Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

Wydział Informatyki

Damian Kacprowicz

OCENA BEZPIECZEŃSTWA SYSTEMÓW TELEINFORMATYCZNYCH PRZETWARZAJĄCYCH INFORMACJE NIEJAWNE

Rozprawa doktorska

przygotowana pod kierunkiem

Promotor

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

Promotor pomocniczy

dr inż. Witold Maćków

Szczecin 2024

Kamili, Ani, Uli

Spis treści

WSTĘP

„W życiu należy kierować się prawdą i dzielić się zdobytą wiedzą”
Profesor Brunon Hołyst

Postęp w dziedzinie technologii teleinformatycznych spowodował, że większość działalności organizacyjnych opiera się na przetwarzaniu informacji w systemach teleinformatycznych. Z jednej strony ułatwia to gromadzenie i przesyłanie informacji, ale z drugiej strony stwarza dodatkowe zagrożenia związane z możliwością przestępczego kopiowania i modyfikacji danych.

Charakterystyka systemów teleinformatycznych wymaga zastosowania odpowiednich zabezpieczeń, aby chronić zasoby systemu przed różnymi zagrożeniami, którym są one narażone w swoim środowisku produkcyjnym. Zasoby systemów teleinformatycznych, w szczególności zasoby informacyjne, są niezwykle ważnymi aktywami organizacji i wymagają odpowiedniej ochrony, niezależnie od ich formy. Bezpieczeństwo elektronicznie przetwarzanych informacji ma fundamentalne znaczenie, zwłaszcza w przypadku poufnych informacji objętych ustawową ochroną.

Wiele norm oraz zaleceń określa potrzebę oceny poziomu bezpieczeństwa dla perspektywy ochrony. Istniejące metody charakteryzują się dużą złożonością a co za tym idzie podatną na błędy. Stosowanie zbyt złożonych metod tworzy ryzyko wykonania oceny bezpieczeństwa jedynie na etapie akredytacji systemów a nie zgodnie z zasadami aplikacji cyklicznie co pewien czas. Brak systematyczności zaniża poziom bezpieczeństwa chronionych systemów.

Koncepcja badawcza obejmuje przegląd istniejących standardów, metod oceny bezpieczeństwa oraz przeprowadzenie indywidualnych wywiadów

pogłębionych z interesariuszami pionów ochrony informacji niejawnych w celu zaproponowania efektywnej procedury oceny poziomu bezpieczeństwa systemu teleinformatycznego.

Proponowana ocena mechanizmów bezpieczeństwa uwzględniać będzie najważniejsze atrybuty bezpieczeństwa tj. poufność, integralność oraz dostępność zawartości informacyjnej systemów teleinformatycznych.

Praca składa się z czterech rozdziałów.

Rozdział pierwszy w ujęciu ontologicznym wskazuje na istotę ochrony. Odpowiada na pytanie na czym należy się skupić aby w ujęciu podmiotowym zapewnić bezpieczeństwo informacji. Analogicznie jak w kryptologii w której dla zapewnienia bezpieczeństwa informacji najistotniejszym zagadaniem w projektowaniu jak i łamaniu nowych szyfrów jest zrozumienie zjawisk dyfuzji oraz konfuzji informacyjnej tak w ocenie bezpieczeństwa systemów teleinformatycznych najistotniejszym elementem jest określenie gwarantowanej miary – poziomu bezpieczeństwa w odniesieniu do zidentyfikowanego zasobu podlegającego ochronie. Rozdział wprowadza do tematu bezpieczeństwa informacji, przedstawiając podstawowe kategorie informacji wymagających ochrony, argumenty dla ich zabezpieczenia, klasyfikację informacji, proces klasyfikacji i zawartość metadanych plików cyfrowych, cykl funkcjonowania systemu teleinformatycznego oraz kluczowe aspekty ochrony informacji. Obejmuje on również zwrócenie uwagi na różnorodne czynniki i zagrożenia, które mogą mieć wpływ na ich bezpieczeństwo, a także konieczność skoncentrowania się na zarządzaniu ryzykiem i minimalizacji potencjalnych zagrożeń.

Rozdział drugi dostarcza nam konkluzji w jaki sposób do rozwiązania problemu podchodzą organizacje definiujące standardy w ocenie poziomu bezpieczeństwa, jakie są dobre praktyki oraz metody certyfikacji rozwiązań zapewniających bezpieczeństwo informacji. Dostarcza nam wiedzy o próbie określenia gwarantowanej miary poziomu bezpieczeństwa systemów

teleinformatycznych poprzez zastosowanie metod ilościowych, jakościowych jak i mieszanych. Rozdział koncentruje się na ocenie poziomu bezpieczeństwa informacji w systemie, który składa się z kilku etapów. Poszczególne czynności mają na celu ustalenie stopnia ochrony informacji oraz identyfikację zagrożeń i ryzyka z nimi związanego. Pierwszą czynnością jest identyfikacja chronionych zasobów informacyjnych i określenie ich wartości. Następnie dokonuje się identyfikacji zagrożeń i ocenia ich poziom, co umożliwia identyfikację i oszacowanie ryzyka. Proces ten opiera się na analizie wartości informacji, zagrożeń i podatności, a wynikowa ocena ryzyka służy do ustalenia priorytetów w działaniach mających na celu zapewnienie odpowiedniego poziomu bezpieczeństwa informacji.

Trzeci rozdział przedstawia kompleksową metodę oceny bezpieczeństwa informacji. Składa się ona z etapów, które obejmują identyfikację zasobów informacyjnych, zagrożeń, oszacowanie skutków utraty zasobów oraz ocenę ryzyka. Uwypuklonym jest jak ważnym jest zachowanie poufności, integralności i dostępności informacji, a także przeciwdziałanie szkodom poprzez odpowiednie środki ochrony.

Czwarty rozdział omawia różne działania mające na celu utrzymanie zakładanego poziomu bezpieczeństwa informacji. Obejmuje to przeglądy ryzyk, nadzór i kontrolę zgodności z dokumentacją bezpieczeństwa, monitorowanie bezpieczeństwa w czasie rzeczywistym, informowanie o pojawiającym się ryzyku i aktualizowanie zabezpieczeń oraz uświadamianie i szkolenie pracowników. Przedstawione zostają dobre praktyki pozwalające na utrzymanie zakładanego poziomu bezpieczeństwa oraz potencjał aplikacyjny proponowanej metody oceny poziomu bezpieczeństwa systemów teleinformatycznych. Wszystkie te działania są istotne dla zapewnienia trwałego i skutecznego bezpieczeństwa informacji w systemie.

ROZDZIAŁ 1
Ochrona informacji w systemach teleinformatycznych

„Pierwsza wojna światowa była wojną chemików,
druga wojna światowa była wojną fizyków,
trzecia wojna światowa będzie wojną matematyków”
Profesor Jerzy Gawinecki

1 Klasy chronionych informacji

Klasy informacji to rozłączne podzbiory informacji, które są wyróżnione i określone przez ustawę o ochronie informacji niejawnych. Znaczenie poszczególnych klas kształtuje się 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, informacje oznaczone tą klasą są jeszcze bardziej ograniczone 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, 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 są hierarchicznie uporządkowane według następującej kolejności: J < Z < Pf < 0 < 00. Każdy użytkownik, który posiada uprawnienia dostępu do danej klasy (daje rękojmię zachowania tajemnicy), ma również uprawnienia dostępu do wszystkich klas niższych w hierarchii.

W parze z rękojmią zachowania tajemnicy jest 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 w wykonywaniu 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.

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.[1]

[1]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, aby zabezpieczyć interesy bezpieczeństwa obywateli i kraju przed nieuprawnionym dostępem oraz nieuprawnionym ujawnieniem informacji. Jest to istotny element ochrony informacji niejawnych i zapewnienia bezpieczeństwa państwowego.

To, jaką klauzulę nadać reguluje art. 5 ustawy o ochronie informacji niejawnych:

- **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. Przyjęcie tej klauzuli wynika z różnych czynników, takich jak:

- 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: Jeśli ujawnienie informacji stanowiłoby zagrożenie dla bezpieczeństwa wewnętrznego kraju lub porządku konstytucyjnego;
- Zagrożenie sojuszom lub pozycji międzynarodowej Rzeczypospolitej Polskiej: Jeżeli ujawnienie informacji mogłoby zagrozić sojuszom lub pozycji międzynarodowej kraju;

- Osłabienie gotowości obronnej Rzeczypospolitej Polskiej, jeśli ujawnienie informacji mogłoby osłabić gotowość obronną kraju;
- Zagrożenie identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu: Klauzula "ściśle tajne" jest również stosowana w przypadku zagrożenia identyfikacji osób wykonujących czynności operacyjno-rozpoznawcze oraz osób udzielających im pomocy, jeśli zagraża to bezpieczeństwu wykonywanych czynności.
- Zagrożenie życiu lub zdrowiu funkcjonariuszy, żołnierzy lub pracowników wykonujących czynności operacyjno-rozpoznawcze: Jeżeli ujawnienie informacji mogłoby zagrażać życiu lub zdrowiu osób wykonujących czynności operacyjno-rozpoznawcze lub osobom im pomagającym;
- Zagrożenie życiu lub zdrowiu świadków koronnych lub osób im najbliższych: Klauzula "ściśle tajne" jest nadawana w przypadku, gdy ujawnienie informacji mogłoby zagrażać życiu lub zdrowiu świadków koronnych lub ich osób najbliższych.[2]

- klauzula „Tajne”, zgodnie z art. 5 ust. 2 ustawy o ochronie informacji niejawnych nadawana informacjom wrażliwym, których nieuprawnione ujawnienie może spowodować poważną szkodę dla Rzeczypospolitej Polskiej. Przyjęcie tej klauzuli wynika z różnych czynników, takich jak:

- 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, nadaje się klauzulę "tajne".[3]
- Pogorszenie stosunków Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi: Klauzula "tajne" jest stosowana w

[2]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.

[3]Tamże, s. 24.

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, stosuje się klauzulę "tajne".
- Utrudnienie wykonywania czynności operacyjno-rozpoznawczych oraz ścigania sprawców zbrodni: Klauzula "tajne" jest również stosowana 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.
- Zakłócenie funkcjonowania organów ścigania i wymiaru sprawiedliwości: Jeżeli ujawnienie informacji w istotny sposób zakłóciłoby funkcjonowanie organów ścigania i wymiaru sprawiedliwości, nadaje się klauzulę "tajne".
- Przyniesienie znacznej straty interesom ekonomicznym Rzeczypospolitej Polskiej: Klauzula "tajne" jest stosowana 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 wyjątkowo poważna, ale nadal istotna. Poniżej kategorie możliwych szkód, które wymagają nadania klauzuli "poufne":

- Utrudnienie prowadzenia bieżącej polityki zagranicznej Rzeczypospolitej Polskiej: Jeżeli ujawnienie informacji utrudniłoby prowadzenie bieżącej polityki zagranicznej kraju, stosuje się klauzulę "poufne".
- 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, nadaje się klauzulę "poufne".

- Zakłócenie porządku publicznego lub zagrożenie bezpieczeństwu obywateli: Klauzula "poufne" jest stosowana 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, stosuje się klauzulę "poufne".
- Utrudnienie wykonywania zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości: Klauzula "poufne" jest stosowana, 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: Jeżeli ujawnienie informacji zagroziłoby stabilności systemu finansowego.[4]

- klauzula „Zastrzeżone”, zgodnie z art. 5 ust. 4 ustawy o ochronie informacji niejawnych, klauzula "zastrzeżone" 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,

[4]Tamże, s. 24-25.

- 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.[5]

[5]Tamże, s. 25.

2 Ochrona wiedzy w systemach teleinformatycznych

Wiedza ma istotne znaczenie dla danej jednostki organizacyjnej[6] i wymaga ochrony w celu zapewnienia rentowności i ciągłości jej funkcjonowania. 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 zabezpieczone przed nieautoryzowanym odczytem, usunięciem lub zmianą, a zawsze dostępne dla uprawnionego użytkownika systemu.[7]

Bezpieczna informacja to informacja, która spełnia następujące warunki:[8]

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

Spełnienie tych warunków może się różnić w zależności od systemów oraz zależeć od wielu czynników, takich jak klauzula informacji oraz jej znaczenie w danej jednostce organizacyjnej.

Bezpieczny system teleinformatyczny to taki, który zapewnia ochronę danych, które są w nim przetwarzane. Aby to osiągnąć, system musi posiadać mechanizmy do monitorowania dostępu użytkowników do informacji, sprawdzania ich tożsamości oraz autentykacji. Dodatkowo, system powinien być odporny na

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

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

[8] Tamże, s. 20-23.

nieuprawnione manipulacje z zewnątrz, ale także na celowe lub przypadkowe manipulacje. Ważne jest także, aby system działał niezawodnie.

W bezpiecznym systemie teleinformatycznym kluczowym elementem jest ochrona danych. Aby to zagwarantować, konieczne są odpowiednie środki zabezpieczające, które obejmują zarówno aspekty fizyczne, techniczne, jak i 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. Również kluczowe jest utworzenie specjalnych struktur 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.

3 Informacje wrażliwe

Informacja jest zbiorem danych, faktów lub treści, które przekazują lub reprezentują pewne informacje o świecie. Może to być zapisane w różnych formach, takich jak tekst, dźwięk, obraz czy dane numeryczne. Informacja ma na celu przekazywanie wiedzy, powiadomień lub komunikacji między osobami lub systemami.[9]

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

Z formalnego punktu widzenia informacja może być definiowana na różne sposoby, w zależności od dziedziny i kontekstu, w którym jest używana.

[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.

W teorii informacji opracowanej przez Claude'a Shannona informacja jest miarą redukcji niepewności. Zdefiniował on ją jako odwróconą wartość prawdopodobieństwa wystąpienia danego zdarzenia. Informacja jest większa, gdy zdarzenie jest mniej prawdopodobne.[11]

Informacja może być rozumiana jako mierzalna ilość danych, redukcja niepewności, przekaz znaczenia lub treść przetwarzana przez umysł.

W dzisiejszym świecie informacja i wiedza są traktowane jako nowy rodzaj towaru, porównywalny z dobrami materialnymi i energią. Współczesne społeczeństwo globalne, zwane społeczeństwem informacyjnym, jest silnie uzależnione od Internetu i innych masowych źródeł informacji. Termin "informacja" 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.[12]

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.[13]

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.

[11]C. E. Shannon, Mathematical Theory of Communication, Bell System Technical Journal, 1948.

[12]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.

[13]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, takich jak naruszenie prywatności, utrata zaufania, straty finansowe czy kary prawne.

Ważne jest, aby odpowiednio identyfikować, klasyfikować i chronić informacje wrażliwe, aby zapewnić poufność, integralność i dostępność tylko dla uprawnionych osób.

4 Motywacja ochrony informacji

Wprowadzenie zabezpieczeń do systemu teleinformatycznego powinno uwzględniać potrzeby związane z ochroną przetwarzanych w nim informacji. Określenie tych potrzeb powinno opierać się na polityce bezpieczeństwa informacji przynależących do danej jednostki organizacyjnej. Polityka ta określa, czy i jak istotne jest bezpieczeństwo informacji w działalności organizacji, a także wskazuje, które zasoby (informacyjne, materialne, niematerialne) są szczególnie wrażliwe i ich naruszenie mogłoby spowodować poważne straty 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 i 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. Dla sektora wojskowego odpowiednio Służba Kontrwywiadu Wojskowego a dla sektora prywatnego Agencja Bezpieczeństwa Wewnętrznego.

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.

Identyfikacja potencjalnych zagrożeń i analiza podatności systemu wobec tych zagrożeń stanowią kluczowy etap w tworzeniu skutecznych strategii ochrony systemów komputerowych. 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, umożliwiają dostosowanie strategii ochrony do konkretnych zagrożeń i podatności. Systemy komputerowe mogą mieć różne słabe punkty, dlatego ważne jest, aby strategie ochrony były dostosowane do specyficznych zagrożeń. Dzięki identyfikacji tych 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.

Dodatkowo, analiza podatności systemu zwiększa świadomość zagrożeń w organizacji. Pracownicy stają się bardziej uważni na możliwe ryzyka i zdają sobie sprawę, 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 znacząco przyczyniają się do 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.

5 Klasyfikacja i zawartość metadanych plików cyfrowych

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:

- dla dokumentów Zastrzeżonych - metadane z opisem zawartości są jawne,
- 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. Poniżej lista wymaganych pozycji:

1. Symbol oznaczenia klauzuli tajności (puste – jako jawne, Z, Pf, 0 lub 00)
2. Numer kolejny zapisu (numer pozycji)
3. Adnotacje dot. obowiązywania klauzuli tajności, jej zniesienia albo zmiany
4. Data rejestracji dokumentu
5. Nazwa nadawcy/adresata (lub wpis dokument własny)
6. Numer i data dokumentu otrzymanego
7. Nazwa dokumentu lub czego dotyczy
8. Liczba egzemplarzy wytworzonego dokumentu
9. Liczba stron dokumentu lub innych jednostek miary
10. Liczba załączników
11. Liczba stron wszystkich załączników lub innych jednostek miary
12. Nr dokumentu, z którego wykonano wydruk, kopię, wyciąg, wypis, odpis, tłumaczenie, lub numer nośnika

13. Imię i nazwisko lub inne dane identyfikujące wykonawcę dokumentu
14. Data, imię i nazwisko oraz podpis osoby pobierającej dokument (podpis stosujemy przy papierowej wersji dokumentu, w cyfrowym spisie pozycji zastosować należy oddzielną kartę zapoznania się z dokumentem nr ... dla wszystkich pozycji, nie tylko dla tajnych i ściśle tajnych, których jest to konieczne)
15. Potwierdzenie zwrotu dokumentu (data i podpis) (powiązane z kartą zapoznania się)
16. Adnotacje o wykonaniu dokumentu lub załącznika (pozycja w książce doręczeń przesyłek miejscowych/pozycja wykazu przesyłek nadanych/załącznik do pisma nr …)
17. Adnotacje o wybrakowaniu lub przekazaniu do archiwum
18. Informacje uzupełniające/Uwagi (np. symbol klasyfikacyjny wykazu akt)[14]

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

6 Cykl funkcjonowania chronionego systemu teleinformatycznego

Bezpieczeństwo informacji niejawnych przetwarzanych w systemie teleinformatycznym należy uwzględnić we wszystkich etapach cyklu funkcjonowania tego systemu, które obejmują[15]:

1 **Planowanie** – w tym etapie należy uwzględnić wymagania bezpieczeństwa informacji niejawnych i określić odpowiednie środki ochrony, procedury oraz zasady postępowania. W danym etapie określamy:
   1.1 przeznaczenie systemu teleinformatycznego;
   1.2 maksymalną klauzulę tajności informacji niejawnych, które będą przetwarzane w systemie teleinformatycznym;
   1.3 tryb bezpieczeństwa pracy systemu teleinformatycznego;
   1.4 szacunkową liczbę użytkowników;
   1.5 planowaną lokalizację.

2 **Projektowanie** – przy projektowaniu systemu teleinformatycznego należy uwzględnić aspekty bezpieczeństwa informacji, takie jak kontrola dostępu, szyfrowanie danych, zabezpieczenia sieciowe. W danym etapie:
   2.1 przeprowadza się wstępne szacowanie ryzyka dla bezpieczeństwa informacji niejawnych w celu
      2.1.1 określenia wymagań dla zabezpieczeń;
      2.1.2 dokonuje się wyboru zabezpieczeń dla systemu teleinformatycznego w oparciu o wyniki wstępnego szacowania ryzyka dla bezpieczeństwa informacji niejawnych;
   2.2 uzgadnia się z podmiotem akredytującym plan akredytacji obejmujący zakres i harmonogram przedsięwzięć wymaganych do uzyskania akredytacji bezpieczeństwa teleinformatycznego;

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

2.3 uzgadnia się z podmiotem zaopatrującym w klucze kryptograficzne rodzaj oraz ilość niezbędnych urządzeń lub narzędzi kryptograficznych, a także sposób ich wykorzystania;

2.4 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. W danym etapie:

3.1 pozyskuje i wdraża się urządzenia lub narzędzia realizujące zabezpieczenia w systemie teleinformatycznym;

3.2 przeprowadza się testy bezpieczeństwa systemu teleinformatycznego;

3.3 przeprowadza się szacowanie ryzyka dla bezpieczeństwa informacji niejawnych z uwzględnieniem wprowadzonych zabezpieczeń;

3.4 opracowuje się dokument procedur bezpiecznej eksploatacji oraz uzupełnia dokument szczególnych wymagań bezpieczeństwa;

3.5 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.

7 Wartościowanie bezpieczeństwa informacji

Użytkownicy i kierownictwo instytucji chcąc poznać odpowiedź na pytanie czy systemy teleinformatyczne z których korzystają są bezpieczne i czy dane są odpowiednio chronione powinni przeprowadzić proces oceny bezpieczeństwa teleinformatycznego. W trakcie tej oceny dokładnie badane są potencjalne luki w zabezpieczeniach i zagrożenia. Proces ten obejmuje analizę zabezpieczeń fizycznych, takich jak kontrola dostępu, oraz ocenę środków technicznych, które mają chronić system przed zagrożeniami.

Ochrona informacji dotyczy kompleksowego zagadnienia obejmującego bezpieczeństwo informacyjne. Ten obszar obejmuje wszelkie sposoby przekazywania informacji, w tym także komunikację werbalną. Celem jest zapewnienie bezpiecznej i poufnej transmisji informacji, niezależnie od formy, w jakiej się odbywa.

Bezpieczeństwo teleinformatyczne to ochrona komunikacji za pomocą różnych środków łączności, np. telefony, radiostacje czy sieci komputerowe.

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. Powinien być zdolny do wykrywania i zapobiegania incydentom bezpieczeństwa.

Wartościowanie czy 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, np. Evaluation Assurance Level (EAL) w Common Criteria lub klasy bezpieczeństwa D, C, B, A w TCSEC.

Proces oceny bezpieczeństwa można przeprowadzić wewnętrznie, jeśli organizacja ma odpowiednie kompetencje, lub zlecić zewnętrznemu, niezależnemu zespołowi.

8 Wytyczne zapewnienia bezpieczeństwa informacji

Wyróżniamy dwie grupy standardów z zakresu bezpieczeństwa systemów teleinformatycznych:[16]

1) Standardy umożliwiające certyfikację systemów i produktów teleinformatycznych:
   - ISO 15408 (Common Criteria): Jest to międzynarodowy standard oceny bezpieczeństwa systemów informatycznych. Common Criteria określa ogólne wymagania dotyczące bezpieczeństwa i umożliwia porównywanie i certyfikację systemów informatycznych.[17]
   - ITSEC (Information Technology Security Evaluation Criteria): Był to europejski standard oceny bezpieczeństwa systemów teleinformatycznych. ITSEC zawierał kryteria oceny bezpieczeństwa i zasady testowania systemów, umożliwiając certyfikację.[18]
2) Standardy stanowiące dobre praktyki, nie przeznaczone do bezpośredniej certyfikacji systemów, ale służące jako zbiory zaleceń i wytycznych dotyczących najlepszych praktyk w dziedzinie bezpieczeństwa teleinformatycznego. Przykłady takich standardów to:
   - ISO 27001: Jest to międzynarodowy standard zarządzania bezpieczeństwem informacji. ISO 27001 określa wymagania i procesy zarządzania bezpieczeństwem informacji w organizacji.[19]
   - NIST SP 800-53: Jest to standard opracowany przez National Institute of Standards and Technology (NIST) w Stanach Zjednoczonych. SP 800-53 zawiera zbiór kontroli bezpieczeństwa, które można zastosować do systemów teleinformatycznych.[20]

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

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

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

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

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

- CIS Controls: To zestaw kontroli bezpieczeństwa opracowany przez organizację Center for Internet Security (CIS). CIS Controls stanowią praktyczny framework dla organizacji w celu ochrony systemów przed cyberzagrożeniami.[21]

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 TCSEC, ITSEC i Common Criteria) jest podawanie miar w postaci określonych klas, poziomów lub EAL (Evaluation Assurance Level). Te miary służą do klasyfikacji systemów i produktów pod względem ich poziomu bezpieczeństwa lub stopnia spełnienia określonych wymagań.

W przypadku standardów z grupy drugiej, które stanowią tzw. dobre praktyki (takie 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, te standardy stanowią zbiór zaleceń, wytycznych i 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 z grupy 2 dostarczają zaleceń i wytycznych, ale nie mają konkretnych miar, dla których można przeprowadzić formalną certyfikację.

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

Dla systemów ocenianych zgodnie ze standardami z grupy 2 certyfikatów się nie uzyskuje, ponieważ nie zawierają one 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.

Systematyzacja procesu oceny: Standardy zapewniają strukturę i wytyczne dotyczące oceny bezpieczeństwa systemów teleinformatycznych. Audytorzy mogą korzystać z tych standardów jako ramy referencyjnej do przeprowadzenia oceny i porównania wyników.[22]

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 i jednolitości w ocenie.

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.

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

Standardy również 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.

Jednym z pierwszych znaczących osiągnięć w tym obszarze było opracowanie i wydanie tzw. "Pomarańczowej książki" w 1983 roku. 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.

"Pomarańczowa książka" 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 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 zauważyć, 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 i 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" (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 bardziej powszechnie używanym standardem do oceny bezpieczeństwa systemów teleinformatycznych.

Kryteria oceny COBIT dostarcza wytycznych dotyczących kontroli i zarządzania, ale nie definiuje konkretnych kryteriów oceny bezpieczeństwa. Organizacje mogą dostosować framework COBIT do swoich potrzeb i wymagań, aby stworzyć indywidualne kryteria oceny bezpieczeństwa.

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.

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, znany również jako ISO/IEC 27001, jest normą dotyczącą zarządzania bezpieczeństwem informacji. Określa ona wymagania i wytyczne dotyczące 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 związanych 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 kontroli 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.

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 system, który umożliwia organizacjom skuteczne identyfikowanie, analizowanie i zarządzanie ryzykiem związanym z bezpieczeństwem informacji.

Kryteria oceny według ISO/IEC 15408, znany również jako Common Criteria (Wspólne Kryteria), jest międzynarodowym standardem dotyczącym oceny bezpieczeństwa teleinformatycznego. Obejmuje on kryteria oceny, które są stosowane do oceny bezpieczeństwa różnych produktów i systemów informatycznych. Poniżej przedstawiam główne elementy kryteriów oceny bezpieczeństwa według ISO/IEC 15408:

ISO/IEC 15408 definiuje model oceny, który składa się z trzech podstawowych komponentów:

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

ISO/IEC 15408 wprowadza poziomy oceny zwanymi 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 rygorystyczniejsze wymagania dotyczące bezpieczeństwa.

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

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

ISO/IEC 15408 wymaga kompleksowej dokumentacji dotyczącej oceny bezpieczeństwa, w tym opisu systemu lub produktu, oceny ryzyka, wyników testów, procedur oceny, wyników zabezpieczeń funkcjonalnych i poza funkcjonalnych itp.

Ocena bezpieczeństwa teleinformatycznego według ISO/IEC 15408 może być przeprowadzana przez niezależne organizacje.

9 Audyt systemu bezpieczeństwa 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, czy system bezpieczeństwa informacji spełnia określone standardy i wymagania, identyfikację słabych punktów oraz rekomendacje dotyczące usprawnień i zabezpieczeń.[23]

Podczas audytu systemu bezpieczeństwa informacji mogą być podejmowane następujące działania:

- Analiza dokumentacji i procedur: Audytorzy sprawdzają dokumentację związane z bezpieczeństwem informacji, taką jak polityki bezpieczeństwa, procedury, instrukcje, oceny ryzyka itp. Weryfikowane są zgodność dokumentów z obowiązującymi standardami i najlepszymi praktykami.

- Ocena kontroli dostępu: Sprawdzane są procedury kontroli dostępu do systemu, zarządzanie uprawnieniami użytkowników, autentykacja, uwierzytelnianie, zarządzanie hasłami itp. Celem jest upewnienie się, że tylko uprawnione osoby mają dostęp do systemu i danych.

- 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 itp.

- Testowanie zabezpieczeń technicznych: Wykonywane są testy techniczne, takie jak penetracja sieci, testy podatności, skanowanie bezpieczeństwa itp., aby sprawdzić, czy system jest odporny na ataki zewnętrzne.

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

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

- Szkolenie i świadomość użytkowników: Ocena obejmuje również ocenę programów szkoleniowych dotyczących bezpieczeństwa informacji, świadomości użytkowników oraz przestrzegania polityk bezpieczeństwa przez personel.

Proces audytu systemu bezpieczeństwa informacji składa się z różnych elementów, a jeden z nich to sporządzenie listy audytowej (checklisty) według wybranego standardu. Oto kilka ważnych etapów, które mogą być częścią procesu audytu:

Sporządzenie listy audytowej (checklisty): W zależności od wybranego standardu, audytorzy opracowują listę punktów audytowych, które powinny być sprawdzone. Lista ta obejmuje konkretne wymagania i zalecenia dotyczące bezpieczeństwa informacji.[24]

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".

Dokumentacja i dowody: Podczas audytu audytorzy zbierają dokumentację i dowody potwierdzające spełnienie wymagań bezpieczeństwa informacji. Mogą to być dokumenty, procedury, logi systemowe, raporty z testów itp.

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

Audytorzy oceniają ryzyko związane z niedopełnieniem wymagań bezpieczeństwa informacji. Identyfikowane są słabe punkty, luki w zabezpieczeniach oraz potencjalne zagrożenia.

Audytorzy przeprowadzają 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, czy system bezpieczeństwa informacji jest zgodny z obowiązującymi standardami, regulacjami i politykami. Oceniana jest zgodność zarówno formalna, jak i operacyjna.

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

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.

Celem wewnętrznych audytów bezpieczeństwa systemu jest ocena i monitorowanie skuteczności, integralności i zgodności zasad oraz procedur zabezpieczeń informacji w ramach organizacji. Oto kilka kluczowych celów wewnętrznych audytów bezpieczeństwa systemu:

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 bezpieczeństwa informacji.

Identyfikacja słabych punktów: Audyt ma na celu identyfikację i ocenę potencjalnych luk, słabych punktów i zagrożeń w systemie bezpieczeństwa informacji. Mogą to być nieprawidłowości w procedurach, braki w zabezpieczeniach technicznych, niewłaściwe zarządzanie uprawnieniami itp.

Ocena ryzyka: Audyt bezpieczeństwa systemu może pomóc w ocenie ryzyka związanego z bezpieczeństwem informacji. Identifikuje się obszary, w których ryzyko jest wysokie, oraz proponuje działania mające na celu zminimalizowanie tych ryzyk i wzmocnienie zabezpieczeń.

Monitorowanie skuteczności: Audyt systemu bezpieczeństwa informacji służy do monitorowania skuteczności istniejących zabezpieczeń i procedur. Pozwala na ocenę, czy zabezpieczenia są wystarczające i czy działają zgodnie z oczekiwaniami.

Rekomendacje i usprawnienia: 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.

Wspieranie 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.

Udoskonalanie procesów i procedur: 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 doskonali

10 Reguły bezpiecznej architektury bezpieczeństwa

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

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.

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.

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.

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.

Zgodnie z zaleceniami, należy także systematycznie aktualizować listę uprawnionych użytkowników systemu teleinformatycznego, dbając o przestrzeganie wszelkich zasad i wymagań dotyczących bezpieczeństwa."

Bezpieczeństwo fizyczne systemu

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.

Strefy ochronne powinny być również zabezpieczone poprzez system alarmu pożarowego, zgodnie z obowiązującymi przepisami oraz wytycznymi dokumentacji bezpieczeństwa.

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.

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."

Ochrona elektromagnetyczna

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.

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.

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.

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.

Ustawienia konfiguracyjne systemu oraz urządzeń

W procesie zapewniania bezpieczeństwa i funkcjonalności systemu teleinformatycznego, konfiguracja odgrywa kluczową rolę i powinna 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.

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 powinna być 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

Istotną rolę odgrywa prowadzenie dokumentacji dotyczącej napraw i przeglądów diagnostycznych systemu teleinformatycznego, zgodnie z wytycznymi 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 TI.

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.

Zapobiegania i reagowania 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.

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.

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, jest niezwykle istotne. 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

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.

Ochrona informatycznych nośników danych

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 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

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 BIOS-u 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.

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.

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 TI powinien zastosować automatyczną blokadę dostępu po wyczerpaniu nieudanych prób logowania, zgodnie z dokumentacją bezpieczeństwa.

Informacje ogólnodostępne dla użytkowników systemu TI 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

W celu zapewnienia właściwego poziomu bezpieczeństwa systemu teleinformatycznego (TI), istotne jest wyznaczenie obszarów o wysokim ryzyku, które wymagają regularnych audytów wewnętrznych. Te audyty powinny weryfikować zgodność stanu zabezpieczeń TI z opisem w Szczególnych Wdrażania 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 udokumentowane, a zalecenia poaudytowe 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 TI 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 TI 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 TI 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 TI, takich jak administratorzy i inspektorzy Bezpieczeństwa Technologii Informacyjnej (BTI).

Zarządzania ryzykiem

W celu skutecznego zarządzania ryzykiem w systemie teleinformatycznym (TI), 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 TI. 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 incydentów bezpieczeństwa lub po wykryciu nowych zagrożeń lub podatności, które mogą mieć wpływ na bezpieczeństwo informacji.

Czynniki ryzyka bezpieczeństwa systemu TI 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.

Audyty wewnętrzne systemu TI powinny być przeprowadzane zgodnie z ustalonym harmonogramem i zakresem. Rekomendacje poaudytowe muszą być

systematycznie wdrażane, aby zabezpieczyć system przed potencjalnymi zagrożeniami.

Eksploatacja systemu TI 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 TI jest kluczowe dla efektywnego zarządzania ryzykiem i zapewnienia bezpiecznej pracy w systemie.

Zasady i procedury zarządzania zmianami w systemie teleinformatycznym.

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.

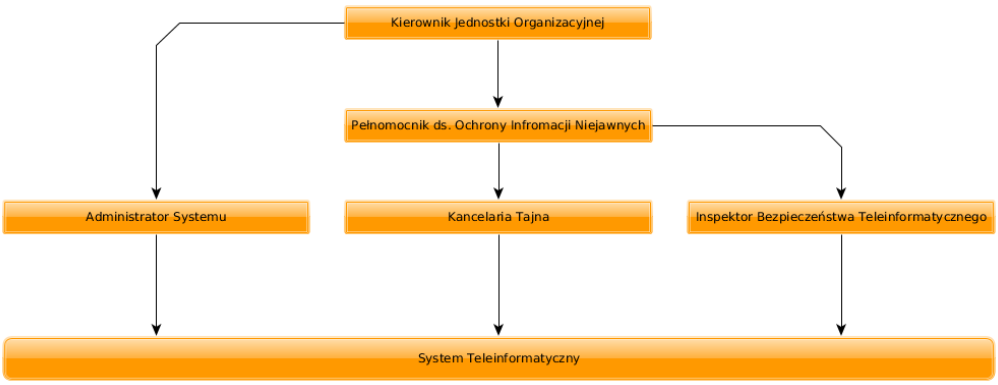
W systemie teleinformatycznym powinny być zdefiniowane szczególne sytuacje, po wystąpieniu których konieczne jest przeprowadzenie ponownej akredytacji bezpieczeństwa. Obejmuje to istotne zmiany w infrastrukturze systemu, kluczowe incydenty bezpieczeństwa oraz pojawienie się nowych zagrożeń, które mogą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

11 Organizacja modelowego ośrodka ochrony

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 gdzie 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.

12 Role i obowiązki personelu ochrony

Skład zespołu

Skład personelu Pionu Ochrony Informacji Niejawnych **nadzorujący** pracę systemu teleinformatycznego:

- **Kierownik Jednostki Organizacyjnej [KJO] –** odpowiada za ochronę informacji niejawnych (organizację i nadzór)
- **Pełnomocnik ds. ochrony informacji niejawnych [POIN] –** odpowiada za przestrzeganie przepisów z OIN (procedury i kontrole)
- **Kierownik Kancelarii Tajnej [KKT] –** odpowiada za rejestrację i obieg informacji niejawnych
- **Administrator Systemu [AS]** – odpowiada za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych w szczególnych wymaganiach bezpieczeństwa oraz procedurach bezpiecznej eksploatacji systemu
- **Inspektor Bezpieczeństwa Teleinformatycznego [IBT]** (systemu teleinformatycznego) – odpowiada za weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji.

Role i zakres odpowiedzialności personelu ochrony

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

- tworzenie odpowiednich warunków organizacyjnych i finansowych w celu zapewnienia właściwego poziomu ochrony, przetwarzanych w systemie teleinformatycznym, informacji niejawnych;
- Powołanie i obsadą 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, szczegółowe obowiązki:

- 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;
- 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 przepustkowego 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 (tj. teleinformatycznego) 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.

- **Inspektora Bezpieczeństwa Teleinformatycznego** odpowiedzialny jest 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 właściwego 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 „teleinformatycznego”, w zakresie wykorzystywania urządzeń i narzędzi służących do ochrony informacji niejawnych;

- prowadzenie kontroli stanu zabezpieczeń systemu „teleinformatycznego”, w tym poprzez analizowanie i archiwizowanie rejestrów zdarzeń w systemie (logów);
- prowadzenie aktualnego wykazu osób mających uprawnienia do dostępu do systemu „teleinformatycznego”;
- prowadzenie kontroli poprawności przydzielania w systemie „teleinformatycznego” kont użytkownikom i zakresu uprawnień nadanych użytkownikom;
- udział w pracy 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;
- przeprowadzanie okresowo testów bezpieczeństwa systemu „teleinformatycznego” 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 „teleinformatycznego”;
- 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 itp.);

- reagowanie na sygnały o incydentach w zakresie bezpieczeństwa, wyjaśnianie ich przyczyn, okresowe przeglądanie i dokumentowanie logów systemowych;
- przeprowadzanie okresowej analizy zagrożeń;
- tworzenie planów awaryjnych i organizowanie treningów w ich realizacji;
- prowadzenie Dziennika Inspektora Bezpieczeństwa Teleinformatycznego, w którym dnotowuje wszystkie zdarzenia mające wpływ na bezpieczeństwo systemu oraz informacje o przeprowadzonych okresowych kontrolach czynności wykonywanych przez administratora systemu.

◦ **Administratora Systemu** – odpowiedzialny jest 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 w Stanowisku Komputerowym - „teleinformatycznego” , 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 „teleinformatycznego";
- 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 „teleinformatycznego”. Wyłączanie kont tych użytkowników, którzy utracili formalne uprawnienia do pracy w systemie „teleinformatycznego” (np. zostali przeniesieni bądź zwolnieni, przebywają na urlopie bezpłatnym itp.) - dotyczy to zwłaszcza osób zatrudnionych na czas określony, na umowę-zlecenie itp.
- przygotowanie i utrzymywanie wykazu osób zapoznanych z Procedurami Bezpiecznej Eksploatacji;
- prowadzenie wyrywkowych kontroli, czy użytkownicy nie mają szerszego dostępu do zasobów systemu niż wynika to z pierwotnie przydzielonych im uprawnień;
- współpraca z użytkownikami systemu „teleinformatycznego” 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: 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** – do obowiązków i odpowiedzialności należy:
  - właściwa organizacja ochrony wszystkich zasobów (technicznych i informacyjnych) wykorzystywanych w systemie „teleinformatycznego”;
  - 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;
  - postępowania w przypadku pożaru i zaistnienia zagrożeń środowiskowych;
  - postępowania w przypadku incydentu w systemie.
  - 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 wyższej niż klauzula wykorzystywanego dysku twardego z systemem operacyjnym;
- przetwarzania 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 POIN.

13 Przydzielenie uprawnień

Dla zapewnienia ochrony informacji niejawnych w systemie teleinformatycznego, dostęp do jego zasobów jest realizowany na podstawie wniosku o przydzielenie uprawnień do wskazanego zasobu systemu teleinformatycznego. Pole „powód działania” powinno zawierać informację o pozycji do której dostęp ma uzyskać Użytkownik. Poniższy wniosek wypełniany od góry do doły przez poszczególne osoby przedstawia schemat przepływu informacji pozwalający na uzyskanie dostępu do systemu.

<table>
<tr><th colspan="4">Wniosek o przydzielenie uprawnień do systemu teleinformatycznego</th></tr>
<tr><td rowspan="8">Wypełnia Kierownik Komórki Organizacyjnej</td><td rowspan="2">Komórka organizacyjna wnioskująca</td><td>.....
(Nazwa komórki organizacyjnej)</td><td rowspan="2">.....
.....
(Data, Podpis Kierownika KO)</td></tr>
<tr><td>.....
(Imię i nazwisko Kierownika KO)</td></tr>
<tr><td>Imię i nazwisko Użytkownika</td><td colspan="2"></td></tr>
<tr><td>Działanie
- niepotrzebne wykreślić</td><td colspan="2">Nadanie/Odebranie uprawnień</td></tr>
<tr><td rowspan="4">Poziom dostępu/klauzula informacji niejawnych
- niepotrzebne wykreślić</td><td colspan="2">ZASTRZEŻONE</td></tr>
<tr><td colspan="2">POUFNE</td></tr>
<tr><td colspan="2">TAJNE</td></tr>
<tr><td colspan="2">ŚCIŚLE TAJNE</td></tr>
<tr><td>Powód działania</td><td colspan="2"></td></tr>
<tr><td>Planowana data zakończenia prac</td><td colspan="2">……..
(Data)</td></tr>
<tr><td rowspan="3">Wypełnia Pełnomocnik Ochrony</td><td rowspan="3">Poświadczenie bezpieczeństwa osobowego upoważniające do dostępu do informacji niejawnych</td><td>……
(Klauzula)</td><td rowspan="3">Oświadczam, że Użytkownik posiada poświadczenie bezpieczeństwa osobowego oraz szkolenie z zakresu ochrony informacji niejawnych upoważniające do dostępu do informacji niejawnych o wnioskowanej klauzuli.</td></tr>
<tr><td>……
(Numer)</td></tr>
<tr><td>……
(Ważne do)</td></tr>
</table>

Informacji Niejawnych	*Zaświadczenie o odbyciu szkolenia z zakresu ochrony informacji niejawnych*	…… (Numer)	…… (Data, Podpis POIN)
Wypełnia	Akceptacja	…… (Data, Podpis KJO)	
Wypełnia	Oświadczenia	Oświadczam, że zostałem przeszkolony przez Administratora systemu w zakresie bezpieczeństwa teleinformatycznego oraz zostałem zapoznany z dokumentem *„Procedury Bezpiecznej Eksploatacji dla systemu „teleinformatycznego”*, w zakresie dotyczącym użytkowników systemu i zrozumiałem zasady bezpiecznego przetwarzania informacji niejawnych w systemie teleinformatycznym. …… (Data, Podpis Użytkownika)	
Wypełnia	Potwierdzenie działań w systemie	…… (Data, Podpis Administratora)	

Tabela 1: Wniosek o przydzielenie uprawnień do systemu teleinformatycznego

ROZDZIAŁ 2
Ocena poziomu bezpieczeństwa informacji w świetle własnych badań

„Bezpieczeństwo to rzecz względna. Możesz dopłynąć tak blisko brzegu, że prawie czujesz grunt pod nogami, po czym nagle roztrzaskujesz się na skałach.”

Jodi Picoult, Tam gdzie ty

1 Zagadnienia definicyjne

W rozdziale drugim przyjęto następującą terminologię:

Analiza ryzyka - proces identyfikacji ryzyk, określenia ich wielkości i identyfikowania obszarów, które mogą być objęte skutkami wystąpienia zagrożenia.

Dostępność - właściwość określająca, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym.

Informowanie o ryzyku - powiadamianie o pojawiającym się ryzyku osób odpowiedzialnych za zarządzanie ryzykiem.

Integralność - właściwość określająca, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony.

Monitorowanie ryzyka - proces ciągłego przeglądu ryzyk powstałych w skutek użytkowania systemu teleinformatycznego oraz dostosowywania zabezpieczeń do nowo powstałych ryzyk w celu utrzymania ryzyk szczątkowych na akceptowalnym poziomie.

Podatność - słabość zasobu lub zabezpieczenia systemu teleinformatycznego, która może zostać wykorzystana przez zagrożenie.

Poufność - właściwość zapewniająca, że informacja nie jest ujawniana nieuprawnionym do tego podmiotom.

Przetwarzanie informacji niejawnych - wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie.

Ryzyko - ryzyko dla bezpieczeństwa informacji niejawnych, kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji.

Ryzyko szczątkowe - ryzyko pozostające po procesie postępowania z ryzykiem, podlegające procesowi akceptacji ryzyka.

System teleinformatyczny – jest to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych.[25]

Szacowanie ryzyka - w rozumieniu Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych - całościowy proces analizy i oceny ryzyka.

[25]Art. 2 pkt 3 Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1204, z późniejszymi zmianami.

Właściciel ryzyka - osoba (podmiot) odpowiedzialna za utrzymanie zabezpieczeń obniżających ryzyko do poziomu akceptowalnego.

Zabezpieczenia - środki o charakterze fizycznym, technicznym lub organizacyjnym zmniejszające ryzyko.

Zagrożenie - potencjalna przyczyna niepożądanego zdarzenia, które może wywołać szkodę w zasobach systemu teleinformatycznego.

Zarządzanie ryzykiem - skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji, z uwzględnieniem ryzyka.

Zasoby systemu teleinformatycznego - informacje przetwarzane w systemie, jak również osoby, usługi, oprogramowanie, dane i sprzęt oraz inne elementy mające wpływ na bezpieczeństwo tych informacji.

2 Środowisko bezpieczeństwa

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.

3 Identyfikacja i oszacowanie wartości informacji przetwarzanych w systemie

Identyfikacja informacji polega na określeniu ich charakterystyki, lokalizacji, sposobu przetwarzania oraz ewentualnych oznaczeń.

Rodzaje poufnych informacji jakie są przetwarzane w systemie teleinformatycznym ustala kierownik jednostki organizacyjnej. Wszystkie zasoby informacyjne, które są przetwarzane w systemie, należy sklasyfikować według ich rodzaju i miejsca przetwarzania. W ramach każdej grupy informacji, należy także dokonać podziału na kategorie zgodnie z klauzulami niejawności, którymi są oznaczone.

Zespół odpowiedzialny za analizę ryzyka ma obowiązek identyfikować wszystkie klauzule dotyczące poufnych informacji przetwarzanych w systemie TI oraz dokładnie rozumieć, jak te informacje wpływają na wykonywane przez jednostkę organizacyjną zadania. Zakres dokonanych ustaleń powinien być precyzyjnie dostosowany do zakresu analizy ryzyka, który został określony.

Efektem pracy zespołu będzie utworzenie listy zasobów informacyjnych, uporządkowanych według ich rodzaju oraz klauzuli tajności. Każda z tych kategorii zostanie opisana za pomocą unikalnego zestawu wymagań dotyczących funkcjonowania i zabezpieczeń, które będą obejmować aspekty związane z integralnością, poufnością i dostępnością.

Zgodnie z artykułem 6.1 Ustawy o Ochronie Informacji Niejawnych (UOIN), właścicielem informacji niejawnych jest osoba, która posiada upoważnienie do podpisywania dokumentu. Ta osoba, poprzez nadanie klauzuli tajności danej informacji niejawnej, określa jej poziom wrażliwości (dotyczący atrybutu

"poufność"). Jednocześnie określa także potencjalne konsekwencje nieuprawnionego ujawnienia tej informacji, które są mierzone na podstawie szkód mogących wystąpić zarówno dla jednostki organizacyjnej, jak i państwa, zgodnie z artykułem 5 UOIN.

Wartość informacji niejawnych przetwarzanych w systemach TI może być oszacowana poprzez przeprowadzenie rozmowy z właścicielem tych informacji lub innymi osobami, które posiadają autorytet w kwestii oceny tych informacji.

Wartość informacji może być oszacowana za pomocą metody jakościowej, wykorzystując kilku stopniową skalę wartości, gdzie informacja może zostać sklasyfikowana jako niska, średnia lub wysoka. Przy tym podejściu bierze się pod uwagę zarówno straty bezpośrednie, jak i pośrednie, które mogą wyniknąć dla jednostki organizacyjnej lub państwa w przypadku nieuprawnionego ujawnienia, utraty, modyfikacji lub braku dostępu do danej informacji niejawnej.

Proces identyfikacji informacji niejawnych powinien finalizować się stworzeniem spisu tych informacji, który jest strukturalnie uporządkowany zgodnie z hierarchią ich ważności oraz oszacowanymi skutkami nieuprawnionego ujawnienia, utraty, modyfikacji lub braku dostępu do nich. Następnie taki wykaz informacji niejawnych powinien być poddany zatwierdzeniu przez kierownika jednostki organizacyjnej.

4 Identyfikacja i oszacowanie wartości zasobów system

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 TI, które mają istotne znaczenie dla zapewnienia ochrony przetwarzanych w nim informacji poufnych.

Proces identyfikacji zasobów systemu TI, 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 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.

5 Identyfikacja zagrożeń i określenie ich poziomu

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.

6 Identyfikacja podatności na ryzyka, określenie ich poziomu

Zespół analizy ryzyka ma także za zadanie opracować listę potencjalnych słabych punktów (czyli podatności) systemu TI. Ta lista powinna być uporządkowana według prawdopodobieństwa ich wykorzystania przez wcześniej zidentyfikowane zagrożenia, które mogą występować w środowisku eksploatacji systemu. Jest to kluczowy krok, 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 TI.

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 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, na przykład:

- Mogą wynikać z luk w ochronie fizycznej systemu TI, co oznacza niedostateczne zabezpieczenia dostępu do sprzętu i infrastruktury.
- Mogą wynikać z niewłaściwych rozwiązań organizacyjnych, takich jak błędy w zarządzaniu bezpieczeństwem informacji.
- Mogą być spowodowane brakami lub lukami w procedurach dotyczących bezpiecznej eksploatacji systemu.
- Mogą wynikać z braku odpowiedniego szkolenia personelu, co prowadzi do nieświadomych naruszeń zasad bezpieczeństwa.

- 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: Jest 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, katastrofy naturalne itp.

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 często 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.

7 Identyfikacja i oszacowanie ryzyka

Zespół analizy ryzyka, aby ocenić prawdopodobieństwo wystąpienia konkretnego zagrożenia związanego z daną podatnością systemu TI, 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 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.

8 Badanie opinii interesariuszy ochrony informacji niejawnych

Cele badawcze poprzez badanie opinii kluczowych interesariuszy w zakresie ochrony informacji niejawnych obejmowało:

Weryfikację i wkład empiryczny oparty na obserwacjach w celu potwierdzenia lub poprawienia obecnej wiedzy w dziedzinie ochrony informacji niejawnych.

Weryfikację zrozumienia perspektywy i doświadczeń użytkowników w zakresie ochrony informacji niejawnych pozwalających na identyfikację kluczowych obszarów ryzyka oraz potrzeb, co skutecznie może wpłynąć na doskonalenie strategii i działań ochronnych, poprawiając ogólną skuteczność ochrony informacji niejawnych.

Identyfikację Potrzeb oraz Problemów/Wyzwań Interesariuszy.

Badanie tezy : ***Zastosowanie zbyt złożonych metod oceny bezpieczeństwa systemów, skoncentrowanych na etapie akredytacji, może prowadzić do obniżenia ich poziomu bezpieczeństwa, zgodnie z normami i zaleceniami branżowymi.***

W ramach pracy badawczej zbadano przytoczoną tezę. Obejmuje ona kilka kwestii:

Potrzebę oceny bezpieczeństwa, krytykę istniejących metod, ryzyko związane z akredytacją, ryzyko braku systematyczności wynikającej ze złożoności metod. Zidentyfikowanie potrzeb, problemów, wyzwań oraz obszarów ryzyka związanych z ochroną informacji niejawnych. Analizę Zagrożeń, Pain-Points i Kierunków Zmian.

Ocena zagrożeń dla bezpieczeństwa informacji niejawnych, identyfikacja obszarów, które sprawiają największe trudności (pain-points), oraz zarysowanie potencjalnych kierunków zmian w celu ich rozwiązania.

Ogląd w Perspektywę Użytkowników poprzez zrozumienie perspektywy, opinii i doświadczeń użytkowników w kontekście ochrony informacji niejawnych, aby uwzględnić ich potrzeby i opinie w procesie doskonalenia działań ochronnych.

Poprzez powyższe cele badawcze, możemy wzbogacić wiedzę na temat ochrony informacji niejawnych oraz lepiej dostosować strategie i działania do realnych potrzeb i wyzwań.

Wybrana metoda badawcza to IDI z podejściem jakościowym. Możliwość pogłębienia wypowiedzi i zadawania dodatkowych uzupełniających pytań, ze względu na naturę tematu nie można zastosować podejścia ilościowego. Grupa interesariuszy nie jest szeroka i trudno dostępna.

Poszczególni uczestnicy mieli możliwość udzielenia swoich opinii w sposób pełniejszy i bardziej szczegółowy, co wpłynęło na jakość zebranych danych.

Anonimowość i prywatność zostały zapewnione w trakcie indywidualnych wywiadów, co sprawiło, 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.

Grupa docelowa badania obejmowała Audytorów Akredytujących oraz pracowników Pionu Ochrony Informacji Niejawnych, w tym:

- Kierownicy Jednostek Organizacyjnych (KJO)
- ASN – Administratorzy Systemów Niejawnych
- POIN – Pełnomocnicy ds. Ochrony Informacji Niejawnych
- IBT – Inspektorzy Bezpieczeństwa Teleinformatycznego
- Kierownicy Kancelarii Tajnych Narodowych oraz Międzynarodowych

- Kierownicy Kancelarii Kryptograficznych NATO oraz UE

Łącznie przeprowadzono 32 wywiady.

Scenariusz wywiadu obejmował weryfikację hipotez i realizację celów badania gdzie wykorzystano poniższe pytania:

Perspektywa						
KJO	POIN	ASN	IBN	Użytkownik	Audytor	Kierownik KT/ KTM Kierownik KK UE/NATO
Jakie są wykorzystywane metody oceny bezpieczeństwa systemów niejawnych?						
Metody oceny ryzyka, testy penetracyjne i ocena zgodności z regulacjami.	Ocena zgodności z regulacjami prawnymi. Testy fizyczne zabezpieczeń. Audyt ochrony informacji niejawnych. Analiza ryzyka związanego z dostępem i przetwarzaniem informacji niejawnyc	Testy ustawień zabezpieczeń oraz testy penetracyjne. Testy wirusów i złośliwego oprogramowania. Audyt bezpieczeństwa, testy penetracyjne, monitorowanie zdarzeń (SIEM).	Monitorowanie zdarzeń i reagowanie na incydenty. Audyt systemów i infrastruktury pod kątem zgodności z politykami bezpieczeństwa. Analiza incydentów bezpieczeństwa i wniosków z nich płynących. Testy	Edukacja w zakresie cyberbezpieczeństwa, monitorowanie ruchu sieciowego, regularna aktualizacja systemów.	Poprzez ocenę dokumentacji bezpieczeństwa, politykę ochrony, audyt deklarowanych środków ochrony. Metody sugerowane w wydawanych zaleceniach dla personelu ochrony. Metody bazujące na ISO 27k. Audyt bezpieczeństwa, ocena zgodności z regulacjami, analiza zdarzeń.	Ocena zgodności z regulacjami prawnymi. Monitorowanie dostępu i przepływu dokumentów. Kontrola poufności dokumentów. Sprawdzanie zgodności z politykami dotyczącymi dokumentów.

	h. Monitorowanie i kontrola dostępu do informacji niejawnych.		penetracyjne w celu identyfikacji luk w zabezpieczeniach.			
Jakie są zalety stosowania analizy ryzyka i oceny podatności systemów?						
Poprawa priorytetyzacji działań związanych z bezpieczeństwem. Zminimalizowanie ryzyka dla firmy i ochrona reputacji. Zgodność z przepisami, co chroni firmę przed konsekwencjami prawno-finansowymi. Optymalizacja alokacji zasobów w celu minimalizacji ryzyka. Ułatwienie podejmowania świadomych	Zwiększenie świadomości organizacyjnej na temat ryzyka i sposobów jego zarządzania. Zminimalizowanie nieoczekiwanych incydentów i strat finansowych. Identyfikacja i ocena ryzyka związanego z utratą poufności,	Poprawa priorytetyzacji działań związanych z bezpieczeństwem. Identyfikacja potencjalnych zagrożeń i ich wpływu na organizację. Pomoc w identyfikacji i priorytetyzacji zagrożeń. Ułatwienie dostosowania działań do konkretnyc	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.	Pozwala na zrozumienie potencjalnych zagrożeń i odpowiednie zachowanie.	Pomoże w identyfikacji i ocenie potencjalnych zagrożeń. Ułatwi dostosowanie działań do rzeczywistych zagrożeń.	Identyfikacja potencjalnych zagrożeń związanych z bezpieczeństwem dokumentów. Ułatwienie wdrożenia odpowiednich kontroli i zabezpieczeń. Minimalizacja ryzyka utraty, ujawnienia lub manipulacji dokumentami.

decyzji dotyczących inwestycji w bezpieczeństwo. Umocnienie zaufania klientów i partnerów biznesowych poprzez właściwe zarządzanie ryzykiem.	integralności i dostępności informacji niejawnych. Skuteczne wdrożenie środków ochrony informacji niejawnych. Zgodność z obowiązującymi przepisami i dotyczącymi ochrony informacji niejawnych.	h ryzyk.				
Jakie korzyści przynosi stosowanie tych metod w organizacji?						
Zwiększenie poziomu ochrony przed zagrożeniami. Wzrost zaufania klientów i partnerów biznesowych. Optymalne	Minimalizacja ryzyka ujawnienia informacji niejawnych. Zgodność z regulacjami dotyczący	Wzrost poziomu bezpieczeństwa i zmniejszenie ryzyka ataków. Skuteczne reagowanie na incydenty i szybkie zamykanie	Wzrost poziomu ochrony systemów i danych. Skuteczniejsze reagowanie na incydenty bezpieczeństwa. Spójność i	Zwiększenie świadomości w zakresie bezpieczeństwa. Zminimalizowanie ryzyka	Wzrost zgodności z regulacjami i wymaganiami branżowymi. Zminimalizowanie ryzyka i zapewnienie odpowiedniego poziomu bezpieczeństwa.	Wzrost ochrony poufności i integralności dokumentów. Skuteczniejsze reagowanie na sytuacje, w których bezpieczeństwo dokumentów może być zagrożone. Zgodność działań z politykami i wymaganiami

wykorzystanie zasobów firmy.	mi ochrony informacji niejawnych. Ulepszenie reputacji organizacji jako rzetelnego opiekuna informacji niejawnych.	luk w zabezpieczeniach.	zgodność działań z politykami bezpieczeństwa.			dotyczącymi dokumentacji.
Czy używasz dostępnych narzędzi do przeprowadzania analizy ryzyka i oceny podatności systemów?						
Realizowane przez POIN	Nie używam zautomatyzowanych systemów.	Narzędzia takie jak Nessus, OpenVAS, SIEM (Security Information and Event Management).	Odnośnie podatności systemów:. Narzędzia do skanowania podatności systemów, np. Nessus, OpenVAS. Narzędzia do monitorowania zdarzeń bezpieczeństwa, np. SIEM.	-	Narzędzia takie jak ISO 31000, FAIR, CRAMM.	
Jakie są główne minusy obecnie stosowanych metod oceny bezpieczeństwa?						
Wysokie koszty implementacji i utrzymania	Wysoki koszt wdrożenia i utrzymani	Wysoki koszt implementacji i utrzymania	Wysoki koszt implementacji i utrzymania	-	Wysoki koszt implementacji i utrzymania niektórych zaawansowanych	Wysoki koszt implementacji i utrzymania niektórych zaawansowanych

niektórych zaawansowanych metod. Możliwość nadmiernego skupienia się na jednym rodzaju zagrożenia kosztem innych. Czasochłonność niektórych metod, szczególnie przy dużych systemach i infrastrukturze.	a niektórych zaawansowanych narzędzi ochrony informacji niejawnych. Możliwość generowania fałszywie pozytywnych lub negatywnych wyników, co wpływa na skuteczność oceny ryzyka związanego z informacjami niejawnymi.	niektórych zaawansowanych metod. Możliwość generowania fałszywie pozytywnych lub negatywnych wyników.	niektórych zaawansowanych narzędzi.		metod. Możliwość nadmiernego skupienia się na jednym rodzaju zagrożenia kosztem innych.	narzędzi do zarządzania dokumentami.
W jaki sposób obecnie identyfikowane są ewentualne luki w systemie bezpieczeństwa?						
Luki są identyfikowane poprzez regularne audyty wewnętrzne i zewnętrzne,	Poprzez regularne kontrole, audyty oraz współpracę z	Dzięki regularnym testom penetracyjnym, monitorowaniu logów	Poprzez monitorowanie sieci, audyty bezpieczeństwa i raportowan	Z mojego punktu widzenia, luki są identyfikowane przez specjalistów IT	Przez przeglądy dokumentacji, audyty systemów oraz testy zgodności z ustalonymi procedurami.	Poprzez uważne monitorowanie i kontrolę procesów obiegu dokumentów oraz audyty wewnętrzne.

monitorowanie operacji oraz wykorzystanie systemów wykrywania włamań.	zewnętrznymi ekspertami i agencjami.	systemowych oraz korzyściom z narzędzi bezpieczeństwa.	ie przez użytkowników.	oraz powiadomienia systemowe.		
Czy istnieją ograniczenia lub wyzwania związane z implementacją nowych metod oceny bezpieczeństwa w organizacji?						
Tak, głównym wyzwaniem jest koszt i czas potrzebny na wdrożenie oraz konieczność przeszkolenia personelu.	Ograniczenia prawne i administracyjne mogą utrudniać szybkie wdrożenie nowych metod.	Główne wyzwania to złożoność nowych metod oraz potrzeba dostosowania istniejącej infrastruktury.	Wyzwania obejmują techniczną złożoność oraz potrzebę integrowania nowych metod z istniejącą infrastrukturą.	Wydaje się, że główne wyzwania to skomplikowane procedury oraz dodatkowe obowiązki dla użytkowników.	Brak ograniczeń. Jedynym wymogiem jest przeprowadzenie rzetelnego procesu oraz udokumentowanie go w taki sposób, aby mógł zostać poddany przeglądowi i akceptacji przez audytorów akredytujących.	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?						
Liczymy na zminimalizowanie ryzyka, zwiększenie efektywności monitoringu oraz lepsze dostosowanie do zmieniających się zagrożeń.	Oczekujemy lepszej identyfikacji zagrożeń oraz pełniejszej zgodności z przepisami i regulacja	Oczekujemy lepszej detekcji zagrożeń oraz bardziej efektywnej reakcji na incydenty.	Oczekujemy wyższej dokładności w identyfikowaniu zagrożeń oraz lepszego zarządzania ryzykiem.	Oczekuję większego bezpieczeństwa i mniejszej liczby zakłóceń w pracy.	Oczekuję większej precyzji w wykrywaniu luk i bardziej efektywnej automatyzacji procesów audytów.	Oczekuję lepszego śledzenia obiegu dokumentów i większej kontroli nad dostępem do informacji niejawnych.

	mi.					
Czy istnieją przypadki, w których aktualnie stosowane metody oceny bezpieczeństwa okazały się nieskuteczne?						
Zdarzały się przypadki niewykrycia nowych typów zagrożeń, co wskazuje na potrzebę ciągłego doskonalenia metod.	Tak, w niektórych przypadkach nie zdołano wykryć wyrafinowanych ataków socjotechnicznych.	Zdarzały się incydenty spowodowane przez zaawansowane ataki, które nie zostały wykryte na czas.	Tak, zdarzały się przypadki niewykrycia zaawansowanych ataków APT (Advanced Persistent Threat).	Nie mam bezpośredniego wglądu, ale wiem, że były incydenty, które wymagały interwencji.	Tak, przypadki naruszeń i incydentów bezpieczeństwa wskazują na niedoskonałości obecnych metod.	Zdarzały się przypadki nieautoryzowanego dostępu do dokumentów, co wskazuje na potrzebę doskonalenia metod.
Jakie są główne atuty obecnych praktyk w obszarze oceny bezpieczeństwa?						
Skuteczność w większości przypadków, zgodność z normami międzynarodowymi oraz systematyczność działań.	Zgodność z prawem, systematyczność oraz wsparcie zewnętrznych instytucji.	Dojrzałość metod, ich zgodność z branżowymi standardami oraz dość wysoka skuteczność.	Solidność, zgodność z regulacjami i wieloletnie doświadczenie w ich stosowaniu.	Pewność, że systemy są regularnie monitorowane i audytowane.	Dojrzałość procedur oraz ich zgodność z uznanymi standardami branżowymi.	Systematyczność i strukturalność procesów obiegu dokumentów.
Jakie kroki podejmowane są w obecnych metodach w celu zapewnienia ciągłej poprawy i aktualizacji procedur związanych z bezpieczeństwem?						
Regularne przeglądy polityk bezpieczeństwa, szkolenia dla personelu oraz korzystanie z	Regularne szkolenia, aktualizacje dokumentów oraz ciągła współpraca z	Aktualizacje systemów, regularne szkolenia oraz audyty wewnętrzne i	Regularne przeglądy i audyty, konsultacje z ekspertami zewnętrznymi oraz wprowadz	Szkolenia dla użytkowników, regularne aktualizacje oprogramowania i zabezpieczeń.	Przeglądy okresowe, weryfikacje zgodności z normami oraz integracja z nowymi narzędziami audytowymi.	Regularne szkolenia pracowników, aktualizacje procedur oraz integracja z systemami monitoringu.

najnowszych technologii bezpieczeństwa.	profesjonalistami ds. bezpieczeństwa.	zewnętrzne.	anie nowych technologii.			

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

1. **Wysoki koszt implementacji i utrzymania:**

   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 hipotezę dotyczącą

2. **Możliwość generowania fałszywie pozytywnych lub negatywnych wyników**

   Wszyscy 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:**

   Uczestnicy 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:**

- Wszyscy uczestnicy podkreślają ryzyko nadmiernego skoncentrowania się na jednym rodzaju zagrożenia (np. cyberataki) kosztem innych aspektów bezpieczeństwa, takich jak zagrożenia fizyczne czy ludzkie.

5. **Wymagana specjalistyczna wiedza 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.

9 Negatywne aspekty złożoności metod ochrony informacji

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

1. 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.

2. 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.

3. 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.

4. 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.

5. 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 analiza ISO 15408 pod kątem wcześniej wspomnianych pięciu przyczyn:

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

ROZDZIAŁ 3

Proponowana metoda oceny bezpieczeństwa

„Prostota jest szczytem wysublimowania.”

Leonardo da Vinci

1 Ogólne problemy metodologiczne oceny poziomu ochrony

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).[26]

Specyfika ochrony systemów teleinformatycznych przetwarzających informacje wrażliwe wymaga ochrony fizycznych składników systemu jak i wartości niematerialnych takich jak prawa własności intelektualnej, umowy, bazy danych, wiedzę pracowników, reputację jednostki organizacyjnej.

[26]Prusak Rafał, Kardas Edyta, Zarządzanie ryzykiem bezpieczeństwa informacji w świetle wymagań normatywnych

Elementy niematerialne są trudne do wyrażenia w konkretnych wartościach liczbowych, dlatego istotne jest zastosowanie różnorodnych metod oceny, obejmujących zarówno podejście ilościowe, jak i jakościowe, aby właściwie zrozumieć i wycenić te aktywa.

Dzięki podejściu "dziel i zwyciężaj" poprzez dekompozycję na podsystemy i ich międzysystemowe połączenia, ocena ryzyka w dużych i złożonych systemach może być bardziej efektywna i zrozumiała. Poprzez podzielenie dużego systemu na mniejsze części, można skoncentrować się na ocenie poziomu bezpieczeństwa dla poszczególnych podsystemów, co ułatwia identyfikację i zarządzanie ryzykiem.

Ocenę ryzyka możemy zrealizować przy pomocy tabeli:

Odpowiedzialność	Zasób	Zagrożenie	Przeciwdziałanie	Wpływ na	Podatność	Skutek	Poziom ryzyka
	1			Poufność/ Integralność/ Dostępność			
	2						
	…						
	n						

Tabela 2: Ocena Ryzyka

W macierzy, poszczególne rzędy reprezentują zasoby systemu, które podlegają ochronie, natomiast kolumny obrazują: właściciela danego ryzyka, zidentyfikowane zagrożenie, przeciwdziałanie zagrożeniu, wpływ na - cecha (poufność, dostępność, integralność) na jaką wpływa zagrożenie, poziom podatności, poziom skutku oraz wynikający z całej oceny poziom ryzyka.

Istotną zaletą jest możliwość cyklicznego powtarzania i przeglądu ryzyk bez nadmiernego nakładu pracy a jednocześnie dający wysoki poziom bezpieczeństwa.

Proponowana metoda oceny poziomu bezpieczeństwa systemu, bazująca na przedstawionej macierzy, prezentuje bardziej swobodne podejście do oceny ryzyka. Pomimo tego korzysta z tych samych zasad i procesów co większość powszechnych

metod. Proces ilustruje etapy analizy ryzyka i może stanowić praktyczne narzędzie do oceny poziomu bezpieczeństwa systemu.

Ocena poziomów zagrożeń, poziomów podatności oraz poziomów ryzyka może być z powodzeniem przeprowadzona metodą ekspercką, która łączy aspekty ilościowe i jakościowe, opierając się na poziomie wymagań dotyczących bezpieczeństwa, związanym z ochroną poufności, integralności i dostępności informacji.

Ocena poziomu bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym powinna być realizowana w ramach następujących procesów postępowania z ryzykiem:

a) Wstępnego szacowania.

b) Postępowania w przypadku zmiany wartości ryzyk.

c) Akceptacji ryzyk.

d) Monitorowania ryzyk.

W procesie określania ryzyk dla bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym, należy zidentyfikować:

- Zagrożenia systemu teleinformatycznego.
- Podatności systemu na te zagrożenia.
- Potencjalne skutki wystąpienia incydentu bezpieczeństwa teleinformatycznego.
- Środki zabezpieczające wdrożone w odniesieniu do poufności, integralności i dostępności przetwarzanych w systemie informacji niejawnych.

W ramach oceny bezpieczeństwa systemu teleinformatycznego istotne jest dokładne oszacowanie poziomów zagrożeń i podatności związanych z systemem. Należy również rozpoznać i ocenić zagrożenia oraz podatności wynikające z zastosowania środków zabezpieczających. Oszacowanie poziomów ryzyka

związanych z bezpieczeństwem informacji niejawnych przetwarzanych w systemie jest kluczowe. Przypisanie właścicieli poszczególnych ryzyk, którzy będą odpowiedzialni za akceptację określonych poziomów ryzyk jako akceptowalnych, jest ważnym krokiem. Należy określić wymagania bezpieczeństwa w kontekście ryzyka oraz pogrupować ryzyka w określone kategorie ryzyk szczątkowych. Należy również ustalić akceptowalny poziom ryzyka w jednostce organizacyjnej.

Ocena ryzyka bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym jest kluczowa w szeregu sytuacji. Przede wszystkim, powinna być przeprowadzana przed podjęciem decyzji o implementacji środków zabezpieczających w systemie. Dodatkowo, powinna być dokonana przed wprowadzeniem jakichkolwiek zmian w systemie. Konieczne jest także przeprowadzenie oceny po wykryciu nowych zagrożeń dla bezpieczeństwa informacji niejawnych w systemie teleinformatycznym lub identyfikacji nowych podatności systemu na określone zagrożenia, które nie zostały uwzględnione podczas wcześniejszej oceny bezpieczeństwa. W przypadku zaistnienia istotnego incydentu bezpieczeństwa teleinformatycznego w systemie teleinformatycznym, konieczne jest podjęcie oceny ryzyka. Podobnie, gdy ulegnie zmianie lub zostanie rozszerzone przeznaczenie, zadania lub funkcjonalność systemu teleinformatycznego, istotne jest ponowne oszacowanie ryzyka. Należy także regularnie, co najmniej dwa razy w roku, przeprowadzać ocenę ryzyka w ramach procesu zarządzania ryzykiem w systemie teleinformatycznym.

Zarządzanie ryzykiem w ramach ochrony informacji niejawnych w systemie teleinformatycznym powinno być realizowane w sposób ciągły, dążąc do zapewnienia odpowiedniego poziomu bezpieczeństwa informacji w tym systemie. Ma to na celu także dostosowanie zabezpieczeń systemu do zidentyfikowanych zagrożeń oraz spełnienie konkretnych potrzeb. Ważne jest również szybkie reagowanie i wprowadzanie zmian w systemach zabezpieczeń, zwłaszcza w odpowiedzi na nowe zagrożenia i zidentyfikowane podatności w systemie. Kolejnym istotnym aspektem jest pozyskiwanie informacji dotyczących skuteczności stosowanych środków zabezpieczających.

2 Otoczenie systemu – środowisko bezpieczeństwa

System Teleinformatyczny powinien zostać odpowiednio skonfigurowany w jednostce organizacyjnej, aby umożliwić przetwarzanie informacji niejawnych o klauzuli do ŚCIŚLE TAJNE, NATO COSMIC TOP SECRET oraz TRÈS SECRET UE/ EU TOP SECRET. Przejść proces utwardzania systemu. W ramach systemu teleinformatycznego przetwarzane będą zarówno informacje niejawne własne, jak i przyjęte od jednostek organizacyjnych współpracujących. Konieczne jest precyzyjne określenie lokalizacji systemu teleinformatycznego, uwzględniając adres, kondygnację i usytuowanie względem ulic. Należy dokładnie sprawdzić, czy pomieszczenie, w którym zainstalowano system, spełnia określone standardy dotyczące strefy ochrony elektromagnetycznej, i posiada wymagany certyfikat potwierdzający zgodność. Zestaw komputerowy, w skład którego wchodzą stacja robocza, różne dyski twarde z różnym poziomem klauzul poufności, monitor LCD, klawiatura, mysz, drukarka i skaner, powinien być starannie skompletowany. Dane wejściowe należy wprowadzać do Systemu teleinformatycznego za pośrednictwem klawiatury zestawu komputerowego, nośników danych typu CD i DVD oraz przenośnych nośników, takich jak pendrive. Dane wyjściowe należy wyprowadzać w postaci informacji wyświetlanych na ekranie LCD, wydruków wykonywanych na drukarce oraz danych zapisanych na płytach CD i DVD. W Systemie teleinformatycznego zastosowano wyjmowane dyski twarde, które zostały zarejestrowane zgodnie z określonym poziomem klauzul w Kancelarii Tajnej oraz Kancelarii Tajnej Międzynarodowej. Przyjęto wielopoziomowy tryb bezpieczeństwa pracy, ograniczając dostęp użytkowników do informacji niejawnych zgodnie z zasadą wiedzy niezbędnej. Kontrola dostępu opiera się na uznaniowej zasadzie, a uprawnienia są przydzielane przez Kierownika Kancelarii Tajnej. Wszyscy użytkownicy Systemu teleinformatycznego muszą przejść odpowiednie szkolenia w zakresie ochrony informacji niejawnych oraz procedur

bezpiecznej eksploatacji. Szczegółowe informacje dotyczące środków zabezpieczających i procedur bezpiecznej eksploatacji są zawarte w dokumentacji bezpieczeństwa teleinformatycznego - Szczególnych Wymaganiach Bezpieczeństwa oraz Procedurach Bezpiecznej Eksploatacji systemu teleinformatycznego."

3 Otoczenie systemu – kontekst bezpieczeństwa

Z analizy otoczenia systemu, jego środowiska, w jakim się znajduje wynika, że kontekst oceny bezpieczeństwa powinien obejmować następujące aspekty:

- jakiego poziomu informacje będą przetwarzane w systemie:
  - Narodowe: JAWNE, ZASTRZEŻONE, POUFNE, TAJNE, ŚCIŚLE TAJNE,
  - Sojuszu Północnoatlantyckiego: NATO UNCLASSIFIED (NU), NATO RESTRICTED (NR), NATO CONFIDENTIAL (NC), NATO SECRET (NS), NATO COSMIC TOP SECRET (CTS),
  - Unii Europejskiej: RESTREINT UE/ EU RESTRICTED, CONFIDENTIEL UE/ EU CONFIDENTIAL, SECRET UE/ EU SECRET, TRÈS SECRET UE/ EU TOP SECRET
  - Europejska Agencja Kosmiczna: ESA RESTRICTED, ESA CONFIDENTIAL, ESA SECRET, ESA TOP SECRET.
- poufności, dostępności i integralności tych informacji,
- implementacji właściwych środków zabezpieczających, zgodnych z wymogami prawnymi,
- organizacji systemu ochrony informacji niejawnymi w jednostce organizacyjnej,
- szkolenia w zakresie bezpieczeństwa osobowego,
- szkolenia z zakresu ochrony informacji niejawnych,
- zastosowanych środków ochrony fizycznej i technicznej,

- instalacji i eksploatacji elementów systemu z uwzględnieniem ich ograniczeń certyfikacyjnych,
- ochrony elektromagnetycznej.

4 Otoczenie systemu – rodzaje informacji

W ramach Systemu teleinformatycznego przetwarzane są poufne informacje związane z działalnością jednostki organizacyjnej. Ten system obejmuje przetwarzanie informacji klasyfikowanych jako ŚCIŚLE TAJNE, NATO COSMIC TOP SECRET (CTS), TRÈS SECRET UE/ EU TOP SECRET, ESA TOP SECRET. W ramach tego systemu są przetwarzane zarówno informacje niejawne własne, jak i te przyjęte od jednostek współpracujących w realizacji projektów oraz umów. Obejmują one dokumentację techniczną zamówień, projektów, umów i kontraktów objętych tajemnicą, dokumentację bezpieczeństwa systemów teleinformatycznych jednostki, dokumentację pełnomocnika ochrony zgodną z wymaganiami ustawy o ochronie informacji niejawnych i rozporządzeń wykonawczych, dokumenty związane z działalnością Pionu Ochrony Informacji Niejawnych, a także inne dokumenty o charakterze poufnym."

5 Odpowiedzialność personelu

W projektowanych systemach ochrony informacji wrażliwych należy stosować „zasadę dwóch” w kontekście, gdzie człowiek jest uznawany za potencjalnie najsłabsze ogniwo w systemie, skupiamy się na zminimalizowaniu ryzyka związanego z błędami lub działaniami nieumyślnymi dokonywanymi przez ludzi. Oznacza to, że kluczowe operacje lub procesy powinny być zaprojektowane w taki sposób, aby wymagały dwóch niezależnych działań lub potwierdzeń, zanim zostaną zrealizowane.

Przykłady zastosowania zasady dwóch w kontekście bezpieczeństwa, gdzie człowiek jest uznawany za potencjalnie najsłabsze ogniwo, mogą obejmować:

- Autoryzacja dwuetapowa: Aby uzyskać dostęp do pewnych zasobów lub informacji, użytkownik musi przejść dwuetapowy proces autoryzacji, np. wprowadzenie hasła oraz potwierdzenie kodem otrzymanym na telefon.
- Potwierdzenie transakcji: W systemach finansowych, szczególnie w bankowości internetowej, konieczne jest potwierdzenie ważnych transakcji za pomocą dwóch niezależnych czynników, na przykład wprowadzenie hasła i zatwierdzenie kodem z aplikacji autoryzacyjnej.
- Zarządzanie zasobami kluczowymi: Procesy związane z dostępem do kluczowych zasobów lub systemów mogą wymagać potwierdzenia lub autoryzacji przez dwóch niezależnych administratorów lub członków zespołu.

Zastosowanie zasady dwóch w powyższych kontekstach ma na celu zwiększenie bezpieczeństwa poprzez minimalizację ryzyka ludzkich błędów lub działań nieautoryzowanych, a jednocześnie zachowanie wydajności i użyteczności systemu.

Kierownik jednostki organizacyjnej zawsze odpowiada za ciągłość procesu zarządzania ryzykiem i nadzór nad szacowaniem ryzyka w kontekście bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym.

"Zasada dwóch" to podejście, które kładzie nacisk na podwójne zabezpieczenie, w celu zwiększenia bezpieczeństwa i minimalizacji potencjalnych zagrożeń. Oznacza to, że każda kluczowa operacja lub decyzja, zwłaszcza dotycząca bezpieczeństwa, powinna być potwierdzana lub kontrolowana przez co najmniej dwie niezależne i niezwiązane ze sobą osoby lub systemy.

Zastosowanie zasady dwóch zapewnia zwiększoną pewność i niezależność w kluczowych aspektach bezpieczeństwa. Przejście przez dwie niezależne oceny, autoryzacje lub potwierdzenia zabezpiecza przed ewentualnymi błędami, działaniami nieautoryzowanymi lub zaniedbaniami. Pozwala to na bardziej skuteczne zarządzanie ryzykiem i zminimalizowanie ewentualnych negatywnych konsekwencji.

Wynika z tego, że ocena poziomu bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznego powinna być realizowana w pełnym składzie zespołu pionu ochrony informacji niejawnych:

- Kierownika Jednostki Organizacyjnej
- Pełnomocnik ds. Ochrony Informacji Niejawnych;
- Inspektor Bezpieczeństwa Teleinformatycznego;
- Administrator systemu.

6 Założenia wstępne w metodzie oceny poziomu bezpieczeństwa

System teleinformatyczny powinien mieć zidentyfikowane zasoby, które wymagają ochrony. Ochrona tych zasobów w systemie ma kluczowe znaczenie dla zapewnienia poufności, dostępności i integralności przetwarzanych w nim informacji niejawnych. Należy przeprowadzić identyfikację zagrożeń dla bezpieczeństwa informacji niejawnych przetwarzanych w Systemie teleinformatycznym, uwzględniając zidentyfikowane zasoby. W procesie szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w Systemie teleinformatycznym, należy skoncentrować uwagę tylko na zagrożeniach, dla których stwierdzono podatność w systemie. Proces szacowania ryzyka obejmuje następujące etapy, które trzeba przeprowadzić: identyfikację zasobów podlegających ochronie w systemie teleinformatycznym, rozpoznanie zagrożeń dla

określonych w systemie zasobów, oszacowanie skutków utraty zasobów w kontekście poufności, dostępności i integralności, ocenę podatności zasobów na zidentyfikowane zagrożenia oraz określenie rozmiaru zidentyfikowanych ryzyk.

W trakcie oceny skutków utraty zasobów w kontekście poufności, ustalamy poziomy poufności zgodne z ustawowymi klauzulami oraz odpowiadające im zakresy wartości liczbowych, bazując na poniższej tabeli:

Poziom poufności	Wartość liczbowa
Jawne	0
Zastrzeżone/NATO RESTRICTED /RESTREINT UE/EU RESTRICTED	1-3
Poufne/NATO CONFIDENTIAL/ CONFIDENTIEL UE/EU CONFIDENTIAL	4-5
Tajne/NATO SECRET/ SECRET UE/EU SECRET	6-7
Ściśle Tajne/NATO COSMIC TOP SECRET/ TRÈS SECRET UE/ EU TOP SECRET	8-10

Tabela 3: Enumeracja poziomów poufności

W trakcie analizy skutków utraty zasobów dotyczących dostępności, określamy poziomy wymagań związanych z zachowaniem dostępności oraz odpowiadające im przedziały wartości liczbowych, zgodnie z informacjami zawartymi w poniższej tabeli:

Poziom dostępności	Wartość liczbowa	Wyznacznik
Niski	1-3	Brak dostępności informacji przez dłuższy okres czasu nie będzie znacząco wpływał na wykonywanie zadań przez jednostkę organizacyjną.
Średni	4-6	Brak dostępu do informacji może znacząco wpłynąć na realizację zadań, dlatego konieczne jest przywrócenie dostępności w ciągu 3-4 dni.
Wysoki	7-8	Niedostępność informacji może znacząco zakłócić działalność jednostki organizacyjnej, wymagając przywrócenia dostępności w ciągu krótkiego okresu, tj. kilku godzin.
Krytyczny	9	Działalność jednostki organizacyjnej jest niemożliwa, a odzyskanie dostępności musi nastąpić w ciągu kilku minut.
Absolutny	10	Utrata dostępności informacji jest niedopuszczalna.

Tabela 4: Enumeracja poziomów dostępności

W kontekście analizy skutków utraty integralności zasobów wyznaczono cztery poziomy wymagań dotyczących konieczności zachowania integralności, oraz określono odpowiadające im przedziały wartości liczbowych (1-10) w każdej z tych kategorii, jak przedstawiono w poniższej tabeli:

Poziom integralności	Wartość liczbowa
Niskie wymagania	1-3
Średnie wymagania	4-7
Wysokie wymagania	8-9
Obligatoryjne wymagania	10

Tabela 5: Enumeracja poziomów integralności

Oszacowanie stopnia narażenia zasobów w systemie teleinformatycznym na identyfikowane zagrożenia przeprowadzono z wykorzystaniem przedstawionej tabeli:

Poziom podatności	Wartość liczbowa
Brak	0
Niski	1-4
Średni	5-7
Wysoki	8-9
Krytyczny	10

Tabela 6: Enumeracja poziomów podatności

Ocenę wielkości zidentyfikowanych ryzyk przeprowadzono, uwzględniając wartość poszczególnych zasobów, ustalaną na podstawie wymagań dotyczących ochrony poufności, dostępności i integralności. Określono to na podstawie oszacowanych wartości liczbowych, które reprezentują skutki ujawnienia, utraty, modyfikacji lub braku dostępności zasobów. Dodatkowo brano pod uwagę poziomy zagrożeń, które mogą wpłynąć na poszczególne zasoby, oraz szacowane wartości liczbowe poziomów podatności na te zagrożenia.

Określenie poziomów ryzyka związanych z **poufnością** oparto na wartościach liczbowych, które zostały ustalone zgodnie z poniższą tabelą:

Poziom ryzyka	Wartość liczbowa
Niski	1-23
Średni	24-47
Wysoki	48-70
Maksymalny	71-100

Tabela 7: Enumeracja poziomów ryzyka dla poufności

Określenie poziomów ryzyka związanych z **dostępnością** oparto na wartościach liczbowych, które zostały ustalone zgodnie z poniższą tabelą:

Poziom ryzyka	Wartość liczbowa
Niski	1-20
Średni	21-60
Wysoki	61-80
Maksymalny	81-100

Tabela 8: Enumeracja poziomów ryzyka dla dostępności

Określenie poziomów ryzyka związanych z **integralnością** oparto na wartościach liczbowych, które zostały ustalone zgodnie z poniższą tabelą:

Poziom ryzyka	Wartość liczbowa
Niski	1-20
Średni	21-60
Wysoki	61-80
Maksymalny	81-100

Tabela 9: Enumeracja poziomów ryzyka dla integralności

Do przeliczenia wielkości ryzyk zastosowano niżej podane macierze.

Poziomy ryzyka w odniesieniu do poufności		Niski				Średni			Wysoki		Krytyczny
		1	2	3	4	5	6	7	8	9	10
Zastrzeżone	1	1	2	3	4	5	6	7	8	9	10
	2	2	4	6	8	10	12	14	16	18	20
	3	3	6	9	12	15	18	21	24	27	30
Poufne	4	4	8	12	16	20	24	28	32	36	40
	5	5	10	15	20	25	30	35	40	45	50
Tajne	6	6	12	18	24	30	36	42	48	54	60
	7	7	14	21	28	35	42	49	56	63	70
Ściśle Tajne	8	8	16	24	32	40	48	56	64	72	80
	9	9	18	27	36	45	54	63	72	81	90
	10	10	20	30	40	50	60	70	80	90	100

Tabela 10: Poziomy ryzyka w odniesieniu do poufności

Poziomy ryzyka w odniesieniu do dostępności		Niski				Średni			Wysoki		Krytyczny
		1	2	3	4	5	6	7	8	9	10
Niski	1	1	2	3	4	5	6	7	8	9	10
	2	2	4	6	8	10	12	14	16	18	20
	3	3	6	9	12	15	18	21	24	27	30
Średni	4	4	8	12	16	20	24	28	32	36	40
	5	5	10	15	20	25	30	35	40	45	50
	6	6	12	18	24	30	36	42	48	54	60
Wysoki	7	7	14	21	28	35	42	49	56	63	70
	8	8	16	24	32	40	48	56	64	72	80
Krytyczny	9	9	18	27	36	45	54	63	72	81	90
Absolutny	10	10	20	30	40	50	60	70	80	90	100

Tabela 11: Poziomy ryzyka w odniesieniu do dostępności

Poziomy ryzyka w odniesieniu do integralności		Niski				Średni			Wysoki		Krytyczny
		1	2	3	4	5	6	7	8	9	10
Niski	1	1	2	3	4	5	6	7	8	9	10
	2	2	4	6	8	10	12	14	16	18	20
	3	3	6	9	12	15	18	21	24	27	30
Średni	4	4	8	12	16	20	24	28	32	36	40
	5	5	10	15	20	25	30	35	40	45	50
	6	6	12	18	24	30	36	42	48	54	60
	7	7	14	21	28	35	42	49	56	63	70
Wysoki	8	8	16	24	32	40	48	56	64	72	80
	9	9	18	27	36	45	54	63	72	81	90
Obligatoryjny	10	10	20	30	40	50	60	70	80	90	100

Tabela 12: Poziomy ryzyka w odniesieniu do integralności

7 Identyfikacja zasobów

W każdej jednostce organizacyjnej istnieją różnorodne typy informacji, które wymagają zabezpieczenia. Informacje niejawne mogą być sklasyfikowane z różnymi poziomami tajności, co determinuje różny stopień ich ochrony.

Pierwszym krokiem w proponowanej metodzie jest podział informacji przetwarzanych w systemie na grupy, zależnie od obszaru działalności jednostki organizacyjnej (podział według rodzaju informacji). To pozwoli na ocenę podatności interesów jednostki organizacyjnej na ujawnienie, utratę, modyfikację lub brak dostępu do tych informacji. Równocześnie pozwoli zidentyfikować źródła zagrożeń dla tych informacji i określić, dla kogo mogą być one atrakcyjne.

Następnie w obrębie każdej z tych grup informacji powinny być wyodrębnione te, które wymagają podobnego poziomu ochrony, określonego klauzulą tajności. Ważne jest zauważenie, że pogrupowane w ten sposób informacje podlegają odpowiedzialności jednej osoby za ich bezpieczeństwo, takiej jak kierownik działu, departamentu lub biura. Ta osoba powinna uczestniczyć w oszacowaniu skutków ewentualnej utraty, ujawnienia lub modyfikacji tych informacji. W wyniku tej segregacji powstaną wydzielone kategorie zasobów informacyjnych, które mają określone wspólne wymagania dotyczące funkcjonowania i zabezpieczeń - ZS1, ZS2, ZS3 itd.

Dla każdej kategorii zasobów informacyjnych zostanie stworzony rząd w macierzy. Dla każdego z nich będzie konieczne oszacowanie potrzeby utrzymania integralności, poufności i dostępności.

Podobnie, należy wyodrębnić pozostałe zasoby systemu, które wymagają ochrony. Ocena potrzeby ochrony ich poufności, integralności lub dostępności będzie zależała od ich charakteru. Standardowe oprogramowanie lub sprzęt komputerowy

będzie wymagać oceny głównie w zakresie dostępności (zapewnienie niezawodności). Z drugiej strony, sprzęt kryptograficzny, klucze szyfrów, hasła, dokumentacja bezpieczeństwa systemu, wymagać będą oceny także w kontekście poufności.

Jeśli zasoby mogą być istotne dla więcej niż jednego aspektu bezpieczeństwa (integralność, poufność i dostępność), powinny pojawić się wielokrotnie w odpowiednich miejscach macierzy.

W ramach przykładowego systemu teleinformatycznego zidentyfikowano zasoby wymagające ochrony. Zagwarantowanie bezpieczeństwa tych zasobów w systemie jest kluczowe dla zachowania poufności, dostępności i integralności informacji niejawnych przetwarzanych w tym systemie teleinformatycznym.

Zasób	Opis	Cecha bezpieczeństwa		
		Poufność	Dostępność	Integralność
ZAS-01	Informacje niejawne własne	X	X	X
ZAS-02	Informacje niejawne powierzone	X	X	X
ZAS-03	Gotowość do przetwarzania informacji		X	
ZAS-04	Wizerunek organizacji	X	X	X
ZAS-05	Elementy systemu IT	X	X	X
ZAS-06	Nośniki danych	X	X	X
ZAS-07	Oprogramowanie systemu	X	X	X
ZAS-08	Hasło Inspektora BTI	X	X	
ZAS-09	Hasło Administratora IT	X	X	
ZAS-10	Hasła Użytkowników IT	X	X	
ZAS-11	Kopie bezpieczeństwa systemu		X	X
ZAS-12	Kopie bezpieczeństwa danych	X	X	X
ZAS-13	Dane z audytów bezpieczeństwa	X	X	
ZAS-14	Personel ochrony		X	
ZAS-15	Administrator IT	X	X	X
ZAS-16	Użytkownicy IT	X	X	X
ZAS-17	Pomieszczenia		X	
ZAS-18	Infrastruktura		X	
ZAS-19	Dokumentacja i procedury operacyjne	X		
ZAS-20	Dane osobowe użytkowników systemu	X		

Tabela 13: Zasoby systemu podlegające ochronie

8 Identyfikacja zagrożeń

Następnym krokiem jest identyfikacja zagrożeń dla integralności, poufności i dostępności dla każdej kategorii zasobów informacyjnych przetwarzanych w systemie. Każde zidentyfikowane zagrożenie powinno zostać zapisane w nagłówku kolumny, a w razie potrzeby dodać odpowiednią liczbę kolumn. Niektóre zagrożenia mogą występować dla więcej niż jednego atrybutu bezpieczeństwa (integralności, poufności i dostępności), więc powinny pojawić się wielokrotnie w odpowiednich miejscach macierzy.

Zagrożenia dla bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznego zostały określone w odniesieniu do poufności, dostępności i integralności zidentyfikowanych zasobów systemu.

W procesie szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznego zostały zidentyfikowane tylko te zagrożenia, dla których stwierdzono istnienie podatności w systemie.

W poniższej tabeli zostały wyszczególnione zagrożenia w odniesieniu do poufności, dostępności i integralności zasobów w systemie teleinformatycznego oraz wskazano źródło tych zagrożeń, tzn. siły natury oraz celowe lub przypadkowe działanie człowieka.

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-12			x	

		ZAS-10, ZAS-16					
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,			x	

			ZAS-6, ZAS-7				
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	ZAS-1, ZAS-2, ZAS-4	ZAS-1, ZAS-2, ZAS-3, ZAS-4,	ZAS-1, ZAS-2, ZAS-4, ZAS-5,	x		x

	personelu wpływająca na kontynuację pracy systemu.		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-7			
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		x	x

			ZAS-5, ZAS-7, ZAS-17				
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		ZAS-1, ZAS-2, ZAS-3, ZAS-4,	ZAS-5	x		x

	czynników losowych, jak i celowych działań ludzi.		ZAS-5, ZAS-17				
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	Błędy i pomyłki	ZAS-1,	ZAS-1,	ZAS-1,			x

-28	administratora systemu wpływające na bezpieczeństwo informacji.	ZAS-2, ZAS-4, ZAS-12	ZAS-2, ZAS-3, ZAS-4, ZAS-5, ZAS-6, ZAS-7, ZAS-12, ZAS-13	ZAS-2			
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-5			x

			ZAS-12, ZAS-13				
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	ZAS-1, ZAS-2, ZAS-12	ZAS-1, ZAS-2, ZAS-3,	ZAS-7, ZAS-11, ZAS-12			x

	wpływające na wydajność pracy.		ZAS-4, ZAS-5, ZAS-7, ZAS-11, ZAS-12				
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	ZAS-1, ZAS-2, ZAS-4	ZAS-3, ZAS-4, ZAS-5				x

	socjotechnik.						
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	ZAS-1, ZAS-2, ZAS-4,	ZAS-1, ZAS-2, ZAS-3,	ZAS-1, ZAS-2			x

	wpływających na integralność i poufność informacji.	ZAS-12	ZAS-4, ZAS-5, ZAS-6, ZAS-7, ZAS-12, ZAS-13				
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		ZAS-1, ZAS-2, ZAS-3,	ZAS-1, ZAS-2, ZAS-7			x

	monitorowania systemu.		ZAS-4, ZAS-7				
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

9 Przeciwdziałanie zagrożeniom

W Systemie teleinformatycznego zastosowano odpowiednie środki zabezpieczające dla zidentyfikowanych zagrożeń. Działania te zostały wdrożone zgodnie z wymaganiami ustawowymi, mając na celu zapewnienie niezbędnego poziomu bezpieczeństwa informacji niejawnych przetwarzanych w tym systemie.

Lp.	Zagrożenie	Opis środków mających na celu ochronę systemu teleinformatycznego przed różnymi rodzajami zagrożeń i są 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.
Zg-1	Pożar w lokalizacji firmy	- System przeciwpożarowy. - Przenośny sprzęt gaśniczy. - Instrukcja bezpieczeństwa pożarowego. - Szkolenia personelu.
Zg-2	Zalanie pomieszczenia systemu w wyniku awarii instalacji	- Lokalizacja pomieszczenia systemu. - Okresowe przeglądy infrastruktury technicznej.
Zg-3	Wyładowanie atmosferyczne	- Instalacja odgromowa. - Zabezpieczenia urządzeń. - Procedury eksploatacji urządzeń.
Zg-4	Katastrofa budowlana	- Pomieszczenie systemu o wzmocnionej konstrukcji budowlanej.
Zg-5	Awaria sieci zasilania elektrycznego	- Centralny system gwarantowanego zasilania. - Kontrole stanu instalacji zasilania elektrycznego.

Lp.	Zagrożenie	Opis środków mających na celu ochronę systemu teleinformatycznego przed różnymi rodzajami zagrożeń i są 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.
Zg-6	Awaria urządzeń gwarantowanego zasilania	- Kontrole stanu instalacji zasilania awaryjnego. - Procedury wykonywania kopii zapasowych. - Procedura serwisowania.
Zg-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.
Zg-8	Działania dywersyjne i sabotażowe	- System kontroli dostępu. - System sygnalizacji włamania i napadu. - Zabezpieczenia fizyczne.
Zg-9	Infiltracja elektromagnetyczna	- Sprzętowa Strefa Ochrony Elektromagnetycznej. - Certyfikowane urządzenia z obniżoną emisją. - Procedury eksploatacji.
Zg-10	Awaria środków ochrony fizycznej i technicznych środków wspomagających	- Procedury postępowania w przypadku awarii systemów ochrony technicznej. - Przeglądy systemów ochrony technicznej.

Lp.	Zagrożenie	Opis środków mających na celu ochronę systemu teleinformatycznego przed różnymi rodzajami zagrożeń i są 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.
Zg-11	Kradzież urządzenia systemu	- System kontroli dostępu. - System sygnalizacji włamania i napadu. - Zabezpieczenia fizyczne. - Nadzór i szkolenia personelu. - Kontrole użytkowników. - Zaufani użytkownicy.
Zg-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.
Zg-13	Wykorzystywanie systemu (urządzenia) do celów nie związanych z jego przeznaczeniem	- Nadzór i szkolenia personelu. - Kontrole użytkowników.

Lp.	Zagrożenie	Opis środków mających na celu ochronę systemu teleinformatycznego przed różnymi rodzajami zagrożeń i są 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.
Zg-14	Niewłaściwe kwalifikacje personelu bezpieczeństwa teleinformatycznego	- Procedury kadrowe. - Poświadczenia bezpieczeństwa. - Szkolenia w ABW/SKW i zakresie bezpieczeństwa informacji.
Zg-15	Zmiany (rotacja) personelu, choroba, czasowa niedostępność personelu	- Planowanie kadry. - Planowanie urlopów i działalności bieżącej. - Procedury.
Zg-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.
Zg-17	Nieznajomość procedur przez użytkowników systemu	- Nadzór i szkolenia personelu. - Kontrole użytkowników.
Zg-18	Niewłaściwa eksploatacja urządzenia (systemu)	- Procedury dotyczące użytkowania urządzeń. - Procedury serwisowania urządzeń. - Procedury wykonywania kopii zapasowych. - Przeglądy systemów ochrony technicznej.

Lp.	Zagrożenie	Opis środków mających na celu ochronę systemu teleinformatycznego przed różnymi rodzajami zagrożeń i są 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.
Zg-19	Wykorzystanie urządzeń spoza systemu (strefy ochronnej)	- Procedury zarządzania konfiguracją systemu. - Nadzór personelu. - Procedury użytkowania urządzeń. - Procedury serwisowania urządzeń.
Zg-20	Pozostawienie niezabezpieczonego urządzenia (teleinformatycznego)	- Procedury zasad użytkowania systemu. - Nadzór personelu. - Szkolenia użytkowników.
Zg-21	Pozostawienie niezabezpieczonego dokumentu niejawnego	- Procedury zarządzania dokumentami niejawnymi. - Rejestracja i ewidencjonowanie dokumentów. - Szkolenia personelu. - Kontrole użytkowników. - Zaufani użytkownicy.
Zg-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	Opis środków mających na celu ochronę systemu teleinformatycznego przed różnymi rodzajami zagrożeń i są 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.
Zg-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.
Zg-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.
Zg-25	Przekazanie dokumentów niejawnych osobom nieuprawnionym	- Procedury zarządzania dokumentami niejawnymi. - Rejestracja i ewidencjonowanie dokumentów. - Szkolenia personelu. - Kontrole użytkowników. - Zaufani użytkownicy.

Lp.	Zagrożenie	Opis środków mających na celu ochronę systemu teleinformatycznego przed różnymi rodzajami zagrożeń i są 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.
Zg-26	Brak odpowiednich cech etyczno-moralnych użytkowników	- Zaufani użytkownicy. - Wdrożenie PBE dotyczących nadawania uprawnień i szkolenia użytkowników. - Kontrole użytkowników.
Zg-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.
Zg-28	Błędy i pomyłki administratora systemu	- Procedury kadrowe. - Szkolenia w ABW. - Szkolenia w zakresie bezpieczeństwa informacji.
Zg-29	Błędy i pomyłki użytkowników systemu	- Szkolenia personelu. - Procedury analizowania i archiwizowania rejestru zdarzeń. - Kontrole użytkowników. - Zaufani użytkownicy.

Lp.	Zagrożenie	Opis środków mających na celu ochronę systemu teleinformatycznego przed różnymi rodzajami zagrożeń i są 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.
Zg-30	Brak procedur gromadzenia i archiwizowania danych oraz wykonywania kopii	- Konfiguracja systemów operacyjnych. - Procedury archiwizowania i tworzenia kopii zapasowych. - Przeglądy dziennika zdarzeń.
Zg-31	Niewłaściwe działanie oprogramowania urządzenia (systemu)	- Konfiguracja systemów operacyjnych. - Procedury odtwarzania systemu i oprogramowania z kopii zapasowych. - Przeglądy dziennika zdarzeń. - Wykonywanie testów bezpieczeństwa.
Zg-32	Brak bieżącego monitorowania pracy systemu	- Procedury audytowania bezpieczeństwa. - Procedury analizowania i archiwizowania rejestru zdarzeń. - Procedury wykonywania kopii bezpieczeństwa. - Wykonywanie testów bezpieczeństwa.
Zg-33	Nieuprawniony dostęp do systemu (zasobów informacyjnych systemu)	- Procedury nadawania uprawnień użytkownikom. - System kontroli dostępu. - System sygnalizacji włamania i napadu. - Audyty bezpieczeństwa.

Lp.	Zagrożenie	Opis środków mających na celu ochronę systemu teleinformatycznego przed różnymi rodzajami zagrożeń i są 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.
Zg-34	Brak certyfikatu elementu systemu	- Akredytacja bezpieczeństwa Systemu. - Kontrole elementów systemu. - Procedury eksploatacji środków ochrony elektromagnetycznej.
Zg-35	Modyfikacja parametrów instalacyjnych przez osoby nieuprawnione	- Konfiguracja systemów operacyjnych. - Przeglądy dziennika zdarzeń.
Zg-36	Wprowadzenie do systemu szkodliwego oprogramowania	- Konfiguracja systemów operacyjnych. - Procedury nadawania uprawnień użytkownikom. - Polityka i procedury antywirusowe.
Zg-37	Nieuprawnione kopiowanie danych na informatycznych nośnikach danych	- Konfiguracja systemów operacyjnych. - Procedury eksportu danych. - Przeglądy dziennika zdarzeń.
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.

Lp.	Zagrożenie	Opis środków mających na celu ochronę systemu teleinformatycznego przed różnymi rodzajami zagrożeń i są 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.
39	Zagrożenie wynikające z wprowadzenia dezinformacji i manipulacji informacjami	- Weryfikacja i weryfikacja źródła informacji. - Wdrożenie procedur weryfikacji informacji przed ich użyciem.
40	Wyciek informacji w wyniku zaawansowanego ataku phishingowego	- Szkolenia w zakresie rozpoznawania i unikania ataków phishingowych. - Użycie filtrowania wiadomości e-mail i antyspamowych.
41	Skomplikowane procedury dostępu do systemu wpływające na wydajność pracy	- Optymalizacja procedur dostępu. - Użycie autoryzacji dwuskładnikowej w celu zwiększenia bezpieczeństwa przy jednoczesnym ułatwieniu dostępu.
42	Zagrożenie ze strony zanieczyszczonych nośników danych wpływające na integralność danych	- Skanowanie nośników danych przed ich użyciem. - Wdrożenie procedur zarządzania nośnikami danych.

Lp.	Zagrożenie	Opis środków mających na celu ochronę systemu teleinformatycznego przed różnymi rodzajami zagrożeń i są 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.
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.
44	Ujawnienie informacji wynikające z wykorzystania podsłuchu	- Zastosowanie zabezpieczeń akustycznych w pomieszczeniach. - Wdrożenie procedur audytu systemów antysłuchowych.
45	Wyłudzenie informacji niejawnych za pomocą socjotechnik	- Szkolenia personelu w zakresie rozpoznawania socjotechnik. - Weryfikacja tożsamości przed ujawnieniem poufnych informacji.
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.

Lp.	Zagrożenie	Opis środków mających na celu ochronę systemu teleinformatycznego przed różnymi rodzajami zagrożeń i są 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.
47	Ujawnienie informacji wynikające z nieostrzeżenia przez zabezpieczenia antywirusowe	- Regularna aktualizacja oprogramowania antywirusowego. - Wdrożenie procedur reagowania na alarmy antywirusowe.
48	Błąd ludzki w procesie przetwarzania informacji wpływający na bezpieczeństwo danych	- Szkolenia w zakresie bezpieczeństwa informacji.- Wdrożenie procedur weryfikacji procesów przetwarzania danych.
49	Ujawnienie informacji w wyniku wykorzystania exploitów	- Regularna aktualizacja oprogramowania w celu usuwania potencjalnych luk bezpieczeństwa.- Wdrożenie zabezpieczeń przed znanymi exploitami.
50	Wykorzystanie słabych haseł przez intruzów wpływających na integralność i poufność informacji	- Wymuszenie na użytkownikach używania silnych haseł.- Wdrożenie autoryzacji dwuskładnikowej.

Lp.	Zagrożenie	Opis środków mających na celu ochronę systemu teleinformatycznego przed różnymi rodzajami zagrożeń i są 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.
51	Zagrożenie wynikające z braku aktualizacji oprogramowania wpływające na bezpieczeństwo systemu	- Wdrożenie procedur aktualizacji oprogramowania.- Regularna kontrola i stosowanie dostępnych łatek bezpieczeństwa.
52	Niedostateczne zabezpieczenia przeciwwłamaniowe	- Wdrożenie systemów detekcji włamań i środków przeciwdziałania. - Monitoring i reagowanie na potencjalne ataki.
53	Nieautoryzowane modyfikacje konfiguracji systemu wpływające na integralność i dostęp do systemu	- Ograniczenie uprawnień dostępu do konfiguracji systemu.- Monitoring zmian w konfiguracji.
54	Atak na system teleinformatyczny z wykorzystaniem ransomware wpływający na integralność danych	- Regularne tworzenie kopii zapasowych danych.- Wdrożenie procedur odtwarzania systemu po ataku ransomware.

Lp.	Zagrożenie	Opis środków mających na celu ochronę systemu teleinformatycznego przed różnymi rodzajami zagrożeń i są 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.
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.
56	Nieodpowiednie procedury zarządzania i dystrybucji kluczy kryptograficznych wpływające na bezpieczeństwo systemu	- Wdrożenie procedur zarządzania kluczami kryptograficznymi. - Audyt i kontrola procesów dystrybucji kluczy.
57	Nieprawidłowa identyfikacja i uwierzytelnianie użytkowników	- Wdrożenie autoryzacji dwuskładnikowej. - Regularna weryfikacja tożsamości użytkowników.
58	Brak mechanizmów audytu bezpieczeństwa i monitorowania systemu	- Wdrożenie narzędzi monitorujących i audytu bezpieczeństwa.- Regularne przeglądy dzienników zdarzeń.

Lp.	Zagrożenie	Opis środków mających na celu ochronę systemu teleinformatycznego przed różnymi rodzajami zagrożeń i są 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.
59	Nieuprawnione ujawnienie informacji na skutek niewłaściwego zarządzania dokumentami niejawnymi	- Wdrożenie procedur kontroli dostępu do dokumentów niejawnych. - Szkolenia personelu w zakresie zarządzania dokumentami niejawnymi.
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.

10 Oszacowanie skutków kompromitacji systemu

Poufność informacji w systemie

Zachowanie poufności informacji jest kluczowym aspektem w ochronie danych niejawnych. Osoby odpowiedzialne za nadawanie klauzul informacjom niejawnych powinny dokładnie przeanalizować różne kategorie zasobów informacyjnych, oceniając wymagania związane z zachowaniem poufności. Ustalono odpowiednie poziomy poufności, które zostały dostosowane do ustawowych klauzul, a każdemu z nich przypisano odpowiednie zakresy wartości:

Klauzula	Poziom
Jawne	0
Zastrzeżone	1-3
Poufne	4-5
Tajne	6-7
Ściśle tajne	8-10

Tabela 14: Enumeracja poziomów skutków dla utraty poufności

W kontekście zagrożeń poufności informacji, w kolumnie dotyczącej każdej kategorii zasobów informacyjnych, powinno być odnotowane potencjalne skutki ujawnienia tych informacji. Ta ocena pozwala na właściwe zabezpieczenie informacji i minimalizację ryzyka ich nieuprawnionego ujawnienia.

Integralność informacji w systemie

W utrzymaniu integralności informacji w systemie teleinformatycznym odgrywa kluczową rolę. Osoby odpowiedzialne za nadanie klauzuli tajności informacjom są także odpowiedzialne za określenie wymagań dotyczących zachowania integralności w każdej wydzielonej kategorii zasobów informacyjnych.

Zaproponowano cztery poziomy wymagań dotyczących zachowania integralności, które odpowiadają przedziałom wartości liczbowych (1-10) dla każdej z tych kategorii:

Wymaganie integralności	Poziom
Niskie	1-3
Średnie	4-7
Wysokie	8-9
Krytyczne	10

Tabela 15: Enumeracja poziomów skutków dla utraty integralności

W kolumnie dotyczącej konkretnego zagrożenia dla integralności, powinna zostać umieszczona wartość odpowiadająca określonej kategorii zasobów informacyjnych (ZAS-xx), wybrana na podstawie przyjętego poziomu wymagań związanych z zachowaniem integralności. Wartość 1 oznacza niewielkie skutki utraty integralności, podczas gdy wartość 10 wskazuje na skutki o krytycznie wysokim stopniu powagi. Ta ocena poziomu integralności pozwala na właściwe zabezpieczenie informacji i minimalizację ryzyka utraty ich integralności.

Dostępność informacji w systemie

Zapewnienie ciągłej dostępności do informacji stanowi kluczowy aspekt w zarządzaniu bezpieczeństwem w systemie teleinformatycznym. Osoba odpowiedzialna za bezpieczeństwo informacji powinna sklasyfikować je na podstawie wymagań związanych z zachowaniem dostępności oraz czasem, jaki może minąć do momentu przywrócenia dostępu, uwzględniając priorytety jednostki organizacyjnej.

Zakres tego oceniania powinien obejmować także inne zasoby systemu teleinformatycznego , które biorą udział w przetwarzaniu informacji, takie jak wyposażenie czy oprogramowanie.

Zaproponowane poziomy wymagań dotyczących zachowania dostępności, wraz z odpowiadającymi im przedziałami wartości w odniesieniu do skutków, są następujące:

Niskie wymagania (1-3): Oznaczają, że dłuższa niedostępność informacji nie będzie miała większego wpływu na funkcjonowanie jednostki organizacyjnej.
Średnie wymagania (4-6): Oznaczają, że niedostępność informacji może znacząco wpłynąć na działalność, a jej przywrócenie powinno nastąpić w ciągu kilku dni.
Wysokie wymagania (7-8): Oznaczają, że niedostępność informacji może spowodować poważne szkody i konieczne jest przywrócenie dostępności w ciągu kilku godzin.

Ekstremalne wymagania (9): Oznaczają, że działalność jednostki organizacyjnej zostanie sparaliżowana, a przywrócenie dostępności musi nastąpić w ciągu kilku minut.
Absolutne wymagania (10): Oznaczają, że utrata dostępności informacji jest niedopuszczalna.

Dla każdej kategorii zasobów informacyjnych powinien być wybrany odpowiedni poziom dostępności i przypisana wartość liczbową, odzwierciedlająca potencjalny wpływ utraty dostępności w danym zakresie. W przypadku istnienia różnych poziomów dostępności dla danej grupy zasobów, podział powinien zostać skorygowany, aby uwzględnić różnice w dostępności zasobów. W ten sposób możliwe jest zróżnicowanie i odpowiednie zabezpieczenie dostępu do informacji.

Oszacowane skutki utraty zasobów w Systemie teleinformatycznego w odniesieniu do ich poufności, dostępności i integralności:

Oznaczenie zasobu	**Nazwa zasobu**	**Skutki w odniesieniu do:**		
		Poufności	**Dostępności**	**Integralności**
Zs-1	Informacje niejawne własne przetwarzane w wyniku działalności firmy	**7**	**7**	**8**
Zs-2	Informacje niejawne powierzone lub przejęte z innych systemów (podmiotów).	**7**	**7**	**8**
Zs-3	Gotowość do przetwarzania informacji, zdolność do działania w trybie ciągłym	-	**7**	-
Zs-4	Wizerunek firmy	**6**	**8**	**7**
Zs-5	Elementy Systemu teleinformatycznego	-	**8**	**9**
Zs-6	Informatyczne nośniki danych niejawnych	**7**	**8**	**8**
Zs-7	Oprogramowanie systemu	-	**7**	**9**
Zs-8	Hasło Inspektora Bezpieczeństwa	**6**	**8**	-

	Teleinformatycznego			
Zs-9	Hasła Administratora Systemu teleinformatycznego	**7**	**8**	-
Zs-11	Kopie bezpieczeństwa systemu operacyjnego	-	**7**	**8**
Zs-12	Kopie bezpieczeństwa danych	**7**	**7**	**9**
Zs-13	Dane z audytów bezpieczeństwa	-	**8**	**-**
Zs-14	Personel POIN	-	**6**	-
Zs-15	Administrator Systemu	-	**7**	-
Zs-16	Użytkownicy Systemu teleinformatycznego	-	**7**	-
Zs-17	Pomieszczenie, infrastruktura	-	**7**	**-**
Zs-18	Infrastruktura	-	**7**	**-**
Zs-19	Dokumentacja i procedury operacyjne	-	**7**	**-**
Zs-20	Dane osobowe użytkowników systemu	-	**7**	**-**

11 Oszacowanie podatności zasobów

Następnym krokiem jest oszacowanie podatności każdej kategorii zasobów systemu informacyjnych na zidentyfikowane zagrożenia. Wartości te powinny być obliczone, biorąc pod uwagę prawdopodobieństwo wystąpienia danego zagrożenia oraz podatność systemu, która może przyczynić się do potencjalnych szkód.

W tym etapie analizy powinny być zdefiniowane wszystkie istniejące środki ochrony, wprowadzone w celu zmniejszenia prawdopodobieństwa wystąpienia zagrożeń lub ograniczenia podatności systemu na te zagrożenia.

Do oszacowania posłużyć mogą poniższe poziomy podatności, wraz z odpowiadającymi im przedziałami wartości:

Brak (0).
Niski poziom (1-4).
Średni poziom (5-7).
Wysoki poziom (8-9).
Ekstremalny poziom (10).

Dla każdej pary: określona kategoria zasobów i zidentyfikowane dla tej kategorii zagrożenie (ZS-x/ZG-y), należy wybrać odpowiedni poziom podatności i przypisać mu odpowiednią liczbę z podanego przedziału wartości. Jeśli dla jakiejś pary zasobów i zagrożeń oszacowano podatność na tym samym poziomie, należy dokonać dodatkowego zróżnicowania za pomocą wartości liczbowych z odpowiedniego przedziału. Ostateczne wartości podatności dla każdej kategorii zasobów informacyjnych i dla każdego zidentyfikowanego zagrożenia powinny być wpisane w odpowiednich komórkach macierzy.

W procesie oceny ryzyka dokonano oszacowania poziomów podatności zasobów w Systemie teleinformatycznego na identyfikowane zagrożenia związane z poufnością, dostępnością i integralnością przetwarzanych informacji niejawnych.

Podczas oceny poziomów podatności uwzględniono istniejące środki zabezpieczające wdrożone w Systemie teleinformatycznego.

Ostateczne oszacowania podatności systemu dla zidentyfikowanych par zasób/zagrożenie (Zs-x/Zg-x) dotyczących poufności, dostępności i integralności informacji niejawnych przetwarzanych w systemie przedstawiono w poniższej tabeli:

Oznaczenie zasobu	Oznaczenie zagrożenia	Podatność w odniesieniu do:		
		Poufności	Dostępności	Integralności
Zs-1	Zg-1	-	4	-
Zs-1	Zg-2	-	5	-
Zs-1	Zg-3	-	3	-
Zs-1	Zg-4	-	3	-
Zs-1	Zg-5	-	5	-
Zs-1	Zg-6	-	4	-
Zs-1	Zg-7	5	-	-
Zs-1	Zg-8	-	3	-
Zs-1	Zg-9	2	-	-
Zs-1	Zg-10	3	5	-
Zs-1	Zg-11	3	3	-
Zs-1	Zg-12	3	3	-
Zs-1	Zg-13	2	-	-
Zs-1	Zg-14	2	3	2
Zs-1	Zg-15	3	2	2
Zs-1	Zg-16	2	2	3
Zs-1	Zg-17	3	4	4
Zs-1	Zg-18	2	3	-

Zs-1	**Zg-19**	**4**	**-**	**-**
Zs-1	**Zg-20**	**3**	**-**	**3**
Zs-1	**Zg-21**	**4**	**-**	**-**
Zs-1	**Zg-22**	**3**	**-**	**-**
Zs-1	**Zg-23**	**5**	**-**	**-**
Zs-1	**Zg-24**	**-**	**6**	**-**
Zs-1	**Zg-25**	**3**	**-**	**-**
Zs-1	**Zg-26**	**3**	**4**	**4**
Zs-1	**Zg-27**	**-**	**5**	**-**
Zs-1	**Zg-28**	**2**	**3**	**2**
Zs-1	**Zg-29**	**3**	**5**	**3**
Zs-1	**Zg-30**	**2**	**3**	**-**
Zs-1	**Zg-31**	**-**	**4**	**-**
Zs-1	**Zg-32**	**2**	**3**	**3**
Zs-1	**Zg-33**	**3**	**4**	**3**
Zs-1	**Zg-34**	**2**	**-**	**-**
Zs-1	**Zg-35**	**3**	**4**	**-**
Zs-1	**Zg-36**	**-**	**3**	**3**
Zs-1	**Zg-37**	**2**	**-**	**-**
Zs-2	**Zg-1**	**-**	**4**	**-**
Zs-2	**Zg-2**	**-**	**5**	**-**
Zs-2	**Zg-3**	**-**	**3**	**-**
Zs-2	**Zg-4**	**-**	**3**	**-**
Zs-2	**Zg-5**	**-**	**5**	**-**
Zs-2	**Zg-6**	**-**	**4**	**-**
Zs-2	**Zg-7**	**5**	**-**	**-**
Zs-2	**Zg-8**	**-**	**3**	**-**
Zs-2	**Zg-9**	**2**	**-**	**-**
Zs-2	**Zg-10**	**3**	**5**	**-**
Zs-2	**Zg-11**	**3**	**3**	**-**
Zs-2	**Zg-12**	**3**	**3**	**-**
Zs-2	**Zg-13**	**2**	**-**	**-**
Zs-2	**Zg-14**	**2**	**3**	**2**
Zs-2	**Zg-15**	**3**	**2**	**2**
Zs-2	**Zg-16**	**2**	**2**	**3**

Zs-2	**Zg-17**	**3**	**4**	**4**
Zs-2	**Zg-18**	**2**	**3**	**-**
Zs-2	**Zg-19**	**4**	**-**	**-**
Zs-2	**Zg-20**	**3**	**-**	**3**
Zs-2	**Zg-21**	**4**	**-**	**-**
Zs-2	**Zg-22**	**3**	**-**	**-**
Zs-2	**Zg-23**	**5**	**-**	**-**
Zs-2	**Zg-24**	**-**	**6**	**-**
Zs-2	**Zg-25**	**3**	**-**	**-**
Zs-2	**Zg-26**	**3**	**4**	**4**
Zs-2	**Zg-27**	**-**	**5**	**-**
Zs-2	**Zg-28**	**2**	**3**	**2**
Zs-2	**Zg-29**	**3**	**5**	**3**
Zs-2	**Zg-30**	**2**	**3**	**-**
Zs-2	**Zg-31**	**-**	**4**	**-**
Zs-2	**Zg-32**	**2**	**3**	**3**
Zs-2	**Zg-33**	**3**	**4**	**3**
Zs-2	**Zg-34**	**2**	**-**	**-**
Zs-2	**Zg-35**	**3**	**4**	**-**
Zs-2	**Zg-36**	**-**	**3**	**3**
Zs-2	**Zg-37**	**2**	**-**	**-**
Zs-3	**Zg-1**	**-**	**6**	**-**
Zs-3	**Zg-2**	**-**	**5**	**-**
Zs-3	**Zg-3**	**-**	**3**	**-**
Zs-3	**Zg-4**	**-**	**3**	**-**
Zs-3	**Zg-5**	**-**	**6**	**-**
Zs-3	**Zg-6**	**-**	**5**	**-**
Zs-3	**Zg-8**	**-**	**3**	**-**
Zs-3	**Zg-10**	**-**	**4**	**-**
Zs-3	**Zg-11**	**-**	**2**	**-**
Zs-3	**Zg-12**	**-**	**3**	**-**
Zs-3	**Zg-13**	**-**	**3**	**-**
Zs-3	**Zg-14**	**-**	**2**	**-**
Zs-3	**Zg-15**	**-**	**5**	**-**
Zs-3	**Zg-16**	**-**	**3**	**-**

Zs-3	**Zg-17**	**-**	**4**	**-**
Zs-3	**Zg-18**	**-**	**3**	**-**
Zs-3	**Zg-24**	**-**	**5**	**-**
Zs-3	**Zg-26**	**-**	**3**	**-**
Zs-3	**Zg-27**	**-**	**3**	**-**
Zs-3	**Zg-28**	**-**	**2**	**-**
Zs-3	**Zg-29**	**-**	**5**	**-**
Zs-3	**Zg-30**	**-**	**3**	**-**
Zs-3	**Zg-31**	**-**	**3**	**-**
Zs-3	**Zg-32**	**-**	**2**	**-**
Zs-3	**Zg-34**	**-**	**2**	**-**
Zs-3	**Zg-35**	**-**	**3**	**-**
Zs-3	**Zg-36**	**-**	**2**	**-**
Zs-4	**Zg-1**	**-**	**4**	**-**
Zs-4	**Zg-2**	**-**	**3**	**-**
Zs-4	**Zg-3**	**-**	**2**	**-**
Zs-4	**Zg-4**	**-**	**2**	**-**
Zs-4	**Zg-5**	**-**	**5**	**-**
Zs-4	**Zg-6**	**-**	**5**	**-**
Zs-4	**Zg-7**	**3**	**-**	**-**
Zs-4	**Zg-8**	**-**	**3**	**-**
Zs-4	**Zg-9**	**2**		**-**
Zs-4	**Zg-10**	**3**	**5**	**-**
Zs-4	**Zg-11**	**3**	**3**	**-**
Zs-4	**Zg-12**	**4**	**4**	**-**
Zs-4	**Zg-13**	**3**	**-**	**-**
Zs-4	**Zg-14**	**2**	**2**	**2**
Zs-4	**Zg-15**	**3**	**2**	**2**
Zs-4	**Zg-16**	**2**	**2**	**2**
Zs-4	**Zg-17**	**3**	**2**	**2**
Zs-4	**Zg-18**	**3**	**-**	**-**
Zs-4	**Zg-19**	**2**	**-**	**-**
Zs-4	**Zg-20**	**3**	**-**	**-**
Zs-4	**Zg-21**	**3**	**-**	**-**
Zs-4	**Zg-22**	**2**	**-**	**-**

Zs-4	**Zg-23**	**3**	**-**	**-**
Zs-4	**Zg-24**	**-**	**5**	**-**
Zs-4	**Zg-25**	**3**	**-**	**-**
Zs-4	**Zg-26**	**2**	**2**	**2**
Zs-4	**Zg-28**	**3**	**2**	**3**
Zs-4	**Zg-29**	**3**	**3**	**-**
Zs-4	**Zg-30**	**-**	**3**	**-**
Zs-4	**Zg-31**	**-**	**2**	**-**
Zs-4	**Zg-32**	**3**	**3**	**3**
Zs-4	**Zg-33**	**3**	**2**	**3**
Zs-4	**Zg-34**	**2**	**2**	**-**
Zs-4	**Zg-35**	**2**	**3**	**-**
Zs-4	**Zg-36**	**-**	**3**	**-**
Zs-4	**Zg-37**	**3**	**-**	**-**
Zs-5	**Zg-1**	**-**	**4**	**-**
Zs-5	**Zg-2**	**-**	**3**	**-**
Zs-5	**Zg-3**	**-**	**2**	**-**
Zs-5	**Zg-4**	**-**	**2**	**-**
Zs-5	**Zg-5**	**-**	**5**	**-**
Zs-5	**Zg-6**	**-**	**5**	**-**
Zs-5	**Zg-8**	**-**	**2**	**2**
Zs-5	**Zg-11**	**-**	**3**	**-**
Zs-5	**Zg-12**	**-**	**4**	**2**
Zs-5	**Zg-13**	**-**	**4**	**2**
Zs-5	**Zg-14**	**-**	**3**	**3**
Zs-5	**Zg-15**	**-**	**4**	**3**
Zs-5	**Zg-16**	**-**	**3**	**3**
Zs-5	**Zg-17**	**-**	**4**	**4**
Zs-5	**Zg-18**	**-**	**5**	**3**
Zs-5	**Zg-20**	**-**	**2**	**3**
Zs-5	**Zg-24**	**-**	**5**	**5**
Zs-5	**Zg-26**	**-**	**3**	**3**
Zs-5	**Zg-27**	**-**	**4**	**-**
Zs-5	**Zg-28**	**-**	**3**	**-**
Zs-5	**Zg-29**	**-**	**4**	**-**

Zs-5	**Zg-30**	**-**	**2**	**-**
Zs-5	**Zg-31**	**-**	**3**	**2**
Zs-5	**Zg-32**	**-**	**2**	**2**
Zs-5	**Zg-33**	**-**	**2**	**3**
Zs-5	**Zg-34**	**-**	**2**	**-**
Zs-5	**Zg-35**	**-**	**3**	**-**
Zs-6	**Zg-1**	**-**	**4**	**-**
Zs-6	**Zg-2**	**-**	**3**	**-**
Zs-6	**Zg-7**	**3**	**-**	**-**
Zs-6	**Zg-8**	**-**	**2**	**-**
Zs-6	**Zg-11**	**3**	**3**	**-**
Zs-6	**Zg-12**	**3**	**3**	**-**
Zs-6	**Zg-13**	**2**	**-**	**-**
Zs-6	**Zg-14**	**2**	**2**	**-**
Zs-6	**Zg-16**	**3**	**-**	**-**
Zs-6	**Zg-17**	**3**	**4**	**-**
Zs-6	**Zg-21**	**3**	**4**	**4**
Zs-6	**Zg-23**	**4**	**-**	**-**
Zs-6	**Zg-26**	**3**	**5**	**3**
Zs-6	**Zg-27**	**-**	**4**	**-**
Zs-6	**Zg-28**	**-**	**2**	**-**
Zs-6	**Zg-29**	**-**	**3**	**-**
Zs-7	**Zg-1**	**-**	**4**	**-**
Zs-7	**Zg-2**	**-**	**3**	**-**
Zs-7	**Zg-8**	**-**	**3**	**3**
Zs-7	**Zg-11**	**-**	**3**	**-**
Zs-7	**Zg-13**	**-**	**3**	**2**
Zs-7	**Zg-14**	**-**	**2**	**2**
Zs-7	**Zg-15**	**-**	**4**	**3**
Zs-7	**Zg-16**	**-**	**3**	**2**
Zs-7	**Zg-18**	**-**	**5**	**3**
Zs-7	**Zg-26**	**-**	**3**	**3**
Zs-7	**Zg-28**	**-**	**3**	**-**
Zs-7	**Zg-29**	**-**	**5**	**-**
Zs-7	**Zg-30**	**-**	**2**	**2**

Zs-7	**Zg-31**	**-**	**4**	**-**
Zs-7	**Zg-32**	**-**	**3**	**4**
Zs-7	**Zg-33**	**-**	**2**	**2**
Zs-7	**Zg-35**	**-**	**3**	**2**
Zs-7	**Zg-36**	**-**	**2**	**2**
Zs-8	**Zg-1**	**-**	**4**	**-**
Zs-8	**Zg-7**	**2**	**-**	**-**
Zs-8	**Zg-8**	**-**	**3**	**-**
Zs-8	**Zg-14**	**2**	**-**	**-**
Zs-8	**Zg-15**	**-**	**2**	**-**
Zs-9	**Zg-1**	**-**	**4**	**-**
Zs-9	**Zg-7**	**2**	**-**	**-**
Zs-9	**Zg-14**	**2**	**-**	**-**
Zs-9	**Zg-15**	**-**	**2**	**-**
Zs-11	**Zg-1**	**-**	**4**	**-**
Zs-11	**Zg-4**	**-**	**3**	**-**
Zs-11	**Zg-12**	**-**	**3**	**-**
Zs-11	**Zg-14**	**-**	**3**	**-**
Zs-11	**Zg-15**	**-**	**4**	**-**
Zs-11	**Zg-16**	**-**	**4**	**-**
Zs-11	**Zg-30**	**-**	**3**	**2**
Zs-12	**Zg-1**	**-**	**4**	**-**
Zs-12	**Zg-4**	**-**	**3**	**-**
Zs-12	**Zg-7**	**-**	**3**	**-**
Zs-12	**Zg-8**	**-**	**3**	**3**
Zs-12	**Zg-12**	**3**	**3**	**-**
Zs-12	**Zg-14**	**2**	**2**	**-**
Zs-12	**Zg-15**	**-**	**3**	**-**
Zs-12	**Zg-16**	**3**	**2**	**-**
Zs-12	**Zg-17**	**3**	**5**	**4**
Zs-12	**Zg-23**	**3**	**-**	**-**
Zs-12	**Zg-26**	**3**	**2**	**-**
Zs-12	**Zg-28**	**-**	**4**	**-**
Zs-12	**Zg-29**	**-**	**6**	**-**
Zs-12	**Zg-30**	**2**	**4**	**4**

Zs-12	**Zg-31**	**-**	**4**	**-**
Zs-12	**Zg-32**	**-**	**4**	**-**
Zs-13	**Zg-1**	**-**	**4**	**-**
Zs-13	**Zg-8**	**-**	**2**	**-**
Zs-13	**Zg-14**	**-**	**3**	**-**
Zs-13	**Zg-15**	**-**	**5**	**-**
Zs-13	**Zg-28**	**-**	**4**	**-**
Zs-13	**Zg-31**	**-**	**4**	**-**
Zs-13	**Zg-32**	**-**	**3**	**-**
Zs-14	**Zg-15**	**-**	**5**	**-**
Zs-15	**Zg-15**	**-**	**5**	**-**
Zs-16	**Zg-15**	**-**	**5**	**-**
Zs-17	**Zg-1**	**-**	**4**	**-**
Zs-17	**Zg-2**	**-**	**3**	**-**
Zs-17	**Zg-4**	**-**	**2**	**-**
Zs-17	**Zg-8**	**-**	**3**	**-**
Zs-17	**Zg-10**	**-**	**5**	**-**
Zs-17	**Zg-15**	**-**	**5**	**-**
Zs-17	**Zg-18**	**-**	**3**	**-**
Zs-17	**Zg-24**	**-**	**5**	**-**
Zs-17	**Zg-27**	**-**	**3**	**-**

12 Określenie poziomu ryzyk

Kolejnym etapem będzie określenie potencjalnych zagrożeń dla działalności jednostki organizacyjnej, poprzez oszacowanie potencjalnych strat wynikających z ujawnienia, utraty, modyfikacji lub braku dostępu do każdej zidentyfikowanej kategorii zasobów systemu. Aby to zrobić, konieczne będzie uwzględnienie:

a) Wartości informacji, wyznaczonej przez wymagania dotyczące ochrony ich integralności, poufności i dostępności, reprezentowane przez wartości liczbowe opisujące skutki ich ujawnienia, utraty, modyfikacji lub braku dostępności.

b) Zagrożeń, które mogą wpłynąć na te wymagania.
c) Zidentyfikowanych podatności na te zagrożenia, reprezentowane przez oszacowane wartości liczbowe.

Efektem tego procesu będzie wartość ryzyka określona dla każdej kategorii zasobów systemu i zagrożenia, uzyskana poprzez pomnożenie wartości odpowiadających skutkom i podatności. Obliczone wartości liczbowe zostaną wpisane w odpowiednie komórki macierzy.

Kolejnym krokiem będzie przekształcenie obliczonych wartości liczbowych ryzyka na poziomy wielkości ryzyka dla każdej kategorii zasobów systemu i zagrożenia. Zaproponowane poziomy wielkości ryzyka dla obliczonych wartości liczbowych ryzyka to:

Niski (1-20)
Średni (21-60)
Wysoki (61-80)
Maksymalny (81-100)
Przy użyciu kolorowania lub podkreślenia zostaną wyodrębnione komórki macierzy o jednakowym poziomie ryzyka. Określenie wielkości ryzyka pozwoli skupić uwagę na obszarach, które mogą mieć największy potencjalny wpływ na działalność jednostki organizacyjnej, podczas gdy inne ryzyka o niższym poziomie mogą być akceptowalne.

W pełnym zakresie analizy ryzyka należy również uwzględnić inne ryzyka, takie jak utrata zaufania publicznego, utrata korzyści ze współpracy, itp. Zakres procesu analizy zależy od ustaleń dokonanych we wstępnej fazie i zaakceptowanych przez kierownictwo jednostki organizacyjnej.

Warto zauważyć, że większość strat jest spowodowana przypadkowymi zdarzeniami, ze względu na wysokie prawdopodobieństwo ich wystąpienia i

częstotliwość, chociaż wpływ każdego takiego zdarzenia jest zazwyczaj ograniczony. Zagrożenia losowe, szczególnie pożar, stanowią istotne wyjątki (niskie prawdopodobieństwo, ale duże straty).

Z drugiej strony, działania celowe (umyślne) wydają się mieć bardziej niebezpieczne skutki, ale cechuje je mniejsze prawdopodobieństwo i częstotliwość. Przykłady to formy przestępstw, które często są popełniane przez dobrze wykształconych pracowników, takie jak kradzież i oszustwo. Mogą one powodować materialne straty, ponieważ przestępcy ci posiadają rozległą wiedzę na temat działania systemów i mają dostęp do specyficznych narzędzi umożliwiających popełnienie i ukrycie działalności kryminalnej.

W opracowanej metodologii określono poziomy ryzyka w oparciu o oszacowanie podatności zasobów w Systemie teleinformatycznego względem zidentyfikowanych zagrożeń dotyczących poufności, integralności i dostępności tych zasobów, a także uwzględniono skutki utraty tych zasobów pod kątem poufności, dostępności i integralności.

Aby skutecznie zarządzać ryzykiem związanym z bezpieczeństwem informacji niejawnych przetwarzanych w Systemie teleinformatycznego, przyporządkowano właścicieli każdemu z ryzyk.

Wyniki oceny poziomu ryzyka zostały zestawione w tabeli:

Odpowiedzialność	Zasób	Zagrożenie	Przeciwdziałanie	Wpływ na	Podatność	Skutek	Poziom ryzyka	Poziom ryzyka
AS	ZAS-1	ZAG-13		Poufność	2	7	14	niski
AS	ZAS-1	ZAG-13		Poufność	2	7	14	niski
AS	ZAS-1	ZAG-17		Poufność	3	7	21	średni

Odpowiedzialność	Zasób	Zagrożenie	Przeciwdziałanie	Wpływ na	Podatność	Skutek	Poziom ryzyka	Poziom ryzyka
AS	ZAS-1	ZAG-17		Dostępność	4	7	28	średni
AS	ZAS-1	ZAG-17		Integralność	4	8	32	średni
AS	ZAS-1	ZAG-18		Poufność	2	7	14	niski
AS	ZAS-1	ZAG-18		Dostępność	3	7	21	średni
AS	ZAS-1	ZAG-19		Poufność	4	7	28	średni
AS	ZAS-1	ZAG-20		Poufność	3	7	21	średni
AS	ZAS-1	ZAG-20		Integralność	3	8	24	średni
AS	ZAS-1	ZAG-31		Dostępność	4	7	28	średni
AS	ZAS-1	ZAG-33		Poufność	3	7	21	średni
AS	ZAS-1	ZAG-33		Dostępność	4	7	28	średni
AS	ZAS-1	ZAG-33		Integralność	3	8	24	średni
AS	ZAS-1	ZAG-35		Poufność	3	7	21	średni
AS	ZAS-1	ZAG-35		Dostępność	4	7	28	średni
AS	ZAS-1	ZAG-36		Dostępność	3	7	21	średni
AS	ZAS-1	ZAG-36		Integralność	3	8	24	średni
AS	ZAS-2	ZAG-13		Poufność	2	7	14	niski
AS	ZAS-2	ZAG-17		Poufność	3	7	21	średni
AS	ZAS-2	ZAG-17		Dostępność	4	7	28	średni
AS	ZAS-2	ZAG-17		Integralność	4	8	32	średni
AS	ZAS-2	ZAG-18		Poufność	2	7	14	niski
AS	ZAS-2	ZAG-18		Dostępność	3	7	21	średni
AS	ZAS-2	ZAG-19		Poufność	4	7	28	średni
AS	ZAS-2	ZAG-20		Poufność	3	7	21	średni
AS	ZAS-2	ZAG-20		Integralność	3	8	24	średni
AS	ZAS-2	ZAG-31		Dostępność	4	7	28	średni
AS	ZAS-2	ZAG-33		Poufność	3	7	21	średni
AS	ZAS-2	ZAG-33		Dostępność	4	7	28	średni

Odpowiedzialność	Zasób	Zagrożenie	Przeciwdziałanie	Wpływ na	Podatność	Skutek	Poziom ryzyka	Poziom ryzyka
AS	ZAS-2	ZAG-33		Integralność	3	8	24	średni
AS	ZAS-2	ZAG-35		Poufność	3	7	21	średni
AS	ZAS-2	ZAG-35		Dostępność	4	7	28	średni
AS	ZAS-2	ZAG-36		Dostępność	3	7	21	średni
AS	ZAS-2	ZAG-36		Integralność	3	8	24	średni
AS	ZAS-3	ZAG-13		Dostępność	3	7	21	średni
AS	ZAS-3	ZAG-17		Dostępność	4	7	28	średni
AS	ZAS-3	ZAG-18		Dostępność	3	7	21	średni
AS	ZAS-3	ZAG-31		Dostępność	3	7	21	średni
AS	ZAS-3	ZAG-35		Dostępność	3	7	21	średni
AS	ZAS-3	ZAG-36		Dostępność	2	7	14	niski
AS	ZAS-4	ZAG-13		Poufność	3	6	18	niski
AS	ZAS-4	ZAG-17		Poufność	3	6	18	niski
AS	ZAS-4	ZAG-17		Dostępność	2	8	16	niski
AS	ZAS-4	ZAG-17		Integralność	2	7	14	niski
AS	ZAS-4	ZAG-18		Poufność	3	6	18	niski
AS	ZAS-4	ZAG-19		Poufność	2	7	14	niski
AS	ZAS-4	ZAG-20		Poufność	3	6	18	niski
AS	ZAS-4	ZAG-31		Dostępność	2	8	16	niski
AS	ZAS-4	ZAG-33		Poufność	3	6	18	niski
AS	ZAS-4	ZAG-33		Dostępność	2	8	16	niski
AS	ZAS-4	ZAG-33		Integralność	3	7	21	średni
AS	ZAS-4	ZAG-35		Poufność	2	6	12	niski
AS	ZAS-4	ZAG-35		Dostępność	3	8	24	średni
AS	ZAS-4	ZAG-36		Dostępność	3	8	24	średni
AS	ZAS-5	ZAG-13		Dostępność	4	8	32	średni
AS	ZAS-5	ZAG-13		Integralność	2	9	18	niski

Odpowiedzialność	Zasób	Zagrożenie	Przeciwdziałanie	Wpływ na	Podatność	Skutek	Poziom ryzyka	Poziom ryzyka
AS	ZAS-5	ZAG-17		Dostępność	4	8	32	średni
AS	ZAS-5	ZAG-17		Integralność	4	9	36	średni
AS	ZAS-5	ZAG-18		Dostępność	5	8	40	średni
AS	ZAS-5	ZAG-18		Integralność	3	9	27	średni
AS	ZAS-5	ZAG-20		Dostępność	2	8	16	niski
AS	ZAS-5	ZAG-20		Integralność	3	9	27	średni
AS	ZAS-5	ZAG-31		Dostępność	3	8	24	średni
AS	ZAS-5	ZAG-31		Integralność	2	9	18	niski
AS	ZAS-5	ZAG-33		Dostępność	2	8	16	niski
AS	ZAS-5	ZAG-33		Integralność	3	9	27	średni
AS	ZAS-6	ZAG-13		Poufność	2	7	14	niski
AS	ZAS-6	ZAG-17		Poufność	3	7	21	średni
AS	ZAS-6	ZAG-17		Dostępność	4	8	32	średni
AS	ZAS-7	ZAG-13		Dostępność	3	7	21	średni
AS	ZAS-7	ZAG-13		Integralność	2	9	18	niski
AS	ZAS-7	ZAG-18		Dostępność	5	7	35	średni
AS	ZAS-7	ZAG-18		Integralność	3	9	27	średni
AS	ZAS-7	ZAG-31		Dostępność	4	7	28	średni
AS	ZAS-7	ZAG-33		Dostępność	2	7	14	niski
AS	ZAS-7	ZAG-33		Integralność	2	9	18	niski
AS	ZAS-7	ZAG-35		Dostępność	3	7	21	średni
AS	ZAS-7	ZAG-35		Integralność	2	9	18	niski
AS	ZAS-7	ZAG-36		Dostępność	2	7	14	niski
AS	ZAS-7	ZAG-36		Integralność	2	9	18	niski
AS	ZAS-12	ZAG-17		Poufność	3	7	21	średni
AS	ZAS-12	ZAG-17		Dostępność	5	7	35	średni
AS	ZAS-12	ZAG-17		Integralność	4	9	36	średni

Odpowiedzialność	Zasób	Zagrożenie	Przeciwdziałanie	Wpływ na	Podatność	Skutek	Poziom ryzyka	Poziom ryzyka
AS	ZAS-12	ZAG-31		Dostępność	4	7	28	średni
AS	ZAS-13	ZAG-31		Dostępność	4	8	32	średni
AS	ZAS-17	ZAG-18		Dostępność	3	7	21	średni
AS	ZAS-18	ZAG-31		Dostępność	4	8	32	średni
AS	ZAS-18	ZAG-18		Dostępność	3	7	21	średni
AS	ZAS-19	ZAG-31		Dostępność	4	8	32	średni
AS	ZAS-19	ZAG-18		Dostępność	3	7	21	średni
AS	ZAS-20	ZAG-31		Dostępność	4	8	32	średni
AS	ZAS-20	ZAG-18		Dostępność	3	7	21	średni
AS	ZAS-20	ZAG-31		Dostępność	4	8	32	średni
IBTI	ZAS-1	ZAG-5		Dostępność	5	7	35	średni
IBTI	ZAS-1	ZAG-6		Dostępność	4	7	28	średni
IBTI	ZAS-1	ZAG-9		Poufność	2	7	14	niski
IBTI	ZAS-1	ZAG-10		Poufność	3	7	21	średni
IBTI	ZAS-1	ZAG-10		Dostępność	5	7	35	średni
IBTI	ZAS-1	ZAG-21		Poufność	4	7	28	średni
IBTI	ZAS-1	ZAG-22		Poufność	3	7	21	średni
IBTI	ZAS-1	ZAG-24		Dostępność	6	7	42	średni
IBTI	ZAS-1	ZAG-28		Poufność	2	7	14	niski
IBTI	ZAS-1	ZAG-28		Dostępność	3	7	21	średni
IBTI	ZAS-1	ZAG-28		Integralność	2	8	16	niski
IBTI	ZAS-1	ZAG-29		Poufność	3	7	21	średni
IBTI	ZAS-1	ZAG-29		Dostępność	5	7	35	średni
IBTI	ZAS-1	ZAG-29		Integralność	3	8	24	średni
IBTI	ZAS-1	ZAG-32		Poufność	2	7	14	niski
IBTI	ZAS-1	ZAG-32		Dostępność	3	7	21	średni
IBTI	ZAS-1	ZAG-32		Integralność	3	8	24	średni

Odpowiedzialność	Zasób	Zagrożenie	Przeciwdziałanie	Wpływ na	Podatność	Skutek	Poziom ryzyka	Poziom ryzyka
IBTI	ZAS-1	ZAG-34		Poufność	2	7	14	niski
IBTI	ZAS-1	ZAG-37		Poufność	2	7	14	niski
IBTI	ZAS-2	ZAG-5		Dostępność	5	7	35	średni
IBTI	ZAS-2	ZAG-6		Dostępność	4	7	28	średni
IBTI	ZAS-2	ZAG-9		Poufność	2	7	14	niski
IBTI	ZAS-2	ZAG-10		Poufność	3	7	21	średni
IBTI	ZAS-2	ZAG-10		Dostępność	5	7	35	średni
IBTI	ZAS-2	ZAG-21		Poufność	4	7	28	średni
IBTI	ZAS-2	ZAG-22		Poufność	3	7	21	średni
IBTI	ZAS-2	ZAG-24		Dostępność	6	7	42	średni
IBTI	ZAS-2	ZAG-28		Poufność	2	7	14	niski
IBTI	ZAS-2	ZAG-28		Dostępność	3	7	21	średni
IBTI	ZAS-2	ZAG-28		Integralność	2	8	16	niski
IBTI	ZAS-2	ZAG-29		Poufność	3	7	21	średni
IBTI	ZAS-2	ZAG-29		Dostępność	5	7	35	średni
IBTI	ZAS-2	ZAG-29		Integralność	3	8	24	średni
IBTI	ZAS-2	ZAG-32		Poufność	2	7	14	niski
IBTI	ZAS-2	ZAG-32		Dostępność	3	7	21	średni
IBTI	ZAS-2	ZAG-32		Integralność	3	8	24	średni
IBTI	ZAS-2	ZAG-34		Poufność	2	7	14	niski
IBTI	ZAS-2	ZAG-37		Poufność	2	7	14	niski
IBTI	ZAS-3	ZAG-5		Dostępność	6	7	42	średni
IBTI	ZAS-3	ZAG-6		Dostępność	5	7	35	średni
IBTI	ZAS-3	ZAG-10		Dostępność	4	7	28	średni
IBTI	ZAS-3	ZAG-24		Dostępność	5	7	35	średni
IBTI	ZAS-3	ZAG-28		Dostępność	2	7	14	niski
IBTI	ZAS-3	ZAG-29		Dostępność	5	7	35	średni

Odpowiedzialność	Zasób	Zagrożenie	Przeciwdziałanie	Wpływ na	Podatność	Skutek	Poziom ryzyka	Poziom ryzyka
IBTI	ZAS-3	ZAG-32		Dostępność	2	7	14	niski
IBTI	ZAS-3	ZAG-34		Dostępność	2	7	14	niski
IBTI	ZAS-4	ZAG-5		Dostępność	5	8	40	średni
IBTI	ZAS-4	ZAG-6		Dostępność	5	8	40	średni
IBTI	ZAS-4	ZAG-9		Poufność	2	6	12	niski
IBTI	ZAS-4	ZAG-10		Poufność	3	6	18	niski
IBTI	ZAS-4	ZAG-10		Dostępność	5	8	40	średni
IBTI	ZAS-4	ZAG-21		Poufność	3	6	18	niski
IBTI	ZAS-4	ZAG-22		Poufność	2	6	12	niski
IBTI	ZAS-4	ZAG-24		Dostępność	5	8	40	średni
IBTI	ZAS-4	ZAG-28		Poufność	3	6	18	niski
IBTI	ZAS-4	ZAG-28		Dostępność	2	8	16	niski
IBTI	ZAS-4	ZAG-28		Integralność	3	7	21	średni
IBTI	ZAS-4	ZAG-29		Poufność	3	6	18	niski
IBTI	ZAS-4	ZAG-29		Dostępność	3	8	24	średni
IBTI	ZAS-4	ZAG-32		Poufność	3	6	18	niski
IBTI	ZAS-4	ZAG-32		Dostępność	3	8	24	średni
IBTI	ZAS-4	ZAG-32		Integralność	3	7	21	średni
IBTI	ZAS-4	ZAG-34		Poufność	2	6	12	niski
IBTI	ZAS-4	ZAG-34		Dostępność	2	8	16	niski
IBTI	ZAS-4	ZAG-37		Poufność	3	6	18	niski
IBTI	ZAS-5	ZAG-6		Dostępność	5	8	40	średni
IBTI	ZAS-5	ZAG-24		Dostępność	5	8	40	średni
IBTI	ZAS-5	ZAG-24		Integralność	3	9	27	średni
IBTI	ZAS-5	ZAG-28		Dostępność	3	8	24	średni
IBTI	ZAS-5	ZAG-29		Dostępność	4	8	32	średni
IBTI	ZAS-5	ZAG-32		Dostępność	2	8	16	niski

Odpowiedzialność	Zasób	Zagrożenie	Przeciwdziałanie	Wpływ na	Podatność	Skutek	Poziom ryzyka	Poziom ryzyka
IBTI	ZAS-5	ZAG-32		Integralność	2	9	18	niski
IBTI	ZAS-5	ZAG-34		Dostępność	2	8	16	niski
IBTI	ZAS-5	ZAG-35		Dostępność	3	8	24	średni
IBTI	ZAS-6	ZAG-21		Poufność	3	7	21	średni
IBTI	ZAS-6	ZAG-21		Dostępność	4	8	32	średni
IBTI	ZAS-6	ZAG-21		Integralność	4	8	32	średni
IBTI	ZAS-6	ZAG-28		Dostępność	2	8	16	niski
IBTI	ZAS-6	ZAG-29		Dostępność	3	8	24	średni
IBTI	ZAS-7	ZAG-28		Dostępność	3	7	21	średni
IBTI	ZAS-7	ZAG-29		Dostępność	5	7	35	średni
IBTI	ZAS-7	ZAG-32		Dostępność	3	7	21	średni
IBTI	ZAS-7	ZAG-32		Integralność	4	9	36	średni
IBTI	ZAS-12	ZAG-28		Dostępność	4	7	28	średni
IBTI	ZAS-12	ZAG-29		Dostępność	6	7	42	średni
IBTI	ZAS-12	ZAG-32		Dostępność	4	7	28	średni
IBTI	ZAS-13	ZAG-28		Dostępność	4	8	32	średni
IBTI	ZAS-13	ZAG-32		Dostępność	3	8	24	średni
IBTI	ZAS-17	ZAG-10		Dostępność	5	7	35	średni
IBTI	ZAS-17	ZAG-24		Dostępność	5	7	35	średni
IBTI	ZAS-18	ZAG-28		Dostępność	4	8	32	średni
IBTI	ZAS-18	ZAG-32		Dostępność	3	8	24	średni
IBTI	ZAS-18	ZAG-10		Dostępność	5	7	35	średni
IBTI	ZAS-18	ZAG-24		Dostępność	5	7	35	średni
IBTI	ZAS-19	ZAG-28		Dostępność	4	8	32	średni
IBTI	ZAS-19	ZAG-32		Dostępność	3	8	24	średni
IBTI	ZAS-19	ZAG-10		Dostępność	5	7	35	średni
IBTI	ZAS-19	ZAG-24		Dostępność	5	7	35	średni

Odpowiedzialność	Zasób	Zagrożenie	Przeciwdziałanie	Wpływ na	Podatność	Skutek	Poziom ryzyka	Poziom ryzyka
IBTI	ZAS-20	ZAG-28		Dostępność	4	8	32	średni
IBTI	ZAS-20	ZAG-32		Dostępność	3	8	24	średni
IBTI	ZAS-20	ZAG-10		Dostępność	5	7	35	średni
IBTI	ZAS-20	ZAG-24		Dostępność	5	7	35	średni
IBTI	ZAS-20	ZAG-28		Dostępność	4	8	32	średni
IBTI	ZAS-20	ZAG-32		Dostępność	3	8	24	średni
INTI	ZAS-5	ZAG-5		Dostępność	5	8	40	średni
KJO	ZAS-1	ZAG-14		Poufność	3	7	21	średni
KJO	ZAS-1	ZAG-14		Dostępność	2	7	14	niski
KJO	ZAS-1	ZAG-14		Integralność	2	8	16	niski
KJO	ZAS-1	ZAG-15		Poufność	3	7	21	średni
KJO	ZAS-1	ZAG-15		Dostępność	2	7	14	niski
KJO	ZAS-1	ZAG-15		Integralność	2	8	16	niski
KJO	ZAS-2	ZAG-14		Poufność	3	7	21	średni
KJO	ZAS-2	ZAG-14		Dostępność	2	7	14	niski
KJO	ZAS-2	ZAG-14		Integralność	2	8	16	niski
KJO	ZAS-2	ZAG-15		Poufność	3	7	21	średni
KJO	ZAS-2	ZAG-15		Dostępność	2	7	14	niski
KJO	ZAS-2	ZAG-15		Integralność	2	8	16	niski
KJO	ZAS-3	ZAG-14		Dostępność	2	7	14	niski
KJO	ZAS-3	ZAG-15		Dostępność	5	7	35	średni
KJO	ZAS-4	ZAG-14		Poufność	2	6	12	niski
KJO	ZAS-4	ZAG-14		Dostępność	2	8	16	niski
KJO	ZAS-4	ZAG-14		Integralność	2	7	14	niski
KJO	ZAS-4	ZAG-15		Poufność	3	6	18	niski
KJO	ZAS-4	ZAG-15		Dostępność	2	8	16	niski
KJO	ZAS-4	ZAG-15		Integralność	2	7	14	niski

Odpowiedzialność	Zasób	Zagrożenie	Przeciwdziałanie	Wpływ na	Podatność	Skutek	Poziom ryzyka	Poziom ryzyka
KJO	ZAS-5	ZAG-14		Dostępność	3	8	24	średni
KJO	ZAS-5	ZAG-14		Integralność	3	9	27	średni
KJO	ZAS-5	ZAG-15		Dostępność	4	8	32	średni
KJO	ZAS-5	ZAG-15		Integralność	3	9	27	średni
KJO	ZAS-6	ZAG-14		Poufność	2	7	14	niski
KJO	ZAS-6	ZAG-14		Dostępność	2	8	16	niski
KJO	ZAS-7	ZAG-14		Dostępność	2	7	14	niski
KJO	ZAS-7	ZAG-14		Integralność	2	9	18	niski
KJO	ZAS-7	ZAG-15		Dostępność	4	7	28	średni
KJO	ZAS-7	ZAG-15		Integralność	3	9	27	średni
KJO	ZAS-8	ZAG-14		Poufność	2	6	12	niski
KJO	ZAS-8	ZAG-15		Dostępność	2	8	16	niski
KJO	ZAS-9	ZAG-14		Poufność	2	7	14	niski
KJO	ZAS-9	ZAG-15		Dostępność	2	8	16	niski
KJO	ZAS-11	ZAG-14		Dostępność	3	7	21	średni
KJO	ZAS-11	ZAG-15		Dostępność	4	7	28	średni
KJO	ZAS-11	ZAG-15		Dostępność	4	7	28	średni
KJO	ZAS-12	ZAG-14		Poufność	2	7	14	niski
KJO	ZAS-12	ZAG-14		Dostępność	2	7	14	niski
KJO	ZAS-12	ZAG-15		Dostępność	3	7	21	średni
KJO	ZAS-13	ZAG-14		Dostępność	3	8	24	średni
KJO	ZAS-13	ZAG-15		Dostępność	5	8	40	średni
KJO	ZAS-14	ZAG-15		Dostępność	5	6	30	średni
KJO	ZAS-15	ZAG-15		Dostępność	5	7	35	średni
KJO	ZAS-16	ZAG-15		Dostępność	5	7	35	średni
KJO	ZAS-17	ZAG-15		Dostępność	5	7	35	średni
KJO	ZAS-18	ZAG-14		Dostępność	3	8	24	średni

Odpowiedzialność	Zasób	Zagrożenie	Przeciwdziałanie	Wpływ na	Podatność	Skutek	Poziom ryzyka	Poziom ryzyka
KJO	ZAS-18	ZAG-15		Dostępność	5	8	40	średni
KJO	ZAS-18	ZAG-15		Dostępność	5	6	30	średni
KJO	ZAS-18	ZAG-15		Dostępność	5	7	35	średni
KJO	ZAS-18	ZAG-15		Dostępność	5	7	35	średni
KJO	ZAS-18	ZAG-15		Dostępność	5	7	35	średni
KJO	ZAS-19	ZAG-14		Dostępność	3	8	24	średni
KJO	ZAS-19	ZAG-15		Dostępność	5	8	40	średni
KJO	ZAS-19	ZAG-15		Dostępność	5	6	30	średni
KJO	ZAS-19	ZAG-15		Dostępność	5	7	35	średni
KJO	ZAS-19	ZAG-15		Dostępność	5	7	35	średni
KJO	ZAS-19	ZAG-15		Dostępność	5	7	35	średni
KJO	ZAS-20	ZAG-14		Dostępność	3	8	24	średni
KJO	ZAS-20	ZAG-15		Dostępność	5	8	40	średni
KJO	ZAS-20	ZAG-15		Dostępność	5	6	30	średni
KJO	ZAS-20	ZAG-15		Dostępność	5	7	35	średni
KJO	ZAS-20	ZAG-15		Dostępność	5	7	35	średni
KJO	ZAS-20	ZAG-15		Dostępność	5	7	35	średni
KJO	ZAS-20	ZAG-14		Dostępność	3	8	24	średni
KJO	ZAS-20	ZAG-15		Dostępność	5	8	40	średni
POIN	ZAS-1	ZAG-1		Dostępność	4	7	28	średni
POIN	ZAS-1	ZAG-2		Dostępność	5	7	35	średni
POIN	ZAS-1	ZAG-3		Dostępność	3	7	21	średni
POIN	ZAS-1	ZAG-4		Dostępność	3	7	21	średni
POIN	ZAS-1	ZAG-7		Poufność	5	7	35	średni
POIN	ZAS-1	ZAG-8		Dostępność	3	7	21	średni
POIN	ZAS-1	ZAG-11		Poufność	3	7	21	średni
POIN	ZAS-1	ZAG-11		Dostępność	3	7	21	średni

Odpowiedzialność	Zasób	Zagrożenie	Przeciwdziałanie	Wpływ na	Podatność	Skutek	Poziom ryzyka	Poziom ryzyka
POIN	ZAS-1	ZAG-12		Poufność	3	7	21	średni
POIN	ZAS-1	ZAG-12		Dostępność	3	7	21	średni
POIN	ZAS-1	ZAG-16		Poufność	2	7	14	niski
POIN	ZAS-1	ZAG-16		Dostępność	2	7	14	niski
POIN	ZAS-1	ZAG-16		Integralność	3	8	24	średni
POIN	ZAS-1	ZAG-23		Poufność	5	7	35	średni
POIN	ZAS-1	ZAG-25		Poufność	3	7	21	średni
POIN	ZAS-1	ZAG-26		Poufność	3	7	21	średni
POIN	ZAS-1	ZAG-26		Dostępność	4	7	28	średni
POIN	ZAS-1	ZAG-26		Integralność	4	8	32	średni
POIN	ZAS-1	ZAG-27		Dostępność	5	7	35	średni
POIN	ZAS-1	ZAG-30		Poufność	2	7	14	niski
POIN	ZAS-1	ZAG-30		Dostępność	3	7	21	średni
POIN	ZAS-2	ZAG-1		Dostępność	4	7	28	średni
POIN	ZAS-2	ZAG-2		Dostępność	5	7	35	średni
POIN	ZAS-2	ZAG-3		Dostępność	3	7	21	średni
POIN	ZAS-2	ZAG-4		Dostępność	3	7	21	średni
POIN	ZAS-2	ZAG-7		Poufność	5	7	35	średni
POIN	ZAS-2	ZAG-8		Dostępność	3	7	21	średni
POIN	ZAS-2	ZAG-11		Poufność	3	7	21	średni
POIN	ZAS-2	ZAG-11		Dostępność	3	7	21	średni
POIN	ZAS-2	ZAG-12		Poufność	3	7	21	średni
POIN	ZAS-2	ZAG-12		Dostępność	3	7	21	średni
POIN	ZAS-2	ZAG-16		Poufność	2	7	14	niski
POIN	ZAS-2	ZAG-16		Dostępność	2	7	14	niski
POIN	ZAS-2	ZAG-16		Integralność	3	8	24	średni
POIN	ZAS-2	ZAG-23		Poufność	5	7	35	średni

Odpowiedzialność	Zasób	Zagrożenie	Przeciwdziałanie	Wpływ na	Podatność	Skutek	Poziom ryzyka	Poziom ryzyka
POIN	ZAS-2	ZAG-25		Poufność	3	7	21	średni
POIN	ZAS-2	ZAG-26		Poufność	3	7	21	średni
POIN	ZAS-2	ZAG-26		Integralność	4	8	32	średni
POIN	ZAS-2	ZAG-27		Dostępność	5	7	35	średni
POIN	ZAS-2	ZAG-30		Poufność	2	7	14	niski
POIN	ZAS-2	ZAG-30		Dostępność	3	7	21	średni
POIN	ZAS-3	ZAG-1		Dostępność	6	7	42	średni
POIN	ZAS-3	ZAG-2		Dostępność	5	7	35	średni
POIN	ZAS-3	ZAG-3		Dostępność	3	7	21	średni
POIN	ZAS-3	ZAG-4		Dostępność	3	7	21	średni
POIN	ZAS-3	ZAG-8		Dostępność	3	7	21	średni
POIN	ZAS-3	ZAG-11		Dostępność	2	7	14	niski
POIN	ZAS-3	ZAG-12		Dostępność	3	7	21	średni
POIN	ZAS-3	ZAG-16		Dostępność	3	7	21	średni
POIN	ZAS-3	ZAG-26		Dostępność	3	7	21	średni
POIN	ZAS-3	ZAG-27		Dostępność	3	7	21	średni
POIN	ZAS-3	ZAG-30		Dostępność	3	7	21	średni
POIN	ZAS-4	ZAG-1		Dostępność	4	8	32	średni
POIN	ZAS-4	ZAG-2		Dostępność	3	8	24	średni
POIN	ZAS-4	ZAG-3		Dostępność	2	8	16	niski
POIN	ZAS-4	ZAG-4		Dostępność	2	8	16	niski
POIN	ZAS-4	ZAG-7		Poufność	3	6	18	niski
POIN	ZAS-4	ZAG-8		Dostępność	3	8	24	średni
POIN	ZAS-4	ZAG-11		Poufność	3	6	18	niski
POIN	ZAS-4	ZAG-11		Dostępność	3	8	24	średni
POIN	ZAS-4	ZAG-12		Poufność	4	6	24	średni
POIN	ZAS-4	ZAG-12		Dostępność	4	8	32	średni

Odpowiedzialność	Zasób	Zagrożenie	Przeciwdziałanie	Wpływ na	Podatność	Skutek	Poziom ryzyka	Poziom ryzyka
POIN	ZAS-4	ZAG-16		Poufność	2	6	12	niski
POIN	ZAS-4	ZAG-16		Dostępność	2	8	16	niski
POIN	ZAS-4	ZAG-16		Integralność	2	7	14	niski
POIN	ZAS-4	ZAG-23		Poufność	3	6	18	niski
POIN	ZAS-4	ZAG-25		Poufność	3	6	18	niski
POIN	ZAS-4	ZAG-26		Poufność	2	6	12	niski
POIN	ZAS-4	ZAG-26		Dostępność	2	8	16	niski
POIN	ZAS-4	ZAG-26		Integralność	2	7	14	niski
POIN	ZAS-4	ZAG-30		Dostępność	3	8	24	średni
POIN	ZAS-5	ZAG-1		Dostępność	4	8	32	średni
POIN	ZAS-5	ZAG-2		Dostępność	3	8	24	średni
POIN	ZAS-5	ZAG-3		Dostępność	2	8	16	niski
POIN	ZAS-5	ZAG-4		Dostępność	2	8	16	niski
POIN	ZAS-5	ZAG-8		Dostępność	2	8	16	niski
POIN	ZAS-5	ZAG-8		Integralność	2	9	18	niski
POIN	ZAS-5	ZAG-11		Dostępność	3	8	24	średni
POIN	ZAS-5	ZAG-12		Dostępność	4	8	32	średni
POIN	ZAS-5	ZAG-12		Integralność	2	9	18	niski
POIN	ZAS-5	ZAG-16		Dostępność	3	8	24	średni
POIN	ZAS-5	ZAG-16		Integralność	3	9	27	średni
POIN	ZAS-5	ZAG-26		Dostępność	3	8	24	średni
POIN	ZAS-5	ZAG-26		Integralność	3	9	27	średni
POIN	ZAS-5	ZAG-27		Dostępność	4	8	32	średni
POIN	ZAS-5	ZAG-30		Dostępność	2	8	16	niski
POIN	ZAS-6	ZAG-1		Dostępność	4	8	32	średni
POIN	ZAS-6	ZAG-2		Dostępność	3	8	24	średni
POIN	ZAS-6	ZAG-7		Poufność	3	7	21	średni

Odpowiedzialność	Zasób	Zagrożenie	Przeciwdziałanie	Wpływ na	Podatność	Skutek	Poziom ryzyka	Poziom ryzyka
POIN	ZAS-6	ZAG-8		Dostępność	2	8	16	niski
POIN	ZAS-6	ZAG-11		Poufność	3	7	21	średni
POIN	ZAS-6	ZAG-11		Dostępność	3	8	24	średni
POIN	ZAS-6	ZAG-12		Poufność	3	7	21	średni
POIN	ZAS-6	ZAG-12		Dostępność	3	8	24	średni
POIN	ZAS-6	ZAG-16		Poufność	3	7	21	średni
POIN	ZAS-6	ZAG-23		Poufność	4	7	28	średni
POIN	ZAS-6	ZAG-26		Poufność	3	7	21	średni
POIN	ZAS-6	ZAG-26		Dostępność	5	8	40	średni
POIN	ZAS-6	ZAG-26		Integralność	3	8	24	średni
POIN	ZAS-6	ZAG-27		Dostępność	4	8	32	średni
POIN	ZAS-7	ZAG-1		Dostępność	4	7	28	średni
POIN	ZAS-7	ZAG-2		Dostępność	3	7	21	średni
POIN	ZAS-7	ZAG-8		Dostępność	3	7	21	średni
POIN	ZAS-7	ZAG-8		Integralność	3	9	27	średni
POIN	ZAS-7	ZAG-11		Dostępność	3	7	21	średni
POIN	ZAS-7	ZAG-16		Dostępność	3	7	21	średni
POIN	ZAS-7	ZAG-16		Integralność	2	9	18	niski
POIN	ZAS-7	ZAG-26		Dostępność	3	7	21	średni
POIN	ZAS-7	ZAG-26		Integralność	3	9	27	średni
POIN	ZAS-7	ZAG-30		Dostępność	2	7	14	niski
POIN	ZAS-7	ZAG-30		Integralność	2	9	18	niski
POIN	ZAS-8	ZAG-1		Dostępność	4	8	32	średni
POIN	ZAS-8	ZAG-7		Poufność	2	6	12	niski
POIN	ZAS-8	ZAG-8		Dostępność	3	8	24	średni
POIN	ZAS-9	ZAG-1		Dostępność	4	8	32	średni
POIN	ZAS-9	ZAG-7		Poufność	2	7	14	niski

Odpowiedzialność	Zasób	Zagrożenie	Przeciwdziałanie	Wpływ na	Podatność	Skutek	Poziom ryzyka	Poziom ryzyka
POIN	ZAS-11	ZAG-1		Dostępność	4	7	28	średni
POIN	ZAS-11	ZAG-4		Dostępność	3	7	21	średni
POIN	ZAS-11	ZAG-12		Dostępność	3	7	21	średni
POIN	ZAS-11	ZAG-16		Dostępność	4	7	28	średni
POIN	ZAS-11	ZAG-30		Dostępność	3	7	21	średni
POIN	ZAS-11	ZAG-30		Integralność	2	8	16	niski
POIN	ZAS-12	ZAG-1		Dostępność	4	7	28	średni
POIN	ZAS-12	ZAG-4		Dostępność	3	7	21	średni
POIN	ZAS-12	ZAG-7		Dostępność	3	7	21	średni
POIN	ZAS-12	ZAG-8		Dostępność	3	7	21	średni
POIN	ZAS-12	ZAG-8		Integralność	3	9	27	średni
POIN	ZAS-12	ZAG-12		Poufność	3	7	21	średni
POIN	ZAS-12	ZAG-12		Dostępność	3	7	21	średni
POIN	ZAS-12	ZAG-16		Poufność	3	7	21	średni
POIN	ZAS-12	ZAG-16		Dostępność	2	7	14	niski
POIN	ZAS-12	ZAG-23		Poufność	3	7	21	średni
POIN	ZAS-12	ZAG-26		Poufność	3	7	21	średni
POIN	ZAS-12	ZAG-26		Dostępność	2	7	14	niski
POIN	ZAS-12	ZAG-30		Poufność	2	7	14	niski
POIN	ZAS-12	ZAG-30		Dostępność	4	7	28	średni
POIN	ZAS-12	ZAG-30		Integralność	4	9	36	średni
POIN	ZAS-13	ZAG-1		Dostępność	4	8	32	średni
POIN	ZAS-13	ZAG-8		Dostępność	2	8	16	niski
POIN	ZAS-17	ZAG-1		Dostępność	4	7	28	średni
POIN	ZAS-17	ZAG-2		Dostępność	3	7	21	średni
POIN	ZAS-17	ZAG-4		Dostępność	2	7	14	niski
POIN	ZAS-17	ZAG-8		Dostępność	3	7	21	średni

Odpowiedzialność	Zasób	Zagrożenie	Przeciwdziałanie	Wpływ na	Podatność	Skutek	Poziom ryzyka	Poziom ryzyka
POIN	ZAS-17	ZAG-27		Dostępność	3	7	21	średni
POIN	ZAS-18	ZAG-8		Dostępność	2	8	16	niski
POIN	ZAS-18	ZAG-1		Dostępność	4	7	28	średni
POIN	ZAS-18	ZAG-2		Dostępność	3	7	21	średni
POIN	ZAS-18	ZAG-4		Dostępność	2	7	14	niski
POIN	ZAS-18	ZAG-8		Dostępność	3	7	21	średni
POIN	ZAS-18	ZAG-27		Dostępność	3	7	21	średni
POIN	ZAS-19	ZAG-8		Dostępność	2	8	16	niski
POIN	ZAS-19	ZAG-1		Dostępność	4	7	28	średni
POIN	ZAS-19	ZAG-2		Dostępność	3	7	21	średni
POIN	ZAS-19	ZAG-4		Dostępność	2	7	14	niski
POIN	ZAS-19	ZAG-8		Dostępność	3	7	21	średni
POIN	ZAS-20	ZAG-27		Dostępność	3	7	21	średni
POIN	ZAS-20	ZAG-8		Dostępność	2	8	16	niski
POIN	ZAS-20	ZAG-1		Dostępność	4	7	28	średni
POIN	ZAS-20	ZAG-2		Dostępność	3	7	21	średni
POIN	ZAS-20	ZAG-4		Dostępność	2	7	14	niski
POIN	ZAS-20	ZAG-8		Dostępność	3	7	21	średni
POIN	ZAS-20	ZAG-27		Dostępność	3	7	21	średni
POIN	ZAS-20	ZAG-8		Dostępność	2	8	16	niski
POIN	ZAS-2	ZAG-26		Dostępność	4	7	28	średni

1) Użyte skróty:
   - KJO – Prezes Zarządu xyx – Kierownik Jednostki Organizacyjnej;
   - POIN – Pełnomocnik ds. Ochrony Informacji Niejawnych;
   - IBTI – Inspektor Bezpieczeństwa teleinformatycznego;

- AS – Administrator Systemu „teleinformatycznego”.

2) Oświadczenia właścicieli ryzyk:

Oświadczam, że: • ***Zaznajomiłem/am się z informacjami dotyczącymi ryzyka związanego z bezpieczeństwem informacji niejawnych przetwarzanych w systemie.*** • ***Akceptuję przytoczone oceny poziomów ryzyka.*** • ***Zobowiązuję się do pełnienia roli właściciela tych ryzyk zgodnie z przedstawionymi wyżej informacjami.*** • ***Akceptuje pozostałe ryzyko szczątkowe.***	
Administrator Systemu	**Inspektor** **Bezpieczeństwa Teleinformatycznego**
……..…..……	……..…..……
Pełnomocnik **ds. Ochrony Informacji Niejawnych**	**Kierownik Jednostki Organizacyjnej**
……..…..……	……..…..……

Tabela 16: Oświadczenia właścicieli ryzyk

13 Ocena ryzyka

W wyniku przeprowadzonej analizy ryzyka powstaje hierarchiczna lista potencjalnych zagrożeń dla informacji przetwarzanych w systemie oraz dla zasobów, które ten system chroni. Niezależnie od wybranej metody szacowania ryzyka, czy to manualnie czy z wykorzystaniem specjalistycznego oprogramowania do analizy ryzyka, lista ta ma wyłaniać, które zagrożenia są najpoważniejsze dla jednostki organizacyjnej i dlatego należy je ograniczać w pierwszej kolejności. To z kolei pozwala na właściwy dobór środków zabezpieczających, optymalny zarówno pod względem wymagań dotyczących bezpieczeństwa informacji niejawnych przetwarzanych w systemie TI, jak i nakładów finansowych niezbędnych do zaimplementowania zabezpieczeń.

Na podstawie opracowanej listy zagrożeń określane są szczególne wymagania, jakie projektowany system musi spełnić, aby osiągnąć odpowiedni poziom bezpieczeństwa. To stanowi fundament do stworzenia dokumentów takich jak "Szczególne Wymagania Bezpieczeństwa" oraz "Procedury Bezpiecznej Eksploatacji", niezbędnych do rozpoczęcia procesu akredytacji systemu teleinformatycznego.

Proces szacowania ryzyka zamyka się w sporządzeniu sprawozdania, które jest prezentowane kierownictwu jednostki organizacyjnej. Sprawozdanie to zawiera zestaw wymagań dotyczących bezpieczeństwa systemu, wypracowanych w oparciu o przewidywane zagrożenia i istniejące podatności systemu.

Informacje uzyskane podczas analizy ryzyka stanowią cenny zasób na przestrzeni całego cyklu życia systemu teleinformatycznego i powinny być zachowane dla ewentualnych przyszłych analiz i przeglądów ryzyka.

14 Dobieranie środków ochrony

Kolejnym działaniem w zarządzaniu ryzykiem, które ma na celu stworzenie bezpiecznego systemu teleinformatycznego dla danej jednostki organizacyjnej, jest dobranie odpowiednich zabezpieczeń. Zabezpieczenia, mające charakter fizyczny, techniczny lub organizacyjny, stosowane są komplementarnie we wszystkich obszarach występowania ryzyka.

Aby zapewnić odpowiedni i zrównoważony zestaw środków ochrony, który spełnia wymagania ustawowe dotyczące ochrony informacji oraz osiąga akceptowalny poziom bezpieczeństwa systemu, zespół analizy ryzyka powinien dokładnie przeanalizować każdy zidentyfikowany w poprzednim etapie zasób systemu teleinformatycznego oraz związane z nim zagrożenia i odpowiadającą mu podatność systemu. Należy przy tym uwzględnić zarówno istniejące środki ochrony, jak i te, które są zaplanowane do wdrożenia.

Można również podejść do zagadnienia od drugiej strony, analizując każde z osobna zidentyfikowane zagrożenie oraz odpowiadający mu słaby punkt systemu i związane z nim zasoby systemu, a następnie dostosować odpowiednie środki ochrony.

W procesie tym należy stale pamiętać, że każde zidentyfikowane zagrożenie ma znaczenie dla bezpieczeństwa tylko wtedy, gdy istnieje słaby punkt systemu (podatność systemu), który może być wykorzystany przez to zagrożenie. Analogicznie, słaby punkt ma znaczenie tylko wtedy, gdy występuje odpowiadające mu zagrożenie.

Opracowując listę środków ochrony dla danego systemu teleinformatycznego, należy uwzględnić wymagania bezpieczeństwa określone w różnych przepisach prawnych oraz standardach. Środki ochrony mogą działać na różne sposoby,

zabezpieczając informacje i zasoby systemu poprzez zmniejszenie prawdopodobieństwa wystąpienia danego zagrożenia, redukcję podatności systemu, ograniczenie szkód w przypadku ich wystąpienia lub wykrywanie zaistniałych przypadków zmiany, ujawnienia lub utraty.

Decyzja, który środek lub ich kombinacja jest najbardziej odpowiednia, zależy od okoliczności i warunków środowiska eksploatacji, w którym system teleinformatyczny działa.

Kierownik jednostki organizacyjnej może przenieść ryzyko na inny podmiot poprzez np. wynajęcie firmy ochroniarskiej odpowiedzialnej za ochronę fizyczną obiektu. Jednakże nie oznacza to przeniesienia odpowiedzialności za możliwe skutki ujawnienia, utraty lub modyfikacji informacji niejawnych. Kierownik nadal ponosi wszelkie konsekwencje zgodnie z art. 14 Ustawy o ochronie informacji niejawnych.

Optymalizacja wydatków jest kolejnym ważnym elementem w doborze środków ochrony. Należy znaleźć równowagę między kosztami wprowadzenia zabezpieczeń a wymaganiami przepisów dotyczących ochrony informacji, które związane są z koniecznością osiągnięcia poziomu zabezpieczeń.

Podczas doboru środków ochrony, należy uwzględnić różne czynniki, takie jak łatwość zastosowania danego środka, wymagania związane z etapem rozwoju systemu, skuteczność danego środka, a także funkcje, jakie ma pełnić dany środek ochrony.

Ostateczny etap tego procesu powinien skończyć się opracowaniem listy zalecanych środków ochrony po uwzględnieniu już istniejących zabezpieczeń.

15 Akceptacja ryzyka szczątkowego

Ryzyko szczątkowe w systemie teleinformatycznym zawsze pozostaje, mimo wdrożenia różnych środków ochrony. To ryzyko, które nie da się całkowicie wyeliminować. Istnieją różne zasoby systemu, które mogą być nie wpełni zabezpieczone, albo koszty ich pełnego zabezpieczenia są zbyt wysokie w porównaniu do wartości tych zasobów. Czasem również może wystąpić niewłaściwa ocena zagrożeń lub podatności zasobów.

W procesie akceptacji ryzyka szczątkowego dokonuje się przeglądu zastosowanych środków ochrony i ocenia ich skuteczność względem zidentyfikowanych ryzyk. Następnie ryzyko szczątkowe jest identyfikowane i oszacowywane, a dla każdego chronionego zasobu dokonywana jest klasyfikacja jako "akceptowane" lub "nie do zaakceptowania".

Ocena stopnia, w jakim wybrane środki ochrony zmniejszają ryzyko, opiera się na działaniu tych środków wobec wcześniej zidentyfikowanych ryzyk:

a) Eliminacja ryzyka - wszystkie niezbędne środki ochrony całkowicie eliminują rzeczywiste lub potencjalne słabe punkty.
b) Zapobieganie utracie informacji i zasobów - jeśli ryzyko nie może być całkowicie wyeliminowane, zastosowane środki zmniejszają je jak najbardziej.
c) Ograniczenie utraty informacji i zasobów - jeśli zapobieganie utracie nie jest możliwe, zaimplementowane środki ograniczają ryzyko do poziomu akceptowalnego.

Ryzyko uznane jako "akceptowalne" oznacza, że straty, jakie jednostka organizacyjna mogłaby ponieść w przypadku zaistnienia ryzyka, są znane i dopuszczalne. Natomiast ryzyko nieakceptowalne nie może być tolerowane i wymaga wprowadzenia dodatkowych zabezpieczeń.

Decyzje odnośnie każdego zidentyfikowanego ryzyka w systemie, które mają na celu redukcję tego ryzyka do akceptowalnego poziomu, wymagają zatwierdzenia przez kierownika jednostki organizacyjnej. Jest to kluczowa decyzja biznesowa, związana z zatwierdzeniem dodatkowych kosztów zabezpieczeń. Te koszty są nakładem mającym na celu zapewnienie bezpieczeństwa informacji niejawnych przetwarzanych w systemie.

W przypadku przetwarzania informacji niejawnych, zgodnie z postanowieniami Ustawy o Ochronie Informacji Niejawnych (UOIN), ryzyko szczątkowe musi być zaakceptowane przez kierownika jednostki organizacyjnej. Jest to ważne ze względu na istotność ochrony informacji niejawnych i konieczność podejmowania świadomych decyzji dotyczących akceptowalnego poziomu ryzyka w tym kontekście.

Ryzyko szczątkowe, pomimo podejmowania środków ochrony, pozostaje zawsze obecne. Dlatego też jest to obszar, który będzie wymagał szczególnej uwagi w dalszych etapach procesu zarządzania ryzykiem. Analiza, monitorowanie i ewentualne dostosowywanie zabezpieczeń wobec tego ryzyka będą kluczowymi elementami dalszego procesu zarządzania bezpieczeństwem informacji niejawnych w systemie.

ROZDZIAŁ 4

Utrzymanie zakładanego poziomu bezpieczeństwa

„Wyszczerbić miecz lecz czyste mieć sumienie”
Budka Suflera „Lubię ten stary obraz”

1 Elementy procesu zarządzania ryzykiem

W procesie zarządzania ryzykiem, celem jest utrzymanie poziomu bezpieczeństwa systemu teleinformatycznego określonego w polityce bezpieczeństwa jednostki organizacyjnej. Procesy realizowane w tej fazie obejmują analizę ryzyka, właściwe zabezpieczenia oraz edukację i świadomość dotyczącą zagrożeń.

Analiza Ryzyka:
Proces ten polega na zdobywaniu wiedzy o wielkości i miejscach występowania ryzyka. Zidentyfikowane wcześniej ryzyka nie są stałe, dlatego analiza ryzyka jest okresowo powtarzana. Wprowadzane zmiany, takie jak nowe aplikacje, sprzęt czy zwiększenie liczby użytkowników, mogą wpłynąć na poziom ryzyka. Analiza ryzyka pozwala na identyfikację nowych zagrożeń i ocenę ryzyka wynikającego z tych zmian.

Zabezpieczenia:
Eliminacja lub ograniczenie ryzyka odbywa się poprzez właściwie dobrane zabezpieczenia. Są to środki ochrony fizycznej, technicznej oraz przyjęte zasady postępowania, nakazy, zakazy i procedury. Zabezpieczenia obejmują także uświadamianie zagrożeń, ich skutków dla jednostki organizacyjnej oraz opracowywanie programów szkoleń z zakresu bezpieczeństwa.

Uświadamianie i Szkolenia:
Edukacja i świadomość pracowników są kluczowymi elementami w zarządzaniu ryzykiem. Programy szkoleń dotyczące bezpieczeństwa pozwalają na lepsze zrozumienie zagrożeń oraz skutków nieprawidłowych działań. Uświadomienie pracowników o ryzyku, procedurach bezpieczeństwa i odpowiednich postępowaniach przyczynia się do zminimalizowania potencjalnych ryzyk.

Ostatecznym celem tej fazy jest utrzymanie aktualnego poziomu bezpieczeństwa poprzez regularną analizę i aktualizację działań prewencyjnych oraz środków ochronnych. Procesy te pozwalają na adaptację do zmieniających się warunków i zagrożeń, co przyczynia się do zminimalizowania ryzyka i zapewnienia stabilności systemu teleinformatycznego.

2 Ocena skuteczności zabezpieczeń

Zarządzanie ryzykiem w trakcie eksploatacji systemu to ciągły proces, który obejmuje planowane i okresowe przeglądy ryzyka oraz reakcję na zmiany, incydenty lub naruszenia bezpieczeństwa. Kluczowe kroki w tym procesie to:

Planowane Przeglądy Ryzyka:
Określanie częstotliwości i harmonogramu przeglądów ryzyka, zazwyczaj zalecane są coroczne przeglądy. Częstotliwość ta jest ustalana w dokumencie Szczególne Wymagania Bezpieczeństwa (SWB) danego systemu i akceptowana podczas procesu akredytacji.

Dodatkowe Analizy Ryzyka:
Dodatkowe analizy ryzyka są przeprowadzane w przypadku rozbudowy, modernizacji systemu lub zmian w środowisku eksploatacji. Zmiany te mogą wpłynąć na bezpieczeństwo systemu, dlatego konieczne jest zidentyfikowanie nowych zagrożeń, oszacowanie ryzyka i dostosowanie zabezpieczeń.

Reakcja na Incydenty:
W przypadku stwierdzenia naruszenia bezpieczeństwa systemu, ujawnienia informacji, zniszczenia, modyfikacji lub braku dostępu do zasobów informacyjnych, przeprowadzane są postępowania wyjaśniające. Incydenty te skutkują wpisaniem na listę nowych ryzyk i wprowadzeniem zabezpieczeń, aby zapobiec powtórzeniu się incydentu.

Przegląd Procedur Bezpiecznej Eksploatacji:
Okresowy przegląd procedur bezpiecznej eksploatacji ma na celu ocenę ich kompleksowości i adekwatności do przyjętej polityki bezpieczeństwa informacji i obowiązujących przepisów prawnych.

Zarządzanie ryzykiem w trakcie eksploatacji systemu jest istotne dla zapewnienia ciągłości i skuteczności działań związanych z bezpieczeństwem informacji. Regularne monitorowanie, analiza, reakcja na zmiany i incydenty oraz dostosowywanie zabezpieczeń pozwala na utrzymanie odpowiedniego poziomu bezpieczeństwa w dynamicznym środowisku IT.

3 Odporność systemu teleinformatycznego na potencjalne zagrożenia

Kontrole i nadzór nad bezpieczeństwem systemu są kluczowe dla zapewnienia jego odporności na potencjalne zagrożenia. Inspektor Bezpieczeństwa Teleinformatycznego pełni istotną rolę w tym procesie, a ich działania obejmują:

Sprawdzenie Zgodności z SWB:
Inspektor BTI powinien kontrolować zgodność zabezpieczeń z dokumentem Szczególne Wymagania Bezpieczeństwa (SWB) danego systemu. SWB zawiera wytyczne dotyczące bezpieczeństwa i jest podstawą dla implementacji zabezpieczeń.

Kontrola Zgodności z Analizą Ryzyka:
Sprawdzanie, czy zaimplementowane środki ochrony odpowiadają listom niezbędnych zabezpieczeń, wynikającym z przeprowadzonej analizy ryzyka. To pozwala na weryfikację, czy środki ochrony adekwatnie reagują na identyfikowane zagrożenia.

Ocena Przestrzegania Procedur Bezpieczeństwa:
Kontrola przestrzegania procedur bezpiecznej eksploatacji przez użytkowników systemu. Zapewnienie, że wszyscy użytkownicy stosują się do ustalonych procedur, jest kluczowe dla utrzymania poziomu bezpieczeństwa.

Monitorowanie Skuteczności Środków Ochrony:
Śledzenie i monitorowanie efektywności zabezpieczeń w praktyce. Inspektor BTI ocenia, czy zastosowane środki ochrony działają zgodnie z założeniami i czy są skuteczne w minimalizowaniu ryzyka.

Kontrola Zgodności z Polityką Bezpieczeństwa:

Zapewnienie, że system i jego zabezpieczenia są zgodne z polityką bezpieczeństwa ustaloną dla danego systemu. To obejmuje również ocenę, czy system spełnia wymagania określone w polityce bezpieczeństwa.

Przeglądy Okresowe i Po Zmianach:
Okresowe przeglądy zabezpieczeń eksploatowanego systemu zgodnie z ustalonym terminarzem kontroli. Dodatkowo, kontrola systemu po wprowadzeniu zmian lub w przypadku zmiany warunków bezpieczeństwa lub polityki.

Przeprowadzanie tych kontroli w sposób regularny i systematyczny pozwala na utrzymanie odpowiedniego poziomu bezpieczeństwa systemu oraz na reakcję na zmieniające się zagrożenia i warunki eksploatacji. Kontrole te są kluczowe na każdym etapie życia systemu, począwszy od jego planowania i rozwoju, aż po wymianę lub wycofanie z użycia.

4 Monitorowanie bezpieczeństwa

Monitorowanie bezpieczeństwa jest kluczowym aspektem w zarządzaniu ryzykiem i utrzymaniu poziomu bezpieczeństwa systemu informacyjnego. Obejmuje ono śledzenie różnych aspektów systemu w celu wykrycia wszelkich nieprawidłowości, nieautoryzowanych działań lub prób naruszenia bezpieczeństwa. Oto kluczowe elementy monitorowania bezpieczeństwa:

Czynniki Ryzyka:
Monitorowanie powinno obejmować wszystkie czynniki ryzyka zidentyfikowane w analizie ryzyka. Dzięki temu można śledzić ich zmiany i ewentualne wpływy na bezpieczeństwo systemu.

Monitorowanie Działalności Użytkowników:
Śledzenie aktywności użytkowników w systemie, w tym logowanie, próby nieudanego logowania, dostęp do określonych zasobów czy podejrzane aktywności.

Monitorowanie Ruchu Sieciowego:
Analiza ruchu w sieci w celu wykrywania nieprawidłowości, prób ataków lub nieautoryzowanego dostępu.

Logi Systemowe:
Regularne przeglądanie i analiza logów systemowych, które rejestrują zdarzenia systemowe, dostępy, modyfikacje i inne aktywności w systemie.

Działanie Systemów Alarmowych:
Monitorowanie działania systemów alarmowych, które sygnalizują wszelkie podejrzane lub niebezpieczne sytuacje.

Monitorowanie Działania Zabezpieczeń Fizycznych i Technicznych:

Ocena działania zabezpieczeń fizycznych, takich jak kamery, kontrola dostępu, oraz zabezpieczeń technicznych, takich jak firewall'e, antywirusy, systemy detekcji intruzów.

Regularne Przeglądy:
Okresowe przeglądy logów i wyników monitorowania, co pozwala na szybkie wykrycie anomalii i odpowiednie reagowanie na potencjalne zagrożenia.

Procedury i Raportowanie:
Określenie procedur monitorowania, w tym częstotliwość kontroli, sposób składania raportów oraz osoby odpowiedzialne za monitorowanie i reagowanie na incydenty.

Monitorowanie powinno być integralną częścią procesu zarządzania ryzykiem, pozwalając na reagowanie na zmieniające się warunki i nowe zagrożenia w celu utrzymania poziomu bezpieczeństwa informacji niejawnych.

5 Obsługa incydentów bezpieczeństwa

Zgłaszanie i badanie incydentów bezpieczeństwa to kluczowy element utrzymania bezpieczeństwa w systemie informatycznym. Poniżej przedstawiono kluczowe kroki i elementy, które należy uwzględnić w procedurach zgłaszania i badania incydentów:

Definicja Incydentu:
Określenie, co jest uznawane za incydent bezpieczeństwa. Może to obejmować próby nieautoryzowanego dostępu, utratę danych, naruszenia poufności, ataki złośliwe oprogramowanie itp.

Wzór Raportu Incydentu:
Opracowanie wzoru raportu, który zawierać będzie istotne informacje o incydencie, takie jak data i godzina zdarzenia, opis incydentu, osoby zaangażowane, ewentualne straty czy zakłócenia, oraz wszelkie inne szczegóły istotne dla analizy i reakcji.

Obowiązkowe Zgłaszanie:
Określenie, które incydenty muszą być obowiązkowo zgłaszane, do kogo i w jakim czasie. Zgłaszanie może być związane z rangą incydentu oraz konsekwencjami dla systemu i organizacji.

Procedury Zgłaszania:
Wytyczenie jasnych procedur zgłaszania incydentów, włącznie z odpowiedzialnymi za przyjmowanie zgłoszeń oraz formami komunikacji (np. e-mail, formularz online, telefonicznie).

Badanie Incydentu:

Określenie procedur i zasad badania zgłoszonych incydentów. Wskazanie osób odpowiedzialnych za przeprowadzanie analizy, zbieranie dowodów, identyfikację przyczyn oraz wypracowanie działań naprawczych.

Decyzje i Działania Poprawcze:
Określenie procesu podejmowania decyzji po zbadaniu incydentu, które mogą obejmować wprowadzenie nowych zabezpieczeń, zmiany w polityce bezpieczeństwa, uaktualnienia procedur itp.

Uczenie się z Incydentów:
Zobowiązanie do wyciągania wniosków z analizy incydentów w celu unikania powtórek w przyszłości. Może to obejmować doskonalenie szkoleń w zakresie bezpieczeństwa, aktualizację procedur czy zwiększenie świadomości pracowników.

Poufność i Ochrona Danych:
Zapewnienie, że procedury związane z incydentami uwzględniają zachowanie poufności i odpowiednie zabezpieczenie danych związanych z incydentem.

Raportowanie i Analiza Trendów:
Ustanowienie procesu regularnego raportowania incydentów oraz analizy trendów, co pozwoli na zidentyfikowanie wzorców i ulepszenie systemu bezpieczeństwa.

Szkolenia i Świadomość:
Zapewnienie szkoleń dla personelu w zakresie procedur zgłaszania incydentów i zasad postępowania w przypadku naruszeń bezpieczeństwa.

Dbałość o skuteczne i efektywne procedury zgłaszania i badania incydentów ma kluczowe znaczenie dla utrzymania poziomu bezpieczeństwa systemu informatycznego i minimalizowania negatywnych skutków incydentów bezpieczeństwa.

6 Utrzymanie aktualnego poziomu wiedzy

Prowadzenie skutecznych szkoleń z zakresu bezpieczeństwa informacji jest kluczowe dla zwiększenia świadomości pracowników i ukształtowania właściwych nawyków w organizacji. Poniżej przedstawiam kluczowe elementy, które powinny być uwzględnione w programie szkoleń dotyczących bezpieczeństwa systemu TI:

Polityka Bezpieczeństwa:
Wyjaśnienie celów i założeń polityki bezpieczeństwa organizacji oraz konsekwencji jej naruszenia. Zaznaczenie, że każdy pracownik ma obowiązek przestrzegania tej polityki.

Podstawy Bezpieczeństwa:
Omówienie podstawowych zagrożeń i podatności związanych z bezpieczeństwem informacji, takich jak ataki hakerskie, phishing, złośliwe oprogramowanie itp.

Zasady Korzystania z Systemu:
Wprowadzenie do zasad bezpiecznego korzystania z systemu informatycznego, w tym zabezpieczanie hasłami, zamykanie sesji, aktualizowanie oprogramowania i przeglądarki, unikanie niebezpiecznych stron internetowych itp.

Ochrona Danych:
Edukacja na temat odpowiedniego przechowywania, przetwarzania i udostępniania danych. Zaznaczenie roli każdego pracownika w zabezpieczaniu informacji.

Zarządzanie Hasłami:
Szkolenie w zakresie bezpiecznego tworzenia, przechowywania i aktualizowania haseł. Podkreślenie konieczności unikania używania tych samych haseł do różnych kont.

Procedury Bezpieczeństwa:
Omówienie konkretnych procedur związanych z bezpieczeństwem, takich jak procedury zgłaszania incydentów, procedury dostępu do kluczowych zasobów, procedury zamykania systemu itp.

Zabezpieczenia Fizyczne:
Uświadomienie pracownikom o znaczeniu zabezpieczeń fizycznych, takich jak zamki, kontrola dostępu do pomieszczeń, zabezpieczanie sprzętu itp.

Szkolenia Praktyczne:
Organizacja symulacji incydentów, aby pracownicy mogli nauczyć się, jak reagować w przypadku potencjalnych zagrożeń.

Monitorowanie i Raportowanie:
Edukacja w zakresie monitorowania aktywności oraz raportowania wszelkich podejrzanych zdarzeń lub incydentów.

Aktualizacje i Śledzenie Postępów:
Zaznaczenie konieczności regularnego aktualizowania wiedzy pracowników z zakresu bezpieczeństwa oraz śledzenia postępów w ich rozwoju w tej dziedzinie.

Przestrzeganie Przepisów Prawnych:
Zapoznanie z obowiązującymi przepisami prawnymi dotyczącymi ochrony danych i informacji w systemach TI.

Regularne szkolenia i przypomnienia pomagają w ugruntowaniu wiedzy pracowników oraz zminimalizowaniu ryzyka związanego z incydentami bezpieczeństwa. Ważne jest, aby program szkoleń był aktualizowany w zależności od zmian w technologii, zagrożeń i polityki organizacji.

7 Warunki utrzymania wysokiego poziomu bezpieczeństwa

Należy wprowadzić procedury bezpiecznej eksploatacji w systemie teleinformatycznym oraz sieciowych rozwiązań, obejmujące zabezpieczenie poszczególnych stanowisk i ich połączeń. Procedury te powinny uwzględniać minimalizowanie podatności systemu poprzez odpowiednie konfiguracje, aktualizacje oraz monitorowanie aktywności.

W celu zapewnienia ciągłości działania systemu teleinformatycznego zaleca się wprowadzenie procedur dotyczących awaryjnego przywracania funkcjonalności. Powinny być opracowane i przetestowane scenariusze przywracania usług w przypadku incydentów lub awarii, w tym przywracanie danych z kopii zapasowych oraz szybka reakcja na potencjalne zagrożenia.

Istotnym elementem utrzymania bezpieczeństwa jest nadzór nad wydajnością systemu teleinformatycznego. Zaleca się regularne monitorowanie obciążenia systemu, wykrywanie ewentualnych anomalii i podejrzanej aktywności, oraz dostosowywanie zasobów w zależności od potrzeb w celu uniknięcia przeciążeń.

Należy przeprowadzać regularne testy bezpieczeństwa, obejmujące penetrację systemu, analizę podatności oraz ocenę zabezpieczeń aplikacji. Wyniki tych testów powinny być wykorzystywane do wprowadzania poprawek i ulepszeń w środkach ochrony.

Zaleca się wdrożenie i przestrzeganie procedur postępowania w przypadku incydentów bezpieczeństwa. W momencie wykrycia potencjalnego naruszenia bezpieczeństwa lub incydentu, powinny być określone kroki postępowania, w tym raportowanie incydentu, izolacja systemu, przywracanie działania systemu, analiza incydentu i wprowadzenie odpowiednich poprawek.

Istotnym elementem zarządzania ryzykiem jest ciągłe doskonalenie środków ochrony oraz procedur bezpieczeństwa. Zaleca się regularne przeglądy, aktualizacje i ulepszanie dokumentacji bezpieczeństwa, wdrażając nowe rozwiązania i technologie zgodnie z aktualnymi wymaganiami i zagrożeniami.

W procesie zarządzania ryzykiem zaleca się aktywny udział właścicieli ryzyk, administratorów systemu, użytkowników oraz zespołu odpowiedzialnego za bezpieczeństwo. Współpraca i wymiana informacji między tymi grupami pozwoli na skuteczniejsze identyfikowanie, ocenę i zarządzanie ryzykiem w systemie teleinformatycznym.

WNIOSKI

Ocena poziomu bezpieczeństwa wraz z wprowadzeniem środków zabezpieczających w różnych fazach cyklu funkcjonowania systemu teleinformatycznego umożliwia ocenę i projektowanie zabezpieczeń, które są ekonomicznie uzasadnione i adekwatne do ryzyka.

Prawidłowo przeprowadzona analiza ryzyka pozwala zidentyfikować wszystkie potencjalne zagrożenia i dobrać odpowiednie środki ochrony. Ryzyk nie da się całkowicie wyeliminować, ale można je kontrolować i zredukować.

Ludzie w organizacji często są źródłem zagrożeń, a właściwa edukacja i uświadamianie są kluczowe dla efektywnego zarządzania ryzykiem. Potrzebne jest zrozumienie, że czynniki ludzkie mogą być słabym ogniwem w systemach bezpieczeństwa.

Profesjonalna ocena poziomu bezpieczeństwa pozwala zidentyfikować realne zagrożenia, często nieoczywiste, i skoncentrować się na priorytetach. Wartość tej analizy jest w zrozumieniu, że nie wszystkie zagrożenia są technologiczne, ale również związane z ludźmi, procesami i sytuacjami.

Poparcie kierownictwa na wszystkich szczeblach organizacji jest kluczowe dla skuteczności działań związanych z bezpieczeństwem teleinformatycznym. Brak wsparcia może być poważną przeszkodą dla skutecznego zarządzania ryzykiem.

Analiza dobrych praktyk i metod oceny poziomu bezpieczeństwa jest istotnym elementem opracowania skutecznej ścieżki oceny zabezpieczeń systemów teleinformatycznych.

Skuteczne zarządzanie ryzykiem w systemach teleinformatycznych wymaga holistycznego podejścia, które uwzględnia aspekty technologiczne, ludzkie i organizacyjne. Odpowiednie edukowanie, monitorowanie, i ocena ryzyka są kluczowymi elementami tego procesu.

Literatura

1. Trusted Computer System Evaluation Criteria. DoD. 15 August 1983. CSC-STD-001-83.
2. A. Nowak, W. Scheffs. Zarządzanie bezpieczeństwem informacyjnym. Warszawa: AON, 2009.
3. BS 7799-1:1999: Part 1: "Code of practice for Information Security Management". BSI.
4. BS 7799-2:1999: Part 2 "Specification for Information Security Management Systems". British Standards Institute.
5. COBIT™ Control Objectives. April 1998. 2nd Edition. COBIT Steering Committe and the Information Systems Audit and Control Foundation.
6. Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. May 1998. Version 2.0. CCIB-98-026.
7. Common Criteria for Information Technology Security Evaluation. Part 2: Security functional requirements. May 1998. Version 2.0. CCIB-98-027
8. Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance requirements. May 1998. Version 2.0. CCIB-98-028.
9. COSO ERM – Zarządzanie ryzykiem korporacyjnym – zintegrowana struktura ramowa.
10. Ulsch, MacDonnell, Cyber Threat!. How to Manage the Growing Risk of Cyber Attacks, Wiley 2014, ISBN 1118836359
11. Atle Refsdal Bjørnar Solhaug Ketil Stølen, Cyber-Risk Management, Springer 2015, ISBN 3319235699
12. D. Atkins i inni. Internet Security. Professional Reference. New Riders Publishing, 1997 (tłum. LT&P 1997 – Bezpieczeństwo Internetu).
13. D. R. Ahmad i inni, Hack Proofing Your Network, Syngress Publishing Inc. 2002.
14. Donald L. Pipkin, (2002). Bezpieczeństwo Informacji. W P. D.L., Bezpieczeństwo Informacji (strony 188-194). WNT.

15. Detecting and Mitigating Robotic Cyber Security Risks, Kumar 2017, ISBN 1522521542
16. F. Bień. Zarządzanie cyklem życia informacji. Boston: IT Security Review nr 3, 2017.
17. F. Wołowski, J. Zawiła-Niedźwiecki. Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny normami polskimi i międzynarodowymi. Kraków-Warszawa: Edu-Libri, 2012.
18. Griffor, Edward, Handbook of System Safety and Security. Cyber Risk, Syngress 2017, ISBN 0128037733
19. Hubbard, Douglas W.; Seiersen, Richard, How to Measure Anything in Cybersecurity Risk, Wiley 2016, ISBN 1119085292
20. I. Krysowaty, P. N. (2006). Informacja w systemach IT jako towar strategiczny. W Informacja w systemach IT jako towar strategiczny (strony 115-116). Radom: Instytut Technologii Eksploatacyjnej.
21. Agrawal, Manish; Campoe, Alex; Pierce, Eric, Information Security and IT Risk, Management, Wiley 2014, ISBN 9781118335895
22. Peltier, Thomas R. (Thomas R. Peltier Associates, Wyandotte, Michigan, USA), Information Security Risk Analysis, 3ed., Press 2010, ISBN 1439839565
23. Mark Talabis, Information Security Risk Assessment Toolkit. Practical Assessments, Syngress 2012, ISBN 1597497355
24. Raymond Pompon, IT Security Risk Control Management. An Audit Preparation Plan, Press 2016, 1484221397
25. André Loske, IT Security Risk Management in the Context of Cloud Computing, Springer 2015, 3658113391
26. ITSEC. Version 1.2. June 1991.
27. J. Brdulak, R. Sobczak (red.) Wybrane problemy zarządzania bezpieczeństwem informacji. Warszawa: SGH, 2014.
28. J. Janczak, A. Nowak. Bezpieczeństwo informacyjne Wybrane problemy. Warszawa: AON, 2013.

29. J. Łuczak, M. Tyburski. Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001. Poznań: WUE, 2010.
30. J. Scambray, S. McClure, G. Kurtz. Hacking Exposed McGraw-Hill 2001 (tłum. Translator 2001 - Hakerzy - cała prawda). T. Kifner. Polityka bezpieczeństwa i ochrony informacji. Helion 1999.
31. Jaworska, A. (2020, listopad 27). Encyklopedia zarządzania. Pobrano z lokalizacji Encyklopedia zarządzania: https://mfiles.pl/pl/index.php/ISO_13335
32. K. Liderman, Bezpieczeństwo teleinformatyczne, IAiR WAT 2001.
33. L. Klander. Hacker Proof. Jamsa Press, 1997. (tłum. MIKOM 1998).
34. Leszek Klimiuk, R. S. (2020, Sierpień 12). Encyklopedia zarządzania. Pobrano z lokalizacji https://mfiles.pl/pl/index.php/Zarz%C4%85dzanie_ryzykiem
35. Liderman, K. (2003). Oszacowanie jakościowe ryzyka dla potrzeb bezpieczeństwa teleinformatycznego. Warszawa, Instytut Teleinformatyki i Automatyki WAT, Polska.
36. Liderman, K. (2009). Analiza ryzyka i ochrona informacji w systemach komputerowych. Warszawa: PWN.
37. Łuczak, J., 2009, Metody szacowania ryzyka – kluczowe elementy systemu zarządzania bezpieczeństwem informacji ISO/ IEC 27001, Zeszyty Naukowe Akademii Morskiej w Szczecinie / Scientific Journals Maritime University of Szczecin, 19 (91), s. 63-70.
38. M. Kaeo, Designing Network Security, CISCO Press 1999 (tłum. MIKOM 2000 – Tworzenie bezpiecznych sieci).
39. M. Molski, M. Ł. (2007). Przewodnik audytora systemów informatycznych. Gliwice: Helion.
40. M. Pałęga. Ocena poziomu zagrożeń bezpieczeństwa informacji za pomocą macierzy ryzyka. Wybrane zagadnienia dotyczące usprawniania procesów w przedsiębiorstwie. Pod red. M. Ogórek, T. Bajor Częstochowa: Wydawnictwo WiPiTM Politechniki Częstochowskiej, 2016.

41. M. Strebe, Ch. Perkins. Firewalls. SYBEX Inc. 2000 (tłum. MIKOM 2000 - Firewalls - ściany ogniowe).
42. Managing Risk and Information Security. Protect to Enable, 2ed., Press 2016, 1484214560
43. Norma ISO/ IEC TR 13335.
44. Norma ISO/IEC 27001:2005.
45. Norma ISO/IEC 27005:2011.
46. P. Mazurek. Realizacja szacowania ryzyka w wybranym przedsiębiorstwie.
47. PN-EN ISO 9001:2015 Systemy zarządzania jakością – Wymagania. Warszawa: PKN, 2015.
48. PN-I-02000: Technika informatyczna. informatycznych. Terminologia. Zabezpieczenia w systemach
49. PN-I-13335-1: 1999. Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych.
50. PN-I-13335-1:1999 Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych. Warszawa: PKN, 1999.
51. PN-IEC 62198:2005 - wersja polska. (2005). Zarządzanie ryzykiem przedsięwzięcia --Wytyczne stosowania.
52. PN-ISO/IEC 27001:2014 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania. Warszawa: PKN, 2013.
53. PN-ISO/IEC 27005:2014 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji. Warszawa: PKN, 2013.
54. Reduce Risk and Improve Security on IBM Mainframes, IBM 2015, 0738441023
55. Risk Management Guide for Information Technology Systems NIST SP800-30

56. Risks and Security of Internet and Systems. 11th Conf. CRiSIS, Springer 2017, 3319548751
57. Risks and Security of Internet and Systems. 12th Conf. CRiSIS, Springer 2018, 9783319766867
58. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego, Dz. U. Nr 159, poz.948.
59. Rządowe Centrum Bezpieczeństwa. Ocena ryzyka na potrzeby zarządzania kryzysowego. Raport o zagrożeniach bezpieczeństwa narodowego,
60. S. Garfinkel, G. Spafford. Practical Unix and Internet Security, O'Reilly&Associates Inc. 1996. (tłum. RM 1997 – Bezpieczeństwo w Unixie i Internecie). E. Amoroso. Intrusion Detection. AT&T Inc. 1999 (tłum. RM 1999 - Wykrywanie intruzów).
61. Stróżyk, Zarządzanie ryzykiem w bezpieczeństwie informacji.
62. T. Kaczmarek. Ryzyko i zarządzanie ryzykiem Ujęcie interdyscyplinarne. Warszawa: Difin, 2008.
63. T. Kifner. Polityka bezpieczeństwa i ochrony informacji. Gliwice: Helion, 1999.
64. T. Polaczek: Audyt bezpieczeństwa informacji w praktyce. Gliwice: Helion, 2006.
65. T. Sasor. Ryzyko i polityka bezpieczeństwa w przedsiębiorstwie wirtualnym. Informatyka i współczesne zarządzanie. pod red. J. Kisielnicki, J. Grabara, J. Nowak, Katowice: PTI, 2015.
66. Technika informatyczna - Techniki bezpieczeństwa - Zarządzanie ryzykiem w bezpieczeństwie informacji - PN-ISO/IEC 27005.
67. Technika informatyczna - Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji - Wymagania - PN-ISO/IEC 27001
68. The Complete Guide to Cybersecurity Risks and Controls, Auerbach 2016, 1498740545
69. The Complete Guide to Cybersecurity Risks and Controls, Pierce 2017, 1722677996

70. Domenic Antonucci, The Cyber Risk Handbook. Creating and Measuring Effective, Wiley 2017
71. Trusted Computer Standards Evaluation Criteria. Departament Obrony Stanów Zjednoczonych. (1985).
72. Understanding Cyberrisks in IoT. When Smart Things Turn Against You, Boyle 2019, 1948976641
73. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, Dz. U. Nr 182, poz. 1228.
74. W. Stallings, Network and Internetwork Security Principles and Practice, Prentice Hall 1994 (tłum. WNT 1997 – Ochrona danych w sieci i intersieci w teorii i praktyce).
75. Cyber Security. The Lifeline of Information and Communication, Springer 2020, ISBN 3030317021
76. A Leader's Guide to Cybersecurity. Why Boards Need to Lead, Domet 2020, 1633697991
77. 200+ Ways to Protect Your Privacy. Simple Ways, Rogers 2019, 1721400125
78. A Big Security Fix and Performance Manual - The Essential Guide to Computer Security, Hoss 2017
79. A Guide To Cyber Security, Mitra 2018, 1727359526
80. A Human Readable Guide to Cyber Security, Christian 2015, B00UWR5DL2
81. A Leader's Guide to Cybersecurity. Why Boards Need to Lead, Domet 2020, 1633697991
82. A Multidisciplinary Introduction to Information Security, Press 2011, 1420085905
83. Accounting Information Systems and Cyber Security, 2016, B01N5H39G7
84. Advances in Artificial Intelligence for Protection and Security, World 2009, 9812790322
85. Advances in Cyber Security. Principles, Techniques, and Applications, Springer 2019, 9811314829

86. Advances in Digital Forensics IX. 9th Conf. IFIP WG, Springer 2014, 3642411479
87. Advances in Digital Forensics X. 10th Conf. IFIP, Springer 2014, 9783662449516
88. Advances in Digital Forensics XI. 11th Conf. IFIP, Springer 2015, 9783319241227
89. Advances in Digital Forensics XII. 12th Conf. IFIP, Springer 2016, 3319462784
90. Advances in Digital Forensics XIII. 13th Conf. IFIP, Springer 2017, 331967207X
91. Advances in Human Factors in Cybersecurity. Conf. AHFE, Springer 2016, 3319419315
92. Advances in Information and Computer Security. 10th Conf. IWSEC, Springer 2018, 3319224247
93. Advances in Information and Computer Security. 13th Conf. IWSEC, Springer 2018, 3319979159
94. Advances in Information and Computer Security. 14th Conf. IWSEC, Springer 2019, 9783030268336
95. Advances in Information and Computer Security. 6th Conf. IWSEC, Springer 2011, 3642251404
96. Advances in Information and Computer Security. 9th Conf. IWSEC Springer 2014, 331909842X
97. Advances in Information Security and Assurance, Springer 2009, 3642026168
98. Advances in Intelligence and Security Informatics, Press 2012, 0123972000
99. Advances in Security in Computing and Communications, Sen 2017, 9535133462
100. Adwanced Hacking. The Blueprint Advance Techniques, Cyberpunk 2017, B06ZZLKY46
101. Algorithms, Architectures and Information Systems Security, World 2008, 9812836233

102. An Introduction To The World Of Hacking, Steinbach 2015, B00WTZCYBW
103. Analysis and Design of Networked Control Systems under Attacks, Press 2019, 9781138612754
104. Analyzing Computer Security. A Threat, Pearson 2012, 0132789469
105. Applied Computation and Security Systems. Vol. 1, Springer 2014, 8132219848
106. Applied Information Security. A Hands-on Approach, Springer 2011, 3642244734
107. Assessment of Current Cybersecurity Practices in the Public Domain. SNL 2016, 1541296052
108. Attack and Defend Computer Security, 2ed., Wiley 2014, 111890673X
109. Attacking Network Protocols. A Hacker's Guide, Forshaw 2017, 1593277504
110. Autonomous Cyber Deception. Reasoning, Adaptive Planning, Springer 2019, 3030021092
111. Availability, Reliability and Security in Information Systems. Conf., Springer 2013, 364240510X
112. Behavioral Cybersecurity. Applications of Personality, Press 2019, 1138617784
113. Beyond Cybersecurity. Protecting Your Digital Business, Wiley 2015, 1119026849
114. Big Data Analytics in Cybersecurity, Auerbach 2017, 1498772129
115. Big Data Technologies for Monitoring of Computer Security, Springer 2018, 3319790358
116. BIT WARS. Cyber Crime, Hacking & Information Warfare, Hyslip 2015, 1514673150
117. Black Code. Inside the Battle for Cyberspace, McClelland 2013, 0771025335

118. Breakthrough Perspectives in Network and Communications Security, IGI 2009, 1605661481
119. CEH Certified Ethical Hacker All-in-One Exam Guide, 4ed., Walker 2019, 126045455X
120. CEH Certified Ethical Hacker Practice Exams, 3ed., MgH 2016, 1259836606
121. CEH v10 Certified Ethical Hacker Study Guide, Sybex 2019, 1119533198
122. CEH v9. Certified Ethical Hacker Version 9 Study Guide, 3ed., Sybex 2016, 1119252245
123. Certified Ethical Hacker (CEH) Foundation Guide, Press 2016, 1484223241
124. China and Cybersecurity. Espionage, Strategy and Politics, Press 2015, 0190201266
125. Chinese Cybersecurity and Cyberdefense, Wiley 2015, 1848216149
126. CISM Certified Information Security Manager Practice Exams, MgH 2019, 9781260456127
127. CISSP Cert Guide, 3ed., McMillan 2018, 0789759691
128. CISSP. Certified Information Systems Security Professional, 5ed., Sybex 2011, 9780470944981
129. CISSP Guide to Security Essentials, Gregory 2014, 1285060423
130. CISSP (ISC)2. Certified Information Systems Security, 8ed., Sybex 2018, 1119475937
131. Combatting Cybercrime and Cyberterrorism. Challenges, Springer 2016, 3319389297
132. Communication System Security, Press 2012, 1439840369
133. Communications and Multimedia Security. 15th Conf. IFIP, Springer 2014, 366244884X
134. Communications and Multimedia Security. Conf., Springer 2005, 0387244859

135. CompTIA CSA+ Cybersecurity Analyst Certification All-in-One Exam Guide, Maymi 2017, 126001181X
136. Computation, Cryptography and Network Security, Springer 2015, 3319182749
137. Computational Intelligence for Privacy and Security, Springer 2012, 3642252362
138. Computational Intelligence in Security for Information Systems. Conf., Springer 2011, 3642213227
139. Computer and Cyber Security. Principles, Algorithm, Applications, Press 2018, 0815371330
140. Computer and Information Security Handbook, 3ed., Morgan 2017, 0128038438
141. Computer Forensics and Cyber Crime. An Introduction, 3ed., Pearson 2013, 0132677717
142. Computer Forensics. Cybercriminals, Laws, and Evidence, Maras 2014, 1449692222
143. Computer Security. Art and Science, 2ed., Bisrop 2017, 0321712331
144. Computer Security Basics, OReilly 2006, 0596006691
145. Computer Security Fundamentals, 4ed., Pearson 2019, 0135774772
146. Computer Security Handbook, Wiley 2014, 1118127064
147. Computer Security. Principles and Practice, 4ed., Pearson 2018, 9781292220611
148. Computer Security Principles, Barnes 2018, B07J283F42
149. Computer Security, Privacy and Politics, Press 2008, 1599048043
150. Concise Guide to CompTIA Security+, RGC 2015, B00WEBA05I
151. Conference on Applications and Techniques in Cyber Security, Springer 2017, 3319670700
152. Conflict and Cooperation in Cyberspace, Taylor 2013, 146659201X
153. Construction Safety Informatics, Springer 2019, 9811357609
154. Counterterrorism and Cybersecurity. Total Information Awareness, 2ed., Springer 2015, 3319172433

155. Critical Approaches to Security. An Introduction, Rouledge 2013, 0415680174
156. Critical Information Infrastructures Security. 12th Conf. CRITIS, Springer 2018, 3319998420
157. Critical Information Infrastructures Security. 13th Conf. CRITIS, Springer 2018, 3030058484
158. Critical Information Infrastructures Security. 9th Conf. CRITIS, Springer 2016, 331931663X
159. Current and Emerging Trends in Cyber Operations, Palgrave 2015, 1137455543
160. Cyber and Electromagnetic Threats in Modern Relay Protection, Press 2014,1482264315
161. Cyber Attack, Cyber Crime, Cyber Warfare – Cyber Complacency, Osborne 2014, 1493581287
162. Cyber Attack. The Threat to America in the Age of Cyber Warfare, Clint 2016, B01AKE59EC
163. Cyber Attacks. Survival Manual, Selby 2017, B075VLD2KY
164. Cyber Conflict. Competing National Perspectives, Wiley 2012, 1848213506
165. Cyber Crime and Cyber Terrorism Investigator's Handbook, Syngress 2014, 0128007435
166. Cyber Crime Investigations. Bridging the Gaps, Syngerss 2007, 1597491330
167. Cyber Crime. Technology Turns Into A Curse, Hossain 2015, B00TJV360C
168. Cyber Crisis Management. Overcoming the Challenges in Cyberspace, Ryder 2019, 9389165520
169. Cyber Deception. Building the Scientific Foundation, Springer 2016, 331932697X
170. Cyber Defense. An International View, USArmy 2015, B015DL19UK

171. Cyber Defense and Situational Awareness, Springer 2015, 3319113909
172. Cyber Denial, Deception and Counter Deception, Springer 2015, 3319251317
173. Cyber Enigma. Unravelling the Terror in the Cyber World, Routledge 2019, 0367322641
174. Cyber Forensics. From Data to Digital Evidence, Press 2012, 1118273664
175. Cyber Insecurity. Navigating the Perils, Harrison 2016, 1442272848
176. Cyber Operations. Building, Defending, and Attacking, 2ed., Press 2019, 1484242939
177. Cyber Power. Crime, Conflict and Security in Cyberspace, Press 2013, 146657304X
178. Cyber Reconnaissance, Surveillance and Defense, Syngress 2014, 0128013087
179. Cyber Security. 15th Conf. CNCERT, Springer 2019, 9811366209
180. Cyber Security. 2nd Conf. CSS, Springer 2016, 331928312X
181. Cyber Security. A practitioner's guide, BCS 2017, 9781780173436
182. Cyber Security. A Starter Guide to Cyber Security for Beginners, Kali 2019, B081M3ND9K
183. Cyber Security. An Introduction, Gower 2015, 147246673X
184. Cyber Security. Analytics, Technology and Automation, Springer 2015, 331918301X
185. Cyber Security and Global Information Assurance, IGI 2009, 1605663263
186. Cyber Security and IT Infrastructure Protection, Syngress 2013, 0124166814
187. Cyber Security and Privacy. 4th Conf. CSP, Springer 2015, 331925359X
188. Cyber Security and Privacy. Conf., Springer 2013, 3642412041
189. Cyber Security and Privacy. Conf., Springer 2017, 3319125737

190. Cyber Security Awareness for CEOs and Management, Syngress 2016, 0128051108
191. Cyber Security Basics. Removing Cognitive Barriers, Franke 2016, 1522952195
192. Cyber Security Comprehensive Beginners Guide to Learn the Basics, Walker 2019, 1075257670
193. Cyber Security. Conf. CSI, Springer 2018, 9811085358
194. Cyber Security. Deterrence and IT Protection for Critical Infrastructures, Springer 2013, 3319022784
195. Cyber Security Engineering. A Practical Approach for Systems, Addison 2016, 0134189809
196. Cyber Security Essentials, Press 2011, 1439851239
197. Cyber Security for Cyber Physical Systems, Springer 2018, 3319758799
198. Cyber Security For You, Turner 2016, B01KPGY914
199. Cyber Security in Organizations, Fritzvold 2017, 172018996X
200. Cyber Security in Parallel and Distributed Computing, Wiley 2019, 9781119488057
201. Cyber Security Policy Guidebook, Wiley 2012, 1118027809
202. Cyber Security. Power and Technology, Springer 2018, 3319753061
203. Cyber Security. Shocking Facts That You Need to Know, Whitehill 2015, B015D7GBU2
204. Cyber Security. Simply. Make it Happen, Springer 2017, 3319465287
205. Cyber Security Standards. Practices and Industrial Applications, Premier 2011, 1609608518
206. Cyber Security. The Beginners Guide to Learning The Basics, Zhang 2019, 1698238533
207. Cyber Security. The Lifeline of Information and Communication, Springer 2020, 3030317021
208. Cyber Security. Threats and Responses, Jones 2019, 1440861730

209. Cyber Security. Ultimate Beginners Guide to Learn the Basics, LLC 2019, B07XGCD6L5
210. Cyber Security. Understand Hacking and Protect Yourself, Studios 2017
211. Thomas J. Shaw, David D. Coleman, Gregory S. White, Dwayne Williams, Tytuł: Cyber Security, Wydawnictwo: Wiley, Rok wydania: 2013
212. Brink, Alexis, Tytuł: Cyber Self-Defense: Expert Advice to Avoid Online Predators, Wydawnictwo: Identity Press, Rok wydania: 2014.
213. Cyber Situational Awareness Issues and Research, Springer 2009, 1441901396
214. DECYZJA RADY z dnia 23 września 2013 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (2013/488/UE)
215. DECYZJA KOMISJI (UE, Euratom) 2015/444 z dnia 13 marca 2015 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE
216. Przepisy bezpieczeństwa Europejskiej Agencji Kosmicznej uregulowane są w dokumencie ESA/REG/004 z dnia 1 lipca 2020 r.
217. SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANIZATION (NATO) Note by the Secretary General
218. Revision 1 to C-M(2002)49 dated 17 June 2002
219. AC/35-D/2000 – Dyrektywa Bezpieczeństwa Osobowego;
220. AC/35-D/2001 – Dyrektywa Bezpieczeństwa Fizycznego;
221. AC/35-D/2002 – Dyrektywa Bezpieczeństwa Obiegu Informacji;
222. AC/35-D/2003 – Dyrektywa Projektów Niejawnych i Bezpieczeństwa Przemysłowego;
223. AC/35-D/2004 – Dyrektywa podstawowa INFOSEC;
224. AC/35-D/2005 – Dyrektywa zarządzania INFOSEC w systemach teleinformatycznych (CIS).

225. Imed El Fray, Mirosław Kurkowski , Jerzy Pejaś, Witold Maćków, A new mathematical model for analytical risk assessment and prediction in IT systems, Control and Cybernetics vol. 41 (2012) No. 1

Indeks tabel