Zeszyty Naukowe SGSP 2021
2021, Nr 79, s. 83–103
ISSN: 0239-5223

DOI: 10.5604/01.3001.0015.2889

MGR INŻ. DOMINIKA BUJAK
absolwentka Szkoły Głównej Służby Pożarniczej
e-mail: dominika.bujak@tlen.pl

DR INŻ. MAGDALENA GIKIEWICZ
Szkoła Główna Służby Pożarniczej
e-mail: mgikiewicz@sgsp.edu.pl
ORCID: 0000-0002-4568-6750

WYKORZYSTANIE OPROGRAMOWANIA WSPOMAGAJĄCEGO ANALIZĘ SIECIOWĄ METODĄ „ŚCIEŻKI KRYTYCZNEJ" W ASPEKCIE OPRACOWYWANIA PLANU OCHRONY INFRASTRUKTURY KRYTYCZNEJ W POLSCE

ABSTRAKT

Artykuł przedstawia możliwości wykorzystania oprogramowania WinQSB wspomagającego analizę sieciową metodą „ścieżki krytycznej" w aspekcie opracowywania planu ochrony infrastruktury krytycznej w Polsce. W materiale uwzględniono najważniejsze definicje oraz podstawy prawne dotyczące infrastruktury krytycznej, a także odniesiono się do ogólnej charakterystyki ochrony obiektów infrastruktury krytycznej. W dalszej kolejności opisano optymalizację decyzji w zarządzaniu bezpieczeństwem poprzez wykorzystanie analizy sieciowej, co pozwoliło na zaprezentowanie

wykorzystania oprogramowania wspomagającego analizę sieciową do opracowania Planu Ochrony Infrastruktury Krytycznej w Przedsiębiorstwie Wodociągów i Kanalizacji.

SŁOWA KLUCZOWE

zarządzanie bezpieczeństwem, metoda ścieżki krytycznej, infrastruktura krytyczna, plan ochrony infrastruktury krytycznej, oprogramowanie, operator infrastruktury krytycznej

Przyjęty: 17.05.2021; Zrecenzowany: 08.09.2021; Zatwierdzony: 08.09.2021

THE USE OF THE NETWORK ANALYSIS SUPPORTING SOFTWARE BY THE CRITICAL PATH METHOD IN THE ASPECT OF DEVELOPING A CRITICAL INFRASTRUCTURE PROTECTION PLAN

ABSTRACT

The article presents the possibilities of using the WinQSB software supporting network analysis using the "critical path" method in the aspect of developing a critical infrastructure protection plan in Poland. The material presents the most important definitions and legal grounds for critical infrastructure, as well as the general characteristics for the protection of critical infrastructure facilities. Additionally, the optimization of decisions in safety management through the use of network analysis was discussed, in order to present a proprietary approach to the examination of the Critical Infrastructure Protection Plan in the Water and Sewerage Company. Particular emphasis was placed on the presentation of the results of tests performed with the use of the WinQSB software in the case study.

KEYWORDS

security management, Critical Path Method, critical infrastructure, Critical Infrastructure Protection Plan, software, Critical Infrastructure Operator

Received: 17.05.2021; Reviewed: 08.09.2021; Accepted: 08.09.2021

WSTĘP

Kluczowy wpływ na bezpieczeństwo państwa, jego obywateli oraz funkcjonowania wielu instytucji ma niezakłócone działanie infrastruktury krytycznej (IK). Ponadto ścisłe powiązania i zależności między poszczególnymi systemami IK dodatkowo wymuszają ochronę ciągłości jej funkcjonowania. W związku z powyższym niezwykle ważne jest właściwe wyznaczenie infrastruktury krytycznej, identyfikacja zagrożeń oraz odpowiednie zaplanowanie i realizacja jej ochrony. Odpowiedzią na tego typu potrzeby jest ciągłe rozwijanie i doskonalenie, stosownie do zmieniających się uwarunkowań tego procesu.

Obiekty oraz systemy zaliczane do infrastruktury krytycznej powinny posiadać plany ochrony infrastruktury krytycznej (POIK). POIK jest dokumentem określającym działania adekwatne do rodzaju i skali zagrożenia. Rzetelnie i szczegółowo przygotowany plan jest nieodzownym narzędziem do celów ochrony infrastruktury krytycznej. Opisane w nim działania wpływają na usprawnienie procesu decyzyjnego podczas występowania zagrożeń, dlatego niezbędne jest odpowiednie przygotowanie przed rozpoczęciem jego tworzenia.

Według autorek użyteczne jest pisemne rozplanowanie zbierania potrzebnych informacji, prowadzenia badań oraz wcześniejsze wykonanie zapisu całego dokumentu. W tym celu zastosowano w artykule metodę ścieżki krytycznej, która pozwala na określenie: czynności wykonywanych po sobie, czynności wykonywanych równocześnie oraz czynności, które można rozpocząć później, nie wpływając na opóźnienie realizacji całego przedsięwzięcia. Wykorzystanie tej metody pozwala na udoskonalenie procesu tworzenia planu oraz monitorowania jego realizacji.

Sposób podejścia do opracowania Planu Ochrony Infrastruktury Krytycznej dla Przedsiębiorstwa Wodociągów i Kanalizacji opiera się na własnych obserwacjach autorek oraz subiektywnej ocenie eksperta ds. zarządzania bezpieczeństwem.

1. WPROWADZENIE DO PROBLEMATYKI INFRASTRUKTURY KRYTYCZNEJ W POLSCE

Dzięki intensywnemu rozwojowi gospodarczemu i społecznemu mieszkańcy Polski od kilkunastu lat mogą korzystać z usług pozwalających na utrzymanie

odpowiedniego standardu życia. Ma to szczególne znaczenie również ze względu na sprawne funkcjonowanie społeczeństwa, państwa i gospodarki oraz ich dalszy rozwój [1]. Jednocześnie postęp cywilizacyjny oraz globalizacja przyczyniają się do uzależnienia wysoko uprzemysłowionych państw od dostaw wody, żywności, energii, technologii czy usług bankowo-finansowych, przez co stają się bardzo wrażliwe na ich utratę [2]. W przeszłości poczucie bezpieczeństwa utożsamiane było głownie z niewystępowaniem zagrożeń zewnętrznych, jednak obecnie kojarzone jest ono przede wszystkim ze sprawnym funkcjonowaniem, zarówno w części technologicznej (energetyka, łączność, transport, edukacja, zakłady wytwórcze itp.), jak i społecznej (ochrona ludności, opieka medyczna itp.) infrastruktury państwa. „Usługi te oraz dostarczająca je infrastruktura zostały określone mianem infrastruktury krytycznej" [3]. Zgodnie z ustawą z 26 kwietnia 2007 r. o zarządzaniu kryzysowym infrastruktura krytyczna (IK) 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" [4]. Przytoczone w definicji ścisłe powiązania i zależności pomiędzy elementami infrastruktury krytycznej mogą powodować tzw. efekt domina. Oznacza to, że zakłócenie działania jednego z nich wpływa na pozostałe elementy systemu i oddziałuje na ciągłość funkcjonowania instytucji, administracji publicznej, prywatnych przedsiębiorstw oraz całego społeczeństwa [2, 5]. Uszkodzenia bądź zniszczenia infrastruktury krytycznej mogą być spowodowane działalnością człowieka (uszkodzenia urządzeń i systemów oraz zaniedbania w ich terminowej obsłudze) lub siłami natury (pożary, powodzie, upały, niskie temperatury, huraganowe wiatry), których konsekwencją jest ryzyko utraty ciągłości świadczenia kluczowych usług. Ponadto rozwijająca się globalizacja stwarza dogodne warunki organizacjom przestępczym, głównie terrorystycznym i cyberterrorystycznym, na dostęp do obiektów IK. Incydenty tego typu wpływają również negatywnie na mienie, zdrowie, życie obywateli oraz rozwój gospodarczy państwa. W związku z tym „należy stwierdzić, że infrastruktura krytyczna pełni kluczową rolę w funkcjonowaniu państwa i życiu jego obywateli, a jej ochrona jest jednym z priorytetów stojących przed państwem polskim" [6]. Obowiązek ten spoczywa głównie na administracji rządowej i samorządowej.

Ochrona obiektów wchodzących w skład krajowej infrastruktury krytycznej (KIK) wiąże się przede wszystkim z wysokimi kosztami. W związku z tym proces wyznaczania tejże infrastruktury powinien charakteryzować się pełną starannością i odpowiednim przygotowaniem. Wskazówki w formie ogólnych zasad organizowania ochrony obiektów można odnaleźć w ustawie o ochronie osób i mienia [7].

Infrastrukturę krytyczną tworzy wiele obiektów i instalacji, które dzielą się na systemy:

a) zaopatrzenia w energię, surowce energetyczne i paliwa,
b) łączności,
c) sieci teleinformatycznych,
d) finansowe,
e) zaopatrzenia w żywność,
f) zaopatrzenia w wodę,
g) ochrony zdrowia,
h) transportowe,
i) ratownicze,
j) zapewniające ciągłość działania administracji publicznej,
k) produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych [4].

Wymieniony skład systemów należących do infrastruktury krytycznej nie jest przypadkowy ze względu na ogromne znaczenie dla bezpieczeństwa państwa. Właściwe ich rozmieszczenie oraz ochrona przyczyniają się do minimalizacji skutków zdarzeń podczas wystąpienia sytuacji kryzysowych. W związku z tym wysoki poziom rozwinięcia IK wpływa na zwiększenie bezpieczeństwa wewnętrznego, wzrost gospodarczy, a także poprawia standard życia społecznego [8].

2. UWARUNKOWANIA OCHRONY INFRASTRUKTURY KRYTYCZNEJ W POLSCE

Z powodu swojej złożoności ochrona obiektów infrastruktury krytycznej stanowi duże wyzwanie. Wynika ono z wielowariantowości zagrożeń, m.in. katastrof, awarii, działania sił natury czy ataków terrorystycznych i cyberterrorystycznych. Kwestia ochrony IK ma wpływ na bezpieczeństwo narodowe

i jest zadaniem danego państwa. Zgodnie z europejskimi aktami prawnymi ochrona IK rozumiana jest jako „wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków" [9].

Podstawę prawną stanowi również ustawa o powszechnym obowiązku obrony Rzeczpospolitej Polskiej. Zgodnie z nią do zadań w ramach zapewniania zewnętrznego bezpieczeństwa państwa należy „określanie obiektów szczególnie ważnych dla bezpieczeństwa państwa (…) oraz przygotowywanie ich szczególnej ochrony" [10]. Ponadto rozporządzenie Rady Ministrów normuje reguły ochrony szczególnie ważnych dla bezpieczeństwa i obronności państwa obiektów [11]. Na podstawie wspomnianych dokumentów opracowano podstawy ochrony IK, która polega na zapobieganiu zagrożeniom, ograniczaniu skutków w przypadków ich zaistnienia oraz podejmowaniu działań naprawczych [5].

Na ochronę infrastruktury krytycznej składają się przygotowanie i prowadzenie. Przygotowanie to czynności oraz starania wykonywane z myślą o czymś, co ma nastąpić, zawierające w sobie zadania planowania oraz organizowania [7].

Planowanie to inaczej przygotowywanie, układanie, opracowywanie, zamierzanie czegoś, patrzenie w przyszłość [12]. Czynność ta identyfikowana jest z procesem składającym się z opracowywania planów, przewidywania przyszłości oraz działań skierowanych na osiągnięcie założonego celu [13]. Planować można jedynie to, na co ma się wpływ. Pozostające poza kontrolą planującego zdarzenia mogą być jedynie prognozowane lub przewidywane.

Planowanie ochrony obiektów infrastruktury krytycznej ma na celu opracowanie koncepcji działania składającej się z:

- analizy zadania i wytycznych;
- oceny obiektu i jego otoczenia;
- analizy i oceny zagrożeń;
- kalkulacji sił i środków,
- oceny zmian w obiekcie [7].

Według K. Sienkiewicz-Małyjurek i F. Krynojewskiego ochrona IK realizowana jest w sześciu etapach:

1) sporządzanie wykazu IK – odpowiednie rozpoznanie elementów infrastruktury krytycznej umożliwiające określenie właściwych działań w celu jej ochrony,

2) analiza ryzyka zagrożeń dla rozpoznanej IK – identyfikacja, ocena i monitorowanie poziomu ryzyka w celu określenia działań skierowanych na obniżenie jego negatywnego wpływu na funkcjonowanie IK,
3) opracowanie wykazu sił i środków do ochrony IK – przygotowanie zasobów zapewniających bezpieczeństwo IK,
4) wyznaczanie działań wykonywanych w sytuacji zagrożenia – opracowanie gotowych instrukcji postępowania w przypadku wystąpienia zagrożeń wynikających z analizy ryzyka,
5) wyznaczanie działań odtwarzających IK – przygotowanie form współpracy i wsparcia przy odtwarzaniu IK,
6) przygotowanie kanałów komunikacji – wyznaczenie osób odpowiedzialnych za utrzymywanie kontaktów z właściwymi podmiotami w zakresie ochrony IK [5].

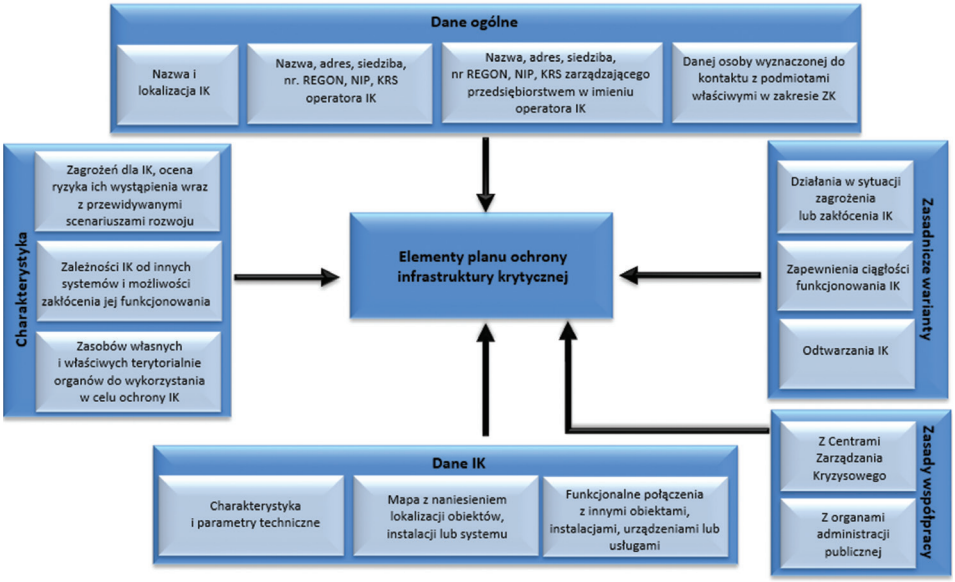
Zgodnie z Dyrektywą Rady 2008/114/WE z 8 grudnia 2008 r. elementy zaliczone do IK powinny posiadać swoje plany ochrony przewidujące działania adekwatne do rodzaju i skali zagrożenia [8, 9]. Obowiązek posiadania planu ochrony infrastruktury krytycznej uznaje się również za spełniony, jeżeli istnieje plan przygotowany na podstawie innych przepisów, ale odpowiadający wymogom POIK. Ustawa z 26 kwietnia 2007 r. o zarządzaniu kryzysowym obliguje do opracowywania powyższych planów właścicieli oraz samoistnych i zależnych posiadaczy obiektów, instalacji lub urządzeń IK [4]. Potwierdzeniem do sporządzenia planu jest decyzja uzyskana od dyrektora Rządowego Centrum Bezpieczeństwa o uznaniu systemu/obiektu za infrastrukturę krytyczną. Operator IK sporządza plan w terminie 9 miesięcy od daty otrzymania od dyrektora RCB informacji o ujęciu w wykazie. Sposób tworzenia, aktualizacje, strukturę oraz warunki uznania POIK określa rozporządzenie Rady Ministrów z 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej [14]. Rysunek 1 przedstawia strukturę planu zgodną z powyższym rozporządzeniem. Jednak operator IK może zawrzeć w planie również inne elementy, biorąc pod uwagę specyfikę IK lub charakterystykę zagrożeń. Następnie POIK musi zostać podpisany przez operatora tej infrastruktury. Plan ten jest dokumentem niejawnym. Opracowany POIK wymaga uzgodnienia z:

a) „wojewodą,
b) komendantem wojewódzkim Państwowej Straży Pożarnej,
c) komendantem wojewódzkim Policji,

d) dyrektorem regionalnego zarządu gospodarki wodnej,
e) wojewódzkim inspektorem nadzoru budowlanego,
f) wojewódzkim lekarzem weterynarii,
g) państwowym wojewódzkim inspektorem sanitarnym,
h) dyrektorem urzędu morskiego,
i) ministrem lub kierownikiem urzędu centralnego, we właściwości którego znajduje się system, do którego została zaliczona dana infrastruktura krytyczna [14]."

W przypadku niespełnienia wymogów określonych w rozporządzeniu przedstawienia metod niegwarantujących bezpieczeństwa IK lub braku spójności z NPOIK wymienione podmioty powinny odmówić uzgodnienia planu [14].

Przygotowany POIK wraz z arkuszem uzgodnień operator IK przedkłada do zatwierdzenia dyrektorowi RCB w terminie 14 dni od daty ostatniego uzgodnienia. Dyrektor ma 90 dni od daty przedłożenia na zatwierdzenie planu. Aktualizacja planów ochrony infrastruktury krytycznej odbywa się w zależności od potrzeb, jednak nie rzadziej niż raz na dwa lata [14].



Rys. 1. Elementy planu ochrony infrastruktury krytycznej
Źródło: opracowanie własne na podstawie [14]

3. OPTYMALIZACJA DECYZJI W ZARZĄDZANIU BEZPIECZEŃSTWEM POPRZEZ WYKORZYSTANIE ANALIZY SIECIOWEJ

W przeciwdziałaniu zdarzeniom powodującym zagrożenia bezpieczeństwa konieczne jest ich przewidywanie, odpowiednio wczesne wykrywanie oraz przygotowanie na wypadek, gdyby zapobieganie było nieskuteczne. Pozwala to m.in. na podejmowanie właściwych decyzji podczas wystąpienia sytuacji kryzysowych [15].

E. Kołodziński wyróżnia siedem etapów klasycznego procesu decyzyjnego:

1. „identyfikowanie sytuacji decyzyjnej,
2. sformułowanie problemu decyzyjnego,
3. zbudowanie modelu decyzyjnego,
4. wyznaczenie decyzji dopuszczalnych,
5. wyznaczenie decyzji optymalnej,
6. podjęcie decyzji ostatecznej" [16].

Zbiór wszystkich czynników wpływających na podjęcie decyzji określa się sytuacją decyzyjną. Osoba podejmująca decyzję wybiera zwykle opcję zgodną z ustalonymi warunkami ograniczającymi. Taką decyzję określa się jako dopuszczalną. Decydent może mieć jednak nawet kilkadziesiąt wariantów, z których kilka spełniałoby warunki ograniczające. W związku z tym ma do wyboru kilka dopuszczalnych decyzji. Biorąc pod uwagę wyznaczone cele, niektóre decyzje mogą okazać się lepsze od innych. Należy zatem zastanowić się, którą decyzję wybrać. Osoba podejmująca decyzję wybiera najlepszą opcję według określonego kryterium, na podstawie którego możemy ocenić decyzje jako gorsze lub lepsze. Kryterium to nazywane jest kryterium wyboru, natomiast wybraną na jego podstawie decyzję – optymalną. Należy pamiętać, że określenie kryterium wyboru jest niezbędne przy podejmowaniu decyzji do wskazania decyzji optymalnej [17].

Procesy decyzyjne w zarządzaniu bezpieczeństwem charakteryzują się dużą złożonością. Utrudnieniem dla decydenta jest również stres związany z odpowiedzialnością za podejmowane decyzje oraz ograniczony zwykle czas na ich podejmowanie. Rozwiązanie tych problemów może stanowić wykorzystanie oprogramowania komputerowego do wspomagania czynności wykonywanych przez decydenta w poszczególnych etapach procesu decyzyjnego.

Optymalizację decyzji w zarządzaniu bezpieczeństwem można wykorzystać także podczas wyłaniania infrastruktury krytycznej bądź planowania sposobów jej ochrony. Pozwala to na ograniczanie kosztów, czasu i poziomu ryzyka. Są to działania, na które składa się wiele czynności. W związku z tym znaczące jest kontrolowanie ich przebiegu poprzez panowanie zarówno nad czasami realizacji poszczególnych czynności, jak i całego przedsięwzięcia [18]. Jak się okazuje, niektóre z nich mogą być wykonywane równolegle, natomiast pozostałe rozpoczynają się dopiero po zakończeniu innych działań [19]. W takim przypadku pomocne okazują się metody programowania sieciowego, które pozwalają na poprawne i efektywne zaplanowanie realizacji projektu [18].

Jedną z metod programowania sieciowego jest metoda ścieżki krytycznej, określana również metodą CPM (z ang. Critical Path Method), która została opracowana w latach 50-tych XX w. w Stanach Zjednoczonych. Jest to deterministyczna technika, wspomagająca analizę czasową danego przedsięwzięcia [20].

Przeprowadzanie obliczeń ręcznych wspomagających analizę sieciową jest procesem żmudnym i wymagającym dużego nakładu pracy. W związku z tym określenie decyzji optymalnej może wiązać się ze zbyt wysokimi kosztami w stosunku do korzyści wynikających z jej zastosowania. Ponadto, przy wykonywaniu obliczeń ręcznych, istnieje większe prawdopodobieństwo popełnienia błędów rachunkowych, co prowadzi do rekomendacji nieefektywnej decyzji przy uwzględnieniu kosztu jej przygotowania.

W celu uniknięcia przedstawionych powyżej trudności warto wykorzystywać możliwości stwarzane przez rozwój technologiczny. Jednym z takich rozwiązań jest oprogramowanie pod nazwą WinQSB (z ang. Windows Quantitative Support for Business). Jest to darmowy zestaw dziewiętnastu narzędzi umożliwiających rozwiązywanie zadań z zakresu programowania matematycznego i wspomagających użytkownika w realizacji procesu obliczeniowego.

WinQSB jest przeznaczony do starszych wersji systemu operacyjnego Windows, jednak uruchomienie maszyny wirtualnej umożliwia jego pracę również na innych systemach. Ponadto w tym programie do oznaczenia liczb dziesiętnych używa się kropki zamiast przecinka, natomiast daty w raportach generowane są w standardzie amerykańskim, tj. mm-dd-rrrr [21]. W celu wspomagania analizy sieciowej wykorzystuje się moduł PERT_CPM.

4. WYKORZYSTANIE OPROGRAMOWANIA WSPOMAGAJĄCEGO ANALIZĘ SIECIOWĄ DO OPRACOWANIA PLANU OCHRONY INFRASTRUKTURY KRYTYCZNEJ W PRZEDSIĘBIORSTWIE WODOCIĄGÓW I KANALIZACJI

W związku z dużym znaczeniem dla bezpieczeństwa państwa i życia jego obywateli niektóre obiekty PWiK kwalifikuje się jako infrastrukturę krytyczną. Zgodnie z dyrektywą Rady 2008/114/WE z 8 grudnia 2008 r. opracowuje się dla nich plany ochrony infrastruktury krytycznej [9]. Zawierają one m.in. podstawowe dane dotyczące IK, charakterystykę zagrożeń oraz warianty działania w sytuacji zagrożenia. POIK określa również zasady współpracy z właściwymi miejscowo centrami zarządzania kryzysowego i organami administracji publicznej. Ponadto plany te wyposażają współpracujące podmioty w gotowe narzędzia diagnostyczne, jak również w bazę roboczą służącą skutecznemu przygotowaniu i reagowaniu podczas wystąpienia zagrożeń oraz odtwarzaniu IK.

Celem POIK jest określenie zasobów własnych oraz zasobów właściwych terytorialnie organów, które będą wykorzystywane w celu ochrony infrastruktury krytycznej. W ten sposób plan ma zagwarantować natychmiastową interwencję w przypadku zakłóceń działania IK, a także ograniczyć ich rozwój. Plan ochrony infrastruktury krytycznej powinien być aktualizowany w zależności od potrzeb wynikających ze zmian legislacyjnych oraz doświadczeń praktycznych, jednak nie rzadziej niż raz na dwa lata.

W niniejszym artykule jako przykład wykorzystania oprogramowania wspomagającego analizę sieciową metodą „ścieżki krytycznej" przyjęto opracowanie Planu Ochrony Infrastruktury Krytycznej dla Przedsiębiorstwa Wodociągów i Kanalizacji. W tym celu stworzono harmonogram czynności w formie tabeli zawierający czynności, które należy wykonać, czasy ich trwania oraz określono czynności je poprzedzające. Sformułowanie zadań oraz oszacowanie czasów jest subiektywną oceną autorki pracy oraz eksperta do spraw zarządzania bezpieczeństwem wykonanych podczas wywiadu eksperckiego. Ekspert posiada kilkunastoletnie doświadczenie w pracy w zarządzaniu kryzysowym, przedsiębiorstwach wodociągów i kanalizacji oraz opracowywaniu planów ochrony infrastruktury krytycznej,

Tab. 1. Harmonogram opracowania Planu Ochrony Infrastruktury Krytycznej

1. Czynność	2. Opis czynności	3. Czynności poprzedzające	4. Czas trwania t_{ij} (dni)
CHARAKTERYSTYKA OBIEKTU			
A	określenie danych ogólnych zawierając: podstawowe informacje dotyczące obiektu IK, operatora IK, osoby odpowiedzialnej za utrzymanie kontaktów z zakresu ochrony IK oraz dane osoby sporządzającej Plan	-	7
B	sporządzenie charakterystyki obiektu uwzględniającej: podstawowe parametry techniczne, procesy technologiczne, zapotrzebowanie na reagenty chemiczne i surowce energetyczne oraz ochrona fizyczna i techniczna obiektu	A	25
C	utworzenie mapy z naniesieniem lokalizacji obiektu PWiK	A	3
FUNKCJONALNE POŁĄCZENIA Z INNYMI OBIEKTAMI, INSTALACJAMI, URZĄDZENIAMI LUB USŁUGAMI			
D	stworzenie planu sieci wodociągowej miasta z podziałem na strefy zasilania	C	8
E	przygotowanie zakresu stref obsługiwanych przez poszczególne oczyszczalnie ścieków	D	8
OCHRONA OSOBOWA I TELEINFORMATYCZNA OBIEK IK			
F	opracowanie postępowania: w sprawie zatrudnienia oraz z osobami odchodzącymi z pracy	A	4
G	sformułowanie zasad ochrony kluczowego personelu	F	6
H	określenie postępowania z usługodawcami i podwykonawcami	G	5
I	stworzenie procedur ochrony teleinformatycznej	H	10

cd. Tab. 1.

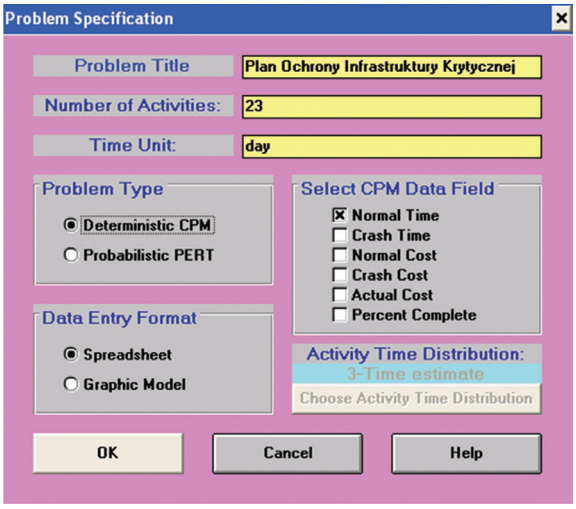
1. Czynność	2. Opis czynności	3. Czynności poprzedzające	4. Czas trwania t_{ij} (dni)
CHARAKTERYSTYKA			
J	identyfikacja zagrożeń dla infrastruktury krytycznej oraz ocena ryzyka ich wystąpienia wraz z przewidywalnymi scenariuszami rozwoju zdarzeń	E	30
K	weryfikacja zależności infrastruktury krytycznej od pozostałych systemów infrastruktury krytycznej oraz możliwości zakłócenia jej funkcjonowania w wyniku zakłóceń powstałych w pozostałych systemach infrastruktury krytycznej	J	10
L	przygotowanie zasad dostaw reagentów oraz zabezpieczenie dostępu do miejsc składowania materiałów niebezpiecznych dla osób nieupoważnionych	B, K	5
M	określenie zasobów własnych możliwych do wykorzystania w celu ochrony infrastruktury krytycznej	L	3
N	określenie zasobów właściwych terytorialnie organów, możliwych do wykorzystania w celu ochrony infrastruktury krytycznej	L	6
ZASADNICZE WARIANTY			
O	wskazanie czynności po wprowadzeniu stopni alarmowych	I, M, N	15
P	wskazanie działań w sytuacji zagrożenia lub zakłócenia funkcjonowania infrastruktury krytycznej	O	5
Q	opracowanie sposobu komunikacji z mediami	P	2
R	zapewnienie ciągłości funkcjonowania infrastruktury krytycznej	Q	10
S	definiowanie możliwości odtwarzania infrastruktury krytycznej	R	8

cd. Tab. 1.

1. Czynność	2. Opis czynności	3. Czynności poprzedzające	4. Czas trwania t_{ij} (dni)
ZASADY WSPÓŁPRACY			
T	określenie zasad współpracy z właściwymi miejscowo centrami zarządzania kryzysowego	S	5
U	określenie zasad współpracy z właściwymi miejscowo organami administracji publicznej	S	8
INFORMACJE DODATKOWE			
V	planowanie szkoleń w ramach ochrony infrastruktury krytycznej	T, U	2
W	uzgodnienia/podpisywanie arkusza uzgodnień	V	45

Źródło: opracowano na podstawie [14] oraz subiektywnej oceny eksperta do spraw zarządzania bezpieczeństwem

Na podstawie sporządzonego harmonogramu czynności uzupełniono okno modułu PERT_CPM pakietu WinQSB. Problem zatytułowano jako Plan Ochrony Infrastruktury Krytycznej, wpisano liczbę czynności (21) oraz określono jednostkę czasu (dzień – day).



Rys. 2. Okno wyboru specyfikacji modułu PERT_CPM pakietu WinQSB
Źródło: opracowanie własne

W oparciu o stworzony harmonogram czynności uzupełniono również kolejne okno. Wprowadzono czynności bezpośrednio poprzedzające oraz czasy trwania czynności rozpatrywanych.

Activity Number	Activity Name	Immediate Predecessor (list number/name, separated by ',')	Normal Time
1	A		7
2	B	A	25
3	C	A	3
4	D	C	8
5	E	D	8
6	F	A	4
7	G	F	6
8	H	G	5
9	I	H	10
10	J	E	30
11	K	J	10
12	L	B,K	5
13	M	L	3
14	N	L	6
15	O	I,M,N	15
16	P	O	5
17	Q	P	2
18	R	Q	10
19	S	R	8
20	T	S	5
21	U	S	8
22	V	T,U	2
23	W	V	45

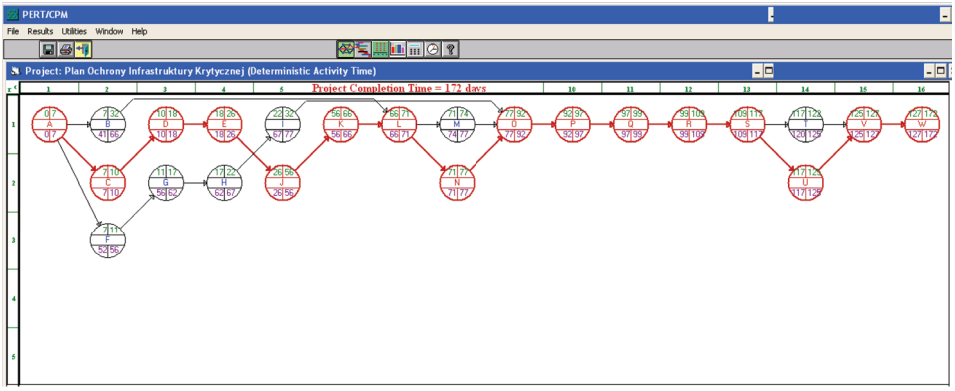
Rys. 3. Okno wprowadzanych danych czynności poprzedzających oraz czasów trwania rozpatrywanych czynności
Źródło: opracowanie własne

W dalszej kolejności program wygenerował tabelę zawierającą najwcześniejszy moment rozpoczęcia czynności, najwcześniejszy moment zakończenia czynności, najpóźniejszy moment rozpoczęcia czynności oraz najpóźniejszy moment zakończenia czynności, rezerwy czasowe dla każdej czynności, a także wskazano czynności krytyczne tworzące ścieżkę krytyczną.

03-04-2021 15:22:05	Activity Name	On Critical Path	Activity Time	Earliest Start	Earliest Finish	Latest Start	Latest Finish	Slack (LS-ES)
1	A	Yes	7	0	7	0	7	0
2	B	no	25	7	32	41	66	34
3	C	Yes	3	7	10	7	10	0
4	D	Yes	8	10	18	10	18	0
5	E	Yes	8	18	26	18	26	0
6	F	no	4	7	11	52	56	45
7	G	no	6	11	17	56	62	45
8	H	no	5	17	22	62	67	45
9	I	no	10	22	32	67	77	45
10	J	Yes	30	26	56	26	56	0
11	K	Yes	10	56	66	56	66	0
12	L	Yes	5	66	71	66	71	0
13	M	no	3	71	74	74	77	3
14	N	Yes	6	71	77	71	77	0
15	O	Yes	15	77	92	77	92	0
16	P	Yes	5	92	97	92	97	0
17	Q	Yes	2	97	99	97	99	0
18	R	Yes	10	99	109	99	109	0
19	S	Yes	8	109	117	109	117	0
20	T	no	5	117	122	120	125	3
21	U	Yes	8	117	125	117	125	0
22	V	Yes	2	125	127	125	127	0
23	W	Yes	45	127	172	127	172	0
	Project	Completion	Time	=	172	days		
	Number of	Critical	Path(s)	=	1			

Rys. 4. Czasy czynności
Źródło: opracowanie własne

Następny etap polegał na wygenerowaniu sieci czynności dla POIK w formie graficznej, którą przedstawia rysunek 5. Ścieżka krytyczna została oznaczona na czerwono. Jest to ciąg czynności – opóźnienie którejkolwiek z nich opóźni zakończenie całego przedsięwzięcia. Wyznaczenie ścieżki krytycznej ułatwia monitorowanie przebiegu projektu oraz ocenę wpływu opóźnień rozpoczęcia czynności na końcowy termin [22].



Rys. 5. Sieć czynności z oznaczoną na czerwono ścieżką krytyczną
Źródło: opracowanie własne

Ostatni etap to przedstawianie czynności krytycznych podczas tworzenia POIK.

03-04-2021	Critical Path 1
1	A
2	C
3	D
4	E
5	J
6	K
7	L
8	N
9	O
10	P
11	Q
12	R
13	S
14	U
15	V
16	W
Completion Time	172

Rys. 6. Okno z wyszczególnionymi czynnościami krytycznymi przedsięwzięcia
Źródło: opracowanie własne

Całkowity czas realizacji tworzenia planu wyniesie 172 dni. Czynności A, C, D, E, J, K, L, N, O, P, Q, R, S, U, V, W to czynności krytyczne. Oznacza to, że nie mogą być rozpoczęte później oraz zostać wydłużone, ponieważ spowodowały to opóźnienie realizacji przedsięwzięcia. Dla czynności B, F, G, H, I, M oraz T istnieją rezerwy czasowe, w związku z czym mogą one zostać rozpoczęte później (w granicach ich rezerw czasowych) bez wpływu na końcowy termin realizacji całego przedsięwzięcia. Zidentyfikowanie ścieżki krytycznej pozwala na kontrolę realizacji zadań, od których zależy moment zakończenia projektu.

5. PODSUMOWANIE

Przeciwdziałanie i zapobieganie wszelkim zagrożeniem bezpieczeństwa państwa powinno być priorytetowym zadaniem organów rządowych, administracji publicznej oraz podmiotów gospodarczych. Ze względu na istotny wpływ infrastruktury krytycznej na państwo i jakość życia obywateli jej odpowiednie funkcjonowanie oraz ochrona jest niezwykle ważna. Ponadto ochrona IK może przybierać wymiar międzynarodowy, ponieważ zakłócenie jej poprawnego działania w jednym kraju może wpływać na jej funkcjonowanie w innym. Zatem ochrona infrastruktury krytycznej powinna być sprawowana nie tylko podczas sytuacji kryzysowej, ale także w czasie pokoju. Należy ją również stale monitorować i dostosowywać do zachodzących zmian w celu zapewnienia pełnej integralności oraz ciągłości działań.

Na ochronę IK składają się przygotowanie i prowadzenie. Przygotowanie określa czynności wykonywane z myślą o czymś, co ma nastąpić oraz zawiera zadania planowania, czyli świadomego dążenia do celu przez określone wcześniej działania. Planowanie ochrony obiektów IK składa się z pięciu etapów: analizy zadania i wytycznych, oceny obiektu wraz z jego otoczeniem, analizy i oceny zagrożeń, kalkulacji sił i środków oraz oceny zmian w obiekcie.

Wykonywanie planu dla konkretnych obiektów IK może się bardzo różnić od siebie. Zależy to przede wszystkim od specyfiki danej infrastruktury krytycznej oraz charakterystyki zagrożeń, a także od doświadczenia i kompetencji osób przygotowujących niezbędne procedury oraz dokumenty planistyczne. Ze względu na dużą liczbę zadań do wykonania postanowiono wykorzystać w tym celu metodę ścieżki krytycznej. Jest to jedna z metod analizy sieciowej pozwalająca na graficzne planowanie przedsięwzięć,

usprawniająca przebieg ich wykonania oraz umożliwiająca kontrolowanie ich przebiegu poprzez panowanie nad czasami realizacji poszczególnych zadań oraz całego przedsięwzięcia.

Zastosowanie metody ścieżki krytycznej pozwala określić czynności krytyczne, których nie można rozpocząć później niż zostało to ustalone oraz rozciągnąć w czasie ich wykonania, ponieważ wpłynęłoby to na opóźnienie realizacji całego przedsięwzięcia.

REFERENCES/BIBLIOGRAFIA

1. Bujak D., Modlińska A., *Bezpieczeństwo Polski w świetle ochrony infrastruktury krytycznej* [w:] Gikiewicz M., Tryboń M., Prędecka A., Bralewski A., *Interdyscyplinarność bezpieczeństwa – teoria, praktyka, edukacja,* Szkoła Główna Służby Pożarniczej, Warszawa 2017.
2. Tyburska A. (red.), *Ochrona infrastruktury krytycznej*, Szczytno 2010.
3. Narodowy Program Ochrony Infrastruktury Krytycznej (2020), RCB.
4. Ustawa z 26 kwietnia 2007 r. o zarządzaniu kryzysowym (tj. Dz.U. z 2020 r. poz. 1856).
5. Sienkiewicz-Małyjurek K., Krynojewski F., *Zarządzanie kryzysowe w administracji publicznej,* Wydanie II, Difin, Warszawa 2010.
6. Narodowy Program Ochrony Infrastruktury Krytycznej (2013), RCB.
7. Lidwa W., Krzeszowski W., Więcek W., Kamiński P., *Ochrona infrastruktury krytycznej,* Akademia Obrony Narodowej, Warszawa 2012.
8. Mroczko F., *Wybrane problemy ochrony infrastruktury krytycznej* [w:] Gałecki A., Kurkiewicz A., Mikołajczyk S., *Infrastruktura krytyczna w procesie zarządzania w sytuacjach kryzysowych*, Poznań 2014.
9. Dyrektywa Rady 2008/114/WE z 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony, art. 2. (Dz.Urz. UE L 345 z 23.12.2008).
10. Ustawa z 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz.U. z 2021 r. poz. 372).
11. Rozporządzenie Rady Ministrów z 18 stycznia 2019 r. zmieniające rozporządzenie w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony (Dz.U. z 2019 r. poz. 250).

12. Dunaj B. (red.), *Słownik współczesnego języka polskiego*, tom II, Przegląd Reader's Digest, Warszawa 2001.
13. Kitler W. (red.), *Planowanie cywilne w zarządzaniu kryzysowym,* Akademia Obrony Narodowej, Warszawa 2011.
14. Rozporządzenie Rady Ministrów z 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (Dz.U. z 2010 r. nr 83 poz. 542).
15. http://www.uwm.edu.pl/mkzk/download/wprowadzenie.pdf (dostęp 26.02.2021).
16. Kołodziński (red.), *Wspomaganie decyzji w bezpieczeństwie,* Wojskowa Akademia Techniczna, Warszawa 2014.
17. http://tarapata.strefa.pl/p_efektywnosc_systemow_informatycznych/download/optymalizacja_decyzji_inwestycyjnych_czI.pdf (dostęp 20.02.2021).
18. Majchrzak E. (red.), *Badania operacyjne. Teoria i zastosowania*, Wydawnictwo Politechniki Śląskiej, Gliwice 2007.
19. Sikora W. (red.), *Badania operacyjne*, PWE, Warszawa 2008.
20. https://mfiles.pl/pl/index.php/CPM (dostęp 20.02.2021).
21. https://pdf.helion.pl/e_oefr/e_oefr.pdf (dostęp 26.02.2021).
22. Kukuła K. (red. nauk.), *Badania operacyjne w przykładach i zadaniach*, wyd. V, Wydawnictwo Naukowe PWN, Warszawa 2004.

DOMINIKA BUJAK – absolwentka studiów I stopnia na kierunku inżynieria bezpieczeństwa cywilnego oraz studiów II stopnia na kierunku inżynieria bezpieczeństwa pożarowego w Szkole Głównej Służby Pożarniczej. Szczególnymi zainteresowaniami naukowymi autorki są badania operacyjne, zarządzanie kryzysowe w Polsce i w Portugalii, infrastruktura krytyczna oraz instalacje tryskaczowe.

DOMINIKA BUJAK – Graduate of the first degree course in civil safety engineering and the second degree course in fire safety engineering at the Main School of Fire Service. Her specific scientific interests include operational research, crisis management in Poland and Portugal, critical infrastructure and sprinkler systems.

MAGDALENA GIKIEWICZ – kierownik Zakładu Bezpieczeństwa Powszechnego Szkoły Głównej Służby Pożarniczej oraz kierownik zespołu SGSP międzynarodowego projektu badawczego EU-SENSE. W przeszłości była kierownikiem Zakładu Metodologii i Badań SGSP. Bierze udział w projektach badawczych realizowanych na rzecz obronności i bezpieczeństwa państwa finansowanych przez Ministerstwo Nauki i Szkolnictwa Wyższego oraz Narodowe Centrum Badań i Rozwoju. Pełni

funkcje przewodniczącej i członkini komitetów naukowych, programowych oraz organizacyjnych licznych krajowych i międzynarodowych konferencji oraz seminariów naukowych. Zainteresowania naukowe dr inż. Magdaleny Gikiewicz dotyczą bezpieczeństwa powszechnego, badań operacyjnych, w tym optymalizacji i programowania sieciowego, zarządzania kryzysowego, w tym planowania cywilnego, kultury bezpieczeństwa, w tym badania poziomu bezpieczeństwa, narzędzi kształtowania kultury bezpieczeństwa, metodologii badań w naukach o bezpieczeństwie.

MAGDALENA GIKIEWICZ – Head of the Department of Public Security at the Main School of Fire Service and team leader of the Main School of Fire Service international research project EU-SENSE. In the past she was the head of the Department of Methodology and Research at the Main School of Fire Service. She participates in research projects for national defence and security funded by the Ministry of Science and Higher Education and the National Centre for Research and Development. She is a chairperson and a member of scientific, programme and organisational committees of numerous national and international conferences and scientific seminars. Magdalena Gikiewicz's scientific interests include general security, operational research including optimisation and network programming, crisis management including civilian planning, security culture including security level research, tools for shaping security culture, research methodology in security sciences.