Journal of KONBiN 2019
Volume 49, Issue 2
DOI 10.2478/jok-2019-0037

Barbara Tchórzewska-Cieślak, Janusz R. Rak, Dawid Szpak
Rzeszow University of Technology (Politechnika Rzeszowska)

METHOD OF ANALYSIS AND ASSESSMENT OF ICT SYSTEM SAFETY IN A WATER COMPANY

Metoda analizy i oceny bezpieczeństwa systemu teleinformatycznego przedsiębiorstwa wodociągowego

Abstract: *An important and very often overlooked issue in risk analysis in water supply systems is ICT safety. Water companies should take actions to protect the process of water delivery and water distribution from disruption or takeover of control by external entities. The aim of the work is to develop an author's method of analysis and assessment of the ICT system safety in a water company. It was assumed that the measure of ICT safety loss is the risk related to its functioning.*
Keywords: water supply system, ICT system, safety

Streszczenie: *Istotnym, a bardzo często pomijanym zagadnieniem w analizie ryzyka w systemach wodociągowych jest bezpieczeństwo teleinformatyczne. Przedsiębiorstwa wodociągowe powinny podjąć działania uniemożliwiające podmiotom zewnętrznym zakłócenie lub przejęcie kontroli nad procesem dostawy i dystrybucji wody. Celem pracy jest opracowanie autorskiej metody analizy i oceny bezpieczeństwa systemu teleinformatycznego w przedsiębiorstwie wodociągowym. Przyjęto, że miarą utraty bezpieczeństwa teleinformatycznego jest ryzyko związane z jego funkcjonowaniem.*
Słowa kluczowe: wodociąg, system teleinformatyczny, bezpieczeństwo

1. Introduction

According to the Act [13], critical infrastructure consist of ICT network systems and water supply systems. They are the key systems for the society and the state functioning. Therefore, they must be characterized by a high safety level. The definition of ICT safety is to protect and processed information, stored and transmitted by ICT systems against undesired disclosure, modification, destruction

or disallowing of its processing [4, 5]. Detailed identification of threats is very important [3]. Safety of critical infrastructure systems includes also functional safety and information protection [2, 9].

The collective water supply system (CWSS) seems to be a potential target of the attack due to the large range of its impact and the direct impact of on the tap water on the consumers health [12]. An important and very often overlooked issue in the CWSS risk analysis is protection against cybercrimes and cyberterrorism. For this purpose water supply companies should take actions to prevent disrupting or taking control of the water supply and distribution processes by external entities by applying safety procedures in cyberspace.

Cyberattacks on CWSS in highly developed countries (especially in the United States of America) are becoming more and more common every year. For example, in October 2018, the ONWASA water supply company reported an attack on the CWSS in Onslow, North Carolina. The water supply company did not handle with the attack, so they needed help from an external company dealing with the cybercrimes. As a result of the cyberattack, some of the databases were lost. The FBI, Department of Homeland Security and authorities of the state of North Carolina took care of this case [14].

Nowadays practically all CWSS use modern computer software such as SCADA or GIS, and water treatment processes are fully automated [1, 6]. The communication between individual subsystems included in the CWSS usually use GPRS data transmission. Therefore, interference of remote control elements by third parties may lead to disruptions in the CWSS functioning and result as threatens in the water consumers safety.

The aim of the study is to develop an original method of analysis and assessment of the ICT system safety in a water supply company. It was assumed that the measure of ICT system safety loss is the risk related to its functioning.

2. The concept of ICT system safety

Information are divided into sensitive and insensitive due to its importance to the user. Sensitive informations are protected and divided into classified informations and personal informations. The basic attributes of ICT systems are related to their safety [5]:

- confidentiality - access to the specific information is available only for authorized entities,
- availability - feature of being available and usable at any request, within the prescribed time by an authorized entity,

- accountability - the property of unambiguously assigning action to a given entity,
- assets - all that has value for the entity managing the ICT system,
- authenticity - feature that ensures the identity of the resource or entity is consistent with the declared,
- confidentiality - feature that ensures that information is not disclosed or shared with unauthorized items,
- data integrity - feature that ensures that the data has not been altered or removed in an unauthorized way,
- threat - potential cause of an undesirable event, which may result in loss or damage to the system and/or the entity,
- vulnerability - weakness of the resource, that can be used by a threat,
- risk - the possibility that a given threat will exploit the vulnerability of the resource, to cause losses or destruction of this resource with a given probability,
- risk analysis - risk identification process, determining its value and areas requiring additional security,
- risk management - the identification process, controlling and eliminating or minimizing the probability of undesirable events, which may have a negative impact on the quantity and quality of the ICT system resources,
- safeguard - a practice, procedure or mechanism that reduces the risk,
- reliability - feature which means intended correct functioning with the expected efficiency.

ICT resources are subject to many types of threats. They are of natural or human origin and may be accidental or intentional. Examples of threats to ICT resources:

- natural random causes:
  - atmospheric discharge,
  - earthquake,
  - flood,
  - fire,
- human accidental causes,
  - mistakes, omissions,
  - deleting the file,
  - incorrect referral,
  - mechanical damage,
- human intentional operation,
  - wiretapping,
  - modification of information,

- hacking into the system,
- malicious code,
- theft.

Examples of security against threats:

- anti-interference software of the communication system,
- access control mechanisms,
- digital signatures,
- encryption to obtain confidentiality,
- firewalls,
- network monitoring and analysis tools,
- stand-by power supply,
- backups.

The ICT safety management processes include [5]:

- system configuration management,
- changes management process in the ICT system,
- raising awareness of he needs related to the safety comfort,
- risk management:
  - risk analysis,
  - accountability,
  - monitoring the effectiveness of security and ensuring accountability,
  - emergency scenario planning,
  - procedures for restoring system functions after an undesirable event.

3. Analysis of ICT safety in a water supply company

One of the main stages of safety management is risk analysis are:

- risk identification,
- risk assessment,
- risk financing.

Identification of risk mainly consists of risk factors analysis, their sources, identification of weak points and the consequences of their occurrence. Generally, the analysis concerns undesirable events that may occur in the system with a certain probability of "P" and cause specific losses "C", which may result as a loss of system safety. These events may be individual (incidental), it may be a series of events or a single event that induce the series of events (domino effect) [7].

The process of risk assessment consists of determining (estimating) its numerical value and comparing it with the adopted, normative values. The most common scale of risk levels is the three-level scale according to [7,8]:

- tolerable risk - r_T,
- controlled risk - r_K,
- unacceptable risk - r_N.

The acceptance of criteria values depends on many factors, including expert assessments, as well as the risk assessment methodology adopted for example, 2,3,4 or 5-parameter matrix methods [7,8].

The analysis of the results can be carried out on the basis of:

- percentage distribution of risk according to category (type) of risk,
- distribution of unacceptable risks,
- distribution of vulnerabilities according to the distribution of unacceptable risks,
- providing an indicator of unacceptable risks Wr_N - the ratio of the number of unacceptable risks to the total number of risks in a given category. It shows which types of risks are moving towards the unaccepted risk.

The analysis of three-parameter risk definition: r = f (P, C, O) was adopted. The individual risk parameters were assigned with the appropriate point weights for the adopted scale (Table 1). This relation can be described by a formula, which can be used to prepare a risk matrix (Table 2) [2,3]:

$$r = \frac{P \cdot C}{O} \tag{1}$$

where:

P – point weight related to the probability of a given adverse event,

C – point weight related to the amount of losses,

O – point weight related to the protective system against threats.

Table 1

Point weights for the levels scale of individual risk parameters: P,C and O

Scale level / Parameter	Low - L	Medium - M	High - H
	Scale		
P, C, O	1	2	3

Table 2

Risk values (risk matrix)

C·P	O		
	1	2	3
	r		
1	1	0,5	0,33
2	2	1	0,67
3	3	1,5	1
4	4	2	1,33
6	6	3	2
9	9	4,5	3

In this way, 18 possible risk values were obtained. The criteria values for individual levels are as follows:

- tolerable risk r_T: [0,33÷2),
- controlled risk r_K: [2÷4),
- unacceptable risk r_N:[4÷9].

4. Application example

Individual values of Wr risk indicators for particular risks were calculated according to the following formulas [10, 11]:

- tolerable risk index Wr_T:

$$Wr_T = \frac{r_T}{\sum r_{TKN}} \tag{2}$$

- controlled risk index Wr_K:

$$Wr_K = \frac{r_K}{\sum r_{TKN}} \tag{3}$$

where:

$$\sum r_{TKN} = \sum_i r_T + \sum_j r_K + \sum_k r_N \tag{4}$$

- acceptable risk index Wr_A:

$$Wr_A = \frac{r_A}{\sum r_{TKN}} \tag{5}$$

where:

$$r_A = \sum r_{TK} = \sum_i r_T + \sum_j r_K \tag{6}$$

r_A- acceptable risk.

- unacceptable risk index Wr_N:

$$Wr_T = \frac{r_N}{\sum r_{TKN}} \tag{7}$$

The analysis method is as follows. Based on the risk identification for representative emergency scenarios, in the analysis of the ICT system safety of the water supply company, the number of risks in the range of adopted risk scale was calculated. On this basis of these calculations, the Wr risk index for each scale was calculated (table 3) [11].

Table 3

An example of analysis of various types of risks

Category	Incident/ type of risk	Number of risks on a given scale			$\sum r_{KT}$	$\sum r_{NKT}$	Wr_T	Wr_K	Wr_A	Wr_N
		r_T	r_K	r_N						
A	System damage	3	5	1	8	9	0,33	0,56	0,89	0,11
B	Software damage	4	5	2	9	11	0,36	0,45	0,82	0,18
C	Data loss	2	3	2	5	7	0,29	0,43	0,71	0,29
D	Disclosure of data	3	5	3	8	11	0,27	0,45	0,73	0,27
E	Data theft	1	2	1	3	4	0,25	0,50	0,75	0,25

On the basis of values in tab. 3 it was found that the value of the Wr_N index is the highest for category C. It means that in the area of securing the system against the possibility of data loss, the CWSS operator should take actions to eliminate the most important risk factors. For the presented example of risk analysis related to the ICT system operation of a water supply company, the highest risk indicator was obtained for acceptable risk, being the sum of tolerated and controlled risk, and the smallest for unaccepted risk.

5. Summary

ICT safety is an important and very often overlooked issue in the CWSS risk analysis. Water companies should make decisions to prevent operators from external interference or take control over the process of supply and distribution of water.

The values of risk indexes for individual types of undesirable events determine the risk of failures in a percentage form. This allows prioritization process of undesirable events and identifying the situations posing a threat.

The matrix method is an expert method and requires the appointment of an appropriate team consisting of experienced persons with appropriate competences. The team leader should be a water company. The team should be supported by an external company dealing with cybercrime.

6. References

1. Boryczko K., Tchorzewska-Cieslak B.: Analysis and assessment of the risk of lack of water supply using the EPANET program. Environmental Engineering IV - Proceedings of the Conference on Environmental Engineering IV, 2013.
2. Janczak J., Nowak A.: Bezpieczeństwo informacyjne. Wybrane problemy. Wydawnictwo: Akademia Obrony Narodowej, Warszawa 2013.
3. Jóźwiak I., Laskowski W. Szleszyński A.: Wykorzystanie drzewa użyteczności w procesie planowania i wdrożenia systemu bezpieczeństwa informacji. Journal of KONBiN, 2,3(14,15) 2010.
4. Liderman K.: Analiza ryzyka dla potrzeb bezpieczeństwa teleinformatycznego. Biuletyn Instytutu Automatyki i Robotyki, 16/2001.
5. Liderman K.: Bezpieczeństwo teleinformatyczne. Wydawnictwo Instytutu Automatyki i Robotyki Wojskowej Akademii Technicznej, Warszawa 2001.

6. Piegdoń I., Tchórzewska-Cieślak B.: Methods of visualizing the risk of lack of water supply. Safety and Reliability: Methodology and Applications - Proceedings of the European Safety and Reliability Conference, ESREL 2014.
7. Rak J.: Podstawy bezpieczeństwa systemów zaopatrzenia w wodę. Wydawnictwo PAN - Komitet Inżynierii Środowiska t. 28, Lublin 2005.
8. Rak J., Tchórzewska-Cieślak B.: Metody analizy i oceny ryzyka w systemie zaopatrzenia w wodę. Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2005.
9. Śliwiński M.: Bezpieczeństwo funkcjonalne i ochrona informacji w obiektach i systemach infrastruktury krytycznej. Seria monografie nr 171. Wydawnictwo Politechniki Gdańskiej, Gdańsk 2018.
10. Tchórzewska-Cieślak B., Piegdoń I.: Metoda identyfikacji ryzyka awarii sieci wodociągowych. Wydawnictwo Instytutu Technicznego Wojsk Lotniczych, Journal of KONBiN, z.1 (37) 2016, DOI 10.1515/jok-2016-0004.
11. Tchórzewska-Cieślak B., Rak J.: Bezpieczeństwo informatyczne firmy wodociągowej. Ośrodek Informacji „Technika instalacyjna w budownictwie". Instal, z.12, 57-60, 2007.
12. Żuber M.: Infrastruktura krytyczna państwa jako obszar potencjalnego oddziaływania terrorystycznego. Rocznik Bezpieczeństwa Międzynarodowego, 8/2014, 178-197.
13. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późniejszymi zmianami).
14. https://www.cyberdefence24.pl/fbi-wszczelo-dochodzenie-ws-cyberataku-na-wodociagi-w-karolinie-pln.

METODA ANALIZY I OCENY BEZPIECZEŃSTWA SYSTEMU TELEINFORMATYCZNEGO PRZEDSIĘBIORSTWA WODOCIĄGOWEGO

1. Wprowadzenie

Zgodnie z Ustawą o zarządzaniu kryzysowym [13] w skład infrastruktury krytycznej wchodzą m.in. systemy sieci teleinformatycznych oraz zaopatrzenia w wodę. Są to systemy kluczowe dla funkcjonowania społeczeństwa i państwa. W związku z tym muszą się charakteryzować wysokim poziomem bezpieczeństwa. Przez bezpieczeństwo teleinformatyczne rozumie się ochronę informacji przetwarzanej, przechowywanej i przesyłanej za pomocą systemów teleinformatycznych przed niepożądanym ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania [4, 5]. Bardzo istotna jest szczegółowa identyfikacja zagrożeń [3]. Na bezpieczeństwo systemów zaliczanych do infrastruktury krytycznej składa się bezpieczeństwo funkcjonalne oraz ochrona informacji [2, 9].

System zbiorowego zaopatrzenia w wodę (SZZW) wydaje się potencjalnym celem ataku zewnętrznego ze względu na bardzo duży zasięg oddziaływania oraz bezpośredni wpływ dostarczanej wody na zdrowie konsumentów [12]. Istotnym, a bardzo często pomijanym zagadnieniem w analizie ryzyka w SZZW jest zabezpieczenie przed cyberprzestępstwami oraz cyberterroryzmem. W tym celu przedsiębiorstwa wodociągowe powinny podjąć działania uniemożliwiające podmiotom zewnętrznym zakłócenie lub przejęcie kontroli nad procesem dostawy i dystrybucji wody, m.in. przez zastosowanie procedur zapewnienia bezpieczeństwa w cyberprzestrzeni.

Cyberataki na SZZW w krajach wysoko rozwiniętych (szczególnie w Stanach Zjednoczonych) stają się z każdym rokiem coraz bardziej powszechne. Przykładowo w październiku 2018 r. spółka wodociągowa ONWASA odnotowała atak na infrastrukturę miejskiej sieci wodociągowej w miejscowości Onslow w Karolinie Północnej. Przedsiębiorstwo wodociągowe nie było w stanie sobie samo poradzić z atakiem, konieczna była pomoc ze strony firmy zewnętrznej zajmującej się

cyberprzestępstwami. W wyniku cyberataku utracono część baz danych. Wyjaśnieniem sprawy zajęły się m.in. FBI, Departament Bezpieczeństwa Wewnętrznego oraz władze stanu Północna Karolina [14].

Obecnie praktycznie wszystkie SZZW wykorzystują nowoczesne oprogramowanie komputerowe typu SCADA czy GIS, a procesy uzdatniania wody są w pełni zautomatyzowane [1, 6]. Komunikacja pomiędzy poszczególnymi podsystemami wchodzącymi w skład SZZW odbywa się zwykle z wykorzystaniem transmisji danych GPRS. W związku z tym zakłócenie pracy elementów zdalnego sterowania przez osoby trzecie może doprowadzić do zakłóceń w funkcjonowaniu SZZW, a w rezultacie zagraża bezpieczeństwu konsumentów wody.

Celem pracy jest opracowanie autorskiej metody analizy i oceny bezpieczeństwa systemu teleinformatycznego w przedsiębiorstwie wodociągowym. Przyjęto, że miarą utraty bezpieczeństwa teleinformatycznego jest ryzyko związane z jego funkcjonowaniem.

2. Pojęcie bezpieczeństwa teleinformatycznego

Ze względu na znaczenie dla użytkownika informacje dzieli się na wrażliwe i niewrażliwe. Informacje wrażliwe podlegają ochronie i dzielą się na informacje niejawne i dane osobowe. Podstawowe atrybuty systemów teleinformatycznych związane z ich bezpieczeństwem to [5]:

- tajność (ang. *confidentiality*) – dostęp do określonych informacji posiadają wyłącznie podmioty do tego uprawnione,
- dostępność (ang. *availability*) – właściwość polegająca na byciu dostępnym i możliwym do wykorzystania na każde żądanie, w założonym czasie, przez autoryzowany podmiot,
- rozliczalność (ang. *accountability*) – właściwość polegająca na zapewnieniu jednoznacznego przypisania działania danemu podmiotowi,
- zasoby (ang. *assets*) – to wszystko, co ma wartość dla podmiotu zarządzającego systemem teleinformatycznym,
- autentyczność (ang. *authenticity*) – właściwość zapewniająca, że tożsamość zasobu lub podmiotu jest zgodna z deklarowaną,
- poufność (ang. *confidentiality*) – właściwość zapewniająca, że informacja nie jest ujawniona lub udostępniana przedmiotom nieuprawnionym (nieautoryzowanym),
- integralność danych (ang. *data integrity*) – właściwość zapewniająca, że dane nie zostały zmienione lub usunięte w sposób nieautoryzowany,

- zagrożenie (ang. *threat*) – potencjalna przyczyna niepożądanego zdarzenia, którego skutkiem może być strata lub szkoda dla systemu lub/i podmiotu,
- podatność (ang. *vulnerability*) – słabość zasobu, która może być wykorzystana przez zagrożenie,
- ryzyko (ang. *risk*) – możliwość, że określone zagrożenie wykorzysta podatność zasobu, aby z danym prawdopodobieństwem spowodować straty lub zniszczenie tegoż zasobu,
- analiza ryzyka (ang. *risk analysis*) – proces identyfikacji ryzyka, określenie jego wartości i obszarów wymagających dodatkowych zabezpieczeń,
- zarządzanie ryzykiem (ang. *risk management*) – proces identyfikacji, kontrolowanie i eliminowanie lub minimalizowanie prawdopodobieństwa zaistnienia niepożądanych zdarzeń, które mogą mieć negatywny wpływ na ilość i jakość zasobów systemu teleinformatycznego,
- zabezpieczenie (ang. *safeguard*) – praktyka, procedura lub mechanizm redukujący ryzyko,
- niezawodność (ang. *reliability*) – właściwość oznaczająca zamierzone poprawne funkcjonowanie z oczekiwaną efektywnością.

Zasoby teleinformatyczne podlegają wielu rodzajom zagrożeń. Mają one pochodzenie naturalne lub ludzkie i mogą mieć charakter przypadkowy lub celowy. Przykłady zagrożeń zasobów teleinformatycznych:

- naturalne losowe,
  - wyładowanie atmosferyczne,
  - trzęsienie ziemi,
  - podtopienie w wyniku powodzi,
  - pożar,
- ludzkie przypadkowe,
  - pomyłki, pominięcia,
  - skasowanie pliku,
  - błędne skierowanie,
  - uszkodzenia fizyczne (mechaniczne),
- ludzkie rozmyślne (celowe),
  - podsłuch,
  - modyfikacja informacji,
  - włamanie do systemu,
  - złośliwy kod,
  - kradzież.

Przykłady zabezpieczeń przed zagrożeniami to:

- oprogramowanie antyzakłóceniowe systemu komunikacji,

- mechanizmy kontroli dostępu,
- podpisy cyfrowe,
- szyfrowanie w celu uzyskania poufności,
- zapory sieciowe,
- narzędzia monitoringu i analizy sieci,
- zasilanie rezerwowe,
- kopie zapasowe.

Procesy zarządzania bezpieczeństwem systemów teleinformatycznych to [5]:

- zarządzanie konfiguracją systemu,
- zarządzanie zmianami w systemie teleinformatycznym,
- uświadamianie potrzeb związanych z komfortem bezpieczeństwa,
- zarządzanie ryzykiem,
  - analiza ryzyka,
  - rozliczalność,
  - monitorowanie efektywności zabezpieczeń i zapewnienia rozliczalności,
  - planowanie scenariuszy awaryjnych,
  - procedury odtwarzania funkcji systemu po wystąpieniu zdarzenia niepożądanego.

3. Analiza bezpieczeństwa teleinformatycznego w przedsiębiorstwie wodociagowym

Jednym z głównym etapów zarządzania bezpieczeństwem jest analiza ryzyka, a w szczególności:

- identyfikacja ryzyka,
- ocena ryzyka,
- finansowanie ryzyka.

Identyfikacja ryzyka polega głównie na analizie czynników ryzyka, ich źródeł, określeniu tzw. słabych punktów oraz konsekwencji (skutków) ich występowania. Najczęściej analiza ta dotyczy zdarzeń niepożądanych, które mogą pojawić się w systemie z określonym prawdopodobieństwem P i wywołać określone straty C, co może skutkować utratą bezpieczeństwa systemu. Zdarzenia te mogą mieć charakter pojedynczy (incydentalny), może być to seria zdarzeń lub pojedyncze zdarzenie wywołujące serię następnych (tzw. efekt domina) [7].

Proces oceny ryzyka polega na wyznaczeniu (oszacowaniu) jego liczbowej wartości i porównaniu go z przyjętymi wartościami kryterialnymi. Najczęściej spotykaną skalą poziomów ryzyka jest skala trójstopniowa wg zasady [7,8]:

- ryzyko tolerowane – r_T,
- ryzyko kontrolowane – r_K,
- ryzyko nieakceptowane – r_N.

Przyjęcie wartości kryterialnych zależy od wielu czynników, m.in. ocen ekspertów oraz przyjętej metody szacowania ryzyka, jak np. metody matrycowe 2-,3-,4- lub 5-parametryczne [7,8]. Analizę wyników można przeprowadzić w oparciu o:

- rozkład procentowy ryzyka wg kategorii (rodzaju) ryzyka,
- rozkład ryzyk nieakceptowanych,
- rozkład podatności według rozkładu ryzyk nieakceptowanych,
- podanie wskaźnika ryzyk nieakceptowanych Wr_N – stosunek liczby ryzyk nieakceptowanych do całkowitej liczby ryzyk w danej kategorii, pokazuje on, które z rodzajów ryzyk zmierzają w stronę ryzyka nieakceptowanego.

W analizie przyjęto trójparametryczną definicję ryzyka: $r = f(P, C, O)$. Poszczególnym parametrom ryzyka przypisuje się odpowiednie wagi punktowe dla przyjętej skali, co przedstawiono w tab. 1. Zależność ta jest opisana przez wzór, który można wykorzystać do sporządzenia matrycy ryzyka (tab. 2) [2,3]:

$$r = \frac{P \cdot C}{O} \tag{1}$$

gdzie:

P – waga punktowa związana z prawdopodobieństwem wystąpienia danego zdarzenia niepożądanego,

C –waga punktowa związana z wielkością strat,

O – waga punktowa związana z ochroną systemu przed zagrożeniami.

Tabela 1

Wagi punktowe dla poziomów skali poszczególnych parametrów ryzyka: P,C i O

Poziom skali / Parametr	Niski - L	Średni - M	Wysoki - H
	Waga		
P, C, O	1	2	3

Tabela 2

Wartości ryzyka (matryca ryzyka)

C·P	O		
	1	2	3
	r		
1	1	0,5	0,33
2	2	1	0,67
3	3	1,5	1
4	4	2	1,33
6	6	3	2
9	9	4,5	3

W ten sposób otrzymano 18 możliwych wartości ryzyka. Wartości kryterialne dla poszczególnych poziomów przedstawiają się następująco:

- ryzyko tolerowane r_T: [0,33÷2),
- ryzyko kontrolowane r_K: [2÷4),
- ryzyko nieakceptowane r_N:[4÷9].

4. Przykład aplikacyjny

Poszczególne wartości wskaźników ryzyka *Wr* dla poszczególnych ryzyk obliczono wg następujących wzorów [10, 11]:

- wskaźnik ryzyka tolerowanego Wr_T

$$Wr_T = \frac{r_T}{\sum r_{TKN}} \tag{2}$$

- wskaźnik ryzyka kontrolowanego Wr_K

$$Wr_K = \frac{r_K}{\sum r_{TKN}} \tag{3}$$

gdzie:

$$\sum r_{TKN} = \sum_i r_T + \sum_j r_K + \sum_k r_N \tag{4}$$

- wskaźnik ryzyka akceptowalnego Wr_A

$$Wr_A = \frac{r_A}{\sum r_{TKN}} \tag{5}$$

gdzie

$$r_A = \sum r_{TK} = \sum_i r_T + \sum_j r_K \tag{6}$$

r_{A-} ryzyko akceptowalne

- wskaźnik ryzyka nieakceptowalnego Wr_N

$$Wr_T = \frac{r_N}{\sum r_{TKN}} \tag{7}$$

Sposób analizy jest następujący. Na podstawie identyfikacji ryzyka dla reprezentatywnych scenariuszy awaryjnych w analizie bezpieczeństwa przykładowego systemu teleinformatycznego firmy wodociągowej obliczono liczbę ryzyk mieszczących się w przyjętej skali ryzyka. Na tej podstawie obliczono wskaźnik ryzyka *Wr* dla każdej skali, co przedstawiono w tab. 3 [11].

Tabela 3

Przykład analizy różnych rodzajów ryzyk

Kategoria	Zdarzenie / rodzaj ryzyka	Liczba ryzyk w danej skali			$\sum r_{KT}$	$\sum r_{NKT}$	Wr_T	Wr_K	Wr_A	Wr_N
		r_T	r_K	r_N						
A	Uszkodzenie systemu	3	5	1	8	9	0,33	0,56	0,89	0,11
B	Uszkodzenie oprogramowania	4	5	2	9	11	0,36	0,45	0,82	0,18
C	Utrata danych	2	3	2	5	7	0,29	0,43	0,71	0,29
D	Ujawnienie danych	3	5	3	8	11	0,27	0,45	0,73	0,27
E	Kradzież danych	1	2	1	3	4	0,25	0,50	0,75	0,25

Na podstawie tab. 3 stwierdzono, że wartości wskaźnika Wr_N jest największa dla kategorii C, co oznacza, że w obszarze zabezpieczenia systemu przed możliwością utraty danych operator SZZW powinien podjąć działania w celu

wyeliminowania najistotniejszych funkcjonalnie czynników ryzyka. Dla przedstawionego przykładu analizy ryzyka związanego z funkcjonowaniem systemu teleinformatycznego przedsiębiorstwa wodociągowego największy wskaźnik ryzyka otrzymano dla ryzyka akceptowalnego będącego sumą ryzyka tolerowanego i kontrolowanego, a najmniejszy dla ryzyka nieakceptowanego.

5. Podsumowanie

Istotnym, a bardzo często pomijanym zagadnieniem w analizie ryzyka w SZZW jest bezpieczeństwo teleinformatyczne. Przedsiębiorstwa wodociągowe powinny podjąć działania uniemożliwiające podmiotom zewnętrznym zakłócenie lub przejęcie kontroli nad procesem dostawy i dystrybucji wody.

Wartości indeksów ryzyka dla poszczególnych typów zdarzeń niepożądanych określają ryzyko awarii w formie procentowej. Pozwala to na priorytetyzację zdarzeń niepożądanych, a tym samym wskazanie sytuacji stanowiących zagrożenie.

Metoda matrycowa jest metodą ekspercką i wymaga powołania odpowiedniego zespołu składającego się z osób doświadczonych, posiadających odpowiednie kompetencje. Liderem zespołu powinno być przedsiębiorstwo wodociągowe. Zespół powinno wspomagać przedsiębiorstwo zewnętrzne zajmujące się walką z cyberprzestępczością.

6. Literatura

1. Boryczko K., Tchorzewska-Cieslak B.: Analysis and assessment of the risk of lack of water supply using the EPANET program. Environmental Engineering IV - Proceedings of the Conference on Environmental Engineering IV, 2013.
2. Janczak J., Nowak A.: Bezpieczeństwo informacyjne. Wybrane problemy. Wydawnictwo: Akademia Obrony Narodowej, Warszawa 2013.
3. Jóźwiak I., Laskowski W. Szleszyński A.: Wykorzystanie drzewa użyteczności w procesie planowania i wdrożenia systemu bezpieczeństwa informacji. Journal of KONBiN, 2,3(14,15) 2010.
4. Liderman K.: Analiza ryzyka dla potrzeb bezpieczeństwa teleinformatycznego. Biuletyn Instytutu Automatyki i Robotyki, 16/2001.
5. Liderman K.: Bezpieczeństwo teleinformatyczne. Wydawnictwo Instytutu Automatyki i Robotyki Wojskowej Akademii Technicznej, Warszawa 2001.

6. Piegdoń I., Tchórzewska-Cieślak B.: Methods of visualizing the risk of lack of water supply. Safety and Reliability: Methodology and Applications - Proceedings of the European Safety and Reliability Conference, ESREL 2014.
7. Rak J.: Podstawy bezpieczeństwa systemów zaopatrzenia w wodę. Wydawnictwo PAN - Komitet Inżynierii Środowiska t. 28, Lublin 2005.
8. Rak J., Tchórzewska-Cieślak B.: Metody analizy i oceny ryzyka w systemie zaopatrzenia w wodę. Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2005.
9. Śliwiński M.: Bezpieczeństwo funkcjonalne i ochrona informacji w obiektach i systemach infrastruktury krytycznej. Seria monografie nr 171. Wydawnictwo Politechniki Gdańskiej, Gdańsk 2018.
10. Tchórzewska-Cieślak B., Piegdoń I.: Metoda identyfikacji ryzyka awarii sieci wodociągowych. Wydawnictwo Instytutu Technicznego Wojsk Lotniczych, Journal of KONBiN, z.1 (37) 2016, DOI 10.1515/jok-2016-0004.
11. Tchórzewska-Cieślak B., Rak J.: Bezpieczeństwo informatyczne firmy wodociągowej. Ośrodek Informacji „Technika instalacyjna w budownictwie". Instal, z. 12, 57-60, 2007.
12. Żuber M.: Infrastruktura krytyczna państwa jako obszar potencjalnego oddziaływania terrorystycznego. Rocznik Bezpieczeństwa Międzynarodowego, 8/2014, 178-197.
13. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 z późniejszymi zmianami).
14. https://www.cyberdefence24.pl/fbi-wszczelo-dochodzenie-ws-cyberataku-na-wodociagi-w-karolinie-pln.