wasilewski.pdf

** Komisja Europejska, *Słownik pojęć z zakresu społeczeństwa informacyjnego*; cyt. za: J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, File:///D:/dokument/Downloads/janusz%20Wasilewski%20(1).pdf, dostęp 11.11.2016.

*** Ministerstwo Administracji i Cyfryzacji, *Polityka ochrony cyberprzestrzeni Rzeczpospolitej Polskiej*, Warszawa 2013. File://D:/dokument/Downloads/POlityka_Ochrony_Cyberprzestrzeni_RP_148x210_wersja_pl.pdf, dostęp 11.11.2016.

**** Rządowy Program Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011–2016, Warszawa 2010, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf

Źródło: opracowanie własne.

[3] *Globalizacja-proces nieodwracalny, rozmowa z prof. Z Baumanem z Leeds University*, http://www.panol.lublin.pl/biul_6/art_610.htm, z lipca 2011, cyt za: http://www.aplikanci.profinfo.pl/gfx/lexisnexis/userfiles/files/Pojecie-cyberprzestrzeni-we-wspolczesnym-polskim-porzadku-prawnym.pdf, dostęp 11.11.2016.

Ponieważ w rachunkowości nie zdefiniowano jednoznacznie pojęcia cyberprzestrzeni, na potrzeby niniejszego opracowania przyjmuje się założenie, że cyberprzestrzeń będzie miała zasięg podmiotowy (metoda podmiotowa jest przyjęta w rachunkowości za obowiązującą, dlatego na potrzeby niniejszego opracowania zawężono zasięg cyberprzestrzeni do podmiotu) i w tym kontekście będzie to cyfrowa przestrzeń danego pomiotu gospodarczego do przetwarzania, prezentowania i wymiany informacji z innymi użytkownikami. Cyberprzestrzeń jest zatem wytworem przedsiębiorstwa, charakteryzuje ją rozległość, złożoność, różnorodność baz danych, zróżnicowany dostęp do danych jej poszczególnych użytkowników (głównie pracowników, ale również użytkowników zewnętrznych) oraz różnorodne powiązania między użytkownikami. Koszty cyberprzestępczości, które są przedmiotem analizy niniejszego opracowania, będą wynikać z funkcjonowania cyberprzestrzeni w podmiocie gospodarczym i poza nim. Analiza zjawiska prowadzona będzie z uwzględnieniem rachunkowości finansowej oraz elementów rachunkowości zarządczej.

2. Uzasadnienie wyboru tematu

Cyberataki i tego typu zagrożenia to coraz popularniejsza forma przestępczości, pochłaniająca coraz więcej środków pieniężnych na działania prewencyjne i usuwanie szkód oraz coraz więcej kosztów podmiotów gospodarczych. Według raportu PWC głównym celem ataków są spółki świadczące usługi finansowe[4], ale zagrożenie dotyczy każdego podmiotu gospodarczego oraz osoby fizycznej.

W Australii ataki dotknęły głównie linii lotniczych, sieci hoteli i firm z sektora usług finansowych. Z raportu CSIS prowadzonego w 2013 r. w Stanach Zjednoczonych wynika, że 3 tysiące firm otrzymało od rządu powiadomienie o ataku hakerskim; większość tych podmiotów prowadzi sprzedaż detaliczną. W Wielkiej Brytanii koszty cyberprzestępstw w tej branży wyniosły 850 mln dolarów[5].

Ponemon Institute podjął próbę oszacowania kosztów, które ponoszą podmioty gospodarcze, będące ofiarami cyberataków. Zgodnie z ich raportem wyciek danych to dla podmiotu koszt bezpośredni średnio 65 euro związany z usunięciem

[4] PWC, *Zarządzanie ryzykiem w cyberprzestrzeni. Kluczowe obserwacje z wyników ankiety „globalny stan bezpieczeństwa informacji 2015"*, www.pwc.pl/bezpieczenstwo-biznesu, dostęp 11.11.2016.

[5] A. Ścibor, *Przeciwdziłanie cyberprzestępczości – raport McAfee i Centrum CSIS*, https://avlab.pl/przeciwdzialanie-cyberprzestepczosci-raport-mcafee-i-centrum-csis, dostęp 11.11.2016.

zagrożenia i jego efektów oraz 125 euro kosztów pośrednich. Koszty ponoszone po wykradnięciu danych, tj. praca helpdesków, wewnętrznych zespołów śledczych, komunikacja wewnętrzna to ponad 1 400 000 euro. Koszty związane z wykrywaniem i eskalacją (audyt, zarządzanie kryzysowe, postępowania sądowe) – ponad 500 000 euro[6]. Powyższe fakty świadczą o narastającym problemie powstawania kosztów cyberprzestępczości oraz przenoszeniu przestępczości do cyberprzestrzeni. Według prognoz firmy analitycznej Cybersecurity Ventures liczba danych, które będą musiały zostać objęte cyberochroną, wzrośnie pięćdziesięciokrotnie. Koszty cyberprzestępczości wzrosną z 3 bln dolarów w 2016 r. do 6 bln dolarów w 2021 r.[7]. Szacuje się, że koszty cyberprzestępczości w 2013 r. w USA wynosiły 38 mld USD, w Europie 12 mld USD; 38% spośród nich to następstwa oszustw[8].

W celu potwierdzenia istotności podejmowanych rozważań, w 2017 r. autorka podjęła się zbadania 50 studentów Uniwersytetu Ekonomicznego w Katowicach. Spośród osób objętych badaniem prawie 90% zetknęło się z cyberprzestępczością, 30% poniosło osobiście koszty, wynikające z przestępstw w cyberprzestrzeni, 100% ankietowanych uważa problem cyberprzestępczości za istotny, prawie 60% ankietowanych obawia się zagrożeń w cyberprzestrzeni.

Według raportu Center for Strategic and International Studies (CSIS) zatytułowanego „Net Losses – Estimating the Global Cost of Cybercrime" cyberprzestępczość wpływa negatywnie na innowacje, krajowe rynki, handel, konkurencyjność oraz wzrost gospodarczy. Szczególną szkodę wyrządza własności intelektualnej[9].

Na świecie podejmowane są różnorodne inicjatywy na rzecz zwiększenia bezpieczeństwa w sieci. W Polsce od 2008 r. powołany został CERT.GOV.PL (ang. Computer Emergency Response Team) – Rządowy Zespół Reagowania na Incydenty Komputerowe, którego zadaniem jest zapewnianie i rozwijanie zdolności jednostek organizacyjnych administracji publicznej Rzeczypospolitej Polskiej do ochrony przed cyberzagrożeniami[10].

---

[6] *Bezpieczeństwo danych: jak nie dać się cyberprzestępcy?*, http://www.egospodarka.pl/127088, Bezpieczenstwo-danych-jak-nie-dac-się-cyberprzestepcy,1,12,1.html, dostęp 11.11.2016.

[7] M. Duszczyk, *Koszty cyberprzestępczości podwoją się do 2021 roku*, http://www.rp.pl/Telekomunikacja-i-IT/309309935-Koszty-cyberprzestępczości-podwoja-sie-do-2021-roku.html, dostęp 11.11.2016.

[8] M. Czyżak, *Cyberprzestępczość a rozwój społeczeństwa informacyjnego*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług" 2015, nr 117, s. 665–673.

[9] J. Michalczyk, *Koszty cyberprzestępczości*, http://www.it-professional.pl/archiwum/art,5047, koszty-cyberprzestepczosci.html, dostęp 11.11.2016.

[10] J. Żuk, M. Żuk, *Zagrożenie w cyberprzestrzeni a bezpieczeństwo jednostki*, „Rozprawy społeczne" 2016, t. 10, nr 3, s. 71–77.

Powyższe informacje potwierdzają wagę i istotność problemów cyberprzestępczości. W odniesieniu do rachunkowości przedsiębiorstw te kwestie nie stały się jeszcze przedmiotem regulacji prawnych, praktyka podmiotów gospodarczych sprowadza się najczęściej do standardowego ujęcia kosztów *ex post* albo ujmowania programów typu *security*. Dodatkowym argumentem przemawiającym za poparciem wszechstronnych inicjatyw, wobec których rachunkowość się nie izoluje (o czym świadczy podjęcie takiego odważnego tematu na Forum Rachunkowości), jest dążenie autorki do wszechstronności podejmowanych w rachunkowości problemów informacyjnych, zgodnie z postawą opisaną przez K. Dąbrowskiego. Dąbrowski, w książce zatytułowanej „Trud istnienia" twierdzi, że w wielu naukach empirycznych o wyodrębnionym zakresie i określonych metodach badawczych spotykamy dwa odrębne typy postaw uczonych. Jedni, dążąc do głębszego rozumienia zasadniczych problemów nauki, szukają rozwiązań zarówno w wąskim zakresie danej dyscypliny, jak i poza nim; drudzy, aby zachować niezależność swoich metod, aby się „nie rozpraszać" nie wychodzą poza zakres swej specjalności[11].

3. Pojęcie kosztów cyberprzestępczości i ich ujęcie księgowe

Koszty cyberprzestępczości są związane z realizacją zagrożeń występujących w cyberprzestrzeni, które zostały opisane w literaturze przedmiotu. Najdokładniejszy katalog zagrożeń zawiera CERT.GOV.pl, który to zaprezentowano w tabeli 2.

Zdaniem autorki, dla rachunkowości przydatniejszy będzie przedstawiony poniżej podział kosztów cyberprzestępczości na cztery podstawowe grupy:

1) koszty związane z kradzieżą lub wyłudzeniem poufnych informacji, w celu ich wykorzystania na szkodę podmiotu gospodarczego; powinny być zaliczane do pozostałej działalności operacyjnej (inne pozostałe koszty operacyjne) i prezentowane w rachunku zysków i strat (sprawozdaniu z całkowitych dochodów) w wyniku z działalności operacyjnej;
2) koszty związane z niszczeniem, uszkodzeniem mienia oraz informacji – te również zaliczane powinny być do działalności pozostałej operacyjnej i prezentowane w rachunku zysków i strat (sprawozdaniu z całkowitych dochodów) w wyniku

[11] M. Berdel-Dudzińska, *Pojęcie*..., op.cit.

z działalności operacyjnej (nieplanowe odpisy umorzeniowe lub inne pozostałe koszty operacyjne);

3) koszty procesów sądowych związane z cyberprzestępczością – pozostałe koszty operacyjne lub rozwiązanie rezerwy / biernych rozliczeń międzyokresowych kosztów;
4) koszty podjętych działań ochraniających przed cyberprzestępczością – jeżeli dotyczą ochrony przed ryzykiem operacyjnym, to koszty podstawowej działalności operacyjnej, w szczególnych przypadkach mogą być również w formie czynnych rozliczeń międzyokresowych kosztów.

Tabela 2. Katalog zagrożeń według CERT.GOV.pl

<table>
<tr><td colspan="2">Zagrożenia</td><td colspan="5">Podatności</td></tr>
<tr><td rowspan="8">Działania celowe</td><td>Oprogramowanie złośliwe</td><td>Wirus</td><td>Robak sieciowy</td><td>Koń trojański</td><td>Dialer</td><td>Klient botnetu</td></tr>
<tr><td>Przełamanie zabezpieczeń</td><td>Nieuprawnione logowanie</td><td colspan="2">Włamanie na konto / ataki sieciowe</td><td colspan="2">Włamanie do aplikacji</td></tr>
<tr><td>Publikacje w sieci internet</td><td>Treści obraźliwe</td><td>Pomawianie/ Zniesławienie</td><td colspan="2">Naruszenie praw autorskich</td><td>Dezinformacja</td></tr>
<tr><td>Gromadzenie informacji</td><td>Skanowanie</td><td>Podsłuch</td><td>Inżynieria społeczna</td><td>Szpiegostwo</td><td>SPAM</td></tr>
<tr><td rowspan="3">Sabotaż komputerowy</td><td colspan="2">Nieuprawniona zmiana informacji</td><td colspan="3">Nieuprawniony dostęp lub nieuprawnione wykorzystanie informacji</td></tr>
<tr><td colspan="2">Atak odmowy dostępu (np. DDoS, DOS)</td><td colspan="3">Skasowanie danych</td></tr>
<tr><td colspan="2">Wykorzystanie podatności w urządzeniach</td><td colspan="3">Wykorzystanie podatności aplikacji</td></tr>
<tr><td>Czynnik ludzki</td><td colspan="2">Naruszenie procedur bezpieczeństwa</td><td colspan="3">Naruszenie obowiązujących przepisów prawnych</td></tr>
<tr><td>Cyberterroryzm</td><td colspan="5">Przestępstwa o charakterze terrorystycznym popełnione w cyberprzestrzeni</td></tr>
<tr><td rowspan="2">Działania niecelowe</td><td>Wypadki i zdarzenia losowe</td><td>Awarie sprzętowe</td><td>Awarie łącza</td><td colspan="3">Awarie (błędy oprogramowania)</td></tr>
<tr><td>Czynnik ludzki</td><td>Naruszenie procedur</td><td>Zaniedbanie</td><td>Błędna konfiguracja urządzenia</td><td>Brak wiedzy</td><td>Naruszenie praw autorskich</td></tr>
</table>

Źródło: http://www.cert.gov.pl

Koszty związane z kradzieżą lub wyłudzeniem poufnych informacji, w celu ich wykorzystania na szkodę podmiotu gospodarczego, to m.in.:

- kradzieże tożsamości, danych pracownika,
- incydenty obraźliwych i nielegalnych treści dotyczące pracowników lub podmiotu gospodarczego,
- przełamanie zabezpieczeń dostępu wewnątrz systemu,
- ataki socjotechniczne, np. phishing, wyłudzanie informacji przez podszywanie się pod osobę godną zaufania albo fikcyjną instytucję i oszustwa z tym związane,
- hacking komputerowy – ominięcie zabezpieczeń systemowych i uzyskanie nieautoryzowanego dostępu do informacji podmiotu gospodarczego,
- podsłuch komputerowy – nieuprawnione przechwycenie wszelkich informacji podmiotu gospodarczego, znajdujących się w cyberprzestrzeni.

Koszty związane z niszczeniem, uszkodzeniem mienia oraz informacji to m.in.:

- bezprawne niszczenie informacji, jej uszkadzanie, usuwanie lub zmiana treści informacji, np. ataki z użyciem szkodliwego oprogramowania wirusowego,
- niszczenie sprzętu i oprogramowania,
- wprowadzenie kodu złośliwego z sieci LAN lub WAN, które spowoduje np. brak aktualizacji oprogramowania,
- blokowanie dostępu do usług (mail bomb, DoS, DDoS),
- blokowanie dostępu do istotnych informacji, skierowanych do upoważnionych w podmiocie gospodarczym osób,
- zakłócenie automatycznego przetwarzania informacji,
- sabotaż komputerowy – zakłócenia lub paraliżowanie funkcjonowania systemu informacyjnego w podmiocie gospodarczym.

Określenie wartości wymienionych kosztów cyberprzestępczości nie jest prostym zadaniem. Niektóre z nich są oczywiste do oszacowania, np. koszty zniszczenia sprzętu elektronicznego lub oprogramowania, koszty utraconych zasobów pieniężnych – w wartości wynikającej z ksiąg rachunkowych, koszty procesów sądowych – w wartości nominalnej. Inne koszty cyberprzestępczości należy szacować racjonalnie, są to np. koszty blokowanych dostępów do usług, zakłócenia w przetwarzaniu informacji i inne – tu wyraźnie musi być oszacowana szkoda, która powstała w wyniku cyberprzestępczości, często są to koszty zasądzone w drodze sądowej lub przyjęte w ramach zadośćuczynienia za szkodę – w sytuacji polubownego rozwiązania sporu.

Warto zaznaczyć, że na koszty związane z cyberprzestępczością powinna być, zdaniem autorki, tworzona rezerwa, bierne rozliczenia międzyokresowe kosztów

(gdy prawdopodobieństwo zaistnienia kosztów jest większe), ewentualnie czynne rozliczenia międzyokresowe kosztów w przypadku poniesionych kosztów ochrony przed cyberprzestępczością, choć nie ma wyraźnych wskazań w tym zakresie w regulacjach rachunkowości. Podobnie jak nie ma wskazania tej grupy kosztów w wyliczanych w ustawie o rachunkowości pozycjach pozostałych kosztów operacyjnych, choć są wyliczone koszty dochodzone na drodze sądowej.

4. Koszty cyberprzestępczości jako element zarządzania

Rozpatrując funkcjonalną systematykę kosztów cyberprzestępczości, dostosowaną do potrzeb zarządzania procesowego, należy rozróżnić dwie podstawowe grupy kosztów, związane z wykonywanymi procesami ochronnymi i zarządczymi. Pierwszą grupę stanowią koszty zapobiegania cyberatakom i ochrony przed nimi, powstające na skutek podejmowania takich właśnie procesów, które zaliczyć można do procesu zarządzania ryzykiem operacyjnym. Drugą grupę kosztów funkcjonalnych stanowią koszty zarządzania, głównie zarządzania zmianą lub przez zmianę, związane identyfikacją i usuwaniem skutków cyberataków.

Koszty identyfikacji i usuwania skutków cyberataków to w szczególności narzędzia i systemy do wykrywania włamań, przechowywania danych o użytkownikach oraz monitorowania ich zachowań, narzędzia wykrywania włamań, złośliwych kodów i innych zagrożeń, koszty likwidacji konsekwencji cyberataku oraz doprowadzenia cyberprzestrzeni przedsiębiorstwa do stanu bezpiecznego. Są to pozycje kosztów odpowiadające zadaniom zarządczym, a więc związane z zachodzącymi procesami, wprowadzanymi w życie zarówno przed cyberatakiem, jak i *ex post*. Na wyróżnienie w tej grupie zasługują koszty ubezpieczeń od następstw cyberataków, które stają się coraz popularniejsze, zwłaszcza w podmiotach finansowych, z sektora telekomunikacyjnego i produkcji przemysłowej i które mają stanowić element strategii zarządzania ryzykiem. W Stanach Zjednoczonych SEC OCIE wydał wytyczne, aby podmioty z sektora finansowego zawierały ubezpieczenia przed cyberyzykiem[12]. Podejmowane aktywności z zakresu rachunkowości zarządczej, generujące koszty tej grupy, to działania legislacyjno-regulujące w postaci tworzenia instrukcji i zarządzeń, działania proceduralno-organizacyjne, edukacyjne oraz działania techniczne. Ze względu na stale zmieniające się zagrożenia i wymagania

[12] PWC, *Zarządzanie*..., op.cit.

biznesu, działania zarządcze często wyprowadzane są z modelu zarządzania zmianą lub zarządzania przez zmianę, procesu który łączy ze sobą elementy składowe teorii zarządzania, metod i technik organizowania oraz wiedzy socjologicznej, psychologicznej, ekonomicznej i technicznej[13]. Należy jednak pamiętać, że zmianami nie da się w pełny sposób zarządzać, można je jedynie wyprzedzać, antycypować oraz naprawiać konsekwencje[14]. Dlatego centralne miejsce w ochronie przed cyberatakami mają działania z zakresu zarządzania ryzykiem, z którymi związana jest kolejna grupa kosztów cyberprzestępczości z systematyki funkcjonalnej.

Koszty zapobiegania i ochrony przed ryzykiem to grupa kosztów ponoszonych *ex ante*, przed potencjalnym cyberatakiem; stanowi ukoronowanie działań zarządczych związanych z cyberprzestępczością. Zaliczamy do nich m.in. koszty szkoleń pracowników, koszty zabezpieczeń kontroli dostępu, koszty wprowadzania instrumentów zapobiegających przed cyberatakami, takich jak szyfrowanie wiadomości e-mail, systemy zapobiegania włamaniom i utracie danych oraz niszczeniu sprzętu elektronicznego i oprogramowania. W ustanowieniu własnej procedury w tym zakresie można posiłkować się m.in. *Metodyką zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych*[15]. Zgodnie z tym dokumentem zarządzanie ryzykiem cyberprzestrzeni odbywa się według modelu przedstawionego na rysunku 1.

W procedurze zarządzania ryzykiem rozróżniamy przedstawione niżej elementy[16].

1. Identyfikowanie ryzyka w poszczególnych kategoriach zagrożeń.
2. Analiza ryzyka, na którą składają się:
   - szacowanie następstw,
   - szacowanie prawdopodobieństwa incydentu,
   - określenie poziomu ryzyka.
3. Ocena ryzyka, polegająca na porównaniu wyznaczonych poziomów ryzyka z ryzykiem akceptowalnym przyjętym dla danej kategorii aktywności.

---

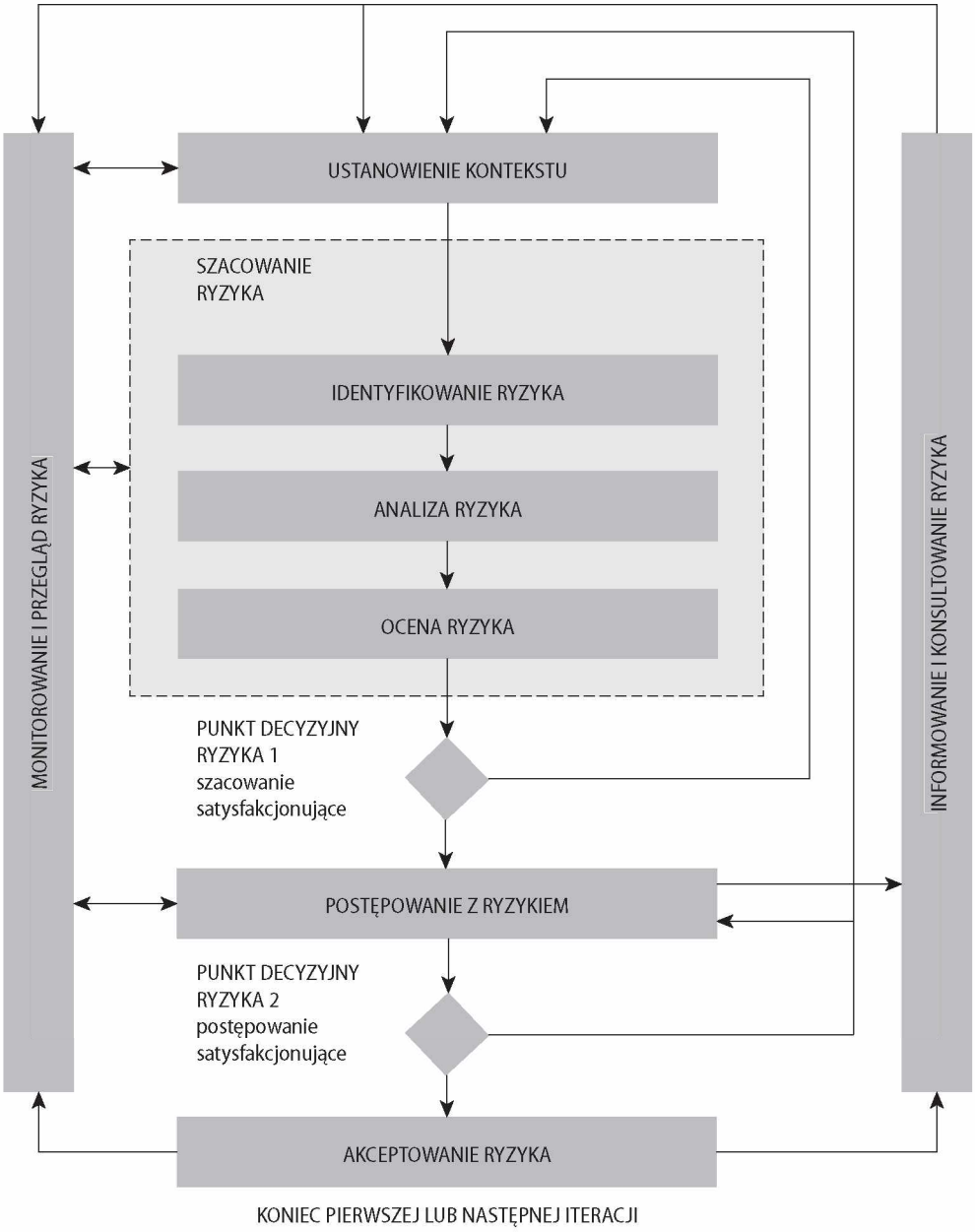
[13] M. Bratnicki, *Zarządzanie zmianami w przedsiębiorstwie*, Wydawnictwo A.E. w Katowicach, Katowice 1998, s. 9.

[14] P.F. Drucker, *Zarządzanie XXI wieku – wyzwania*, Wydawnictwo MT Biznes, Warszawa 2009, s. 83.

[15] *Metodyka zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych*, Warszawa 2015, Krmc.mc.gov.pl/.../MetodykaZarządzaniaRyzykiemCRP2015v18ZZKR

[16] Ibidem.

Rysunek 1. Model zarządzania ryzykiem cyberprzestępczości



Źródło: *Metodyka zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych*, Krmc.mc.gov.pl/…/MetodykaZarządzaniaRyzykiemCRP2015v18ZZKR

4. Postępowanie z ryzykiem, które może polegać na:
   - zastosowaniu zabezpieczenia,
   - unikaniu ryzyka,
   - przeniesieniu ryzyka,
   - akceptacji ryzyka.
5. Informowanie o ryzyku – rejestry ryzyka, raporty.
6. Dokumenty i zapisy.
7. Raportowanie i terminy działań w zarządzaniu ryzykiem.

Rządy wielu państw podejmują działania informujące i zabezpieczające, polegające na gromadzeniu i publikowaniu danych dotyczących cyberprzestępczości, informują o możliwościach ochrony, formułują własną politykę cyberprzestrzeni oraz metodyki zarządzania ryzykiem cyberprzestępczości. Przedsiębiorstwa korzystające z rządowej ochrony cyberprzestrzeni najczęściej stosują w ramach narzędzi zarządzania ubezpieczenie lub ochronę ze strony specjalistycznej firmy przed cyberatakami, samodzielnie zaś najczęściej stosują strategię koncentracji na najbardziej wartościowych aktywach oraz największych dla nich zagrożeniach. Wśród respondentów badania przeprowadzonego przez PWC 80% deklaruje, że polityka bezpieczeństwa spółki jest dobrze dostosowana do celów biznesowych. W Polsce klasyfikację wartości biznesowej danych dokonuje 36% badanych, 60% badanych przeprowadziło jakąś formę zarządzania aktywami, 34% respondentów badania PWC nie kieruje wydatków na bezpieczeństwo do najbardziej zyskownych pionów działalności. Do tego należy dodać, że światowe wydatki na bezpieczeństwo w ostatnich kilku latach nie przekroczyły 4% całego budżetu przeznaczonego na informatykę[17].

Najbardziej pasującym procesem zarządczym związanym z cyberprzestępczością jest proces zarządzania zmianą, który dzięki złożoności oraz etapowości w czasie, zmierza w ogólnym rozrachunku do osiągnięcia postawionego na początku celu ogólnego. Wskazaniem do wprowadzenia zmian jest zarówno otoczenie, względem którego przedsiębiorstwo powinno mieć określoną politykę działania, jak i przedsiębiorstwo, w którym każdy potencjalnie jest obciążony zmianą. Pierwszym krokiem jest przygotowanie ludzi i przedsiębiorstwa do zmian, drugim krokiem jest sama zmiana, trzecim – konsolidacja zmian w systemie[18]. Istnieje wiele propozycji autorów w zakresie faz (etapów) zarządzania zmianą. W opracowaniu posiłkowano

[17] PWC, *Zarządzanie...*, op.cit.

[18] J. Furman, M. Kuczyńska-Chałada, *Change Management in Lean Enterprise*, „Economics and Management" 2016, nr 2, s. 24–31.

się propozycją R. Wendta[19], którą dostosowano do zarządzania kosztami cyberprzestępczości. Należy także zaznaczyć, że zmiana może być dokonywana *ex post*, po zaistnieniu incydentu w cyberprzestrzeni oraz usunięciu jego skutków, ale może być również przeprowadzona *ex ante*, w drodze partycypacji potencjalnych zagrożeń. Oba sposoby wprowadzania zmian mają charakter udoskonalający metodykę postępowania z cyberprzestępczością, jednak ponieważ zalecany i preferowany jest sposób drugi, ten zostanie poddany dalszemu wyjaśnieniu. W rozpatrywaniu tego zagadnienia stosować należy nurt zintegrowany zarządzania zmianą, łączący w sobie elementy nurtu systemowego oraz behawioralnego[20].

Proponuje się następujące etapy (fazy) procesu zarządzania zmianą w odniesieniu do kosztów cyberprzestępczości:

1) określenie krytycznych elementów struktury cyberprzestrzeni (nurt systemowy) oraz zachowań pracowniczych (nurt behawioralny), wystawionych na ryzyko operacyjne związane z kosztami cyberprzestępczości[21];
2) określenie stopnia zagrożenia kosztami cyberprzestępczości i decyzja o podjęciu lub nie działań ochronnych przed cyberprzestępczością – metody wykorzystane w szacunkach ryzyka operacyjnego;
3) przygotowanie się do wdrożenia zmiany; etap ten obejmuje projektowanie zmian, analizę krytycznych elementów cyberprzestrzeni od kątem reakcji na zmianę – w warunkach cyberataku, monitorowanie zachowań pracowniczych i ich przekonania do zmiany; zmiana najczęściej obejmuje wprowadzenie działań prewencyjnych i monitorujących w krytycznych elementach strukturalnych, celem odstraszenia potencjalnych cyberprzestępców, badanie funkcjonowania kodów dostępu, destabilizację *status quo* i przeszkolenie pracowników z zakresie pożądanych zachowań, badanie możliwości i kosztów podjęcia środków ochronnych oraz reakcji w sytuacji zagrożenia cyberatakiem, a także wybór właściwego momentu i oczekiwanie na realizację zmiany;
4) realizacja zmiany; wprowadzenie projektowanych instrumentów w życie;
5) wzmocnienie wdrożonych zmian;

[19] R. Wendt, *Zarządzanie zmianą w polskiej firmie*, Dom Wydawniczy Zachorek, Warszawa 2010, s. 41–82.

[20] A. Zarębska, *Zmiany organizacyjne w przedsiębiorstwie. Teoria i praktyka*, Difin, Warszawa 2002, s. 35–73.

[21] A. Sujova, K. Marcinekova, *The Assignment of Starting Points within Management of Change*, „Zeszyty Naukowe Wyższej Szkoły Humanitas: Zarządzanie" 2016, nr 4, s. 367–376.

6) synchronizacja i kompatybilność działań między poszczególnymi obszarami, w rachunkowości właściwe informacje zwrotne, pozwalające dostosować poziom rezerw do rzeczywistego zagrożenia cyberatakiem.

Zaznaczyć należy, że proces zarządzania zmianą należy projektować w szczegółach wciąż na nowo, dostosowując się do wykonywanych aktywności w cyberprzestrzeni oraz przedsięwziętych instrumentów. Trzymanie się proponowanego schematu ułatwia wdrożenie zmiany i pozwala na zachowanie powtarzalności zadań w warunkach zmienności.

5. Podsumowanie

Koszty cyberprzestępczości oraz zarządzanie ryzykiem cyberprzestępczości stanowią nową kategorię w systemie rachunkowości w zakresie jej ujmowania i sprawozdawania, jak również jako istotnej kategorii zarządzania, zwłaszcza w odniesieniu do zarządzania ryzykiem. Ze względu na dość dużą i rosnącą częstotliwość takich incydentów oraz istotne konsekwencje ekonomiczne i finansowe cyberataków, nakłady na eliminację tego typu zagrożeń mogą stać się interesującą kategorią sprawozdawczą, zwłaszcza dla potencjalnych kontrahentów, nawiązujących współpracę z podmiotem gospodarczym. Jak wskazują badania PWC, ataki koncentrują się zwłaszcza na podmiotach finansowych, liniach lotniczych oraz przedsiębiorstwach przemysłowych (a więc podmiotach, z którymi większość łączą jakieś stosunki handlowe); często są to także małe spółki, które mają pełnić funkcję przyczółka do wejścia przez nie do innych podmiotów[22]. W artykule przedstawiono systematykę rodzajową oraz funkcjonalną kosztów cyberprzestępczości, zasady ich ujmowania w księgach rachunkowych i skutki sprawozdawcze. Poruszono także problematykę zarządzania tymi kosztami.

Bibliografia

Wydawnictwa zwarte

1. Bratnicki M., *Zarządzanie zmianami w przedsiębiorstwie*, Wydawnictwo A.E. w Katowicach, Katowice 1998.

[22] PWC, *Zarządzanie...*, op.cit.

2. Drucker P.F., *Zarządzanie XXI wieku – wyzwania*, Wydawnictwo MT Biznes, Warszawa 2009.
3. Kopaliński W., *Słownik wyrazów obcych i zwrotów obcojęzycznych z almanachem*, Wydawnictwo Naukowe PWN, Warszawa 2000.
4. Wendt R., *Zarządzanie zmianą w polskiej firmie*, Dom Wydawniczy Zachorek, Warszawa 2010.
5. Zarębska A., *Zmiany organizacyjne w przedsiębiorstwie. Teoria i praktyka*, Difin, Warszawa 2002.

Artykuły naukowe

1. Czyżak M., *Cyberprzestępczość a rozwój społeczeństwa informacyjnego*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego, Ekonomiczne Problemy Usług" 2015, nr 117.
2. Furman J., Kuczyńska-Chałada M., *Change Management in Lean Enterprise*, „Economics and Mangement" 2016, nr 2.
3. Sujova A., Marcinekova K, *The Assignment of Starting Points within Management of Change*, „Zeszyty Naukowe Wyższej Szkoły Humanitas: Zarządzanie" 2016, nr 4.
4. Żuk J., Żuk M., *Zagrożenie w cyberprzestrzeni a bezpieczeństwo jednostki*, „Rozprawy społeczne" 2016, t. 10, nr 3.

Materiały internetowe

1. Berdel-Dudzińska M., *Pojęcie cyberprzestrzeni we współczesnym polskim porządku prawnym*, http://www.aplikanci.profinfo.pl/gfx/lexisnexis/userfiles/files/Pojecie-cyberprzestrzeni-we-wspolczesnym-polskim-porzadku-prawnym.pdf
2. *Bezpieczeństwo danych: jak nie dać się cyberprzestępcy?*, http://www.egospodarka.pl/127088, Bezpieczenstwo-danych-jak-nie-dac-się-cyberprzestepcy,1,12,1.html
3. Duszczyk M., *Koszty cyberprzestępczości podwoją się do 2021 roku*, http://www.rp.pl/Telekomunikacja-i-IT/309309935-Koszty-cyberprzestępczości-podwoja-sie-do-2021-roku.html
4. Gibson W, *Neuromancer*, tłumacz fragmentu P. Cholewa, Katowice 2009, Książnica, s. 59, cyt. za: J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-fad9287e-d6f2-4713-ad9e-472717378ab4/c/Janusz_Wasilewski.pdf
5. *Globalizacja – proces nieodwracalny, rozmowa z prof. Z Baumanem z Leeds University*, http://www.panol.lublin.pl/biul_6/art_610.htm, z lipca 2011, cyt. za: http://www.aplikanci.profinfo.pl/gfx/lexisnexis/userfiles/files/Pojecie-cyberprzestrzeni-we-wspolczesnym-polskim-porzadku-prawnym.pdf.
6. http://www.cert.gov.pl.

7. Komisja Europejska, *Słownik pojęć z zakresu społeczeństwa informacyjnego*, cyt. za: J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, File:///D:/dokument/Downloads/janusz%20Wasilewski%20(1).pdf
8. *Metodyka zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych*, Warszawa 2015, Krmc.mc.gov.pl/.../MetodykaZarządzaniaRyzykiemCRP2015v18ZZKR
9. Michalczyk J., *Koszty cyberprzestępczości*, http://www.it-professional.pl/archiwum/art,5047, koszty-cyberprzestepczosci.html
10. Ministerstwo Administracji i Cyfryzacji, *Polityka ochrony cyberprzestrzeni Rzeczpospolitej Polskiej*, Warszawa 2013, File://D:/dokument/Downloads/POlityka_Ochrony_Cyberprzestrzeni_RP_148x210_wersja_pl.pdf
11. PWC, *Zarządzanie ryzykiem w cyberprzestrzeni. Kluczowe obserwacje z wyników ankiety „globalny stan bezpieczeństwa informacji 2015"*, www.pwc.pl/bezpieczenstwo-biznesu
12. *Rządowy Program Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011–2016*, Warszawa 2010, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf
13. Ścibor A., *Przeciwdziłanie cyberprzestępczości – raport McAfee i Centrum CSIS*, https://avlab.pl/przeciwdzialanie-cyberprzestepczosci-raport-mcafee-i-centrum-csis

Costs of Cybercrime. Accounting Prospects

Summary

Due to the growing informatisation of different aspects of corporate operation, it is crucial for the future accounting solutions to determine precisely what cybercrime and cybercrime costs are. The article is aimed at the explanation and analysis of accounting problems related to cybercrime, in particular:
- classification of cybercrime costs, useful from the accounting perspective,
- principles of presentation of cybercrime in account books,
- problems of cybercrime costs management, especially drawing up stages of implementation of the change management process in relation to cybercrime costs.

The undertaken study resulted in the identification of cybercrime costs in type and process classification, adjustable to the conditions of management of these costs. Furthermore, the article deals with the problems of managerial accounting connected with cybercrime costs and operational risk management. It presents a scheme (stages) of implementation of the

change management process related to cybercrime, based on the integrated approach to change management including a systemic and behavioural trend. The research method includes the literature analysis and surveys. Another technique used is attribute listing, a variation of the Gordon technique.

Keywords: cybercosts, cybercrime costs, cybercrime cost management