ZACHODNIOPOMORSKI UNIWERSYTET TECHNOLOGICZNY W SZCZECINIE

WYDZIAŁ INFORMATYKI

mgr inż. Damian Kacprowicz

Ocena bezpieczeństwa systemów teleinformatycznych przetwarzających informacje niejawne

Rozprawa doktorska

Promotor: prof. zw. dr hab. dr h.c. mult. Brunon Hołyst

Promotor pomocniczy: dr inż. Witold Maćków

Szczecin 2025

Kamili, Ani, Uli

Spis treści

WSTĘP

Współczesny rozwój technologii teleinformatycznych oraz szeroka implementacja rozwiązań cyfrowych w niemal każdej dziedzinie życia publicznego i prywatnego stawiają przed organizacjami nowe wyzwania w zakresie ochrony informacji. Przetwarzanie danych stało się fundamentem działalności administracji publicznej, instytucji finansowych, służb mundurowych czy przedsiębiorstw. Niemniej jednak, rosnąca zależność od systemów informatycznych stwarza również poważne zagrożenia związane z naruszeniem poufności, integralności i dostępności przetwarzanych informacji. W szczególności, kwestie związane z ochroną informacji niejawnych, których wyciek lub niewłaściwe przetwarzanie mogą mieć konsekwencje o charakterze narodowym lub międzynarodowym, wymagają szczególnej uwagi. W kontekście tych wyzwań istotnym staje się opracowanie i wdrożenie skutecznych metod oceny oraz monitorowania bezpieczeństwa systemów teleinformatycznych, w szczególności tych, które obsługują dane wrażliwe, objęte specjalnymi regulacjami prawnymi. Z tego względu niniejsza praca koncentruje się na analizie mechanizmów zapewniających bezpieczeństwo tych systemów, z uwzględnieniem narzędzi oceny ryzyka oraz działań mających na celu minimalizowanie zagrożeń związanych z przetwarzaniem informacji niejawnych.

Struktura pracy

Struktura pracy odzwierciedla logiczny ciąg prowadzenia badań naukowych, począwszy od identyfikacji problemu badawczego, przez przegląd istniejących rozwiązań i analizę potrzeb praktyki, aż po propozycję własnego modelu oraz jego weryfikację:

1. W pierwszej kolejności zdefiniowano problem nadmiernej złożoności istniejących metod oceny bezpieczeństwa systemów przetwarzających informacje niejawne. *(Wstęp; Rozdział 2.9)*

2. Następnie postawiono główną tezę oraz tezę pomocniczą, zakładające możliwość opracowania mniej złożonego narzędzia oceny mechanizmów ochrony ale jednocześnie zapewniającego wysoki poziom bezpieczeństwa. *(Wstęp; Rozdział 2.10–2.11)*

3. Dokonano przeglądu aktualnych metod oceny poziomu bezpieczeństwa i ich ograniczeń, zarówno jakościowych, ilościowych, jak i mieszanych, z uwzględnieniem aspektów formalnych i normatywnych. *(Rozdział 2.10, 2.12; Rozdział 5.1)*

4. Przeprowadzono badania jakościowe wśród interesariuszy zajmujących się ochroną informacji niejawnych, w celu poznania praktycznych potrzeb i słabych stron dotychczasowych rozwiązań. *(Rozdział 2.8)*

5. Na tej podstawie opracowano autorski **Model Oceny Ryzyka Ochrony Informacji Niejawnych (MOROIN)**, oparty na sformalizowanej macierzy ryzyka, podatności i skutków. *(Rozdział 2.11; Rozdział 3.1–3.4)*

6. Model MOROIN został poddany **eksperymentalnej weryfikacji** w systemach rzeczywistych i symulowanych, zgodnie z metodologią badań technicznych właściwych dla dyscypliny informatyka techniczna i telekomunikacja. *(Rozdział 3.5–3.12; Rozdział 5.2–5.4)*

7. Wyniki wdrożenia zestawiono z innymi metodami oceny poziomu bezpieczeństwa, stosując obiektywne metryki porównawcze (wg Pandeya i Mustafy), w celu potwierdzenia skuteczności proponowanego podejścia. *(Rozdział 5.1, 5.5)*

8. Pracę zamyka podsumowanie i wnioski, które wskazują na praktyczność i zgodność modelu MOROIN z aktualnymi wymaganiami technicznymi w zakresie bezpieczeństwa systemów teleinformatycznych. *(Podsumowanie)*

Praca składa się z pięciu rozdziałów.

Rozdział 1 wprowadza w problematykę bezpieczeństwa informacji oraz omawia podstawowe zasady ochrony informacji niejawnych. Przedstawione zostaną najważniejsze kategorie informacji wymagających zabezpieczenia oraz zagrożenia, które wpływają na ich bezpieczeństwo. Rozdział ten analizuje również podstawowe pojęcia związane z zarządzaniem ryzykiem, które stanowi fundament oceny bezpieczeństwa.

Rozdział 2 skupia się na przeglądzie istniejących norm i standardów oceny bezpieczeństwa systemów teleinformatycznych, analizując różnorodne podejścia – ilościowe, jakościowe oraz mieszane metody oceny poziomu bezpieczeństwa. Rozdział bada ograniczenia związane ze złożonością tych metod. **Kluczowym elementem jest projekt Modelu Oceny Ryzyka Ochrony Informacji Niejawnych (MOROIN), który mimo uproszczonej struktury może być wykorzystany w narzędziach zarządzania ryzykiem.** W rozdziale tym analizowane są także opinie interesariuszy systemów ochrony informacji niejawnych oraz ich rzeczywiste potrzeby w zakresie ochrony informacji, co pozwala na lepsze zrozumienie uwarunkowań w zakresie skuteczności oraz praktycznych zalet zaproponowanego modelu.

Rozdział 3 przedstawia wykorzystaną metodę oceny bezpieczeństwa systemów teleinformatycznych opartą na formalnym modelowaniu ryzyka. Zastosowanie formalnych technik umożliwia bardziej precyzyjną analizę zagrożeń oraz lepsze zrozumienie dynamiki ryzyk, co wpływa na poziom ochrony informacji niejawnych.

Rozdział 4 omawia procesy monitorowania ryzyk oraz utrzymania zakładanego poziomu bezpieczeństwa systemów, w tym przeglądy ryzyk, audyty bezpieczeństwa, monitorowanie w czasie rzeczywistym oraz systematyczne szkolenie personelu. Rozdział

ten kończy się przedstawieniem dobrych praktyk, które mogą zostać zastosowane w celu zapewnienia trwałej ochrony informacji w systemach teleinformatycznych.

Rozdział 5 przedstawia ocenę porównawczą modelu MOROIN względem wybranych istniejących metod oceny ryzyka, takich jak CRAMM, OCTAVE, NIST SP 800-30, ISO/IEC 27005. W pierwszej części zastosowano uznaną w literaturze metodykę porównawczą, analizując m.in. elastyczność, możliwość automatyzacji, zrozumiałość wyników oraz skalowalność. W kolejnych podrozdziałach zaprezentowano wybrane trzy eksperymenty: dwa przeprowadzone w rzeczywistych systemach (pracujących w trybie bezpieczeństwa dedykowanym i systemowym) oraz jeden w środowisku symulowanym (pracującym w trybie bezpieczeństwa wielopoziomowym). Rozdział kończy się podsumowaniem wyników eksperymentów i potwierdzeniem, że model MOROIN jest dostosowany do realiów ochrony informacji niejawnych.

Przedstawienie problemu badawczego

Głównym problemem badawczym poruszanym w niniejszej pracy jest paradoks polegający na tym, że jak pokazuje praktyka nadmiernie skomplikowane metody oceny bezpieczeństwa systemów teleinformatycznych, stosowane w procesie ich akredytacji, mogą prowadzić do obniżenia rzeczywistego poziomu ochrony, mimo zgodności z obowiązującymi normami i standardami branżowymi. Skomplikowane podejścia niejednokrotnie prowadzą do błędów w implementacji, a ich brak systematycznego stosowania w cyklu życia systemu może powodować, że systemy, choć formalnie zgodne z wymogami, są mniej bezpieczne w praktyce. Zjawisko to szczególnie dotyka systemów przetwarzających informacje wrażliwe, gdzie zaniechania w ocenie ryzyka i przeciwdziałanie nim mogą mieć poważne konsekwencje dla bezpieczeństwa danych.

Uzasadnienie podjęcia tematu

Ochrona informacji niejawnych oraz ich przetwarzanie w zgodzie z normami, jest elementem zapewnienia bezpieczeństwa narodowego i organizacyjnego. Jednakże, coraz bardziej złożone systemy informatyczne wymagają równie skomplikowanych narzędzi oceny ich bezpieczeństwa, co prowadzi do zwiększenia ryzyka popełniania błędów. Zidentyfikowanie tego problemu oraz opracowanie nowego narzędzia, które umożliwia ocenę poziomu bezpieczeństwa, jest istotne zarówno z punktu widzenia teorii, jak i praktyki.

Cel pracy i pytania badawcze

Celem pracy jest **opracowanie bardziej precyzyjnego oraz mniej złożonego** w praktyce **narzędzia oceny bezpieczeństwa** systemów teleinformatycznych, które przetwarzają informacje wrażliwe, **z wykorzystaniem formalnego modelowania ryzyka.** Formalne modelowanie, jako narzędzie analizy złożonych systemów, umożliwia bardziej przejrzyste i zautomatyzowane podejście do oceny ryzyka, co może znacząco wpłynąć na poprawę skuteczności ochrony danych. W tym kontekście kluczowe są następujące pytania badawcze:

1 W jaki sposób modelowanie formalne może wspierać proces oceny ryzyka w ochronie informacji niejawnych?

2 Jak zintegrować różne standardy certyfikacyjne i dobre praktyki w procesie oceny bezpieczeństwa systemów teleinformatycznych?
3 Jakie są relacje między metodami ilościowymi a jakościowymi w ocenie bezpieczeństwa i które z nich są bardziej adekwatne w różnych scenariuszach?
4 Jak wykorzystać metody mieszane do uzyskania bardziej kompleksowej oceny bezpieczeństwa systemów teleinformatycznych i jakie korzyści wynikają z połączenia podejść ilościowych i jakościowych?
5 Jak oceniać systemy teleinformatyczne w dynamicznym środowisku, biorąc pod uwagę ciągłe zmiany w zagrożeniach cybernetycznych?
6 Jak uwzględnić specyficzne wymagania i kontekst organizacyjny w procesie oceny bezpieczeństwa, zważywszy na różnice między sektorami przemysłowymi bądź branżami?

Zakres pracy

Praca skupia się na analizie istniejących metod oceny bezpieczeństwa systemów teleinformatycznych w kontekście ochrony informacji niejawnych, a także na analizie formalnych modeli ryzyka, które mogą uprościć i usprawnić ten proces. Obejmuje ona przegląd międzynarodowych standardów bezpieczeństwa, analizę luk oraz wywiady pogłębione z interesariuszami odpowiedzialnymi za ochronę informacji niejawnych. Wywiady te miały na celu zebranie doświadczeń interesariuszy oraz praktycznych informacji na temat stosowanych obecnie metod oceny bezpieczeństwa i napotykanych wyzwań. Na podstawie zebranych danych została przeprowadzona analiza luk, aby zidentyfikować obszary, w których obecne metody są niewystarczające.

Następnie, wyniki przeglądu standardów i wywiadów zostały zintegrowane w celu zaproponowania ulepszonej i bez nadmiernej złożoności procedury oceny poziomu bezpieczeństwa systemów teleinformatycznych, opartej na zaprojektowanym **Modelu Oceny Ryzyka Ochrony Informacji Niejawnych (MOROIN)**. Procedura ta jest oparta na formalnym modelowaniu ryzyka, które uwzględnia specyfikę systemów przetwarzających informacje niejawne, z naciskiem na ochronę poufności, integralności oraz dostępności danych.

Biorąc pod uwagę powyższe oraz zalecenia instytucji odpowiedzialnych za wydawanie świadectw akredytacji bezpieczeństwa systemów teleinformatycznych, naturalnym stało się zaproponowanie modelu formalnego analizy ryzyka minimalnego ze względu na jego złożoność strukturalną i obliczeniową oraz akceptowalnego przez podmioty akredytujące.

Wyniki pracy dostarczają narzędzia nie tylko do oceny obecnego poziomu ryzyka, ale również do jego monitorowania i ciągłej aktualizacji, co jest istotne w dynamicznie zmieniającym się środowisku zagrożeń cyberbezpieczeństwa.

W pracy pokazano, że narzędzie wykorzystujące model MOROIN stanowi postęp w zakresie oceny poziomu bezpieczeństwa systemów przetwarzających informacje wrażliwe. Podstawową nowością jest nie tylko zastosowanie formalnych metod w analizie ryzyka w kontekście oceny systemów przetwarzających informacje niejawne, ale także ich integracja

w spójną metodologię, która została wdrożona w praktyce. Wynikiem wdrożenia MOROIN w projektach akredytacyjnych, zakończonych sukcesem, jest realna ocena jej merytorycznej wartości. W porównaniu z rozwiązaniami omawianymi w literaturze, MOROIN uwzględnia dynamiczne zmiany w systemach teleinformatycznych oraz zmniejsza złożoność ocen, oferując bardziej precyzyjne narzędzia do oceny ryzyka.

Zaprojektowany model jest weryfikacją i potwierdzeniem skuteczności istniejących podejść. Praca ma wartość jako potwierdzenie stosowalności i spójności podejścia z istniejącymi normami i zaleceniami. Ponadto zaprojektowane narzędzie wykorzystujące model formalny analizy ryzyka okazał się skuteczny w ocenie poziomu bezpieczeństwa systemów przetwarzających informacje niejawne o różnych poziomach klauzul dla systemów pracujących we wszystkich trybach bezpieczeństwa (dedykowanym, systemowym, wielopoziomowym). **Najistotniejszym aspektem jest możliwość zastosowania modelu nie tylko do standardowej oceny przepływów danych z niższej do wyższej klasy tajności, co jest powszechnie praktykowane, ale także nowatorskie podejście do oceny bezpieczeństwa przy transferze danych z wyższej do niższej klasy. To podejście odpowiada na istniejące wyzwania związane z przesyłaniem informacji z klauzul o wyższym poziomie do niższych, które w obecnych rozwiązaniach są ograniczone. Przykładem zastosowania proponowanego narzędzia jest możliwość oceny poziomu bezpieczeństwa systemu przeznaczonego do sanityzacji wiadomości wymienianych w zautomatyzowanych systemach dowodzenia.**

ROZDZIAŁ 1
Ochrona informacji w systemach teleinformatycznych

Rozdział pierwszy rozprawy stanowi część poznawczą, obejmującą szczegółową analizę aktualnego stanu wiedzy na temat ochrony informacji. W ujęciu ontologicznym wskazuje na istotę ochrony, odpowiadając na pytanie, na czym należy się skupić, aby w ujęciu przedmiotowym zapewnić bezpieczeństwo informacji. Analogicznie jak w kryptologii, gdzie dla zapewnienia bezpieczeństwa informacji najistotniejszym zagadnieniem przy projektowaniu czy łamaniu szyfrów jest zrozumienie zjawisk dyfuzji, konfuzji informacyjnej oraz złożoności obliczeniowej problemu na jakim bazuje dany szyfr, tak w ocenie bezpieczeństwa systemów teleinformatycznych kluczowym elementem jest określenie gwarantowanej miary – poziomu bezpieczeństwa w odniesieniu do zidentyfikowanego zasobu podlegającego ochronie.

W ramach tego rozdziału przedstawione zostają podstawowe kategorie informacji wymagających ochrony, wraz z uzasadnieniem konieczności ich zabezpieczenia. Omawiana jest klasyfikacja informacji, proces klasyfikacji oraz zawartość meta-danych plików cyfrowych. Ponadto, analizowany jest cykl funkcjonowania systemu teleinformatycznego oraz kluczowe aspekty ochrony informacji, co umożliwia zrozumienie, jakie mechanizmy są niezbędne do zapewnienia integralności i poufności danych i informacji w systemach.

Rozdział zwraca również uwagę na różnorodne czynniki i zagrożenia, które mogą wpływać na bezpieczeństwo informacji, podkreślając znaczenie zarządzania ryzykiem oraz minimalizacji potencjalnych zagrożeń. Ta część pracy stanowi zatem teoretyczną podstawę dalszych analiz, będących fundamentem dla rozwoju własnych badań empirycznych i wypracowania innowacyjnych rozwiązań w zakresie ochrony informacji w systemach teleinformatycznych.

1.1 Klasy chronionych informacji

Podrozdział dotyczący klasyfikacji informacji niejawnych znalazł się w niniejszej rozprawie w celu ukazania, jak istotne jest odpowiednie kategoryzowanie informacji w kontekście ochrony danych. Klasy te, ustalone przez przepisy prawa, mają na celu zapewnienie, że poziom ochrony jest adekwatny do stopnia wrażliwości informacji. W kontekście tezy badawczej, która zakłada, że zbyt złożone systemy ochrony informacji mogą nie prowadzić do zwiększenia poziomu bezpieczeństwa, klasyfikacja informacji staje

się kluczowym punktem odniesienia. Perspektywa ta pozwala na zrozumienie, że właściwie dobrane mechanizmy ochrony mogą być bardziej efektywne niż nadmiernie skomplikowane i kosztowne systemy. Odpowiednie przypisanie klauzul tajności ma na celu nie tylko ochronę, ale także minimalizację zbędnych obciążeń i ryzyka, co jest kluczowe dla osiągnięcia optymalnego poziomu bezpieczeństwa w systemach teleinformatycznych.

Klasyfikację informacji niejawnych i jej znaczenie dla ochrony danych, analizował między innymi Dumitru [1] gdzie zwrócił uwagę, że proces klasyfikacji informacji jest elementem zapewnienia odpowiedniego poziomu ochrony danych, podkreślając znaczenie dostosowania mechanizmów ochrony do wrażliwości informacji.

Obecnie obowiązująca w Polsce *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* definiuje „klasy informacji" jako rozłączne podzbiory informacji. Klasy te określone są następująco:

- **Klasa J – JAWNE**

  Informacje oznaczone tą klasą są dostępne dla wszystkich użytkowników, niezależnie od ich uprawnień. Są to informacje publiczne, które nie są objęte żadnymi ograniczeniami dostępności.

- **Klasa Z – ZASTRZEŻONE**

  Informacje oznaczone tą klasą są ograniczone i dostępne tylko dla użytkowników posiadających odpowiednie uprawnienia. Są to informacje niejawne, które wymagają ochrony przed nieuprawnionym dostępem.

- **Klasa Pf – POUFNE**

  Dostępność informacji oznaczonych tą klasą jest jeszcze bardziej ograniczona niż w przypadku klasy Z. Dostęp do nich mają użytkownicy posiadający specjalne uprawnienia związane z konkretnymi potrzebami służbowymi.

- **Klasa 0 – TAJNE**

  Informacje oznaczone tą klasą są tajne i dostępne tylko dla użytkowników posiadających wysoki poziom uprawnień. Są to informacje o szczególnej wrażliwości, które muszą być ściśle chronione.

- **Klasa 00 – ŚCIŚLE TAJNE**

[1] Dumitru, I.-A. (2022). Classification of Information. International Journal of Information Security and Cybercrime, 11(1), 15–24. ijisc.com

Informacje oznaczone tą klasą są ściśle tajne i dostęp do nich mają tylko wyjątkowo upoważnione osoby. Są to najbardziej poufne informacje, które wymagają najwyższego stopnia ochrony.

Klasy te ustalają poziomy dostępności informacji dla użytkowników posiadających określone uprawnienia. Klasy informacji jako zbiory danych są uporządkowane hierarchicznie, wstępująco według opisanej kolejności, czyli Jawne, Zastrzeżone, Poufne, Tajne, Ściśle Tajne. Każdy użytkownik, który posiada uprawnienia dostępu do danej klasy, zatem daje rękojmię zachowania tajemnicy, ma również uprawnienia dostępu do wszystkich klas niższych w hierarchii.

W parze z rękojmią zachowania tajemnicy stoi nieodzowna zasada wiedzy uzasadnionej, która określa, że informacje niejawne powinny być udostępnione tylko tym osobom, które są upoważnione do ich otrzymania na podstawie konkretnych obowiązków służbowych lub zadań, którymi się zajmują. Celem zasady jest minimalizacja ryzyka ujawnienia poufnych informacji oraz kontrola dostępu do nich. Ograniczenie dostępu do tych informacji tylko do osób, które rzeczywiście ich potrzebują do wykonywania swoich obowiązków, zmniejsza potencjalne ryzyko wycieku poufnych danych lub wykorzystania ich w sposób niepożądany.

Hierarchiczna struktura klas informacji i uprawnienia dostępu do klas zapewnia odpowiednią kontrolę i ochronę informacji, zgodnie z ich stopniem poufności i wrażliwości.

Przy hierarchicznej klasyfikacji informacji niejawnych oraz zasad kontroli dostępu, warto odwołać się do pracy naukowej obejmującej przegląd modeli kontroli dostępu, w tym hierarchicznych struktur uprawnień, gdzie autorzy podkreślają znaczenie odpowiedniego przypisywania poziomów dostępu w celu minimalizacji ryzyka nieuprawnionego ujawnienia informacji[2].

W ustawie o ochronie informacji niejawnych wyróżniane są cztery klauzule tajności: "ściśle tajne", "tajne", "poufne" i "zastrzeżone". Przy nadawaniu klauzuli tajności uwzględnia się stopień wpływu danej informacji na bezpieczeństwo obywateli i kraju. Istnieje możliwość oznaczenia różnych części dokumentu (materiału) różnymi klauzulami tajności, w zależności od ich wrażliwości.[3]

---

[2] Farhadighalati, Nastaran, et al. "A Systematic Review of Access Control Models: Background, Existing Research, and Challenges." IEEE Access (2025).

[3] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2023 r. poz. 756, 1030).

Osoba, która jest uprawniona do podpisania dokumentu lub oznaczenia innego materiału, jest odpowiedzialna za nadanie odpowiedniej klauzuli tajności. W praktyce oznacza to, że nie zawsze jest to osoba, która sporządziła dokument, lecz często osoba, która dokonała podpisu, na przykład przełożony. Decyzja dotycząca nadania klauzuli tajności opiera się na ocenie ryzyka i właściwej klasyfikacji informacji, zgodnie z przepisami i wytycznymi dotyczącymi ochrony informacji niejawnych.

Nadanie właściwej klauzuli tajności ma na celu zapewnienie odpowiedniego poziomu ochrony informacji, tak aby zabezpieczyć je przed nieuprawnionym dostępem oraz nieuprawnionym ujawnieniem, a w konsekwencji chronić interesy obywateli i kraju w obszarze bezpieczeństwa. Jest to istotny element zapewnienia bezpieczeństwa państwowego.

Art. 5 ustawy o ochronie informacji niejawnych reguluje sposób przypisania klauzuli bezpieczeństwa. **Klauzula „Ściśle tajne”**, zgodnie z art. 5 ust. 1 ustawy o ochronie informacji niejawnych, jest nadawana informacjom niejawnym, których nieuprawnione ujawnienie może spowodować wyjątkowo poważną szkodę dla Rzeczypospolitej Polskiej. U podstaw przyjęcia tej klauzuli leżą zróżnicowane czynniki ryzyka lub zagrożenia, w szczególności:

- zagrożenie niepodległości, suwerenności lub integralności terytorialnej Rzeczypospolitej Polskiej, jeżeli ujawnienie informacji mogłoby zagrozić niepodległości, suwerenności lub integralności terytorialnej kraju,
- zagrożenie bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu Rzeczypospolitej Polskiej, jeżeli ujawnienie informacji stanowiłoby zagrożenie dla bezpieczeństwa wewnętrznego kraju lub porządku konstytucyjnego,
- zagrożenie sojuszy lub pozycji międzynarodowej Rzeczypospolitej Polskie, jeżeli ujawnienie informacji mogłoby zagrozić sojuszom lub pozycji międzynarodowej kraju,
- osłabienie gotowości obronnej Rzeczypospolitej Polskiej, jeżeli ujawnienie informacji mogłoby osłabić gotowość obronną kraju,
- zagrożenie identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu, a także innych osób wykonujących czynności operacyjno-rozpoznawcze oraz osób

udzielających im pomocy, jeśli zagraża to bezpieczeństwu wykonywanych czynności,

- zagrożenie życia lub zdrowia funkcjonariuszy, żołnierzy lub pracowników służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu, a także innych osób wykonujących czynności operacyjno-rozpoznawcze oraz osób udzielających im pomocy, jeżeli ujawnienie informacji mogłoby zagrażać życiu lub zdrowiu tych osób,
- zagrożenie życia lub zdrowia świadków koronnych lub osób im najbliższych, jeżeli ujawnienie informacji mogłoby zagrażać ich życiu lub zdrowiu.[4]

Klauzula „Tajne”, zgodnie z art. 5 ust. 2 ustawy o ochronie informacji niejawnych, nadawana jest informacjom wrażliwym, których nieuprawnione ujawnienie może spowodować poważną szkodę dla Rzeczypospolitej Polskiej. Przyjęcie tej klauzuli oparte jest na różnych przesłaniach, w szczególności:

- uniemożliwienie realizacji zadań związanych z ochroną suwerenności lub porządku konstytucyjnego Rzeczypospolitej Polskiej, jeżeli ujawnienie informacji uniemożliwiłoby skuteczną realizację zadań związanych z ochroną suwerenności lub porządku konstytucyjnego kraju,
- pogorszenie stosunków Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi, w przypadku, gdy ujawnienie informacji mogłoby prowadzić do pogorszenia stosunków między Polską a innymi państwami lub organizacjami międzynarodowymi,
- zakłócenie przygotowań obronnych państwa lub funkcjonowania Sił Zbrojnych Rzeczypospolitej Polskiej, jeśli ujawnienie informacji zakłóciłoby przygotowania obronne kraju lub funkcjonowanie Sił Zbrojnych,
- utrudnienie wykonywania czynności operacyjno-rozpoznawczych oraz ścigania sprawców zbrodni, w przypadku, gdy ujawnienie informacji utrudniłoby wykonywanie czynności operacyjno-rozpoznawczych mających na celu zapewnienie bezpieczeństwa państwa lub ściganie sprawców zbrodni przez uprawnione służby lub instytucje,

[4] K. Mordaszewski, D. Laskowski, Prawne aspekty ochrony informacji. Wybrane zagadnienia, w „Nowe Techniki badań kryminalistycznych a bezpieczeństwo informacji, red. B. Hołyst, J. Pomykała, P. Potejko. PWN. 2014, s. 23.

- zakłócenie funkcjonowania organów ścigania i wymiaru sprawiedliwości, jeżeli ujawnienie informacji w istotny sposób zakłóciłoby funkcjonowanie organów ścigania i wymiaru sprawiedliwości,
- przyniesienie znacznej straty interesom ekonomicznym Rzeczypospolitej Polskiej, w przypadku, gdy ujawnienie informacji przyniosłoby znaczne straty interesom ekonomicznym kraju.

Klauzula „Poufne”, zgodnie z art. 5 ust. 3 ustawy o ochronie informacji niejawnych, jest nadawana informacjom niejawnym, których nieuprawnione ujawnienie może spowodować szkodę dla Rzeczypospolitej Polskiej. W tym przypadku, szkoda nie musi być poważna czy wyjątkowo poważna, ale nadal istotna. Potencjalne kategorie szkód, które wymagają nadania klauzuli "poufne" to:

- utrudnienie prowadzenia bieżącej polityki zagranicznej Rzeczypospolitej Polskiej, jeżeli ujawnienie informacji utrudniłoby prowadzenie bieżącej polityki zagranicznej kraju,
- utrudnienie realizacji przedsięwzięć obronnych lub negatywny wpływ na zdolność bojową Sił Zbrojnych, jeśli ujawnienie informacji utrudniłoby realizację przedsięwzięć obronnych lub negatywnie wpłynęłoby na zdolność bojową Sił Zbrojnych,
- zakłócenie porządku publicznego lub zagrożenie bezpieczeństwu obywateli, w przypadku, gdy ujawnienie informacji zakłóciłoby porządek publiczny lub stanowiłoby zagrożenie dla bezpieczeństwa obywateli,
- utrudnienie wykonywania zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów Rzeczypospolitej Polskiej, jeżeli ujawnienie informacji utrudniłoby wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów kraju,
- utrudnienie wykonywania zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości, gdy ujawnienie informacji utrudniłoby wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych, oraz organom wymiaru sprawiedliwości,

- zagrożenie stabilności systemu finansowego Rzeczypospolitej Polskiej, gdy ujawnienie informacji zagroziłoby stabilności systemu finansowego w kraju.

Klauzula „Zastrzeżone”, zgodnie z art. 5 ust. 4 ustawy o ochronie informacji niejawnych, jest nadawana informacjom niejawnym, którym nie przypisano wyższej klauzuli tajności. Nadawanie klauzuli "zastrzeżone" jest uzasadnione, gdy nieuprawnione ujawnienie tych informacji może mieć szkodliwy wpływ na wykonywanie zadań przez organy władzy publicznej lub inne jednostki organizacyjne w zakresie:

- obrony narodowej,
- polityki zagranicznej,
- bezpieczeństwa publicznego,
- przestrzegania praw i wolności obywateli,
- wymiaru sprawiedliwości,
- interesów ekonomicznych Rzeczypospolitej Polskiej.

Klauzula "zastrzeżone" jest stosowana dla informacji, które nie spełniają kryteriów wymaganych do nadania wyższych klauzul tajności, ale nadal mają znaczenie dla wymienionych obszarów działania organów publicznych.

1.2 Ochrona wiedzy w systemach teleinformatycznych

Podrozdział ukazuje fundamentalne znaczenie ochrony informacji dla funkcjonowania jednostek organizacyjnych. W szczególności, podkreśla on, że bezpieczeństwo informacji w systemach teleinformatycznych opiera się na zapewnieniu poufności, integralności i dostępności danych. W kontekście tezy zakładającej, że zbyt złożone systemy ochrony informacji mogą nie zwiększać poziomu bezpieczeństwa, analiza ta jest niezbędna do zrozumienia, które elementy systemu rzeczywiście przyczyniają się do ochrony, a które mogą jedynie komplikować zarządzanie bezpieczeństwem, nie dostarczając jednocześnie bez realnych czy istotnych korzyści. Podrozdział ten pozwala zbadać, czy bardziej przemyślane i ukierunkowane podejście do ochrony danych – zamiast nadmiernej złożoności – może prowadzić do równie skutecznej, a nawet lepszej ochrony informacji w systemach teleinformatycznych.

Wiedza ma istotne znaczenie dla danej jednostki organizacyjnej i wymaga ochrony w celu zapewnienia rentowności i ciągłości jej funkcjonowania.[5] To właśnie wiedza jest najważniejszym czynnikiem w osiąganiu sukcesu i jest elementem przyczyniającym się do wzrostu wartości przedsiębiorstwa. Bezpieczeństwo informacji w systemach teleinformatycznych oznacza, że są one chronione przed nieautoryzowanym odczytem, usunięciem lub zmianą, i jednocześnie zawsze dostępne dla uprawnionego użytkownika systemu.[6]

Bezpieczna informacja to taka informacja, która spełnia następujące warunki:

1. **Poufność** – która oznacza, że jedynie osoby uprawnione mają możliwość uzyskania dostępu do niej.
2. **Integralność –** która oznacza, że informacja pozostaje nietknięta i niezmieniona w stosunku do pierwotnego stanu, w jakim została utworzona przez autora, i żadna nieuprawniona osoba nie może niezauważenie zmienić jej zawartości.
3. **Dostępność** – która oznacza, że osoby uprawnione mają możliwość uzyskania dostępu do informacji na żądanie.

Sposób i poziom spełnienie tych warunków może się różnić w zależności od rodzaju systemu, wykorzystywanych klauzul informacji a także ich znaczenia w danej jednostce organizacyjnej. Bezpieczny system teleinformatyczny to taki, który zapewnia ochronę danych, które są w nim przetwarzane.[7] Aby to osiągnąć, system musi posiadać mechanizmy do monitorowania dostępu użytkowników do informacji, sprawdzania ich tożsamości oraz autentykacji. Co więcej, system powinien być odporny zarówno na nieuprawnione manipulacje z zewnątrz, jak i celowe bądź przypadkowe manipulacje użytkowników wewnętrznych Ważne jest, aby system działał niezawodnie. Konieczne są także odpowiednie środki zabezpieczające, które obejmują aspekty fizyczne, techniczne, organizacyjne i proceduralne. Wprowadzenie odpowiedniej polityki ochrony informacji, dostosowanej do specyficznych potrzeb danej jednostki organizacyjnej, stanowi kolejny niezbędny krok w zapewnieniu bezpieczeństwa danych przetwarzanych w systemach teleinformatycznych. Związane jest to także z utworzeniem specjalnych struktur

[5] Skrzypek, E. "Kapitał intelektualny jako czynnik stymulujący rozwój przedsiębiorstwa,[w:] S. Partycki (red.)." Strategia rozwoju społecznej gospodarki rynkowej w Polsce (2002), s. 35.

[6] R. J. Sutton, Bezpieczeństwo telekomunikacji Praktyka i Zarządzanie, wyd. WKŁ. 2004, s. 17.

[7] Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego

organizacyjnych, na przykład pionu ochrony informacji niejawnych, aby efektywnie zarządzać bezpieczeństwem teleinformatycznym i chronić dane przed nieuprawnionymi dostępami oraz celowymi lub przypadkowymi manipulacjami. Wszystkie te działania łącznie tworzą kompleksową i skuteczną ochronę informacji przetwarzanych elektronicznie.

1.3 Informacje wrażliwe

Podrozdział definiuje i klasyfikuje informacje, które ze względu na swoją naturę wymagają szczególnej ochrony. Opis tych informacji pozwala zrozumieć, dlaczego pewne dane są bardziej podatne na zagrożenia i jakie konsekwencje może mieć ich nieuprawnione ujawnienie. W kontekście tezy zakładającej, że zbyt złożone systemy ochrony mogą nie zawsze zwiększać poziomu bezpieczeństwa, analiza kategorii informacji wrażliwych pozwala ocenić czy obecne mechanizmy ochrony są proporcjonalne do poziomu ryzyka. Podrozdział ten pomaga także zidentyfikować, które informacje wymagają zastosowania zaawansowanych zabezpieczeń, a które mogą być chronione w sposób bardziej uproszczony, co może prowadzić do bardziej efektywnego i skutecznego zarządzania bezpieczeństwem w systemach teleinformatycznych.

Informacja może być definiowana na różne sposoby, w zależności od dziedziny i kontekstu, w którym jest używana.

W teorii informacji opracowanej przez Shannona informacja jest miarą redukcji niepewności. Autor zdefiniował on ją jako odwróconą wartość prawdopodobieństwa wystąpienia danego zdarzenia. Informacja jest większa, gdy zdarzenie jest mniej prawdopodobne.[8] Informacja może być też rozumiana jako mierzalna ilość danych, przekaz znaczenia lub treść przetwarzana przez umysł.

Z kolei Hołyst i Pomykała definiują informację jako zbiór danych, faktów lub treści, które przekazują lub reprezentują pewne informacje o świecie. Może ona być zapisana w różnych formach, takich jak tekst, dźwięk, obraz czy dane numeryczne. Informacja ma na celu przekazywanie wiedzy, powiadomień lub komunikacji między osobami czy systemami.[9]

---

[8]Shannon, Claude E. "A mathematical theory of communication." The Bell system technical journal 27.3 (1948): 379-423.

[9] B. Hołyst, J. Pomykała, Cyberprzestępczość i kryptograficzna ochrona informacji, [w:] Metody biometryczne i kryptograficzne w zintegrowanych systemach bezpieczeństwa, red. B. Hołyst, J. Pomykała, wyd. WSM. 2021, str. 63.

Informacja może być podstawą podejmowania decyzji, rozwiązywania problemów, zdobywania wiedzy i porozumiewania się. Przetwarzanie informacji, z kolei, obejmuje gromadzenie, analizę, interpretację, przechowywanie i przekazywanie danych w celu uzyskania mających znaczenie informacji.

Podstawowymi elementami informacji są znaki lub symbole, które mają określone znaczenie i są zrozumiałe dla odbiorcy. Informacja może być przekazywana za pomocą różnych środków komunikacji, takich jak język mówiony, pismo, komunikacja elektroniczna, telefonia, Internet, media drukowane, radio, telewizja.[10]

Współczesna technologia informacyjna umożliwia przechowywanie, przetwarzanie i przesyłanie ogromnych ilości informacji w bardzo szybki sposób. Informacja odgrywa kluczową rolę we wszystkich dziedzinach życia, od nauki i biznesu po media społecznościowe i rozrywkę.

W dzisiejszym świecie informacja i wiedza są traktowane jako nowy rodzaj towaru, porównywalny z dobrami materialnymi czy źródłami energii. Współczesne społeczeństwo globalne, zwane społeczeństwem informacyjnym, jest silnie związane z Internetem i innymi masowymi źródłami informacji. Termin "informacja" w tym kontekście odnosi się nie tylko do faktów lub domniemanej wiedzy, ale także do reguł preferencji w różnych dziedzinach, takich jak ważność i użyteczność. W praktyce, gdy informujemy kogoś o kimś lub czymś, przekazujemy mu fakty lub dzielimy się naszą wiedzą i preferencjami na ten temat.[11]

Informacja wrażliwa odnosi się do informacji, która jest szczególnie ważna, poufna, chroniona prawnie lub wrażliwa na dostęp, udostępnienie lub wykorzystanie przez nieuprawnione osoby. Może to obejmować takie informacje jak dane osobowe, tajemnice handlowe, poufne informacje rządowe, dane medyczne czy informacje bankowe.[12]

Definicja informacji wrażliwej może różnić się w zależności od kontekstu i regulacji prawnych. W wielu przypadkach istnieją specjalne zasady i przepisy dotyczące ochrony i bezpieczeństwa informacji wrażliwej, które mają na celu zapobieganie jej nieuprawnionemu ujawnieniu, utracie lub nadużyciu.

---

[10] T. Polaczek, Audyt bezpieczeństwa informacji, Helion, 2014.

[11] B. Hołyst, J. Pomykała, Cyberprzestępczość i kryptograficzna ochrona informacji, [w:] Metody biometryczne i kryptograficzne w zintegrowanych systemach bezpieczeństwa, red. B. Hołyst, J. Pomykała, wyd. WSM. 2021, s. 54-55.

[12] B. Hołyst, Kryminalistyka, wyd. Wolters Kluwer, s. 1350-1359, Warszawa, 2023.

W przypadku organizacji i przedsiębiorstw, informacja wrażliwa często wymaga szczególnych środków ochrony, takich jak uwierzytelnianie, szyfrowanie, kontrola dostępu oraz ścisłe zasady bezpieczeństwa. Nieupoważnione ujawnienie takiej informacji może prowadzić do poważnych konsekwencji, w szczególności naruszenie prywatności, utrata zaufania, straty finansowe czy kary prawne. Z tego powodu ważne jest, aby odpowiednio identyfikować, klasyfikować i chronić informacje wrażliwe, to znaczy zapewnić ich poufność, integralność i dostępność tylko dla uprawnionych osób.

1.4 Motywacja ochrony informacji

Ten podrozdział jest istotny w kontekście badanej tezy, ponieważ ukazuje, dlaczego organizacje decydują się na wprowadzenie zabezpieczeń w swoich systemach teleinformatycznych. Zrozumienie motywacji stojących za ochroną informacji ma wpływ na ocenę czy zastosowane środki bezpieczeństwa są adekwatne i proporcjonalne do zagrożeń. W kontekście tezy zakładającej, że zbyt złożone systemy ochrony mogą nie przynosić oczekiwanych korzyści, analiza motywacji pozwala zbadać, w jakim stopniu polityka bezpieczeństwa i potrzeby organizacji wpływają na projektowanie systemów ochrony. Pozwala to także w ustaleniu czy istniejące mechanizmy zabezpieczające rzeczywiście służą ochronie kluczowych zasobów, czy też mogą prowadzić do nadmiernej komplikacji, która niekoniecznie przekłada się na wyższy poziom bezpieczeństwa.

Wprowadzenie zabezpieczeń do systemu teleinformatycznego powinno uwzględniać potrzeby związane z ochroną przetwarzanych w nim informacji. Najlepiej aby te zdefiniowane potrzeby zawrzeć w polityce bezpieczeństwa informacji danej jednostki organizacyjnej lub całej organizacji. Polityka bezpieczeństwa informacji określa czy i jak istotne jest bezpieczeństwo informacji w działalności organizacji, a także wskazuje, które zasoby – informacyjne, materialne, niematerialne – są szczególnie wrażliwe, a ich naruszenie mogłoby spowodować poważne straty lub konsekwencje dla organizacji.

Zapewnienie bezpieczeństwa uzależnione jest od rodzaju działalności prowadzonej przez organizację oraz stopnia, w jakim ta działalność jest uzależniona od elektronicznego przetwarzania informacji. Zależy również od wielkości organizacji, środowiska eksploatacji, jak również jej kultury organizacyjnej. Dla każdej jednostki organizacyjnej opracowywany jest specyficzny zestaw zasad, celów i wymagań dotyczących przetwarzania informacji w systemach teleinformatycznych. Ten szczegółowy plan stanowi uzasadnienie dla potrzeby zapewnienia bezpieczeństwa i jest dostosowany do konkretnych wymagań tej jednostki.

Potrzeby ochrony informacji w organizacji mogą również wynikać z wymogów ustawowych, takich jak ustawa o ochronie informacji niejawnych czy ustawa o ochronie danych osobowych. Wymogi ustawowe nakładają obowiązek zapewnienia bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych. Przykładem takiego wymogu jest konieczność uzyskania zgody administracyjnej w celu przetwarzania informacji o charakterze poufnym. Takie zgody wydaje Służba Kontrwywiadu Wojskowego dla sektora wojskowego oraz Agencja Bezpieczeństwa Wewnętrznego odpowiednio dla sektora prywatnego.

W sytuacjach, gdy przetwarzane informacje nie są objęte prawną ochroną, potrzeba ochrony może wynikać z wymogów statutowych, umów, kontraktów oraz zobowiązań wobec partnerów handlowych, kontrahentów i dostawców usług. Decyzje dotyczące poziomu ochrony tych informacji zależą od kierownictwa organizacji oraz od uzgodnień z partnerami biznesowymi.

Przy motywacji organizacji do wdrażania zabezpieczeń w systemach teleinformatycznych oraz wpływu polityki bezpieczeństwa informacji na projektowanie tych systemów badanie Hong, Yuxiang, i Steven Furnell [13] analizuje, jak postrzegana formalizacja organizacyjna wpływa na intencje pracowników dotyczące przestrzegania polityki bezpieczeństwa informacji, sugerując, że jasno określone zasady i procedury mogą zwiększać zgodność z polityką bezpieczeństwa.

Identyfikacja potencjalnych zagrożeń i analiza podatności systemu wobec tych zagrożeń stanowią etap w tworzeniu skutecznych strategii ochrony systemów teleinformatycznych. Działania te są niezwykle istotne z kilku powodów. Po pierwsze, umożliwiają skuteczne zarządzanie ryzykiem. Analiza podatności pozwala dokładnie ocenić jakie ryzyko niesie ze sobą dane zagrożenie dla systemu. To z kolei pozwala na opracowanie adekwatnych strategii zarządzania ryzykiem, podejmowanie decyzji dotyczących alokacji zasobów na ochronę, implementację kontroli bezpieczeństwa i planowanie działań reakcyjnych.

Po drugie, działania te umożliwiają dostosowanie strategii ochrony do konkretnych zagrożeń i podatności. Systemy komputerowe mogą mieć różne słabe punkty, dlatego ważne

[13] Hong, Yuxiang, and Steven Furnell. "Motivating information security policy compliance: Insights from perceived organizational formalization." Journal of Computer Information Systems 62.1 (2022): 19-28.

jest, aby strategie ochrony były dostosowane do specyficznych zagrożeń. Dzięki identyfikacji zagrożeń możliwe staje się opracowanie spersonalizowanych strategii ochrony.

Po trzecie, analiza podatności i zagrożeń pozwala na efektywne wykorzystanie zasobów. Znając potencjalne zagrożenia i podatności, można zoptymalizować alokację dostępnych zasobów. Skierowanie ich tam, gdzie ryzyko jest większe, przyczynia się do efektywnego wykorzystania zasobów finansowych, ludzkich i technologicznych.

Po czwarte, analiza podatności systemu zwiększa świadomość zagrożeń w samej organizacji. Pracownicy stają się bardziej uważni na możliwe ryzyka i wiedzą, jak należy reagować w przypadku wystąpienia konkretnych zagrożeń.

Wreszcie, identyfikacja zagrożeń i podatności pozwala na skuteczne planowanie i prewencję. Na tej podstawie można opracować plany reagowania na potencjalne incydenty oraz wprowadzić odpowiednie środki prewencyjne. Działania te przyczyniają się do znaczącego zmniejszenia ryzyka wystąpienia incydentu.

Analiza podatności i identyfikacja zagrożeń to niezwykle istotne elementy procesu ochrony systemów komputerowych. Stanowią one fundament dla skutecznej strategii zapewnienia bezpieczeństwa systemu.

1.5 Klasyfikacja i zawartość metadanych plików cyfrowych

Podrozdział ten jest istotny w kontekście badanej tezy, ponieważ metadane odgrywają priorytetową rolę w zarządzaniu i ochronie informacji w systemach teleinformatycznych. Analiza klasyfikacji i zawartości metadanych umożliwia zrozumienie, w jaki sposób informacje o plikach – takie jak data utworzenia, autor czy poziom poufności – mogą wpływać na skuteczność zabezpieczeń. W kontekście tezy zakładającej, że zbyt złożone systemy ochrony mogą nie przynosić oczekiwanych korzyści, podrozdział ten pozwala ocenić, czy właściwe zarządzanie metadanymi może stanowić efektywną alternatywę dla bardziej skomplikowanych mechanizmów ochrony. Wartym uwagi jest praca[14] Meghanandha i Umesha Naik gdzie szczegółowo analizują standardy metadanych, ich rolę w organizacji i ochronie informacji, a także interoperacyjności w systemach teleinformatycznych. W swojej pracy podkreślają znaczenie takich standardów jak MARC,

[14] Meghanandha, Umesha Naik. "A Comparative Review of Metadata, Communication, Content, and Digital Preservation Standards in Modern Libraries." American Journal of Information Science and Technology, vol. 9, no. 1, Feb. 2025, pp. 24–33. Science Publishing Group, DOI:10.11648/j.ajist.20250901.13.

Dublin Core czy PREMIS w zarządzaniu danymi oraz ich wpływ na efektywność zabezpieczeń cyfrowych.

Dodatkowo, klasyfikacja metadanych jest kluczowa dla zapewnienia, że tylko uprawnione osoby mają dostęp do danych, co jest centralnym elementem każdego systemu bezpieczeństwa informacji.

W przypadku, gdy opis zawartości dokumentu w metadanych zawierałby informacje określone w art. 5 ust. 1, 2, 3 lub 4 ustawy o ochronie informacji niejawnych to metadanym nadajemy klauzule. Metadane zawierające opis zawartości dokumentu powoduje nadanie im klauzuli:

1. dla dokumentów Zastrzeżonych - metadane z opisem zawartości są jawne,
2. dla dokumentów Poufnych, Tajnych, Ściśle Tajnych – metadane z opisem zawartości są zastrzeżone za wyjątkiem przesłanek określonych w art. 5 ust. 1, 2 i 3 ustawy o ochronie informacji niejawnych.

W praktyce przy dokumentach kancelaryjnych opis zawartości przygotowuje się tak, aby maksymalna klauzula była zastrzeżona.

Metadane pliku powinny zawierać wszelkie informacje identyfikujące dokument niejawny. Zakres wskazanych pozycji jest następujący:

- symbol oznaczenia klauzuli tajności (puste – jako jawne, Z, Pf, 0 lub 00),
- numer kolejny zapisu (numer pozycji),
- adnotacje dotyczące obowiązywania klauzuli tajności, jej zniesienia albo zmiany,
- data rejestracji dokumentu,
- nazwa nadawcy i adresata lub wpis „dokument własny”,
- numer i data dokumentu otrzymanego,
- nazwa dokumentu lub czego dotyczy,
- liczba egzemplarzy wytworzonego dokumentu,
- liczba stron dokumentu lub innych jednostek miary,
- liczba załączników,
- liczba stron wszystkich załączników lub innych jednostek miary,
- nr dokumentu, z którego wykonano wydruk, kopię, wyciąg, wypis, odpis, tłumaczenie, lub numer nośnika,
- imię i nazwisko lub inne dane identyfikujące wykonawcę dokumentu,
- data, imię i nazwisko oraz podpis osoby pobierającej dokument przy czym podpis stosujemy przy papierowej wersji dokumentu, w cyfrowym spisie pozycji

zastosować należy oddzielną kartę zapoznania się z dokumentem dla wszystkich pozycji, nie tylko dla tajnych i ściśle tajnych, których jest to konieczne,

- potwierdzenie zwrotu dokumentu – data i podpis w karcie zapoznania się z dokumentem,
- adnotacje o wykonaniu dokumentu lub załącznika (pozycja w książce doręczeń przesyłek miejscowych lub pozycja wykazu przesyłek nadanych lub załącznik do pisma,
- adnotacje o wybrakowaniu lub przekazaniu do archiwum,
- informacje uzupełniające, uwagi (np. symbol klasyfikacyjny wykazu akt)[15].

1.6 Cykl funkcjonowania chronionego systemu teleinformatycznego

Podrozdział tan opisuje pełny proces, przez który przechodzi system teleinformatyczny, od jego projektowania przez eksploatację do wycofania z użytku. Zrozumienie tego cyklu jest niezbędne do oceny, w jaki sposób różne etapy życia systemu wpływają na skuteczność stosowanych środków ochrony. W kontekście tezy zakładającej, że zbyt złożone systemy ochrony mogą nie zwiększać poziomu bezpieczeństwa, analiza cyklu funkcjonowania systemu pozwala na zbadanie, które etapy mogą być narażone na nadmierną komplikację, a które wymagają prostszych i bardziej efektywnych rozwiązań. Pozwala to na identyfikację momentów, w których strategiczne, ale nieskomplikowane podejście do ochrony może być wystarczające, co jest zgodne z zasadą, że prostsze rozwiązania mogą czasem być bardziej skuteczne i łatwiejsze do zarządzania w dłuższej perspektywie.

Wartym uwagi jest praca Mykoniati i Lambrinoudakis[16] która przedstawia cykl życia systemów telekomunikacyjnych z uwzględnieniem ich odporności na awarie oraz kompleksowo analizuje etapy projektowania, testowania i eksploatacji systemów w kontekście zapewnienia ich przetrwania w trudnych warunkach operacyjnych.

[15] Rozporządzenie rady ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych

[16] Mykoniati, Maria, i Costas Lambrinoudakis. "Software Development Lifecycle for Survivable Mobile Telecommunication Systems." Advances in Science, Technology and Engineering Systems Journal, vol. 6, no. 4, 2021, pp. 259–277. DOI: 10.25046/aj060430.

Bezpieczeństwo informacji niejawnych przetwarzanych w systemie teleinformatycznym należy uwzględnić we wszystkich etapach cyklu funkcjonowania tego systemu, które obejmują[17]:

1. **Planowanie**

   W tym etapie należy uwzględnić wymagania bezpieczeństwa informacji niejawnych i określić odpowiednie środki ochrony, procedury oraz zasady postępowania. Na etapie planowania określamy przeznaczenie systemu teleinformatycznego, maksymalną klauzulę tajności informacji niejawnych, które będą przetwarzane w systemie teleinformatycznym, tryb bezpieczeństwa pracy systemu teleinformatycznego, szacunkową liczbę użytkowników oraz planowaną lokalizację.

2. **Projektowanie**

   Przy projektowaniu systemu teleinformatycznego należy uwzględnić aspekty bezpieczeństwa informacji, takie jak kontrola dostępu, szyfrowanie danych i zabezpieczenia sieciowe. Na tym etapie przeprowadza się wstępne szacowanie ryzyka dla bezpieczeństwa informacji niejawnych w celu określenia wymagań dla zabezpieczeń, dokonuje się wyboru zabezpieczeń dla systemu teleinformatycznego w oparciu o wyniki wstępnego szacowania ryzyka dla bezpieczeństwa informacji niejawnych, uzgadnia się z podmiotem akredytującym plan akredytacji obejmujący zakres i harmonogram przedsięwzięć wymaganych do uzyskania akredytacji bezpieczeństwa teleinformatycznego, uzgadnia się z podmiotem zaopatrującym w klucze kryptograficzne rodzaj oraz ilość niezbędnych urządzeń lub narzędzi kryptograficznych, a także sposób ich wykorzystania, oraz opracowuje się dokument szczególnych wymagań bezpieczeństwa.

3. **Wdrażanie**

   Podczas implementacji systemu należy zadbać o prawidłowe wdrożenie środków ochrony, przeprowadzenie testów bezpieczeństwa oraz odpowiednie szkolenie personelu w zakresie ochrony informacji niejawnych. Na tym etapie pozyskuje i wdraża się urządzenia lub narzędzia realizujące zabezpieczenia w systemie

[17] Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego.

teleinformatycznym, przeprowadza się testy bezpieczeństwa systemu teleinformatycznego, przeprowadza się szacowanie ryzyka dla bezpieczeństwa informacji niejawnych z uwzględnieniem wprowadzonych zabezpieczeń, opracowuje się dokument procedur bezpiecznej eksploatacji oraz uzupełnia się dokument szczególnych wymagań bezpieczeństwa. Finalnie, system teleinformatyczny poddaje się akredytacji bezpieczeństwa teleinformatycznego.

4. **Eksploatacja**

   W trakcie codziennego funkcjonowania systemu teleinformatycznego należy monitorować i zarządzać bezpieczeństwem informacji, reagować na incydenty bezpieczeństwa oraz regularnie aktualizować i audytować środki ochrony.

5. **Likwidacja**

   Podczas wycofywania systemu z eksploatacji należy zapewnić bezpieczne usunięcie i zniszczenie informacji niejawnych oraz odpowiednie zabezpieczenie danych przed nieuprawnionym dostępem.

1.7 Wartościowanie bezpieczeństwa informacji

Podrozdział ten dostarcza kluczowych informacji na temat metod określania miar odporności systemów teleinformatycznych. Zrozumienie tych metod umożliwi dalsze badanie czy bardziej rozbudowane rozwiązania ochronne rzeczywiście oferują lepszą ochronę, czy też mogą okazać się mniej skuteczne w porównaniu do prostszych, ale lepiej dopasowanych mechanizmów ochrony.

Użytkownicy oraz kadra zarządzająca firm i instytucji, chcąc upewnić się, że systemy teleinformatyczne, z których korzystają, są odpowiednio zabezpieczone i chronią dane w sposób właściwy, powinni przeprowadzić proces oceny bezpieczeństwa tych systemów. W ramach takiej oceny analizowane są szczegółowo możliwe słabe punkty w zabezpieczeniach oraz identyfikowane są potencjalne zagrożenia, które mogą wpłynąć na bezpieczeństwo danych. Proces ten obejmuje analizę zabezpieczeń fizycznych, takich jak kontrola dostępu, oraz ocenę środków technicznych, które mają chronić system przed zagrożeniami.[18]

Ochrona informacji dotyczy kompleksowego zagadnienia obejmującego bezpieczeństwo informacyjne. Ten obszar obejmuje wszelkie sposoby przekazywania

[18] ISO/IEC 27001:2013 Information Security Management Systems (ISMS)

informacji, w tym także komunikację werbalną. Celem jest zapewnienie bezpiecznej i poufnej transmisji informacji, niezależnie od formy, w jakiej się odbywa.

Bezpieczeństwo teleinformatyczne skupia się na ochronie informacji przetwarzanych, przechowywanych i przesyłanych przez systemy teleinformatyczne. Podstawowe elementy bezpieczeństwa informacji to tajność, integralność i dostępność. Tajność chroni przed dostępem osób nieuprawnionych, integralność zapewnia, że dane są nienaruszone, a dostępność umożliwia korzystanie z danych na żądanie.

System bezpieczeństwa powinien łączyć różne rodzaje zabezpieczeń: organizacyjne, kadrowe, fizyczne, techniczne oraz sprzętowo-programowe. Jednocześnie, powinien być zdolny do wykrywania i zapobiegania incydentom bezpieczeństwa.

Wartościowanie czy też ocena poziomu bezpieczeństwa teleinformatycznego polega na określeniu odporności systemu na czynniki mogące zagrażać poufności, integralności i dostępności danych. Wynik tej oceny to raport z opisem testów mających potwierdzić lub zaprzeczyć podatnościom systemu. Miary odporności określa się na podstawie standardów, na przykład Evaluation Assurance Level (EAL) w Common Criteria lub klas bezpieczeństwa D, C, B, A w TCSEC (Trusted Computer System Evaluation Criteria). Proces oceny bezpieczeństwa można przeprowadzić wewnętrznie, jeśli organizacja ma odpowiednie kompetencje, lub zlecić zewnętrznemu, niezależnemu zespołowi.

Temat wartościowania bezpieczeństwa informacji pozostaje nadal niezwykle istotny i aktualny w dzisiejszym środowisku cyfrowym. Wraz z rosnącą złożonością systemów teleinformatycznych oraz dynamicznie rozwijającymi się zagrożeniami cybernetycznymi, konieczne jest ciągłe doskonalenie metod oceny i zarządzania ryzykiem bezpieczeństwa. Jak pokazują badania, takie jak te opublikowane w czasopiśmie[19] Electronics w 2022 roku, rozwój ram i standardów bezpieczeństwa informacji jest kluczowy dla zapewnienia skutecznej ochrony danych w organizacjach. W związku z tym, temat ten nadal jest przedmiotem badań naukowych i praktycznych wdrożeń, co potwierdza jego istotną rolę w dziedzinie bezpieczeństwa informacji. Temat również omówiony został przez

[19] Hamed Taherdoost, Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview, Electronics 2022, 11(14), 2181; https://doi.org/10.3390/electronics11142181

Ciekanowskiego i Starczewskiego [20] w pracy zawarto uwarunkowania bezpieczeństwa zarówno informacji, jak i systemów teleinformatycznych, ze szczególnym uwzględnieniem instrukcji zarządzania systemem teleinformatycznym oraz ochrony fizycznej procesu przetwarzania informacji niejawnych.

1.8 Wytyczne zapewnienia bezpieczeństwa informacji

W tym podrozdziale będą przedstawione kluczowe wytyczne oraz standardy dotyczące zapewnienia bezpieczeństwa informacji, które mogą pomóc w zrozumieniu, jakie praktyki i zasady są rekomendowane do skutecznej ochrony danych. Analiza tych wytycznych pozwoli na ocenę czy zaawansowane rozwiązania ochronne rzeczywiście przynoszą korzyści w zakresie bezpieczeństwa, czy też ich złożoność może wprowadzać dodatkowe wyzwania. Dzięki tym informacjom możliwe będzie lepsze zrozumienie czy i w jaki sposób złożoność systemów ochrony wpływa na poziom zabezpieczeń w kontekście rzeczywistych potrzeb organizacji.

Wyróżniamy dwie grupy standardów z zakresu bezpieczeństwa systemów teleinformatycznych. [21] Pierwszy to standardy umożliwiające certyfikację systemów i produktów teleinformatycznych takie jak:

1. ISO 15408 (Common Criteria) – międzynarodowy standard oceny bezpieczeństwa systemów informatycznych, który określa ogólne wymagania dotyczące bezpieczeństwa i umożliwia porównywanie i certyfikację systemów informatycznych.[22]
2. ITSEC (Information Technology Security Evaluation Criteria) – europejski standard oceny bezpieczeństwa systemów teleinformatycznych, który zawiera kryteria oceny bezpieczeństwa i zasady testowania systemów, umożliwiając certyfikację.[23]

---

[20] Ciekanowski, Zbigniew, i Jarosław Starczewski. "Uwarunkowania bezpieczeństwa informacji i systemów teleinformatycznych." Współczesne Problemy Zarządzania, vol. 6, no. 1(12), 2018, pp. 151–160. DOI: 10.52934/wpz.111.

[21] K. Liderman, Standardy w ocenie bezpieczeństwa teleinformatycznego, Biuletyn Instytutu Automatyki i Robotyki, 17/2002.

[22] Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408-1:2022.

[23] Information Technology Security Evaluation Criteria (ITSEC), 1991.

Drugi to standardy stanowiące dobre praktyki, które nie są przeznaczone do bezpośredniej certyfikacji systemów, ale służą jako zbiory zaleceń i wytycznych dotyczących najlepszych praktyk w dziedzinie bezpieczeństwa teleinformatycznego. Przykłady takich standardów to:

3. ISO 27001 – międzynarodowy standard zarządzania bezpieczeństwem informacji, który określa wymagania i procesy zarządzania bezpieczeństwem informacji w organizacji.[24]
4. NIST SP 800-53 – standard opracowany przez National Institute of Standards and Technology (NIST) w Stanach Zjednoczonych, który zawiera zbiór zasad kontroli bezpieczeństwa, które można zastosować do systemów teleinformatycznych.[25]
5. CIS Controls – zestaw kontroli bezpieczeństwa opracowany przez organizację Center for Internet Security (CIS), który stanowi praktyczny przewodnik dla organizacji w celu ochrony systemów przed cyber-zagrożeniami.[26]

Obie grupy standardów mają swoje unikalne zastosowania i służą jako wytyczne do zapewnienia bezpieczeństwa w dziedzinie teleinformatyki.

Cechą charakterystyczną standardów z grupy pierwszej, takich jak ITSEC, Common Criteria czy opisany dalej TCSEC, jest podawanie miar w postaci określonych klas, poziomów lub EAL (Evaluation Assurance Level). Miary te służą do klasyfikacji systemów i produktów pod względem ich poziomu bezpieczeństwa lub stopnia spełnienia określonych wymagań.

W przypadku standardów z grupy drugiej, takich jak ISO 27001, NIST SP 800-53, CIS Controls), nie wystawia się certyfikatów, ponieważ nie definiują one konkretnych miar lub klas bezpieczeństwa, dla których można by przeprowadzić formalną certyfikację. Zamiast tego standardy te stanowią zbiór zaleceń, wytycznych i zasad kontroli bezpieczeństwa, które organizacje mogą wdrażać jako część swojego systemu zarządzania bezpieczeństwem informacji lub jako najlepsze praktyki w celu poprawy bezpieczeństwa systemów teleinformatycznych.

Podsumowując, standardy z grupy 1 zawierają miary w formie klas, poziomów E0-E6 lub EAL, które umożliwiają ocenę i klasyfikację systemów, podczas gdy standardy

[24] Norma PN-EN ISO/IEC 27001:2022.

[25] Norma NIST Special Publication 800-53 Rev. 5, 2020.

[26] CIS Critical Security Controls® Version 8, 2021.

z grupy 2 dostarczają zaleceń i wytycznych, ale nie mają konkretnych miar, dla których można przeprowadzić formalną certyfikację.

Obie grupy standardów, zarówno te związane z certyfikacją systemów i produktów teleinformatycznych (grupa 1), jak i standardy stanowiące dobre praktyki (grupa 2), mogą służyć jako podstawa do przeprowadzania audytów w zakresie bezpieczeństwa teleinformatycznego dla konkretnych systemów teleinformatycznych.

Standardy w obu grupach mają kilka zalet z perspektywy oceny poziomu bezpieczeństwa. Po pierwsze, systematyzacja procesu oceny zapewnia strukturę i wytyczne dotyczące oceny bezpieczeństwa systemów teleinformatycznych. Audytorzy mogą korzystać z tych standardów jako ramy referencyjnej do przeprowadzenia oceny i porównania wyników.[27]

Po drugie, procesy oceny standardów dostarczają ustalonych procedur i wymagań, co umożliwia audytorom powtarzalność procesu oceny. Można wykorzystać te same zasady i wytyczne dla różnych systemów teleinformatycznych, co prowadzi do spójności, jednolitości i porównywalności oceny.

Po trzecie, standardy stanowią platformę odniesienia dla audytorów, co pozwala na pomiary i porównanie osiągniętych wyników. Audytorzy mogą ocenić systemy teleinformatyczne zgodnie z określonymi standardami i porównać te wyniki z przyjętymi miarami.

Po czwarte, standardy mogą służyć jako punkt wyjścia przy formułowaniu kontraktów na przeprowadzenie audytu. Zawarcie klauzuli w kontrakcie, wskazującej na konkretny standard lub zalecenia, pozwala na jasne określenie zakresu oceny i ułatwia rozliczalność przedsięwzięcia audytowego.

W ten sposób standardy zapewniają spójność, jasność i wytyczne dla procesu audytu bezpieczeństwa teleinformatycznego, co przyczynia się do skutecznego oceniania systemów teleinformatycznych i zapewnienia odpowiedniego poziomu bezpieczeństwa.

Próby standaryzacji zagadnień związanych z ochroną i oceną bezpieczeństwa informacji w systemach informatycznych sięgają połowy lat sześćdziesiątych. W tym okresie systemy wielodostępne oraz sieci komputerowe zaczęły być powszechnie wykorzystywane, co wymagało odpowiednich zabezpieczeń.

---

[27] Liderman, Krzysztof. "Standardy w ocenie bezpieczeństwa teleinformatycznego." *Biuletyn Instytutu Automatyki i Robotyki* 8.17 (2002): 97-119.

Jednym z pierwszych znaczących osiągnięć w tym obszarze było opracowanie i wydanie w 1983 roku tzw. "Pomarańczowej książki". Były to zalecenia opracowane na zlecenie Departamentu Obrony Stanów Zjednoczonych (Department of Defense - DoD). "Pomarańczowa książka" miała istotny wpływ na sposób rozumienia problematyki bezpieczeństwa w systemach informatycznych i stała się podstawą do opracowywania lokalnych standardów w tym zakresie na wiele lat. Zawierała wytyczne dotyczące bezpieczeństwa systemów informatycznych i skupiała się na aspektach takich jak kontrole dostępu, zarządzanie uprawnieniami, audytowanie oraz ochrona danych. Wprowadziła terminologię i podejście, które miały duże znaczenie dla dalszego rozwoju dziedziny bezpieczeństwa informatycznego.

Opracowanie "Pomarańczowej książki" stanowiło kamień milowy w rozwoju standardów bezpieczeństwa informacji. Miała ona zasadniczy wpływ na rozwój dziedziny oraz późniejsze inicjatywy standaryzacyjne, takie jak TCSEC (Trusted Computer System Evaluation Criteria) czy Common Criteria.

Kryteria oceny według TCSEC (Trusted Computer System Evaluation Criteria), znane również jako kryteria Orange Book, były używane w przeszłości do oceny bezpieczeństwa systemów teleinformatycznych. TCSEC opisywał szereg klas bezpieczeństwa, które były wykorzystywane do klasyfikacji systemów pod względem ich poziomu bezpieczeństwa. W TCSEC wyróżnia się klasy bezpieczeństwa, oznaczone następującymi literami:

- **Klasa D (minimalne wymagania bezpieczeństwa)**
  Systemy tej klasy obejmowały podstawowe zabezpieczenia, takie jak kontrole dostępu i ochrona hasła. Klasyfikacja D była najniższym poziomem bezpieczeństwa według TCSEC.
- **Klasa C1 (etap poprawności)**
  Systemy klasy C1 wprowadzały dodatkowe środki bezpieczeństwa, takie jak kontrola dostępu na poziomie użytkownika, zabezpieczanie plików oraz zarządzanie etykietami.
- **Klasa C2 (etap kontrolowany)**
  Systemy klasy C2 miały bardziej rozbudowane funkcje bezpieczeństwa, w tym kontrolę dostępu na poziomie obiektu, audytowanie zdarzeń oraz ochronę przed atakami zewnętrznymi.
- **Klasa B1 (etap etykietowany)**

Systemy klasy B1 wymagały implementacji ścisłego zarządzania bezpieczeństwem, w tym etykietowania i kontroli dostępu na podstawie etykiet, zabezpieczeń sieciowych oraz audytowania systemu.

- **Klasa B2 (etap strukturalny)**
  Systemy klasy B2 wprowadzały dodatkowe środki bezpieczeństwa, takie jak kontrola dostępu na podstawie reguł, ochrona pamięci i zarządzanie kluczami kryptograficznymi.
- **Klasa B3 (etap ograniczony)**
  Systemy klasy B3 miały zaawansowane mechanizmy bezpieczeństwa, takie jak kontrola dostępu w oparciu o role, bezpieczeństwo systemu plików oraz zarządzanie kluczami kryptograficznymi.
- **Klasa A1 (etap weryfikowany formalnie)**
  Systemy klasy A1 były najwyższym poziomem bezpieczeństwa według TCSEC i wymagały najbardziej rygorystycznego procesu weryfikacji formalnej. Obejmowały one m.in. formalne dowody bezpieczeństwa, specjalne zabezpieczenia sprzętowe i oprogramowanie oraz wysoce zaufane komponenty.

Warto zaznaczyć, że TCSEC został zastąpiony przez standard Common Criteria, który obecnie jest szeroko stosowany do oceny bezpieczeństwa teleinformatycznego.

Kryteria oceny bezpieczeństwa teleinformatycznego według ITSEC (Information Technology Security Evaluation Criteria) zostały opracowane w celu zapewnienia jednolitego podejścia do oceny bezpieczeństwa systemów teleinformatycznych. ITSEC było jednym z ważnych standardów z grupy 1, które umożliwiały certyfikację systemów i produktów teleinformatycznych. Poniżej przedstawiam podstawowe informacje na temat kryteriów oceny bezpieczeństwa według ITSEC:

Poziomy bezpieczeństwa	ITSEC definiuje siedem poziomów bezpieczeństwa, oznaczanych jako E0-E6. Wyższy poziom oznacza bardziej rygorystyczne wymagania bezpieczeństwa.
Składniki bezpieczeństwa	ITSEC identyfikuje 12 składników bezpieczeństwa, które są brane pod uwagę podczas oceny systemu. Składniki te obejmują zarządzanie bezpieczeństwem, polityki bezpieczeństwa, identyfikację i autoryzację, zarządzanie kluczami, bezpieczeństwo komunikacji,

	zarządzanie zdarzeniami, kontrolę dostępu, ochronę danych, wykrywanie ataków, reagowanie na incydenty, bezpieczeństwo fizyczne oraz dokumentację.
Procedury oceny	ITSEC dostarcza szczegółowe procedury oceny, które audytorzy mogą wykorzystać do przeprowadzenia oceny bezpieczeństwa systemów. Procedury te obejmują m.in. analizę dokumentacji, testy bezpieczeństwa, inspekcje kodu źródłowego i ewentualnie testy penetracyjne.
Ewaluacja	ITSEC wprowadza proces ewaluacji, który ma na celu ocenę i przypisanie systemowi odpowiedniego poziomu bezpieczeństwa na podstawie spełnienia określonych wymagań. Ewaluacja może być przeprowadzana przez niezależne zespoły lub laboratoria certyfikacyjne.
Zaufanie do bezpieczeństwa	ITSEC wprowadza pojęcie "zaufania do bezpieczeństwa" (ang. *security assurance*), które odnosi się do stopnia pewności, że system zabezpieczeń działa zgodnie z oczekiwaniami. ITSEC określa sześć poziomów zaufania do bezpieczeństwa, od E0 do E6.

Kryteria oceny bezpieczeństwa według ITSEC były szeroko stosowane w przeszłości, jednak w miarę rozwoju innych standardów, takich jak Common Criteria, znaczenie ITSEC zmalało. Obecnie Common Criteria jest szerzej używanym standardem do oceny bezpieczeństwa systemów teleinformatycznych.

Przy ocenie bezpieczeństwa teleinformatycznego według COBIT, istotne jest uwzględnienie specyficznych aspektów bezpieczeństwa, takich jak:

- **Identyfikacja i ocena ryzyka**

  COBIT podkreśla znaczenie identyfikacji zagrożeń i oceny ryzyka związanych z bezpieczeństwem. Organizacje powinny przeprowadzać ocenę ryzyka, aby zidentyfikować potencjalne luki i wrażliwości, które mogą wpływać na bezpieczeństwo systemów teleinformatycznych.
- **Wdrażanie kontroli bezpieczeństwa**

COBIT dostarcza wytyczne dotyczące definiowania i wdrażania kontroli bezpieczeństwa. Organizacje powinny opracować odpowiednie kontrole, które pomogą zabezpieczyć systemy teleinformatyczne przed zagrożeniami i naruszeniami.

- **Polityki bezpieczeństwa**

  COBIT zachęca do opracowania i wdrożenia jasnych polityk bezpieczeństwa. Polityki te powinny określać oczekiwania dotyczące bezpieczeństwa informacji, procedury, odpowiedzialności i prawa użytkowników.

- **Zarządzanie uprawnieniami i dostępem**

  COBIT podkreśla znaczenie skutecznego zarządzania uprawnieniami i kontrolą dostępu do systemów teleinformatycznych. Organizacje powinny zapewnić, że tylko uprawnione osoby mają dostęp do systemów i danych, a zarządzanie uprawnieniami odbywa się zgodnie z określonymi zasadami i procedurami.

- **Monitorowanie i reagowanie**

  COBIT zaleca monitorowanie systemów teleinformatycznych w celu wykrywania incydentów bezpieczeństwa oraz szybkiego i skutecznego reagowania na nie. Organizacje powinny wprowadzić mechanizmy monitorowania, logowania zdarzeń, raportowania incydentów i prowadzenia audytów bezpieczeństwa.

Kryteria oceny COBIT dostarczają wytycznych w zakresie kontroli i zarządzania, ale nie definiują konkretnych kryteriów oceny bezpieczeństwa. Organizacje mogą dostosować zakres COBIT do swoich potrzeb i wymagań, aby stworzyć indywidualne kryteria oceny bezpieczeństwa.

Ocena bezpieczeństwa teleinformatycznego według COBIT może być przeprowadzana przez wewnętrzne zespoły audytowe lub zlecona zewnętrznym firmom specjalizującym się w audytach bezpieczeństwa. W oparciu o zasady COBIT organizacje mogą ocenić skuteczność swoich praktyk i procedur bezpieczeństwa oraz identyfikować obszary wymagające usprawnienia.

Kryteria oceny według standardu BS 7799/ ISO/IEC 27001, znanego również jako ISO/IEC 27001, są normą dotyczącą zarządzania bezpieczeństwem informacji. Określa ona wymagania i wytyczne w zakresie wdrożenia, zarządzania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji (Information Security Management System - ISMS). Główne założenia standardu BS 7799/ISO/IEC 27001 obejmują:

Ocena ryzyka	Standard wymaga przeprowadzenia systematycznej oceny ryzyka związanego z bezpieczeństwem informacji, aby zidentyfikować zagrożenia, podatności i potencjalne skutki incydentów.
Zarządzanie ryzykiem	BS 7799/ISO/IEC 27001 nakłada obowiązek na organizacje, aby wprowadziły proces zarządzania ryzykiem, obejmujący identyfikację, analizę, ocenę i kontrolę ryzyka, w celu minimalizacji szkód wynikających z incydentów. Standard wymaga opracowania dokumentowanej polityki bezpieczeństwa informacji, która jest zgodna z celami organizacji oraz regulacjami i przepisami obowiązującymi.
Zarządzanie zasobami	Organizacje muszą odpowiednio zarządzać zasobami ludzkimi, fizycznymi i technologicznymi, aby zapewnić bezpieczeństwo informacji.
Bezpieczeństwo fizyczne	Standard BS 7799/ISO/IEC 27001 obejmuje również wymagania dotyczące zabezpieczeń fizycznych, takich jak kontrola dostępu do pomieszczeń, monitorowanie i ochrona sprzętu, a także zabezpieczenie przed zagrożeniami zewnętrznymi.
Plany ciągłości działania	Standard wymaga opracowania planów ciągłości działania i odzyskiwania po awarii, które umożliwią organizacji szybkie przywrócenie normalnych operacji po wystąpieniu incydentu lub katastrofy.

Standard BS 7799/ISO/IEC 27001 stanowi kompleksowe podejście do zarządzania bezpieczeństwem informacji i służy jako ramowy schemat, który umożliwia organizacjom skuteczne identyfikowanie, analizowanie i zarządzanie ryzykiem związanym z bezpieczeństwem informacji.

Kryteria oceny według ISO/IEC 15408, znanego również jako Common Criteria (Wspólne Kryteria), to międzynarodowy standard w zakresie oceny bezpieczeństwa teleinformatycznego. Obejmuje on kryteria, które są stosowane do oceny bezpieczeństwa różnych produktów i systemów informatycznych. ISO/IEC 15408 definiuje model oceny, który składa się z trzech podstawowych komponentów:

1. **Model zagrożeń (Threat Model)**, który obejmuje identyfikację potencjalnych zagrożeń dla systemu lub produktu.
2. **Model bezpieczeństwa (Security Model)**, który definiuje poziomy bezpieczeństwa oraz wymagania dotyczące zabezpieczeń.
3. **Model oceny (Evaluation Model)**, który określa procedury i kryteria oceny, które są stosowane do oceny systemu lub produktu.

ISO/IEC 15408 wprowadza poziomy oceny zwane Evaluation Assurance Level (EAL). Każdy poziom odzwierciedla określone wymagania i metody oceny. Skala EAL obejmuje 7 poziomów, od EAL1 (najniższy) do EAL7 (najwyższy). Wyższy poziom oznacza większą kompleksowość oceny i bardziej rygorystyczne wymagania dotyczące bezpieczeństwa.

ISO/IEC 15408 definiuje zestaw zabezpieczeń funkcjonalnych, które odnoszą się do różnych aspektów bezpieczeństwa, takich jak kontrole dostępu, uwierzytelnianie, szyfrowanie czy zarządzanie kluczami. Zabezpieczenia funkcjonalne są oceniane pod kątem ich skuteczności i zgodności z wymaganiami bezpieczeństwa.

Standard uwzględnia również zabezpieczenia poza-funkcjonalne, które odnoszą się do takich aspektów jak dokumentacja, procesy zarządzania, zapewnienie integralności oceny, niezawodność środowiska oceny, odpowiedzialność i niezawisłość oceny. Aspekty te ocenia się również pod kątem ich zgodności z wymaganiami.

ISO/IEC 15408 wymaga kompleksowej dokumentacji dotyczącej oceny bezpieczeństwa, w tym opisu systemu lub produktu, oceny ryzyka, procedur oceny, wyników testów, wyników badania zabezpieczeń funkcjonalnych i poza-funkcjonalnych. Ocena bezpieczeństwa teleinformatycznego według ISO/IEC 15408 może być przeprowadzana przez niezależne organizacje.

1.9 Audyt systemu bezpieczeństwa informacji

W tym podrozdziale będzie omówiony proces audytu, który ocenia na zgodność systemów bezpieczeństwa informacji z obowiązującymi standardami i wytycznymi. Audyt ten pozwala na identyfikację ewentualnych luk i niedoskonałości w systemach ochrony, a także na ocenę ich rzeczywistej skuteczności. Zrozumienie tego procesu umożliwi ocenę, czy bardziej złożone systemy rzeczywiście zapewniają lepszą ochronę, czy też ich skomplikowana struktura może prowadzić do nowych problemów i obniżać poziom zabezpieczeń. Analiza wyników audytu dostarczy istotnych informacji na temat realnych

korzyści i wyzwań związanych z wdrażaniem zaawansowanych rozwiązań ochrony informacji.

Audyt systemu bezpieczeństwa informacji to proces, w ramach którego sprawdzane są zabezpieczenia, procedury i kontrole mające na celu ochronę informacji w systemie informatycznym. Audyt ma na celu ocenę systemu bezpieczeństwa informacji pod kątem spełnienie standardów i wymagań, identyfikację słabych punktów systemu oraz wskazanie rekomendacji dotyczących usprawnień i zabezpieczeń.[28]

Podczas audytu systemu bezpieczeństwa informacji mogą być podejmowane następujące działania:

1. **Analiza dokumentacji i procedur**
   Audytorzy sprawdzają dokumentację związane z bezpieczeństwem informacji, taką jak polityki bezpieczeństwa, procedury, instrukcje, oceny ryzyka . Weryfikowana jest zgodność dokumentów z obowiązującymi standardami i najlepszymi praktykami.
2. **Ocena kontroli dostępu**
   Sprawdzane są procedury kontroli dostępu do systemu, zarządzanie uprawnieniami użytkowników, autentykacja, uwierzytelnianie, zarządzanie hasłami. Celem jest upewnienie się, że tylko uprawnione osoby mają dostęp do systemu i danych.
3. **Analiza zabezpieczeń fizycznych**
   Audytorzy mogą dokonać inspekcji fizycznej miejsca przechowywania serwerów, centrów danych i innych urządzeń. Sprawdzane są zabezpieczenia fizyczne, takie jak systemy kontroli dostępu, monitorowanie, ochrona przed pożarem, klimatyzacja.
4. **Testowanie zabezpieczeń technicznych**
   Wykonywane są testy techniczne, takie jak penetracja sieci, testy podatności, skanowanie bezpieczeństwa, aby sprawdzić, czy system jest odporny na ataki zewnętrzne.
5. **Ocena zarządzania incydentami i kontynuacji działania**

[28] Information Security Auditor. Careers in Information Security, BCS 2016, ISBN 1780172168

Sprawdzane są procedury zarządzania incydentami bezpieczeństwa, reagowania na awarie, plany kontynuacji działania w przypadku wystąpienia zakłóceń czy awarii systemowych.

6. **Szkolenie i budowanie świadomości użytkowników**

   Ocena obejmuje weryfikację programów szkoleniowych dotyczących bezpieczeństwa informacji, świadomości użytkowników oraz przestrzegania polityk bezpieczeństwa przez personel.

Proces audytu systemu bezpieczeństwa informacji składa się z różnych elementów. Jednym z nich jest sporządzenie listy audytowej (tzw. checklisty) według wybranego standardu. W zależności od wybranego standardu, audytorzy opracowują listę punktów audytowych, które powinny być sprawdzone. Lista ta obejmuje konkretne wymagania i zalecenia dotyczące bezpieczeństwa informacji.[29]

Kolejnym krokiem jest ocena spełnienia punktów audytowych. Audytorzy analizują każdy punkt audytowy na liście i oceniają, czy dany element spełnia wymagania. Wynik może być zaklasyfikowany jako "spełnione", "nie spełnione", "spełnione częściowo" lub "nie dotyczy".

Podczas audytu audytorzy zbierają dokumentację i dowody potwierdzające spełnienie wymagań bezpieczeństwa informacji. Mogą to być dokumenty, procedury, logi systemowe czy raporty z testów. Audytorzy oceniają ryzyko związane z niedopełnieniem wymagań bezpieczeństwa informacji. Identyfikowane są słabe punkty, luki w zabezpieczeniach oraz potencjalne zagrożenia.

Audytorzy przeprowadzają także wywiady i rozmowy z odpowiedzialnymi osobami, zarządzającymi systemem bezpieczeństwa informacji, pracownikami IT i innymi interesariuszami. Celem jest uzyskanie informacji na temat praktyk, procedur i działań związanych z bezpieczeństwem informacji.

Audytorzy sprawdzają takie na ile system bezpieczeństwa informacji jest zgodny z obowiązującymi standardami, regulacjami i politykami. Oceniana jest zarówno zgodność formalna, jak i operacyjna.

Po przeprowadzeniu audytu audytorzy sporządzają raport z wynikami, który zawiera informacje o spełnieniu punktów audytowych, zidentyfikowanych słabych punktach, rekomendacjach usprawnień i zaleceniach dotyczących poprawy bezpieczeństwa informacji.

[29] R. Pompon, IT Security Risk Control Management An Audit Preparation Plan, Apres, 2016.

Ważne jest, aby proces audytu był dokładny, niezależny i obiektywny, a wyniki audytu powinny być wykorzystane do doskonalenia systemu bezpieczeństwa informacji i podejmowania działań naprawczych.

Poza audytami zewnętrznymi prowadzone mogą być również audyty wewnętrzne, których celem jest ocena i monitorowanie skuteczności, integralności i zgodności zasad oraz procedur zabezpieczeń informacji w ramach organizacji. Audyty wewnętrze realizują kilka kluczowych celów. Pierwszym z nich jest ocena zgodności. Audyt bezpieczeństwa systemu ma na celu ocenę czy system i jego zabezpieczenia są zgodne z obowiązującymi politykami, standardami, przepisami i regulacjami wewnętrznymi i zewnętrznymi. Dzięki temu można ustalić, czy organizacja przestrzega wymagań i norm prawnych w zakresie bezpieczeństwa informacji.

Drugim celem jest identyfikacja słabych punktów. Audyt ukierunkowany jest na identyfikację i ocenę potencjalnych luk, słabych punktów i zagrożeń w systemie bezpieczeństwa informacji. Mogą to być nieprawidłowości w procedurach, braki w zabezpieczeniach technicznych czy niewłaściwe zarządzanie uprawnieniami.

Trzecim celem audytów wewnętrznych jest ocena ryzyka. Audyt bezpieczeństwa systemu może pomóc w ocenie ryzyka związanego z bezpieczeństwem informacji. Identyfikuje się obszary, w których ryzyko jest wysokie oraz proponuje działania mające na celu zminimalizowanie tych zagrożeń i wzmocnienie zabezpieczeń.

Czwartym celem jest monitorowanie skuteczności. Audyt systemu bezpieczeństwa informacji służy do monitorowania skuteczności istniejących zabezpieczeń i procedur. Pozwala na ocenę, czy zabezpieczenia są wystarczające oraz czy działają zgodnie z oczekiwaniami.

Piątym celem jest wskazanie możliwych usprawnień. Audyt dostarcza rekomendacji i zaleceń dotyczących poprawy systemu bezpieczeństwa informacji. Na podstawie wyników audytu można wprowadzać usprawnienia, wdrażać nowe polityki i procedury oraz podjąć działania naprawcze w celu zwiększenia bezpieczeństwa.

Kolejnym celem jest wsparcie obszaru zarządzania ryzykiem. Audyt bezpieczeństwa systemu dostarcza informacji, które wspierają proces zarządzania ryzykiem. Pomaga w identyfikacji, ocenie i zarządzaniu ryzykiem związanym z bezpieczeństwem informacji, umożliwiając podejmowanie odpowiednich decyzji i alokację zasobów.

Na koniec, udoskonalanie procesów i procedur to kolejne ważne zadanie. Audyt systemu bezpieczeństwa informacji może przyczynić się do doskonalenia procesów,

procedur i praktyk związanych z bezpieczeństwem informacji. Na podstawie wyników audytu można wprowadzać ulepszenia, dostosować polityki do zmieniających się wymagań i doskonalić procedury.

W niniejszej pracy odniesiono się do współczesnych badań dotyczących skuteczności audytów cyberbezpieczeństwa, aby lepiej zrozumieć ich rolę w ocenie i zgodności systemów ochrony informacji. W pracy Hossaina i in.[30] autorzy koncentrują się na kluczowych czynnikach wpływających na skuteczność audytów cyberbezpieczeństwa, analizując je z perspektywy instytucjonalnej. Badanie to podkreśla znaczenie czynników instytucjonalnych, takich jak presja regulacyjna, oczekiwania interesariuszy oraz formalizacja struktur organizacyjnych, w kształtowaniu wyników audytu i jego wpływu na zarządzanie ryzykiem. Z kolei w pracy Jamila i Aleneziego[31] autorzy przedstawiają szczegółowy przegląd procesów związanych z przeprowadzaniem efektywnych audytów, zwracając uwagę na znaczenie identyfikacji zagrożeń oraz reagowania na nie. Szczególny nacisk położony jest na praktyczne aspekty audytu, takie jak analiza podatności, planowanie reakcji na incydenty oraz optymalizacja środków ochronnych w oparciu o uzyskane wyniki. Oba opracowania wskazują, że audyt nie tylko służy weryfikacji zgodności z normami, ale także stanowi narzędzie usprawniające adaptację mechanizmów ochrony do realnych potrzeb organizacyjnych i aktualnego krajobrazu zagrożeń.

1.10 Reguły bezpiecznej architektury bezpieczeństwa

Podrozdział odgrywa istotną rolę w kontekście badanej tezy dotyczącej efektywności rozbudowanych systemów ochrony informacji. W tym rozdziale szczegółowo opisane są zasady, które wpływają na projektowanie i zarządzanie systemami teleinformatycznymi, takie jak bezpieczeństwo osobowe, ochrona elektromagnetyczna, zapewnienie ciągłości działania oraz konfiguracja systemów i urządzeń. Analiza tych reguł pozwala na ocenę, czy złożone mechanizmy ochrony są rzeczywiście skuteczniejsze w zabezpieczaniu informacji, czy też mogą wprowadzać dodatkowe komplikacje, które obniżają efektywność

[30] Hossain, Md. Mahmud, et al. "Key Drivers of Cybersecurity Audit Effectiveness: A Neo-Institutional Perspective." International Journal of Auditing, 2023. Wiley Online Library, https://doi.org/10.1111/ijau.12365

[31] Jamil, D., and R. M. Alenezi. "Reviewing the Processes for Conducting Effective Cybersecurity Audits, Including Threat Identification and Response." ResearchGate, 2023, www.researchgate.net/publication/386342884

zabezpieczeń. Dzięki szczegółowemu omówieniu zasad takich jak zarządzanie ryzykiem, kontrola dostępu, czy reagowanie na incydenty bezpieczeństwa, możliwe będzie sprawdzenie, czy bardziej zaawansowane rozwiązania w zakresie bezpieczeństwa są w stanie sprostać wymaganiom rzeczywistego środowiska teleinformatycznego, czy też prostsze i lepiej dostosowane mechanizmy mogą zapewnić równie wysoką, a nawet wyższą skuteczność ochrony.

W kontekście analizy efektywności rozbudowanych systemów ochrony informacji, istotne jest zrozumienie zasad zarządzania bezpieczeństwem informacji oraz praktyk reagowania na incydenty. Dronov i Dronova[32] przedstawili kluczowe zasady zarządzania bezpieczeństwem informacji, podkreślając znaczenie proaktywnego podejścia opartego na analizie i przewidywaniu ryzyka, co pozwala na opracowanie odpowiednich środków zaradczych przed wystąpieniem incydentów. Z kolei Tøndel i in. [33] przeprowadzili systematyczny przegląd literatury dotyczącej zarządzania incydentami bezpieczeństwa informacji, wskazując na zgodność praktyk z normą ISO/IEC 27035 oraz identyfikując wyzwania związane z wdrażaniem zaleceń standardów w praktyce organizacyjnej. Obie prace podkreślają, że skuteczność systemów ochrony informacji zależy nie tylko od ich złożoności, ale przede wszystkim od odpowiedniego zarządzania ryzykiem, kontroli dostępu oraz efektywnego reagowania na incydenty.

Bezpieczeństwa osobowe

W jednostce organizacyjnej niezbędne jest wskazanie osób formalnie odpowiedzialnych za funkcjonowanie i bezpieczeństwo systemu teleinformatycznego, z precyzyjnie określonym zakresem zadań i odpowiedzialności związanych z ochroną informacji wrażliwych przetwarzanych w tym systemie. Użytkownicy systemu powinni posiadać aktualne poświadczenia bezpieczeństwa lub inne formalne uprawnienia do dostępu do informacji o najwyższym stopniu poufności. Konieczne jest, aby wszyscy użytkownicy

[32] Dronov, V. Y., i G. A. Dronova. "Principles of Information Security Management System." Journal of Physics: Conference Series, vol. 2182, 2022, 012092. IOP Publishing, https://doi.org/10.1088/1742-6596/2182/1/012092

[33] Tøndel, Inger Anne, Maria B. Line, i Martin Gilje Jaatun. "Information Security Incident Management: Current Practice as Reported in the Literature." Computers & Security, vol. 45, 2014, ss. 42–57. Elsevier, https://doi.org/10.1016/j.cose.2014.05.003

systemu odbyli obowiązkowe szkolenie w zakresie ochrony systemów teleinformatycznych, zgodnie z przepisami prawa.[34]

Administratorzy systemu oraz inspektorzy bezpieczeństwa teleinformatycznego powinni ukończyć specjalistyczne szkolenia dotyczące bezpieczeństwa teleinformatycznego, zgodnie z wymogami prawa. Przed przydzieleniem użytkownikom dostępu do systemu, konieczne jest zapewnienie odpowiedniego przeszkolenia dotyczącego zasad bezpiecznego funkcjonowania i praktycznego stosowania procedur bezpiecznej eksploatacji.[35]

W jednostce organizacyjnej należy regularnie organizować szkolenia dodatkowe, zwiększające świadomość użytkowników systemu teleinformatycznego w zakresie zagrożeń oraz szkolenia związane z obsługą aplikacji i stosowaniem środków ochrony fizycznej. Użytkownicy systemu muszą potwierdzić zapoznanie się i zrozumienie procedur bezpiecznej eksploatacji systemu.[36]

W przypadku zakończenia zatrudnienia użytkownika systemu teleinformatycznego, konieczne jest całkowite zablokowanie jego dostępu do systemu oraz skuteczne rozliczenie z posiadanych zasobów, zgodnie z obowiązującymi procedurami. Jednocześnie jednostka organizacyjna musi utrzymać dostęp do zasobów pozostających w dyspozycji zwalnianego pracownika. Przy przeniesieniu na inne stanowisko lub zmianie zakresu zadań, należy przeglądać i weryfikować uprawnienia dostępu do informacji, usług i zasobów systemowych.[37]

Istotne jest określenie zasad podejmowania decyzji dotyczących wykorzystania posiadanych zasobów informacyjnych w przypadku zwolnienia lub przeniesienia pracowników na inne stanowiska. Należy przestrzegać wymagań dotyczących bezpieczeństwa osobowego związanego z dostępem do systemu teleinformatycznego przez osoby niebędące użytkownikami systemu, takie jak personel serwisowy, pracownicy zewnętrznych firm, dostawcy oprogramowania i systemów aplikacyjnych.[38]

---

[34] Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie szczegółowych zasad ochrony informacji niejawnych

[35] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych

[36] Norma ISO/IEC 27001:2017

[37] ISO/IEC 27002:2022 – Praktyczne zasady zabezpieczania informacji

[38] NIST SP 800-53 – Security and Privacy Controls

Zgodnie z przyjętą praktyką, należy także systematycznie aktualizować listę uprawnionych użytkowników systemu teleinformatycznego, dbając o przestrzeganie wszelkich zasad i wymagań dotyczących bezpieczeństwa.[39]

Bezpieczeństwo fizyczne systemu[40]

W procesie projektowania systemu teleinformatycznego, kluczowe jest właściwe dostosowanie rodzajów stref ochronnych oraz ich precyzyjna lokalizacja dla poszczególnych komponentów systemu. Te strefy, określone formalnie, muszą dokładnie korespondować z opisem zawartym w dokumentacji bezpieczeństwa.

Bezpieczeństwo stref ochronnych, obejmujących drzwi, okna, otwory wentylacyjne i inne elementy, musi być w pełni zabezpieczone zarówno pod względem konstrukcyjnym, jak i mechanicznym, zgodnie z wytycznymi dokumentacji bezpieczeństwa. Okna w tych strefach muszą być odpowiednio zabezpieczone przed potencjalnym podsłuchem, zarówno w ciągu dnia, jak i nocy. Wszystkie wejścia do stref ochronnych muszą być kontrolowane przez system kontroli dostępu. Ponadto, działanie systemu sygnalizacji włamania i napadu, zabezpieczającego te strefy, powinno być właściwie nadzorowane i utrzymane. Niezbędne jest skuteczne funkcjonowanie systemu dozoru CCTV, z odpowiednio zabezpieczonymi rejestratorami, umożliwiające odtworzenie zdarzeń w przypadku incydentu bezpieczeństwa.[41] Strefy ochronne powinny być również zabezpieczone poprzez system alarmu pożarowego, zgodnie z obowiązującymi przepisami oraz wytycznymi dokumentacji bezpieczeństwa.[42]

Nadzór nad sprzętem wnoszonym i wynoszonym powinien być wprowadzony do stref ochronnych. Okablowanie systemu teleinformatycznego, zarówno informacyjne, jak i zasilające, musi być zabezpieczone zgodnie z zapisami zawartymi w specjalnej dokumentacji.[43]

---

[39] ISO/IEC 27001:2017 – Systemy zarządzania bezpieczeństwem informacji

[40] Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych

[41] Żabicki D., https://www.ochrona-bezpieczenstwo.pl/ochrona-informacji/prawo/2346-nowe-standardy-w-systemach-kontroli-dostepu-przeglad-aktualnych-norm-i-przepisow

[42] Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych

[43] Norma PN-ISO/IEC 27001:2017

Ważne jest, aby elementy systemów wspomagających pracę systemu teleinformatycznego, takie jak zasilanie, klimatyzacja czy monitoring warunków środowiskowych, zapewniały ciągłą i niezawodną pracę systemu, zgodnie z wytycznymi dokumentacji.

Zarządzanie dostępem fizycznym, obejmujące nadawanie i blokowanie uprawnień wejścia do stref ochronnych, musi być zgodne z wytycznymi dokumentacji bezpieczeństwa. Wartość list dostępu do stref ochronnych powinna być regularnie aktualizowana. Nieodłączną częścią bezpieczeństwa jest weryfikacja i rejestracja osób wchodzących do stref ochronnych. Procedury przyznawania i odbierania środków kontroli dostępu fizycznego, takich jak klucze, karty czy hasła, powinny być zgodne z przyjętą polityką bezpieczeństwa. Ustawienia tych środków, jak kody czy hasła, powinny być okresowo zmieniane, zgodnie z wytycznymi tej polityki bezpieczeństwa.[44]

Ochrona elektromagnetyczna[45]

W kontekście otoczenia, w którym przetwarzane są informacje niejawne, istotne jest wyznaczenie sprzętowej strefy ochrony elektromagnetycznej (SSOE) dla systemu teleinformatycznego. Ta strefa stanowi fundamentalny element zapewnienia bezpieczeństwa. Kluczowe jest, aby urządzenia składające się na system teleinformatyczny posiadały aktualne certyfikaty ochrony elektromagnetycznej. Te dokumenty potwierdzają zgodność z odpowiednimi standardami i normami, a także świadczą o spełnieniu wymogów bezpieczeństwa w kontekście elektromagnetycznym.

Zapewnienie ochrony elektromagnetycznej musi obejmować nie tylko posiadanie certyfikatów, ale również właściwą eksploatację zastosowanych środków. Wdrożone rozwiązania bezpieczeństwa elektromagnetycznego muszą być eksploatowane zgodnie z dokumentacją bezpieczeństwa systemu teleinformatycznego oraz wymaganiami wynikającymi z posiadanych certyfikatów. To gwarantuje, że system zachowuje swoją integralność i niezawodność w kontekście elektromagnetycznym, co ma kluczowe znaczenie dla ochrony informacji niejawnych.

[44] https://bip.abw.gov.pl/bip/informacje-niejawne-1/nadzor-nad-systemem-oc/bezpieczenstwo-fizyczn/150,Kancelarie-tajne-Bezpieczenstwo-fizyczne.html

[45] https://ochrona-niejawnych.pl/ochrona-elektromagnetyczna2/

Zapewnienie Ciągłości Działania i Bezpieczeństwa Systemu

W kontekście zapewnienia ciągłości działania systemu teleinformatycznego, istotne jest prowadzenie aktualnego wykazu osób odpowiedzialnych za tę ciągłość w jednostce, wraz z danymi kontaktowymi.[46] Osoby odpowiedzialne za realizację planu ciągłości działania powinny być należycie przeszkolone, obejmując zarówno zakres obowiązków, jak i częstotliwość, z jaką powinni wykonywać określone zadania.

Plan ciągłości działania systemu teleinformatycznego musi być regularnie testowany i aktualizowany, zgodnie z wytycznymi określonymi w przyjętej polityce bezpieczeństwa. Wartościowe są również testy kopii zapasowych zgodnie z ustalonymi częstotliwościami.[47] Kluczowe jest wprowadzenie i testowanie skutecznych mechanizmów umożliwiających odzyskiwanie danych i przywracanie systemu do pierwotnego stanu po zakłóceniu, awarii lub innym incydencie bezpieczeństwa teleinformatycznego.

Niezbędne jest tworzenie oraz właściwe przechowywanie kopii zapasowych danych systemu teleinformatycznego, systemów operacyjnych, oprogramowania krytycznego, elementów systemu oraz dokumentacji bezpieczeństwa, zgodnie z wytycznymi polityki bezpieczeństwa. Dodatkowo, należy zadbać o zabezpieczenie urządzeń oraz systemów zasilania awaryjnego, aby w przypadku incydentu zapewnić nieprzerwaną pracę systemu.[48]

Ustawienia konfiguracyjne systemu oraz urządzeń[49]

Konfiguracja odgrywa kluczową rolę w procesie zapewniania bezpieczeństwa i funkcjonalności systemu teleinformatycznego. Powinna ona być zgodna z opisem zawartym w Szczególnych Wymaganiach Bezpieczeństwa (SWB). Osoby odpowiedzialne za zarządzanie konfiguracją systemu muszą posiadać kompleksową wiedzę oraz skrupulatnie wykonywać swoje obowiązki.

---

[46] ISO/IEC 27001 - wytyczne dotyczące ciągłości działania (klauzula 17.1: Kontrola ciągłości działania) oraz wymaga, aby organizacje miały plan ciągłości działania.

[47] ISO 22301 - Norma dotycząca zarządzania ciągłością działania, która szczegółowo opisuje procesy związane z planowaniem, wdrażaniem, utrzymywaniem i doskonaleniem systemu zarządzania ciągłością działania.

[48] NIST SP 800-34 - Wytyczne amerykańskiego Narodowego Instytutu Standardów i Technologii dotyczące planowania ciągłości działania w kontekście systemów informacyjnych. Dokument ten opisuje procesy, które organizacje powinny wdrożyć, aby zapewnić ciągłość działania

[49] NIST SP 800-128 - Wytyczne amerykańskiego Narodowego Instytutu Standardów i Technologii dotyczące zarządzania konfiguracją. Dokument ten koncentruje się na praktykach związanych z zarządzaniem konfiguracją systemów informacyjnych, w tym na rolach i odpowiedzialnościach.

Istotne jest przestrzeganie zasad i procedur związanych z aktualizacją bezpiecznej konfiguracji systemu teleinformatycznego. Warto również przechowywać starsze wersje bezpiecznej konfiguracji systemu, aby zachować pełną transparentność.

W systemie teleinformatycznym niezbędna jest jasno określona lista zatwierdzonego oprogramowania, obejmującego zarówno systemy operacyjne, aplikacje, jak i narzędzia. Konieczne jest również sprecyzowanie rodzajów zmian konfiguracyjnych, które muszą być odpowiednio udokumentowane w dokumentacji bezpieczeństwa systemu.

Należy zadbać o systematyczne testowanie i ocenę planowanych zmian konfiguracyjnych pod kątem ich wpływu na funkcjonowanie i bezpieczeństwo systemu teleinformatycznego. Analiza nowego oprogramowania w środowisku testowym jest nieodzowna przed wprowadzeniem go do środowiska operacyjnego.

Wprowadzenie zakazu wykorzystywania nieautoryzowanych urządzeń, nośników i oprogramowania przez użytkowników systemu teleinformatycznego jest ważnym krokiem w zabezpieczaniu systemu. Należy nadzorować i kontrolować przestrzeganie tego zakazu. Konfiguracja systemu teleinformatycznego powinna skutecznie zapobiegać nieuprawnionym zmianom dokonywanym przez użytkowników, takim jak instalacja nieautoryzowanego oprogramowania. Ważne jest również zastosowanie minimalnej funkcjonalności, dostosowanej do wymaganych zadań systemu.

Regularne przeglądy systemu teleinformatycznego są istotne dla identyfikacji i eliminacji zbędnych funkcji, portów, protokołów oraz usług. Użytkownicy powinni być świadomi swojej odpowiedzialności za powierzone urządzenia i oprogramowanie. Jednostki organizacyjne powinny przeprowadzać inwentaryzację elementów systemu teleinformatycznego i okablowania, zapewniając kompletność i klarowność w zarządzaniu sprzętem i oprogramowaniem dostępnym dla użytkowników systemu teleinformatycznego.

Utrzymanie systemu[50]

Istotną rolę w tym obszarze odgrywa prowadzenie dokumentacji dotyczącej napraw i przeglądów diagnostycznych systemu teleinformatycznego, zgodnie z wytycznymi

[50] NIST SP 800-53 - Wytyczne amerykańskiego Narodowego Instytutu Standardów i Technologii dotyczące zabezpieczeń systemów informacyjnych. Zawiera wytyczne dotyczące zarządzania dostępem, dokumentowania napraw oraz przeglądów systemów.

dokumentacji bezpieczeństwa systemu. Konieczne jest także kontrolowanie wykorzystania urządzeń i narzędzi diagnostycznych w systemie teleinformatycznym.

Przyznawanie uprawnień dostępu do systemu dla pracowników serwisu musi być ściśle zgodne z dokumentacją bezpieczeństwa systemu. Dodatkowo, naprawy elementów systemu teleinformatycznego poza lokalizacją organizacji muszą być przeprowadzane i dokumentowane zgodnie z ustaleniami zawartymi w dokumentacji bezpieczeństwa systemu teleinformatycznego. Nadzorowanie oraz odpowiednie dokumentowanie prac naprawczych i przeglądów wykonywanych przez serwisy zewnętrzne są niezwykle ważne. Warunki umów serwisowych z dostawcami zewnętrznymi powinny być zgodne z zapisami zawartymi w Standardowych Wymaganiach Bezpieczeństwa.

W jednostce organizacyjnej należy wyznaczyć osoby odpowiedzialne za nadzór nad pracami naprawczymi i przeglądami wykonywanymi przez serwisy zewnętrzne, aby zapewnić pełną kontrolę nad procesem serwisowym systemu teleinformatycznego.

Zapobieganie i reagowanie na incydenty bezpieczeństwa teleinformatycznego

W systemie teleinformatycznym należy regularnie przeprowadzać testy bezpieczeństwa, mające na celu weryfikację poprawności działania poszczególnych zabezpieczeń. Konieczne jest wprowadzenie zasad i procedur bieżącej analizy oraz oceny bezpieczeństwa systemu teleinformatycznego.

Stosowanie testów penetracyjnych lub narzędzi do automatycznej analizy i oceny skuteczności zabezpieczeń zgodnie z Szczególnymi Wymaganiami Bezpieczeństwa jest kluczowe. Dodatkowo, konieczne jest ustanowienie procedur związanych z przygotowywaniem planu działań naprawczych lub korekcyjnych w przypadku stwierdzenia nieprawidłowości podczas weryfikacji lub konieczności wprowadzenia zmian.[51]

Regularne szkolenia pracowników w zakresie reagowania na incydenty bezpieczeństwa oraz okresowe ćwiczenia w jednostce organizacyjnej są nieodzowne. W systemie teleinformatycznym powinny być zastosowane skuteczne mechanizmy i procedury zapobiegające incydentom, w tym działaniu oprogramowania złośliwego oraz szybkiej detekcji i powiadamiania o incydentach.

[51] NIST SP 800-115 - Wytyczne dotyczące testowania i oceny bezpieczeństwa systemów informacyjnych, które obejmują testy penetracyjne oraz analizy bezpieczeństwa.

Przeprowadzanie ponownego procesu szacowania ryzyka po znaczących incydentach bezpieczeństwa jest kluczowe. Dodatkowo, niezbędne jest zastosowanie skutecznych metod postępowania z incydentami bezpieczeństwa i dokumentowanie przypadków incydentów wraz z wyjaśnieniem przyczyn ich wystąpienia.

Wprowadzenie i aktualizacja mechanizmów ochrony przed kodem złośliwym, zgodnie z polityką i procedurami zarządzania zmianami konfiguracji, to kolejne ważne zadanie. Monitorowanie zdarzeń wpływających na bezpieczeństwo informacji niejawnych przetwarzanych w systemie teleinformatycznym jest kluczowym aspektem zapewnienia ciągłości działania i bezpieczeństwa systemu.

Zasady wprowadzania poprawek oraz aktualizacji oprogramowania[52]

Poprawki i aktualizacje do oprogramowania oraz systemu operacyjnego powinny być wdrażane na bieżąco, poddawane odpowiednim testom oraz starannie udokumentowane. Istotne jest zdefiniowanie przypadków, w których konieczne jest przeprowadzenie testów bezpieczeństwa systemu dla wprowadzanych poprawek i aktualizacji, aby ocenić wpływ na efektywność kluczowych elementów systemu oraz potencjalne „efekty uboczne". System teleinformatyczny powinien automatycznie wykrywać i reagować na nieautoryzowane zmiany w oprogramowaniu i konfiguracji, zapewniając w ten sposób dodatkową warstwę zabezpieczeń.[53]

Ochrona informatycznych nośników danych[54]

W systemie teleinformatycznym powinien istnieć wykaz rodzajów informatycznych nośników danych, które są dopuszczone do wykorzystania. Oznaczenia nośników wykorzystywanych do przetwarzania informacji niejawnych powinny być zgodne z obowiązującymi przepisami w tym zakresie. Nośniki zawierające informacje niejawne powinny być właściwie ewidencjonowane i przechowywane. Należy również właściwie

---

[52] ISO/IEC 27002 - Uzupełnienie normy ISO/IEC 27001, zawiera wytyczne dotyczące wprowadzania poprawek i aktualizacji, podkreślając znaczenie dokumentacji oraz testowania poprawek przed ich wdrożeniem.

[53] ISO/IEC 27001 - Międzynarodowa norma dotycząca zarządzania bezpieczeństwem informacji, która w klauzuli 12.6 wskazuje na konieczność zarządzania zmianami i aktualizacjami w systemach informacyjnych

[54] ISO/IEC 27001 - Międzynarodowa norma dotycząca zarządzania bezpieczeństwem informacji, która odnosi się do zarządzania zasobami i ich bezpieczeństwem, w tym nośnikami danych. Klauzula 8.1 odnosi się do identyfikacji i zarządzania aktywami, co obejmuje również nośniki danych.

realizować zasady przydzielania uprawnień użytkownikom do korzystania z nośników oraz dokładnie rozliczać użytkowników z posiadanych nośników.

Wdrożone powinny być odpowiednie środki służące zabezpieczeniu nośników oznaczonych klauzulami, które są przekazywane pomiędzy różnymi strefami ochronnymi. Konieczne jest określenie zasad ewentualnego obniżania klauzul tajności nośników. Dodatkowo, należy wdrożyć identyfikację i uwierzytelnianie użytkowników oraz urządzeń w celu zwiększenia poziomu bezpieczeństwa systemu teleinformatycznego.

Identyfikacja i uwierzytelniania użytkowników oraz urządzeń[55]

W systemie teleinformatycznym należy wprowadzić skuteczne mechanizmy uwierzytelniania użytkowników podczas dostępu do urządzeń i usług, zgodnie z opisem zawartym w przyjętej polityce bezpieczeństwa. Istotne jest prawidłowe dystrybuowanie i ewidencjonowanie narzędzi wykorzystywanych w procesie identyfikacji i uwierzytelnienia, takich jak karty chipowe i tokeny.

Hasła użytkowników systemu muszą spełniać określone standardy dotyczące długości, złożoności i regularnej zmiany, zgodnie z przyjętą polityką bezpieczeństwa. W szczególności, hasła administratora systemu, inspektora BTI oraz hasła dostępu do systemu BIOS muszą być szczególnie zabezpieczone i zdeponowane w miejscu zapewniającym maksymalne bezpieczeństwo.

Należy również zabezpieczyć oraz bezpiecznie zdeponować wszystkie niezbędne hasła administracyjne, w tym te do urządzeń sieciowych, aby umożliwić właściwe zarządzanie systemem. Dodatkowo, konieczne jest wdrożenie skutecznych mechanizmów uwierzytelniania urządzeń w systemie, włączając w to urządzenia peryferyjne, podczas próby ich podłączenia do systemu teleinformatycznego.

Kontrola dostępu do systemu

W systemie teleinformatycznym konieczne jest prowadzenie rzetelnego rejestru użytkowników uprawnionych do pracy, szczegółowo opisującego ich posiadane uprawnienia. Ważne jest, aby ten rejestr był regularnie aktualizowany i nadzorowany zgodnie z przyjętą dokumentacją bezpieczeństwa.

[55] ISO/IEC 27001 - Międzynarodowa norma dotycząca systemów zarządzania bezpieczeństwem informacji. Zawiera wymagania dotyczące kontroli dostępu (klauzula 9), które odnoszą się do uwierzytelniania użytkowników i urządzeń.

Zarządzanie kontami użytkowników w systemie TI, obejmujące m.in. zakładanie, przyznawanie uprawnień, ich modyfikację, blokowanie czy usuwanie, musi być zgodne z wytycznymi zawartymi w dokumentacji bezpieczeństwa. Dodatkowo, monitorowanie aktywności użytkowników powinno odbywać się zgodnie z ustalonymi w SWB okresami i zakresem przeglądu.[56]

W przypadku sieci systemów TI rozlokowanych w różnych lokalizacjach, konieczne jest stosowanie mechanizmów kontroli dostępu przepływu danych, zgodnie z wytycznymi zawartymi w SWB. Istotne jest również wprowadzenie separacji oraz zróżnicowanego zakresu uprawnień, wynikających z przydzielonych ról w systemie TI.

Zasada przyznawania „minimum uprawnień" niezbędnych do wykonywania pracy w systemie jest kluczowa dla zapewnienia bezpieczeństwa. Dodatkowo, system teleinformatyczny powinien zastosować automatyczną blokadę dostępu po wyczerpaniu nieudanych prób logowania.

Informacje ogólnodostępne dla użytkowników systemu teleinformatycznego muszą być zarządzane zgodnie z zapisami dokumentacji bezpieczeństwa, a system nie może być połączony z otwartymi systemami i sieciami. Zaleca się stosowanie mechanizmów współdzielenia zasobów zgodnych z wytycznymi zawartymi w SWB, z dbałością o bezpieczeństwo przekazywanych informacji.

Audyt wewnętrzny bezpieczeństwa systemu[57]

W celu zapewnienia właściwego poziomu bezpieczeństwa systemu teleinformatycznego, istotne jest wyznaczenie obszarów o wysokim ryzyku, które wymagają regularnych audytów wewnętrznych. Te audyty powinny weryfikować zgodność stanu zabezpieczeń TI z opisem w Szczególnych Wymagań Bezpieczeństwa (SWB) i zastosowanych środków ochrony.

Audyt wewnętrzny powinien być przeprowadzany zgodnie z zaplanowaną częstotliwością określoną w Polityce Bezpieczeństwa Eksploatacyjnego (PBE). Osoby odpowiedzialne za przeprowadzanie audytów powinny być wyznaczone, a ich zadania w tym zakresie jasno określone. Audyty wewnętrzne powinny być starannie

[56] NIST SP 800-53 - Wytyczne Narodowego Instytutu Standardów i Technologii dotyczące zabezpieczeń systemów informacyjnych, które obejmują zasady dotyczące kontroli dostępu, zarządzania kontami użytkowników oraz monitorowania aktywności.

[57] Harold F. Tipton, Mickey Krause, Information Security Management Handbook, 1999

udokumentowane, a zalecenia wskazane w wynikach audytu muszą być skutecznie zrealizowane.

W systemie TI ważne jest zdefiniowanie zdarzeń, które podlegają procedurom audytu bezpieczeństwa ze względu na ich istotność dla bezpieczeństwa systemu. Należy także zapewnić, że w systemie TI występują elementy generujące zapisy audytowe, takie jak mechanizmy systemowe i zasady inspekcji. Lista audytowanych zdarzeń powinna być regularnie przeglądana i aktualizowana. system teleinformatyczny powinien tworzyć precyzyjne zapisy audytowe, zawierające informacje o rodzaju zdarzenia, dacie, miejscu i czasie, źródle zdarzenia, skutkach oraz tożsamości użytkownika związanego ze zdarzeniem.

Aby uniknąć utraty informacji z powodu przepełnienia, system teleinformatyczny powinien zapewnić odpowiednią pojemność baz danych zawierających informacje o audytowanych zdarzeniach. Zapisy audytowe powinny być okresowo analizowane, a także przeglądane w różnych repozytoriach, by uzyskać kompleksowy obraz stanu bezpieczeństwa systemu.

Ważne jest także, aby system teleinformatyczny zabezpieczył informacje i narzędzia audytowe przed nieuprawnionym dostępem, modyfikacją i usunięciem, ograniczając jednocześnie dostęp do tych zapisów wyłącznie dla personelu odpowiedzialnego za funkcjonowanie i bezpieczeństwo systemu teleinformatycznego, takich jak administratorzy i inspektorzy Bezpieczeństwa Technologii Informacyjnej (BTI).

Zarządzanie ryzykiem[58]

W celu skutecznego zarządzania ryzykiem w systemie teleinformatycznym, konieczne jest formalne powołanie struktury organizacyjnej odpowiedzialnej za ten obszar. Powinna być utworzona i skoordynowana struktura, której zadaniem będzie nadzór nad zarządzaniem ryzykiem oraz wdrażanie odpowiednich środków zaradczych.

Zgodnie z ustalonym planem, należy regularnie przeprowadzać przeglądy ryzyka, które pozwolą na identyfikację i ocenę zagrożeń dla systemu teleinformatycznego. Na podstawie wyników tych przeglądów, konieczne jest podjęcie działań wynikających z zaleceń i rekomendacji.

Istotne jest opracowanie listy zmian, które wymagają dodatkowego szacowania ryzyka. Dodatkowe szacowanie ryzyka powinno mieć miejsce w przypadku istotnych

[58] PN-EN ISO/IEC 27001:2023-08 – norma międzynarodowa standaryzująca systemy zarządzania bezpieczeństwem informacji.

incydentów bezpieczeństwa lub po wykryciu nowych zagrożeń lub podatności, które mogą mieć wpływ na bezpieczeństwo informacji.

Czynniki ryzyka bezpieczeństwa systemu teleinformatycznego muszą być monitorowane na bieżąco, a wszelkie naruszenia bezpieczeństwa powinny być odpowiednio raportowane i zarządzane. Wprowadzone ryzyka szczątkowe muszą być zaakceptowane przez właściwego Kierownika Jednostki Organizacyjnej.

Eksploatacja systemu teleinformatycznego powinna odbywać się zgodnie z warunkami akredytacji bezpieczeństwa TI. Ponadto, konieczne jest regularne prowadzenie szkoleń dla użytkowników systemu, mających na celu uświadomienie zagrożeń oraz promowanie bezpiecznej eksploatacji systemu.

Określenie zasad i odpowiedzialności za organizowanie, prowadzenie i dokumentowanie szkoleń dla użytkowników systemu teleinformatycznego jest kluczowe dla efektywnego zarządzania ryzykiem i zapewnienia bezpiecznej pracy w systemie.

Zasady i procedury zarządzania zmianami w systemie teleinformatycznym[59]

Wprowadzanie zmian oraz aktualizacja dokumentacji bezpieczeństwa systemu teleinformatycznego powinna odbywać się zgodnie z ustalonymi zasadami i procedurami. Proces ten powinien być starannie kontrolowany i monitorowany, aby zapewnić, że wszelkie zmiany są wprowadzane w sposób bezpieczny i zgodny z obowiązującymi wytycznymi.

W systemie teleinformatycznym powinny być zdefiniowane szczególne sytuacje, po wystąpieniu których konieczne jest przeprowadzenie ponownej akredytacji bezpieczeństwa. Obejmuje to istotne zmiany w infrastrukturze systemu, kluczowe incydenty bezpieczeństwa oraz pojawienie się nowych zagrożeń, które mogą wpłynąć na bezpieczeństwo informacji.

Dla systemu teleinformatycznego należy określić zasady i procedury postępowania w przypadku zakończenia eksploatacji. Konieczne jest zaplanowanie procesu wygaszania systemu, w tym zabezpieczenie danych, migrację do innych rozwiązań lub odpowiedniego zabezpieczenia infrastruktury, aby uniknąć potencjalnych zagrożeń po zakończeniu eksploatacji systemu.

Podsumowując niniejszy podrozdział warto dodać, że jest on elementem pracy, który dostarcza danych do wsparcia tez. Wkład własny będzie polegać na wypracowaniu nowych

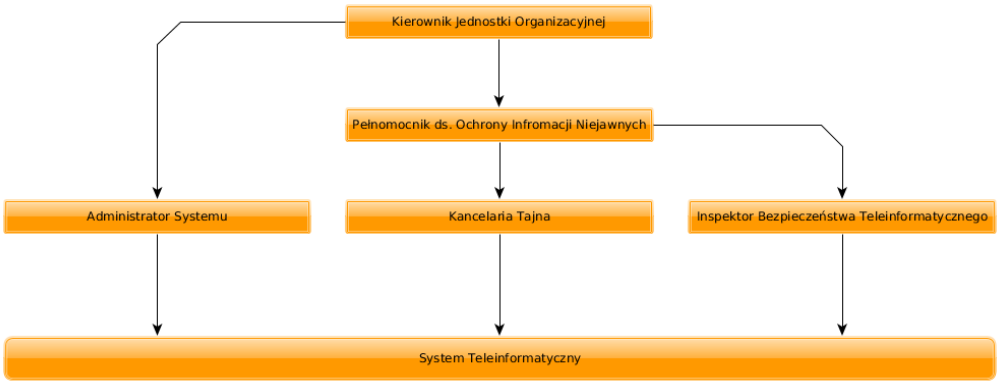
[59] ISO/IEC 20000-1:2018 - Standard dotyczący zarządzania usługami IT, który zawiera wytyczne dotyczące zarządzania zmianami jako części cyklu życia usług IT. Zawiera on wymagania dotyczące procesów związanych z zarządzaniem zmianami.

modeli, rozwiązań oraz podejść do zarządzania ryzykiem i ochrony informacji, które uwzględniają zarówno złożoność systemów, jak i ich rzeczywistą efektywność w kontekście bezpieczeństwa.

1.11 Organizacja modelowego ośrodka ochrony

Podrozdział ma znaczenie dla weryfikacji tezy dotyczącej skuteczności różnych podejść do ochrony informacji w systemach teleinformatycznych. W tej części rozdziału omawiane są zasady i struktury organizacyjne, które powinny być wdrożone, aby efektywnie zarządzać bezpieczeństwem informacji w ośrodkach ochrony. Analiza organizacji modelowego ośrodka ochrony pozwala na ocenę, czy złożoność struktury zarządzania i przyjętych procedur rzeczywiście wpływa na podniesienie poziomu bezpieczeństwa, czy też może prowadzić do nieefektywności. Przyglądając się, jak zorganizowane są zespoły odpowiedzialne za bezpieczeństwo, jakie mechanizmy kontroli i nadzoru są stosowane, oraz jakie procedury są wdrażane, można lepiej zrozumieć, czy bardziej złożona organizacja ośrodka ochrony przyczynia się do lepszej ochrony danych i informacji, czy też może okazać się, że prostsze, ale bardziej zintegrowane rozwiązania są równie skuteczne.

System teleinformatyczny w świetle ustawy o ochronie informacji niejawnych jest system teleinformatycznym przetwarzającym informacje niejawne. Biorąc pod uwagę powyższe system musi pracować w środowisku i na zasadach określonych w tejże ustawie. Dla zapewniania ochrony informacji niejawnych należy zorganizować pion ochrony informacji niejawnych zgodnie z poniższym schematem.



Schemat 1: Schemat modelowego ośrodka ochrony

W ramach pionu ochrony należy przypisać role i obowiązki personelowi pionu ochrony zgodnie z aktualnym stanem prawnym. W sytuacji gdy taka komórka organizacyjna jest już powołana należy rozszerzyć zakres obowiązków związany z prawidłową

eksploatacją systemu zgodnie z dokumentacją bezpieczeństwa tj. Szczególnymi Wymaganiami Bezpieczeństwa oraz Procedurami Bezpiecznej Eksploatacji.

W kontekście analizy skuteczności różnych podejść do ochrony informacji w systemach teleinformatycznych, istotne jest zrozumienie zasad organizacji i zarządzania w modelowych ośrodkach ochrony. W pracy Vielbertha i in.[60] przeprowadzono systematyczne badanie centrów operacji bezpieczeństwa (SOC), identyfikując kluczowe wyzwania związane z ich strukturą organizacyjną oraz efektywnością w zarządzaniu bezpieczeństwem informacji. Autorzy podkreślają, że złożoność struktury SOC może zarówno wspierać, jak i hamować skuteczność operacyjną, w zależności od implementacji i zarządzania. Z kolei w badaniu Tøndela i in. dokonano przeglądu praktyk zarządzania incydentami bezpieczeństwa informacji, wskazując na znaczenie jasno zdefiniowanych ról i procedur w efektywnym reagowaniu na incydenty. **Analiza ta sugeruje, że dobrze zorganizowane i przejrzyste struktury mogą zwiększać skuteczność ochrony, podczas gdy nadmierna komplikacja może prowadzić do nieefektywności. Obie prace podkreślają, że równowaga między złożonością a przejrzystością organizacyjną jest kluczowa dla efektywnego zarządzania bezpieczeństwem informacji w ośrodkach ochrony.**

1.12 Role i obowiązki personelu ochrony

Podrozdział jest ważnym elementem analizy tezy dotyczącej efektywności systemów ochrony informacji. Skupia się on na zrozumieniu, jak przypisane role i obowiązki wpływają na skuteczność ochrony danych w systemach teleinformatycznych. Dokładne przyjrzenie się, jakie funkcje pełnią członkowie personelu ochrony, oraz jakie mają zadania, pozwala ocenić, czy skomplikowana struktura ról i obowiązków rzeczywiście przyczynia się do zwiększenia bezpieczeństwa, czy też może prowadzić do nieefektywności i błędów w zabezpieczeniach. Poprzez analizę przydzielonych zadań, odpowiedzialności i kompetencji, można sprawdzić, czy bardziej rozbudowane i specjalistyczne podejście do zarządzania bezpieczeństwem przynosi wymierne korzyści, czy też może prostsze, bardziej zintegrowane rozwiązania są równie skuteczne. W kontekście badanej tezy, ten podrozdział pomoże ustalić, w jaki sposób organizacja ról i obowiązków personelu wpływa na zdolność systemów ochrony do efektywnego przeciwdziałania zagrożeniom.

[60] Vielberth, Manfred, et al. "Security Operations Center: A Systematic Study and Open Challenges." *IEEE Access*, vol. 8, 2020, pp. 227756–227779. IEEE, https://doi.org/10.1109/ACCESS.2020.3045514

W analizie efektywności systemów ochrony informacji, istotne jest zrozumienie wpływu przypisanych ról i obowiązków personelu na skuteczność zabezpieczeń. W badaniu przeprowadzonym przez Hina i in.[61] autorzy przedstawili wielowarstwową perspektywę odpowiedzialności w cyberbezpieczeństwie, podkreślając znaczenie zaangażowania różnych interesariuszy, w tym liderów organizacji, w kształtowanie kultury bezpieczeństwa. Z kolei w pracy [62] omówiono rolę świadomości polityki cyberbezpieczeństwa w zwiększaniu zdolności reaktywnych w łańcuchu dostaw, wskazując, że jasne określenie obowiązków personelu oraz ich świadomość polityki bezpieczeństwa przyczyniają się do lepszej odporności na incydenty. Obie prace sugerują, że odpowiednie przypisanie ról i obowiązków oraz zwiększanie świadomości personelu są kluczowe dla skuteczności systemów ochrony informacji.

W **skład personelu** Pionu Ochrony Informacji Niejawnych **nadzorującego** pracę systemu teleinformatycznego wchodzą[63]:

1. **Kierownik Jednostki Organizacyjnej** [w skrócie **KJO**] **–** odpowiada za ochronę informacji niejawnych (organizację i nadzór)
2. **Pełnomocnik ds. ochrony informacji niejawnych** [w skrócie **POIN**] **–** odpowiada za przestrzeganie przepisów o ochronie informacji niejawnych (procedury i kontrole).
3. **Kierownik Kancelarii Tajnej** [w skrócie **KKT**] **–** odpowiada za rejestrację i obieg informacji niejawnych.
4. **Administrator Systemu** [w skrócie **AS**] – odpowiada za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych w szczególnych wymaganiach bezpieczeństwa oraz procedurach bezpiecznej eksploatacji systemu.
5. **Inspektor Bezpieczeństwa Teleinformatycznego lub Systemu Teleinformatycznego** [w skrócie **IBT**] – odpowiada za weryfikację i bieżącą

[61] Hina, S., et al. "Being Responsible in Cybersecurity: A Multi-Layered Perspective." Information Systems Frontiers, 2025. Springer, https://doi.org/10.1007/s10796-025-10588-0

[62] Lai-Wan Wong, Voon-Hsien Lee, Garry Wei-Han Tan, Keng-Boon Ooi, Amrik Sohal. "The Role of Cybersecurity and Policy Awareness in Shifting Employee Behavior." Journal of Strategic Information Systems, 2022. https://doi.org/10.1016/j.ijinfomgt.2022.102520

[63] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych - regulacje dotyczące zasad ochrony informacji niejawnych, w tym wskazania odpowiedzialności poszczególnych osób.

kontrolę zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji.

Członkowie personelu Pionu Ochrony Informacji Niejawnych pełnią różne role i mają zróżnicowany zakres odpowiedzialności.[64]

Kierownik Jednostki Organizacyjnej jest odpowiedzialny za ochronę informacji niejawnych, w tym za ochronę informacji niejawnych przetwarzanych w systemie teleinformatycznym – zgodnie z art. 14. Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Do jego zakresu jego obowiązków i odpowiedzialności należy w szczególności:

- tworzenie odpowiednich warunków organizacyjnych i finansowych w celu zapewnienia właściwego poziomu ochrony, przetwarzanych w systemie teleinformatycznym, informacji niejawnych,
- powołanie i obsada stanowisk pełnomocnika ochrony, kierownika kancelarii tajnej oraz inspektora bezpieczeństwa teleinformatycznego,
- wyznaczanie i odwoływanie na stanowisko Administratora Systemu;
- przedstawianie ABW/SKW szczególnych wymagań bezpieczeństwa oraz procedur bezpiecznej eksploatacji,
- wyrażenie zgody na dostęp do zasobów systemu teleinformatycznego.

Pełnomocnik ds. Ochrony Informacji Niejawnych odpowiada za zapewnienie ochrony informacji niejawnych w jednostce organizacyjnej, w tym również w odniesieniu do systemu teleinformatycznego – zgodnie z art. 14., ust. 2. Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Jego szczegółowe obowiązki obejmują:

- kierowanie i odpowiedzialność za terminową i rzetelną realizację zadań Pionu Ochrony Informacji Niejawnych w zakresie spraw związanych z zapewnieniem ochrony informacji niejawnych, określonych w dokumentach ustawowych, normatywnych i innych, odrębnie określanych przez Kierownika Jednostki Organizacyjnej,

[64] Art. 14. Ustawy o ochronie informacji niejawnych - odnosi się do obowiązków i odpowiedzialności . Przepis ten szczegółowo opisuje odpowiedzialność KJO za ochronę informacji niejawnych

- opracowywanie i wdrażanie przedsięwzięć związanych z realizacją zadań wynikających z Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych oraz obowiązujących w tym zakresie dokumentów wykonawczych (rozporządzenia, zarządzenia, zalecenia i wytyczne ABW lub SKW),
- udział w pracach zespołu ds. zarządzania ryzykiem w systemie teleinformatycznego, zgodnie z wymaganiami określonymi w Rozporządzeniu Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego,
- zapewnienie ochrony eksploatowanych systemów teleinformatycznych przetwarzających informacje niejawne (w tym systemu teleinformatycznego) oraz zapewnienie jego ochrony fizycznej,
- opracowywanie i aktualizowanie, wymagającego akceptacji Kierownika Jednostki Organizacyjnej, Planu ochrony informacji niejawnych, w tym w razie wprowadzenia stanu nadzwyczajnego nadzorowanie jego realizacji,
- sprawowanie nadzoru nad funkcjonowaniem systemu ochrony, a w szczególności ochrony pomieszczeń podlegających szczególnej ochronie, w tym funkcjonowaniem i eksploatacją zainstalowanych systemów i urządzeń alarmowych (SSWiN), kontroli dostępu (SKD),
- organizowanie systemu przepustek i nadzorowanie realizacji przedsięwzięć w tym zakresie,
- bieżące nadzorowanie stosowania środków ochrony fizycznej,
- zapewnienie bezpieczeństwa fizycznego w strefach ochronnych,
- opracowywanie i przekazywanie do KJO potrzeb finansowych, związanych z właściwym funkcjonowaniem systemu ochrony informacji niejawnych, w tym systemów teleinformatycznych do przetwarzania informacji niejawnych,
- organizowanie i uczestniczenie w opracowywaniu dokumentów regulujących problematykę ochrony informacji niejawnych, przetwarzanych w systemach teleinformatycznych,
- opracowanie programów organizacyjno-użytkowych, projektów koncepcyjnych i technicznych związanych z budową systemów teleinformatycznych,
- opracowanie dokumentacji bezpieczeństwa teleinformatycznego,

- bieżące informowanie Kierownika Jednostki Organizacyjnej o przebiegu współpracy z Agencją Bezpieczeństwa Wewnętrznego lub Służbą Kontrwywiadu Wojskowego,
- powiadamianie Kierownika Jednostki Organizacyjnej o przypadkach stwierdzonych naruszeń przepisów o ochronie informacji niejawnych i podejmowanie niezwłocznie działań zmierzających do wyjaśnienia okoliczności tych naruszeń oraz ograniczenia ich negatywnych skutków,
- przeprowadzanie zwykłych postępowań sprawdzających na pisemne polecenie Kierownika Jednostki Organizacyjnej,
- powiadamianie Agencji Bezpieczeństwa Wewnętrznego lub Służby Kontrwywiadu Wojskowego o naruszeniu przepisów o ochronie informacji niejawnych oznaczonych klauzulą Poufne lub wyższą,
- występowanie z wnioskiem do Kierownika Jednostki Organizacyjnej o wyznaczenie Kierownika Kancelarii Tajnej/Kancelarii Tajnej Międzynarodowej oraz wyznaczanie pracownika, posiadającego stosowne poświadczenie bezpieczeństwa,
- przeprowadzanie kontroli ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji,
- okresowych (co najmniej raz na trzy lata) kontroli ewidencji, materiałów i obiegu dokumentów niejawnych,
- opracowanie i przedkładanie do zatwierdzenia Kierownikowi Jednostki Organizacyjnej instrukcji dotyczącej sposobu i trybu przetwarzania informacji niejawnych oraz zakresu i warunków stosowania środków bezpieczeństwa fizycznego w celu ich ochrony,
- opracowanie i przedkładanie do zatwierdzenia Kierownikowi Jednostki Organizacyjnej dokumentacji określającej poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą,
- planowanie, organizowanie oraz przeprowadzanie szkoleń z zakresu ochrony informacji niejawnych dla pracowników Pionu Ochrony Informacji Niejawnych oraz personelu systemu teleinformatycznego i wydawanie zaświadczeń, stwierdzających odbycie tego przeszkolenia,

- prowadzenie aktualnego wykazu osób zatrudnionych albo wykonujących czynności zlecone, które posiadają uprawnienia do dostępu do informacji niejawnych, oraz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto.

Kierownik Kancelarii Tajnej jest odpowiedzialny za:[65]

- bezpośredni nadzór nad obiegiem dokumentów,
- udostępnianie lub wydawanie dokumentów osobom do tego uprawnionym,
- egzekwowanie zwrotu dokumentów,
- kontrolę przestrzegania właściwego oznaczania i rejestrowania dokumentów w kancelarii oraz jednostce organizacyjnej,
- prowadzenie bieżącej kontroli postępowania z dokumentami,
- wykonywanie poleceń pełnomocnika ochrony,

Inspektora Bezpieczeństwa Teleinformatycznego jest odpowiedzialny za weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego ze Szczególnymi Wymaganiami Bezpieczeństwa oraz przestrzegania Procedur Bezpiecznej Eksploatacji – zgodnie z art. 52 Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Do podstawowych obowiązków Inspektora Bezpieczeństwa Teleinformatycznego należy:

- prowadzenie kontroli poprawności realizacji zadań przez Administratora Systemu, w tym właściwe zarządzania konfiguracją systemu teleinformatycznego oraz uprawnieniami przydzielanymi użytkownikom,
- prowadzenie kontroli znajomości i przestrzegania przez użytkowników systemu zasad ochrony informacji niejawnych oraz procedur bezpiecznej eksploatacji w systemie teleinformatycznym, w zakresie wykorzystywania urządzeń i narzędzi służących do ochrony informacji niejawnych,

[65] Rozporządzenie Rady Ministrów z dnia 1 czerwca 2010 r. w sprawie organizacji i funkcjonowania kancelarii tajnych

- prowadzenie kontroli stanu zabezpieczeń systemu teleinformatycznego, w tym poprzez analizowanie i archiwizowanie rejestrów zdarzeń w systemie (twz. logów),
- prowadzenie aktualnego wykazu osób mających uprawnienia do dostępu do systemu,
- prowadzenie kontroli poprawności przydzielania kont użytkownikom i zakresu uprawnień nadanych użytkownikom,
- udział w pracy zespołu ds. zarządzania ryzykiem, zgodnie z wymaganiami określonymi w Rozporządzeniu Prezesa Rady Ministrów z dnia 20 lipca 2011r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego,
- przeprowadzanie okresowo testów bezpieczeństwa systemu zgodnie z zatwierdzonym planem testów,
- informowanie Pełnomocnika ds. Ochrony Informacji Niejawnych o wszelkich zdarzeniach związanych lub mogących mieć związek z bezpieczeństwem informacji niejawnych w systemie,
- uczestniczenie w opracowywaniu programów organizacyjno-użytkowych oraz projektów koncepcyjnych i technicznych, wykonywanych w związku z budową niejawnych systemów teleinformatycznych oraz w opracowywaniu dokumentacji bezpieczeństwa teleinformatycznego;
- monitorowanie zmian (np. w funkcjonowaniu mechanizmów zabezpieczeń, aktualizacji oprogramowania),
- reagowanie na sygnały o incydentach w zakresie bezpieczeństwa, wyjaśnianie ich przyczyn,
- przeprowadzanie okresowej analizy zagrożeń;
- tworzenie planów awaryjnych i organizowanie treningów w ich realizacji;
- prowadzenie Dziennika Inspektora Bezpieczeństwa Teleinformatycznego, w którym odnotowuje się wszystkie zdarzenia mające wpływ na bezpieczeństwo systemu oraz informacje o przeprowadzonych okresowych kontrolach czynności wykonywanych przez administratora systemu.

Administrator Systemu jest odpowiedzialny za funkcjonowanie systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa

przewidzianych dla tego systemu - zgodnie z art. 52 Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Do podstawowych obowiązków Administratora Systemu należy:

- udział w przygotowaniu i aktualizacji Szczególnych Wymagań Bezpieczeństwa i Procedur Bezpiecznej Eksploatacji systemów teleinformatycznych do przetwarzania informacji niejawnych,
- udział w pracy zespołu ds. zarządzania ryzykiem, zgodnie z wymaganiami określonymi w Rozporządzeniu Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego,
- przechowywanie i nadzór nad zatwierdzoną dokumentacją bezpieczeństwa teleinformatycznego systemu oraz udostępnianie odpowiednich procedur Użytkownikom systemu,
- wdrażanie Procedur Bezpiecznej Eksploatacji,
- wdrażanie środków zabezpieczających w systemie,
- szkolenie użytkowników systemu teleinformatycznego w zakresie jego bezpiecznej eksploatacji,
- współpraca z Inspektorem Bezpieczeństwa Teleinformatycznego, w zakresie zarządzania bezpieczeństwem systemu,
- wykonywanie okresowo wraz z Inspektorem Bezpieczeństwa Teleinformatycznego testów bezpieczeństwa systemu zgodnie z zatwierdzonym planem testów,
- konfigurowanie urządzeń wchodzących w skład systemu teleinformatycznego i oprogramowania systemu,
- utrzymywanie zgodności konfiguracji i parametrów systemu teleinformatycznego z jego dokumentacją bezpieczeństwa oraz innymi dokumentami normatywnymi,
- zapewnienie zgodności rozwiązań technicznych i programowych systemu teleinformatycznego z wymaganiami w dokumentacji bezpieczeństwa,
- zapewnienie, aby wszyscy użytkownicy systemu teleinformatycznego byli zapoznani z obowiązującymi w systemie zasadami i procedurami bezpieczeństwa,
- bieżąca kontrola przestrzegania zasad bezpieczeństwa oraz realizacji Procedur Bezpiecznej Eksploatacji przez użytkowników systemu,

- systematyczne kontrolowanie funkcjonowania mechanizmów zabezpieczeń oraz poprawności działania systemu,
- monitorowanie zmian (np. w funkcjonowaniu mechanizmów zabezpieczeń),
- przeglądanie plików zawierających informacje o wybranych zdarzeniach w systemie – logów systemowych przy współudziale Inspektora Bezpieczeństwa Teleinformatycznego,
- reagowanie na sygnały o incydentach w zakresie bezpieczeństwa i usuwanie ich skutków,
- prowadzenie ewidencji sprzętu i oprogramowania,
- zarządzanie kontami użytkowników systemu teleinformatycznego (na polecenie Kierownika Jednostki Organizacyjnej), wdrażanie uprawnień w systemie wynikających z przydzielonych praw dostępu oraz przydzielanie pierwszych haseł dostępu dla użytkowników systemu,
- wyłączanie kont tych użytkowników, którzy utracili formalne uprawnienia do pracy (np. zostali przeniesieni bądź zwolnieni, przebywają na urlopie bezpłatnym), co dotyczy to zwłaszcza osób zatrudnionych na czas określony,
- przygotowanie i utrzymywanie wykazu osób zapoznanych z Procedurami Bezpiecznej Eksploatacji,
- prowadzenie wyrywkowych kontroli sprawdzających czy użytkownicy nie mają szerszego dostępu do zasobów systemu niż wynika to z pierwotnie przydzielonych im uprawnień,
- współpraca z użytkownikami systemu w celu uniknięcia powtarzających się błędów w działaniach użytkowników i określanie ich przyczyn,
- przygotowywanie i utrzymywanie dokumentacji zawierającej bieżące dane z eksploatacji systemu zgodne z Procedurami Bezpiecznej Eksploatacji takich jak wykazy użytkowników, rejestr szkoleń, wykaz sprzętu i oprogramowania, rejestr przeglądów i serwisowania elementów systemu, wykaz zmian w Procedurach Bezpiecznej Eksploatacji,
- wykonywanie kopii zapasowych systemu operacyjnego oraz archiwizowanie systemowego dziennika zdarzeń systemu wspólnie z Inspektorem Bezpieczeństwa Teleinformatycznego,

- informowanie Pełnomocnika ds. Ochrony Informacji Niejawnych o wszelkich wykrytych lukach, naruszeniach i zagrożeniach w systemie,
- zgłaszanie Pełnomocnikowi ds. Ochrony Informacji Niejawnych potrzeb w zakresie serwisowania urządzeń systemu,
- prowadzenie Dziennika Administratora.

Użytkownicy Systemu są natomiast odpowiedzialni za:

- właściwa organizacja ochrony wszystkich zasobów (technicznych i informacyjnych) wykorzystywanych w systemie teleinformatycznym,
- traktowanie każdej utraty lub celowego uszkodzenia jakiegokolwiek informatycznego nośnika danych zwierającego informacje niejawne jako incydentu bezpieczeństwa teleinformatycznego i natychmiastowe zgłaszanie tego incydentu do Pełnomocnika ds. Ochrony Informacji Niejawnych,
- przestrzeganie wszystkich procedur bezpiecznej eksploatacji, które dotyczą użytkowników systemu, a w szczególności dotyczących: uruchamiania, zamykania systemu, kończenia pracy w systemie,
- przeciwdziałania infekcjom wirusowym,
- oznaczania, rejestrowania, obiegu i niszczenia dokumentów,
- postępowanie zgodnie z procedurami bezpiecznej eksploatacji w przypadku pożaru i zaistnienia zagrożeń środowiskowych,
- przestrzegania zakazu wprowadzania do systemu oprogramowania bez wiedzy i zgody Administratora Systemu,
- wykorzystywania w systemie oprogramowania nie wchodzącego w skład konfiguracji zgodnej z zatwierdzoną dokumentacją bezpieczeństwa,
- używania informatycznych nośników danych niejawnych o klauzuli nie wyższej niż klauzula wykorzystywanego dysku twardego z systemem operacyjnym,
- nie przetwarzanie dokumentów niejawnych o klauzuli wyższej niż klauzula systemu,
- właściwe tworzenie i zmiana haseł dostępu do systemu, zgodnie z odpowiednią procedurą bezpiecznej eksploatacji,
- niezwłoczne informowanie personelu POIN o wszystkich nieprawidłowościach w pracy systemu teleinformatycznego,

- przekazywanie do Kancelarii Tajnej wykorzystywanych dokumentów niejawnych i informatycznych nośników danych niejawnych, w przypadku braku warunków do ich przechowywania w pomieszczeniu służbowym zgodnie z obowiązującymi przepisami,
- podejmowanie decyzji o niszczeniu niejawnych dokumentów roboczych, (kontrolnych, niepełnowartościowych) wytworzonych w trakcie realizacji zadań (projektów) w porozumieniu z Kierownikiem Kancelarii Tajnej,
- niezwłoczna rejestracja wytworzonych dokumentów niejawnych w Kancelarii Tajnej,
- udział w szkoleniach organizowanych przez personel Pionu Ochrony Informacji Niejawnych

1.13 Podsumowanie Rozdziału 1

Rozdział pierwszy niniejszej rozprawy doktorskiej stanowi wszechstronne wprowadzenie do problematyki ochrony informacji, integrując analizę aktualnego stanu wiedzy z kluczowymi aspektami zapewnienia bezpieczeństwa systemów teleinformatycznych. Szczegółowo omówiono w nim podstawowe kategorie informacji wymagających ochrony oraz proces ich klasyfikacji, co jest istotne dla skutecznego zarządzania bezpieczeństwem informacji.

W kontekście klasyfikacji informacji, badanie przeprowadzone przez Zadeh i in.[66] proponuje ramy kwantyfikacji i klasyfikacji ryzyka cybernetycznego, adresując istotną lukę badawczą w ocenie naruszeń bezpieczeństwa. Autorzy podkreślają znaczenie precyzyjnej klasyfikacji informacji w celu skutecznego zarządzania ryzykiem.

Analiza cyklu funkcjonowania systemu teleinformatycznego uwzględnia kluczowe mechanizmy ochrony informacji, takie jak integralność, poufność i dostępność danych. W tym zakresie, praca Diesch i in. [67] przedstawia kompleksowy model czynników

[66] Amir Zadeh, Brandon Lavine, Hamed Zolbanin, Donald Hopkins. "A cybersecurity risk quantification and classification framework for informed risk mitigation decisions." Decision Analytics Journal Volume 9, December 2023, https://doi.org/10.1016/j.dajour.2023.100328

[67] Rainer Diesch, Matthias Pfaff, Helmut Krcmar. "A Comprehensive Model of Information Security Factors for Decision-Makers." Computers & Security, vol. 92, 2020, https://doi.org/10.1016/j.cose.2020.101747

bezpieczeństwa informacji, który wspiera decydentów w podejmowaniu świadomych decyzji dotyczących ochrony danych.

Rozdział ten dostarcza również istotnych informacji na temat różnych czynników i zagrożeń wpływających na bezpieczeństwo informacji, podkreślając znaczenie zarządzania ryzykiem i minimalizacji potencjalnych zagrożeń. Przegląd literatury dokonany przez Cremer i in[68] analizuje dostępność danych w kontekście ryzyka, wskazując na potrzebę skutecznego zarządzania ryzykiem w celu ochrony zasobów informacyjnych.

W kontekście badanej tezy, rozdział ten odgrywa istotną rolę, dostarczając teoretycznego tła dla oceny skuteczności różnych mechanizmów ochrony informacji. Poprzez zrozumienie aktualnych metod klasyfikacji i zabezpieczeń, możliwe jest ocenienie, czy bardziej rozbudowane systemy ochrony rzeczywiście oferują lepszą efektywność w porównaniu do prostszych, ale lepiej dopasowanych rozwiązań. W związku z tym, rozdział stanowi istotny krok w kierunku weryfikacji tezy badawczej i opracowania skuteczniejszych strategii ochrony informacji.

[68] Frank Cremer, Barry Sheehan, Michael Fortmann, Arash N. Kia, Martin Mullins, Finbarr Murphy & Stefan Materne . "Cyber Risk and Cybersecurity: A Systematic Review of Data Availability." The Geneva Papers on Risk and Insurance - Issues and Practice (2022) 47:698–736, https://doi.org/10.1057/s41288-022-00266-6

ROZDZIAŁ 2
Ocena poziomu bezpieczeństwa w świetle własnych badań

Rozdział drugi stanowi element rozprawy, w którym zaprezentowane i przeanalizowane są wyniki przeprowadzonych badań. Rozdział ten ma na celu weryfikację głównej tezy, że **zastosowanie zbyt złożonych metod oceny bezpieczeństwa systemów w procesie ich akredytacji, może paradoksalnie prowadzić do obniżenia ich poziomu bezpieczeństwa**, pomimo ich zgodności z normami i zaleceniami branżowymi, wraz z tezą pomocniczą, która stwierdza, że **formalne modelowanie oraz analiza złożonych metod oceny bezpieczeństwa, dostarczają narzędzi do efektywnego zarządzania ryzykiem**, szczególnie w kontekście ochrony informacji niejawnych.

W ramach tego rozdziału podjęto próbę oceny rzeczywistego poziomu bezpieczeństwa systemów teleinformatycznych, analizując zarówno czynniki techniczne, jak i organizacyjne. Podrozdziały obejmują między innymi: **podstawowe definicje** związane z bezpieczeństwem informacji, **środowisko bezpieczeństwa**, a także procesy **identyfikacji i oszacowania wartości informacji** oraz **zasobów systemu**. Rozdział przedstawia również **identyfikację zagrożeń**, **podatności na ryzyka** oraz sposoby ich oszacowania. Istotnym elementem jest badanie **opinii interesariuszy ochrony informacji niejawnych**, które pozwala zrozumieć rzeczywiste potrzeby i postrzeganie złożonych metod ochrony.

Jednym z ważniejszych tematów jest także analiza **negatywnych aspektów złożoności metod ochrony informacji**, która pozwala lepiej zrozumieć, dlaczego bardziej rozbudowane mechanizmy mogą okazać się mniej efektywne. W końcowej części rozdziału przedstawiono **model formalny**, który umożliwia bardziej efektywną ocenę poziomu ryzyka i dostosowanie metod ochrony do rzeczywistych potrzeb systemu.

Rozdział ten pełni rolę w dowodzeniu tezy badawczej, ponieważ dostarcza nie tylko teoretycznych narzędzi do oceny poziomu bezpieczeństwa, ale również empirycznych dowodów na to, że nadmiernie złożone metody mogą prowadzić do nieskuteczności w praktyce. Przeprowadzona analiza oraz formalne modelowanie stanowią istotny wkład w lepsze zrozumienie zależności między skomplikowaniem metod ochrony a ich rzeczywistą efektywnością.

2.1 Podstawowe definicje

Podrozdział wprowadza pojęcia niezbędne do zrozumienia dalszych analiz związanych z oceną poziomu bezpieczeństwa informacji. Definiuje on terminologię, która będzie używana w kontekście badań empirycznych, w tym pojęcia takie jak bezpieczeństwo informacji, zagrożenia, podatności, ryzyko oraz zasoby systemu teleinformatycznego. Precyzyjne zrozumienie tych definicji jest niezbędne dla właściwego przeprowadzenia oceny i weryfikacji badanej tezy dotyczącej skuteczności różnych metod ochrony informacji.

W rozdziale drugim zastosowano następujące pojęcia:

Analiza ryzyka – proces polegający na rozpoznawaniu potencjalnych zagrożeń, ocenie ich wielkości oraz wskazaniu obszarów, które mogą być narażone na skutki tych zagrożeń.

Dostępność – cecha, która oznacza, że zasób w systemie teleinformatycznym jest dostępny do użytku przez uprawnione osoby, w określonym czasie, na ich żądanie.

Informowanie o ryzyku – przekazywanie informacji o pojawiających się zagrożeniach odpowiedzialnym za zarządzanie ryzykiem.

Integralność – właściwość zasobu systemu teleinformatycznego, która gwarantuje, że nie został on zmieniony w sposób nieuprawniony.

Monitorowanie ryzyka – proces stałego nadzorowania ryzyk związanych z użytkowaniem systemu teleinformatycznego, a także dostosowywania zabezpieczeń w odpowiedzi na pojawiające się zagrożenia, aby utrzymać ryzyko na akceptowalnym poziomie.

Podatność – słaba strona zasobu lub zabezpieczenia systemu, która może zostać wykorzystana przez zagrożenie.

Poufność – cecha, która zapewnia, że dostęp do informacji mają jedynie osoby upoważnione.

Przetwarzanie informacji niejawnych – wszystkie działania wykonywane na informacjach niejawnych, takie jak ich tworzenie, modyfikowanie, kopiowanie, klasyfikowanie, przechowywanie, przesyłanie oraz udostępnianie.

Ryzyko – w kontekście bezpieczeństwa informacji niejawnych, ryzyko oznacza kombinację prawdopodobieństwa wystąpienia niepożądanego zdarzenia i jego skutków.

Ryzyko szczątkowe – ryzyko, które pozostaje po zastosowaniu środków zaradczych i wymaga oceny oraz akceptacji.

System teleinformatyczny – zespół urządzeń i oprogramowania, które współpracują, umożliwiając przetwarzanie, przechowywanie, wysyłanie oraz odbieranie danych.

Szacowanie ryzyka – zgodnie z Ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych to proces obejmujący analizę i ocenę ryzyka.

Właściciel ryzyka – osoba lub podmiot odpowiedzialny za utrzymywanie zabezpieczeń na poziomie, który minimalizuje ryzyko do akceptowalnego poziomu.

Zabezpieczenia – środki, które mogą mieć charakter fizyczny, techniczny lub organizacyjny, a ich celem jest zmniejszenie poziomu ryzyka.

Zagrożenie – potencjalna przyczyna zdarzenia, które może wyrządzić szkody w zasobach systemu teleinformatycznego.

Zarządzanie ryzykiem – zorganizowane działania mające na celu zarządzanie bezpieczeństwem informacji, z uwzględnieniem występujących zagrożeń.

Zasoby systemu teleinformatycznego – wszelkie elementy przetwarzane w systemie, takie jak informacje, osoby, usługi, oprogramowanie, dane oraz sprzęt, które mają wpływ na bezpieczeństwo przetwarzanych informacji.

2.2 Rozpoznanie środowiska operacyjnego

Podrozdział koncentruje się na etapie rozpoznania środowiska, w którym funkcjonuje system teleinformatyczny. Zrozumienie tego środowiska jest niezbędne do identyfikacji potencjalnych zagrożeń i podatności, które mogą wpłynąć na bezpieczeństwo informacji i zasobów systemu. W podrozdziale omówione są aspekty fizycznej ochrony zasobów, takich jak pomieszczenia, sprzęt i miejsca składowania danych, a także znaczenie dokładnych schematów instalacji technicznych. Ten etap analizy umożliwia skuteczniejsze określenie poziomów ryzyka i wprowadzenie adekwatnych mechanizmów zabezpieczających. W kontekście analizy środowiska operacyjnego systemów teleinformatycznych, ważnym jest zrozumienie zarówno fizycznych, jak i cyfrowych aspektów wpływających na bezpieczeństwo informacji. Przeprowadzenie szczegółowego rozpoznania środowiska umożliwia identyfikację potencjalnych zagrożeń i podatności, co jest niezbędne do skutecznego zarządzania ryzykiem i wdrożenia odpowiednich mechanizmów ochronnych.

Badanie przeprowadzone przez Guzman i in.[69] podkreśla znaczenie zintegrowanej analizy bezpieczeństwa w systemach, wskazując na konieczność uwzględnienia zarówno aspektów cyfrowych, jak i fizycznych w ocenie podatności. Autorzy przedstawiają podejście, które łączy analizę ryzyka związanego z bezpieczeństwem informacji z oceną fizycznych zabezpieczeń, co pozwala na bardziej kompleksowe zrozumienie potencjalnych zagrożeń.

Z kolei w pracy Rehak i in.[70] omówiono konwergencję bezpieczeństwa w zakładach przemysłowych, zwracając uwagę na potrzebę integracji systemów bezpieczeństwa fizycznego i informatycznego. Autorzy wskazują, że takie podejście umożliwia lepsze zarządzanie ryzykiem oraz skuteczniejsze reagowanie na incydenty, które mogą mieć zarówno charakter fizyczny, jak i cyfrowy.

Analiza środowiska operacyjnego obejmuje również ocenę podatności fizycznych, takich jak zabezpieczenia pomieszczeń, sprzętu czy miejsc przechowywania danych. Dokładne schematy instalacji technicznych oraz znajomość infrastruktury są kluczowe dla identyfikacji potencjalnych słabych punktów systemu. W pracy DeSmit i in. [71] przedstawiono podejście do oceny podatności w inteligentnych systemach produkcyjnych, podkreślając znaczenie identyfikacji ścieżek ataku oraz oceny prawdopodobieństwa ich powodzenia.

W kontekście zarządzania ryzykiem, istotne jest również przeprowadzenie kompleksowej oceny zagrożeń i podatności. Jak wskazano w pracy Ralston i in.[72], ocena podatności polega na analizie podatności systemu na określone zagrożenia, co pozwala na skuteczniejsze planowanie działań ochronnych i minimalizację ryzyka.

Podsumowując, skuteczne rozpoznanie środowiska operacyjnego wymaga podejścia, które uwzględnia zarówno aspekty fizyczne, jak i cyfrowe. Integracja analiz

---

[69] Guzman, Nelson H. Carreras, Igor Kozine, and Mary Ann Lundteigen. "An integrated safety and security analysis for cyber-physical harm scenarios." Safety science 144 (2021): 105458.

[70] Rehak, David, et al. "Convergence of Safety and Security within Process Plants." Journal of Loss Prevention in the Process Industries (2025): 105579.

[71] DeSmit, Zach, et al. "An approach to cyber-physical vulnerability assessment for intelligent manufacturing systems." Journal of Manufacturing Systems 43 (2017): 339-351

[72] Ralston, Patricia AS, James H. Graham, and Jefferey L. Hieb. "Cyber security risk assessment for SCADA and DCS networks." ISA transactions 46.4 (2007): 583-594.

bezpieczeństwa, ocena podatności oraz znajomość infrastruktury technicznej są kluczowe dla zapewnienia wysokiego poziomu ochrony informacji w systemach teleinformatycznych.

Rozpoznanie środowiska, w którym działa system teleinformatyczny jest pierwszym etapem w określeniu potencjalnych zagrożeń dla zasobów systemu. W tym zadaniu przydatne mogą być szczegółowe plany pomieszczeń, na których zostanie zaznaczone rozmieszczenie zasobów systemu. Na tych planach lub szkicach sytuacyjnych powinny być uwzględnione miejsca, w których będą przetwarzane informacje o określonym stopniu poufności, a także zasoby materialne systemu, które wymagają ochrony. Przykładowymi zasobami, które wymagają ochrony, mogą być:

- Pomieszczenia, w których zainstalowany jest sprzęt teleinformatyczny. Ochrona tych pomieszczeń obejmuje zabezpieczenia fizyczne, takie jak kontrola dostępu, monitoring wideo, alarmy antywłamaniowe oraz odpowiednie warunki środowiskowe, takie jak kontrola temperatury i wilgotności, aby zapewnić prawidłowe działanie sprzętu. Zapobieganie nieupoważnionemu dostępowi do tych pomieszczeń jest niezwykle ważne dla zabezpieczenia danych i utrzymania stabilności systemu teleinformatycznego.
- Sprzęt teleinformatyczny w tym komputery, serwery, routery, przełączniki, drukarki, skanery, monitory, plotery, monitory, elementy wprowadzania i wyprowadzania informacji z/do systemu oraz urządzenia teleinformatyczne, które są kluczowe dla funkcjonowania systemu.
- Miejsca składowania danych, kopii zapasowych i archiwalnych.
- Pomieszczenia, w których pracują użytkownicy systemu oraz te szczególnie ważne dla działania systemu.

W fazie opisu środowiska należy uzyskać schematy sieci elektrycznej, wodnokanalizacyjnej, systemu ogrzewania, wentylacyjnej i klimatyzacyjnej. Schematy są niezbędne do identyfikacji potencjalnych zagrożeń oraz podatności i tym samym oceny ryzyka związanego z możliwym nieprawidłowym funkcjonowaniem tych systemów (awarie zasilania, zalania, awarie ogrzewania czy problemy z wentylacją i klimatyzacją). Posiadanie tej wiedzy pozwala w późniejszych etapach określić poziomy ryzyk co daje możliwość wprowadzenia mechanizmów je niwelujących.

2.3 **Identyfikacja informacji podlegających ochronie**

Podrozdział odnosi się do kluczowego etapu analizy bezpieczeństwa systemów teleinformatycznych, jakim jest dokładna identyfikacja przetwarzanych informacji oraz oszacowanie ich wartości. Proces ten pozwala na określenie poufności, integralności i dostępności informacji, co jest niezbędne do właściwego zarządzania ryzykiem. Podrozdział ten omawia także metody klasyfikacji informacji według klauzul tajności oraz ustalenie ich wagi dla organizacji i państwa, co bezpośrednio wpływa na dalsze decyzje dotyczące poziomu zabezpieczeń.

W kontekście identyfikacji informacji podlegających ochronie w systemach teleinformatycznych, kluczowe jest precyzyjne określenie wartości przetwarzanych danych oraz ich klasyfikacja pod kątem poufności, integralności i dostępności. Proces ten stanowi fundament skutecznego zarządzania ryzykiem i implementacji adekwatnych mechanizmów zabezpieczających.

Badanie przeprowadzone przez Rahmana i in.[73] przedstawia metodologię, która integruje wytyczne proceduralne z praktycznymi metrykami oceny dla organizacyjnej oceny ryzyka IT i cyberbezpieczeństwa. Autorzy podkreślają znaczenie systematycznej identyfikacji aktywów informacyjnych oraz oceny ich wartości w kontekście poufności, integralności i dostępności, co jest niezbędne do skutecznego zarządzania ryzykiem i ochrony kluczowych zasobów organizacji.

Z kolei Mouanda[74] analizuje różnice między bezpieczeństwem informacji a zapewnieniem informacji, koncentrując się na znaczeniu identyfikacji i klasyfikacji informacji w kontekście zarządzania ryzykiem. Autor wskazuje, że dokładna identyfikacja informacji podlegających ochronie pozwala na lepsze dostosowanie strategii bezpieczeństwa do rzeczywistych potrzeb organizacji, minimalizując ryzyko naruszeń i strat. Ponadto, standard ISO/IEC 27005:2022 dostarcza wytycznych dotyczących zarządzania ryzykiem bezpieczeństwa informacji, kładąc nacisk na proces identyfikacji, oceny i traktowania ryzyka związanego z aktywami informacyjnymi. Standard ten podkreśla znaczenie klasyfikacji informacji według ich wartości i wrażliwości, co umożliwia

[73] Rahman, Mir Mehedi, et al. "AssessITS: Integrating procedural guidelines and practical evaluation metrics for organizational IT and Cybersecurity risk assessment." arXiv preprint arXiv:2410.01750 (2024).

[74] Mouanda, Guy. "Unseen Power of Information Assurance over Information Security." arXiv preprint arXiv:2411.00799 (2024).

skuteczne przypisanie odpowiednich poziomów ochrony i implementację adekwatnych środków bezpieczeństwa.

Skuteczna identyfikacja informacji podlegających ochronie wymaga zastosowania systematycznych metod oceny wartości danych oraz ich klasyfikacji pod kątem poufności, integralności i dostępności. Wykorzystanie ram zarządzania ryzykiem, takich jak 'AssessITS' czy wytyczne ISO/IEC 27005:2022, wspiera organizacje w efektywnym zarządzaniu bezpieczeństwem informacji i minimalizacji potencjalnych zagrożeń

Rozpoznanie informacji obejmuje ustalenie ich cech, miejsca przechowywania, metod przetwarzania oraz ewentualnych oznaczeń. Wszelkie zasoby informacyjne w systemie muszą być sklasyfikowane według ich rodzaju oraz lokalizacji przetwarzania. W obrębie każdej kategorii informacji konieczne jest dokonanie podziału na podkategorie zgodnie z przypisanymi im klauzulami niejawności.

Wartość informacji niejawnych przetwarzanych w systemach teleinformatycznego można oszacować poprzez rozmowy z właścicielem tych informacji lub innymi autorytetami w zakresie ich oceny. Metoda jakościowa może być zastosowana do oszacowania wartości informacji, przy użyciu skali, na której klasyfikuje się informacje jako niskie, średnie lub wysokie. W tym podejściu uwzględniane są zarówno straty bezpośrednie, jak i pośrednie, które mogą wyniknąć dla jednostki organizacyjnej lub państwa w przypadku nieautoryzowanego ujawnienia, utraty, modyfikacji lub braku dostępu do danej informacji niejawnej.

Administrator systemu, Inspektor Bezpieczeństwa Teleinformatycznego, Pełnomocnik ds. Ochrony Informacji Niejawnych oraz Kierownik Jednostki Organizacyjnej przeprowadzają wspólnie proces szacowanie ryzyka w którym to identyfikują wszystkie klauzule dotyczące poufnych danych w systemie teleinformatycznym oraz ustalają, w jaki sposób te informacje wpływają na działania jednostki organizacyjnej. Zakres przeprowadzonych ustaleń powinien być ściśle dostosowany do określonego zakresu analizy ryzyka. Efektem pracy będzie stworzenie wykazu zasobów informacyjnych, zorganizowanych według rodzaju oraz klauzuli tajności. Każda kategoria zostanie opisana poprzez unikalny zbiór wymagań dotyczących ich funkcjonowania i zabezpieczeń, obejmujących aspekty integralności, poufności i dostępności.

Proces identyfikacji informacji niejawnych powinien kończyć się stworzeniem zorganizowanego spisu tych informacji, uporządkowanego według hierarchii ich ważności oraz oszacowanych konsekwencji nieuprawnionego ujawnienia, utraty, modyfikacji lub

braku dostępu do nich. Taki wykaz informacji niejawnych powinien następnie zostać zatwierdzony przez kierownika jednostki organizacyjnej.

Właścicielem informacji niejawnych jest osoba, która ma upoważnienie do podpisywania odpowiednich dokumentów[75]. Ta osoba, nadając klauzulę tajności konkretnej informacji, określa jej poziom wrażliwości w kontekście atrybutu „poufność". Określa tym samym potencjalne skutki nieuprawnionego ujawnienia tej informacji, które są mierzone na podstawie możliwych szkód zarówno dla jednostki organizacyjnej, jak i dla państwa.

2.4 Identyfikacja zasobów podlegających ochronie

Zrozumienie wartości zasobów pozwala na skuteczniejsze i bardziej dostosowane podejście do oceny ryzyka, co jest niezbędne do uniknięcia nieefektywnych rozwiązań. **W kontekście tezy pomocniczej,** identyfikacja zasobów i ich wartości umożliwia modelowanie ryzyka oraz zastosowanie formalnych analiz, co dostarcza narzędzi do bardziej precyzyjnego określenia poziomu ryzyka i skuteczności środków ochrony. W ten sposób, proces ten wspiera argumentację o konieczności uproszczenia metod oceny, a także dostarcza solidnych podstaw do dalszych badań w obszarze bezpieczeństwa informacji.

Zespół ds. analizy ryzyka, przy aktywnym zaangażowaniu kierownika jednostki organizacyjnej oraz specjalistów zajmujących się bezpieczeństwem i funkcjonowaniem systemów teleinformatycznych, jest zobowiązany do przygotowania spisu wszystkich kluczowych aktywów systemu teleinformatycznego, które mają istotne znaczenie dla zapewnienia ochrony przetwarzanych w nim informacji poufnych.

Proces identyfikacji zasobów systemu teleinformatycznego, które wymagają ochrony, obejmuje zarówno aktywa materialne, takie jak dyski, monitory, kable sieciowe, nośniki kopii zapasowych, oprogramowanie, dokumentacja związana z funkcjonowaniem systemu i jego bezpieczeństwem, a także podręczniki i inne fizyczne elementy, jak i aktywa niematerialne. Do aktywów niematerialnych zalicza się aspekty takie jak przeszkolony personel, który umożliwia ciągłość działania systemu, publiczny wizerunek jednostki organizacyjnej, reputacja, motywacja pracowników oraz relacje interpersonalne. Te elementy są brane pod uwagę tylko wtedy, gdy mają wpływ na bezpieczeństwo informacji

[75] Artykuł 6.1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2023 r. poz. 756, 1030).

oraz procesy przetwarzania oraz wykonywania zadań stawianych przed daną jednostką organizacyjną.

Zespół przeprowadzający analizę ryzyka jest odpowiedzialny za ocenę wartości zidentyfikowanych zasobów w kontekście ich roli w realizacji zadań systemu oraz wpływu na reputację i wiarygodność jednostki organizacyjnej. Dodatkowo, wartość tych zasobów powinna być oceniana z perspektywy potencjalnych strat, które wynikają z nieosiągniętych zysków, kosztów straconego czasu oraz kosztów naprawy lub wymiany niesprawnych elementów systemu.

Każda pozycja na sporządzonej liście powinna być skorelowana z potencjalnym szkodą, jaką jednostka organizacyjna mogłaby ponieść w przypadku utraty dostępności, integralności lub poufności informacji. W procesie oceny wartości zasobów, odpowiednie działy w jednostce organizacyjnej, takie jak dział finansowo-księgowy, dział planowania i inwestycji, powinny brać udział w celu dokładnego określenia tych potencjalnych strat i ich wpływu na organizację.

Rozpoznanie zasobów systemu oraz określenie ich wartości jest kluczowym krokiem, który pozwala na wyznaczenie obszarów, gdzie znajdują się najbardziej cenne aktywa. W rezultacie można skoncentrować najefektywniejsze środki ochronne na tych obszarach, co zwiększa bezpieczeństwo informacji i minimalizuje ryzyko ich utraty lub nieuprawnionego dostępu.

W przypadku niematerialnych elementów zasobów systemu, takich jak renoma firmy czy jej wizerunek, które są trudne do oceny przy użyciu tradycyjnych metod ilościowych, stosuje się różnorodne metody oceny, zarówno ilościowe, jak i jakościowe. Pozwala to na dokładniejsze określenie wartości tych niematerialnych aktywów oraz ich wpływu na organizację.

W efekcie prac zespołu powstanie lista zasobów systemu, które wymagają ochrony, a ta lista będzie uporządkowana w hierarchii ich znaczenia dla realizacji zadań przez jednostkę organizacyjną. Ostateczna lista zostanie zatwierdzona przez kierownika jednostki organizacyjnej, co będzie kluczowym etapem w procesie zapewnienia bezpieczeństwa tych zasobów oraz osiągnięcia celów organizacji.

2.5 Identyfikacja zagrożeń dla chronionego systemu

Podrozdział ma na celu zidentyfikowanie potencjalnych zagrożeń dla poufnych informacji przetwarzanych w systemach teleinformatycznych. Skupiając się na różnych

źródłach zagrożeń, zarówno wewnętrznych, jak i zewnętrznych, oraz ich możliwych skutkach, zespół odpowiedzialny za bezpieczeństwo może lepiej ocenić ryzyko, jakie niesie ze sobą każde zagrożenie. Oprócz klasyfikacji zagrożeń według prawdopodobieństwa wystąpienia, analiza ta jest istotna dla testowania tezy głównej, wskazując, że złożone metody oceny mogą być nieefektywne, gdy nie uwzględniają kluczowych ryzyk. W rezultacie, uporządkowanie zagrożeń według ich priorytetu umożliwia skoncentrowanie zasobów ochronnych tam, gdzie są one najbardziej potrzebne, co z kolei wspiera skuteczniejsze zarządzanie bezpieczeństwem informacji.

W kontekście identyfikacji zagrożeń dla systemów teleinformatycznych przetwarzających poufne informacje, kluczowe jest zrozumienie zarówno wewnętrznych, jak i zewnętrznych źródeł potencjalnych ataków oraz ich możliwych skutków. Systematyczna analiza tych zagrożeń pozwala zespołom ds. bezpieczeństwa na skuteczniejszą ocenę ryzyka i priorytetyzację działań ochronnych.

Standard ISO/IEC 27005:2022 dostarcza wytycznych dotyczących zarządzania ryzykiem bezpieczeństwa informacji, podkreślając znaczenie identyfikacji zagrożeń jako kluczowego etapu w procesie oceny ryzyka. Zaleca on systematyczne podejście do identyfikacji potencjalnych źródeł zagrożeń, co umożliwia lepsze zrozumienie ryzyka i skuteczniejsze jego zarządzanie.

W badaniu przeprowadzonym przez Sinha i in.[76] omówiono zastosowanie sztucznej inteligencji w ocenie ryzyka bezpieczeństwa informacji. Autorzy wskazują, że wykorzystanie narzędzi opartych na AI może znacząco skrócić czas potrzebny na wykrycie i neutralizację zagrożeń, co zwiększa odporność organizacji na ataki.

Ponadto, w pracy McCoya i in.[77] przedstawiono model relewancji do rankingowania podatności w oparciu o zagrożenia, który integruje dane z różnych źródeł w celu automatycznego priorytetyzowania podatności. Takie podejście pozwoliłoby organizacjom skupić zasoby na najbardziej krytycznych zagrożeniach, co jest kluczowe dla efektywnego zarządzania ryzykiem.

---

[76] Sinha, Aditya Roshan, Kunal Singla, and Teresa Matoso Manguangua Victor. "Artificial intelligence and machine learning for cybersecurity applications and challenges." Risk Detection and Cyber Security for the Success of Contemporary Computing (2023): 109-146.

[77] McCoy, Corren G. A relevance model for threat-centric ranking of cybersecurity vulnerabilities. Diss. Old Dominion University, 2022.

Zespół analizy ryzyka opracowuje listę wszystkich potencjalnych zagrożeń, które mogą prowadzić do nieuprawnionego ujawnienia, utraty, modyfikacji lub ograniczenia dostępu do informacji niejawnych przetwarzanych w systemach teleinformatycznych jednostki organizacyjnej. Konieczne jest zidentyfikowanie każdego zagrożenia dla opisanych wcześniej grup informacji niejawnych przetwarzanych w systemie oraz dla zasobów systemu, uwzględniając aspekty bezpieczeństwa informacji, takie jak naruszenie poufności, integralności lub dostępności. Utrata tych kluczowych cech związanych z ochroną informacji niejawnych niesie ze sobą ryzyko strat i szkód dla jednostki organizacyjnej lub państwa. Szkoda może wystąpić tylko wtedy, gdy określone, potencjalne zagrożenie koresponduje z podatnością systemu, którą to zagrożenie może wykorzystać.

Źródłami zagrożeń mogą być czynniki związane z naturą lub ludźmi, w tym pracownikami lub osobami spoza organizacji. Działania ludzkie mogą być zarówno przypadkowe, np. błędy lub zaniedbania, jak i celowe, np. kradzież, sabotaż, wandalizm, itp. Motywacje mogą obejmować chęć zysku, zemstę, ciekawość i inne. Każde zagrożenie powinno być opisane pod kątem źródła (czy jest zewnętrzne czy wewnętrzne), celu, motywacji (np. zysk finansowy, zemsta), stopnia potencjalnej szkodliwości (rozmiaru szkód mogących wyniknąć z tego zagrożenia, które wpłynąć mogą na ujawnienie/utrata, modyfikację lub ograniczenie dostępu do informacji niejawnych lub innych zasobów systemu), oraz częstotliwości występowania.

Wszystkie zidentyfikowane rodzaje zagrożeń dla informacji objętych klasyfikacją oraz zasobów systemu powinny zostać szczegółowo przedstawione, wraz z oszacowaniem prawdopodobieństwa ich wystąpienia. Prawdopodobieństwo to stanowi podstawę do określenia poziomu zagrożenia, który może być sklasyfikowany według trzystopniowej skali: niski, średni, lub wysoki. W przeciwieństwie do różnorodnych zasobów systemu, zagrożenia są ogólnego typu. Rodzaje zagrożeń i ich poziomy mogą ulec zmianie, dlatego proces szacowania zagrożeń powinien być regularnie aktualizowany. Dla zdarzeń okresowych, prawdopodobieństwo można oszacować statystycznie na podstawie dostępnych danych, takich jak raporty gromadzone przez jednostkę organizacyjną. Pewne oszacowania można pozyskać od różnych źródeł, w tym firm ubezpieczeniowych, instytutów meteorologicznych.

Dane dotyczące częstotliwości występowania klęsk żywiołowych obejmują całe otoczenie jednostki organizacyjnej. Zespół analizy ryzyka, przystępując do identyfikacji przewidywanych zagrożeń dla budowanego systemu, powinien w pierwszej kolejności

określić, kto mógłby być zainteresowany przetwarzanymi w systemie informacjami. Należy wziąć pod uwagę zagrożenia wynikające z źródeł zewnętrznych i wewnętrznych. Pośród pracowników jednostki organizacyjnej zagrożenia mogą wywołać także inni pracownicy mający dostęp do strefy ochronnej, np. personel pomocniczy (sprzątaczki, konserwatorzy itp.). Spośród źródeł zagrożeń zewnętrznych szczególne uwzględnienie wymagają atrakcyjność chronionych zasobów dla obcych wywiadów, konkurencji, przestępczości, dziennikarzy czy hakerów. Po ustaleniu potencjalnych źródeł zagrożeń konieczne jest określenie celu ataku, a także środków i metod, jakimi potencjalny sprawca mógłby się posłużyć.

Wypracowany wykaz przewidywanych zagrożeń dla informacji niejawnych i zasobów systemu, uporządkowany według malejącego prawdopodobieństwa ich wystąpienia, pozwala zidentyfikować obszary, w których środki ochrony powinny być wdrożone w pierwszej kolejności.

2.6 Identyfikacja podatności dla chronionego systemu

Podrozdział skupia się na identyfikacji słabych punktów systemów teleinformatycznych, które mogą być wykorzystane przez wcześniej zidentyfikowane zagrożenia. Ten proces jest kluczowy dla efektywnego zarządzania ryzykiem, ponieważ pozwala skoncentrować się na obszarach najbardziej narażonych na ataki. Podatności mogą wynikać z różnych źródeł, takich jak luki w zabezpieczeniach, błędy w zarządzaniu czy braki w szkoleniu personelu. Zrozumienie ich krytyczności umożliwia skoncentrowanie działań na ich eliminacji, co jest istotne w kontekście badanej tezy głównej, która podkreśla znaczenie skutecznych metod oceny bezpieczeństwa, uwzględniających identyfikację i ocenę podatności jako kluczowych elementów procesu akredytacji systemów, co w efekcie zwiększa bezpieczeństwo informacji w jednostce organizacyjnej.

W procesie zarządzania ryzykiem w systemach teleinformatycznych kluczowe jest zidentyfikowanie podatności, czyli słabych punktów, które mogą zostać wykorzystane przez potencjalne zagrożenia. Podatności te mogą wynikać z różnych źródeł, takich jak luki w zabezpieczeniach, błędy w zarządzaniu czy niedostateczne szkolenie personelu. Skuteczna identyfikacja i ocena tych podatności pozwala na priorytetyzację działań naprawczych oraz efektywne alokowanie zasobów w celu minimalizacji ryzyka.

W opracowaniu [78] przeprowadzonym przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) przedstawiono ramy oceny zdolności krajowych w zakresie cyberbezpieczeństwa, które podkreślają znaczenie systematycznej identyfikacji i analizy podatności w celu zwiększenia odporności systemów informacyjnych.

Ponadto, analiza [79] przeprowadzona przez amerykańską Agencję ds. Cyberbezpieczeństwa i Infrastruktury (CISA) w roku fiskalnym 2023 wykazała, że skuteczne zarządzanie podatnościami wymaga nie tylko ich identyfikacji, ale także priorytetyzacji działań naprawczych opartych na ryzyku kompromitacji. Raport podkreśla, że wiele naruszeń bezpieczeństwa wynika z niezałatanych, znanych podatności, co wskazuje na potrzebę usprawnienia procesów zarządzania nimi.

W kontekście polskim, raport [80] Najwyższej Izby Kontroli zwraca uwagę na konieczność stosowania zasad minimalizujących ryzyko nieuprawnionego dostępu do systemów informatycznych, co obejmuje regularne przeprowadzanie audytów bezpieczeństwa oraz aktualizację polityk zarządzania podatnościami.

Skuteczna identyfikacja i zarządzanie podatnościami w systemach teleinformatycznych są nieodzownymi elementami procesu zarządzania ryzykiem, które wymagają systematycznego podejścia, uwzględniającego zarówno aspekty techniczne, jak i organizacyjne.

Zespół analizy ryzyka ma także za zadanie opracować listę potencjalnych słabych punktów (czyli podatności) systemu teleinformatycznego. Ta lista powinna być uporządkowana według prawdopodobieństwa ich wykorzystania przez wcześniej zidentyfikowane zagrożenia, które mogą występować w środowisku eksploatacji systemu. Jest to etap, który pozwoli na skoncentrowanie uwagi na tych punktach, które są najbardziej narażone na potencjalne ataki i zagrożenia, co z kolei umożliwi lepsze zarządzanie ryzykiem i wzmocnienie ochrony systemu teleinformatycznego.

Podatność związana z przetwarzanymi informacjami poufnymi lub zasobami systemu teleinformatycznego (TI) oznacza dowolną wewnętrzną słabość lub lukę w systemie zabezpieczeń, która teoretycznie mogłaby być wykorzystana do spowodowania szkód w systemie TI lub działalności danej jednostki organizacyjnej. Innymi słowy, jest to

[78] ENISA. "Ramy Oceny Zdolności Krajowych." Grudzień 2020

[79] CISA. "Fiscal Year 2023 Risk and Vulnerability Assessments."

[80] NIK. "RealIzacja pRzez podmIoty państwowe zadań w zakresie ochrony cyberprzestrzenI RP" kpb-4101-002-00/2014, Czerwiec 2015

istniejący punkt, który stanowi potencjalne ryzyko i może być wykorzystany przez potencjalnych atakujących do naruszenia bezpieczeństwa informacji lub działalności organizacji. Takie podatności mogą mieć różne źródła. Po pierwsze mogą wynikać z luk w ochronie fizycznej systemu teleinformatycznego, co oznacza niedostateczne zabezpieczenia dostępu do sprzętu i infrastruktury. Po drugie, mogą także wynikać z niewłaściwych rozwiązań organizacyjnych, takich jak błędy w zarządzaniu bezpieczeństwem informacji. Po trzecie, mogą być spowodowane brakami lub lukami w procedurach dotyczących bezpiecznej eksploatacji systemu. Po czwarte, mogą wynikać z braku odpowiedniego szkolenia personelu, co prowadzi do nieświadomych naruszeń zasad bezpieczeństwa. Po piąte, mogą mieć źródło w błędach w oprogramowaniu lub wadliwym działaniu urządzeń, które tworzą potencjalne zagrożenia dla bezpieczeństwa informacji.

Podatność konkretnego systemu lub zasobu odnosi się do stopnia, w jakim ten system lub zasób jest podatny na potencjalne szkody lub ataki. Samo istnienie podatności nie jest przyczyną szkody; stanowi ono jedynie potencjalną lukę, która może być wykorzystana przez potencjalnych atakujących do spowodowania szkód. Na przykład, brak odpowiednich zabezpieczeń kryptograficznych przy przesyłaniu informacji niejawnych poza strefy ochronne jest przykładem podatności, która może stworzyć możliwość ujawnienia informacji. Ostateczna szkoda zależy od tego, czy atakujący wykorzysta tę podatność, dlatego zarządzanie i eliminacja podatności jest kluczowym elementem zapewnienia bezpieczeństwa informacji i systemów.

Definicja szkody często jest przedstawiana jako suma trzech elementów:

1. Zagrożenie – to potencjalne niebezpieczeństwo lub sytuacja, która może stanowić ryzyko dla systemu lub zasobu. Zagrożenie może wynikać z różnych czynników, takich jak atakujący, błąd ludzki, awarie sprzętu czy katastrofy naturalne.
2. Podatność – odnosi się do słabości lub luk w systemie lub zasobie, która może być potencjalnie wykorzystana przez atakującego. To jest punkt, który może zostać wykorzystany, aby spowodować szkody.
3. Atak – to próba wykorzystania podatności w celu spowodowania szkód lub naruszenia systemu lub zasobu. Atak może przybierać różne formy, w zależności od celów atakującego i rodzaju podatności.

Definicja ta pomaga zrozumieć, że szkoda nie wynika tylko z samego ataku, ale jest efektem połączenia zagrożenia, podatności i rzeczywistego działania atakującego.

Zarządzanie ryzykiem polega na minimalizowaniu podatności i odpowiednim reagowaniu na zagrożenia i ataki.

W każdym systemie teleinformatycznym (TI) lub jednostce organizacyjnej, nie wszystkie podatności będą wykorzystywane przez zagrożenia. Istotne jest przede wszystkim przeanalizowanie tych podatności, które są powiązane z konkretnymi zagrożeniami. Warto również uwzględnić zmiany zachodzące w środowisku oraz istniejące zabezpieczenia.

Oznacza to, że nie każda podatność stanowi natychmiastowe ryzyko, ale wartościowe jest zrozumienie, które z nich są najbardziej krytyczne w danym kontekście. Analiza ryzyka pozwala określić, które podatności mają potencjał do wywołania szkód i jakie kroki można podjąć, aby minimalizować te ryzyka. Przy uwzględnieniu zmian w środowisku i dostępnych środków ochronnych, można dostosować strategię zarządzania ryzykiem w celu lepszego zabezpieczenia systemu lub jednostki organizacyjnej.

Dla każdego elementu na liście słabych punktów systemu ważne jest oszacowanie prawdopodobieństwa ich wykorzystania przez wcześniej zidentyfikowane zagrożenia. To pozwoli na określenie poziomu podatności systemu, czyli przypisanie każdej zidentyfikowanej podatności jednej z wartości, takich jak "niski," "średni," lub "wysoki." Ocena ta może być dokonana na podstawie przeglądu urządzeń lub poprzez przeprowadzenie wywiadu z odpowiednim personelem odpowiedzialnym za bezpieczeństwo. Dzięki tej klasyfikacji można lepiej zrozumieć, które podatności są bardziej krytyczne i wymagają natychmiastowych działań w celu zwiększenia poziomu ochrony.

2.7 Określenie ryzyk dla chronionego systemu

W podrozdziale przedstawione jest jak zespół analizy ryzyka koncentruje się na ocenie prawdopodobieństwa wystąpienia zagrożeń związanych z istniejącymi podatnościami systemu teleinformatycznego. Kluczowym krokiem jest przegląd środków ochrony, aby ocenić ich adekwatność i skuteczność w kontekście wymogów bezpieczeństwa informacji niejawnych. Współpraca z odpowiednimi służbami bezpieczeństwa, jest istotna dla minimalizacji ryzyka. Proces oszacowania ryzyka powinien być realizowany dla każdego zidentyfikowanego zagrożenia, a rezultaty przedstawione kierownikowi jednostki, co umożliwi omówienie i akceptację działań zaradczych. Takie podejście jest zgodne z główną tezą badania, podkreślając potrzebę systematycznej oceny bezpieczeństwa, co w efekcie wspiera skuteczną ochronę informacji.

W analizie ryzyka w systemach teleinformatycznych kluczowe jest zrozumienie różnych metod oceny i zarządzania ryzykiem. W pracy Nalluri i in.[81] autorzy przedstawiają hybrydowe podejście oparte na logice rozmytej do oceny ryzyka w łańcuchu dostaw telekomunikacyjnych, podkreślając znaczenie ekonomicznych aspektów ryzyka w zarządzaniu zrównoważonym łańcuchem dostaw. Z kolei w pracy Ali i in.[82] omówiono różne metody oceny ryzyka bezpieczeństwa informacji w kontekście przetwarzania w chmurze, wskazując na potrzebę dostosowania tradycyjnych metod do specyfiki środowiska chmurowego. Natomiast w opracowaniu ZenGRC[83] przedstawiono pięciostopniowy proces przeprowadzania oceny ryzyka cyberbezpieczeństwa, kładąc nacisk na identyfikację zagrożeń, ocenę podatności oraz wdrażanie odpowiednich środków zaradczych.

Zespół analizy ryzyka, aby ocenić prawdopodobieństwo wystąpienia konkretnego zagrożenia związanego z daną podatnością systemu teleinformatycznego, powinien przeprowadzić kompleksowy przegląd istniejących środków ochrony. W trakcie tego przeglądu należy dokładnie ocenić, czy te środki są odpowiednie, skuteczne i wystarczające do spełnienia podstawowych wymagań bezpieczeństwa informacji niejawnych, jakie określone są w ustawach oraz ewentualnych aktach wykonawczych. Dodatkowo, należy uwzględnić wszelkie zalecenia i wytyczne dostarczane przez odpowiednie służby bezpieczeństwa, takie jak ABW (Agencja Bezpieczeństwa Wewnętrznego) lub SKW (Służba Kontrwywiadu Wojskowego). Wszystko to ma na celu zagwarantowanie odpowiedniego poziomu ochrony informacji niejawnych i minimalizację ryzyka związanego z ich bezpieczeństwem.

Oszacowanie ryzyka powinno być przeprowadzone oddzielnie dla każdego zidentyfikowanego zagrożenia znajdującego się na wcześniej sporządzonej liście. Po dokładnej ocenie ryzyka i stworzeniu listy, na której zagrożenia są uporządkowane według ocen ich wielkości, zespół analizy ryzyka powinien przedstawić te wnioski kierownikowi jednostki. Wspólnie z kierownikiem jednostki powinni omówić zaproponowane działania

---

[81] Nalluri, V., and L. S. Chen. "Risk assessment for sustainability on telecom supply chain: A hybrid fuzzy approach." Uncertain Supply Chain Management 10.2 (2022): 559-576.

[82] Ali, Tarek, Mohammed Al-Khalidi, and Rabab Al-Zaidi. "Information security risk assessment methods in cloud computing: Comprehensive review." Journal of Computer Information Systems (2024): 1-28.

[83] ZenGRC. "5 Steps to Performing a Cybersecurity Risk Assessment." ZenGRC Blog, 2023, https://www.zengrc.com/blog/5-steps-to-performing-a-cybersecurity-risk-assessment/. Dostęp 04.2025.

mające na celu zarządzanie ryzykiem. Następnie zespół powinien uzyskać akceptację kierownika jednostki dla tych działań, co jest kluczowym krokiem w procesie zapewnienia bezpieczeństwa informacji niejawnych i minimalizacji ryzyk.

2.8 Badanie opinii interesariuszy ochrony informacji niejawnych

Niniejszy podrozdział poświęcony jest omówieniu problemu i celów badawczych oraz metodologii badania wykorzystanej do ich weryfikacji. Cele badawcze koncentrują się na weryfikacji i doskonaleniu metod ochrony informacji niejawnych poprzez zrozumienie perspektywy kluczowych interesariuszy. Analiza doświadczeń i potrzeb pozwala na identyfikację kluczowych obszarów ryzyka w zakresie strategii ochronnych. W ramach badania została podjęta kwestia zastosowania skomplikowanych metod oceny bezpieczeństwa i ich wpływu na skuteczność ochrony. Zastosowanie jakościowego podejścia poprzez indywidualne wywiady pogłębione umożliwiła uzyskanie szczegółowych informacji, z zachowaniem poufności i anonimowości. Rozdział zakończy się podsumowaniem wniosków zebranych od uczestników, które mogą posłużyć do poprawy efektywności działań w obszarze ochrony informacji niejawnych.

Przygotowanie badania opinii obejmuje sformułowanie problemu badawczego i celów badawczych, wybór adekwatnej metody badawczej oraz przygotowanie narzędzi badawczych. [84] Problem badawczy może być zbiorem pytań i tez, które chcemy zweryfikować i zrozumieć.

W niniejszej pracy problem badawczy został określony w tezach:

Zastosowanie zbyt złożonych metod oceny bezpieczeństwa systemów w procesie ich akredytacji może prowadzić do obniżenia poziomu bezpieczeństwa tych systemów, pomimo ich zgodności z normami i zaleceniami branżowymi.

Teza pomocnicza: Modelowanie i analiza formalna złożonych metod oceny bezpieczeństwa systemów dostarcza narzędzi do efektywnego wyznaczania poziomu ryzyk w zakresie ochrony informacji niejawnych.

W oparciu o zaprezentowaną tezę określono cele badawcze, które obejmują:

[84] Por. M. Kaczmarek, I. Olejnik, A. Springer, *Badania jakościowe – metody i zastosowania*, Warszawa 2013, s. 39.

- **Weryfikację tezy i wkład empiryczny** oparty na obserwacjach w celu potwierdzenia, wzbogacenia lub poprawienia aktualnego stanu wiedzy w dziedzinie ochrony informacji niejawnych.
- **Identyfikację potrzeb oraz problemów i wyzwań** Interesariuszy w obszarze ochrony informacji niejawnych.
- **Poznanie i zrozumienie** perspektywy oraz doświadczeń użytkowników w zakresie ochrony informacji niejawnych, co wraz z identyfikacją potrzeb i kluczowych obszarów ryzyka może wpłynąć na doskonalenie strategii i działań ochronnych, poprawiając ogólną skuteczność ochrony informacji niejawnych.
- **Ocena istniejących rozwiązań i zaprojektowanego modelu formalnego** oceny bezpieczeństwa systemów informatycznych.

Wymienione cele badawcze poza weryfikacją samej tezy pozwolą wzbogacić wiedzę na temat ochrony informacji niejawnych oraz lepiej dostosować strategie i działania do realnych potrzeb i wyzwań.

W ramach przeprowadzonej pracy badawczej skoncentrowano się w szczególności na kilku kwestiach. Po pierwszej, potrzebie oceny bezpieczeństwa systemów ochrony informacji niejawnych**,** ocenie i krytyce istniejących metod, ryzykach związanych z akredytacją oraz ryzyku braku systematyczności wynikającej ze złożoności metod oceny. Po drugie, identyfikacji potrzeb, problemów, wyzwań oraz obszarów ryzyka związanych z ochroną informacji niejawnych. Po trzecie, analizie i ocenie zagrożeń dla bezpieczeństwa informacji niejawnych oraz identyfikacji obszarów, które sprawiają największe trudności (tzw. punkty bólu) i określeniu potencjalnych kierunków zmian, które mogą je zniwelować. Po czwarte, wgląd w perspektywę Interesariuszy poprzez zrozumienie ich opinii i doświadczeń w obszarze ochrony informacji niejawnych, tak aby uwzględnić ich potrzeby w procesie doskonalenia działań ochronnych.

W procesie badawczym wykorzystano podejście jakościowo z wykorzystaniem indywidualnych wywiadów pogłębionych (*In-Depth Interview* – IDI). Zgodnie z teorią i praktyką badań *„pogłębiony wywiad indywidualny ma na celu (...) rozwiązanie problemów o charakterze jakościowym, zatem tych, których zadaniem jest poszukiwanie odpowiedzi na pytanie 'dlaczego?'* [85] Do głównych zalet tego podejścia, istotnych jednocześnie z perspektywy tezy i badania przeprowadzonego w ramach tej pracy, należy zaliczyć

[85] M. Kaczmarek, I. Olejnik, A. Springer, *Badania jakościowe – metody i zastosowania*, Warszawa 2013, s. 114.

możliwość poruszania wrażliwych i trudnych tematów, umożliwienie dotarcia i sprawdzenie opinii trudno dostępnych grup respondentów, możliwość poznania i pogłębienia indywidualnych potrzeb oraz opinii rozmówców i większa elastyczność procesu badawczego. Wywiady indywidualne sprawdzają się w szczególności w tych obszarach, które nie mogą być weryfikowane przy wykorzystaniu innych metod, w szczególności ilościowych, ze względu na tematykę badania, jej złożoność czy osobisty lub poufny charakter, jak również dostępność respondentów. Taką trudno dostępną populacją badawczą są w szczególności eksperci i praktycy gospodarczy.[86]

Za wykorzystaniem indywidualnych wywiadów pogłębionych w tej pracy badawczej przemawiały zarówno względy praktyczne, jak i merytoryczne. Grupa docelowa badania, czyli osoby pracujące z informacjami niejawnymi, to wąska i trudno dostępna grupa. Brak operatu badawczego, z którego można wylosować respondentów do badania był jedną z przesłanek, które uniemożliwiły zastosowanie podejścia ilościowego. Za decydujące czynniki przy wyborze metody badawczej należy jednak uznać wrażliwy, poufny charakter poruszanego tematu oraz możliwości, które oferuje sama metoda, w szczególności możliwość pogłębienia wypowiedzi i zadawania dodatkowych, uzupełniających pytań. Poszczególni uczestnicy mieli możliwość udzielenia swoich opinii w sposób pełniejszy i bardziej szczegółowy, co wpłynęło na jakość zebranych danych. Bezpośredni charakter i prywatność rozmowy sprawiły, że uczestnicy mogli swobodnie dzielić się informacjami, unikając obaw związanych z ujawnieniem ich tożsamości lub treści rozmowy. Dzięki temu uzyskano bardziej otwarte i szczere odpowiedzi od respondentów.

Dodatkowo, indywidualne wywiady pogłębione pozwoliły na lepsze zrozumienie kontekstu i subtelności sytuacji, w których uczestnicy pracowali z informacjami niejawnymi. To umożliwiło zbadanie opinii w sposób bardziej zróżnicowany i dopasowany do indywidualnych doświadczeń każdego rozmówcy.

W rezultacie, indywidualne wywiady pogłębione były skutecznym narzędziem pozwalającym na uzyskanie głębszych i bardziej kompleksowych informacji od respondentów, co było niezwykle istotne w kontekście pracy z informacjami niejawnymi. Zastosowane podejście gwarantowało pełną poufność oraz jakość zebranych danych.

Dobór próby badawczej miał charakter celowy. Polega on na dobraniu takich osób, które tworzą kompletny i zróżnicowany zbiór empirycznych przykładów umożliwiających

[86] Por. A. Kaniewska-Sępa, G. Leszczyński, B. Pilarczyk, *Badania marketingowe na rynku business to business,* Kraków 2006, s. 121.

pogłębione rozpoznanie badanego zjawiska oraz realizację celów badania.[87] Kryterium zróżnicowania próby było zajmowane stanowisko i związany z nim zakres pełnionych obowiązków w obszarze ochrony informacji niejawnych. Grupa docelowa badania obejmowała użytkowników systemów ochrony informacji niejawnych, Audytorów Akredytujących oraz pracowników Pionu Ochrony Informacji Niejawnych, w tym:

1. Kierowników Jednostek Organizacyjnych (*dalej w skrócie KJO*)
2. Administratorów Systemów Niejawnych (*dalej w skrócie ASN*)
3. Pełnomocników ds. Ochrony Informacji Niejawnych (*dalej w skrócie POIN*)
4. Inspektorów Bezpieczeństwa Teleinformatycznego (*dalej w skrócie IBT*)
5. Kierowników Kancelarii Tajnych Narodowych oraz Międzynarodowych (*dalej w skrócie Kierownik KT/KTM*)
6. Kierowników Kancelarii Kryptograficznych NATO oraz UE (*dalej w skrócie Kierownik KK UE/NATO*)

Łącznie przeprowadzono 32 wywiady. Rozmowy były realizowane według ramowego scenariusza wywiadu, który określał podstawowe obszary i pytania planowanej dyskusji. Pytania miały w większości charakter otwarty, aby zachęcić badanych do wypowiedzi oraz wyrażania swoich opinii i postaw. Przebieg rozmowy był swobodny, zdeterminowany wiedzą, zakresem obowiązków oraz opiniami badanych.

Ramowy scenariusz wywiadu obejmował następujące pytania:

1. Jakie metody są wykorzystywane przez Pana/Panią do oceny bezpieczeństwa systemów niejawnych?
2. Jakie korzyści Pana/Pani zdaniem przynosi stosowanie tych metod w organizacji?
3. Jakie są Pana/Pani zdaniem mocne strony, zalety stosowania analizy ryzyka i oceny podatności systemów?
4. Czy używa Pan/Pani dostępnych narzędzi do przeprowadzania analizy ryzyka i oceny podatności systemów? Jakich?
5. Jakie są Pana/Pani zdaniem największe atuty obecnych praktyk w obszarze oceny bezpieczeństwa?

[87] D. Maison, *Jakościowe metody badań marketingowych* [w:] D. Maison, A. Noga-Bogomilski (red.), *Badania marketingowe. Od teorii do praktyki*, Gdańsk 2007, s. 10-13.

6. Jakie są Pana/Pani zdaniem słabe strony, minusy obecnie stosowanych metod oceny bezpieczeństwa?
7. W jaki sposób identyfikowane są potencjalne luki w systemie bezpieczeństwa?
8. Czy w Pana/Pani opinii istnieją ograniczenia lub wyzwania związane z implementacją nowych metod oceny bezpieczeństwa w organizacji? Jakie?
9. Jakie są oczekiwania co do skuteczności nowych metod w porównaniu z aktualnie stosowanymi?
10. Czy zna Pan/Pani przypadki, w których aktualnie stosowane metody oceny bezpieczeństwa okazały się nieskuteczne? Jakie? Co zawiodło?
11. Jakie kroki podejmowane są w obecnych metodach w celu zapewnienia ciągłej poprawy i aktualizacji procedur związanych z bezpieczeństwem?

Zakres informacji pozyskanych podczas wywiadów był zróżnicowany. Wynikał w głównej mierze z perspektywy i zakresu obowiązków realizowanych przez respondenta w ramach systemu ochrony informacji niejawnych. Zestawienie kluczowych informacji uzyskanych podczas rozmów prezentują poniższe tabele.

JAKIE METODY SĄ WYKORZYSTYWANE PRZEZ PANA/PANIĄ DO OCENY BEZPIECZEŃSTWA SYSTEMÓW NIEJAWNYCH?

KJO	• metody oceny ryzyka • testy penetracyjne • ocena zgodności z regulacjami
POIN	• ocena zgodności z regulacjami prawnymi • testy fizyczne zabezpieczeń • audyt ochrony informacji niejawnych • analiza ryzyka związanego z dostępem i przetwarzaniem informacji niejawnych • monitorowanie i kontrola

ASN	• testy ustawień zabezpieczeń • testy penetracyjne • testy detekcji wirusów i złośliwego oprogramowania • audyty bezpieczeństwa • monitorowanie zdarzeń (SIEM)
IBT	• monitorowanie zdarzeń i reagowanie na incydenty • analiza incydentów bezpieczeństwa i wniosków z nich płynących • audyt systemów i infrastruktury pod kątem zgodności z politykami bezpieczeństwa • testy penetracyjne w celu identyfikacji luk w zabezpieczeniach
UŻYTKOWNIK	• edukacja w zakresie cyberbezpieczeństwa • monitorowanie ruchu sieciowego • regularna aktualizacja systemów
AUDYTOR	• poprzez ocenę dokumentacji bezpieczeństwa, politykę ochrony, audyt deklarowanych środków ochrony • metody rekomendowane w wydawanych zaleceniach dla personelu ochrony • metody bazujące na ISO 27k • audyt bezpieczeństwa • ocena zgodności z regulacjami • analiza zdarzeń
KIEROWNIK KT/KTM LUB KIEROWNIK KK	• ocena zgodności z regulacjami prawnymi • monitorowanie dostępu i przepływu dokumentów • kontrola poufności dokumentów

UE/NATO	• sprawdzanie zgodności z politykami dotyczącymi dokumentów

JAKIE KORZYŚCI PANA/PANI ZDANIEM PRZYNOSI STOSOWANIE TYCH METOD W ORGANIZACJI?

KJO	• zwiększenie poziomu ochrony przed zagrożeniami • wzrost zaufania klientów i partnerów biznesowych • optymalne wykorzystanie zasobów firmy
POIN	• minimalizacja ryzyka ujawnienia informacji niejawnych • zgodność z regulacjami dotyczącymi ochrony informacji niejawnych • ulepszenie reputacji organizacji jako rzetelnego opiekuna informacji niejawnych
ASN	• wzrost poziomu bezpieczeństwa i zmniejszenie ryzyka ataków • skuteczne reagowanie na incydenty i szybkie zamykanie luk w zabezpieczeniach
IBT	• wzrost poziomu ochrony systemów i danych • skuteczniejsze reagowanie na incydenty bezpieczeństwa • spójność i zgodność działań z politykami bezpieczeństwa
UŻYTKOWNIK	• zwiększenie świadomości w zakresie bezpieczeństwa • minimalizowanie ryzyka

AUDYTOR	• wzrost zgodności z regulacjami i wymaganiami branżowymi • minimalizowanie ryzyka i zapewnienie odpowiedniego poziomu bezpieczeństwa.
KIEROWNIK KT/KTM LUB KIEROWNIK KK UE/NATO	• wzrost ochrony poufności i integralności dokumentów. • skuteczniejsze reagowanie na sytuacje, w których bezpieczeństwo dokumentów może być zagrożone • zgodność działań z politykami i wymaganiami dotyczącymi dokumentacji

JAKIE SĄ PANA/PANI ZDANIEM MOCNE STRONY, ZALETY STOSOWANIA ANALIZY RYZYKA I OCENY PODATNOŚCI SYSTEMÓW?

KJO	• ułatwienie i poprawa priorytetyzacji działań związanych z bezpieczeństwem • zminimalizowanie ryzyka dla firmy i ochrona jej reputacji • zgodność z przepisami, co chroni firmę przed konsekwencjami prawno-finansowymi o • optymalizacja alokacji zasobów w celu minimalizacji ryzyka • ułatwienie podejmowania świadomych decyzji dotyczących inwestycji w bezpieczeństwo • umocnienie zaufania klientów i partnerów biznesowych poprzez właściwe zarządzanie ryzykiem
POIN	• zwiększenie świadomości organizacyjnej na temat ryzyka i sposobów jego zarządzania

	• zminimalizowanie nieoczekiwanych incydentów i strat finansowych • identyfikacja i ocena ryzyka związanego z utratą poufności, integralności i dostępności informacji niejawnych • skuteczne wdrożenie środków ochrony informacji niejawnych • zgodność z obowiązującymi przepisami dotyczącymi ochrony informacji niejawnych
ASN	• ułatwienie i poprawa priorytetyzacji działań związanych z bezpieczeństwem • identyfikacja potencjalnych zagrożeń i ich wpływu na organizację • pomoc w identyfikacji i priorytetyzacji zagrożeń • ułatwienie dostosowania działań do konkretnych ryzyk
IBT	• usprawnienie procesu oceny i zarządzania ryzykiem • identyfikacja słabych punktów i potencjalnych zagrożeń dla systemów • skuteczne planowanie i wdrażanie zabezpieczeń • minimalizacja ryzyka ataków i naruszeń bezpieczeństwa
UŻYTKOWNIK	• zrozumienie potencjalnych zagrożeń i odpowiednie zachowanie
AUDYTOR	• identyfikacja i ocena potencjalnych zagrożeń • dostosowanie działań do rzeczywistych zagrożeń
KIEROWNIK	• identyfikacja potencjalnych zagrożeń związanych z

KT/KTM LUB KIEROWNIK KK UE/NATO	bezpieczeństwem dokumentów • ułatwienie wdrożenia odpowiednich kontroli i zabezpieczeń • minimalizacja ryzyka utraty, ujawnienia lub manipulacji dokumentami

CZY UŻYWA PAN/PANI DOSTĘPNYCH NARZĘDZI DO PRZEPROWADZANIA ANALIZY RYZYKA I OCENY PODATNOŚCI SYSTEMÓW? JAKICH?

KJO	• zadanie realizowane przez Pełnomocnika Ochrony Informacji Niejawnych
POIN	• nie używam zautomatyzowanych systemów
ASN	• narzędzia do skanowania podatności systemów, takie jak Nessus, OpenVAS • narzędzia do monitorowania zdarzeń bezpieczeństwa, takie jak SIEM (Security Information and Event Management)
IBT	• narzędzia do skanowania podatności systemów, takie jak Nessus, OpenVAS • narzędzia do monitorowania zdarzeń bezpieczeństwa, takie jak SIEM (Security Information and Event Management)
UŻYTKOWNIK	---
AUDYTOR	• narzędzia takie jak ISO 31000, FAIR, CRAMM
KIEROWNIK KT/KTM LUB KIEROWNIK KK	---

UE/NATO	

JAKIE SĄ PANA/PANI ZDANIEM NAJWIĘKSZE ATUTY OBECNYCH PRAKTYK W OBSZARZE OCENY BEZPIECZEŃSTWA?

KJO	• skuteczność w większości przypadków • zgodność z normami międzynarodowymi • systematyczność działań
POIN	• zgodność z prawem • systematyczność działań • wsparcie zewnętrznych instytucji
ASN	• dojrzałość metod • zgodność metod z branżowymi standardami • dość wysoka skuteczność
IBT	• solidność • zgodność z regulacjami • wieloletnie doświadczenie w ich stosowaniu
UŻYTKOWNIK	• pewność, że systemy są regularnie monitorowane i audytowane
AUDYTOR	• dojrzałość procedur • zgodność procedur z uznanymi standardami branżowymi
KIEROWNIK KT/KTM LUB KIEROWNIK KK UE/NATO	• systematyczność działań • strukturalność procesów obiegu dokumentów

JAKIE SĄ PANA/PANI ZDANIEM SŁABE STRONY, MINUSY OBECNIE STOSOWANYCH METOD OCENY BEZPIECZEŃSTWA?

KJO	• wysoki koszt wdrożenia i utrzymania niektórych zaawansowanych narzędzi ochrony informacji niejawnych • sytuacja nadmiernego skupienia się na jednym rodzaju zagrożenia kosztem innych • czasochłonność niektórych metod, szczególnie przy dużych systemach i infrastrukturze
POIN	• wysoki koszt wdrożenia i utrzymania niektórych zaawansowanych narzędzi ochrony informacji niejawnych • możliwość generowania fałszywie pozytywnych lub fałszywie negatywnych wyników, co wpływa na skuteczność oceny ryzyka związanego z informacjami niejawnymi
ASN	• wysoki koszt wdrożenia i utrzymania niektórych zaawansowanych narzędzi ochrony informacji niejawnych • możliwość generowania fałszywie pozytywnych lub fałszywie negatywnych wyników, co wpływa na skuteczność oceny ryzyka związanego z informacjami niejawnymi • zbyt duża uwaga poświęcana jednemu rodzajowi zagrożenia (złośliwe oprogramowania, zabezpieczenia fizyczne lub zabezpieczenia proceduralne), prowadząc do zaniedbania innych potencjalnych ryzyk

IBT	• wysoki koszt wdrożenia i utrzymania niektórych zaawansowanych narzędzi ochrony informacji niejawnych • nadmierne skupienie się na jednym typie zagrożenia, takim jak złośliwe oprogramowanie, zabezpieczenia fizyczne czy proceduralne, może skutkować pominięciem innych istotnych ryzyk • ryzyko pojawienia się błędnych ocen bezpieczeństwa
UŻYTKOWNIK	---
AUDYTOR	• wysoki koszt wdrożenia i utrzymania niektórych zaawansowanych narzędzi ochrony informacji niejawnych • sytuacja nadmiernego skupienia się na jednym rodzaju zagrożenia kosztem innych • zagrożenie, że oceny bezpieczeństwa mogą być nieprawidłowe, co prowadzi do niewłaściwej interpretacji poziomu ochrony
KIEROWNIK KT/KTM LUB KIEROWNIK KK UE/NATO	• wysoki koszt wdrożenia i utrzymania niektórych zaawansowanych narzędzi do zarządzania dokumentami

W JAKI SPOSÓB IDENTYFIKOWANE SĄ POTENCJALNE LUKI W SYSTEMIE BEZPIECZEŃSTWA?

KJO	• regularne audyty wewnętrzne i zewnętrzne • monitorowanie operacji • wykorzystanie systemów wykrywania włamań

POIN	• regularne kontrole, audyty • współpraca z zewnętrznymi ekspertami i agencjami
ASN	• regularne testy penetracyjne • monitorowanie logów systemowych • wykorzystanie narzędzi bezpieczeństwa
IBT	• monitorowanie sieci • audyty bezpieczeństwa • raportowanie przez użytkowników
UŻYTKOWNIK	• identyfikowane przez specjalistów IT oraz powiadomienia systemowe
AUDYTOR	• przeglądy dokumentacji • audyty systemów • testy zgodności z ustalonymi procedurami
KIEROWNIK KT/KTM LUB KIEROWNIK KK UE/NATO	• uważne, skrupulatne monitorowanie i kontrolę procesów obiegu dokumentów • audyty wewnętrzne

CZY W PANA/PANI OPINII ISTNIEJĄ OGRANICZENIA LUB WYZWANIA ZWIĄZANE Z IMPLEMENTACJĄ NOWYCH METOD OCENY BEZPIECZEŃSTWA W ORGANIZACJI? JAKIE?

KJO	• tak, głównym wyzwaniem jest koszt i czas potrzebny na wdrożenie oraz konieczność przeszkolenia personelu
POIN	• ograniczenia prawne i administracyjne mogą

	utrudniać szybkie wdrożenie nowych metod
ASN	• główne wyzwania to złożoność nowych metod i potrzeba dostosowania istniejącej infrastruktury
IBT	• wyzwania obejmują techniczną złożoność i potrzebę integrowania nowych metod z istniejącą infrastrukturą
UŻYTKOWNIK	• wydaje się, że główne wyzwania to skomplikowane procedury oraz dodatkowe obowiązki dla użytkowników
AUDYTOR	• brak ograniczeń • jedynym wymogiem jest przeprowadzenie rzetelnego procesu oraz udokumentowanie go w taki sposób, aby mógł zostać poddany przeglądowi i akceptacji przez audytorów akredytujących
KIEROWNIK KT/KTM LUB KIEROWNIK KK UE/NATO	• trudności związane z integracją nowych metod z już istniejącymi procedurami obiegu dokumentów

JAKIE SĄ OCZEKIWANIA CO DO SKUTECZNOŚCI NOWYCH METOD W PORÓWNANIU Z AKTUALNIE STOSOWANYMI?

KJO	• zminimalizowanie ryzyka • zwiększenie efektywności monitoringu • większa elastyczność, dostosowanie się do zmieniających się zagrożeń
POIN	• lepsza identyfikacja zagrożeń • większa zgodność z przepisami i regulacjami

ASN	• skuteczniejsza detekcja zagrożeń • bardziej sprawna, efektywna reakcja na incydenty
IBT	• wyższa dokładność w identyfikowaniu zagrożeń • lepsze zarządzanie ryzykiem
UŻYTKOWNIK	• zwiększenie bezpieczeństwa • mniejsza liczba zakłóceń w pracy
AUDYTOR	• większa precyzja w wykrywaniu luk • bardziej efektywna automatyzacja procesów audytowych
KIEROWNIK KT/KTM LUB KIEROWNIK KK UE/NATO	• lepsze śledzenie obiegu dokumentów • większa kontrola nad dostępem do informacji niejawnych

CZY ZNA PAN/PANI PRZYPADKI, W KTÓRYCH AKTUALNIE STOSOWANE METODY OCENY BEZPIECZEŃSTWA OKAZAŁY SIĘ NIESKUTECZNE? JAKIE? CO ZAWIODŁO?

KJO	• tak, zdarzały się przypadki niewykrycia nowych typów zagrożeń, co wskazuje na potrzebę ciągłego doskonalenia metod
POIN	• tak, w niektórych przypadkach nie udało się wykryć wyrafinowanych ataków socjotechnicznych
ASN	• tak, zdarzały się incydenty spowodowane przez zaawansowane ataki, które nie zostały wykryte na czas
IBT	• tak, zdarzały się przypadki niewykrycia

	zaawansowanych ataków APT - Advanced Persistent Threat
UŻYTKOWNIK	---
AUDYTOR	• tak, były przypadki naruszeń i incydentów bezpieczeństwa, które wskazują na niedoskonałości obecnych metod
KIEROWNIK KT/KTM LUB KIEROWNIK KK UE/NATO	• tak, zdarzały się przypadki nieautoryzowanego dostępu do dokumentów co wskazuje na potrzebę doskonalenia metod kontroli dostępu

JAKIE KROKI PODEJMOWANE SĄ W OBECNYCH METODACH W CELU ZAPEWNIENIA CIĄGŁEJ POPRAWY I AKTUALIZACJI PROCEDUR ZWIĄZANYCH Z BEZPIECZEŃSTWEM?

KJO	• regularne przeglądy polityk bezpieczeństwa • szkolenia dla personelu • korzystanie z najnowszych technologii bezpieczeństwa
POIN	• regularne szkolenia • aktualizacje dokumentów • ciągła współpraca z profesjonalistami ds. bezpieczeństwa
ASN	• aktualizacje systemów • regularne szkolenia • audyty wewnętrzne i zewnętrzne
IBT	• regularne przeglądy i audyty

	• konsultacje z ekspertami zewnętrznymi • wprowadzanie nowych technologii
UŻYTKOWNIK	• szkolenia dla użytkowników • regularne aktualizacje oprogramowania i zabezpieczeń
AUDYTOR	• przeglądy okresowe • weryfikacje zgodności z normami • integracja z nowymi narzędziami audytowymi
KIEROWNIK KT/KTM LUB KIEROWNIK KK UE/NATO	• regularne szkolenia pracowników • aktualizacje procedur • integracja z systemami monitoringu

Analizując odpowiedzi interesariuszy pełniących rożne role w systemie ochrony informacji niejawnych można zauważyć kilka wspólnych wniosków:

1. **Wysoki koszt implementacji i utrzymania systemów ochrony informacji niejawnych**

   Zarówno kierownicy, administratorzy, jak i audytorzy oraz inni uczestnicy zauważają, że zaawansowane metody i narzędzia bezpieczeństwa mogą generować wysokie koszty związane z wdrożeniem, utrzymaniem, szkoleniami i dostosowaniem do potrzeb organizacji. **To pozwala zweryfikować pozytywnie postawioną tezę dotyczącą wpływu nadmiernie złożonych metod oceny bezpieczeństwa systemów na obniżenie ich efektywności, ponieważ zwiększone koszty i skomplikowanie procesu mogą prowadzić do opóźnień, trudności w implementacji oraz ograniczenia realnej ochrony systemów, mimo formalnej zgodności z normami.**
2. **Możliwość generowania fałszywie pozytywnych lub fałszywie negatywnych wyników**

Uczestnicy dostrzegają problem potencjalnego występowania błędnych wyników w ocenie bezpieczeństwa, co może prowadzić do nieprawidłowych decyzji i nadmiernego zaufania lub nieufności do systemów i procedur zabezpieczeń.

3. **Wyzwania związane z interpretacją wyników**
   Interesariusze zauważają trudności w interpretacji wyników analizy ryzyka i oceny podatności, co może utrudniać właściwe podejmowanie decyzji oraz planowanie i implementację skutecznych środków zabezpieczeń.
4. **Możliwość nadmiernego skupienia się na jednym rodzaju zagrożenia kosztem innych**
   Uczestnicy podkreślają ryzyko nadmiernego skoncentrowania się na jednym rodzaju zagrożenia (np. cyberataki) kosztem innych aspektów bezpieczeństwa, takich jak zagrożenia fizyczne czy ludzkie.
5. **Wymóg specjalistycznej wiedzy i umiejętności**
   Wprowadzenie skutecznych metod oceny bezpieczeństwa wymaga specjalistycznej wiedzy i umiejętności, co może stanowić wyzwanie dla pionu ochrony i wymagać odpowiedniego szkolenia i rozwoju kompetencji personelu.

Podsumowując, wspólne wnioski dotyczące minusów wykorzystywanych metod w ocenie bezpieczeństwa obejmują koszty wynikające z czasochłonności analizy ryzyka, trudności w interpretacji wyników, ryzyka nadmiernego skupienia się na jednym aspekcie bezpieczeństwa oraz potrzebie specjalistycznej wiedzy i umiejętności. Działania mające na celu przezwyciężenie tych wyzwań powinny uwzględniać odpowiednie zarządzanie zasobami, edukację personelu i rozwój kompetencji w zakresie bezpieczeństwa informacji.

2.9 Negatywne aspekty złożoności metod ochrony informacji

Złożoność procesów bezpieczeństwa może obniżać poziom bezpieczeństwa z kilku powodów. Oto kilka potencjalnych przyczyn:

- Błędy ludzkie – im bardziej skomplikowany jest system bezpieczeństwa, tym większe jest prawdopodobieństwo popełnienia błędów ludzkich podczas projektowania, wdrożenia i utrzymania tego systemu. Nawet najbardziej doświadczeni specjaliści mogą popełniać błędy w skomplikowanych systemach, co może prowadzić do poważnych luk w bezpieczeństwie.
- Niezrozumienie – skomplikowane procesy mogą prowadzić do tego, że pracownicy nie zrozumieją w pełni procedur bezpieczeństwa. Jeśli reguły są zbyt

skomplikowane lub niejasne, użytkownicy mogą nieświadomie naruszać zasady bezpieczeństwa, co zwiększa ryzyko incydentów.

- Opóźnienia w reakcji – zbyt złożone procedury mogą prowadzić do opóźnień w reakcji na incydenty bezpieczeństwa. Jeśli procesy są zbyt skomplikowane, czas potrzebny do zidentyfikowania, zrozumienia i odpowiedzi na incydent może być zbyt długi, co zwiększa szanse na straty.
- Koszty – skomplikowane systemy bezpieczeństwa mogą być kosztowne w utrzymaniu. Firmy często muszą inwestować w zaawansowane technologie, szkolenia pracowników i utrzymanie systemów, co może prowadzić do tego, że pewne aspekty bezpieczeństwa są zaniedbywane ze względu na ograniczone zasoby.
- Przejrzystość – zbyt skomplikowane procedury mogą utrudniać śledzenie działań użytkowników i identyfikację nieprawidłowości. Brak przejrzystości może prowadzić do tego, że ataki czy nieprawidłowości pozostaną niezauważone, a zatem bezpieczeństwo będzie narażone.

W związku z tym, ważne jest, aby projektować procesy bezpieczeństwa w taki sposób, aby były zrozumiałe, efektywne i możliwe do utrzymania. Optymalizacja złożoności procesów może przyczynić się do zwiększenia skuteczności i efektywności działań bezpieczeństwa.

Przykładowo norma ISO 15408, znana również jako Common Criteria (CC), jest międzynarodowym standardem służącym do oceny bezpieczeństwa produktów i systemów informatycznych. Chociaż standard ten jest bardzo użyteczny i powszechnie stosowany, można znaleźć pewne aspekty, które mogą być uznane za zbyt złożone, co może wpływać na skuteczność implementacji. Poniżej zaprezentowana jest analiza standardu ISO 15408 pod kątem wcześniej wspomnianych pięciu przyczyn:

- Błędy ludzkie: ISO 15408 jest obszernym standardem złożonym z wielu dokumentów. Skomplikowana terminologia i techniczne szczegóły mogą sprawić, że pracownicy odpowiedzialni za wdrażanie i utrzymanie systemów bezpieczeństwa mogą popełnić błędy interpretacyjne. Duża liczba terminów technicznych i wymagań może prowadzić do niejasności, co z kolei może skutkować błędnymi decyzjami podczas implementacji.

- Niezrozumienie: Standard ISO 15408 jest specyficzny i wymaga dogłębnego zrozumienia technicznego. To może sprawić, że użytkownicy końcowi, a nawet niektórzy specjaliści z obszarów niezwiązanych bezpośrednio z bezpieczeństwem informatycznym, będą mieć trudności z zrozumieniem i przestrzeganiem jego wymagań.
- Opóźnienia w reakcji: Proces uzyskiwania certyfikacji zgodnie z ISO 15408 może być czasochłonny i kosztowny. Długotrwałe procedury oceny mogą prowadzić do opóźnień w dostarczeniu produktów na rynek, co w niektórych przypadkach może być niepraktyczne, zwłaszcza w dziedzinie technologii, gdzie tempo zmian jest bardzo szybkie.
- Koszty: Implementacja i uzyskanie certyfikacji zgodnie z ISO 15408 może wymagać znacznych nakładów finansowych i zasobów. Dla mniejszych przedsiębiorstw może to stanowić znaczne obciążenie, co może prowadzić do ograniczonego dostępu do zaawansowanych rozwiązań bezpieczeństwa.
- Przejrzystość: Znaczna liczba dokumentów i technicznych detalów w standardzie może utrudniać przejrzystość procesów. To może prowadzić do trudności w śledzeniu działań i ocenie skuteczności działań bezpieczeństwa.

Chociaż ISO 15408 jest bardzo cenionym standardem, jego złożoność może wprowadzać pewne wyzwania, szczególnie dla mniejszych firm i osób, które nie są specjalistami z zakresu bezpieczeństwa informatycznego. Podejście do standardów bezpieczeństwa musi być zindywidualizowane i dopasowane do konkretnych potrzeb i warunków każdej organizacji. To, co może być skuteczne i adekwatne dla jednej firmy, niekoniecznie będzie odpowiednie dla innej. Kluczowe jest pełne zrozumienie kontekstu działania organizacji, w tym jej środowiska pracy, infrastruktury technologicznej, zasobów ludzkich i finansowych oraz rodzajów zagrożeń, z którymi się styka. Tylko wtedy można opracować odpowiednie strategie bezpieczeństwa, które są zarówno skuteczne, jak i realistyczne do wdrożenia.

Po zakończeniu etapu badań, którego wyniki pozwoliły na zidentyfikowanie kluczowych problemów i oczekiwań związanych z oceną bezpieczeństwa systemów teleinformatycznych, konieczne stało się przeprowadzenie analizy modeli formalnych. Przegląd istniejących metod oceny ryzyka w celu zgłębienia teoretycznych i praktycznych podstaw, które kształtują obecne standardy bezpieczeństwa oraz na identyfikację ich mocnych i słabych stron.

Wyniki badania ankietowego jasno wskazały na wyzwania, przed którymi stoją organizacje w obszarze wdrażania i utrzymania systemów bezpieczeństwa. Część respondentów zwróciła uwagę na to, że aktualne podejścia charakteryzują się wysoką złożonością oraz dużą ilością formalnych procedur, co prowadzi do obciążeń organizacyjnych i operacyjnych. Na podstawie tych wyników zdecydowano się na analizę modeli formalnych w celu zrozumienia, jak istniejące standardy oceny ryzyka przekładają się na ich codzienne stosowanie oraz które ich elementy mogą stanowić przeszkodę w efektywnym zarządzaniu bezpieczeństwem.

Przegląd modeli formalnych mający na celu porównanie istniejących metod oceny ryzyka, zwłaszcza pod kątem ich zgodności z normami branżowymi, takimi jak ISO/IEC 27001, ISO/IEC 27002 oraz ISO/IEC 27005. Analiza obejmująca także ocenę, w jakim stopniu standardowe podejścia odpowiadają na realne potrzeby i problemy identyfikowane przez praktyków oraz osoby odpowiedzialne za ochronę informacji. Poprzez ocenę mocnych stron oraz ograniczeń tych modeli formalnych możliwe będzie stworzenie bazy dla zaprojektowania, uproszczonego formalnego modelu oceny ryzyka, który nie tylko będzie zgodny z wymaganiami branżowymi, ale także odpowie na zdiagnozowane w badaniu potrzeby dotyczące przejrzystości i efektywności.

W tym kontekście przegląd istniejących modeli formalnych stanowi nie tylko podstawę merytoryczną dla opracowania własnej koncepcji, ale także umożliwia krytyczną analizę, która pozwala zrozumieć ograniczenia skomplikowanych metod i wskazać elementy wymagające usprawnienia.

Biorąc pod uwagę powyższe oraz zalecenia instytucji odpowiedzialnych za wydawanie świadectw akredytacji bezpieczeństwa systemów teleinformatycznych, konieczne okazało się opracowanie modelu analizy ryzyka minimalnego ze względu na jego złożoność strukturalną i obliczeniową, a jednak akceptowalnego przez podmioty akredytujące.

2.10 Modele formalne

Pod koniec XX-go i na początku XXI-ego wieku opracowano wiele struktur formalnych mających za zadanie modelowanie i analizę bezpieczeństwa systemów

informatycznych. Zdaniem autora rozprawy najlepszy przegląd wspomnianych technik został przeprowadzony w pracy Imeda El Fray pod tytułem. *„Metoda określająca zaufanie do systemu informacyjnego w oparciu o proces szacowania i postępowania z ryzykiem”*. Poniżej znajdują się opisy poszczególnych systemów tego typu.

Model zaproponowany przez Roberta H. Courtney'ego Jr. z IBM Corporation stanowił jedno z pionierskich narzędzi do analizy ryzyka w systemach informatycznych. W końcówce lat 80. XX-go wieku został on przyjęty jako standard rządowy w Stanach Zjednoczonych. Model ten, innowacyjny w swoim podejściu, zakładał wprowadzenie systematycznego procesu oceny ryzyka, który miał na celu identyfikację zagrożeń oraz oszacowanie potencjalnych konsekwencji incydentów w systemach informatycznych. Następnie w szeregu publikacji podjęto próbę dalszego rozwoju tego modelu, wprowadzając ulepszenia, które miały na celu bardziej precyzyjne oszacowanie ryzyka związanego z bezpieczeństwem informacji. Jednak te modyfikacje, pomimo ich innowacyjnego charakteru, nie są w pełni zgodne z aktualnymi wymaganiami i wytycznymi wynikającymi z międzynarodowych norm dotyczących analizy ryzyka i zarządzania ryzykiem, takich jak normy ISO/IEC 27005 oraz wytyczne NIST.[88]

Kolejną istotną ewolucję modelu zaproponował Parker[89], który w swoich pracach uwzględnił kluczowy aspekt, jakim jest wpływ czynnika ludzkiego na ryzyko incydentów bezpieczeństwa. Wprowadzając nowoczesne podejście oparte na interdyscyplinarnych badaniach, Parker połączył wiedzę matematyczną z doświadczeniem ekspertów IT, co pozwoliło na bardziej wszechstronne podejście do zarządzania ryzykiem. Jego pięciofazowy model nie tylko spełniał wymogi standardów bezpieczeństwa, takich jak NIST SP 800-30, ale również integrował mechanizmy uwzględniające dynamicznie zmieniające się zagrożenia oraz podatności, z jakimi muszą mierzyć się współczesne organizacje.

Model Parkera, w przeciwieństwie do wcześniejszych podejść, wyróżniał się większą elastycznością i kompleksowością, pozwalając na dostosowanie procesu zarządzania ryzykiem do specyfiki danej organizacji oraz jej zasobów teleinformatycznych.

---

[88] Cyt za: El Fray, Imed. *Metoda określająca zaufanie do systemu informacyjnego w oparciu o proces szacowania i postępowania z ryzykiem.* Wyd. Stowarzyszenie Przyjaciół Wydziału Informatyki w Szczecinie, Szczecin, 2013.

[89] D. B. Parker (1981) *Computer Security Management.* Reston Publishing Company Inc., Reston VA, US

Uwzględnienie takich elementów jak analiza ryzyka związanego z błędami ludzkimi, niepełną wiedzą użytkowników oraz możliwością nadużyć, nadało temu modelowi większą praktyczną użyteczność, szczególnie w kontekście ochrony informacji niejawnych. Dodatkowo model ten wspierał wykorzystanie zaawansowanych technik analizy danych, co pozwalało na ciągłe monitorowanie i aktualizowanie strategii zarządzania ryzykiem w odpowiedzi na pojawiające się nowe zagrożenia.

Poszczególne fazy modelu Parkera można przedstawić w następujący sposób.

Faza 1: **Identyfikacja i klasyfikacja zasobów** – w tym etapie następuje rozpoznanie wszystkich zasobów informacyjnych, technologicznych i ludzkich w organizacji oraz ich odpowiednie skategoryzowanie pod kątem ich wartości i krytyczności dla funkcjonowania systemu.

Faza 2: **Identyfikacja zagrożeń** – analiza zagrożeń obejmuje nie tylko samą identyfikację potencjalnych ryzyk, ale również zbadanie ich źródeł, motywacji działań, jak np. motywy przestępcze czy przypadkowe błędy.

Faza 3: **Ocena ryzyka** – po identyfikacji zagrożeń następuje ocena ich potencjalnych konsekwencji. W tej fazie analizowane są możliwe skutki zagrożeń dla zasobów oraz prawdopodobieństwo ich wystąpienia.

Faza 4: **Identyfikacja, wybór oraz wdrożenie zabezpieczeń** – organizacja wybiera odpowiednie środki ochronne, biorąc pod uwagę ich efektywność, koszty, oraz pilność wdrożenia. Zabezpieczenia muszą być dopasowane do specyficznych zagrożeń oraz możliwości organizacji.

Faza 5: **Implementacja systemu zabezpieczeń** – po wyborze zabezpieczeń, następuje ich wdrożenie, przy jednoczesnym monitorowaniu, czy wybrane środki odpowiadają poziomowi ryzyka, który organizacja jest w stanie zaakceptować.

Według Parkera ryzyko można oszacować za pomocą wzoru, który uwzględnia poziom zagrożenia, podatności systemu oraz wartość chronionych zasobów.

$$R = \left(\frac{\sum_m T_1(\sum_{i=1}^{m} w_i p_i)}{m}\right)\left(\frac{\sum_n T_2\left(\sum_{j=1}^{n} w_j p_j\right)}{n}\right)$$

gdzie, wartości w modelu Parkera to:

R – wartość ryzyka, którą oblicza się na podstawie zebranych danych ankietowych dotyczących prawdopodobieństwa i skutków incydentu.

i – liczba pytań ankietowych, które dotyczą oceny prawdopodobieństwa wystąpienia incydentu.

j – liczba pytań ankietowych odnoszących się do oceny skutków, jakie mogą wystąpić w wyniku incydentu.

m, n – liczba respondentów biorących udział w ankiecie, gdzie m odnosi się do pytań związanych z prawdopodobieństwem, a n do pytań o skutki.

wi, wj – wagi przypisane poszczególnym pytaniom z grupy i i j, które pomagają określić ich istotność w całkowitej ocenie ryzyka.

pi, pj – wartości wynikające z odpowiedzi na pytania dotyczące prawdopodobieństwa (pi) i skutków (pj), które są używane do wyliczenia ryzyka.

T1 – tabela, która określa prawdopodobieństwo wystąpienia danego zdarzenia, czyli jak często dany incydent może się wydarzyć.

T2 – tabela opisująca negatywne skutki incydentu, służąca do oceny potencjalnych strat, które mogą wyniknąć z incydentu.

Model Parkera uwzględnia te wszystkie zmienne, aby precyzyjnie określić poziom ryzyka w systemie informacyjnym.

Metoda Parkera, mimo że stanowi istotny krok w analizie ryzyka, ma swoje ograniczenia. Przede wszystkim brakuje powszechnie dostępnych źródeł wiedzy na temat aktualnych zagrożeń, podatności systemów oraz możliwych scenariuszy incydentów. Proces identyfikacji i klasyfikacji zasobów, wykrywania podatności oraz przypisywania im odpowiednich zagrożeń wymaga zaangażowania zespołu ekspertów. Oznacza to, że skuteczność i precyzja analizy w dużej mierze zależy od wiedzy, doświadczenia i umiejętności tych specjalistów. Wiąże się to z wysokimi kosztami, zarówno w kontekście pracy, jak i czasu potrzebnego na przeprowadzenie dokładnej oceny ryzyka. Długotrwały proces analizy może stanowić barierę, zwłaszcza w środowiskach, gdzie czas reakcji jest kluczowy.

Co więcej, wartości szacujące prawdopodobieństwo wystąpienia incydentów oraz ich potencjalne negatywne skutki, które są podstawą dla decyzji o ryzyku w tej metodzie, opierają się na danych empirycznych z lat osiemdziesiątych. Dane te, zebrane w okresie, kiedy krajobraz zagrożeń cybernetycznych był znacznie mniej złożony, są dziś już przestarzałe. Współczesna informatyka rozwija się w zawrotnym tempie, a zagrożenia stale ewoluują, zarówno pod względem ilości, jak i różnorodności. Nowoczesne cyberataki są coraz bardziej zaawansowane i dynamiczne, przez co dawne metody prognozowania mogą być niewystarczające w obliczu dzisiejszych wyzwań.

Brak bieżących danych i poleganie na starzejących się informacjach z przeszłości oznacza, że wartości prawdopodobieństw i potencjalnych szkód zawarte w T1 i T2 mogą nie oddawać rzeczywistego stanu zagrożeń. To sprawia, że oceny ryzyka mogą być niedokładne, co z kolei prowadzi do podejmowania decyzji, które nie w pełni odpowiadają aktualnym potrzebom w zakresie bezpieczeństwa. W efekcie metoda Parkera, choć cenna w swoim czasie, wymaga dostosowania do współczesnych realiów, aby móc skutecznie sprostać rosnącej liczbie zagrożeń w dzisiejszym, szybko zmieniającym się środowisku technologicznym.

Alternatywne podejście do określania wagi ryzyka, oparte na rachunku prawdopodobieństwa, zaproponował Żurek[90]. Zdaniem autora, wagę ryzyka R, wyrażoną jako liczba rzeczywista, można obliczyć za pomocą następującego wzoru:

$$R = PR \cdot SR = (PR \cdot WG \cdot 100) - D$$

gdzie:

- *R* to waga ryzyka,
- *PR* oznacza prawdopodobieństwo wystąpienia ryzyka,
- *SR* odnosi się do potencjalnych skutków ryzyka,
- *WG* jest wagą przypisaną skutkom,
- *D* to współczynnik wrażliwości modelu.

Z powyższego wzoru wynika, że potencjalny skutek ryzyka SR jest wielkością bezwymiarową. Waga skutku *WG* reprezentuje poziom podatności systemu bezpieczeństwa na przełamanie, czyli określa, jak łatwo można naruszyć jego funkcje, mechanizmy czy inne elementy. Im wyższa wartość *WG,* tym większa podatność systemu na potencjalne zagrożenia, co oznacza, że skutki przełamania mogą być poważniejsze. Z kolei współczynnik wrażliwości *D* jest miarą odporności systemu na naruszenia, która wynika z zastosowanych środków bezpieczeństwa. Określa, w jakim stopniu wdrożone mechanizmy ochronne są skuteczne w zapobieganiu incydentom. Wyższa wartość współczynnika *D* oznacza większą odporność systemu, a tym samym mniejsze prawdopodobieństwo skutecznego ataku.

---

90 B. Żurek, (1999) RMS Program Used in Risk Management, Conference Proceeding "Project Management – experience and Methods", Gdańsk, Poland

Uwzględniając liczbę zasobów, które są bardziej podatne na ryzyko, szacowanie ryzyka z wykorzystaniem wzoru staje się bardziej precyzyjne. Zwiększenie liczby zasobów narażonych na wyższe prawdopodobieństwo wystąpienia zagrożenia sprawia, że waga ryzyka wzrasta, co prowadzi do bardziej złożonego procesu oceny. Ostatecznie, ocena ryzyka staje się bardziej realistyczna i dostosowana do rzeczywistych warunków, ponieważ uwzględnia zarówno poziom zagrożenia, jak i skuteczność wdrożonych zabezpieczeń.

Wzór staje się w tym kontekście narzędziem umożliwiającym dokładniejsze oszacowanie ryzyka, uwzględniając różnorodne czynniki, takie jak liczba zasobów, ich podatność oraz skuteczność zabezpieczeń.

$$R = \left(PR_{max} \cdot 100 \cdot \sum_{i} WG_i \right) - D$$

gdzie:

- *WG* to współczynnik określający wagę skutku, który reprezentuje znaczenie i wpływ danej zmiany ryzyka systemu informatycznego na jego ogólną funkcjonalność i bezpieczeństwo. Wartość tej wagi może być używana do priorytetyzacji zmian w zależności od ich potencjalnego efektu na system.

- WG_i to waga przypisana do i-tego skutku, która określa znaczenie danego wpływu w kontekście wszystkich rozważanych skutków dla systemu informatycznego. Każda waga *WGi* uwzględnia specyficzny efekt, który dana zmiana ryzyka wywołuje, co pozwala na bardziej precyzyjną ocenę całościowego ryzyka systemu.

Biorąc pod uwagę różne scenariusze incydentów, które cechują się największym prawdopodobieństwem wystąpienia, można obliczyć uśrednioną wagę ryzyka. Taka wartość pozwala na uzyskanie kompleksowego obrazu ogólnego poziomu zagrożeń, na jakie narażona jest organizacja. Uśredniona waga ryzyka uwzględnia zarówno najczęstsze zagrożenia, jak i potencjalne skutki incydentów, co pozwala na bardziej dokładne określenie stanu ryzyka.

Dzięki temu organizacja jest w stanie lepiej zrozumieć, które obszary wymagają priorytetowej uwagi i gdzie konieczne mogą być dodatkowe zabezpieczenia. Waga ta dostarcza także narzędzi do bardziej efektywnego zarządzania zasobami oraz wyznaczania strategii bezpieczeństwa, pozwalając na zbalansowanie inwestycji w ochronę z realnymi zagrożeniami. Tym samym, uśredniona waga ryzyka staje się kluczowym wskaźnikiem w podejmowaniu decyzji dotyczących minimalizacji ryzyka oraz poprawy ogólnego bezpieczeństwa organizacji.

$$R_s = \frac{\sum_n R_n}{n} = \frac{\sum_n [(PR_{max} \cdot 100 \cdot \sum_i WG_i) - D]}{n}$$

gdzie:

- R_s to całkowita waga ryzyka, która stanowi sumaryczne odzwierciedlenie wpływu wszystkich zidentyfikowanych skutków zmian w systemie informatycznym. Oznacza ona łączną wartość ważoną ryzyka, uwzględniającą wszystkie czynniki wpływające na ryzyko i ich przypisane wagi, co pozwala na ocenę całościowego poziomu ryzyka systemu.

- n jest numerem kolejnego scenariusza, który reprezentuje różne możliwe sytuacje lub zdarzenia brane pod uwagę w procesie oceny ryzyka systemu informatycznego. Każdy scenariusz opisuje unikalny zestaw warunków i zdarzeń, które mogą wpływać na poziom ryzyka.

Przedstawiona metoda ma istotną wadę wynikającą z subiektywności w określaniu wartości *WG*, czyli wagi skutku. Decyzja o tym, jaką wartość przypisać skutkom potencjalnych incydentów, zależy w dużej mierze od indywidualnych ocen i doświadczeń zespołu odpowiedzialnego za analizę ryzyka. Taka subiektywność może prowadzić do niejednorodności wyników i problemów z ich porównywalnością, a w skrajnych przypadkach – do niedoszacowania lub przeszacowania ryzyka w odniesieniu do konkretnych zasobów.

Ponadto uśrednianie wagi ryzyka, które proponuje ta metoda, jest sprzeczne z podstawowymi zasadami zarządzania ryzykiem w systemach bezpieczeństwa. W zarządzaniu ryzykiem kluczowe jest uwzględnienie, że różne zasoby organizacji mają różne poziomy podatności i znaczenie strategiczne. Traktowanie wszystkich zasobów jednakowo, poprzez uśrednianie ryzyka, nie oddaje prawdziwego obrazu zagrożeń. Na przykład, utrata jednego kluczowego zasobu, takiego jak dane klientów, może mieć katastrofalne skutki, które mogą zaważyć na dalszym funkcjonowaniu organizacji, nawet jeśli inne zasoby nie są równie krytyczne. Uśrednione podejście zniekształca te różnice, co może prowadzić do błędnych decyzji dotyczących priorytetów ochrony.

Co więcej, metoda ta nie uwzględnia specyficznej charakterystyki incydentów, które mogą występować często, ale generują niewielkie skutki, w porównaniu do rzadkich, lecz znacznie bardziej niszczycielskich wydarzeń. Takie podejście może zaniżać ryzyko związane z poważnymi incydentami, których wystąpienie, choć rzadkie, może mieć druzgocący wpływ na bezpieczeństwo systemu. Metody takie jak te opracowane przez Courtney'a i później na jej bazie rozwijane lepiej rozróżniają te dwa typy zagrożeń,

zapewniając bardziej precyzyjną ocenę ryzyka, która bierze pod uwagę zarówno częstotliwość, jak i skalę skutków incydentów.

W rezultacie metoda ta, pomimo swoich zalet, nie jest w pełni zgodna z nowoczesnymi standardami zarządzania ryzykiem, gdzie kluczową rolę odgrywa indywidualna ocena ryzyka dla poszczególnych zasobów oraz balansowanie pomiędzy zdarzeniami o różnej częstotliwości i skutkach. Współczesne podejścia do zarządzania ryzykiem kładą nacisk na holistyczną ocenę zagrożeń, która lepiej uwzględnia złożoność współczesnych systemów informatycznych i różnorodność potencjalnych incydentów bezpieczeństwa.

Również Liderman, w swojej pracy[91], podjął się analizy matematycznych modeli oceny ryzyka, skupiając się na aspekcie relacyjnym w kontekście systemów bezpieczeństwa teleinformatycznego. Jego model nie jest zaprojektowany do obliczania wagi ryzyka, co czyni go innym podejściem w porównaniu do tradycyjnych metod oceny. Zamiast tego, autor koncentruje się na stworzeniu formalnej struktury, która opisuje poprawne funkcjonowanie systemu bezpieczeństwa w określonym środowisku, gdzie mogą występować różnorodne zagrożenia.

Definiując system bezpieczeństwa jako uporządkowaną piątkę elementów, Liderman wskazuje na konieczność zrozumienia interakcji między poszczególnymi komponentami oraz ich wpływu na bezpieczeństwo całego systemu. Ta uporządkowana piątka obejmuje różne aspekty, takie jak:

$$S_{TE} = (O_T, B_T, R_T, R_B, \Omega_T)$$

$O_T = \{o_i : i = 1, \dots, m\}$ – niepusty zbiór obiektów systemu, które posiadają ujawnione podatności. Mogą to być różne zasoby systemu, takie jak urządzenia, aplikacje, bazy danych czy inne komponenty wymagające ochrony,

$B_T = \{b_p : p = 1, \dots, r\}$ – zbiór zabezpieczeń stosowanych w systemie, które mają na celu ochronę obiektów przed znanymi podatnościami i zagrożeniami. Zbiór ten obejmuje środki techniczne, takie jak zapory ogniowe, systemy detekcji włamań, szyfrowanie, a także procedury i polityki bezpieczeństwa,

[91]K. Liderman (2008) Analiza ryzyka I ochrona informacji w systemach komputerowych. PWN, Warszawa, Polska

$R_T = \{r_s : s = 1, \dots, t\}$ – zbiór podatności istniejących w systemie, które mogą zostać wykorzystane przez potencjalne zagrożenia. Są to znane słabości w obiektach systemu, które narażają go na ryzyko ataku, np. luki w oprogramowaniu czy błędy konfiguracji,

$R_R \subseteq R_T$ – zbiór podatności, które są chronione przed zagrożeniami za pomocą zabezpieczeń ze zbioru B. Są to te podatności, które zostały odpowiednio zidentyfikowane

$\Omega_T = \{\omega_z : z = 1, \dots, w\}$ – niepusty podzbiór relacji, który jest określony jako iloczyn kartezjański $O_T \times R_T \times B_T$. Relacje te opisują, jak obiekty ze zbioru O_T są powiązane z podatnościami ze zbioru R_T i jakie zabezpieczenia z B_T chronią te podatności. Mówiąc prościej, pokazuje, w jaki sposób poszczególne obiekty w systemie są podatne na ryzyko i jakie środki ochrony zostały wdrożone, aby zabezpieczyć te słabości.

W tym modelu Liderman stara się zbudować strukturę, która nie tylko identyfikuje zagrożenia, ale również określa, jak są one kontrolowane poprzez zastosowane środki ochrony. Model ten ma na celu stworzenie relacji między podatnościami, zagrożeniami i środkami bezpieczeństwa, co pozwala na lepsze zarządzanie ryzykiem w systemach teleinformatycznych. Dzięki temu organizacje mogą dokładnie zobaczyć, które obiekty są narażone, jakie podatności istnieją, i które z nich są skutecznie chronione przed potencjalnymi incydentami.

Proponowana przez Lidermana struktura obejmuje także warunek bezpieczeństwa, który zakłada, że dla każdego obiektu i związanej z nim podatności na zagrożenie musi istnieć odpowiednie zabezpieczenie, które to zagrożenie eliminuje lub minimalizuje:

$$\forall(o_i \in O_T)\forall(r_s \in R_T)\exists\left(b_p \in B_T\right): \omega\left(o_i, r_s, b_p\right)$$

a objęcie mechanizmami ochrony, minimalizuje ryzyko ich wykorzystania przez potencjalnych napastników.

Liderman w swojej pracy wprowadza pojęcie tzw. ścieżek penetracji systemu, które odnoszą się do możliwych dróg, jakimi zagrożenia mogą przenikać przez system zabezpieczeń. W tym kontekście zdefiniował również niesprzeczność systemu zabezpieczeń, czyli spójność środków ochrony względem potencjalnych zagrożeń, co odgrywa kluczową rolę w zapewnieniu efektywności ochrony.

Proponowany przez Lidermana model relacyjny stanowi istotny krok w kierunku stworzenia formalnego modelu bezpiecznego systemu informacyjnego. Mimo jego wartości w analizie struktury zagrożeń i zabezpieczeń, model ten ma pewne ograniczenia — nie umożliwia precyzyjnych obliczeń wag ryzyka, ani nie pozwala na pełną ocenę zagrożeń czy planowanie działań w zakresie zarządzania ryzykiem w systemach informatycznych.

W ramach swoich badań Liderman opracował również metodę szacowania ryzyka, którą nazwał L-RAC, bazującą na zasadzie burzy mózgów. Metoda ta angażuje grupę ekspertów do wspólnego identyfikowania zagrożeń i oceny ryzyka, opierając się na kolektywnym poszukiwaniu kreatywnych rozwiązań. Celem L-RAC jest nie tylko zidentyfikowanie podatności systemu, ale także ocena najbardziej prawdopodobnych i najgroźniejszych zagrożeń. Jednak skuteczność tej metody zależy w dużej mierze od doświadczenia uczestniczących specjalistów, co może prowadzić do pewnej subiektywności w ocenie ryzyka.

Alternatywna metoda oceny ryzyka, zaproponowana przez Marcello[92], opiera się na koncepcji rywalizacji pomiędzy stronami, w której każda z nich dąży do osiągnięcia swoich celów. W ramach tego modelu analizowane są różnorodne czynniki, które mogą wpływać na poziom ryzyka w systemach informatycznych.

Jednym z kluczowych elementów tego podejścia jest gotowość strony atakującej do podejmowania ryzykownych działań, które mają na celu przełamanie zabezpieczeń systemu. Oznacza to, że im większa jest determinacja i zasoby atakującego, tym wyższe ryzyko, jakie niesie ze sobą ewentualny atak. Z drugiej strony, również gotowość obrońców do wprowadzania skutecznych działań ochronnych jest istotna. Strony odpowiedzialne za bezpieczeństwo muszą być przygotowane na różne scenariusze ataku, co wymaga odpowiednich zasobów, wiedzy i strategii, aby skutecznie przeciwdziałać zagrożeniom.

Kolejnym ważnym aspektem analizowanym w tym podejściu jest przewidywalność narzędzi i metod wykorzystywanych przez stronę przeciwną. Jeśli obrońcy potrafią przewidzieć, jakie techniki ataku mogą być zastosowane, mają większe szanse na wdrożenie odpowiednich zabezpieczeń. Na przykład, jeśli znane są metody phishingowe stosowane przez atakujących, organizacja może wprowadzić szkolenia dla pracowników w celu zwiększenia świadomości i minimalizacji ryzyka.

Na podstawie tych czynników Marcello opracował wzór, który ma na celu określenie poziomu ryzyka w systemie informacyjnym. Proponowany model uwzględnia interakcję pomiędzy różnymi stronami, co pozwala na lepsze zrozumienie dynamiki rywalizacji i wpływu, jaki wywiera na bezpieczeństwo systemów informatycznych. Poniżej znajduje się

[92] G. Manunta (2000) Security and Methodology, Cranfield Security Centre, The Royal Military College of Science, Cranfield University, Wiltshire.

wzór zaproponowany przez Marcello na wyznaczenie poziomu ryzyka w systemie informacyjnym:

$$R = \Theta^2 \cdot \Psi \cdot \frac{1}{t^2} \cdot F$$

gdzie:

- Θ to poziom znajomości atakowanego systemu przez atakującego, który określa, jak szczegółowa jest jego wiedza na temat luk i funkcjonowania systemu, co wpływa na skuteczność potencjalnego ataku,

- Ψ to współczynnik określający relację pomiędzy poziomem akceptowalnego ryzyka ze strony broniącej a poziomem ryzyka, na jakie jest gotowa strona atakująca. Wskaźnik ten pomaga ocenić równowagę między działaniami obronnymi a agresywnymi próbami naruszenia systemu,

- $\frac{1}{t^2}$ to miara stopnia, w jakim atakujący nie posiada wiedzy na temat architektury, mechanizmów bezpieczeństwa oraz funkcjonowania atakowanego systemu. Wyższy poziom nieznajomości systemu przez atakującego może zwiększać skuteczność zabezpieczeń i utrudniać przeprowadzenie skutecznego ataku,

- F to stopień pewności atakującego, że jego działania zakończą się sukcesem w przełamaniu zabezpieczeń systemu. Im wyższy poziom przekonania o sukcesie, tym większe prawdopodobieństwo, że atakujący podejmie dalsze kroki, wierząc, że jego atak przyniesie pożądane rezultaty.

Interesującą koncepcję analizy i zarządzania ryzykiem przedstawił Ryba[93] który jest autorem metodyki MIR-2M. Zgodnie z tą metodą, proces oceny ryzyka dla każdego systemu informatycznego w organizacji przebiega według następujących etapów:

Etap 1 – identyfikacja kluczowych czynników wpływających na poziom ryzyka. Podejście to analizuje dziewięć ujednoliconych grup elementów (komponentów systemu informatycznego), które są brane pod uwagę przy tworzeniu wektora ryzyka:

$$\vec{R}_{S_i} = \varsigma_\lambda(\lambda_{S_i}) \cdot \vec{\lambda} + \varsigma_\rho(\lambda\rho_{S_i}) \cdot \vec{\rho} + \varsigma_\upsilon(\upsilon_{S_i}) \cdot \vec{\upsilon} + \varsigma_\omega(\omega_{S_i}) \cdot \vec{\omega} + \varsigma_\eta(\eta_{S_i}) \cdot \vec{\eta} + \varsigma_\theta(\theta_{S_i}) \cdot \vec{\theta} + + \varsigma_\tau(\tau_{S_i}) \cdot \vec{\tau} + \varsigma_\kappa(\kappa_{S_i}) \cdot \vec{\kappa} + \varsigma_\varphi(\varphi_{S_i}) \cdot \vec{\varphi}$$

gdzie:

[93] M. Ryba (2006) Wielowymiarowa metodyka analizy i zarządzania ryzykiem systemów informatycznych – MIR-2M, rozprawa doktorska, Kraków.

- ς stanowi funkcję normalizacyjną, która przekształca komponenty systemu informatycznego na wspólny przedział wartości,

- $\vec{\lambda}$ reprezentuje kategorię dostępności systemu informatycznego,

- $\vec{\rho}$ odnosi się do kategorii poufności danych w systemie informatycznym,

- $\vec{\upsilon}$ stanowi wskaźnik transmisji danych przez interfejsy systemu informatycznego, uwzględniając kierunek i rodzaj interfejsu, ilość przesyłanych danych na jednostkę czasu oraz liczbę dostępnych interfejsów w systemie,

- $\vec{\omega}$ odnosi się do skali systemu informatycznego,

- $\vec{\eta}$ oznacza zgodność z wymaganiami polityki bezpieczeństwa,a,

- $\vec{\theta}$ reprezentuje kategorię bezpieczeństwa systemów informatycznych,

- $\vec{\tau}$ określa skuteczność systemu monitorowania bezpieczeństwa,

- $\vec{\kappa}$ wskazuje na poziom konkurencyjności systemu informatycznego,

- $\vec{\varphi}$ mierzy wydajność procesu zarządzania zmianami.

Etap 2 – ustalenie wartości wag odzwierciedlających wpływ poszczególnych czynników na ogólny poziom ryzyka dla konkretnego systemu informatycznego. Wagi te są dostosowywane w zależności od sektora, w którym operuje dana organizacja.

$$\vec{R}_{S_i} = \vec{\Psi}_{S_i} \times \vec{R}_{S_i}$$

gdzie:

- $\vec{R}_{S_i}$ stanowi wektor ryzyka dla systemu informatycznego S_i,

- $\vec{\Psi}_{S_i}$ jest wektorem priorytetyzacji współrzędnych wektora ryzyka systemu informatycznego S_i, który ilustruje wagi wpływu poszczególnych komponentów ryzyka na łączny poziom ryzyka tego systemu.

Etap 3 – wyznaczenie ważonego wektora ryzyka. Ten wektor uwzględnia wpływ branży, w której funkcjonuje organizacja, na poziom ryzyka danego systemu informatycznego.

$$R_{S_i} = \left\|\vec{R}_{S_i}\right\|$$

Etap 4 – ustalenie końcowego poziomu ryzyka dla konkretnego systemu informatycznego.

$$\underline{R}_{S_i} = \left\|\vec{R}_{S_i}\right\|$$

Poziom ryzyka zdefiniowano jako wartość $R_{S_i} \in R$ odpowiadającą długości wektora $\vec{R}_{S_i}$, który jest ważonym wektorem ryzyka dla danego systemu informatycznego S_i. Wartość ta pozwala ocenić skalę zagrożeń w systemie – jeśli R_{S_i} przekracza 35, system narażony jest na najwyższy poziom ryzyka, co sugeruje konieczność natychmiastowej interwencji w celu zminimalizowania zagrożeń. Natomiast gdy wynik R_{S_i} znajduje się poniżej 10, oznacza to, że ryzyko jest znikome, a system funkcjonuje w bezpiecznych warunkach, nie wymagając pilnych działań zabezpieczających.

Proces zarządzania ryzykiem systemów informatycznych rozpoczyna się od oszacowania kosztu zmiany poziomu ryzyka. W pierwszym kroku należy dokładnie przeanalizować, jakie koszty mogą wynikać z modyfikacji ryzyka, uwzględniając zarówno aspekty biznesowe, jak i wartość pieniądza w czasie. Oznacza to, że przy ocenie zmian ryzyka trzeba brać pod uwagę nie tylko bezpośrednie wydatki związane z zabezpieczeniami, ale również długoterminowy wpływ tych wydatków na organizację, biorąc pod uwagę inflację, stopę zwrotu oraz inne wskaźniki finansowe.

$$\check{\Phi}_{\Delta\vec{R}_{S_i}^k} = \sum_{l=0}^{L} \frac{{}^lU_{S_i}^k - {}^lI_{S_i}^k - {}^lM_{S_i}^k - \Delta\mu_{S_i}^k}{(1+r)^l}$$

gdzie:

L – jest to czas, przez który przewiduje się użytkowanie systemu informatycznego S_i (wyrażony w latach),

${}^lU_{S_i}^k$ – oszczędności w danym roku l wynikające ze zmiany poziomu ryzyka systemu informatycznego opisanego za pomocą wektora $\Delta\vec{R}_{S_i}^k$ obejmują na przykład obniżenie kosztów ubezpieczeniowych. Zmniejszenie ryzyka może prowadzić do niższych składek ubezpieczeniowych, gdyż system S_i, o mniejszym ryzyku wymaga mniejszych nakładów na ochronę. Takie oszczędności mogą także objąć inne korzyści finansowe, jak mniejsze koszty związane z zarządzaniem incydentami czy mniejszą potrzebę inwestowania w dodatkowe zabezpieczenia.

${}^lI_{S_i}^k$ – wydatki inwestycyjne w danym roku l na system informatyczny S_i związane z wdrożeniem zmian ryzyka opisanych wektorem $\Delta\vec{R}_{S_i}^k$ systemu S_i,

${}^lM_{S_i}^k$ – wydatki w danym roku l związane z utrzymaniem mechanizmów w systemie S_i, które powodują zmiany ryzyka opisane wektorem $\Delta\vec{R}_{S_i}^k$ systemu S_i, mogą to być m.in. koszty serwisowania, aktualizacji oprogramowania, monitorowania zagrożeń, oraz

zapewnienia odpowiednich zasobów ludzkich do obsługi systemu. Równocześnie r to stopa dyskontowa, która odnosi się do okresu planowanej eksploatacji systemu S_i, $\Delta\mu_{S_i}^k$ to zmiana wielkości oczekiwanej rocznej straty, określa różnicę w przewidywanych stratach finansowych związanych z ryzykiem w systemie informatycznym S_i po wdrożeniu tych mechanizmów.

– *k* oznacza liczbę możliwych do zrealizowania zmian w systemie informatycznym, które mogą mieć wpływ na poziom ryzyka tego systemu. Każda z tych zmian jest rozważana w kontekście jej wpływu na bezpieczeństwo, niezawodność lub inne czynniki związane z ryzykiem, a ich wdrożenie może skutkować zwiększeniem lub zmniejszeniem tego ryzyka

Kolejnym krokiem w procesie zarządzania ryzykiem jest ocena znaczenia każdej planowanej zmiany oraz jej wpływu na ryzyko systemu informatycznego. W tym etapie przeprowadza się również analizę ekonomiczną, która pozwala ocenić, czy wprowadzenie danej zmiany jest opłacalne z punktu widzenia kosztów i korzyści. Ocenia się, w jakim stopniu zmiana wpłynie na obniżenie ryzyka oraz jakie oszczędności lub zyski może przynieść w dłuższym okresie, uwzględniając wartość pieniądza w czasie.

$$\chi\left(\Delta R_{S_i}^k\right) = \frac{\Delta R_{S_i}^k}{\check{\Phi}_{\Delta\vec{R}_{S_i}^k}}$$

$$\varsigma_{S_i}^k = 2^{h_{S_i}^k} \cdot \chi\left(\Delta R_{S_i}^k\right)$$

gdzie:

- $h_{S_i}^k$ współczynnik określający znaczenie danej zmiany, który odzwierciedla wpływ tej zmiany na ryzyko systemu informatycznego, pomagając ocenić jej priorytet oraz potencjalną korzyść w kontekście całościowego zarządzania ryzykiem,

- $\Delta R_{S_i}^k$ zmiana poziomu ryzyka systemu informatycznego S_i, uwzględniająca wagę poszczególnych czynników wpływających na to ryzyko

- $\check{\Phi}_{\Delta\vec{R}_{S_i}^k}$ to prognozowany koszt związany z wprowadzeniem zmiany ryzyka systemu informatycznego, opisanej przez dany wektor $\Delta\vec{R}_{S_i}^k$. Koszt ten obejmuje wydatki na wdrożenie nowych mechanizmów, utrzymanie systemu oraz inne czynniki niezbędne do zmniejszenia lub zarządzania ryzykiem zgodnie z założeniami zmiany

- $\varsigma_{S_i}^k$ alternatywne scenariusze ekonomiczne dla różnych systemów.

Model zaprezentowany powyżej stanowi solidną podstawę teoretyczną dla analizy i zarządzania ryzykiem w systemach informatycznych. Jego podstawy opierają się na

wytycznych normy NIST SP 800-30, co czyni go przydatnym narzędziem w kontekście ograniczania ryzyka. Ponadto model czerpie inspirację z różnych metod, co może wzbogacać jego zastosowanie w praktyce.

Jednakże, implementacja tego modelu w organizacjach napotyka liczne trudności. Jednym z głównych powodów jest potrzeba posiadania zaawansowanej wiedzy i umiejętności przez osoby odpowiedzialne za jego wprowadzenie. Co więcej, model nie spełnia niektórych wymogów normy ISO/IEC 27005.

Analizując metody oraz normy dotyczące oceny parametrów ryzyka w kontekście wymagań ISO/IEC 27005, można zauważyć, że większość z przedstawionych formalnych podejść nie jest zgodna z obowiązującymi standardami, zarówno krajowymi, jak i międzynarodowymi. Taka sytuacja może wynikać z faktu, że celem formalnych metod analizy ryzyka jest zoptymalizowanie procesów obliczeniowych w złożonych systemach informatycznych.

Interesującym rozwiązaniem jest formalny model systemu informacyjnego zaprezentowany w pracy[94] gdzie autorem jest Imed El Fray. Rozważany model wykazuje szerokie możliwości zastosowania i może być efektywnie użyty do analizy konkretnej organizacji oraz jej zasobów informatycznych, co czyni go istotnym narzędziem w procesie zarządzania ryzykiem.

El Fray definuje zbiór A określający zasoby:

$$A = \{a_i \,:\, i = 1, \ldots, n_A\}$$

Dodatkowo bierze pod uwagę następujące zbiory skończone:

$V = \{v_j : j = 1, \ldots, n_V\}$ zestaw podatności systemu, który obejmuje różnorodne słabości, luki i zagrożenia, które mogą być wykorzystane przez atakującego w celu naruszenia integralności, poufności lub dostępności danych,

$T = \{t_k : k = 1, \ldots, n_T\}$ zbiór potencjalnych zagrożeń, które mogą wpłynąć na system, obejmujący różnorodne czynniki ryzyka, takie jak ataki złośliwego oprogramowania, nieautoryzowany dostęp, awarie sprzętowe, błędy ludzkie czy katastrofy naturalne, które mogą prowadzić do uszkodzenia lub utraty danych,

[94] I. El Fray, *Metoda określająca zaufanie do systemu informacyjnego w oparciu o proces szacowania i postępowania z ryzykiem*, wyd. Stowarzyszenie Przyjaciół Wydziału Informatyki w Szczecinie, Szczecin, 2013.

$S = \{s_l : l = 1, \ldots, n_S\}$ zbiór możliwych scenariuszy incydentów, które mogą wystąpić w obrębie systemu informatycznego. Scenariusze te obejmują różnorodne sytuacje, takie jak włamania do systemu, wycieki danych, awarie systemów oraz inne nieprzewidziane zdarzenia, które mogą negatywnie wpłynąć na funkcjonowanie organizacji. Każdy scenariusz powinien uwzględniać kontekst incydentu, potencjalne przyczyny, skutki oraz możliwe reakcje ze strony organizacji w celu minimalizacji skutków tych incydentów,

$DP = \{dp_s : s = 1, \ldots, n_{DP}\}$ zbiór środków mających na celu redukcję potencjalnych zagrożeń, które mogą wpłynąć na bezpieczeństwo systemu informatycznego. Środki te obejmują różnorodne strategie, techniki oraz narzędzia, które organizacja może wdrożyć, aby zminimalizować ryzyko wystąpienia incydentów. Przykłady tych środków to zabezpieczenia fizyczne, polityki bezpieczeństwa, procedury awaryjne, a także rozwiązania technologiczne, takie jak zapory ogniowe, oprogramowanie antywirusowe czy systemy monitorowania. Celem tych działań jest zbudowanie silnej obrony przed potencjalnymi atakami oraz zwiększenie odporności organizacji na różnorodne zagrożenia,

$DI = \{di_t : t = 1, \ldots, n_{DI}\}$ zbiór środków mających na celu ograniczenie wpływu negatywnych zdarzeń na system informatyczny. Te środki obejmują różne działania, strategie i technologie, które organizacja wdraża, aby zminimalizować skutki ewentualnych incydentów. Przykłady obejmują plany awaryjne, procedury przywracania danych, szkolenia dla pracowników oraz systemy monitorowania, które pomagają w szybkiej reakcji na występujące zagrożenia. Celem tych działań jest nie tylko ochrona przed atakami, ale także zapewnienie ciągłości operacyjnej i minimalizacja strat w przypadku wystąpienia problemów.

Wymienione zbiory obejmują różnorodne elementy, które są kluczowe w analizie ryzyka systemu informatycznego. Składają się one z podatności zasobów na potencjalne zagrożenia, samych zagrożeń, scenariuszy ryzyka oraz środków, które mogą zredukować potencjał i skutki tych zagrożeń.

Aby ułatwić analizę, El Fray wprowadza funkcję pomocniczą, która definiuje wartość konkretnego zasobu, uwzględniając podstawowe parametry bezpieczeństwa, takie jak AIC, czyli dostępność, integralność i poufność. Dodatkowo, uwzględnia także inne istotne parametry, takie jak AUT (autentyczność) i NR (niezaprzeczalność).

Funkcja ta może być wykorzystana do oceny ryzyka i określenia, jakie zasoby są kluczowe dla utrzymania bezpieczeństwa systemu, a także do identyfikacji obszarów, które wymagają dodatkowej ochrony lub usprawnień w kontekście zarządzania ryzykiem.

$$value_A\colon A \rightarrow R$$

Zasoby systemu informatycznego mogą być narażone na różnorodne zagrożenia. W praktyce dane zagrożenie może wystąpić wyłącznie wtedy, gdy zasób wykazuje określoną podatność. Ta naturalna podatność, określana jako NV, może wynikać z różnych czynników, w tym zdarzeń „siły wyższej" oraz niezamierzonych i zamierzonych działań.

W celu dokładniejszej analizy ryzyka, El Fray wprowadza kolejną funkcję pomocniczą.

$$value_V\colon V \rightarrow R$$

Funkcja ta określa wartość konkretnego naturalnego narażenia w zależności od parametrów: AEV, które obejmują wypadki (Accident), błędy (Error) oraz działania zamierzone (Voluntary). Funkcja ta pozwala na lepsze zrozumienie, w jaki sposób różne rodzaje zagrożeń wpływają na ogólną podatność zasobów oraz na ocenę ryzyka, z jakim się one stykają.

Funkcja ta, podobnie jak wcześniejsza, może być skonfigurowana przy użyciu odpowiedniej tablicy, co pozwala na elastyczne dostosowanie parametrów do konkretnych potrzeb systemu.

Każdy system informatyczny, niezależnie od jego charakterystyki, dysponuje różnorodnymi środkami zaradczymi, które mają na celu ograniczenie zarówno potencjału zagrożeń, jak i ich skutków, które mogą wpływać na zasoby. W zależności od specyfiki zagrożeń oraz kontekstu operacyjnego, wdrażane są odpowiednie mechanizmy ochronne, które mają na celu minimalizację ryzyka.

Aby skutecznie zarządzać tymi środkami, konieczne jest zdefiniowanie ich wartości oraz efektów, jakie mogą przynieść w kontekście redukcji ryzyka. W tym celu El Fray wprowadził dwie dodatkowe funkcje:

1. $value_{DP}\colon DP \times S \times N \rightarrow R$
2. $value_{DI}.\colon DI \times S \times N \rightarrow R$

Funkcje określają wartości środków zmniejszających potencjalność zagrożeń oraz ich wpływ na zasoby systemu. Te funkcje pozwalają na precyzyjne określenie, jakie działania należy podjąć w obliczu zidentyfikowanych zagrożeń, a także umożliwią monitorowanie efektywności zastosowanych środków zaradczych.

Dalej El Fray zdefiniował funkcję, która przypisuje zbiory podatności do poszczególnych aktywów w systemie. Ta funkcja ma na celu określenie rzeczywistej

wartości podatności, która wynika z analizy i porównania naturalnego narażenia z wdrożonymi w organizacji środkami bezpieczeństwa.

Definicja 1. Podatność systemu informacyjnego IS definuje jako dowolną funkcję typu:

$$vul: A \rightarrow 2^V$$

powyższa definicja funkcji podatności pozwala na identyfikację konkretnych słabości związanych z poszczególnymi aktywami w systemie. Każde aktywo, w zależności od jego charakterystyki oraz wdrożonych środków ochrony, może mieć różny poziom podatności.

Dzięki tej konstrukcji sformułował ogólną definicję zagrożenia dla systemu. Ogólne zagrożenie zdefiniował jako kombinację wszystkich podatności zidentyfikowanych w systemie, co pozwala na lepsze zrozumienie oraz ocenę ryzyk, które mogą wpłynąć na bezpieczeństwo systemu informacyjnego. To podejście umożliwia organizacjom skuteczniejsze zarządzanie ryzykiem poprzez precyzyjne identyfikowanie i adresowanie specyficznych zagrożeń związanych z różnymi zasobami.

Definicja 2. Ogólne zagrożenie systemu El Fray zdefiniował jako dowolną funkcję:

$$thr: \overline{A \times V} \rightarrow 2^T$$

gdzie zbiór $\overline{A \times V}$ jest zbiorem wszystkich par (a, v) , które należą do zbioru $A \times V$ i spełniają warunek: $\exists_{X \subseteq V}\big(v \in X \wedge X \in vul(a)\big)$.

Podana funkcja definiuje zagrożenia dla aktywów z zbioru A w kontekście ich podatności ze zbioru V.

Definicja 3. Zbiór czwórek, które zostaną określone poniżej, nazwał systemem informacyjnym IS .

$$IS = \left\{\left(a, value_A(a), vul(a), thr(a, v)\right) \ : \ a \in A \wedge (a, v) \in \overline{A \times V}\right\}$$

Według tej definicji system informacyjny stanowi zbiór aktywów, które mają przypisane określone wartości oraz potencjalne podatności. Te podatności mogą być narażone na wykorzystanie przez różne zagrożenia. W ramach tego systemu, scenariusze ryzyka są przypisane do aktywów, które wykazują wrażliwość na te zagrożenia. Oznacza to, że każde aktywo, w zależności od swojej wartości i podatności, może być analizowane pod kątem różnych możliwych incydentów, które mogą zagrozić jego integralności, dostępności lub poufności. Takie podejście pozwala na lepsze zrozumienie ryzyk związanych z danym systemem i na opracowanie skutecznych strategii ochrony przed zagrożeniami.

Definicja 4. Ogólny scenariusz ryzyka systemu zdefiniował jako dowolną funkcję:

$$scen: \overline{A \times T} \rightarrow 2^S$$

gdzie: zbiór $\overline{A \times T}$ to zbiór wszystkich par (a, t) należących do $A \times T$ i spełniających warunek $\exists_{v \in V} \exists_{X \subseteq T} \big(t \in X \wedge X \in thr(a, v)\big)$.

Funkcja ta określa scenariusze ryzyka dla aktywów ze zbioru A w odniesieniu do ich zagrożeń ze zbioru T.

Aby oszacować wartość ryzyka dla danego systemu, konieczne jest zdefiniowanie działań, które podejmuje organizacja. Te działania obejmują wdrożenie środków bezpieczeństwa mających na celu potencjalną redukcję ryzyka oraz jego wpływu. Właściwe określenie tych działań jest kluczowe, ponieważ pozwala na skuteczne zarządzanie ryzykiem i zapewnienie bezpieczeństwa systemu informacyjnego. Działania te zostały zdefiniowane w następujący sposób.

Definicja 5. Ogólnym działaniem możliwości jest funkcja, która opisuje działania podejmowane w organizacji w celu redukcji prawdopodobieństwa wystąpienia podatności.

$$mis_{pot}: \overline{A \times S} \rightarrow 2^{DP}$$

gdzie: zbiór $\overline{A \times S}$ to zbiór wszystkich par (a, s) przynależących do $A \times S$ oraz spełniających określony warunek $\exists_{t \in T} \exists_{X \subseteq S} \big(s \in X \wedge X \in scen(a, t)\big)$.

Funkcja ta definiuje potencjalne działania, które można podjąć w odniesieniu do aktywów z określonego zbioru oraz ich powiązanych scenariuszy ryzyka ze zbioru S. Umożliwia to organizacji identyfikację konkretnych kroków, które mogą być wdrożone w celu zminimalizowania ryzyka, na jakie narażone są te zasoby. Dzięki temu możliwe staje się skuteczniejsze planowanie działań zapobiegawczych oraz alokacja odpowiednich środków bezpieczeństwa, co przyczynia się do zwiększenia ogólnego poziomu ochrony systemu informacyjnego.

Nie wszystkie przewidziane potencjalne działania muszą być wprowadzone w danym systemie. W związku z tym El Fray wyprowadził pojęcie zbioru działań, które zostały już zastosowane:

$$\overline{DP} = \Big\{(s, dp) \in S \times DP \ : \ \exists_{a \in A} \exists_{X \subseteq S} \Big(dp \in X \wedge X \in mis_{pot}(a, s)\Big)\Big\}$$

Zbiór ten obejmuje konkretne środki, które organizacja zdecydowała się wdrożyć, aby zminimalizować ryzyko i zabezpieczyć swoje zasoby. Taka klasyfikacja pozwala skupić się na rzeczywistych rozwiązaniach ochronnych, co z kolei ułatwia ocenę ich efektywności

oraz dalsze planowanie działań prewencyjnych. Z kolei ogólne działanie wpływu definiuje się w analogiczny sposób do ogólnego działania.

Definicja 6. Ogólne działanie mające na celu minimalizację wpływu. Działanie związane ze środkami wdrożonymi w organizacji, które redukują skutki zagrożeń, przedstawił jako funkcję:

$$mis_{imp}: \overline{A \times S} \rightarrow 2^{DI}$$

Funkcja przedstawiona wskazuje na działania, które mają wpływ na aktywa należące do określonego zbioru oraz na zagrożenia związane z tymi aktywami, zdefiniowane w zbiorze T.

Nie wszystkie przewidziane działania mające na celu ograniczenie wpływu muszą być implementowane w danym systemie informacyjnym. Dlatego El Fray zaproponował zbiór działań wpływowych, które faktycznie zostały wdrożone:

$$\overline{DI} = \left\{(s, di) \in S \times DI \ : \ \exists_{a \in A} \exists_{X \subseteq S} \left(di \in X \wedge X \in mis_{pot}(a, s)\right)\right\}$$

Działania te mogą obejmować różne strategie przyjęte przez organizację w celu zminimalizowania negatywnych skutków zagrożeń dla jej zasobów. Taki zbiór umożliwia dokładną ocenę skuteczności zastosowanych środków ochrony i pomaga w zarządzaniu ryzykiem w kontekście ochrony systemu przed potencjalnymi zagrożeniami.

Zbiór ten określa działania interwencyjne, które zostały wdrożone w kontekście konkretnego scenariusza ryzyka. Działania te mogą mieć charakter wykrywczy, korygujący lub też mogą pełnić rolę ochronną, paliatywną i regeneracyjną.

Metody używane do ustalania wag dla działań potencjalnych oraz oddziałujących są uzależnione od stosowanych w organizacji procedur audytowych. Aby wyznaczyć wagi dla działań związanych z potencjalnością i wpływem, wartości obliczone dla poszczególnych działań mają być pozyskiwane z tabel M^s_{pot} i M^s_{imp}. Wiersze oraz kolumny tych tabel są związane z oboma rodzajami działań. Tablica M^s_{pot} jest uzależniona od wartości naturalnej ekspozycji, a wartości zawarte w tabelach M^s_{pot} i M^s_{imp} powinny odzwierciedlać znaczenie krytycznych procesów biznesowych w danej organizacji.

Dla każdego scenariusza, s który pełni rolę poprzednika w określonej parze z zestawu $\overline{DP}$, jest obliczana tablica oznaczona jako M^s_{pot}. Analogicznie, dla par z zestawu $\overline{DI}$ tworzone są tablice M^s_{imp}. Oprócz tych obliczeń, wprowadzane są także dodatkowe zbiory tablic, które mają na celu ułatwienie analizy i oceny ryzyka w danym systemie:

$$M_{pot} = \ s : \exists_{dp \in DP}(s, dp) \in \overline{DP}\{M^s_{pot}\} \quad \text{i}$$

$$M_{imp} = \ s : \exists_{di \in DI}(s, di) \in \overline{DI}\{M^s_{imp}\}$$

Tablica M^s_{pot} zawiera wartości, które są związane z potencjalnymi działaniami związanymi z danym scenariuszem ryzyka. Natomiast tablica M^s_{imp} koncentruje się na oddziaływaniach oraz działaniach, które mogą mieć wpływ na zidentyfikowane zagrożenia.

Wprowadzenie tych zbiorów tablic pozwala na bardziej szczegółową analizę ryzyka oraz na lepsze zrozumienie, w jaki sposób poszczególne scenariusze mogą wpływać na aktywa organizacji. Dzięki temu można podejmować bardziej świadome decyzje dotyczące wdrażania odpowiednich środków zabezpieczających, co w efekcie przyczynia się do zwiększenia ogólnego poziomu bezpieczeństwa systemu informacyjnego.

Następnie dla każdej tablicy M^s_{imp} obliczana jest tablica oznaczona jako $M^{s,a}_{imp}$. Wagi w tej tablicy również opierają się na wartościach aktywów, które są reprezentowane jako $value_a(a)$. Dzięki temu możliwe jest uwzględnienie wpływu wartości aktywów na całościową ocenę ryzyka.

$$M^a_{imp} = \ s : \exists_{di \in DI}(s, di) \in \overline{DI}\{M^{s,a}_{imp}\}$$

Tablica $M^{s,a}_{imp}$ ma na celu dostarczenie dodatkowych informacji, które mogą być kluczowe w procesie podejmowania decyzji dotyczących strategii zarządzania ryzykiem. Analiza ta pozwala na lepsze zrozumienie, jak różne wartości aktywów mogą oddziaływać na potencjalne zagrożenia oraz skutki, jakie mogą wynikać z wdrożonych działań zabezpieczających.

Dalsze zestawienie tablic ma na celu stworzenie kompleksowego obrazu sytuacji ryzyka, co może prowadzić do bardziej efektywnego planowania działań naprawczych i prewencyjnych w organizacji. W ten sposób systematycznie buduje się bazę wiedzy, która ułatwia analizę i zarządzanie ryzykiem w kontekście bezpieczeństwa systemów informacyjnych.

Dla każdej pary tablic M^s_{pot} i $M^{s,a}_{imp}$ definiowana jest tablica $M^{s,a}$ zgodnie z wcześniej opisanym podejściem. Dodatkowo, wprowadzono zbiór wszystkich istotnych tablic, oznaczony jako $M = \ (a, s) \in \overline{A \times S}\{M^{s,a}\}$

Z każdej z wymienionych tablic generujemy odpowiednie wagi: W^s_{pot}, W^s_{imp}, $W^{s,a}_{imp}$, $W^{s,a}$, W^a. Gdzie $W = a \in A\{W^a\}$ obejmuje wszystkie wartości zasobów w systemie. Na

tej podstawie możemy obliczyć wagę ryzyka dla całego systemu, która jest oznaczona jako W_{IS}.

Waga ryzyka W_{imp}^{s} ma kluczowe znaczenie, ponieważ pozwala na oszacowanie potencjalnych zagrożeń w kontekście całego systemu informacyjnego. Wspólnie z pozostałymi wagami, takimi jak $W_{imp}^{s,a}$, $W^{s,a}$ i W^{a}, mogą one dostarczyć holistycznego widoku na poziom ryzyka, co jest niezbędne do skutecznego zarządzania bezpieczeństwem informacji. Umożliwia to organizacjom podejmowanie bardziej świadomych decyzji dotyczących inwestycji w środki ochrony oraz strategii reagowania na ewentualne incydenty.

Cała powyższa konstrukcja pozwala na formalne zdefiniowanie systemu bezpieczeństwa.

System ten można opisać jako zbiór zasobów, które mają przypisane różne wartości oraz podatności, a także są narażone na konkretne zagrożenia. W kontekście tego systemu wprowadzamy różne działania mające na celu minimalizację ryzyka oraz jego skutków, co wiąże się z wdrażaniem odpowiednich środków ochrony.

Konstrukcja ta uwzględnia zarówno potencjalne zagrożenia, jak i sposoby ich neutralizacji, co tworzy ramy do analizy ryzyka w organizacji. Dodatkowo, poprzez zdefiniowanie odpowiednich wag dla działań i zasobów, możliwe jest przeprowadzenie szczegółowych ocen oraz oszacowań, które pozwolą na lepsze zrozumienie dynamiki ryzyka w systemie.

Ostatecznie, ta formalna definicja systemu bezpieczeństwa staje się fundamentem dla dalszych analiz, które mają na celu poprawę ochrony informacji oraz efektywności zarządzania ryzykiem w organizacji.

Definicja 7. Systemem bezpieczeństwa informacji $\mathrm{SEC_{IS}}$ systemu IS jest:

$$\left(IS, V, vul, T, thr, S, scen, DP, mis_{pot}, DI, mis_{imp}, M, W, W_{IS}\right)$$

Dzięki temu system SEC_{IS}uwzględnia wszystkie kryteria określone w standardach OECD odnoszące się do informacji o bezpieczeństwie w danym systemie IS.

Poniżej mamy formalną definicję grafu G ilustrującego proces obliczania wag ryzyka systemu, W_{IS}.

Definicja 8. Niech $G = (Ve, E)$ będzie grafem, w którym wartość:

$$Ve = \{IS\} \cup A \cup scen\left(\overline{A, T}\right) \cup \overline{DP_{v_i}} \cup \overline{DI_{t_i}} \cup M_{pot} \cup M_{imp} \cup M \cup W \cup \{W_{IS}\},$$

to zbiór wierzchołków a E jest najmniejszym zbiorem spełniającym następujące warunki:

(1) $E \subseteq Ve \times Ve$,

(2) $(IS, a) \in E$, dla dowolnego $a \in A$,

(3) $(a, s) \in E$, dla dowolnego y $a \in A$i $s \in S$, jeżeli $s \in scen(a)$,

(4) $\big(s, (s, dp)\big) \in E$, dla dowolnego $s \in S$i $dp \in DP$, jeżeli $(s, dp) \in \overline{DP}$,

(5) $\big(s, (s, di)\big) \in E$, dla dowolnego $s \in S$i $di \in DI$, jeżeli $(s, di) \in \overline{DI}$,

(6) $\Big((s, dp), \big(M^s_{pot}, W^s_{pot}\big)\Big) \in E$, dla dowolnego $s \in S$i $dp \in DP$, jeżeli $(s, dp) \in \overline{DP}$,

(7) $\Big((s, di), \big(M^s_{imp}, W^s_{imp}\big)\Big) \in E$, dla dowolnego $s \in S$i $di \in DI$, jeżeli $(s, di) \in \overline{DI}$,

(8) $\Big(\big(M^s_{pot}, W^s_{pot}\big), (M^s, W^s)\Big) \in E$, dla dowolnego $s \in S$,

(9) $\Big(\big(M^s_{imp}, W^s_{imp}\big), \big(M^{s,a}_{imp}, W^{s,a}_{imp}\big)\Big) \in E$, dla dowolnego $(a, s) \in \overline{A \times S}$,

(10) $\Big(\big(M^{s,a}_{imp}, W^{s,a}_{imp}\big), \big(M^{s,a}, W^{s,a}\big)\Big) \in E$, dla dowolnego $(a, s) \in \overline{A \times S}$,

(11) $\Big(\big(M^{s,a}, W^{s,a}\big), W^a\Big) \in E$, dla dowolnego $(a, s) \in \overline{A \times S}$,

(12) $(W_a, W_{IS}) \in E$, dla dowolnego $a \in A$.

Poniżej przykład oceny ryzyka w systemie informatycznym z wykorzystaniem zaproponowanego podejścia.

Rozważmy pewien zbiór zasobów (aktywa) oznaczony jako A , w którym wyróżniamy jeden istotny element $a \in A$, odnoszący się do zasobu: „Bazy danych klientów zawierające wrażliwe informacje osobowe”. Przykładowo, przyjmijmy, że wartość tego zasobu wynosi $value_A(a) = (3,4,4,3,4)$.

Powyższe wartości są uzależnione od parametrów bezpieczeństwa, takich jak dostępność, integralność i poufność (AIC), oraz dodatkowych parametrów, takich jak autentyczność (AUT) i niezaprzeczalność (NR). Wartości tych parametrów są ustalane zgodnie z przyjętym systemem klasyfikacji zasobów, który jest zgodny z funkcjonalnością danej instytucji. W szczególności, ocena parametrów ma na celu uwzględnienie sytuacji, w których (a) nieuprawnione osoby mogą uzyskać dostęp do zasobu oraz (b) w wyniku pewnych manipulacji dokonanych na zasobie może zostać zakwestionowana jego cecha niezaprzeczalności.

Rozważmy zbiór podatności V, który zawiera tylko jeden element $v \in V$. Przez podatność rozumiemy „Złośliwe usunięcie danych osobowych" o wartości $value_V(v) = (0,0,2)$. Niech vul będzie funkcją podatności, która spełnia warunki $v \in X$ dla pewnego $X \in vul(a)$.

Dodatkowo rozważamy zbiór zagrożeń T, w którym znajduje się zagrożenie $t \in T$ o nazwie „Usunięcie oprogramowania". Niech thr będzie funkcją zagrożeń, która spełnia warunki $t \in X$ dla pewnego $X \in thr(a, v)$.

Niech S będzie zbiorem scenariuszy ryzyka, w którym $r \in S$ oraz $scen$ to funkcje scenariuszy, spełniające warunki $r \in X$ dla pewnego $X \in scen(a, t)$. Ponadto rozważamy tylko jeden scenariusz, mianowicie r, który odpowiada za sytuację „Dane użytkowników zostały usunięte".

Sukces danego scenariusza zależy od wdrożonych środków bezpieczeństwa, które zmniejszają potencjalne ryzyko związane z podatnościami i zagrożeniami odnoszącymi się do tego scenariusza. Dla analizowanego scenariusza uwzględniamy dwa środki $dp_1, dp_2 \in DP$, dp_1 i dp_2, które zmniejszają potencjał zagrożeń. dp_1 odnosi się do „Monitorowania dostępu do bazy danych użytkowników", natomiast dp_2 to „Monitorowania dostępu do bazy danych administratorów". Dodatkowo, rozważamy środki $di_1, di_2, di_3 \in DI$, które mają na celu ograniczenie wpływu zagrożeń. di_1 oznacza „Nadzór nad działaniami użytkowików", di_2 to minimalny plan „Kopii zapasowej danych osobowych przechowywanych w bazie danych", a di_3 odnosi się do „Ubezpieczenia strat". Przyjmujemy, że wartości w naszym przykładzie mają następujące ustalone wartości: $value_{DP}(dp_1) = 2$, $value_{DP}(dp_2) = 2$, $value_{DI}(di_1) = value_{DI}(di_2) = 3$, $value_{DI}(di_3) = 2$.

Wartości poszczególnych środków zmniejszających wpływ lub potencjalność, przedstawione w tym przykładzie, są obliczane na podstawie kwestionariuszy audytu wiedzy Mehari. Niech funkcje mis_{pot} i mis_{imp} odpowiadają tym środkom, gdzie mamy następujące zależności:

$$\forall_{i=1,2,3}\exists_{X\subseteq DP}\left(dp_i \in X \wedge X \in mis_{pot}(a,r)\right) \quad \text{i} \quad \forall_{i=1,2}\exists_{X\subseteq DI}\left(di_i \in X \wedge X \in mis_{imp}(a,r)\right).$$

Po obliczeniu wartości środków redukujących potencjalność oraz oszacowanego wpływu, możliwe jest ustalenie ich wag W^s_{pot} i W^s_{imp}. Wagi te zależą od wygenerowanych macierzy M^s_{imp} i M^s_{pot}.

Liczba generowanych tablic dla danego zasobu zależy od wartości parametrów bezpieczeństwa AIC, AUT i NR, zdarzenia związanego z podatnością AEV dla tego zasobu oraz od konkretnych wartości DP i DI, które są elementami danego scenariusza ryzyka.

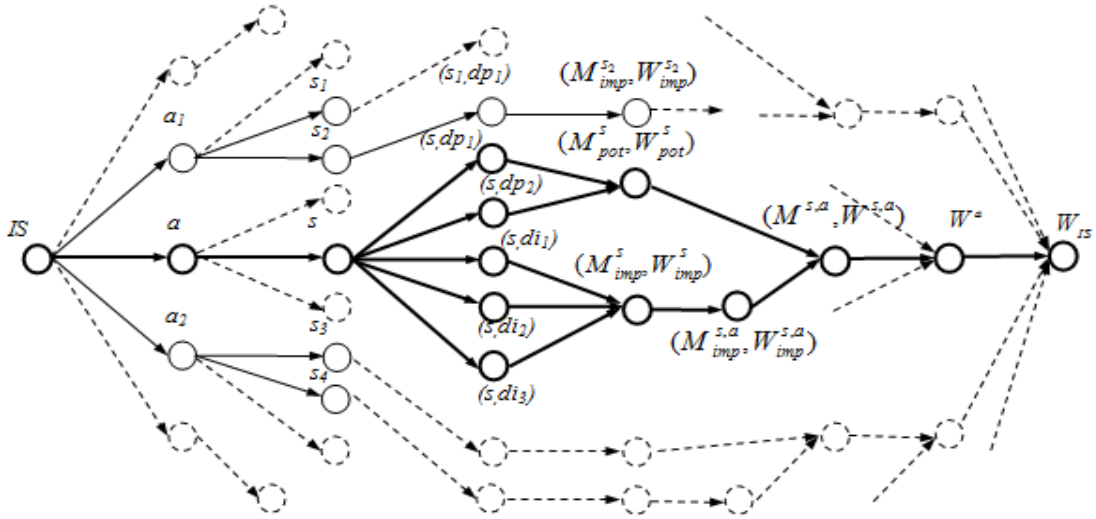
Uwzględniając wartości zasobów oraz obliczone wcześniej wagi W_{imp}^{s} (z tablicy M_{imp}^{s}), obliczamy wagi wpływu $W_{imp}^{s,a}$ z wygenerowanych tablic $M_{imp}^{s,a}$. Na ostatnim etapie tej analizy, wartości ryzyka W_S są obliczane na podstawie wcześniej wygenerowanych tablic M^s. Wartości te zależą od wartości wpływu i ryzyka.

W przykładzie możemy określić tablice M_{imp}^{s},M_{pot}^{s}, $M_{imp}^{s,a}$ i M^s.

Na koniec obliczamy wagi dla $W_{pot}^{s} = 2$, $(value_V(v) = 2, value_{DP}(dp_1) = 2, value_{DP}(dp_2) = 2)$, $W_{imp}^{s} = 2$, $(value_{DI}(di_1) = 3, value_{DI}(di_2) = 3, value_{DI}(di_3) = 2,$ $W_{imp}^{s,a} = 3$ $(value_A(a) = 3, W_{imp}^{s} = 2)$, $W^s = 3$ $(W_{imp}^{s,a} = 3, W_{pot}^{s} = 2)$ i wagi $W^s = 3$.

Wartość ryzyka całego systemu zależy od wartości innych scenariuszy. Gdyby system składał się tylko z jednego zasobu oraz innego obiektu rozważanego w przykładzie, wtedy wartość ryzyka systemu, W_{IS} równałaby się W^s.

Poniżej graf, który ilustruje obliczenia wartości ryzyka dla omawianego przykładowego systemu. Grubsze linie na grafie wskazują na te elementy obliczeń, które zostały wykorzystane w przedstawionym przykładzie.



Graf przedstawiający równoległe obliczenia wagi ryzyka systemu

Poniżej opisano algorytm El Fray obliczenia ryzyka:

a) Wprowadzenie danych do systemu:

◦ wprowadź zbiór aktywów A,

◦ wprowadź wartości dla vul i thr funkcje zależne od zbioru A,

b) Zbuduj graf systemu i oblicz wartości:

◦ oblicz wagi funkcji scenariuszy,

◦ określ zbiór $\overline{A \times S}$,

◦ równolegle oblicz wagi funkcji mis_{pot} i mis_{imp},

◦ równolegle oblicz tablice M^{s}_{pot}, M^{s}_{imp}, $M^{s,a}_{imp}$, $M^{s,a}$

◦ oblicz wagi W^{s}_{pot}, W^{s}_{imp}, $W^{s,a}_{imp}$, $W^{s,a}$

◦ oblicz wagi W^{a}

◦ oblicz wagę ryzyka systemu W_{IS}.

Nieustanny wzrost liczby potencjalnych scenariuszy zagrożeń związanych z podatnościami nowoczesnych rozwiązań programowych, narzędzi oraz systemów informatycznych prowadzi do wydłużenia i skomplikowania procesów analizy ryzyka, szczególnie w kontekście obecnie dostępnych ram metodologicznych. W rezultacie powstaje znaczne opóźnienie między wygenerowaniem wyników analizy a wdrożeniem odpowiednich środków bezpieczeństwa w systemie.

Paralelizacja obliczeń w kontekście oceny ryzyka to technika, która pozwala na równoczesne wykonywanie wielu obliczeń, co znacząco zwiększa efektywność całego procesu. W przeciwieństwie do metody sekwencyjnej, która wykonuje operacje jedna po drugiej, paralelizacja wykorzystuje wielowątkowość lub architekturę rozproszoną, aby podzielić zadania na mniejsze, niezależne fragmenty, które mogą być przetwarzane jednocześnie.

Dzięki takiemu podejściu, czas potrzebny na przeprowadzenie analizy ryzyka ulega znacznemu skróceniu, co jest szczególnie ważne w systemach, w których występuje duża liczba zasobów i potencjalnych zagrożeń. W sytuacjach, gdy mamy do czynienia z setkami lub nawet tysiącami scenariuszy ryzyka, tradycyjne podejście sekwencyjne może prowadzić do długotrwałych i czasochłonnych procesów analizy. Przykładowo, w przypadku oceny ryzyka związanego z nowymi rozwiązaniami programowymi czy systemami informatycznymi, konieczność analizy każdego scenariusza z osobna może skutkować poważnymi opóźnieniami w identyfikacji zagrożeń i wdrożeniu odpowiednich środków zaradczych.

Wykorzystanie równoległych obliczeń nie tylko przyspiesza obliczenia, ale także umożliwia bardziej efektywne wykorzystanie zasobów komputerowych. Systemy z wieloma

rdzeniami procesora mogą w pełni wykorzystać swoją moc obliczeniową, co prowadzi do optymalizacji czasu pracy i zwiększenia wydajności. Dodatkowo, równoległe przetwarzanie danych może ułatwić integrację nowych narzędzi analitycznych i metod oceny ryzyka, co w rezultacie może przyczynić się do uzyskania bardziej precyzyjnych wyników.

Równoległe obliczenia w metodzie oceny ryzyka stanowią istotny krok naprzód w procesie analizy, który pozwala na szybsze reagowanie na pojawiające się zagrożenia i zwiększa ogólną skuteczność systemu zarządzania bezpieczeństwem.

Kolejnym etapem było przeprowadzenie analizy współczesnych modeli formalnych wykorzystywanych w ocenie ryzyka systemów teleinformatycznych. Tematyka ta pozostaje w pełni aktualna, co potwierdzają liczne prace naukowe opublikowane w ostatnich pięciu latach. W pracy Kunza, Schneidera i Banse[95] zaproponowano metodologię ciągłej oceny ryzyka w środowiskach chmurowych, umożliwiającą automatyczne przypisywanie zagrożeń do zasobów na podstawie ich profilu. Z kolei w badaniu opublikowanym w International Journal of Information Security[96] zaprezentowano metamodelowe podejście do oceny ryzyka cyberbezpieczeństwa, wspierające kompleksową analizę i podejmowanie decyzji. Tarek i współautorzy[97] dokonali porównania sześciu wiodących metod oceny ryzyka (m.in. ISO 27005, OCTAVE, NIST SP 800–30) w kontekście chmurowym, wykazując konieczność ich adaptacji do charakterystyki nowoczesnych środowisk IT. Tematyka ryzyka w technologiach IoT została rozwinięta w modelu IoTSRM2[98], uwzględniającym najlepsze praktyki bezpieczeństwa Internetu Rzeczy. Podobny charakter ma systematyczny przegląd ryzyka w chmurze[99], który klasyfikuje metody oceny według typów modeli dostarczania

[95] Kunz, Immanuel, Angelika Schneider, and Christian Banse. "A continuous risk assessment methodology for cloud infrastructures." 2022 22nd IEEE International Symposium on Cluster, Cloud and Internet Computing (CCGrid). IEEE, 2022.

[96] Ekstedt, Mathias, et al. "Yet another cybersecurity risk assessment framework." International Journal of Information Security 22.6 (2023): 1713-1729.

[97] Ali, Tarek, Mohammed Al-Khalidi, and Rabab Al-Zaidi. "Information security risk assessment methods in cloud computing: Comprehensive review." Journal of Computer Information Systems (2024): 1-28.

[98] Popescu, Traian Mihai, Alina Madalina Popescu, and Gabriela Prostean. "Iot security risk management strategy reference model (Iotsrm2)." Future Internet 13.6 (2021): 148.

[99] Annunziata, Giusy, et al. "Security Risk Assessment on Cloud: A Systematic Mapping Study." Proceedings of the 28th International Conference on Evaluation and Assessment in Software Engineering. 2024.

oraz walidacji. Inne opracowania, m.in. autorstwa Babaei i in.[100], koncentrują się na wykorzystaniu sztucznej inteligencji i uczenia maszynowego do wykrywania ryzyka i anomalii. W obszarze IoMT i systemów medycznych zwrócono uwagę na konieczność formalnych ram oceny ryzyka[101], a nowe technologie i ich ryzyka zostały szczegółowo opisane w opracowaniach ISACA[102] i ISA/IEC[103]. **Analiza tych prac wykazuje, że modele formalne nadal odgrywają kluczową rolę w zarządzaniu ryzykiem w kontekście dynamicznie rozwijających się technologii cyfrowych.**

Choć w literaturze istnieje wiele prac poświęconych analizie ryzyka, w tym również tych opublikowanych w ostatniej dekadzie, wiele z nich koncentruje się na ogólnych aspektach tej problematyki. Brakuje jednak rozwiązań, które uwzględniałyby specyficzne wymagania dotyczące bezpieczeństwa systemów przetwarzających informacje niejawne oraz dostosowanie do polskich oraz międzynarodowych regulacji prawnych. W podrozdziale, rozdziału 2, zatytułowanym *Modele formalne,* przeprowadzono przegląd istniejących metod formalnych, a w wyniku tej analizy wyprowadzono formalną metodę. Metoda została opracowana w odpowiedzi na wnioski uzyskane z badania przeprowadzonego wśród interesariuszy ochrony informacji niejawnych (podrozdział *Badanie opinii interesariuszy ochrony informacji niejawnych, rozdziału 2)*, którzy wskazali, że aktualnie stosowane w praktyce metody są zbyt złożone i nie spełniają oczekiwań w zakresie efektywności.

W przeciwieństwie do samego przeglądu literatury, praca wnosi oryginalność poprzez zaproponowanie metody formalnej, która odpowiada na konkretne potrzeby związane z bezpieczeństwem informacji niejawnych i regulacjami prawnymi. Dowodem na skuteczność tej metodologii jest wykorzystanie jej w rzeczywistych procesach

---

[100] Babaei, Aptin, et al. "A Review of Machine Learning-based Security in Cloud Computing." arXiv preprint arXiv:2309.04911 (2023).

[101] Svandova, Katerina, and Zdenek Smutny. "Internet of Medical Things Security Frameworks for Risk Assessment and Management: A Scoping Review." Journal of Multidisciplinary Healthcare (2024): 2281-2301.

[102] KELLY, MICHAEL, and ADELINE CHAN. "Performing Risk Assessments of Emerging Technologies." ISACA Journal 6 (2022).

[103] "Cybersecurity Risk Assessment According to ISA/IEC 62443-3-2." ISA Global Cybersecurity Alliance, 2023. https://gca.isa.org/blog/cybersecurity-risk-assessment-according-to-isa-iec-62443-3-2. Dostęp 04.2025.

akredytacyjnych. W ten sposób praca przyczynia się do rozwoju narzędzi i metod, które mają bezpośrednie zastosowanie w praktyce, a nie tylko w teorii, co stanowi wkład w obszar analizy ryzyka w kontekście systemów bezpieczeństwa informacji wrażliwych.

2.11 Model Oceny Ryzyka Ochrony Informacji Niejawnych – MOROIN

W świetle tezy głównej i pomocniczej, opracowanie prostszego modelu oceny ryzyka znajduje pełne uzasadnienie. Teza główna wskazuje, że nadmiernie złożone metody oceny bezpieczeństwa systemów mogą paradoksalnie obniżyć ich faktyczny poziom bezpieczeństwa, mimo formalnej zgodności z normami. W tym kontekście opracowanie modelu o uproszczonej strukturze odpowiada na potrzebę efektywniejszego podejścia, które unika niepotrzebnych komplikacji, a jednocześnie spełnia wymogi służb odpowiedzialnych za ochronę informacji niejawnych.

Model przedstawiony w analizie, jako strukturalnie prostszy od bardziej złożonych metod, takich jak CRAMM czy NIST SP 800-30, został stworzony w odpowiedzi na praktyczne zapotrzebowanie podmiotów, które muszą spełnić wymagania takich instytucji jak ABW (Agencja Bezpieczeństwa Wewnętrznego), SKW (Służba Kontrwywiadu Wojskowego) oraz organizacji międzynarodowych jak ACT NATO (Allied Command Transformation North Atlantic Treaty Organization). Zgodnie z tezą pomocniczą, modelowanie i analiza formalna mogą dostarczać efektywnych narzędzi do oceny poziomu ryzyka. Jednak, jak pokazują badania, nie zawsze złożoność metody prowadzi do lepszych rezultatów w praktyce. Uproszczony model nie tylko spełnia formalne wymogi, ale także pozwala na szybsze i mniej kosztowne obliczenia, co ma kluczowe znaczenie w kontekście zarządzania ryzykiem w systemach teleinformatycznych.

Motywacja do stworzenia takiego modelu opiera się na potrzebie zapewnienia bardziej efektywnej metody oceny ryzyka, która nie będzie obciążona nadmierną ilością zmiennych i stopni złożoności, charakterystycznych dla bardziej formalnych podejść. Matematycznie model ten można uznać za minimalny, czyli taki, który zawiera tylko te elementy, które są absolutnie niezbędne do skutecznej analizy ryzyka. To sprawia, że jest on łatwiejszy do implementacji i użycia w rzeczywistych środowiskach, gdzie czas reakcji i prostota procesu mają kluczowe znaczenie.

Ponadto, akceptacja tego modelu w procesie akredytacji przez instytucje zajmujące się bezpieczeństwem krajowym jak i struktur międzynarodowych, stanowi silny dowód na

to, że spełnia on zarówno standardy praktyczne, jak i formalne. **W ten sposób zaproponowany model harmonijnie wpisuje się w postulaty obu tez: umożliwia bardziej efektywne zarządzanie bezpieczeństwem poprzez eliminację nadmiernej złożoności, jednocześnie dostarczając narzędzia do skutecznego wyznaczania poziomu ryzyk, szczególnie w kontekście ochrony informacji niejawnych.**

Model formalny analizy ryzyka dla systemu teleinformatycznego jest zbudowany z macierzy i systemu funkcji określających badane wartości, które integrują elementy procesu: identyfikacji zasobów, zagrożeń, podatności, oraz oszacowanie ryzyka.

2.11.1 Kluczowe pojęcia

Zasób (ZAS-x) to kategoria informacji lub element systemu teleinformatycznego, który wymaga ochrony.

Zagrożenie (ZAG-y) to potencjalne niebezpieczeństwo, które może wpłynąć na integralność, poufność lub dostępność zasobów.

Podatność (POD-z) to stopień, w jakim dany zasób jest narażony na dane zagrożenie.

Skutek (S_k) to skutki utraty poufności, integralności lub dostępności zasobów (wyrażone w skali 1-10).

Poziom ryzyka (R) to wartość wynikająca z połączenia oceny podatności i skutku dla każdego z trzech atrybutów bezpieczeństwa (poufności, integralności, dostępności).

2.11.2 Formalny Model Analizy Ryzyka

2.11.2.1 Definicja. Macierz zasobów i zagrożeń

Określmy zestaw zasobów $ZAS = \{zas_1, zas_2, \dots, zas_n\}$ oraz zagrożeń

$ZAG = \{zag_1, zag_2, \dots, zag_m\}$, gdzie n oraz m są odpowiednio dużymi liczbami naturalnymi. Widzimy, że elementy tych zbiorów można ustawić w macierz o n wierszach i m kolumnach.

Dla każdego zasobu i zagrożenia ocenia się możliwą podatność (oznaczane dalej: POD_z) oraz skutek dla każdego z trzech aspektów S_k: poufności, integralności, dostępności.

Dla systemu teleinformatycznego, przykładowe zasoby mogą obejmować:

- **ZAS-1**: Serwer aplikacji (hostuje stronę internetową firmy)
- **ZAS-2**: Baza danych klientów (zawiera wrażliwe informacje o klientach)

Natomiast zagrożenia to:

- **ZAG-1**: Atak DDoS (Distributed Denial of Service) – ma na celu zablokowanie dostępu do systemu przez przeciążenie go żądaniami.
- **ZAG-2**: Nieautoryzowany dostęp – próba uzyskania dostępu do systemu przez osobę nieuprawnioną.

2.11.2.2 Definicja. Podatność

Podatność na dane zagrożenie dla danego zasobu określa funkcja POD_z z iloczynu kartezjańskiego $ZAS \times ZAG$ w zbiór wartości liczbowych jak niżej:

$$POD_z: ZAS \times ZAG \rightarrow \{0,1, \dots ,10\},$$

Wartościami tej funkcji są wartości podatności na określone zasoby i zagrożenia. Jeżeli $POD_z(zas_i, zag_j) = 0$, dla pewnych $i \in \{1, \dots, n\}$ oraz $j \in \{1, \dots m\}$ oznacza, że zasób zas_i nie jest narażony na zagrożenie zag_j.

Przykład:

Podatność serwera aplikacyjnego (ZAS-1) na atak DDoS (ZAG-1) może być oceniona na 7, co oznacza stosunkowo wysoką podatność. Z kolei podatność na nieautoryzowany dostęp (ZAG-2) mogłaby wynosić 5, co wskazuje na umiarkowaną podatność.

2.11.2.3 Definicja. Skutek utraty atrybutu bezpieczeństwa

Skutek utraty atrybutu bezpieczeństwa ze względu na jedną z trzech własności: *poufność, integralność, dostępność* dla zasobu zas_i jest oceniany w skali 1 – 10. Określają to trzy funkcje

$$Sconf: ZAS \rightarrow \{1, \dots ,10\},$$

$$Sint: ZAS \rightarrow \{1, \dots ,10\},$$

$$Savail: ZAS \rightarrow \{1, \dots ,10\},$$ gdzie:

- funkcja $Sconf$ określa skutek utraty poufności,
- funkcja $Sint$ skutek utraty integralności,
- funkcja $Savail$ skutek utraty dostępności.

Przykład:

Dla serwera aplikacyjnego (ZAS-1) skutek utraty poufności (Sconf) na skutek ataku DDoS może być oceniony na 1 (minimalny), utrata integralności (Sint) na 2, a dostępności (Savail) na 8 (znaczący wpływ).

2.11.2.4 **Definicja. Poziom ryzyka**

Poziom ryzyka dla każdego zasobu zas_i i zagrożenia zag_j dla pewnych $i \in \{1, \dots, n\}$ oraz $j \in \{1, \dots m\}$ jest obliczany dla każdego z trzech aspektów oddzielnie. Określają to odpowiednie funkcje.

Dla poufności:

$Rconf: ZAS \times ZAG \rightarrow \{0,1, \dots ,10\} \times \{1, \dots ,10\}$, gdzie dla dowolnych $i \in \{1, \dots, n\}$ oraz $j \in \{1, \dots m\}$ mamy: $Rconf(zas_i, zag_j) = POD_z(zas_i, zag_j) \times Sconf(zas_i)$.

Dla integralności:

$Rint: ZAS \times ZAG \rightarrow \{0,1, \dots ,10\} \times \{1, \dots ,10\}$, gdzie dla dowolnych $i \in \{1, \dots, n\}$ oraz $j \in \{1, \dots m\}$ mamy: $Rint(zas_i, zag_j) = POD_z(zas_i, zag_j) \times Sint(zas_i)$.

Dla dostępności:

$Ravail: ZAS \times ZAG \rightarrow \{0,1, \dots ,10\} \times \{1, \dots ,10\}$, gdzie dla dowolnych $i \in \{1, \dots, n\}$ oraz $j \in \{1, \dots m\}$ mamy: $Ravail(zas_i, zag_j) = POD_z(zas_i, zag_j) \times Savail(zas_i)$.

Przykład:

Ryzyko dla poufności serwera aplikacyjnego w przypadku ataku DDoS wynosi:

$Rconf(zas_1, zag_1) = POD_1(zas_1, zag_1) \times Savail(zas_1) = 7 \times 1 = 7$

Z kolei ryzyko dla dostępności:

$Ravail(zas_1, zag_1) = POD_1(zas_1, zag_1) \times Savail(zas_1) = 7 \times 8 = 56$

2.11.2.5 **Definicja. Interpretacja ryzyka**

Poziom ryzyka R dla każdego z atrybutów jest interpretowany oddzielnie, zgodnie z ustaloną klasyfikacją:

- niski: $1 \leq R \leq 19$,
- średni: $20 \leq R \leq 49$,
- wysoki: $50 \leq R \leq 69$,
- maksymalny: $70 \leq R \leq 100$.

Przykład:

Ryzyko dla dostępności serwera aplikacyjnego w wyniku ataku DDoS wynosi 56, co oznacza wysoki poziom ryzyka ($50 \leq R \leq 69$). Ryzyko dla poufności, wynoszące 7, oznacza niski poziom ryzyka ($1 \leq R \leq 19$).

2.11.2.6 **Macierz ryzyka**

Dla każdego zasobu zas_i i zagrożenia zag_j dla dowolnych $i \in \{1, \dots, n\}$ oraz $j \in \{1, \dots m\}$ tworzymy macierz przedstawiającą poziomy ryzyka dla każdego z trzech aspektów (poufność, integralność, dostępność). W przygotowanej macierzy dla każdego zasobu i zagrożenia osobno oceniamy poziom ryzyka dla poufności, integralności i dostępności.

Przykład:

Analiza ryzyka dla dwóch zasobów (serwera i bazy danych) oraz dwóch zagrożeń (atak DDoS i nieautoryzowany dostęp), wraz z oceną podatności, skutków dla poufności, integralności, dostępności, oraz wyliczeniem ryzyka dla każdego aspektu przedstawia się następująco:

Zasób	Zagrożenie	Podatność	Poufność (Skutek)	Integralność (Skutek)	Dostępność (Skutek)	Ryzyko Poufność	Ryzyko Integralność	Ryzyko Dostępność
zas_1	zag_1	7	1	2	8	7	14	56
zas_1	zag_2	5	6	5	4	30	25	20
zas_2	zag_1	4	3	3	7	12	12	28
zas_2	zag_2	8	9	8	5	72	64	40

Wnioski:

1. Analiza ryzyka ujawnia kluczowe zagrożenia dla serwera aplikacji (ZAS-1) i bazy danych klientów (ZAS-2). Serwer aplikacji jest stosunkowo podatny na ataki DDoS (7/10), co stwarza wysokie ryzyko dla dostępności (56), podczas gdy skutki dla poufności i integralności są minimalne. Z kolei podatność na nieautoryzowany dostęp wynosi 5/10, co prowadzi do znaczącego ryzyka dla poufności (30), integralności (25) i dostępności (20). W przypadku bazy danych, jej podatność na ataki DDoS jest niższa (4/10), ale blokada dostępu może poważnie wpłynąć na dostępność (ryzyko 28), a skutki dla poufności i integralności są umiarkowane (12). Jednakże, nieautoryzowany dostęp do bazy danych stanowi największe zagrożenie z ryzykiem poufności wynoszącym 72 i integralności 64, natomiast dostępność jest mniej zagrożona (40).
2. Największe ryzyko występuje w przypadku zagrożenia nieautoryzowanego dostępu do bazy danych klientów (ZAS-2, ZAG-2), szczególnie w zakresie poufności i integralności. Wymaga to natychmiastowych działań zabezpieczających.

3. Ataki DDoS mają wysoki wpływ na dostępność serwera aplikacji (ZAS-1, ZAG-1) i bazy danych (ZAS-2, ZAG-1), więc wdrożenie środków ochrony przed tego rodzaju zagrożeniami powinno być również priorytetem.
4. Ryzyko związane z poufnością i integralnością serwera aplikacji jest umiarkowane, ale nie wymaga natychmiastowej interwencji, w przeciwieństwie do bazy danych.
5. W oparciu o powyższe wyniki, organizacja może zaplanować adekwatne środki ochrony i kontrolę ryzyka, koncentrując się na zasobach i zagrożeniach o najwyższych poziomach ryzyka.
6. Na podstawie oceny ryzyka dla każdego aspektu bezpieczeństwa oddzielnie, organizacja może podejmować decyzje dotyczące priorytetyzacji działań zabezpieczających, koncentrując się na tych zasobach, które mają wysoki poziom ryzyka w jednym lub więcej aspektach (poufność, integralność, dostępność).

2.12 Podsumowanie rozdziału 2

Rozdział drugi stanowi element rozprawy, w którym szczegółowo analizowane są wyniki badań oraz weryfikacja tezy głównej, mówiącej o tym, że nadmiernie skomplikowane metody oceny bezpieczeństwa systemów teleinformatycznych mogą paradoksalnie obniżać ich faktyczny poziom bezpieczeństwa, mimo zgodności z normami. Jednym z głównych zagadnień tego rozdziału jest analiza wpływu skomplikowania metod ochrony informacji na praktyczną skuteczność zarządzania ryzykiem. W tym kontekście przedstawiono Model Oceny Ryzyka Ochrony Informacji Niejawnych (MOROIN), opracowany w odpowiedzi na wymagania krajowych instytucji odpowiedzialnych za ochronę informacji oraz organizacji międzynarodowych, mający na celu dostarczenie o małej skali złożoności narzędzia do oceny ryzyka.

MOROIN, w odróżnieniu od bardziej złożonych modeli, cechuje się uproszczoną strukturą, która umożliwia skuteczniejszą ocenę poziomu ryzyka przy jednoczesnym spełnianiu formalnych wymagań. Teza pomocnicza przedstawia, że formalne modelowanie i analiza ryzyka mogą dostarczać skutecznych narzędzi do zarządzania bezpieczeństwem informacji niejawnych, jednak badania wykazały, że nadmierna złożoność metody nie zawsze prowadzi do lepszych rezultatów w praktyce.

Rozdział podkreśla, że uproszczony model MOROIN, mimo swojej niskiej złożoności, spełnia wszystkie formalne wymogi akredytacyjne stawiane przez kluczowe instytucje bezpieczeństwa, takie jak ABW, SKW oraz NATO. Dzięki swojej strukturze,

model ten pozwala na szybsze i mniej kosztowne obliczenia w porównaniu do innych metod. Został on zaprojektowany w taki sposób, aby minimalizować liczbę zmiennych, co czyni go bardziej efektywnym i elastycznym narzędziem w kontekście rzeczywistych warunków działania systemów teleinformatycznych.

W rozdziale zaprezentowano także przegląd istniejących norm i metod oceny ryzyka, które często są nadmiernie rozbudowane i trudne w implementacji. Wskazano, że bardziej złożone modele, choć oferują dokładne obliczenia, mogą być obciążające i mało praktyczne w rzeczywistych warunkach. Z kolei model MOROIN, jako strukturalnie prostszy, eliminuje te problemy i koncentruje się wyłącznie na niezbędnych elementach procesu oceny ryzyka.

Dzięki swojej elastyczności MOROIN dostosowuje się do specyficznych wymagań każdego systemu teleinformatycznego przetwarzającego informacje wrażliwe, co czyni go bardziej uniwersalnym narzędziem, zarówno w kontekście krajowych instytucji bezpieczeństwa, jak i międzynarodowych organizacji. W porównaniu z innymi metodami, takimi jak MEHARI, IT-Grundschutz, CRAMM, NIST SP 800-30 czy EBIOS, model MOROIN oferuje prostsze i bardziej intuicyjne podejście do zarządzania ryzykiem, co pozwala na łatwiejszą implementację w środowisku operacyjnym.

Przegląd norm wskazał, że chociaż niektóre z bardziej złożonych metod, jak CRAMM czy EBIOS, spełniają wymogi norm ISO/IEC 27005, to ich zastosowanie jest ograniczone ze względu na brak elastyczności lub zbyt skomplikowaną dokumentację. Z kolei model MOROIN, mimo swojej uproszczonej konstrukcji, pozwala na pełne spełnienie wymagań zarządzania ryzykiem w kontekście ochrony informacji niejawnych. Istotnym faktem jest, że miary i parametry ryzyka używane w analizach, zarówno jakościowe, jak i ilościowe, powinny być odpowiednio dostosowane do specyfiki systemu, co umożliwia ich precyzyjne wdrożenie w praktyce.

Rozdział ten dostarcza zarówno teoretycznych narzędzi, jak i empirycznych dowodów na to, że uproszczony model oceny ryzyka, taki jak MOROIN, może być bardziej efektywny w ochronie informacji niejawnych niż bardziej złożone metody. Analiza negatywnych skutków złożoności tradycyjnych metod potwierdza, że uproszczone podejście może prowadzić do lepszego zarządzania bezpieczeństwem, co ma kluczowe znaczenie w praktyce. Wskazanie tych mankamentów w obszarze zarządzania ryzykiem otwiera nową perspektywę dla dalszego rozwoju strategii ochrony informacji, oferując alternatywne, bardziej praktyczne podejście, które może być łatwo zaadaptowane w różnych środowiskach organizacyjnych.

ROZDZIAŁ 3

Implementacja modelu MOROIN w ocenie poziomu bezpieczeństwa systemów teleinformatycznych

Rozdział szczegółowo omawia zastosowanie formalnego modelu MOROIN w kontekście oceny poziomu bezpieczeństwa systemów informacyjnych. Wykorzystywany model jest narzędziem do analizy ryzyka, umożliwiając precyzyjne wyliczenie poziomów ryzyka w odniesieniu do zdefiniowanych zagrożeń oraz podatności systemu. Rozdział stanowi kompleksowy przewodnik po poszczególnych etapach wykorzystania modelu MOROIN w procesie oceny bezpieczeństwa, zapewniając jednocześnie kontekst teoretyczny i praktyczny.

Podejście z Rozdziału 3, choć oparte na modelu MOROIN, wykracza poza samą analizę ryzyka – stanowi zintegrowany cykl zarządzania bezpieczeństwem informacji niejawnych, uwzględniający m.in. odpowiedzialność personelu, analizę zasobów, środki ochrony oraz akceptację ryzyka szczątkowego.

Na wstępie, rozdział przedstawia przyjęte założenia, które stanowią fundament dla zastosowania modelu w badanym systemie. Następnie, dokonano szczegółowego opisu rodzaju chronionych informacji, podkreślając ich znaczenie i wymagania bezpieczeństwa. Zagadnieniami omawianymi w rozdziale są pojęcia ryzyka szczątkowego oraz odpowiedzialności personelu bezpieczeństwa, które są istotne dla zrozumienia i zarządzania procesami bezpieczeństwa w organizacji.

Każdy krok zastosowania modelu MOROIN został wyjaśniony, począwszy od identyfikacji zasobów, przez analizę zagrożeń, po szacowanie i ocenę ryzyka.

Dzięki strukturalnemu podejściu, niniejszy rozdział nie tylko demonstruje, jak można wdrożyć model MOROIN w praktyce, ale również podkreśla rolę odpowiedzialnego personelu bezpieczeństwa w ciągłym monitorowaniu oraz doskonaleniu procedur bezpieczeństwa informacyjnego.

3.1 Zarządzanie ryzykiem informacji wrażliwych z modelem MOROIN

Na ocenę poziomu bezpieczeństwa systemów teleinformatycznych możemy spojrzeć poprzez pryzmat metod szacowania ryzyka.

Z przeglądu istniejących norm i dobrych praktyk wynika, że w każdej z nich mamy do czynienia z trzema rodzajami metod: ilościowej, jakościowej oraz mieszanej. W ilościowym podejściu do szacowania ryzyka kluczowe jest ustalenie dwóch głównych parametrów: wartości skutku i prawdopodobieństwa wystąpienia danego ryzyka. Natomiast w podejściu jakościowym mamy do czynienia z subiektywną oceną, która jest oparta na najlepszych praktykach i doświadczeniu. Efektem takiej oceny są listy potencjalnych zagrożeń z określeniem ich relatywnego ryzyka (niskiego, średniego, wysokiego).[104]

Specyfika ochrony systemów teleinformatycznych przetwarzających informacje wrażliwe wymaga uwzględnienia zarówno fizycznych składników systemu, jak i wartości niematerialnych, takich jak prawa własności intelektualnej, umowy, bazy danych, wiedza pracowników oraz reputacja jednostki organizacyjnej. Te niematerialne elementy często trudno wyrazić w konkretnych wartościach liczbowych, dlatego konieczne jest stosowanie różnorodnych metod oceny, obejmujących zarówno podejścia ilościowe, jak i jakościowe, aby właściwie zrozumieć i ocenić te aktywa.

Warto zastosować metodę „dziel i zwyciężaj", która umożliwia podział rozległych systemów na podsystemy oraz powiązania między nimi, co znacznie ułatwia i usprawnia ocenę ryzyka w przypadku dużych, złożonych struktur. Dzięki rozbiciu dużego systemu na mniejsze elementy możliwa staje się bardziej szczegółowa analiza poziomu bezpieczeństwa poszczególnych podsystemów, co sprzyja identyfikowaniu i zarządzaniu ryzykiem.

Model Oceny Ryzyka Ochrony Informacji Niejawnych (MOROIN) można zastosować do realizacji takich procesów oceny ryzyka. Pozwala on na uporządkowane zebranie danych w tabeli, która uwzględnia zasoby, zagrożenia, podatności i potencjalne skutki. Kolumny w tej tabeli obejmują m.in. właściciela ryzyka, zidentyfikowane zagrożenie, przeciwdziałanie zagrożeniu, wpływ na atrybuty bezpieczeństwa (poufność, dostępność, integralność), poziom podatności, poziom skutku oraz poziom ryzyka wynikający z całej oceny. Taka struktura umożliwia cykliczne powtarzanie i przegląd ryzyk, bez znacznego nakładu pracy, jednocześnie zapewniając wysoki poziom bezpieczeństwa.

Ocena poziomów zagrożeń, podatności oraz ryzyka może być z sukcesem przeprowadzona metodą ekspercką, która integruje aspekty ilościowe i jakościowe, bazując

[104] Pałęga, Michał. "Zarządzanie ryzykiem bezpieczeństwa informacji w świetle wymagań normatywnych." Systemy Wspomagania w Inżynierii Produkcji 6 (2017).

na poziomie wymagań dotyczących bezpieczeństwa, szczególnie w zakresie ochrony poufności, integralności i dostępności informacji.

Ocena poziomu bezpieczeństwa informacji niejawnych w systemie teleinformatycznym powinna się odbywać w ramach następujących procesów postępowania z ryzykiem:

1. Wstępne szacowanie
2. Działania w przypadku zmiany poziomu ryzyka
3. Akceptacja ryzyka
4. Monitorowanie ryzyka

W procesie określania ryzyka, należy zidentyfikować:

1. Zagrożenia dla systemu teleinformatycznego.
2. Podatności systemu na te zagrożenia.
3. Potencjalne skutki wystąpienia incydentów bezpieczeństwa.
4. Środki zapobiegawcze w odniesieniu do zagrożeń wpływających na poufność, integralność i dostępność.

Przydzielenie właścicieli ryzyka, odpowiedzialnych za akceptację określonych poziomów ryzyka, jest ważnym krokiem w procesie zarządzania bezpieczeństwem informacji.

Ocena ryzyka powinna być wykonywana przed wdrożeniem środków zabezpieczających, przed zmianami systemowymi, w odpowiedzi na nowe zagrożenia lub po wystąpieniu incydentu bezpieczeństwa. Regularne, co najmniej półroczne, przeprowadzanie ocen jest niezbędne do zapewnienia ciągłości procesu zarządzania ryzykiem.

Zarządzanie ryzykiem w systemach chroniących informacje niejawne powinno być realizowane w sposób ciągły, zapewniając odpowiedni poziom bezpieczeństwa i dostosowanie zabezpieczeń do zidentyfikowanych zagrożeń. Ważne jest szybkie reagowanie na nowe zagrożenia, ich ocena i poprawa skuteczności stosowanych środków zabezpieczających.

3.2 Środowisko bezpieczeństwa przykładowego systemu

W celu przedstawienia w praktyce zastosowania metody MOROIN, analizujemy przykładowy system teleinformatyczny zainstalowany w jednostce organizacyjnej. Przyjmujemy, że system ten musi być odpowiednio skonfigurowany i zabezpieczony, aby umożliwić przetwarzanie informacji niejawnych o najwyższych poziomach tajności, takich jak: ŚCIŚLE TAJNE, NATO COSMIC TOP SECRET, TRÈS SECRET UE/EU TOP SECRET oraz ESA TOP SECRET. Proces utwardzania systemu obejmuje zarówno aspekty techniczne, jak i organizacyjne oraz proceduralne, wymagając dokładnego określenia lokalizacji systemu, spełnienia norm dotyczących strefy ochrony elektromagnetycznej i wdrożenia procedur ochrony.

W analizowanym systemie przetwarzane są zarówno informacje niejawne własne, jak i przyjęte od jednostek współpracujących w realizacji projektów oraz umów. Informacje te obejmują dokumentację techniczną zamówień, projektów, umów i kontraktów objętych tajemnicą, a także dokumenty związane z działalnością Pionu Ochrony Informacji Niejawnych. Zgodnie z modelem MOROIN, zasady zarządzania tymi informacjami muszą uwzględniać ich poufność, dostępność oraz integralność.

Kontrola dostępu i szkolenia użytkowników odgrywają również rolę w zapewnianiu bezpieczeństwa. W systemie zastosujemy wielopoziomowy tryb bezpieczeństwa pracy a uprawnienia użytkowników będą przydzielane przez Kierownika Jednostki Organizacyjnej zgodnie z zasadą wiedzy uzasadnionej. Wszyscy użytkownicy przejdą obowiązkowe szkolenie w zakresie ochrony informacji niejawnych oraz procedur bezpiecznej eksploatacji, co jest spójne z wymaganiami MOROIN dotyczącymi ciągłego zarządzania ryzykiem.

Analiza obejmuje identyfikację zagrożeń i podatności oraz oszacowanie potencjalnych skutków incydentów bezpieczeństwa, zgodnie z wymaganiami norm bezpieczeństwa. Pozwoli to na zastosowanie właściwych środków zabezpieczających, takich jak ochrona elektromagnetyczna i techniczna. Procedury te muszą być zgodne z certyfikacyjnymi ograniczeniami i prawnymi wymogami dotyczącymi ochrony informacji niejawnych.

Proces ciągłego monitorowania i oceny ryzyka, w tym przypisanie odpowiedzialności za określone ryzyka, pozwala na adaptacyjne i skuteczne zarządzanie bezpieczeństwem informacji, spełniając rygory zarówno narodowe, jak i międzynarodowe. W ten sposób przykładowy system teleinformatyczny, wykorzystując model MOROIN,

demonstruje ochronę informacji niejawnych poprzez holistyczne podejście do bezpieczeństwa, obejmujące aspekty techniczne, proceduralne i organizacyjne.

3.3 Odpowiedzialność personelu

W systemach zarządzania bezpieczeństwem informacji, gdzie czynniki ludzkie mogą stanowić najsłabsze ogniwo, niezbędne jest wdrożenie skutecznych mechanizmów minimalizujących ryzyko operacyjne. W procesie oceny poziomu bezpieczeństwa systemu, szczególną uwagę należy poświęcić roli i odpowiedzialności personelu, aby zapewnić bezpieczeństwo informacji niejawnych.

Jednym z fundamentalnych elementów strategii zabezpieczającej jest „zasada dwóch", która zakłada dodatkową warstwę zabezpieczeń poprzez wymaganie podwójnej autoryzacji dla krytycznych operacji lub organizacyjnie nadzór nad systemem poprzez dwie osoby, pracujące w dwóch działach i niepodlegające bezpośrednio pod tego samego przełożonego. Taka praktyka jest szczególnie istotna w ochronie informacji niejawnych, ponieważ pomaga zredukować ryzyko błędów ludzkich lub nieumyślnych działań, mogących prowadzić do poważnych incydentów bezpieczeństwa.

W wielu systemach, aby uzyskać dostęp do poufnych danych, użytkownicy są zobowiązani do przejścia przez dwa niezależne kroki weryfikacyjne.

Skuteczne zarządzanie ryzykiem w systemach przetwarzających informacje niejawne wymaga zaangażowania osób, które pełnią określone role w ramach organizacji:

- Kierownik Jednostki Organizacyjnej, odpowiedzialny za nadzór nad procesem zarządzania ryzykiem, z naciskiem na jego ciągłość i efektywność w ochronie informacji niejawnych.
- Pełnomocnik ds. Ochrony Informacji Niejawnych, koordynuje operacje bezpieczeństwa i zapewnia zgodność z obowiązującymi politykami i procedurami.
- Inspektor Bezpieczeństwa Teleinformatycznego, przeprowadza techniczne audyty, analizuje ryzyko teleinformatyczne oraz identyfikuje luki w zabezpieczeniach, proponując środki zapobiegawcze.
- Administrator Systemu, zarządza codziennymi operacjami systemu, wdraża mechanizmy bezpieczeństwa i monitoruje ich skuteczność poprzez regularne oceny ryzyka.

Wprowadzenie zasady dwóch i zdefiniowanie jasnych odpowiedzialności personelu umożliwia stworzenie spójnego i wielowarstwowego podejścia do zarządzania ryzykiem w systemach przetwarzających informacje niejawne. Dzięki zintegrowanej pracy zespołu ds. bezpieczeństwa oraz wprowadzeniu mechanizmów podwójnej kontroli operacji, organizacja może skutecznie minimalizować potencjalne zagrożenia związane z czynnikiem ludzkim i zwiększać poziom ochrony informacji. Ostatecznie takie działania ułatwiają bardziej efektywne zarządzanie ryzykiem i ograniczają prawdopodobieństwo wystąpienia incydentów bezpieczeństwa.

3.4 Założenia wstępne w ocenie poziomu bezpieczeństwa

Implementując model MOROIN w analizowanym przykładzie systemu, definiujemy wartości wykorzystywane przy ocenie poziomu bezpieczeństwa. Model ten wspiera proces poprzez dostarczanie strukturalnego podejścia do identyfikacji i oceny zasobów. Model pomaga w przypisaniu poziomów wpływu, umożliwiając tym samym precyzyjne zdefiniowanie priorytetów ochrony. Ocena podatności zasobów na zidentyfikowane zagrożenia prowadzi do świadomego określenia, które obszary wymagają największej uwagi. Ostateczne określenie rozmiaru ryzyk dostarcza narzędzi niezbędnych do podejmowania efektywnych decyzji dotyczących zarządzania bezpieczeństwem, zapewniając zgodność z regulacjami oraz gotowość do reakcji na rzeczywiste zagrożenia.

Podczas oceny skutków utraty **poufności** zasobów określamy poziomy zgodne z ustawowymi klauzulami oraz przypisujemy im odpowiednie zakresy wartości liczbowych, zgodnie z poniższą tabelą:

Poziom poufności	Wartość liczbowa
Jawne	0
Zastrzeżone / NATO RESTRICTED /RESTREINT UE/EU RESTRICTED	1,2,3
Poufne / NATO CONFIDENTIAL/ CONFIDENTIEL UE/EU CONFIDENTIAL	4,5,6
Tajne / NATO SECRET/ SECRET UE/EU SECRET	7,8,9
Ściśle Tajne / NATO COSMIC TOP SECRET/ TRÈS SECRET UE/ EU TOP SECRET	10

Tabela 1: Enumeracja poziomów skutków dla utraty pufności

Podczas oceny skutków utraty **dostępności** zasobów określamy poziomy dostępności, przypisując im odpowiednie wartości liczbowe, zgodnie z poniższą tabelą:

Poziom dostępności	Wartość liczbowa	Wyznacznik
Niski	1,2	Długotrwały brak dostępu do informacji nie wpłynie istotnie na działania jednostki organizacyjnej.
Średni	3,4,5	Brak dostępu do informacji może znacząco utrudnić realizację zadań, dlatego dostępność powinna zostać przywrócona w ciągu 3-4 dni.
Wysoki	6,7,8	Ograniczenie dostępu do informacji może poważnie zaburzyć funkcjonowanie jednostki, wymagając przywrócenia dostępności w krótkim czasie, tj. w ciągu kilku godzin.
Krytyczny	9	Brak dostępu do informacji uniemożliwia działalność jednostki, a przywrócenie dostępu musi nastąpić w ciągu kilku minut.
Absolutny	10	Utrata dostępności informacji jest absolutnie niedopuszczalna.

Tabela 2: Enumeracja poziomów skutków dla utraty dostępności

W kontekście analizy skutków utraty **integralności** zasobów wyznaczamy cztery poziomy wymagań dotyczących konieczności zachowania integralności, oraz określamy odpowiadające im przedziały wartości liczbowych (1-10) w każdej z tych kategorii, jak przedstawiono w poniższej tabeli:

Poziom integralności	Wartość liczbowa
Niskie wymagania	1, 2, 3
Średnie wymagania	4, 5, 6
Wysokie wymagania	7, 8, 9
Obligatoryjne wymagania	10

Tabela 3: Enumeracja poziomów skutków dla utraty integralności

Oszacowanie stopnia narażenia zasobów w systemie teleinformatycznym na identyfikowane zagrożenia przeprowadzamy z wykorzystaniem przedstawionej tabeli:

Poziom podatności	Wartość liczbowa
Brak	0
Niski	1,2,3
Średni	4,5,6
Wysoki	7,8,9
Krytyczny	10

Tabela 4: Enumeracja poziomów podatności

Ocenę wielkości zidentyfikowanego ryzyka przeprowadzamy, uwzględniając wartość poszczególnych zasobów, ustalaną na podstawie wymagań dotyczących ochrony poufności, dostępności i integralności. Określamy to na podstawie oszacowanych wartości liczbowych, które reprezentują skutki ujawnienia, modyfikacji lub braku dostępności zasobów. Dodatkowo bierzemy pod uwagę poziomy zagrożeń, które mogą wpłynąć na poszczególne zasoby, oraz szacowane wartości liczbowe poziomów podatności na te zagrożenia.

Określenie poziomów ryzyka związanych opieramy na wartościach liczbowych, których przyjmujemy wartości zgodnie z poniższą tabelą:

Poziom ryzyka	Wartość liczbowa
Niski	1-19
Średni	20-49
Wysoki	50-69
Maksymalny	70-100

Tabela 5: Enumeracja poziomów ryzyka

3.5 Analiza zasobów

W strukturach organizacyjnych istnieje wiele odmian informacji, których ochrona jest niezbędna. Dokumenty i dane niejawne mogą być opatrzone różnymi poziomami klauzul tajności, co determinuje zróżnicowane wymogi dotyczące ich zabezpieczenia.

Pierwszym krokiem w procesie jest klasyfikacja informacji przetwarzanych w systemie na grupy kategorii, w zależności od dziedziny działania jednostki (podział według specyfiki informacji). Taka klasyfikacja umożliwia oszacowanie podatności zasobów jednostki na ryzyko ujawnienia, utraty, modyfikacji lub niedostępności. Jednocześnie pozwala ona na identyfikację potencjalnych źródeł zagrożeń oraz ocena, dla jakich podmiotów informacje te mogą przedstawiać wartość.

W dalszej części procesu, w obrębie każdej z wyodrębnionych grup informacyjnych, wskazuje się te, dla których wymagany jest jednakowy poziom ochrony, określony klauzulą tajności. Istotne jest, aby zespoły informacji podlegały nadzorowi jednej osoby odpowiedzialnej za ich bezpieczeństwo, takiej jak kierownik działu, departamentu czy biura. Osoba ta powinna uczestniczyć w analizie skutków potencjalnej utraty, ujawnienia bądź modyfikacji tych danych. Rezultatem tego procesu będzie wyodrębnienie kategorii zasobów informacyjnych o wspólnych wymogach funkcjonowania i zabezpieczeń.

Dla każdej zidentyfikowanej kategorii zostanie przypisany wiersz w macierzy zabezpieczeń. Konieczne będzie określenie wymogów dotyczących utrzymania integralności, poufności oraz dostępności dla każdej kategorii. Podobnie, należy zidentyfikować inne zasoby systemowe wymagające zabezpieczenia. Ocena potrzeby ochrony ich aspektów bezpieczeństwa będzie uzależniona od ich charakterystyki. Standardowe oprogramowanie oraz hardware będą wymagały oceny pod kątem dostępności (zapewnienie niezawodności), natomiast urządzenia kryptograficzne, klucze szyfrujące, hasła oraz dokumentacja bezpieczeństwa systemu będą wymagały również oceny w kontekście poufności. Jeżeli zasoby są istotne w kontekście więcej niż jednego wymiaru

bezpieczeństwa (integralności, poufności, dostępności), powinny być wielokrotnie uwzględniane w odpowiednich rubrykach macierzy.

W ramach przykładowego systemu teleinformatycznego przeprowadzana jest identyfikacja zasobów wymagających ochrony. Zapewnienie bezpieczeństwa tych zasobów w systemie teleinformatycznym jest kluczowe dla utrzymania poufności, integralności oraz dostępności informacji niejawnych przetwarzanych w tym systemie.

Nr	Nazwa	Atrybut
ZAS-01	Informacje niejawne własne	Poufność, Integralność
ZAS-02	Informacje niejawne powierzone	Poufność, Integralność
ZAS-03	Gotowość do przetwarzania informacji	Dostępność
ZAS-04	Wizerunek organizacji	Poufność, Dostępność, Integralność
ZAS-05	Elementy systemu IT	Poufność, Dostępność, Integralność
ZAS-06	Nośniki danych	Poufność, Integralność
ZAS-07	Oprogramowanie systemu	Poufność, Dostępność, Integralność
ZAS-08	Hasło Inspektora BTI	Poufność
ZAS-09	Hasło Administratora IT	Poufność
ZAS-10	Hasła Użytkowników IT	Poufność
ZAS-11	Kopie bezpieczeństwa systemu	Poufność, Dostępność, Integralność
ZAS-12	Kopie bezpieczeństwa danych	Poufność, Dostępność, Integralność
ZAS-13	Dane z audytów bezpieczeństwa	Poufność, Integralność
ZAS-14	Personel ochrony	Dostępność
ZAS-15	Administrator IT	Poufność, Integralność
ZAS-16	Użytkownicy IT	Poufność, Dostępność
ZAS-17	Pomieszczenia	Dostępność
ZAS-18	Infrastruktura	Dostępność, Integralność
ZAS-19	Dokumentacja i procedury operacyjne	Poufność, Integralność
ZAS-20	Dane osobowe użytkowników systemu	Poufność, Integralność

Tabela 6: Analiza zasobów

3.6 Analiza zagrożeń

Następnym etapem w procesie zarządzania bezpieczeństwem informacji jest identyfikacja potencjalnych zagrożeń, które mogą wpłynąć na integralność, poufność oraz dostępność poszczególnych kategorii zasobów informacyjnych przetwarzanych w systemie. Każde zidentyfikowane zagrożenie starannie odnotowujemy w nagłówku odpowiedniej kolumny macierzy ryzyka, dokonując niezbędnych rozszerzeń w jej strukturze, jeśli zajdzie taka potrzeba. Ponieważ pewne zagrożenia mogą oddziaływać na kilka aspektów bezpieczeństwa jednocześnie, uwzględniamy je adekwatnie w różnych sekcjach macierzy.

W odniesieniu do systemów teleinformatycznych, szczegółowo definiujemy zagrożenia dla bezpieczeństwa informacji niejawnych. Podczas przeprowadzania rzetelnej analizy ryzyka koncentrujemy się wyłącznie na identyfikacji tych zagrożeń, dla których potwierdziliśmy istnienie podatności w systemie. Poniższa tabela porządkuje rozpoznane zagrożenia, jednocześnie wskazując ich źródła, obejmujące zarówno siły natury, jak i intencjonalne lub przypadkowe działania ludzkie.

Dokładna identyfikacja i analiza zagrożeń stanowi krytyczny element zabezpieczeń organizacji, będąc instrumentalną w opracowywaniu skutecznych strategii ochronnych i minimalizujących potencjalne skutki ataków lub nieprzewidzianych zdarzeń destabilizujących operacyjność systemów czy procesów.

Zagrożenie	Opis	Wpływa na			Źródło zagrożenia		
		Poufność	Dostępność	Integralność	Siły natury	Celowe działanie człowieka	Przypadkowe działania człowieka
ZAG-01	Incydent związany z pożarem w firmowej lokalizacji.		ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-6, ZAS-7, ZAS-8, ZAS-9, ZAS-10, ZAS-11, ZAS-12, ZAS-13, ZAS-17			x	x
ZAG-02	Zalanie pomieszczenia systemu w wyniku niesprawności instalacji.		ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-6, ZAS-7, ZAS-17		x	x	x

ZAG-03	Uszkodzenie sprzętu spowodowane wyładowaniem atmosferycznym.		ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5		x		
ZAG-04	Katastrofa budowlana wpływająca na system teleinformatyczny.		ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-11 ZAS-12, ZAS-17		x		x
ZAG-05	Przerwa w zasilaniu elektrycznym zakłócająca działanie systemu.		ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5		x		x
ZAG-06	Awaria urządzeń zasilania awaryjnego wpływająca na ciągłość pracy systemu.		ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5		x		x
ZAG-07	Próba działalności wywiadowczej ze strony obcych służb specjalnych i rządów.	ZAS-1, ZAS-2, ZAS-4, ZAS-6, ZAS-8, ZAS-9, ZAS-10, ZAS-16	ZAS-12			x	

ZAG-08	Sabotaż i działania dywersyjne wpływające na pracę systemu.		ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-6, ZAS-7, ZAS-8, ZAS-12, ZAS-13, ZAS-14, ZAS-17	ZAS-5, ZAS-7 ZAS-12		x	
ZAG-09	Infiltracja elektromagnetyczna wpływająca na bezpieczeństwo danych.	ZAS-1, ZAS-2, ZAS-4				x	
ZAG-10	Awaria środków ochrony fizycznej i środków wspomagających wpływająca na dostęp do systemu.	ZAS-1, ZAS-2, ZAS-4	ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-17		x		x
ZAG-11	Kradzież urządzenia systemu i naruszenie bezpieczeństwa.	ZAS-1, ZAS-2, ZAS-4, ZAS-6	ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-6, ZAS-7			x	

ZAG-12	Kradzież nośników danych niejawnych i dokumentów niejawnych.	ZAS-1, ZAS-2, ZAS-4, ZAS-6, ZAS-12	ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-6, ZAS-11, ZAS-12	ZAS-5		x	
ZAG-13	Nieautoryzowane użycie urządzenia systemu do celów niezwiązanym z jego przeznaczeniem.	ZAS-1, ZAS-2, ZAS-4, ZAS-6	ZAS-3, ZAS-5, ZAS-7	ZAS-5, ZAS-7		x	
ZAG-14	Niewłaściwe kwalifikacje personelu ds. bezpieczeństwa teleinformatycznego.	ZAS-1, ZAS-2, ZAS-4, ZAS-6, ZAS-8, ZAS-9, ZAS-10, ZAS-11 ZAS-12	ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-6, ZAS-7, ZAS-11 ZAS-12, ZAS-13,	ZAS-1, ZAS-2, ZAS-4, ZAS-5, ZAS-7		x	x

ZAG-15	Rotacja personelu, choroby i niedostępność tymczasowa personelu wpływająca na kontynuację pracy systemu.	ZAS-1, ZAS-2, ZAS-4	ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-7, ZAS-8, ZAS-9, ZAS-10, ZAS-11 ZAS-12, ZAS-13, ZAS-14, ZAS-15, ZAS-16, ZAS-17	ZAS-1, ZAS-2, ZAS-4, ZAS-5, ZAS-7	x		x
ZAG-16	Brak procedur i planów ochrony informacji niejawnych.	ZAS-1, ZAS-2, ZAS-4, ZAS-6, ZAS-12	ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-7, ZAS-11, ZAS-12	ZAS-1, ZAS-2, ZAS-4, ZAS-5, ZAS-7			x
ZAG-17	Brak znajomości procedur przez użytkowników systemu.	ZAS-1, ZAS-2, ZAS-4, ZAS-6, ZAS-12	ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-6, ZAS-12	ZAS-1, ZAS-2, ZAS-4, ZAS-5, ZAS-12		x	x

ZAG-18	Niewłaściwa eksploatacja urządzenia systemu.	ZAS-1, ZAS-2, ZAS-4	ZAS-1, ZAS-2, ZAS-3, ZAS-5, ZAS-7, ZAS-17	ZAS-5, ZAS-7		x	x
ZAG-19	Wykorzystanie urządzeń spoza strefy ochronnej systemu.	ZAS-1, ZAS-2, ZAS-4				x	x
ZAG-20	Pozostawienie niezabezpieczonego urządzenia teleinformatycznego.	ZAS-1, ZAS-2, ZAS-4	ZAS-5	ZAS-1, ZAS-2, ZAS-5		x	x
ZAG-21	Pozostawienie niezabezpieczonego dokumentu niejawnego.	ZAS-1, ZAS-2, ZAS-4, ZAS-6	ZAS-6	ZAS-6		x	x
ZAG-22	Próba podglądu monitora systemu lub wydruku przez nieuprawnione osoby.	ZAS-1, ZAS-2, ZAS-4				x	x
ZAG-23	Wyprowadzenie niezabezpieczonych dokumentów (nośników) poza strefę ochronną.	ZAS-1, ZAS-2, ZAS-4, ZAS-6 ZAS-12				x	x

ZAG-24	Uszkodzenia i awarie urządzeń systemu, zarówno te wynikające z czynników losowych, jak i celowych działań ludzi.		ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-17	ZAS-5	x		x
ZAG-25	Ujawnienie informacji niejawnych w wyniku przekazania ich osobom nieuprawnionym.	ZAS-1, ZAS-2, ZAS-4, ZAS-12				x	x
ZAG-26	Brak właściwych cech etyczno-moralnych u użytkowników systemu.	ZAS-1, ZAS-2, ZAS-4, ZAS-6, ZAS-12	ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-6, ZAS-7, ZAS-12	ZAS-1, ZAS-2, ZAS-4, ZAS-5, ZAS-6, ZAS-7		x	x
ZAG-27	Utrata dostępu do pomieszczenia systemu na skutek zagubienia klucza lub niesprawności zamka, a także kradzieży kluczy do pomieszczeń służbowych i szaf na dokumenty niejawne.		ZAS-1, ZAS-2, ZAS-3, ZAS-5, ZAS-6, ZAS-17			x	x

ZAG-28	Błędy i pomyłki administratora systemu wpływające na bezpieczeństwo informacji.	ZAS-1, ZAS-2, ZAS-4, ZAS-12	ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-6, ZAS-7, ZAS-12, ZAS-13	ZAS-1, ZAS-2			x
ZAG-29	Błędy i pomyłki użytkowników systemu wpływające na integralność i poufność danych.	ZAS-1, ZAS-2, ZAS-4	ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-6, ZAS-7, ZAS-12	ZAS-1, ZAS-2			x
ZAG-30	Brak procedur gromadzenia i archiwizacji danych oraz wykonywania kopii zapasowych.	ZAS-1, ZAS-2, ZAS-12	ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-7, ZAS-11, ZAS-12	ZAS-7, ZAS-11, ZAS-12			x

ZAG-31	Niewłaściwe działanie oprogramowania urządzenia systemu.		ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-7, ZAS-12, ZAS-13	ZAS-5			x
ZAG-32	Brak bieżącego monitorowania pracy systemu.	ZAS-1, ZAS-2, ZAS-4	ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-7, ZAS-12, ZAS-13	ZAS-1, ZAS-2, ZAS-4, ZAS-5, ZAS-7			x
ZAG-33	Nieuprawniony dostęp do systemu i zasobów informacyjnych systemu.	ZAS-1, ZAS-2, ZAS-4	ZAS-1, ZAS-2, ZAS-4, ZAS-5, ZAS-7	ZAS-1, ZAS-2, ZAS-4, ZAS-5, ZAS-7		x	
ZAG-34	Brak certyfikatu dla elementu systemu wpływającego na bezpieczeństwo.	ZAS-1, ZAS-2, ZAS-4	ZAS-3, ZAS-4, ZAS-5				x
ZAG-35	Modyfikacja parametrów instalacyjnych przez osoby nieuprawnione.	ZAS-1, ZAS-2, ZAS-4	ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-7	ZAS-7		x	

ZAG-36	Wprowadzenie szkodliwego oprogramowania do systemu.		ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-7	ZAS-1, ZAS-2, ZAS-7			x
ZAG-37	Nieuprawnione kopiowanie danych na informatycznych nośnikach danych.	ZAS-1, ZAS-2, ZAS-4				x	x
ZAG-38	Zmiana niepożądanych parametrów w kodzie źródłowym.		ZAS-1, ZAS-2, ZAS-3, ZAS-5, ZAS-6, ZAS-17			x	x
ZAG-39	Zagrożenie wynikające z wprowadzenia dezinformacji i manipulacji informacjami.	ZAS-1, ZAS-2, ZAS-4, ZAS-12	ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-6, ZAS-7, ZAS-12, ZAS-13	ZAS-1, ZAS-2			x
ZAG-40	Wyciek informacji w wyniku zaawansowanego ataku phishingowego.	ZAS-1, ZAS-2, ZAS-4	ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-6, ZAS-7, ZAS-12	ZAS-1, ZAS-2			x

ZAG-41	Skomplikowane procedury dostępu do systemu wpływające na wydajność pracy.	ZAS-1, ZAS-2, ZAS-12	ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-7, ZAS-11, ZAS-12	ZAS-7, ZAS-11, ZAS-12			x
ZAG-42	Zagrożenie ze strony zanieczyszczonych nośników danych wpływające na integralność danych.		ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-7, ZAS-12, ZAS-13	ZAS-5			x
ZAG-43	Brak procedur zabezpieczających przed włamaniem fizycznym.	ZAS-1, ZAS-2, ZAS-4	ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-7, ZAS-12, ZAS-13	ZAS-1, ZAS-2, ZAS-4, ZAS-5, ZAS-7			x
ZAG-44	Ujawnienie informacji wynikające z wykorzystania podsłuchu.	ZAS-1, ZAS-2, ZAS-4	ZAS-1, ZAS-2, ZAS-4, ZAS-5, ZAS-7	ZAS-1, ZAS-2, ZAS-4, ZAS-5, ZAS-7		x	

ZAG-45	Wyłudzenie informacji niejawnych za pomocą socjotechnik.	ZAS-1, ZAS-2, ZAS-4	ZAS-3, ZAS-4, ZAS-5				x
ZAG-46	Niewłaściwa kontrola dostępu do dokumentów niejawnych wpływająca na poufność informacji.	ZAS-1, ZAS-2, ZAS-4	ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-7	ZAS-7		x	
ZAG-47	Ujawnienie informacji wynikające z nieostrzeżenia przez zabezpieczenia antywirusowe.		ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-7	ZAS-1, ZAS-2, ZAS-7			x
ZAG-48	Błąd ludzki w procesie przetwarzania informacji wpływający na bezpieczeństwo danych.	ZAS-1, ZAS-2, ZAS-4				x	x
ZAG-49	Ujawnienie informacji w wyniku wykorzystania exploitów.		ZAS-1, ZAS-2, ZAS-3, ZAS-5, ZAS-6, ZAS-17			x	x

ZAG-50	Wykorzystanie słabych haseł przez intruzów wpływających na integralność i poufność informacji.	ZAS-1, ZAS-2, ZAS-4, ZAS-12	ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-6, ZAS-7, ZAS-12, ZAS-13	ZAS-1, ZAS-2			x
ZAG-51	Zagrożenie wynikające z braku aktualizacji oprogramowania wpływające na bezpieczeństwo systemu.	ZAS-1, ZAS-2, ZAS-4	ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-6, ZAS-7, ZAS-12	ZAS-1, ZAS-2			x
ZAG-52	Niedostateczne zabezpieczenia przeciwwłamaniowe.	ZAS-1, ZAS-2, ZAS-12	ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-7, ZAS-11, ZAS-12	ZAS-7, ZAS-11, ZAS-12			x

ZAG-53	Nieautoryzowane modyfikacje konfiguracji systemu wpływające na integralność i dostęp do systemu.		ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-7, ZAS-12, ZAS-13	ZAS-5			x
ZAG-54	Atak na system teleinformatyczny z wykorzystaniem ransomware wpływający na integralność danych.	ZAS-1, ZAS-2, ZAS-4	ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-7, ZAS-12, ZAS-13	ZAS-1, ZAS-2, ZAS-4, ZAS-5, ZAS-7			x
ZAG-55	Ujawnienie informacji na skutek błędów w procesie transmisji danych.	ZAS-1, ZAS-2, ZAS-4	ZAS-1, ZAS-2, ZAS-4, ZAS-5, ZAS-7	ZAS-1, ZAS-2, ZAS-4, ZAS-5, ZAS-7		x	
ZAG-56	Nieodpowiednie procedury zarządzania i dystrybucji kluczy kryptograficznych wpływające na bezpieczeństwo systemu.	ZAS-1, ZAS-2, ZAS-4	ZAS-3, ZAS-4, ZAS-5				x

ZAG-57	Nieprawidłowa identyfikacja i uwierzytelnianie użytkowników.	ZAS-1, ZAS-2, ZAS-4	ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-7	ZAS-7		x	
ZAG-58	Brak mechanizmów audytu bezpieczeństwa i monitorowania systemu.		ZAS-1, ZAS-2, ZAS-3, ZAS-4, ZAS-7	ZAS-1, ZAS-2, ZAS-7			x
ZAG-59	Nieuprawnione ujawnienie informacji na skutek niewłaściwego zarządzania dokumentami niejawnymi.	ZAS-1, ZAS-2, ZAS-4				x	x
ZAG-60	Atak hakerski z wykorzystaniem technik inżynierii społecznej wpływający na bezpieczeństwo systemu	ZAS-1, ZAS-2, ZAS-5				x	x

Tabela 7: Analiza zagrożeń

3.7 Identyfikacja zabezpieczeń

W systemie teleinformatycznego stosujemy odpowiednie środki zabezpieczające dla zidentyfikowanych zagrożeń. Działania te wdrażamy zgodnie z wymaganiami ustawowymi, mając na celu zapewnienie niezbędnego poziomu bezpieczeństwa informacji niejawnych przetwarzanych w tym systemie.

Rozwiązania to opis środków mających na celu ochronę systemu teleinformatycznego przed różnymi rodzajami zagrożeń. Stanowią integralną częścią planu bezpieczeństwa informacji. Ważne jest, aby regularnie aktualizować te środki zabezpieczające, szkolić personel w zakresie bezpieczeństwa informacji i przeprowadzać testy bezpieczeństwa, aby utrzymać system w jak najwyższym stanie bezpieczeństwa.

Lp.	Zagrożenie	Rozwiązania
ZAG-1	Pożar w lokalizacji firmy	- System przeciwpożarowy. - Przenośny sprzęt gaśniczy. - Instrukcja bezpieczeństwa pożarowego. - Szkolenia personelu.
ZAG-2	Zalanie pomieszczenia systemu w wyniku awarii instalacji	- Lokalizacja pomieszczenia systemu. - Okresowe przeglądy infrastruktury technicznej.
ZAG-3	Wyładowanie atmosferyczne	- Instalacja odgromowa. - Zabezpieczenia urządzeń. - Procedury eksploatacji urządzeń.
ZAG-4	Katastrofa budowlana	- Pomieszczenie systemu o wzmocnionej konstrukcji budowlanej.
ZAG-5	Awaria sieci zasilania elektrycznego	- Centralny system gwarantowanego zasilania. - Kontrole stanu instalacji zasilania elektrycznego.
ZAG-6	Awaria urządzeń gwarantowanego zasilania	- Kontrole stanu instalacji zasilania awaryjnego. - Procedury wykonywania kopii zapasowych. - Procedura serwisowania.
ZAG-7	Działalność wywiadowcza ze strony obcych służb specjalnych i rządów	- System kontroli dostępu. - System sygnalizacji włamania i napadu. - Zabezpieczenia fizyczne. - Ochrona elektromagnetyczna. - Zaufani użytkownicy. - Kontrole użytkowników.
ZAG-8	Działania dywersyjne i sabotażowe	- System kontroli dostępu. - System sygnalizacji włamania i napadu. - Zabezpieczenia fizyczne.
ZAG-9	Infiltracja elektromagnetyczna	- Sprzętowa Strefa Ochrony Elektromagnetycznej. - Certyfikowane urządzenia z obniżoną emisją. - Procedury eksploatacji.

Lp.	Zagrożenie	Rozwiązania
ZAG-10	Awaria środków ochrony fizycznej i technicznych środków wspomagających	- Procedury postępowania w przypadku awarii systemów ochrony technicznej. - Przeglądy systemów ochrony technicznej.
ZAG-11	Kradzież urządzenia systemu	- System kontroli dostępu. - System sygnalizacji włamania i napadu. - Zabezpieczenia fizyczne. - Nadzór i szkolenia personelu. - Kontrole użytkowników. - Zaufani użytkownicy.
ZAG-12	Kradzież informatycznych nośników danych niejawnych i dokumentów niejawnych	- System kontroli dostępu. - System sygnalizacji włamania i napadu. - Zabezpieczenia fizyczne. - Procedury zarządzania dokumentami. - Rejestracja i ewidencjonowanie dokumentów. - Szkolenia personelu. - Kontrole użytkowników. - Zaufani użytkownicy.
ZAG-13	Wykorzystywanie systemu (urządzenia) do celów nie związanych z jego przeznaczeniem	- Nadzór i szkolenia personelu. - Kontrole użytkowników.
ZAG-14	Niewłaściwe kwalifikacje personelu bezpieczeństwa teleinformatycznego	- Procedury kadrowe. - Poświadczenia bezpieczeństwa. - Szkolenia w ABW/SKW i zakresie bezpieczeństwa informacji.
ZAG-15	Zmiany (rotacja) personelu, choroba, czasowa niedostępność personelu	- Planowanie kadry. - Planowanie urlopów i działalności bieżącej. - Procedury.

Lp.	Zagrożenie	Rozwiązania
ZAG-16	Brak procedur i planów w zakresie ochrony informacji niejawnych	- Wdrożenie PBE. - Akredytacja bezpieczeństwa Systemu teleinformatycznego. - Opracowanie Planu ochrony. - Instrukcje przetwarzania informacji niejawnych. - Testy bezpieczeństwa.
ZAG-17	Nieznajomość procedur przez użytkowników systemu	- Nadzór i szkolenia personelu. - Kontrole użytkowników.
ZAG-18	Niewłaściwa eksploatacja urządzenia (systemu)	- Procedury dotyczące użytkowania urządzeń. - Procedury serwisowania urządzeń. - Procedury wykonywania kopii zapasowych. - Przeglądy systemów ochrony technicznej.
ZAG-19	Wykorzystanie urządzeń spoza systemu (strefy ochronnej)	- Procedury zarządzania konfiguracją systemu. - Nadzór personelu. - Procedury użytkowania urządzeń. - Procedury serwisowania urządzeń.
ZAG-20	Pozostawienie niezabezpieczonego urządzenia (teleinformatycznego)	- Procedury zasad użytkowania systemu. - Nadzór personelu. - Szkolenia użytkowników.
ZAG-21	Pozostawienie niezabezpieczonego dokumentu niejawnego	- Procedury zarządzania dokumentami niejawnymi. - Rejestracja i ewidencjonowanie dokumentów. - Szkolenia personelu. - Kontrole użytkowników. - Zaufani użytkownicy.
ZAG-22	Podgląd monitora systemu lub wydruku	- Procedury zasad użytkowania systemu. - Nadzór personelu. - Szkolenia użytkowników. - Szkolenia w zakresie obiegu i postępowania z dokumentami niejawnymi.

Lp.	Zagrożenie	Rozwiązania
ZAG-23	Wyniesienie niezabezpieczonego dokumentu (nośnika) poza strefę ochronną	- Procedury zarządzania dokumentami niejawnymi. - Procedury Planu ochrony informacji niejawnych. - Nadzór personelu. - Rejestracja i ewidencjonowanie dokumentów. - Szkolenia personelu. - Kontrole użytkowników. - Zaufani użytkownicy.
ZAG-24	Uszkodzenia i awarie urządzeń systemu (losowe i spowodowane przez ludzi)	- Procedury użytkowania urządzeń. - Procedury serwisowania urządzeń. - Procedury wykonywania kopii zapasowych. - Przeglądy systemów ochrony technicznej. - Procedury postępowania w przypadku awarii.
ZAG-25	Przekazanie dokumentów niejawnych osobom nieuprawnionym	- Procedury zarządzania dokumentami niejawnymi. - Rejestracja i ewidencjonowanie dokumentów. - Szkolenia personelu. - Kontrole użytkowników. - Zaufani użytkownicy.
ZAG-26	Brak odpowiednich cech etyczno-moralnych użytkowników	- Zaufani użytkownicy. - Wdrożenie PBE dotyczących nadawania uprawnień i szkolenia użytkowników. - Kontrole użytkowników.
ZAG-27	Utrata dostępu do pomieszczeń w wyniku utraty klucza lub niesprawności zamka, zagubienia, wyłudzenia, kradzieży kluczy do pomieszczeń służbowych, szaf na dokumenty niejawne itp.	- Procedury zarządzania kluczami. - Procedury wymiany zamków, kluczy i kodów. - Procedury eksploatacji środków ochrony technicznej.

Lp.	Zagrożenie	Rozwiązania
ZAG-28	Błędy i pomyłki administratora systemu	- Procedury kadrowe. - Szkolenia w ABW. - Szkolenia w zakresie bezpieczeństwa informacji.
ZAG-29	Błędy i pomyłki użytkowników systemu	- Szkolenia personelu. - Procedury analizowania i archiwizowania rejestru zdarzeń. - Kontrole użytkowników. - Zaufani użytkownicy.
ZAG-30	Brak procedur gromadzenia i archiwizowania danych oraz wykonywania kopii	- Konfiguracja systemów operacyjnych. - Procedury archiwizowania i tworzenia kopii zapasowych. - Przeglądy dziennika zdarzeń.
ZAG-31	Niewłaściwe działanie oprogramowania urządzenia (systemu)	- Konfiguracja systemów operacyjnych. - Procedury odtwarzania systemu i oprogramowania z kopii zapasowych. - Przeglądy dziennika zdarzeń. - Wykonywanie testów bezpieczeństwa.
ZAG-32	Brak bieżącego monitorowania pracy systemu	- Procedury audytowania bezpieczeństwa. - Procedury analizowania i archiwizowania rejestru zdarzeń. - Procedury wykonywania kopii bezpieczeństwa. - Wykonywanie testów bezpieczeństwa.
ZAG-33	Nieuprawniony dostęp do systemu (zasobów informacyjnych systemu)	- Procedury nadawania uprawnień użytkownikom. - System kontroli dostępu. - System sygnalizacji włamania i napadu. - Audyty bezpieczeństwa.
ZAG-34	Brak certyfikatu elementu systemu	- Akredytacja bezpieczeństwa Systemu. - Kontrole elementów systemu. - Procedury eksploatacji środków ochrony elektromagnetycznej.

Lp.	Zagrożenie	Rozwiązania
ZAG-35	Modyfikacja parametrów instalacyjnych przez osoby nieuprawnione	- Konfiguracja systemów operacyjnych. - Przeglądy dziennika zdarzeń.
ZAG-36	Wprowadzenie do systemu szkodliwego oprogramowania	- Konfiguracja systemów operacyjnych. - Procedury nadawania uprawnień użytkownikom. - Polityka i procedury antywirusowe.
ZAG-37	Nieuprawnione kopiowanie danych na informatycznych nośnikach danych	- Konfiguracja systemów operacyjnych. - Procedury eksportu danych. - Przeglądy dziennika zdarzeń.
ZAG-38	Zmiana niepożądanych parametrów w kodzie źródłowym	- Regularne przeglądy kodu źródłowego w poszukiwaniu niepożądanych zmian. - Wdrożenie procedur kontroli zmian w kodzie. - Weryfikacja autentyczności kodu przed wdrożeniem.
ZAG-39	Zagrożenie wynikające z wprowadzenia dezinformacji i manipulacji informacjami	- Weryfikacja i weryfikacja źródła informacji. - Wdrożenie procedur weryfikacji informacji przed ich użyciem.
ZAG-40	Wyciek informacji w wyniku zaawansowanego ataku phishingowego	- Szkolenia w zakresie rozpoznawania i unikania ataków phishingowych. - Użycie filtrowania wiadomości e-mail i antyspamowych.
ZAG-41	Skomplikowane procedury dostępu do systemu wpływające na wydajność pracy	- Optymalizacja procedur dostępu. - Użycie autoryzacji dwuskładnikowej w celu zwiększenia bezpieczeństwa przy jednoczesnym ułatwieniu dostępu.

Lp.	Zagrożenie	Rozwiązania
ZAG-42	Zagrożenie ze strony zanieczyszczonych nośników danych wpływające na integralność danych	- Skanowanie nośników danych przed ich użyciem. - Wdrożenie procedur zarządzania nośnikami danych.
ZAG-43	Brak procedur zabezpieczających przed włamaniem fizycznym	- Wdrożenie środków bezpieczeństwa fizycznego, takich jak kamery i kontrole dostępu. - Przeprowadzanie okresowych szkoleń dla personelu dotyczących procedur bezpieczeństwa fizycznego.
ZAG-44	Ujawnienie informacji wynikające z wykorzystania podsłuchu	- Zastosowanie zabezpieczeń akustycznych w pomieszczeniach. - Wdrożenie procedur audytu systemów antysłuchowych.
ZAG-45	Wyłudzenie informacji niejawnych za pomocą socjotechnik	- Szkolenia personelu w zakresie rozpoznawania socjotechnik. - Weryfikacja tożsamości przed ujawnieniem poufnych informacji.
ZAG-46	Niewłaściwa kontrola dostępu do dokumentów niejawnych wpływająca na poufność informacji	- Wdrożenie procedur kontroli dostępu i nadzoru dokumentów niejawnych. - Użycie kategorii dostępu w systemach zarządzania dokumentami.
ZAG-47	Ujawnienie informacji wynikające z nie-ostrzeżenia przez zabezpieczenia antywirusowe	- Regularna aktualizacja oprogramowania antywirusowego. - Wdrożenie procedur reagowania na alarmy antywirusowe.

Lp.	Zagrożenie	Rozwiązania
ZAG-48	Błąd ludzki w procesie przetwarzania informacji wpływający na bezpieczeństwo danych	- Szkolenia w zakresie bezpieczeństwa informacji.- Wdrożenie procedur weryfikacji procesów przetwarzania danych.
ZAG-49	Ujawnienie informacji w wyniku wykorzystania exploitów	- Regularna aktualizacja oprogramowania w celu usuwania potencjalnych luk bezpieczeństwa.- Wdrożenie zabezpieczeń przed znanymi exploitami.
ZAG-50	Wykorzystanie słabych haseł przez intruzów wpływających na integralność i poufność informacji	- Wymuszenie na użytkownikach używania silnych haseł.- Wdrożenie autoryzacji dwuskładnikowej.
ZAG-51	Zagrożenie wynikające z braku aktualizacji oprogramowania wpływające na bezpieczeństwo systemu	- Wdrożenie procedur aktualizacji oprogramowania.- Regularna kontrola i stosowanie dostępnych łatek bezpieczeństwa.
ZAG-52	Niedostateczne zabezpieczenia przeciwwłamaniowe	- Wdrożenie systemów detekcji włamań i środków przeciwdziałania. - Monitoring i reagowanie na potencjalne ataki.
ZAG-53	Nieautoryzowane modyfikacje konfiguracji systemu wpływające na integralność i dostęp do systemu	- Ograniczenie uprawnień dostępu do konfiguracji systemu. - Monitoring zmian w konfiguracji.

Lp.	Zagrożenie	Rozwiązania
ZAG-54	Atak na system teleinformatyczny z wykorzystaniem ransomware wpływający na integralność danych	- Regularne tworzenie kopii zapasowych danych.- Wdrożenie procedur odtwarzania systemu po ataku ransomware.
ZAG-55	Ujawnienie informacji na skutek błędów w procesie transmisji danych	- Zastosowanie zabezpieczeń szyfrowania i tunelowania danych w trakcie transmisji. - Szkolenia personelu w zakresie bezpiecznej transmisji danych.
ZAG-56	Nieodpowiednie procedury zarządzania i dystrybucji kluczy kryptograficznych wpływające na bezpieczeństwo systemu	- Wdrożenie procedur zarządzania kluczami kryptograficznymi. - Audyt i kontrola procesów dystrybucji kluczy.
ZAG-57	Nieprawidłowa identyfikacja i uwierzytelnianie użytkowników	- Wdrożenie autoryzacji dwuskładnikowej. - Regularna weryfikacja tożsamości użytkowników.
ZAG-58	Brak mechanizmów audytu bezpieczeństwa i monitorowania systemu	- Wdrożenie narzędzi monitorujących i audytu bezpieczeństwa.- Regularne przeglądy dzienników zdarzeń.
ZAG-59	Nieuprawnione ujawnienie informacji na skutek niewłaściwego zarządzania dokumentami niejawnymi	- Wdrożenie procedur kontroli dostępu do dokumentów niejawnych. - Szkolenia personelu w zakresie zarządzania dokumentami niejawnymi.

Lp.	Zagrożenie	Rozwiązania
ZAG-60	Atak hakerski z wykorzystaniem technik inżynierii społecznej wpływający na bezpieczeństwo systemu	- Szkolenia w zakresie rozpoznawania i unikania ataków inżynierii społecznej. - Użycie filtrów antyspamowych i antyphishingowych.

Tabela 8: Identyfikacja zabezpieczeń

3.8 Szacowanie ryzyka

Szacowanie ryzyka w przykładowym systemie opieramy na metodyce MOROIN. Model ten został opracowany, aby skutecznie oszacować ryzyko z uwzględnieniem atrybutów bezpieczeństwa: poufności, integralności i dostępności informacji. Podejście to pozwala przypisać wartości liczbowe dla skutków utraty każdego z atrybutów, ocenić podatności zasobów oraz wyznaczyć poziom ryzyka, co umożliwia skoncentrowanie działań zabezpieczających na obszarach o najwyższym ryzyku.

Zachowanie poufności danych niejawnych jest podstawą ochrony informacji wrażliwych. W modelu MOROIN każdemu zasobowi przypisywana jest wartość odzwierciedlająca skutki jego utraty, co umożliwia ocenę ryzyka w odniesieniu do klauzul poufności, takich jak „zastrzeżone", „poufne", „tajne" i „ściśle tajne". Dzięki temu można odpowiednio zdefiniować wymagania ochronne dla każdego zasobu.

Kolejną cechą jest integralność, która ma zapewnić, że informacje pozostają nienaruszone i spójne. W modelu MOROIN ocena skutków utraty integralności opiera się na klasyfikacji zasobów według poziomów, które odzwierciedlają skalę zagrożenia wynikającego z ich ewentualnej modyfikacji. Dzięki temu procesowi zasoby krytyczne mogą być zabezpieczone bardziej rygorystycznie, co minimalizuje ryzyko modyfikacji przez osoby nieuprawnione.

Ostatnią cechą jest dostępność, która gwarantuje, że zasoby są w dyspozycji dla uprawnionych użytkowników wtedy, gdy są potrzebne. W MOROIN każde zasoby ocenia się pod kątem ich dostępności, biorąc pod uwagę potencjalny wpływ utraty dostępu na działalność organizacji. Klasyfikacja obejmuje poziomy od niskiego do absolutnego, gdzie najwyższe poziomy oznaczają zasoby o krytycznym znaczeniu, które muszą być dostępne w trybie ciągłym.

Model MOROIN przewiduje ocenę podatności zasobów na różnorodne zagrożenia. Ocena ta uwzględnia czynniki takie jak stopień narażenia na konkretne zagrożenia oraz dostępne środki ochrony. Proces ten pozwala na identyfikację najsłabszych punktów systemu, na które mogą mieć wpływ różne zagrożenia, od fizycznych po cyfrowe.

Analiza ryzyka w modelu MOROIN łączy ocenę skutków utraty każdego atrybutu z poziomem podatności zasobów na zagrożenia. Wynikiem jest klasyfikacja ryzyka dla każdego zasobu, która pozwala wyróżnić obszary o największym znaczeniu dla bezpieczeństwa. Wyniki analizy wskazują poziomy ryzyka, które są następnie interpretowane w celu podjęcia odpowiednich działań ochronnych.

Przykładowe wyniki obliczonego poziomu ryzyka dla wybranego zasobu zostały przedstawione w poniższej w tabeli, gdzie V – Podatność, P – Poufność, I – Integralność, D – Dostępność, RP – Ryzyko utraty poufności, RI – Ryzyko utraty integralności, RD – Ryzyko utraty dostępności:

Zasób	Zagrożenie	V	P	I	D	RP	RI	RD
ZAS-01 Informacje niejawne własne	ZAG-01 Incydent związany z pożarem w firmowej lokalizacji	6	9	8	3	54	48	18
ZAS-01 Informacje niejawne własne	ZAG-02 Zalanie pomieszczenia systemu	5	8	7	5	40	35	25
ZAS-01 Informacje niejawne własne	ZAG-03 Uszkodzenie sprzętu wyładowaniem atmosferycznym	4	7	6	6	28	24	24
ZAS-01 Informacje niejawne własne	ZAG-04 Katastrofa budowlana wpływająca na system	6	9	8	7	54	48	42
ZAS-01 Informacje niejawne własne	ZAG-05 Przerwa w zasilaniu	5	7	6	6	35	30	30
ZAS-01 Informacje niejawne własne	ZAG-06 Awaria zasilania awaryjnego	4	8	7	6	32	28	24
ZAS-01 Informacje niejawne własne	ZAG-07 Próba działalności wywiadowczej	8	10	9	4	80	72	32
ZAS-01 Informacje niejawne własne	ZAG-08 Sabotaż i działania dywersyjne	7	9	8	5	63	56	35
ZAS-01 Informacje niejawne własne	ZAG-09 Infiltracja elektromagnetyczna	6	8	7	4	48	42	24
ZAS-01 Informacje niejawne własne	ZAG-10 Awaria środków ochrony fizycznej	5	7	6	5	35	30	25
ZAS-01 Informacje niejawne własne	ZAG-11 Kradzież urządzenia systemu	6	9	8	5	54	48	30
ZAS-01 Informacje niejawne własne	ZAG-12 Kradzież nośników danych niejawnych	7	10	9	6	70	63	42
ZAS-01 Informacje niejawne własne	ZAG-13 Nieautoryzowane użycie urządzenia	5	7	6	4	35	30	20
ZAS-01 Informacje niejawne własne	ZAG-14 Niewłaściwe kwalifikacje personelu	4	6	5	3	24	20	12
ZAS-01 Informacje niejawne własne	ZAG-15 Rotacja personelu, choroby	3	5	4	3	15	12	9
ZAS-01 Informacje niejawne własne	ZAG-16 Brak procedur ochrony informacji	7	10	9	4	70	63	28

Zasób	Zagrożenie	V	P	I	D	RP	RI	RD
ZAS-01 Informacje niejawne własne	ZAG-17 Brak znajomości procedur	5	7	6	4	35	30	20
ZAS-01 Informacje niejawne własne	ZAG-18 Niewłaściwa eksploatacja urządzenia	6	8	7	5	48	42	30
ZAS-01 Informacje niejawne własne	ZAG-19 Wykorzystanie urządzeń spoza strefy ochronnej	7	9	8	6	63	56	42
ZAS-01 Informacje niejawne własne	ZAG-20 Pozostawienie niezabezpieczonego urządzenia	6	8	7	5	48	42	30
ZAS-01 Informacje niejawne własne	ZAG-21 Pozostawienie niezabezpieczonego dokumentu	7	9	8	6	63	56	42
ZAS-01 Informacje niejawne własne	ZAG-22 Podgląd monitora przez nieuprawnione osoby	6	9	8	4	54	48	24
ZAS-01 Informacje niejawne własne	ZAG-23 Wyprowadzenie dokumentów poza strefę ochronną	7	10	9	5	70	63	35
ZAS-01 Informacje niejawne własne	ZAG-24 Uszkodzenia i awarie urządzeń	5	7	6	5	35	30	25
ZAS-01 Informacje niejawne własne	ZAG-25 Ujawnienie informacji przez osoby nieuprawnione	8	10	9	6	80	72	48
ZAS-01 Informacje niejawne własne	ZAG-26 Brak właściwych cech etyczno-moralnych u użytkowników	5	8	7	4	40	35	20
ZAS-01 Informacje niejawne własne	ZAG-27 Utrata dostępu do pomieszczenia	4	6	5	3	24	20	12
ZAS-01 Informacje niejawne własne	ZAG-28 Błędy administratora systemu	6	7	6	5	42	36	30
ZAS-01 Informacje niejawne własne	ZAG-29 Błędy użytkowników wpływające na integralność danych	7	8	7	4	56	49	28
ZAS-01 Informacje niejawne własne	ZAG-30 Brak procedur gromadzenia i archiwizacji danych	5	9	8	5	45	40	25
ZAS-01 Informacje niejawne własne	ZAG-31 Niewłaściwe działanie oprogramowania	6	7	6	5	42	36	30

Zasób	Zagrożenie	V	P	I	D	RP	RI	RD
ZAS-01 Informacje niejawne własne	ZAG-32 Brak bieżącego monitorowania systemu	7	8	7	4	56	49	28
ZAS-01 Informacje niejawne własne	ZAG-33 Nieuprawniony dostęp do systemu	9	10	9	6	90	81	54
ZAS-01 Informacje niejawne własne	ZAG-34 Brak certyfikatu elementu systemu	5	8	7	4	40	35	20
ZAS-01 Informacje niejawne własne	ZAG-35 Modyfikacja parametrów przez osoby nieuprawnione	6	9	8	5	54	48	30
ZAS-01 Informacje niejawne własne	ZAG-36 Wprowadzenie szkodliwego oprogramowania	8	10	9	6	80	72	48
ZAS-01 Informacje niejawne własne	ZAG-37 Nieuprawnione kopiowanie danych	7	9	8	5	63	56	35
ZAS-01 Informacje niejawne własne	ZAG-38 Zmiana parametrów w kodzie źródłowym	6	8	7	5	48	42	30
ZAS-01 Informacje niejawne własne	ZAG-39 Zagrożenie wynikające z dezinformacji	5	7	6	4	35	30	20
ZAS-01 Informacje niejawne własne	ZAG-40 Wyciek informacji z ataku phishingowego	8	10	9	6	80	72	48
ZAS-01 Informacje niejawne własne	ZAG-41 Skomplikowane procedury dostępu wpływające na wydajność	4	6	5	3	24	20	12
ZAS-01 Informacje niejawne własne	ZAG-42 Zanieczyszczone nośniki danych	6	8	7	5	48	42	30
ZAS-01 Informacje niejawne własne	ZAG-43 Brak procedur zabezpieczających przed włamaniem fizycznym	7	9	8	6	63	56	42
ZAS-01 Informacje niejawne własne	ZAG-44 Ujawnienie informacji przez podsłuch	8	9	8	4	72	64	32
ZAS-01 Informacje niejawne własne	ZAG-45 Wyłudzenie informacji za pomocą socjotechnik	9	10	9	6	90	81	54
ZAS-01 Informacje niejawne własne	ZAG-46 Niewłaściwa kontrola dostępu do dokumentów	7	9	8	5	63	56	35

Zasób	Zagrożenie	V	P	I	D	RP	RI	RD
ZAS-01 Informacje niejawne własne	ZAG-47 Ujawnienie informacji przez błędy w transmisji danych	6	8	7	4	48	42	24
ZAS-01 Informacje niejawne własne	ZAG-48 Błąd ludzki w procesie przetwarzania informacji	7	9	8	5	63	56	35
ZAS-01 Informacje niejawne własne	ZAG-49 Wykorzystanie exploitów	8	10	9	6	80	72	48
ZAS-01 Informacje niejawne własne	ZAG-50 Wykorzystanie słabych haseł przez intruzów	7	9	8	5	63	56	35
ZAS-01 Informacje niejawne własne	ZAG-51 Brak aktualizacji oprogramowania	6	8	7	5	48	42	30
ZAS-01 Informacje niejawne własne	ZAG-52 Niedostateczne zabezpieczenia przeciwwłamaniowe	7	9	8	6	63	56	42
ZAS-01 Informacje niejawne własne	ZAG-53 Nieautoryzowane modyfikacje konfiguracji systemu	6	9	8	5	54	48	30
ZAS-01 Informacje niejawne własne	ZAG-54 Atak ransomware	9	10	9	6	90	81	54
ZAS-01 Informacje niejawne własne	ZAG-55 Ujawnienie informacji przez błędy transmisji danych	7	9	8	4	63	56	28
ZAS-01 Informacje niejawne własne	ZAG-56 Niewłaściwe zarządzanie kluczami kryptograficznymi	8	10	9	5	80	72	40
ZAS-01 Informacje niejawne własne	ZAG-57 Nieprawidłowa identyfikacja użytkowników	7	9	8	6	63	56	42
ZAS-01 Informacje niejawne własne	ZAG-58 Brak audytu bezpieczeństwa	6	8	7	4	48	42	24
ZAS-01 Informacje niejawne własne	ZAG-59 Nieuprawnione ujawnienie informacji	8	10	9	6	80	72	48
ZAS-01 Informacje niejawne własne	ZAG-60 Atak hakerski wykorzystujący inżynierię społeczną							

Tabela 9: Szacowanie ryzyka

Zastosowanie modelu MOROIN umożliwia zarządzanie ryzykiem poprzez skoncentrowanie się na obszarach o najwyższym poziomie zagrożenia. Analiza pozwala na ocenę podatności zasobów i zidentyfikowanie krytycznych zasobów, dla których należy wdrożyć dodatkowe zabezpieczenia. Na przykład, zasoby o najwyższym ryzyku, mogą wymagać wzmocnionej ochrony, aby zapewnić bezpieczeństwo poufnych informacji.

Pamiętać również należy, że wymogiem formalnym jest umieszczanie w raporcie z analizy ryzyka deklaracji: Administratora Systemu, Inspektora Bezpieczeństwa Teleinformatycznego, Pełnomocnika ds. Ochrony Informacji Niejawnych, Kierownika Jednostki Organizacyjnej, że mają świadomość ryzyk związanych z bezpieczeństwem informacji niejawnych przetwarzanych w badanym systemie oraz akceptują przedstawione oceny poziomów ryzyk. Zobowiązują się do pełnienia roli właściciela tych ryzyk zgodnie oraz akceptują ryzyko szczątkowe wynikające z przeprowadzonej analizy. Zobowiązują się również do podjęcia wszelkich działań wynikających z przypisanych mi obowiązków w celu minimalizacji potencjalnych zagrożeń i zapewnienia bezpieczeństwa systemu.

3.9 Ocena ryzyka

W wyniku przeprowadzonej analizy ryzyka, opartej na modelu MOROIN, powstaje hierarchiczna lista potencjalnych zagrożeń dla informacji oraz zasobów chronionych przez system teleinformatyczny. Niezależnie od zastosowanej metody szacowania ryzyka – manualnej lub z użyciem specjalistycznego oprogramowania – lista ta służy identyfikacji zagrożeń najpoważniejszych dla jednostki organizacyjnej, które wymagają priorytetowego ograniczenia. Takie podejście umożliwia odpowiedni dobór środków zabezpieczających, uwzględniający zarówno wymogi ochrony informacji niejawnych przetwarzanych w systemie, jak i efektywność kosztową wdrożonych zabezpieczeń.

Na podstawie tej hierarchicznej listy zagrożeń formułowane są szczególne wymagania dla projektowanego systemu, które zapewnią osiągnięcie zamierzonego poziomu bezpieczeństwa. Stanowią one fundament do opracowania dokumentów, takich jak „Szczególne Wymagania Bezpieczeństwa" oraz „Procedury Bezpiecznej Eksploatacji", niezbędnych dla procesu akredytacji systemu teleinformatycznego.

Proces szacowania ryzyka kończy się sporządzeniem raportu. Raport ten zawiera zespół wymagań bezpieczeństwa systemu, opracowany na podstawie przewidywanych zagrożeń i zidentyfikowanych podatności systemu. Informacje uzyskane podczas analizy ryzyka stanowią istotny zasób w trakcie całego cyklu życia systemu i powinien być archiwizowany na potrzeby przyszłych analiz oraz przeglądów ryzyka.

3.10 Dobieranie środków ochrony

Następnym krokiem w zarządzaniu ryzykiem dla zapewnienia bezpieczeństwa systemu teleinformatycznego jest wybór odpowiednich zabezpieczeń. Ochrona ta może obejmować środki fizyczne, techniczne i organizacyjne, które wzajemnie się uzupełniają i są stosowane w każdym obszarze, gdzie zidentyfikowano ryzyko.

Aby stworzyć odpowiedni zestaw zabezpieczeń, który spełnia wymagania prawne dotyczące ochrony informacji i zapewnia akceptowalny poziom bezpieczeństwa systemu, zespół analizujący ryzyko powinien dokładnie przejrzeć każdy zasób oraz powiązane z nim zagrożenia i podatności systemu. Należy brać pod uwagę zarówno już wdrożone środki ochrony, jak i te planowane do wprowadzenia. Można również przeanalizować poszczególne zagrożenia i słabe punkty systemu, dopasowując do nich odpowiednie środki ochrony.

Ważne jest, by pamiętać, że zagrożenie ma wpływ na bezpieczeństwo tylko wtedy, gdy istnieje słaby punkt, który to zagrożenie może wykorzystać. Podobnie, podatność systemu ma znaczenie jedynie w połączeniu z odpowiadającym jej zagrożeniem.

Tworząc listę zabezpieczeń dla systemu, należy uwzględnić przepisy prawne oraz standardy dotyczące ochrony informacji. Zabezpieczenia mogą spełniać różne funkcje: zmniejszać prawdopodobieństwo wystąpienia zagrożenia, redukować podatności systemu, minimalizować potencjalne straty lub wykrywać przypadki naruszenia poufności, integralności lub dostępności informacji.

Wybór środków ochrony zależy od specyfiki i warunków środowiska, w którym system funkcjonuje. Na przykład, kierownik jednostki może zdecydować się na przeniesienie ryzyka związanego z ochroną fizyczną obiektu na zewnętrzną firmę ochroniarską, ale nadal odpowiada za konsekwencje potencjalnego naruszenia poufności czy integralności informacji.

Ważnym elementem jest także optymalizacja kosztów – należy zrównoważyć wydatki na zabezpieczenia z wymogami prawnymi dotyczącymi ochrony informacji. Przy doborze zabezpieczeń trzeba uwzględnić takie aspekty jak łatwość wdrożenia, skuteczność, etap rozwoju systemu oraz funkcje, które zabezpieczenia mają spełniać.

Proces ten kończy się opracowaniem ostatecznej listy zalecanych zabezpieczeń, uwzględniającej zarówno istniejące, jak i nowe środki ochrony.

3.11 Akceptacja ryzyka szczątkowego

Ryzyko szczątkowe to poziom ryzyka, który pozostaje w systemie teleinformatycznym mimo wdrożenia licznych środków ochrony. Nie da się go całkowicie wyeliminować, ponieważ zawsze istnieją zasoby, których pełne zabezpieczenie byłoby zbyt kosztowne lub trudne do osiągnięcia, zwłaszcza gdy koszt ochrony przekracza wartość samego zasobu. Ryzyko szczątkowe może również wynikać z błędnej oceny zagrożeń lub podatności.

Podczas procesu akceptacji ryzyka szczątkowego przeprowadzana jest ocena skuteczności wdrożonych zabezpieczeń i ich wpływu na zmniejszenie ryzyka. Następnie identyfikuje się pozostałe ryzyko szczątkowe i ocenia jego poziom, przypisując każdemu zasobowi klasyfikację „akceptowalne” lub „nieakceptowalne”.

Przy ocenie skuteczności środków ochrony rozważa się ich wpływ na ryzyko w trzech aspektach:

Eliminacja ryzyka – zastosowanie środków ochrony, które całkowicie niwelują słabe punkty systemu.

Ograniczenie ryzyka utraty – jeśli ryzyko nie może być wyeliminowane, środki ochrony maksymalnie je zmniejszają.

Zmniejszenie skutków – w sytuacji, gdy pełne zapobieganie jest niemożliwe, zabezpieczenia ograniczają ryzyko do poziomu akceptowalnego.

Ryzyko ocenione jako „akceptowalne" oznacza, że organizacja może tolerować potencjalne straty, które mogłyby wyniknąć z jego wystąpienia. Natomiast ryzyko „nieakceptowalne" wymaga wdrożenia dodatkowych zabezpieczeń. Każda decyzja dotycząca akceptacji ryzyka szczątkowego musi być zatwierdzona przez kierownika jednostki organizacyjnej, ponieważ ma ona wpływ na zasoby finansowe i strategiczne jednostki.

W przypadku systemów przetwarzających informacje niejawne, zgodnie z wymogami Ustawy o Ochronie Informacji Niejawnych (UOIN), to kierownik jednostki jest odpowiedzialny za akceptację ryzyka szczątkowego, co podkreśla wagę tej decyzji. Ryzyko szczątkowe wymaga ciągłego monitorowania i okresowej oceny, aby utrzymać je na poziomie akceptowalnym oraz, w razie potrzeby, dostosować zabezpieczenia do zmieniających się warunków i zagrożeń, zapewniając bezpieczeństwo informacji niejawnych przez cały cykl życia systemu.

3.12 Podsumowanie Rozdziału 3

Rozdział ten przedstawia kompleksowe podejście do oceny bezpieczeństwa systemów informacyjnych, ukazując praktyczne zastosowanie modelu MOROIN jako narzędzia w zarządzaniu ryzykiem informacji wrażliwych. Poprzez analizę środowiska bezpieczeństwa przykładowego systemu oraz ocenę zasobów i zagrożeń, dostarczono podstaw do zrozumienia struktury i dynamiki ryzyka bezpieczeństwa.

Każdy podrozdział został skonstruowany, by dostarczać szczegółowych informacji na temat wspierających elementów modelu, takich jak identyfikacja zabezpieczeń, szacowanie i ocena ryzyka, oraz proces doboru środków ochrony. Podkreślono również rolę personelu odpowiedzialnego za bezpieczeństwo, co stanowi ważny aspekt w kontekście implementacji skutecznych procedur bezpieczeństwa.

Założenia wstępne oraz akceptacja ryzyka szczątkowego są uzupełniającymi składnikami omawianego modelu, umożliwiając organizacjom przyjęcie zrównoważonego

podejścia w kontekście nieuchronnych ryzyka związanych z przetwarzaniem informacji. Przedstawione podejście kładzie szczególny nacisk na łączenie aspektów teoretycznych z praktycznymi rozwiązaniami, co wspiera podejmowanie świadomych decyzji w dynamicznie zmieniającym się krajobrazie bezpieczeństwa.

Podsumowując, zasady i strategie wyłaniające się z analizy modelu MOROIN stwarzają możliwość nie tylko efektywnego zarządzania ryzykiem, ale także zachęcają do ciągłego ulepszania i adaptacji procedur bezpieczeństwa. Rozdział ten stanowi fundament do dalszych badań i implementacji innowacyjnych metod zwiększających poziom bezpieczeństwa w środowiskach przetwarzających informacje wrażliwe.

ROZDZIAŁ 4

Utrzymanie zakładanego poziomu bezpieczeństwa

Rozdział ma na celu ukazanie zintegrowanego i wielopłaszczyznowego podejścia do utrzymania i zarządzania bezpieczeństwem systemów teleinformatycznych. Podejście to uwzględnia potrzebę ciągłego doskonalenia strategii ochronnych w oparciu o najlepsze praktyki i nowoczesne metody oceny ryzyka, podkreślając, że wsparcie kierownictwa na wszystkich szczeblach organizacji jest nieodzowne dla sukcesu w tych działaniach.

4.1 Elementy procesu zarządzania ryzykiem

Zarządzanie ryzykiem w systemach teleinformatycznych ma na celu zapewnienie odpowiedniego poziomu bezpieczeństwa, zgodnie z polityką bezpieczeństwa organizacji. Proces ten opiera się na trzech głównych filarach: analizie ryzyka, wdrażaniu zabezpieczeń oraz edukacji pracowników na temat potencjalnych zagrożeń.

Analiza ryzyka polega na ciągłym monitorowaniu możliwych zagrożeń i podatności systemu. Ponieważ zagrożenia mogą się zmieniać, analiza ta powinna być przeprowadzana regularnie, zwłaszcza po wprowadzeniu istotnych zmian, takich jak instalacja nowych aplikacji, sprzętu czy zwiększenie ilości użytkowników. Systematyczne oceny ryzyka pozwalają na szybkie wykrycie nowych zagrożeń i ocenę, czy dotychczasowe środki ochrony są nadal skuteczne.

Zabezpieczenia mają na celu zredukowanie ryzyka poprzez stosowanie odpowiednich środków ochronnych. Obejmują one zarówno zabezpieczenia fizyczne i techniczne, jak i zasady postępowania czy procedury. Istotne jest także zwiększanie świadomości zagrożeń wśród pracowników oraz prowadzenie szkoleń z zakresu bezpieczeństwa. Efektywny system zabezpieczeń chroni nie tylko przed zagrożeniami, ale również zmniejsza ryzyko błędów pracowników poprzez jasne procedury i regularne edukowanie na temat zasad bezpieczeństwa.

Edukacja pracowników w obszarze zagrożeń i zasad bezpieczeństwa jest kluczowa dla skutecznego zarządzania ryzykiem. Regularne szkolenia i aktualizacje procedur pomagają w utrwaleniu wiedzy na temat potencjalnych zagrożeń i właściwych reakcji w trudnych sytuacjach. Dzięki temu pracownicy są lepiej przygotowani do rozpoznawania i zgłaszania ryzykownych sytuacji.

Głównym celem tych działań jest utrzymanie stabilnego bezpieczeństwa systemu, które efektywnie odpowiada na dynamiczne zagrożenia. Regularna ocena ryzyka i aktualizacja zabezpieczeń pozwalają na elastyczne dostosowywanie się do nowych wyzwań i minimalizują potencjalne ryzyko, co jest kluczowe dla stabilności i ciągłości działania systemu teleinformatycznego.

4.2 Ocena skuteczności zabezpieczeń

Ocena skuteczności zabezpieczeń w systemach to proces ciągłego zarządzania ryzykiem podczas ich użytkowania. Obejmuje on planowane oraz regularne przeglądy ryzyka, a także reagowanie na zmiany, incydenty i naruszenia bezpieczeństwa.

Planowane przeglądy ryzyka polegają na ustalaniu częstotliwości i harmonogramu takich działań, z reguły odbywają się one raz do roku. Szczegółowy harmonogram i zasady przeprowadzania przeglądów są określone w dokumencie dotyczącym wymagań bezpieczeństwa danego systemu, przyjętym podczas procesu jego akredytacji.

Dodatkowe analizy ryzyka są konieczne w przypadku rozbudowy, modernizacji systemu lub zmiany w środowisku jego działania. Takie sytuacje mogą wpłynąć na poziom bezpieczeństwa, dlatego istotne jest, aby zidentyfikować nowe zagrożenia, ocenić ryzyko oraz zaktualizować zabezpieczenia.

Reakcja na incydenty to kluczowy element, gdy dochodzi do naruszeń bezpieczeństwa, takich jak utrata danych, ich modyfikacja lub brak dostępu do informacji. W takich przypadkach przeprowadzane są postępowania wyjaśniające. Incydenty te prowadzą do aktualizacji listy ryzyk oraz wprowadzenia nowych zabezpieczeń, aby zapobiec ich powtórzeniu się.

Przegląd procedur bezpiecznej eksploatacji służy regularnej weryfikacji ich pełności i zgodności z polityką bezpieczeństwa informacji oraz obowiązującymi przepisami.

Zarządzanie ryzykiem w trakcie eksploatacji systemu jest kluczowe dla zapewnienia ciągłości i skuteczności działań na rzecz ochrony danych. Dzięki ciągłemu monitorowaniu, analizom, reakcji na zmiany oraz incydentom, a także dostosowywaniu zabezpieczeń, można utrzymać wysoki poziom bezpieczeństwa w dynamicznie zmieniającym się środowisku IT.

4.3 Odporność systemu teleinformatycznego na potencjalne zagrożenia

Odporność systemu teleinformatycznego na potencjalne zagrożenia wiąże się z koniecznością ścisłej kontroli i nadzoru nad jego bezpieczeństwem. Kluczową rolę w tym procesie odgrywa Inspektor Bezpieczeństwa Teleinformatycznego. Jego zadania obejmują kilka kluczowych obszarów.

Pierwszym z nich jest sprawdzenie zgodności systemu z dokumentem Szczególne Wymagania Bezpieczeństwa (SWB). Dokument ten zawiera wytyczne dotyczące bezpieczeństwa i jest podstawą do wdrażania odpowiednich zabezpieczeń. Inspektor powinien kontrolować zgodność zabezpieczeń z tym dokumentem.

Kolejnym ważnym działaniem jest kontrola zgodności z analizą ryzyka. Polega to na sprawdzaniu, czy zaimplementowane środki ochrony odpowiadają tym, które zostały uznane za niezbędne podczas analizy ryzyka. Weryfikacja ta pozwala upewnić się, że stosowane środki skutecznie adresują zidentyfikowane zagrożenia.

Inspektor przeprowadza również ocenę przestrzegania procedur bezpieczeństwa przez użytkowników systemu. Zapewnienie, że wszyscy korzystają z systemu zgodnie z ustalonymi procedurami, jest kluczowe dla utrzymania bezpieczeństwa.

Monitorowanie skuteczności zastosowanych środków ochrony to kolejny aspekt działań Inspektora. Regularnie sprawdza on, jak praktyczne są założone środki ochrony i czy skutecznie minimalizują ryzyko.

Zadaniem Inspektora jest również kontrola zgodności systemu z polityką bezpieczeństwa. Obejmuje to ocenę, czy system i jego zabezpieczenia spełniają wszystkie wymagania określone w tej polityce.

Regularne przeglądy zabezpieczeń, wykonywane zgodnie z ustalonym harmonogramem, oraz dodatkowe kontrole po wprowadzeniu jakichkolwiek zmian w systemie bądź warunkach jego działania, pozwalają na stałe utrzymywanie wysokiego poziomu bezpieczeństwa. Takie kontrole są niezbędne na każdym etapie życia systemu, od jego planowania poprzez rozwój, aż po ewentualne wycofanie z użycia.

Regularne i systematyczne kontrole pozwalają na szybkie reagowanie na zmieniające się zagrożenia i warunki, co jest kluczowe dla zapewnienia odpowiedniego poziomu bezpieczeństwa systemu teleinformatycznego.

4.4 Monitorowanie bezpieczeństwa

Monitorowanie bezpieczeństwa jest kluczowym elementem zarządzania ryzykiem w systemach informacyjnych, niezbędnym do utrzymania ich stabilności. Polega na stałym śledzeniu różnych aspektów systemu, w celu wykrycia nieprawidłowości, nieautoryzowanych działań oraz prób naruszenia bezpieczeństwa. Ważnym elementem tego procesu jest monitorowanie czynników ryzyka zidentyfikowanych podczas analizy ryzyka, co pozwala na bieżące śledzenie ich zmian i wpływu na system. Istotne jest także śledzenie aktywności użytkowników, w tym ich logowań, prób nieudanego logowania oraz dostępu do zasobów. Do tego dochodzi analiza ruchu sieciowego, która umożliwia wykrywanie nieprawidłowości czy prób ataków. Regularna weryfikacja logów systemowych dostarcza informacji o zdarzeniach w systemie oraz aktywności użytkowników. Istotne jest również monitorowanie działania systemów alarmowych, sygnalizujących wszelkie podejrzane sytuacje oraz ocenę skuteczności zabezpieczeń fizycznych i technicznych, takich jak systemy kontroli dostępu czy programy antywirusowe. Regularne przeglądy logów i wyników monitorowania pozwalają na szybkie wykrycie anomalii i odpowiednią reakcję na potencjalne zagrożenia. Ważne jest również posiadanie jasno określonych procedur monitorowania, w tym ustalenie, kto jest odpowiedzialny za ten proces oraz jak będą sporządzane raporty. Monitorowanie bezpieczeństwa stanowi integralny element zarządzania ryzykiem, pozwalając na szybkie adaptacje do zmieniających się zagrożeń.

Zgłaszanie i badanie incydentów bezpieczeństwa są kluczowe dla utrzymania ochrony systemu informatycznego. Ważne jest jasne określenie, co uznaje się za incydent bezpieczeństwa, takie jak próby nieautoryzowanego dostępu, utrata danych czy ataki złośliwego oprogramowania. Opracowanie wzoru raportu na incydent, zawierającego informacje jak data, godzina, opis zdarzenia oraz zaangażowane osoby, jest niezbędne dla skutecznej analizy i reakcji. Kluczowe jest też określenie, które incydenty muszą być zgłaszane oraz w jakim czasie, w zależności od ich znaczenia i wpływu na system. Jasne procedury zgłaszania incydentów, wskazujące osoby odpowiedzialne i preferowane metody kontaktu, zapewniają sprawne działanie całego systemu bezpieczeństwa. Proces badania incydentów powinien obejmować analizę, zbieranie dowodów i identyfikację przyczyn, a także ustalenie potrzebnych zmian w obecnych zabezpieczeniach. Decyzje podjęte po badaniu incydentu mogą prowadzić do wprowadzenia nowych zabezpieczeń czy aktualizacji procedur. Z kolei wyciąganie wniosków z takich zdarzeń, pozwala na uniknięcie powtórzeń i doskonalenie systemów bezpieczeństwa. Ważne jest, by zadbać o poufność i ochronę

danych dotyczących incydentów. Regularne raportowanie przypadków oraz analiza trendów pozwalają na identyfikację wzorców i ulepszenie systemu. Ostatecznie, szkolenia w zakresie procedur zgłaszania i reagowania na incydenty są nieodzowne dla podniesienia świadomości pracowników oraz skuteczności działań ochronnych.

4.5 Utrzymanie aktualnego poziomu wiedzy

Prowadzenie efektywnych szkoleń z zakresu bezpieczeństwa informacji jest kluczowe dla zwiększenia świadomości pracowników i wypracowania odpowiednich nawyków w organizacji. Szkolenia powinny zaczynać się od wyjaśnienia celów i priorytetów polityki bezpieczeństwa organizacji oraz skutków jej naruszenia. Ważne jest, aby każdy pracownik rozumiał, że przestrzeganie jej jest jego obowiązkiem. Kolejnym ważnym elementem są podstawy bezpieczeństwa, które obejmują naukę o najczęstszych zagrożeniach, takich jak ataki hackerskie, phishing czy złośliwe oprogramowanie. Istotne są także zasady korzystania z systemu, które uczulają na znaczenie ochrony poprzez odpowiednie zabezpieczanie hasłami, zamykanie sesji po pracy, regularne aktualizacje oprogramowania i unikanie niebezpiecznych stron internetowych. W szkoleniach powinna znaleźć się również edukacja dotycząca ochrony danych, czyli jak należy je przechowywać, przetwarzać i udostępniać, przypominając, że każdy pracownik ma swoją rolę w zabezpieczaniu informacji. Aspektem, na który należy zwrócić uwagę, jest zarządzanie hasłami, gdzie pracownicy uczą się, jak tworzyć silne i unikalne hasła oraz je bezpiecznie przechowywać i regularnie aktualizować. Szkolenia powinny także pokrywać procedury bezpieczeństwa, w tym sposoby zgłaszania incydentów, zasady uzyskiwania dostępu do kluczowych zasobów oraz poprawne wyłączanie systemu. Zabezpieczenia fizyczne, takie jak ochrona pomieszczeń czy zabezpieczenie sprzętu, muszą być również omawiane z uwagi na ich znaczenie dla ogólnego bezpieczeństwa. Warto organizować praktyczne szkolenia w formie symulacji incydentów, które pozwolą pracownikom zmierzyć się z potencjalnymi zagrożeniami w kontrolowanym środowisku. Dodatkowo, edukacja w zakresie monitorowania działań oraz umiejętność raportowania wszelkich podejrzanych zdarzeń czy incydentów są kluczowe dla szybkiej reakcji. Wiedza pracowników powinna być regularnie aktualizowana, a ich postępy monitorowane, co podkreśla konieczność ciągłego doskonalenia w dziedzinie bezpieczeństwa. Poznanie obowiązujących przepisów prawnych związanych z ochroną danych i informacji w systemach teleinformatycznych powinno być także integralnym elementem szkoleń. Regularne, dynamiczne szkolenia i przypomnienia

pomagają nie tylko umocnić wiedzę pracowników, ale również zmniejszają ryzyko związane z możliwymi incydentami. Programy szkoleniowe muszą być nieustannie aktualizowane, odzwierciedlając zmieniające się technologie, nowe zagrożenia i modyfikacje polityki organizacyjnej.

4.6 Warunki utrzymania wysokiego poziomu bezpieczeństwa

Wprowadzenie procedur bezpiecznej eksploatacji w systemach teleinformatycznych i rozwiązaniach sieciowych jest kluczowe dla ochrony poszczególnych stanowisk oraz ich połączeń. Te procedury powinny koncentrować się na minimalizowaniu podatności systemu poprzez właściwą konfigurację, regularne aktualizacje i stałe monitorowanie aktywności użytkowników. Aby zapewnić ciągłość działania systemu, konieczne jest opracowanie procedur awaryjnego przywracania funkcji. Obejmuje to przygotowanie i przetestowanie scenariuszy odtwarzania usług w przypadku incydentów lub awarii, takich jak odzyskiwanie danych z kopii zapasowych oraz szybkie reagowanie na potencjalne zagrożenia. Nadzór nad wydajnością systemu teleinformatycznego też odgrywa kluczową rolę w utrzymaniu bezpieczeństwa. Zalecane jest regularne monitorowanie obciążenia systemu, wykrywanie wszelkich anomalii i podejrzanej aktywności oraz dostosowywanie zasobów w celu uniknięcia przeciążeń. Regularne testy bezpieczeństwa, które obejmują penetrację systemu, analizę podatności i ocenę zabezpieczeń aplikacji, są niezbędne. Wyniki tych testów służą do wdrażania poprawek i ulepszeń środków ochrony. W przypadku wykrycia incydentów bezpieczeństwa, zaleca się przestrzeganie określonych procedur. Powinny one obejmować raportowanie incydentu, izolację zainfekowanego systemu, przywracanie działania oraz analizę zdarzenia, po której następuje wprowadzenie niezbędnych poprawek. Zarządzanie ryzykiem w systemie teleinformatycznym wymaga ciągłego doskonalenia środków ochrony oraz procedur bezpieczeństwa. W tym celu zaleca się regularne przeglądy, aktualizacje i ulepszanie dokumentacji, jak również wdrażanie nowych technologii zgodnie z bieżącymi wyzwaniami i zagrożeniami. W procesie zarządzania ryzykiem powinny uczestniczyć osoby odpowiedzialne za różne aspekty systemu, takie jak właściciele ryzyk, administratorzy systemu, użytkownicy oraz zespoły odpowiedzialne za bezpieczeństwo. Taka współpraca i wymiana informacji między wszystkimi zainteresowanymi stronami przyczynia się do skuteczniejszego identyfikowania, oceny i zarządzania ryzykiem.

4.7 Podsumowanie Rozdziału 4

Ocena poziomu bezpieczeństwa wraz z wdrożeniem środków ochronnych na różnych etapach funkcjonowania systemu teleinformatycznego umożliwia projektowanie zabezpieczeń, które są ekonomicznie uzasadnione i proporcjonalne do istniejącego ryzyka. Przeprowadzona w sposób właściwy analiza ryzyka pozwala na identyfikację wszystkich potencjalnych zagrożeń i dobór odpowiednich środków ochrony. Choć ryzyk nie da się całkowicie wyeliminować, możliwa jest ich kontrola i redukcja. W organizacji ludzie często stają się źródłem zagrożeń, dlatego odpowiednia edukacja i zwiększanie świadomości są kluczowe dla skutecznego zarządzania ryzykiem. Istotne jest zrozumienie, że to czynniki ludzkie mogą być najsłabszym ogniwem w systemach bezpieczeństwa. Profesjonalna ocena poziomu bezpieczeństwa umożliwia identyfikację realnych, często nieoczywistych zagrożeń i skupienie się na priorytetach. Wartością tej analizy jest uświadomienie, że zagrożenia nie zawsze mają charakter technologiczny, ale mogą również dotyczyć ludzi, procesów oraz sytuacji. Kluczowe dla powodzenia działań związanych z bezpieczeństwem teleinformatycznym jest wsparcie kierownictwa na wszystkich szczeblach organizacji. Brak poparcia może stanowić istotną przeszkodę w skutecznym zarządzaniu ryzykiem. Analiza najlepszych praktyk i metod oceny poziomu bezpieczeństwa stanowi kluczowy element w tworzeniu efektywnej strategii oceny zabezpieczeń systemów teleinformatycznych. Zarządzanie ryzykiem w tych systemach wymaga podejścia holistycznego, które uwzględnia aspekty technologiczne, ludzkie i organizacyjne. Edukacja, monitorowanie oraz ocena ryzyka są podstawowymi elementami tego procesu.

ROZDZIAŁ 5

Ocena porównawcza MOROIN

Celem Rozdziału 5 jest przeprowadzenie oceny porównawczej metodyki MOROIN z innymi podejściami stosowanymi w analizie ryzyka w systemach informacyjnych. Punktem odniesienia są metodyki CRAMM, OCTAVE, NIST SP 800-30 czy ISO/IEC 27005.

Analiza została oparta na dwóch filarach: po pierwsze, na systematycznym porównaniu metodyki MOROIN z wykorzystaniem zestawu atrybutów zaproponowanych przez Pandeya i Mustafę, stanowiących uznane kryteria oceny metod oceny ryzyka. Po drugie, na studiach przypadków dotyczących rzeczywistych i symulowanych systemów teleinformatycznych funkcjonujących w trzech kluczowych trybach bezpieczeństwa: dedykowanym, systemowym i wielopoziomowym.

W ramach każdego z przypadków dokonano weryfikacji operacyjnej skuteczności metodyki MOROIN w środowiskach ochrony informacji niejawnych, przy czym szczególny nacisk położono na zgodność z wymaganiami formalnymi, kompletność procesów dokumentacyjnych, możliwość automatyzacji oraz redukcję błędów decyzyjnych. Rozdział kończy się podsumowaniem wskazującym na przewagi podejścia proponowanego podejścia.

5.1 Ocena metody MOROIN według atrybutów porównawczych Pandeya i Mustafy

Podejście z Rozdziału 3, choć oparte na modelu MOROIN, wykracza poza samą analizę ryzyka – stanowi zintegrowany cykl zarządzania bezpieczeństwem informacji niejawnych, uwzględniający m.in. odpowiedzialność personelu, analizę zasobów, środki ochrony, akceptację ryzyka szczątkowego oraz monitorowanie stanu bezpieczeństwa.

Na podstawie atrybutów porównawczych przedstawionych w pracy autorstwa S.K. Pandey i K. Mustafy[105], przeprowadzono analizę metody MOROIN w kontekście siedmiu kluczowych kryteriów. Porównanie obejmowało takie metody jak COBRA, CORAS,

[105] Pandey, Santosh K., K. Mustafa "A comparative study of risk assessment methodologies for information systems." Bulletin of Electrical Engineering and Informatics 1.2 (2012): 111-122.

CRAMM, OCTAVE, SOMAP. Wyniki jednoznacznie wskazują na pełne spełnienie każdego z nich.

1. Atrybut – Quantification

MOROIN wykorzystuje formalny model matematyczny wyznaczenia poziomu ryzyka. Model operuje na wartościach liczbowych, zapewniając wysoką precyzję i możliwość automatycznej analizy.

2. Atrybut – Integration of Security Attributes

Model osobno analizuje i integruje aspekty poufności (C), integralności (I) oraz dostępności (A) w decyzjach ryzykowych. Wyniki dla poszczególnych cech mają wpływ na dobór zabezpieczeń oraz akceptację ryzyka.

3. Atrybut – Integration of Threats and Vulnerabilities

W strukturze MOROIN zagrożenia i podatności są łączone: podatności wpływają bezpośrednio na ocenę prawdopodobieństwa. Model uwzględnia również istniejące środki ochrony, redukujące skutki lub prawdopodobieństwo.

4. Atrybut – Requirements Phase Perspective

Etap przygotowawczy MOROIN koncentruje się na analizie kontekstu, funkcji systemu, otoczenia organizacyjnego i formalnych wymagań. Proces integruje się z fazą wymagań systemu informatycznego.

5. Atrybut – Accuracy level / Validation

Model został zastosowany w rzeczywistym środowisku ochrony informacji niejawnych, poza modelowym podejściem przedstawionym w rozdziale 3, metoda została zastosowana w rzeczywistym systemie przeznaczonym do przetwarzania informacji wrażliwych. W wyniku przeprowadzenia Analizy Ryzyka zostały wprowadzone odpowiednie zabezpieczenia wynikające ze zidentyfikowanych zagrożeń. Pozwoliło to na opracowanie Szczególnych Wymagań Bezpieczeństwa gdzie określono tryb pracy systemu, jego opis funkcjonalny oraz zabezpieczenia techniczne. W dalszym kroku z Analizy Ryzyka opracowano Procedury Bezpiecznej Eksploatacji, które uzupełniły w sposób organizacyjny zabezpieczenia techniczne. W końcu Analiza Ryzyka na bazie MOROIN pozwoliła na

przeprowadzenie utwardzania wybranego systemu operacyjnego. Całość Projektu podlegała ocenie i zatwierdzeniu dokumentacji Władzy Bezpieczeństwa a w kolejnym kroku przeprowadzenie audytu na zgodność dokumentacji z wdrożonymi zabezpieczeniami.

System uzyskując Świadectwo Akredytacji Bezpieczeństwa Systemu Teleinformatycznego potwierdził skuteczność podejścia MOROIN.

Innym przykładem jest zastosowanie w systemach sanityzacji i filtracji danych w przepływach informacji pomiędzy różnymi poziomami wrażliwości informacji w Zautomatyzowanych Systemach Dowodzenia.

6. Atrybut – Standard Compliance

MOROIN jest oparty na wymaganiach zawartych w ISO/IEC 27001, ITSEC, Common Criteria oraz narodowymi przepisami ochrony informacji niejawnych. Posiada strukturę zgodną z wymaganiami audytowalności.

7. Atrybut – Supporting Tools

Model został zaprojektowany z myślą o wykorzystaniu narzędzi wspierających: arkuszy kalkulacyjnych, aplikacji wspierających podjęcie decyzję oraz systemów typu SIEM. Dzięki temu możliwa jest automatyzacja procesu oceny poziomu bezpieczeństwa.

Podsumowując, model MOROIN spełnia wszystkie atrybuty określone przez Pandeya i Mustafę, przewyższając w tym zakresie inne analizowane metody oceny poziomu bezpieczeństwa.

5.2 Eksperyment numer 01 – system rzeczywisty w trybie dedykowanym

W ramach realizacji projektu zabezpieczenia systemu przeznaczonego do przetwarzania informacji niejawnych w **trybie bezpieczeństwa dedykowanym**, przeprowadzono analizę możliwości zastosowania różnych metodyk oceny ryzyka i przygotowania systemu do akredytacji bezpieczeństwa. Celem było wyłonienie najbardziej efektywnego podejścia – zarówno pod względem merytorycznym, jak i operacyjnym.

Kontekst i charakterystyka trybu dedykowanego

W trybie dedykowanym system teleinformatyczny działa w środowisku o ściśle kontrolowanej i jednorodnej klasyfikacji dostępu. W tym modelu:

- wszyscy użytkownicy posiadają poświadczenia bezpieczeństwa (lub upoważnienia) co najmniej równe klauzuli informacji przetwarzanych w systemie,
- wszyscy użytkownicy mają dostęp do wszystkich informacji przechowywanych lub przetwarzanych przez system,
- środowisko pracy systemu jest zazwyczaj wyizolowane fizycznie i logicznie od innych sieci i systemów.

Tryb dedykowany cechuje się najniższym stopniem złożoności formalnej, jednak nadal wymaga:

- jednoznacznego potwierdzenia poziomu uprawnień wszystkich użytkowników,
- formalnego ograniczenia fizycznego dostępu do komponentów systemu (pomieszczenia, terminale, sieci),
- zgodności z procedurami ochrony fizycznej i osobowej dla danego poziomu klasyfikacji.

Zastosowanie metodyki MOROIN

Metodyka MOROIN (Model Oceny Ryzyka Ochrony Informacji Niejawnych) została wdrożona w pełnym zakresie w ramach przygotowania systemu do akredytacji, gdzie wykonano:

- kompleksową **analizę ryzyka** uwzględniającą scenariusze zagrożeń,
- dobór środków technicznych i organizacyjnych zabezpieczeń,
- opracowanie dokumentów Szczególnych Wymagań Bezpieczeństwa (SWB) oraz Procedur Bezpiecznej Eksploatacji (PBE),
- proces **utwardzania** środowiska operacyjnego,
- przygotowanie dokumentacji zgodnej z wymaganiami Władzy Bezpieczeństwa.

W wyniku przeprowadzonego audytu oraz pozytywnej oceny kompletności dokumentacji, system uzyskał zgodę na pracę w okresie 5 lat. Cały proces od analizy do zatwierdzenia dokumentacji trwał 21 dni roboczych, a audyt nie wykazał błędów formalnych.

Próba zastosowania innych metodyk

Na etapie przygotowawczym rozważano również możliwość zastosowania trzech alternatywnych metodyk: NIST SP 800-30, ISO/IEC 27005 oraz OCTAVE. Każda z nich została ostatecznie odrzucona po przeprowadzeniu analizy ich zgodności z wymaganiami formalnymi, poziomu dopasowania do kontekstu krajowego oraz stopnia wsparcia dla procesu przygotowania do akredytacji.

Metodyka NIST SP 800-30 oferowała solidne podstawy oceny ryzyka, jednak nie uwzględniała krajowej klasyfikacji systemów oraz nie zawierała struktury dokumentacyjnej zgodnej z wymaganiami. Próba jej zastosowania wiązałaby się z koniecznością dodatkowej adaptacji, co oznaczałoby wydłużenie procesu o co najmniej 10–15 dni roboczych oraz zwiększenie ryzyka błędów formalnych.

W przypadku ISO/IEC 27005, mimo międzynarodowego uznania, problemem okazała się niezgodność formatu i zakresu analiz z wymaganiami dla systemów niejawnych. Brak powiązania z procesem utwardzania oraz konieczność tłumaczenia modeli zagrożeń na krajowe struktury organizacyjno-techniczne uniemożliwiły jej skuteczne wykorzystanie w ramach analizowanego projektu.

Metodyka OCTAVE, skoncentrowana głównie na analizie zagrożeń z poziomu organizacyjnego i identyfikacji aktywów, nie umożliwiała precyzyjnego odwzorowania architektury technicznej systemu ani przygotowania dokumentacji formalnej wymaganej na potrzeby akredytacji. Ze względu na te ograniczenia została odrzucona już na etapie projektowym.

Wnioski

Na podstawie analizy przypadku rzeczywistego systemu teleinformatycznego wykazano, że metodyka MOROIN jako jedyna spełniła wszystkie kluczowe kryteria formalne, techniczne i organizacyjne wymagane w procesie uzyskania akredytacji bezpieczeństwa. Jej zastosowanie pozwoliło na kompletne przygotowanie systemu do przetwarzania informacji niejawnych systemu pracującego w dedykowanym trybie bezpieczeństwa, co zostało **potwierdzone poprzez pozytywny wynik oceny akredytacyjnej.**

Pozostałe metodyki – mimo swojego uznania i skuteczności w środowiskach cywilnych – nie zapewniały odpowiedniego poziomu kompatybilności z krajowymi wymaganiami prawnymi i operacyjnymi.

5.3 Eksperyment numer 02 – system rzeczywisty w trybie systemowym

Kontekst i charakterystyka trybu systemowego

W trybie systemowym system teleinformatyczny umożliwia:

- dostęp użytkownikom do tylko tych informacji, które zostały im przypisane na podstawie roli lub funkcji,
- wymagane jest posiadanie poświadczeń (lub upoważnień) co najmniej równych klauzuli systemu jako całości (najwyższej przetwarzanej w systemie),
- system operacyjny musi egzekwować kontrolę logiczną dostępu, bazując na przypisaniach ról, obiektów i praw dostępu (np. mechanizmy RBAC, MAC).

Tryb systemowy jest najczęściej stosowany w praktyce i wymaga:

- wyraźnego rozdzielenia ról i przydziału uprawnień na poziomie systemowym i aplikacyjnym,
- stosowania polityk segmentacji danych i przestrzeni logicznych użytkowników,
- jednoznacznego przyporządkowania informacji do użytkowników i/lub ról funkcjonalnych.

Zastosowanie metodyki MOROIN

Metodyka MOROIN podobnie jak w Eksperymencie numer 01 została wdrożona w pełnym zakresie w ramach przygotowania systemu do akredytacji. W jej ramach wykonano:

- kompleksową **analizę ryzyka** uwzględniającą scenariusze zagrożeń,
- dobór środków technicznych i organizacyjnych zabezpieczeń,
- opracowanie dokumentów Szczególnych Wymagań Bezpieczeństwa (SWB) oraz Procedur Bezpiecznej Eksploatacji (PBE),
- proces **utwardzania** środowiska operacyjnego,
- przygotowanie dokumentacji zgodnej z wymaganiami Władzy Bezpieczeństwa.

W wyniku przeprowadzonego audytu oraz pozytywnej oceny kompletności dokumentacji, system uzyskał zgodę na pracę w okresie 5 lat. Cały proces od analizy do

zatwierdzenia dokumentacji trwał 27 dni roboczych, a audyt nie wykazał błędów formalnych.

Wnioski

Na podstawie analizy przypadku rzeczywistego systemu teleinformatycznego wykazano, że metodyka MOROIN dla systemu pracującego w trybie systemowym bezpieczeństwa również spełniła wszystkie kryteria formalne, techniczne i organizacyjne wymagane w procesie uzyskania akredytacji bezpieczeństwa. Jej zastosowanie pozwoliło na kompletne przygotowanie systemu do przetwarzania informacji niejawnych systemu pracującego w systemowym trybie bezpieczeństwa, co zostało **potwierdzone poprzez pozytywny wynik audytu akredytacyjnego oraz uzyskanie Świadectwa Bezpieczeństwa Teleinformatycznego.**

5.4 Eksperyment numer 03 – system symulowany w trybie wielopoziomowym

Kolejnym przypadkiem zastosowania metodyki jest jej wykorzystanie w systemach[106] sanityzacji i filtracji danych w środowiskach wymiany informacji pomiędzy domenami o różnych poziomach klasyfikacji w Zautomatyzowanych Systemach Dowodzenia[107].

Kontekst i charakterystyka trybu wielopoziomowego

W trybie wielopoziomowym system teleinformatyczny umożliwia:

- dostęp użytkownikom posiadającym poświadczenia bezpieczeństwa o klauzuli niższej niż system,

- rozgraniczenie dostępu fizycznego do informacji na podstawie poświadczeń użytkownika i klasyfikacji informacji,

- współistnienie danych różnych klauzul przy zachowaniu ich rozdzielności i kontroli przepływu.

Tryb ten niesie największe wymagania techniczne i proceduralne, w tym:

---

[106] Kacprowicz D., „Sanityzacja informacji w bezpilotowych systemach ewakuacji medycznej w kontekście kształtowania świadomości sytuacyjnej pola walki” w Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne, nr 2, 2024, s. 18-21.

[107] Kacprowicz, D., „Interoperacyjność bezpilotowego systemu ewakuacji medycznej w kontekście standardów NATO.” Elektronika: konstrukcje, technologie, zastosowania 65 (2024).

- sanityzację informacji przy deklasyfikacji (np. maskowanie, anonimizacja),

- egzekwowanie techniczne polityki dostępu do informacji zgodnie z zasadą wiedzy uzasadnionej.

Formalny opis eksperymentu – walidacja podejścia MOROIN w trybie wielopoziomowym.

Celem eksperymentu jest potwierdzenie tezy pomocniczej pracy:

„Modelowanie i analiza formalna złożonych metod oceny bezpieczeństwa systemów dostarcza narzędzi do efektywnego wyznaczania poziomu ryzyk w zakresie ochrony informacji niejawnych."

Eksperyment miał wykazać, że modelowanie ryzyka za pomocą formalnej funkcji obliczeniowej (jak w MOROIN) umożliwia:

- precyzyjne i jednoznaczne wykrycie ryzyka deklasyfikacji,

- automatyczne podejmowanie decyzji wsparte danymi wejściowymi,

- ograniczenie subiektywności oraz skrócenie czasu decyzji.

Projekt eksperymentu:

Rodzaj eksperymentu obejmuje symulację studium przypadku z zastosowaniem rzeczywistych parametrów funkcjonowania systemu informacyjnego w trybie bezpieczeństwa wielopoziomowym, przetwarzającego dane: Ściśle Tajne, Tajne, Poufne i Zastrzeżone. Scenariusz zakłada kontrolowaną deklasyfikację informacji z poziomu wyższego do niższego z użyciem bramy międzysystemowej i algorytmu decyzji ryzykowej.

Dla każdej wiadomości określono:

- poziom początkowy i docelowy klasyfikacji,

- zastosowano model MOROIN do obliczenia poziomu ryzyka – R,

- w przypadku przekroczenia progu R = 20 (wysokie ryzyko) zastosowano reguły sanityzacji danych: maskowanie, anonimizację lub modyfikację współrzędnych (wprowadzenie dezinformacji).

Dane obejmowały 30 wiadomości zawierających dane operacyjne m.in: lokalizacje, stan zasobów, ID urządzeń, czas operacji. Parametry ryzyka (Prawdopodobieństwo, Skutek) zostały określone w oparciu o kontekst taktyczny i politykę bezpieczeństwa systemu.

Wyniki i obserwacje:

W każdym przypadku system automatycznie oszacował ryzyko i – zależnie od wartości – dokonał klasyfikacji jako dopuszczalne lub wymagające sanityzacji. Dla wiadomości o wysokim ryzyku system skutecznie uruchomił mechanizmy sanityzacji, ograniczając możliwość nieautoryzowanego ujawnienia danych.

Zaobserwowano również znaczącą redukcję czasu podejmowania decyzji, wysoką powtarzalność klasyfikacji oraz pełną zgodność ze zdefiniowaną polityką bezpieczeństwa informacji.

Wnioski:

Eksperyment potwierdził, że formalne modelowanie ryzyka w systemach przetwarzających informacje niejawne – w szczególności w trybie wielopoziomowym – pozwala na skuteczne, precyzyjne i zautomatyzowane wyznaczanie poziomu ryzyk. Umożliwia to podjęcie odpowiednich działań zabezpieczających, takich jak sanityzacja danych lub blokada transmisji.

Dzięki zastosowaniu modelu MOROIN:

- decyzje były mierzalne i oparte na wartościach liczbowych,
- mechanizm podejmowania decyzji był powtarzalny i wolny od subiektywności,
- ryzyko błędu ludzkiego zostało istotnie zredukowane.

W konsekwencji, teza pomocnicza rozprawy została jednoznacznie potwierdzona – formalne podejście modelowania ryzyka dostarcza narzędzia do zarządzania ryzykiem w środowiskach informacji niejawnych.

5.5 Podsumowanie Rozdziału 5

Przeprowadzona ocena porównawcza wykazała, że metodyka MOROIN spełnia wszystkie atrybuty skutecznej metody oceny ryzyka, a jej wartość została dodatkowo potwierdzona w praktyce – systemy zaprojektowane na jej podstawie przeszły pozytywnie audyty akredytacyjne przeprowadzane przez niezależne jednostki nadzoru bezpieczeństwa teleinformatycznego. **Wynik ten stanowi bezpośredni dowód, że podejście to jest merytorycznie co najmniej równoznaczne z uznanymi metodykami**

międzynarodowymi, a w kontekście krajowym – bardziej dostosowane do specyfiki formalnej i technicznej ochrony informacji niejawnych.

Dzięki zastosowaniu formalnego modelowania opartego na liczbowej ocenie zagrożeń, podatności oraz skutków, MOROIN umożliwia precyzyjne wyznaczanie poziomu ryzyk oraz automatyzację decyzji związanych z doborem zabezpieczeń, sanityzacją danych oraz zarządzaniem ryzykiem szczątkowym. **Zastosowanie metodyki we wszystkich trzech trybach bezpieczeństwa – dedykowanym, systemowym i wielopoziomowym – wykazało jej pełną zdolność adaptacji do specyfiki operacyjnej i wymogów akredytacyjnych.**

W efekcie, Rozdział 5 jednoznacznie potwierdza, że MOROIN stanowi kompletne, mierzalne i praktycznie zweryfikowane narzędzie do przygotowania systemów teleinformatycznych do przetwarzania informacji niejawnych. Zgromadzone dowody empiryczne i formalne potwierdzają zasadność tezy pomocniczej rozprawy, wskazując na wyższość modelowania formalnego jako podejścia inżynierskiego w dziedzinie oceny ryzyka i bezpieczeństwa informacji.

PODSUMOWANIE

Rozprawa miała na celu zidentyfikowanie i rozwiązanie problemu zbyt dużej złożoności istniejących metod oceny bezpieczeństwa systemów teleinformatycznych przetwarzających informacje niejawne. W punkcie wyjścia zauważono że, zgodność z obowiązującymi normami i standardami nie zawsze przekłada się na rzeczywiste bezpieczeństwo systemu – szczególnie gdy metody oceny są zbyt skomplikowane i trudne do konsekwentnego wdrożenia w praktyce.

Dla lepszego uchwycenia logicznego ciągu badań, całość rozprawy można przedstawić w następujących etapach:

1. **Zidentyfikowano problem badawczy** polegający na nadmiernej złożoności istniejących metod oceny bezpieczeństwa systemów teleinformatycznych, co może prowadzić do błędów i obniżenia rzeczywistego poziomu ochrony informacji niejawnych. *(Wstęp; Rozdział 1, 2.9)*
2. **Następnie postawiono główną tezę oraz tezę pomocniczą,** zakładające możliwość opracowania mniej złożonego narzędzia ale jednocześnie zapewniającego wysoki poziom bezpieczeństwa. (Wstęp; Rozdział 2.10–2.11)
3. **Dokonano przeglądu aktualnych metod** stosowanych w ocenie ryzyka (ISO/IEC 27005, NIST SP 800-30, CRAMM, OCTAVE itd.), ze szczególnym uwzględnieniem ich ograniczeń w kontekście praktycznego zastosowania i zgodności z realiami systemów przetwarzających informacje niejawne. *(Rozdział 2.10, 2.12; Rozdział 5.1)*
4. **Przeprowadzono badania jakościowe** z interesariuszami odpowiedzialnymi za ochronę informacji niejawnych, identyfikując rzeczywiste potrzeby, problemy oraz oczekiwania wobec narzędzi do oceny bezpieczeństwa. *(Rozdział 2.8)*
5. **Opracowane narzędzie zostało poddane weryfikacji eksperymentalnej** w środowiskach rzeczywistych (systemy pracujące w trybach dedykowanych oraz systemowych) oraz symulowanych (systemy pracujące w trybach wielopoziomowych). Badania objęły potwierdzenie zgodności z wymaganiami, możliwość automatyzacji oraz skalowalność rozwiązania.

Wyniki eksperymentów potwierdziły pod względem merytorycznym poprawność zaproponowanego modelu w warunkach rzeczywistych. *(Rozdział 3; Rozdział 5.2–5.4)*

6. **Dokonano porównania z innymi metodami**, wykorzystując podejście Pandeya i Mustafy oraz zestawiając proponowane narzędzie z istniejącymi podejściami pod względem złożoności, zgodności z normami, prostoty interpretacji i możliwości automatyzacji. *(Rozdział 5.1, 5.5)*
7. **Sformułowano końcowe wnioski**, w których pokazano, że proponowane narzędzie spełnia wymagania formalne i praktyczne, oferując realne wsparcie dla procesów bezpieczeństwa systemów teleinformatycznych w środowiskach wysokiego ryzyka. *(Podsumowanie)*.

W ramach badań zastosowano wiele narzędzi i metod charakterystycznych dla dyscypliny informatyka techniczna i telekomunikacja, w tym:

- **zaprojektowanie formalnego modelu ryzyka**, zbudowanego w oparciu o techniczne podejście do strukturalnej analizy systemów informacyjnych,
- **eksperymenty systemowe** (systemy teleinformatyczne pracujące w trybach dedykowanym, systemowym i wielopoziomowym), które stanowią element klasycznej metodologii badań,
- **analizę porównawczą zaprojektowanego narzędzia**, która pozwoliła umieścić rozwiązanie w szerszym kontekście nauk o bezpieczeństwie teleinformatycznym,
- **badania jakościowe z wykorzystaniem wywiadów pogłębionych**, ukierunkowane na interesariuszy odpowiedzialnych za ochronę informacji niejawnych, co odpowiada kierunkowi badań opisanemu przez Hong i Furnella, wykazujących wpływ organizacyjnej formalizacji na przestrzeganie polityk bezpieczeństwa informacji.

Na podstawie wyników przeprowadzonych badań oraz eksperymentalnej weryfikacji w środowisku operacyjnym wykazano, że opisane podejście z wykorzystaniem modelu MOROIN:

1. Redukuje poziom złożoności analizy przy jednoczesnym zachowaniu spójności z normami takimi jak ISO/IEC 27001 i ISO/IEC 15408,
2. Pozwala na praktyczne zastosowanie do oceny przepływów informacji zarówno z niższej do wyższej klasy tajności, jak i odwrotnie – co stanowi nowatorskie podejście do zarządzania bezpieczeństwem w systemach pracujących w trybach bezpieczeństwa wielopoziomowych,
3. Umożliwia automatyzację procesu oceny ryzyka poprzez sformalizowaną macierz zasobów, zagrożeń i podatności – zgodnie z aktualnymi trendami opisanymi m.in. przez Taherdoosta w przeglądzie ram cyberbezpieczeństwa i standardów informacji[108].
4. **Osiągnięto istotny postęp w kierunku wspomagania procesu decyzyjnego w zakresie deklasyfikacji informacji. Możliwość przypisania poziomu ryzyka do konkretnych depesz lub porcji danych może stanowić realne wsparcie dla operatora odpowiedzialnego za klasyfikację informacji i przypisanie jej do odpowiedniego odbiorcy lub zasobu (np. zasubskrybowanego OIG'a). Wynik ten otwiera nowy obszar badań, w którym potencjalnie możliwe będzie przejście od subiektywnej oceny wrażliwości informacji do jej obiektywnego, ilościowego wartościowania. Tym samym, decyzje dotyczące zmiany poziomu wrażliwości danych mogłyby być podejmowane na podstawie mierzalnych kryteriów, co zwiększyłoby transparentność i powtarzalność procesu decyzyjnego.**

Dzięki połączeniu podejść ilościowych i jakościowych, a także ich osadzeniu w praktyce systemowej, zaproponowany model odpowiada na dynamiczne potrzeby współczesnych systemów ochrony informacji i wpisuje się w rozwój **technicznych metod inżynierii systemów teleinformatycznych**. Model może stanowić podstawę dalszych badań naukowych oraz wdrożeń w sektorach wymagających wysokiego

[108] Taherdoost, Hamed. "Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview." *Electronics* 11.14 (2022): 2181.

poziomu ochrony informacji – zarówno w administracji publicznej, jak i w środowiskach przemysłowych.

Praca dostarcza odpowiedzi na pytania badawcze:

W jaki sposób modelowanie formalne może wspierać proces oceny ryzyka w ochronie informacji niejawnych? Modelowanie formalne w ocenie ryzyka informacji niejawnych, jak wskazuje rozprawa, umożliwia przejrzyste i zautomatyzowane podejście do analizy ryzyka, co wpływa na precyzyjniejsze określenie poziomu ryzyka. Zastosowanie formalnych modeli, takich jak MOROIN, pozwala zredukować złożoność procesu i zmniejszyć prawdopodobieństwo błędów wynikających z manualnej oceny. Modele formalne dostarczają miar oraz narzędzi do systematycznego analizowania zagrożeń i podatności, co wspiera skuteczne podejmowanie decyzji dotyczących ochrony danych.

Jak efektywnie zintegrować różne standardy certyfikacyjne i dobre praktyki w procesie oceny bezpieczeństwa systemów teleinformatycznych? W pracy podkreślono, że integracja różnych standardów, takich jak ISO 15408 (Common Criteria), ISO 27001, czy NIST SP 800-53, może być wspierana przez wspólną platformę odniesienia. Wykorzystanie modeli oceny ryzyka pozwala na porównywanie różnych wymagań i ich adaptację do specyfiki systemów. Standaryzacja i wypracowanie procedur w oparciu o mieszane podejścia ilościowe i jakościowe pomagają zharmonizować wymagania certyfikacyjne i dobre praktyki.

Jakie są relacje między metodami ilościowymi a jakościowymi w ocenie bezpieczeństwa i które z nich są bardziej adekwatne w różnych scenariuszach? Metody ilościowe oferują precyzyjne miary ryzyka i są przydatne w analizach, gdzie potrzebna jest ścisła ocena liczbowych parametrów. Z kolei metody jakościowe pomagają uwzględniać kontekst i subiektywne aspekty ryzyka, co jest ważne w bardziej złożonych i dynamicznych środowiskach. W pracy wskazano, że połączenie obu metod (metody mieszane) pozwala na uzyskanie kompleksowej oceny.

Jak wykorzystać metody mieszane do uzyskania bardziej kompleksowej oceny bezpieczeństwa systemów teleinformatycznych i jakie korzyści wynikają z połączenia podejść ilościowych i jakościowych? Połączenie metod ilościowych i jakościowych umożliwia nie tylko uzyskanie dokładnych wyników, ale również uwzględnienie kontekstu operacyjnego i specyficznych uwarunkowań organizacyjnych. Modele mieszane, jak wskazano w pracy, oferują elastyczność i głębszą analizę dzięki wykorzystaniu najlepszych

cech obu podejść. Korzyści obejmują większą adaptacyjność do zmieniających się zagrożeń oraz bardziej zrównoważone decyzje.

Jak oceniać systemy teleinformatyczne w dynamicznym środowisku, biorąc pod uwagę ciągłe zmiany w zagrożeniach cybernetycznych? W pracy wskazano, że skuteczna ocena systemów w zmiennym środowisku wymaga implementacji mechanizmów obejmujących regularne audyty i aktualizację środków ochrony. Modele formalne umożliwiają szybsze dostosowanie się do nowych zagrożeń dzięki możliwości zautomatyzowania procesów, które są łatwiejsze do aktualizacji.

Jak uwzględnić specyficzne wymagania i kontekst organizacyjny w procesie oceny bezpieczeństwa, zważywszy na różnice między sektorami przemysłowymi bądź branżami? Uwzględnienie specyfiki organizacyjnej w ocenie bezpieczeństwa można osiągnąć poprzez adaptację modelu oceny ryzyka do potrzeb danej branży i specyficznych zagrożeń, na jakie jest narażona. W pracy opisano, jak analiza wymagań i kontekstu pomaga dostosować środki ochrony do poziomu ryzyka i celów strategicznych organizacji.

Wyniki przeprowadzonych badań wskazują, że zaproponowane narzędzie, wykorzystujące formalny model oceny ryzyka, może być użyteczne jako alternatywa dla tradycyjnych, złożonych metod. Może ono odpowiadać na potrzeby organizacji, które – przy zachowaniu wysokiego poziomu bezpieczeństwa – poszukują rozwiązań operacyjnych i łatwiejszych do utrzymania. Proponowane podejście umożliwia ograniczenie ryzyka błędów wynikających z nadmiernej złożoności procesów oceny, a jednocześnie pozwala na zachowanie zgodności z obowiązującymi standardami, takimi jak ISO/IEC 27005.

W badaniach zwrócono uwagę na znaczenie podejścia mieszanego – łączącego techniki ilościowe i jakościowe – które może przyczynić się do pełniejszego obrazu poziomu bezpieczeństwa. Analizy ilościowe pozwalają na określenie parametrów ryzyka, natomiast komponent jakościowy umożliwia uwzględnienie specyfiki środowisk operacyjnych. Opinie interesariuszy uzyskane w toku badań sugerują, że uproszczone i elastyczne narzędzia mogą być preferowane w praktyce ze względu na łatwość implementacji i możliwość dostosowania do różnych warunków organizacyjnych.

Zaprojektowane narzędzie wykorzystujące model formalny zostało przetestowane w rzeczywistych warunkach systemowych, w tym w środowiskach objętych formalnym procesem akredytacyjnym. Narzędzie zostało przyjęte przez użytkowników technicznych, m.in. administratorów i inspektorów bezpieczeństwa w strukturach wojskowych i administracyjnych. Przykład zastosowania modelu w analizie systemu wsparcia ewakuacji medycznej z wykorzystaniem bezzałogowych statków powietrznych pokazuje możliwość wykorzystania tej metodyki również w systemach o wysokiej złożoności i znaczeniu operacyjnym.

Zaproponowane rozwiązanie może być rozpatrywane jako wkład w rozwój podejść do zarządzania ryzykiem w systemach teleinformatycznych, zwłaszcza w kontekście informacji niejawnych.

Badania miały charakter eksperymentalny i porównawczy. W pracy podkreślono również znaczenie ciągłego monitorowania ryzyka oraz dostosowywania stosowanych narzędzi do zmieniającego się krajobrazu zagrożeń.

Przedstawione wyniki mogą znaleźć zastosowanie w sektorze publicznym i przemysłowym, w szczególności w organizacjach przetwarzających dane wrażliwe.

Rekomenduje się dalsze badania, których celem byłaby pogłębiona walidacja proponowanego rozwiązania w różnych środowiskach i branżach, a także analiza jego potencjału w zakresie automatyzacji oraz integracji z istniejącymi systemami zarządzania bezpieczeństwem informacji.

Literatura

[1] Dumitru, I.-A. (2022). Classification of Information. International Journal of Information Security and Cybercrime, 11(1), 15–24. ijisc.com

[2] Farhadighalati, Nastaran, et al. "A Systematic Review of Access Control Models: Background, Existing Research, and Challenges." IEEE Access (2025).

[3] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2023 r. poz. 756, 1030).

[4] K. Mordaszewski, D. Laskowski, Prawne aspekty ochrony informacji. Wybrane zagadnienia, w „Nowe Techniki badań kryminalistycznych a bezpieczeństwo informacji, red. B. Hołyst, J. Pomykała, P. Potejko. PWN. 2014, s. 23.

[5] Skrzypek, E. "Kapitał intelektualny jako czynnik stymulujący rozwój przedsiębiorstwa,[w:] S. Partycki (red.)." Strategia rozwoju społecznej gospodarki rynkowej w Polsce (2002), s. 35.

[6] R. J. Sutton, Bezpieczeństwo telekomunikacji Praktyka i Zarządzanie, wyd. WKŁ. 2004, s. 17.

[7] Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego

[8] Shannon, Claude E. "A mathematical theory of communication." The Bell system technical journal 27.3 (1948): 379-423.

[9] B. Hołyst, J. Pomykała, Cyberprzestępczość i kryptograficzna ochrona informacji, [w:] Metody biometryczne i kryptograficzne w zintegrowanych systemach bezpieczeństwa, red. B. Hołyst, J. Pomykała, wyd. WSM. 2021, str. 63.

[10] T. Polaczek, Audyt bezpieczeństwa informacji, Helion, 2014.

[11] B. Hołyst, J. Pomykała, Cyberprzestępczość i kryptograficzna ochrona informacji, [w:] Metody biometryczne i kryptograficzne w zintegrowanych systemach bezpieczeństwa, red. B. Hołyst, J. Pomykała, wyd. WSM. 2021, s. 54-55.

[12] B. Hołyst, Kryminalistyka, wyd. Wolters Kluwer, s. 1350-1359, Warszawa, 2023.

[13] Hong, Yuxiang, and Steven Furnell. "Motivating information security policy compliance: Insights from perceived organizational formalization." Journal of Computer Information Systems 62.1 (2022): 19-28.

[14] Meghanandha, Umesha Naik. "A Comparative Review of Metadata, Communication, Content, and Digital Preservation Standards in Modern Libraries." American Journal of Information Science and Technology, vol. 9, no. 1, Feb. 2025, pp. 24–33. Science Publishing Group, DOI:10.11648/j.ajist.20250901.13.

[15] Rozporządzenie rady ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych

[16] Mykoniati, Maria, i Costas Lambrinoudakis. "Software Development Lifecycle for Survivable Mobile Telecommunication Systems." Advances in Science, Technology and Engineering Systems Journal, vol. 6, no. 4, 2021, pp. 259–277. DOI: 10.25046/aj060430.

[17] Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego.

[18] ISO/IEC 27001:2013 Information Security Management Systems (ISMS)

[19] Hamed Taherdoost, Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview, Electronics 2022, 11(14), 2181; https://doi.org/10.3390/electronics11142181

[20] Ciekanowski, Zbigniew, i Jarosław Starczewski. "Uwarunkowania bezpieczeństwa informacji i systemów teleinformatycznych." Współczesne Problemy Zarządzania, vol. 6, no. 1(12), 2018, pp. 151–160. DOI: 10.52934/wpz.111.

[21] K. Liderman, Standardy w ocenie bezpieczeństwa teleinformatycznego, Biuletyn Instytutu Automatyki i Robotyki, 17/2002.

[22] Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408-1:2022.

[23] Information Technology Security Evaluation Criteria (ITSEC), 1991.

[24] Norma PN-EN ISO/IEC 27001:2022.

[25] Norma NIST Special Publication 800-53 Rev. 5, 2020.

[26] CIS Critical Security Controls® Version 8, 2021.

[27] Liderman, Krzysztof. "Standardy w ocenie bezpieczeństwa teleinformatycznego." Biuletyn Instytutu Automatyki i Robotyki 8.17 (2002): 97-119.

[28] Information Security Auditor. Careers in Information Security, BCS 2016, ISBN 1780172168
[29] R. Pompon, IT Security Risk Control Management An Audit Preparation Plan, Apres, 2016.
[30] Hossain, Md. Mahmud, et al. “Key Drivers of Cybersecurity Audit Effectiveness: A Neo-Institutional Perspective.” International Journal of Auditing, 2023. Wiley Online Library, https://doi.org/10.1111/ijau.12365
[31] Jamil, D., and R. M. Alenezi. “Reviewing the Processes for Conducting Effective Cybersecurity Audits, Including Threat Identification and Response.” ResearchGate, 2023, www.researchgate.net/publication/386342884
[32] Dronov, V. Y., i G. A. Dronova. "Principles of Information Security Management System." Journal of Physics: Conference Series, vol. 2182, 2022, 012092. IOP Publishing, https://doi.org/10.1088/1742-6596/2182/1/012092
[33] Tøndel, Inger Anne, Maria B. Line, i Martin Gilje Jaatun. "Information Security Incident Management: Current Practice as Reported in the Literature." Computers & Security, vol. 45, 2014, ss. 42–57. Elsevier, https://doi.org/10.1016/j.cose.2014.05.003
[34] Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie szczegółowych zasad ochrony informacji niejawnych
[35] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych
[36] Norma ISO/IEC 27001:2017
[37] ISO/IEC 27002:2022 – Praktyczne zasady zabezpieczania informacji
[38] NIST SP 800-53 – Security and Privacy Controls
[39] ISO/IEC 27001:2017 – Systemy zarządzania bezpieczeństwem informacji
[40] Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych
[41] Żabicki D., https://www.ochrona-bezpieczenstwo.pl/ochrona-informacji/prawo/2346-nowe-standardy-w-systemach-kontroli-dostepu-przeglad-aktualnych-norm-i-przepisow
[42] Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych
[43] Norma PN-ISO/IEC 27001:2017
[44] https://bip.abw.gov.pl/bip/informacje-niejawne-1/nadzor-nad-systemem-oc/bezpieczenstwo-fizyczn/150,Kancelarie-tajne-Bezpieczenstwo-fizyczne.html
[45] https://ochrona-niejawnych.pl/ochrona-elektromagnetyczna2/
[46] ISO/IEC 27001 - wytyczne dotyczące ciągłości działania (klauzula 17.1: Kontrola ciągłości działania) oraz wymaga, aby organizacje miały plan ciągłości działania.
[47] ISO 22301 - Norma dotycząca zarządzania ciągłością działania, która szczegółowo opisuje procesy związane z planowaniem, wdrażaniem, utrzymywaniem i doskonaleniem systemu zarządzania ciągłością działania.
[48] NIST SP 800-34 - Wytyczne amerykańskiego Narodowego Instytutu Standardów i Technologii dotyczące planowania ciągłości działania w kontekście systemów informacyjnych. Dokument ten opisuje procesy, które organizacje powinny wdrożyć, aby zapewnić ciągłość działania
[49] NIST SP 800-128 - Wytyczne amerykańskiego Narodowego Instytutu Standardów i Technologii dotyczące zarządzania konfiguracją. Dokument ten koncentruje się na praktykach związanych z zarządzaniem konfiguracją systemów informacyjnych, w tym na rolach i odpowiedzialnościach.
[50] NIST SP 800-53 - Wytyczne amerykańskiego Narodowego Instytutu Standardów i Technologii dotyczące zabezpieczeń systemów informacyjnych. Zawiera wytyczne dotyczące zarządzania dostępem, dokumentowania napraw oraz przeglądów systemów.
[51] NIST SP 800-115 - Wytyczne dotyczące testowania i oceny bezpieczeństwa systemów informacyjnych, które obejmują testy penetracyjne oraz analizy bezpieczeństwa.
[52] ISO/IEC 27002 - Uzupełnienie normy ISO/IEC 27001, zawiera wytyczne dotyczące wprowadzania poprawek i aktualizacji, podkreślając znaczenie dokumentacji oraz testowania poprawek przed ich wdrożeniem.
[53] ISO/IEC 27001 - Międzynarodowa norma dotycząca zarządzania bezpieczeństwem informacji, która w klauzuli 12.6 wskazuje na konieczność zarządzania zmianami i aktualizacjami w systemach informacyjnych

[54] ISO/IEC 27001 - Międzynarodowa norma dotycząca zarządzania bezpieczeństwem informacji, która odnosi się do zarządzania zasobami i ich bezpieczeństwem, w tym nośnikami danych. Klauzula 8.1 odnosi się do identyfikacji i zarządzania aktywami, co obejmuje również nośniki danych.

[55] ISO/IEC 27001 - Międzynarodowa norma dotycząca systemów zarządzania bezpieczeństwem informacji. Zawiera wymagania dotyczące kontroli dostępu (klauzula 9), które odnoszą się do uwierzytelniania użytkowników i urządzeń.

[56] NIST SP 800-53 - Wytyczne Narodowego Instytutu Standardów i Technologii dotyczące zabezpieczeń systemów informacyjnych, które obejmują zasady dotyczące kontroli dostępu, zarządzania kontami użytkowników oraz monitorowania aktywności.

[57] Harold F. Tipton, Mickey Krause, Information Security Management Handbook, 1999

[58] PN-EN ISO/IEC 27001:2023-08 – norma międzynarodowa standaryzująca systemy zarządzania bezpieczeństwem informacji.

[59] ISO/IEC 20000-1:2018 - Standard dotyczący zarządzania usługami IT, który zawiera wytyczne dotyczące zarządzania zmianami jako części cyklu życia usług IT. Zawiera on wymagania dotyczące procesów związanych z zarządzaniem zmianami.

[60] Vielberth, Manfred, et al. "Security Operations Center: A Systematic Study and Open Challenges." IEEE Access, vol. 8, 2020, pp. 227756–227779. IEEE, https://doi.org/10.1109/ACCESS.2020.3045514

[61] Hina, S., et al. "Being Responsible in Cybersecurity: A Multi-Layered Perspective." Information Systems Frontiers, 2025. Springer, https://doi.org/10.1007/s10796-025-10588-0

[62] Lai-Wan Wong, Voon-Hsien Lee, Garry Wei-Han Tan, Keng-Boon Ooi, Amrik Sohal. "The Role of Cybersecurity and Policy Awareness in Shifting Employee Behavior." Journal of Strategic Information Systems, 2022. https://doi.org/10.1016/j.ijinfomgt.2022.102520

[63] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych - regulacje dotyczące zasad ochrony informacji niejawnych, w tym wskazania odpowiedzialności poszczególnych osób.

[64] Art. 14. Ustawy o ochronie informacji niejawnych - odnosi się do obowiązków i odpowiedzialności . Przepis ten szczegółowo opisuje odpowiedzialność KJO za ochronę informacji niejawnych

[65] Rozporządzenie Rady Ministrów z dnia 1 czerwca 2010 r. w sprawie organizacji i funkcjonowania kancelarii tajnych

[66] Amir Zadeh, Brandon Lavine, Hamed Zolbanin, Donald Hopkins. "A cybersecurity risk quantification and classification framework for informed risk mitigation decisions." Decision Analytics Journal Volume 9, December 2023, https://doi.org/10.1016/j.dajour.2023.100328

[67] Rainer Diesch, Matthias Pfaff, Helmut Krcmar. "A Comprehensive Model of Information Security Factors for Decision-Makers." Computers & Security, vol. 92, 2020, https://doi.org/10.1016/j.cose.2020.101747

[68] Frank Cremer, Barry Sheehan, Michael Fortmann, Arash N. Kia, Martin Mullins, Finbarr Murphy & Stefan Materne . "Cyber Risk and Cybersecurity: A Systematic Review of Data Availability." The Geneva Papers on Risk and Insurance - Issues and Practice (2022) 47:698–736, https://doi.org/10.1057/s41288-022-00266-6

[69] Guzman, Nelson H. Carreras, Igor Kozine, and Mary Ann Lundteigen. "An integrated safety and security analysis for cyber-physical harm scenarios." Safety science 144 (2021): 105458.

[70] Rehak, David, et al. "Convergence of Safety and Security within Process Plants." Journal of Loss Prevention in the Process Industries (2025): 105579.

[71] DeSmit, Zach, et al. "An approach to cyber-physical vulnerability assessment for intelligent manufacturing systems." Journal of Manufacturing Systems 43 (2017): 339-351

[72] Ralston, Patricia AS, James H. Graham, and Jefferey L. Hieb. "Cyber security risk assessment for SCADA and DCS networks." ISA transactions 46.4 (2007): 583-594.

[73] Rahman, Mir Mehedi, et al. "AssessITS: Integrating procedural guidelines and practical evaluation metrics for organizational IT and Cybersecurity risk assessment." arXiv preprint arXiv:2410.01750 (2024).

[74] Mouanda, Guy. "Unseen Power of Information Assurance over Information Security." arXiv preprint arXiv:2411.00799 (2024).

[75] Artykuł 6.1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2023 r. poz. 756, 1030).

[76] Sinha, Aditya Roshan, Kunal Singla, and Teresa Matoso Manguangua Victor. "Artificial intelligence and machine learning for cybersecurity applications and challenges." Risk Detection and Cyber Security for the Success of Contemporary Computing (2023): 109-146.

[77] McCoy, Corren G. A relevance model for threat-centric ranking of cybersecurity vulnerabilities. Diss. Old Dominion University, 2022.

[78] ENISA. "Ramy Oceny Zdolności Krajowych." Grudzień 2020

[79] CISA. "Fiscal Year 2023 Risk and Vulnerability Assessments."

[80] NIK. "RealIzacja pRzez podmIoty państwowe zadań w zakresie ochrony cyberprzestrzenI RP" kpb-4101-002-00/2014, Czerwiec 2015

[81] Nalluri, V., and L. S. Chen. "Risk assessment for sustainability on telecom supply chain: A hybrid fuzzy approach." Uncertain Supply Chain Management 10.2 (2022): 559-576.

[82] Ali, Tarek, Mohammed Al-Khalidi, and Rabab Al-Zaidi. "Information security risk assessment methods in cloud computing: Comprehensive review." Journal of Computer Information Systems (2024): 1-28.

[83] ZenGRC. "5 Steps to Performing a Cybersecurity Risk Assessment." ZenGRC Blog, 2023, https://www.zengrc.com/blog/5-steps-to-performing-a-cybersecurity-risk-assessment/. Dostęp 04.2025.

[84] Por. M. Kaczmarek, I. Olejnik, A. Springer, Badania jakościowe – metody i zastosowania, Warszawa 2013, s. 39.

[85] M. Kaczmarek, I. Olejnik, A. Springer, Badania jakościowe – metody i zastosowania, Warszawa 2013, s. 114.

[86] Por. A. Kaniewska-Sępa, G. Leszczyński, B. Pilarczyk, Badania marketingowe na rynku business to business, Kraków 2006, s. 121.

[87] D. Maison, Jakościowe metody badań marketingowych [w:] D. Maison, A. Noga-Bogomilski (red.), Badania marketingowe. Od teorii do praktyki, Gdańsk 2007, s. 10-13.

[88] Cyt za: El Fray, Imed. Metoda określająca zaufanie do systemu informacyjnego w oparciu o proces szacowania i postępowania z ryzykiem. Wyd. Stowarzyszenie Przyjaciół Wydziału Informatyki w Szczecinie, Szczecin, 2013.

[89] D. B. Parker (1981) Computer Security Management. Reston Publishing Company Inc., Reston VA, US

[90] B. Żurek, (1999) RMS Program Used in Risk Management, Conference Proceeding "Project Management – experience and Methods", Gdańsk, Poland

[91] K. Liderman (2008) Analiza ryzyka I ochrona informacji w systemach komputerowych. PWN, Warszawa, Polska

[92] G. Manunta (2000) Security and Methodology, Cranfield Security Centre, The Royal Military College of Science, Cranfield University, Wiltshire.

[93] M. Ryba (2006) Wielowymiarowa metodyka analizy i zarządzania ryzykiem systemów informatycznych – MIR-2M, rozprawa doktorska, Kraków.

[94] El Fray, Metoda określająca zaufanie do systemu informacyjnego w oparciu o proces szacowania i postępowania z ryzykiem, wyd. Stowarzyszenie Przyjaciół Wydziału Informatyki w Szczecinie, Szczecin, 2013.

[95] Kunz, Immanuel, Angelika Schneider, and Christian Banse. "A continuous risk assessment methodology for cloud infrastructures." 2022 22nd IEEE International Symposium on Cluster, Cloud and Internet Computing (CCGrid). IEEE, 2022.

[96] Ekstedt, Mathias, et al. "Yet another cybersecurity risk assessment framework." International Journal of Information Security 22.6 (2023): 1713-1729.

[97] Ali, Tarek, Mohammed Al-Khalidi, and Rabab Al-Zaidi. "Information security risk assessment methods in cloud computing: Comprehensive review." Journal of Computer Information Systems (2024): 1-28.

[98] Popescu, Traian Mihai, Alina Madalina Popescu, and Gabriela Prostean. "Iot security risk management strategy reference model (Iotsrm2)." Future Internet 13.6 (2021): 148.

[99] Annunziata, Giusy, et al. "Security Risk Assessment on Cloud: A Systematic Mapping Study." Proceedings of the 28th International Conference on Evaluation and Assessment in Software Engineering. 2024.

[100] Babaei, Aptin, et al. "A Review of Machine Learning-based Security in Cloud Computing." arXiv preprint arXiv:2309.04911 (2023).

[101] Svandova, Katerina, and Zdenek Smutny. "Internet of Medical Things Security Frameworks for Risk Assessment and Management: A Scoping Review." Journal of Multidisciplinary Healthcare (2024): 2281-2301.

[102] KELLY, MICHAEL, and ADELINE CHAN. "Performing Risk Assessments of Emerging Technologies." ISACA Journal 6 (2022).

[103] "Cybersecurity Risk Assessment According to ISA/IEC 62443-3-2." ISA Global Cybersecurity Alliance, 2023. https://gca.isa.org/blog/cybersecurity-risk-assessment-according-to-isa-iec-62443-3-2. Dostęp 04.2025.

[104] Pałęga, Michał. "Zarządzanie ryzykiem bezpieczeństwa informacji w świetle wymagań normatywnych." Systemy Wspomagania w Inżynierii Produkcji 6 (2017).

[105] Pandey, Santosh K., K. Mustafa "A comparative study of risk assessment methodologies for information systems." Bulletin of Electrical Engineering and Informatics 1.2 (2012): 111-122.

[106] Kacprowicz D., „Sanityzacja informacji w bezpilotowych systemach ewakuacji medycznej w kontekście kształtowania świadomości sytuacyjnej pola walki" w Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne, nr 2, 2024, s. 18-21.

[107] Kacprowicz, D., „Interoperacyjność bezpilotowego systemu ewakuacji medycznej w kontekście standardów NATO." Elektronika: konstrukcje, technologie, zastosowania 65 (2024).

[108] Taherdoost, Hamed. "Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview." *Electronics* 11.14 (2022): 2181.

Literatura uzupełniająca

[1] AC/35-D/2000 – Dyrektywa Bezpieczeństwa Osobowego.Zródło https://bip.abw.gov.pl/download/1/1208/AC35-D2000REV8.pdf. Dostęp 04.2025.

[2] AC/35-D/2001 – Dyrektywa Bezpieczeństwa Fizycznego. Źródło: https://bip.abw.gov.pl/download/1/1209/AC35-D2001REV3.pdf. Dostęp 04.2025.

[3] AC/35-D/2002 – Dyrektywa Bezpieczeństwa Obiegu Informacji. Źródło: https://bip.abw.gov.pl/download/1/1210/AC35-D2002REV5.pdf. Dostęp 04.2025.

[4] AC/35-D/2003 – Dyrektywa Projektów Niejawnych i Bezpieczeństwa Przemysłowego.Źródło: https://bip.abw.gov.pl/download/1/1211/ac35d2003rev5.pdf. Dostęp 04.2025.

[5] AC/35-D/2004 – Dyrektywa podstawowa INFOSEC. Źródło: https://bip.abw.gov.pl/download/1/1212/AC35D2004REV2.pdf. Dostęp 04.2025.

[6] AC/35-D/2005 – Dyrektywa zarządzania INFOSEC w systemach teleinformatycznych. Źródło: https://bip.abw.gov.pl/download/1/1213/AC35D2005REV2.pdf. Dostęp 04.2025.

[7] Agrawal, M.; Campoe, A.; Pierce, E., Information Security and IT Risk Management, Wiley, 2014, ISBN 9781118335895.

[8] Alberts, C. J., Dorofee, A. J., OCTAVE Method Implementation Guide Version 2.0, Carnegie Mellon University - Software Engineering Institute, Pittsburgh, Pennsylvania, US, 2001.

[9] Anderson, R. Inżynieria zabezpieczeń. WNT, Warszawa, Polska, 2006.

[10] Andrews, J. D., Dunnett, S. J. Event-tree analysis using binary decision diagrams. IEEE Transactions on Reliability, Vol. 49, Iss. 2, pp. 230-239, 2000.

[11] Andrews, J. D., Ridley, L. M. Application of the cause-consequence diagram method to static systems. Reliability Engineering & System Safety, Vol. 75, Iss. 1, pp. 47–58, 2002.

[12] Antonucci, D., The Cyber Risk Handbook. Creating and Measuring Effective Risk Management Strategies, Wiley, 2017.

[13] Kohnke, A. The Complete Guide to Cybersecurity Risks and Controls, 2016, ISBN 1498740545.

[14] Bandyopadhyay, K., Mykytyn, P. P., Mykytyn, K., "A framework for integrated risk management in information technology", Management Decision, Vol. 37, Iss. 5, pp. 437 – 445, 1999.

[15] Baskerville, R., Information Systems Security Design Methods: Implications for Information Systems Development, Computing Surveys, Vol. 25, No. 4, 1994.

[16] Bedford, T., Cooke, R. Probabilistic risk analysis foundations and methods. Cambridge University Press, New York, USA, 2001.

[17] Bhattacharya, Bhargab B., Algorithms, Architectures and Information Systems Security, 2008, ISBN 9812836233.

[18] Białas, A., Lisek, K. Integrated, Business-Oriented, Two-Stage Risk Analysis. Proceedings of the International Multiconference on Computer Science and Information Technology, pp. 617–628, 2007.

[19] Bień, F., Zarządzanie cyklem życia informacji, IT Security Review, Boston, nr 3, 2017.

[20] Bjørnar, S., Refsadal., A., Stølen, K., Cyber-Risk Management, Springer, 2015, ISBN 3319235699.

[21] British Standards Institute, BS 7799-1:1999: Part 1: "Code of practice for Information Security Management", BSI.

[22] British Standards Institute, BS 7799-2:1999: Part 2: "Specification for Information Security Management Systems", British Standards Institute.

[23] Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 100-2: IT Grundschutz Methodology, Bonn, Deutsche, 2008.

[24] CCIB, Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model, Version 2.0, 1998, CCIB-98-026.

[25] CCIB, Common Criteria for Information Technology Security Evaluation. Part 2: Security functional requirements, Version 2.0, 1998, CCIB-98-027.

[26] CCIB, Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance requirements, Version 2.0, 1998, CCIB-98-028.

[27] Clemen, R. T., Winkler, R. L. Combining probability distributions from experts in risk analysis. Risk Analysis, Vol. 19, Iss. 2, pp. 187-203, 1999.

[28] COBIT Steering Committee i Information Systems Audit and Control Foundation, COBIT™ Control Objectives, 2nd Edition, 1998.

[29] COBRA, Consultative, Objective and Bi-functional Risk Analysis, Disaster Recovery Planning Group, UK, 1991.

[30] CRAMM, CCTA Risk Analysis and Management Method, Central Computing and Telecommunications Agency, UK, 1987.

[31] Decyzja Komisji, UE, Euratom. 2015/444 z dnia 13 marca 2015 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE.

[32] Decyzja Rady z dnia 23 września 2013 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE, 2013/488/UE..

[33] Departament Obrony Stanów Zjednoczonych, Trusted Computer Standards Evaluation Criteria, 1985.

[34] Dhillon, G., Torkzadeh, G. Value-focused assessment of information system security in organizations. Information Systems Journal, Vol. 16, Iss. 3, pp. 293–314, 2006.

[35] DoD, Trusted Computer System Evaluation Criteria, CSC-STD-001-83, 1983.

[36] El Fray, I. A comparative study of risk assessment methods, MEHARI & CRAMM with a new formal model of risk assessment, FoMRA. in information systems. In A. Cortesi et al., Eds..: CISIM 2012, LNCS 7564, pp. 428–442, 2012.

[37] El Fray, I. About Some Application of Risk Analysis and Evaluation. Artificial Intelligence and Security in Computing Systems, The Springer International Series in Engineering and Computer Science Volume 752, pp. 283-292, 2003.

[38] El Fray, I. An approach to determine the Evaluation Assurance Level to the system based on the results of risk analysis. Pomiary, Automatyka, Kontrola, R. 57, nr 7, pp. 770-773, 2011.

[39] El Fray, I. Trust construction for security functions and mechanisms of IT system using results of risk analysis. Pomiary, Automatyka, Kontrola, R. 55, nr 10, pp. 893-843, 2009.

[40] El Fray, I., Hyla, T., Maćków, W., Pejaś, J. Authentication and authorization in multilevel security systems for public administration. Pomiary, Automatyka, Kontrola, R. 56, nr 8, pp. 983-986, 2010.

[41] El Fray, I., Kurkowski, M., Pejaś, J., Maćków, W., A new mathematical model for analytical risk assessment and prediction in IT systems, Control and Cybernetics, Vol. 41, Iss. 1, pp. 241-268, 2012.

[42] Federal Information Processing Standard 65, Guideline for Automatic Data Processing Risk Analysis, National Bureau of Standards, US, 1979.

[43] FERMA, Risk Management Standard, Federation of European Risk Management in Dynamic Open Systems, London, UK, 2003.

[44] Griffor, Edward, Handbook of System Safety and Security. Cyber Risk, Syngress, 2017, ISBN 0128037733.

[45] Herman, P. How to Integrate Trust Management into a Risk Analysis Process. 2nd International Workshop on Trust Management in Dynamic Open Systems, London, UK, 2003.

[46] Hu, S., Fang, Q., Xia, H., Xi, Y. Formal safety assessment based on relative risks model in ship navigation. Reliability Engineering & System Safety, Vol. 92, Iss. 3, pp. 369–377, 2007.

[47] Hubbard, D. i inni, How to Measure Anything in Cybersecurity Risk, Wiley, 2016, ISBN 1119085292.

[48] Humphreys, E., Information security management standards: Compliance, governance and risk management, Information Security Technical Report, Volume 13, Issue 4, pp. 247–255, 2008.

[49] Hyla, T., El Fray, I., Maćków, W., Pejaś, J. Long-term preservation of digital signatures for multiple groups of related documents. Information Security, IET, Vol. 6, Iss. 3, pp. 219 – 227, 2012.

[50] Information Systems Audit and Control Association, Standard 050.050.030 – IS Auditing Guideline – Use of Risk Assessment in Audit Planning, ISACA, USA-CA, 2000.

[51] ISO/IEC 15408-1, Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model, International Organization for Standardization, Genève, Suisse, 2005.

[52] ISO/IEC 15408-2, Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements, International Organization for Standardization, Genève, Suisse, 2005.

[53] ISO/IEC 15408-3, Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements, International Organization for Standardization, Genève, Suisse, 2005.

[54] ISO/IEC 18045, Information technology – Security techniques – Methodology for IT security evaluation, International Organization for Standardization, Genève, Suisse, 2005.

[55] ISO/IEC 27000 Information technology - Security techniques - Overview and vocabulary. International Organization for Standardization, Genève, Suisse, 2009.

[56] ISO/IEC 27001 Information technology - Security techniques - Information security management systems – Requirements. International Organization for Standardization, Genève, Suisse, 2005.

[57] ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management. International Organization for Standardization, Genève, Suisse, 2005.

[58] ISO/IEC 27003 Information technology - Security techniques - Information security management system implementation guidance. International Organization for Standardization, Genève, Suisse, 2010.

[59] ISO/IEC 27004 Information technology - Security techniques - Information security management – Measurement. International Organization for Standardization, Genève, Suisse, 2009.

[60] ISO/IEC 27006 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems. International Organization for Standardization, Genève, Suisse, 2011.

[61] ISO/IEC 27007 Information technology - Security techniques - Guidelines for information security management systems auditing. International Organization for Standardization, Genève, Suisse, 2011.

[62] ISO/IEC 27011 Information technology - Security techniques - Information security management guidelines for telecommunications organizations. International Organization for Standardization, Genève, Suisse, 2008.

[63] ISO/IEC 27799 Information technology - Security techniques - Information security management in health. International Organization for Standardization, Genève, Suisse, 2008.

[64] ISO/IEC Guide 73 Risk management – Vocabulary – Guidelines for use in standards. International Organization for Standardization, Genève, Suisse, 2009.

[65] ISO/IEC TR 13335-1 Information technology - Guidelines for the management of IT Security - Part 1: Concepts and models for IT security. International Organization for Standardization, Genève, Suisse, 1996.

[66] ISO/IEC TR 13335-1 Information technology - Guidelines for the management of IT Security - Part 4: Selection of safeguards. International Organization for Standardization, Genève, Suisse, 2000.

[67] ISO/IEC TR 13335-2 Information technology - Guidelines for the management of IT Security - Part 2: Managing and planning IT Security. International Organization for Standardization, Genève, Suisse, 1997.

[68] ISO/IEC TR 13335-3 Information technology - Guidelines for the management of IT Security - Part 3: Techniques for the management of IT Security. International Organization for Standardization, Genève, Suisse, 1998.

[69] ISO/IEC TR 13335-5 Information technology - Guidelines for the management of IT Security - Part 5: Management guidance on network security. International Organization for Standardization, Genève, Suisse, 2001.

[70] ITSEC. Information Technology Security Evaluation Criteria. Preliminary harmonised Criteria COM, 90.314, Version 1, 1991.

[71] Jacoub, S. M., Ammar, H. H. A methodology for architectural-level reliability risk analysis. IEEE Transactions on Software Engineering, Vol. 28, Iss. 6, pp. 529-547, 2001.

[72] Jøsang, A., Knapskog, S. J. A Metric for Trusted Systems. Norway, 1998.

[73] Kaczmarek, T., Ryzyko i zarządzanie ryzykiem. Ujęcie interdyscyplinarne, Difin, Warszawa, 2008.

[74] Kennedy, R., Kirwan, B. Development of a Hazard and Operability-based method for identifying safety management vulnerabilities in high risk systems. Safety Science, Vol. 30, Iss. 3, pp. 249–274, 1998.

[75] Kifner, T., Polityka bezpieczeństwa i ochrony informacji, Helion, Gliwice, 1999.

[76] Kouns, J., Minoli, D. Information Security Risk Management Defined. Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk. Wiley, USA, 2010.

[77] Krysowaty, I.; N., P., Informacja w systemach IT jako towar strategiczny, Instytut Technologii Eksploatacyjnej, Radom, 2006.

[78] Liderman, K., Analiza ryzyka i ochrona informacji w systemach komputerowych, PWN, Warszawa, 2009.

[79] Liderman, K., Bezpieczeństwo teleinformatyczne, Instytut Teleinformatyki i Automatyki WAT, 2001.

[80] Liderman, K., Oszacowanie jakościowe ryzyka dla potrzeb bezpieczeństwa teleinformatycznego, Instytut Teleinformatyki i Automatyki WAT, Warszawa, 2003.

[81] Loske, André, IT Security Risk Management in the Context of Cloud Computing, Springer, 2015, ISBN 3658113391.

[82] Łuczak, J., Metody szacowania ryzyka – kluczowe elementy systemu zarządzania bezpieczeństwem informacji ISO/IEC 27001, Zeszyty Naukowe Akademii Morskiej w Szczecinie, 2009.

[83] Łuczak, J.; Tyburski, M., Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001, WUE, Poznań, 2010.

[84] Managing Risk and Information Security, Press, 2ed., 2016, ISBN 1484214560.

[85] MARION, Méthodologie d'Analyse des Risques Informatique et d'Optimation par Niveau, CLUSIF, France, 1998.

[86] Mayer, N., Humbert, J. P. La gestion des risques pour les systèmes d'information. MISC-Éditions Diamond. Vol. 24, pp. 1-7, 2006.

[87] Mazurek, P., Realizacja szacowania ryzyka w wybranym przedsiębiorstwie.

[88] MEHARI, Méthode Harmonisée d'Analyse de Risques, CLUSIF, France, 2010.

[89] MEHARI. Evaluation guide for security services. Clusif France, 2010.

[90] MEHARI. Fundamental concepts and functional specifications. Clusif France, 2010.

[91] MEHARI. Processing guide for risk analysis and management. Clusif France, 2010.

[92] MEHARI. Risk analysis and treatment guide. Clusif France, 2010.

[93] MEHARI. Security stakes analysis and classification guide. Clusif France, 2010.

[94] Molski, M.; Ł., M., Przewodnik audytora systemów informatycznych, Helion, Gliwice, 2007.

[95] NIST, Risk Management Guide for Information Technology Systems, SP800-30.

[96] Pałęga, M., Ocena poziomu zagrożeń bezpieczeństwa informacji za pomocą macierzy ryzyka. Wybrane zagadnienia dotyczące usprawniania procesów w przedsiębiorstwie, Pod red. M. Ogórek, T. Bajor, Wydawnictwo WiPiTM Politechniki Częstochowskiej, Częstochowa, 2016.

[97] Pejaś, J., El Fray, I. Some methods of the analysis and risk assessment in the PKI system services providers. Enhanced Methods in Computer Security, Biometric and Artificial Intelligence Systems, The Springer International Series in Engineering and Computer Science, Vol. 852, pp. 61-70, 2005.

[98] Pejaś, J., El Fray, I. Wady i zalety narzędzi do zarządzania ryzykiem w systemach informacyjnych. X Krajowa Konferencja Zastosowań Kryptografii: ENIGMA - 2006, pp. 245-259, 2006.

[99] Pejaś, J., El Fray, I., Ruciński, A. Authentication protocol for software and hardware components in distributed electronic signature creation system. Electrical Review, R. 88 NR 10b, pp. 192-197, 2012.

[100] Peltier, T., Information Security Risk Analysis, 3rd Edition, Press, Wyandotte, Michigan, 2010, ISBN 1439839565.

[101] Pierce, The Complete Guide to Cybersecurity Risks and Controls, 2017, ISBN 1722677996.

[102] Pipkin, D. L., Bezpieczeństwo Informacji, WNT, 2002

[103] PN-I-02000, Technika informatyczna. Terminologia. Zabezpieczenia w systemach.

[104] PN-I-13335-1:1999, Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych, PKN, Warszawa, 1999.

[105] PN-ISO/IEC 27005:2014, Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji, PKN, Warszawa, 2013.

[106] Polaczek, T., Audyt bezpieczeństwa informacji w praktyce, Helion, Gliwice, 2006.

[107] Pompon, R., IT Security Risk Control Management. An Audit Preparation Plan, Press, 2016, ISBN 1484221397.

[108] Press, Cyber and Electromagnetic Threats in Modern Relay Protection, 2014, ISBN 1482264315.

[109] Przepisy bezpieczeństwa Europejskiej Agencji Kosmicznej, ESA/REG/004 z dnia 1 lipca 2020.

[110] Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego, Dz. U. Nr 159, poz. 948.

[111] Ryba, M. Oparta na koncepcji rywalizacji metoda analizy ryzyka systemów informatycznych. Computer Science, UWND AGH, Kraków, Poland, 2004.

[112] Ryba, M. Wielowymiarowa metodyka analizy i zarządzania ryzykiem systemów informatycznych – MIR-2M, rozprawa doktorska, Kraków, Polska, 2006.

[113] Rybarek, A., Topolnicki, Z. Przykład zastosowania metody HAZOP do analizy zagrożeń. Bezpieczeństwo Przemysłowe, T.1, pp. 95-100, 2008.

[114] Rządowe Centrum Bezpieczeństwa, Ocena ryzyka na potrzeby zarządzania kryzysowego, Raport o zagrożeniach bezpieczeństwa narodowego.

[115] Spears, J. L., Barki, H., User participation in information systems security risk management, MIS Quarterly, Vol. 34, No. 3, pp. 503-522, 2010.

[116] Stoneburner, G., Goguen, A., Feringa, A., NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology, Gaithersburg, US, 2002.

[117] Stoneburner, G., Hayden, C., Feringa, A. NIST Special Publication 800-27 Rev. A: Engineering Principles for Information Technology Security, A Baseline for Achieving Security.. National Institute of Standards and Technology, Gaithersburg, USA, 2004.

[118] Talabis, Mark, Information Security Risk Assessment Toolkit. Practical Assessments, Syngress, 2012, ISBN 1597497355.

[119] TCSEC. Trusted Computer System Evaluation Criteria. U.S. Department of Defense, DOD 5200.28-STD, Orange Book., USA, 1985.

[120] Vose, D. Risk Analysis: A Quantitative Guide. John Wiley & Sons, West Sussex, UK, 2008.

[121] Wołowski, F.; Zawiła-Niedźwiecki, J., Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny normami polskimi i międzynarodowymi, Edu-Libri, Kraków-Warszawa, 2012.

[122] Zhao, D. M., Wang, J. H. Using Fuzzy Logic And Entropy Theory To Risk Assessment Of The Information Security. Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, Guangzhou, Vol. 4, pp. 2448 – 2453, 2005.

Indeks tabel