ZASTOSOWANIE SYSTEMÓW INFORMATYCZNYCH DO DOKUMENTOWANIA ZDARZEŃ KRYZYSOWYCH

Dorota WOJTYTO, Wiesław KULMA

Streszczenie: W artykule przedstawiono systemy informatyczne, które wspomagają dokumentowanie zdarzeń kryzysowych, przepływ informacji o zagrożeniach, a także proces zarządzania ryzykiem tymi zdarzeniami. Wśród narzędzi komputerowych, które mogą być wykorzystane w tym celu na uwagę zasługują dwa: program *e-risk* oraz *e-CZK* (elektroniczne Centrum Zarządzania Kryzysowego). W artykule zaprezentowano główne funkcjonalności tych programów oraz przykładowe ich zastosowanie.

Słowa kluczowe: zdarzenia kryzysowe, dokumentowanie, przepływ informacji, wspomaganie komputerowe, *e-CZK*, zarządzanie ryzykiem, *e-risk*, zarządzanie kryzysowe.

1. Wprowadzenie

Otoczenie zewnętrzne przedsiębiorstwa oprócz uwarunkowań społecznych, ekonomicznych, międzynarodowych, prawno-politycznych, technologicznych oraz demograficznych jest determinowane również poprzez występowanie różnego rodzaju zdarzeń kryzysowych, które często występują nagle, niespodziewanie, są nieprzewidywalne lub charakteryzują się wysokim poziomem strat. Sytuacje te mają niebagatelny wpływ na realizowanie celów przedsiębiorstwa. Mogą one spowodować zakłócenia w jego funkcjonowaniu lub całkowicie sparaliżować działalność gospodarczą na danym terenie. Dlatego też istotnym jest identyfikacja, analiza oraz ocena tych zagrożeń w kontekście całościowego funkcjonowania przedsiębiorstwa.

Wśród zdarzeń kryzysowych, które stanowią zagrożenia zewnętrzne dla organizacji można wyróżnić przede wszystkim zagrożenia naturalne, techniczne oraz społeczne [7]. Często też do tego podziału zalicza się zagrożenia militarne. Jednakże w dobie współczesnych problemów bezpieczeństwa znacznie częściej przywiązuje się uwagę do zagrożeń asymetrycznych, głównie działań o podłożu terrorystycznym. Stąd zagrożenia zewnętrzne dla przedsiębiorstwa stanowią jednocześnie zagrożenia bezpieczeństwa państwa. Ich rozmiar, rodzaj, charakterystyka przebiegu, poziom strat oraz czas powstawania i trwania odpowiednio klasyfikuje je jako sytuacje kryzysowe.

Występowanie zagrożeń naturalnych jest podyktowane głównie zmianami klimatycznymi. Ponadto współmiernie postęp cywilizacyjny oraz nasilająca się interwencja człowieka w środowisko przyczyniają się do zaistnienia incydentów, często na coraz szerszą skalę. Zwiększone ryzyko rozprzestrzeniania się zagrożeń naturalnych wynika także ze swobody poruszania się człowieka po świecie. Sprzyja to niejednokrotnie rozwojowi, np. epidemii i jej odmian [11]. Przyczyną powstawania zagrożeń naturalnych są czynniki związane między innymi z ruchami skorupy ziemskiej, przeobrażającym się klimatem oraz oddziaływaniem żywiołów [7]. Źródłem zagrożeń naturalnych są siły przyrody oraz czynniki fizyczne [11]. Do najczęściej występujących zagrożeń kryzysowych zaliczamy: powodzie, huragany, pożary naturalne (np. lasów), trzęsienia ziemi, epidemie, osuwiska, intensywne i długotrwałe opady atmosferyczne, susza, mrozy itp.

Z kolei zagrożenia techniczne są wynikiem działalności gospodarczej człowieka, uwarunkowane, postępem naukowo-technicznym oraz rozwojem cywilizacyjnym społeczeństwa [6]. Podstawowy podział zagrożeń technicznych to: pożary, katastrofy górnicze, budowlane i komunikacyjne, awarie oraz skażenia.

Zagrożenia społeczne to procesy internacjonalizacji, które powodują zagrożenia dla rozmaitych dziedzin funkcjonowania społeczeństwa, państwa, struktur gospodarczych, a ich skutki mają charakter negatywny. Do zagrożeń tych należą: problemy demograficzne, migracje, niepokoje społeczne, przestępczość zorganizowana oraz zagrożenia ekonomiczne.

Na uwagę zasługuje również zjawisko terroryzmu, które w doświadczeniach ubiegłych lat pokazuje, że jest to zagrożenie, które potrafi całkowicie zdominować i sparaliżować funkcjonowanie struktur gospodarczych i administracyjnych. Główne obiekty tych działań to urzędy, budynki użyteczności publicznej, instalacje przemysłowe, środki komunikacyjne, a także obiekty gospodarcze.

Problematykę zagrożeń i sytuacji kryzysowych bezpieczeństwa państwa reguluje *Ustawa o zarządzaniu kryzysowym*. Priorytetowe założenia tego aktu normatywnego wskazują, że zajmowanie się zagrożeniami kryzysowymi polegają przede wszystkim na: zapobieganiu ich powstawania, przygotowaniu się na ich wystąpienie, reagowaniu w przypadku ich zaistnienia oraz odbudowy i powrotu do stanu sprzed sytuacji kryzysowej [9]. Są wobec tego przygotowywane przez administrację państwową plany i działania, które zmierzają do właściwego przewidywania i przygotowania się do nadejścia zagrożenia oraz minimalizowania jego potencjalnych skutków. Ponadto *Ustawa o zarządzaniu kryzysowym* wskazuje na kilka ważnych elementów, które dotyczą sytuacji kryzysowych, a mianowicie [9]: gromadzenie informacji o zagrożeniach, analizę zebranych informacji o nich, identyfikację, analizę oraz ocenę ryzyka zagrożeń, monitorowanie zdarzeń, pełnienie całodobowego dyżuru w celu zapewnienia przepływu informacji, zapewnienie koordynacji polityki informacji organów administracji publicznej w czasie sytuacji kryzysowej, informowanie podmiotów biorących udział w zarządzaniu kryzysowym o potencjalnych zagrożeniach oraz działaniach podjętych przez właściwe organy, dokumentowanie podjętych działań oraz współdziałanie z centrami zarządzania kryzysowego.

Biorąc pod uwagę powyższe założenia wynikające z *Ustawy o zarządzaniu kryzysowym* oraz pogłębiający się rozwój społeczeństwa informacyjnego można stwierdzić, że zastosowanie systemów informatycznych do wspomagania działań związanych z zagrożeniami kryzysowymi to nadrzędny imperatyw. Ułatwiają one bowiem zarówno obsługę zdarzeń kryzysowych, ich dokumentowanie, dystrybucję informacji, proces zarządzania ryzykiem, a jednocześnie są doskonałą bazą danych dla wszystkich osób, które zajmują się tą problematyką.

2. Proces zarządzania ryzykiem zdarzeń kryzysowych z wykorzystaniem programu komputerowego *e-risk*

Zgonie z normą PN-ISO 31000:2012 [5] proces zarządzania ryzykiem zdarzeniami kryzysowymi składa się z kilku etapów: określenia celów i zadań danej organizacji, identyfikacji zagrożeń, analizy ryzyka, oceny ryzyka, reakcji na ryzyko oraz monitorowania i komunikacji. W niniejszej pracy wspomaganie komputerowe procesu zarządzania ryzykiem dotyczy zastosowania programu informatycznego *e-risk*. Jest to narzędzie uniwersalne, które może być zarówno wdrożone w przedsiębiorstwie, jak i w jednostkach administracji samorządowej.

Oprogramowanie ułatwia przeprowadzenie procesu zarządzania ryzykiem na każdym etapie oraz uzyskanie w prosty sposób dostępu do informacji i bazy danych. Jednocześnie jest oparte na wielu standardach zarządzania ryzykiem, w tym COSO II (zintegrowane zarządzanie ryzykiem) czy normie PN-ISO 31000:2012 [4].

Na potrzeby niniejszej pracy przeprowadzono przykładowy proces zarządzania ryzykiem zagrożeń kryzysowych za pomocą aplikacji *e-risk portal*, wersja 4.7.3 na licencji Politechniki Częstochowskiej.

W celu przybliżenia funkcjonalności programu *e-risk* proces zarządzania ryzykiem przeprowadzono dla jednostki samorządowej, dla której jako główny obiekt wybrano Szkołę Podstawową. Jako cel wskazano zapobieganie zagrożeniom zewnętrznym dla organizacji i minimalizowanie ich skutków. Następnie zidentyfikowano trzy zagrożenia (definiowane w programie jako *zdarzenia*): powódź, strajk i pożar. Są to odpowiednio zagrożenia: naturalne, społeczne i techniczne. Analiza ryzyka polegała na określeniu głównych parametrów: prawdopodobieństwa i skutków zagrożeń. Wybrano do tego celu następującą metodyką w skali pięciostopniowej: 1-prawie niemożliwe, 2-mało prawdopodobne, 3-możliwe, 4-prawdopodobne, 5-bardzo możliwe. Podobną skalę wybrano dla trzech rodzajów strat: finansowych, organizacyjnych i wpływających na bezpieczeństwo ludzi, gdzie 1-oznacza stratę nieznaczącą, 2-niewielką, 3-średnią, 4-istotną, 5-katastrofalną. Zasadniczym celem analizy było określenie wartości ryzyka poprzez przemnożenia wartości prawdopodobieństwa i skutków (zgodnie ze wzorem R=PxS, gdzie R- ryzyko, P- prawdopodobieństwo, S-skutki/ straty). Ocena ryzyka polegała na określeniu poziomu ryzyka, według następującej skali: 1-3 oznacza ryzyko małe, 4-12 to ryzyko średnie oraz 15-25 to ryzyko duże. Następnie etap reakcji na ryzyko polegał na określeniu *mechanizmów kontroli* (wybrano: zakup gaśnic, wały przeciwpowodziowe, zbiornik retencyjny, przeglądy techniczne) w stosunku do zidentyfikowanych zagrożeń oraz ocenę skuteczności tych mechanizmów kontroli. Na tym etapie wskazano również sposób postępowania z wyznaczonym poziomem ryzyka.

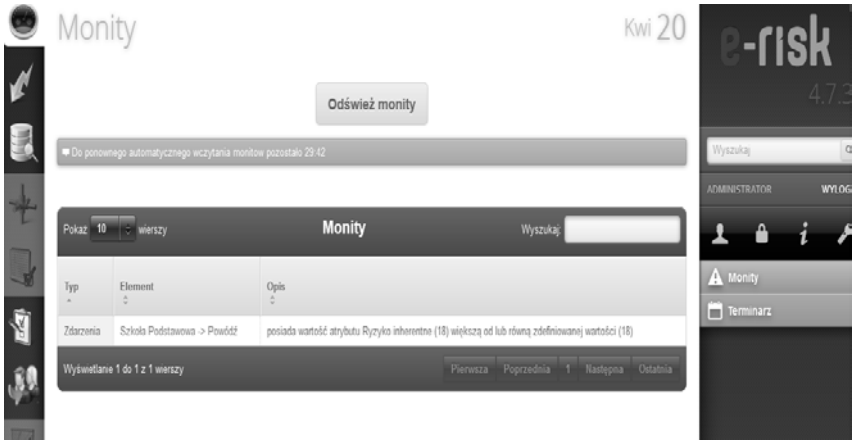
Pierwszą zasadniczą funkcjonalnością programu jest tworzenie dowolnej liczby baz danych, w zależności od potrzeb jednostki. Stąd na potrzeby pracy utworzono bazę danych pod nazwą *Risk*. Po jej wyborze utworzono okno *„Monity”*, które pełni rolę informacyjną o nadchodzących zdarzeniach lub zadaniach do wykonania (rys. 1). W tym miejscu istotne jest również sprecyzowanie terminarza, który przypomina o wykonaniu czynności związanych z zarządzaniem ryzykiem w wyznaczonym czasie. Za pomocą tej funkcji programu realizowany jest etap kontroli procesu zarządzania ryzykiem.

Tworzenie bazy danych ma na celu przygotowanie odpowiednich danych do przeprowadzenia analizy ryzyka. Poprzez kreator formularzy definiuje się elementy, które będą poddawane analizie i ocenie. W pracy przygotowano definicje dla wybranej jednostki samorządowej wraz z badanymi obiektami, przyporządkowano jej występujące lub potencjalne zagrożenia, a następnie mechanizmy kontroli (środki zapobiegawcze) w stosunku do zdefiniowanych zdarzeń (zagrożeń), co przedstawiają rysunki 2−4.

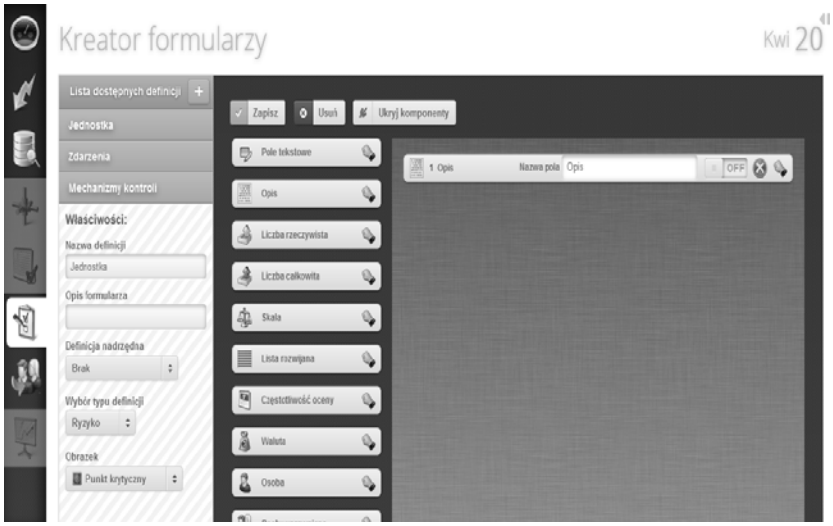
W zależności od definiowanego czynnika przyporządkowuje się mu jego właściwości. Czynnikami tymi są: *jednostka, zdarzenia, mechanizmy kontroli*. Do *właściwości* należą: opis, lista rozwijalna, pole tekstowe, częstotliwość i inne. Dla jednostki samorządowej określa się przede wszystkim jej szczegółowy opis. Z kolei *zdarzenie* posiada takie właściwości, jak: opis zdarzenia, przyczyny wystąpienia oraz częstotliwość oceny. Z listy rozwijalnej określono kategorię zagrożenia (naturalne, techniczne, społeczne), przykładową pięciostopniową skalę prawdopodobieństwa wraz z uzasadnieniem. Następnie określono pięciostopniową skalę skutków finansowych, organizacyjnych i wpływających na zdrowie i

bezpieczeństwo ludzi, także wraz z uzasadnieniem wyboru. Dla *mechanizmów kontroli* określono takie właściwości, jak: opis poszczególnych mechanizmów kontroli, roczna częstotliwość oceny oraz skuteczność mechanizmów kontroli.

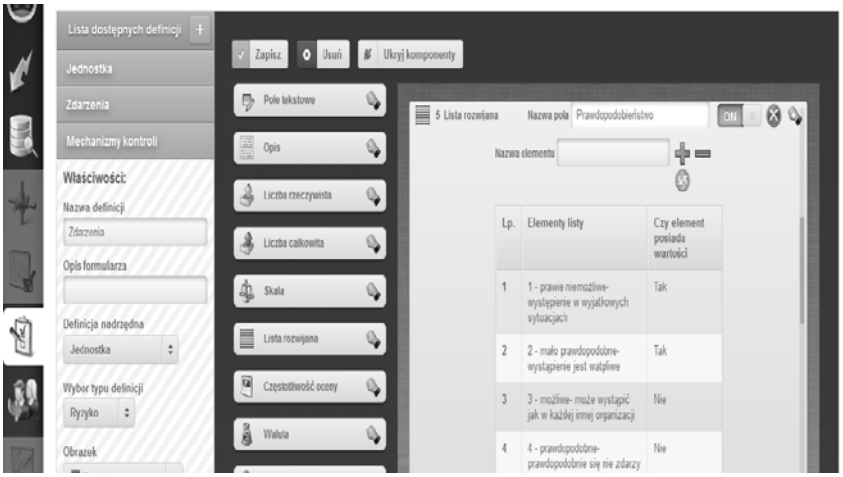
Zarówno dla zdefiniowanych *zdarzeń* (tutaj: powódź, pożar, strajk), jak i *mechanizmów kontroli* (tutaj: zakup gaśnic, wały przeciwpowodziowe, zbiornik retencyjny, przeglądy techniczne) można dokonywać oceny lub edycji w celu uzupełnienia danych (rys. 5.). Natomiast po czynnościach oceny nie można dokonywać zmian, chyba że termin aktualizacji na to wskazuje.



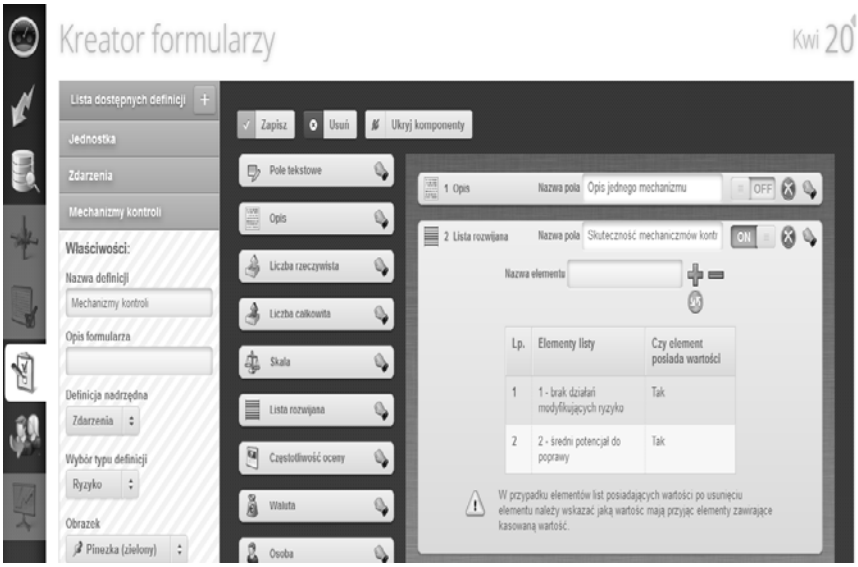
Rys. 1. Okno aplikacji *e-risk* „Monity”
Źródło: opracowanie własne na podstawie użytkowania aplikacji *e-risk.*



Rys. 2. Kreator formularzy dla jednostki w programie *e-risk*
Źródło: opracowanie własne na podstawie użytkowania aplikacji *e-risk.*



Rys. 3. Kreator formularzy dla zdarzenia w programie *e-risk.*
Źródło: opracowanie własne na podstawie użytkowania aplikacji *e-risk.*



Rys. 4. Kreator formularzy dla mechanizmów kontroli w programie *e-risk*
Źródło: opracowanie własne na podstawie użytkowania aplikacji *e-risk.*

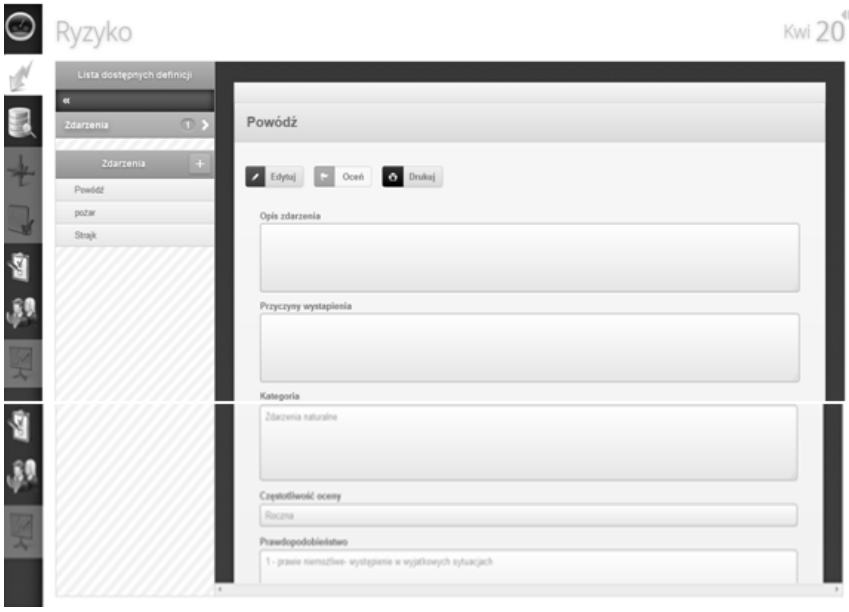
Zasadniczym etapem stosowania aplikacji *e-risk* jest właściwa analiza ryzyka zdefiniowanych *zagrożeń* (rys. 6.). W tym celu na panelu pojawiają się te parametry, które można porównywać, obliczać, a następnie formułować wnioski końcowe. Dlatego też dokonano obliczeń związanych z wartością ryzyka inherentnego i rezydualnego (szczątkowego). Ryzyko inherentne stanowi nic innego, jak iloczyn prawdopodobieństwa i skutków. Termin ten stosuje się, gdy mamy dodatkowo do czynienia z ryzykiem rezydualnym, a zatem takim, które pozostaje na poziomie niekaceptowalnym lub częściowo akceptowalnym po zastosowaniu mechanizmów kontroli i należy go powtórnie zmniejszyć

poprzez odpowiednie działania. Następnie w programie zdefiniowano poszczególne rodzaje reakcji na wyznaczone ryzyko: akceptacja, działanie, unikanie, ograniczanie oraz dzielenie się. W tym celu dokonano opisu planowanych działań w odpowiedzi na to ryzyko. Wybrane elementy definicji zdarzenia są poddawane ocenie za pomocą przycisku *„ON" (ocena).*

Ocena poszczególnych parametrów zagrożeń, jak również analiza ryzyka i całościowy proces zarządzania ryzykiem znajduje się w kompetencjach osoby uprawnionej, czyli administratora pełniącego rolę, np. menedżera ryzyka. Funkcja osoby zajmującej się problematyką ryzyka dotyczy: tworzenia relacji i raportów, określanie terminarzu oraz kontrola monitów, jak również definiowanie parametrów ryzyka dla zagrożeń i ich dalsza analiza.

W pracy zastosowano analizę dla *jednostki, zdarzeń i mechanizmów kontroli*. Analiza polega na wyborze atrybutów spośród dostępnej listy, a następnie poprzez przycisk *generuj* dokonywaniu obliczeń. Wyniki można przedstawić na wykresie (rys.7.). Dane z wykresu można także wygenerować w arkuszu kalkulacyjnym *Excel*. Ponadto istnieje funkcja raportowania poprzez generowanie danych z bazy i publikacja ich w dowolnym formacie.

Wyniki analizy i oceny wybranych zagrożeń przedstawiono za pomocą *macierzy ryzyka*, która uwzględnia dwa parametry dla zdarzenia powodzi: *prawdopodobieństwa i strat związanych z ochroną zdrowia i bezpieczeństwem ludzi.* Macierz obrazuje trzy poziomy ryzyka: niski (kolor zielony), średni (kolor żółty), wysoki (kolor czerwony). Dla analizowanego w niniejszej pracy zagrożenia (tu: powódź), poziom ten jest niski (oznaczony jako numer „1" w macierzy): P=1 i S=1, stąd R=1 (rys. 8.). W związku z tym reakcja na ryzyko w przypadku zidentyfikowanego zagrożenia powodzią będzie polegała jedynie na akceptacji.

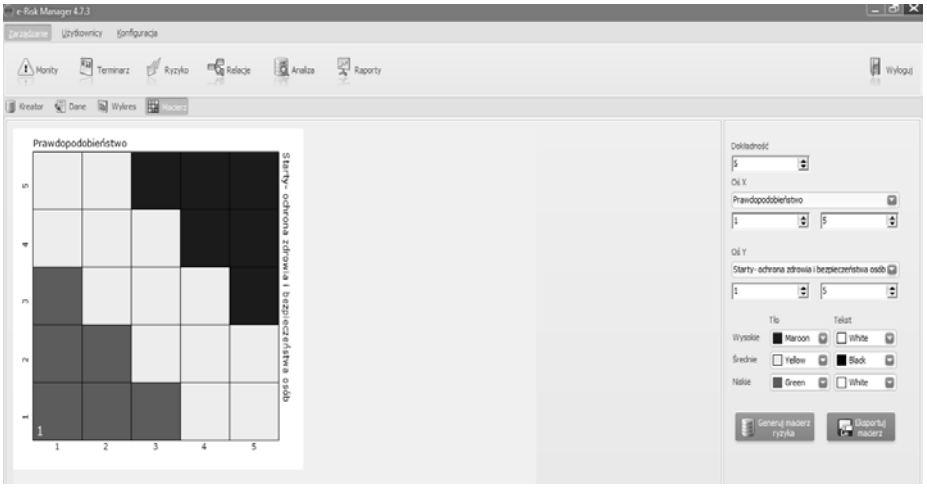


Rys. 5. Definiowanie ryzyka dla zdarzeń w programie *e-risk*
Źródło: opracowanie własne na podstawie użytkowania aplikacji *e-risk.*

Rys. 6. Analiza ryzyka w programie *e-risk*
Źródło: opracowanie własne na podstawie użytkowania aplikacji *e-risk.*

Rys. 7. Tworzenie wykresów w programie *e-risk*
Źródło: opracowanie własne na podstawie użytkowania aplikacji *e-risk.*

Podsumowując rozważania dotyczące zastosowania aplikacji informatycznej *e-risk* do wspomagania procesu zarządzania ryzykiem dla zdarzeń kryzysowych, można stwierdzić, że bez wątpienia posiada ona funkcjonalności, które można wykorzystać dla dowolnej liczby zagrożeń, zarówno dla zagrożeń wewnętrznych organizacji, jak i zewnętrznych (naturalne, techniczne, społeczne). W programie można realizować poszczególne etapy procesu zarządzania ryzykiem, dzięki czemu może być on przeprowadzony w sposób holistyczny.



Rys. 8. Macierz ryzyka w programie *e-risk*
Źródło: opracowanie własne na podstawie użytkowania aplikacji *e-risk.*

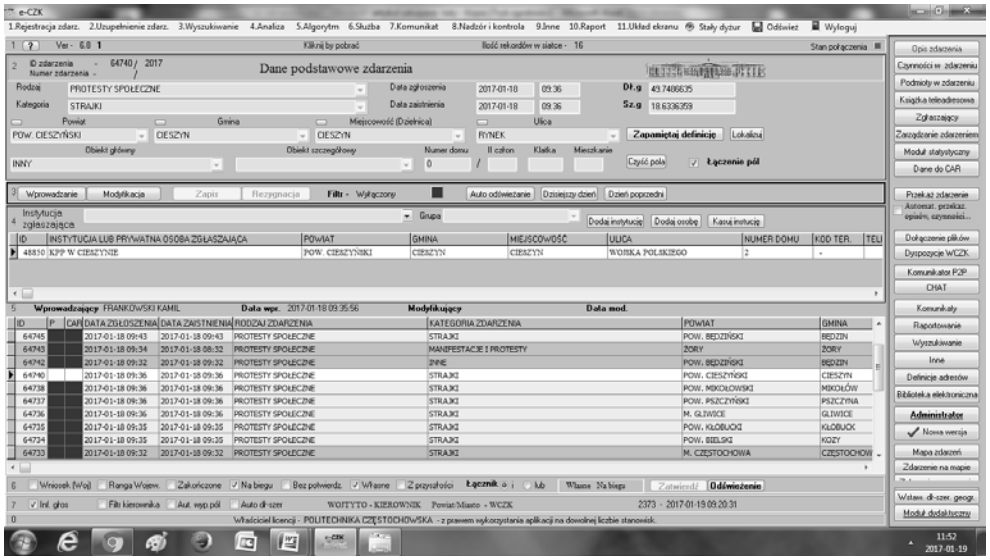
3. Proces dokumentowania i dystrybucji informacji o zdarzeniach kryzysowych z wykorzystaniem programu komputerowego *e- CZK*

Procedura przepływu informacji o zdarzeniach kryzysowych polega na przyjęciu zgłoszenia o zdarzeniu, następnie wstępnej analizie i rejestracji tego zdarzenia, monitorowaniu go, a w konsekwencji działaniach logistycznych polegających na powiadamianiu (informowaniu), komunikowaniu oraz ostrzeganiu ludności o zaistniałej sytuacji.

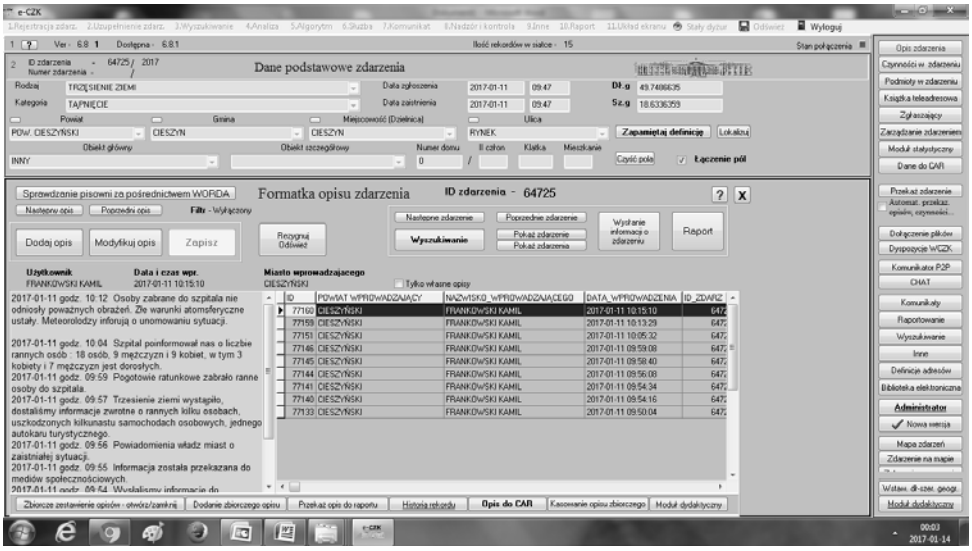
Aplikacja *e-CZK* (Elektroniczne Centrum Zarządzania Kryzysowego) jest przeznaczona do rejestracji zdarzeń zaistniałych na danym terenie administracyjnym (program obsługuje zagrożenia z województwa śląskiego). Pozwala ona na przepływ informacji o zdarzeniach pomiędzy poszczególnymi podmiotami, które biorą udział w danym zdarzeniu kryzysowym (służby, jednostki administracji samorządowej-powiaty), a także na przepływnie informacji pomiędzy nimi (w relacji powiat–województwo). Ponadto narzędzie to jest wykorzystywane do pełnego dokumentowania zagrożeń i ich stałego nadzoru. Program *e-CZK* stanowi doskonałe źródło informacji statystycznych, wykorzystywanych między innymi do zarządzania ryzykiem (a zatem aplikacja *e-CZK* może posłużyć jako baza danych o zagrożeniach dla programu *e-risk*) [2].

Podstawowe funkcje aplikacji przedstawiają się następująco: rejestracja zdarzenia, uzupełnienie zdarzenia, wyszukiwanie zagrożeń, analiza, algorytmy, służba, komunikaty, nadzór i kontrola, raportowanie i inne. Ekran główny aplikacji przedstawia rysunek 9. Zawiera on listę zdarzeń aktualnie zarejestrowanych na terenie danego powiatu (należącego do województwa śląskiego) i pozostających w realizacji. Użytkownik przy wykorzystaniu filtra może zmieniać zawartość siatki rekordów. Ekran główny pozwala także na szybkie rejestrowanie instytucji lub osób zgłaszających.

.



Rys. 9. Ekran główny apliakcji *e-CZK*
Źródło: [2,3]



Rys. 10. Formatka *Opis zdarzenia* w apliakcji *e-CZK*
Źródło: [2,3]

Pierwszą zasadniczą funkcją dokumentowania zdarzeń kryzysowych w programie *e-CZK* jest rejestracja zdarzenia. Polega ona w pierwszej kolejności na określeniu rodzaju, kategorii zagrożenia, dacie zgłoszenia i dacie zaistnienia, wskazania dokładnej lokalizacji. Następnie dokonuje się opisu zdarzenia, tj. w sposób krótki i zwięzły zredagowanie

informacji o przebiegu zdarzenia i dokumentowania kolejnych, napływających komunikatów na temat aktualnej sytuacji kryzysowej (rys. 10.).

Kolejną czynnością przy rejestracji zdarzenia w apliakcji *e-CZK* jest wskazanie czynności podjętych w związku z zagrożeniem przez podmioty biorące w nim udział. Polega to na dokumentowanie tych czynności wykonanych w trakcie obsługi zdarzenia, a następnie wskazanie aktualnego stanu ich realizacji. Czynności te mogą także być wprowadzane poprzez moduł algorytmów. Natomiast formatka *Podmioty w zdarzeniu* jest przeznaczona do dokumentowania podmiotów (instytucje, służby, jednostki samorządowe), które obsługują dane zagrożenie. Każde zdarzenie może posiadać wiele podmiotów. Są one wprowadzane na podstawie książki teleadresowej. Ta z kolei stanowi zbiór podmiotów i osób prywatnych z możliwością zastrzeżenia numeru.

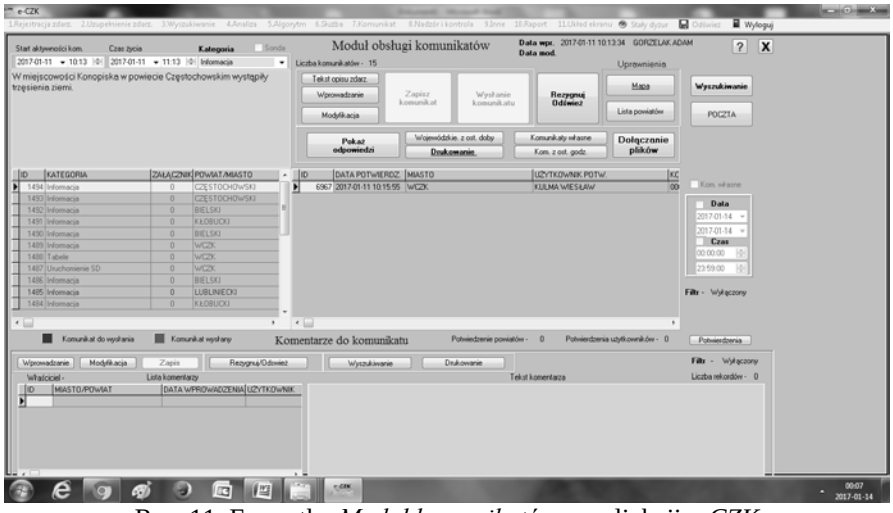
Przy dokumentowaniu zdarzenia kryzysowego ważnym elementem jest również wskazanie instytucji zgłaszającej. Każde zdarzenie może posiadać wiele osób i podmiotów zgłaszających wprowadzanych także na podstawie książki teleadresowej.

Bardzo istotną funkcjonalność apliakcji *e-CZK* stanowi *Zarządzanie zdarzeniem.* Jest to moduł pozwalający na przypisywanie uprawnień do zdarzenia dla powiatów oraz nadawanie rangi wojewódzkiej. W przypadku zdarzeń o randze wojewódzkiej moduł ten nadzoruje całość „życia" zdarzenia. Dyżurny WCZK (Wojewódzkiego Centrum Zarządzania Kryzysowego) monitoruje całość obsługi zdarzeń wojewódzkich. Przypisuje uprawnienia do zdarzeń dla powiatów oraz akceptuje wnioski skierowane z powiatów.

Równie istotną funkcjonalnością aplikacji *e-CZK* jest *Moduł komunikatów*. Polega on na przesyłaniu informacji tekstowych pomiędzy podmiotami biorącymi udział w obsłudze zdarzenia. Każdy komunikat może posiadać dowolną ilość komentarzy i załączników. Za pośrednictwem modułu rozsyłane mogą być zarówno informacje, ostrzeżenia, jak i polecenia. Każdorazowe odebranie komunikatu przez odbiorcę jest rejestrowane. Wysyłanie komunikatów może odbywać się przy pomocy listy dostępnych jednostek biorących udział w zdarzeniu lub mapy województwa. Użytkownik może potwierdzić odbiór i zamknąć okno lub odpowiedzieć do nadawcy komunikatu. Komunikat będzie się pojawiał do czasu potwierdzenia odbioru. Istnieją trzy metody wysyłania komunikatów: poprzez moduł obsługi komunikatów, komunikator tzw. „P2P" (rys. 11.) lub CHAT.

W aplikacji *e-CZK* możliwe jest posługiwanie się *Modułem raportowania.* Umożliwia on tworzenie raportu zgodnie z indywidualnie określonymi punktami oraz raportowanie zawartości siatki rekordów bądź pojedynczego zdarzenia. Raport budowany jest zgodnie z parametrami zadeklarowanymi przez użytkownika. Może być generowany jako dobowy, tygodniowy, miesięczny lub wysyłany do Centralnej Aplikacji Raportującej (system raportowania o zagrożeniach dla służb i instytucji o zasięgu krajowym stworzone przez Rządowe Centrum Bezpieczeństwa) [10].

Narzędzie informatyczne *e-CZK* oprócz opisanych w niniejszej pracy funkcjonalności posiada także inne zastosowania. Za jej pomocą można wyszukiwać zdarzenia z przeszłości, tworzyć tabele statystyczne, analizować i porównywać wyniki. Oprogranmowanie zawiera także formularz zapytań służący zbieraniu informacji, a następnie możliwość tworzenia tabel i wykresów z danymi. Ponadto w aplikacji istnieje możliwość wymiany i przesyłania plików oraz interakcji z mapami graficznymi. Użycie aplikacji wymaga dostępu do sieci internetowej.



Rys. 11. Formatka *Moduł komunikatów* w apliakcji *e-CZK*
Źródło: [2,3]

5. Wnioski

Podsumowując rozważania dotyczące zastosowania systemów informatycznych do dokumentowania zdarzeń kryzysowych można przytoczyć kilka wniosków. Po pierwsze, zagrożenia kryzysowe stanowią istotną część otoczenia zewnętrznego przedsiębiorstwa, które wpływają na jego funkcjonowania. Występowanie zdarzeń kryzysowych mogą powodować czasowe zakłócenia w działalności gospodarczej oraz generować duże straty (przede wszystkim ludzkie i materialne). Co prawda zagrożeniami kryzysowymi zajmują się wyspecjalizowane do tego jednostki administracji samorządowej i rządowej w ramach ogólnego bezpieczeństwa państwa, których obowiązki wynikają z *Ustawy o zarządzaniu kryzysowym*, jednakże każde przedsiębiorstwo powinno oceniać ryzyko występowania tego rodzaju zagrożeń (między innymi ze względu na ubezpieczenie przedsiębiorstwa). Nie należy zatem bagatelizować zjawisk kryzysowych (często nagłych, niespodziewanych, nieprzewidywalnych), gdyż mogą one stanowić nieodwracalne skutki dla przedsiębiorstwa.

Postęp technologii informatycznej wymusza konieczność posługiwania się narzędziami komputerowymi, które w znaczny sposób ułatwiają obsługę dokumentowania zagrożeń kryzysowych oraz wymianę informacji o nich pomiędzy zainteresowanymi i uprawnionymi do tego osobami. Jednocześnie stanowią one doskonałą bazę danych, wielokrotnie wykorzystywaną do różnego rodzaju analiz statystycznych.

Oprogramowanie komputerowe *e-risk* służy do realizacji procesu zarządzania ryzykiem zagrożeń kryzysowych i jest oparte na międzynarodowych standardach zarządzania ryzykiem. Narzędzie to jest stosunkowo elastyczne i można go dostosować do różnego rodzaju zagrożeń, zarówno bezpieczeństwa państwa, jak i zagrożeń wewnętrznych przedsiębiorstwa. Program ten wykorzystuje wiele funkcjonalności, które są uniwersalne i realizują proces w sposób holistyczny (uwzględnia wszystkich siedem etapów procesu zarządzania ryzykiem). Ponadto informacje stanowiące bazę danych programu mogą być wykorzystywane między innymi dla potrzeb programu *e-CZK*.

Narzędzie informatyczne *e-CZK* jest przeznaczone głównie do dokumentowania zagrożeń kryzysowych w każdej fazie ich występowania, tj. zapobiegania, przygotowania,

reagowania i odbudowy. Dzięki temu możliwe jest analizowanie zdarzeń kryzysowych i tym samym ustalania priorytetów w planach przygotowania się na nadejście zagrożeń i minimalizowania ich skutków. Ponadto oprogramowanie to znacznie ułatwia komunikację i wymianę informacji pomiędzy poszczególnymi podmiotami, które obsługują to zdarzenie. Aplikacja ta stanowi jednak narzędzie specjalistyczne i jest głównie wykorzystywane w administracji państwowej, stąd jej wdrożenie w przedsiębiorstwie nie spełniałoby swej podstawowej funkcji i nie byłoby wobec tego w żaden sposób efektywne.

Pomimo wielu zalet opisywanych w niniejszej pracy systemów informatycznych, ich wdrożenie, czy zastosowanie może powodować pewne trudności. Wynikają one głownie z przygotowania merytorycznego osób odpowiedzialnych za ich obsługę. Często wpływ na to mają także działania organizacyjne, dostęp do odpowiedniej infrastruktury technicznej, czy integracji z innymi systemami informatycznymi.

Literatura

1. Lidwa W., Krzeszowski W., Więcek W., Zarządzanie w sytuacjach kryzysowych, Wyd. AON, Warszawa 2010.
2. Materiały udostępnione przez autora aplikacji e-CZK, Katowice 2014.
3. Materiały udostępnione przez WBiZK Śląskiego Urzędu Wojewódzkiego w Katowicach, 2014.
4. Materiały szkoleniowe, Zarządzanie ryzykiem z wykorzystaniem narzędzia informatycznego e-risk, Wyd. PBSG, Poznań 2015.
5. Norma PN-ISO 31000:2012.
6. Sobolewski G., Organizacja i funkcjonowanie Centrum Zarządzania Kryzysowego, Wyd. AON, Warszawa 2011.
7. Sobolewski G., Zagrożenia kryzysowe, Wyd. AON, Warszawa 2011.
8. Stawnicka J., Winiewski B., Socha R. (red.), Zarządzanie kryzysowe. Teoria, praktyka, konteksty, badania, Wyd. WiPWSP, Szczytno 2011.
9. Ustawa z dn. 26 kwietnia 2007 o zarządzaniu kryzysowym, Dz.U. 2007 Nr 89 poz. 590.
10. www.rcb.gov.pl [odczyt: 19.01.2017].
11. Zagrożenia okresowe występujące w Polsce, Wyd. WAiPBMiAZ RCB, Warszawa 2010.

Dr inż. Dorota WOJTYTO
Dr Wiesław KULMA
Wydział Inżynierii Produkcji i Technologii Materiałów
Politechnika Częstochowska
Al. Armii Krajowej 19
42-200 Częstochowa
e-mail: dorota.wojtyto@onet.eu;
wkulma@onet.pl