ZESZYTY NAUKOWE WSOWL

Nr 3 (161) 2011 ISSN 1731-815

NAUKI O BEZPIECZEŃSTWIE

Jan JAGIELSKI*

WYBRANE UWARUNKOWANIA BEZPIECZEŃSTWA

W artykule przedstawiono uwarunkowania bezpieczeństwa w obszarze techniki i w obszarze społecznym. Przedstawiono relacje wyzwanie – zagrożenie. Zdefiniowano pojęcie bezpieczeństwa w technice i bezpieczeństwa w społeczeństwie. Podano sposoby zapewnienia bezpieczeństwa w technice na przykładzie systemu informatycznego. Przedstawiono sytuację w systemie społecznym na podstawie faktów opisujących zagrożenia ze strony środowiska naturalnego na przykładzie zjawisk powodziowych na Dolnym Śląsku.

Słowa kluczowe: *bezpieczeństwo, wypadek, ryzyko, defekty projektowania, tolerowanie defektów, unikanie defektów, system ochrony, środowisko, powódź*

WPROWADZENIE

Bezpieczeństwo jest terminem bardzo trudnym do prostej interpretacji. Można spotkać wiele definicji bezpieczeństwa. Ich wielość wynika z istoty tego, czym bezpieczeństwo jest. Możemy mówić o bezpieczeństwie na poziomie globalnym, regionalnym i narodowym[1]. Bezpieczeństwo narodowe pozostaje w ścisłym związku z bezpieczeństwem międzynarodowym jako wypadkową bezpieczeństwa każdego i wszystkich państw. Bezpieczeństwo międzynarodowe jest stanem, w którym państwa uważają, że nie zagraża im atak militarny, presja lub przymus gospodarczy i dzięki temu są zdolne do swobodnego rozwoju i postępu. Bezpieczeństwo jest też pewnością państwa lub grupy państw do przeciwstawienia się sytuacji kryzysowej. Istnieje też poziom bezpieczeństwa społeczeństwa i poziom bezpieczeństwa jednostki ludzkiej dotyczący bezpośrednio człowieka.

* prof. dr hab. inż. Jan JAGIELSKI – Instytut Metrologii Elektrycznej Uniwersytetu Zielonogórskiego

[1] J. Pawłowski, *Słownik terminów z zakresu Bezpieczeństwa Narodowego*, Akademia Obrony Narodowej, Warszawa 2009, s. 35.

W artykule zostaną poruszone kwestie bezpieczeństwa społeczeństwa na poziomie człowieka i otaczającego środowiska. Środowisko to technika jako środki wytwarzane przez człowieka oraz przyroda jako naturalne otoczenie. W analizie bezpieczeństwa możemy wyróżnić dwa negatywnie wartościowane zjawiska. Są to wyzwanie i zagrożenie. Wyzwanie to nowe sytuacje, w których występują niezbywalne potrzeby implikujące podjęcie przez państwo działań zapewniających określony stan bezpieczeństwa. Zagrożeniami są nierozwiązane wyzwania. Zagrożenia mają charakter naturalny, jak i mogą być powodowane lub potęgowane przez człowieka

1. CHARAKTERYSTYKA BEZPIECZEŃSTWA W OBSZARZE TECHNIKI

W odniesieniu do techniki, bezpieczeństwo (ang. *safety*) to charakterystyka systemu intuicyjnie oznaczająca, że użytkowanie systemu technicznego jest wolne od wypadku. Użytkowanie jest tu wyzwaniem, które nie powinno zamienić się w zagrożenie. Wypadkami (ang. *accident*) nazywa się niepożądane i nieplanowane zdarzenia, powodujące duże straty materialne, zranienia lub śmierć ludzi albo skażenia środowiska.

Gwałtowny rozwój społeczeństwa informatycznego implikuje niebywały wzrost ilości i szybkości wymiany informacji. Istotną rolę odgrywają systemy informatyczne[2]. Ich specyfiką jest to, że one same nie stanowią zagrożenia wypadkowego, ale mogą to powodować sygnały przez te systemy generowane. Odnosi się to zwłaszcza do oprogramowania jako szczególnego produktu.

Do ilościowego określenia zagrożenia wypadkami wykorzystywane jest pojęcie ryzyka (ang. *risk*). Ryzyko jest miarą dotyczącą szansy na zaistnienie wypadku i związanych z nim potencjalnych skutków. Pojęcie to umożliwia zdefiniowanie bezpieczeństwa jako gwarancji, że ryzyko związane z użytkowaniem systemu nie przekracza akceptowalnego poziomu.

W analizie bezpieczeństwa i możliwości jego zapewnienia, szczególną uwagę przykłada się do sytuacji poprzedzających powstanie wypadków. Wyróżniono w tym celu pojęcie hazardu (ang. *hazard*) oznaczające stan systemu prowadzący w bezpośredni sposób do wypadku. Występowaniu hazardów zapobiega system ochrony (ang. *safety protection system*), który może też ograniczać skutki wypadków. Analiza bezpieczeństwa koncentruje się na potencjalnie negatywnych skutkach działania systemu. Obejmuje analizę zagrożeń, analizę ryzyka wynikającego z tych zagrożeń, jak i identyfikację działań, które należy podjąć w celu kontroli, eliminacji lub redukcji zagrożeń. W ogólnym przypadku zdarzenia niebezpieczne mogą być powodowane defektami projektowania (ang. *design faults*) i defektami przypadkowymi (ang. *random faults*). Defekty projektowania wprowadzane są, w sposób niezamierzony, w fazie projektowania i obejmują wytwarzanie elementu niespełniającego założonych wymagań lub błędne określenie wymagań. Defekty przypadkowe obejmują wadliwe funkcjonowanie poprawnie zaprojektowanych i wykonanych elementów (starzenie, korozja, nadmierna temperatura, naprężenia mechaniczne).

[2] J. Górski, *Bezpieczeństwo przemysłowych zastosowań komputerów*, III Krajowa Konferencja „Diagnostyka Procesów Przemysłowych", Jurata,7 – 10 września, 1998, s. 201-211.

2. BEZPIECZEŃSTWO A PROJEKTOWANIE

W projektowaniu stosowane są różne podejścia[3]. Jedno z nich oparte jest na tolerancji defektów (ang. *fault tollerance*), dzięki wprowadzeniu do systemu mechanizmów wykrywania oraz usuwania uszkodzeń. Inne podejście oparte na zapobieganiu defektom (ang. *fault prevention*) zawiera aspekt unikania defektów i aspekt usuwania defektów. Unikanie defektów to techniki upewniania się o braku błędów projektowych i implementacyjnych. Znaczenie ma tu przestrzegania odpowiednich, unormowanych standardów postępowania na etapie projektowania i implementacji oraz kontrola jakości[4].

Drugi aspekt to usuwanie defektów, jakie mogłyby powstać w wytworzonej implementacji systemu. Do implementacji używa się komponentów wysoce niezawodnych wykluczających w znacznym stopniu defekty niewykrywalne (ang. *fault intollerance*), które mogą objawić się dopiero podczas użytkowania systemu, a którym nie można zapobiec i zbudować mechanizmu kompensacyjnego.

Kolejne możliwe podejście do konstruowania systemów niezawodnych to systemy z wykrywaniem defektów (ang. *fault detection*). Błędy wywoływane defektami mogą być wykrywane dopiero w jakiś czas po ich zaistnieniu.

Opracowano szereg standardów bezpieczeństwa dla różnych obszarów zastosowań obejmujących stosowne cykle procedur. Cykl rozpoczyna się zdefiniowaniem wymagań bezpieczeństwa w zakresie funkcji bezpieczeństwa i poziomu bezpieczeństwa. Grupa wymagań funkcji bezpieczeństwa definiuje warunki nakładane na zachowanie się systemu, których spełnienie gwarantuje bezpieczeństwo. Poziom bezpieczeństwa jest poziomem pewności, że dana funkcja bezpieczeństwa będzie poprawnie realizowana przez system.

3. ANALIZA BEZPIECZEŃSTWA

Analiza bezpieczeństwa ma na celu określenia stopnia bezpieczeństwa systemu. W jej zakres wchodzi analiza hazardu i analiza ryzyka. Analiza hazardu to identyfikacja sytuacji niebezpiecznych i ich przyczyn. Analiza ryzyka to identyfikacja częstości i skutków zdarzeń niebezpiecznych.

Analiza bezpieczeństwa, aby dała spodziewany skutek, musi być procesem ponawianym podczas tworzenia systemu, jego oceny przez niezależną instytucję certyfikującą, w celu zaakceptowania systemu. Występuje także podczas eksploatacji systemu jako sprawdzenie lub poprawienie stopnia jego bezpieczeństwa. Mieszczą się w niej także analizy wykonywane po wypadkach.

W analizie bezpieczeństwa stosowane jest podejście deterministyczne w zakresie identyfikacji przyczyn hazardu i podejście probabilistyczne w zakresie częstości jego występowania. Analiza deterministyczna identyfikuje związki przyczynowo-skutkowe mające wpływ na istnienie hazardu. Jest ona ukierunkowana bardziej na identyfikację dodatkowych mechanizmów bezpieczeństwa i analizę defektów projektowania. Określa zachowania systemu prowadzące do hazardu oraz identyfikuje na tej podstawie wymagania bezpieczeństwa.

---

[3] Z. Kowalczuk, *Systemy wykrywające, analizujące i tolerujące usterki*, PWNT, Gdańsk 2009.

[4] *Functional safety: safety- related systems*, International Elektrotechnical Commision standard draft, IEC 1508, 1994.

Analiza probabilistyczna jest głównym środkiem analizy defektów przypadkowych. Określa szansę wystąpienia hazardu na podstawie spodziewanej częstości wystąpienia awarii poszczególnych elementów systemu.

4. CHARAKTERYSTYKA BEZPIECZEŃSTWA SPOŁECZEŃSTWA

W odniesieniu do ludzi bezpieczeństwo[5] identyfikowane jest z pewnością (ang. *safety*) i oznacza brak zagrożenia fizycznego (ang. *danger*) albo ochronę przed nim. Oznacza też zdolność przetrwania, niezależność, tożsamość i pewność rozwoju. Zagrożenia mogą mieć charakter realny jako odbicie stanu rzeczy odnoszonego do oceny w określonym momencie czasu. Zagrożenia potencjalne to ekstrapolacja przewidywanego przebiegu wydarzeń i towarzyszących im niekorzystnych zmian. W definicji eksponuje się czynnik obiektywny jako brak rzeczywistego zagrożenia i czynnik subiektywny jako brak poczucia zagrożenia. Przykładem zagrożenia nękającego społeczeństwo są powodzie. Zagrożenie jest pochodną wyzwania, gdy nie podjęto działań zapewniających odpowiedni poziom bezpieczeństwa. Wyzwania to nowe sytuacje, w których występują niezbywalne potrzeby implikujące podjęcie przez państwo działań zapewniających określony stan bezpieczeństwa. Jedną z przyczyn generujących wyzwania i zagrożenia jest upadek opieki lekarskiej, inną postępująca bieda, czy oddziaływanie środowiska. Środowisko doświadcza nas w ostatnim czasie powodziami. W dalszej kolejności przedstawiona zostanie relacja: wyzwanie – zagrożenie na podstawie faktów opisujących sytuację powodziową na Dolnym Śląsku.

5. WYZWANIE ZAGROŻENIEM

Trudno mówić o powodzi jako zjawisku nowym. Społeczeństwo Dolnego Śląska nękane było wielokrotnie dotkliwymi powodziami. Skala powodzi była zróżnicowana i niektóre przypadki, ze względu na ogrom zniszczeń, miały znaczenie przełomowe i inspirujące do podejmowania środków i przedsięwzięć zaradczych. Takie dwie wyróżniające daty to rok 1887 i rok 1997. Nieco nowsze daty to lata 2002, 2009, 2010.

I tak powódź w 1887 roku w dorzeczu Bobru, Kwisy i Nysy Szalonej zniszczyła kilkanaście miejscowości[6]. W odpowiedzi na ten kataklizm opracowany został Program Ochrony Przeciwpowodziowej Podsudecia autorstwa prof. Otto Inze. W opracowaniu programu uczestniczyli inżynierowie z całej Europy. Na podstawie tego programu parlament niemiecki w 1900 roku przyjął uchwałę wcielającą program w życie. Realizacja programu zajęła 15 lat i wybudowano wówczas 10 zbiorników retencyjnych i 3 energetyczne zbiorniki wodne (elektrownie wodne). Dały one ogólna rezerwę powodziową przekraczającą 100 mln m^3.

Główne zadanie zbiorników polegało na odciążeniu głównego cieku w momencie kulminacji, spłaszczeniu fali powodziowej, by w ostateczności dać czas na ewakuację. Dawały one wobec tego bezpieczeństwo częściowe. By uzyskać bezpieczeństwo zakwalifikowane do poziomu wysokiego, niezbędny jest system w pełni sprawnych urządzeń i budowli hydrotechnicznych. Należą do nich obwałowania, jazy, przepusty kanały, śluzy i poldery. Te ostatnie nie mogą być zabudowywane.

---

[5] T. Jemioło, A. Dawidczyk, *Wprowadzenie do metodologii badań obronności*. Akademia Obrony Narodowej, Warszawa 2007.

[6] M. Lis, *Poldery, wały, zapory*, [w:] „Nowiny Jeleniogórskie", nr 35/2010, s. 9.

Ta gorzka prawda została obnażona w roku, 1997 czyli niespełna 100 lat od realizacji wymienionego wcześniej planu niemieckiego. Powódź z 1997 r. nazwana została powodzią tysiąclecia i z wielu względów była wypadkiem przełomowym. Była to pierwsza tak wielka katastrofa naturalna w nowej Polsce, różnej pod względem politycznym i gospodarczym. Powódź ujawniła słabe przygotowanie struktur państwa do radzenia sobie w tak trudnej sytuacji. Uzmysłowiła też konieczność opracowania szeroko zakrojonego planu działań ograniczających możliwość kolejnej katastrofy. Plan taki, pod nazwą „Program dla Odry 2006", został przyjęty w lipcu 2001 roku.

Powódź w roku 2002, jak i tegoroczne powodzie w różnych regionach Polski, niejako sugerują przyjrzenie się realizacji planu, wg, którego miano kompleksowo zagospodarować zlewnię rzeki Odry. Priorytetowe inwestycje miały chronić przed powodzią duże skupiska ludności oraz zabezpieczać obszary, na których powodzie są zjawiskami częstymi i gwałtownymi. Założono zwiększenie retencji zbiornikowej w dorzeczu Odry o 250 mln m^3 i retencji na polderach o około 100 mln m^3. Inspekcja NIK w 2007 roku wykazała zaniechania, braki planów i harmonogramów oraz niedostateczne wykorzystanie środków w latach 2002-2006. Z zaplanowanych 1,4 mld zł wykorzystano zaledwie 599 mln.

Kolejna inspekcja NIK w 2009 r. ujawniła, że z przyznanej przez Bank Światowy i Bank Rozwoju Rady Europy pożyczki w wysokości ponad 340 mln euro zostało wykorzystane w ciągu dwóch lat niespełna 3 mln zł przy kosztach obsługi zadłużenia 3,5 mln. Program miał ratować życie ludzkie i ograniczać gigantyczne straty materialne. Te w roku 1997 wyniosły w województwie dolnośląskim i opolskim 10 mld zł. Tyle w założeniu miała kosztować realizacja planu.

Szczególnie dotykanymi przez powódź są Kotlina Kłodzka i Dolny Śląsk. Realizacja planu niemieckiego na Dolnym Śląsku dała łagodniejszy przebieg powodzi w stosunku do Kotliny Kłodzkiej przy tej samej skali opadów.

Powodzie roku 2010 dostarczyły nowych faktów. Najniebezpieczniejsze okazały się małe rzeczki, dopływy, które popadły w zapomnienie. Latami nieczyszczone niepogłębiane, przypominające śmietniki utraciły drożność. Mury oporowe popękane grożą rozsypaniem do reszty przy następnym wezbraniu wody, w ślad za nimi runą chronione domy. Pojawiły się nowe osiedla mieszkaniowe na terenach zalewowych. Nieznani sprawcy ukradli elementy systemu monitorującego poziom wody. Także lekkomyślność ekologów nie sprzyja poprawie bezpieczeństwa.

ZAKOŃCZENIE

System bezpieczeństwa ukierunkowany jest na przeciwdziałanie wszelkim zagrożeniom. W obecnej dekadzie prym wiodą zagrożenia niemilitarne. O bezpieczeństwie możemy mówić, gdy brak jest rzeczywistego zagrożenia i brak poczucia zagrożenia. Wymienione wcześniej obwałowania, jazy, przepusty kanały, śluzy i poldery to urządzenie techniczne, które powinny być dobrze zaprojektowane, wykonane i użytkowane zgodnie z przeznaczeniem i zgodnie z prawem. Wyzwania przeradzają się w zagrożenie przez daleko idącą nonszalancję i lekkomyślność, trudno wytłumaczalnej w państwie prawa, jakim według często wygłaszanych stwierdzeń Polska jest.

LITERATURA

1. Górski J., *Bezpieczeństwo przemysłowych zastosowań komputerów*, III Krajowa Konferencja „Diagnostyka Procesów Przemysłowych", Jurata, 7 – 10 września 1998 r., s. 201-211.
2. Jemioło T., Dawidczyk A., *Wprowadzenie do metodologii badań obronności*, Akademia Obrony Narodowej, Warszawa 2007.
3. *Functional safety: safety- related systems*, International Elektrotechnical Commision standard draft, IEC 1508, 1994.
4. Lis M., *Poldery, wały, zapory*, [w:] „Nowiny Jeleniogórskie", nr 35/2010, s. 9.
5. Kowalczuk Z., *Systemy wykrywające, analizujące i tolerujące usterki*, PWNT, Gdańsk, 2009.
6. Pawłowski J., *Słownik terminów z zakresu bezpieczeństwa narodowego*, Akademia Obrony Narodowej, Warszawa 2009.
7. Wojnarowski J., *System obronności państwa*, Akademia Obrony Narodowej, Warszawa 2005.

SELECTED CONDITIONINGS OF SAFETY

Summary

The paper presents the issues of the safety of the society at human and environment level. Safety results from the relation of challenge vs. threat. Challenges are technical systems and the environment. In technical systems, safety, event, risk, design faults and random faults are qualified. In the social system, elements of the safety protection system before flood are presented.

Key words: *safety, accident, danger, design faults, faults toleration, faults avoidance, protection system, natural environment, flood*

Artykuł recenzował: dr hab. inż. Zenon ZAMIAR, prof. nadzw. WSOWL