Załącznik nr 3
Polityki Bezpieczeństwa Informacji
Świętokrzyskiego Urzędu
Wojewódzkiego

Procedura zarządzania ryzykiem w Systemie Zarządzania Bezpieczeństwem Informacji[1]

[1] Na podstawie metodyki zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych przygotowanej przez Ministerstwo Administracji i Cyfryzacji (obecnie Ministerstwo Cyfryzacji)

1. Wprowadzenie

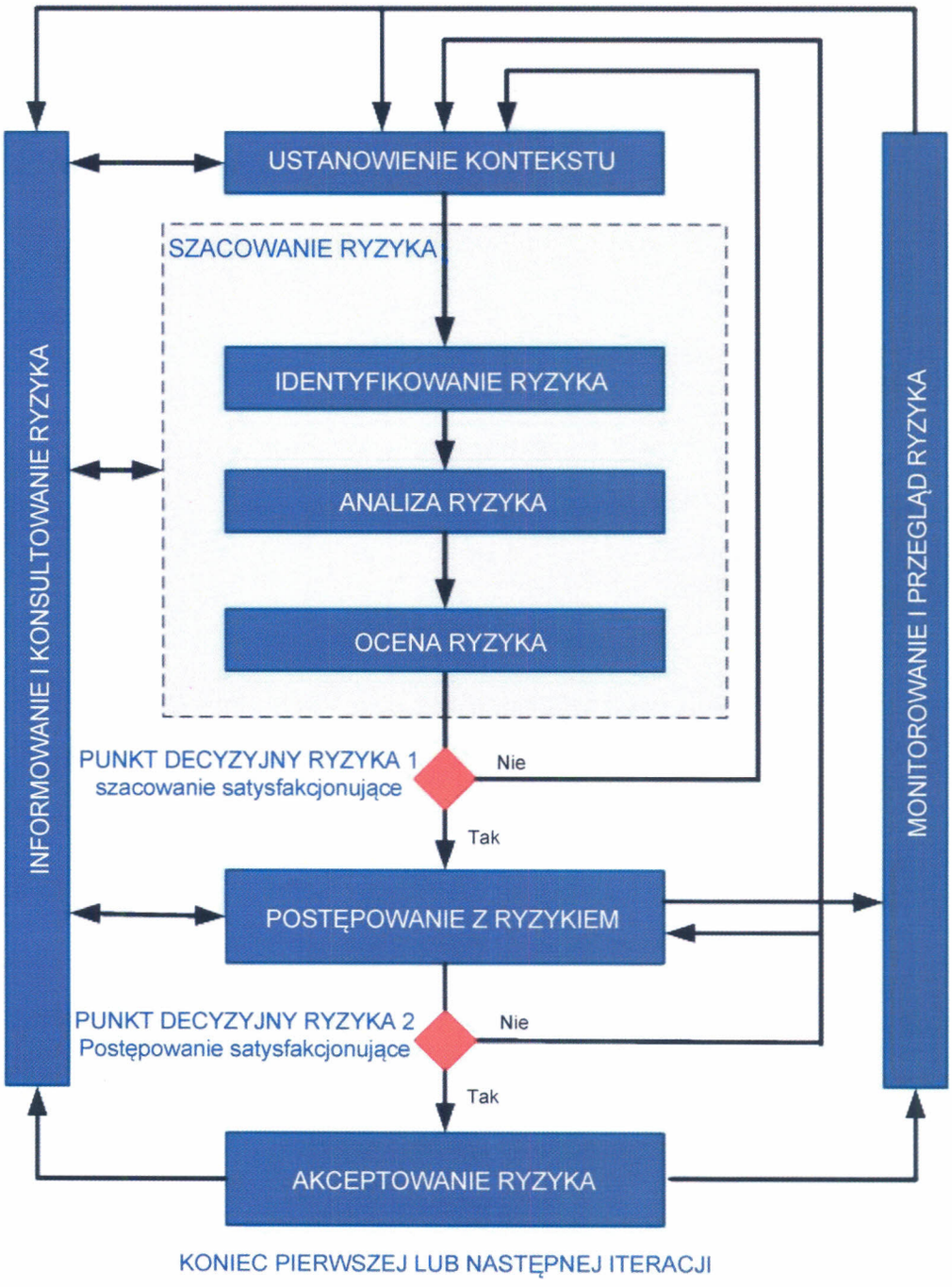
Celem niniejszego dokumentu jest ustanowienie metodyki zarządzania ryzykiem w Systemie Zarządzania Bezpieczeństwem Informacji w Urzędzie w zakresie zagrożeń pochodzących z cyberprzestrzeni. Poprzez zarządzanie ryzykiem należy rozumieć działania polegające na:

- szacowaniu ryzyka,
- postępowaniu z ryzykiem,
- akceptowaniu ryzyka,
- monitorowaniu ryzyka,
- informowaniu o ryzyku

w ramach ustalonego kontekstu.

Opracowanie bazuje na Polskiej Normie PN-ISO/IEC 27005:2014 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji.
Niniejsza metodyka w zakresie szacowania ryzyka przyjmuje podejście zasobowe. Za zasób należy uznawać system teleinformatyczny wraz zasobami informacyjnymi przetwarzanymi przez system.

Zarządzanie ryzykiem w bezpieczeństwie informacji odbywa się zgodnie z modelem przedstawionym na Rysunku 1.



Rysunek 1: Model procesu zarządzania ryzykiem (za Polską Normą PN ISO/IEC 27005)

2. Procedura zarządzania ryzykiem

2.1 Identyfikowanie ryzyka

Identyfikowanie ryzyka przeprowadza się w poszczególnych kategoriach zagrożeń.
Początkową identyfikację ryzyk przeprowadza osoba odpowiedzialna za dany zasób i przekazuje wyniki identyfikacji do osoby odpowiedzialnej za wykonanie analizy ryzyka. Cały proces koordynuje pełnomocnik ds. bezpieczeństwa cyberprzestrzeni danej instytucji.

Rozdział 5 określa wykaz zagrożeń i związanych z nimi podatności. Wykaz zagrożeń i podatności może zostać rozszerzony w miarę potrzeb. Identyfikację ryzyk prowadzi się okresowo (nie rzadziej niż raz na rok) lub ad hoc.
Identyfikacja ad hoc dokonywana jest w przypadku zaobserwowania zagrożenia dla systemu, którego horyzont materializacji jest krótszy od okresowej identyfikacji ryzyk, a zwłoka w identyfikacji miałaby istotne znaczenie dla systemu. Identyfikacją ad hoc dokonywana jest także w przypadku wystąpienia incydentu teleinformatycznego, którego skutkiem była utrata bezpieczeństwa informacji mająca charakter katastrofalny. W szczególności identyfikację ryzyk przeprowadza się przed oddaniem systemu do eksploatacji.

Źródła potencjalnych ryzyk mogą być zgłoszone osobie odpowiedzialnej za szacowanie ryzyka w każdym momencie, przez każdego interesariusza systemu.

2.2 Analiza ryzyka

Analizy ryzyk dokonuje osoba wyznaczona przez pełnomocnika ds. bezpieczeństwa cyberprzestrzeni danej instytucji. Na analizę ryzyka składają się:

- szacowanie następstw,
- szacowanie prawdopodobieństwa incydentu,
- określenie poziomu ryzyka.

2.2.1 Szacowanie następstw (skutków)

Szacowanie następstw polega na rozważeniu jakie skutki dla zasobów informacyjnych lub systemów teleinformatycznych niesie ze sobą zmaterializowanie się zagrożeń z uwzględnieniem podatności zasobów lub systemów. Następstwa mogą mieć charakter materialny (np. koszt odtworzenia danego zasobu lub przywrócenia jego sprawności) lub niematerialny (np. utrata wizerunku podmiotu w społeczeństwie). W określonych sytuacjach następstwo (skutek) może przekształcać się w samoistne zagrożenie, wywołując kolejne ryzyko. Wskazane jest aby szacowanie następstw (skutków) było prowadzone w odniesieniu do określonych scenariuszy incydentów.

2.2.2 Szacowanie prawdopodobieństwa incydentu

Szacowanie prawdopodobieństwa incydentu ma na celu ustalenie częstotliwości z jaką mogą pojawiać się określone incydenty. Pod uwagę powinny być brane następujące okoliczności:

- doświadczenie szacującego oraz statystyki dotyczące podobnych zdarzeń,
- w przypadku zagrożeń antropogennych atrakcyjność zasobu lub efektu skutku dla wywołującego incydent,

- dla zagrożeń o charakterze przypadkowym położenie geograficzne, warunki pogodowe itp., które mogą oddziaływać na powstawanie błędnych działań użytkowników zasobów informacyjnych lub systemów teleinformatycznych,
- rodzaje podatności,
- istniejące zabezpieczenia.

2.2.3 Określanie poziomu ryzyka

Określanie poziomu ryzyka polega na przypisaniu danemu zagrożeniu prawdopodobieństwa oddziaływania na zasoby informacyjne lub system teleinformatyczny oraz ustaleniu wpływu materializacji zagrożenia na:

1) dostępność systemu lub informacji,
2) integralność systemu lub informacji,
3) poufność informacji przetwarzanej w systemie,

a następnie wyznaczeniu poziomu ryzyka.

Poziom ryzyka wyznacza się według następującego wzoru:

$$R_p = P \times (S_d + S_i + S_p)$$

gdzie:

R_p – pierwotny poziom ryzyka,
P – wartość przypisana prawdopodobieństwu materializacji zagrożenia, $P \in \{0,1,2,3,4\}$

gdzie:

0 – zdarzenie nieprawdopodobne (zagrożenie nie występuje),
1 – zdarzenie prawie nieprawdopodobne,
2 – zdarzenie mało prawdopodobne,
3 – zdarzenie wysoce prawdopodobne,
4 – zdarzenie niemal pewne.

S_d – wartość przypisana skutkowi dla dostępności informacji,
S_i – wartość przypisana skutkowi dla integralności informacji,
S_p – wartość przypisana skutkowi dla poufności informacji,

$(S_d, S_i, S_p) \in \{0,1,2,3,4\}$

gdzie:

0 – zdarzenie nie powoduje skutku (brak podatności),
1 – zdarzenie wywołuje niewielki skutek,
2 – zdarzenie wywołuje znaczący skutek,
3 – zdarzenie wywołuje bardzo znaczący skutek,
4 – zdarzenie wywołuje skutek katastrofalny.

2.3 Ocena ryzyka

Ocena ryzyka polega na porównaniu wyznaczonych poziomów ryzyka z ustalonymi wstępnie kryteriami akceptowania ryzyka i umożliwia ustalenie priorytetów w zarządzaniu ryzykiem. Kryteria akceptacji ryzyka ustala dany podmiot z uwzględnieniem niniejszej metodyki. Kryteria i kompetencje w zakresie akceptacji ryzyka zatwierdza kierownik podmiotu.

Ryzyka, dla których wartość pierwotnego poziomu, jest niższa lub równa 20%[2] poziomu maksymalnego (Rp ≤ 9,6) uznaje się a priori za ryzyka szczątkowe, które nie podlegają procedurze postępowania z ryzykiem. Ryzyka dla których poziom przekracza 20% poziomu ryzyka maksymalnego (Rp > 9,6), podlegają procedurze postępowania z ryzykiem.

2.4 Postępowanie z ryzykiem

Ryzyka, które na poziomie oceny nie zostały uznane za ryzyka szczątkowe, podlegają procedurze postępowania z ryzykiem. Postępowanie z ryzykiem może polegać na:

1) wpływaniu na zmianę poziomu ryzyka poprzez zastosowanie zabezpieczenia,
2) unikaniu ryzyka,
3) przeniesieniu ryzyka,
4) akceptacji ryzyka mimo, że jego poziom przekracza poziom ryzyka szczątkowego.

2.4.1 Sterowanie ryzykiem

Sposobem postępowania z ryzykiem jest ograniczanie poziomu ryzyka poprzez zastosowanie środka sterowania ryzykiem w postaci zabezpieczenia, dobranego adekwatnie do charakteru tego ryzyka.

Na etapie postępowania z ryzykiem dokonuje się ponownego estymowania poziomu ryzyka z uwzględnieniem zabezpieczenia. Przeliczenie dokonywane jest według wzoru: $Rk=Px(Sd/Cd+Si/Ci+Sp/Cp)$

gdzie:

Rk – końcowy poziom ryzyka,

P, Sd, Si, Sp zdefiniowane w pkt. 2.2.3,

C – skuteczność zabezpieczenia,

$(Cd,Ci,Cp) \in \{1,2,3,4\}$

gdzie:

1 – brak zabezpieczenia,

2 – zabezpieczenie ogranicza poziom ryzyka,

3 – zabezpieczenie w istotny sposób ogranicza poziom ryzyka,

4 – zabezpieczenie w bardzo istotny sposób ogranicza poziom ryzyka.

Zastosowanie zabezpieczenia musi uwzględniać wpływ zastosowania zabezpieczenia na pozostałe atrybuty bezpieczeństwa i samo w sobie może stanowić czynnik ryzyka. Przykładowo: zastosowanie zabezpieczenia ograniczającego ryzyko utraty poufności może spowodować podniesienie ryzyka utraty dostępności. W takim przypadku należy powrócić do estymacji początkowego poziomu ryzyka z uwzględnieniem zastosowanego zabezpieczenia.

2.4.2 Unikanie ryzyka

[2] przy ustalaniu progów poziomów ryzyka, od których zależy sposób postępowania z ryzykiem, przyjęto zasadę Pareto

W przypadku realizacji zadań publicznych unikanie ryzyka, co do zasady, nie ma zastosowania.

2.4.3 Przeniesienie ryzyka

W przypadku realizacji zadań publicznych przeniesienie ryzyka, co do zasady, nie ma zastosowania. Niemniej przeniesienie ryzyka może być zasadne w postaci ubezpieczenia składników majątkowych systemu.

2.4.4 Akceptacja ryzyka

W wyniku przeliczenia poziomów ryzyk uzyskuje się wartość końcową poziomu ryzyka. Ryzyka, dla których końcowy poziom ryzyka jest niższy lub równy 20% poziomu maksymalnego ($Rk \leq 9,6$) podlegają automatycznej akceptacji, ale pozostają pod nadzorem właściciela ryzyka w celu ich monitorowania. Ryzyka dla których poziom zawiera się w przedziale $9,6 < Rk \leq 38,4$ podlegają akceptacji według zasad ustalonych w podmiocie lub dokonywana jest ich ponowna analiza. Ryzyka dla których poziom ryzyka jest większy od 80% poziomu maksymalnego ($Rk > 38,4$), przedstawiane są do akceptacji kierownictwa podmiotu.

2.5 Informowanie o ryzyku

Ryzyka, poprzez rejestr ryzyk, powinny być komunikowane wszystkim interesariuszom procesów biznesowych (zadań publicznych). Do interesariuszy należy w szczególności minister właściwy do spraw informatyzacji.

W raporcie o ryzykach przesyłanym do ministra właściwego do spraw informatyzacji na podstawie Polityki Ochrony Cyberprzestrzeni RP, nie komunikuje się ryzyk szczątkowych.

3 Dokumenty i zapisy

W zakresie zarządzania ryzykiem utrzymywane są następujące dokumenty:

1) aktualny dokument Metodyka zarządzania ryzykiem,
2) rejestr ryzyk,
3) zgłoszenia ryzyk przez interesariuszy w postaci dokument Informacja o ryzyku.

4 Raportowanie i terminy działań w zarządzaniu ryzykiem

Raportowaniu podlegają analizy ryzyka sporządzone odrębnie dla każdego systemu teleinformatycznego utrzymywanego przez podmiot raportujący. Raportowanie w zakresie analizy ryzyka odbywa się w następujący sposób:

1) dokonanie w Urzędzie analizy ryzyka w terminie do 31 grudnia każdego roku,
2) przekazanie ministrowi właściwemu do spraw informatyzacji, do dnia 31 stycznia roku następnego po wykonanej analizie ryzyka, oświadczenie o dokonanej analizie ryzyka wraz z informacją o ryzykach w formie Rejestru Ryzyk,

Minister właściwy do spraw informatyzacji przekazuje do dnia 31 marca Prezesowi Rady Ministrów informację o stanie bezpieczeństwa cyberprzestrzeni RP wraz z wnioskami

dotyczącymi niezbędnych działań w obszarze bezpieczeństwa informacji wynikających z przeprowadzonej analizy ryzyka w podmiotach zobowiązanych (urzędach).

5 Kategorie zagrożeń

Wyróżnia się następujące kategorie zagrożeń w interakcji systemu teleinformatycznego i cyberprzestrzeni oraz przykładowych podatności powodujących, że materializacja zagrożenia będzie miała oddziaływanie na zasób informacyjny lub system teleinformatyczny:

Lp.	Podatności
1. Kategoria zagrożenia: Wniknięcie kodu złośliwego z sieci WAN	
1.	brak lub złe umiejscowienie w systemie, lub brak aktualizacji oprogramowania typu AV
2.	brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja zapór sieciowych (firewall)
3.	brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja oprogramowania IPS/IDS i jego sond
4.	niewłaściwa konfiguracja mechanizmów bezpieczeństwa w sieciach WAN
5.	brak monitorowania obciążenia serwerów
6.	podatność użytkowników na oddziaływanie metod inżynierii społecznej w celu uzyskania informacji lub wprowadzenia kodu złośliwego
2. Kategoria zagrożenia: Wprowadzenie kodu złośliwego z sieci LAN	
1.	brak lub złe umiejscowienie w systemie, lub brak aktualizacji oprogramowania typu AV
2.	brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja zapór sieciowych (firewall)
3.	brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja oprogramowania IPS/IDS i jego sond
4.	niewłaściwa konfiguracja mechanizmów bezpieczeństwa w sieciach LAN
3. Kategoria zagrożenia: Atak typu DDoS lub DoS	
1.	brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja zapór sieciowych (firewall)
2.	brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja oprogramowania IPS/IDS i jego sond
3.	brak nadzoru nad ruchem w sieci (QoS)
4.	brak monitorowania obciążenia serwerów
5.	błąd oprogramowania
6.	utrata dostępu do usług sieci WAN (w tym Internetu) w wyniku ataku na komponenty sieci WAN
7.	Wykorzystywanie do obsługi systemu przestarzałego sprzętu
8.	Nie podejmowanie działań w celu wymiany sprzętu na nowocześniejszy (zapewniający wsparcie techniczne)
4. Kategoria zagrożenia: Nieautoryzowany dostęp do informacji	
1.	brak nadzoru nad uprawnieniami użytkowników, uprawnienia nieadekwatne do zadań
2.	zbyt wolne wnoszenie zmian uprawnień użytkowników

3.	brak kontroli dostępu fizycznego do elementów systemu
5. Kategoria zagrożenia: Nieumiejętne posługiwanie się systemem przez użytkownika	
1.	brak właściwych szkoleń użytkowników w zakresie użycia systemu
2.	brak kontroli jakości danych wprowadzanych do systemu
3.	odzyskanie informacji z nośników wycofanych z użycia
4.	podatność użytkowników na oddziaływanie metod inżynierii społecznej w celu uzyskania informacji lub wprowadzenia kodu złośliwego.
6. Kategoria zagrożenia: Przełamanie zabezpieczeń dostępu wewnątrz systemu	
1.	brak nadzoru nad uprawnieniami użytkowników, uprawnienia nieadekwatne do zadań (np. możliwość instalacji programów, w tym służącym przełamaniu zabezpieczeń)
2.	zbyt wolne wnoszenie zmian uprawnień użytkowników
3.	brak nadzoru nad aktywnością użytkowników w systemie
4.	brak lub złe umiejscowienie w systemie, lub brak aktualizacji oprogramowania typu AV
.	brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja zapór sieciowych (firewall)
6.	brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja oprogramowania IPS/IDS i jego sond
7. Kategoria zagrożenia: Podsłuch danych, przechwyt danych	
1.	brak nadzoru nad ruchem w sieci (QoS)
2.	emisja ujawniająca
3.	brak szyfrowania w łączach WAN
4.	podsłuch informacji w sieci wewnętrznej (LAN)
5.	pozyskanie informacji z nośników wycofanych z użycia
8. Kategoria zagrożenia: Włamanie do systemu teleinformatycznego z sieci zewnętrznej WAN (przełamanie zabezpieczeń)	
1.	brak aktualizacji oprogramowania systemowego
2.	brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja zapór sieciowych (firewall)
3.	brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja oprogramowania IPS/IDS i jego sond
4.	brak nadzoru nad ruchem w sieci (QoS)
5.	brak monitorowania obciążenia serwerów
6.	podatność użytkowników na oddziaływanie metod inżynierii społecznej w celu uzyskania informacji lub wprowadzenia kodu złośliwego
9. Kategoria zagrożenia: System podmiotu (urzędu) źródłem zakłóceń w cyberprzestrzeni	
1.	brak nadzoru nad ruchem w sieci (QoS)
2.	brak lub złe umiejscowienie w systemie, lub brak aktualizacji oprogramowania typu AV
3.	brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja zapór sieciowych (firewall)
4.	brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja oprogramowania IPS/IDS i jego sond

6. Kategorie zabezpieczeń

Przykłady zabezpieczeń przed zagrożeniami systemu teleinformatycznego pochodzącymi z cyberprzestrzeni:

Lp.	Możliwe zabezpieczenia
1. Kategoria zagrożenia: Wniknięcie kodu złośliwego z sieci WAN	
1.	Budowanie topologii sieci z uwzględnieniem obszarów bezpiecznych i zdemilitaryzowanych (DMZ)
2.	Translacja adresów sieciowych
3.	Zapory sieciowe skonfigurowane według zasady „wszystko jest zabronione, z wyjątkiem tego na co wyrażono zgodę"
4.	Oprogramowanie klasy AV na styku sieci WAN z LAN
5.	Systemy klasy IDS/IPS
6.	Serwery PROXY (w tym utrzymywanie czarnej listy adresów URL oraz adresów IP)
7.	Wykrywanie i blokowanie spamu
8.	Procedury utrzymania zabezpieczeń wymienionych w pkt. 3 - 6
9.	Procedury reagowania na wykryte incydenty
2. Kategoria zagrożenia: Wprowadzenie kodu złośliwego z sieci LAN	
1.	Oprogramowanie klasy AV na stacjach roboczych
2.	Blokowanie portów USB na stacjach roboczych
3.	Nadzór nad niewykorzystywanymi zakończeniami sieci LAN
4.	Autoryzacja dostępu do serwera DHCP
5.	Blokowanie możliwości instalowania oprogramowania przez użytkownika
6.	Weryfikacja zainstalowanego oprogramowania na stacjach roboczych
7.	Procedury uaktualnienia oprogramowania (instalacja łat)
8.	Zabezpieczenie odpowiednich środków finansowych zapewniających wymianę sprzętu (zgodnie z obowiązującą w Urzędzie 'Strategią rozwoju informatyzacji"
3. Kategoria zagrożenia: Atak typu DDoS lub DoS	
1.	Monitorowanie ruchu w sieci
2.	Stosowanie techniki rozpraszania danych (CDN – content delivery network).
3.	Przejście na statyczne wersje serwisu po wykryciu ataku typu DDoS/DoS
4.	Umowy z dostawcami usługi dostępu do Internetu zawierające klauzule przenoszące działania przeciw atakowi na dostawcę
5.	Blokowanie ruchu sieciowego z określonych adresów IP
6.	Procedury postępowania na wypadek wykrycia ataku DDoS/DoS
4. Kategoria zagrożenia: Nieautoryzowany dostęp do informacji	
1.	Procedury nadawania i odbierania uprawnień w systemie
2.	Procedury przeglądania uprawnień w systemach
3.	Stosowanie zasady wiedzy koniecznej (need to know)
4.	Rozpraszanie uprawnień (zasada „czterech par oczu")
5. Kategoria zagrożenia: Nieumiejętne posługiwanie się systemem przez użytkownika	
1.	Szkolenia wstępne dla pracowników nowozatrudnionych
2.	Okresowe szkolenia dla pracowników już zatrudnionych
3.	Stosowanie aplikacji weryfikujących jakość wprowadzanych danych

6. Kategoria zagrożenia: Przełamanie zabezpieczeń dostępu wewnątrz systemu	
1.	Blokowanie możliwości instalowania oprogramowania przez użytkownika
2.	Utwardzanie stacji roboczych (eliminacja zbędnych użytkownikowi funkcji systemu operacyjnego i zbędnych aplikacji)
3.	Blokowanie możliwości uruchomienia systemu operacyjnego z nośnika wymiennego
4.	Weryfikacja, czy na stacji roboczej znajduje się wyłącznie dopuszczalne oprogramowanie
5.	Okresowe przeglądanie logów stacji roboczej przez administratorów
6.	Procedury postępowania w przypadku wykrycia anomalii i sposoby dokumentowania takiego postępowania
7. Kategoria zagrożenia: Podsłuch danych, przechwyt danych	
1.	Stosowanie strefowania
2.	Stosowanie urządzeń o obniżonej emisji ujawniającej
3.	Ekranowanie pomieszczeń
4.	Prowadzenie okablowania sieciowego w zamkniętych kanałach, nadzór nad krosownicami
5.	Stosowanie światłowodów w miejsce połączeń galwanicznych
6.	Nadzór nad niewykorzystywanymi zakończeniami sieci LAN (odłączanie niewykorzystanych zakończeń na krosownicach)
8. Kategoria zagrożenia: System podmiotu (urzędu) źródłem zakłóceń w cyberprzestrzeni	
1.	Nadzór nad ruchem wychodzącym
2.	Procedury reagowania na wykrycie botnet w sieci podmiotu
3.	Procedury reagowania na próby rozsyłania spamu
4.	Wykrywanie nielegalnych działań ze strony użytkowników wewnętrznych systemu.

Załącznik Nr 1 – Wytyczne do przeprowadzenia estymacji ryzyka i ograniczania ryzyka

A. Estymacja ryzyka

Określanie pierwotnego poziomu ryzyka odbywa się zgodnie ze wzorem:

$$Rp = P \times (Sd + Si + Sp)$$

gdzie:

Rp – pierwotny poziom ryzyka,

P – wartość przypisana prawdopodobieństwu materializacji zagrożenia, $P \in \{0,1,2,3,4\}$

gdzie:

0 – zdarzenie nieprawdopodobne (zagrożenie nie występuje),
1 – zdarzenie prawie nieprawdopodobne,
2 – zdarzenie mało prawdopodobne,
3 – zdarzenie wysoce prawdopodobne,
4 – zdarzenie niemal pewne.

Sd – wartość przypisana skutkowi dla dostępności informacji,
Si – wartość przypisana skutkowi dla integralności informacji,
Sp – wartość przypisana skutkowi dla poufności informacji, $(Sd, Si, Sp) \in \{0,1,2,3,4\}$

gdzie:

0 – zdarzenie nie powoduje skutku,
1 – zdarzenie wywołuje niewielki skutek,
2 – zdarzenie wywołuje znaczący skutek,
3 – zdarzenie wywołuje bardzo znaczący skutek,
4 – zdarzenie wywołuje skutek katastrofalny.

Podczas doboru wartości przypisywanej prawdopodobieństwu materializacji zagrożenia należy przyjąć następujące zasady:

1) Wartość 0 należy przyjąć, jeśli zdarzenie jest wysoce nieprawdopodobne w odniesieniu do systemu lub informacji przetwarzanej w systemie, lub charakter zagrożenia ujętego w rozdziale 5 jest nieadekwatny do specyfiki systemu.
2) Wartość 1 należy przyjąć, jeśli częstotliwość materializacji zagrożenia jest liczona co najmniej w dziesiątkach lat lub brak jest informacji by zagrożenie zmaterializowało się w podobnych podmiotach w kraju lub na świecie.
3) Wartość 2 należy przyjąć, jeśli częstotliwość materializacji zagrożenia jest liczona w pojedynczych latach lub zagrożenie z danej kategorii zmaterializowało się w podobnych podmiotach w kraju lub na świecie w pojedynczych przypadkach.
4) Wartość 3 należy przyjąć, jeśli materializacja zagrożenia może wystąpić kilka razy w roku.

5) Wartość 4 należy przypisać zagrożeniu, które wielokrotnie materializowało się w ciągu roku w danym podmiocie lub w podobnych podmiotach w kraju lub na świecie.

Podczas doboru wartości przypisywanej skutkowi dla odpowiednich atrybutów bezpieczeństwa informacji należy przyjąć ogólną zasadę, że o ile materializacja zagrożenia, z uwagi na istotę tego zagrożenia, nie wywołuje wpływu na dany atrybut bezpieczeństwa informacji należy przyjąć Sd,i,p=0, w pozostałych przypadkach należy przyjąć następujące zasady:

Dla skutku utraty dostępności:

1) Jeżeli okres czasu utraty dostępności informacji lub usług systemu, spowodowany materializacją zagrożenia, mieści się w okresie czasu założonym w planie zapewnienia ciągłości działania (RTO – Recovery Time Objective)[3], a przywrócenie pełnego dostępu do informacji lub usług systemu nie wiąże się z dodatkowymi kosztami należy przyjąć Sd=1.
2) Jeżeli okres czasu utraty dostępności informacji lub usług systemu, spowodowany zagrożeniem, mieści się w okresie czasu założonym w planie zapewnienia ciągłości działania (RTO – Recovery Time Objective), ale przywrócenie dostępu do informacji wiąże się z dodatkowymi kosztami należy przyjąć Sd=2.
3) Jeżeli okres czasu utraty dostępności informacji lub usług systemu, spowodowany zagrożeniem, znacząco nie mieści się w okresie czasu założonym w planie zapewnienia ciągłości działania (RTO – Recovery Time Objective) należy przyjąć Sd=3.
4) Jeżeli okres czasu utraty dostępności informacji lub usług systemu, spowodowany zagrożeniem, wielokrotnie przekracza czas założony w planie zapewnienia ciągłości działania (RTO – Recovery Time Objective) lub jeżeli spowodowana zagrożeniem utrata dostępności informacji jest nieodwracalna należy przyjąć Sd=4.

Dla skutku utraty integralności:

1) Jeżeli spowodowana zagrożeniem utrata integralności informacji jest łatwo wykrywalna i przywrócenie integralności nie powoduje nadmiernych kosztów należy przyjąć Si=1.
2) Jeżeli spowodowana zagrożeniem utrata integralności informacji jest trudno wykrywalna i informacja taka może zostać użyta w procesach decyzyjnych, jednak istnieje możliwość skorygowania decyzji należy przyjąć Si=2.

[3] RTO jest kategorią, którą posługuje się planowanie ciągłości działania i oznacza czas przez jaki system może być niedostępny, nie powodując przy tym nieodwracalnych skutków dla realizowanych zadań.

3) Jeżeli spowodowana zagrożeniem utrata integralności informacji jest trudno wykrywalna i informacja taka może zostać użyta w procesach decyzyjnych i nie istnieje możliwość skorygowania decyzji należy przyjąć Si=3.
4) Jeżeli spowodowana zagrożeniem utrata integralności informacji może okazać się niewykrywalna należy przyjąć Si=4.

Uwaga:
W praktyce może pojawić się problem korelacji atrybutu dostępności z atrybutem integralności, przyjmujący postać dylematu – czy informacja zniekształcona poprzez utratę integralności jest informacją dostępną, czy też wraz z utratą integralności nastąpiła utrata dostępności. Na potrzeby niniejszej analizy należy przyjąć, że utrata integralności informacji nie powoduje automatycznej utraty dostępności. Atrybuty dostępności i integralności informacji należy rozpatrywać rozłącznie.

Dla skutku utraty poufności:
1) Jeżeli utrata poufności dotyczy spraw mniejszej wagi, odnosi się do pojedynczych przypadków i nie wiąże się z odpowiedzialnością karną albo administracyjną osób odpowiedzialnych za zapewnienie ochrony takiej informacji należy przyjąć Sp=1.
2) Jeżeli utrata poufności dotyczy informacji o charakterze wrażliwym[4] lub odnosi się do licznych przypadków, jednak nie wiąże się z odpowiedzialnością karną albo administracyjną osób odpowiedzialnych za zapewnienie ochrony takiej informacji należy przyjąć Sp=2.
3) Jeżeli utrata poufności dotyczy informacji o charakterze wrażliwym lub odnosi się do licznych przypadków, wpływa w sposób znaczący na wizerunek urzędu i organu, który ten urząd obsługuje, jednak nie wiąże się z odpowiedzialnością karną osób odpowiedzialnych za zapewnienie ochrony takiej informacji, jednak może wiązać się z odpowiedzialnością administracyjną, należy przyjąć Sp=3.
4) Jeżeli utrata poufności może prowadzić do naruszenia interesów osób trzecich i może prowadzić do roszczeń odszkodowawczych ze strony tych osób, a także do odpowiedzialności karnej osób odpowiedzialnych za zapewnienie ochrony takiej informacji należy przyjąć Sp=4.

B. Ograniczanie ryzyka

Ograniczanie poziomu ryzyka prowadzone jest w procesie postępowania z ryzykiem. Podstawowym sposobem postępowania z ryzykiem w przypadku podmiotów sektora rządowego jest stosowanie zabezpieczeń. Estymację poziomu ryzyka po zastosowaniu zabezpieczeń prowadzi się na podstawie następującego wzoru:

$$Rk=Px(Sd/Cd+Si/Ci+Sp/Cp)$$

gdzie:

[4] Pojęcie „wrażliwość" należy rozumieć słownikowo, a nie w kategoriach ustawy o ochronie danych osobowych.

Rk – końcowy poziom ryzyka,

C – skuteczność środka sterowania ryzykiem (zabezpieczenia) w odniesieniu do atrybutu bezpieczeństwa informacji $(Cd,Ci,Cp) \in \{1,2,3,4\}$ dla środka sterowania ryzykiem wynikającym z zagrożeń,

gdzie:

1 – brak środka sterowania ryzykiem (zabezpieczenia),

2 – środek sterowania ryzykiem (zabezpieczenie) ogranicza poziom ryzyka,

3 – środek sterowania ryzykiem (zabezpieczenie) w istotny sposób ogranicza poziom ryzyka,

4 – środek sterowania (zabezpieczenie) w bardzo istotny sposób ogranicza poziom ryzyka.

Podczas doboru wartości wskaźnika skuteczności zabezpieczenia należy przyjąć następujące zasady:

1) Jeżeli brak jest możliwości zastosowania zabezpieczenia lub zastosowanie zabezpieczenia jest niecelowe (np. w przypadku S=0) należy przyjąć C=1.
2) Jeżeli zabezpieczenie powoduje obniżenie skutku Sd,i,p o jeden stopień należy przyjąć C=2.
3) Jeżeli zabezpieczenie powoduje obniżenie skutku Sd,i,p o dwa stopnie należy przyjąć C=3.
4) Jeżeli zabezpieczenie powoduje obniżenie skutku Sd,i,p o co najmniej trzy stopnie należy przyjąć C=4.