POLSKA AKADEMIA NAUK
Instytut Badań Systemowych

BADANIA SYSTEMOWE
Inżynieria Środowiska

BEZPIECZEŃSTWO SYSTEMÓW ZBIOROWEGO ZAOPATRZENIA W WODĘ

Janusz Rak
Barbara Tchórzewska-Cieślak
Jan Studziński

Warszawa 2013

POLSKA AKADEMIA NAUK
INSTYTUT BADAŃ SYSTEMOWYCH

Seria: BADANIA SYSTEMOWE
Tom 72

Redaktor naukowy:
Prof. dr hab. inż. Jakub Gutenbaum

Warszawa 2013

POLSKA AKADEMIA NAUK
INSTYTUT BADAŃ SYSTEMOWYCH

Janusz Rak

Barbara Tchórzewska-Cieślak

Jan Studziński

BEZPIECZEŃSTWO SYSTEMÓW ZBIOROWEGO ZAOPATRZENIA W WODĘ

Warszawa 2013

Autorzy:

Prof. dr hab. inż. Janusz R. Rak
Politechnika Rzeszowska
rakjan@prz.edu.pl

Dr hab. inż. Barbara Tchórzewska-Cieślak
Politechnika Rzeszowska
cbarbara@prz.edu.pl

Dr hab. inż. Jan Studziński
IBS PAN Warszawa
studzins@ibspan.waw.pl

Recenzenci:

Prof. dr hab. inż. Janusz Łomotowski
Uniwersytet Przyrodniczy we Wrocławiu

Dr hab. inż. Izabela Zimoch
Politechnika Śląska w Gliwicach

Skład: Aneta M. Pielak

Wydawca:
Instytut Badań Systemowych
Polska Akademia Nauk
Newelska 6, 01-447 Warszawa
www.ibspan.waw.pl

Publikacja wydana ze środków projektów rozwojowych
Narodowego Centrum Badań i Rozwoju
nr NR 14-0006-10/2010 oraz NR 14-0011-10/2010

ISSN 0208-8029
ISBN 83-894-7549-9

13. Odporność systemów zbiorowego zaopatrzenia w wodę na zagrożenia terrorystyczne i cyberterrorystyczne

13.1. Definicje terroryzmu

Słowo terror wywodzi się z języka łacińskiego (*terrere* – przerażać). Oznacza grozę, strach, obawę i trwogę, a więc uczucia, które powstają wskutek stosowania przemocy, okrucieństwa i gwałtu (Zubrzycki, 2008). Za pierwowzór terroryzmu uważa się dyktaturę Jakobinów, których rządy związane były ze zbrodnią, strachem oraz przemocą i pochłonęły wiele ofiar wśród sprzeciwiających się tej formie rządzenia. Tak więc paradoksalnie, terror narodził się jako metoda wdrożona przez władzę państwową do utrzymania posłuszeństwa wśród poddanych. Polegał na tym, aby bać się władzy i pod wpływem strachu być jej spolegliwym. W ten sposób terror stał się filozofią działania opartą o przemoc i stosowaną do osiągnięcia zamierzonego celu. Uważa się, że terror nie jest pojęciem tożsamym z terroryzmem. Terroryzm, to taktyka lub technika, przy pomocy której akt przemocy lub groźba jego dokonania ma służyć wytworzeniu poczucia strachu lub wymuszeniu określonego celu. Jest to zjawisko o charakterze rozwojowym, o czym świadczy następujące porównanie. Na początku XX wieku rosyjscy rewolucjoniści przygotowali zamach na Wielkiego Księcia S. Aleksandrowicza poprzez rzucenie bomby pod nadjeżdżający powóz. Z chwilą, kiedy powóz z księciem nadjechał, zamachowiec zobaczył w powozie dzieci księcia i odstąpił od planowanej akcji, aby uniknąć jego zdaniem niepotrzebnych ofiar. Jakże inne podejście w tym względzie mieli terroryści dokonujący zamachów w Nowym Jorku (2001 r.), Madrycie (2004r.) czy Londynie (2005 r.) (Hoffman, 1999; Rak, 2009a).

Atak terrorystyczny z 11 września 2001 roku na wieże World Trade Center oraz Pentagon, spowodował przewartościowanie postrzegań zagrożenia terroryzmem i walki z nim. Zamach ten uznano za akt wojny i przyjęto doktrynę użycia wszelkich możliwych środków, aby wygrać tę wojnę w wymiarze międzynarodowym. W literaturze fachowej funkcjonuje wiele różnych definicji terroryzmu (Hoffman, 1999; Rak, 2009a; Zubrzycki, 2008):

- jest to zaplanowana, umotywowana politycznie przemoc wobec celów nieuczestniczących w walce, stosowana przez subnarodowe grupy czy

tajnych agentów, mająca na celu oddziaływanie na społeczeństwo (wg Departamentu Stanu USA),

- jest to bezprawne użycie siły lub przemocy wobec osób lub mienia, aby zastraszyć lub wywrzeć przymus na rząd, ludność cywilną albo części wyżej wymienionych w celu promocji celów politycznych lub społecznych (wg FBI),
- jest to bezprawne użycie lub groźba użycia siły czy przemocy wobec osoby lub mienia, aby wymuszać lub zastraszać rządy czy społeczeństwa, często dla osiągnięcia celów politycznych, religijnych albo ideologicznych (wg Departamentu Obrony USA).
- jest planowaną, zorganizowaną i zazwyczaj uzasadnioną ideologicznie działalnością osób lub grupy, mającą na celu wymuszenie od władz państwa, społeczeństwa lub poszczególnych osób określonych świadczeń, zachowań lub postaw, a realizowaną w przestępczych formach obliczonych na wywołanie szerokiego i maksymalnie zastraszającego rozgłosu w opinii publicznej,
- jest to działalność przestępcza na tle politycznym zorganizowanych grup przestępczych o charakterze antypaństwowym.

Podejmowane przez te ugrupowania akty terrorystyczne zmierzają do wymuszenia określonych ustępstw. Ugrupowania te osiągają swój cel poprzez wywołanie strachu i paniki w opinii publicznej, a służy temu podkładanie bomb w miejscach publicznych czy zamachy na życie znanych osób (Hoffman, 1999).

Jednocześnie stwierdza się, że współczesny terroryzm postrzegany jest w kategoriach wojny psychologicznej. Na podstawie międzynarodowych statystyk, w realizacji swoich celów terroryści posługują się (Zubrzycki, 2008):

- zamachami bombowymi – 43%,
- podpaleniami – 27%,
- bronią palną – 21%,
- porwaniami i wzięciem zakładników - 5%,
- sabotażem – 4%.

Nowa koncepcja organizacyjna grup terrorystycznych ma charakter sieciowy, co stanowi odejście od klasycznej struktury hierarchicznej i związanej z tym stałej lokalizacji. Często nie jest sprecyzowany aspekt ideowy ataku, a jedynym

celem jest wzbudzenie strachu w konkurencyjnych znienawidzonych społecznościach. Trudno jest określić miejsca i czas ataków, jednak na podstawie dotychczasowych statystyk wśród celów potencjalnych działań terrorystycznych należy wymienić: obiekty administracji rządowej i służb mundurowych, przedstawicielstwa dyplomatyczne, centra handlowe, sportowe i rozrywkowe, siedziby korporacji, środki komunikacji masowej, świątynie i obiekty infrastruktury krytycznej – lotniska, mosty i węzły drogowe specjalnego znaczenia, elektrownie atomowe i systemy zaopatrzenia w wodę do spożycia (Rak, 2009a; Zubrzycki, 2008).

W analizach zagrożeń dla SZZW należy zwrócić uwagę na zdarzenia niepożądane w tzw. cyberprzestrzeni , która definiowana jest jako przestrzeń przetwarzania informacji tworzona przez systemy teleinformatyczne. Ataki terrorystyczne w cyberprzestrzeni mogą stanowić poważne zagrożenie dla bezpieczeństwa SZZW z uwagi na coraz powszechniejsze wykorzystanie nowoczesnych technik informatycznych w zarządzaniu tymi systemami.

13.2. Pojęcie strachu i lęku

Oba odczucia w życiu codziennym ludzie identyfikują zamiennie. Trudność w rozróżnieniu wynika z faktu, że objawy fizjologiczne obu emocji są bardzo do siebie podobne. Uważa się, że strach to specyficzny stymulator rozwoju i wielu zmian w życiu człowieka (np. w obawie przed utratą pracy podnosimy swoje kwalifikacje zawodowe), w tym także w obliczu rzeczywistego zagrożenia wartości priorytetowych. W języku polskim istnieje wiele synonimów pojęcia strachu: bojaźń, konsternacja, obawa, onieśmielenie, popłoch, przerażenie, niepokój, nerwowość, trwoga, zatroskanie i zaniepokojenie. Według Encyklopedii PWN – „strach to reakcja o charakterze wrodzonym pojawiająca się w sytuacji realnego, rozpoznawalnego zagrożenia (w odniesieniu od niemającego uchwytnej przyczyny lęku), towarzyszą jej liczne objawy fizjologiczne".

Uważa się, że strach jest związany z bodźcem zagrażającym, zaś lęk powstaje na bodziec nie do końca określony. Inaczej mówiąc, strach jest reakcją na aktualne zagrożenie zewnętrzne, natomiast lęk jest reakcją na zagrożenie wyobrażone, którego źródło tkwi w psychice człowieka. Strach powstaje w odpowiedzi na bezwarunkowe bodźce awersyjne, specyficzne, na bodźce warunkowe sygnalizujące niebezpieczeństwo i bodźce nowe – nieznane (Marx, 1995; Rak, 2009a).

13.3. Charakterystyka oszustwa

Cechą oszustwa jest świadome, umyślne i celowe działanie, które w sposób nieuprawniony ma przynieść korzyści osobie fizycznej lub organizacji. Do tej grupy zalicza się kradzież, przekupstwo, defraudacja, nieprawidłowości w dokumentach itp. Badania wskazują, że 80% oszustw popełniają pracownicy danej firmy, a 20% ludzie z zewnątrz. Metody popełniania oszustwa, to fałszowanie lub wprowadzanie zmian w dokumentach, celowe niewłaściwe stosowanie zasad, fałszywe przedstawienie lub pomijanie faktów. Oszustwa popełnione na szkodę firmy mają na celu przysparzanie pośrednich lub bezpośrednich korzyści pracownikowi, osobie lub firmie zewnętrznej. Oszustwa popełnione w celu przysparzania korzyści firmie polegają na uzyskaniu korzyści poprzez uzyskanie przewagi w sposób nieuczciwy lub nierzetelny, co wprowadza w błąd podmioty zewnętrzne. Sprawcy takich oszustw z reguły uzyskują przy tym pośrednią korzyść osobistą.

Oszustwa pojawiają się wówczas, gdy zaistnieją okoliczności, które sprzyjają ich popełnianiu i możliwości ukrycia. Zapobieganie oszustwom i ich wykrywanie polega na podjęciu stosownych działań poprzedzonych identyfikacją i oceną ryzyka ich popełnienia. W analizie ryzyka zakłada się, że każdy pracownik w sprzyjających okolicznościach może popełnić oszustwo i musi podlegać kontroli. Metody zarządzania i sterowania ryzykiem dają możliwości jego ograniczenia w aspekcie popełnienia oszustwa. Pierwszoplanowe działania powinny dotyczyć zmian organizacyjnych i kontrolnych poprzez prewencję, detekcję oraz monitorowanie ich skuteczności.

Ważną rolą prewencyjną jest zatrudnienie pracowników o wysokim morale etycznym na stanowiskach wrażliwych. Sprzyja temu sprawdzanie kandydata pod względem wykształcenia, historii zatrudnienia i referencji z poprzednich miejsc i stanowisk pracy.

Osobną kategorię stanowią nieprawidłowości popełniane przez pracowników. Polegają one na naruszeniu przepisów w wyniku niezamierzonego błędu, przeoczenia lub nieznajomości prawa. Mają one konsekwencje bezpośrednich strat finansowych lub marnotrawstwa.

Audyty wewnętrzne i zewnętrzne poprzez analizę i ocenę ryzyka wskazują metody zapobiegania i wykrywania oszustw lub nieprawidłowości w funkcjonowaniu firmy.

13.4. Zagrożenie czynnikami chemicznymi

Broń chemiczna to trucizny, które produkuje się ze składników prekursorów o działaniu powodującym śmierć lub czyniących człowieka niezdolnym do działania. Swoje działanie objawiają także w stosunku do zwierząt i roślin. Trucizna kojarzona jest często z gazem, jednak w normalnej temperaturze i ciśnieniu atmosferycznym tej odmiany się nie stosuje. Najczęściej występuje w postaci ciekłej, co wymaga pojemników ciśnieniowych, a najskuteczniej jest ją przekształcić w postać aerozolu z fazy ciekłej lub ciała stałego. Można ją stosować jako jednoskładnikową (unitarną) lub dwuskładnikową (binarną) – postać toksyczna powstaje przy zmieszaniu się dwóch składników (Croddy, Perez-Armendariz, Hart, 2003).

Prekursory trujących środków chemicznych mają zastosowanie w cywilnej działalności przemysłowej, co stanowi o tzw. „podwójnym zastosowaniu", przez co są dostępne w handlu. Przykładem substancji chemicznej tego rodzaju jest triodiglikol używany w produkcji cywilnej do wytwarzania tworzyw sztucznych, barwników, atramentu, a używany także do produkcji iperytu siarkowego. Dopiero konwencja o zakazie broni chemicznej z 1993 roku wprowadziła globalną kontrolę obrotu wieloma prekursorami mającymi zastosowanie do produkcji broni chemicznej, takimi jak: trichlorek fosforu, cyjanek sodu, difluorek metylofosforanowy, pentasiarczek fosforu i inne. Produkcja tego rodzaju środków w zasadzie nie różni się od standardów laboratoryjnych. Stosuje się podwójne systemy uszczelnień i specjalne systemy wentylacyjne wyposażone w filtry. Niektóre substancje chemiczne przetwarzane w produkcji mają silne właściwości korozyjne (związki fosforoorganiczne). Wymaga to instalacji o podwyższonej odporności na korozję, co z drugiej strony utrudnia prowadzenie tajnej produkcji.

Środki chemiczne, które są traktowane, jako broń chemiczna, dzielą się na cztery kategorie: duszące, działające na krew, parzące i paraliżujące. Ich przykładami są: adamsyt, chlorocyjan, cyjanowodór, difosgen, fosgen, iperyt, luizyt, sarin, soman, tabun (Croddy, Perez-Armendariz, Hart, 2003; Świątczak i inni, 2008).

Środki chemiczne są wykorzystywane nie tylko, jako broń chemiczna. Znane są tzw. dymy maskujące na bazie białego fosforu do kamuflowania właściwych operacji. Z kolei mikstury cuchnące używane są do maskowania substancji toksycznych. Są to związki z grupy merkaptanów. Nieznośne zapachy mogą być nietoksyczne. Znane są także przypadki tzw. „wandalizmu chemicznego". Podczas niektórych akcji protestacyjnych protestanci używają kwasu masłowego, którego wstrętny odór zjełczałego masła jest trudny do usunięcia (jest to związek aktywny chemicznie), po czym opuszczają miejsce akcji (Croddy, Perez-Armendariz, Hart, 2003; Rak, 2009a).

13.5. Zagrożenie czynnikami biologicznymi

Do broni biologicznej można zaliczyć szereg czynników, takich jak bakterie, grzyby, wirusy, toksyny bakteryjne i inne. Produkcja tego rodzaju czynników polega na hodowli kultur patogenów. Niektóre patogeny, wytwarzające toksyny chorobotwórcze, występują w naturalnym otoczeniu człowieka (Blazes i inni, 2002). Bakteria wąglika (*Bacillus anthracis*) występuje w glebie, powodując choroby zwierząt gospodarskich. Teoretycznie istnieje możliwość wyizolowania tego mikroorganizmu, np. w ubojni czy gospodarstwie hodowlanym, i wytworzeniu kultury bakteryjnej. Jednak bardziej prawdopodobny wydaje się być zakup lub kradzież małej liczby kultur z instytutu badawczego i namnożenie ich w znacznych ilościach w bardzo krótkim czasie (Płusa, 2002).

Wybrane gatunki drobnoustrojów, które mogą być wykorzystane do produkcji broni biologicznej, organizacja Centrem for Diseases Contro and Prevention dzieli na trzy grupy (Blazes i inni, 2002):

- kategoria A, to najbardziej niebezpieczne drobnoustroje Bacillus anthracis, Pasteurella pestis, Francisella tularensis, Clostridium botulinum, Poxvirus Mariole, i wirusy gorączek krwotocznych,
- kategoria B obejmuje drobnoustroje dające stosunkowo niewysoki odsetek śmiertelności; są to bakterie: Rickettsiae, Staphylococcus ureus wytwarzający enterotoksynę B, Salmonella sp., Shigella sp., Escherichia coli 0157:H7, Wibrio cholerae, a także Cryptosporidium parvum,
- kategoria C, to bakteria Mycobasterium tuberculosis oraz wirusy Nipah, Hantanna i żółtej febry.

Patogeny należące do dwóch ostatnich grup przenoszone są drogą kropelkową i poprzez skażoną żywność lub wodę (Blazes i inni, 2002; Croddy, Perez-Armendariz, Hart, 2003).

Produkcja środków biologicznych jest stosunkowo łatwa do ukrycia, gdyż nie wymaga dużych powierzchni magazynowych na materiały wyjściowe. Możliwa jest masowa produkcja w instalacjach do fermentacji, np. w browarze. Badania nad właściwościami rozpylania mogą być prowadzone z wykorzystaniem zwykłego rozpylacza do środków ochrony roślin. Produkcję broni biologicznej można znacznie łatwiej utajnić, niż wytwarzanie broni chemicznej.

Środki biologiczne należy uczynić odpornymi na proces przechowywania (starzenie). W tym celu można odwadniać kultury poprzez zamrażanie lub liofilizację (suszenie ze stanu zamrożenia). Otrzymuje się w ten sposób suchy materiał – bakterie i stabilizator, które mogą być zmielone na proszek o granulacji optymalnej do wytworzenia aerozolu. Działanie środków biologicznych może być rozłożone w czasie, jeżeli materiał bakteryjny umieści się w mikrokapsułkach, z których uwalniany jest w sposób zaprogramowany. Identyfikacja patogenów, które mogą być użyte w ataku bioterrorystycznym, może być przeprowadzona jedynie w specjalistycznym laboratorium mikrobiologicznym z zastosowaniem niestandardowych metod diagnostycznych (Blazes i inni, 2002; Croddy, Perez-Armendariz, Hart, 2003; Płusa, 2002; Rak, 2009a).

13.6. Sposoby rozpraszania

Rozpraszanie punktowe, to przede wszystkim wykorzystanie różnorodnej amunicji, a rozpraszanie liniowe, to urządzenie rozpylające. Zawsze jednak istnieje możliwość prymitywnej formy ataku, szczególnie w pomieszczeniach zamkniętych. Obecnie mówi się o projektowaniu ataku biologicznego i chemicznego, który musi uwzględniać warunki otoczenia. Przy użyciu broni na wolnym powietrzu należy brać pod uwagę warunki pogodowe (temperatura, kierunek wiatru, prognoza opadu atmosferycznego, oświetlenie słoneczne, możliwości wystąpienia stanu inwersji powietrza, wilgotność powietrza itp.), co zdecydowanie różni się od ataku w klimatyzowanym pomieszczeniu centrum handlowego, gdzie znany jest obieg powietrza. Duża wilgotność powietrza, opad atmosferyczny sprzyjają neutralizacji działania tych środków (Suligowski, 2005; Szuster, 2004).

Bioaerozole o rozmiarach cząsteczek 0,1÷10 mikronów są niewidoczne gołym okiem (zdolność rozdzielcza oka zaczyna się od 30 mikronów wzwyż). Większość preparatów broni biologicznej jest przygotowywana w postaci aerozolu. W tej formie działają one szybciej i skuteczniej w porównaniu z rozpuszczaniem w wodzie. Wydzieloną grupę stanowią mikroorganizmy, którymi można zakazić żywność i wodę, dla których nie opracowano dotąd postaci aerozolu. Należą do niej: *Salmonella sp.*, *Shigella sp.*, *Escherichia coli* 0157:H7, *Vibrio cholerae* i *Cytosporidium parvum* (Croddy, Perez-Armendariz, Hart, 2003; Rak, 2009a).

13.7. Wrażliwość systemów zbiorowego zaopatrzenia w wodę

System zbiorowego zaopatrzenia w wodę aglomeracji miejskiej w wielu analizach związanych z tzw. przeglądami terroryzmu chemicznego i biologicznego zajmuje pierwszoplanową rolę. W USA istnieje 16800 publicznych systemów zaopatrzenia w wodę, z czego zaledwie 3000 dostarcza wodę do 70% mieszkańców kraju. Struktury przestrzenne SZZW są bardzo rozległe i skomplikowane. Źródła wody znajdują się nieraz w odległości od kilku do kilkudziesięciu kilometrów od miasta i mogą mieć charakter zbiorników wód powierzchniowych bądź podziemnych. Scenariusz zatrucia źródeł pozyskiwania wody dla dużych miast wydaje się mało prawdopodobny. Toksyny biologiczne, mimo dużej toksyczności, rozpuszczone w tysiącach a nawet dziesiątkach tysięcy m^3 wody w źródle, na skutek rozcieńczenia byłyby mało efektywne. Dodatkowo w procesie uzdatniania wody stosuje się dezynfekcję (chlor, ozon), w wyniku której środki biologiczne znacznie tracą na swej szkodliwości. Ponadto wiele trucizn powodowałoby zabarwienie wody i nadawało jej specyficzny zapach, powodując dodatkowo śnięcie ryb, co jest bardzo dobrym wskaźnikiem skażenia wody. Prowadzony jest biomonitoring wody podawanej z ujęcia do stacji uzdatniania, polegający na hodowli ryb wskaźnikowych (ujęcia zatokowe) i skorupiaków (Bajer, 2001; Blazes i inni, 2002; Dhillon, 1986; Dul, 2004; Korczak i inni, 2005).

Podsystem dystrybucji wody ze względu na swoją rozległość przestrzenną i łatwość dostępu (np. hydranty, komory i studzienki wodociągowe) powinien być monitorowany pod względem parametrów pracy (Leszczyńska, Sozański, 2004; Łomotowski, 2007; Świderska-Bróż, Wolska, 2005). Patrole powinny być rutynowe w rejonach centrów administracji i zarządzania, tak cywilnych, jak i mundurowych (Rak, 2009a).

Coraz powszechniej używa się kamer do obserwacji strategicznych miejsc SZZW. Stosuje się systemy alarmowe, które powiadamiają operatora o włamaniu do obiektu SZZW. W ten sposób chronione są sieciowe zbiorniki wody czystej. Dodatkowo, zarządzający SZZW wynajmują firmy ochroniarskie. Prewencyjnie należy zakazać pływania łodziami, łowienia ryb, korzystania z terenów i dróg w okolicach ujęć wody.

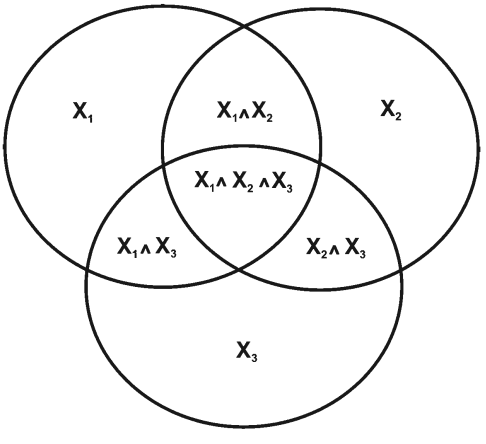
Współcześnie, w świetle wydarzeń na świecie związanych z aktami terrorystycznymi, analiza zagrożeń z tym związanych wydaje się być drogą do zabezpieczenia się przed nimi. W przypadku próby skażenia wody czynnikami chemicznymi bądź toksynami biologicznymi wykonywany raz na dobę monitoring jakości fizykochemicznej wody wydaje się być skuteczny. Oznaczenia tych parametrów

wykonuje się szybko, nowoczesnymi metodami, i wyniki znane są już po ok. 1 h od poddania próbki analizie. W przypadku analiz bakteriologicznych wody wyniki badań znane są dopiero po 24h, 36h i 72h. To stwarza pewne zagrożenie dostania się do sieci wody o niewłaściwych parametrach bakteriologicznych. Ponadto wykonywane analizy bakteriologiczne nie uwzględniają wszystkich czynników, które mogły zostać użyte celowo do skażenia wody. Identyfikacja pewnych czynników biologicznych (np. wirusów) jest możliwa tylko w wysoce specjalistycznych laboratoriach biologii molekularnej. Jednak z drugiej strony, stosowana dezynfekcja wody przed wprowadzeniem jej do sieci powinna eliminować większość mikroorganizmów. Zagrożeniem mogą być jedynie bakterie w formie przetrwalnikowej – organizmy bardzo odporne na działanie środków dezynfekcyjnych (Kowal, 2003).

13.8. Globalne skażenie wody wodociągowej

Globalne skażenie wody wodociągowej może wystąpić na skutek trzech zdarzeń elementarnych: X_1 – incydentalnego zanieczyszczenia wody w źródle poboru, X_2 – nieefektywnego procesu uzdatniania wody, X_3 – monitoring nie wykrywa zanieczyszczenia wody uzdatnionej w sieci wodociągowej. Każdemu z tych zdarzeń można przypisać prawdopodobieństwo związane z oceną eksperta: $P(E_i) = P(X_i)$ (Radkowski, 2003).

Na rys. 13.1 przedstawiono trzy obszary zdarzeń związanych z globalnym skażeniem wody wodociągowej (Radkowski, 2003).



Rys. 13.1. Ilustracja współzależności wystąpienia globalnego skażenia wody wodociągowej.

Aby wyznaczyć prawdopodobieństwo globalnego skażenia wody wodociągowej (P_G), należy najpierw określić następujące relacje cząstkowe (Rak, 2009a; Radkowski, 2003):

$$Y_1 = \sum_{i}^{3} P(X_i) \tag{13.1}$$

$$Y_2 = \sum_{i}^{3} P(X_i) \cdot P(X_j) \tag{13.2}$$

$$Y_3 = P(X_i) \cdot P(X_j) \cdot P(X_k) \tag{13.3}$$

a następnie wyznaczyć prawdopodobieństwo globalnego skażenia wody wodociągowej:

$$P_G = \sum_{i=1}^{3} (-1)^{i+1} \cdot Y_i \tag{13.4}$$

Po rozwinięciu równania (13.4) otrzymuje się:

$$\begin{aligned} P_G = {} & P(X_1) + P(X_2) + P(X_3) - P(X_1) \cdot P(X_2) - P(X_1) \cdot P(X_3) - \\ & - P(X_2) \cdot P(X_3) + P(X_1) \cdot P(X_2) \cdot P(X_3) \end{aligned} \tag{13.5}$$

Dodatkowo można wyznaczyć prawdopodobieństwo:

- zdarzenia awaryjnego z udziałem $X_1 \wedge X_2 \wedge X_3$:

$$P(X_1 \wedge X_2 \wedge X_3) = P(X_1) \cdot P(X_2) \cdot P(X_3) \tag{13.6}$$

- zdarzenia awaryjnego z udziałem $X_1 \wedge X_2$ w układzie $X_1 - X_2 - X_3$:

$$P(X_1 \wedge X_2) = P(X_1) \cdot P(X_2) - P(X_1) \cdot P(X_2) \cdot P(X_3) \tag{13.7}$$

- zdarzenia awaryjnego z udziałem $X_2 \wedge X_3$ w układzie $X_1 - X_2 - X_3$:

$$P(X_2 \wedge X_3) = P(X_2) \cdot P(X_3) - P(X_1) \cdot P(X_2) \cdot P(X_3) \tag{13.8}$$

- zdarzenia awaryjnego z udziałem $X_1 \wedge X_3$ w układzie $X_1 - X_2 - X_3$:

$$P(X_1 \wedge X_3) = P(X_1) \cdot P(X_3) - P(X_1) \cdot P(X_2) \cdot P(X_3) \tag{13.9}$$

Znając prawdopodobieństwo globalnego skażenia wody wodociągowej, zgodnie z formułą (13.4), można wyznaczyć (Rak, 2009a):

- ryzyko związane ze stratami materialnymi:

$$r_m = P_G \cdot C_m \tag{13.8}$$

- ryzyko związane z utratą życia ludzkiego:

$$r_1 = P_G \cdot C_1 \tag{13.9}$$

- ryzyko związane z powikłaniami zdrowotnymi:

$$r_z = P_G \cdot C_z \tag{13.10}$$

- ryzyko globalne związane ze skażeniem wody wodociągowej:

$$r_G = P_G(C_m + C_1 + C_z) \tag{13.11}$$

Wszystkie trzy rodzaje ryzyka mają charakter wartości oczekiwanej strat, które mogą być wyrażone w wartości pieniężnej. O ile oszacowanie kosztów finansowych związanych ze stratami C_m i C_z nie sprawia trudności, o tyle oszacowanie kosztów C_1 budzi wątpliwości natury etyczno-moralnej. Można w tym względzie posłużyć się danymi z firm ubezpieczeniowych (np. odszkodowanie w wyniku wypadku samochodowego ze skutkiem śmiertelnym).

Procedurę kategoryzacji wartości ryzyka według skali trójstopniowej (tolerowane, kontrolowane, nieakceptowane) przeprowadza się zgodnie z zasadami podanymi w pracach (Li i inni, 2009; Markowski, 2006; Rak, Tchórzewska-Cieślak, 2005a, 2006b).

ISSN 0208-8029
ISBN 83-894-7549-9

INSTYTUT BADAŃ SYSTEMOWYCH
POLSKIEJ AKADEMII NAUK
tel.: (+48) 22 3810246 / 22 3810277 / 22 3810241 / 22 3810273
e-mail: biblioteka@ibspan.waw.pl