

ODPORNOŚĆ SYSTEMU ZAOPATRZENIA W WODĘ NA ZAGROŻENIA TERRORYSTYCZNE

Prof. dr hab. inż. Janusz R. RAK
Katedra Zaopatrzenia w Wodę i Odprowadzania Ścieków
Wydział Budownictwa i Inżynierii Środowiska
Politechnika Rzeszowska
al. Powstańców Warszawy 6
35-959 Rzeszów
e-mail: rakjan@prz.edu.pl

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.

Praca stawia sobie za cel odpowiedź na pytanie, czy możliwa jest wizja zamaskowanych na czarno osobników skradających się pod osłoną nocy w pobliżu obiektów wodociągowych celem dodania do wody śmiertelnych substancji?

Definicje terroryzmu

W literaturze fachowej funkcjonuje wiele różnych definicji terroryzmu

- 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 realizowane w przestępczych formach obliczonych na wywołanie szerokiego i maksymalnie zastraszonego rozgłosu w opinii publicznej
- jest to działalność przestępcza na tle politycznym zorganizowanych grup przestępczych o charakterze antypaństwowym

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 społeczeństwach. 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.

Pojęcie strachu i lęku

Według Encyklopedii PWN – „strach to reakcja o charakterze wrodzonym pojawiająca się w sytuacji realnego, rozpoznawalnego zagrożenia (w odniesieniu od nie mającego 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.

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 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.

Zagrozenie 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.

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 akcji protestacyjnej protestanci używali kwasu masłowego, którego wstrętny odór zjełczałego masła jest trudny do usunięcia (jest to związek aktywny chemicznie), po czym opuszczali miejsce akcji.

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.

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.

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.

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.

Wskaźnik odporności systemu

Systemy techniczne narażone są na dwa podstawowe rodzaje ryzyka: bezpośrednie i pośrednie. Ryzyko bezpośrednie (r_b) związane jest z zagrożeniami generowanymi wewnątrz systemu. Ryzyko pośrednie (r_p) związane jest z zagrożeniami generowanymi w otoczeniu systemu, a mającymi negatywny wpływ na jego funkcjonowanie.

Miarą odporności systemu na te dwa rodzaje ryzyka jest wskaźnik odporności definiowany w następujący sposób:

$$I_r = \frac{r_b}{r_b + r_p}$$

Ryzyko r_b identyfikowane jest z tzw. ryzykiem poznawalnym, a ryzyko r_p z ryzykiem losowym.

Interpretacja skrajnych wartości I_r jest następująca

$I_r = 0$, to $r_b = 0$, system narażony jest tylko na ryzyko zewnętrzne (pośrednie), które z natury rzeczy jest mało poznawalne i często losowe.
System uważa się za nieodporny na zagrożenia.

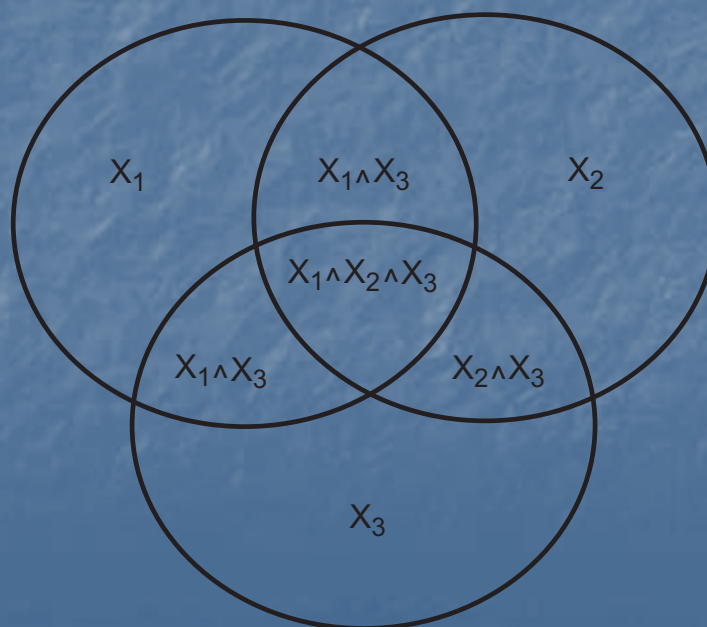
$I_r = 1$, to $r_p = 0$, system narażony jest tylko na ryzyko wewnętrzne (bezpośrednie), które z natury rzeczy jest poznawalne, i które można redukować.
System uważa się za odporny na zagrożenia.

W konkluzji należy stwierdzić, że im bliżej I_r jest jedności, to tym SZZW jest bardziej odporny na zagrożenia.

Globalne skażenie wody wodociągowej

Globalne skażenie wody wodociągowej może wystąpić na skutek trzech zdarzeń elementarnych: X_1 – incyidentalnego 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: $P(E_i) = P(X_i)$.

Na rysunku przedstawiono trzy obszary zdarzeń związanych z globalnym skażeniem wody wodociągowej.



Podsumowanie

- Atak z użyciem środków chemicznych lub biologicznych jest szczególnie groźny ze względu na swój charakter – jest niewidzialny i niesłyszalny, a objawy w przypadku broni biologicznej pojawiają się dopiero po kilku dobach. Przedmiotem ataku mogą być bezpośrednio ludzie, zwierzęta, uprawy rolne, powietrze, gleba, woda itp. Tego typu akty terrorystyczne mogą być anonimowe, gdyż dywersant odpowiedzialny za spowodowanie skażenia ma czas na opuszczenie miejsca zdarzenia.
- Akty terrorystyczne w swej naturze mają gwałtowny charakter i oprócz powodowania ofiar porażają umysł człowieka. Powodują dezorientację, zamieszanie wśród ludzi, zwiększanie niepewności i sianie paniki. Możliwość użycia broni chemicznej bądź biologicznej najlepiej ilustruje cytat „jest ona bombą atomową ludzi biednych”. Koszty jej produkcji są relatywnie niskie, jeżeli uwzględni się zasięg działania, w stosunku do broni konwencjonalnej.

- Specjalnie obserwowane i patrolowane powinny być fragmenty sieci wodociągowej w pobliżu centrów władzy administracyjnej i służb mundurowych. Postuluje się w tym zakresie stosowanie monitoringu z wykorzystaniem kamer video i alarmów ujawniających włamania do obiektów wodociagowych.
- Współcześnie pojawiła się nowa forma terroryzmu związana z atakami hakerów na serwery instytucji publicznych, którą nazwano cyberterroryzmem. Cyberterroryzm wykorzystuje technologie informatyczne do wywierania presji psychologicznej i wyrządzania szkód z pobudek politycznych, ideologicznych lub religijnych.

DZIĘKUJĘ ZA UWAGĘ