KANCELARIA PREZESA
RADY MINISTRÓW

Polityka Bezpieczeństwa Informacji CEPiK

Wyciąg z Polityki Bezpieczeństwa Informacji CEPiK

KANCELARIA PREZESA
RADY MINISTRÓW

Metryka dokumentu

Właściciel	Minister właściwy ds. informatyzacji			
Tryb zatwierdzenia				
Stan	Uzgodniony	Daty obowiązywania		
Założenia	Dokument stanowi wyciąg Polityki Bezpieczeństwa Informacji CEPiK			
Adresaci	Uprawnieni Interesariusze CEPiK			
Historia dokumentu	Wersja	Data	Autor	Opis zmian
	1.0	17.11.2021	Zespół COI	Opracowanie dokumentu
	1.1	25.02.2022	KPRM, MSWiA	Uzgodnienia

KANCELARIA PREZESA RADY MINISTRÓW

Spis treści

1. Cel

Celem niniejszego dokumentu jest wskazanie najważniejszych zasad obowiązujących w zakresie zarządzania bezpieczeństwem informacji w CEPiK (Centralna Ewidencja Pojazdów i Kierowców) oraz uzyskanie i utrzymanie odpowiednio wysokiego poziomu bezpieczeństwa zasobów rozumiane jako zapewnienie poufności, integralności i dostępności zasobów, a także zapewnienie rozliczalności podejmowanych działań.

Przedmiotowy dokument stanowi wyciąg z dokumentu zasadniczego, jakim jest Polityka Bezpieczeństwa Informacji CEPiK (PBI CEPiK) i stanowi kompendium podstawowej wiedzy z zakresu Systemu Zarządzania Bezpieczeństwem Informacji CEPiK (SZBI CEPiK) oraz przeznaczony jest dla uprawnionych Interesariuszy systemu.

Przedmiotem dokumentu jest określenie kluczowych zasad dotyczących zapewnienia bezpieczeństwa informacji (danych) CEPiK, obejmujących zabezpieczenia:

a. organizacyjne obszaru zawierającego dane (informacje) podlegające ochronie;
b. techniczne systemu informacyjnego zawierającego dane podlegające ochronie;

w zakresie:

a. aktywów systemu;
b. klasyfikacji informacji;
c. postepowania z informacją;
d. kontroli dostępu do informacji;
e. obsługi nośników zawierających informacje;
f. bezpieczeństwa fizycznego i środowiskowego;
g. postępowania z incydentami bezpieczeństwa informacji;
h. zarządzania ryzykiem;
i. monitorowania i nadzoru nad zmianą.

2. Opis systemu

CEPiK, czyli Centralna Ewidencja Pojazdów i Kierowców, łączy w sobie dwie ewidencje:

a. Centralną Ewidencję Pojazdów (CEP) oraz
b. Centralną Ewidencję Kierowców (CEK).

W Centralnej Ewidencji Pojazdów gromadzone są dane o pojazdach, które zostały zarejestrowane w Polsce. Szczegółowy zakres danych i informacji gromadzonych w CEP określa ustawa z dnia 20 czerwca 1997 r. Prawo o Ruchu Drogowym.

W Centralnej Ewidencji Kierowców gromadzone są dane o użytkownikach, którzy posiadają uprawnienia do kierowania pojazdami silnikowymi ale również o użytkownikach, którym cofnięto te uprawnienia czy też użytkownikach nieposiadających uprawnień, które mają zakaz prowadzenia pojazdów. Szczegółowy zakres danych i informacji gromadzonych w CEK określa ustawa z dnia 20 czerwca 1997 r. Prawo o Ruchu Drogowym.

CEPiK integruje dane pochodzące z różnych źródeł, zapewnia wsparcie dla:

a) procesów związanych z rejestracją pojazdów i wydawaniem dokumentów potwierdzających uprawnienia do kierowania pojazdami,
b) procesów związanych z przeprowadzeniem badań technicznych pojazdów,
c) działań organów odpowiedzialnych za bezpieczeństwo państwa i obywateli.

Właścicielem systemu jest minister właściwy ds. informatyzacji, który jest odpowiedzialny za zapewnienie bezpieczeństwa danych i systemu. Bezpieczeństwo systemu adresowane w niniejszej PBI odnosi się do odpowiednich regulacji prawnych dotyczących bezpieczeństwa systemów informatycznych, ochrony danych osobowych, a także odpowiednich dokumentów strategicznych dotyczących funkcjonowania systemów administracji rządowej.

3. Odpowiedzialność

3.1. Odpowiedzialność w zakresie bezpieczeństwa

Obowiązek przestrzegania postanowień Polityki Bezpieczeństwa Informacji CEPiK dotyczy wszystkich Interesariuszy, w szczególności Interesariuszy wewnętrznych mających wpływ na kształt i funkcjonowanie systemu. Wszyscy pracownicy oraz współpracownicy Interesariuszy wewnętrznych mają obowiązek zapoznania się z treścią i postanowieniami PBI CEPiK.

Za bezpieczeństwo informacji odpowiedzialny jest każdy pracownik/ współpracownik Interesariusza.

Właściciel Systemu CEPiK pełni rolę najwyższego kierownictwa w zakresie zarządzania bezpieczeństwem informacji CEPiK i przetwarzanych w nim danych. Jest on odpowiedzialny za

utrzymanie i rozwój systemu, stosuje się do wszelkich wymaganych przepisów prawa. Najwyższe Kierownictwo ustanawia zasady dotyczące zarządzania bezpieczeństwem informacji poprzez opracowanie i wdrożenie niniejszej Polityki Bezpieczeństwa Informacji, zgodnej z normą ISO 27001, której celem jest zapewnienie bezpieczeństwa i ochrony danych przetwarzanych w ramach systemu CEPiK:

Gestor Systemu CEPiK jest odpowiedzialny za kierunki rozwoju systemu od strony biznesowej, za zdefiniowanie ról i odpowiedzialności w systemie bezpieczeństwa oraz za ich przegląd i aktualizację. Zapewnia również właściwy nadzór nad Polityką Bezpieczeństwa Informacji CEPiK i związanymi z nią dokumentami, stanowiącymi dokumentację bezpieczeństwa systemu.

3.2. Odpowiedzialność w zakresie kompetencji

Właściciel systemu oraz każdy z interesariuszy realizujący działania na rzecz systemu zobowiązani są do zapewnienia odpowiednich kompetencji (tj. wiedza, umiejętności, doświadczenie, wykształcenie, szkolenia, staże, udziały w konferencjach, itp.) w zakresie bezpieczeństwa informacji swoim pracownikom mającym dostęp do danych i systemu oraz dokumentacji technicznej i eksploatacyjnej adekwatnie do realizowanych funkcji w zakresie eksploatacji, utrzymania i rozwoju systemu. Nabywanie, utrzymanie i rozwój kompetencji jest procesem realizowanym w trybie ciągłym przez właściwe komórki organizacyjne każdego z interesariuszy CEPiK. Zakres posiadanych kompetencji podlega okresowej weryfikacji i ocenie.

3.3. Wykaz ról i odpowiedzialności

W zarządzaniu bezpieczeństwem informacji CEPiK istotne znaczenie ma zdefiniowanie ról i odpowiedzialności. Podstawą do tego są regulacje prawne dotyczące Centralnej Ewidencji Pojazdów i Kierowców oraz zapisy PBI CEPiK wraz z związanymi z nią procedurami i politykami, które definiują role i ich funkcje w zapewnieniu bezpieczeństwa informacji w rozwoju, eksploatacji i utrzymaniu CEPiK.

Role i ich odpowiedzialności podlegają okresowej weryfikacji oraz powinny być aktualizowane każdorazowo w przypadku rozbudowy systemu i zmian prawnych, które mogą wpłynąć na zakres odpowiedzialności poszczególnych ról.

Zdefiniowane role i ich odpowiedzialności znajdują się w „Wykazie ról i odpowiedzialności CEPiK", załączniku nr 1.4 do PBI CEPiK.

4. Zgodność prawna

CEPiK działa w ramach określonych przez akty prawne RP. Polityka Bezpieczeństwa Informacji CEPiK jest oparta oraz pozostaje w zgodności z obowiązującymi przepisami prawnymi:

1. Konstytucja Rzeczypospolitej Polskiej;
2. Ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 2070);
3. Ustawą z dnia 20 czerwca 1997 r. Prawo o ruchu drogowym (Dz. U. z 2021 r. poz. 450, z późn. zm.);
4. Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247);
5. Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781);
6. Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119 z 04.05.2016, s. 1);
7. Ustawą z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz. U. z 2019 r. poz. 848);
8. Ustawą z dnia 5 sierpnia 2010 o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742).
9. Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018 poz. 1560 z późn. zm.)

5. Interesariusze i użytkownicy CEPiK

W ramach PBI CEPiK można wymienić i scharakteryzować następujące grupy interesariuszy:

1. Właściciel systemu CEPiK – Minister właściwy ds. informatyzacji, podmiot decyzyjny w sprawach związanych z eksploatacją, utrzymaniem i rozwojem systemu CEPiK;
2. Interesariusze wewnętrzni – interesariusze mający bezpośredni wpływ na funkcjonowanie CEPiK pod kątem m.in. prawnym, organizacyjnym, technicznym;

3. Interesariusze zewnętrzni – interesariusze uprawnieni bezpośrednio wskazani w „Prawo o ruchu drogowym” jako podmioty udostępniające/ przekazujące i pobierające dane;
4. Interesariusze indywidualni – podmioty indywidualne korzystające z CEPiK, które wykażą w tym interes prawny, który wynika z przepisów prawa, adekwatnie do wskazanego interesu.

Wykaz interesariuszy został opisany w dokumencie „Wykaz interesariuszy i użytkowników CEPiK”, załączniku nr 1.2 do PBI CEPiK.

Zakres uprawnień i zadań podmiotów uprawnionych wynika z przepisów prawa (wyszczególnionych w rozdziale 4 niniejszego dokumentu), a udostępnienie danych może być realizowane w zakresie niezbędnym do realizacji zadań publicznych, określonych w przepisach.

6. Zapewnienie bezpieczeństwa informacji

Proces zarządzania bezpieczeństwem informacji jest działaniem realizowanym w sposób ciągły, w oparciu o podejście systemowe zapewniające w sposób uniwersalny adekwatność stosowanych środków ochrony informacji. Wszystkie czynności realizowane w tym procesie podlegają dokumentowaniu oraz cyklicznemu przeglądowi oraz są na bieżąco monitorowane. Zapewnienie ochrony informacji jest realizowane w wielu płaszczyznach jednocześnie zarówno w zakresie organizacyjnym jak i technicznym.

Interesariusze realizujący zadania w ramach systemu zapewniają niezbędne zasoby osobowe, finansowe i lokalowe dla realizacji wdrożenia, utrzymywania i ciągłego doskonalenia postanowień niniejszej Polityki w zakresie odpowiednim dla zakresu oddziaływania i kompetencji każdego z interesariuszy. Najwyższe kierownictwo - minister właściwy ds. informatyzacji zapewnia, że zdefiniowane w PBI CEPiK rozwiązania organizacyjne i techniczne bezpieczeństwa oraz cele stosowania zabezpieczeń informacji są zgodne ze strategicznym kierunkiem rozwoju, eksploatacji i utrzymania systemu oraz celem zapewnienia wysokiego poziomu bezpieczeństwa oraz zapewnia niezbędne zasoby osobowe, finansowe i lokalowe dla wdrożenia, utrzymywania oraz ciągłego doskonalenia postanowień niniejszej polityki.

Wszelkie działania operacyjne w zakresie zarządzania systemem bezpieczeństwa informacji pozostają w zakresie odpowiedzialności Gestora systemu CEPiK.

6.1. Aktywa systemu

Aktywa systemu teleinformatycznego to kluczowe zasoby wykorzystywane przez system takie jak:

a) dokumentacja systemu,
b) zasoby ludzkie,
c) infrastruktura lokalowa,
d) infrastruktura IT.

Proces zarządzania aktywami realizowany jest w celu wyeliminowania zagrożeń, czyli niepożądanych zdarzeń, mogących mieć wpływ na informacje.

System CEPiK korzysta z wielu źródeł danych – realizuje funkcje i procesy biznesowe wykorzystując dane zawarte w poszczególnych rejestrach państwowych. W tym zakresie aktywa systemu związane z bezpieczeństwem informacji oraz środkami przetwarzania informacji są zinwentaryzowane a ich ewidencja na bieżąco aktualizowana.

Wykaz aktywów systemu w zakresie zarządzania ryzykiem w CEPiK zawarty jest w „Wykazie aktywów systemu w zakresie zarządzania ryzykiem CEPiK", załączniku nr 2.7 do PBI CEPiK.

6.2. Klasyfikacja i postępowanie z informacją

Procedura oznaczania informacji opiera się o zasadę konsekwencji „wycieku" informacji podlegających ochronie. Oznaczenie informacji polega modelowo na podziale informacji na informację publiczną oraz informacje podlegające szczególnej ochronie.

6.2.1. Odpowiedzialność

Do stosowania zasad związanych z oznaczaniem informacji zobowiązani są wszyscy uczestnicy dowolnych procesów w obszarze CEPiK.

Rolą odpowiedzialną za zapewnienie adekwatnego oznaczania informacji jest Właściciel Informacji.

6.2.2. Zasady oznaczania informacji

Zasady oznaczania informacji obowiązują w systemie CEPiK i dotyczą wszystkich rodzajów informacji, które w ramach systemu mogą zostać wytworzone oraz obejmuje wszystkie obszary systemu CEPiK. Oznaczanie informacji ma na celu zapewnienie bezpieczeństwa informacji poprzez między innymi

zachowanie pełnej świadomości osoby posiadającej dostęp do danej informacji jak i świadomość konsekwencji wynikających z ich nieprawidłowego przetwarzania (użycia).

Wszelkie odstępstwa od niniejszej procedury wymagają zgody upoważnionego Właściciela Biznesowego Systemu (na podstawie upoważnienia od Najwyższego Kierownictwa).

W ramach procedury oznaczaniu podlegają wszelkie informacje podlegające ochronie zgodnie z opracowaną Polityką Bezpieczeństwa Informacji. Poniżej opisano poszczególne etapy procedury w kolejności ich występowania:

1. Informacja – identyfikacja informacji podlegającej ochronie, występująca i przekazywana w dowolnej formie: elektronicznej, papierowej, werbalnej. Źródłem powstania informacji podlegającej oznaczaniu może być dowolny uczestnik dowolnego procesu w ramach centrum przetwarzania danych. Istotnymi i głównymi miejscami w systemie są informacje występujące w formie elektronicznej – repozytoria danych i rejestry danych. Odpowiedzialność w tym zakresie przypisana jest do Właściciela Informacji.
2. Klasyfikacja informacji – czynność polegająca na określeniu rodzaju zidentyfikowanej informacji zgodnie ze schematem klasyfikacji informacji. Klasyfikacja informacji ma bezpośredni wpływ na dalszą obsługę informacji. W szczególności dotyczy to systemów elektronicznych, przetwarzania danych, na których odbywa się instalacja systemów powierzonych obsługujących różne dane. Odpowiedzialność w tym zakresie przypisana jest do Właściciela Informacji.
3. Oznaczenie informacji – czynność polegająca na oznaczeniu informacji w adekwatny do rodzaju informacji sposób, np. forma papierowa – opisanie komentarzem, forma elektroniczna – oznaczenie cyfrowe, forma werbalna – powiadomienie o jej znaczeniu. Zapis dotyczy także oznaczenia dokumentów gromadzonych w formie elektronicznej np. bazy danych, zasoby pamięci masowej przechowujących/ przetwarzających dane. Odpowiedzialność w tym zakresie przypisana jest do Właściciela Informacji.
4. Obsługa Informacji – wykorzystywanie w normalnej pracy organizacji informacji chronionej zgodnie z jej przeznaczeniem oraz zgodnie z dokonaną jej wcześniejszą klasyfikacją.
5. Cykliczna weryfikacja procesu – powtarzalna czynność wykonywana w określonych odstępach czasu polegająca na przeglądzie adekwatności, celowości i użyteczności.

6. Cykliczna weryfikacja poprawności oznaczenia informacji – powtarzalna czynność wykonywana w określonych odstępach czasu polegająca na przeglądzie poprawności oznaczenia informacji podlegająca nadzorowi Właściciela Informacji.

6.2.3. Klasyfikacja informacji

Klasyfikacja informacji opiera się o zasadę oceny negatywnych konsekwencji dostępu osób nieupoważnionych do informacji podlegającej ochronie. Właściciel Informacji powinien zapewnić jasne i klarowne zasady oznaczania informacji poprzez opracowanie zasad i wytycznych czy instrukcji szczegółowych oznaczania danych.

Informacje zostały skategoryzowane odpowiednio na:

a. informacje publiczne;
b. informacje prawnie chronione zawierające Dane Osobowe lub Tajemnicę Przedsiębiorstwa;
c. informacje niejawne.

„Dokument roboczy" czyli będący w trakcie tworzenia, nie może zostać upubliczniony na żadnym etapie jego opracowywania.

Klasyfikacja informacji została szerzej opisana w dokumencie „Polityka klasyfikacji informacji CEPiK", załączniku nr 2.8 do PBI CEPiK.

6.2.4. Sposoby oznaczenia informacji

Sklasyfikowane informacje powinny zostać w sposób formalny i jednoznaczny oznaczone w celu zapewnienia pełnej świadomości użytkownika, który daną informację będzie w przyszłości wykorzystywał.

Sposoby oznaczenia informacji zostały szerzej opisane w dokumencie „Polityka klasyfikacji informacji CEPiK", załączniku nr 2.8 PBI CEPiK.

Żaden „dokument roboczy" czyli będący w trakcie opracowywania nie może zostać upubliczniony na żadnym etapie jego opracowywania.

Przyjęto, że każdy dokument, który nie zawiera adnotacji o klasyfikacji stanowi dokument roboczy i nie może bez dodatkowych ustaleń z Właścicielem Informacji zostać udostępniony publicznie.

6.2.5. Bieżąca obsługa informacji

Istotnym elementem związanym z zarządzaniem informacją jest jej obsługa bieżąca. Zasady określające reguły postepowania z kategoriami informacji zostały przedstawione w dokumencie „Polityka klasyfikacji informacji CEPiK", w załączniku nr 2.8 do PBI CEPiK

6.2.6. Przechowywanie dokumentów

Wszystkie oznaczone informacje (z wyłączeniem informacji werbalnej) powinny być rejestrowane w odpowiednio zabezpieczonych repozytoriach wraz ze spisem oznaczonych dokumentów. W przypadku automatycznej generacji listy oznaczonych dokumentów, spis powinien być cyklicznie eksportowany i zabezpieczany (nie dotyczy dokumentów oznaczonych jako niejawne).

6.2.7. Uwagi dodatkowe

Wszelkie naruszenia bezpieczeństwa informacji i danych osobowych powinny zostać bez zbędnej zwłoki zgłoszone zgodnie z „Procedurą zgłaszania incydentów związanych z bezpieczeństwem informacji", załącznikiem nr 2.23 do Polityki Bezpieczeństwa Informacji CEPiK.

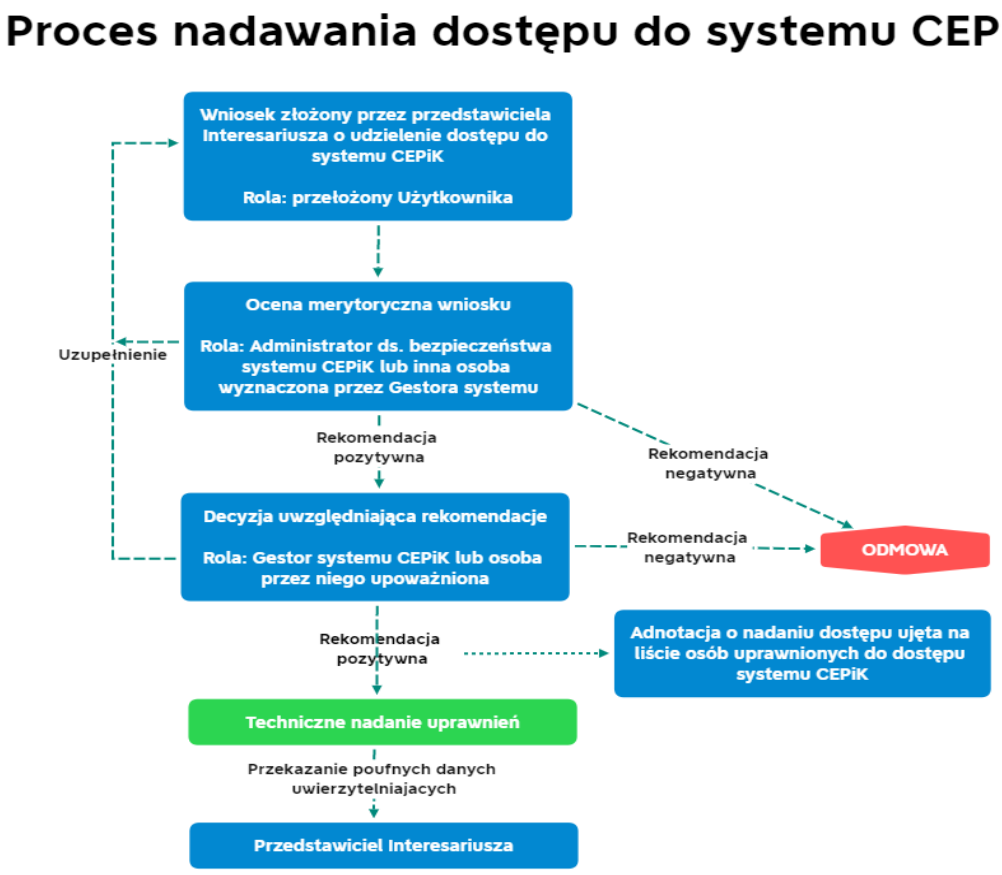
6.3. Kontrola dostępu do informacji

6.3.1. Nadawanie uprawnień

Przydzielanie dostępu do systemu informatycznego CEPiK realizowane jest w oparciu o następujące zasady:

1. Minimalnych przywilejów – każdy użytkownik posiada prawa dostępu do zasobów ograniczone wyłącznie do tych, które są niezbędne do wykonywania powierzonych mu obowiązków.
2. Wiedzy koniecznej – każdy użytkownik posiada wiedzę o zasobach ograniczoną wyłącznie do zagadnień, które są niezbędne do realizacji powierzonych mu zadań.
3. Domniemanej odmowy – wszystkie działania, które nie są jawnie dozwolone są zabronione.

Poniżej na Rysunku nr 1, przedstawiono diagram procesu nadania dostępu do systemu CEPiK.

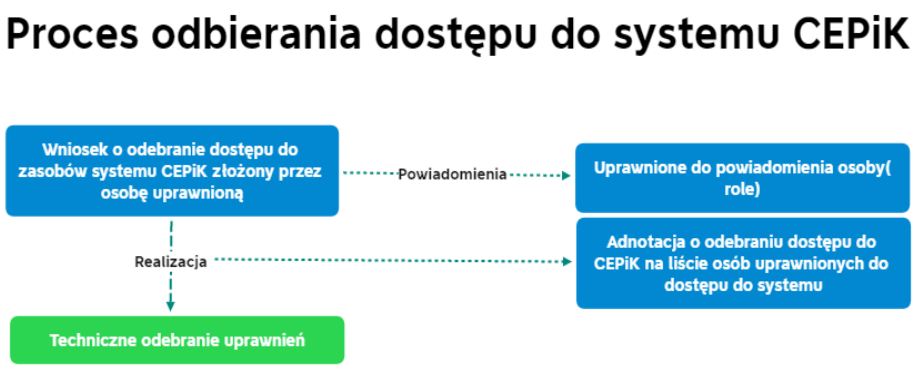


Rysunek 1 Proces nadania dostępu do CEPiK

6.3.2. Odbieranie uprawnień

Odbieranie dostępu to czynność polegająca na zablokowaniu możliwości logowania się użytkownika do zasobów systemu CEPiK.

Poniżej na rysunku nr 2 przedstawiono schemat procesu odebrania dostępu do systemu CEPiK.



Rysunek 2. Proces odbierania dostępu do systemu CEPiK

6.3.3. Kontrola i przegląd uprawnień

Z uwagi na konieczność zapewnienia skuteczności działania procesu nadawania, zmiany i odbierania uprawnień dostępu do systemu informatycznego CEPiK należy okresowo przeprowadzać kontrole i przeglądy obejmujące następujące zagadnienia:

1. Przegląd procedur w zakresie adekwatności, przydatności oraz aktualności kontroli uprawnień.
2. Weryfikacja poprawności realizacji procesu zarządzania uprawnieniami na zgodność z zasadami opisanymi w odpowiedniej dokumentacji.
3. Weryfikacja funkcjonujących ról oraz zasadności zakresu nadanych lub zmodyfikowanych uprawnień w odniesieniu do dostarczonych wniosków.
4. Kontrola wykonania procesu odebrania uprawnień zgodnie z terminami uwzględnionymi w dostarczonych wnioskach.
5. Przegląd w zakresie funkcjonujących w systemie profili, których czas ostatniego logowania użytkownika wzbudza wątpliwości w zakresie zasadności funkcjonowania dostępu do systemu.
6. Kontrola aktualności danych zawartych w dokumencie „Lista osób uprawnionych do dostępu do systemu CEPiK", którego draft stanowi załącznik nr 1 do „Polityki kontroli dostępu CEPiK", załączniku nr 2.10 do PBI CEPiK, w odniesieniu do stanu faktycznego dostępnego w systemie.

Kontrola i przegląd opisanych powyżej obszarów powinna odbywać się cyklicznie, nie rzadziej niż raz w roku. W przypadku wykrycia niezgodności niezwłocznie należy podjąć odpowiednie działania korygujące w zakresie adekwatnym do zidentyfikowanego problemu oraz wdrożyć środki naprawcze mające na celu wyeliminowanie lub zmniejszenie prawdopodobieństwa jego wystąpienia w przyszłości.

Szczegółowo zagadnienia z zakresu kontroli i przeglądu uprawnień opisano w dokumencie **Błąd! Nie można odnaleźć źródła odwołania.** ~~„Polityka kontroli dostępu CEPiK" – załączniku nr 2.10 do PBI CEPiK~~.

6.4. Zabezpieczenia kryptograficzne

Centrum przetwarzania danych CEPiK implementuje, jak również udostępnia szereg mechanizmów kryptograficznych, które muszą być uwarunkowane wymaganiami zależnymi od zidentyfikowanego poziomu ochrony przetwarzanych w systemie zbiorów danych zgodnie z załącznikiem nr 2.8 „Polityka klasyfikacji informacji CEPiK" do Polityki Bezpieczeństwa Informacji CEPiK. Ochronie kryptograficznej

powinny podlegać dane przetwarzane na nośnikach fizycznych, w bazach danych, systemach plików, jak również dane przesyłane za pośrednictwem sieci telekomunikacyjnych, poczty elektronicznej oraz systemów obsługi zgłoszeń serwisowych. Należy mieć jednak na uwadze, aby w stosunku do obszarów stosowania zabezpieczeń kryptograficznych zawsze stosować zasadę nadmiarowości tj. ochronę kryptograficzną należy stosować we wszystkich uzasadnionych przypadkach, również w takich, które nie zostały uregulowane polityką bezpieczeństwa informacji.

Zakres, adekwatność i skuteczność wdrożonych zabezpieczeń kryptograficznych w odniesieniu do przetwarzanych danych w CEPiK podlega ocenie w trybie ciągłym oraz może ulec modyfikacji na wypadek pozyskanych informacji o lukach i podatnościach zastosowanych mechanizmów lub z powodu wystąpienia innych przesłanek powodujących podwyższenie ryzyka utraty możliwości zapewnienia atrybutów bezpieczeństwa, w szczególności poufności, integralności oraz rozliczalności.

Szczegółowo zagadnienia z zakresu zabezpieczeń kryptograficznych opisano w dokumencie „Polityka zabezpieczeń kryptograficznych CEPiK", załączniku nr 2.11 do PBI CEPiK.

6.5. Bezpieczeństwo stanowisk pracy

6.5.1. Zasady przetwarzania informacji na stacjach roboczych

Interesariusze wewnętrzni i zewnętrzni mają możliwość połączenia się z systemem CEPiK zarówno przez sieci wydzielone jak i za pośrednictwem sieci publicznej.

Zalecanym sposobem podłączenia infrastruktury interesariuszy systemu jest wykorzystanie dedykowanej wydzielonej sieci teleinformatycznej z zachowaniem pełnej separacji stacji roboczych systemu od innych sieci.

Interesariusze łączący się z systemem przez sieć publiczną muszą zestawić bezpieczne połączenie VPN z wykorzystaniem certyfikatu VPN. Dopiero po zestawieniu połączenia VPN mają możliwość skorzystania z aplikacji w przeglądarce internetowej stacji roboczej łączącej się z systemem. Autoryzacja i uwierzytelnienie interesariusza w aplikacjach systemu CEPiK są realizowane w oparciu o posiadany certyfikat SSL umieszczony na mikroprocesorowej karcie kryptograficznej.

Z kolei interesariusze łączący się z systemem przez sieć wydzieloną mają możliwość skorzystania z aplikacji systemu bez konieczności zestawiania bezpiecznego połączenia VPN – w tym przypadku

autoryzacja i uwierzytelnienie w aplikacjach systemu CEPiK są realizowane w oparciu o posiadany przez interesariusza certyfikat SSL umieszczony na mikroprocesorowej karcie kryptograficznej.

Szczegółowe zasady dotyczące integracji z siecią dostępową do systemu CEPIK są przedstawione w dokumencie „Polityka korzystania z sieci i usług sieciowych CEPiK" stanowiącym załącznik nr 2.18 do dokumentu głównego PBI CEPiK.

Zasady kont i haseł:

1. Wbudowane konto administratora powinno być używane tylko w przypadku wykonywania czynności administratora.
2. Każdemu użytkownikowi stacji roboczej powinno być założone oddzielne konto bez przypisanych uprawnień administratora o ile nie jest to wymagane do bieżącej pracy.
3. Długość hasła konta administratora lub użytkownika z uprawnieniami administratora powinna wynosić nie mniej niż 12 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny).
4. Okres ważności hasła nie powinien być dłuższy niż 30 dni.
5. Długość hasła konta użytkownika powinna wynosić nie mniej niż 10 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny).
6. Zaleca się wprowadzić regulacje sankcjonujące zmianę pin-kodu mikroprocesorowych kart kryptograficznych nie rzadziej niż co 30 dni.
7. Jeśli to możliwe zalecane jest zastąpienie logowania tradycyjnego (login i hasło) logowaniem z użyciem kart mikroprocesorowych, czytników cech biometrycznych, kluczy bezprzewodowych.
8. Zaleca się wprowadzić stosowne regulacje sankcjonujące sposoby przechowywania nazw użytkowników i haseł oraz zabraniające udostępnia ich innym osobom.

Ochrona antywirusowa:

1. Wymagane jest zainstalowanie oprogramowania antywirusowego oraz wdrożenie regulacji zapewniających aktualizację sygnatur antywirusowych nie rzadziej niż raz w tygodniu.
2. Zalecane jest wdrożenie regulacji zapewniających pełne skanowanie antywirusowe stacji co najmniej 1 raz w tygodniu w przypadku braku ochrony w czasie rzeczywistym i nie mniej niż 1 raz w miesiącu w przypadku stosowania ochrony w czasie rzeczywistym.

System operacyjny:

1. Wymagane jest stosowanie systemów operacyjnych w wersjach wspieranych przez ich producentów.
2. Wymagane jest wdrożenie regulacji związanych z aktualizowaniem systemu operacyjnego oraz wykorzystywanego oprogramowania zgodnie z zaleceniami producentów.
3. Zaleca się konfigurację „kosza" systemowego, aby nie przechowywał usuniętych plików.

Informatyczne nośniki danych:

1. W przypadku stosowania dysków twardych umieszczonych w wyjmowanych kieszeniach powinny być one wyposażone w zamknięcie na kluczyk i zamknięte, gdy znajduje się w nich dysk. Po zakończonej pracy zalecane jest usunięcie dysku i jego dalsze przechowywanie w zabezpieczonej szafie.
2. Powinny być wdrożone regulacje zapewniające obsługę informatycznych nośników danych, podłączanych okresowo do stacji, tak aby po zakończeniu pracy były one usuwane ze stacji i przechowywane w bezpieczny sposób.
3. Informatyczne nośniki danych, które będą służyły do wynoszenia informacji poza obręb pomieszczenia powinny być wyposażone w oprogramowanie lub rozwiązanie sprzętowe umożliwiające szyfrowanie danych z użyciem hasła dostępowego nie krótszego niż 10 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny).

Umiejscowienie sprzętu oraz zalecenia organizacyjne:

1. Stacja robocza powinna być ustawiona w miejscu uniemożliwiającym do niej dostęp osobom nieupoważnionym.
2. Zalecane jest takie ustawienie monitora, aby nie było możliwości podejrzenia danych wyświetlonych na ekranie przez osoby nieuprawnione oraz ustawienie czasu automatycznego uruchamiania wygaszacza ekranu na maksymalnie 5 minut. Wznowienie pracy powinno wymagać podania hasła.
3. Zalecane jest blokowanie stacji przy każdorazowym opuszczeniu stanowiska.
4. Zalecane jest takie ustawienie drukarki, aby nie było możliwości podejrzenia bądź pobrania wydruków przez osoby nieuprawnione.

Szczegółowe wytyczne związane z zasadami przetwarzania informacji na stacjach roboczych zostały ujęte w dokumencie „Wytyczne dla stacji roboczych obsługi systemu CEPiK", załączniku nr 2.3 do PBI CEPiK.

W celu zapobieżenia ujawnieniu, zniszczeniu lub kradzieży informacji systemu zawartych na dokumentach papierowych oraz informatycznych nośnikach danych zaleca się stosowanie zasad „czystego biurka". Dla zabezpieczenia informacji przechowywanych na serwerach, stacjach roboczych oraz urządzeniach mobilnych zaleca się stosowanie zasad „czystego ekranu".

Podstawowe zasady:

1. Chronione nieużywane informacje systemu należy przechowywać w sejfie, zamykanej szafie lub szufladzie.
2. Stanowisko pracy, powinno być tak zaplanowane, aby żadna osoba postronna nie mogła podglądać chronionych informacji niezależnie od ich formy.
3. Opuszczając pokój (niezależnie na jak długo) należy zamknąć drzwi na klucz, lub zablokować dostęp do pomieszczenia aktywując inne dostępne zabezpieczenia oraz schować do zamykanej szafy lub szuflady wszelkie istotne dokumenty i nośniki informacji.
4. Każdorazowe odejście od stacji roboczej powinno zostać poprzedzone zamknięciem sesji lub zablokowaniem komputera za pomocą mechanizmu blokowania ekranu i klawiatury przy użyciu hasła, tokenu lub innego mechanizmu uwierzytelniania użytkownika lub innych dostępnych zabezpieczeń, w tym mechanicznych.
5. Po zakończeniu pracy wszystkie dokumenty i nośniki informacji systemu istotne z punktu widzenia bezpieczeństwa informacji należy przechowywać w zamykanych, zabezpieczonych i w miarę możliwości ognioodpornych szafach. Nie powinny pozostać niezabezpieczone, gdyż w razie kradzieży, katastrofy naturalnej lub aktu terroru mogłyby dostać się w niepowołane ręce, zostać uszkodzone lub zniszczone.
6. Po zakończeniu pracy należy zamknąć wszystkie aktywne sesje oraz wylogować się z systemu lub aktywować oprogramowanie blokujące klawiaturę i wygaszacz ekranu zabezpieczony hasłem.
7. Nie należy pozostawiać nawet na chwilę bez opieki wydruków oraz kopiowanych dokumentów, które zostały wykonane na faksach, kserokopiarkach i drukarkach, tzn. : należy odebrać je z urządzenia w taki sposób, aby żadna osoba postronna nie mogła się zapoznać z ich zawartością.

6.5.2. Zasady przesyłania informacji

W systemie CEPiK komunikacja elektroniczna odbywa się poprzez n/w kanały komunikacyjne:

- poczta elektroniczna,

- system elektronicznego obiegu dokumentów (SEOD, systemy EOD),
- system ePUAP/PZ.

W zakresie bezpieczeństwa przesyłania informacji dostępnymi kanałami komunikacji elektronicznej obowiązują następujące zasady ogólne:

1. Każda informacja powinna być odpowiednio i jednoznacznie oznaczona i sklasyfikowana;
2. Każda wiadomość ma wyraźnie wskazanego adresata. Wiadomości elektroniczne są przesyłane tylko do wyselekcjonowanej, dedykowanej osoby lub grupy osób.
3. Wiadomości nie są przekazywane dalej, do kolejnych odbiorców bez wyraźnej, pisemnej zgodny jej pierwotnego nadawcy.
4. Wiadomości powinny zawierać właściwą adnotację o przeznaczeniu dla konkretnego adresata lub grupy adresatów i zobowiązaniu postronnego odbiorcę wiadomości do jej usunięcia.
5. Wiadomości i dokumenty w SEOD są przydzielane do odpowiednich spraw/teczek z ograniczonym dostępem tylko dla osób/ról dla nich właściwych.
6. Wiadomości i dokumenty w ePUAP są przydzielane do odpowiednich skrytek z ograniczonym dostępem tylko dla osób/ról dla nich właściwych.
7. Dozwolone jest korzystanie wyłącznie ze służbowej poczty elektronicznej. Każdy interesariusz zapewnia do stosowania sprawny i bezpieczny system pocztowy.
8. Komunikacja powinna być prowadzona właściwym trybem administracyjnym, czy prawnym, jeśli taki ma zastosowanie do przedmiotu komunikacji.
9. W przypadku informacji niejawnych, w rozumieniu ustawy o ochronie informacji niejawnych, mają zastosowanie odrębne od PBI CEPiK regulacje wynikające z postanowień tej ustawy. Informacje niejawne nie są przekazywane w formie wiadomości elektronicznych.
10. Przy przesyłaniu informacji stosowane są odpowiednie zabezpieczenia w zależności od użytego kanału komunikacji. Stosuje się między innymi: ochronę antywirusową, szyfrowanie wiadomości, szyfrowanie połączenia, podpis elektroniczny, zabezpieczenie kopii, zabezpieczenie dostępu do systemu, uwierzytelnianie, zabezpieczenie danych systemu, rozliczalność.

Szczegółowo zasady wymiany informacji przesyłanych przy użyciu wszystkich rodzajów środków łączności opisano w dokumencie „Polityka przesyłania informacji”, załączniku nr 2.19 do PBI CEPiK.

6.5.3. Obsługa nośników zawierających informacje

Forma papierowa (lub pokrewne)

Sposób zarządzania użytych nośników papierowych zależy od rodzaju informacji naniesionych na te nośniki i podlega wytycznym dotyczącym obsługi tych informacji, zgodnie z obowiązującymi przepisami prawa. Okres przechowywania użytych nośników (z naniesioną informacją) jest regulowany odpowiednimi przepisami prawa zgodnie z „Polityką klasyfikacji informacji CEPiK", załącznikiem nr 2.8 do PBI CEPiK. W przypadku dokumentów w postaci papierowej, do których nie mają zastosowania wyżej określone przepisy prawa przyjmuje się, że dane powinny być przechowywane w sposób odpowiednio zabezpieczony przez okres nie krótszy niż 2 lata, od momentu ustania przyczyny, dla której zostały wytworzone. Po tym okresie musi zostać niezwłocznie podjęta decyzja przez Właściciela Informacji o archiwizacji dokumentu lub jego zniszczeniu.

Forma cyfrowa

Każdy cyfrowy nośnik informacji przed przekazaniem go do eksploatacji powinien być odpowiednio zewidencjonowany (w oparciu co najmniej o numer seryjny, nazwę oraz typ) przez Interesariusza.
Przyjęto, że wszystkie rodzaje nośników umieszczonych CEPiK zawierają dane podlegające szczególnej ochronie, mającej na celu zapewnienie ich bezpieczeństwa. Nośniki cyfrowe użyte w CEPiK muszą być zabezpieczone w sposób uniemożliwiający dostęp do nich przez osoby nieupoważnione, poprzez ograniczenie dostępu fizycznego do stanowiska pracy – miejsca jego zainstalowania.
Po zakończeniu eksploatacji nośnik powinien zostać nieodwracalnie zniszczony – zlikwidowany, przy użyciu rekomendowanych urządzeń oraz oprogramowania.

Procedury postępowania z nośnikami danych wraz z wykazem rekomendowanych urządzeń i oprogramowania trwale usuwającego dane opisano w dokumencie „Polityka postępowania z nośnikami wymiennymi", załączniku nr 2.9 do PBI CEPiK.

Uwaga: Nie podlegają procedurze likwidacji nośniki stanowiące dowody w sprawie lub zabezpieczone w ramach zabezpieczania informacji, które mogą stanowić materiał dowodowy.

6.6. Zarządzanie ryzykiem

Poprzez zarządzanie ryzkiem rozumie się proces, którego zadaniem jest określenie zagrożeń w poddawanym ocenie obszarze oraz ich minimalizacja. Celem polityki zarządzania ryzykiem

bezpieczeństwa informacji jest zachowanie, co najmniej: poufności, integralności oraz dostępności informacji.

Proces zarządzania ryzykiem wiąże się ze stosowaniem określonych reguł we wszystkich obszarach i czynnościach, które mogą być zagrożone wystąpieniem określonych słabości (podatności). Działania zmierzające do obsługi danego ryzyka powinny być prowadzone cyklicznie (np. systematyczna ocena podatności systemu wraz z analizą ryzyka) jak również, jeżeli wymaga tego sytuacja - ad-hoc (np. ocena ryzyka wynikającego ze zmiany w procesie lub zmiany w oprogramowaniu).

Proces zarządzania ryzkiem powinien obejmować następujące części:

1. Identyfikacja kontekstu (otoczenia) – określenie zakresu i granic oraz kryteriów: oceny, skutków i akceptacji ryzyka.
2. Szacowanie ryzyka – identyfikacja, analiza oraz ocena ryzyka.
3. Postępowanie z ryzykiem – modyfikacja, akceptacja, unikanie oraz podzielenie ryzyka.
4. postępowanie z ryzykiem – modyfikacja, akceptacja, unikanie oraz współdzielenie ryzyka,
5. informowanie i konsultowanie ryzyka,
6. monitorowanie i przegląd ryzyka.

Przyjęto, że podczas prowadzenia procesów zarządzania ryzykiem należy stosować techniki jakościowe, oparte na wiedzy eksperckiej dające w dosyć szybkim okresie pogląd całościowy ocenianych aktywów.

Wszystkie czynniki, które mogą mieć wpływ na poziom zidentyfikowanego już ryzyka, jak również powodować nowe zagrożenia, muszą podlegać procesowi monitorowania oraz przeglądu tego obszaru. W ramach monitoringu oraz przeglądu należy zwrócić uwagę na zmiany w zakresie: środowiska (kontekstu) systemu, wykazu zidentyfikowanych aktywów, adekwatności kryteriów oceny ryzyka, przyjętych kryteriów skutków oraz prawdopodobieństwa. Uprawnieni interesariusze systemu CEPiK powinni mieć dokonane analizy ryzyka (jeżeli ma to odniesienie) w kontekście funkcjonowania systemu.

6.7. Postępowanie z incydentami bezpieczeństwa informacji

Każdy pracownik instytucji będącej interesariuszem CEPiK realizujący w nim zadania ma obowiązek dbać o bezpieczeństwo informacji w systemie zgodnie z dokumentami polityk bezpieczeństwa

informacji, oraz reagować na zdarzenia, które mogą wskazywać na wystąpienie incydentu bezpieczeństwa informacji i informować o zdiagnozowanych słabościach systemu.

Obsługa incydentów związanych z bezpieczeństwem informacji jest realizowana priorytetowo w stosunku do innych zgłoszeń, a w przypadku incydentów związanych z naruszeniem bezpieczeństwa informacji prawnie chronionych (np. dane osobowe), przepisy prawa wymagają reakcji we wskazanym okresie od wykrycia incydentu oraz informowania osób, w kompetencji których znajduje się nadzór nad przestrzeganiem przepisów dotyczących bezpieczeństwa informacji.

Zdarzenia, które wiążą się lub mogą wiązać się z naruszeniem bezpieczeństwa informacji to, m.in. naruszenie dowolnego atrybutu bezpieczeństwa systemu (m.in.: poufność, integralność, dostępność, autentyczność) w wyniku umyślnych lub nieumyślnych działań, w szczególności:

- dostęp do systemu osoby nie posiadającej upoważnienia do przetwarzania danych,
- włamanie do systemu lub jego dowolnego komponentu,
- połączenie wydzielonej infrastruktury systemu z dowolną siecią zewnętrzną bez zgody właściciela biznesowego systemu,
- nieuprawnione pozyskanie informacji,
- udostępnienie danych z systemu osobom nieuprawnionym,
- utrata aktywu/zasobu systemu (komputer przenośny, pendrive, dysk, płyta CD z danymi, telefon, dokument, itp.),
- destrukcja danych i oprogramowania systemu,
- próba sabotażu lub sabotaż systemu skutkujący niedostępnością,
- piractwo, kradzież oprogramowania systemu lub oprogramowania wspomagającego (np. licencjonowane oprogramowanie bazy danych),
- oszustwo i fałszerstwo danych systemu,
- szpiegostwo dotyczące danych zawartych w systemie oraz danych dotyczących systemu,
- ujawnienie lub podejrzenie ujawnienia osobom trzecim haseł dostępowych do dowolnych komponentów systemu,
- długotrwała niedostępność systemu lub jego dowolnego komponentu,
- wykrycie szkodliwego oprogramowania w dowolnym komponencie CEPiK.

6.7.1. Zgłaszanie incydentów

Uprawniony interesariusz CEPiK lub każdy z użytkowników systemu ma obowiązek zgłosić zdarzenia mogące wskazywać na wystąpienie incydentu w obszarze bezpieczeństwa informacji CEPiK bezpośrednio w systemie ITSM lub w przypadku braku takiej możliwości: na adres poczty elektronicznej: service_desk_cepik@coi.gov.pl lub telefonicznie na nr.: (42) 25 35 499.

W treści zgłoszenia należy przekazać następujące informacje:

1. imię i nazwisko oraz dane kontaktowe,
2. miejsce wystąpienia incydentu bezpieczeństwa (np. pomieszczenie do przetwarzania danych CEPiK w urzędzie gminy),
3. opis incydentu bezpieczeństwa zawierający informacje:
   a) na czym polega incydent i czy dotyczy bezpieczeństwa danych prawnie chronionych (danych osobowych, informacji niejawnych, tajemnicy przedsiębiorstwa),
   b) jakiego elementu systemu (aplikacji) dotyczy,
   c) dotyczące daty i godziny wystąpienia lub wykrycia incydentu,
   d) na temat wpływu incydentu na elementy systemu,
   e) czy incydent nadal trwa lub czy występuje okresowo w sposób powtarzalny,
4. wstępną ocenę realnych lub potencjalnych skutków incydentu bezpieczeństwa (oszacowanie szkód),
5. podjęte dotychczas działania.

Jeśli osoba zgłaszająca posiada dodatkowe informacje techniczne w postaci konfiguracji sprzętowej, systemu operacyjnego, adresacji sieciowej urządzeń i innych znanych jej kwestii technicznych - dane te powinny być niezwłocznie przekazane po nawiązaniu kontaktu bezpośrednio do linii wsparcia „bezpieczeństwo” w uzgodnionym bezpiecznym kanale komunikacyjnym, przy czym przekazanie danych inicjuje pracownik linii wsparcia „bezpieczeństwo”.

Pracownik Service Desk może żądać od osoby zgłaszającej incydent bezpieczeństwa informacji uzupełnienia opisu w systemie ITSM, jeśli przekazane informacje nie pozwalają na podjęcie dalszych działań.

Niezależnie, czy w toku dalszych działań zgłoszone zdarzenie zostanie sklasyfikowane jako incydent bezpieczeństwa lub inne zdarzenie - Service Desk informuje o tym osobę zgłaszającą. Osoba zgłaszająca jest również informowana za pośrednictwem systemu ITSM o rozwiązaniu incydentu.

Osoba zgłaszająca ma obowiązek ponadto:

1. poinformować o zaistniałym zdarzeniu swojego bezpośredniego przełożonego,
2. współpracować z komórką odpowiedzialną za bezpieczeństwo informacji jednostki KPRM lub podmiotu realizującego zadania na rzecz jednostki KPRM w przedmiotowym obszarze oraz w razie potrzeby realizować przekazane wytyczne i zalecenia,
3. zabezpieczyć miejsce zdarzenia, istotne dane lub urządzenia teleinformatyczne zgodnie z posiadaną wiedzą do czasu podjęcia dalszych działań przez komórki organizacyjne odpowiedzialne za bezpieczeństwo informacji. Zabezpieczenie to należy realizować m.in. poprzez:
   a) bezzwłoczne zanotowanie wszystkich istotnych szczegółów dotyczących zdarzenia,
   b) archiwizację wiadomości lub innych informacji dotyczących zdarzenia np. komunikatów z systemu antywirusowego,
   c) zabezpieczenie zrzutów ekranowych lub zdjęć obrazujących wystąpienie zdarzenia wskazującego na naruszenie bezpieczeństwa informacji,
   d) zabezpieczenie urządzenia, nośnika informacji (np.: dokument papierowy, płyta CD z danymi systemu lub dotyczącymi systemu) jak również innego dowodu wskazującego na możliwość naruszenia bezpieczeństwa informacji.

Zabrania się działań mogących spowodować utrudnienia w wyjaśnieniu przyczyn incydentu bezpieczeństwa informacji w tym niszczenia, usuwania, ukrywania, modyfikowania informacji i materiałów zawierających dane związane z przedmiotowym incydentem.

Szczegółowy opis zgłaszania incydentów bezpieczeństwa informacji znajduje się w dokumencie „Procedura zgłaszania incydentów związanych z bezpieczeństwem informacji”, załączniku nr 2.22 do PBI CEPiK.

6.7.2. Obsługa incydentów

Każde przyjęte zgłoszenia podlega klasyfikacji i zostaje wprowadzone do systemu ITSM przez Zespół Pracowników Service Desk. W przypadku kiedy zgłoszenie jest traktowane jako incydent bezpieczeństwa informacji, zostaje ono niezwłocznie przekazane do wyznaczonych uprawnionych pracowników osób odpowiedzialnych za bezpieczeństwo informacji u Interesariusza.

Pracownik Service Desk przekazuje za pośrednictwem systemu ITSM wstępnie skategoryzowane zgłoszenie dotyczące bezpieczeństwa informacji do właściwej linii wsparcia „bezpieczeństwo” lub

„utrzymanie” będącej w strukturach komórki organizacyjnej odpowiedzialnej za bezpieczeństwo informacji podmiotu realizującego zadania z zakresu eksploatacji i utrzymania systemu na rzecz urzędu obsługującego ministra właściwego ds. informatyzacji. Następnie żąda niezwłocznego potwierdzenia, że zgłoszenie dotyczy incydentu bezpieczeństwa informacji w wybranej kategorii.

Pracownik właściwej linii wsparcia potwierdza lub zaprzecza, że zgłoszenie dotyczy incydentu w obszarze bezpieczeństwa informacji. W przypadku, gdy zgłoszenie nie dotyczy incydentu bezpieczeństwa wskazuje właściwą linię wsparcia, w której kompetencji znajduje się rozwiązanie przedmiotowego zgłoszenia i zwraca je do Service Desk.

O zagrożeniach w obszarze cyberprzestrzeni niezwłocznie informuje CERT wypełniając formularz dla zgłaszających incydent (dostępny na stronie www.incydent.cert.pl) i wysyłając e-maila na adres: cert@cert.pl

Ponadto jeśli w wyniku incydentu doszło lub mogło dojść do naruszenia bezpieczeństwa informacji prawnie chronionych o incydencie są informowane właściwe organy ścigania. Za informowanie organów ścigania odpowiedzialny jest kierownik komórki organizacyjnej w urzędzie obsługującym ministra ds. informatyzacji, w którego kompetencji znajduje się eksploatacja i utrzymanie CEPiK.

Za dokumentowanie incydentów bezpieczeństwa informacji odpowiedzialni są pracownicy linii wsparcia „bezpieczeństwo” w strukturach podmiotu realizującego zadania z zakresu eksploatacji i utrzymania systemu na rzecz jednostki KPRM, którzy wprowadzają dane oddzielnie do:

1. rejestru incydentów związanych z bezpieczeństwem informacji w CEPiK,
2. rejestru wykrytych podatności w CEPiK.

Szczegółowe zasady dotyczące reakcji na incydenty bezpieczeństwa informacji opisane są w dokumencie „Procedura reakcji na incydenty związane z bezpieczeństwem informacji”, załączniku nr 2.23 do PBI CEPiK. Sposób zabezpieczania materiału dowodowego opisany jest w dokumencie „Procedura przetwarzania informacji, które mogą stanowić materiał dowodowy CEPiK”, załączniku nr 2.24 do PBI CEPiK.

6.8. Nadzorowanie odstępstw, niezgodności i działań korygujących

Minister właściwy ds. informatyzacji, umocowany przez niego Gestor systemu lub inny pracownik obsługujący urząd właściwy do obsługi ministra właściwego ds. informatyzacji odpowiedzialny jest za akceptację odstępstwa.

Osoby (role) wnioskujące o odstępstwa zobowiązane są do podjęcia odpowiednich działań w formie pisemnej, określenia celu, powodu i propozycji postępowania alternatywnego w ramach odstępstwa oraz określenie jego wpływu na bezpieczeństwo informacji oraz system. Gestor systemu nadzoruje procesowanie odstępstw, niezgodności i działań korygujących, a także zapewnia podejmowanie skutecznych działań korygujących.

Zapewnienie właściwego nadzorowania i procesowania odstępstw, niezgodności i działań korygujących jest kluczowe dla zapewnienia wysokiego poziomu bezpieczeństwa systemu poprzez zapobieganie wykonywania nieuzasadnionych zmian technicznych bądź architektonicznych w systemie oraz wprowadzanie możliwych rozwiązań korygujących eliminujących przyczyny niezgodności w celu zapobiegania ich powtórnego występowania.

Wszelkie informacje dotyczące odstępstw, niezgodności i działań korygujących podlegają udokumentowaniu.

6.9. Monitoring i nadzór

Przegląd zarządzania

Ocena skuteczności wdrożonych zasad zapewniających bezpieczeństwo informacji jest kluczowym elementem systemu zarządzania bezpieczeństwem informacji. Ocena powinna być dokonywana cyklicznie, podczas przeglądu zarządzania gdzie analizowane są takie elementy jak: wyniki audytów systemu, skuteczność zastosowanych zabezpieczeń, zarządzanie incydentami bezpieczeństwa, realizację celów bezpieczeństwa informacji, działania korygujących.

Audyt wewnętrzny

Audyt wewnętrzny służy potwierdzeniu zgodności systemu CEPiK z wymaganiami dotyczącymi bezpieczeństwa informacji, zarówno w kontekście przepisów prawa stanowionego jak i innych regulacji normatywnych czy wewnętrznych. Jest mechanizmem niezależnej oceny,

weryfikującym poziom świadomości i kompetencji użytkowników. Audyt wewnętrzny jest procesem systematycznym - cyklicznie powtarzalnym, który powinien być przeprowadzony co najmniej 1 raz do roku.