Analiza ryzyka na potrzeby bezpieczeństwa informacyjnego według zaleceń normy PN-ISO/IEC 27005

Krzysztof LIDERMAN

Instytut Teleinformatyki i Cyberbezpieczeństwa, Wydział Cybernetyki, WAT,
ul. gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
krzysztof.liderman@wat.edu.pl

STRESZCZENIE: W artykule przedstawiono podstawy formalne oszacowania ryzyka IT metodą jakościową zgodną z wytycznymi zawartymi w normie PN-ISO/IEC 27005:2014-01. Ryzykiem IT nazywa się ryzyko związane z realizacją zagrożeń powodujących szkody w systemach teleinformatycznych i przetwarzanych w nich zasobach informacyjnych.

SŁOWA KLUCZOWE: bezpieczeństwo informacyjne, norma PN-ISO/IEC 27005, oszacowanie ryzyka IT

Ekspert „od ryzyka”:
osoba, która wykonuje precyzyjne zgadywanie na podstawie niewiarygodnych danych dostarczonych przez osoby o wątpliwej wiedzy.

definicja „z Internetu”

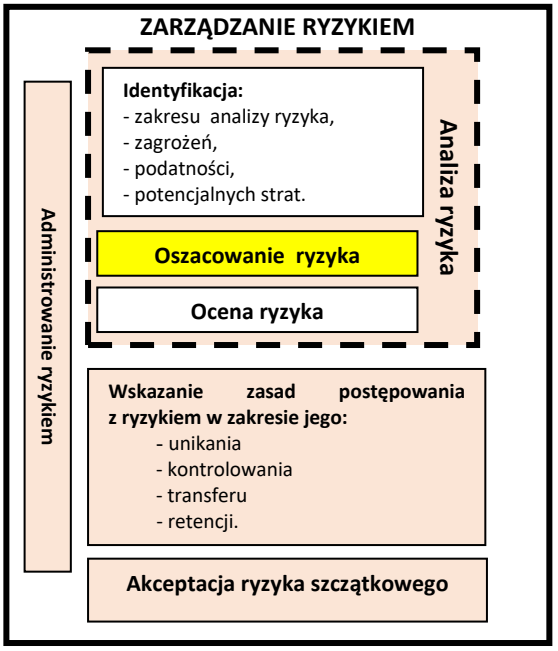
1. Wprowadzenie

Zarządzanie ryzykiem jest to systematyczne stosowanie polityki, procedur i praktyki zarządzania do zadań ustalania kontekstu ryzyka, jego identyfikowania, analizowania, wyznaczania, postępowania z ryzykiem oraz monitorowania i komunikowania ryzyka[1]. Podstawowe elementy tego procesu można przedstawić w formie graficznej jak na rys. 1. Żeby spełnić formalne wymagania

[1] Definicja za PN-IEC 62198 [3].

definicji zarządzania, jakość realizacji wymienionych w niej zadań powinna być mierzalna, a cały proces powinien układać się w cykl Deminga.

Pierwszym podstawowym elementem procesu zarządzania ryzykiem jest (pod)proces analizy ryzyka. Kluczowym zadaniem tego podprocesu jest wyznaczanie wartości ryzyka i to zagadnienie jest opisane w tym artykule. Opis jest skonkretyzowany na ryzyko IT, gdzie ryzykiem IT nazywa się ryzyko związane z realizacją zagrożeń powodujących szkody w systemach teleinformatycznych i przetwarzanych w nich zasobach informacyjnych.



Rys. 1. Podstawowe elementy zarządzania ryzykiem

Obecnie nie tylko w Polsce, ale i na świecie, w zakresie analizy ryzyka IT zaleca się przeprowadzanie jej zgodnie z wytycznymi normy ISO/IEC 27005. Na przykład w Polsce wykonywanie analizy ryzyka według wytycznych normy PN-ISO/IEC 27005 dla systemów IT eksploatowanych w podmiotach administracji publicznej narzuca rozporządzenie: *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*[2], w którym okresową analizę ryzyka nakazuje punkt 3 ustępu 2 paragrafu 20:

[2] *Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów*

§20.1. Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

2. Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań:

(…)

3) **przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji** oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.

Natomiast w ustępie 3 ww. paragrafu stwierdza się:

3. Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym:

1) PN-ISO/IEC 17799 – w odniesieniu do ustanawiania zabezpieczeń;

2) **PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem**;

3) PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

W proces zarządzania ryzykiem są zaangażowane role, których nazwy są zwykle podawane w literaturze przedmiotu i praktyce korporacyjnej w postaci anglojęzycznych akronimów:

- CISO (ang. *Chief Information Security Officer*) – rola do nadzoru i kontroli realizacji przyjętych w {Podmiot}[3] zasad bezpieczeństwa oraz do podejmowania decyzji w sprawach określonych zapisami Polityki Bezpieczeństwa Informacji.

publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych; Dz. U. 2012 poz. 526;
(źródło: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20120000526).

[3] Dalej w artykule jako ogólną nazwę organizacji, dla której jest przeprowadzana analiza ryzyka, przyjęto słowo „Podmiot", ujęte w nawiasy klamrowe. W przypadku konkretyzacji zapisów metodyki ALR-27005, w to miejsce należy wpisać nazwę organizacji (np. Wojskowa Akademia Techniczna) bądź jej symbol (np. WAT).

- CRO (ang. *Chief Risk Officer*) – rola uprawniająca do akceptacji ryzyka.
- CTO (ang. *Chief Technical Officer*) – rola właściciela ryzyka IT.

W dalszej części artykułu jest przedstawiony zarys propozycji czteroetapowej metodyki analizy ryzyka IT, o nazwie ARL-27005, w której wykorzystuje się jakościową metodę oszacowania wartości ryzyka w sposób zalecany w normie PN-ISO/IEC 27005:2014[4]. W metodyce określono czynności analizy, wskazano role odpowiedzialne za wykonanie danych czynności, zaproponowano wzorce zapisu wyników czynności.

Przyjęto, że każde zagrożenie można przypisać do jednej z trzech klas:

- „Siły wyższe" − oznaczane dalej symbolem **SW**. Należą do nich wszystkie zdarzenia, na które uprawniony podmiot − dysponent lub właściciel systemu teleinformatycznego albo zasobu informacyjnego, nie ma wpływu. Do zdarzeń takich należą katastrofy naturalne, promieniowanie kosmiczne, emisja ujawniająca itp.
- Celowe działanie wrogiego podmiotu − oznaczane dalej symbolem **CE**. Wrogi podmiot może być indywidualny (typu „samotny haker") lub grupowy (np. grupa przestępcza typu APT).
- Błędne działanie uprawnionego podmiotu − oznaczane dalej symbolem **BŁ**. Uprawnionym podmiotem jest zwykle pracownik konkretnej organizacji {Podmiot}.

2. Metodyka ARL-27005[5]

ETAP I: IDENTYFIKACJE

1) Zidentyfikować (odpowiedzialny – CTO):
   - zasoby poddawane analizie,
   - procesy poddawane analizie,

[4] W analizie ryzyka IT powinny być wykorzystane, w razie potrzeby, informacje z Rejestru Ryzyka {Podmiot}, a wyniki analizy powinny być w tym Rejestrze zapisane.

[5] Metodyka została przygotowana na podstawie zapisów normy PN-ISO/IEC 27005:2014. Norma ta została przez Polski Komitet Normalizacyjny (PKN) wycofana 12.10.2021. Najnowsza oryginalna wersja tej normy to ISO/IEC 27005:2022 *Information security, cybersecurity and privacy protection - Guidance on managing information security risks*, wprowadzona 25.10.2022 r. Zastąpiła ona wydanie z roku 2018. W chwili pisania tego artykułu nie są znane zamierzenia PKN w sprawie wydania normy polskiej. Warto zauważyć, że Narodowe Standardy Cyberbezpieczeństwa za podstawę w dziedzinie zarządzania ryzykiem mają standardy NIST (NSC-800-30 wer.1.0, NSC-800-37 wer.1.0, NSC-800-39 wer.1.0; dostęp 05.11.2022) a nie ISO/IEC.

- usługi poddawane analizie.

Wynikiem identyfikacji powinny być wstępnie wypełnione tabele 1-3.

2) Wstępnie zidentyfikować (odpowiedzialny – CTO) zagrożenia[6] istotne dla działalności biznesowej Podmiotu. Wynikiem identyfikacji powinna być wstępnie wypełniona tabela 4.
3) Metodą „burzy mózgów" (patrz np. [1] rozdz. 3.4.3) uzupełnić tabele 1-4.

ETAPII: SZACOWANIE RYZYKA

Wykonać procedurę opisaną w rozdziale 3.

ETAP III: OCENA RYZYKA

Uszeregować otrzymane wartości zmiennych $RYZYKO_{dzjpz}$ według wielkości. Analogicznie, w razie potrzeby, uszeregować wartości zmiennych $RYZYKO_{dpjpz}$ dla procesów. Czynności wykonywane w tym punkcie składają się na **proces oceny ryzyka**.

Tab. 1. Wzorzec arkusza opisu zasobu (przykład)

ARKUSZ nr ……. OPISU ZASOBU	
Typ zasobu: [infrastrukturalny, teleinformatyczny, informacyjny, systemu ochrony]	
Identyfikator zasobu: [symbol identyfikacyjny]	
Opis zasobu:	[krótki opis zasobu]
Umiejscowienie zasobu:	[wskazanie fizycznej lokalizacji zasobu; wskazanie numeru schematu, na którym jest zaznaczony]
Właściciel zasobu:	[dane właściciela zasobu: stanowisko, telefon]
Możliwe (szacowane) straty w przypadku realizacji zagrożenia dla:	Poufności: [np. kwota w określonej walucie lub opisowo] Integralności: [np. kwota w określonej walucie lub opisowo] Dostępności: [np. kwota w określonej walucie] Rozliczalności: [np. kwota w określonej walucie]
Inne dane w zależności od rodzaju zasobu:	np. dla zasobu typu teleinformatycznego (komputer): jaki producent, jaki dostawca, jaki okres eksploatacji, gdzie pliki konfiguracyjne itp.

[6] Należy rozróżniać zagrożenie $\delta_k \in \Delta$ od sposobu jego realizacji $\delta|d_n \in D$. Szczegóły – patrz rozdz. 3.1.

Tab. 2. Wzorzec arkusza opisu procesu (przykład)

ARKUSZ nr ……. OPISU PROCESU	
Typ procesu: [krytyczny, kluczowy, wspomagający]	
Identyfikator procesu: [symbol identyfikacyjny]	
Opis procesu:	[krótki opis procesu]
System IT realizujący proces:	[wskazanie systemu IT, w którym proces jest realizowany i wykorzystywane zasoby]
Właściciel procesu:	[dane właściciela procesu: stanowisko, telefon]
Możliwe (szacowane) straty w przypadku realizacji zagrożenia dla:	Poufności: [np. kwota w określonej walucie lub opisowo] Integralności: [np. kwota w określonej walucie lub opisowo] Dostępności: [np. kwota w określonej walucie] Rozliczalności: [np. kwota w określonej walucie]
Inne dane w zależności od rodzaju procesu:	np. powiązanie z innymi procesami itp.

Tab. 3. Wzorzec arkusza opisu usługi (przykład)

ARKUSZ nr ……. OPISU USŁUGI	
Typ usługi: [wewnętrzna, zewnętrzna]	
Identyfikator usługi: [symbol identyfikacyjny]	
Opis usługi:	[krótki opis usługi]
Klient/wykonawca usługi:	[wskazanie nazw i kontaktów]
Dane o umowie:	[dane nt. umowy na świadczenie usługi: symbole identyfikacyjne, gdzie jest przechowywana, okres obowiązywania]
Możliwe (szacowane) straty w przypadku realizacji zagrożenia dla:	Poufności: [np. kwota w określonej walucie lub opisowo] Integralności: [np. kwota w określonej walucie lub opisowo] Dostępności: [np. kwota w określonej walucie] Rozliczalności: [np. kwota w określonej walucie]
Inne dane w zależności od rodzaju usługi:	np. powiązanie z innymi usługami, wykorzystywane procesy i zasoby itp.

Tab. 4. Wzorzec arkusza opisu zagrożenia i sposobu jego realizacji (przykład)

ARKUSZ nr ……. OPISU ZAGROŻENIA	
Identyfikator zagrożenia: [symbol zagrożenia: SW – „siły wyższe”; CE – działania celowe; BŁ – działania błędne]	
Zagrożenie:	[jednozdaniowa nazwa opisowa zagrożenia]
Scenariusz realizacji zagrożenia dla:	[**Poufności:** kilkuzdaniowy opis słowny lub w postaci schematu blokowego lub NIE DOTYCZY] [**Integralności:** kilkuzdaniowy opis słowny lub w postaci schematu blokowego lub NIE DOTYCZY] [**Dostępności:** kilkuzdaniowy opis słowny lub w postaci schematu blokowego lub NIE DOTYCZY] [**Rozliczalności:** kilkuzdaniowy opis słowny lub w postaci schematu blokowego lub NIE DOTYCZY]
Zasoby, na które zagrożenie może mieć wpływ i szkody:	[lista: zasób/szkoda/właściciel zasobu]
Procesy, na które zagrożenie może mieć wpływ i szkody:	[lista: proces/szkoda/właściciel procesu]
Usługi, na które zagrożenie może mieć wpływ i szkody:	[lista: usługa/szkoda/symbole identyfikacyjne umowy]
Potencjał zagrożenia:	[kilkuzdaniowy opis słowny]

ETAP IV: AKCEPTACJI RYZYKA

1) Ustalić, jakie wartości ryzyka są akceptowane w {Podmiot}. Ponieważ na wartość ryzyka składają się dwa elementy – prawdopodobieństwo (możliwość) zajścia incydentu (MZI) oraz wielkość szkód (ST) – **należy odnieść się do obu tych elementów**[7], inaczej wskazanie wartości ryzyka będzie nieprecyzyjne. Przyjmuje się, że wartości ryzyka równe lub poniżej wartości akceptowalnych oznaczają **ryzyko akceptowalne**, wobec którego (w zasadzie) nie podejmuje się działań minimalizujących.

[7] Na przykład (tabela 7): akceptujemy tylko zdarzenia (incydenty), których możliwość zajścia jest co najwyżej na poziomie „średni”, a ich skutki nie mogą być większe niż „niskie”. Taka decyzja wskazuje konkretne ryzyko o wartości 2. Widać, że jest jeszcze jedno ryzyko o wartości 2, ale nie spełnia warunków akceptacji – możliwość zajścia jest na poziomie „niski”, ale skutki mają wartość „średnie”.

2) Uzyskać od CRO zatwierdzenie ryzyka akceptowalnego.
3) Dla ryzyka o wartościach **nieakceptowanych** wykonać czynności z kolejnego etapu zarządzania ryzykiem, tj. etapu minimalizowania ryzyka (poza niniejszą metodyką).

3. Procedura szacowania ryzyka IT

3.1. Założenia

- dany jest zbiór zagrożeń Δ takich, że $\delta_k \in \Delta$, gdzie δ_k jest konkretnym, zidentyfikowanym zagrożeniem dotyczącym zasobu $z_i \in Z$ (lub, analogicznie, procesu $p_j \in P$), podlegającemu analizie ryzyka;
- dany jest zasób $z_i \in Z$, gdzie Z to zbiór zasobów oraz proces $p_j \in P$, podlegające analizie ryzyka;
- z_i może mieć podatności $pz_{zi} \in PZ_z$, gdzie PZ_z to podzbiór podatności zasobów należących do zbioru Z. Podobnie, proces p_j może mieć podatności $pz_{pi} \in PZ_p$, gdzie PZ_p to podzbiór podatności procesów należących do zbioru P;
- podatność może być wykorzystana przez zagrożenie $\delta | d_n \in D$, gdzie D to zbiór zidentyfikowanych sposobów d_n realizacji zagrożeń mogących oddziaływać na zasoby Z lub procesy P;
- analiza ryzyka jest przeprowadzona w wariancie zasobowym lub procesowym (w zależności od konkretnych potrzeb);
- w oszacowaniach wykorzystuje się oceny opisowe (czyli analiza ryzyka jest przeprowadzana tzw. metodą jakościową).

Należy określić:

1) Jednolite oceny symboliczne[8] dla cech (zmiennych): zagrożeń δ_k i sposobów ich realizacji $d_n \in D$, podatności $p_j \in P$, szkód i strat oraz ryzyka. Te cechy to:
   - możliwość realizacji zagrożenia, oznaczona dalej jako MRZ,
   - stopień podatności, oznaczony dalej jako PZ,
   - możliwość zajścia incydentu (tj. poniesienia szkód spowodowanych realizacją określonego zagrożenia), oznaczona dalej jako MZI,
   - wielkość szkód, oznaczona dalej jako ST,
   - wielkość ryzyka, oznaczona dalej jako RYZYKO.

[8] Tak będą nazywane miary w szacowaniach jakościowych w odróżnieniu od miar liczbowych (miar prawdopodobieństwa, tj. liczb z przedziału [0,1]) w przypadku oszacowań ilościowych. Miary symboliczne mogą być opisowe (np. wysoki, średni, niski) lub w postaci liczb (ilości punktów, zakresów przedziałów itd.).

2) Sposób wyznaczania ocen.

Przyjmuje się następujący system K przypisywania ocen opisowych wybranym cechom:

$$K = \langle CECHA, OCENA, PROCEDURA \rangle$$

gdzie:

– CECHA – zbiór cech (zmiennych) {MRZ, PZ, MZI, ST, RYZYKO}.

– OCENA – zbiór ocen opisowych {K, W, S, N} gdzie[9]:

K – prawdopodobieństwo (możliwość), stopień lub szkoda KRYTYCZNA,

W – prawdopodobieństwo (możliwość), stopień lub szkoda WYSOKA,

S – prawdopodobieństwo (możliwość), stopień lub szkoda ŚREDNIA,

N – prawdopodobieństwo (możliwość), stopień lub szkoda NISKA.

Ten zbiór ocen opisowych jest odwzorowywany na przyjęty arbitralnie czteroelementowy zbiór liczb naturalnych:

$$\{K, W, S, N\} \rightarrow \{4, 3, 2, 1\} \quad (1)$$

co ilustruje tabela 5.

Tab. 5. Odwzorowanie ocen opisowych w czteroelementowy zbiór liczb

Prawdopodobieństwo realizacji zagrożenia (MRZ)	**Podatność (PZ)**	**Szkody (ST)**	**Wartość liczbowa**	
Niskie	Niska	Niskie	**1**	
Średnie	Średnia	Średnie	**2**	
Wysokie	Wysoka	Wysokie	**3**	
Prawie pewne	Krytyczna	Krytyczne	**4**	

– PROCEDURA – podaje sposób przypisania wartości ocen opisowych ze zbioru OCENA cechom ze zbioru CECHA (np. decyzją ekspertów w ramach sesji „burzy mózgów” – patrz np. [1] rozdz. 3.4.3).

[9] Ten zbiór ocen został w tym artykule przyjęty arbitralnie, w celu zachowania zgodności z propozycjami zawartymi w normie PN-ISO/IEC 27005. W ogólnym przypadku zbiór ten może być dowolny zarówno co do liczności, jak i nazw.

3.2. Podstawowe czynności formalne procesu szacowania ryzyka

W celu oszacowania ryzyka powstania strat określonej wielkości, **dla zasobu** $z_i \in Z$ (gdzie Z to zbiór zasobów podlegających analizie ryzyka), **konkretnego zagrożenia δ** oraz **sposobu jego realizacji** $d_n \in D$ i **podatności** $pz_j \in PZ_z$, należy[10]:

1) Dla $d_n \in D$ oszacować prawdopodobieństwo (możliwość) MRZ realizacji zagrożenia δ_k „jako takiego”[11], tzn. podać wartość: ocena(MRZ_d). Na przykład, gdy oceniono prawdopodobieństwo realizacji zagrożenia δ_k w sposób d_n jako „wysoką”, otrzymuje się: ocena(MRZ_d)=W.
2) Oszacować stopień podatności $pz_{zj} \in PZ_z$ zasobu $z_i \in Z$, która to podatność może być wykorzystana przez zagrożenie (jedno lub więcej), tzn. podać wartość: ocena(PZ_z).
3) Wykonać odwzorowanie według formuły (1):

$$\text{ocena}(MRZ_d) \rightarrow \{4, 3, 2, 1\}$$
$$\text{ocena}(PZ_z) \rightarrow \{4, 3, 2, 1\}$$

4) Oszacować według formuły (2) prawdopodobieństwo (możliwość) MZI_{dpz} zajścia incydentu (dokładniej: zajścia zdarzenia takiego, że zagrożenie δ_k w sposób $d_n \in D$ wykorzysta podatność $pz_{zj} \in PZ_z$ do spowodowania szkody):

$$\text{ocena}(MZI_{dpz}) = \text{ocena}(MRZ_d) \times \text{ocena}(PZ_z) \quad (2)$$

gdzie × oznacza arytmetyczną operację mnożenia.

5) Oszacować wielkość szkód $st_{zj} \in ST$ dla zasobu $z_i \in Z$, powstałych w wyniku realizacji zagrożenia δ_k w sposób d_n; tzn. podać wartość: ocena(ST_{dzj}).
6) Wykonać odwzorowanie według formuły (1):

$$\text{ocena}(ST_{dzj}) \rightarrow \{4, 3, 2, 1\}$$

7) Oszacować według formuły (3) ryzyko; dokładniej: zajścia zdarzenia takiego, że zagrożenie δ_k wykorzysta w sposób $d_n \in D$ podatność $p_{zj} \in PZ_z$ do

[10] Dalej proces szacowania ryzyka będzie pokazany tylko dla zasobu, ponieważ dla procesów ze zbioru P wykonuje się go analogicznie.

[11] Na tym etapie szacujemy „potencjalność” zagrożenia. Np. oceniając możliwość kradzieży sprzętu komputerowego z siedziby organizacji nie bierzemy pod uwagę krat, zamków, systemów alarmowych itp. w które wyposażony jest budynek (to wpływa na podatność na kradzież, co rozpatrywane jest w kolejnym etapie) tylko bierzemy pod uwagę to, że budynek ten znajduje się w dzielnicy w której mieszka dużo złodziei (podobno „prawdziwi” złodzieje na swoim terenie nie kradną, ale czasy się zmieniają).

spowodowania szkody, a wielkość poniesionych strat będzie miała wartość: ocena(ST_{dzj}):

$$\text{ocena}(RYZYKO_{dzjpz}) = \text{ocena}(MZI_{dpz}) \times \text{ocena}(ST_{dzj}) \qquad (3)$$

Zbiory wartości liczbowych ocen możliwych do uzyskania przez zmienne MZI oraz RYZYKO ilustrują tabele 6 i 7.

Używając przyjętych ocen opisowych, można wskazać zmienną o jakiej wartości liczbowej wypadkowej przypisać do jakiej oceny opisowej ze zbioru {K, W, S, N}. **Założenie:** oceną opisową (wypadkową) jest ocena wyższa z dwóch składowych, czyli ma zastosowanie formuła max{OCENA}.

W tabelach 6 i 7 uzyskane wyniki zastosowania formuły max{OCENA} są podane w nawiasach okrągłych. W tabeli 7 obok ocen liczbowych wypadkowych podane są zbiory ocen opisowych {MRZ, PZ} sprzyjających zajściu zdarzenia (w tym przypadku − incydentu) o konkretnej wartości liczbowej. Informacja ta jest istotna, ponieważ wskazuje, po identyfikacji konkretnych wartości MRZ i PZ, jakie istnieją możliwości minimalizowania ryzyka, czyli jakie są możliwości oddziaływania na składowe ryzyka.

Stosując podaną zasadę do zbioru {MZI, ST}, można określić przyporządkowanie uzyskanych wartości ryzyka do zbioru ocen opisowych (patrz tabela 6 − wartości opisowe są podane w nawiasach okrągłych).

Uwaga: podanych wartości ocen opisowych ryzyka **nie należy utożsamiać z ryzykiem akceptowalnym lub nieakceptowanym**. To, jakie ryzyko o jakiej wartości jest ryzykiem akceptowalnym, jest decyzją właściciela ryzyka lub osoby uprawnionej do takiej decyzji. W {Podmiot} osobą uprawnioną jest osoba pełniąca rolę CRO; progi akceptacji („apetyt na ryzyko") określa Zarząd {Podmiot}.

Tab. 6. Wartości ocen dla MZI (szare pole)

PZ \ MRZ	1	2	3	4
1	1 (N)	2 (S)	3 (W)	4 (K)
2	2 (S)	4 (S)	6 (W)	8 (K)
3	3 (W)	6 (W)	9 (W)	12 (K)
4	4 (K)	8 (K)	12 (K)	16 (K)

Tab. 7. Wartości ocen dla RYZYKA (szare pole)[12]

ST / MZI	1	2	3	4
1	**1** (N) {N, N}	**2** (S) {N, S}	**3** (W) {N, W}	**4** (K) {N, K}
2	**2** (S) {S, N} {N, S} {S, S}	**4** (S) {S, N} {N, S} {S, S}	**6** (W) {S, N} {N, S} {S, S}	**8** (K) {S, N} {N, S} {S, S}
3	**3** (W) {W, N} {N, W} {S, W} {W, S} {W, W}	**6** (W) {W, N} {N, W} {S, W} {W, S} {W, W}	**9** (W) {W, N} {N, W} {S, W} {W, S} {W, W}	**12** (K) {W, N} {N, W} {S, W} {W, S} {W,W}
4	**4** (K) {K, N} {N, K} {K, S} {S, K} {W, K} {K, W} {K, K}	**8** (K) {K, N} {N, K} {K, S} {S, K} {W, K} {K, W} {K, K}	**12** (K) {K, N} {N, K} {K, S} {S, K} {W, K} {K, W} {K, K}	**16** (K) {K, N} {N, K} {K, S} {S, K} {W, K} {K, W} {K, K}

8) Czynności 1-7 powtórzyć:
   a) dla każdego zidentyfikowanego sposobu realizacji d_n zagrożenia δ_k na zasobie z_i;
   b) czynność a) powtarzać dla kolejnych zagrożeń ze zbioru Δ i sposobów realizacji ze zbioru D, aż do wyczerpania zagrożeń i sposobów ich realizacji na zasobie z_i;
   c) dla kolejnego zasobu ze zbioru Z wykonać czynności z punktu 8a i b aż do wyczerpania zbioru Z;
   d) w razie potrzeby wykonać analogiczne czynności dla zbioru procesów P poddawanych analizie ryzyka.
9) Wynikiem realizacji czynności z punktu 8 powinny być wypełnione tabele 8-11:

[12] W szarych polach, w nawiasach okrągłych, podana jest ocena opisowa wartości ryzyka. W nawiasach klamrowych są podane zdarzenia ({MRZ, PZ} – patrz tabela 6) sprzyjające zaistnieniu ryzyka o tej wartości.

Tab. 8. Przypisania wartości: zagrożeń, podatności, możliwości, strat, ryzyka dla atrybutu POUFNOŚĆ dla zasobu z_i

ZAGROŻENIE [MRZ]	**PODATNOŚĆ** [PZ]	**MOŻLIWOŚĆ** [MZI] = [MRZ] × [PZ]	**STRATY** [ST]	**RYZYKO$_{PF}$** [MZI] × [ST]
- 1 -	**- 2 -**	**- 3 -**	**- 4 -**	**- 5 -**
{SW_{PF}, CE_{PF}, $BŁ_{PF}$}	PZ_{SWPF} ( ) PZ_{CEPF} ( ) $PZ_{BŁPF}$ ( )			

Opis podatności:

$PZ1_{SWPF}$ ( )
$PZ2_{SWPF}$ ( )
...
$PZ1_{CEPF}$ ( )
$PZ2_{CEPF}$ ( )
…
$PZ1_{BŁPF}$ ( )
$PZ2_{BŁPF}$ ( )
...

Uwaga: podatność całkowitą PZ_{XXPF} na konkretną realizację zagrożenia ustala się, analizując zidentyfikowane podatności cząstkowe (opisane pod tabelą jako: $PZ1_{SWPF}$ ( ), $PZ2_{SWPF}$ ( ), …).

Tab. 9. Przypisania wartości: zagrożeń, podatności, możliwości, strat, ryzyka dla atrybutu INTEGRALNOŚĆ dla zasobu z_i

ZAGROŻENIE [MRZ]	**PODATNOŚĆ** [PZ]	**MOŻLIWOŚĆ** [MZI] = [MRZ]× [PZ]	**STRATY** [ST]	**RYZYKO$_I$** [MZI]× [ST]
- 1 -	**- 2 -**	**- 3 -**	**- 4 -**	**- 5 -**
{SW_I, CE_I, $BŁ_I$}	Analogicznie jak w tabeli 8			

Opis podatności:

$PZ1_{SWI}$ ( )
$PZ2_{SWI}$ ( )
...
$PZ1_{CEI}$ ( )
$PZ2_{CEI}$ ( )

…

$PZ1_{BŁI}$ ( )

$PZ2_{BŁI}$ ( )

...

Tab. 10. Przypisania wartości: zagrożeń, podatności, możliwości, strat, ryzyka dla atrybutu DOSTĘPNOŚĆ dla zasobu z_i

ZAGROŻENIE [MRZ]	**PODATNOŚĆ** [PZ]	**MOŻLIWOŚĆ** [MZI] = [MRZ] × [PZ]	**STRATY** [ST]	**RYZYKO$_D$** [MZI]× [ST]
- 1 -	**- 2 -**	**- 3 -**	**- 4 -**	**- 5 -**
{SW_D, CE_D, $BŁ_D$}	Analogicznie jak w tabeli 8			

Opis podatności:

$PZ1_{SWD}$ ( )

$PZ2_{SWD}$ ( )

...

$PZ1_{CED}$ ( )

$PZ2_{CED}$ ( )

…

$PZ1_{BŁD}$ ( )

$PZ2_{BŁD}$ ( )

...

Tab. 11. Przypisania wartości: zagrożeń, podatności, możliwości, strat, ryzyka dla atrybutu ROZLICZALNOŚĆ dla zasobu z_i

ZAGROŻENIE [MRZ]	**PODATNOŚĆ** [PZ]	**MOŻLIWOŚĆ** [MZI] = [MRZ] × [PZ]	**STRATY** [ST]	**RYZYKO$_R$** [MZI]× [ST]
- 1 -	**- 2 -**	**- 3 -**	**- 4 -**	**- 5 -**
{SW_R, CE_R, $BŁ_R$}	Analogicznie jak w tabeli 8			

Opis podatności:

$PZ1_{SWR}$ ( )

$PZ2_{SWR}$ ( )

...

$PZ1_{CER}$ ( )

$PZ2_{CER}$ ( )

…

$PZ1_{BŁR}$ ( )

$PZ2_{BŁR}$ ( )

...

Uwaga! Dla procesów i usług należy utworzyć i wypełnić tabele analogiczne jak dla zasobu (tj. na wzór tabel 8-11).

4. Podsumowanie

W artykule przedstawiono sposób szacowania wartości ryzyka zgodny z zaleceniami normy PN-ISO/IEC 27005. W normie zaleca się użycie metody jakościowej[13] z wykorzystaniem wartości liczbowych. W praktyce oceny do analizy ryzyka tą metoda pozyskuje się zwykle od ekspertów, którzy swoje opinie wyrażają jednak w sposób opisowy słowny, a nie liczbowy, posługując się takimi stwierdzeniami, jak: wysoki, krytyczny, możliwy, nieprawdopodobny, niski itp. Metoda zamieszczona w normie zakłada przekształcenie takich ocen na liczby i dalsze działania na tak przekształconych ocenach opisowych.

Zdaniem piszącego te słowa, przypomina to sięganie prawą ręką do lewej kieszeni spodni − prościej byłoby działać bezpośrednio na słownych ocenach opisowych przedstawionych przez ekspertów. Przykłady takiej metody są zamieszczone w rozdz. 3 w pracy [1] i w artykule [2].

Przykłady zastosowania przedstawionej w tym opracowaniu metodyki zostaną zaprezentowane w kolejnym artykule.

Literatura

[1] LIDERMAN K., *Bezpieczeństwo informacyjne. Nowe wyzwania*, PWN Warszawa, 2017.

[2] LIDERMAN K., *Risk of undesired changes to significant information quality criteria*, Teleinformatics Review, Nr 3-4(47), WAT, Warszawa 2019, pp. 31-55.

[3] PN-IEC 62198:2005, *Zarządzanie ryzykiem przedsięwzięcia – Wytyczne stosowania*.

[4] PN-ISO/IEC 27005:2014, *Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji*.

[13] Taka jest ogólnie przyjęta nazwa tej metody, chociaż trafniejsza byłaby nazwa „metoda ocen opisowych”.

[5] *Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*, Dz. U. 2012 Nr 0 poz. 526.

Risk analysis for information security in accordance with PN-ISO/IEC 27005 recommendation

ABSTRACT: The paper considers the problem of IT risk evaluation with the use of a quality method based on the PN-ISO/IEC 27005:2014-01 recommendation. It addresses risks associated with the realization of threats that result in damages to telecommunications systems and processed information resources.

KEYWORDS: information security, PN-ISO/IEC 27005, IT risk evaluation

Praca wpłynęła do redakcji: 23.11.2022 r.