Warszawa, dnia 11 września 2017 r.

Poz. 69

DECYZJA NR 46
MINISTRA SPORTU I TURYSTYKI[1)]

z dnia 11 września 2017 r.

w sprawie wprowadzenia „Polityki Bezpieczeństwa Informacji Ministerstwa Sportu i Turystyki”

Na podstawie art. 36 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922) oraz § 20 rozporządzenia 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 2016 r. poz. 113 i 1744) zarządza się, co następuje:

§ 1. Wprowadza się „Politykę Bezpieczeństwa Informacji Ministerstwa Sportu i Turystyki”, stanowiącą załącznik do decyzji.

§ 2. Decyzja wchodzi w życie z dniem 15 września 2017 r.

Minister Sportu i Turystyki

Witold Bańka

[1)] Minister Sportu i Turystyki kieruje działami administracji rządowej – kultura fizyczna oraz turystyka, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 17 listopada 2015 r. w sprawie szczegółowego zakresu działania Ministra Sportu i Turystyki (Dz. U. poz. 1911).

Załącznik
do Decyzji nr ……..
Ministra Sportu i Turystyki
z dnia ……

Polityka Bezpieczeństwa Informacji Ministerstwa Sportu i Turystyki

Wprowadzenie

Ministerstwo Sportu i Turystyki, zwane dalej „Ministerstwem", realizując zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali System Zarządzania Bezpieczeństwem Informacji, zapewniający: poufność, dostępność i integralność informacji.
Na dokumentację Systemu Zarządzania Bezpieczeństwem Informacji składa się Polityka Bezpieczeństwa Informacji oraz szereg innych regulacji wewnętrznych: polityk, instrukcji, wytycznych, regulaminów i procedur ustanowionych w urzędzie.
Kierownictwo Ministerstwa, rozumiejąc konieczność zapewnienia odpowiedniego poziomu ochrony informacji w realizowanych zadaniach, a także spełnienia wymagań prawnych w odniesieniu do ochrony informacji, ustanawia Politykę Bezpieczeństwa Informacji zgodną z 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. Kierownictwo Ministerstwa deklaruje pełne wsparcie dla podejmowanych działań w zakresie bezpieczeństwa oraz zapewnienie niezbędnych zasobów i czasu na ich realizację.

1. Cel

Celem Polityki Bezpieczeństwa Informacji jest określenie zasad stosowanych w Ministerstwie w celu zapewnienia odpowiedniego zabezpieczenia przetwarzanych przez Ministerstwo Sportu i Turystyki informacji, z zachowaniem ich poufności, dostępności i integralności. Powyższy cel osiągany jest poprzez:

- określenie przez Ministerstwo kierunków rozwoju zarządzania bezpieczeństwem;
- określenie ról w systemie zarządzania bezpieczeństwem informacji i przypisanie im obowiązków i uprawnień w tym zakresie;
- zapewnienie odpowiedniego zaangażowania pracowników w utrzymanie bezpieczeństwa systemów informacyjnych;
- spełnienie wszelkich wymogów obowiązującego prawa odnośnie ochrony informacji przetwarzanych w Ministerstwie;
- przeprowadzania analizy ryzyka i wdrażania zabezpieczeń adekwatnych do ich wyników;
- ciągłe doskonalenie wdrożonej Polityki Bezpieczeństwa Informacji.

Polityka Bezpieczeństwa Informacji jest zbiorem zasad, które obowiązane są stosować wszystkie osoby posiadające dostęp do zasobów informacyjnych. Określa również zasady ochrony infrastruktury, zasobów informatycznych i ludzkich. Niniejszy dokument dotyczy wszystkich pracowników w rozumieniu w szczególności ustawy o służbie cywilnej oraz przepisów Kodeksu Pracy, a także innych osób mających dostęp do informacji chronionych Ministerstwa (np. pracowników firm zewnętrznych wykonujących określone prace).

2. Słownik pojęć

Określenia użyte w Polityce Bezpieczeństwa Informacji oznaczają:

Aktywa – wszystko co ma wartość dla instytucji (zasoby ludzkie, finansowe, informacyjne, organizacyjne, technologiczne i fizyczne);

Bezpieczeństwo Informacji – zachowanie poufności, integralności i dostępności; dodatkowo,

mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność, które można osiągnąć wdrażając odpowiedni zestaw zabezpieczeń (polityki, procesy, procedury, struktury organizacyjne, funkcje oprogramowania, sprzętu, itp.);

Dane – element informacji, który może być przetwarzany (rejestrowany, modyfikowany, przechowywany, itp.) w systemie informatycznym w postaci elektronicznej (np.: pliki, wiadomości pocztowe, itp.) lub może przybierać postać papierową (wydruki);

Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej; możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności poprzez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne;

Dostępność – zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów, na każde uzasadnione żądanie w ustalonym czasie;

Incydent Bezpieczeństwa – pojedyncze zdarzenie lub seria niepożądanych, niespodziewanych zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia funkcjonowania instytucji, zagrażają bezpieczeństwu informacji lub stanowią naruszenie obowiązujących zasad bezpieczeństwa;

Informacja – wszystko, co posiada logiczne znaczenie jako przekaz treści i może być praktycznie wykorzystane, skutkując osiągnięciem celu;

Integralność – właściwość polegająca na tym, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony;

Minister – Minister Sportu i Turystyki;

Poufność – właściwość zapewniająca, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom fizycznym;

Przetwarzanie Informacji – jakiekolwiek operacje wykonywane na informacji, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie;

Ryzyko – wpływ zagrożeń na cele; potencjalna sytuacja, w której określone zagrożenie wykorzystując podatność aktywów lub grupy aktywów powoduje szkodę dla instytucji;

Strony trzecie – pracownicy przedsiębiorców świadczący usługi dla Ministerstwa, dostawcy, praktykanci, wolontariusze, stażyści, osoby wykonujące czynności na podstawie umów cywilnoprawnych;

System teleinformatyczny (system informatyczny) – zestaw urządzeń (w tym komputerów), programów i narzędzi programowych oraz metod postępowania i procedur, stosowanych w celu przetwarzania danych;

System Zabezpieczeń – zestaw zabezpieczeń stosowanych w określonym obszarze, w tym Techniczne Systemy Zabezpieczeń oraz niektóre części systemu informatycznego, dedykowane do nadzoru nad bezpieczeństwem obszaru, np. systemy PPOŻ, alarmowe, monitoring, systemy kontroli dostępu, systemy ochrony przyłącza internetowego, system antywirusowy;

System Zarządzania Bezpieczeństwem Informacji – część systemu zarządzania organizacją, oparta na podejściu wynikającym z ryzyka, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji. System zarządzania zawiera strukturę organizacyjną, polityki, planowane działania, zakresy odpowiedzialności, zasady, procedury, procesy i zasoby;

Użytkownik systemu – należy przez to rozumieć osobę upoważnioną do przetwarzania danych w Ministerstwie. Użytkownikiem może być pracownik Ministerstwa, osoba wykonująca czynności na podstawie umowy cywilnoprawnej, praktykant, wolontariusz lub stażysta;

Właściciel Aktywów – jednostka, komórka organizacyjna lub osoba, która ma zatwierdzoną kierowniczą odpowiedzialność za określone Aktywa;

Zabezpieczenie – środki służące zarządzaniu ryzykiem, łącznie z politykami, procedurami, zaleceniami, praktyką lub strukturami organizacyjnymi, które mogą mieć naturę administracyjną, techniczną, zarządczą lub prawną;

Zarządzanie Ryzykiem – stały, powtarzalny proces, w ramach którego podejmowane są różne

przedsięwzięcia w celu ograniczenia prawdopodobieństwa wystąpienia ryzyka i ewentualnych jego skutków.

3. Struktura dokumentacji Systemu Zarządzania Bezpieczeństwa Informacji

Na dokumentację w zakresie Systemu Zarządzania Bezpieczeństwem Informacji w Ministerstwie składają się: Polityka Bezpieczeństwa Informacji oraz inne dokumenty (polityki, instrukcje, procedury, regulaminy, szablony umów) określające zasady i sposób zarządzania bezpieczeństwem aktywów informacyjnych i zasobów materialnych Ministerstwa. Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji ma strukturę hierarchiczną. Poszczególne poziomy dokumentacji opisują system zarządzania bezpieczeństwem informacji na różnych poziomach szczegółowości.

4. Obowiązki i uprawnienia w Systemie Zarządzania Bezpieczeństwem Informacji

Zespół SZBI

W Ministerstwie działa Zespół do spraw Systemu Zarządzania Bezpieczeństwem Informacji w Ministerstwie Sportu i Turystyki, jako organ pomocniczy Ministra, zwany dalej „Zespołem”.

Do zadań Zespołu należy w szczególności:

1) opracowanie, monitorowanie, aktualizowanie i doskonalenie Polityki Bezpieczeństwa Informacji;
2) analiza incydentów naruszenia bezpieczeństwa informacji i określanie działań korygujących;
3) doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji;
4) koordynacja realizacji zaleceń poaudytowych, przedstawionych po realizacji audytu Systemu Zarządzania Bezpieczeństwem Informacji.

Kierownictwo Ministerstwa

Kierownictwo Ministerstwa jest odpowiedzialne za procesy zabezpieczania informacji, a w szczególności za:

1) definiowanie potrzeb w zakresie poprawy ochrony informacji i bezpieczeństwa systemów przetwarzających dane w organizacji;
2) akceptację lub wyrażenie potrzeby obniżenia poziomu ryzyka związanego z przetwarzaniem informacji;
3) zapewnienie wsparcia organizacyjno-finansowego przy wdrażaniu mechanizmów zabezpieczenia informacji i systemów informatycznych;
4) zatwierdzanie dokumentów związanych z ochroną informacji;
5) przestrzeganie wymagań związanych z zabezpieczeniem informacji i systemów informatycznych.

Dyrektorzy komórek organizacyjnych

1. Dyrektorzy komórek organizacyjnych są odpowiedzialni za prawidłowy przebieg zadań zapewniający bezpieczeństwo informacji, w tym w szczególności:

1) określanie znaczenia informacji dla realizacji zadań w komórkach organizacyjnych;
2) akceptowanie ryzyka związanego z przetwarzaniem informacji w systemie informatycznym w podległych komórkach organizacyjnych lub określenie konieczności jego obniżenia;
3) proponowanie sposobu realizacji mechanizmów ochrony informacji z uwzględnieniem specyfiki pracy danej komórki organizacyjnej;

4) określanie uprawnień podległych sobie pracowników w zakresie dostępu do informacji przetwarzanych w systemach informatycznych i usług udostępnianych przez te systemy;
5) informowanie administratorów systemów informatycznych o konieczności odebrania uprawnień pracownikom, z którymi rozwiązano umowę o pracę;
6) delegowanie pracowników na szkolenia w zakresie bezpieczeństwa informacji i systemów informatycznych;
7) zapewnianie podstawowego szkolenia w zakresie korzystania z systemów informatycznych dla nowo przyjętych pracowników;
8) zapewnianie pracownikom specjalistycznych szkoleń związanych z obsługą rozwiązań informatycznych funkcjonujących w ramach danej komórki organizacyjnej;
9) aktywny udział w procesie reagowania na incydenty w zakresie bezpieczeństwa systemu informatycznego i wyciąganie konsekwencji dyscyplinarnych wobec podległych sobie pracowników zamieszanych w tego typu incydenty.

Pracownicy Ministerstwa

Pracownicy są zobowiązani do:
1) przestrzegania zasad bezpieczeństwa informacji i systemów informatycznych;
2) aktywnego udziału w szkoleniach dotyczących bezpieczeństwa informacji i systemów informatycznych;
3) informowania o incydentach w zakresie bezpieczeństwa informacji oraz systemów informatycznych;
4) aktywnego udziału we wdrażaniu mechanizmów bezpieczeństwa poprzez ocenę ich skuteczności na swoim stanowisku pracy;
5) ochrony danych zgodnie z określonymi zasadami poufności.

Inni użytkownicy systemu informatycznego

1. Strony trzecie korzystające z systemu informatycznego Ministerstwa zobowiązane są przestrzegać obowiązujących zasad ochrony informacji.

2. Szczegółowe zasady przestrzegania przez strony trzecie zasad ochrony informacji określa umowa o współpracy. Ponadto w przypadku konieczności dostępu współpracownika do informacji niebędących powszechnie dostępnymi może okazać się konieczne podpisanie oddzielnej umowy o poufności.

Pełnomocnik SZBI

1. Pełnomocnikiem SZBI jest wyznaczona w Ministerstwie osoba odpowiedzialna za stworzenie, wdrożenie i nadzorowanie standardów zabezpieczenia informacji przetwarzanych w Ministerstwie.
2. Pełnomocnika SZBI powołuje Minister.
3. Do obowiązków Pełnomocnika SZBI należą:
1) koordynacja procesu analizy ryzyka związanego z przetwarzaniem informacji w systemach informatycznych;
2) ocena ryzyka z uwzględnieniem informacji otrzymanych od właścicieli informacji;
3) opiniowanie zmian w systemach informatycznych pod kątem ich wpływu na bezpieczeństwo przetwarzanych informacji;
4) koordynacja działań związanych z uświadamianiem pracownikom znaczenia ochrony informacji;
5) uwzględnienie prawnych aspektów ochrony informacji w zabezpieczeniu systemów informatycznych;
6) reprezentowanie Kierownictwa w istotnych sprawach związanych z SZBI wewnątrz i na zewnątrz Ministerstwa;
7) dbałość o prawidłowe funkcjonowanie, aktualność i adekwatność SZBI.

Administrator Systemu Informatycznego

1. Administrator Systemu Informatycznego jest osobą odpowiedzialną za zapewnienie prawidłowego funkcjonowania systemów informatycznych.
2. Administratora Systemu Informatycznego powołuje Minister.
3. Do obowiązków Administratora Systemu Informatycznego w zakresie bezpieczeństwa informacji należą:
1) implementacja mechanizmów bezpieczeństwa w administrowanej infrastrukturze informatycznej;
2) nadawanie uprawnień użytkownikom systemu informatycznego zgodnie z wnioskami ich przełożonych;
3) zapewnienie pomocy użytkownikom przy korzystaniu z systemu informatycznego;
4) tworzenie kopii zapasowych informacji przechowywanych w systemach informatycznych;
5) instalacja i uaktualnianie oprogramowania oraz zarządzanie licencjami;
6) monitorowanie działania systemu informatycznego i przekazywanie informacji o zagrożeniach administratorowi bezpieczeństwa informacji;
7) aktywny udział w procesie reagowania na incydenty w zakresie bezpieczeństwa oraz w usuwaniu ich skutków.

Audytor wewnętrzny

Audytor wewnętrzny bierze udział w procesie bezpieczeństwa informacji poprzez ocenę zgodności przebiegu procesów zachodzących w urzędzie zgodnie z obowiązującymi wytycznymi, standardami, normami bezpieczeństwa informacji w zakresie określonym w ustawie z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2016 r. poz. 1870, 1948, 1984, 2260 oraz z 2017 r. poz. 191). W tym zakresie Audytor Wewnętrzny odpowiada za:
1) przeprowadzanie audytów wewnętrznych SZBI;
2) opracowanie raportów z przeprowadzanych audytów i przedstawienie ich Kierownictwu.

5. Proces zarządzania ryzykiem

Zarządzanie ryzykiem odnosi się do aktywów organizacji. Aktywa są zidentyfikowane i poddane kontroli ich użycia a następnie poddane analizie, jakim zagrożeniom podlegają oraz jakie to niesie ze sobą skutki. Na tej podstawie, w oparciu o istniejącą Metodykę szacowania ryzyka szacowane jest ryzyko, a następnie podejmowane decyzje mające na celu obniżenie ryzyka do poziomu akceptowalnego.

6. Zabezpieczenia

Ministerstwo powinno dobierać cele stosowania zabezpieczeń i zabezpieczenia adekwatne do wymagań prawnych i wyników analizy ryzyka dla bezpieczeństwa informacji. Zabezpieczenia fizyczne, techniczne i organizacyjne powinny uzupełniać się wzajemnie zapewniając wspólnie wymagany poziom bezpieczeństwa informacji. W doborze celów stosowania zabezpieczeń i zabezpieczeń należy kierować się zaleceniami Polskiej Normy PN-ISO/IEC 17799.

W Ministerstwie wydzielono następujące obszary zarządzania:

1. Obszar bezpieczeństwa informacji – obejmuje zasady związane z bezpieczeństwem informacji, w tym:

1) zasady postępowania z informacjami, zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
2) zasady zawierania w umowach ze stronami trzecimi postanowień gwarantujących odpowiedni poziom bezpieczeństwa informacji;
3) zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
4) podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji.

2. Obszar bezpieczeństwa teleinformatycznego – obejmuje zasady związane z bezpieczeństwem teleinformatycznym, w tym:

1) utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;
2) dbałość o aktualizację oprogramowania;
3) minimalizacje ryzyka utraty informacji w wyniku awarii;
4) ochronę przed błędami, utratą, nieuprawnioną modyfikacją;
5) stosowanie mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisów prawa;
6) zapewnienie bezpieczeństwa plików systemowych;
7) redukcje ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych;
8) niezwłoczne podejmowanie działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa;
9) kontrole zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;
10) zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniem lub zakłóceniem, przez:
    - monitorowanie dostępu do informacji,
    - czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
    - zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji.

3.Obszar utrzymania SZBI – obejmuje zasady związane z utrzymaniem Bezpieczeństwa Informacji, w tym:

1) zasady związane z zarządzaniem ryzykiem w bezpieczeństwie informacji;
2) zasady obsługi incydentów naruszenia bezpieczeństwa informacji;
3) zasady przeprowadzania okresowych audytów w zakresie bezpieczeństwa informacji;
4) nadzór i aktualizacje regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.

4. Obszar bezpieczeństwa osobowego – obejmuje zasady realizacji szkoleń osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:

1) zagrożenia bezpieczeństwa informacji;
2) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna;
3) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

Zachowanie poufności informacji przetwarzanych w Ministerstwie zapewnia m.in. podpisane „Oświadczenie o poufności", określone w Polityce ochrony danych osobowych w Ministerstwie Sportu i Turystyki.

5. Obszar ochrony danych osobowych obejmuje zasady związane z przetwarzaniem danych osobowych oraz sposoby ich zabezpieczania w systemach informatycznych i zbiorach papierowych.

7. Podstawowe zasady bezpieczeństwa informacji

Zarządzanie bezpieczeństwem informacji w Ministerstwie opiera się na następujących zasadach:

1) **zasada uprawnionego dostępu –** każdy pracownik przeszedł szkolenie z zasad ochrony informacji, spełnia kryteria dopuszczenia do informacji i podpisał stosowne oświadczenie o zachowaniu poufności;
2) **zasada przywilejów koniecznych –** każdy pracownik posiada prawa dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań;
3) **zasada wiedzy koniecznej –** każdy pracownik posiada wiedzę o systemie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań;
4) **zasada usług koniecznych –**udostępniane powinny być tylko takie usługi jakie są konieczne do realizacji zadań Ministra;
5) **zasada asekuracji –** każdy mechanizm zabezpieczający musi być ubezpieczony drugim, innym (podobnym); w przypadkach szczególnych może być stosowane dodatkowe (trzecie) niezależne zabezpieczenie;
6) **zasada świadomości zbiorowej –** wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych i aktywnie uczestniczą w tym procesie;
7) **zasada indywidualnej odpowiedzialności –** za bezpieczeństwo poszczególnych elementów odpowiadają konkretne osoby;
8) **zasada obecności koniecznej –** prawo przebywania w określonych miejscach mają tylko osoby upoważnione;
9) **zasada stałej gotowości –** system jest przygotowany na wszelkie zagrożenia; niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających;
10) **zasada kompletności –** skuteczne zabezpieczenie jest tylko wtedy, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i ogniwa ogólnie pojętego procesu przetwarzania informacji;
11) **zasada ewolucji –** każdy system musi ciągle dostosowywać mechanizmy wewnętrzne do zmieniających się warunków zewnętrznych;
12) **zasada adekwatności –** używane środki techniczne i organizacyjne muszą być adekwatne do sytuacji;
13) **zasada świadomej konwersacji –** nie zawsze i wszędzie trzeba mówić, co się wie, ale zawsze i wszędzie trzeba wiedzieć co, gdzie i do kogo się mówi;
14) **zasada segregacji zadań –** zadania i uprawnienia powinny być tak podzielone, aby jedna osoba nie mogła zdobyć pełni władzy nad całym systemem.

Dobór zabezpieczeń powinien opierać się na celu ich stosowania oraz adekwatności do wymagań prawnych i wyników analizy ryzyka dla bezpieczeństwa informacji.

8. Utrzymanie odpowiedniego poziomu bezpieczeństwa informacji

1. System Zarządzania Bezpieczeństwem Informacji uwzględnia procesy utrzymania odpowiedniego poziomu bezpieczeństwa, w tym:
   1) zarządzanie ryzykiem;
   2) zarządzanie dostępem do zasobów;
   3) monitorowanie poziomu bezpieczeństwa;
   4) zarządzanie incydentem bezpieczeństwa;
   5) nadzór nad dokumentacją Systemu Zarządzania Bezpieczeństwem Informacji.

2. Nakłady ponoszone na zabezpieczenia powinny być poprzedzone analizą ryzyka i kosztów, adekwatnie do potencjalnych strat spowodowanych naruszeniem bezpieczeństwa.