dr Zbigniew Grzywna
Wyższa Szkoła Zarządzania Marketingowego i Języków Obcych, Katowice

Wpływ incydentu na bezpieczeństwo informacji w zarzadzaniu podmiotem

Wprowadzenie

Celem tego artykułu jest ukazanie zagrożeń możliwych do wystąpienia w postaci incydentów, czyli zdarzeń, które swym oddziaływaniem mogą zagrozić funkcjom istnienia podmiotu. Dokonano wcześniej szereg badań, lecz w artykule mogą znaleźć się jedynie jego krótkie podsumowania. Interpretacja pojęć związanych z kryzysem sytuacją kryzysową jest dopasowana do obszarów problematyki poruszonej w niniejszym artykule. Poznawcza i sprawcza kontrola nad coraz liczniejszymi zagrożeniami, które wpływają na poziom bezpieczeństwa informacji to rola specjalistów. W zarządzaniu podmiotami często występuje potoczne określenie kryzys w firmie. To sygnał, przyczyna oraz potrzeba obiektywnego poznawania uwarunkowań powodujących kryzys, czy sytuacje kryzysowe. Postępowanie badawcze pozwalające gromadzić tą wiedzę, wymaga myślenia kreatywnego i podejścia twórczego. Wówczas możliwe będą działania nastawione na innowacyjne rozwiązywanie problemów dotyczących powstawania czy przeciwdziałania powstawaniu wszelkim sytuacjom o znamionach kryzysu. Konieczna więc jest wnikliwa obserwacja stanu przygotowań podmiotu do możliwości wystąpienia zawirowań mogących zakończyć się upadkiem.

Szereg występujących czynników umacniających pozycję, nasuwa potrzebę zadania pytań dotyczących między innymi co mogłoby pozytywnie wpłynąć na poprawę bezpieczeństwa podmiotu, co poprawić w relacjach interpersonalnych, jak poprawić efektywność. W oparciu o aktualne ustawodawstwo krajowe i unijne dokonano sygnalnego ukazania zakresów odpowiedzialności poszczególnych ośrodków decyzyjnych, a także ich obowiązki i kompetencje, wynikające z zapewnienia bezpieczeństwa. W artykule wykorzystano szereg informacji zaczerpniętych z literatury przedmiotu, a także z najaktualniejszego ustawodawstwa (z odsyłaniem do źródeł). Ujęto w nim pozycje zwarte, ar-

ISSN: 1898-4509

tykuły zamieszczone w periodykach. Niejednokrotnie posiłkowano się publikacjami obcojęzycznymi. W badaniach zwrócono uwagę i skoncentrowano się na incydentach, bezpieczeństwie podmiotu i fazach cyklu zarządzania w sytuacjach noszących znamiona kryzysu. Ta sfera dotyczy głównie sposobów postępowania podmiotów, które związane są z zarządzaniem

Celem przeprowadzonych badań było przeanalizowanie uwarunkowań działania podczas wykrycia zagrożenia. W konsekwencji pozwoliło skupić się na incydentach, czyli czymś, co może potencjalnie działać niekorzystnie na podmiot a nawet go zniszczyć czy wyeliminować z rynku.. Wskazuje się w artykule, że ważna też będzie wiedza na temat wszelkich zagrożeń o różnym charakterze czy stopniu oddziaływań oraz pozytywnych i negatywnych aspektach funkcjonowania podmiotu. Przedmiotem badań, w ujęciu ogólnym były zagadnienia dotyczące bezpieczeństwa i wszelkich nawet sygnałów potencjalnych zagrożeń Przede wszystkim chodziło o przygotowanie specjalistów do działań profilaktycznych wpływających na stan stałego funkcjonowania. Pozwoli to gromadzić informacje na przyszłość, wpływając na sposób zachowań w stosunku do współpracowników czy kontrahentów w tym, o wzajemnych relacjach w obszarze współpracy czy współdziałania Tak określony przedmiot badań oznacza, iż analizy badawcze koncentrowały się na poszukiwaniu mechanizmów i czynników warunkujących powstawanie zagrożeń i przeciwstawianie się nim. Zdecydowano, że poszukiwania badawcze dotyczyć będą zagrożeń, które łatwiej eliminować niż skutki, które występują ze zdecydowanie większymi konsekwencjami.

1. Sytuacja kryzysowa a bezpieczeństwo

Kryzys, jako zjawisko złożone i unikalne w swoim przebiegu posiada pewne cechy ogólne, obejmujące kolejne etapy powstania, przesilenia i zakończenia. Można w nim wyróżnić określone fazy procesu, w których zmienia się natężenie zagrożenia:

- Rozpoznanie symptomów,
- Eskalacje i przesilenie,
- Deeskalację zakończoną nowym poziomem stabilizacji.

Aby zilustrować przebieg sytuacji kryzysowej można posłużyć się przykładem awarii zasilania i związany z tym brak dostępu do informacji. Załóżmy, że problem wystąpił w hipotetycznym podmiocie czy przedsiębiorstwie, którego działalność opiera się na świadczeniu usług w oparciu o dostęp do tej informacji (na przykład Panorama Firm).

Jak zostało zapisane w ustawie w wielkim uproszczeniu można powiedzieć że, kryzys i sytuacja kryzysowa jest pewnym odchyleniem od „stanu normalności". Umożliwienie identyfikacji sytuacji kryzysowej wymaga, więc w pierwszej kolejności zdefiniowania tego stanu. Analizując powyższy wykres, stan normalny stanowi granicę, w której krzywa znajduje się w granicach zdarzeń standardowych – funkcjonowania standardowego. Aby zidentyfikować odchylenia, działanie w tym stanie powinno obejmować monitorowanie zidentyfikowanych zagrożeń za pomocą dostępnych środków. W normalnej sytuacji, odchylenia te będą miały akceptowalny poziom, w którym nie istnieje zagrożenie dla działalności przedsiębiorstwa czy podmiotu.

Dobrym przykładem wydaje się być wystąpienie awarii zasilania, spowoduje to, że pojawią się symptomy kryzysu – praca firmy zostanie przerwana. Co istotne, o ile sama awaria może mieć charakter nagły to kryzys z nią związany nie musi mieć tego samego charakteru, w przytoczonej sytuacji możliwe jest rozpoznanie przyczyn oraz źródeł kryzysu, które go wywołują, zanim takowe wystąpią. Warto zauważyć, że możliwe jest skuteczne przeciwdziałanie problemowi na przykład poprzez zapewnienie zapasowego źródła zasilania. Niezbędnym warunkiem do wdrożenia procesu naprawczego jest jednak wczesna identyfikacja możliwości wystąpienia sytuacji kryzysowej. Przeciwnie natomiast, ignorowanie symptomów w momencie, gdy już istnieją może doprowadzić do negatywnych konsekwencji (na przykład bankructwo), a zarządzenie problemem stanie się niemożliwe. Takim działaniem może być traktowanie problemu jako zakłócenia, które „samo się rozwiąże".

Reasumując powyższe rozważania należy zauważyć, że najważniejszym elementem związanym z podejmowaniem decyzji w przebiegu kryzysu i sytuacji kryzysowej jest umiejętność rozpoznania oznak. Wymaga to zidentyfikowania problemów w odniesieniu do:

a) Miejsca powstania – poszukuje się źródeł kryzysu. Istotne jest przy tym, aby odróżnić symptomy kryzysu od jego przyczyn. Symptomy są, bowiem objawem zjawiska a nie jego powodem. Brak dostępu do danych przedsiębiorstwa jest właśnie symptomem a nie źródłem kryzysu.
b) Fazy procesu – analizuje się przebieg kryzysu w czasie. Identyfikacja fazy pozwala na wdrażanie właściwych mechanizmów decyzyjnych. Kryzys dostępności usług będzie tym intensywniejszy im dłużej trwa przerwa.

c) Problemów rozwojowych. Bada się zjawiska, których istnienie ma charakter ogólny i które mogły doprowadzić do zaistnienia przyczyn kryzysu. Zwykle element ten dotyczy fazy deeskalacji a zjawiska te mogą dotyczyć na przykład błędnych decyzji zarządczych.

Symptomy informują, więc o pojawiającym się zagrożeniu. Dla wspomnianego już przypadku awarii zasilania serwera danych będzie to na przykład wzrost ilości skarg od klientów na niedostępność usług przedsiębiorstwa. Zlekceważenie oznak eskaluje sytuację, która zacznie wykraczać poza poziom normalny. Początkowo dla opanowania problemu wystarczające może być reagowanie standardowe, bez wdrażania procedur kryzysowych. Wchodzenie w wyższe obszary sygnalizuje rozwój sytuacji kryzysowej, co w efekcie powinno prowadzić do uruchomienia procedur nadzwyczajnych. Pojawia się konieczność walki z przyczynami i skutkami zagrożenia. Wymaga to przyjęcia strategii obronnej i podjęcia działań naprawczych. Krytycznym czynnikiem jest tu dostępność aktualnych informacji o stanie zagrożenia oraz posiadanych rezerwach czasowych, które zawsze są deficytowe w takiej sytuacji. o ilości dostępnego czasu może decydować na przykład umowa z klientami, gwarantująca określoną dostępność usług. w przypadku usług bankowych mogą to być nawet minuty.

Oprócz zdefiniowana stanu normalnego istotne jest rozróżnienie pomiędzy sytuacją kryzysową a samym kryzysem oraz rozróżnienie rodzaju zjawisk kryzysowych. w przypadku sytuacji kryzysowej opanowanie sytuacji wymaga mniejszych nakładów i jest mniej wymagające, presja czasu jest mniejsza a margines błędu decyzyjnego większy. Przykładowe różnice w zarządzaniu kryzysem a sytuacją kryzysową w zależności od natężenia tych zjawisk. W zależności od rodzaju przedsiębiorstwa czy podmiotu i poziomu jego usług awaria zasilania serwera danych może zarówno wywołać sytuacje kryzysową o niskim natężeniu jak i kryzys, którego natężenie będzie wysokie. Inaczej będzie w przypadku banku internetowego powstrzymanie strat będzie wymagało radykalnych i szybkich decyzji w celu zapewnienia ciągłości działania. Inaczej, dla sklepu, który przyjmuje zamówienia poprzez Internet jako usługa dodatkowa, adaptacja do sytuacji kryzysowej będzie stopniowa i dotycząca jedynie obszaru zamówień internetowych.

Podobnie rozróżnienie rodzaju zjawisk kryzysowych wpływa na sposób postrzegania problemu i podejmowania decyzji. Na przykład dla kryzysów nagłych tempo wprowadzania i wdrażania zmian musi być szybkie, a podejmowane decyzje radykalne. Przykładowy podział zaproponowany przez B. Barczaka i K. Bartusika (2009,

s. 15), przedstawiony w tabeli, w porównaniu z innym obrazuje mechanizmy związane z zarządzaniem kryzysem w zależności od jego typu.

W zależności rodzaju kryzysu oraz podejmowanych decyzji (lub ich braku) natężenie sytuacji kryzysowej zmienia się. w obszarze konfrontacji uwidocznionej na schemacie z każdą chwilą rośnie prawdopodobieństwo podejmowania decyzji wykraczających poza standardowe procedury. Zaczyna pojawiać się konieczność walki z atakującymi przyczynami, ale również skutkami zagrożeń. Wymaga to przyjęcia koncepcji walki z zagrożeniem oraz realizacji działań naprawczych. Niezbędne może być opracowanie planów oraz scenariuszy uwzględniających dostępne środki i zasoby.

Ostatecznie faza eskalacji każdego kryzysu musi się zakończyć prowadząc ostatecznie do przesilenia – opanowania sytuacji lub porażki. Osiągnięcie przesilenia oznacza, że cykl kryzysu wchodzi w fazę deeskalacji. Na tym etapie najbardziej istotne jest usunięcie skutków. W zależności od ich rodzaju konieczne może być podjęcie odmiennych strategii, wymagających odmiennych nakładów finansowych i czasowych.

Tab.1 Kryteria i rodzaje kryzysów

Kryterium	Rodzaj kryzysu
Według tempa przebiegu i czasu trwania	**Kryzys nagły/natychmiastowy** – charakteryzuje go brak czasu na działania, planowanie. Decyzje muszą być intensywne i radykalne. **Kryzys przewlekły** – może trwać miesiącami a nawet latami. Długi okres nie sprzyja podjęciu skutecznych działań i szybkich decyzji w celu opanowania kryzysu. Zmiany są zwykle doraźne i obejmujące wybrane obszary objęte kryzysem.
Według miejsca powstania przyczyn	**Kryzys wewnętrzny** – spowodowany jest czynnikami występującymi wewnątrz. Wpływ decyzji na czynniki wewnętrzne jest duży co może ułatwić zarządzanie. **Kryzys zewnętrzny –** spowodowany jest czynnikami zewnętrznymi, na które zarządzanie nie ma wpływu. Reakcja może obejmować jedynie odpowiedź na zagrożenie.
Według wywołanych skutków	**Kryzys destrukcyjny –** powoduje zniszczenie, na przykład upadek organizacji. Zwykle decyzje podejmowane w obliczu takiego kryzysu są nieskuteczne. **Kryzys twórczy** – doprowadza do dalszego rozwoju. Właściwe podejście decyzyjne i dostrzeżenie szans w kryzysie może być źródłem korzyści z kryzysu.
Według przyczyn, które wywołują kryzys	**Kryzys rzeczywisty** – odnosi się do faktycznych problemów i spowodowany jest różnymi czynnikami. Zarządzanie wymaga zidentyfikowania tych przyczyn. **Kryzys wirtualny** – został sztucznie wytworzony na przykład w celu doprowadzenia do jakiejś zmiany. Przyczyny często mogą być nieuchwytne co utrudnia zarządzanie i zwykle pozwala jedynie na reagowanie.

Źródło: A. Stabryła (2010, s. 15).

Na przykład, jeśli problem w sposób istotny dotknął klientów, to najtrudniejszym do usunięcia skutkiem kryzysu może być utrata reputacji przedsiębiorstwa czy podmiotu, a przypominam że podmiotem może być nawet instytucja państwa. W fazie deeskalacji istotne jest zgromadzenie informacji niezbędnych do lepszego przygotowania na wystąpienie podobnych zjawisk w przyszłości. Niezbędne jest przygotowanie lub aktualizacja koncepcji, scenariuszy i planów walki z zagrożeniami. Szczególnie istotna może tu być analiza problemów rozwojowych, które umożliwiły powstanie sytuacji kryzysowej, po to, aby w nowej fazie stabilizacji przygotowanie do następnego kryzysu i zarządzania jego problemami było lepsze. W omawianym przykładzie awarii zasilania wnioski z kryzysu mogą dotyczyć zapewnienia awaryjnych linii zasilania, lepszej komunikacji z klientami czy też wprowadzenia systemów zapasowego przetwarzania danych.

2. Przedsiębiorstwo lub podmiot w kryzysie

Przytoczony przykład kryzysu wynikającego z wystąpienia awarii zasilania pozwala uzmysłowić czytelnikowi, że podobnie jak w innych dziedzinach życia, również w każdej organizacji a także w przedsiębiorstwie, występują kryzysy związane z różnymi zagadnieniami. Co istotne, kryzysy te mogą dotyczyć wszystkich etapów istnienia. Co więcej, analizując literaturę problematyki zjawisk kryzysowych można zauważyć, że kryzys w przedsiębiorstwie jest postrzegany jako jedna z faz jego rozwoju, a pojawienie się sytuacji kryzysowej stanowi dla organizacji nową sytuację, która jest zarówno zagrożeniem jak i bardzo często szansą, której odpowiednie wykorzystanie może doprowadzić do silniejszego rozwoju.

Jak już wykazano kryzys jako zjawisko ma charakter uniwersalny. Z tego powodu przedstawione ogólne ujęcie procesowe problematyki kryzysu ma takie samo zastosowanie w przedsiębiorstwach jak i innych dziedzinach życia. w odniesieniu do podmiotów czy firm, Grażyna Gierszewska (2003, s. 38) określa kryzys w przedsiębiorstwie jako sytuację bądź stan, w którym wskutek spiętrzenia się trudności zagrożona jest realizacja podstawowych jego funkcji, przy jednoczesnym ograniczeniu zdolności organizacji do zlikwidowania zaistniałych sytuacji lub stanu. Za przyczyny kryzysu uznaje się wszystkie wewnętrzne i zewnętrzne czynniki, które mogą wywoływać stan kryzysowy w układzie, jakim jest przedsiębiorstwo. Kryzys w organizacji wywołuje wiele przyczyn, których zwykle nie można wyodrębnić jako jednej. Mogą to być zarówno źródła istniejące w samej organizacji jak i w jej otoczeniu.

Niezależnie od źródeł kryzysu w pojawiającej się sytuacji kryzysowej towarzyszy najczęściej destabilizacja podmiotu czy przedsiębiorstwa. W koncepcji Elżbiety Urbanowskiej-Sojkin (2010) można wyróżnić cztery fazy rozwoju sytuacji kryzysowej w przedsiębiorstwie:

1. Swoje oddziaływanie objawiają czynniki zarówno wewnętrzne jak i zewnętrzne.
2. Następuje antycypacja kryzysu; podejmowane są działania mające na celu identyfikację problemów i ich przyczyn,
3. W wyniku podjętych działań następuje poprawa sytuacji,
4. Następuje utrwalenie pozytywnych efektów

Według takiej koncepcji, każde przedsiębiorstwo funkcjonuje w określonym otoczeniu, które stanowi zbiór czynników zewnętrznych i wewnętrznych. Otoczenie zewnętrzne złożone jest z makro i mikrootoczenia. Otoczenie to posiada wysoki stopień niepewności i zmienności, co wpływa na warunki funkcjonowania oraz efektywność podmiotów gospodarczych. Makrootoczenie stanowi zespół warunków funkcjonowania przedsiębiorstwa wynikających z tego, że działa ono w określonym kraju i regionie, w danym układzie politycznym, prawnym, systemowym, a nawet w określonej strefie klimatycznej. Stanowi ono zespół szerokich wymiarów i sił, wśród których działa organizacja, a które tworzą ogólny kontekst dla tych działań (Jacek Saranowski, Edward Kirejczyk, 2007, s. 37). Przedsiębiorstwo nie ma wpływu na warunki zewnętrzne. Ich nieprzewidywalność może być przyczyną powstawania sytuacji kryzysowych. Przykładem takiego zdarzenia może być zmiana koniunktury wywołana kryzysem globalnym, co w efekcie może pociągnąć za sobą kryzys przedsiębiorstwa.

Mikrootoczenie natomiast stanowi ogół podmiotów, które poprzez powiązania transakcyjne i oddziaływania konkurencyjne wpływają bezpośrednio lub pośrednio na stan i efekty działalności gospodarczej organizacji. Stanowią one konkretne organizacje lub grupy, które mogą wpływać na przedsiębiorstwo. Mikrootoczenie są to więc klienci, konkurencja, dostawcy, itd.

W przeciwieństwie do makrootoczenia, przedsiębiorca może wpływać na strategię konkurencyjną. Sytuacje kryzysowe, które mogą powstawać na skutek oddziaływań w mikrootoczeniu firmy mogą być na przykład spowodowane niewłaściwą strategią marketingową lub przeinwestowaniem. W największym stopniu za efektywność działalności gospodarczej odpowiadają jednak czynniki wewnętrzne. Czynniki te również mogą mieć wpływ na powstawanie sytuacji kryzysowych, gdyż zwykle wynikają z problemów, bądź błędów w zarządzaniu firmą na wszystkich szczeblach tj. strategicznym, taktycznym oraz

operacyjnym. Przykłady rozróżnienia źródeł często wymienianych w literaturze polskiej, wraz z rozróżnieniem na wewnętrzne i zewnętrzne, przedstawia poniżej tabela.

Tab. 2. Zagrożenia wewnętrzne i zewnętrzne

Wewnętrzne (endogeniczne)	Zewnętrzne (egzogeniczne)
- Niewłaściwa strategia przedsiębiorstwa - Brak kompetencji wewnętrznych - Błędne decyzje finansowe, strategiczne itd. - Zły system motywacyjny - Słaba pozycja rynkowa - Nieprzygotowanie do sytuacji kryzysowej	- Kryzys gospodarczy - Gwałtowne zmiany kosztów (na przykład podatkowych) - Spadek popytu na strategicznym rynku - Ograniczona dostępność finansowania - Czynniki losowe: pożar, susza itd.

Źródło: Opracowanie własne.

Zdaniem autora przytoczone przykłady nie wyczerpują problematyki. O wiele szersze podejście do możliwych źródeł kryzysu zaproponował M. Sułek (2008, s. 23), dostrzegając również inne zdarzenia, które mogą wpłynąć na organizacje. Według niego, możliwość wystąpienia problemów jest ściśle związana z określonymi ryzykami występującymi w konkretnej organizacji oraz stopniem podatności na te zagrożenia. Wśród możliwych ryzyk pojawiają się dodatkowo te związane z informacją i jej przetwarzaniem. Przykładowo bank internetowy będzie bardziej narażony na kradzież pieniędzy z kont swoich klientów (kradzież informacji), niż na fizyczny atak przestępców.

Jako źródła kryzysu wskazać można:

- porwanie zarządu,
- bojkot usługi,
- katastrofa naturalna niszczy główną bazę danych,
- sabotaż,
- kradzież informacji,
- włamanie do systemu komputerowego,
- wyciek szkodliwych materiałów,
- napad na personel,
- atak terrorystyczny,
- katastrofę naturalną niszczą siedzibę,
- zgon głównych udziałowców w katastrofie
- awarią zasilania
- szkodliwą plotkę.

W proponowanych kategoriach mieści się, przytoczony wcześniej jako przykład, kryzys związany z awarią zasilania i brakiem dostępu do danych.

Choć podawane przykłady przyczyn wydają się znacznie różnić, w ujęciu procesowym wywołane przez nie kryzysy mają wspólne cechy. Dzięki temu możliwe jest wdrożenie jednolitych mechanizmów przygotowania na kryzys. Kwestiom związanym z sytuacją kryzysową wywołaną przez zdarzenia informatyczne w przedsiębiorstwach czy podmiotach należy poświęcić wiele uwagi jednak artykuł je jedynie sygnalizuje.

Podsumowanie

Postawiona na wstępie hipoteza została zweryfikowana pozytywnie ukazując ważkość profilaktyki. Przygotowanie do wystąpienia kryzysu i zarządzanie jego skutkami w założeniu pozwala na kontrolowane przesilenie kryzysu, które następuje zanim kryzys osiągnie intensywność zagrażającą egzystencji przedsiębiorstwa. „Uzdrawianie przedsiębiorstwa nie jest [więc] zajmowaniem się bankrutem. Walka z kryzysem to nie podział masy upadłościowej", którą może się stać organizacja przyjmująca bierną postawę wobec kryzysu (Grzywna, 2012, s. 39-40).

Przesilenie kryzysu prowadzi do etapu deeskalacji, będącego interwencją, pokryzysową, którego celem jest wyciągnięcie wniosków zarówno z przyczyn wystąpienia negatywnych zjawisk, jak i analiza przeprowadzonych procesów naprawczych. Niezbędnym elementem są tu zadania związane z przywróceniem normalnego funkcjonowania:

- Powrót operacji do stanu normalnego z działania awaryjnego,
- Powrót do normalnych miejsc prowadzenia działalności,
- Pomiar efektów zarządzana w sytuacji kryzysowej (ocena istotnych czynników, takich jak zasoby finansowe, zdolność kredytowa, jakość, udział w rynku, opinie klientów),
- Analiza skuteczności zastosowanych procedur, mechanizmów, kompetencji, komunikacji.

Na tym etapie następuje również usuwanie skutków oddziaływania kryzysu. w zależności od przyczyn i typu kryzysu procesy te mogą być długotrwałe. Na przykład, jeśli kryzys wymagał zaangażowania rezerw finansowych to ich odbudowa może wymagać pewnego okresu. Całkowite zamknięcie kryzysu nastąpi dopiero wówczas, gdy sytuacja wróci do stanu stabilnego, sprzed wystąpienia kryzysu. Niezbędnym składnikiem zamknięcia jest przygotowanie raportów i sprawozdań, zawierających opis wszystkich zda-

rzeń, działań i wyciągnięte wnioski w sposób, który umożliwi wykorzystanie doświadczeń w przyszłości. Niezbędnym elementem zarządzania sytuacją kryzysową jest, bowiem nauka (*lesons learnt*).

Przedstawione w niniejszym artykule zagadnienia związane z incydentami, bezpieczeństwem, kryzysem w podmiotach i jego przebiegiem w ujęciu ogólnym miały na celu wprowadzenie do problematyki. Zostały zawężone głównie do problemów informatycznych w kolejnych artykułach czy dalszych rozważaniach problemy tego typu zostaną zawarte w kategorii incydentów bezpieczeństwa informacji, które mogą stanowić źródło sytuacji kryzysowych i kryzysów. Zjawiska tego typu mają szczególne znaczenie w nowoczesnych przedsiębiorstwach, które swoją działalność opierają na przetwarzaniu informacji. W niniejszym artykule została wskazana konieczność identyfikowania zagrożeń w określonych obszarach ryzyka działalności gospodarczej a także zostały przedstawione możliwości zarządzania skutkami ich wystąpienia. Problematyka ta wymaga jednak dalszych badań i dyskusji, czego przykładem może być ten artykuł.

Literatura

Barczak B., Bartusik K. (2012): *Istota, uwarunkowania i następstwa kryzysu*, w: (red.) Stabryła A., *Zarządzanie w kryzysie*, Kraków, Wydawnictwo Mfiles.pl

Breński W., Olesiuk A. (2008): *Strategiczne szanse polskiej gospodarki w kontekście globalizacji*, Warszawa, Difin

Gierszewska G. (2003): *Analiza strategiczna przedsiębiorstwa*, Warszawa, PWE

Grzywna Z. (2012): *Bezpieczeństwo i zagrożenia w aglomeracjach*, Katowice, WSZMiJO

ISO/IEC 27001 – Zarządzanie bezpieczeństwem informacji, BSI 2007

ISO/IEC 27035:2011, Information technology, Security techniques – Information security incident managements, BSI 2011

Jurcak V., Olak A., Mika J. (2014): *Bezpieczeństwo w warunkach globalizacji – wybrane zagadnienia*, Ostrowiec Św., WSBiP

Olak A. (2013): *Bezpieczeństwo publiczne w administracji*, [w:] Labuzik M., Dziekański P., Olak A., *Polityka bezpieczeństwa w warunkach integracji europejskiej – zarys problematyki*, Ostrowiec Św., Stowarzyszenie „Nauka, Edukacja, Rozwój"

Olak, A., Krauz, A. (2013): *Zintegrowany system bezpieczeństwa państwa – nowe uwarunkowania*, materiały pokonferencyjne Národná a medzinárodná bezpečnosť 2013: medzinárodná vedecká konferencia, Liptovský Mikuláš, Akadémia ozbrojených síl generála Milana Rastislava Štefánika, CD-ROM

Nogalski B., Macinkiewicz H. (2004.): *Zarządzanie antykryzysowe przedsiębiorstwem*, Warszawa, Centrum Doradztwa i Informacji Difin Sp. z o.o.

Rozporządzenie Rady Ministrów w sprawie *Narodowego Programu Ochrony Infrastruktury Krytycznej* z 30 kwietnia 2010, Dz.U. 2010 nr 83 Poz. 541

Sarnowski J., Kirejczyk E. (2007): *Zarządzanie przedsiębiorstwem turystycznym*, Warszawa, ALMAMER Wyższa Szkoła Ekonomiczna

Sułek M. (2008): *Programowanie gospodarczo-obronne*, Warszawa, Bellona

Toffler A., (2006): *Trzecia Fala*, Poznań, Wydawnictwo Kurpisz

Urbanowska-Sojkin E. (2010): *Informacyjne wspomaganie wyborów strategicznych przedsiębiorstw w warunkach niepewności – antycypacja kryzysów*, „Studia i Prace Kolegium Zarządzania i Finansów" nr 98

Ustawa z 26 kwietnia 2007 r. o *Zarządzaniu Kryzysowym,* Dz.U. 2007 nr 89 poz. 590

Ustawa z 5 sierpnia 2010 r. o *Ochronie Informacji Niejawnych*, Dz.U. 2010 nr 182 poz. 1228

Ustawia z 16 lipca 2004 r. *Prawo telekomunikacyjne* (Dz. U. z 2004 r. Nr 171, poz. 1800) z późniejszymi zmianami

Walas-Trębacz J., Ziarko J. (2011): *Podstawy zarządzania kryzysowego*, część 2, Kraków, Krakowska Akademia im. A. Frycza-Modrzewskiego,

Włodarczyk M., Marjański A.(2009): *Bezpieczeństwo i zarządzanie kryzysowe – aktualne wyzwania*, Łódź, Wydawnictwo Green

Zarządzanie w kryzysie (2010): (red.) Stabryła A., Kraków, Wydawnictwo Mfiles.pl

Zbigniew Grzywna

The influence of incident on entity management

Abstract

The beginning of the 21st century is the period of the intensive development of the Western Civilization changing from industrial epoch based on industry and resources to informative epoch where most important issues are information and knowledge. Because of the change, there are new problems and threats which have not existed before. In the industrial world, we are afraid of physical threats – fires, thefts and sabotage. In the world of information, virtual threats must be added as well. Various occurrences where rules of management are not observed can lead to critical situation or crisis and as a result can ruin a particular subject. What is more, computer-related occurrences must also be mentioned. Different occurrences and information security incidents will be taken into consideration in the article, such as serious threats which can cause crisis in organization if suitable management mechanism was not prepared.

Key words: *critical situation, incydent in information, preparind for threats, information security*