KANCELARIA PREZESA
RADY MINISTRÓW

Polityka Bezpieczeństwa Informacji CEPiK

Wytyczne dla stacji roboczych obsługi CEPiK

Załącznik nr 2.3 do Polityki Bezpieczeństwa Informacji CEPiK

KANCELARIA PREZESA
RADY MINISTRÓW

Metryka dokumentu

Właściciel	Minister właściwy ds. informatyzacji			
Tryb zatwierdzenia				
Stan	Uzgodniony	Daty obowiązywania		
Założenia	Dokument stanowi załącznik do Polityki Bezpieczeństwa Informacji CEPiK			
Adresaci	Interesariusze wewnętrzni i zewnętrzni 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 opracowania jest określenie wymagań, dopuszczalnych warunków oraz zasad bezpieczeństwa informacji przetwarzanych na stacjach roboczych w lokalizacjach interesariuszy łączących się z systemem CEPiK. Dokument został opracowana zgodnie z wytycznymi normy ISO/IEC 27001.

2. Odpowiedzialność

Odpowiedzialność została rozdzielona pomiędzy role odpowiadające za realizację określonych w polityce zadań zgodnie z załącznikiem do dokumentu Polityka Bezpieczeństwa Informacji CEPiK nr 1.4 „Wykaz ról i odpowiedzialności CEPiK".

3. Terminy i definicje

Terminologia zdefiniowana jest w „Słowniku pojęć CEPiK" załączniku nr 1.3 do PBI CEPiK.

4. Powiązania

Dokument nadrzędny:

1. Polityka Bezpieczeństwa Informacji CEPIK.

Dokumenty powiązane stanowiące załączniki do dokumentu nadrzędnego:

1. Słownik pojęć CEPIK (załącznik nr 1.3 do PBI CEPiK),
2. Wykaz ról i odpowiedzialności CEPIK (załącznik nr 1.4 do PBI CEPiK),
3. Polityka korzystania z sieci i usług sieciowych CEPIK (załącznik nr 2.18 do PBI CEPiK),
4. Procedura zgłaszania incydentów związanych z bezpieczeństwem informacji CEPIK (załącznik 2.22 do PBI CEPiK).

5. Realizacja

5.1. Podstawowe wymagania dotyczące podłączania infrastruktury interesariuszy do systemu CEPIK

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.

5.2. Wytyczne dotyczące ochrony fizycznej pomieszczeń oraz urządzeń, w których zlokalizowane są stacje robocze

Interesariusze systemu CEPiK mają obowiązek zapewnić poziom ochrony fizycznej pomieszczeń, w których są zlokalizowane stacje robocze przeznaczone do przetwarzania informacji w systemie. Poziom ten jest zgodny z aktualnymi przepisami dotyczącymi ochrony danych osobowych uwzględniając rozwiązania zapewniające ochronę odpowiednią do zagrożeń. Zaleca się stosowanie

rozwiązań organizacyjnych oraz technicznych - systemowych i kompleksowych np.: zgodnych z normą PN ISO/IEC 27001 ze szczególnym uwzględnieniem zabezpieczenia fizycznego:

a) Pomieszczeń i ich lokalizacji.
b) Drzwi i okien.
c) Urządzeń technicznych w tym stacji roboczych.
d) Informatycznych nośników danych.

5.3. Wytyczne dotyczące konfiguracji urządzeń sieciowych służących do nawiązywania komunikacji za pomocą sieci dedykowanej

1. Użytkownicy łączący się z systemem CEPiK poprzez sieci dedykowane powinni stosować się do wymagań i zaleceń określonych dla konkretnej sieci dedykowanej.
2. Urządzenia sieciowe (takie jak routery oraz przełączniki sieciowe) pozwalające na dostęp do sieci dedykowanej powinny być zabezpieczone przed nieuprawnionym dostępem osób trzecich.
3. Administracja zdalna powinna być odpowiednio zabezpieczona przed nieuprawnionym dostępem za pomocą mechanizmów uwierzytelnienia routera (np. login i hasło o odpowiedniej złożoności) i uruchomiona wyłącznie na jednym porcie wewnętrznym, do którego ma dostęp wyłącznie administrator danego urządzenia.
4. Powinna być wdrożona reglamentacja dostępu do sieci np. na podstawie adresów MAC.

5.4. Wytyczne dotyczące konfiguracji urządzeń sieciowych służących do nawiązywania połączeń VPN przez sieć publiczną

1. Użytkownicy łączący się z systemem CEPiK poprzez sieć publiczną, aby uzyskać dostęp do systemu CEPiK, muszą zestawić bezpieczne połączenie VPN z wykorzystaniem certyfikatu.
2. Urządzenia sieciowe (takie jak routery) pozwalające na zestawienie połączeń VPN powinny być zabezpieczone przed nieuprawnionym dostępem osób trzecich.
3. Urządzenie powinno być zabezpieczone w sposób uniemożliwiający osobom nieuprawnionym pozyskanie kluczy prywatnych do certyfikatu VPN, zainstalowanych w urządzeniu.
4. Administracja zdalna powinna być odpowiednio zabezpieczona przed nieuprawnionym dostępem za pomocą mechanizmów uwierzytelnienia routera (np. login i hasło o odpowiedniej

złożoności) i uruchomiona wyłącznie na jednym porcie wewnętrznym, do którego ma dostęp wyłącznie administrator danego urządzenia.

5. Powinna być wdrożona reglamentacja dostępu do sieci np. na podstawie adresów MAC.
6. Powinna być wdrożona polityka blokowania dostępu do i z sieci publicznej w czasie, w którym jest nawiązane połączenie VPN z wykorzystaniem sieci Internet.
7. Oprogramowanie służące do zestawiania połączeń VPN (typu Remote Access) powinno być zabezpieczone w taki sposób, aby uniemożliwić dostęp do kluczy prywatnych osobom nieuprawnionym oraz powinno wymuszać blokowanie dostępu do i z sieci publicznej do danej stacji komputerowej w czasie, w którym jest nawiązane połączenie VPN z wykorzystaniem sieci Internet (jest to wymuszone przez konfigurację urządzeń po stronie systemu CEPiK).

5.5. Wymagania dotyczące łącza dostępowego

Łącze dostępowe (symetryczne lub asymetryczne) niezależnie czy realizowane jest poprzez sieć dedykowaną, czy publiczną powinno mieć minimalną przepustowość dwukierunkową 512 kb/s dla stacji roboczej i umożliwiać nawiązywanie połączeń z serwerem ozz.CEPiK.gov.pl poprzez porty 443 i 444.

5.6. Wytyczne dotyczące konfiguracji stacji roboczych

Ustawienia BIOS:

1. Zmiana ustawień BIOS wymaga podania hasła.
2. Wyłączona jest możliwość uruchamiania systemu z sieci lub innych nośników niż dysk twardy komputera.
3. Dostęp do BIOS powinien być zabezpieczony hasłem składającym się z minimum 8 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny).

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.

Zapora sieciowa:

1. Wymagane jest zastosowanie zapory ogniowej (sprzętowe lub programowe rozwiązanie) oraz wdrożenie regulacji zapewniających jej bieżącą aktualizację.

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.

Kopie zapasowe:

1. Zalecane jest wdrożenie procedur tworzenia kopii zapasowych zapewniających wykonywanie kopii nie rzadziej niż raz na 7 dni.
2. Składowanie kopi zapasowych powinno odbywać się w innym budynku bądź pomieszczeniu w odpowiednio zabezpieczonej szafie.

Zasilanie awaryjne:

1. Stacje robocze powinny być dołączone do sieci energetycznej z wykorzystaniem urządzeń podtrzymujących zasilanie i umożliwiających bezpieczne zakończenie pracy w przypadku utraty zasilania podstawowego.

5.7. Wytyczne dotyczące środowisk wirtualnych udostępniających wirtualne stacje robocze

1. Zabezpieczenia serwerów udostępniających środowiska wirtualne oraz zabezpieczenia systemu udostępnianego z wykorzystaniem środowiska wirtualnego powinny być na poziomie nie mniejszym niż opisany w rozdziale 5.5.
2. Uprawnienia do katalogu oraz dostęp do folderu udostępnianego powinny zostać ograniczone tylko do użytkowników stacji wirtualnej.
3. Uprawnienia do katalogu oraz dostęp do folderu udostępnianego powinien uniemożliwiać skopiowanie pliku maszyny przez osobę inną niż administrator.
4. Stosowanie stacji wirtualnych na przenośnych informatycznych nośnikach danych nie jest zalecane. W przypadku konieczności stosowania rozwiązania zaleca się, aby nośnik plików stacji wirtualnej był w całości zaszyfrowany oraz należy wdrożyć regulacje zapewniające prawidłowe posługiwanie się nośnikami, prowadzić ewidencję przenośnych informatycznych nośników danych. Ponadto nośniki nie powinny być wynoszone poza obszar przetwarzania danych osobowych lub jeśli zachodzi taka konieczność muszą być wyposażone w rozwiązanie umożliwiające szyfrowanie danych z użyciem hasła dostępowego nie krótszego niż 10 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny) uniemożliwiające skorzystanie z danych po max 3 próbach nieudanego podania hasła do odblokowania nośnika.

5.8. Wytyczne dotyczące stosowania urządzeń przenośnych (laptop, tablet, itp.) jako stacji roboczych

1. Zabezpieczenia oraz konfiguracja mechanizmów bezpieczeństwa i systemu na poziomie nie mniejszym niż w rozdziale 5.5.
2. Stacje przenośną w miejscach korzystania należy zabezpieczyć linką antykradzieżową przymocowaną do stałego elementu wyposażenia (o ile jest to możliwe).

3. Stan baterii stacji przenośnej musi umożliwiać bezpieczne zamknięcie systemu po zaniku zasilania sieciowego.
4. Partycja lub dysk stacji przenośnej na której są składowane dane powinien być w całości zaszyfrowany przy wykorzystaniu sprzętowego modułu szyfrowania lub programowo, przy użyciu minimum algorytmu AES256.

5.9. Podstawowe wymagania sprzętowe dla stacji roboczych

Konfiguracja sprzętowa stacji roboczej powinna uwzględniać wymagania systemu operacyjnego.
Minimalna konfiguracja potrzebna do uruchomienia aplikacji CEPiK dla systemu Windows:

1. dostęp do sieci dedykowanej lub sieci publicznej,
2. procesor min. 1GHz,
3. Pamięć RAM: 1 GB (32-bit) lub 2 GB (64-bit)
4. dysk twardy HDD/SSD z min. 50GB wolnego miejsca (32-/64-bit),
5. min. 1 wolny port USB,
6. Karta graficzna: obsługująca DirectX 9.0
7. Wyświetlacz: o rozdzielczości 800 x 600 pikseli.

5.10. Wymagania dla czytników kart oraz kart kryptograficznych

1. Czytnik posiadający certyfikacje: ISO 7816 T=0, T=1, CAC i EM, I2C/Extended I2C kart z wolnym dostępem do pamięci i 2/3.
2. Zakres pamięci EEPROM od 32 kB.
3. Układ procesorowy i maszyna wirtualna Java muszą posiadać certyfikat FIPS 140-2 level 3, zaś cała karta musi posiadać certyfikat CC (Common Criteria) EAL-4.
4. Interfejs stykowy - zgodny z ISO/IEC 7816 T=0/T=1.
5. Sprzętowe generowanie kluczy RSA o długości 2048 bitów.
6. Realizacja na karcie SHA-1, SHA-2.
7. Obsługa systemów operacyjnych z rodziny Windows 32/64bit aktualnie wspieranych przez producenta.
8. Wsparcie certyfikatów zgodnie z X.509 v.3.
9. Biblioteka PKCS#11 zgodna z wersją standardu 2.10, 2.11.

10. Oprogramowanie umożliwiające odczyt zawartości karty, wygenerowanie/skasowanie kluczy RSA, odczytanie/usunięcie/zapisanie certyfikatów kluczy, odczytanie/usunięcie dowolnych obiektów prywatnych PKCS#11 (zależnych od aplikacji), ustanawianie kluczy domyślnych dla CSP, skasowanie karty; zmianę PINU i/lub PINu administratora oraz na odblokowanie karty przy pomocy PIN-u administratora.
11. Karta spersonalizowana (zainicjowana), z min. jednym tokenem, zabezpieczona kodem PIN (4 cyfry) oraz kodem PIN administratora (8 cyfr).

5.11. Wymagania dotyczące oprogramowania instalowanego na stacjach roboczych

Lp.	Rodzaj	Implementacja	Uwagi
1	System operacyjny	Microsoft Windows ze wsparciem producenta	Zastosowany system operacyjny musi wspierać sterowniki urządzeń peryferyjnych niezbędnych do pracy. Data i godzina systemowa musi być zgodna z rzeczywistą.
2	JAVA	Java SE 8 Runtime Environment (JRE) Update 40 lub wersja nowsza	Niezbędna do uruchamiania appletów w przeglądarce internetowej.
3	Oprogramowanie antywirusowe	Zapewniające skanowanie w czasie rzeczywistym	Oprogramowanie powinno posiadać aktualne definicje i bazy antywirusowe.
4	Czytnik PDF	Acrobat Reader lub inny.	W wersji aktualnej.
5	Przeglądarka Internetowa	Mozilla Firefox (>= 4.0) Internet Explorer (>= 11.0) Google Chrome (>= 70) Microsoft Edge	Należy stosować aktualne wersje przeglądarek zawierające wszystkie poprawki bezpieczeństwa udostępnione przez producenta. Stacja robocza musi mieć zainstalowane dodatki umożliwiające uruchamianie

			apletów języka Java, dla wszystkich wykorzystywanych typów przeglądarek.
6	Sterowniki urządzeń peryferyjnych	Oprogramowanie niezbędne do obsługi, kart, czytników kart kryptograficznych i drukarek	Sterowniki do obsługi kart powinny być zainstalowane zarówno w systemie jak i przeglądarce internetowej (dot. m.in. Mozilla Firefox). Przed zainstalowaniem sterowników, należy upewnić się, że przeglądarki są już zainstalowane.

5.12. Wytyczne dotyczące zasad „czystego biurka" oraz „czystego ekranu"

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.

5.13. Zgłaszanie zdarzeń wskazujących na naruszenie 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 jak również informować o zdiagnozowanych słabościach systemu.

Szybka reakcja stanowi podstawowy element skutecznego ograniczenia następstw takich zdarzeń, dlatego nie należy zwlekać z podejmowaniem działań niezależnie od okoliczności. 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 których kompetencji znajduje się nadzór nad przestrzeganiem przepisów dotyczących bezpieczeństwa informacji (Administrator Bezpieczeństwa ds. obszaru CEPiK, IOD w zakresie danych osobowych, ADO).

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:

1. Dostęp do systemu osoby nie posiadającej upoważnienia do przetwarzania danych;
2. Włamanie do systemu lub jego dowolnego komponentu,
3. Połączenie wydzielonej infrastruktury systemu z dowolną siecią zewnętrzną bez zgody właściciela biznesowego systemu,

4. Nieuprawnione pozyskanie informacji,
5. Udostępnienie danych z systemu osobom nieuprawnionym,
6. Utrata aktywu/zasobu systemu (komputer stacjonarny/przenośny, pendrive, dysk, płyta CD/DVD z danymi, dokument, itp.)
7. Destrukcja danych i oprogramowania systemu,
8. Próba sabotażu lub sabotaż systemu skutkujący niedostępnością,
9. Piractwo, kradzież oprogramowania systemu lub oprogramowania wspomagającego,
10. Oszustwo i fałszerstwo danych systemu,
11. Szpiegostwo dotyczące danych zawartych w systemie oraz danych dotyczących systemu,
12. Ujawnienie lub podejrzenie ujawnienia osobom trzecim haseł dostępowych do dowolnych komponentów systemu,
13. Długotrwała niedostępność systemu lub jego dowolnego komponentu,
14. Wykrycie szkodliwego oprogramowania w dowolnym komponencie systemu, np.:
    - wirusy komputerowe,
    - makrowirusy,
    - robaki,
    - konie trojańskie,
    - bomby logiczne,
    - rootkity,
    - programy szpiegujące,
    - programy reklamowe,
    - keyloggery.

Proces obsługi zdarzeń związanych z bezpieczeństwem informacji realizowany jest zgodnie z odpowiednimi procedurami, stanowiącymi załączniki do PBI CEPiK, a samą czynność zgłaszania reguluje „Procedura zgłaszania incydentów związanych z bezpieczeństwem informacji CEPiK", (załącznik nr 2.22. do PBI CEPiK).