PRACE NAUKOWE Akademii im. Jana Długosza w Częstochowie
Technika, Informatyka, Inżynieria Bezpieczeństwa 2018, t. VI, s. 649–659

http://dx.doi.org/10.16926/tiib.2018.06.46

Teresa Bajor, Marlena Krakowiak
Zakład Ergonomii i Inżynierii Bezpieczeństwa
Instytut Przeróbki Plastycznej i Inżynierii Bezpieczeństwa
Wydział Inżynierii Produkcji i Technologii Materiałów
Politechnika Częstochowska
al. Armii Krajowej 19, 42–200 Częstochowa,
e-mail: bajor.teresa@wip.pcz.pl, krakowiak.marlena@wip.pcz.pl

ZARZĄDZANIE KRYZYSOWE A BEZPIECZEŃSTWO INFORMACJI

Streszczenie. Wszechobecna informatyzacja i miniaturyzacja spowodowała, że powszechność stosowania rozwiązań mobilnych stała się już niemal normalnością. Przesyłanie informacji za pomocą poczty elektronicznej stosowanej w urządzeniach mobilnych, czy korzystanie z aplikacji typu: Messenger wymaga zachowania szczególnej ostrożności, zwłaszcza przy ich zastosowaniu w działaniach z obszaru zarządzania kryzysowego. Organizacja działań ratowniczych na różnych poziomach działalności jednostek administracji wymaga określenia sposobu doboru środków zapobiegawczych oraz dróg przepływu informacji. Odpowiednio zaplanowana logistyka prowadzonych działań ratowniczych oraz zachowanie poufności przesyłanych informacji jest gwarancją sukcesu danego przedsięwzięcia.
Celem pracy jest wykazanie zasadności podejmowanych działań związanych z bezpieczeństwem przesyłania informacji w aspekcie podjętego tematu.
Słowa kluczowe: zarządzanie kryzysowe, sytuacja kryzysowa, bezpieczeństwo informacji.

CRISIS MANAGEMENT AND INFORMATION SECURITY

Abstract. The ubiquitous computerization and miniaturization has made the widespread use of mobile solutions almost normal. The transmission of information by means of e-mail used in mobile devices or the use of applications such as: Messenger requires special care, especially when used in activities in the field of crisis management. The organization of rescue operations at various levels of activity of administration units requires defining the manner of selection of preventive measures and paths of information flow. Properly

planned logistics of conducting rescue operations and maintaining confidentiality of transmitted information is a guarantee of the success of a given undertaking.
The purpose of the work is to demonstrate the legitimacy of actions undertaken related to the security of information transmission in the aspect of the subject taken.
Keywords: crisis management, crisis situation, information security.

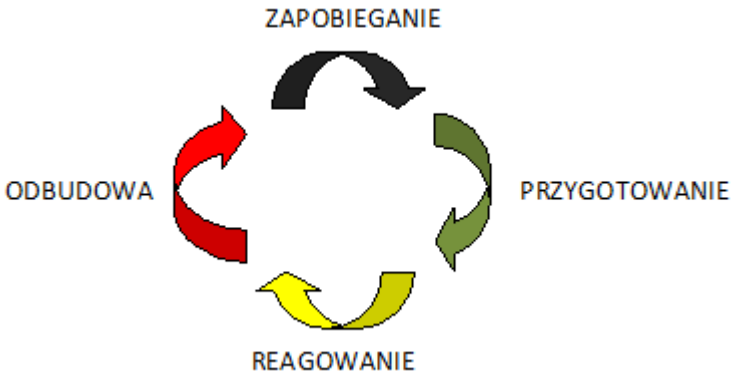
Wprowadzenie

Działania w zakresie zarządzania kryzysowego wymagają ostrożności, rozwagi i świadomości konsekwencji podejmowania złych decyzji. Jasność przekazywanych informacji z zachowaniem bezpiecznych kanałów przepływu informacji jest bardzo ważnym elementem podejmowanych przedsięwzięć. W sytuacjach kryzysowych czy zagrożenia życia i zdrowia, precyzja i bezpieczeństwo przekazywania informacji są kluczowymi punktami osiągnięcia sukcesu. Wybór właściwych kanałów przekazywania treści z uwzględnieniem doboru nowoczesnych środków komunikacji wymaga zachowania odpowiednich środków bezpieczeństwa.

Sytuacja kryzysowa

Analizując sytuację kryzysową należy przede wszystkim uwzględnić definicję sytuacji kryzysowej, która zawarta jest w ustawie [1] z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. Zgodnie z art. 3 ust. 1, sytuacją kryzysową jest sytuacja wpływająca negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołująca znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków. Zgodnie z art. 2 w/w ustawy, celem zarządzania kryzysowego jest zapobieganie takim sytuacjom oraz przejmowanie nad nimi kontroli w drodze zaplanowanych działań, a także usuwanie ich skutków oraz odtwarzanie zasobów i infrastruktury krytycznej.

Gdy obserwujemy otaczający świat widzimy, że sytuacje kryzysowe zdarzają się bardzo często. Mają one miejsce podczas katastrof naturalnych, awarii technicznych, działań terrorystycznych, zakłóceń porządku publicznego, jak również zagrożeń bezpieczeństwa państwa i obywateli. Zaistnienie takiej sytuacji wymaga podjęcia odpowiednich działań na każdym etapie realizacji przedsięwzięcia – w obszarze planowania, organizowania, realizacji i kontroli. Wpisują się one w obszar reagowania będący jedną z czterech faz zarządzania kryzysowego (Rys. 1) zdefiniowanego w ustawie [1].



Rys.1. Fazy zarządzania kryzysowego [1]

Działania podejmowane w ramach fazy reagowania polegają na podejmowaniu odpowiednich kroków w celu udzielania pomocy poszkodowanym, zahamowania rozwoju występujących zagrożeń oraz ograniczenia strat i zniszczeń. Niejednokrotnie scenariusze rzeczywistych działań są odmienne od tych analizowanych na etapie przygotowania, dlatego zachowanie ostrożności podczas przekazywania informacji jest tak bardzo istotne.

Okres reagowania należy zatem definiować jako czas, w którym należy, adekwatnie do wyzwań, podejmować zaplanowane i skoordynowane działania eliminujące zagrożenia powodujące znaczne straty i zniszczenia, a także konkretne akcje w ramach dostarczania pomocy ludności poszkodowanej, aby zapewnić jej minimalny standard życia w bardzo trudnym dla niej okresie. Faza reagowania obejmuje działania ratownicze, bezpośrednio związane z likwidacją lub opanowaniem zaistniałej sytuacji kryzysowej. Ważnym składnikiem na tym etapie jest pomoc najbardziej poszkodowanej ludności. Są to m.in. czynności, takie jak: prowadzenie ewakuacji, zapewnienie zastępczych miejsc zakwaterowania dla poszkodowanych oraz ograniczenie wtórnych strat i zniszczeń.

Przytaczając słowa dyrektora Rządowego Centrum Bezpieczeństwa (RCB), problematyka sytuacji kryzysowej jest we współczesnym świecie bardziej skomplikowana [2]: „sytuacja kryzysowa to już nie tylko powódź, pożar, epidemia czy awaria o rozległych skutkach. Coraz częściej mamy do czynienia z np. aktami terrorystycznymi czy zagrożeniami hybrydowymi". Nie można również nie zwrócić uwagi na dezinformację, która stanowi bardzo ważną część zagrożeń hybrydowych. Koniecznie należy zwrócić uwagę na nowe typy zagrożeń, które wymagają dostosowania narzędzi zarządzania kryzysowego, a także modyfikacji niektórych z funkcjonujących dotychczas procedur, zarówno pod względem metodologicznym, jak i praktycznym. [2]

Analizując informacje zawarte w dokumencie pt.: „Narodowy Program Ochrony Infrastruktury Krytycznej", można znaleźć ogólne wytyczne dotyczące wymiany informacji pomiędzy poszczególnymi uczestnikami zajmującymi się ochroną infrastruktury krytycznej. Stworzona na potrzeby działań służb specjalna platforma internetowa ma służyć jako forum wymiany informacji na temat zagrożeń i podatności oraz opracowywania wytycznych do strategii i rozwiązań w celu ograniczenia ryzyka zakłócenia funkcjonowania infrastruktury krytycznej. W tym aspekcie duże znaczenie ma bezpieczeństwo informacji wymienianych w ramach platformy. I tutaj wiodącą jest rola administracji publicznej, która podejmie wszelkie działania zmierzające do zapewnienia odpowiedniego poziomu ochrony i zaufania w zakresie dostępu osób postronnych do platformy i do ochrony tajemnicy przedsiębiorstwa.

Pozytywne zakończenie sytuacji kryzysowej z punktu widzenia zarządzania kryzysowego wymaga udziału elementów podsystemu kierowania oraz podmiotów wykonawczych. Podmioty te realizują zadania w ramach systemu zarządzania kryzysowego zazwyczaj w wąskim obszarze i specjalności, w oparciu o zasady zawarte w obowiązujących aktach prawnych. W systemie zarządzania kryzysowego szczególny nacisk położony jest na organizację współdziałania oraz koordynację działań prowadzonych przez poszczególne podmioty, co pozwala na efektywną realizację zadań zarządzania kryzysowego, a także racjonalne wykorzystanie posiadanych sił i środków.

W systemie zarządzania kryzysowego organizacja współdziałania dotyczy zarówno organów administracji publicznej pełniących funkcje decyzyjne, jak również podmiotów wykonawczych realizujących zadania w ramach podsystemu wykonawczego. Współdziałanie w systemie decyzyjnym odbywa się na poziomie gminnym, powiatowym oraz wojewódzkim i dotyczy takich obszarów, jak [3]:

- wzajemne informowanie o sytuacjach mogących stanowić zagrożenie dla sąsiednich gmin, powiatów lub województw,
- organizacja łączności, ostrzeganie oraz współdziałanie w przypadku prowadzenia wspólnych działań,
- wymiana informacji o podjętych działaniach,
- wymiana informacji o siłach i środkach możliwych do wydzielenia w celu wsparcia działań prowadzonych przez sąsiednie gminy, powiaty lub województwa,
- możliwość pomocy w ewakuacji ludności,
- możliwość pozyskania specjalistów, specjalistycznych maszyn i środków transportu.

W ramach systemu wykonawczego współdziałanie pomiędzy podmiotami wykonawczymi zarządzania kryzysowego odbywa się na wszystkich poziomach struktury organizacyjnej tych podmiotów i dotyczy [3]:

- monitorowania zagrożeń i wzajemnej wymiany informacji o zagrożeniach, podejmowanych działaniach oraz użytych siłach i środkach,
- tworzenia, doskonalenia i wdrażania zasad oraz procedur współdziałania,
- prowadzenia szkoleń i ćwiczeń oraz udostępnianie bazy szkoleniowej według potrzeb,
- uzgadniania i prowadzenia działań ratowniczych oraz wzajemnej pomocy dotyczącej sił i środków w zakresie realizacji zleconych zadań,
- wymiany doświadczeń uzyskanych w zakresie realizowanych zadań.

Współdziałanie w sytuacjach kryzysowych jest przygotowywane i koordynowane przez koordynatora działań. Jego rolą jest zarówno inicjowanie współdziałania zmierzającego do zainicjowania konkretnych przedsięwzięć, jak również opracowanie harmonogramu ich realizacji. Harmonogram taki sprowadza się do podziału danego przedsięwzięcia na zadania, które w całości są przypisane poszczególnym podmiotom uczestniczącym w tym współdziałaniu. Harmonogram określa czas oraz kolejność realizacji poszczególnych zadań w uzgodnieniu z zainteresowanymi podmiotami. W fazie realizacji przedsięwzięcia koordynator czuwa nad terminowością i rzetelnością poszczególnych zadań przez wyznaczone do tego podmioty. Jeśli zaistnieje taka konieczność, koordynator dokonuje korekty w przyjętym harmonogramie oraz rozstrzyga spory kompetencyjne zaistniałe w trakcie realizacji danego przedsięwzięcia [4].

Z prawnego punktu widzenia w myśl Ustawy o zarządzaniu kryzysowym do działań realizowanych w ramach koordynacji do zadań zarządzania kryzysowego zalicza się [5]:

- ujęcie w planach zarządzania kryzysowego elementów współdziałania między uczestnikami tego zarządzania,
- współdziałanie Rządowego Centrum Bezpieczeństwa, ministrów kierujących działaniami administracji rządowej oraz kierowników urzędów centralnych, wojewodów, starostów i wójtów z Szefem Agencji Bezpieczeństwa Wewnętrznego w zakresie zapobiegania, przeciwdziałania i usuwania skutków zdarzeń o charakterze terrorystycznym oraz z centrami zarządzania kryzysowego organów administracji publicznej,
- współdziałanie centrów zarządzania kryzysowego z podmiotami prowadzącymi akcje ratownicze, poszukiwawcze i humanitarne,
- monitorowanie potencjalnych zagrożeń, a także możliwości ich wystąpienia oraz rozwoju,
- wzajemne alarmowanie, ostrzeganie i zapewnianie obiegu informacji o przebiegu sytuacji kryzysowej,
- udzielanie wzajemnej pomocy podczas realizowanych zadań z zarządzania kryzysowego odpowiednio do potrzeb i posiadanych możliwości.

Realizacja wszystkich tych działań jest niezbędna dlatego, że zadania wykonywane w ramach zarządzania kryzysowego są podejmowane przez różne wyspecjalizowane podmioty, a ponadto mają charakter wieloetapowy, a w związku

z tym każdy z podmiotów wykonuje określone zadania zgodnie ze swoimi kompetencjami i możliwościami [4].

Z punktu widzenia organizacji harmonogramu działań i przypisanych zadań na poszczególnych szczeblach organizacji systemu wszystko wydawałoby się w porządku. Jednak nie należy zapominać o sposobie przekazywania informacji i jej bezpieczeństwie, gdyż nie uwzględnienie tego aspektu może zniweczyć każde, nawet najlepiej zaplanowane, działanie. Szczególnie w przypadku systemu zarządzania kryzysowego, który jest jednym z najważniejszych filarów bezpieczeństwa kraju.

Bezpieczeństwo informacji

Jednostki administracji publicznej mają ustawowy obowiązek zapewnienia odpowiednich zasad organizacji ochrony informacji, zarówno tych klasyfikowanych, jak i niepodlegających klasyfikacji. Niebezpieczeństwa związane z ochroną informacji bardzo często wiążą się z brakiem świadomości osób pracujących w jednostkach administracji. Sam sposób przechowywania dokumentów w formie papierowej niejednokrotnie może być źródłem wycieku danych do osób postronnych. Jednym z problemów jest niestosowanie się do „zasady czystego biurka" - czyli braku pozostawiania w miejscu pracy żadnych dokumentów w widocznym miejscu, w celu uniemożliwienia dostępu do nich osobom postronnym. Kolejnym problemem jest gromadzenie pism urzędowych na biurkach w dziale obsługi klienta, co daje możliwość zapoznania się z ich treścią osobom postronnym. Można by tu było przytaczać, jeszcze wiele przykładów braku świadomości działań pracowników administracji. Nawet telefony przedstawicieli banków, skierowane do działu personalnego z prośbą o potwierdzenie zatrudnienia konkretnej osoby, w pewnych okolicznościach mogą stanowić naruszenie zasad udostępniania danych. Jednak nie każdy urzędnik ma wiedzę o tym, że udzielenie takiej informacji jest związane z bezprawnym udostępnieniem danych osobowych [6–8].

Od 25 maja 2018 roku w Polsce obowiązuje Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), którego celem jest doprowadzenie do pełnej harmonizacji prawa w ramach UE i swobodnego przepływu danych osobowych [9]. Ogólne rozporządzenie o ochronie danych jest częścią pakietu UE dotyczącego reformy ochrony danych [10], razem z dyrektywą o ochronie danych w obszarze policji i wymiaru sprawiedliwości [11].

Wejście tego rozporządzenia nakłada zmiany procedur funkcjonowania na każdym poziomie administracji publicznej, szczególnie w przypadku działań z zakresu zarządzania kryzysowego. Sposób zbierania informacji, jej selekcjonowania, analizowania i przekazywania w sytuacji kryzysowej może być utrudniony. Na pewno w momencie dostosowywania procedur oraz oprogramowania administracji.

Sama świadomość bezpiecznego przetwarzania i przechowywania danych jest jednak nie wystarczająca. W przypadku zarządzania kryzysowego, gdy zagrożenie stanowi atak terrorystyczny, celowe działanie powodujące dezinformację jest bardzo istotne. Zatem wybór odpowiednich kanałów przekazywania informacji oraz zastosowanie właściwych narzędzi jej przekazywania, z określeniem drogi przepływu informacji, wraz z zastosowaniem adekwatnych środków bezpieczeństwa może stanowić o sukcesie podejmowanych działań.

Warto zadać sobie pytanie: „Jakie znaczenie dla przeciętnego obywatela ma ochrona danych osobowych?". Większość społeczeństwa nie zdaje sobie sprawy ze znaczenia i potrzeby ochrony danych osobowych. Brak rozwagi przy ich udostępnianiu lub po prostu brak zapytania o cel i podstawę żądania konkretnych danych osobowych spowodowane mogą być ilością wykonywanych równocześnie czynności i operacji oraz powszechnym pośpiechem. Warto zatem zwrócić uwagę, iż przepisy zawarte w rozporządzeniu RODO mają chronić obywateli przed bezprawnym wykorzystywaniem ich danych. Z prawem tym skorelowane są również uprawnienie do żądania od podmiotu będącego tzw. administratorem danych, m.in. uaktualnienia, sprostowania lub usunięcia danych osobowych, jeśli zostały pozyskane w sposób niezgodny z prawem, są nieaktualne, nieprawdziwe lub stały się zbędne, gdyż zrealizowany został cel, dla którego je pozyskano.

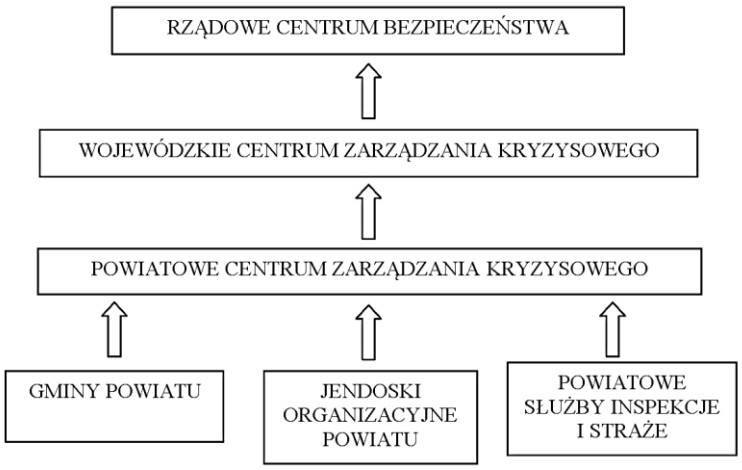
W przypadku przedsiębiorców sytuacja wygląda dobrze, gdyż mają świadomość jej powagi, szczególnie w czasach, gdy pozyskane informacje są cennym dobrem, a ich utrata oznacza wymierne straty finansowe. Odbudowanie bazy danych może być bardzo kosztowne, a niejednokrotnie nawet niemożliwe. W przypadku przedsiębiorstw wyciek danych może skutkować utratą zaufania ze strony klientów, a niejednokrotnie nawet postępowaniami sądowymi, np. z tytułu naruszenia dóbr osobistych, co może oznaczać konieczność wypłaty odszkodowań. Za naruszenie obowiązku zabezpieczenia danych osobowych oraz za udostępnianie danych osobowych osobom nieupoważnionym wprowadzona w życie ustawa przewiduje odpowiedzialność karną w postaci kary grzywny, kary ograniczenia albo pozbawienia wolności. Jednak o jej zastosowaniu zawsze decyduje sąd.

Problem w przypadku ochrony danych osobowych leży po stronie braku świadomości obywateli - brak odpowiedniej wiedzy na temat potrzeby chronienia swoich danych, brak świadomości ich wartości i znaczenia. Wielu obywateli tzw. informacje wrażliwe, takie jak np. imię, nazwisko, adres zamieszkania czy

numer PESEL udostępnia niejednokrotnie z własnej inicjatywy na portalach społecznościowych. Taki sposób postępowania powoduje, że tracą kontrolę nad tym, co się z tymi danymi dzieje [12]. Można by przytoczyć jeszcze wiele sposobów pozyskiwania danych osobowych przez osoby tym zainteresowane, przy wykorzystaniu różnych narządzi i motywacji.

W przypadku przesyłania informacji w formie elektronicznej jest ona narażona na zagrożenia wynikające między innymi z nieautoryzowanego dostępu oraz niekontrolowanej modyfikacji przekazywanych danych. W przypadku prowadzenia działalności pomocowej w sytuacji kryzysowej koniecznością jest posiadanie rzetelnych informacji o aktualnej sytuacji w miejscu akcji, a łączność mobilna może być narażona na podsłuch w celu pozyskania poufnych danych. Dezinformacja w celu utrudnienia lub uniemożliwienia niesienia pomocy wymaga zastosowania technik zwiększających odporność na inwigilację elektroniczną oraz zagwarantowanie pewności danych. Przykładem może tu być zastosowanie otwartych standardów, co zwiększa bezpieczeństwo w wyniku przejrzystej formy wymiany danych w dokładnie sprawdzonych kanałach komunikacji. Zastosowanie tego typu standardów pozwala na opracowanie spójnej platformy do budowy systemów wspomagania zarządzania zdarzeniami kryzysowymi. Bezpieczeństwo przekazywanej informacji oraz integralność zapewnia mechanizm certyfikatów cyfrowych oraz szyfrowanie przesyłanych danych. W przypadkach, gdy pomoc niesiona jest na terenach państw trzecich wymagane jest zapewnienie dostępu do treści informacji podmiotom wyznaczonym przez te państwa przy zachowaniu integralności danych [13].

Obieg informacji w zarządzaniu kryzysowym stanowi integralny jego element, który ma na celu zmniejszenie stanu niepewności. Rozwój Internetu i telefonii komórkowej powoduje, że obecnie obieg informacji przebiega każdego dnia w równym tempie, przesyłając i przetwarzając 10^{15} bajta danych. Informacja staje się zatem kluczowym czynnikiem mającym wpływ na bezpieczeństwo obywateli i państwa. Obieg informacji jest podstawą prawidłowego funkcjonowania Systemu Zarządzania Kryzysowego z uwzględnieniem wszystkich jego elementów. Sposób przekazywania informacji w strukturach zarządzania kryzysowego jest zależny od odbiorcy i ustalonej procedury postępowania. W przypadku Rządowego Centrum Bezpieczeństwa, którego zadaniem jest przede wszystkim pozyskiwanie informacji o zagrożeniach oraz ich ocena, nieustanne monitorowanie tych zagrożeń, jak również ocena ryzyka, prognozowanie stanu rozwoju zagrożeń na obszarze jej podlegającemu oraz wykorzystywanie tych informacji w celu opracowania planu zarządzania kryzysowego. Schemat przepływu informacji na potrzeby Rządowego Centrum Bezpieczeństwa z wykorzystaniem Centralnej Aplikacji Raportującej przedstawiono na Rys. 2.



Rys. 2. Schemat przepływu informacji (opracowanie własne na podstawie [14])

Ciągłe monitorowanie zagrożeń, przesyłanie uporządkowanych informacji oraz przetwarzanie danych wymaga zastosowania odpowiednich systemów zabezpieczeń kanałów informacyjnych. Zwłaszcza w dobie kryzysu ogromne znaczenie ma przesyłanie informacji odpowiednim organom w szybkim tempie. Dla uporządkowania sposobu przepływu, zbierania oraz analizy danych opracowano program nazwany Centralną Aplikacją Raportującą (CAR). Zasadniczym celem programu jest usprawnienie przepływu informacji w oparciu o trójstopniowy system raportowania. W chwili wystąpienia zagrożenia lub kryzysu tworzony jest raport inicjujący, zawierający elementarny zestaw informacji (odpowiedzialność jego sporządzenia spoczywa na organie, który w pierwszej kolejności otrzyma informację o zagrożeniu) oraz ocenę ryzyka. Ukończony raport pojawi się na stronie programu i będzie widoczny dla wszystkich zalogowanych użytkowników (informacja dociera w jednej chwili do każdego zainteresowanego podmiotu). W następnej kolejności pojawia się raport poszerzający, który zawiera dane uzupełniające pierwszy raport oraz raport końcowy, czyli skutki i prognoza na przyszłość. [14]

Podstawą budowy polityki bezpieczeństwa informacji jest określenie rangi poszczególnych danych, jakimi dysponuje organizacja. Określenie drogi komunikacji oraz sposobu kodowania danych, jest elementem kluczowym, gdyż tylko wówczas można odnieść sukces w prowadzonych działaniach. Podczas wyboru i określania dróg komunikacji należy mieć świadomość zagrożeń, jakie wynikają z nieautoryzowanego dostępu do danych osób trzecich. W obecnych czasach, gdy powszechnie stosuje się rozwiązania mobilne bardzo ważnym elementem jest świadomość, że każda forma łączności posiada mocne i słabe strony.

Podsumowanie

Bezpieczeństwo informacji i rzetelność jej przekazywania w sytuacjach kryzysowych jest bardzo istotnym elementem prowadzenia działań, zwłaszcza w kontekście współpracy z mediami, które kształtują opinię publiczną, przedstawiając jej wybrane fragmenty rzeczywistości. Realizacja zadań z zakresu zapewnienia bezpieczeństwa publicznego wymaga sprawnego, efektywnego systemu zarządzania kryzysowego, zdolnego do przeciwdziałania różnego rodzaju zagrożeniom poprzez sprawne działanie organów administracji publicznej i podmiotów wykonawczych tworzących podsystem wykonawczy. Dzięki niemu możliwe jest skuteczne rozwiązywanie różnego rodzaju sytuacji kryzysowych przy zaangażowaniu minimum środków przez połączenie wysiłków organów administracji publicznej, instytucji, służb, straży oraz inspekcji odpowiadających za bezpieczeństwo. System jest ukierunkowany na zarządzanie sytuacją kryzysową poprzez działania planistyczno-proceduralne i procesy decyzyjne, a oprócz tego posiada też ustawowo podporządkowane podmioty wykonawcze na poszczególnych jej poziomach, niezbędne do realizacji zadań zarządzania kryzysowego. Rządowe Centrum Bezpieczeństwa realizuje wszystkie swoje zadania w oparciu o informacje uzyskiwane ze wszystkich ośrodków kryzysowych funkcjonujących w ramach administracji publicznej. Dbałość o bezpieczeństwo informacji i brak możliwości pozyskania jej przez osoby trzecie, to jedne z czynników stanowiących gwarancję sukcesu prowadzonych działań.

Literatura

[1] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 lutego 2011 r. w sprawie szczegółowych zasad organizacji krajowego systemu ratowniczo-gaśniczego, Dz. U. z 2011 r., Nr 46, poz. 239 z późn. zm.
[2] https://rcb.gov.pl/zarzadzanie-kryzysowe-to-nie-tylko-reagowanie/- 05.2018
[3] Kitler W.: *Planowanie cywilne w zarządzaniu kryzysowym,* Wydawnictwo Akademii Obrony Narodowej, Warszawa 2011.
[4] Falecki J.: *Dylematy zarządzania kryzysowego w Rzeczypospolitej Polskiej*, Wydawnictwo Instytutu Bezpieczeństwa Narodowego Wyższej Szkoły Humanitas, Sosnowiec 2016
[5] Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym,* Dz. U. z 2015 r., nr 89 poz. 1485 z późn. zm.
[6] http://www.itwadministracji.pl/ - 01.2018
[7] Prauzner T., Bezpieczeństwo i edukacja w zmieniającej się rzeczywistości, [w:] Edukacja XXI wieku, Przestrzenie edukacyjnego współdziałania w budowaniu społeczeństwa obywatelskiego, red. Górecka K., Kukie-

wicz A., 41 t.2, Wydawnictwo Wyższej Szkoły Bezpieczeństwa, Poznań 2017, s.31–40
[8] https://rcb.gov.pl/wp-content/uploads/NPOIK-dokument - 05. 2018
[9] https://giodo.gov.pl/1520143/j/pl - 05.2018
[10] https://ec.europa.eu/info/law/law-topic/data-protection_en - 03. 2018
[11] http://www.strefabiznesu.pl/wiadomosci/a/nadal-nie-chronimy-dostatecznie-naszych-danych-osobowych-skutki-utraty-sa-dotkliwe-i-kosztowne,-03.2018
[12] Dobrakowski R.: Bezpieczeństwo stosowania rozwiązań GSM w sytuacjach kryzysowych, Inżynieria Produkcji: Analiza zagrożeń podstawą funkcjonowania współczesnej organizacji, Seria Monografia nr 71, Częstochowa 2017, s.114–124
[13] http://www.nowastrategia.org.pl/ - 03.2018
[14] Galicki K., Świszcz G.: Usprawnienie procesu obiegu informacji w systemie zarządzania kryzysowego, Przegląd bezpieczeństwa wewnętrznego, nr 9, 2013, s .318–323.