Oszacowania ryzyka IT – studium przypadków

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 na trzech przykładach sposób oszacowania ryzyka IT. Ryzykiem IT nazywa się ryzyko związane z realizacją zagrożeń powodujących szkody w systemach teleinformatycznych i przetwarzanych w nich zasobach informacyjnych. Prezentowane w przykładach oszacowanie ryzyka jest wykonane metodą jakościową, z użyciem czterech ocen opisowych „przekładanych" na wartości liczbowe zgodnie z wytycznymi zawartymi w normie PN-ISO/IEC 27005:2014-01.

SŁOWA KLUCZOWE: bezpieczeństwo informacyjne, realizacja zagrożenia, oszacowanie ryzyka IT

1. Wprowadzenie

Zagrożenia[1] dla systemów teleinformatycznych (IT) oraz zasobów informacyjnych w nich przetwarzanych, można sklasyfikować następująco:

1. **„Siły wyższe"** – zdarzenie zewnętrzne, niemożliwe (lub prawie niemożliwe) do przewidzenia, którego skutkom nie można zapobiec[2].
2. **Działania ludzi:**

[1] Od zagrożenia należy odróżniać sposób jego realizacji, które to rozróżnienie będzie konsekwentnie stosowane w dalszej części artykułu.

[2] Do takich zdarzeń należą m.in. tzw. katastrofy naturalne (trzęsienia ziemi, powodzie itp.), zjawiska przyrodnicze, takie jak emisja ujawniająca oraz zjawiska polityczne, takie jak terroryzm.

2.1. Celowe (nieuprawnione[3] i przestępcze):
   - działania personelu, w tym podsłuchy różnego typu i kradzieże oraz zagubienia nosicieli informacji (sprzętu i dokumentów);
   - działania osób postronnych (klienci, „hakerzy"), w tym różnego typu podsłuchy i kradzieże nosicieli informacji (dokumentów i sprzętu);

2.2. Błędne[4].

Realizacja zagrożeń wpływa niekorzystnie na osiąganie celów biznesowych. COBIT-owe [4] praktyki z zakresu *governance* (EDM03.01: *Ocena, kierowanie, monitorowanie − Zapewnienie optymalizacji ryzyka − Zgodność IT z biznesowymi celami strategicznymi*) wskazują, że zarząd organizacji powinien określić swój „apetyt na ryzyko"[5] i poziom tolerancji ryzyka[6]. Czynniki, które zwiększają poziom ryzyka dla organizacji i jej systemów IT to wrażliwość i objętość przetwarzanych zbiorów danych, krytyczność świadczonych usług, liczba użytkowników, połączenia z siecią publiczną i korzystanie z usług innych podmiotów.

Ogólnie, krytyczność systemów IT jest zależna od wagi ciągłości świadczenia wspieranych procesów biznesowych i usług. Krytyczność systemu może być w praktyce oceniona przez oszacowanie strat finansowych, które mogą wystąpić jako rezultat jego przestoju. Podczas oceny krytyczności systemu jest ważne, aby zrozumieć i uwzględnić wpływ jego przestoju (np. w wyniku awarii) na działanie aplikacji pracujących w stowarzyszonych przepływach biznesowych.

W kolejnych rozdziałach niniejszego artykułu są zaprezentowane trzy przykłady szacowania ryzyka dla różnych zagrożeń i różnych sposobów ich realizacji. Do szacowania ryzyka wykorzystano metodykę opisaną w pracy [3], bazującą na zaleceniach normy PN-ISO/IEC 27005 [6]. W przykładach są wykorzystywane arkusze opisu zasobów oraz arkusze opisu zagrożenia i sposobu jego realizacji, których wzorce przedstawiono w postaci tabel 1 i 2. W przykładach, oprócz rozróżniania zagrożenia i sposobu jego realizacji, są konsekwentnie rozróżniane także szkody i straty.

[3] Działaniami nieuprawnionymi są nazywane takie działania celowe, niepożądane przez dysponenta systemu bądź zasobów danych, które mogą doprowadzić do powstania szkód, ale na które nie ma paragrafów w Kodeksie Karnym („nie wyczerpują ustawowych znamion przestępstwa").

[4] Przykład z 04.10.2021 r. – awaria Facebooka. Powodem awarii była błędna aktualizacja zewnętrznego protokołu trasowania BGP. Specjaliści od sieci Facebooka wprowadzali pewne zmiany w konfiguracji i przez pomyłkę doprowadzili do trwającej kilka godzin awarii.

[5] Czyli poziom ryzyka, który zarząd tej organizacji jest skłonny zaakceptować, aby osiągnąć założone cele biznesowe.

[6] Czyli okresowe, akceptowalne odchylenia od przyjętej wartości „apetytu na ryzyko".

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.

Tab. 2. 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]

2. Szacowania ryzyka IT – przypadek 1

KONTEKST:

W opolskiej firmie Płatnik sp. z o.o. na zlecenie Zarządu przeprowadzono szacowanie ryzyka IT. W tym celu przyjęto metodykę jak w pracy [3], uzupełnioną o przedstawione dalej arkusze opisu zasobu (-ów) i zagrożenia, które zostały wytworzone na podstawie zaproponowanych wzorców (tabela 1 i 2), podczas realizacji tej metodyki.

W tym przykładzie przyjmuje się, że jednym ze zdarzeń zidentyfikowanych w ramach „burzy mózgów", szkodliwych dla działalności biznesowej firmy Płatnik Sp. z o.o., jest zdarzenie:

ZD_25: Pożar w budynku firmy Płatnik sp. z o.o. przy ul. Moczarowej 3 w Opolu

Zarząd firmy Płatnik sp. z o.o. określił „apetyt na ryzyko" jak w tabeli 3.

Tab. 3. „Apetyt na ryzyko" – tabela ocen opisowych wielkości strat

Ocena opisowa wielkości STRAT	Interpretacja
Krytyczne	powyżej 800 tys. zł/rok
Wysokie	do 800 tys. zł/rok
Średnie	do 100 tys. zł/rok
Niskie	do 50 tys. zł/rok

Dalej została przedstawiona szczegółowa analiza dla zagrożenia klasy **SW**, realizującego się jako uderzenie pioruna w dach obiektu (zasobu infrastrukturalnego) o identyfikatorze [3/Moczarowa]. Przyjęto, że zdarzenie to nie wpływa na poufność i integralność zasobów informacyjnych. Schemat wykonanej analizy przedstawiony został na rysunku 1.

W celu otrzymania pełnej analizy (i ryzyka) dla zdarzenia:

ZD_25: Pożar w budynku firmy Płatnik sp. z o.o. przy ul. Moczarowej 3 w Opolu

należy przeprowadzić ją także dla:

- zagrożenia klasy **CE,** realizującego się jako podpalenie obiektu [3/Moczarowa] przez zewnętrzny wrogi podmiot;
- zagrożenia klasy **BŁ,** realizującego się jako zaprószenie ognia przez pracownika firmy Płatnik.

ZAGROŻENIE	SPOSÓB REALIZACJI	SKUTEK (INCYDENT)	SZKODA	STRATA	RYZYKO
SW	1(**N**) UDERZENIE PIORUNA $PZ1_{SW}$: brak instalacji odgromowej $PZ2_{SW}$: zła konserwacja instalacji odgromowej 2(**S**) PZn_{SW}:	**POŻAR**	SPALONY DACH MZI=MRZ×PZ= =1×2=2 **MZI_{SW} = S**	95 tys. zł. **2(S)**	2 ×2=**4** **RYZYKO=S**
CE	1(**N**) PODPALENIE $PZ1_{CE}$: źle wyszkolona ochrona $PZ2_{CE}$: brak nadzoru nad pracownikami ochrony 1(**N**) PZn_{CE}:		SPALONY BUDYNEK MZI=MRZ×PZ= =1×1=1 **MZI_{CE} = N**	10 mln. zł. **4(K)**	1×4=**4** **RYZYKO=K**
BŁ	1(**N**) ZAPRÓSZENIE OGNIA $PZ1_{BŁ}$: brak szkolenia p.poż. $PZ2_{BŁ}$: brak wyznaczonych stref dla palaczy 2(**S**) $PZn_{BŁ}$:...		SPALONY KOSZ NA ŚMIECI MZI=MRZ×PZ= =1×2=2 **$MZI_{BŁ}$=S**	200 zł. **1(N)**	2×1=**2** **RYZYKO=S**

Oznaczenia:

- MRZ, PZ, MZI, ST, RYZYKO, × – jak w pracy [3].
- Symbol typu 1(**N**) oznacza: wartość opisowa „Niska”, liczbowo „1”.

Uwaga: ze względów edycyjnych wyliczenia wartości MZI_{xy} zostały umieszczone w kolumnie SZKODY, chociaż formalnie powinny znajdować się w kolumnie SKUTEK (INCYDENT).

Rys. 1. Szacowanie ryzyka dla zdarzenia o skutku „Pożar”

ANALIZA:

ARKUSZ nr 25 OPISU ZASOBU	
Typ zasobu: [infrastrukturalny, ~~teleinformatyczny, informacyjny, systemu ochrony~~]	
Identyfikator zasobu: [3/Moczarowa]	
Opis zasobu:	Czterokondygnacyjny budynek wykonany w technologii „Lipsk”
Umiejscowienie zasobu:	Opole, ul. Moczarowa 3
Właściciel zasobu:	Firma Płatnik Sp. z o.o., tel. 77 261 84 85
Możliwe (szacowane) straty w przypadku realizacji zagrożenia dla:	Poufności: nie dotyczy Integralności: nie dotyczy Dostępności: do 12 mln zł Rozliczalności: nie dotyczy
Inne dane w zależności od rodzaju zasobu:	Budynek wybudowany w 1979 roku

ARKUSZ nr 25.1 OPISU ZAGROŻENIA	
Identyfikator zagrożenia: SW	
Zagrożenie:	Zjawisko atmosferyczne – burza z piorunami. Realizacja: piorun uderzający w dach obiektu [3/Moczarowa]
Scenariusz realizacji zagrożenia dla:	**Poufności:** NIE DOTYCZY **Integralności:** NIE DOTYCZY **Dostępności:** zależnie od stanu zabezpieczeń ppoż. oraz działania służb ochrony fizycznej obiektu i Straży Pożarnej może dojść: – tylko do uszkodzenia dachu budynku z powodu wznieconego przez piorun ognia oraz ograniczonych uszkodzeń infrastruktury teleinformatycznej w wyniku wody lanej przez Straż Pożarną (straty NISKIE); – uszkodzenia górnych pięter budynku z powodu wznieconego przez piorun ognia oraz ograniczonych uszkodzeń infrastruktury teleinformatycznej w wyniku wody lanej przez Straż Pożarną (straty ŚREDNIE); – wypalenia wszystkich pięter budynku z powodu wznieconego przez piorun ognia oraz zniszczenia

	infrastruktury teleinformatycznej w wyniku wody lanej przez Straż Pożarną (straty KRYTYCZNE); **Rozliczalności:** NIE DOTYCZY
Zasoby, na które zagrożenie może mieć wpływ i szkody:	[3/Moczarowa]/w skrajnym przypadku: całkowite spalenie budynku/xxx yyy *Zasoby powiązane: zasoby teleinformatyczne zlokalizowane w obiekcie (3/Moczarowa)*
Procesy, na które zagrożenie może mieć wpływ i szkody:	Wszystkie procesy biznesowe związane z zasobami teleinformatycznymi zlokalizowanymi w [3/Moczarowa]: *[lista: proces/szkoda/właściciel procesu]*
Usługi, na które zagrożenie może mieć wpływ i szkody:	Wszystkie, które są świadczone za pomocą zasobów teleinformatycznych zlokalizowanych w [3/Moczarowa]: *[lista: usługa/szkoda/symbole identyfikacyjne umowy]*
Potencjał zagrożenia:	Wysoki: w przypadku strat KRYTYCZNYCH i braku infrastruktury zapasowej może doprowadzić do bankructwa firmy z powodu strat wywołanych zdarzeniem i utraty klientów z powodu przerwania świadczenia usług

Analogicznie należy wypełnić arkusze opisu zagrożenia nr 25.2 i 25.3 dla zagrożeń z klasy CE i BŁ.

Na podstawie analizy danych historycznych z Rejestru Ryzyka prowadzonego od 10 lat w firmie Płatnik sp. z o.o. (nie znaleziono zapisu incydentu „pożar wywołany uderzeniem pioruna") oraz uzyskanych z Komendy Głównej Straży Pożarnej w Opolu danych za ostatnie 10 lat nt. zdarzenia „pożar wywołany uderzeniem pioruna w zabudowie miejskiej" stwierdzono, że zdarzenie takie należy do zdarzeń rzadkich i przypisano mu ocenę opisową NISKIE (liczbowo 1).

Tab. 4. Przypisania wartości: zagrożeń, podatności, możliwości, strat, ryzyka dla atrybutu DOSTĘPNOŚĆ dla zasobu (3/Moczarowa)

ZAGROŻENIE [MRZ]	**PODATNOŚĆ** [PZ]	**MOŻLIWOŚĆ** [MZI] = [MRZ] × [PZ]	**STRATY** [ST]	**RYZYKO$_D$** [MZI] × [ST]
- 1 -	**- 2 -**	**- 3 -**	**- 4 -**	**- 5 -**
SW_D1(N)	PZ_{SWD} 2(S)	2(S)=1(N) × 2(S)	2(S)	2(S) × 2(S) = **4 (S)**

Opis zidentyfikowanych podatności:

W zakresie działania „sił wyższych” (SW_D) zidentyfikowano następujące podatności:

$PZ1_{SWD}$: brak instalacji odgromowej.

$PZ2_{SWD}$: niewłaściwie konserwowana instalacja odgromowa.

$PZ3_{SWD}$: niewłaściwie eksploatowana instalacja ppoż.

$PZ4_{SWD}$: brak przypisania obowiązków i odpowiedzialności w zakresie ochrony ppoż.

$PZ5_{SWD}$: niewłaściwie wdrożone DRP.

W zakresie celowej działalności człowieka (CE_D) zidentyfikowano następujące podatności:

$PZ1_{CED}$: źle wyszkolona ochrona fizyczna obiektów.

$PZ2_{CED}$: niewłaściwy nadzór nad pracownikami ochrony fizycznej obiektów.

$PZ3_{CED}$: niewłaściwie eksploatowana instalacja ppoż.

$PZ4_{CED}$: brak przypisania obowiązków i odpowiedzialności w zakresie ochrony ppoż.

$PZ5_{CED}$: niewłaściwie wdrożone DRP.

W zakresie błędów popełnianych przez człowieka ($BŁ_D$) zidentyfikowano następujące podatności:

$PZ1_{BŁD}$: brak szkolenia p.poż. dla pracowników firmy Płatnik sp. z o.o.

$PZ2_{BŁD}$: brak wyznaczonych stref dla palaczy.

$PZ3_{BŁD}$: niewłaściwie eksploatowana instalacja ppoż.

$PZ4_{CED}$: brak przypisania obowiązków i odpowiedzialności w zakresie ochrony ppoż.

$PZ5_{CED}$: niewłaściwie wdrożone DRP.

Komentarz: ponieważ to jest tylko przykład, zbiór podatności jest ograniczony. W praktyce, w ramach sesji burzy mózgów, identyfikowanie podatności i przygotowywanie ich opisów powinno być prowadzone tak długo, aż zabraknie pomysłów i/lub danych. Uwaga ta dotyczy także dwóch pozostałych przykładów. Z podanego przykładu widać (frazy zielone), że ta sama podatność może być istotna dla różnych sposobów realizacji zagrożenia o skutku „POŻAR”. Nasuwa to oczywisty wniosek, że zbiór takich podatności, na kolejnym etapie zarządzania ryzykiem (etap minimalizowania ryzyka), powinien być minimalizowany w pierwszej kolejności.

Na podstawie podatności cząstkowych oszacowano podatność całkowitą związaną ze zdarzeniem „pożar” i (w tym przypadku) zagrożeniem typu SW_D. Na podstawie wyników wizji lokalnej przeprowadzonej przez eksperta stwierdzono,

że jest instalacja odgromowa, ale jest źle konserwowana, czyli całkowity poziom podatności w tym przypadku oceniono jako ŚREDNI (liczbowo 2). Szczegóły – patrz tabela 5.

Tab. 5. Interpretacja ocen opisowych dla podatności[7] związanych ze zdarzeniem „pożar" i zagrożenia typu SW_D

OCENA	INTERPRETACJA
K	~(jest instalacja odgromowa) ∧ ~(właściwa konserwacja instalacji odgromowej)
W	–
S	~(jest instalacja odgromowa) ∧ (właściwa konserwacja instalacji odgromowej) ∨ (jest instalacja odgromowa) ∧ ~(właściwa konserwacja instalacji odgromowej)
N	(jest instalacja odgromowa) ∧ (właściwa konserwacja instalacji odgromowej)

Uwaga: symbole ∧, ∨ oraz ~ to funktory zdaniotwórcze odpowiednio „i", „lub" oraz „nieprawda, że". Uwaga ta dotyczy także pozostałych dwóch przykładów.

Po zasięgnięciu opinii eksperta z dziedziny ochrony ppoż. stwierdzono, że pomimo złej konserwacji instalacji odgromowej, ze względu na niewielką odległość obiektu od remizy Straży Pożarnej, szkody w najgorszym przypadku powinny się ograniczyć do spalenia górnych pięter budynku i ograniczonych uszkodzeń infrastruktury teleinformatycznej. Szacunkowe straty wyceniono na ok. 95 tys. zł. Czyli poziom strat oceniono jako ŚREDNI (liczbowo 2).

Oszacowania są zebrane w tabeli 4. Z przyjętej metody szacowania ryzyka (patrz [3]) wynika, że ryzyko zajścia zdarzenia:

ZD_25: Pożar w budynku firmy Płatnik Sp. z o.o. przy ul. Moczarowej 3 w Opolu

na skutek realizacji zagrożenia typu „siła wyższa" jest na poziomie ŚREDNI.

Tabelę 4 należy uzupełnić o oszacowania utraty dostępności obiektu (zasobu infrastrukturalnego) 3/Moczarowa na skutek pożaru wywołanego celową działalnością człowieka (CE_D) oraz błędami popełnionymi przez człowieka ($BŁ_D$). Elementy takiej analizy są zamieszczone na rys. 1.

[7] W tej tabeli liczbę podatności ograniczono do dwóch. W praktyce ich liczba będzie zależna od wyników identyfikacji, a sposób ich złożenia, w celu uzyskania interpretacji ocen, będzie zależał od wiedzy i decyzji analityka ryzyka lub wspierającego go eksperta dziedzinowego. Uwaga ta dotyczy także pozostałych przykładów.

3. **Szacowania ryzyka IT – przypadek 2** (bez SW i CE)

KONTEKST:

W opolskiej firmie Płatnik sp. z o.o. na zlecenie Zarządu przeprowadzono szacowanie ryzyka IT. W tym celu przyjęto metodykę jak w pracy [3], uzupełnioną
o przedstawione dalej arkusze opisu zasobu (-ów) i zagrożenia, które zostały wytworzone na podstawie zaproponowanych wzorców (tabela 1 i 2), podczas realizacji tej metodyki.

W tym przykładzie przyjmuje się, że jednym ze zdarzeń zidentyfikowanych w ramach „burzy mózgów", szkodliwych dla działalności biznesowej firmy Płatnik sp. z o.o., jest zdarzenie:

ZD_35: Błąd w oprogramowaniu firmy Płatnik sp. z o.o. uniemożliwiający prawidłową realizację płatności Klienta

Stwierdzono przy tym, że występujący błąd nie może być wynikiem sabotażu (czyli realizacji zagrożenia z klasy CE), a klasa SW z oczywistych względów nie jest brana pod uwagę.

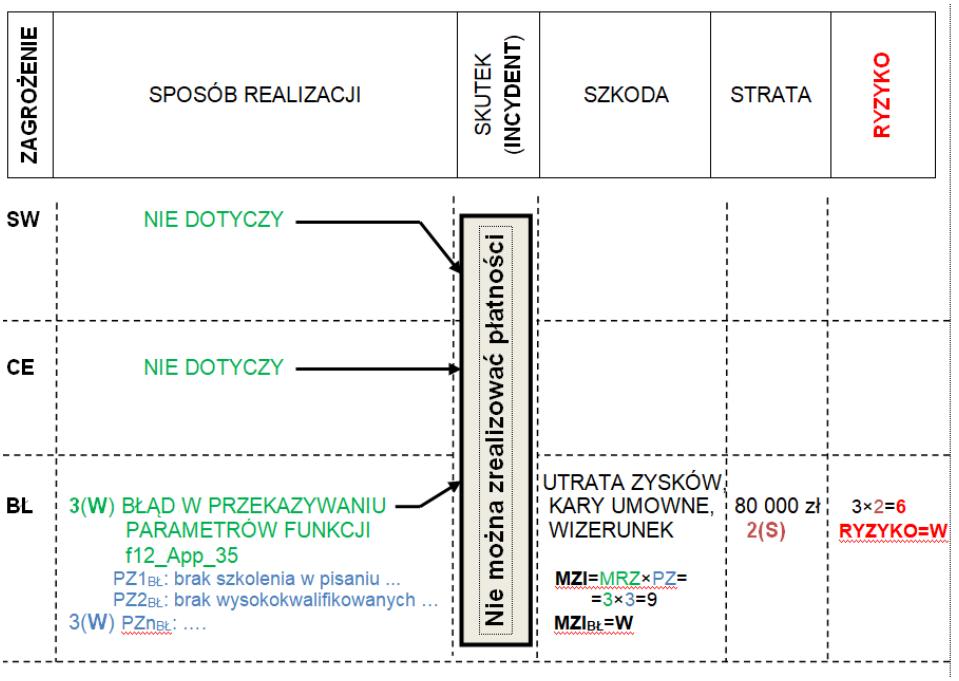
Zarząd firmy Płatnik sp. z o.o. określił „apetyt na ryzyko" jak w tabeli 6.

Tab. 6. „Apetyt na ryzyko" – tabela ocen opisowych wielkości strat

Ocena opisowa wielkości STRAT	Interpretacja
Krytyczne	powyżej 800 tys. zł/rok
Wysokie	do 800 tys. zł/rok
Średnie	do 100 tys. zł/rok
Niskie	do 50 tys. zł/rok

Dalej jest przedstawiona szczegółowa analiza dla zagrożenia klasy **BŁ** realizującego się jako „Błąd w przekazywaniu parametrów funkcji f12_App_35".

Schemat wykonanej analizy przedstawiono na rysunku 2.



Oznaczenia:

- MRZ, PZ, MZI, ST, RYZYKO, × – jak w pracy [3].
- Symbol typu 1(**N**) oznacza: wartość opisowa „Niska”, liczbowo „1”.

Uwaga: ze względów edycyjnych wyliczenia wartości MZI_{xy} zostały umieszczone w kolumnie SZKODY, chociaż formalnie powinny znajdować się w kolumnie SKUTEK (INCYDENT).

Rys. 2. Szacowanie ryzyka dla zdarzenia o skutku „Nie można zrealizować płatności”

ANALIZA:

ARKUSZ nr 35 OPISU ZASOBU	
Typ zasobu: [~~infrastrukturalny, teleinformatyczny~~, informacyjny, ~~systemu ochrony~~]	
Identyfikator zasobu: [App_35/Platnik]	
Opis zasobu:	Moduł realizacji płatności Klienta wykonany w Pythonie
Umiejscowienie zasobu:	Chmura AWS
Właściciel zasobu:	Firma Płatnik Sp. z o.o., tel. 77 261 84 85
Możliwe (szacowane) straty w przypadku realizacji zagrożenia dla:	Poufności: nie dotyczy Integralności: nie dotyczy Dostępności: do 100 tys. zł Rozliczalności: nie dotyczy

Inne dane w zależności od rodzaju zasobu:	Wykonawcą błędnego modułu jest ZP_3

ARKUSZ nr 35.3 OPISU ZAGROŻENIA	
Identyfikator zagrożenia: BŁ	
Zagrożenie:	Błąd kodowania popełniony przez zespół programistyczny ZP_3.
Scenariusz realizacji zagrożenia dla:	**Poufności:** NIE DOTYCZY **Integralności:** NIE DOTYCZY **Dostępności:** Po zainstalowaniu w środowisku produkcyjnym nowej wersji modułu App_35/Platnik, u kilku klientów realizujących operacje płatnicze został zasygnalizowany błąd (Error 35) sugerujący nieprawidłowe działanie funkcji f12_App_35. Skutkiem tego błędu było przerwanie realizacji płatności. Oprócz komunikatu (Error 35), na ekranie klienta nie zostały wyświetlone żadne inne informacje, a program zawiesił swoje działanie. **Rozliczalności:** NIE DOTYCZY
Zasoby, na które zagrożenie może mieć wpływ i szkody:	Wszystkie funkcje wywoływane z modułu App_35/Płatnik
Procesy, na które zagrożenie może mieć wpływ i szkody:	Wszystkie biznesowe procesy płatnicze: *[lista: proces/szkoda/właściciel procesu]*
Usługi, na które zagrożenie może mieć wpływ i szkody:	Wszystkie usługi płatnicze: *[lista: usługa/szkoda/symbole identyfikacyjne umowy]*
Potencjał zagrożenia:	Wysoki: część klientów nie może realizować płatności, co rzutuje na wizerunek firmy Płatnik Sp. z o.o. jako wiarygodnego dostawcy usług płatniczych. Tracone są zyski z niezakończonych transakcji, niektórym sklepom internetowym muszą być wypłacone kary umowne.

Oprogramowanie płatnicze jest uaktualniane średnio co trzy miesiące przez programistów zatrudnionych w firmie Płatnik. Na podstawie analizy danych historycznych z Rejestru Ryzyka prowadzonego od 10 lat w firmie Płatnik stwierdzono, że zdarzenie typu „błąd w oprogramowaniu, którego skutkiem jest

brak możliwości zrealizowania operacji płatniczej" występuje średnio raz w ciągu roku (tj. co czwartą aktualizację). Powiadamiany o incydentach Zarząd firmy Płatnik uznał, że w związku z ostrą konkurencją na rynku usług płatniczych częstość występowania błędu tego typu jest zbyt duża i należy dążyć do jej zmniejszenia. Aktualną częstość występowania tego błędu oceniono w związku z tym jako WYSOKĄ (liczbowo 3).

Tab. 7. Przypisania wartości: zagrożeń, podatności, możliwości, strat, ryzyka dla atrybutu DOSTĘPNOŚĆ dla zasobu (App_35/Platnik)

ZAGROŻENIE [MRZ]	**PODATNOŚĆ** [PZ]	**MOŻLIWOŚĆ** [MZI] = [MRZ] × [PZ]	**STRATY** [ST]	**RYZYKO$_D$** [MZI] × [ST]
- 1 -	**- 2 -**	**- 3 -**	**- 4 -**	**- 5 -**
BŁ$_D$ 3(W)	PZ$_{BŁD}$ 3(W)	9(W) = 3(W) × 3(W)	2(S)	3(W) × 2(S) = **6(W)**

Opis zidentyfikowanych podatności:

PZ1$_{BŁD}$: brak szkolenia z pisania bezpiecznego kodu dla programistów z firmy Płatnik sp. z o.o.

PZ2$_{BŁD}$: brak w zespole ZP_3 programistów o wysokich kwalifikacjach.

PZ3$_{BŁD}$: niewykonywanie testów regresyjnych zaktualizowanego oprogramowania w środowisku zapasowym przed zainstalowaniem w środowisku produkcyjnym.

PZ4$_{BŁD}$: niewłaściwy nadzór nad procesem testowania.

Na podstawie podatności cząstkowych oszacowano podatność całkowitą związaną ze zdarzeniem ZD_35 i (w tym przypadku) zagrożeniem typu BŁ$_D$. Na podstawie wywiadów z programistami z zespołu ZP_3 stwierdzono, że wszyscy są programistami młodszymi i nie przeszli żadnego szkolenia z pisania bezpiecznego kodu. Całkowity poziom podatności w tym przypadku oceniono jako WYSOKI (liczbowo 3). Szczegóły – patrz tabela 8.

Tab. 8. Interpretacja ocen opisowych dla podatności związanych ze zdarzeniem ZD_35 i zagrożenia typu BŁ

OCENA	**INTERPRETACJA**
K	–
W	~(jest starszy programista w zespole) ∧ ~(są szkolenia z pisania bezpiecznego kodu)
S	~(jest starszy programista w zespole) ∧ (są szkolenia z pisania bezpiecznego kodu) ∨ (jest starszy programista w zespole) ∧ ~(są szkolenia z pisania bezpiecznego kodu)
N	(jest starszy programista w zespole) ∧ (są szkolenia z pisania bezpiecznego kodu)

Po zasięgnięciu opinii dyrektora działu ds. kluczowych klientów stwierdzono, że błąd tego typu ujawnia się tylko w przypadku szczególnych kombinacji wprowadzanych przez klientów znaków, co oznacza że kluczowi klienci albo zostali dotknięci tym błędem tylko raz w ciągu 10 lat (jak wynika z Rejestru Ryzyka) lub wcale. W związku z tym uznano, że szkody w najgorszym przypadku powinny się ograniczyć do nieznacznych strat wizerunkowych oraz sporadycznie wypłaconej kary umownej. Szacunkowe straty wyceniono na ok. 80 tys. zł, czyli poziom strat oceniono jako ŚREDNI (liczbowo 2).

Oszacowania są zebrane w tabeli 7. Z przyjętej metody szacowania ryzyka (patrz [3]) wynika, że ryzyko zajścia zdarzenia:

ZD_35: Błąd w oprogramowaniu firmy Płatnik sp. z o.o., uniemożliwiający prawidłową realizację płatności Klienta

na skutek realizacji zagrożenia typu „błąd ludzki" jest na poziomie WYSOKI.

4. Szacowania ryzyka IT – przypadek 3 (bez SW i BŁ)

KONTEKST:

W opolskiej firmie Płatnik sp. z o.o. na zlecenie Zarządu przeprowadzono szacowanie ryzyka IT. W tym celu przyjęto metodykę jak w pracy [3], uzupełnioną o przedstawione dalej arkusze opisu zasobu (-ów) i zagrożenia, które zostały wytworzone na podstawie zaproponowanych wzorców (tabela 1 i 2), podczas realizacji tej metodyki.

W tym przykładzie przyjmuje się, że jednym ze zdarzeń zidentyfikowanych w ramach „burzy mózgów", szkodliwych dla działalności biznesowej firmy Płatnik sp. z o.o., jest zdarzenie:

ZD_42: Wyciek informacji wrażliwej (dane dotyczące umów) z firmy Płatnik sp. z o.o.

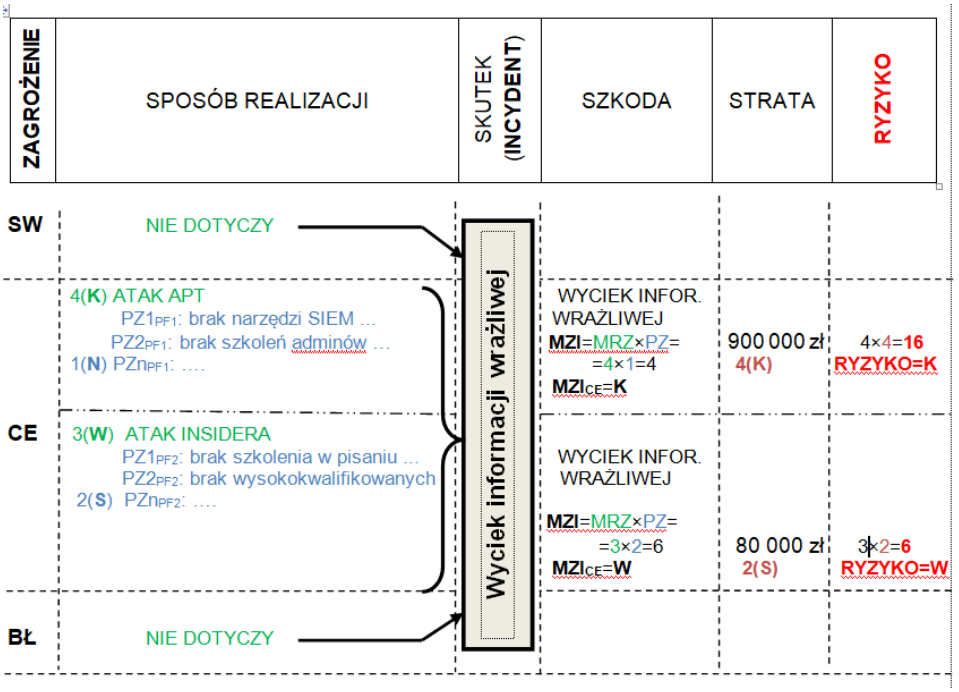
Stwierdzono, że istnieją dwa realne scenariusze wydarzeń (oba z klasy **CE**):

1) wrogi **podmiot wewnętrzny** (ang. *insider*) wyprowadził informacje nt. umów podpisanych z klientami firmy Płatnik sp. z o.o.;
2) wrogi **podmiot zewnętrzny** skutecznie zrealizował atak typu APT i w ciągu 6 miesięcy wyprowadził dane nt. wszystkich umów firmy Płatnik sp. z o.o.

Zarząd firmy Płatnik sp. z o.o. określił „apetyt na ryzyko" jak w tabeli 9.

Tab. 9. „Apetyt na ryzyko" – tabela ocen opisowych wielkości strat

Ocena opisowa wielkości STRAT	Interpretacja
Krytyczne	powyżej 800 tys. zł/rok
Wysokie	do 800 tys. zł/rok
Średnie	do 100 tys. zł/rok
Niskie	do 50 tys. zł/rok



Oznaczenia:

- MRZ, PZ, MZI, ST, RYZYKO, × – jak w pracy [3].
- Symbol typu 1(**N**) oznacza: wartość opisowa „Niska", liczbowo „1".

Uwaga: ze względów edycyjnych wyliczenia wartości MZI_{xy} zostały umieszczone w kolumnie SZKODY, chociaż formalnie powinny znajdować się w kolumnie SKUTEK (INCYDENT).

Rys. 3. Szacowanie ryzyka dla zdarzenia o skutku „Wyciek informacji wrażliwej"

Dalej jest przedstawiona szczegółowa analiza dla zagrożenia klasy **CE** (dwa warianty) realizującego się jako: „Wyciek informacji wrażliwej (dane dotyczące umów) z firmy Płatnik sp. z o.o.". Schemat wykonanej analizy przedstawiono na rysunku 3.

ANALIZA:

ARKUSZ nr 42 OPISU ZASOBU	
Typ zasobu: [~~infrastrukturalny, teleinformatyczny~~, informacyjny, ~~systemu ochrony~~]	
Identyfikator zasobu: [Katalog_UMOWY]	
Opis zasobu:	W katalogu UMOWY są przechowywane w plikach .docx i .pdf umowy zawarte z dostawcami usług i usługobiorcami firmy Płatnik Sp. z o.o.
Umiejscowienie zasobu:	Chmura AWS (kopia), dysk w stacji roboczej ST_22 w siedzibie firmy Płatnik Sp. z o.o.
Właściciel zasobu:	Firma Płatnik sp. z o.o. , tel. 77 261 84 85
Możliwe (szacowane) straty w przypadku realizacji zagrożenia dla:	Poufności: 900 000 zł Integralności: nie dotyczy Dostępności: nie dotyczy Rozliczalności: nie dotyczy
Inne dane w zależności od rodzaju zasobu:	Stacja robocza ST_22 należy do Działu Księgowości

ARKUSZ nr 42.1 OPISU ZAGROŻENIA	
Identyfikator zagrożenia: CE	
Zagrożenie:	Wrogi podmiot wewnętrzny realizujący atak fizyczny i wrogi podmiot zewnętrzny realizujący atak zdalny.
Scenariusz realizacji zagrożenia dla:	**Poufności:** 1) Wrogi podmiot zewnętrzny (CE_{PF1}): W wyniku wykrytego i zablokowanego dopiero po 172 dniach ataku APT zostały wyprowadzone dane wszystkich umów zarówno zarchiwizowanych, jak i zawartych w czasie trwania ataku. 2) Wrogi podmiot wewnętrzny (*insider*; CE_{PF2}): Po zmianie zarządu firmy i licznych zwolnieniach z pracy, znacząco pogorszyły się stosunki pomiędzy personelem i kierownictwem. Spowodowało to zwiększoną podatność pracowników na przekupstwo ze strony konkurencji. Jeden z przekupionych pracowników księgowości mający legalny dostęp do zasobu teleinformatycznego ST_22, zanim odebrano mu dostęp do obiektów i systemów firmy Płatnik, korzystając z aparatu fotograficznego (zdjęcia ekranu monitora komputera), wyprowadził dane o 10 umowach zawartych z usługobiorcami firmy Płatnik w ciągu ostatnich trzech miesięcy. **Integralności:** NIE DOTYCZY **Dostępności:** NIE DOTYCZY **Rozliczalności:** NIE DOTYCZY
Zasoby, na które zagrożenie może mieć wpływ i szkody:	Brak
Procesy, na które zagrożenie może mieć wpływ i szkody:	Procesy związane z organizacją przetargów: *[lista: proces/szkoda/właściciel procesu]*
Usługi, na które zagrożenie może mieć wpływ i szkody:	Wszystkie zamawiane usługi: *[lista: usługa/szkoda/symbole identyfikacyjne umowy]*
Potencjał zagrożenia:	Średni: rzutuje na wizerunek firmy Płatnik Sp. z o.o. jako wiarygodnego partnera biznesowego.

Tab. 10. Przypisania wartości: zagrożeń, podatności, możliwości, strat, ryzyka dla atrybutu POUFNOŚĆ dla zasobu (Chmura AWS/ST_22)

ZAGROŻENIE [MRZ]	**PODATNOŚĆ** [PZ]	**MOŻLIWOŚĆ** [MZI] = [MRZ] × [PZ]	**STRATY** [ST]	**RYZYKO$_P$** [MZI] × [ST]
- 1 -	**- 2 -**	**- 3 -**	**- 4 -**	**- 5 -**
CE_{PF1}: 4(K) CE_{PF2}: 3(W)	PZ_{PF1} 1(N) PZ_{PF2} 2(S)	4(K) =4(K) × 1(N) 6(W) = 3(W) × 2(S)	4(K) 2(S)	4(K) × 4(K) = **16(K)** 3(W) × 2(S) = **6(W)**

Opis zidentyfikowanych podatności:

$PZ1_{PF1}$: brak narzędzi typu SIEM.

$PZ1_{PF2}$: brak mechanizmów zapewniania lojalności pracowników.

$PZ2_{PF1}$: administratorzy techniczni sieci i systemów nie zostali przeszkoleni w zakresie rozpoznawania symptomów ataków zdalnych.

$PZ2_{PF2}$: brak procedur bezpieczeństwa pracy z informacjami wrażliwymi.

$PZ3_{PF1}$: dzienniki zdarzeń systemów i urządzeń nie są przeglądane w celu znalezienia anomalii świadczących o ataku.

$PZ3_{PF2}$: brak procedur nadzoru nad działaniami pracowników ze strony personelu Departamentu Bezpieczeństwa.

$PZ4_{PF1}$: brak procedur pozyskiwania informacji o najnowszych sposobach realizacji ataków i ich symptomach.

$PZ4_{PF2}$: brak narzędzi z zakresu ochrony technicznej (kamer, rejestratorów WE/WY itp.) umożliwiających nadzór nad działaniami pracowników.

Na podstawie podatności cząstkowych oszacowano podatność całkowitą związaną ze zdarzeniem ZD_42 i (w tym przypadku) zagrożeniem typu CE_{PF1} i CE_{PF2}. Na podstawie wyników wizji lokalnej przeprowadzonej przez eksperta oraz podstawie wywiadów z personelem Departamentu Bezpieczeństwa i Księgowości stwierdzono że:

- W zakresie CE_{PF1} – admini techniczni są regularnie kierowani na szkolenia z zakresu rozpoznawania symptomów ataków zdalnych oraz wykorzystują w swojej pracy narzędzia SIEM, czyli poziom podatności oceniono jako NISKI (liczbowo 1).
- W zakresie CE_{PF2} – jest co prawda nadzór ze strony Departamentu Bezpieczeństwa nad działaniami pracowników, ale w firmie nie ma wdrożonych żadnych mechanizmów zapewniania lojalności, czyli poziom podatności oceniono jako ŚREDNI (liczbowo 2).Szczegóły – patrz tabela 11.

Tab. 11. Interpretacja ocen opisowych dla podatności związanych ze zdarzeniem ZD_42 i zagrożenia typu CE

OCENA	INTERPRETACJA
K /CE_{PF1}	~(są używane SIEM) ∧ ~(admini są przeszkoleni)
W/CE_{PF1}	–
S/CE_{PF1}	~(są używane SIEM) ∧ (admini są przeszkoleni) ∨ (są używane SIEM) ∧ ~(admini są przeszkoleni)
N/CE_{PF1}	(są używane SIEM) ∧ (admini są przeszkoleni)
K/CE_{PF2}	–
W/CE_{PF2}	~(jest nadzór) ∧ ~(są mechanizmy zapewniania lojalności)
S/CE_{PF2}	~(jest nadzór) ∧ (są mechanizmy zapewniania lojalności)∨ (jest nadzór) ∧ ~(są mechanizmy zapewniania lojalności)
N/CE_{PF2}	(jest nadzór) ∧ (są mechanizmy zapewniania lojalności)

Dla CE_{PF1}: Po sprawdzeniu Rejestru Ryzyka stwierdzono, że w minionych dziesięciu latach było 5 przypadków ataków typu APT o średnim czasie wykrycia 20 dni (przy średniej światowej 180 dni). Biorąc pod uwagę wzmożoną działalność grup APT oraz fakt, że Płatnik jest instytucją finansową (czyli atrakcyjnym celem dla przestępczych podmiotów zewnętrznych), oceniono możliwość zaistnienia w najbliższym czasie ataku APT jako KRYTYCZNĄ (liczbowo 4), a przypuszczalne straty związane z karami umownymi wyceniono na ok. 900 000 zł, czyli także jako KRYTYCZNE (liczbowo 4).

Dla CE_{PF2}: Po sprawdzeniu Rejestru Ryzyka stwierdzono, że w minionych dziesięciu latach nie było przypadków nielojalnych działań pracowniczych. Możliwość przeprowadzenia szkodliwych działań przez *insidera* z perspektywy historycznej oceniono zatem jako niską. Ale uwzględniając aktualne trendy w działaniu grup APT (wzmożone pozyskiwanie *insiderów*) oraz występujące po raz pierwszy od dziesięciu lat poważne konflikty na linii Zarząd-pracownicy, zdecydowano, że możliwość przeprowadzenia szkodliwych działań przez wrogi podmiot wewnętrzny należy ocenić jako WYSOKĄ (liczbowo 3). Biorąc pod uwagę to, że poszczególni pracownicy mają dostęp do zasobów informacyjnych, przyznawany na zasadzie „wiedzy koniecznej" i „minimalnego środowiska pracy" (czyli w praktyce mogą ujawnić tylko część umów) oraz wysokość kar umownych związanych z ujawnieniem informacji wrażliwych, oszacowano możliwe straty na ok. 80 tys. zł, czyli jako ŚREDNIE (liczbowo 2).

Oszacowania są zebrane w tabeli 10. Z przyjętej metody szacowania ryzyka (patrz [3])[8] wynika, że ryzyko zajścia zdarzenia:

ZD_42: Wyciek informacji wrażliwej (dane dotyczące umów) z firmy Płatnik Sp. z o.o.

na skutek realizacji zagrożenia typu „Działanie celowe" jest na poziomie KRYTYCZNY.

4. Podsumowanie

W artykule przedstawiono trzy przykłady szacowania ryzyka IT. Przykłady te, dla których podstawy formalne są zawarte w pracach [1] i [3], uwzględniają następujące założenia:

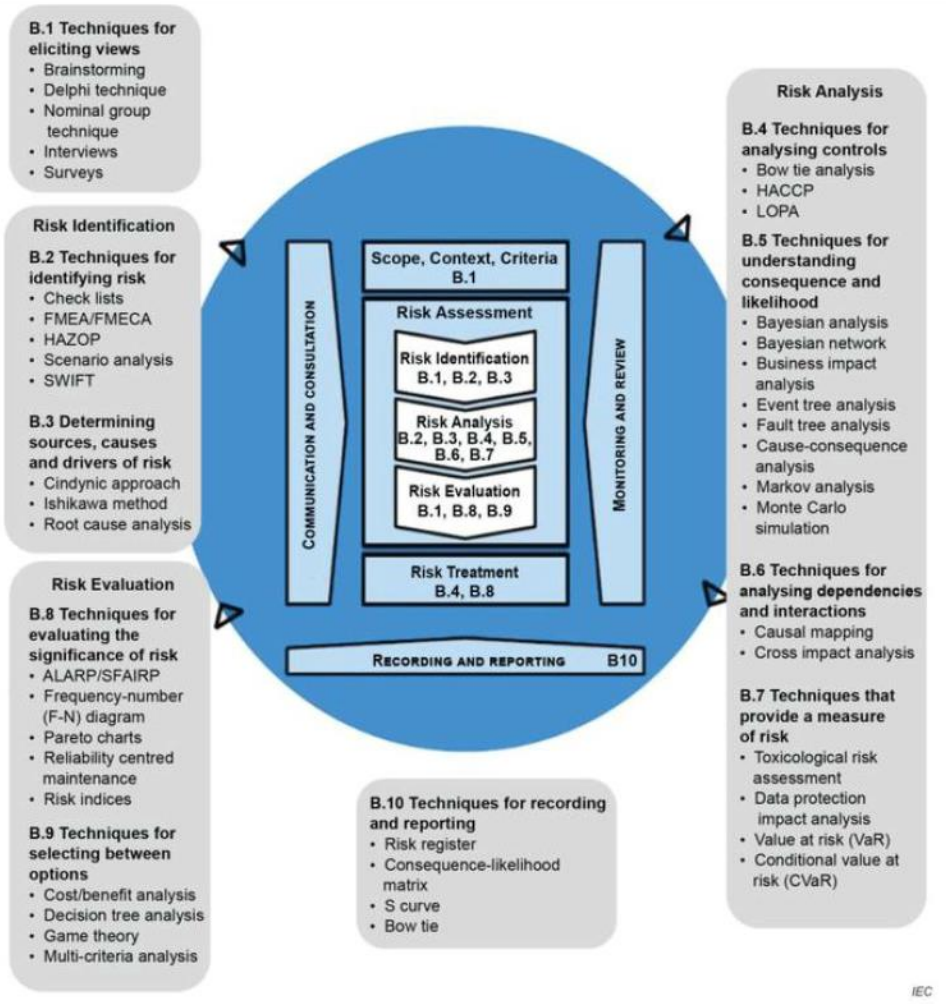
1. Zbiór zagrożeń jest trójelementowy (SW, CE, BŁ).
2. Metody szacowania to:
   - metoda autorska (patrz [1], [3]), opisowa, wykorzystująca oceny opisowe ze zbioru {**N**iskie, **Ś**rednie, **W**ysokie, **K**rytyczne} oraz
   - metoda według ISO/IEC 27005 [6] wykorzystująca oceny liczbowe ze zbioru {**1**, **2**, **3**, **4**}.
3. Dostępne są dane historyczne, np. z Rejestru Ryzyka prowadzonego przez podmiot, dla którego jest prowadzona analiza ryzyka oraz dane z wywiadów z ekspertami.

Celem artykułu było pokazanie możliwości praktycznego wyliczenia wartości ryzyka. Warto zauważyć, że konsekwentnie rozróżnianie zagrożenia i sposobu jego realizacji[9], co jest pokazane na rys. 1-3, uwidacznia w zakresie minimalizacji ryzyka możliwości działania proaktywnego, które to możliwości zwykle są niedostrzegane przy „widzeniu" tylko zagrożenia i jego skutku (np. na rys. 1 – pożaru).

Dla Czytelnika, który jest zainteresowany szerszym spektrum technik stosowanych przy ocenie ryzyka (głównie jakościowych), warta polecenia jest norma [7], która zawiera specyfikację i opis 40 technik szacowania ryzyka przyporządkowanych do procesów zarządzania ryzykiem według normy [5] (patrz rys. 4).

[8] $\max\{\text{RYZYKO}(CE_{PF1}), \text{RYZYKO}(CE_{PF2})\} = \max\{K, W\} = \mathbf{K}$

[9] Czyli także uwidocznienie podatności, które mogą być wykorzystane przy konkretnej realizacji zagrożenia i które mogą być w ramach przeciwdziałania tej konkretnej realizacji minimalizowane.



Rys. 4. Zastosowanie technik szacowania ryzyka w procesie zarządzania ryzykiem według normy ISO 31000 (za [7])

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] LIDERMAN K., *Analiza ryzyka na potrzeby bezpieczeństwa informacyjnego według zaleceń normy PN-ISO/IEC 27005*. Przegląd Teleinformatyczny, Nr 8(26) 1-4. WAT, Warszawa 2022, s. 19-34.

[4] COBIT® 5, *Metodyka biznesowa w zakresie nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi*, An ISACA® Framework, wersja językowa polska.

[5] PN-ISO 31000:2012, *Zarządzanie ryzykiem – Zasady i wytyczne*, PKN 2012.

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

[7] PN-EN IEC 31010:2020-01, *Zarządzanie ryzykiem – Techniki oceny ryzyka*, wersja językowa angielska.

IT risk evaluation – case study

ABSTRACT: The paper presents, through three examples, an IT risk evaluation method. IT risk is associated with the realization of threats that cause damage to teleinformatics systems and processed information resources. The quality risk evaluation method, demonstrated through these examples, involves four descriptive scores translated into numerical values in accordance with the PN-ISO/IEC 27005:2014-01 recommendation.

KEYWORDS: information security, threat realization, IT risk evaluation

Praca wpłynęła do redakcji: 29.11.2022 r.