Bezpieczeństwo systemów wodociągowych w aspekcie zagrożeń w cyberprzestrzeni

Security of water supply systems in light of threats in cyberspace

BARBARA TCHÓRZEWSKA-CIEŚLAK, JANUSZ R. RAK, MATEUSZ ROŻNOWSKI

DOI 10.36119/15.2024.5.5

Systemy zbiorowego zaopatrzenia w wodę (SZZW) wraz z postępem technologicznym rozwijają się w kierunku automatycznego sterowania wszystkich procesów produkcji wody. Wprowadzanie nowoczesnych technologii w tym sztucznej inteligencji wiąże się równocześnie z licznymi zagrożeniami wewnętrznymi i zewnętrznymi. Systemy zbiorowego zaopatrzenia w wodę należą do tzw. infrastruktury krytycznej, co wiąże się z koniecznością ich specjalnej ochrony. Awarie systemów informatycznych mogą skutkować wyciekiem danych wrażliwych i/lub przekazem błędnych danych (informacji) do operatora systemu. W pracy przedstawiono zagadnienia bezpieczeństwa w eksploatacji systemu wodociągowego z uwzględnieniem zagrożeń w tzw. cyberprzestrzeni. System zbiorowego zaopatrzenia w wodę został scharakteryzowany jako system cyber-fizyczny, rozwijający się w kierunku inteligentnego systemu technicznego. Zaprezentowane zostały przykładowe poziomy zarządzania procesami SZZW z wykorzystaniem nowoczesnych systemów informatycznych. Autorzy omówili pojęcie bezpieczeństwa informatycznego. W pracy zaproponowano także metodę wykorzystania entropii jako miary niepewności informacji, która może zostać zastosowana w analizie ryzyka w procesie zarządzania bezpieczeństwem informatycznym przedsiębiorstw wodociągowych.
Słowa kluczowe: systemy zaopatrzenia w wodę, bezpieczeństwo, cyberprzestrzeń

Collective water supply systems (CWSS), along with technological progress, are developing towards automatic control of all water production processes. The introduction of modern technologies, including artificial intelligence, is associated with numerous internal and external threats. Collective water supply systems belong to the so-called critical infrastructure, which requires special protection. Attacks on IT systems may result in the leakage of sensitive data and/or the transmission of incorrect data (information) to the system operator. The work presents safety issues in the operation of the water supply system, taking into account the risks in the so-called cyberspace. The collective water supply system has been characterized as a cyber-physical system, developing towards an intelligent technical system. Examples of management levels of CWSS processes using modern IT systems were presented. The authors discussed the concept of IT security. The work also proposes a method of using entropy as a measure of information uncertainty, which can be used in risk analysis in the IT security management process of water supply companies.
Keywords: water supply systems, security, cyberspace

Wstęp

Zgodnie z zapisami Dyrektywy Rady 2008/114/WE w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony [4], państwa członkowskie wprowadziły stosowne akty prawne regulujące problematykę ochrony infrastruktury krytycznej. Infrastruktura krytyczna to składniki lub części infrastruktury, które mają istotne znaczenie dla utrzymania podstawowych funkcji społecznych, w tym łańcucha dostaw, zdrowia, bezpieczeństwa, ochrony i dobrobytu społeczno –gospodarczego [15]. Do infrastruktury krytycznej wg w/w Dyrektywy należą: sektor energetyczny, przemysł jądrowy, technologie informacyjno – komunikacyjne (ICT) (sieci informatyczne, internet, systemy automatyzacji i kontroli, świadczenie usług komunikacyjnych), systemy zaopatrzenia w wodę (dostawy wody do spożycia, kontrola jakości wody, monitorowanie i ilościowa kontrola zasobów wodnych), systemy zaopatrzenia w żywność, ochrona zdrowia, sektor finansowy, transport, przemysł chemiczny, przestrzeń kosmiczna i infrastruktura badawcza [15]. Ochrona infrastruktury krytycznej to wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności tej infrastruktury. Celem wdrożenia tych działań jest zapobieganie zagrożeniom, ograniczenie i neutralizacja ich ewentualnych skutków oraz szybkie odtworzenie infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie [11,29].

Systemy zbiorowego zaopatrzenia w wodę (SZZW) stanowią istotny element

prof. dr hab. inż. Barbara Tchórzewska-Cieślak https://orcid.org/0000-0002-7622-6749, prof. dr hab. inż. Janusz R. Rak https://orcid.org/0000-0001-7713-5841, mgr inż. Mateusz Rożnowski https://orcid.org/0009-0007-9323-6408 – Politechnika Rzeszowska im. Ignacego Łukasiewicza, Wydział Budownictwa, Inżynierii Środowiska i Architektury, Katedra Zaopatrzenia w Wodę i Odprowadzania Ścieków, Rzeszów. Adres do korespondencji / Corresponding Author: e-mail: cbarbara@prz.edu.pl, rakjan@prz.edu.pl, m.roznowski@prz.edu.pl

infrastruktury krytycznej, a ich prawidłowe funkcjonowanie ma bezpośredni wpływ na zdrowie społeczeństwa. Obiekty wodociągowe muszą posiadać zdolność do dostawy wody o odpowiedniej jakości, pod odpowiednim ciśnieniem oraz w odpowiedniej ilości w sposób ciągły, niezawodny z uwzględnieniem priorytetu bezpieczeństwa zdrowotnego konsumentom wody. Nowoczesna eksploatacja SZZW polega na prowadzeniu stałej kontroli pracy wszystkich podsystemów tworzących SZZW, z wykorzystaniem narzędzi informatycznych. W szczególności obejmuje procesy [20,31]:

- monitoringu jakości wody na ujęciach wody,
- stałej kontroli parametrów jakości wody po jej uzdatnieniu z uwzględnieniem monitoringu stabilności chemicznej i biologicznej wody wodociągowej,
- monitoringu jakości wody w zbiornikach wody uzdatnionej oraz w wybranych punktach na sieci wodociągowej,
- kontroli pracy urządzeń technicznych w pompowniach wodociągowych oraz urządzeń technologicznych na stacjach uzdatniania wody,
- modernizacji technologii uzdatniania wody zgodnie z obowiązującymi standardami,
- pomiarze ciśnienia i natężenia przepływu w sieci wodociągowej,
- monitoringu stanu przewodów z uwzględnieniem analizy obrostów i biofilmu;
- monitoringu i analizie awaryjności i strat wody.

Wprowadzeniu nowoczesnych technologii kompleksowego sterowania, monitoringu i zarządzania SZZW, oraz systemów kontroli i nadzoru, mogą towarzyszyć zagrożenia wynikające z awarii lub błędów oprogramowania, awarii zasilania, błędów operatorów tych systemów czy celowych działań osób trzecich (ataki w tzw. cyberprzestrzeni). Analiza i ocena tych zagrożeń powinna być elementem analizy bezpieczeństwa dostawy wody opartej na analizie ryzyka. Wykorzystywanie nowoczesnych technologii ma wiele zalet i stanowi nieodzowny element nowoczesnej eksploatacji, jednocześnie istnieje prawdopodobieństwo, że przetwarzane i wykorzystywane w eksploatacji informacje mogą być błędne, a podejmowane w związku z tym decyzje nieprawidłowe [36].

Cyberbezpieczeństwo jest zbiorem najlepszych praktyk, rozwiązań technologicznych czy procesów ułatwiających ochronę przed atakami hakerskimi [40]. Świadomość istniejących zagrożeń wymaga zwiększenia zabezpieczeń informatycznych dla systemów baz danych przedsiębiorstw zajmujących się produkcją i dystrybucją wody. Działania te są konieczne w związku z narastającą liczbą ataków hakerskich celujących w tzw. systemy cyber-fizyczne (CPS – ang. cyber-physical system), do których należy SZZW. Zagrożenie atakami na infrastrukturę informatyczną SZZW jest obecnie jednym z największych problemów eksploatacyjnych [5,26,32,38].

W 2015 roku Departament Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych odnotował 25 zjawisk ataków związanych z cyberbezpieczeństwem w sektorze gospodarki wodnej. Cyberataki na obiekty infrastruktury krytycznej w wielu przypadkach nie są przekazywane do szerszej informacji publicznej. Identyfikacja takich ataków często jest procesem niepewnym i złożonym. Odpowiedź na występujące ataki wymaga opracowanego planu działania, nowoczesnych zabezpieczeń, odpowiedniego doświadczenia oraz umiejętności. Kluczowa jest zdolność do sprawnej identyfikacji ataków [6].

Celem pracy jest przedstawienie zagadnień związanych z cyberbezpieczeństwem systemów zbiorowego zaopatrzenia w wodę.

Bezpieczeństwo w eksploatacji systemu wodociągowego

Bezpieczeństwo SZZW jest pojęciem odnoszącym się do zdolności systemu, który w sposób bezpieczny wykonuje założone funkcje, unika zagrożeń i narażeń oraz ewentualne straty w nim są minimalizowane. Na tej podstawie bezpieczeństwo SZZW można przedstawić korzystając z cech systemu takich jak [18, 35]:

- ochranialność (ang. security), jest cechą, która określa w systemie jego adaptację do ochrony konsumentów wody oraz operatora systemu przed konsekwencjami wewnętrznych oraz zewnętrznych narażeń,
- nieszkodliwość (ang. reliability), jest cechą systemu określającą adaptację systemu do ograniczania negatywnego wpływu funkcjonowania na środowisko naturalne;
- podatność na zagrożenie (ang. vulnerbility), jest cechą opisującą adaptację systemu w aspekcie unikania zagrożeń. Głównymi składowymi podatności są: wrażliwość, ekspozycja (narażenie), odporność, elastyczność (sprężystość);
- funkcjonalność (ang. practicality), będąca cechą opisującą prawidłowość zaprojektowania oraz funkcjonowania systemu w warunkach normalnych i kryzysowych (ekstremalnych), dodatkowo obejmuje kompatybilność oraz sterowalność.

W odniesieniu do konsumentów wody do spożycia, bezpieczeństwo rozumiane jest jako prawdopodobieństwo uniknięcia zagrożenia, wynikającego ze spożycia wody o jakości niezgodnej z obowiązującym normatywem lub jej brakiem. Paradygmatem jest uznanie, jako miary utraty bezpieczeństwa SZZW tzw. „funkcji ryzyka" opisującej zależności pomiędzy przyjętymi parametrami ryzyka [16,17]. Ocena i analiza bezpieczeństwa systemów zbiorowego zaopatrzenia w wodę jest pojęciem złożonym, zawierającym w sobie analizę potencjalnych zagrożeń, skutków i tzw. barier (systemów) bezpieczeństwa. Analiza jest prowadzona w szczególności w kierunku bezpieczeństwa zdrowotnego odbiorców wody, jak również zagrożeń powstałych w wyniku deficytu lub całkowitego zaprzestania dostaw oraz zagrożeń dla środowiska. Istotnym jest, aby proces ten posiadał elementy analizy istniejącego stanu oraz potencjalnie możliwych zagrożeń, jak również zawierał zbiór procedur zabezpieczających oraz naprawczych [18,35]. Rozwinięta definicja ryzyka, w której wprowadza się dodatkowo tzw. parametr ochronny, jako odwrotnie proporcjonalny do wielkości ryzyka [18,20,30], bądź alternatywnie jako parametr podatności na zagrożenie [18,22].

Podatność na zagrożenie powiązane jest z czynnikami takimi jak [21]:

- niezawodnym działaniem obiektów;
- efektywnym i sprawnym usuwaniem awarii;
- możliwością technologii mobilnej uzdatniania wody do spożycia lub czasowego użycia alternatywnych opcji;
- ilością dostępnych źródeł poboru wody;
- metody rezerwowania oraz strukturą połączeń danych elementów w sieci wodociągowej.

Ochrona wiąże się z [21,35]:

- monitoringiem jakości oraz środkami zaradczymi na złą jakość ujmowanej wody;
- strefami pośrednimi i bezpośrednimi ochrony ujęć wody;
- monitoringiem i zarządzaniem pracą sieci wodociągowej pod względem parametrów hydraulicznych;
- posiadaniem wody czystej w zbiornikach sieciowych;

- alternatywnymi opcjami zaopatrzenia w sytuacjach kryzysowych konsumentów w wodę przeznaczoną do spożycia.

Zgodnie z ustawa o zarządzaniu kryzysowym [15] analiza ryzyka powinna zawierać:

- siatkę bezpieczeństwa – należy przez to rozumieć zestawienie potencjalnych zagrożeń ze wskazaniem podmiotu wiodącego przy ich usuwaniu oraz podmiotów współpracujących;
- mapę zagrożenia – należy przez to rozumieć mapę przedstawiającą obszar geograficzny objęty zasięgiem zagrożenia z uwzględnieniem różnych scenariuszy zdarzeń;
- mapę ryzyka – należy przez to rozumieć mapę lub opis przedstawiający potencjalnie negatywne skutki oddziaływania zagrożenia na ludzi, środowisko, mienie i infrastrukturę.

Zgodnie z Dyrektywą 2020/2184 w sprawie jakości wody przeznaczonej do spożycia przez ludzi [3] eksploatacja SZZW powinna obejmować dodatkowo:

- ocenę ryzyka i zarządzanie ryzykiem w obszarze zasilania punktów poboru wody przeznaczonej do spożycia przez ludzi,
- ocenę ryzyka i zarządzanie ryzykiem od punktu poboru do konsumenta.

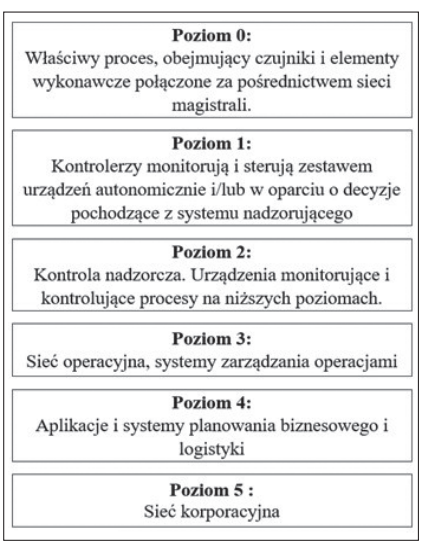
Tego typu analizy powinny zawierać również analizę zagrożeń wynikających z eksploatacji systemów informatycznych. W tym aspekcie można wykorzystać normy:

- PN-EN ISO/IEC 27001:2023-08 Norma standaryzująca bezpieczeństwo informacji, cyberbezpieczeństwo i ochronę prywatności – Systemy zarządzania bezpieczeństwem informacji [7],
- ISO/IEC 27005:2014-01 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji (Information technology – Security techniques – Information security risk management) [8],
- NSC 800-39: Zarządzanie ryzykiem bezpieczeństwa informacji Przegląd struktury organizacyjnej, misji i systemu informatycznego, Narodowy Standard Cyberbezpieczeństwa 01/04/2022 [14].

Wykorzystanie systemów informatycznych w zarządzaniu systemami wodociągowymi

Systemy zbiorowego zaopatrzenia w wodę można scharakteryzować jako rodzaj systemów cyber-fizycznych (CPS). Łączą one w sobie możliwości obliczeniowe oraz fizyczne, wykorzystując je do kontrolowania i monitoringu fizycznych procesów produkcji wody wodociągowej. W przeszłości bezpieczeństwo informatyczne SZZW osiągano w większości poprzez ograniczanie dostępu zewnętrznych podmiotów do elementów sterujących [37]. Wraz z rozwojem technologii, sztucznej inteligencji i tzw. „internetu rzeczy" (ang. Internet of Things – IoT), SZZW, rozwijają się w kierunku inteligentnych systemów technicznych. Połączenie internetu rzeczy oraz metod analizy nazywa się „przemysłowym internetem rzeczy" (ang. Industrial Internet of Things – IIoT). Dzięki ciągłemu rozwojowi inteligentnych systemów technicznych, IIoT zostaje wdrożony do przemysłowych systemów sterowania (ang. industrial control systems – ICS). Celem tego połączenia jest poprawa umiejętności wykrywania oraz kontroli, jak również poprawa integracji z procesami biznesowymi. System IIoT polega na połączeniu wielu poziomów (warstw) systemów cyberfizycznych, w celu zautomatyzowania procesów, ułatwienia podejmowania decyzji oraz wykorzystywania danych w czasie rzeczywistym. Proces ten służy do analizy systemu, w celu poprawy jego wydajności, niezawodności oraz bezpieczeństwa funkcjonowania [28]. Taki postęp technologiczny pozwala na rozwój przedsiębiorstw wodociągowych, które mają możliwość korzystania z nowoczesnych systemów informatycznych [37,38].

Przemysłowy system sterowania kieruje się szeregiem unormowanych poziomów, celem prawidłowego i niezawodnego działania. Rysunek 1 przedstawia przykładowe poziomy zarządzania procesami SZZW [28].



Rys.1
Poziomy zarządzania procesami SZZW (na podstawie [28])
Fig.1 Levels of process management in collective water supply system (based on [28])

Płynne sterowanie procesami SZZW wymaga zbierania szeregu informacji (danych) dotyczących działania poszczególnych elementów SZZW, przekazywania ich w czasie rzeczywistym do operatora systemu, archiwizowania tych danych oraz alarmowania odpowiednich służb utrzymania ruchu. Operator analizując zarejestrowane dane ma możliwość zdalnego sterowania poszczególnymi elementami SZZW, może podejmować odpowiednie decyzje dotyczące pracy systemu np. przejściu na sterowanie remontowe lub awaryjne. Jednocześnie podejmuje decyzję o wysłaniu odpowiedniej ekipy remontowej na miejsce ewentualnej awarii [34]. Do najczęściej wykorzystywanych systemów informatycznych w eksploatacji SZZW zaliczamy oprogramowanie takie jak:

- SCADA – służące do zbierania danych ze sterowanego procesu, przesyłania ich do centralnego komputera oraz wizualizacji całego procesu. System ten umożliwia stały nadzór nad parametrami procesu produkcji wody, sygnalizuje stany alarmowe, informuje o bieżącym stanie urządzeń i wizualizuje parametry ich pracy. Ponadto system ten umożliwia archiwizację, transmisję i przetwarzanie danych pomiarowych. Umożliwia to prawidłową optymalizację parametrów pracy urządzeń (np. parametrów pracy pomp), zbiorników oraz pracy całej sieci wodociągowej [10,27,34];
- GIS – służący do pozyskiwania, magazynowania, kontroli, analizy oraz przedstawiania danych, które są odniesione przestrzennie względem powierzchni ziemi. Oprogramowania ze środowiska GIS mogą być narażone na ataki w cyberprzestrzeni, które mogą skutkować błędami informacji otrzymywanych przez operatora [9,10,12,27];
- programy do modelowania hydraulicznego SZZW – np. Epanet, WaterCAD, Stanet – modelowanie sieci wodociągowej pozwala na projektowanie nowych odcinków oraz diagnostykę infrastruktury już istniejącej. Model sieci wodociągowej jest wykorzystywany również w analizie potencjalnych wielkości i skutków uszkodzeń w sytuacjach kryzysowych. Ponadto, programy do modelowania SZZW gromadzą dane istniejącej infrastruktury, kreują obrazy systemów wodociągowych, czy też przeprowadzają statyczną ocenę porównawczą symulacji i wyników pomiarów [39].

Pojęcie bezpieczeństwa informatycznego

Pojęcie bezpieczeństwa informatycznego odnosi się m.in. do danych (informacji), które są poprzez systemy informatyczne przetwarzane, przechowywane oraz przesyłane. Normą która obowiązuje w tym kontekście jest PN-EN ISO/IEC 27001: 2023-08, która dotyczy Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). Norma ISO/IEC 27005 – „Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji" prezentuje założenia taktyki zarządzania bezpieczeństwem danych bazujących na zarządzaniu ryzykiem. Elementy, które powinny być uwzględnione w zarządzaniu ryzykiem w bezpieczeństwie informacji to: szacowanie ryzyka, postępowanie z ryzykiem, ustawianie kontekstu, informacje o ryzyku, monitorowanie i przegląd ryzyka oraz akceptacja ryzyka [7,8,18].

Biorąc pod uwagę istotność informacji dla użytkownika rozróżniamy dane wrażliwe i niewrażliwe [14]. Dane wrażliwe, które wymagają ochrony można podzielić na dane niejawne oraz dane osobowe. Pojęcia fundamentalne mające związek z bezpieczeństwem danych i systemami informacji to [11]:

- tajność (ang. confidentiality) – wymogiem dostępu do informacji jest odpowiednie uprawnienie;
- dostępność (ang. availability) – możliwość do dostępu i do wykorzystania danych przez uprawniony podmiot na każde żądanie oraz w każdym czasie;
- rozliczalność (ang. accountability) – dany podmiot ma przypisane jednoznaczne działanie;
- zasoby (ang. assets) – wszelkie dane (informacje), które posiadają wartość dla zarządzającego systemem informatycznym;
- autentyczność (ang. authenticity) – atrybut gwarantujący, że tożsamość podmiotu i/lub zasobu jest współmierna z deklarowaną,
- poufność (ang. confidentiality) – dane udostępniane są tylko podmiotom do tego uprawionym;
- integralność danych (ang. data integrity) – dane nie zostały usunięte lub przeformowane w sposób nieuprawiony;
- zagrożenie (ang. threat) – prawdopodobne zdarzenie niepożądane, w wyniku którego może nastąpić uszkodzenie lub zniszczenie dla podmiotu lub systemu;
- ryzyko (ang. risk) – potencjalnie występująca możliwość, że konkretne zagrożenia wykorzysta podatność zasobu, aby z danym prawdopodobieństwem spowodować straty lub zniszczenie danego zasobu;
- analiza ryzyka (ang. risk analysis) – zdefiniowana jest jako proces rozpoznania ryzyka, który określa jego wielkość oraz elementy potrzebujące zwiększenia zabezpieczeń;
- zarządzanie ryzykiem (ang. risk management) – jest procesem diagnozowania, kontrolowania oraz pozbycia się lub ograniczenia prawdopodobieństwa pojawienia się niepożądanych zdarzeń mogących negatywnie wpłynąć na jakość oraz ilość zasobów systemów informatycznych;
- zabezpieczenie (ang. safeguard) – redukcja ryzyka poprzez odpowiednią praktykę, procedurę lub mechanizm;
- niezawodność (ang. reliability) – element określający zamierzone prawidłowe działanie z przewidywaną efektywnością.

Zasoby informatyczne są narażone na wiele rodzajów zagrożeń. Mogą one mieć pochodzenie ze środowiska naturalnego lub antropogenicznego oraz mieć charakter zagrożenia przypadkowego lub celowego [11,33].

Do przykładowych zagrożeń zasobów informatycznych można zaliczyć [33]:

- naturalne losowe, np.: trafienie piorunu w serwerownie, ruchy płyt tektonicznych (trzęsienie ziemi), zalanie (np. w wyniku powodzi), spalenie (pożar);
- ludzkie przypadkowe, np.: przeoczenie, pomyłka, usunięcie pliku, nieprawidłowe skierowanie, zniszczenie fizyczne;
- ludzkie rozmyślne, np.: inwigilacja, przekształcanie danych, hakowanie systemu, złośliwe oprogramowanie (np. koń trojański), kradzież nośnika danych.

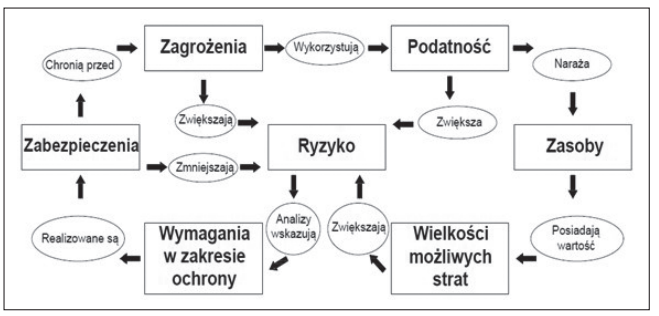
Przykładami zabezpieczeń przed zagrożeniami są [33,37]:

- systemy antyzakłóceniowe sieci komunikacyjnych,
- zabezpieczenia kontroli dostępu,
- zasilacze rezerwowe,
- narzędzia monitorujące i analizujące działania w sieci,
- szyfrowanie danych poufnych,
- tworzenie kopii zapasowych,
- podpisy cyfrowe,
- zapory sieciowe.

Procesami zarządzania bezpieczeństwem systemów informatycznych są [1,24]:

- kierowanie konfiguracją systemu,
- wprowadzanie zmian w systemach informatycznych,
- tłumaczenie potrzeb wymaganych dla komfortu bezpieczeństwa systemów,
- zarządzanie ryzykiem w tym: analizowanie ryzyka, rozliczalność, monitoring sprawności zabezpieczeń, zapewnianie rozliczalności, przewidywanie oraz analiza potencjalnych sytuacji awaryjnych, utworzenie procedury odtwarzającej funkcje systemu po zdarzeniu niepożądanym.

Rysunek 2 przedstawia główne związki, które zachodzą w procesie zarządzania ryzykiem w systemie informatycznym.



Rys.2 Główne związki w zarządzaniu ryzykiem w systemie informatycznym (na podstawie [33])
Fig.2 Main relationships in risk management in the IT system (based on [33])

Entropia jako miara niepewności informacji

Shannon w 1948 roku wprowadził definicję tzw. „ilości informacji" oraz entropii. W 1928 roku pojęcie ilości informacji było rozpatrywane przez Hartley'a [13]. Edwin Thompson Jaynes w roku 1957 sformułował w termodynamice tzw. interpretację maximum entropii (ME), jako szczególne wykorzystanie bardziej ogólnej zasady wnioskowania bayesowskiego. Ilość danych I(A|B), która jest zawarta w zdarzeniu (wiadomości) B w stosunku do zdarzenia A określa się jako liczbę równą [2,13,19]:

$$I(A|B) = \log\frac{P(A|B)}{P(A)} \qquad (1)$$

gdzie:
P(A|B) – prawdopodobieństwo warunkowe zajścia zdarzenia A pod warunkiem zajścia zdarzenia B,
P(A) – prawdopodobieństwo zajścia zdarzenia A.

Jeżeli B=A to znaczy, że nastąpiło zdarzenie A, wówczas I(A|A)=I(A) i jest to ilościowo ilość informacji I(A) zawartej w wiadomości A:

$$I(A|A) = I(A) = -\log P(A) \quad (2)$$

Ilość informacji ma następujące własności [19,35]:

- im większe jest prawdopodobieństwo zdarzenia A, tym mniejsza jest ilość informacji I(A);
- jeżeli zdarzenia A i B są niezależne to I(A|B)=0;
- I(A|B)=I(B|A);
- I(AB)=I(A)+I(B).

Wartość oczekiwana tej informacji E(I) nosi nawę entropii i może być interpretowana jako miara ryzyka niepewności informacji [18,35]. Jest miarą niepewności w zbiorze informacji. Im wyższa entropia tym wyższa niepewność odnośnie posiadanego zbioru informacji. Entropia jest miarą średniej wartości informacji, odpowiadająca zajściu zdarzenia z pewnego zbioru. Zdarzenia w tym zbiorze mają przypisane określone wartości prawdopodobieństwa wystąpienia [2,19]. Wykorzystaniem entropii jako miary informacji zajmuje się teoria informacji [25].

Można ją wyznaczyć korzystając z uproszczonego wzoru [13,19,25]:

$$E(I) = r(I) = -\sum_{i-1}^{n} p(x_i) \cdot log_2 P(x_i) \quad (3)$$

gdzie:

r(I) – ryzyko błędnej informacji (entropia informacji) dla zbioru informacji I;
I – zbiór informacji – $\{x_1,...x_n\}$;
n – liczba możliwych informacji w zbiorze I.

Najważniejsze własności entropii wymieniono poniżej [19,20,35]:

- jest nieujemna;
- jest maksymalna, gdy prawdopodobieństwa zajść zdarzeń są takie same;
- jest równa 0, gdy stany systemu przyjmują wartości 0 albo 1;
- własność superpozycji – gdy dwa systemy są niezależne to entropia sumy systemów równa się sumie entropii;
- maksymalną wartość uzyskuje dla zbioru wydarzeń, równo prawdopodobnych;
- minimalną wartość uzyskuje dla zbioru, w którym jeden element ma prawdopodobieństwo równe 1 (system nie jest obarczony wtedy żadną niepewnością, a otrzymana wiadomość nie jest dla informowanego żadnym zaskoczeniem) – nie niesie niczego nowego.

Należy zauważyć, że jeżeli $p_i = 1$, to E = 0, oraz jeśli prawdopodobieństwa p_i są sobie równe i wynoszą 1|n, to E = ln n, osiągając wartość maksymalną.

Dla prawdopodobieństw a priori p_i stanu systemu obowiązuje formuła [35]:

$$\sum_{i=1}^{n} p_i = 1 \quad (4)$$

gdzie:

n – liczba stanów systemu.

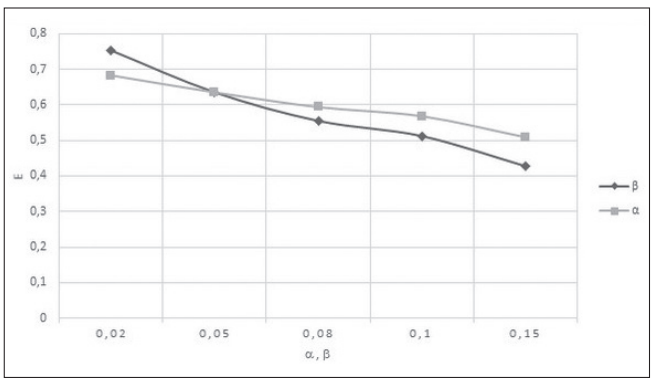
Z pomocą entropii można zweryfikować tzw. efektywność kontroli stanu systemu [19].

Standardowo rozważa się dwa rodzaje błędów [19,21,22]:

α – błąd pierwszego rodzaju polegający na ocenie informacji w rzeczywistości prawdziwej jako nieprawdziwej (błędnej). – Odrzucenie hipotezy prawdziwej;
β – błąd drugiego rodzaju polegający na ocenie informacji w rzeczywistości nieprawdziwej jako prawdziwej. – Przyjęcie hipotezy fałszywej.

Na rysunku 3 przedstawiono zależność entropii (ryzyka błędnej informacji) od błędu I i II –go rodzaju (α i β).

Rys.3
Zależność entropii od błędów I i II rodzaju (α i β). (na podstawie [19])
Fig.3 Dependence of entropy on type I and II errors (α i β) (based on [19])



Przykładowo operator SZZW otrzymuje trzy niezależne informacje w systemie SCADA odnośnie stanów awaryjnych. Zbiór tych informacji można zapisać:

$$I = \{x1, x2, x3\},\ n = 3$$

W wyniki kontroli stanu systemu okazuje się, że dwie informacje są prawdziwe, a jedna jest błędna. Poszczególne wartości prawdopodobieństwa wynoszą:

- dla informacji prawdziwych p_1 i p_2 = 0,666;
- dla informacji fałszywej p_3 = 0,333.

Zgodnie ze wzorem (3) ryzyko błędnej informacji wynosi:

$$r(I) = -(0,666 \cdot log_2 P(0,666) + 0,33 \cdot log_2 P(0,333)) = 0,918$$

Wynik oznacza, że otrzymana informacja obarczona jest dużą niepewnością, co wiąże się z dużym ryzykiem podjęcia błędnej decyzji przez operatora (operator może popełnić błąd I-go lub II-go rodzaju).

Przedstawiona metoda może być wykorzystana w analizach ryzyka dla zagrożeń w systemach informatycznych, które są integralna częścią systemów zarządzania eksploatacją nowoczesnych SZZW. W teorii informacji [25] miara informacji podawana jest w bitach.W tym przypadku wielkość entropii oznacza, że potencjalnie potrzeba 0,918 bitów informacji aby zakodować każdą informację w zbiorze.

Podsumowanie

Systemy informatyczne należą do infrastruktury krytycznej w związku z tym powinny podlegać szczególnej ochronie pod względem bezpiecznego ich funkcjonowania. W związku z pojawiającymi się przypadkami ataków hakerskich na systemy informatyczne SZZW należy opracować odpowiednie procedury, które będą obejmować tematykę cyberbezpieczeństwa w zakresie zapobiegania, wykrywania, reagowania a także na łagodzeniu skutków kończąc.

Problem zabezpieczenia się przed utratą danych lub ich uszkodzeniem ma istotne znaczenie dla bezpiecznego funkcjonowania różnych podmiotów w tym systemów wodociągowych. Można powiedzieć, że nie ma dzisiaj systemu technicznego, dla którego bezpieczeństwo informatyczne nie miałoby kluczowego znaczenia. Problem ten rozwiązywany jest między innymi poprzez:

- projektowanie i wdrażanie kompleksowych systemów zarządzania bezpieczeństwem opartych na analizach ryzyka,
- wewnętrzne i zewnętrzne audyty bezpieczeństwa dla systemów informatycznych,
- stosowania nowoczesnych wielowarstwowych systemów zabezpieczeń,
- systemy kryptografii kwantowej,
- stosowanie nowoczesnego sprzętu,

– projektowanie integralnych systemów automatycznego sterowania odizolowanych od zewnętrznych systemów informatycznych z możliwością przejścia na sterowanie ręczne,
– organizowanie specjalistycznych szkoleń dla obsługi systemów.

W eksploatacji nowoczesnych SZZW opartych na wykorzystaniu inteligentnych systemów zarządzania na każdym etapie produkcji wody, kluczowa jest pewność wykorzystywanych informacji. Pomimo istniejących badań, w których zaproponowano procedury bezpieczeństwa dla SZZW w aspekcie cyberataków (opierających się na ocenie podatności i konsekwencji ataków) temat ten należy w dalszym ciągu rozwijać ze względu na stale rozwijające się technologie, w tym metody sztucznej inteligencji.

Dla przedsiębiorstw wodociągowych problem ten jest obecnie bardzo istotny. Z jednej strony stosowanie nowoczesnych technologii jest obecnie konieczne, a z drugiej stosowanie odpowiednich zabezpieczeń powoduje zwiększenie kosztów eksploatacji całego systemu. Zaproponowana metoda zastosowania entropii w analizie ryzyka niepewności informacji, może być wykorzystana w analizach bezpieczeństwa tych systemów np. na potrzeby planów bezpieczeństwa wody w kontekście zagrożeń dla systemów informatycznych. Przedstawione w publikacji zagadnienia są złożone i wymagają szerokiej analizy inżynierów z różnych branż, w tym specjalistów branży IT oraz zajmujących się cyberbezpieczeństwem.

BIBLIOGRAFIA:

[1] Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Zabezpieczanie informacji
[2] Bolc L., Borodziewicz W., Wójcik M.: Podstawy przetwarzania informacji niepewnej i niepełnej, PWN, 1991.
[3] Dyrektywa Parlamentu Europejskiego I Rady (UE) 2020/2184 z dnia 16 grudnia 2020 r. w sprawie jakości wody przeznaczonej do spożycia przez ludzi
[4] Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony
[5] Falliere N., Murchu L.O.. Chien E.: W32.Stuxnet Dossier (Version 1.4): White Paper, Symantec Security Response: Symantec: Mountain View, CA, USA, 2011.
[6] Hassanzadeh A., Rasekh A., Galelli S., Aghashahi, M., Taormina, R., Ostfeld A.: Banks, M.K. A Review of Cybersecurity Incidents in the Water Sector. J. Environ. Eng. 2020, 146, 03120003.
[7] ISO/IEC 27001 opublikowano 22 sierpnia 2023 r. PN-EN ISO/IEC 27001:2023-08 Norma standaryzująca Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – – Systemy zarządzania bezpieczeństwem informacji.
[8] ISO/IEC 27005:2014 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji (Information technology – Security techniques – Information security risk management)
[9] Kowalska B., Kowalski D., Kwietniewski M., Miszta-Kruk K.: Ocena awaryjności systemu dystrybucji wody z wykorzystaniem bazy danych typu GIS, Zaopatrzenie w wodę, jakość i ochrona wód
[10] Kwietniewski M.: GIS w wodociągach i kanalizacji. PWN, Warszawa 2008.
[11] Liderman K.: Bezpieczeństwo teleinformatyczne. Wydawnictwo Instytutu Automatyki i Robotyki Wojskowej Akademii Technicznej, Warszawa, 2001 r.
[12] Longley P.A., Goodchild M.F., Maguire D.J., Rhind D.W.: GIS teoria i praktyka, Wyd. Nauk. PWN, Warszawa 2008.
[13] Mynarski S.: Elementy teorii systemów i cybernetyki, Państwowe Wydawnictwo Naukowe, Warszawa 1979, s.155
[14] NSC 800-39: Zarządzanie ryzykiem bezpieczeństwa informacji Przegląd struktury organizacyjnej, misji i systemu informatycznego, Narodowy Standard Cyberbezpieczeństwa 01/04/2022
[15] Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 1 grudnia 2022 r. w sprawie ogłoszenia jednolitego tekstu ustawy o zarządzaniu kryzysowym (Poz. 122), Warszawa, 16 styczeń 2023 r.
[16] Rak J.R., Kwietnieski M.: Bezpieczeństwo i zagrożenia systemów zbiorowego zaopatrzenia w wodę, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2011.
[17] Rak J.R., Tchórzewska-Cieślak B. Studziński J.: Bezpieczeństwo systemów zbiorowego zaopatrzenia w wodę, Wydawn. Instytutu Badań Systemowych PAN, Warszawa 2013
[18] Rak J.R., Tchórzewska-Cieślak B.: Ryzyko w eksploatacji systemów zbiorowego zaopatrzenia w wodę, Wydawn. Seidel-Przywecki Sp. z o.o., Rzeszów 2013
[19] Rak J.R., Tchórzewska-Cieślak B.: Czynniki ryzyka w eksploatacji systemów zaopatrzenia w wodę, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2007.
[20] Rak J.R., Tchórzewska-Cieślak B.: Metody analizy i oceny ryzyka w systemie zaopatrzenia w wodę. Oficyna Wydawnicza Politechniki Rzeszowskiej. Rzeszów, 2005
[21] Rak J.R.: Bezpieczeństwo systemów zaopatrzenia w wodę, Polska Akademia Nauk, Instytut Badań Systemowych, Warszawa 2009.
[22] Rak J.R.: Podstawy bezpieczeństwa systemów zaopatrzenia w wodę, Monografie Komitetu Inżynierii Środowiska Polskiej Akademii Nauk, Lublin 2005, vol. 28.
[23] Rak J.R.: Problematyka ryzyka wodociągach, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2014.
[24] Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej
[25] Shannon C.E.: A Mathematical Theory of Communication, Reprinted with corrections from The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, July, October, 1948.
[26] Shin S., Lee S., Burian S.J., Judi D.R., McPherson T.: Evaluating Resilience of Water Distribution Networks to Operational Failures from Cyber-Physical Attacks. J. Environ. Eng. 2020, 146
[27] Studziński J.: Systemy GIS i SCADA oraz model hydrauliczny jako podstawowe elementy zintegrowanej informatyzacji miejskiego systemu zaopatrzenia w wodę, Instytut Badań Systemowych PAN, Warszawa 2012
[28] SWAN Forum. A Layered View of Smart Water Networks.
[29] Szeżyńska M.: Kryptografia i bezpieczeństwo informacji w sytuacjach kryzysowych jako continuum środków technicznych i organizacyjnych. Materiały konferencji naukowej ,, Informatyka w zarządzaniu w sytuacjach kryzysowych. Wydawnictwo Wyższej Szkoły Informatyki , Zarządzania i Administracji w Warszawie. Warszaw 2006.s.38-44.
[30] Szpak D., Boryczko K., Żywiec, J., Piegdoń, I., Tchórzewska-Cieślak, B., Rak, J.R.: Risk Assessment of Water Intakes in South-Eastern Poland in Relation to the WHO Requirements for Water Safety Plans. Resources 2021, 10, 105. https://doi.org/10.3390/resources10100105
[31] Szpak D., Tchórzewska-Cieślak B.: Analiza awaryjności sieci wodociągowej w aspekcie bezpieczeństwa funkcjonowania infrastruktury krytycznej, Chemik, 2014, 68(10), s.862-867.
[32] Tatbul N., Lee T.J., Zdonik S., Alam M., Gottschlich J.: Precision and Recall for Time Series. In Proceedings of the 32nd International Conference on Neural Information Processing Systems, NIPS 2018, Denver, CO, USA, 3–8 December 2018: Curran Associates Inc.: Red Hook, NY, USA, 2018: pp. 1924–1934.
[33] Tchórzewska-Cieślak B., Rak J.: Bezpieczeństwo informatyczne firmy wodociągowej. Ośrodek Informacji „Technika Instalacyjna w Budownictwie". Instal, z.12, s.57-60, 2007
[34] Tchórzewska-Cieślak B., Szpak D.: Propozycja metody analizy i oceny bezpieczeństwa dostawy wody, Ochrona Środowiska, 2015, 37(3), s.43-47.
[35] Tchórzewska-Cieślak B.: Wieloaspektowa analiza bezpieczeństwa w eksploatacji systemów wodociągowych. Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2018
[36] Tchórzewska-Cieślak B.: Characterization of risk function in the analysis and assessment of water supply systems safety, Technical Transaction, Czasopismo Techniczne, 2018, 3)115), s.187-197.
[37] Tuptuk N., Hazell P., Watson J., Hailes S. A.: Systematic Review of the State of Cyber-Security in Water Systems. Water 2021, 13, 81.

NETOGRAFIA:

[38] Kaspersky. BlackEnergy APT Attacks in Ukraine. Available online: https://www.kaspersky.co.uk/resource-center/threats/blackenergy (dostęp 11.02.2024)
[39] https://portalkomunalny.pl/plus/artykul/komputerowe-modelowanie-systemow-zaopatrzenia-w-wode/ (dostęp 07.03.2024)
[40] https://www.microsoft.com/pl-pl/security/business/security-101/what-is-cybersecurity (dostęp 11.03.2024)

■