**Nowoczesne Systemy Zarządzania**
Zeszyt 14 (2019), nr 3 (lipiec-wrzesień)
ISSN 1896-9380, s. 67-80

Instytut Organizacji i Zarządzania
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna
w Warszawie

**Modern Management Systems**
Volume 14 (2019), No. 3 (July-September)
ISSN 1896-9380, pp. 67-80

Institute of Organization and Management
Faculty of Security, Logistics and Management
Military University of Technology

# Zarządzanie ryzykiem jako determinanta cyberbezpieczeństwa

# Risk management as a determinant of cybersecurity

**Grzegorz Mąkosa**
Wojskowa Akademia Techniczna
Wydział Cybernetyki

**Abstrakt.** Celem artykułu jest wykazanie zależności bezpieczeństwa i cyberbezpieczeństwa od ryzyka i zarządzania ryzykiem. Praca przedstawia definicje oraz proces zarządzania ryzykiem zdefiniowany w normie PN EN ISO 27005:2014 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji, składający się z procesów ustanowienia kontekstu, szacowania ryzyka, czyli identyfikacji, analizy oraz oceny ryzyka, postępowania z ryzykiem, informowania i konsultowania oraz monitorowania i przeglądu. W dalszej części artykułu autor przechodzi od definicji bezpieczeństwa, cyberbezpieczeństwa, zarządzania kryzysowego do dokumentów strategicznych, operacyjnych i regulacji prawnych, przedstawiając powiązania i zależności między ryzykiem oraz zarządzaniem ryzykiem a bezpieczeństwem i cyberbezpieczeństwem oraz zarządzaniem kryzysowym jako systemem zarządzania bezpieczeństwem narodowym, ochroną infrastruktury krytycznej, w tym systemów teleinformatycznych cyberprzestrzeni. Przedstawione relacje bezsprzecznie wskazują zarządzanie ryzykiem jako determinantę bezpieczeństwa i cyberbezpieczeństwa.
**Słowa kluczowe:** ryzyko, zarządzanie ryzykiem, bezpieczeństwo, cyberbezpieczeństwo, zarządzanie kryzysowe.

**Abstract.** The aim of the article is to demonstrate the dependence of security and cyber security on risk and risk management. The article presents the definitions and risk management process defined in the PN EN ISO 27005:2014 Information technology standard – Security technology – Risk management in information security, consisting of context-setting processes, risk assessment, i.e. identification, analysis and risk assessment, risk treatment, information and consultation as well as monitoring and review. In the further part of the article, the author proceeds from the definition of security, cybersecurity, crisis management to strategic, operational and legal documents, presenting the relationship and dependence of risk and risk management with security and cybersecurity and crisis management, as a national security management system, critical infrastructure protec-tion, including ICT systems of cyberspace. The presented relationships indicate undeniably risk management as a determinant of security and cybersecurity.
**Keywords:** risk, risk management, security, cybersecurity, crisis management.

## Wstęp

Cyberbezpieczeństwo jako najnowsza i najbardziej wymagająca składowa bezpieczeństwa narodowego i międzynarodowego jest coraz istotniejszym jego komponentem, a zapewnienie odpowiednio wysokiego poziomu cyberbezpieczeństwa jest kluczowym wyzwaniem. Domeną oddziaływania cyberbezpieczeństwa jest cyberprzestrzeń i składające się na nią zasoby informacyjne i systemy teleinformatyczne stanowiące publiczną i prywatną teleinformatyczną infrastrukturę krytyczną oraz infrastrukturę wspomagającą funkcjonowanie pozostałych systemów infrastruktury krytycznej. Najważniejszym wymaganiem w odniesieniu do cyberbezpieczeństwa jest podejście zintegrowane i kompleksowe, obejmujące wszystkie obszary łączące wymiary obronny i ochronny, cywilny i wojskowy, a także publiczny oraz prywatny.

Kwestia cyberbezpieczeństwa jest istotną składową dokumentów strategicznych bezpieczeństwa, m.in. *Strategii Bezpieczeństwa Narodowego RP* i *Doktryny cyberbezpieczeństwa RP*, które zostały poddane bardziej szczegółowej analizie w dalszej części artykułu. Dokumenty te wyznaczają punkty odniesienia i ramy cyberbezpieczeństwa, a także cele i dyrektywy do osiągnięcia odpowiedniego jego poziomu, odnoszące się również do działań związanych z procesami zarządzania ryzykiem i opierające się na nich. Kwestie cyberbezpieczeństwa i ochrony teleinformatycznej infrastruktury krytycznej są także przedmiotem wpływu regulacji w zakresie zarządzania kryzysowego, w tym ustawy o zarządzaniu kryzysowym i *Narodowego Programu Ochrony Infrastruktury Krytycznej* jako dokumentu operacyjnego. Infrastruktura cyberprzestrzeni podlega tym samym zasadom ochrony, co pozostałe systemy infrastruktury krytycznej, a więc rozwiązaniom wygenerowanym na podstawie realizacji procesów związanych z zarządzaniem ryzykiem.

Wymienione dokumenty i regulacje nie definiują wprost istoty procesu zarządzania ryzykiem, jego procesów składowych i powiązań między nimi. Autor proponuje zaaplikowanie do procesów zarządzania bezpieczeństwem i zarządzania kryzysowego odnoszących się do bezpieczeństwa cyberprzestrzeni systemowo ujętego procesu zarządzania ryzykiem, zdefiniowanego w normie PN EN ISO 27005:2014 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji. Proces zarządzania ryzykiem składa się z procesów ustanowienia kontekstu, szacowania ryzyka, czyli identyfikacji, analizy oraz oceny ryzyka, postępowania z ryzykiem, informowania i konsultowania oraz monitorowania i przeglądu. Zastosowanie pełnego, systemowo ujętego procesu zarządzania ryzykiem do definiowania i realizowania celów i zadań wynikających z *Doktryny cyberbezpieczeństwa RP* oraz *Narodowego Programu Ochrony Infrastruktury Krytycznej* w odniesieniu do teleinformatycznej infrastruktury krytycznej cyberprzestrzeni może zapewnić uzyskanie odpowiednio wysokiego poziomu cyberbezpieczeństwa państwa.

## 1. Zarządzanie ryzykiem

Zarządzanie ryzykiem jest procesem będącym podstawą zarządzania organizacjami, systemami, obszarami działalności biznesowej czy administracyjnej. Działania dotyczące zarządzania ryzykiem w organizacji rozwinęły się szczególnie dynamicznie w ostatnich latach. Wraz z rozwojem metod i metodyk związanych z zarządzaniem ryzykiem i wzrostem ich zastosowania pojawiło się wiele definicji ryzyka, zarządzania ryzykiem i procesów zarządzania ryzykiem, które niekiedy są niewłaściwie interpretowane i ze sobą mylone. Autor proponuje przedstawienie wybranych na potrzeby tego artykułu definicji związanych z ryzykiem bezpieczeństwa informacji jako pokrewnych ryzyku cyberbezpieczeństwa i zarządzaniem nim, pochodzących z normy PN EN ISO/IEC 27005:2014 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji.

Zgodnie z treścią przytoczonej normy ryzyko zdefiniowane jest jako wpływ niepewności na cele. Wpływ niepewności powoduje odchylenie od oczekiwań – pozytywne i/lub negatywne. Ryzyko jest często określane w odniesieniu do potencjalnych zdarzeń i ich następstw lub ich kombinacji. Ryzyko w bezpieczeństwie informacji jest związane z potencjalną sytuacją, w której określone zagrożenie wykorzysta podatność aktywów lub grupy aktywów, powodując w ten sposób szkodę dla organizacji (PN ISO/IEC 27005:2014, s. 10). Zarządzanie ryzykiem to skoordynowane działania dotyczące kierowania i nadzorowania organizacji w odniesieniu do ryzyka (PN ISO/IEC 27005:2014, s. 12). Tak zdefiniowane zarządzanie ryzykiem można odnieść również do innych obszarów, w tym do systemu infrastruktury krytycznej i cyberprzestrzeni. Zarządzanie ryzykiem jest procesem, na który składają się, według modelu ISO 27005, procesy (podprocesy), takie jak ustanowienie kontekstu, szacowanie ryzyka, postępowanie z ryzykiem, akceptowanie ryzyka, informowanie o ryzyku oraz monitorowanie i przegląd ryzyka. Model procesu zarządzania ryzykiem przedstawia rysunek 1.

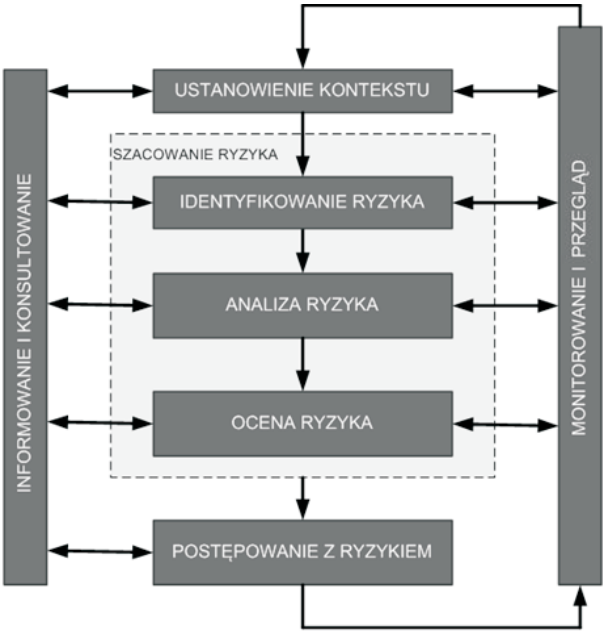
Ustanowienie kontekstu zarządzania ryzykiem jest procesem wyjściowym. To wtedy definiuje się zarządzany pod kątem ryzyka obszar i zakres, np. cyberprzestrzeń, systemy teleinformatyczne infrastruktury krytycznej składające się na cyberprzestrzeń, a także warunki polityczne, ekonomiczne, społeczne, techniczne i technologiczne, prawne, środowiskowe i organizacyjne właściwe dla zdefiniowanego obszaru i zakresu.

W ramach ustanowionego i określonego kontekstu prowadzi się szacowanie. Szacowanie ryzyka to całościowy proces identyfikacji, analizy oraz oceny ryzyka (PN ISO/IEC 27005:2014, s. 10).

Identyfikowanie ryzyka to proces jego wyszukiwania, rozpoznawania i opisywania. Obejmuje on rozpoznanie źródeł ryzyka, zdarzeń, ich przyczyn i potencjalnych następstw. Identyfikowanie ryzyka może obejmować dane historyczne, analizy teoretyczne, pozyskane opinie, opinie ekspertów oraz potrzeby interesariuszy (PN ISO/IEC 27005:2014, s. 11). Po przeprowadzeniu identyfikacji prowadzi się analizę ryzyka.

Jest to proces dążący do poznania charakteru ryzyka oraz określenia jego poziomu. Analiza ryzyka stanowi podstawę do oceny ryzyka oraz podejmowania decyzji w zakresie postępowania z ryzykiem. Zawiera estymację ryzyka (PN ISO/IEC 27005:2014, s. 10). Na podstawie wyników przeprowadzonej analizy realizuje się ocenę ryzyka. To proces porównywania wyników analizy ryzyka z kryteriami ryzyka w celu stwierdzenia, czy ryzyko i/lub jego wielkość są akceptowalne lub tolerowane. Ocena ryzyka wspomaga podejmowanie decyzji w zakresie postępowania z ryzykiem (PN ISO/IEC 27005:2014, s. 11). Zrealizowanie szacowania ryzyka, czyli jego identyfikacja, analiza i ocena, pozwala na wybór strategii i działań postępowania z ryzykiem. Postępowanie z ryzykiem to proces modyfikowania ryzyka. Może on uwzględniać:

- unikanie ryzyka poprzez decyzję o nierozpoczynaniu lub niekontynuowaniu działań powodujących ryzyko;
- podjęcie lub zwiększenie ryzyka w celu wykorzystania szansy;
- usunięcie źródła ryzyka;
- zmianę prawdopodobieństwa;
- zmianę następstw;
- dzielenie ryzyka wraz z inną stroną lub innymi stronami (łącznie z umowami i finansowaniem ryzyka);
- zachowanie ryzyka na podstawie świadomej decyzji.




Rys. 1. Proces zarządzania ryzykiem

Źródło: opracowanie na podstawie (PN ISO/IEC 27005:2014, s. 14)

Postępowanie z ryzykiem, które dotyczy negatywnych skutków, czasem jest nazywane łagodzeniem ryzyka, minimalizacją ryzyka, eliminacją ryzyka, zapobieganiem ryzyku czy redukcją ryzyka. Postępowanie z ryzykiem może doprowadzić do powstania nowych ryzyk lub modyfikacji już istniejących (PN ISO/IEC 27005:2014, s. 11).

Efektywne zarządzanie ryzykiem wymaga stałej komunikacji. Proces informowania i konsultowania to ciągłe i prowadzone w sposób iteracyjny procesy, które są realizowane w celu zapewnienia, przekazywania lub uzyskania informacji, a także w celu porozumiewania się z interesariuszami, odnoszące się do zarządzania ryzykiem. Powyższe informacje mogą odnosić się do istnienia, charakteru, formy, prawdopodobieństwa, ważności, oceny, akceptowalności ryzyka oraz postępowania z ryzykiem. Konsultacje to dwukierunkowy proces świadomej komunikacji organizacji z jej interesariuszami, dotyczący określonego problemu, poprzedzający podejmowanie decyzji w zakresie tego problemu lub ukierunkowanie jego rozwiązania. Konsultacje to proces, który oddziałuje na podejmowanie decyzji bardziej poprzez wywieranie wpływu niż przymus oraz element wejściowy do podejmowania decyzji, ale nie w wyniku zgody większości (PN ISO/IEC 27005:2014, s. 11).

Dopełnieniem zarządzania ryzykiem jest proces monitorowania i przeglądu. W ramach tego procesu realizuje się monitorowanie i przegląd typów ryzyka oraz ich czynników (tzn. wartości aktywów, skutków, zagrożeń, rodzajów podatności, prawdopodobieństwa wystąpienia) w celu identyfikowania każdej zmiany w kontekście organizacji na wczesnym etapie oraz w celu utrzymania obrazu kompletnej mapy ryzyka (PN ISO/IEC 27005:2014, s. 34).

Jak wynika z przedstawionej charakterystyki, zarządzanie ryzykiem jest systemem wzajemnie powiązanych i oddziałujących na siebie procesów ustanowienia kontekstu, szacowania ryzyka, czyli jego identyfikacji, analizy i oceny, postępowania z ryzykiem oraz monitorowania i przeglądu, informowania i konsultowania. Jest to złożony system procesowo-organizacyjny.

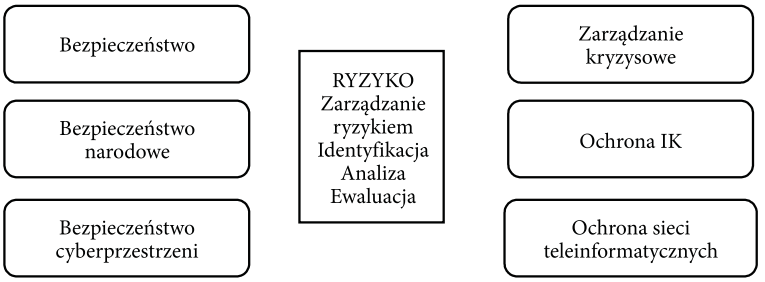
## 2. Zarządzanie ryzykiem a bezpieczeństwo i cyberbezpieczeństwo

Ryzyko i zarządzanie ryzykiem są bezpośrednio i ściśle związane z bezpieczeństwem i cyberbezpieczeństwem oraz zarządzaniem kryzysowym jako systemem zarządzania bezpieczeństwem narodowym.

Relacje ryzyka i zarządzania ryzykiem z bezpieczeństwem i zarządzaniem kryzysowym są dwustronne. Z jednej strony ryzyko jest ściśle zintegrowane z obszarem bezpieczeństwa, w którym wyróżniamy zagadnienia od najogólniejszego i najobszerniejszego bezpieczeństwa, poprzez pośrednie bezpieczeństwo narodowe, do najbardziej skonkretyzowanego bezpieczeństwa cyberprzestrzeni i cyberbezpieczeństwa.

Z drugiej strony relacji mamy powiązanie z najogólniejszym i najobszerniejszym zagadnieniem zarządzania kryzysowego poprzez pośrednie zagadnienie ochrony infrastruktury krytycznej (IK) do najbardziej skonkretyzowanego zagadnienia ochrony sieci i systemów teleinformatycznych.

W celu wykazania i uzmysłowienia tej zależności autor przytacza różne definicje bezpieczeństwa, bezpieczeństwa narodowego, cyberprzestrzeni oraz cyberbezpieczeństwa i przywołuje dokumenty strategiczne definiujące bezpieczeństwo narodowe w celu ukazania, w jaki sposób zagadnienia ryzyka i zarządzania ryzykiem są w nich lokowane i powiązane z kwestiami bezpieczeństwa narodowego.




Rys. 2. Relacje ryzyka i obszarów bezpieczeństwa
Źródło: opracowanie własne

Bezpieczeństwo to stan, który daje poczucie pewności istnienia i gwarancje jego zachowania oraz szanse na doskonalenie. Odznacza się akceptowalnym poziomem ryzyka utraty czegoś dla podmiotu szczególnie cennego – życia, zdrowia, pracy, szacunku, uczuć, dóbr materialnych i dóbr niematerialnych (Wikipedia, 2018a; Łepkowski, 2008, s. 14). Bezpieczeństwo jest naczelną potrzebą człowieka i grup społecznych, jest także podstawową potrzebą państw i systemów międzynarodowych, jego brak wywołuje niepokój i poczucie zagrożenia. Człowiek, grupa społeczna, państwo czy organizacja międzynarodowa starają się oddziaływać na otoczenie zewnętrzne i sferę wewnętrzną, by usuwać, a przynajmniej oddalać zagrożenia, eliminując własny lęk, obawy, niepokój i niepewność. Zagrożenia mogą być skierowane na zewnątrz i do wewnątrz, tak samo powinny być skierowane działania w celu ich likwidowania (Wikipedia, 2018a).

Bezpieczeństwo narodowe jest stanem uzyskanym w rezultacie odpowiednio zorganizowanej obrony i ochrony przed wszelkimi zagrożeniami militarnymi i niemilitarnymi, zarówno zewnętrznymi, jak i wewnętrznymi, z użyciem sił i środków pochodzących z różnych dziedzin działalności państwa (Wikipedia, 2018a; Łepkowski, 2008, s. 169). Bezpieczeństwo narodowe to najważniejsza wartość, potrzeba narodowa i priorytetowy cel działalności państwa, jednostek i grup społecznych,

a jednocześnie proces obejmujący różnorodne środki gwarantujące trwały, wolny od zakłóceń byt i rozwój narodowy (państwa), w tym obronę państwa jako instytucji politycznej oraz ochronę jednostek i całego społeczeństwa, ich dóbr i środowiska naturalnego przed zagrożeniami, które w znaczący sposób ograniczają jego funkcjonowanie lub godzą w dobra podlegające szczególnej ochronie (Wikipedia, 2018a; Kitler, 2011, s. 22-31). Bezpieczeństwo narodowe to także ogół warunków i instytucji chroniących suwerenność państwa, życie i zdrowie obywateli oraz mienie i majątek narodowy. To stan lub warunki, w których zapewniona jest ochrona narodu i terytorium państwa przed atakiem nieprzyjaciela, to zapewnienie stabilnego i harmonijnego rozwoju państwa oraz realizacji jego strategicznych interesów politycznych i ekonomicznych. Bezpieczeństwo narodowe rozumiane jest również jako stan równowagi pomiędzy potencjałem obronnym kraju a zagrożeniem wywołanym możliwością powstania konfliktu. To również pewien stan świadomości społecznej, w którym powstający poziom zagrożeń, dzięki posiadanym zdolnościom obronnym, nie budzi lęku czy obaw o zachowanie uznanych warunków (Wikipedia, 2018b).

We współczesnym świecie bezpieczeństwo państwa w sferze militarnej i pozamilitarnej, zewnętrznej i wewnętrznej zyskało dodatkowy wymiar, jakim – oprócz lądu, wody, powietrza i przestrzeni kosmicznej – jest cyberprzestrzeń.

Cyberprzestrzeń jest jednym z obszarów aktywności państwa, podmiotów prywatnych i obywateli. Cyberprzestrzeń jest również polem konfliktu, na którym przychodzi nam zmierzyć się nie tylko z innymi państwami, ale także z wrogimi organizacjami, jak choćby z grupami ekstremistycznymi, terrorystycznymi czy zorganizowanymi grupami przestępczymi (*Doktryna cyberbezpieczeństwa RP*, 2015, s. 4).

*Doktryna cyberbezpieczeństwa RP* definiuje podstawowe pojęcia związane z bezpieczeństwem cyberprzestrzeni, takie jak „cyberprzestrzeń", „cyberbezpieczeństwo", „bezpieczeństwo cyberprzestrzeni". Pojęcia te są zdefiniowane w następujący sposób:

- **cyberprzestrzeń** – przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci) wraz z powiązaniami między nimi oraz relacjami z użytkownikami;
- **cyberprzestrzeń RP** – cyberprzestrzeń w obrębie terytorium państwa polskiego oraz w miejscach, gdzie funkcjonują przedstawicielstwa RP (placówki dyplomatyczne, kontyngenty wojskowe, jednostki pływające oraz statki powietrzne poza przestrzenią RP podlegające polskiej jurysdykcji);
- **cyberbezpieczeństwo RP (bezpieczeństwo RP w cyberprzestrzeni)** – proces zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni

państwa jako całości, jego struktur, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej, a także będących w ich dyspozycji systemów teleinformatycznych oraz zasobów informacyjnych w globalnej cyberprzestrzeni;

– **bezpieczeństwo cyberprzestrzeni RP** – część cyberbezpieczeństwa państwa, obejmująca zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mających na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni RP wraz ze stanowiącą jej komponent publiczną i prywatną teleinformatyczną infrastrukturą krytyczną oraz bezpieczeństwa przetwarzanych w niej zasobów informacyjnych (*Doktryna cyberbezpieczeństwa RP*, 2015, s. 7).

Bezpieczeństwo w cyberprzestrzeni to najnowsza i współcześnie najbardziej wymagająca dziedzina bezpieczeństwa narodowego, łącząca wymiary obronny i ochronny, cywilny i wojskowy, a także publiczny oraz prywatny. Dlatego też najważniejszym wymaganiem w odniesieniu do cyberbezpieczeństwa jest podejście zintegrowane i kompleksowe, obejmujące wszystkie te obszary (BBN, 2018).

Wraz z pojawieniem się nowych technologii teleinformatycznych oraz rozwojem sieci Internet pojawiły się nowe zagrożenia, takie jak cyberprzestępczość, cyberterroryzm, cyberszpiegostwo, cyberkonflikty z udziałem podmiotów niepaństwowych i cyberwojna rozumiana jako konfrontacja w cyberprzestrzeni między państwami. Obecne trendy rozwoju zagrożeń w cyberprzestrzeni wyraźnie wskazują na rosnący wpływ poziomu bezpieczeństwa obszaru domeny cyfrowej na bezpieczeństwo ogólne kraju. W wyniku rosnącego uzależnienia od technologii teleinformatycznych konflikty w cyberprzestrzeni mogą poważnie zakłócić funkcjonowanie społeczeństw i państw (*Strategia Bezpieczeństwa Narodowego RP*, 2014, s. 19).

Bezpieczne funkcjonowanie systemu teleinformatycznego Rzeczypospolitej Polskiej jest warunkiem niezakłóconego działania całego państwa. Wyzwaniem pozostaje zapewnienie dostępności, integralności i poufności danych przetwarzanych w systemach teleinformatycznych administracji publicznej oraz brak jednolitych zabezpieczeń teleinformatycznych. Jeżeli chodzi o zachowanie bezpieczeństwa, istotne znaczenie ma niewystarczająca wiedza użytkowników na temat zagrożeń w cyberprzestrzeni oraz konieczność rozwiązania dylematu pomiędzy wolnością osobistą i ochroną praw jednostki a stosowaniem środków służących do ochrony państwa (*Strategia Bezpieczeństwa Narodowego RP*, 2014, s. 25).

Zapewnienie bezpieczeństwa Polski w cyberprzestrzeni, w tym bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej, to jedno z podstawowych zadań w dziedzinie bezpieczeństwa państwa. Powinno być ono realizowane zarówno poprzez rozwój zdolności do działań defensywnych (obejmujących ochronę podmiotów działających w cyberprzestrzeni oraz samej cyberprzestrzeni), jak i ofensywnych. Szczególnie ważna jest współpraca i koordynacja działań ochronnych z podmiotami sektora prywatnego – przede wszystkim finansowego, energetycznego,

transportowego, telekomunikacyjnego i opieki zdrowotnej – prowadzenie działań o charakterze prewencyjnym i profilaktycznym w odniesieniu do zagrożeń w cyberprzestrzeni, wypracowanie i stosowanie właściwych procedur komunikacji społecznej w tym zakresie, rozpoznawanie przestępstw dokonywanych w cyberprzestrzeni i zapobieganie im oraz ściganie ich sprawców, prowadzenie walki informacyjnej w cyberprzestrzeni, współpraca sojusznicza, także na poziomie działalności operacyjnej służącej do aktywnego zwalczania cyberprzestępstw, w tym wymiany doświadczeń i dobrych praktyk w celu podnoszenia skuteczności i efektywności działań krajowych (*Strategia Bezpieczeństwa Narodowego RP*, 2014, s. 35).

Strategicznym celem w obszarze cyberbezpieczeństwa RP, sformułowanym w *Doktrynie cyberbezpieczeństwa RP*, jest zapewnienie bezpiecznego funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni, w tym adekwatnego poziomu bezpieczeństwa narodowych systemów teleinformatycznych – zwłaszcza teleinformatycznej infrastruktury krytycznej państwa – a także kluczowych dla funkcjonowania społeczeństwa prywatnych podmiotów gospodarczych, w szczególności wchodzących w skład sektorów: finansowego, energetycznego i ochrony zdrowia (*Doktryna cyberbezpieczeństwa RP*, 2015, s. 9). Dokument określa również sposób osiągnięcia wyznaczonego celu strategicznego, osiąga się go przez realizację zadań prowadzących do osiągania celów o charakterze operacyjnym i preparacyjnym. Główne cele operacyjne to:

- ocena warunków cyberbezpieczeństwa, w tym rozpoznawanie zagrożeń, szacowanie ryzyk i identyfikacja szans;
- zapobieganie (przeciwdziałanie) zagrożeniom, redukowanie ryzyk i wykorzystywanie szans,
- obrona i ochrona własnych systemów i zgromadzonych w nich zasobów;
- zwalczanie (dezorganizowanie, zakłócanie i niszczenie) źródeł zagrożeń (aktywna obrona oraz działania ofensywne);
- po ewentualnym ataku – odtwarzanie sprawności i funkcjonalności systemów tworzących cyberprzestrzeń (*Doktryna cyberbezpieczeństwa RP*, 2015, s. 9).

Jak można zauważyć, działania określone w punktach powyżej są wprost odzwierciedleniem procesów zarządzania ryzykiem, odpowiednio szacowania ryzyka (dla pkt 1) i postępowania z ryzykiem (dla pkt 2, 3 i 4).

Zadania operacyjne ukierunkowane na osiągnięcie strategicznego celu, jakim jest zapewnienie akceptowalnego poziomu bezpieczeństwa Rzeczypospolitej Polskiej w cyberprzestrzeni, powinny być realizowane przez podmioty sektora publicznego (w wymiarze krajowym i międzynarodowym), prywatnego (komercyjnego), obywatelskiego oraz w wymiarze transsektorowym. Do jednych z głównych zadań sektora publicznego w wymiarze krajowym należą rozpoznawanie realnych i potencjalnych źródeł zagrożeń, w tym przez międzynarodową wymianę informacji, oraz ciągła analiza ryzyka w odniesieniu do ważnych obiektów infrastruktury krytycznej.

A jedno z głównych jego zadań na poziomie międzynarodowym to wymiana informacji o podatnościach, zagrożeniach i incydentach (*Doktryna cyberbezpieczeństwa RP*, 2015, s. 14). Wymienione działania podmiotów sektora publicznego stanowią realizację procesów szacowania ryzyka – identyfikację i analizę ryzyka oraz proces komunikacyjny, czyli informowania i konsultowania.

## 3. Zarządzanie ryzykiem a zarządzanie kryzysowe

Bezpieczeństwo narodowe osiągane jest w drodze działań realizowanych w ramach systemu zarządzania kryzysowego. Relacje ryzyka i zarządzania ryzykiem z zarządzaniem kryzysowym pokazano na rysunku 2. Ryzyko jest tam powiązane z najogólniejszym i najobszerniejszym zagadnieniem zarządzania kryzysowego poprzez pośrednie zagadnienie ochrony infrastruktury krytycznej (IK) do najbardziej skonkretyzowanego – ochrony sieci i systemów teleinformatycznych, stanowiących infrastrukturę krytyczną cyberprzestrzeni.

System zarządzania kryzysowego to złożony układ, którego celem jest zapewnienie właściwego poziomu bezpieczeństwa, w tym cyberbezpieczeństwa, skuteczne przeciwdziałanie wszelkiego typu niebezpieczeństwom, a w sytuacji zagrożeń powrót do stanu pierwotnego w możliwie najkrótszym czasie za pomocą dostępnych sił i środków, uwzględniając uzasadnione koszty i ramy obowiązującego systemu prawnego.

Zarządzanie kryzysowe to działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym, która polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej (DzU 2007 nr 89, poz. 590 ze zm., s. 1). Zarządzanie kryzysowe obejmuje cyberbezpieczeństwo będące częścią bezpieczeństwa narodowego.

Zarządzanie kryzysowe funkcjonuje na podstawie planów zarządzania kryzysowego, w tym *Krajowego Planu Zarządzania Kryzysowego* oraz wojewódzkich, powiatowych i gminnych planów zarządzania kryzysowego. Częścią planu zarządzania kryzysowego jest plan główny zawierający m.in. charakterystykę zagrożeń oraz ocenę ryzyka ich wystąpienia, w tym dotyczących infrastruktury krytycznej, a także mapy ryzyka i mapy zagrożeń. Ta część planu powinna zawierać następujące zagadnienia: identyfikacja zagrożeń, charakterystyka zagrożeń (definicja zdarzenia, skutki pierwotne, skutki wtórne) i opis zdarzenia. Jak widać, zagadnienia planu głównego związane z ryzykiem wprost odpowiadają procesom szacowania ryzyka – identyfikacji, analizy oceny – zdefiniowanym w normie PN ISO/IEC 27005:2014, a omówionym powyżej.

*Narodowy Program Ochrony Infrastruktury Krytycznej* (NPOIK) ma za zadanie stworzenie warunków do poprawy bezpieczeństwa infrastruktury krytycznej.

Realizacja celu NPOIK wymaga osiągnięcia wielu celów pośrednich, w tym m.in.:

- wprowadzenie metodyki oceny ryzyka uwzględniającej pełny wachlarz zagrożeń, w tym metodyki postępowania z zagrożeniami o bardzo małym prawdopodobieństwie i katastrofalnych skutkach;
- wprowadzenie skoordynowanego i opartego na ocenie ryzyka podejścia do realizacji zadań z zakresu ochrony IK (NPOIK, 2015, s. 8).

Realizacja wymienionych wyżej celów pośrednich wiąże się z wdrożeniem procesów zarządzania ryzykiem. Cele pośrednie NPOIK przedstawione powyżej odnoszą się do identyfikacji ryzyka uwzględnienia wachlarza zagrożeń, oceny ryzyka – metodyka oceny ryzyka, postępowania z ryzykiem – metodyka postępowania z zagrożeniami oraz wprowadzenie opartego na ocenie ryzyka podejścia do realizacji zadań z zakresu ochrony infrastruktury krytycznej.

Infrastruktura krytyczna to systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje systemy: zaopatrzenia w energię, surowce energetyczne i paliwa, łączności, sieci teleinformatycznych, finansowe, zaopatrzenia w żywność, zaopatrzenia w wodę, ochrony zdrowia, transportowe, ratownicze, zapewniające ciągłość działania administracji publicznej oraz produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych (DzU 2007 nr 89, poz. 590 ze zm., s. 1).

Do infrastruktury krytycznej cyberprzestrzeni można zaliczyć systemy łączności i sieci teleinformatycznych oraz systemy teleinformatyczne wspomagające pracę i funkcjonowanie pozostałych systemów infrastruktury krytycznej, których bezpieczeństwo warunkuje cyberbezpieczeństwo państwa. Tak więc należy uznać, że wszelkie metody, standardy i działania odnoszące się do ochrony infrastruktury krytycznej jednocześnie odnoszą się do ochrony infrastruktury krytycznej cyberprzestrzeni i zapewniania cyberbezpieczeństwa.

Bezpieczeństwo tych systemów, czyli bezpieczeństwo teleinformatyczne, to zbiór zagadnień z dziedziny telekomunikacji i informatyki związany z szacowaniem i kontrolą ryzyka wynikającego z korzystania z komputerów, sieci komputerowych i przesyłania danych do zdalnych lokalizacji, rozpatrywany z perspektywy poufności, integralności i dostępności danych (Wikipedia, 2018c). Zapewnienie bezpieczeństwa teleinformatycznego to zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie nieautoryzowanego oddziaływania na aparaturę kontrolną oraz systemy i sieci teleinformatyczne (NPOIK, 2015, s. 30). Jak widać, definiowane bezpieczeństwo teleinformatyczne jest ściśle warunkowane szacowaniem i kontrolą ryzyka w procesie postępowania z ryzykiem.

Ochronę teleinformatycznej infrastruktury krytycznej należy pojmować jako proces zapewnienia jej bezpieczeństwa. Proces ochrony infrastruktury krytycznej oparty jest na procesach spójnych z procesami zarządzania ryzykiem, zdefiniowanymi w normie PN ISO/IEC 27005:2014 oraz omówionymi powyżej. Składa się z następujących etapów:

- wskazanie zakresu i celów do osiągnięcia w ramach ochrony IK oraz adresatów tych działań;
- identyfikacja krytycznych zasobów, funkcji oraz określenia sieci powiązań (zależności) z innymi systemami IK, w tym podmiotami i organami;
- określenie ról i odpowiedzialności organów uczestniczących w procesie ochrony IK;
- ocena ryzyka;
- wskazanie priorytetów działania i dokonania ich hierarchizacji w zależności od wyników oceny ryzyka;
- rozwój i wdrażanie systemu ochrony infrastruktury krytycznej, w tym opracowanie i akceptacja planów ochrony i odtwarzania IK;
- testowanie (w ramach ćwiczeń) i przegląd (za sprawą audytu i samooceny) systemu ochrony IK oraz pomiar postępów na drodze do osiągnięcia celu;
- doskonalenie, rozumiane jako wprowadzanie modyfikacji i korekt w wyniku testów, przeglądów i pomiarów (NPOIK, 2015, s. 27).

Wszelkie działania podejmowane w celu zapewnienia ochrony IK, w tym IK cyberprzestrzeni, powinny być proporcjonalne do poziomu ryzyka zakłócenia jej funkcjonowania. Dotyczy to tym samym przyjętego modelu ochrony IK, jej rodzajów, a także użytych sił i środków. Z punktu widzenia NPOIK jest to element kluczowy, determinujący i uzasadniający działania podejmowane w celu obniżenia ryzyka zakłócenia funkcjonowania IK do poziomu akceptowalnego. Ocena ryzyka powinna być podstawą określenia standardów ochrony IK cyberprzestrzeni i ustalenia priorytetów działań (NPOIK, 2015, s. 28).

Przeprowadzanie okresowej oceny ryzyka zakłócenia funkcjonowania infrastruktury krytycznej powinno się odbywać:

- wraz z identyfikacją nowych zagrożeń, które wpływają lub mogą wpłynąć na poprawne funkcjonowanie infrastruktury krytycznej;
- wraz z przeglądem (aktualizacją) planu ochrony infrastruktury krytycznej;
- w celu zapewnienia zgodności ze wszystkimi dokumentami rządowymi (NPOIK, 2015, s. 30).

Ocena ryzyka wspomaga podejmowanie decyzji w zakresie procesu postępowania z ryzykiem. Działania podejmowane na rzecz zapewnienia bezpieczeństwa są odzwierciedleniem procesu postępowania z ryzykiem i mają na celu minimalizację ryzyka zakłócenia IK przez:

- zmniejszenie prawdopodobieństwa wystąpienia zagrożenia;
- zmniejszanie podatności;
- minimalizowanie skutków wystąpienia zagrożenia (NPOIK, 2015, s. 30).

Zastosowanie konkretnych środków zapewnienia bezpieczeństwa powinno być ściśle związane z oceną ryzyka zakłócenia funkcjonowania IK, w tym IK cyberprzestrzeni (NPOIK, 2015, s. 31). Ochrona infrastruktury krytycznej oparta jest ściśle na procesach zrządzania ryzykiem, od identyfikacji, przez analizę ocen, do procesu postępowania z ryzykiem, czyli wyboru i wdrażania najbardziej efektywnych środków i działań zwiększających poziom bezpieczeństwa.

## Podsumowanie

Cyberbezpieczeństwo jest istotnym komponentem bezpieczeństwa, dlatego też znajduje ono swoje miejsce w dokumentach strategicznych, operacyjnych i regulacyjnych dotyczących bezpieczeństwa i zarządzania kryzysowego. *Strategia Bezpieczeństwa Narodowego RP*, *Doktryna cyberbezpieczeństwa RP*, ustawa o zarządzaniu kryzysowym i *Narodowy Program Ochrony Infrastruktury Krytycznej* dają kierunkowe dyrektywy i operacyjne wytyczne co do wdrażania systemu bezpieczeństwa, w tym cyberbezpieczeństwa. Wyznaczane punkty odniesienia, ramy, cele, dyrektywy i działania przyczyniające się do osiągnięcia odpowiedniego poziomu cyberbezpieczeństwa odnoszą się do procesów zarządzania ryzykiem i opierają się na działaniach związanych z procesami zarządzania ryzykiem, co zostało przedstawione w treści artykułu, a zatem można powiedzieć, że zarządzanie ryzykiem determinuje cyberbezpieczeństwo. Niemniej jednak zastosowanie pełnego, systemowo ujętego procesu zarządzania ryzykiem, np. przedstawionego w normie PN EN ISO 27005:2014 – Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji, mogłoby przyczynić się do zwiększenia efektywności procesu zarządzania cyberbezpieczeństwem i uzyskania wysokiego jego poziomu.

BIBLIOGRAFIA

[1] *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Biuro Bezpieczeństwa Narodowego, Warszawa 2015.

[2] Kitler W., 2011, *Bezpieczeństwo Narodowe RP. Podstawowe kategorie. Uwarunkowania. System*, Wydawnictwo Akademii Obrony Narodowej, Warszawa.

[3] Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK), 2015, Rządowe Centrum Bezpieczeństwa, Warszawa.

[4] Łepkowski W. (red.), 2008, *Słownik terminów z zakresu bezpieczeństwa narodowego*, Akademia Obrony Narodowej, Warszawa.

[5] PN-ISO/IEC 27005:2014 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji, Polski Komitet Normalizacyjny, Warszawa.

[6] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2014*, 2014, Biuro Bezpieczeństwa Narodowego, Warszawa.

[7] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (DzU 2007 nr 89, poz. 590 ze zm.).

NETOGRAFIA

[1] Wikipedia, 2018a, *Bezpieczeństwo* (dostęp: 15.04.2019), https://pl.wikipedia.org/wiki/Bezpieczenstwo.

[2] Wikipedia, 2018b, *Bezpieczeństwo narodowe* (dostęp: 15.04.2019), https://pl.wikipedia.org/wiki/Bezpieczenstwo_narodowe.

[3] Wikipedia, 2018c, *Bezpieczeństwo teleinformatyczne* (dostęp: 15.04.2019), https://pl.wikipedia.org/wiki/Bezpieczenstwo_teleinformatyczne.