2023

Narodowy Program Ochrony Infrastruktury Krytycznej

Załącznik 1

Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje

RCB
Rządowe Centrum Bezpieczeństwa

1. Jak korzystać z załącznika nr 1

1.1. Co zawiera i dla kogo jest przeznaczony?

Dokument zawiera podstawowe informacje na temat organizacyjnych i technicznych aspektów ochrony infrastruktury krytycznej (IK). Może on posłużyć jako zestaw konkretnych wskazówek dotyczących budowy, organizacji lub funkcjonowania systemu ochrony IK.

W dokumencie można znaleźć odniesienie do podstawowych wymagań i ich wpływu na proces identyfikacji i analizy zagrożeń oraz na szacowanie ryzyk do których zobowiązany jest każdy operator IK. Dokument opisuje również zakres skorelowania ochrony IK z zadaniami z obszaru ciągłości działania[1] i cyberbezpieczeństwa, ale też bezpieczeństwa osobowego, fizycznego, technicznego i prawnego oraz celami operatora IK i posiadanymi przez niego zasobami.

Dokument może być źródłem odniesienia do tworzenia przez operatorów IK jednej lub kilku polityk bezpieczeństwa, opracowań eksperckich stanowiących źródło wiedzy dla osób, które nadzorują IK, jak również dla interesariuszy tj. osób fizycznych i prawnych, podmiotów, służb bezpieczeństwa publicznego i bezpieczeństwa powszechnego, które są zaangażowane bezpośrednio lub pośrednio w ochronę IK.

Dokument przeznaczony jest dla operatorów IK, koordynatorów systemów IK oraz interesariuszy realizujących zadania w ramach IK, jak również podmiotów zainteresowanych wdrażaniem wybranych aspektów bezpieczeństwa w IK w swoich organizacjach.

Stosowane w załączniku rekomendacje mogą być wykorzystywane do opracowywania:

1/ dokumentów koordynatorów poszczególnych systemów IK, w których planuje się umieścić zbiór postanowień i strategii przewidzianych do wdrożenia,
2/ Planu Ochrony Infrastruktury Krytycznej (POIK), o którym mowa w Rozporządzeniu Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (Dz.U.2010 nr 83 poz.542).
3/ rekomendacji w procesach projektowania lub budowy nowych obiektów, które potencjalnie mogą być przewidywane do wykazu obiektów IK.

[1] Ciągłość działania to „zdolność organizacji do przewidywania i reagowania na incydenty i zakłócenia w prowadzonej działalności w celu jej kontynuowania na akceptowalnym poziomie". Staniec, J. Zawiła – J. Niedźwiecki. red., 2008. Zarządzanie ryzykiem operacyjnym. Warszawa: C. H. Beck s.261.

1.2. Czego nie zawiera?

Załącznik nie jest dokumentem zawierającym komplet zasad i informacji na temat ochrony infrastruktury krytycznej. Nie zawiera szczegółowych instrukcji technicznych i procedur organizacyjnych, jednakże może posłużyć jako rozbudowana lista kontrolna do sprawdzenia przyjętych przez operatora IK wymagań stosowanych w procesach oceny ryzyka lub w procesach związanych z podnoszeniem standardów bezpieczeństwa IK.

Opis niektórych środków i zasad ochrony IK do konkretnych obszarów bezpieczeństwa zazwyczaj nie jest oczywisty i jednoznaczny (występują środki, które mogą być przypisane w różnych obszarach), a ponadto nie może być traktowany jako ostateczny.

NPOIK nie rekomenduje jednej metodyki oceny ryzyka, gdyż nie jest to możliwe w zróżnicowanym środowisku bezpieczeństwa.

1.3. Po co dokonujemy oceny ryzyka?

Zasada proporcjonalności i działań opartych na ocenie ryzyka jest jedną z kluczowych zasad dotyczących organizacji i funkcjonalności NPOIK. Oznacza ona, że wszelkie działania podejmowane w celu zapewnienia ochrony IK powinny być proporcjonalne do poziomu ryzyka zakłócenia jej funkcjonowania. Dotyczy to zarówno przyjętego modelu ochrony IK, jej rodzajów, a także użytych sił i środków (aktywów). Z punktu znaczenia tej zasady w praktyce funkcjonalności operatorów i koordynatorów systemów IK oznacza to podejmowanie działań w celu obniżenia ryzyka zakłócenia funkcjonowania IK oraz wskazywanie rekomendacji do ustalenia priorytetów działań.

Przed rozpoczęciem jakichkolwiek analiz związanych z ryzykiem (wpływem niepewności na cel lub postawione cele) należy mieć na uwadze trzy istotne zagadnienia.

Po pierwsze należy pamiętać, że szacowanie ryzyka jest pojęciem kompleksowym, na który zgodnie z normą PN-ISO 31000, składają się następujące procesy:

1) identyfikacja zagrożeń,
2) analizy ryzyk,
3) ewaluacja ryzyk.

Po drugie, NPOIK zwraca uwagę operatorom IK i koordynatorom systemów IK na istotę zarządzania ryzykami oraz współdziałanie zadaniowe wynikające z poziomu współzależności z koordynatorami innych systemów. Dla operatora IK zarządzanie ryzykami i bezpieczeństwem IK jest rekomendacją dla właściwego zarządzania organizacją, gdzie misja publiczna operatora IK rozumiana jako zbiór obowiązków i zadań do realizacji, może być nie zawsze tożsama z celami biznesowymi,

wynikającymi z udziału jego aktywów w jednolitym wykazie obiektów, instalacji, urządzeń i usług tworzących IK.

Po trzecie, analiza zagrożeń i ocena ryzyka a następnie postępowanie z ryzykiem jest procesem cyklicznym wynikającym z obowiązujących dla danej IK przepisów, norm, reżimów eksploatacyjnych lub jakościowych, a ponadto z polityki bezpieczeństwa operatora IK lub zaleceń koordynatora systemu IK, o ile takie zostały przyjęte i wdrożone.

Najlepszym wspólnym mianownikiem dla przeprowadzenia spójnej analizy zagrożeń i oceny ryzyka jest teoria zarządzania ciągłością działania organizacji, a dokładniej jej idea mówiąca o potrzebie niezakłóconej realizacji procesów krytycznych organizacji.

Bardzo dokładne poznanie, zrozumienie i opisanie specyfiki działania organizacji, zarówno w kontekście wewnętrznym jak i zewnętrznym powinno być działaniem priorytetowym, poprzedzającym bezpośrednio proces szacowania ryzyka. Oznacza to wymienienie i usystematyzowanie procesów realizowanych w organizacji. W praktyce w tym celu najczęściej rekomenduje się przeprowadzenie tzw. *analizy wpływu (zdarzenia) na biznes* (BIA – Business Impact Analysis), której efektem jest identyfikacja procesów krytycznych.

Aby w sposób efektywny i wartościowy oszacować ryzyko dla organizacji, należy stworzyć odpowiednie warunki dla całego procesu nazywanego zarządzaniem ryzykiem. Norma PN-ISO 31000 proponuje stworzenie tzw. struktury ramowej zarządzania zapewniającej podstawy i ustalenia, które zostaną wdrożone na każdym poziomie organizacji. Analiza BIA powinna zostać przeprowadzona dla każdego procesu realizowanego przez organizację z uwzględnieniem zależności i relacji pomiędzy poszczególnymi procesami.

Wynikiem analizy BIA powinny być:

- Ocena ryzyka związanego z przerwą w działaniu każdego procesu;
- Ocena strat finansowych i wizerunkowych związanych z przerwami w funkcjonowaniu danego procesu;
- Szacowanie czynników mogących doprowadzić do obniżenia ryzyka awarii w początkowym stadium;
- Szacowanie czasu niezbędnego do usunięcia skutków awarii oraz przywrócenia ciągłości działania;
- Określenie alternatyw, czynników, przy udziale których można utrzymać ciągłość działania;
- Określenie zasobów alternatywnych będących w dyspozycji organizacji;
- Określenie kosztów utrzymania ciągłości działania w zakresie potencjalnego wdrożenia każdego alternatywnego zasobu.

Podstawowe założenia i sposoby przeprowadzania analizy BIA i szacowania ryzyka przeprowadzane są zazwyczaj w następujących krokach:

Krok 1: identyfikacja procesów zachodzących w organizacji

Należy sporządzić usystematyzowaną listę procesów organizacji. Jej tworzenie rozpoczyna się przyjmując za „punkt początkowy" główne cele funkcjonowania organizacji. Ich konkretne brzmienie powinno być zapisane w aktach prawnych (np. statutach). Następnie określa się najistotniejsze procesy niezbędne do ich realizacji. Te z kolei powinno uszczegóławiać się dalej, rozpisując je na szereg podprocesów. Taką dekompozycję celów na procesy prowadzi się do momentu, w którym możliwe jest przedstawienie procesów głównych jako szeregu podstawowych podprocesów (prostych, jednoznacznych), dla których istnieje możliwość określenia konkretnych zasobów niezbędnych do ich realizacji.

1. Pierwszy cel główny mojej organizacji
    a. 1 proces główny
        i. Podproces 1
            1. Zasób 1
            2. Zasób 2
        ii. Podproces 2
            1. Zasób 1
            2. Zasób 3
    b. 2 proces główny
        i. Podproces 3
            1. Zasób 1
            2. Zasób 4
        ii. Podproces 4
            1. Zasób 2
            2. Zasób 4

Krok 2: określenie skutków – identyfikacja procesów krytycznych

Analiza BIA określa, które *procesy* są krytyczne na podstawie oszacowania wartości skutków w różnych odstępach czasu od chwili ich potencjalnego przerwania. Metoda postępowania sprowadza się do określenia jednolitej dla organizacji skali czasu (np. 1h, 12h, 24h, 48h, 7 dni, 14 dni) i przypisaniu każdemu *procesowi* wartości skutków w kolejnych przedziałach czasu. Np. określa się jakie straty finansowe i wizerunkowe poniesie organizacja w przypadku wystąpienia przerwy w realizacji misji publicznej, np. w wyniku przerwy w dostawach energii elektrycznej, która będzie trwała kolejno 1h, 12h, 24h, itd. Na potrzeby sporządzenia spójnej analizy, katalog rodzajów skutków powinien być jednakowy dla całej organizacji. Straty finansowe są wskazywane

najczęściej, niemniej jednak warto uwzględniać też straty wizerunkowe, czy zobowiązania prawne. Aby ułatwić zadanie identyfikacji procesów krytycznych można dla wszystkich rodzajów skutków opracować i opisać wspólną jakościową skalę. Wyboru czynności krytycznych dokonuje się poprzez analizę danych przedstawionych w formie tabelarycznej, w której dla każdego z procesów wskazane są poziomy wszystkich rodzajów skutków w różnych odstępach czasu.

	straty	1 h	3 h	6 h	12 h	24 h	3 dni	7 dni
podproces 1	finansowe							
	wizerunkowe							
podproces 2	finansowe							
	wizerunkowe							
podproces 2	finansowe							
	wizerunkowe							
podproces 3	finansowe							
	wizerunkowe							

Rysunek 1 Etapy tworzenia SOC - security operations center.

Krok 3: wskazanie zasobów

Podstawą szacowania ryzyka dla organizacji jest sprowadzenie go do ryzyka dla jej szeroko rozumianych zasobów. Można bowiem założyć, że ryzyko zakłócenia lub przerwania procesu jest sumą ryzyka niedostępności (w najprostszym ujęciu) wszystkich zasobów niezbędnych do jego realizacji. Kolejnym etapem jest więc określnie minimalnych zasobów niezbędnych do wykonania przede wszystkim krytycznych, zidentyfikowanych w kroku drugim, procesów. Identyfikacja zasobów powinna również przebiegać w systematyczny sposób. Dla przykładu można je wskazać i pogrupować w następujący sposób:

1) zasoby osobowe (kto jest potrzebny do realizacji danej czynności i jakie powinien posiadać kompetencje),
2) zasoby materiałowe (jakiego sprzętu, jakich materiałów używa do realizacji danej czynności),
3) zasoby informacyjne (co muszę wiedzieć, by wykonać czynność i jakimi narzędziami),
4) zasoby finansowe (ile personelu i jakich środków bezpośrednio potrzeba na realizację procesu).

Krok 4: identyfikacja zagrożeń i podatności

Przyjęcie zasady wskazywania konkretnych zasobów pozwala z dużo większą pewnością określać dla nich prawdopodobieństwo wystąpienia różnych zagrożeń. W tym kroku praca grupowa jest szczególnie istotna, gdyż samodzielnie trudno jest przewidzieć całe spektrum niebezpieczeństw. Pod dyskusję poddane powinny zostać wszelkie sugestie dotyczące zagrożeń. Należy współpracować z wieloma pracownikami komórek organizacji oraz wspierać się branżowymi ekspertami.

NPOIK określa podatność jako cechę umożliwiającą oddziaływanie zagrożenia na infrastrukturę. Podatność może być wykorzystana przez zagrożenie, które oddziałując na infrastrukturę, powoduje wystąpienie skutków w postaci zakłócenia funkcjonowania organizacji. Podatność nie musi być czynnikiem, który powoduje szkody, ale jest warunkiem lub zbiorem warunków, które mogą umożliwić zagrożeniu oddziaływanie na organizację, w tym na realizację najważniejszych procesów. Podatność może pochodzić ze źródeł zarówno wewnętrznych, jak i zewnętrznych i istnieć tak długo, dopóki nie wystąpią incydenty lub decyzje w samej organizacji, które spowodują jej zmniejszenie lub usunięcie. Wskazanie ich w etapie szacowania ryzyka jest najłatwiejsze, a jednocześnie w zarządzaniu ryzykiem jest nieuniknione i zarazem najbardziej zasadne, ponieważ podatności sugerują bezpośrednie sposoby na postępowanie z ryzykiem poprzez przygotowanie odpowiedzi – jakie zabezpieczenia należy wprowadzić w procesach zapobiegania zagrożeniom, reagowania na nie i ograniczania ich skutków?

Krok 5: przeanalizowanie ryzyka

Gdy w organizacji znana będzie lista procesów krytycznych oraz przedstawione zostaną możliwe straty wynikające z zakłócenia ich funkcjonowania należy dokonać analizy ryzyka. Zazwyczaj są to proste sumy i/lub iloczyny (np. prawdopodobieństwo x podatność x skutek) wymagające jednak określenia wartości ich składników lub czynników. Warto zwrócić w tym miejscu uwagę, że przyjęło się określać prawdopodobieństwo przerwania procesu, podczas gdy prawdopodobieństwo należy odnieść do wystąpienia zagrożeń dla zasobów wspierających procesy krytyczne. Szczególną uwagę należy zwrócić na te zasoby, które zostały zidentyfikowane w wielu procesach.

Zarówno ryzyko, jak i jego czynniki mogą być mierzone ilościowo lub jakościowo (np. opisowo). Kiedy jest to możliwe i uzasadnione ze względu na łatwość porównywania, należy stosować miary ilościowe. Prawdopodobieństwo i skutki powinny być obszarem oceny ilościowej i jakościowej, natomiast podatność jakościowej. W każdym przypadku przydatne jest stosowanie skalowania i wyboru matrycy ryzyka przez koordynatora systemu IK i operatora IK (przypisania określonym wartościom prawdopodobieństwa, podatności i skutków skal np. 1–5, 1-6, 1-7 lub innych

sprawdzonych i przejętych w procesie zarządzania bezpieczeństwem) z użyciem zakresów liczbowych lub szczegółowego opisu.

Krok 6: ewaluacja ryzyka

Ostatnim elementem procesu szacowania ryzyka jest jego ewaluacja. W języku potocznym, w najprostszym ujęciu, oznacza podjęcie decyzji o jego zaakceptowaniu lub nie. Dla każdego z rodzajów ryzyka przeanalizowanych i zwartościowanych w kroku 5, uwzględniając szeroki kontekst organizacji, jej cele, posiadane siły i środki, poglądy interesariuszy itp. należy zidentyfikować ryzyka we wszystkich obszarach bezpieczeństwa, w tym związanych z IK, które wymagają dalszych działań już nie w procesie szacowania a postępowania z ryzykiem (brak akceptacji ryzyka powinien oznaczać sporządzenie planu jego zmniejszenia). Do metod postępowania z ryzykiem należą, np. transfer (podzielenie się odpowiedzialnością za ryzyko, np. ubezpieczenia), unikanie (np. poprzez podjęcie decyzji o niekontynuowaniu działań powodujących ryzyko), redukcja (wprowadzanie zabezpieczeń – niwelowanie podatności) itp.

Wartość dodaną dla organizacji można uzyskać jedynie wtedy, kiedy przeprowadzone analizy zagrożeń i oceny będą szczegółowe i staranne, a ich autorzy będą posiadali stosowne kompetencje i doświadczenie w tego rodzaju przedsięwzięciach.

Od najwyższych władz organizacji oczekuje się zaangażowania w procesy zarządzania ryzykiem i zarządzania bezpieczeństwem w poszczególnych jego obszarach poprzez:

- ustalenie miar ryzyka oraz cech niezbędnych do ich oceny i kontroli,
- wskazanie gospodarzy ryzyka i koordynatora do zarządzania ryzykiem,
- zapewnienie zintegrowania wymagań w poszczególnych obszarach bezpieczeństwa z kompetencjami nadzorczymi dla tych obszarów oraz kompetencjami kluczowego personelu przeznaczonego do realizacji najważniejszych procesów, usług i wydzielonych zadań związanych z misją publiczną lub (i) biznesową,
- doskonalenie działań i metod oceny ryzyka, służących wzmacnianiu odporności przed zagrożeniami i promowaniu kultury bezpieczeństwa,
- utrzymanie zdolności do aktualizacji planów zarządzania ryzykiem i planów reagowania w ramach cyklicznej ich oceny lub według potrzeb wynikających ze zmiany wewnętrznego i zewnętrznego środowiska bezpieczeństwa,
- „przywództwo i zaangażowanie w kierowaniu i wspieranie personelu w przyczynianiu się do skuteczności SZCD[2] i jego promowanie ciągłego doskonalenia oraz wspieranie innych właściwych ról kierowniczych, aby podkreślić ich zaangażowanie wchodzące w zakres ich odpowiedzialności” [3].

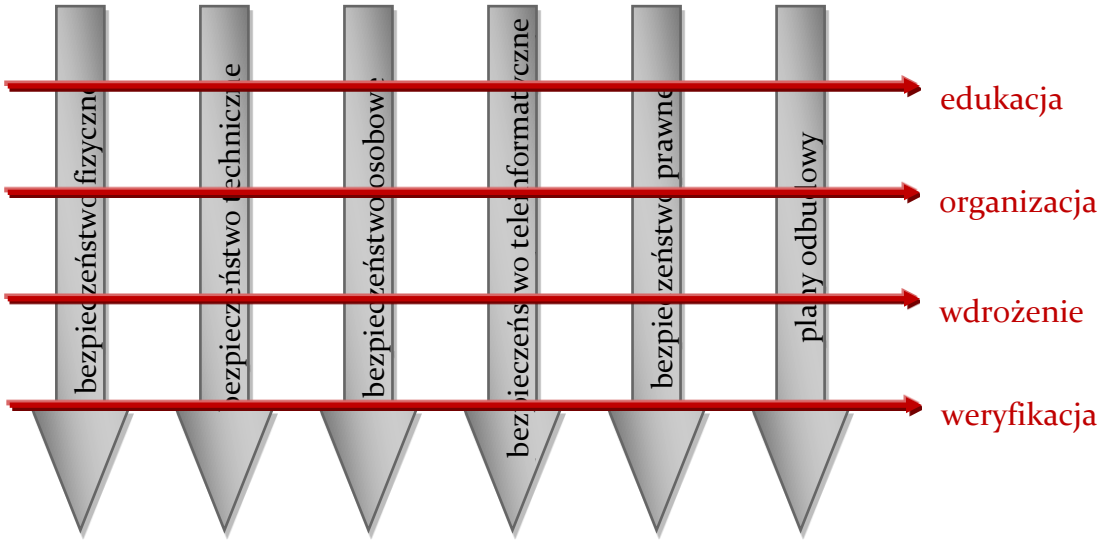
[2] SZCD - System Zarządzania Ciągłością Działania
[3] PN-ISO 22301:2019 Bezpieczeństwo powszechne - System zarządzania ciągłością działania – Wymagania, s.25-26

2. Rekomendacje i dobre praktyki ochrony IK

Należy pamiętać, że ochrony infrastruktury krytycznej nie można pojmować jako wyizolowanej, niezależnie funkcjonującej struktury, a aspekty bezpieczeństwa przenikają wszystkie, nawet z pozoru nieistotne, sfery działalności operatora IK.

Bez względu na to, jakie rodzaje ochrony zostaną wybrane i wprowadzone w życie przez operatora IK, należy mieć na uwadze że cztery elementy mają kluczowe znaczenie we wdrożeniu wszystkich ich rodzajów:

(1) Prowadzenie działań edukacyjnych.
(2) Właściwa struktura organizacyjna pionu lub pionów zarządzania bezpieczeństwem.
(3) Wybór strategii wdrożenia i jej monitoring.
(4) Weryfikacja przyjętych rozwiązań w drodze testów, ćwiczeń, audytów i kontroli oraz ich aktualizacja.



Rysunek 2 Działania przekrojowe w zakresie ochrony IK

2.1. Działania edukacyjne

Prowadzenie działań edukacyjnych i uświadamiających jest podstawowym, często niedocenianym i lekceważonym, sposobem na zapewnienie bezpieczeństwa IK. Działania te mają na celu przybliżenie zasad bezpieczeństwa i powszechną znajomość, zrozumienie, stosowanie i zapewnienie właściwego stosunku pracowników do zasad bezpieczeństwa.

Działania edukacyjne powinny być prowadzone dwuetapowo:

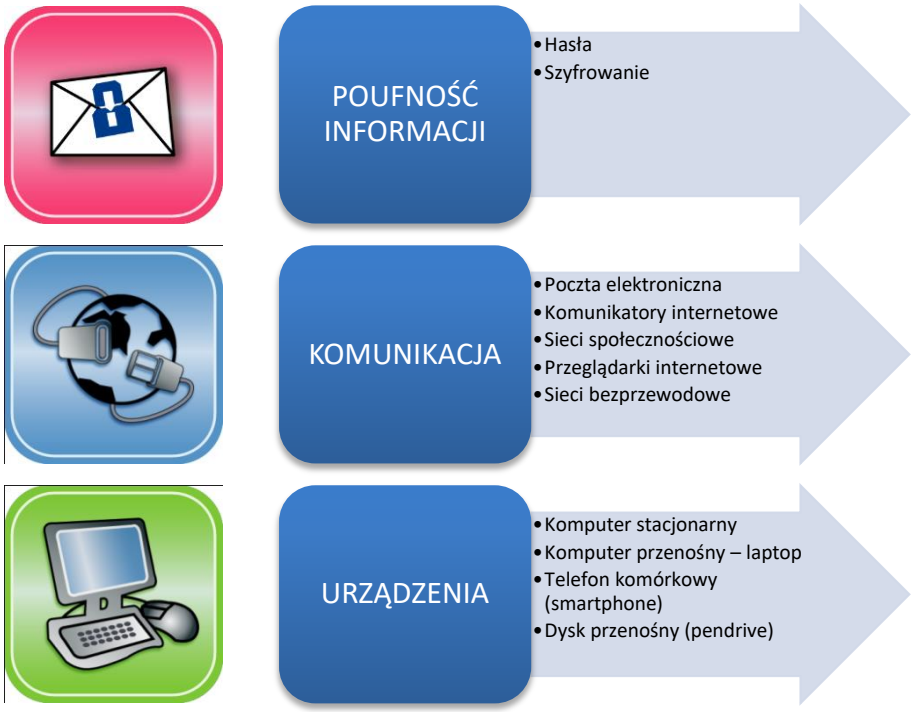
- ETAP I – podstawowe szkolenie bezpieczeństwa dla rozpoczynających pracę.
- ETAP II – stałe działania edukacyjno-uświadamiające dla pracowników.

Dla zdecydowanej większości personelu organizacji zasady bezpieczeństwa są obce, zazwyczaj stanowią utrudnienie w codziennej pracy, a ich poznawanie może być postrzegane jako nudne i niepotrzebne. Dlatego bardzo ważne jest przygotowanie odpowiedniego, praktycznego i atrakcyjnego programu uświadamiającego.

Elementami, które mogą się składać na taki program są:

- szkolenie podstawowe oparte o schemat:
  - przedstawienie studiów przypadku,
  - przekazanie wiedzy teoretycznej,
  - przeprowadzenie ćwiczeń i warsztatów oraz ich podsumowanie w formie uzgodnionych i wdrożonych wniosków i rekomendacji,
- przygotowanie i prezentacje krótkich filmów edukacyjnych odwołujących się do podstawowych zasad bezpieczeństwa lub bieżących wydarzeń przedstawiających zagrożenia. Filmy takie mogą być na przykład przedstawiane w intranecie organizacji,
- rozsyłanie informacji stanowiących alerty zagrożeń, np. na temat rozprzestrzeniającego się wirusa lub metody socjotechnicznej, która jest wykorzystywana przez przestępców komputerowych,
- rozsyłanie elektronicznego periodyku, który w krótkiej, atrakcyjnej i przejrzystej formie przypomina o zasadach bezpieczeństwa, w szczególności w odniesieniu do bieżących wydarzeń. Innym sposobem rozpowszechniania periodyku jest przedstawienie go w formie krótkiego filmu lub strony interaktywnej,
- uświadamianie wizualne przez rozwieszanie w organizacji plakatów na temat zasad bezpieczeństwa,
- konkurs (quiz) z nagrodami.

Trzy podstawowe obszary edukacji na przykładzie zapewnienia bezpieczeństwa teleinformatycznego wraz ze wskazaniem podobszarów szczególnej istotności:



Rysunek 3 Podstawowe obszary edukacji w zakresie zapewnienia bezpieczeństwa teleinformatycznego.

Działaniami edukacyjnymi należy objąć nie tylko personel, w którego zakresie obowiązków znajdują się zadania z zakresu ochrony IK, ale także ten niezwiązany bezpośrednio z tymi zadaniami. W ochronie IK powinni uczestniczyć wszyscy członkowie organizacji – w reakcji na niekorzystne zdarzenia działania wspomagające są równie ważne jak głównie wykonywane.

Działania edukacyjne są podstawowym elementem budowy kultury bezpieczeństwa organizacji. Kultura bezpieczeństwa oznacza współodpowiedzialność członków organizacji za bezpieczeństwo, przejawiające się zaangażowaniem i odpowiedzialnością za procesy dotyczące zarządzania ryzykiem, podatnością na materializację zagrożeń oraz zarządzania procesami reagowania i odtwarzania aktywów.

Bez zbudowania odpowiedniego wsparcia ze strony najwyższego kierownictwa trudno będzie osiągnąć zakorzenienie systemu bezpieczeństwa oraz uzyskać poprawę odporności organizacji na sytuacje materializacji zagrożeń, ale też w zakresie budowania stosownej gotowości personelu, wprowadzania zmian organizacyjnych, operacyjnych i technicznych oraz inwestycyjnych i innowacyjnych. Istota działań edukacyjno-szkoleniowych dla kierownictwa organizacji, polega na zbudowaniu świadomości znaczenia czynników zagrożeń i ryzyka oraz zdolności do określania zadań, uprawnień i delegowania odpowiedzialności za wdrażanie, utrzymanie i doskonalenie mechanizmów zapobiegania zagrożeniom na wszystkich poziomach struktury organizacyjnej operatora IK. Od najwyższego kierownictwa, tj. zarządu i kadry kierowniczej, oczekuje się wysokiej świadomości i kompetencji w zakresie zarządzania procesami oceny ryzyka oraz ochrony i wzmacniania odporności dla usług kluczowych w odniesieniu do zarządzania bezpieczeństwem w poszczególnych jego obszarach poprzez zapewnienie, że:

- polityka bezpieczeństwa jest ustanowiona i aktualna oraz spójna dla wszystkich dziedzin bezpieczeństwa, a ponadto jest zgodna z kierunkiem strategicznym organizacji i danego sektora IK w państwie,
- poszczególne obszary bezpieczeństwa są zintegrowane z kompetencjami nadzorczymi dla tych obszarów oraz kompetencjami kluczowego personelu przeznaczonego do realizacji najważniejszych procesów, usług lub wydzielonych zadań w danej dziedzinie bezpieczeństwa,
- funkcjonują mechanizmy ciągłego doskonalenia działań i metod oceny ryzyka, służące wzmacnianiu odporności infrastruktury i ochrony usług kluczowych oraz promowaniu kultury bezpieczeństwa wśród wszystkich pracowników.

Kluczowym celem edukacji zarządu oraz kadry kierowniczej, a także właścicieli lub koordynatorów ryzyka powinna być budowa zdolności organizacji do zapewnienia funkcjonalności i ciągłości działania w sytuacjach kryzysowych. Ważnym elementem edukacji jest znaczenie kontroli ryzyka, które warto poznawać, mierzyć i porównywać w procesach planistycznych, jak również podczas testów, ćwiczeń i w procesach audytowania, w odniesieniu do przyjętych wymagań przez operatora IK.

W procesach edukacyjnych warto zachęcać kierownictwo do udziału w bezpośrednich działaniach promujących Plan Ochrony Infrastruktury Krytycznej i system zarządzania bezpieczeństwem w organizacji na zasadzie, że „przykład idzie z góry", a także do przywiązywania wagi do znaczenia komunikacji w tej sprawie z załogą.

2.2. Struktura organizacyjna

Osiągnięcie i utrzymanie odpowiedniego poziomu bezpieczeństwa wiąże się ze stworzeniem odpowiedniej struktury organizacyjnej, składającej się ze stanowisk zaangażowanych w pracę na rzecz bezpieczeństwa IK. W strukturze organizacji może funkcjonować jedna komórka odpowiedzialna za jej bezpieczeństwo (wszystkie rodzaje zapewnienia bezpieczeństwa) lub zadania z zakresu bezpieczeństwa mogą być przydzielone do różnych komórek zgodnie z ich kompetencjami, np. do spraw kadrowych (zapewnienie bezpieczeństwa osobowego), teleinformatyki (zapewnienie bezpieczeństwa teleinformatycznego) czy utrzymania infrastruktury (zapewnienie bezpieczeństwa technicznego).

Obydwa modele mają swoje wady i zalety.

Jedna komórka odpowiedzialna za bezpieczeństwo	
zalety	wady
• duża możliwość koordynacji • jednoosobowa odpowiedzialność • integracja wszystkich aspektów bezpieczeństwa w jednej komórce organizacyjnej • niezależność	• mniejszy wgląd w działania innych komórek organizacyjnych i konieczność zbierania szczegółowych informacji o wszelkich ich działaniach • konieczność włączenia w strukturę komórki specjalistów w zakresie każdego rodzaju ochrony • zamknięcie się we własnym obszarze zadaniowym

Tabela 1 Przykładowe zestawienie wad i zalet – w jednej komórce

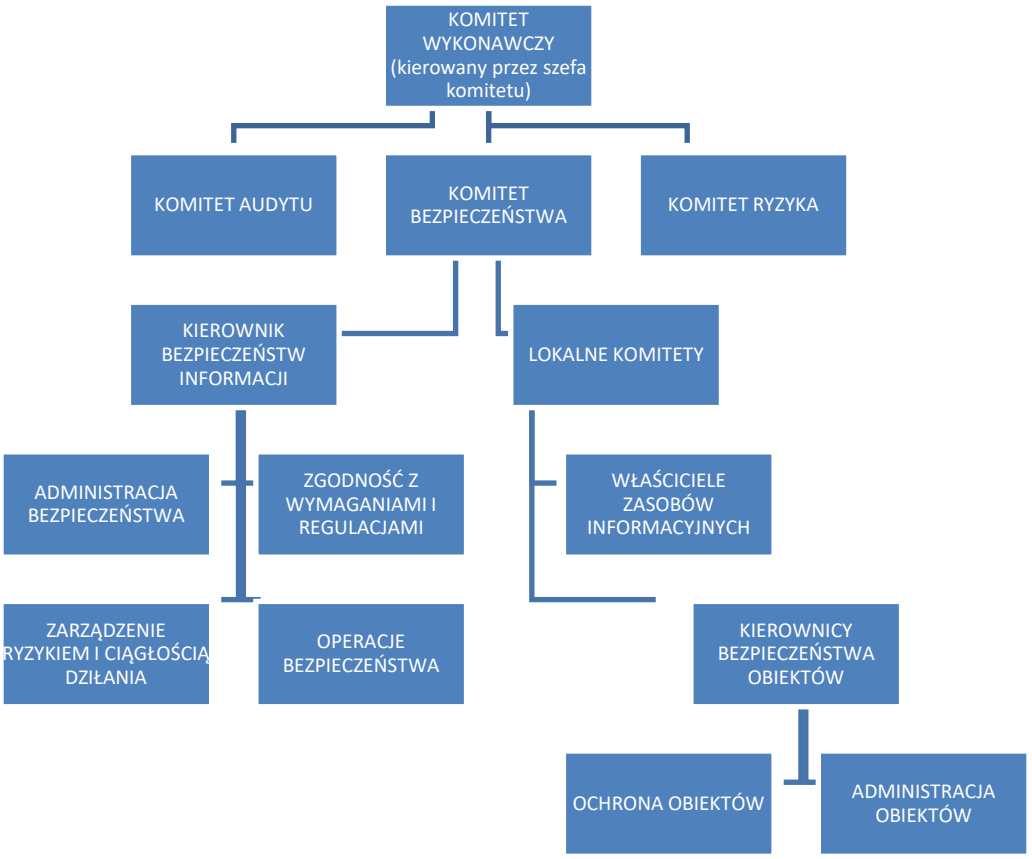
Zadania z zakresu bezpieczeństwa w różnych komórkach organizacyjnych	
zalety	**wady**
• wysoka specjalizacja personelu • inforamcje o działaniach mogących dotyczyć bezpieczeństwa są dostępne wewnątrz komórki • większe zaufanie do pracowników bezpieczeństwa	• rozproszenie informacji z zakresu bezpieczeństwa pomiędzy wiele komórek organizacyjnych • konieczność koordynacji działań wielu komórek organizacyjnych • rozproszenie odpowiedzialności, zwłaszcza w obszarach nakładających się kompetencji

Tabela 2 Przykładowe zestawienie wad i zalet – w różnych komórkach

Wybór konkretnego modelu zależy od przyjętego w organizacji stylu zarządzania, wymagań i możliwości organizacyjno-finansowych.

Niezależnie od tego, skuteczność funkcjonowania wybranego modelu wymaga ścisłej współpracy między wszystkimi komórkami organizacyjnymi. Pomocne w tym zakresie może być wykorzystanie tzw. mostów, czyli osób, które łączą kompetencje lub posiadają wiedzę i doświadczenie w dziedzinie bezpieczeństwa i wybranego fragmentu działalności organizacji.

Jedną z metod podjęcia decyzji o kształcie struktury organizacyjnej jest przyjęcie istniejących modeli struktur organizacyjnych, np. w zakresie zapewnienia bezpieczeństwa teleinformatycznego zastosowanie zabezpieczeń zdefiniowanych w normie PN-ISO/IEC 27002:2017.

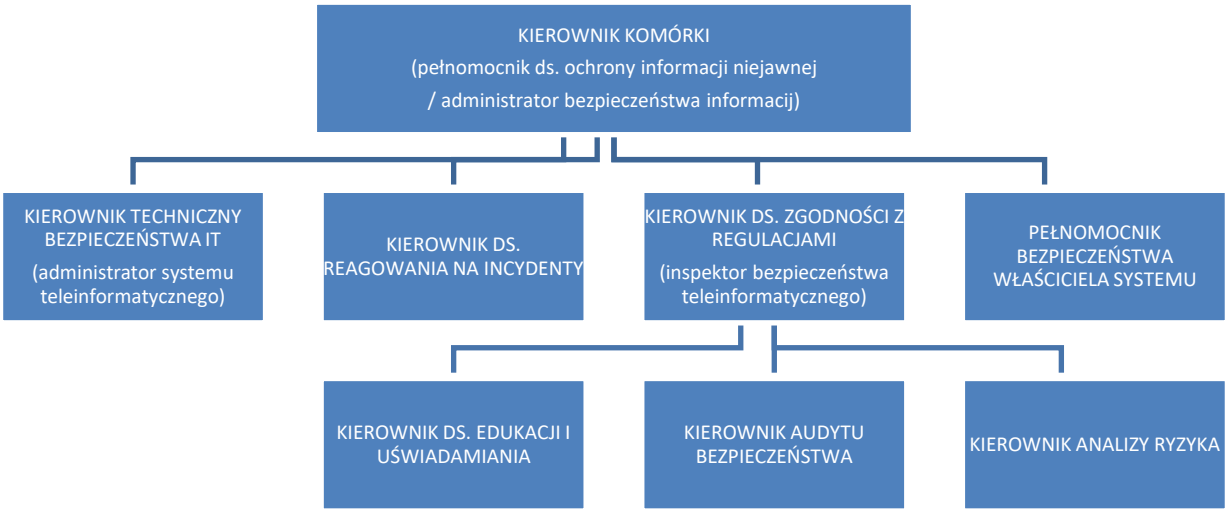


Rysunek 4 Przykładowa struktura organizacyjna pionu bezpieczeństwa teleinformatycznego.

Powyższa struktura jest zalecana dla najbardziej rozbudowanych organizacji, posiadających również swoje regionalne przedstawicielstwa. Jest ona wskazana dla tych organizacji, które chcą wdrożyć kompletny System Zarządzania Bezpieczeństwem Informacji zgodnie z ISO/IEC 27001. Prostszy i bardziej praktyczny model oparty jest o dwie kategorie stanowisk (realizowanych funkcji): obligatoryjne i fakultatywne.

Najlepszym rozwiązaniem jest jednak połączenie obu powyższych systemów. Realizuje się to poprzez zarządzanie bezpieczeństwem IK w scentralizowanej komórce, a zaadresowanie działań związane z wdrażaniem zabezpieczeń, do właściwych komórek organizacyjnych.

W grupie stanowisk obligatoryjnych uwzględniono te stanowiska, które wynikają z dwóch ważnych ustaw związanych z ochroną informacji, tj. ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.



Rysunek 5 Struktura organizacyjna komórki zapewniającej bezpieczeństwo teleinformatyczne.

Poniższa tabela zawiera opis poszczególnych stanowisk wraz ze wskazaniem ich obligatoryjności lub fakultatywności, wskazaniem, któremu ze stanowisk wymaganych w wspomnianych ustawach odpowiada dane stanowisko, oraz wskazaniem, które z innych stanowisk przejmuje zadania danej funkcji w przypadku decyzji o rezygnacji z jej istnienia w strukturze organizacyjnej[4].

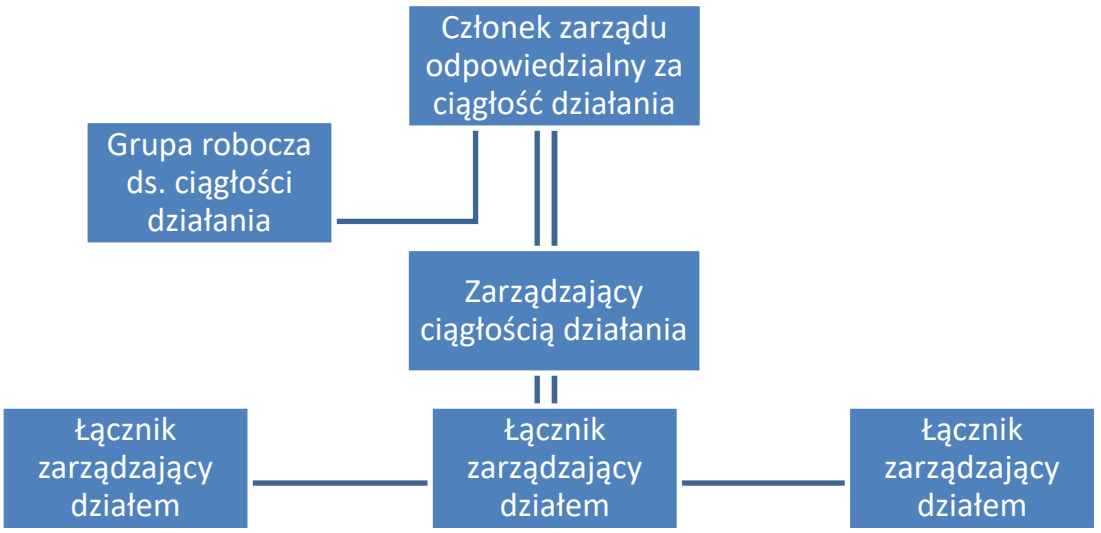
Tabela 3 Opis stanowisk wynikających z właściwych ustaw

STANOWISKO	STANOWISKO WYMAGANE W USTAWIE	ZADANIA	STANOWISKO PRZEJMUJĄCE ZADANIA
KIEROWNIK PIONU BEZPIECZEŃSTWA **(obligatoryjne)**	Tak	Koordynacja działań związanych z całościowym zapewnieniem wymaganego bezpieczeństwa teleinformatycznego organizacji	N/D
KIEROWNIK TECHNICZNY BEZPIECZEŃSTWA IT **(obligatoryjne)**	Tak	Koordynacja działań technicznych związanych z całościowym zapewnieniem bezpieczeństwa teleinformatycznego organizacji	N/D
KIEROWNIK DO SPRAW REAGOWANIA NA INCYDENTY	Nie	Koordynacja obsługi zgłoszeń związanych z naruszeniem bezpieczeństwa teleinformatycznego organizacji	Kierownik ds. zgodności z regulacjami

[4] W celu zapoznania się ze szczegółowym zakresem stanowisk wskazanych w ustawie o ochronie informacji niejawnych oraz ustawie o ochronie danych osobowych należy sięgnąć do treści tychże ustaw.

STANOWISKO	STANOWISKO WYMAGANE W USTAWIE	ZADANIA	STANOWISKO PRZEJMUJĄCE ZADANIA
KIEROWNIK DO SPRAW ZGODNOŚCI Z REGULACJAMI **(obligatoryjne)**	Tak	Nadzór i kontrola nad prawidłowym zaprojektowaniem, wdrożeniem i utrzymaniem zasad i mechanizmów zapewniających bezpieczeństwo teleinformatyczne	N/D
PEŁNOMOCNIK BEZPIECZEŃSTWA WŁAŚCICIELA SYSTEMU	Nie	Reprezentacja właściciela systemu, w celu kontroli tego, aby zasady bezpieczeństwa nie naruszały kluczowych funkcji prawidłowego funkcjonowania systemu zgodnie z zapotrzebowaniem biznesowym	Kierownik ds. zgodności z regulacjami
KIEROWNIK DO SPRAW EDUKACJI I UŚWIADAMIANIA	Nie	Prowadzenie stałych działań uświadamiających i edukacyjnych dla wszystkich szczebli pracowniczych, z głównym celem uświadomienia istotności zasad bezpieczeństwa, najważniejszych zagrożeń i sposobów reagowania w przypadku ich wystąpienia	Kierownik pionu bezpieczeństwa
KIEROWNIK AUDYTU BEZPIECZEŃSTWA	Nie	Przeprowadzanie audytu zgodności stanu rzeczywistego z przyjętymi zasadami bezpieczeństwa	Kierownik ds. zgodności z regulacjami
KIEROWNIK ANALIZY RYZYKA	Nie	Przeprowadzanie analizy ryzyka dla wszystkich istniejących i nowo pojawiających się zagrożeń	Kierownik ds. zgodności z regulacjami

Innym przykładem możliwej do wykorzystania (adaptacji) struktury organizacyjnej jest proponowana w normie BS 25999 (zastąpionej przez normę ISO 22301:2020) dotyczącej zarządzania ciągłością działania organizacji.



Rysunek 6 Przykładowa struktura organizacji ciągłości działania.

W skład grupy roboczej ds. ciągłości działania powinna wchodzić kadra kierownicza poszczególnych komórek organizacyjnych. Zadaniem tej grupy jest:

- kontrola alokacji zasobów,
- ustanawianie priorytetów organizacji w zakresie ciągłości działania,
- ustanawianie strategii działań w zgodzie z celami organizacji,
- rozpowszechnienie znaczenia ciągłości działania w organizacji.

Łącznicy zarządzający działami są odpowiedzialni za wdrożenie procesów związanych z ciągłością działania w podległych im obszarach zadaniowych – to zadanie jest najczęściej dodatkowo przypisane kierującym na poziomie operacyjnym. Skuteczne wprowadzanie tego modelu wymaga, by wszyscy pracownicy rozumieli cel swoich działań w zakresie ciągłości działania i ich znaczenia dla organizacji.

Bez względu na przyjęty model w strukturach organizacji komórka (komórki) do spraw bezpieczeństwa IK powinna zostać umieszczona tak, aby miała zapewnioną odpowiednią pozycję, odzwierciedlającą wagę zasad bezpieczeństwa dla organizacji. Równie ważne jest zapewnienie zarządzającemu bezpieczeństwem i jego zespołowi niezależności wobec innych komórek organizacji. Interesy tych komórek organizacyjnych często są sprzeczne i nieodpowiednio ważne traktowanie zasad bezpieczeństwa na rzecz funkcjonalności i łatwości osiągania celów biznesowych i statutowych może doprowadzić do poważnego zakłócenia funkcjonowania organizacji. Działania na rzecz bezpieczeństwa IK powinny być fragmentem pracy i odpowiedzialności każdego członka organizacji.

2.3. Strategia wdrożenia

Wdrożenie zasad ochrony IK w organizacji nie jest procesem krótkim i łatwym. Oczywiście wiele zależy od wielkości organizacji, dotychczasowego poziomu organizacji bezpieczeństwa oraz przygotowania personelu do takiego wdrożenia. Dlatego warto przeanalizować koncepcję etapowego wdrożenia tych zasad, tak aby cały proces następował systematycznie, w sposób uporządkowany i napotykał na jak najmniej przeszkód. Trzy najpoważniejsze przeszkody we wdrożeniu zasad ochrony to:

- opór pracowników,
- koszty utrzymania,
- koszty implementacji.

Odpowiedni poziom tych przeszkód sprawia, że zasady te są łatwiejsze lub trudniejsze do wdrożenia. Jeśli przypiszemy poziomowi trudności i kosztów wdrożenia miary w skali 1–3 (1 – największy opór, największe koszty, 3 – najmniejszy opór, najmniejsze koszty), to możemy przyjąć, że wskaźnik ŁW (łatwość wdrożenia) możemy obliczyć jako sumę tych ocen:

$$ŁW = Op + Ki + Ku - 3$$

gdzie:

Op – wartość poziomu oporu pracowników,

Ki – wartość kosztów implementacji,

Ku – wartość kosztów utrzymania.

Odejmujemy wartość 3 jako wartość, którą zawsze przyjmuje wskaźnik jako minimum. W ten sposób wartościom wskaźnika nadajemy bardziej przejrzyste wartości w skali 0–6.

Dodatkowo proponowane zasady bezpieczeństwa posiadają różny poziom skuteczności, który można nazwać WE (wskaźnik efektywności). Możemy je również ocenić w skali odpowiadającej wskaźnikowi ŁW, czyli będą one przyjmowały wartości z przedziału 0–6 (0 – najmniej efektywne, 6 – najbardziej efektywne).

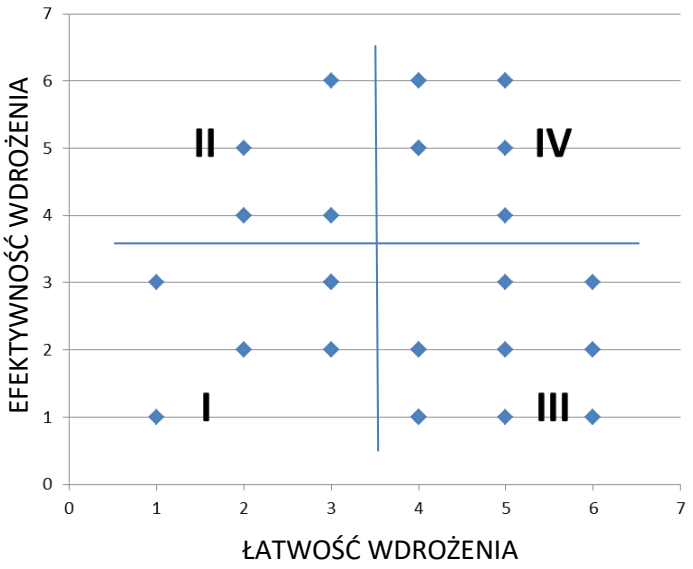
W oparciu o powyższe wartościowanie jesteśmy w stanie stworzyć graficzną reprezentację wartości wskaźników dla wszystkich proponowanych zasad i technik bezpieczeństwa. Dzieląc obszar pokazujący poziom efektywności i łatwość wdrożenia na ćwiartki, otrzymujemy przypisanie poszczególnych zasad bezpieczeństwa do czterech obszarów:

I – zasady mało efektywne i trudne we wdrożeniu,

II – zasady efektywne, ale trudne we wdrożeniu,

III – zasady mało efektywne, ale łatwe we wdrożeniu,

IV – zasady efektywne i łatwe we wdrożeniu.



Rysunek 7 Cztery obszary przypisania zasad bezpieczeństwa.

Taki podział pozwoli nam zidentyfikować poszczególne fazy, przypisać do nich zasady i opracować wdrożenie, np. trójetapowe:

- Etap I – na tym etapie następuje wdrożenie zasad łatwych we wdrożeniu o wysokiej efektywności,
- Etap II – na tym etapie następuje wdrożenie zasad łatwych we wdrożeniu o niskiej efektywności i trudnych we wdrożeniu o wysokiej efektywności,
- Etap III – na tym etapie następuje wdrożenie zasad trudnych we wdrożeniu o niskiej efektywności.

Ocena zastosowanych zasad z punktu widzenia trudności implementacji nie jest zadaniem łatwym. Nie ma przyjętych jednoznacznych norm dla takiej oceny. Może ona zależeć od indywidualnych cech środowiska, w którym zasady te są implementowane, i od osób za to odpowiedzialnych. Niemniej jednak doświadczenia wskazują na pewne uniwersalne cechy tych zasad, które z dużą dozą prawdopodobieństwa pozwalają na ocenę tych zasad. Poniżej pokazano, jak może wyglądać przykładowa tabela oceniająca

wskaźniki łatwości i efektywności wdrożenia oraz końcowe przypisanie danej zasady bezpieczeństwa do etapu wdrożenia.

Tabela 4 Przykładowa tabela oceny wdrażanych zasad bezpieczeństwa

ELEMENTY SYSTEMU ZAPEWNIENIA BEZPIECZEŃSTWA	WSKAŹNIK ŁATWOŚCI WDROŻENIA	WSKAŹNIK EFEKTYWNOŚCI	ETAP WDROŻENIA
OGÓLNE			
Stanowiska i zakres odpowiedzialności			
Edukacja i uświadamianie			
…			
BEZPIECZEŃSTWO FIZYCZNE			
Wydzielenie stref bezpieczeństwa			
Patrole wewnątrz obiektu			
…			
BEZPIECZEŃSTWO TECHNICZNE			
Własne ujęcie wody			
Generatory prądotwórcze			
BEZPIECZEŃSTWO TELEINFORMATYCZNE			
Bezpieczeństwo oprogramowania			
Ochrona stacji roboczych			
BEZPIECZEŃSTWO OSOBOWE			
Wizualna identyfikacja pracowników organizacji			
Kontrola dostępu do stref bezpieczeństwa			
PLAN CIĄGŁOŚCI DZIAŁANIA I ODBUDOWY			
Testowanie planu			

2.4. Weryfikacja przyjętych rozwiązań i ich aktualizacja

Podjęte przez organizację działania w celu zapewnienia bezpieczeństwa IK w danym obszarze powinny zostać zweryfikowane. Weryfikacji podlega:

- adekwatność przyjętych założeń i planów w stosunku do celów i priorytetów ochrony IK,
- poprawność identyfikacji kluczowych dla IK procesów i usług ich wspierających,
- prawidłowość przypisania ról i zakresu odpowiedzialności,
- efektywność wdrożonych rozwiązań w stosunku do poziomu ryzyka zakłócenia funkcjonowania IK,
- skuteczność koordynacji i zarządzania niekorzystnym zdarzeniem,
- przydatność procedur i planów,
- sprawność procesu aktualizacji planów i implementacji wniosków z incydentów do tych planów.

Weryfikacja obejmuje:

- ćwiczenia,
- procesy audytowe,
- samoocenę,
- zarządzanie zgodnością.

2.4.1. Ćwiczenia

Ćwiczenia są jedynym sposobem, poza działaniem w warunkach rzeczywistych zagrożeń, praktycznej weryfikacji działań podjętych w zakresie ochrony IK. Dają możliwość rozwoju pracy zespołowej, podniesienia kompetencji, wzrostu zaufania do własnych możliwości oraz poziomu wiedzy. Ćwiczenia są także okazją do przekonania kadry organizacji do celowości przygotowań na wypadek zagrożeń – pokazują jakie problemy mogłyby w organizacji wystąpić, gdyby organizacja nie była przygotowana na wystąpienie takich problemów.

Ćwiczenia powinny obejmować swoim zakresem wszystkie wdrożone rodzaje ochrony IK (niekoniecznie w tym samym czasie) oraz przygotowanie osób, którym przypisano role i obowiązki w ramach ochrony IK.

Zachowanie realizmu ćwiczeń jest jednym z podstawowych wymogów ich prowadzenia. Należy jednak pamiętać, że nie powinno ono wywołać negatywnych skutków dla IK i organizacji, dlatego należy planować je w taki sposób, by zminimalizować ryzyko rzeczywistego zakłócenia IK jako ich rezultatu.

Każde ćwiczenie powinno mieć jasno zdefiniowane cele i być dokładnie zaplanowane. Po zakończeniu ćwiczenia należy dokonać analizy sprawdzającej osiągnięcie celów. Powinien także zostać sporządzony raport zawierający rekomendacje zmian oraz harmonogram ich

wdrażania.

Skala i złożoność ćwiczeń powinny być dopasowane do wielkości organizacji i celów w zakresie ochrony IK. Skala i złożoność procesów organizacji powinny być brane pod uwagę również określając częstotliwość ćwiczeń – wykonanie ćwiczeń jeden raz nie pozwala na utrzymanie sprawności organizacji oraz nie bierze pod uwagę zmian zachodzących w organizacji. Tylko regularnie powtarzane ćwiczenia są formą potwierdzenia utrzymywanej efektywności przyjętych rozwiązań.

2.4.2. Procesy audytowe

Narzędziem stosowanym do oceny stanu systemu ochrony IK jest audyt. Jest on jednym z ważniejszych elementów tego systemu. Jako proces sprawdzający, czy podjęte działania są zgodne z założeniami i czy założenia są skutecznie wdrażane, jest materiałem służącym do uzyskania informacji na temat aktualnego poziomu ochrony, jego stanu w odniesieniu do funkcjonujących regulacji prawnych oraz powszechnych standardów bezpieczeństwa. Jednym z celów audytu jest podniesienie poziomu bezpieczeństwa i zwiększenie efektywności zastosowanych rozwiązań przez ujawnienie zasobów niewykorzystanych bądź wykorzystanych niewłaściwie oraz potencjalnych luk i podatności systemu.

Prawidłowo przeprowadzony audyt powinien udzielić odpowiedzi na następujące pytania:

- Czy system ochrony IK funkcjonuje zgodnie z przyjętymi zasadami?
- Czy są dowody (zapisy) potwierdzające funkcjonowanie systemu?
- Czy system jest adekwatny do zagrożeń i chronionych wartości?
- Czy system ochrony IK działa poprawnie i może skutecznie zareagować na niekorzystne zdarzenia?
- Jak określono rodzaje zagrożeń, które mogą zaistnieć w związku z zadaniami i funkcjami IK?
- Jakie istniejące czynniki wpływają potęgująco oraz neutralizująco na zagrożenia z uwzględnieniem osób, miejsc i czasu ich występowania?
- Jakie sposoby i środki zaradcze należy zastosować, aby zneutralizować zagrożenia oraz zmniejszyć podatność IK na te zagrożenia?

W procesie audytowania można stosować następujące formy:

- skrócony audyt bezpieczeństwa – w odniesieniu do obiektu, procesu i całej organizacji,

- rozszerzony audyt bezpieczeństwa – odnoszący się do obiektu i procesu przeprowadzanego na podstawie audytu skróconego, gdy któryś z ocenianych parametrów nie osiągnął pożądanego poziomu,
- pełny audyt bezpieczeństwa – proces kompleksowy oceniający organizację.

Audyty powinny być przeprowadzane w ustalonych odstępach czasu, a ich wyniki przedstawiane w formie raportu kierownictwu organizacji. Procesy audytowe powinny być prowadzone w sposób obiektywny i niezależny, w tym celu można skorzystać z kompetentnych osób z lub spoza organizacji. Tę dobrą praktykę należy stosować też do procesu samooceny.

W niektórych sytuacjach uzasadnione jest wykorzystanie audytu zewnętrznego do przeprowadzenia weryfikacji przyjętych rozwiązań (brak kompetencji po stronie organizacji, uzasadniona potrzeba niezależnej oceny, itp.) W takich przypadkach, należy pamiętać o:

- umowie na usługę gwarantującą poufność informacji zebranych przez audytorów w czasie ich prac,
- monitorowaniu dostępu do krytycznych obiektów weryfikowanych przez audytorów (na przykład, weryfikując serwerownię audytorzy powinni być poddani tym samym restrykcjom co inne osoby, którym czasowo udziela się dostępu do chronionych pomieszczeń),
- ustaleniu zasad dostępu do kluczowych dokumentów organizacji, tj. jakiego rodzaju notatki z audytu mogą być sporządzane, jaka dokumentacja przekazana w czasie audytu może być wynoszona poza miejsce audytu (praca własna audytorów poza miejscem prowadzenia audytu), zasady kwitowania przekazania i odbioru dokumentów.

Osoby prowadzące audyt muszą posiadać ważne poświadczenia bezpieczeństwa wydane przez uprawnione do tego służby, odpowiednie do stopnia klauzuli tajności kontrolowanych dokumentów.

2.4.3. Zarządzanie zgodnością (z ang. compliance)

Zarządzanie zgodnością to zbiór procesów mających na celu zapewnienie ciągłej zgodności stanu aktywów (w tym aktywów IK) z obowiązującymi u operatora IK politykami bezpieczeństwa. W odróżnieniu od projektów i programów, które nieodłącznie wiążą się ze zmianami w środowisku bezpieczeństwa, zadaniem zarządzania zgodnością jest utrzymanie stanu zapewniającego oczekiwany poziomu bezpieczeństwa (zapobieganie zmianom niekontrolowanym lub szkodliwym). Procesy zarządzania zgodnością są powiązane z innymi procesami zarządzania aktywami

(zarządzania majątkiem) i częściowo wykorzystują te same rozwiązania np. wspólne bazy danych.

W celu sprawnego zarządzania zgodnością, w coraz większym stopniu wykorzystywane są wyspecjalizowane narzędzia informatyczne do monitorowania zgodności stanu aktywów w trybie on-line, w tym również aktywów stanowiących wyspecjalizowane rozwiązania przemysłowych systemów sterowania. Narzędzia te, w powiązaniu z innymi rozwiązaniami bezpieczeństwa stanowią źródło informacji zarządczej stanowiącej podstawę dla działań w obszarze poprawy bezpieczeństwa.

Bezpieczeństwo nie powinno stanowić obszaru kształtującego przewagę konkurencyjną. W rezultacie, wśród trendów w obszarze zarządzania zgodnością zauważalne stają się działania społeczności skupiających specjalistów z poszczególnych sektorów, którzy podejmują wspólne próby opracowania wymagań bezpieczeństwa, w najlepszym możliwym stopniu uwzględniających wymagania danego sektora. Dokumenty publikowane przez te społeczności stanowią cenne źródło wiedzy na temat najlepszych praktyk bezpieczeństwa.

2.5. Zapewnienie bezpieczeństwa fizycznego

Zapewnienie bezpieczeństwa fizycznego to zespół działań proceduralnych, organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie działań osób, które w sposób nieautoryzowany podjęły próbę dostania się lub znalazły się na terenie IK. Składają się na nie m.in. bezpośrednia ochrona fizyczna oraz zabezpieczenia techniczne (elektroniczne i mechaniczne).
Bezpośrednia ochrona fizyczna oraz zabezpieczenie techniczne realizuje swoje cele m.in. poprzez:

- Prewencję
- Wykrycie
- Przekazanie informacji o wykryciu intruza (alarmowanie)
- Opóźnienie intruza w dotarcia do stref chronionych
- Reakcje/Interwencję za zdarzenie

Oprócz wymienionych funkcji system bezpieczeństwa fizycznego spełniać może funkcje odstraszania napastnika, np. na etapie prewencji (np. tablice informujące), alarmowania (sygnalizatory zewnętrzne) oraz interwencji (wezwanie do zachowania zgodnego z prawem). Częściowo realizowana jest także funkcja dowodowa w przypadku systemów dozoru wizyjnego.

Zaznaczyć należy, że żadne działania zmierzające do zapewnienia bezpieczeństwa fizycznego nie zapewnią całkowitego bezpieczeństwa. Środki ochronne zwiększają jedynie prawdopodobieństwo skutecznego przeciwdziałania.

Implementacja systemu bezpieczeństwa fizycznego powinna przebiegać w następujących krokach:

- ustalenie chronionych podmiotów (elementów),
- przyjęcie podstawowych założeń projektowych[5] dla systemu (ustalenie kto może być potencjalnym atakującym i jego charakterystyki),
- ocena koniecznych czasów opóźnień dla przewidywanych scenariuszy ataku,
- ustalenie chronionych stref i zasad dostępu do nich,
- ustalenie technicznych środków wspomagających (zabezpieczenia technicznego),
- opracowanie procedur pracy systemu (w tym ludzi),
- zainstalowanie i konfiguracja elementów systemu,
- test systemu,
- przegląd procedur,

[5] W literaturze anglojęzycznej występują jako *design basis threat (DBT).*

- test całego systemu bezpieczeństwa,
- systematyczne przeglądy systemu.

Przyjęcie założeń dotyczących wiedzy, umiejętności, wyposażenia oraz determinacji potencjalnych intruzów jest kluczowym elementem projektowania systemu bezpieczeństwa fizycznego. Dobrą techniką jest przeanalizowanie kto może być zainteresowany nieuprawnionym dostępem do chronionego zasobu. Rozpatrujemy tu głównie atrakcyjność chronionego elementu dla określonych grup intruzów.

Przykładowo wejściem na chronioną hałdę może być zainteresowany paralotniarz albo złodziej składowanych na hałdzie materiałów (np. opału) a dostępem do informacji dotyczących bezpieczeństwa państwa o klauzuli „ściśle tajne" wywiad obcego państwa.

Fizyczne ataki na infrastrukturę krytyczną oraz incydenty z jej udziałem nie należą wcale do rzadkości. Poniżej kilka przykładów naruszeń związanych z przełamywaniem systemu bezpieczeństwa fizycznego.

Tabela 5 Przykładowe ataki na infrastrukturę krytyczną

Rodzaj naruszenia	Czas/miejsce	Opis
Zamach terrorystyczny	19.04.1995 Oklahoma City USA	Eksplozja ciężarówki wypełnionej 2300 kg ANFO[6] przed budynkiem federalnym w Oklahoma City. Zginęło 168 osób, ponad 680 zostało rannych. Zamachu dokonał związany z prawicowymi ekstremistami Timothy McVeigh.
Zamach terrorystyczny	24.02.2006 Abqaiq Arabia Saudyjska	Próba ataku na największą na świecie rafinerię ropy. Napastnicy przedarli się przez zewnętrzne ogrodzenie, wysadzając jeden z towarzyszących im samochodów. Pozostałe samochody zamachowców eksplodowały po ostrzelaniu przez strażników przed pokonaniem kolejnego ogrodzenia. Napastnicy byli dobrze przygotowani, uzbrojeni i wyposażeni. Wiadomości o ataku spowodowały wzrost cen ropy naftowej na rynku.

[6] ANFO (Ammonium Nitrate Fuel Oil) – materiał wybuchowy otrzymywany przez nasączanie azotanu amonu (NH_4NO_3) paliwami płynnymi.

Rodzaj naruszenia	Czas/miejsce	Opis
Protest	03.07.2007 Bełchatów Polska	Ekolodzy włamali się na teren elektrowni, wspięli się na chłodnię kominową i wykonali napis „Stop CO_2”.
Protest	03.12.2008 Konin Polska	Ekolodzy włamali się na teren elektrowni, wspięli się na komin i rozpoczęli protest przeciw emisji gazów cieplarnianych.
Zamach terrorystyczny	21.07.2010 Baksana Kabardo--Bałkaria Rosja	Kilku sprawców wtargnęło, zabijając dwóch strażników, do elektrowni wodnej. Wysadzono dwa z trzech generatorów. Sprawcy byli uzbrojeni w broń maszynową oraz granatniki przeciwpancerne.
Zamach terrorystyczny	16.01.2013 In Amenas Algieria	Atak bojówek na pole gazowe, skutkujący czterodniową sytuacją zakładniczą. Śmierć poniosło 67 osób. Produkcję na normalnym poziomie wznowiono po 20 miesiącach.
Naruszenie przestrzeni powietrznej	03.01.2015 Nogent-sur-Seine Francja	Wlot dronów na teren elektrowni jądrowej.
Protest	18.03.2015 Fessenheim Francja	Międzynarodowa grupa ekologów wtargnęła na teren elektrowni jądrowej, żądając jej zamknięcia.
Naruszenie przestrzeni powietrznej	19.03.2021 Buquyaq Arabia Saudyjska	Atak 6 dronów na rafinerię Saudi Aramco. Wywołanie zniszczeń, strachu i niepokoju na rynkach finansowych.
Cyberatak	29.04.2021 USA	Atak ransomeware na ważny rurociąg paliwowy. Colonial Pipeline Co. zapłaciło okup w wysokości 5 mln dolarów.
Cyberataki	Rok 2022	Liczne ataki ransomware, ukierunkowane na IK (m.in. elektrownie, oczyszczalnie wody, szpitale) oraz podmioty administracji publicznej, celem ograniczenia lub wyłączenia danej usługi.

2.5.1. Działania organizacyjne i zapobiegawcze

Wykonywanie zadań w obszarze zapewnienia bezpieczeństwa fizycznego realizuje się m.in. przez zapewnienie ciągłej, 24-godzinnej bezpośredniej ochrony fizycznej obiektów, urządzeń, instalacji i systemów IK. Bezpośrednią ochronę fizyczną powinny wykonywać

wewnętrzna służba ochrony lub podmioty działające zgodnie z ustawą z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz.U. 2021 poz. 1995). Zapewni to m.in. możliwość użycia, zgodnego z prawem, środków przymusu bezpośredniego przez osoby realizujące tę ochronę.

W celu zapewnienia efektywności systemu bezpieczeństwa fizycznego dobrą praktyką jest podział terenu, na którym zlokalizowana jest IK na strefy ochrony[7] i zaprojektowanie ich zgodnie z zasadą ochrony w głąb (ochrona powłokowa). Niekiedy wyróżnia się także strefę zewnętrzną poza obiektem.

Każda ze stref musi być zaprojektowana w celu maksymalnego spowolnienia działań potencjalnego napastnika, a natężenie sił i środków ochrony powinno rosnąć w miarę zbliżania się potencjalnych napastników do strefy chroniącej kluczowe elementy infrastruktury organizacji. W rezultacie zniechęci to napastnika lub da więcej czasu na adekwatną do zagrożenia odpowiedź systemu ochrony lub wykwalifikowaną pomoc.

Przykładowy podział stref ochrony (od najbardziej chronionej):

1 – strefa ochrony wewnętrznej,
2 – strefa ochrony obrysowej,
3 – strefa ochrony peryferyjnej,
4 – strefa ochrony obwodowej (nazywana też z ang. strefą ochrony perymetrycznej),
5 – strefa dozoru zewnętrznego.

Niezależnie od funkcjonujących stref ochrony lub w przypadku braku wydzielenia takich stref, niezbędne jest określenie warunków, w których następuje wzmocnienie poziomu ochrony przez zastosowanie dodatkowych (określonych dla danego stopnia wzmocnienia) środków ochrony, w tym przede wszystkim organizacyjno-proceduralnych.

Należy wprowadzić procedury dotyczące:

(1) zasad wejścia do stref ochrony pracowników, kontrahentów, dostawców, wykonawców, podwykonawców i gości oraz wjazdu ich pojazdów oraz zasady poruszania się po obiekcie, obejmujące: proces rejestracji, wydawania identyfikatorów (przepustek/kart/kodów PIN), przydzielanie poziomu

[7] Strefa ochrony – obszar wraz ze znajdującymi się na nim zasobami, dla którego zostały określone wymagania bezpieczeństwa fizycznego.

uprawnień dostępu do poszczególnych stref, sposoby autoryzacji dostępu do poszczególnych stref ochrony oraz bieżącego nadzoru nad miejscem przebywania, możliwość kontroli uprawnień do przebywania w strefie, możliwość rewizji osobistej, kontroli pojazdów oraz wnoszonych lub wwożonych przedmiotów w sposób określony w wewnętrznej regulacji danego podmiotu, itp.;

(2) zasad użycia elementów identyfikacji (przepustki/klucze/kody/PIN/karty), obejmujące: rejestrację elementów identyfikacji, zasady przechowywania oraz wydawania kluczy do pomieszczeń i stref chronionych, okresową wymianę kodów, tryb wydawania i przyznawania kart;

(3) zasad nadawania i odbierania uprawnień dostępu, zmiany poziomu uprawnień dostępu oraz wydawania i odbierania identyfikatorów;

(4) kontroli środków zapewnienia bezpieczeństwa, obejmujące: odpowiedzialnych za kontrole, odstępy czasu między kontrolami, dokumenty uprawniające do kontroli, protokoły pokontrolne itp.;

(5) serwisowania technicznych środków zapewnienia bezpieczeństwa fizycznego, obejmujące: okresową obsługę zgodnie z dokumentacją techniczną, określone umownie czasy usuwania usterek itp.;

(6) testowania środków zapewnienia bezpieczeństwa, obejmujące przeprowadzanie testów penetracyjnych i ich przebieg, odpowiedzialnych za testy, ustalone okresy czasu prowadzenia testów itp.;

(7) sposobów reakcji ochrony na określone rodzaje zdarzeń. W tym wzmacnianie poszczególnych odcinków chronionych w przypadku wystąpienia dysfunkcjonalności elementów zapewnienia bezpieczeństwa (np. awarii SKD, SSWiN, VSS).

Budując obiekt, który będzie wymagał ochrony, trzeba pamiętać o podstawowych zasadach zabezpieczania: odstraszanie potencjalnych intruzów, wczesne wykrycie ataku, opóźnienie intruza (wydłużenie czasu ataku) i sprawna interwencja. Należy mieć na uwadze zastosowanie urbanistycznych, krajobrazowych, architektonicznych i budowlanych rozwiązań podnoszących bezpieczeństwo oraz zapewnienie wytrzymałości i stabilności konstrukcji, ogrodzenia, możliwość podziału na strefy bezpieczeństwa i innych rozwiązań dla systemu bezpieczeństwa fizycznego. Wskazane jest przeprowadzenie analizy ryzyka dla budowanego obiektu w celu właściwego wprowadzenia takich rozwiązań.

Zauważalna obecność środków systemu bezpieczeństwa fizycznego (płoty, siatki i ich zwieńczenia, kamery systemu telewizji przemysłowej, oświetlenie, obecność pracowników ochrony) zniechęca potencjalnych agresorów. Należy jednak mieć na uwadze, że nie wszystkie środki

ochrony powinny być eksponowane, by nie narażać bezpieczeństwa informacji o budowie systemu zabezpieczenia obiektu. Ponadto wskazane jest objęcie dokumentacji opisującej zastosowany system bezpieczeństwa fizycznego odpowiednią ochroną przed ujawnieniem osobom nieuprawnionym.

Należy dokonywać regularnych, okresowych przeglądów stanu zewnętrznego otoczenia chronionego obiektu (strefy ochrony) biorąc pod uwagę dostęp do obiektu i możliwości obserwacji wzrokowo-technicznej oraz dokonać regulacji terenu, usunięcia przesłaniającej widok roślinności, drzew itp. wewnątrz i na zewnątrz obiektu w sposób konsekwentny, cyklicznie i zgodnie z ustalonym wzorcem. Warto przemyśleć zastosowanie naturalnych barier roślinnych (spowalniających lub wręcz zniechęcających potencjalnych intruzów), np. z róż, czy z nisko rosnących ciernistych krzewów, takich jak berberysy, które dobrze znoszą przycinanie i łatwo można je kształtować.

Należy utworzyć centrum dowodzenia i koordynacji systemu bezpieczeństwa fizycznego w danej jednostce organizacyjnej i wyposażyć je w zintegrowany system informowania (VSS, SSWiN, SKD) o wszelkich stanach anormalnych zaistniałych w strefach ochrony. Zintegrowany system pozwoli pracownikom ochrony na podejmowanie szybkich decyzji i działań zmierzających do neutralizacji ewentualnych zagrożeń. Dla szczególnie ważnych obiektów, należy rozważyć budowę centrum dowodzenia i koordynacji systemu bezpieczeństwa fizycznego w taki sposób, żeby wyłączenie działania jednego centrum nie pozbawiło organizacji możliwości realizacji tej ważnej funkcji. Można to osiągnąć, np. poprzez przygotowanie zapasowego centrum, łącznie z kompetentnym zastępczym personelem, zdolnego do przejęcia zadań podstawowego centrum dowodzenia lub zaprojektować centrum w modelu rozproszonym, tj. działającym równolegle, z co najmniej dwóch różnych budynków (najlepiej oddalonych od siebie). Zapasowe centrum powinno mieć aktualizowane na bieżąco dane z wszystkich funkcjonujących systemów zabezpieczeń (VSS, SSWiN, SKD i innych). Osoby posiadające uprawnienia do kontroli nad zabezpieczeniem technicznym (technicznymi środkami bezpieczeństwa fizycznego) lub dokonywania w nich zmian powinny autoryzować dokonanie tych czynności przez połączenie minimum 2 niezależnych unikalnych identyfikatorów (np.: PIN-karta, PIN-biometria itp.). Jeżeli są to osoby spoza organizacji należy rozważyć potrzebę wykonywania takich prac wspólnie z pracownikiem organizacji lub pod jego nadzorem. Dobrą praktyką jest konieczność podania kodów dostępu pracownika i zewnętrznego serwisanta w celu możliwych zmian konfiguracyjnych. Dodatkowo przedmiotowe zmiany muszą zostać zarejestrowane w dokumentacji IK (np. Książka Serwisu, Książka Służby, czy inne dokumenty rejestrujące zdarzenia dotyczące zabezpieczenia technicznego; np. Książka Elektronicznego Systemu Zabezpieczeń – zgodnie rozporządzeniem MSWiA z 7.09.2010 w sprawie szczegółowych zasad i wymagań,

jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne – Dz.U. 2016 poz. 793).

Po każdym incydencie należy przeprowadzić analizę zdarzenia i w razie potrzeb skorygować stosowane środki ochronne w celu zapobiegania incydentom bezpieczeństwa w przyszłości.

2.5.2. Modele bezpośredniej ochrony fizycznej[8]

Bezpośrednią ochronę fizyczną należy dostosować do uwarunkowań IK oraz otoczenia (społecznego, komunalnego, biznesowego i innych) i specyfiki zagrożeń.

Standardowymi rozwiązaniami w zakresie bezpośredniej ochrony fizycznej jest jej organizacja w formie:

- posterunków (np. wartowniczych, kontrolnych, obserwacyjnych) funkcjonujących w trybie stałym - całodobowym, czasowym - w wybranych porach doby oraz doraźnym - incydentalnie.
- patroli (pieszych i na pojazdach).

Całość systemu zapewnienia bezpieczeństwa fizycznego powinna charakteryzować się następującymi cechami:

(1) **Elastycznością** - niezbędną w sytuacji zdarzenia wykraczającego poza zdarzenia zwykłe, wynikające z funkcjonowania IK i opisane w standardowych procedurach działania służby ochrony;

(2) **Mobilnością** – zwiększająca efektywność procesów ochronnych;

(3) **Komplementarnością** – uzupełnianie się poszczególnych elementów ochrony;

(4) **Kompletnością** – najsłabsza część systemu limituje jego zdolności ochronne;

(5) **Nienaruszalnością** - każda z części składowych systemu musi być chroniona przez inną, a jej zniszczenie, uszkodzenie lub ograniczenie jej funkcjonalności, musi być niezwłocznie i jednoznacznie rozpoznane, a sam system zdiagnozowany jako naruszony.

W trakcie bezpośredniej ochrony fizycznej osoby pełniące służbę wykonują: patrole piesze wewnątrz, jak i na zewnątrz obiektu, patrole samochodowe, kontrole ruchu osobowego, kontrole przesyłek oraz ruchu samochodowego.

Wyróżnia się trzy podstawowe modele bezpośredniej ochrony fizycznej, które można podzielić pod względem rozmieszczenia i poziomu mobilności jednostek ochrony:

(1) model statyczny,
(2) model ruchomy,
(3) model mieszany.

[8] Opracowano na podstawie prezentacji Chief Constable Richarda Thomsona – Civil Nuclear Constabulary, Londyn 18 maja 2011 r.

Model statyczny:

- celem tego typu modelu jest uniemożliwienie osobom postronnym zajęcia terenu przez określony okres czasu,
- jest to model preferowany w sytuacji, gdy utrata obiektu jest niedopuszczalna.

Główne cechy:

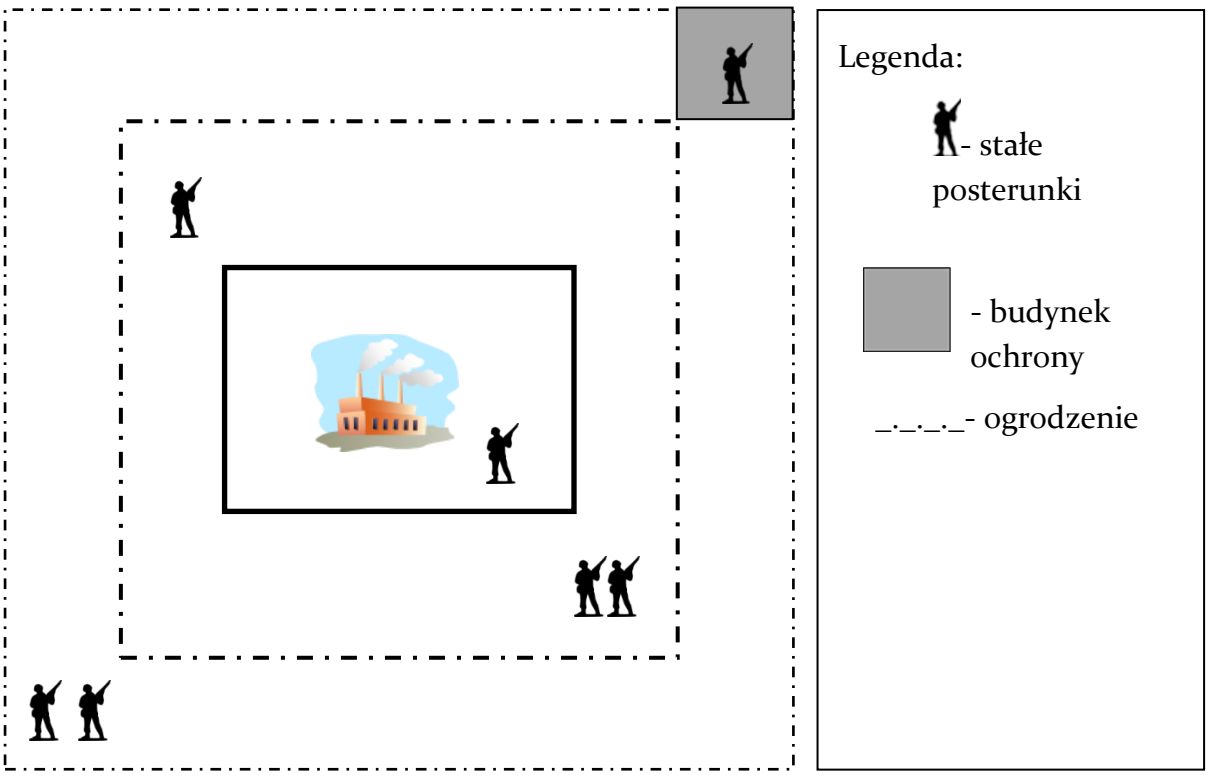
- wielowarstwowa ochrona,
- wielowarstwowy system wykrywania,
- stałe posterunki ochronne.

Zalety:

- prostota budowy,
- bezpieczeństwo (nie ma możliwości, by członek ochrony znalazł się na linii ognia innego członka ochrony),
- proste dowodzenie,
- łatwość przygotowania służby ochrony do działania w opisanym systemie.

Wady:

- brak przemieszczania się ochrony oznacza, że nie zareaguje ona szybko w przypadku wystąpienia sytuacji nieoczekiwanej,
- narażenie na ataki z użyciem samochodów pułapek,
- w zależności od ukształtowania terenu system ten może wymagać dużej grupy pracowników ochrony.



Rysunek 8 Ilustracja funkcjonowania modelu statycznego.

Model ruchomy:

- służby ochrony swobodnie poruszają się po obiekcie i reagują na pojawiające się alarmy lub podejrzane zachowanie.

Główne cechy:

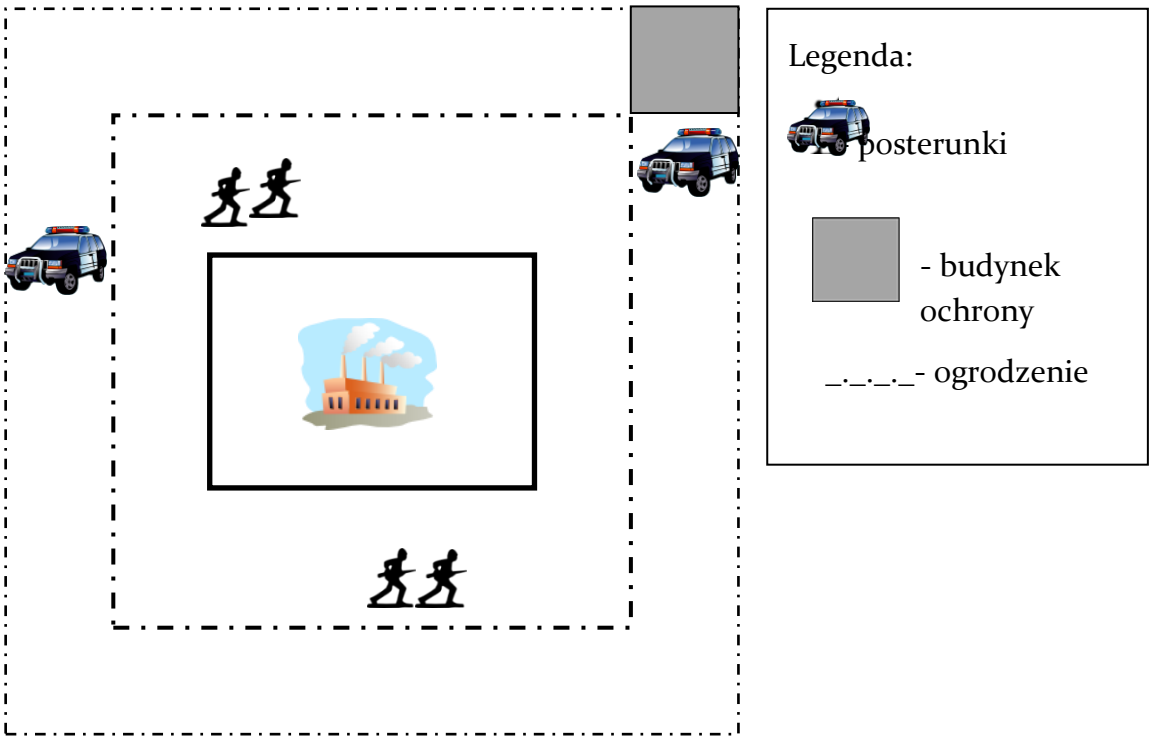
- używane są różne systemy elektroniczne uzupełniające działania służb ochrony,
- służba ochrony może się swobodnie poruszać po całym obiekcie.

Zalety:

- system elastyczny – zarówno patrole, jak i ochrona, dostosowują się do danych warunków lub okoliczności,
- liczebność formacji ochronnej nie musi być duża.

Wady:

- system nie sprawdza się w przypadku prób wielopunktowej penetracji,
- system wymaga wysoko wyszkolonej formacji ochronnej, która musi ciągle podnosić swoje umiejętności przez ćwiczenia i szkolenia.



Rysunek 9 Ilustracja funkcjonowania modelu ruchomego.

Model mieszany:

- zawiera cechy obu modeli opisanych powyżej,
- sprawdza się szczególnie w przypadku dużych obiektów.

Główne cechy:

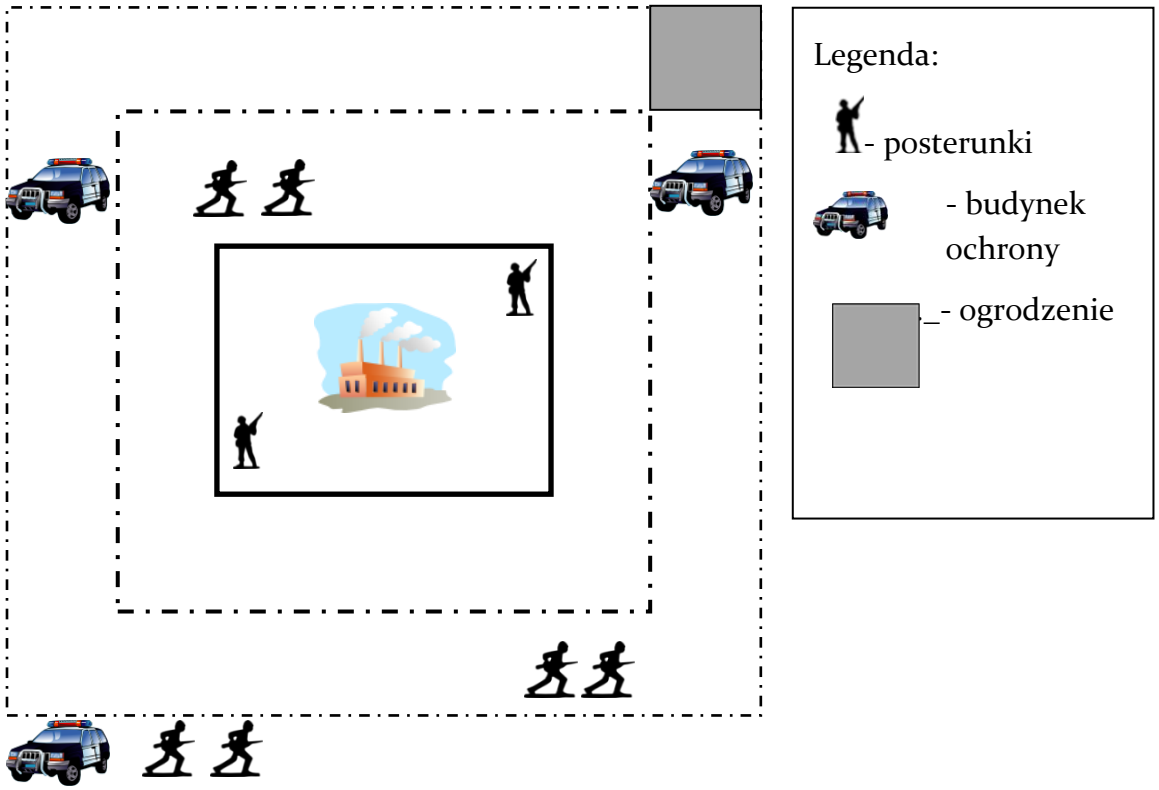
- wielowarstwowa ochrona,
- zgrane elementy ochrony statycznej z ruchomymi patrolami,
- stałe posterunki ochronne.

Zalety:

- patrole obecne również poza obszarem obiektu, co działa odstraszająco,
- parole ruchome stanowią rezerwę w przypadku próby penetracji,
- duża efektywność,
- dobre rozpoznanie sytuacyjne.

Wady:

- wymagający doskonałego przeszkolenia i wyposażenia,
- system skomplikowany,
- kosztowny.



Rysunek 10 Ilustracja funkcjonowania modelu mieszanego

Wybór konkretnego modelu ochrony jest uzależniony od oceny ryzyka zakłócenia funkcjonowania IK, możliwości technicznych oraz finansowych operatora.

Zakres działań pracowników ochrony powinien również obejmować działania polegające na:

- ochronie obszaru IK w jego wyznaczonych granicach, przed nieuprawnionym dostępem za pomocą wszystkich zgodnych z prawem i przyjętych w systemie bezpieczeństwa środków i przedsięwzięć,
- zapewnieniu bezpieczeństwa osób znajdujących się na terenie lub w granicach IK,
- zapobieganiu przedostaniu się na teren IK paczek podejrzanych, np. niewiadomego pochodzenia oraz zawierających substancje niebezpieczne. W tym celu można stosować prześwietlarki, detektory metalu, substancji promieniotwórczych oraz toksycznych oraz formy kontroli osób (przeszukanie odzieży, bagaży, kontrola osobista), kontroli pojazdów (wyznaczone przestrzenie pojazdu: bagażowa, transportowa, narzędziowa, pasażerska, podwozie, etc.),
- ochronie mienia IK przed kradzieżą, zniszczeniem lub uszkodzeniem,
- zapobieganiu zakłóceniom porządku na terenie oraz powiadamianie właściwych przełożonych o zdarzeniach powodujących naruszenie porządku,
- przyjmowaniu, przechowywaniu i wydawaniu depozytów (w tym broni),
- stałym dozorze sygnałów z elektronicznych systemów zabezpieczenia technicznego,
- wykrywaniu zagrożeń klęskami żywiołowymi, awariami technicznymi oraz podejmowaniu i koordynowaniu działań zmierzających do zapobiegania i przeciwdziałania ich skutkom, do czasu przybycia właściwych służb,
- powiadamianiu właściwych przełożonych o zdarzeniach nadzwyczajnych, incydentach bezpieczeństwa, wykroczeniach, przestępstwach.

Pracownicy realizujący ochronę elementów IK powinni być wyposażeni w broń i amunicję służbową oraz inne środki przymusu bezpośredniego, a także: w opatrunki osobiste lub zestawy medyczne, środki łączności radiowej i telefonicznej, latarki, środki transportu oraz w miarę potrzeby inny sprzęt (np. hełmy i kamizelki kuloodporne, maski przeciwgazowe). Konieczne jest zapewnienie przeszkolenia w umiejętnym wykorzystaniu tego wyposażenia.
Operatorzy IK powinni zapewnić pracownikom ochrony możliwość stałego podnoszenia i doskonalenia umiejętności w zakresie:

- przeglądu ról i obowiązków ochrony,
- postępowania pracowników ochrony w zakresie bezpieczeństwa ppoż. (np. aktywny udział w ewakuacji),
- prawa (zadania wynikające z ustawy o ochronie osób i mienia, zasady interwencji, użycia środków przymusu bezpośredniego oraz broni, przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP i inne w razie potrzeby),
- pierwszej pomocy medycznej,
- techniki i taktyki interwencji,
- użycia innych środków przymusu bezpośredniego,
- techniki i taktyki posługiwania się bronią palną,
- technik interwencji bezdotykowej wobec osób nie używających przemocy i siły
- rozpoznania minerskiego i pirotechnicznego (podstawy).

Należy wprowadzić zakaz wnoszenia na teren obiektów IK broni i amunicji, urządzeń rejestrujących obraz typu aparaty fotograficzne, kamery telefony komórkowe i tablety, wyposażone w aparaty fotograficzne itp. przez osoby nieposiadające specjalnych uprawnień lub wykonujących zadania służbowe, które regulują wewnętrzne przepisy. Na czas pobytu w obiekcie powyższe osoby powinny deponować urządzenia elektroniczne rejestrujące obraz i dźwięk w pomieszczeniu depozytowym nadzorowanym przez podmioty realizujące ochronę fizyczną infrastruktury krytycznej.

2.5.3. Techniczne środki zapewnienia bezpieczeństwa fizycznego[9]

Ogrodzenie, zapory mechaniczne, wejścia i wyjścia

Jeśli istnieje taka możliwość, obiekty infrastruktury krytycznej powinny być całkowicie ogrodzone. Ogrodzone powinny być również wyznaczone strefy ochrony. Ogrodzenie powinno spełnić wymóg jak najdłuższego czasu pokonywania przez potencjalnego intruza.

W tym celu:

- konstrukcja ogrodzenia powinna utrudniać wspinanie się na ogrodzenie, jego przecinanie, łamanie i przewracanie,
- wysokość ogrodzenia nad powierzchnią terenu powinna w maksymalny sposób utrudnić jego pokonanie ponad nim,
- dolna krawędź ogrodzenia powinna być trwale zamontowana w podłożu (np. zabetonowana),
- powinno być wyposażone w barierę uniemożliwiającą dokonanie podkopu,
- powinno być wyposażone w bariery wieńczące ogrodzenie z drutu kolczastego lub drutu ostrzowego.

Ogrodzenie może zostać zbudowane jako:

- nieprzejrzyste o konstrukcji murowanej lub z prefabrykowanych segmentów betonowych itp.,
- przejrzyste z siatki lub paneli,
- jeden lub dwa zestawy z korytarzem bezpieczeństwa między nimi.

Ogrodzenie powinno mieć możliwość współpracy z systemami dozoru wizyjnego, pozwalającymi na obserwację ogrodzenia zewnętrznego oraz wszystkich wejść i wyjść z stref ochrony, a także systemami sygnalizacji włamania i napadu, pozwalającymi na jak najwcześniejsze wykrycie intruza.

Należy rozważyć stworzenie pasa buforowego wokół obiektu. Jeśli lokalizacja nie pozwala na utworzenie pasa buforowego, należy stosować mechaniczne bariery zabezpieczające przed wtargnięciem, np. przez samochód. Warto zastosować w takim przypadku elementy typu głazy lub kamienie, które mają wysoką odporność. Odpowiednio zaaranżowane mogą one jednocześnie tworzyć atrakcyjne otoczenie obiektu.

Wejścia na teren IK (jeśli jest taka możliwość, warto rozdzielić wejścia dla pracowników od wejść dla gości i interesantów) oraz bramy wjazdowe dla pojazdów powinny być rozdzielone.

[9] Niekiedy stosuje się określenie „zabezpieczenia techniczne".

Wejścia na teren IK dla pracowników oraz przejścia między strefami ochrony powinny być wyposażone w aktywatory przejścia (elektrozaczepy, rygle elektryczne), kontrolowane przez system kontroli dostępu (SKD) identyfikujący osobę i weryfikujący jej uprawnienia przy użyciu danych uwierzytelniających, takich jak informacje zapamiętane (PIN), albo przechowywane w identyfikatorze (np. indywidualny numer czy obraz cech biometrycznych). Ponadto konstrukcja wejścia powinna umożliwić wzrokową identyfikację wchodzących przez pracownika ochrony.

Niezależnie od propozycji rozdziału wejść należy dążyć do minimalizacji ich liczby. Ułatwia to kontrolę dostępu oraz zmniejsza koszty utrzymania systemu zapewnienia bezpieczeństwa fizycznego. W przypadku zmniejszenia liczby wejść/wyjść pamiętać jednak należy o wymogach związanych z ewakuacją. Pełna rejestracja w SKD (na wejściu i na wyjściu) ułatwia sprawdzenie kompletności ewakuacji (najlepiej w połączeniu z czytnikami obecności, zlokalizowanymi w miejscach zbiórki do ewakuacji – możliwość wykorzystania funkcji SKD - „lista obecności", ang. „Roll Call").

Wysokość bram wjazdowych dla pojazdów powinna być adekwatna do ogrodzenia, włączając w to bariery wieńczące i ochronę przed przeniknięciem pod. Napędy bram (jeśli brama nie jest sterowana ręcznie) powinny być wyposażone w odpowiednie środki w celu zapewnienia ich pełnego funkcjonowania w każdych warunkach pogodowych. Bramy należy wyposażyć w zapory zabezpieczające przed wtargnięciem na teren. Bariery te powinny być z zasady zamknięte, a otwierane jedynie wtedy, gdy autoryzacja osoby uprawnionej do wjazdu zostanie potwierdzona przez system kontroli dostępu lub pracownika ochrony.

Należy także zapewnić miejsce do kontroli pojazdów (ładunku, tożsamości osób i uprawnień do przebywania na terenie obiektu chronionego) przez personel odpowiedzialny za ochronę. Odpowiednie wyposażenie w podesty, lustra, kamery, narzędzia i urządzenia do weryfikacji autentyczności dokumentów itp. zwiększa efektywność kontroli. Miejsce to może być zaaranżowane w formie śluzy, zatoczki, zadaszenia itp. Należy również zapewnić kontrolę w czasie ładowania i rozładunku towarów na terenie IK (nadzór osobowy, z wykorzystaniem kamer VSS itp.).

Oświetlenie i doświetlenie

Jeśli istnieje taka możliwość, obiekty infrastruktury krytycznej powinny być całkowicie oświetlone w stopniu umożliwiającym skuteczne dokonywanie detekcji intruzów, obserwacji, identyfikacji oraz rejestracji. Prawidłowo wykonane oświetlenie ma również działanie odstraszające.

Dobrą praktyką jest widoczność obszaru wewnętrznego obiektu na minimum 100 metrów przy dobrych warunkach pogodowych w nocy (brak mgły i opadów).

Doświetlone powinny być wyznaczone strefy ochrony. Doświetlenie powinno podnosić jakość obserwacji realizowanej przy użyciu systemu dozoru wizyjnego. W wybranych miejscach doświetlenie powinno wspierać wykrycie intruza (strefa ochronna i strefy dojścia do obiektu - tzw. strefy podejścia). Należy pamiętać, że systemy VSS (oprócz wykorzystujących kamery termowizyjne) wykorzystują światło odbite od elementów dozorowanej przestrzeni. Niektóre typy kamer mogą korzystać nie tylko z oświetlenia emitowanego w paśmie widzialnym, ale również emitowanego w paśmie niewidzialnym (w bliskiej podczerwieni). Należy również pamiętać o zapewnieniu zasilania awaryjnego dla oświetlenia dozorowanej przestrzeni, na wypadek wyłączenia zasilania.

Oświetlenie jest jednym z najmniej docenianych elementów systemów ochronnych a z zasady powinno mieć możliwość współpracy z systemami dozoru wizyjnego, systemami SWiN oraz całym systemem zapewnienia bezpieczeństwa fizycznego. Odpowiednie zastosowanie oświetlenia i doświetlenia pozwala na redukcję innych środków zabezpieczenia, ze względu na lepszą możliwość ich wykorzystania.

Systemy kontroli dostępu (SKD)

Dostęp do stref ochrony oraz kluczowych dla funkcjonowania IK pomieszczeń lub obszarów powinien być kontrolowany i ograniczany wyłącznie do uprawnionych osób. Zdolność do takich działań zapewniają systemy kontroli dostępu, które:

(1) umożliwiają zabezpieczanie przed nieuprawnionym dostępem do stref ochrony (także pomieszczeń);
(2) umożliwiają ograniczenie poruszania się po obiekcie osób, które nie są do tego upoważnione;
(3) umożliwiają wydzielenia stref ochrony, do których dostęp będą miały tylko osoby upoważnione;
(4) umożliwiają monitoring czasu przebywania w strefie (także pomieszczeniu),
(5) wspomagają potwierdzanie tożsamości pracowników;
(6) zapewniają odpowiedni poziom praw dostępu dla kontrahentów i gości.
(7) wspomagają nadzorowanie ewakuacji w sytuacjach jej wymagających.

SKD powinien być wprowadzony we wszystkich strefach ochrony i obejmować wszystkie (lub przynajmniej używane) wejścia i wyjścia dla ludzi i bramy wjazdowe dla

pojazdów. Wybrane pomieszczenia wewnątrz stref ochrony powinny być wyposażone w urządzenia blokujące przejście kontrolowane i sterowane przez system kontroli dostępu lub inną metodę identyfikacji wchodzących i kontroli ich prawa dostępu (klucz, wideodomofon). SKD powinien być wspomagany systemem dozoru wizyjnego (VSS), a dostęp do poszczególnych stref powinien być przyznawany tylko i wyłącznie pracownikom, którzy są niezbędni do zapewnienia właściwego funkcjonowania danej strefy lub urządzeń w niej się znajdujących.
SKD można zaprogramować w sposób zapobiegający powtórnemu udzieleniu prawa dostępu w jednym kierunku. Jest to tzw. „blokada użyczenia", ang. „anti-passback". Takie rozwiązanie skutecznie wymusza konieczność rejestracji wejścia i wyjścia ze strefy ochrony oraz zapobiega nieuzasadnionemu przepuszczaniu przez strefy ochrony osób nieupoważnionych. Stwierdzenie obecności użytkownika w określonym obszarze w celu umożliwienia wejścia do innego obszaru powinno odbywać się przy użyciu systemu kontroli dostępu. z wykorzystaniem funkcji tzw. obszarowej blokady użyczenia, ang. area conrolled anti-passback.
Zapewniając kontrolę wejść i osób wchodzących, nie należy zaniedbywać kontroli wyjść i osób wychodzących. Pozwala na to m.in. monitorowanie ewakuacji, np. w razie pożaru. Wobec wyłączenia SKD (np. ewakuacyjnego odblokowania przejść), w niektórych przypadkach ewakuacji wprowadzić należy procedury weryfikacji jej kompletności, np. w formie osoby o funkcji dyżurnego piętra lub poprzez zastosowanie czytników obecności, zlokalizowanych w miejscach zbiórki do ewakuacji (funkcja „lista obecności", ang. „Roll Call".

Systemy dozoru wizyjnego (VSS)[10]

System dozoru wizyjnego (VSS) to system kamer służących do przekazywania obrazu (rzadziej w połączeniu z dźwiękiem) z określonych stref, obszarów lub pomieszczeń w zamkniętym systemie odbiorczym, służący do nadzoru oraz zwiększeniu bezpieczeństwa stref, obszarów lub pomieszczeń, w obrębie których zostały zainstalowane kamery.

System dozoru wizyjnego sprawdza się w przypadku, kiedy wybrane strefy, obszary lub pomieszczenia wymagają stałej kontroli i nadzoru. Zastosowanie VSS pozwala na:

- prowadzenie działań ochronnych z oddalonych miejsc,
- identyfikację rodzaju zdarzenia,
- wykrycie i identyfikację osób oraz pojazdów,
- detekcję ruchu,

[10] Video Surveillance System. W przeszłości stosowano także określenia: „telewizja przemysłowa", „telewizja użytkowa", „telewizja w sieciach zamkniętych (skrót CCTV - close circuit television), a także „telewizja dozorowa" . Nie należy tego mylić z systemami monitoringu wizyjnego obszarów miejskich.

- analizy tła (np. zmiana w porządku parkowania pojazdów, przesunięcie paczki, walizki, palety, etc.)
- zapis obrazu i dźwięku.

Typowy system VSS zwykle składa się z następujących elementów:

- kamer stałych lub ruchomych (z opcją śledzenia),
- systemu tzw. oświetlenia sceny,
- infrastruktury służącej do transmisji wizji (i ew. fonii) oraz sterowania kamerami,
- (rejestratorów) wizji,
- zestawu monitorów i urządzeń sterujących, znajdujących się w centrum dozoru (nazywanym też centrum monitoringu)[11].

Zakres instalacji stałych kamer systemu powinien obejmować granice stref ochrony wraz z wejściami/wyjściami i bramami wjazdowymi/wyjazdowymi dla pojazdów oraz pozostałe używane wejścia/wyjścia i bramy wjazdowe/wyjazdowe dla pojazdów. System VSS zainstalowany przy wejściach, wyjściach do stref ochrony, powinien umożliwić późniejszą identyfikację osób, pojazdów wchodzących i wychodzących z powyższych stref. Kamery ruchome powinny obejmować istotne obszary wewnętrzne i drogi. Przy planowaniu rozmieszczenia kamer należy unikać tzw. martwych pól, tzn. miejsc, części terenów lub obiektów infrastruktury krytycznej, które byłyby poza możliwością podglądu przy wykorzystaniu systemu VSS.
Z systemem VSS powinno współpracować gwarantowane oświetlenie, obejmujące swoim zakresem wejścia/wyjścia i bramy wjazdowe/wyjazdowe dla pojazdów, granice stref ochrony i inne obszary monitorowane przez system.

Systemy sygnalizacji włamania i napadu

Systemy sygnalizacji włamania i napadu (SSWiN) stosuje się w celu wykrycia i rejestracji prób nielegalnego (nieuprawnionego) wejścia do stref ochrony, wybranych obszarów i pomieszczeń oraz do przekazywania, przy użyciu przycisków alarmowych, informacji o wystąpieniu bezpośredniego zagrożenia.

SSWiN oparte są m.in. na urządzeniach:

- wykrywających ruch w strefie objętej ich działaniem;
- wykrywających otwarcie drzwi;
- wykrywających wypełnienie otworów budowlanych (wejścia, okna, inne otwory);
- wykrywających uszkodzenie powierzchni szklanych;
- wykrywających ingerencję w ogrodzenie;
- ostrzegających o zagrożeniach (przyciski alarmowe).

[11] Centrum dozoru (monitoringu) powinno integrować wszystkie systemy wspierające system zapewnienia bezpieczeństwa fizycznego (SKD, SSWiN, VSS).

Potencjalny intruz powinien być wykryty jak najwcześniej, dlatego systemem SWiN powinna być objęta graniczna linia ogrodzenia (strefa ochrony obwodowej) oraz wejścia/wyjścia i bramy wjazdowe/wyjazdowe dla pojazdów (dla każdego elementu oddzielnie) oraz wybrane pomieszczenia i budynki znajdujące się wewnątrz stref ochrony.

Główne drogi oraz okolice wejść i wyjść można wyposażyć w widocznie zainstalowane przyciski alarmowe. Wybrane pomieszczenia lub części stref ochrony można wyposażyć w ukryte przyciski alarmowe sygnalizacji zagrożenia.

Archiwizacja zdarzeń powinna zależeć od charakteru obiektu i obejmować:

- **system VSS**
  - nie krócej niż 14 dni zapisu, w obiektach podlegających rozporządzeniu MSWiA z 7.09.2010 *w sprawie szczegółowych zasad i wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne* (Dz.U. 2016 poz. 793),
  - nie krócej niż 30 dni zapisu, w obiektach podlegających rozporządzeniu RM z 29.05.2012 *w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych* (Dz. U. 2012 poz. 683),
  - nie krócej niż 3 miesiące zapisu, w obiektach podlegających Normom Obronnym.

  Dla obiektów IK sugeruje się utrzymywanie min. 30 dni zapisu.
- **systemy SKD:**
  - nie krócej niż 30 dni zapisu, w obiektach podlegających rozporządzeniu MSWiA z 7.09.2010.

Zgodnie z rozporządzeniem MSWiA z 7.09.2010, „w przypadku wykrycia lub uzasadnionego podejrzenia popełnienia czynu zabronionego zapis z tym związany należy zarchiwizować w sposób niezmniejszający jego jakości. Dotyczy to również zawartości pamięci zdarzeń centrali systemu sygnalizacji włamania i napadu oraz kontroli dostępu, w przypadku występowania związku pomiędzy zawartością pamięci tych urządzeń a czynem zabronionym. Zawartość pamięci powinna być zabezpieczona, a następnie komisyjnie odczytana i zarchiwizowana. Materiałowi archiwalnemu należy nadać kategorię archiwalną dokumentacji dla ochrony zakładu pracy (mienia), zgodnie z zasadami postępowania z materiałami archiwalnymi.” Oznacza to nadanie właściwej kategorii niearchiwalnej np. B2 zgodnie z obowiązującymi w tym zakresie przepisami kancelaryjno-archiwalnymi.

Należy również pamiętać o podtrzymaniu awaryjnym elektronicznych systemów zabezpieczeń, na wypadek zaniku zasilania z sieci energetycznej. Minimalne czasy

gotowości zasilania rezerwowego można znaleźć w odpowiednich normach. Dla obiektów IK sugeruje się uzyskanie czasów gotowości wynoszących:

- SSWiN – 60 godzin,
- SKD – 4 godziny,
- VSS z oświetleniem – 4 godziny.

Należy pamiętać, aby systemy zabezpieczeń technicznych były projektowane, instalowane, konserwowane i eksploatowane z zachowaniem najwyższych standardów jakości. Osoby realizujące usługi w tym zakresie powinny posiadać zaświadczenie o ukończeniu kursu pracownika zabezpieczenia technicznego wydane przez wyspecjalizowaną placówkę kształcenia ustawicznego działającą w systemie oświaty lub posiadać ważne zaświadczenie o wpisie na listę kwalifikowanych pracowników zabezpieczenia technicznego.

Istotne jest, aby wymagania kompetencyjno-kwalifikacyjne osób realizujących usługi w zakresie systemów zabezpieczeń technicznych wynikały wprost lub pośrednio z przepisów prawa, norm, specyfikacji technicznych oraz standardów branżowych, w szczególności mających odniesienie do ustawy o ochronie osób i mienia, wojskowych dokumentów normatywnych, normy PN-EN 16763 Usługi w zakresie systemów ochrony przeciwpożarowej oraz systemów zabezpieczeń technicznych, a także specyfikacji technicznej PKN-CLC/TS 50131-7 Systemy alarmowe, Systemy sygnalizacji włamania i napadu, Część 7: Wytyczne stosowania.

Przykładowe grupy norm, które warto brać pod uwagę dotyczą:

- Systemy alarmowe – Systemy sygnalizacji włamania i napadu – normy PN-EN 50131,
- Systemy alarmowe i elektroniczne systemy zabezpieczeń - Elektroniczne systemy kontroli dostępu– normy PN-EN 60839-11,
- Systemy dozorowe CCTV stosowane w zabezpieczeniach – normy PN-EN 62676,
- Drzwi, okna, ściany osłonowe, kraty i żaluzje - Odporność na włamanie– norma PN-EN 1627:2021-11.

2.5.4. *Standardy bezpieczeństwa dla operatorów IK w zakresie zapobiegania, reagowania i ograniczania skutków zagrożeń stwarzanych przez incydenty z udziałem systemów bezzałogowych*

Systemy bezzałogowe stanowią dla wielu operatorów IK narzędzie do monitorowania zagrożeń, prac serwisowych oraz wspomagania decyzji umożliwiających skuteczne wzmacnianie obszarów bezpieczeństwa fizycznego, technicznego i teleinformatycznego w zakresie zapewnienia ciągłości działania procesów wynikających z realizacji misji publicznej lub biznesowej oraz w zakresie nadzorowanych zadań przez służby kontroli, ochrony i przeciwdziałania zagrożeniom. Systemy bezzałogowe mogą być również narzędziem zagrożenia, którego zmaterializowanym skutkiem może być zakłócenie, przerwanie lub zniszczenie funkcjonalności IK. Aby należycie chronić IK zaproponowano operatorom IK standardy, w których zarekomendowano podstawowe wymagania, jakie powinien spełnić operator IK, aby zorganizować i doskonalić system zapobiegania zagrożeniom, reagowania na nie i ograniczania skutków zagrożeń od incydentów z udziałem systemów bezzałogowych. System ten jest częścią procesu analizy zagrożeń w obszarze bezpieczeństwa fizycznego, ale też jest zintegrowany funkcjonalnie z istniejącymi u operatora IK systemami oceny ryzyka i bezpieczeństwa oraz z planem ochrony infrastruktury krytycznej (POIK).

Zastosowanie Standardów wpływa na proces identyfikacji i analizy zagrożeń oraz na szacowanie ryzyka dla IK przygotowywanego cyklicznie lub według potrzeb przez operatora IK. Wnioski z oceny bezpieczeństwa IK uwzględniającej skutki zagrożeń od incydentów z udziałem systemów bezzałogowych mogą wpływać na wyniki i rekomendacje dla bezpieczeństwa publicznego. Standardy mogą być podstawą do aktualizacji zasad współpracy między operatorem IK, a służbami publicznymi oraz organami administracji publicznej nadzorującymi poszczególne systemy IK.

2.5.4.1 Cel Standardów

Celem Standardów jest wdrażanie mechanizmów wzmacniających odporność na zagrożenia stwarzane przez incydenty z udziałem systemów bezzałogowych oraz usprawnienie ciągłości działania najważniejszych usług i procesów oraz funkcjonalności kluczowych obiektów, instalacji i urządzeń tworzących IK.

Stosowanie Standardów pozwala operatorowi IK na wskazywanie priorytetów związanych z przekroczeniem akceptowanego przez podmiot poziomu ryzyka wystąpienia skutków dla IK, przyjętym dla reprezentatywnych scenariuszy zmaterializowania zagrożenia wywołanego przez incydenty z wykorzystaniem systemów bezzałogowych.

Zastosowanie Standardów umożliwia operatorowi IK organizowanie systemu zapobiegania, reagowania i ograniczania skutków zagrożeń od incydentów z udziałem systemów bezzałogowych, o ile zagrożenia te wynikają z oceny ryzyka. Wdrażanie Standardów wspomaga również mechanizmy wzmacniania systemów bezpieczeństwa zarządzanych przez służby i podmioty realizujące zadania w obszarach porządku i bezpieczeństwa publicznego, społecznego, energetycznego i transportowego.

2.5.4.2 Słownik stosowanych pojęć

W Standardach zastosowane definicje i pojęcia oznaczają:

a) **systemy bezzałogowe** - Systemy Bezzałogowych Pojazdów (Statków) Powietrznych (SBSP), Lądowych (SBPL), Wodnych (SBPW) lub Kosmicznych (SBSK), przygotowane w konfiguracji umożliwiającej realizację określonych misji i zadań wraz z infrastrukturą sterowania i obsługującym ją personelem, składające się z następujących elementów:
   - **platformy/platform bezzałogowych** operujących w środowisku powietrznym, wodnym, lądowym i kosmicznym (*Bezzałogowy Statek Powietrzny/Latający– **BSP**/ **BSL**, Bezzałogowy Statek Nawodny – **BSNW,** Bezzałogowy Statek Podwodny – **BSPW,** Bezzałogowy Pojazd Lądowy – **BPL,** Bezzałogowy Statek Kosmiczny **BSK***) ;
   - **Naziemnej Stacji/Panelu Kontroli – NSK/NPK;**
   - **Naziemnego Terminala Danych – NTD**;
   - **Systemu Łączności i Przesyłania Danych,**

b) **dron, bezzałogowiec** – potoczna nazwa bezzałogowego statku powietrznego, wodnego, lądowego lub kosmicznego,

c) **systemy antydronowe** - systemy przeznaczone do wykrywania, rozpoznania, identyfikacji oraz kinetycznej lub niekinetycznej neutralizacji elementów systemów bezzałogowych,

d) **wtargnięcie systemu bezzałogowego** – nieuprawnione, umyślne lub nieumyślne, wniknięcie (wlot, wjechanie, wpłynięcie) systemu bezzałogowego lub jego elementu w określony obszar lub strefę oddziaływania na elementy IK,

e) **operator systemu bezzałogowego statku powietrznego lub Systemu bezzałogowego**- dowolna osoba prawna lub fizyczna eksploatująca lub zamierzająca eksploatować co najmniej jeden system bezzałogowego statku powietrznego lub systemu bezzałogowego,

f) **pilot bezzałogowego statku powietrznego** –osoba odpowiedzialna za bezpieczne wykonanie lotu przez BSP poprzez ręczne sterowanie lotem albo- w przypadku, gdy BSP lata automatycznie- poprzez monitorowanie jego kursu i utrzymywanie zdolności do interwencji i zmian kursu w każdej chwili; osoba, która musi posiadać wymaganą wiedzę i umiejętności niezbędne do zapewnienia

bezpieczeństwa eksploatacji oraz proporcjonalnie do ryzyka związanego z danym rodzajem operacji; osoba ta powinna wykazać się odpowiednia kondycją zdrowotną, jeśli jest to niezbędne do ograniczenia ryzyka związanego z daną operacją, gdyż na pilocie ciąży odpowiedzialność za szkody wyrządzone przez pilotowany przez niego BSP,

g) **detekcja systemu bezzałogowego** – zdolność odróżnienia systemu bezzałogowego od tła otaczającej przestrzeni, prowadząca do wykrycia, lokalizacji oraz identyfikacji systemu bezzałogowego (np. wykrycie bezzałogowej platformy latającej na niebie),

h) **rozpoznanie systemu bezzałogowego** - zdolność odróżnienia systemu bezzałogowego od innych typów obiektów znajdujących się w przestrzeni powietrznej, na lądzie lub środowisku wodnym; w wyniku procesu rozpoznania można stwierdzić, że rozpoznany został system bezzałogowy (np. odróżnienie bezzałogowej platformy latającej od ptaków),

i) **identyfikacja systemu bezzałogowego** - zdolność do wyróżnienia cech charakterystycznych rozpoznanego systemu bezzałogowego; w wyniku procesu identyfikacji można zidentyfikować główne cechy techniczne np. konstrukcję lub określić konkretny model systemu bezzałogowego lub uzyskać charakterystykę sygnału elektromagnetycznego łącza sterowania systemem bezzałogowym oraz transmisji danych sensorycznych z systemu bezzałogowego, jak również można określić lokalizację stacji sterowania operatora systemu bezzałogowego, (np. określenie marki platformy bezzałogowej, wskazanie miejsca pilota oraz lokalizacji i trajektorii platformy),

j) **detekcja, rozpoznanie i identyfikacja systemu bezzałogowego** - proces realizowany w sposób ciągły automatycznie (bez udziału operatora systemu antydronowego) lub półautomatycznie (z udziałem operatora systemu antydronowego); w celu realizacji procesu detekcji, rozpoznania i identyfikacji wykorzystywane są różne urządzenia rozpoznawcze tj. sensory, mikrofony i kamery; w systemie antydronowym mogą zostać wykorzystane pojedyncze techniki lub kilka jednocześnie np. sensory w zakresie rozpoznania radarowego, elektronicznego i obrazowego w różnej konfiguracji i ilości w zależności od rodzaju systemu antydronowego oraz charakterystyki i topologii IK,

k) **obezwładnienie systemu bezzałogowego** - zdolność do neutralizacji tj. zniszczenia, uszkodzenia lub zakłócenia pracy systemu bezzałogowego lub jego podsystemów lub pozbawienie operatora możliwości sterowania systemem bezzałogowym w celu uniemożliwienia dalszej realizacji misji i zadań przez system bezzałogowy,

l) **incydent** – należy przez to rozumieć sytuację, o której mowa w pkt 5.9 rozporządzenia ministra spraw wewnętrznych i administracji z dnia 22 lipca 2016 r.

w sprawie katalogu incydentów o charakterze terrorystycznym (Dz.U.2017 poz.1517),

m) zdarzenie – należy przez to rozumieć sytuację, która powstała na skutek intencjonalnego lub przypadkowego działania z udziałem systemu bezzałogowego, która niesie zagrożenie dla infrastruktury krytycznej oraz może wywołać negatywne skutki w przestrzeni bezpieczeństwa publicznego,

n) obszar o obowiązkowej ochronie – obszar podlegający obowiązkowej ochronie wynikającej z przepisów lub wskazany przez ministrów, kierowników urzędów centralnych lub wojewodów, odpowiednio wydzielony i oznakowany,

o) strefa oddziaływania – strefa obejmująca obszar obowiązkowej ochrony wraz z obszarem wykraczającym poza ochronę, z którego może nastąpić oddziaływanie ze strony systemu bezzałogowego na IK.

2.5.4.3. Zakres stosowania Standardów

Standardy dotyczą zagrożeń, których źródłem jest umyślne (celowe) lub nieumyślne działanie człowieka, z wykorzystaniem systemu bezzałogowego operującego w powietrzu, wodzie lub na lądzie.

Standardy umożliwią operatorom IK:

1. identyfikowanie obszarów bezpieczeństwa i aktywów podatnych na zagrożenia stwarzane przez systemy bezzałogowe;
2. wdrażanie zasad pozwalających na analizowanie zagrożeń i skutków powstałych lub mogących powstać w następstwie incydentów z udziałem systemów bezzałogowych;
3. doskonalenie metodyki zarządzania ryzykiem, w celu określania priorytetów dla poszczególnych działań związanych z ochroną przed skutkami wykorzystania systemów bezzałogowych,
4. określanie mechanizmów analizowania szans i zagrożeń wynikających ze zmian na rynku producentów i użytkowników systemów bezzałogowych i systemów antydronowych,
5. monitorowanie wymagań prawnych oraz zmian zachodzących w środowisku bezpieczeństwa narodowego, mających odniesienie do systemów bezzałogowych,
6. tworzenie możliwości do testowania, organizacji ćwiczeń i reagowania pracowników i komórek organizacyjnych operatora IK na incydenty związane z systemami bezzałogowymi,
7. doskonalenie zasad zgłaszania i wykonywania misji systemów bezzałogowych, w przypadku dopuszczenia systemów obcych do działania na obszarze IK oraz stosowania własnych systemów bezzałogowych,

8. doskonalenie rozwiązań organizacyjno-technicznych w zakresie wykrywania i neutralizacji systemów bezzałogowych, o ile zostały przyjęte i wdrożone w ramach strategii bezpieczeństwa,
9. tworzenie i doskonalenie metodyki bezpiecznego wdrażania technicznych elementów ochrony przed niepożądanym oddziaływaniem systemów bezzałogowych, w szczególności w zakresie:
   9.1. metod oceny skuteczności rozwiązań technicznych dokonanych przez uznane organizacje trzecie, na podstawie funkcjonujących przepisów prawa oraz norm zharmonizowanych;
   9.2. wieloczynnikowej analizy kontekstu funkcjonowania operatora IK określającej ograniczenia dla wdrożenia ochrony;
   9.3. określenia minimalnych wymagań dla technicznych elementów ochrony, jeśli są przesłanki do zastosowania standardów w zakresie antyterrorystycznym.

Standardy wspomagają proces decyzyjny organów administracji państwowej w zakresie:

1. Diagnozy podatności poszczególnych obszarów bezpieczeństwa, z uwzględnieniem zagrożeń stwarzanych z wykorzystaniem systemów bezzałogowych,
2. Wdrażania wniosków do wzmacniania odporności podmiotów krytycznych w poszczególnych sektorach IK,
3. Opracowywania strategii wzmacniania nadzorowanego bezpieczeństwa, uwzględniającej zastosowanie systemów bezzałogowych i antydronowych.

2.5.4.4. Odwołania normatywne

Regulacje i wymagania dotyczące systemów bezzałogowych wynikają wprost lub pośrednio z europejskiego i krajowego systemu prawnego, posiadającego źródła w rozporządzeniach Parlamentu Europejskiego i Rady Unii Europejskiej oraz w ustawach: prawo lotnicze, prawo telekomunikacyjne, o ochronie osób i mienia, o działaniach antyterrorystycznych, zarządzaniu kryzysowym, jak również z przepisów wykonawczych do tych ustaw.

Wymagania określające standard organizacyjny, techniczny, kompetencyjny oraz system szkolenia i doskonalenia zawodowego, zawarte są także w wymaganiach branżowych i sektorowych, wytycznych oraz zasadach lub zadeklarowanych normach.

Wymagania mogą wynikać także z polityki bezpieczeństwa operatora IK oraz z dokumentów poszczególnych koordynatorów systemów IK.

2.5.4.5. Zakres prac przygotowawczych operatora IK do podjęcia decyzji o tworzeniu systemu zapobiegania, reagowania lub ograniczania skutków zagrożeń stwarzanych przez incydenty z użyciem systemów bezzałogowych

2.5.4.5.1. Określenie kontekstu funkcjonowania operatora IK

Operator określa zewnętrzne oraz wewnętrzne czynniki zagrożeń mogące mieć wpływ na prowadzoną działalność. Identyfikacja tych czynników wraz z wymaganiami ujętymi w NPOIK stanowi podstawę do uruchomienia procesu analizy zagrożeń i oceny ryzyka oraz opracowania (lub aktualizacji) Planu Ochrony Infrastruktury Krytycznej (POIK).

Dobrą praktyką jest, aby zidentyfikowane najważniejsze procesy i aktywa do ich realizacji wskazane przez operatora IK oraz procesy zlecane na zewnątrz lub wynikające ze współzależności z interesariuszami były uwzględnione w procesie szacowania ryzyka. Zidentyfikowanie zagrożeń ze strony incydentów z użyciem systemów bezzałogowych, może skutkować zmianą w podejściu do oceny ryzyka oraz postrzegania bezpieczeństwa IK przez operatora IK lub koordynatora systemu IK. W procesie analizowania zagrożeń i oceny ryzyka dokonuje się zakresu współzależności między operatorem IK, a interesariuszem, o ile jest to wyrażone we współpracy lub projektowanej umowie dotyczącej stosowania systemów bezzałogowych lub antydronowych. Ocena aktualnej lub przyszłej współpracy powinna uwzględniać następujący podmioty:

- mające wpływ, będące pod wpływem lub mogące uważać siebie za podmiot, na który może oddziaływać działalność IK,
- realizujące zadania podwykonawcze w procesach związanych z funkcjonowaniem obiektów, instalacji, urządzeń i usług krytycznych dla operatora IK,
- organy administracji publicznej.

Operator IK powinien uwzględniać również zalecenia po kontroli lub audycie funkcjonalności przez organy administracji publicznej oraz służby realizujące zadania w sferze porządku i bezpieczeństwa publicznego lub bezpieczeństwa powszechnego, jak też uwagi wynikające z uzgadniania POIK i reagowania w czasie incydentów lub po ich wystąpieniu.

2.5.4.5.2. Opracowanie wewnętrznego dokumentu

W procesie analizy bezpieczeństwa IK, mającego wpływ na realizację misji publicznej i biznesowej, operator przygotowuje wewnętrzny dokument, którego celem jest przygotowanie i przedstawienie zasadności lub braku zasadności tworzenia systemu zapobiegania, reagowania lub ograniczania skutków zagrożeń ze strony

systemów bezzałogowych. Opracowanie dokumentu należy poprzedzić oceną wniosków wynikających z procesu identyfikacji i analizy zagrożeń, która może się odbywać według zasad przyjętych i stosowanych przez operatora IK. W kolejnym etapie prac dotyczących identyfikacji ryzyka dla IK od systemów bezzałogowych na poziomie nieakceptowalnym, zasadne jest postępowanie zgodne z przyjętymi przez operatora IK procedurami, której wynikiem powinna być rekomendacja przygotowana dla kierownictwa. W przypadku przygotowania uzasadnienia dotyczącego zasadności utworzenia takiego systemu, zespół rekomendujący wnioski uwzględnia zakres niezbędnych zmian w organizacji oraz odniesienie do potrzeby tworzenia i działań w sferze antydronowej.

Operator IK powinien oszacować ryzyko co najmniej z zastosowaniem:

a) oceny prawdopodobieństwa wystąpienia zidentyfikowanego zagrożenia,
b) oceny skutków bezpośrednich (dla organizacji - operatora) lub / oraz pośrednich (dla stron zainteresowanych) wystąpienia zidentyfikowanego zagrożenia,
c) spójnej i jednoznacznej miary dla opisu prawdopodobieństwa i skutków.

Opracowany po oszacowaniu ryzyka dokument powinien zawierać co najmniej następujące dane:

a) zakres procesów i usług zidentyfikowanych jako krytyczne i objęte ochroną IK,
b) procesy bezpośrednio lub pośrednio związane z zagrożeniami stwarzanymi przez systemy bezzałogowe,
c) powiązania pomiędzy najważniejszymi procesami i usługami a funkcjami wspomagającymi te procesy i usługi, z uwzględnieniem obiektów i instalacji oraz innych aktywów narażonych na zagrożenia ze strony incydentu z wykorzystaniem systemów bezzałogowych.

Dokument powinien zawierać wizualizację zakresu obszarowego i funkcjonalnego IK, z wykorzystaniem dostępnych metod graficznych i elektronicznych.

W przypadku, gdy ryzyko nie występuje lub jest znikome nie ma potrzeby tworzenia odrębnego dokumentu.

W przypadku pozytywnej rekomendacji tworzenia systemu zapobiegania, reagowania lub ograniczania skutków zagrożeń od incydentów z udziałem systemów bezzałogowych dokument powinien określać:

a) zakres działalności, dla której wdrażane są wymagania Standardów,
b) lokalizację obiektów, dla których wdrażany jest system zapobiegania zagrożeniom stwarzanym przez systemy bezzałogowe,
c) środki techniczne oraz mechanizmy organizacyjne, które należy zapewnić aby spełnić wymagania Standardów,
d) zasady nadzorowania tworzonego systemu, który powinien być dostosowany do misji publicznej realizowanej przez operatora IK.

2.5.4.5.3. Zasady zapobiegania zagrożeniom stwarzanym przez systemy bezzałogowe

Zasady zapobiegania, reagowania lub ograniczania skutków zagrożeń stwarzanych przez systemy bezzałogowe, stanowiące część polityki bezpieczeństwa operatora IK, powinny być:

a) adekwatne do zagrożeń stwarzanych przez systemy bezzałogowe i do wyników analizy ryzyka,
b) opracowane w formie pisemnej i zatwierdzone przez kierownictwo,
c) skutecznie zakomunikowane personelowi operatora IK oraz w zależności od oceny ryzyka, dostawcom usług i podwykonawcom,
d) poddawane regularnym przeglądom pod kątem aktualności, przydatności i adekwatności, każdorazowo przy prowadzonej ocenie ryzyka.

Dla osiągnięcia celów określonych w zasadach zapobiegania, reagowania lub ograniczania skutków zagrożeń stwarzanych przez systemy bezzałogowe operator IK powinien:

a) określić zadania elementarne dla realizacji poszczególnych celów,
b) zapewnić zasoby niezbędne do realizacji celów i zadań,
c) wskazać mierzalne kryteria oceny realizacji celów i zadań,
d) określić terminy realizacji poszczególnych celów i zadań.

2.5.4.5.4. Planowanie

Jedną z głównych danych wejściowych niezbędnych do planowania i funkcjonowania mechanizmów zapobiegania zagrożeniom stwarzanym przez systemy bezzałogowe są rezultaty analizy ryzyka. Operator IK powinien udoskonalić istniejącą metodykę zarządzania ryzykiem, odpowiednią dla wielkości i stopnia skomplikowania organizacji lub wdrożyć nową z uwzględnieniem postanowień wynikających z normy PN - ISO 31000 lub innej normy, która wynika z uznanego standardu zarządzania ryzykiem.

Metody zarządzania ryzykiem uwzględniające zagrożenia stwarzane przez systemy bezzałogowe dla IK powinny być zintegrowane z dokumentacją już funkcjonujących systemów bezpieczeństwa oraz zarządzania operatora IK.

Metody zarządzania ryzykiem powinny określać wewnętrzne wymagania organizacji niezbędne dla:

a) identyfikacji zagrożeń związanych z systemami bezzałogowymi,
b) metody szacowania ryzyka,
c) planowania sposobu postępowania z ryzykiem,
d) oceny rezultatów postępowania z ryzykiem i ponownego szacowania ryzyka,
e) sposobu nadzorowania udokumentowanych informacji stanowiących rezultaty zarządzania ryzykiem.

Operator IK powinien być przygotowany do bieżącego identyfikowania oraz monitorowania zagrożenia stwarzanego przez systemy bezzałogowe na podstawie analiz następujących danych:

a) wyników analizy kontekstu działalności,
b) wyników analiz zdarzeń z udziałem systemów bezzałogowych już zaistniałych u operatora,
c) informacji o zdarzeniach z udziałem systemów bezzałogowych zaistniałych w ramach działalności innych operatorów,
d) rezultatów postępowania z ryzykiem w przypadku, gdy zastosowane postępowanie z ryzykiem wywołuje w konsekwencji kolejne zagrożenia,
e) wyników kontroli i audytów – wewnętrznych i zewnętrznych,
f) zgłoszeń i informacji pozyskanych od personelu oraz interesariuszy,
g) zaleceń i wniosków uprawnionych służb i instytucji realizujących misję bezpieczeństwa publicznego,
h) informacji z innych dostępnych źródeł.

Zidentyfikowane zagrożenia powinny zostać przedstawione kierownictwu w postaci udokumentowanej informacji.

2.5.4.6. Zasady odpowiedzialności

Operator IK odpowiada za:

a) opracowanie zasad zapobiegania zagrożeniom stwarzanym przez systemy bezzałogowe,
b) zapewnienie niezbędnych zasobów do wdrożenia, utrzymania i doskonalenia mechanizmów zapobiegania zagrożeniom,
c) wskazanie ról, uprawnień i odpowiedzialności personelu w zakresie realizacji wymagań na rzecz zapobiegania tego rodzaju zagrożeniom,
d) zapewnienie okresowego przeglądu i doskonalenia zasad zapobiegania zagrożeniom stwarzanym przez systemy bezzałogowe,
e) skorygowanie istniejących metodyk zarządzania ryzykiem oraz kryteriów akceptowalności ryzyk pochodzących od systemów bezzałogowych lub opracowanie i wdrożenie nowej metodyki uwzgledniającej zagrożenia stwarzane przez systemy bezzałogowe,
f) promowanie świadomości w zakresie wagi zagrożeń stwarzanych przez systemy bezzałogowe wśród personelu i interesariuszy,
g) stałe analizowanie kontekstu funkcjonowania operatora IK pod kątem zagrożeń stwarzanych przez systemy bezzałogowe,
h) uczestnictwo w kluczowych działaniach wzmacniających bezpieczeństwo operatora IK, w tym w zakresie funkcjonowania mechanizmów zapobiegania zagrożeniom od systemów bezzałogowych, a także we wdrażaniu wniosków z kontroli i audytów wewnętrznych i zewnętrznych,

i) zapewnienie, że wymagania i mechanizmy dotyczące zapobiegania zagrożeniom ze strony systemów bezzałogowych zostały włączone do procesów biznesowych funkcjonujących u operatora IK.

2.5.4.7. Zadania i odpowiedzialność w ramach struktury operatora IK

Kierownictwo powinno określić zadania, uprawnienia i odpowiedzialność za wdrożenie, utrzymanie i doskonalenie mechanizmów zapobiegania zagrożeniom ze strony systemów bezzałogowych na odpowiednich poziomach struktury organizacyjnej operatora IK, w sposób gwarantujący sprawną i efektywną realizację polityki bezpieczeństwa.

Powinna zostać określona metoda, tryb i forma raportowania o incydentach do kierownictwa w zakresie skuteczności istniejących mechanizmów, procedur i instrukcji dotyczących zapobiegania zagrożeniom stwarzanym przez systemy bezzałogowe.

2.5.4.8. Przygotowanie operatorów IK do reagowania na zagrożenia stwarzane przez systemy bezzałogowe

Proces przygotowywania się operatora IK na incydenty z udziałem systemów bezzałogowych powinien zawsze rozpoczynać się od udzielenia odpowiedzi przez właścicieli ryzyk i zarządzających wszystkimi obszarami bezpieczeństwa, które procesy i usługi oraz aktywa są kluczowe dla funkcjonalności oraz czy posiadane zabezpieczenia wystarczają do akceptacji lub tolerowania ryzyk pozwalających na zachowanie odporności oraz ciągłości działania IK. Operator IK w procesie przygotowania się do reagowania powinien:

1. potwierdzić wytypowane procesy i usługi oraz wskazane aktywa, w tym obiekty, instalacje, urządzenia za najważniejsze dla funkcjonowania IK,
2. określić możliwe incydenty dla wytypowanych obiektów np. rozpoznanie elementów składowych IK, celowy atak, przypadkowy upadek, zwykły wlot niekontrolowany,
3. określić potencjalne zagrożenia mające wpływ na IK oraz powodujące krótkie lub długotrwałe przerwanie funkcjonalności IK na podstawie reprezentatywnych scenariuszy zdarzeń,
4. określić prawdopodobieństwo wystąpienia incydentu z udziałem systemów bezzałogowych dla wytypowanych procesów, usług, obiektów, instalacji lub urządzeń,
5. opracować procedury powiadamiania oraz schemat działania osób odpowiedzialnych za reagowanie w przypadku zdarzenia,
6. opracować procedury powiadamiania interesariuszy,
7. przygotować na podstawie wniosków z oceny ryzyka oraz własnych możliwości organizacyjnych, technicznych i finansowych mechanizmy dotyczące zasad

zabezpieczenia przestrzeni otaczającej IK, wraz z procedowaniem jej zamknięcia, ograniczenia czasowego lub wydzielenia i oznakowania,

8. przygotować plan uruchomienia procesu zabezpieczenia obszaru IK systemami antydronowymi zdolnymi skutecznie wykrywać i neutralizować systemy bezzałogowe z wykorzystaniem zasad ujętych w podrozdziale 2.5.4.9. i 2.5.4.10.

Operator IK jest przygotowany do rejestrowania incydentów oraz do przygotowywania raportów ze zdarzeń z udziałem systemów bezzałogowych w których powinien uwzględnić, co najmniej:

1/ osobę lub osoby oraz dział bezpieczeństwa odpowiedzialny za rejestr zdarzeń ,
2/ datę i godziny zdarzenia oraz miejsca lub obiekty objęte incydentem,
3/ rodzaj lub model systemu bezzałogowego oraz kierunek z którego przybył,
4/ podmiot zgłaszający incydent,
5/ rodzaj zdarzenia,
6/ konsekwencje (skutki) zdarzenia.

W wersji rozszerzonej formularz „opis incydentu z udziałem systemu bezzałogowego" powinien rejestrować następujące informacje:

1) lokalizacja incydentu na mapie lub opis lokalizacji,
2) opis miejsca (np. prywatna posesja, bocznica kolejowa),
3) rodzaj zdarzenia (wybór z listy np. przelot/wlot, zawis, obecność/ aktywność, dostarczanie ładunku/ pozostawienie, zdarzenie nieumyślne/ kolizja, uderzenie celowe, sabotaż (detonacja/podpalenie),
4) charakterystyka obiektu/ urządzania (wybór z listy poprzez wskazanie np.: rodzaju napędu: śmigłowe, odrzutowe, rakietowe, swobodne jeżdżące, swobodne pływające, ilość napędów; jednonapędowe, wielonapędowe, posiadające skrzydła, oświetlenie, kolor, szybkość poruszania, wydające dźwięki, inne cechy),
5) opis przyczyny zdarzenia.

Operator IK jest przygotowany do realizacji testów systemu detekcji, o ile podjął decyzje o tworzeniu systemów antydronowych. Ogólne założenia do realizacji testów systemu detekcji na przykładzie bezzałogowych statków powietrznych (BSP) powinny przewidywać następujące zadania:

1. wykonywanie, tak aby uwzględniać różne warunki pogodowe, porę dnia, porę roku oraz różne uwarunkowania pracy chronionego obiektu,
2. naloty BSP powinny być wykonywane z różnych kierunków oraz na różnych wysokościach; w szczególności należy uwzględnić wykonywanie lotów na wysokości poniżej wysokości przeszkód występujących na obszarze, który system ma docelowo ochraniać,

3. podczas testów powinny zostać wykonane naloty w ramach, których zostanie wykorzystanych kilka BSP jednocześnie,
4. proponuje się, aby w ramach każdej z sesji testowej zostały wykonane przynajmniej 5 nalotów, każdy z innego kierunku i na innej wysokości,
5. naloty w testach powinny być wykonywane przy pomocy BSP różnych producentów oraz klas. Zaleca się, aby w trakcie testów użyć BSP przynajmniej dwóch różnych producentów oraz modeli mieszczących się w kategoriach C0, C1, C2, C3, C4, własnej konstrukcji oraz dronem bez nadanej klasy o masie poniżej 25 kg,
6. jeżeli testy nie powinny być lub nie mogą być wykonywane na terenie obiektu IK to powinny być przeprowadzone na innym obiekcie o zbliżonej charakterystyce,
7. testy powinny być wykonywane w kontrolowanym środowisku oraz bezpiecznych warunkach, poza godzinami eksploatacji obiektu lub z jego częściowym wyłączeniem z eksploatacji, tak aby w sytuacji awarii i utraty kontroli nad BSP nie spowodował on zagrożenia dla zdrowia i życia ludzi oraz strat w mieniu;
8. zakończenie testów powinno być podsumowane raportem, w którym należy przedłożyć dane wynikające z pkt 1-7, uwzględniające widoczność oraz warunki pogodowe, w tym temperaturę i siłę wiatru, deszcz, śnieg, a także odniesienie do numeru i rodzaju (modelu) drona, kierunku, wysokości i prędkości jego nalotu, odległości od obiektu w momencie wykrycia a także efektów działania systemu wraz z wnioskami.

2.5.4.9. Propozycja metody oceny skuteczności systemu detekcji platform bezzałogowych

Urządzenia detekcyjne w systemach ochrony IK dobiera się oceniając prawdopodobieństwo detekcji niepożądanej aktywności w danych warunkach.

Dla każdego urządzenia detekcyjnego należy eksperymentalnie ocenić prawdopodobieństwo detekcji platformy bezzałogowej w danych warunkach pracy oraz w wymaganym czasie. Dane warunki pracy urządzenia to warunki, w jakich urządzenie będzie pracować, co oznacza, że ocenie podlega prawdopodobieństwo detekcji platformy bezzałogowej:

→ przy różnych warunkach pogodowych (wilgotność powietrza, mgła, deszcz, śnieg, brak opadów, wysoka temperatura, niska temperatura, dzień, noc, brak wiatru, silny wiatr, środowisko o wysokim poziomie hałasu, środowisko o niskim poziomie hałasu, itd.),

→ w danej lokalizacji (teren płaski, górzysty, teren porośnięty krzakami, lasem, teren zabudowany, teren niezabudowany, droga utwardzona, droga polna, morskie warunki sztormowe, brak sztormu, itd.),

→ w warunkach występowania zewnętrznych źródeł promieniowania elektromagnetycznego (radary dla lotnictwa załogowego, stacje BTS - oryg. base transceiver station przekaźniki radiowe, itd.),

→ dla różnych typów systemów bezzałogowych (multirotor, samolot, śmigłowiec, statek o nietypowym kształcie, pojazd kołowy, pojazd gąsienicowy, bezzałogowa łódź podwodna, bezzałogowa łódź nawodna, itd.),

→ przy różnych sposobach realizacji ataku (lot na wysokim pułapie, lot nisko nad ziemią, lot z dużą prędkością, lot z niewielką prędkością, lot po linii prostej, lot po trajektorii urozmaiconej, jazda po drodze utwardzonej, jazda po drodze gruntowej, w trawie, w lesie, rejs po wodzie spokojnej, rejs w warunkach sztormowych, itd.),

→ przy różnych kompetencjach personelu ochrony fizycznej odpowiedzialnego za obsługę urządzeń detekcyjnych (np. pracownik dobrze wyszkolony, pracownik bez doświadczenia).

Ocenę prawdopodobieństwa detekcji można przeprowadzić w ten sposób, że zlicza się ilość wykryć lecącego bezzałogowego statku powietrznego na sto przelotów lub ilość wykryć jadących pojazdów kołowych lub gąsienicowych na sto przejazdów lub ilość wykryć bezzałogowych platform płynących pod lub na wodzie na sto przepłynięć.

Wykrycia te muszą być prawidłowe. Należy odrzucić wskazania aparatury, która niewłaściwie zinterpretowała wykrycie, rejestrując obiekty nie będące platformami bezzałogowymi. Uwzględnienie tzw. fałszywych detekcji pozwoli określić rzeczywistą ilość prawidłowych wykryć.

Dalsze rozważania prowadzone są dla przykładu lecącego BSP, ale dla pojazdów lub łodzi ocena prawdopodobieństwa będzie odbywała się na podobnej zasadzie.

W przypadku stu wykryć na sto przelotów BSP w danych warunkach prawdopodobieństwo będzie wynosiło 100%, w przypadku nie wykrycia ani jednego przelotu prawdopodobieństwo będzie wynosiło 0%. Dodatkowym parametrem podlegającym ocenie musi być czas detekcji nazwany na potrzeby Standardów wymaganym czasem. Wymagany czas to taki czas, w którym dron zostaje wykryty na tyle wcześnie by mogły zostać uruchomione dedykowane procedury na wypadek danego rodzaju incydentu, w tym ataku platformy bezzałogowej. Prawdopodobieństwo detekcji platformy bezzałogowej w danych warunkach i w wymaganym czasie oznaczamy jako P_{UX}, przy czym indeks *UX* jest *x*-owym urządzeniem detekcyjnym.

Całkowite prawdopodobieństwo detekcji platformy bezzałogowej przez system zbudowany z N urządzeń będzie wyrażone wzorem:

$$P_{całkD} = 1 - (1 - P_{U1})(1 - P_{U2})\dots(1 - P_{UN})$$

Załóżmy, że budowany jest system detekcji platform bezzałogowych zbudowany z trzech urządzeń detekcyjnych. W opisywanym przykładzie, w którym system detekcji zbudowany jest z trzech urządzeń, otrzymamy po testach trzy prawdopodobieństwa $P_{U1}, P_{U2} oraz P_{U3}$.W przypadku opisanego systemu wzór przybiera postać:

$$P_{całkD} = 1 - (1 - P_{U1})(1 - P_{U2})(1 - P_{U3})$$

Przykład: rozważamy system złożony z trzech urządzeń detekcyjnych, których prawdopodobieństwo detekcji wyznaczone dla danych warunków i w wymaganym czasie wynosi odpowiednio: $P_{U1} = 0{,}33, P_{U2} = 0{,}65, P_{U3} = 0{,}54$. Oznacza to, że urządzenia te na sto przelotów wykryły drona odpowiednio: $U1 \rightarrow 33$, $U2 \rightarrow 65$, $U1 \rightarrow 54$ razy. Zatem obliczone całkowite prawdopodobieństwo detekcji drona przez taki system będzie równe:

$$P_{całkD} = 1 - (1 - 0.33)(1 - 0.65)(1 - 0.54)$$

$$P_{całkD} = 0.89$$

lub inaczej zapisując:

$$P_{całkD} = 89\%$$

Wynik ten wskazuje, że system złożony z urządzeń Pu1, Pu2 oraz Pu3 wykryje platformę bezzałogową z prawdopodobieństwem 89%, a więc na sto przelotów wykryje 89 przelotów. Gdyby obiekt był chroniony takim systemem to na każde sto przelotów jedenaście nie zostałoby wykrytych i mogłoby skutecznie przeprowadzić atak.

Zadaniem zarządzającego chronionym obiektem jest wyznaczenie minimalnej wartości progowej $P_{całkD}$ poniżej której system uznaje się za nieskuteczny. W przypadku gdy system uzna się za nieskuteczny, należy podjąć działania mające na celu podniesienie wartości $P_{całkD}$. Można to osiągnąć poprzez:

→ zmianę warunków detekcji, np. w przypadku gdy urządzenie nie radzi sobie dobrze w terenie otwartym, porośniętym krzakami, można wyciąć krzaki,

→ zwiększenie ilości urządzeń detekcyjnych w systemie przy założeniu, że kolejne urządzenia działają na innej zasadzie niż te już użyte do budowy systemu,

→ zmianę urządzenie o najniższym prawdopodobieństwie detekcji na lepsze,

→ w przypadku detekcji pojazdów kołowych lub gąsienicowych stosowanie urządzeń spowalniających,

lub

→ w przypadku gdy nie ma na rynku lepszego modelu urządzenia należy przystąpić do działań prewencyjnych, opisanych w dalszej części podrozdziału, tak by nie dopuścić do rozpoczęcia ataku.

Przykład: zakładamy, że system detekcji platform bezzałogowych opisany powyżej nie spełnia oczekiwań i chcemy by prawdopodobieństwo detekcji systemu było wyższe. Zwiększenie prawdopodobieństwa detekcji zrealizujemy przez dołożenie do systemu innych urządzeń detekcyjnych, działających na innej zasadzie niż te, które już w systemie pracują.

Dostawmy zatem urządzenia o prawdopodobieństwie detekcji platformy bezzałogowej w danych warunkach i w wymaganym czasie odpowiednio: Pu4 = 0.50

oraz Pu5 = 0.60. Tym samym rozważany system złożony jest z pięciu urządzeń detekcyjnych. Zatem obliczone całkowite prawdopodobieństwo detekcji platformy przez taki system będzie równe:

$$P_{całkD} = 1 - (1 - P_{U1})(1 - P_{U2})(1 - P_{U3})(1 - P_{U4})(1 - P_{U5})$$

$$P_{całkD} = 1 - (1 - 0.33)(1 - 0.65)(1 - 0.54)(1 - 0.50)(1 - 0.60)$$

$$P_{całkD} = 0.98$$

lub inaczej zapisując:

$$P_{całkD} = 98\%$$

Wynik ten wskazuje, że system o nieakceptowalnym prawdopodobieństwie detekcji platformy bezzałogowej, po uzupełnieniu go o inne urządzenia detekcyjne jest bardzo skuteczny, a całkowite prawdopodobieństwo detekcji zwiększa się o ok. 10% i wynosi 98%. Gdyby obiekt był chroniony takim systemem to na każde sto przelotów tylko dwa nie zostałyby wykryte i mogłoby skutecznie przeprowadzić atak.

Badając urządzenia detekcyjne należy pamiętać o kilku zasadach, które decydują o skuteczności (a więc prawdopodobieństwie) detekcji:

1. urządzenia detekcyjne muszą być absolutnie od siebie niezależne. Niezależność oznacza, że urządzenia te muszą posiadać różne, odseparowane od siebie źródła zasilania pracujące w warunkach normalnych i źródła zasilania pracujące w przypadku awarii, muszą posiadać różne, odseparowane od siebie, zabezpieczenia przed przerwaniem pracy, urządzenia detekcyjne nie mogą też w żaden sposób na siebie wpływać, np. poprzez wzajemne zakłócenia pracy poprzez silne pole elektromagnetyczne,
2. urządzenia detekcyjne, a także cały system detekcji, muszą być okresowo kontrolowane. Okresowa kontrola wynika z faktu, że każdy obiekt techniczny może ulec uszkodzeniu co spowoduje radykalne obniżenie wartości $P_{całkD}$, może nawet poniżej dopuszczalnej wartości progowej. Kontrola wynika także z faktu, że każdy obiekt techniczny starzeje się. System detekcji powinien być także testowany w każdym przypadku, w którym następuje zmiana warunków pracy systemu. Taką zmianą może być np. wybudowanie budynków lub budowli w rejonie chronionego obiektu,
3. priorytetem dla zarządzającego chronionym obiektem powinno być zapewnienie skutecznej detekcji atakującej platformy bezzałogowej, a nie koszty budowy systemu.

System detekcji platform bezzałogowych uznaje się za właściwie skonstruowany jeśli wartość $P_{całkD}$ jest wyższa niż dopuszczalna, minimalna wartość progowa.

Przy projektowaniu systemu detekcji platform bezzałogowych dla chronionego obiektu należy dobierać urządzenia detekcyjne w taki sposób, aby ich praca nie wpływała negatywnie na działanie urządzeń wykorzystywanych w chronionym obiekcie.

Do negatywnego wpływu można zaliczyć np. pole elektromagnetyczne emitowane przez radar. Jeśli pole, jego częstotliwość i natężenie, zakłócałoby w jakikolwiek sposób pracę chronionego obiektu to należy zrezygnować z takiego urządzenia detekcyjnego albo należy zastosować środki redukujące wpływ pola elektromagnetycznego na urządzenia w chronionym obiekcie, np. poprzez właściwe ekranowanie.

2.5.4.10. Propozycja metody oceny skuteczności systemu neutralizacji platform bezzałogowych

System neutralizacji platform bezzałogowych powinien być zbudowany z urządzeń neutralizujących platformy w różny sposób, tak by prawdopodobieństwo neutralizacji było dostatecznie wysokie. Stosowanie urządzeń działających na różnych zasadach zapewnia, że w każdych warunkach system ten spełni swoje zadanie, czyli zneutralizuje platformę. Urządzenia neutralizujące platformy bezzałogowe powinny być dobrane do systemu po ocenie ich skuteczności, a więc prawdopodobieństwa neutralizowania platformy w danych warunkach i w wymaganym czasie. Ocena prawdopodobieństwa neutralizacji platformy bezzałogowej powinna się odbyć w warunkach takich samych w jakich ocenia się urządzenia służące detekcji platform. Ocenie podlegać powinna skuteczność neutralizacji w zależności od:

→ różnych warunków pogodowych (wilgotność powietrza, mgła, deszcz, śnieg, brak opadów, wysoka temperatura, niska temperatura, dzień, noc, brak wiatru, silny wiatr, itd.),

→ lokalizacji chronionego obiektu (teren płaski, górzysty, teren porośnięty krzakami, lasem, teren zabudowany, teren niezabudowany, droga utwardzona, droga polna, morskie warunki sztormowe, brak sztormu, zaludnienie terenu, itd.),

→ warunków występowania zewnętrznych źródeł promieniowania elektromagnetycznego (radary dla lotnictwa załogowego, stacje BTS, przekaźniki radiowe, itd.),

→ różnych typów systemów bezzałogowych (multirotor, samolot, śmigłowiec, statek o nietypowym kształcie, pojazd kołowy, pojazd gąsienicowy, bezzałogowa łódź podwodna, bezzałogowa łódź nawodna, itd.),

→ sposobów realizacji ataku (lot na wysokim pułapie, lot nisko nad ziemią, lot z dużą prędkością, lot z niewielką prędkością, lot po linii prostej, lot po trajektorii urozmaiconej, jazda po drodze utwardzonej, jazda po drodze gruntowej, w trawie, w lesie, rejs po wodzie spokojnej, rejs w warunkach sztormowych, itd.),

→ różnych kompetencji personelu ochrony fizycznej odpowiedzialnego za obsługę urządzeń detekcyjnych (np. pracownik dobrze wyszkolony, pracownik bez doświadczenia).

Ocenę prawdopodobieństwa neutralizacji można przeprowadzić w ten sposób, że zlicza się ilość neutralizacji lecącego bezzałogowego statku powietrznego na sto

przelotów lub ilość neutralizacji jadących pojazdów kołowych lub gąsienicowych na sto przejazdów lub ilość neutralizacji bezzałogowych platform płynących pod lub na wodzie na sto przepłynięć. Dalsze rozważania prowadzone są dla przykładu lecącego BSP, ale dla pojazdów lub łodzi sposób oceny prawdopodobieństwa neutralizacji będzie taki sam.

Ocenę prawdopodobieństwa neutralizacji platformy bezzałogowej każdego urządzenia neutralizującego można przeprowadzić zliczając ilość skutecznych działań, w wyniku których platforma przestaje stanowić zagrożenie dla chronionego obiektu, na sto prób. Dodatkowym parametrem podlegającym ocenie powinien być wymagany czas potrzebny na skuteczną neutralizację platformy.

Za wymagany czas należy uznać taki czas, w którym platforma zostanie zneutralizowana na tyle szybko by nie była w stanie skutecznie przeprowadzić ataku, np. na tyle szybko by platforma bezzałogowa nie zdołała przewieźć ładunku wybuchowego na tyle blisko celu by jego wybuch spowodował straty lub na tyle szybko by platforma bezzałogowa nie mogła zarejestrować obrazu w misji wywiadowczej.

Prawdopodobieństwo neutralizacji atakującej platformy przez urządzenie oznaczamy symbolem P_{UY} przy czym indeks UY jest symbolem y-kowego urządzenia neutralizującego. Całkowite prawdopodobieństwo neutralizacji platformy bezzałogowej przez system złożony z N urządzeń będzie wyrażone wzorem:

$$P_{całkN} = 1 - (1 - P_{U1})(1 - P_{U2})\dots(1 - P_{UN})$$

Przykład: rozważamy system złożony z trzech urządzeń neutralizujących, których prawdopodobieństwo neutralizacji atakującej platformy bezzałogowej wyznaczone dla danych warunków i w wymaganym czasie wynosi odpowiednio: $P_{U1} = 0{,}50, P_{U2} = 0{,}65, P_{U3} = 0{,}64$. Oznacza to, że urządzenia te na sto przelotów zneutralizowały platformę odpowiednio: $U1 \rightarrow 50$, $U2 \rightarrow 65$, $U3 \rightarrow 64$ razy.

Zatem obliczone całkowite prawdopodobieństwo neutralizacji platformy przez taki system będzie równe:

$$P_{całkN} = 1 - (1 - 0.50)(1 - 0.65)(1 - 0.64)$$

$$P_{całkN} = 0.94$$

lub inaczej zapisując:

$$P_{całkD} = 94\%$$

Wynik ten wskazuje, że system złożony z urządzeń $P_{U1}, P_{U1} oraz P_{U1}$ zneutralizuje platformę z prawdopodobieństwem 94%, a więc na sto przelotów wykryje w przybliżeniu 94 przeloty.

Chcąc określić prawdopodobieństwo neutralizacji platformę przez urządzenie należy pamiętać o kilku zasadach, które decydują o skuteczności (a więc prawdopodobieństwie) neutralizacji:

1. urządzenia do neutralizacji muszą być absolutnie od siebie niezależne. Niezależność oznacza, że urządzenia te muszą posiadać różne, odseparowane od siebie źródła zasilania pracujące w warunkach normalnych i źródła zasilania pracujące w przypadku awarii, muszą posiadać różne, odseparowane od siebie, zabezpieczenia przed przerwaniem pracy, urządzenia te nie mogą też w żaden sposób na siebie wpływać, np. wzajemne zakłócenia pracy poprzez silne pole elektromagnetyczne,
2. urządzenia do neutralizacji, a także cały system neutralizacji, muszą być okresowo kontrolowane. Okresowa kontrola wynika z faktu, że każdy obiekt techniczny może ulec uszkodzeniu co spowoduje radykalne obniżenie wartości $P_{całkN}$, może nawet poniżej dopuszczalnej wartości progowej. Kontrola wynika także z faktu, że każdy obiekt techniczny starzeje się. System neutralizacji powinien być także testowany w każdym przypadku, w którym następuje zmiana warunków pracy systemu. Taką zmianą może być np. wybudowanie budynków lub budowli w rejonie chronionego obiektu,
3. priorytetem dla zarządzającego chronionym obiektem powinno być zapewnienie skutecznej neutralizacji atakującej platformy bezzałogowej, a nie koszty budowy systemu.

System neutralizacji platform bezzałogowych uznaje się za właściwie skonstruowany jeśli wartość $P_{całkN}$ jest wyższa niż dopuszczalna, minimalna wartość progowa.

Przy projektowaniu systemu neutralizacji platform dla chronionego obiektu, należy dobierać urządzenia neutralizujące w taki sposób by ich praca nie wpływała negatywnie na obiekt lub pracujących w jego otoczeniu ludzi. Do takiego negatywnego wpływu można zaliczyć np. upadek platformy bezzałogowej w wyniku zestrzelenia urządzeniem laserowym na elementy wyposażenia obiektu lub ludzi.

Energię kinetyczną upadającej platformy opisujemy wzorem:

$$E_k = \frac{1}{2}mv^2 \ ;$$

gdzie: m – jest masą drona, v – prędkością z jaką dron uderza w przeszkodę.

Konsekwencją upadku platformy nawet z niewielką energią kinetyczną może być zranienie lub śmierć człowieka, a w przypadku uderzenia w obiekt techniczny przerwanie jego pracy. Jeśli ryzyko związane z upadkiem platformy na ludzi lub instalacje byłoby nieakceptowalne, należy zastosować środki redukujące poprzez np. budowę osłon.

2.5.4.11. Podsumowanie

1/ Standardy zostały przygotowane w sposób uniwersalny umożliwiający dostosowanie oraz implementację wymagań przez dowolne organizacje, identyfikujące zagrożenia ze strony systemów bezzałogowych i chcące podnieść poziom bezpieczeństwa oraz zapewnić ciągłość działania, w tym poprzez wdrażanie ochrony antydronowej.

2/ Spełnienie Standardów nie zapewnia pełnej odporności na zagrożenia ze strony systemów bezzałogowych, jednakże dowodzi wysokiej świadomości istoty zagrożeń i zaangażowania operatorów IK oraz właścicieli i zarządców obiektów i obszarów o obowiązkowej ochronie.

3/ Stosowanie Standardów nie oznacza szacowania ryzyka tylko w obszarze bezpieczeństwa fizycznego, ale również w obszarach bezpieczeństwa osobowego, technicznego, w tym technologiczno-procesowego, cybernetycznego oraz w ochronie kluczowych procesów i usług wspomagających te i inne obszary bezpieczeństwa przed celową lub przypadkową ingerencją systemów bezzałogowych.

4/ Postanowienia Standardu odnoszą się do projektowanych lub nowelizowanych umów zawieranych między operatorem IK a podmiotem realizującym usługi z zastosowaniem systemów bezzałogowych lub antydronowych.

2.5.5. Najważniejsze rekomendacje dotyczące zapewnienia bezpieczeństwa fizycznego:

1. Nie rozpoczynaj budowy systemu zapewnienia bezpieczeństwa fizycznego bez wcześniejszego określenia chronionych zasobów i potencjalnego atakującego.
2. System jest tak silny jak jego najsłabsze ogniwo.
3. Techniczne środki zapewnienia bezpieczeństwa fizycznego powinny być nadzorowane przez człowieka.
4. Motywacja i kompetencje pracowników ochrony fizycznej są kluczowe.
5. Procedury niezrozumiałe i niestosowane nie chronią.
6. Osoby upoważnione do stosowania środków przymusu bezpośredniego muszą przechodzić regularne szkolenia z tego zakresu.
7. System zapewnienia bezpieczeństwa fizycznego niepoparty identyfikacją i analizą zagrożeń oraz oceną ryzyka może być nieefektywny.
8. Fizyczne ataki na infrastrukturę krytyczną często prowadzą do ogromnych strat.
9. Cykliczna analiza zagrożeń i ocena ryzyka w przestrzeni bezpieczeństwa IK wymaga odniesienia do incydentów z udziałem systemów bezzałogowych.
10. Tworzenie systemu zapobiegania zagrożeniom, reagowania na nie i ograniczania skutków zagrożeń od incydentów stwarzanych przez systemy bezzałogowe wymaga opiniowania eksperckiego.
11. Jeśli w ocenach bezpieczeństwa IK występują ryzyka nieakceptowalne od incydentów stwarzanych przez systemy bezzałogowe operator IK w uzgodnieniu z koordynatorem systemu IK określa strategię i mechanizmy niezbędne do budowy systemów antydronowych.

2.6. Zapewnienie bezpieczeństwa technicznego

Zapewnienie bezpieczeństwa technicznego to zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania obiektów, instalacji, urządzeń technicznych lub wodnych oraz usług na rzecz zapewnienia ciągłości ich działania.

Podstawowym i najskuteczniejszym sposobem zapewnienia bezpieczeństwa technicznego IK jest przestrzeganie mających zastosowanie do danej infrastruktury aktów prawnych, norm, reżimów eksploatacyjnych oraz realizacja rekomendacji eksperckich i ustaleń wynikających z oceny ryzyka przyjętych i wdrożonych przez koordynatora systemu IK lub operatora IK.

Celem bezpieczeństwa technicznego jest utrzymanie bezpiecznej funkcjonalności relacji pracownicy i kierownictwo – technika, w tym obiekty, instalacje, urządzenia i usługi konserwacyjno- serwisowe – otoczenie oraz zachowanie równowagi tych relacji ze środowiskiem naturalnym i klimatem.

Zakres bezpieczeństwa technicznego, w ramach zarządzania bezpieczeństwem państwa i obywateli, służący zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców, wynika z:

1. ochronnej roli wobec kluczowych usług lub wspomagania procesów i usług na ich rzecz,
2. unikatowości funkcjonalnej infrastruktury, która znalazła się w jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład IK w poszczególnych systemach IK,
3. techniczno - organizacyjnych zabezpieczeń najważniejszych zasobów operatora lub systemu IK,
4. wielkości skutków, szacowanych na podstawie przyjętych metod analizy i oceny ryzyka awarii[12], poważnej awarii[13], katastrofy technicznej, chemicznej lub ekologicznej, w szczególności w zakresie skutków dla pracowników i społeczeństwa, środowiska naturalnego, dóbr dziedzictwa narodowego i gospodarki kraju.

Bezpieczeństwo obiektów technicznych lub wodnych IK zależy od procesów realizowanych przez operatora IK w zakładach, obiektach lub instalacjach w ramach

[12] Stan niesprawności obiektu, instalacji, urządzenia uniemożliwiający jego funkcjonowanie.

[13] Poważna awaria – to zdarzenie, w szczególności emisja, pożar lub eksplozja, powstałe w trakcie procesu przemysłowego, magazynowania lub transportu, w których występuje jedna lub więcej niebezpiecznych substancji, prowadzące do natychmiastowego powstania zagrożenia życia lub zdrowia ludzi lub środowiska lub powstania takiego zagrożenia z opóźnieniem; Art.3 pkt 23 ustawy z dnia 27.04.2001 – Prawo Ochrony Środowiska (Dz. U. 2001 Nr 62 poz. 627).

wszystkich jego etapów i cyklów życia, wymagających zaangażowania pracowników wszystkich szczebli stosujących zasady sprawdzonych praktyk bezpieczeństwa:

- technicznego,
- pożarowego,
- chemicznego,
- technologiczno-procesowego,
- transportu,
- środowiskowego,
- pracy.

Mając na uwadze powyższe założenia, strategia bezpieczeństwa obiektów IK powinna bazować na integracji działań wynikających z systemów zarządzania jakością, środowiskiem, bezpieczeństwem, ciągłością działania oraz ryzykiem, m.in. zgodnie z:

- PN-EN ISO 9001 Systemy zarządzania jakością,
- PN-EN ISO 14001 Systemy zarządzania środowiskowego,
- ISO 45001 – System Zarządzania BHP Systemy zarządzania bezpieczeństwem i higieną pracy,
- OSHA 1910.119 Zarządzanie bezpieczeństwem procesowym (ang. Process Safety Management – PSM),
- PN ISO 31000 Zarządzanie ryzykiem,
- PN-EN ISO 22301 Bezpieczeństwo powszechne. Systemy zarządzania ciągłością działania,
- ISO 22313 Systemy Zarządzania ciągłością działania – poradnik,
- BS 11200:2014 Zarządzanie kryzysowe – wytyczne i dobre praktyki,
- NIST SP 800 – 34 Wytyczne ciągłości działania dla technologii informatycznych,
- HB 221 Business Continuity Management,
- Seveso III – Dyrektywa Parlamentu Europejskiego i Rady 2012/18/UE z dnia 4 lipca 2012 r. w sprawie kontroli zagrożeń poważnymi awariami związanymi z substancjami niebezpiecznymi, zmieniająca, a następnie uchylająca dyrektywę Rady 96/82/WE.

Regulacje dotyczące bezpieczeństwa technicznego wynikają z unijnego i krajowego stanu prawnego, którego kluczowe wymagania zawarte są w kodeksie pracy, prawie ochrony środowiska, prawie wodnym, prawie budowlanym, prawie atomowym, prawie geologicznym i górniczym, prawie energetycznym, w ustawie o ochronie przeciwpożarowej, w ustawie o przewozie towarów niebezpiecznych oraz w innych, jak również w przepisach wykonawczych do tych ustaw. Wiele regulacji wynika wprost z dyrektywy dotyczącej bezpieczeństwa i ochrony zdrowia w miejscu pracy, dyrektywy maszynowej, ciśnieniowej, niskonapięciowej, hałasowej, kompatybilności elektromagnetycznej, przeciwwybuchowej (atex), przeciwdziałania poważnych awarii (seveso III).

Bezpieczeństwo techniczne uwzględnia oddziaływanie wielu ryzyk mających wpływ na IK oraz na skutki, których wystąpienie jest nieakceptowalne ze względu na możliwe koszty własne wynikające z możliwości przerwania misji biznesowej, jak również powodującej koszty społeczne, ekonomiczne, ekologiczne i reputacyjne (wizerunkowe) wynikające z realizowanej w ramach IK misji publicznej. Stąd ważne jest, aby celem zarządzania ryzykiem w obszarze bezpieczeństwa technicznego było niedopuszczenie do strat[14],poprzez utrzymanie lub wzmacnianie odporności[15] rozwiązań techniczno- organizacyjnych zapewniających ochronę i funkcjonalność infrastruktury operatora IK oraz poszczególnych systemów IK. Priorytetem zarządzania bezpieczeństwem technicznym jest zagwarantowanie bezpiecznego użytkowania infrastruktury na wymaganym poziomie, wraz ze spełnieniem oczekiwanej jej funkcjonalności, jak również efektywnym zadziałaniem niezależnych zabezpieczeń w sytuacji zdarzenia niepożądanego. Spełnienie oczekiwanych wymagań służy zapobieganiu niepożądanym zdarzeniom, a w przypadku ich wystąpienia, dającym gwarancje do zadziałania systemów zabezpieczeń przewidzianych do likwidowania zagrożeń, jak również dla ochrony i ratowania zasobów operatora IK oraz zapewnienia ciągłości działania kluczowych procesów i usług przed ewentualnymi skutkami wypadków i awarii.

Przedsięwzięcia z zakresu zarządzania ryzykiem i wzmacnia odporności IK przez operatora IK albo podwykonawców procesów lub dostawców usług na rzecz operatora IK integrują problematykę bezpieczeństwa technicznego w następujących obszarach:

1) bezpieczeństwo procesowe związane z użytkowaniem substancji niebezpiecznych i instalacji technologiczno-procesowych oraz z usługami związanymi z zapewnieniem stosownych produktów w ramach łańcucha dostaw,
2) bezpieczeństwo instalacji i urządzeń technicznych lub wodnych zintegrowanych funkcjonalnie z obiektami i obszarem realizowanych procesów i usług oraz kontrola nad nimi,
3) bezpieczeństwo zawodowe i zdrowotne pracowników – bezpieczeństwo pracy,

[14] strata – to nieuzasadniona zmiana w systemie C-T-O (Człowiek-Technika-Otoczenie), charakteryzująca się utratą życia lub zdrowia ludzi lub zniszczenia innych zasobów, którego następstwem może być przerwanie usług lub procesów prowadzących do utraty usługi kluczowej. Szopa T., Niezawodność i bezpieczeństwo. Warszawa 2016 r.

[15] Odporność to zdolność do zapobiegania i stawiania oporu incydentowi zakłócającemu lub mającemu zakłócić funkcjonowanie organizacji wypełniającej obowiązki operatora infrastruktury krytycznej, łagodzenia lub likwidowania zagrożeń zmaterializowanych z tego incydentu oraz usunięcia jego skutków w celu zachowania funkcjonalności infrastruktury do świadczenia usługi kluczowej na potrzeby utrzymania niezbędnych funkcji społecznych, gospodarczych i publicznych związanych z bezpieczeństwem państwa i obywateli - definicja przyjęta z projektu Dyrektywy Parlamentu Europejskiego i Rady w sprawie odporności podmiotów krytycznych– Nr 2020/0365(COD).

4) bezpieczeństwo ekologiczne związane z przyjętymi wymaganiami wynikającymi z europejskiego prawa o klimacie[16] oraz z polityki państwa na rzecz ochrony środowiska naturalnego i klimatu,
5) bezpieczeństwo infrastruktury krytycznej związane z przyjętymi dyrektywami oraz europejskimi i krajowymi strategiami bezpieczeństwa.

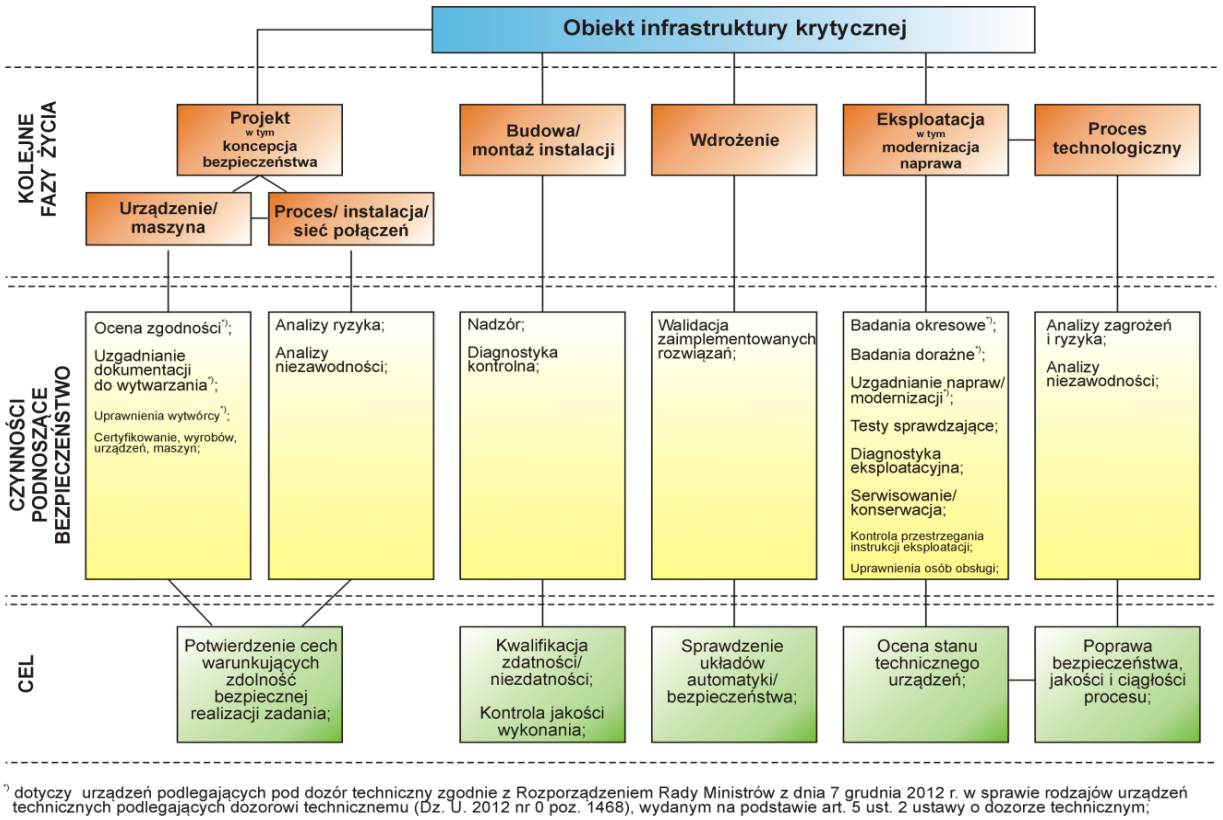
Obiekty wraz ze związanymi z nimi instalacjami i urządzeniami należy projektować i budować, a następnie eksploatować zgodnie z przepisami i przyjętymi do stosowania normami oraz zgodnie z zasadami i dobrymi praktykami wiedzy technicznej i inżynierskiej, zapewniając m.in.:

1) spełnienie wymagań podstawowych dotyczących:
    (a) nośności i stateczności konstrukcji,
    (b) bezpieczeństwa pożarowego,
    (c) higieny, zdrowia i środowiska,
    (d) bezpieczeństwa użytkowania i dostępności,
    (e) ochrony przed hałasem,
    (f) oszczędności energii i izolacyjności cieplnej,
    (g) zrównoważonego wykorzystania zasobów naturalnych.
2) warunki użytkowe zgodne z przeznaczeniem obiektu i instalacji, w szczególności w zakresie:
    (a) zaopatrzenia w wodę i energię elektryczną oraz, odpowiednio do potrzeb, w energię cieplną i paliwa, przy założeniu efektywnego wykorzystania tych czynników,
    (b) usuwania ścieków, wody opadowej i odpadów,
    (c) możliwość utrzymania właściwego stanu technicznego.
3) ochronę pracowników poprzez zastosowanie odpowiednich warunków bezpieczeństwa pracowniczego w warunkach normalnych i w trybie pracy awaryjnej np. pożaru, wybuchu, emisji substancji niebezpiecznej lub innego zagrożenia;
4) ochronę obiektów wpisanych do rejestru zabytków oraz obiektów objętych ochroną konserwatorską;
5) odpowiednie usytuowanie na działce budowlanej i zastosowanie warunków wynikających z zagospodarowania przestrzennego.

W bezpieczeństwie obiektowym dobrą praktyką jest podejście, że każde projektowanie, produkcja, import, budowa oraz eksploatacja urządzeń, instalacji (i sieci) powinny zapewniać racjonalne i oszczędne zużycie paliw lub energii przy zachowaniu:

[16] Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające ramy na potrzeby osiągnięcia neutralności klimatycznej i zmieniające rozporządzenie (UE) 2018/1999 (Europejskie prawo o klimacie) - (dostęp 22 I 2021 r.).

1) niezawodności współdziałania;
2) bezpieczeństwa obsługi i otoczenia, po spełnieniu wymagań ochrony środowiska, bhp, przeciwpożarowej oraz rekomendacji eksperckich i rzeczoznawców;
3) zgodności z wymaganiami Polskich Norm wprowadzonych do obowiązkowego stosowania lub innych zaleceń wynikających z technologii wytwarzania energii i rodzaju stosowanego paliwa.



*) dotyczy urządzeń podlegających pod dozór techniczny zgodnie z Rozporządzeniem Rady Ministrów z dnia 7 grudnia 2012 r. w sprawie rodzajów urządzeń technicznych podlegających dozorowi technicznemu (Dz. U. 2012 nr 0 poz. 1468), wydanym na podstawie art. 5 ust. 2 ustawy o dozorze technicznym;

Rysunek 11 Wybrane czynności podnoszące bezpieczeństwo obiektów technicznych infrastruktury krytycznej w kolejnych fazach życia.

Urządzenia techniczne stwarzające zagrożenie przez:

- rozprężanie gazów znajdujących się pod ciśnieniem różnym od atmosferycznego,
- wyzwolenie energii potencjalnej lub kinetycznej przy przemieszczaniu ludzi lub ładunków w ograniczonym zasięgu (windy, dźwigi, schody ruchome),
- rozprzestrzenianie się materiałów niebezpiecznych podczas ich magazynowania lub transportu objęte są dozorem technicznym!

2.6.1. Cztery podstawowe elementy zapewnienia bezpieczeństwa technicznego

System odporny na zakłócenia powinien cechować się:

- ciągłą dostępnością usługi lub usług,
- niezawodnością,
- zdolnością serwisową,
- bezpieczeństwem.

Zależnie od sytuacji i eksploatacyjnego znaczenia urządzeń wchodzących w skład systemu bezpieczeństwa IK, dodatkowo mogą być także wymagane: krótki czas napraw, konieczność wymiany w ruchu krytycznych elementów, dobre strategie diagnostyczne i odpowiednie zapasy części zamiennych.

Dostępność

Dotychczas, przy projektowaniu systemów priorytetem było stosowanie wysokiej niezawodności elementów, urządzeń i zespołów, co miało być gwarancją zmniejszenia intensywności uszkodzeń systemu. Obecnie, szczególnie w przypadku projektowania nowych lub modernizacji istniejących systemów zaopatrzenia w energię i paliwa, systemów łączności i teleinformatycznych oraz systemów zaopatrzenia w wodę, dużą uwagę zwraca się także na rozwiązania gwarantujące **dostępność** usługi. Utrzymanie wysokiej dostępności wymaga starannego planowania i dobrego zarządzania obsługą.

Termin **dostępność** oznacza możliwość ciągłego korzystania z zasobów systemu w dowolnym czasie. **Procentowe wskaźniki dostępności**, zwane też w polskiej literaturze **wskaźnikami gotowości**, określają projektowany przestój i pozwalają na porównywanie teoretycznego czasu przestoju wynikającego z awaryjności danego systemu.

Tabela 6 Pomiar dostępności[17]

Dostępność	Przestój	Przestój w skali roku	Przestój w skali tygodnia
98%	2%	7 dni, 7 godz., 4 min.	3 godz., 22 min.
99%	1%	3 dni, 15 godz. 32 min.	1 godz., 41 min.
99,8%	0,2%	17 godz., 30 min.	20 min., 10 sek.

[17] Źródło: Evan M., Hal S.: Blueprints for high availability, ed.2, Wiley Publishing, Canada 2003.

Dostępność	Przestój	Przestój w skali roku	Przestój w skali tygodnia
99,9%	0,1%	8 godz., 45 min.	10 min., 5 sek.
99,99%	0,01%	52,5 min.	1 min.
99,999%	0,001%	5,25 min.	6 sec.
99,9999%	0,0001%	31,5 sek.	0,6 sek.

System, który powoduje wyłączenie raz w miesiącu i zawiesza proces na ok. 40 minut, ma dostępność 99,9%. To samo można powiedzieć o systemie, który inicjuje wyłączenie raz w roku, ale na ok. 9 godzin. Zakładając teoretycznie, że naprawa uszkodzonego elementu zajmuje maksymalnie 1 godzinę, to cała linia technologiczna zazwyczaj skazana jest na wielogodzinny przestój, zanim wszystkie elementy zostaną ponownie podłączone i zaczną pracować.

Rzeczywisty, średni czas postoju powinien być szacowany już od momentu stwierdzenia uszkodzenia do momentu przywrócenia systemu do określonego stanu zdatności. Często zdarza się, że czas ten liczony jest dopiero od momentu przystąpienia do naprawy. Dobrą praktyką jest zatem jednoznaczne definiowanie na potrzeby danego operatora IK, co dokładnie rozumiane jest pod pojęciem średni czas naprawy **MTTR (Mean Time To Repairs).**

Dostępność systemów zasilania w energię elektryczną[18]

Wartości wymaganej lub oczekiwanej dostępności dla systemów zasilających w energię elektryczną są bardzo wysokie. Typowa wartość wskaźnika dostępności w punkcie wspólnego przyłączenia wynosi ok. 99,98 % głównie dlatego, że sieć ma redundancję. Oznacza to, że istnieje możliwość przełączania z jednej linii zasilającej na drugą w przypadku zakłóceń w linii pierwszej lub odwrotnie. Linie muszą być w sposób stały monitorowane i obsługiwane. Wysokie poziomy dostępności systemu są zatem determinowane poprawnością koncepcji projektu, prawidłowym wyborem architektury

[18] Źródło: Marshall G., Chapman D.: Jakość zasilania – poradnik, Wyd. Polskie Centrum Promocji Miedzi, Wrocław 2002.

systemu, eliminacją pojedynczych miejsc uszkodzeń, ale także są rezultatem dobrze zaplanowanej obsługi eksploatacyjnej.

Niezawodność

Niezawodność techniczna jest to właściwość określona przez prawdopodobieństwo, że dane urządzenie lub obiekt w systemie będą sprawne w ciągu określonego przedziału, którym może być czas, ale także np. liczba wykonanych czynności. Parametr odnosi się więc do urządzeń wchodzących w skład systemu. Podstawowymi wskaźnikami niezawodności systemu są: średni czas pracy do awarii **MTTF (Mean Time To Failure)** i średni czas między awariami **MTBF (Mean Time Between Failure).** Czynniki wpływające na niezawodność to:

- redundancja urządzeń,
- czas naprawy,
- strategia obsługi, np. stały nadzór, monitoring, oraz
- dobór elementów składowych, w tym: jakość elementów i program ich doboru.

Zdolność serwisowa

Niezależnie od sposobu i czasu użytkowania infrastruktury technicznej, tworzące ją elementy podlegają ciągłemu zużyciu. W przypadku dużych obiektów technicznych, takich jak np. złożone systemy technologiczne, energetyczne, transformatory czy rurociągi, istotnymi czynnikami – wpływającymi na **dostępność** oraz **charakterystyki eksploatacyjno-niezawodnościowe**, a razem wspomagającymi **bezpieczeństwo** eksploatacji – są konserwacje i **remonty**.

W dziedzinie eksploatacji urządzeń i maszyn, oprócz remontów poawaryjnych, wyróżnia się dwa sposoby utrzymania ruchu infrastruktury technologicznej, którymi są:

- remont zapobiegawczy planowany,
- remont wyznaczony na podstawie analizy stanu technicznego.

Pierwszy sposób stosuje się głównie w odniesieniu do takich elementów systemu i wtedy, gdy przerwa remontowa nie powoduje liczących się strat. Remont planowany dla urządzeń lub maszyn realizujących odpowiedzialne zadania, ma na celu minimalizowanie ryzyka wystąpienia zdarzeń nieplanowanych i wynikających z tego strat, ale nie daje on 100% pewności uniknięcia niespodziewanej awarii. Ponadto, często najwięcej awarii zdarza się tuż po remoncie, np. w wyniku błędów personelu popełnianych w trakcie remontu. Remonty zatem mogą okazać się szkodliwe, gdyż starając się przywrócić urządzenie do stanu idealnego, może wystąpić tzw. "efekt

nowości", który oznacza, że wiele komponentów ulega awarii we wczesnym okresie eksploatacji[19].

Dla elementów ważnych funkcyjnie, dobrą praktyką jest określanie optymalnych momentów realizowania ich obsługi technicznej, tj. wyznaczania terminu i zakresu remontu na podstawie wiedzy o stanie technicznym i warunków eksploatacji. Prognoza ich trwałości powinna być wtedy poparta **kompleksowymi badaniami diagnostycznymi**.

Dla urządzeń długo eksploatowanych standardami światowymi zapewniającymi bezpieczeństwo, ale także wysoką dostępność stały się obecnie: **analiza ryzyka RBM (Risk Based Maintenance)** oraz **metodologia utrzymania ruchu ukierunkowana na niezawodność RCM (Reliability Centered Maintenance)**. Odpowiednio wdrożone służą do wydłużenia czasu pracy urządzeń.

Bezpieczeństwo

Każdy obiekt, w tym jego instalacja lub urządzenie (np. maszyna, aparatura, budowla) wymagają różnych środków ochrony i utrzymania poziomu bezpieczeństwa, które w udokumentowany sposób powinny regulować zachowanie ich niezawodności oraz potwierdzać nadzorowanie ich funkcjonalności.

Każdy prawidłowo i bezpiecznie zaprojektowany obiekt IK musi uwzględniać obowiązujące normy i przepisy prawne, zawarte m.in. w:

- Rozporządzeniu Ministra Infrastruktury z dnia 12 kwietnia 2002 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (Dz. U. z 2022 r. poz. 1225),
- Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 7 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz. U. 2022, poz. 1620),
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 24 lipca 2009 r. w sprawie przeciwpożarowego zaopatrzenia w wodę oraz dróg pożarowych (Dz. U. Nr 124, poz.1030),

Spełnienie wymagań określonych w przepisach to jednak spełnienie tylko **minimalnych wymagań**. Przy projektowaniu realizacji nowych procesów może okazać się, że brakuje krajowych przepisów (np. dla przemysłu chemicznego). Zmusza to, projektujących do używania przepisów „przez analogię".

Celem uzupełnienia przepisów lokalnych dobrą praktyką jest używanie przepisów, standardów lub wytycznych międzynarodowych.

[19] Źródło: Smith A. M., Hinchcliffe G.R.: RCM-Gateway to World Class Maintenance, Ed.1., Wyd. *Butterworth Heinemann, 2003.*

Kluczowego znaczenia na etapie projektowania nabiera także zwiększenie nadzoru ze strony rzeczoznawców p.poż. i BHP oraz weryfikacja prawidłowości projektu – np. poprzez wykonanie analizy zagrożeń i oceny bezpieczeństwa oraz modelowanie konsekwencji potencjalnych awarii.

Bezpieczeństwo infrastruktury krytycznej w aspekcie ochrony odgromowej[20]

Wykonanie na etapie projektowania analizy ryzyka zgodnie z wymaganiami PN-EN 62305-2 pozwala ocenić zagrożenie obiektu w skutek wyładowań atmosferycznych, a w rezultacie dobrać odpowiednie środki ochrony w celu obniżenia istniejącego ryzyka do poziomu akceptowalnego.

Na etapie projektowania urządzeń lub instalacji technologicznych powinny być rozważane dwa ściśle ze sobą powiązane zagadnienia:

- prawidłowej realizacji przebiegu procesu,
- zapewnienia bezpieczeństwa w stanach normalnej pracy i stanach awaryjnych.

Oznacza to, że w strukturze obiektów technicznych znajdują się – oprócz **układu funkcjonalnego** niezbędnego do realizacji procesów i zadań do których obiekt jest przeznaczony – **układy bezpieczeństwa,** w tym **automatyka zabezpieczeniowa.** Ich zadaniem jest niedopuszczenie do przekształcenia zakłóceń, wynikających z pracy obiektu, w awarie i katastrofy, a także ograniczenie negatywnych skutków tych zdarzeń, jeżeli już wystąpią. Podstawową funkcją układów bezpieczeństwa, które mogą być również zintegrowane z układami sterowania jest **monitorowanie** istotnych parametrów pracy i **diagnostyka techniczna**[21]**,** która ma na celu wykrycie ewentualnych uszkodzeń lub nieprawidłowości. Działania diagnostyczne często połączone są z **alarmami** optycznymi lub dźwiękowymi oraz **blokadami** przebiegu procesów.

Standardy techniczne dotyczące **systemów bezpieczeństwa** nie nakładają wymogu wdrażania konkretnej technologii, poziomów redundancji lub interwałów czasowych w jakich należy wykonać, np. testowanie sprawdzające. W zakresie ogólnych wymagań stawianych urządzeniom automatyki zabezpieczeniowej, wynikających ze względów niezawodnościowych, wymienia się natomiast stosowanie:

[20] Źródło: PN-EN 62305-2:2012 Ochrona odgromowa – Część 2: Zarządzanie ryzykiem.

[21] Źródło: Zbrowski A., Kozioł S.: Monitorowanie i diagnozowanie procesów i obiektów technicznych w systemach zapewnienia bezpieczeństwa technicznego, *Nauki humanistyczne i społeczne na rzecz bezpieczeństwa*, Nr 1, 2011, s. 59-68.

- minimum dwóch niezależnych rodzajów zabezpieczeń, przy czym każde z nich powinno współpracować z oddzielnymi obwodami pomiarowymi, sterowniczymi i wyłączającymi;
- środków sprzętowo-programowych do **autodiagnostyki**, czyli realizowania funkcji ciągłej kontroli i samo-testowania[22].

Operatorzy obiektów infrastruktury krytycznej powinni być w stanie udokumentować, że realizowane przez nich procesy technologiczne są zaprojektowane i działają w sposób bezpieczny. Stosowane na obiektach systemy bezpieczeństwa i ograniczania skutków awarii mają zazwyczaj strukturę wielowarstwową, wynikającą, np. ze złożoności procesu, przy czym zawsze wpisują się w model trzech niezależnych warstw ochrony (*Tabela 7*):

(1) zapobiegania,
(2) ograniczania,
(3) przeciwdziałania.

Tabela 7 Bezpieczeństwo a trzy niezależne warstwy ochrony[23]

TEORIA	PRAKTYKA
Poziom ochrony zapobiegawczej tzw. warstwa kontrolna **Cel: zapobieganie awarii**	wykonanie Ex (jeżeli jest wymagane) systemy awaryjnego zasilania i podtrzymania podstawowy system pomiarów i sterowania (BPCS – Basic Process Control System, DCS – Distributed Control System) system nadzorujący przebieg procesu (np. SCADA – Supervisory Control And Data Acquisition) alarmy procesowe i systemowe działania operatorów i sterowniczych, np. ręczna korekta systemu wewnętrzne procedury
Poziom ochrony ograniczającej tzw. warstwa bezpieczeństwa **Cel: ochrona obiektu i pracowników przed**	przyrządowe systemy bezpieczeństwa SIS – Safety Instrumented System, jak np. – systemy awaryjnego zatrzymania ESD – Emergency Shutdown System – systemy bezpiecznego zatrzymania SSD – Safety Shutdown System odpowiedzi operatora na alarmy stanów krytycznych

[22] Źródło: Orzyłowski M.: Przemysłowe systemy informatyczne, Cz.9. Autodiagnostyka przemysłowych systemów sterowania, 2003.

[23] Źródło: Opracowanie na podstawie rekomendacji UDT.

TEORIA	PRAKTYKA
skutkami awarii	systemy zrzutu awaryjnego, zawory bezpieczeństwa systemy detekcji wycieku gazu i pożaru bariery, obudowy, tace i in.
Poziom ochrony przeciwdziałającej tzw. warstwa łagodzenia **Cel: przeciwdziałanie skutkom awarii dla ludzi i środowiska**	systemy gaśnicze i neutralizacji (np. instalacje wodne, pianowe, kurtyny wodne, hydranty), personel i ratownicy na obiektach (np. ratownictwo chemiczne) straż pożarna zakładowa/ państwowa ewakuacja pomoc medyczna

Cechą charakterystyczną wielopoziomowego systemu ochrony jest sekwencyjne uruchamianie kolejnych warstw ochrony po nieprawidłowym zadziałaniu warstwy poprzedniej. Rzeczywisty poziom bezpieczeństwa obiektu uzależniony jest zatem od stanu i prawidłowego działania wszystkich warstw ochrony. Dobór odpowiednich rodzajów zabezpieczeń do warstw zapobiegania, ograniczania i przeciwdziałania powinien być ustalany w oparciu o specyfikę i rodzaje zagrożeń. Niektóre warstwy ograniczania skutków awarii mogą być jednofunkcyjne, tzn. że będą przeciwdziałały tylko konkretnym zagrożeniom.

Taca nie zapobiegnie tworzeniu się chmury oparów w przypadku przepełnienia zbiornika z ciekłymi substancjami, ale może być skuteczna w zapobieganiu przenikania czynnika roboczego do gruntu.

2.6.2. Wytyczne dla instalacji, urządzeń i maszyn eksploatowanych

Podczas długotrwałej eksploatacji obserwowane są liczne zmiany w procesie oraz warunkach eksploatacji, które w połączeniu ze zdarzeniami losowymi spowodowanymi, np. błędami człowieka lub działaniem środowiska naturalnego, znacząco wpływają na funkcjonalność, niezawodność i bezpieczeństwo obiektu.

W celu zapobiegania potencjalnym awariom oraz zapewnienia długoterminowej eksploatacji danego obiektu IK, wskazane jest sukcesywne prowadzenie **kompleksowej oceny stanu technicznego** w oparciu o analizy bezpieczeństwa oraz indywidualnie dedykowane programy badań i pomiarów.

Identyfikacja zagrożeń wymaga analizy danych historycznych i zdarzeń z przeszłości, ale uwzględnia również prognozy na przyszłość oparte na wiedzy o tym obiekcie.

W przypadku obiektów długo eksploatowanych, zwłaszcza w sytuacji, gdy nastąpiła kilkukrotna zmiana właściciela obiektu, może okazać się, że:

- dokumentacja techniczna obiektów projektowa/powykonawcza/koncesyjna jest niekompletna lub nieaktualna (np. rysunki nie oddają stanu rzeczywistego rozmieszczenia rurociągów, brakuje obliczeń wytrzymałościowych dla urządzeń ciśnieniowych, itp.),
- nie ma zapisów dotyczących czasu pracy, ilości przestojów i rozruchów,
- prowadzona ocena stanu obiektu opiera się tylko na oględzinach miejsc dostępnych,
- zakresy wykonywanych badań i pomiarów są niepełne lub dotyczą elementów losowo wybieranych.

W takim przypadku – w pierwszej kolejności – celowe jest przeprowadzenie inwentaryzacji, pod kątem weryfikacji danych, które powinny być gromadzone dla zapewnienia bezpieczeństwa eksploatacyjnego. Zebrane informacje będą również przydatne przy przeprowadzaniu oceny ryzyka. Inwentaryzacja dokonywana jest zazwyczaj bez udziału szerokiego zespołu ekspertów.

W drugim etapie, opierając się na informacjach zebranych podczas działań wstępnych, dalsze zadania mogą być realizowane dwutorowo i będą polegały na:

- wyznaczeniu urządzeń lub elementów, które należy poddać ocenie szczegółowej, identyfikacji mechanizmów degradacji i przeprowadzeniu badań diagnostycznych;
- identyfikacji zagrożeń, z uwzględnieniem ich typu i miejsca występowania, oraz wykonaniu ocen ryzyka.

Podstawowym warunkiem dla wykonania prawidłowej oceny bezpieczeństwa eksploatacyjnego obiektu będzie powołanie wykwalifikowanych zespołów i podjęcie decyzji na temat metodologii:

- badań diagnostycznych i analitycznych,
- opracowania oceny ryzyka.

<u>Urządzenia podlegające nadzorowi UDT</u>

Program badań diagnostycznych opracowywany jest indywidualnie dla każdego urządzenia lub elementu, z uwzględnieniem zakresu badań i kryteriów oceny uzyskanych wyników. Dla urządzeń technicznych podlegających pod Urząd Dozoru Technicznego (UDT) wymagane jest uzgodnienie zakresu badań z właściwym terenowo oddziałem UDT.

Końcowym, oczekiwanym rezultatem po zastosowaniu kompleksowej oceny stanu technicznego obiektu IK, opartej na badaniach diagnostycznych i analizach ryzyka, jest

uzyskanie dowodu, że **spełnione są wszystkie warunki techniczne i funkcjonalne, aby obiekt mógł zapewnić bezpieczną i długookresową eksploatację.**

2.6.3. Ogólne wymagania dotyczące obiektów budowlanych

Obiekty wraz ze związanymi z nimi instalacjami i urządzeniami należy projektować i budować, a następnie eksploatować zgodnie z przepisami i przyjętymi do stosowania normami i wynikami z oceny ryzyka oraz zgodnie z zasadami i dobrymi praktykami wiedzy technicznej i inżynierskiej, zapewniając m.in.:

2) spełnienie wymagań podstawowych dotyczących:
    (d) nośności i stateczności konstrukcji,
    (e) bezpieczeństwa pożarowego,
    (f) higieny, zdrowia i środowiska,
    (g) bezpieczeństwa użytkowania i dostępności,
    (h) ochrony przed hałasem,
    (i) oszczędności energii i izolacyjności cieplnej,
    (j) zrównoważonego wykorzystania zasobów naturalnych;
3) warunki użytkowe zgodne z przeznaczeniem obiektu i instalacji, w szczególności w zakresie:
    a) zapewnienia w wodę i energię elektryczną oraz, odpowiednio do potrzeb, w energię cieplną i paliwa, przy założeniu efektywnego wykorzystania tych czynników;
    b) usuwania ścieków, wody opadowej i odpadów;
    c) możliwości utrzymania właściwego stanu technicznego,
6) ochronę pracowników poprzez zastosowanie odpowiednich warunków bezpieczeństwa pracowniczego w warunkach normalnych i w trybie pracy awaryjnej np. pożaru, wybuchu, emisji substancji niebezpiecznej lub innego zagrożenia;
7) ochronę obiektów wpisanych do rejestru zabytków oraz obiektów objętych ochroną konserwatorską;
8) odpowiednie usytuowanie na działce budowlanej i zastosowanie warunków wynikających z zagospodarowania przestrzennego.

W bezpieczeństwie obiektowym dobrą praktyką jest podejście, że każde projektowanie, produkcja, import, budowa oraz eksploatacja urządzeń, instalacji (i sieci) powinny zapewniać racjonalne i oszczędne zużycie paliw lub energii przy zachowaniu:

4) niezawodności współdziałania;
5) bezpieczeństwa obsługi i otoczenia, po spełnieniu wymagań ochrony środowiska, bhp, przeciwpożarowej oraz rekomendacji eksperckich i rzeczoznawców;

6) zgodności z wymaganiami Polskich Norm wprowadzonych do obowiązkowego stosowania lub innych zaleceń wynikających z technologii wytwarzania energii i rodzaju stosowanego paliwa.

Obiekty należy użytkować w sposób zgodny z ich przeznaczeniem i wymaganiami ochrony środowiska oraz utrzymywać w należytym stanie technicznym, nie dopuszczając do nadmiernego pogorszenia ich właściwości użytkowych i sprawności technicznej.

Właściciel lub zarządca obiektu, w szczególności budowlanego jest obowiązany:

(1) utrzymywać i użytkować obiekt zgodnie z zasadami, o których mowa powyżej;
(2) zapewnić, dochowując należytej staranności, bezpieczne użytkowanie obiektu w razie wystąpienia czynników zewnętrznych oddziaływujących na obiekt, związanych z działaniem człowieka lub sił natury, takich jak: wyładowania atmosferyczne, wstrząsy sejsmiczne, silne wiatry, intensywne opady atmosferyczne, osuwiska ziemi, zjawiska lodowe na rzekach i morzu oraz jeziorach i zbiornikach wodnych, pożary lub powodzie, w wyniku których następuje uszkodzenie obiektu budowlanego lub bezpośrednie zagrożenie takim uszkodzeniem, mogące spowodować zagrożenie życia lub zdrowia ludzi, bezpieczeństwa mienia lub środowiska.

Obiekty budowlane powinny być w czasie ich użytkowania poddawane przez właściciela lub zarządcę m.in. kontroli:

(1) okresowej, co najmniej raz w roku, polegającej na sprawdzeniu stanu technicznego:
    a) elementów budynku, budowli i instalacji narażonych na szkodliwe wpływy atmosferyczne i niszczące działania czynników występujących podczas użytkowania obiektu,
    b) instalacji i urządzeń służących ochronie środowiska,
    c) instalacji gazowych oraz przewodów kominowych (dymowych, spalinowych i wentylacyjnych);
(2) okresowej, co najmniej raz na 5 lat, polegającej na sprawdzeniu stanu technicznego i przydatności do użytkowania obiektu budowlanego; kontrolą tą powinno być objęte również badanie instalacji elektrycznej i piorunochronnej w zakresie stanu sprawności połączeń, osprzętu, zabezpieczeń i środków ochrony od porażeń, oporności izolacji przewodów oraz uziemień instalacji i aparatów;
(3) okresowej, co najmniej dwa razy w roku, w terminach do 31 maja oraz do 30 listopada, w przypadku budynków o powierzchni zabudowy przekraczającej 2000 m^2 oraz innych obiektów budowlanych o powierzchni dachu przekraczającej 1000 m^2; osoba dokonująca kontroli jest obowiązana bezzwłocznie pisemnie zawiadomić właściwy organ o przeprowadzonej kontroli;

(4) bezpiecznego użytkowania obiektu każdorazowo w razie wystąpienia czynników zewnętrznych oddziałujących na obiekt, związanych z działaniem człowieka lub sił natury.

Kontrole przeprowadzają osoby posiadające uprawnienia budowlane w odpowiedniej specjalności.

Kontrole stanu technicznego instalacji elektrycznych, piorunochronnych, gazowych i urządzeń chłodniczych mogą przeprowadzać osoby posiadające kwalifikacje wymagane przy wykonywaniu dozoru nad eksploatacją urządzeń, instalacji oraz sieci energetycznych i gazowych.

Właściciel lub zarządca obiektu budowlanego jest obowiązany przechowywać przez okres istnienia obiektu dokumentację budowy, dokumentację powykonawczą i inne dokumenty oraz decyzje dotyczące obiektu, a także, w razie potrzeby, instrukcje obsługi i eksploatacji: obiektu, instalacji i urządzeń związanych z tym obiektem, a także opracowania projektowe i dokumenty techniczne robót budowlanych wykonywanych w obiekcie w toku jego użytkowania.

Właściciel lub zarządca jest obowiązany prowadzić dla każdego budynku oraz obiektu budowlanego niebędącego budynkiem, którego projekt jest objęty obowiązkiem sprawdzenia, książkę obiektu budowlanego, stanowiącą dokument przeznaczony do zapisów dotyczących przeprowadzanych badań i kontroli stanu technicznego, remontów i przebudowy, w okresie użytkowania obiektu budowlanego.

W razie katastrofy budowlanej w budowanym, rozbieranym lub użytkowanym obiekcie budowlanym, kierownik budowy (robót), właściciel, zarządca lub użytkownik jest obowiązany:

(1) zorganizować doraźną pomoc poszkodowanym i przeciwdziałać rozszerzaniu się skutków katastrofy;
(2) zabezpieczyć miejsce katastrofy przed zmianami uniemożliwiającymi prowadzenie postępowania wyjaśniającego w sprawie przyczyn katastrofy budowlanej prowadzonego przez właściwy organ nadzoru budowlanego. Czynności powyższych nie wykonuje się w przypadku ratowania życia lub zabezpieczenia przed rozszerzaniem się skutków katastrofy. W tych przypadkach należy szczegółowo opisać stan po katastrofie oraz zmiany w nim wprowadzone, z oznaczeniem miejsc ich wprowadzenia na szkicach i, w miarę możliwości, na fotografiach;
(3) niezwłocznie zawiadomić o katastrofie:
    a) właściwy organ,
    b) właściwego miejscowo prokuratora i Policję,
    c) inwestora, inspektora nadzoru inwestorskiego i projektanta obiektu budowlanego, jeżeli katastrofa nastąpiła w trakcie budowy,

d) inne organy lub jednostki organizacyjne właściwe w sprawie katastrofy z mocy szczególnych przepisów.

Inwestor, właściciel lub zarządca obiektu budowlanego po zakończeniu postępowania w sprawie przyczyn katastrofy budowlanej jest obowiązany podjąć niezwłocznie działania niezbędne do usunięcia skutków katastrofy budowlanej.

2.6.4. Ochrona przeciwpożarowa

Podstawowe czynności w zakresie ochrony przeciwpożarowej infrastruktury krytycznej to:

- przestrzeganie przeciwpożarowych wymagań techniczno-budowlanych, instalacyjnych i technologicznych,
- wyposażanie budynków, obiektów budowlanych lub terenów w wymagany przepisami podręczny sprzęt gaśniczy i urządzenia przeciwpożarowe:
  - stałe i półstałe urządzenia gaśnicze i zabezpieczające,
  - urządzenia wchodzące w skład systemu sygnalizacji pożarowej i dźwiękowego systemu ostrzegawczego,
  - instalacje oświetlenia ewakuacyjnego oraz oświetlenia awaryjnego,
  - hydranty, zawory hydrantowe,
  - pompy w pompowniach przeciwpożarowych,
  - przeciwpożarowe klapy odcinające,
- urządzenia oddymiające oraz drzwi i bramy przeciwpożarowe, o ile są wyposażone w systemy sterowania,
- urządzenia odciążające i zabezpieczenia przed ciśnieniem wybuchu
- zapewnienie konserwacji oraz naprawy urządzeń przeciwpożarowych i podręcznego sprzętu gaśniczego w sposób gwarantujący ich sprawne i niezawodne funkcjonowanie,
- zapewnienie osobom przebywającym na terenie infrastruktury krytycznej, bezpieczeństwa i możliwość ewakuacji,
- przygotowanie budynków, obiektów budowlanych lub terenów infrastruktury krytycznej do prowadzenia akcji ratowniczej.

Oprócz środków technicznych należy wprowadzić reżimy organizacyjne tj.:

- zapoznanie pracowników z przepisami przeciwpożarowymi,
- ustalenie sposobów postępowania na wypadek powstania pożaru, klęski żywiołowej lub innego miejscowego zagrożenia.

Ponadto do ochrony przeciwpożarowej infrastruktury krytycznej należy zaliczyć:

- stosowanie systemów sygnalizacji pożarowej wyposażonych w urządzenia sygnalizacyjno-alarmowe,

- uwzględnianie wymagań w zakresie ochrony przeciwpożarowej przy zagospodarowaniu i uzbrajaniu terenu,
- połączenie urządzenia sygnalizacji pożarowej z obiektem komendy Państwowej Straży Pożarnej lub obiektem, wskazanym przez właściwego miejscowo komendanta powiatowego (miejskiego) Państwowej Straży Pożarnej,
- zapewnianie dokumentacji projektowej z wymaganiami ochrony przeciwpożarowej,
- obowiązek spełnienia wymagań ochrony przeciwpożarowej przez wytwórcę maszyn, urządzeń i innych wyrobów oraz nabywcę licencji zagranicznych lub maszyn, urządzeń i innych wyrobów pochodzących z importu,
- rozpoczęcie eksploatacji nowej, przebudowanej lub wyremontowanej budowli, obiektu lub terenu, maszyny, urządzenia lub instalacji albo innego wyrobu po spełnieniu wymagań przeciwpożarowych oraz gdy sprzęt, urządzenia pożarnicze i ratownicze oraz środki gaśnicze zapewniają skuteczną ochronę przeciwpożarową,
- zakazywanie wykonywania czynności, które mogą spowodować pożar oraz inne miejscowe zagrożenie, jego rozprzestrzenianie się, utrudnienie prowadzenia działania ratowniczego lub ewakuacji,
- utrzymywanie dróg pożarowych w stanie umożliwiającym ich wykorzystanie przez pojazdy jednostek ochrony przeciwpożarowej,
- zapewnienie właściwych dojazdów do budynków i obiektów dla jednostek ratowniczych,
- wdrażanie instrukcji bezpieczeństwa pożarowego;
- przestrzeganie zasad używania lub przechowywania materiałów niebezpiecznych pożarowo,
- zapewnienie w obiektach urządzeń i instalacji służących do dostarczania wody do celów przeciwpożarowych,
- stosowanie stałych urządzeń gaśniczych związanych na stałe z obiektem,
- stosowanie dźwiękowego systemu ostrzegawczego, umożliwiającego rozgłaszanie sygnałów ostrzegawczych i komunikatów głosowych na potrzeby bezpieczeństwa osób przebywających w obiekcie.

Ewakuacja jest jednym z podstawowych działań mających na celu ochronę życia i zdrowia ludzi oraz zwierząt, a także ratowania mienia, w przypadku wystąpienia pożaru. Bezpieczna ewakuacja ludzi z obiektów jest możliwa przy zachowaniu odpowiednich warunków techniczno-budowlanych dla dróg ewakuacyjnych i elementów wystroju wnętrz. Warunki i organizacja ewakuacji ludzi określone są w instrukcji bezpieczeństwa pożarowego, a praktyczne sposoby jej sprawdzania realizowane są w drodze ćwiczeń. Ewakuacja może mieć również charakter prewencyjny.

Istotne jest, aby systemy ochrony przeciwpożarowej były projektowane, instalowane, konserwowane i eksploatowane z zachowaniem najwyższych standardów jakości. Zaleca się, aby osoby realizujące usługi w tym zakresie posiadały odpowiednie kwalifikacje i kompetencje.

Poprawność i niezawodność działania technicznych systemów ochrony przeciwpożarowej, w szczególności systemów sygnalizacji pożarowej, jest kluczowa do zachowania bezpieczeństwa pożarowego obiektu chronionego. Dobrą praktyką jest aby osoby realizujące usługi w zakresie projektowania, instalowania, konserwacji i eksploatacji systemów ochrony przeciwpożarowej posiadały ukończony kurs lub szkolenie (w odpowiednim obszarze sprzętowym) w uznanej na rynku, niezależnej instytucji szkoleniowej.

Odniesienie do wymagań kompetencyjno-kwalifikacyjnych osób realizujących usługi w zakresie systemów zabezpieczeń technicznych wynika wprost lub pośrednio z przepisów prawa, norm, specyfikacji technicznych oraz standardów branżowych. Odniesienie do wymagań zawarte jest w ustawie o ochronie przeciwpożarowej, Rozporządzeniu MSWIA z dnia 17.09.2021 r. w sprawie uzgadniania projektu zagospodarowania działki lub terenu, projektu architektoniczno-budowlanego, projektu technicznego oraz projektu urządzenia przeciwpożarowego pod względem zgodności z wymaganiami ochrony przeciwpożarowej (Dz.U. 2021 poz.1722 z późn. zm), Rozporządzenia MI z dnia 12.04.2002 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (Dz.U. 2022 poz. 1225 z późn. zm.), specyfikacji technicznej PKN-CEN/TS 54-14:2020-09 Systemy sygnalizacji pożarowej -- Część 14: Wytyczne planowania, projektowania, instalowania, odbioru, eksploatacji i konserwacji, a także w normie PN-EN 16763 Usługi w zakresie systemów ochrony przeciwpożarowej oraz systemów zabezpieczeń technicznych oraz w standardach branżowych.

2.6.5. Działania techniczne mające na celu zmniejszenie uzależnienia funkcjonowania IK od zewnętrznych usług

Dla obiektów, w których zlokalizowane są elementy infrastruktury krytycznej należy przyjmować najwyższe wymagania dotyczące niezawodności zasilania i dostępu do mediów.

Spełnienie powyższych wymagań może zostać osiągnięte przez:

- zasilanie z dwóch niezależnych sieci elektroenergetycznych, wodociągów i sieci łączności lub do transmisji danych. Przewody powinno umieścić się pod ziemią i doprowadzić do różnych miejsc w budynku,
- zasilanie instalacji przez urządzenia podtrzymująco-stabilizujące – pojemność baterii akumulatorów powinna być dobrana z uwzględnieniem wszystkich urządzeń wymagających rezerwowania,

- zasilanie rezerwowe obiektu przez zespół generatorów prądotwórczych – moc zespołu powinna być wystarczająca do zasilania wszystkich urządzeń wymagających rezerwowania, przy uwzględnieniu charakteru obciążenia ze strony tych urządzeń,
- własne ujęcie wody – wydajność ujęcia powinna uwzględniać charakter prowadzonej działalności oraz minimalne wymagania pozwalające na podtrzymanie lub bezpieczne wygaszenie procesów technologicznych. Źródła wody powinny być odseparowane od innych elementów infrastruktury,
- zbiorniki wody (gazu, oleju napędowego itp.), których pojemność powinna uwzględniać minimalne wymagania pozwalające na podtrzymanie lub bezpieczne wygaszenie procesów technologicznych.
- corocznie weryfikowany plan awaryjnych dostawców.

Zagadnienie wymagań dotyczących niezawodności zasilania i dostępu do mediów najlepiej rozpatrzyć już w procesie projektowania infrastruktury. Uwzględnienie tych wymagań we wczesnym etapie pozwoli na podniesienie bezpieczeństwa IK najmniejszym nakładem pracy i kosztów. Podobnie sytuacja wygląda w przypadku remontów lub modernizacji.

2.6.6. Działania techniczne mające na celu zapewnienie ciągłości funkcjonowania IK

Zapewnienie możliwości kontynuacji działalności w lokalizacji zapasowej jest najlepszym sposobem ochrony przed zagrożeniami. Zastosowanie tego sposobu jest jednak uzależnione od technicznych i ekonomicznych możliwości organizacji.

W przypadku braku lokalizacji zapasowej wskazana jest redundancja (nadmiarowość) krytycznych elementów infrastruktury. Dotyczy to w szczególności urządzeń struktury systemu teleinformatycznego, np. serwerów, routerów, switchy. Niemniej to ocena ryzyka zakłócenia funkcjonowania IK powinna być podstawą decyzji, które elementy infrastruktury organizacji powinny zostać zdublowane. Redundancja powinna być zarówno logiczna, jak i fizyczna.

Systemy wentylacji, ogrzewania i klimatyzacji (jeśli są stosowane) należy tak zaplanować, by mogły funkcjonować w trybie wewnętrznej recyrkulacji powietrza, bez konieczności jego wymiany z otoczeniem. Umożliwi to zabezpieczenie przed niepożądanymi, zewnętrznymi zanieczyszczeniami, które mogą się pojawić w razie nieprzewidzianych zdarzeń, takich jak pożar, zapylenie szkodliwymi środkami chemicznymi lub biologicznymi. Poziom bezpieczeństwa można zwiększyć, instalując detektory monitorujące powietrze pod kątem obecności zanieczyszczeń chemicznych, biologicznych, radioaktywnych itp. Urządzenia klimatyzacyjne, których praca jest nieodzowna dla właściwego działania

obsługiwanych urządzeń technologicznych, powinny być projektowane z jednym klimatyzatorem rezerwowym, a co najmniej z jednym pełnym obiegiem chłodniczym.

2.6.7. Bezpieczeństwo technologiczno-procesowe

Bezpieczeństwo technologiczno-procesowe to taki stan technologiczny, aparaturowy, magazynowy, transportowo- logistyczny i organizacyjny projektowania i prowadzenia procesów, który gwarantuje skuteczne zapobieganie uwolnienia się substancji niebezpiecznej lub energii do środowiska pracy i środowiska naturalnego oraz ogranicza i przeciwdziała skutkom tych uwolnień (emisji).

W bezpieczeństwie technologiczno-procesowym każde zagrożenie jest charakteryzowane przez określony czynnik zagrożeń[24], do których zasadniczo należą właściwości substancji i procesów, a także możliwe awarie techniczne i zachowania ludzi, które są źródłem potencjalnych strat dla pracowników, majątku i środowiska, jak również społeczności lokalnych w zależności od uwarunkowań przestrzennych.

W bezpieczeństwie technologiczno-procesowym zagrożenie określa stan procesu produkcyjnego zachodzącego z udziałem substancji chemicznych/energii, których naturalne właściwości fizyczne, chemiczne lub biologiczne, stanowią element wyjściowy do oceny niewłaściwych warunków przebiegu procesu, powstania awarii lub błędnej organizacji i decyzji kierownictwa powodujących powstanie niepożądanych skutków i strat.

Do najbardziej znaczących skutków, przynoszących największe straty, szczególnie w przemyśle, transporcie lub magazynowaniu produktów niebezpiecznych należą zdarzenia z udziałem substancji niebezpiecznych lub substancji, których cechy niebezpieczne dla życia i zdrowia oraz środowiska naturalnego powstają dopiero w wyniku awarii.

2.6.7.1. Wybrane grupy i czynniki zagrożeń w bezpieczeństwie technologiczno-procesowym

Wśród znaczących czynników zagrożeń[25] w obszarze technologiczno-procesowym zaliczyć należy:

- procesy zachodzące pod wysokim i niskim ciśnieniem,
- procesy z gazami skroplonymi pod ciśnieniem lub w stanie wychłodzonym,
- procesy z cieczami przegrzanymi,
- procesy zachodzące w granicach mieszanin wybuchowych oraz w mieszaninach wzbogaconych w tlen,

24 Czynnik zagrożenia technologiczno-procesowego to parametr/wielkość charakteryzująca zagrożenie procesowe.

[25] A. S. Markowski, Bezpieczeństwo procesów przemysłowych. Wydawnictwo Politechniki Łódzkiej, Łódź 2022 r. – rozdział dotyczący zarządzania ryzykiem procesowym w przemyśle.

- procesy utleniania substancji palnych,
- procesy rozdrabniania i mielenia,
- termiczna ekspansja i kruchość materiałowa,
- elektryczność statyczna,
- niebezpieczne właściwości chemiczne substancji/ produktów,
- reaktywność chemiczna powstająca z reakcji dwóch lub więcej substancji niebezpiecznych lub z warunków umożliwiających przekształcenie w drodze reakcji substancji o niskim poziomie zagrożenia w substancję niebezpieczną,
- narażenie na czynniki toksyczne, wybuchowe, pożarowe, związane z przepływem energii, oddziaływaniem promieniowania cieplnego lub niskich temperatur, hałasu, niedoboru tlenu lub czynników chemicznych, biologicznych, radiacyjnych i nuklearnych,
- czynniki ludzkie – niedoświadczenie i brak wystarczającej wiedzy, niskie kwalifikacje, brak kompetencji, niska świadomość zagrożeń i ryzyka lub niska kultura wykonawcza lub zarządcza w zakresie utrzymania bezpieczeństwa procesowego.

W polskim przemyśle rekomendowany jest podział na 5 grup zagrożeń, które nie wyczerpują wszystkich możliwych grup i podziałów w bezpieczeństwie technologiczno- procesowym, jednakże sprawdzają się w praktyce przy identyfikacji zagrożeń i analizie ryzyka, w szczególności:

1. Zagrożenia procesowe, które są związane z warunkami prowadzonych operacji procesowych obejmujących następujące czynniki zagrożeń, w szczególności:
   - wysoka/ niska temperatura,
   - wysokie/niskie ciśnienie,
   - przepełnienie,
   - wybuch lub pożar wewnętrzny,
   - niekompatybilność chemiczną.
2. Zagrożenia materiałowe, które są związane z właściwościami substancji chemicznych lub rodzajem stosowanej energii obejmujące następujące czynniki zagrożeń, w szczególności;
   - struktura chemiczna i bilans tlenu substancji,
   - palność,
   - wybuchowość,
   - reaktywność,
   - toksyczność,
   - korozyjność,
   - niestabilność termiczna,
   - zdolność do autopolimeryzacji,
   - zdolność do przemian fazowych,
   - egzotermiczność,

- zdolność do dyspersji,
- ekotoksyczność.

3. Zagrożenia techniczne, które są związane z aparaturą i wyposażeniem procesowym obejmujące następujące czynniki zagrożeń, w szczególności:
   - utrata integralności lub wyposażenia (rozszczelnienia),
   - mechaniczne np. naprężenia, wady materiałowe, erozja, wibracja,
   - awarie automatyki procesowej,
   - awarie wyposażenia systemów zabezpieczeń procesowych,
   - brak testowania,
   - błędy projektowe w zakresie lokalizacji, struktury instalacji oraz rozmieszczenia, doborze i stosowanych zasad barier bezpieczeństwa,
   - awarie zasilania czynników pomocniczych (np. para wodna, prąd).
4. Zagrożenia organizacyjne, które są związane z niedociągnięciami w zakresie procesów zarządzania bezpieczeństwem obejmujące następujące czynniki zagrożeń, w szczególności:
   - brak polityki bezpieczeństwa procesowego,
   - brak mechanizmów zarządzania ryzykiem,
   - brak wykorzystania analizy i oceny ryzyka (jeśli są stosowane) do zarządzania zmianami i innych mechanizmów zarządzania bezpieczeństwem,
   - niewłaściwe procedury operacyjne (robocze),
   - błędy ludzkie wynikające z braku wiedzy, wyszkolenia, umiejętności na oczekiwanym poziomie, łamania procedur i zasad bezpieczeństwa lub wynikające z zaniedbania,
   - niski poziom utrzymania, serwisowania i konserwacji instalacji i aparatury procesowej,
   - brak ćwiczeń i innych form weryfikacji zasad bezpieczeństwa i postępowania w czasie awarii,
   - niewłaściwa struktura zarządcza w procesach zapobiegania i reagowania przeciwawaryjnego,
   - niska kultura bezpieczeństwa oraz niewłaściwy system komunikacji w procesach bezpieczeństwa procesowego,
   - brak planów reagowania w czasie wypadków i awarii oraz w zakresie ciągłości działania i odtwarzania infrastruktury procesowej,
   - niskie kompetencje kluczowych pracowników wobec wysokich standardów bezpieczeństwa.
5. Zagrożenia zewnętrzne, które są związane z możliwym odziaływaniem czynników zewnętrznych obejmujących następujące czynniki zagrożeń, w szczególności;

- ograniczenie lub przerwanie podstawowych usług i dostaw produktów zapewniających ciągłość działania i funkcjonalność procesów przemysłowych,
- zewnętrzny pożar, wybuch lub emisja substancji niebezpiecznej lub efekt domina wynikający z ich skutków,
- zagrożenie od sił przyrody (powódź, silne wiatry, opady śniegu lub deszczu, wyładowania atmosferyczne, wysokie lub bardzo niskie temperatury powietrza, epidemie),
- niska kultura współpracy administracji publicznej z przedsiębiorstwami realizującymi procesy przemysłowe,
- niskie kompetencje służb i struktur kryzysowych w przygotowaniu i reagowaniu na skutki wystąpienia poważnej awarii przemysłowej,
- cyberatak, sabotaż lub inne formy celowych działań przestępczych,
- błędy w regulacjach prawnych.

Poziom ryzyka procesowego zależy od wielu różnych współzależnych czynników i warunków, których dopiero złożona kombinacja prowadzi do awarii lub katastrofy przemysłowej (poważnej awarii). Niektóre z tych czynników samodzielnie nie powodują stanu zagrożenia, ale w połączeniu z innymi, znacznie zwiększają lub powodują powstanie ryzyk, które w efekcie mogą prowadzić do zmaterializowania zagrożenia i powstania strat. Praktycznym przykładem takich ryzyk są wyniki prac analitycznych na zakładach dużego i zwiększonego ryzyka (ZDR i ZZR)[26], jak również w wielu zakładach podprogowych[27].

W instalacjach procesowych zazwyczaj jest dużo lub bardzo dużo czynników decydujących o poziomie ryzyka procesowego, przy czym specjalne znaczenie mają:

- rodzaj stosowanych substancji i ich niebezpieczne właściwości oraz ich ilość,
- warunki operacyjne realizacji procesu,
- lokalizacja instalacji,
- niezawodność (zawodność) personelu, w tym jego kompetencje,
- właściwe zaprojektowanie pod względem funkcjonalności i odporności na zagrożenia oraz zarządzanie eksploatacją i serwisowaniem,
- system zarządzania ryzykiem i bezpieczeństwem.

[26] Prawo ochrony środowiska- rozdział dotyczący przeciwdziałania poważnym awariom (Seveso III) – wg danych GIOŚ w dniu 31 grudnia 2021 r. w Polsce było zarejestrowanych 477 ZDR i ZZR.

[27] To zwyczajowa nazwa zakładów stosujących znaczące ilości substancji niebezpiecznych, ale nie zaliczonych do ZDR i ZZR, o których mowa w prawie ochrony środowiska- wg danych PIP to około 750 zakładów w Polsce, natomiast wg danych KG PSP to około 1100 zakładów w Polsce.

2.6.7.2. *Ocena zapewnienia bezpieczeństwa instalacji procesowej*

Ocena zapewnienia bezpieczeństwa instalacji procesowej, bez względu na sektor jej zastosowania, jest realizowana poprzez dwa zasadnicze podejścia:

1) oparte o ocenę zgodności, oraz
2) oparte na ocenie ryzyka wystąpienia awarii lub poważnej awarii.

Każde podejście do zapewnienia bezpieczeństwa instalacji procesowej wymaga ze strony operatora IK udokumentowanych działań organizacyjno- technicznych, w szczególności:

1. Charakterystyki instalacji (węzłów procesowych).
2. Identyfikacji zagrożeń.
3. Wyboru reprezentatywnych zdarzeń wypadkowych i awaryjnych.
4. Oceny skutków ze scenariuszy zdarzeń z listy reprezentatywnych zdarzeń wypadkowych i awaryjnych.
5. Oceny prawdopodobieństwa.
6. Obliczania ryzyka.
7. Oceny ryzyka, która prowadzi przez opcje zmniejszania prawdopodobieństwa lub/i skutków wypadków i awarii w celu optymalizacji zarządzania ryzykiem.

Przed uruchomieniem procesu zarządzania ryzykiem, warto poczynić rzetelne prace przygotowawcze i planistyczne, wymagające pracy zespołowej i akceptacji ze strony operatora IK decyzji dotyczących przebiegu poszczególnych elementów składowych związanych z identyfikacją zagrożeń, a następnie z analizą, oceną i postępowaniem z ryzykiem procesowym. Warto też przeanalizować dotychczasowe podejście do analizy i oceny ryzyka, o ile proces zarządzania ryzykiem był cyklicznie realizowany w bezpieczeństwie technologiczno-procesowym.

W ramach prac wstępnych inwentaryzuje się liczbę instalacji, istotność i wpływ czynników na ich bezpieczeństwo i ciągłość procesową, szacuje czas na wykonanie oceny ryzyka oraz czas potrzebny na dyskusje i rekomendacje dla poszczególnych instalacji lub węzłów procesowych, a w efekcie końcowym całego zakładu.

Analizę ryzyka rozpoczyna się od zebrania danych dotyczących właściwości stosowanych substancji chemicznych (np. na bazie kart charakterystyki) oraz dokładnego zapoznania się z danymi historycznymi dotyczącymi zaistniałych wypadków i awarii dla badanej instalacji u operatora IK oraz w innych podmiotach (organizacjach), o podobnym zakresie działalności. W ramach tych prac analizuje się założenia projektowe i wszelkie dokumenty, które opisują i obrazują charakterystykę instalacji lub poszczególnych węzłów procesowych i terenu otoczenia oraz pozwalają zestawić i porównać wymagania i standardy związane z jej bezpieczeństwem, w tym systemami zabezpieczeń, a także dane dotyczące stosowanych substancji wraz z ich

klasyfikacją i ilościami, lokalizacją instalacji, oceną warunków otoczenia, warunków meteo, a także opisu technologii wraz z załączonymi schematami. Proces analityczny związany jest z wizytami na instalacji oraz podsumowaniem dotychczasowych prac z jej specyfiki wraz z doprecyzowaniem planu dalszych działań w ramach kontynuacji procesu analizy zagrożeń i oceny ryzyka.

W pierwszym etapie analizy dokonuje się identyfikacji źródeł zagrożeń wewnętrznych i zewnętrznych oraz identyfikuje się możliwe zdarzenia inicjujące sekwencję zdarzeń awaryjnych z uwzględnieniem przyczyn i skutków. Na tym etapie prac wykorzystuje się różne metody jakościowe, z których najczęściej stosuje się metody kompleksowe HAZOP lub PHA. Możliwe do zastosowania są również inne metody np. uproszczone typu „Co- jeśli?" lub listy kontrolne.

Metoda HAZOP ma charakter uniwersalny i jest najczęściej stosowana w przemyśle, gdyż polega na identyfikacji wszystkich potencjalnych czynników zagrożeń i awarii oraz innych strat występujących w instalacjach procesowych, spowodowanych odchyleniami od normalnych, założonych warunków pracy danej instalacji lub urządzenia. Dwie typowe cechy które charakteryzują tę metodę to: systemowe zastosowanie zestawu słów kluczowych oraz zespół analityczny. W przypadku zastosowania tej metody należy:

1) opracować arkusz roboczy,
2) dokonać podziału instalacji na węzły,
3) określić głębokość analizy, czyli szczegółowość rozpatrywania przyczyn oraz graniczne parametry operacyjne dla każdego węzła procesowego, jak również rodzaj i ilość zawartej substancji chemicznej,
4) dokonać identyfikacji rodzaju odchyleń procesowych istotnych dla każdego węzła instalacji,
5) opracować kryteria wyboru reprezentatywnych zdarzeń awaryjnych (RZA), poprzez matrycę wyboru lub matrycę rankingową (decyzje operatora IK),
6) przeprowadzić analizę HAZOP i na jej podstawie opracować listę zdarzeń awaryjnych (LZA), a następnie listę reprezentatywnych zdarzeń awaryjnych (LRZA).

Metoda PHA koncentruje się na czynnikach zagrożeń związanych z uwolnieniem substancji niebezpiecznych odniesionych do całej instalacji lub oddzielonych jej węzłów. Po przyjęciu arkusza roboczego kolejno dla każdego rodzaju zagrożenia określa się przyczyny, możliwe skutki i rodzaj występujących lub projektowanych systemów bezpieczeństwa. W następnym etapie szacuje się kategorię częstości wystąpienia określonych skutków i kategorię wielkości skutków. Działanie to pozwala określić kategorię ryzyka lub wartość, które poprzedza się wyborem matrycy.

Lista zdarzeń awaryjnych (LZA) może zostać uproszczona do tzw. listy reprezentatywnych zdarzeń awaryjnych, co oznacza, że uwolnienie dotyczy tej samej substancji i jednego typorodzaju aparatury pracującej w zbliżonych parametrach operacyjnych, jak również, że może reprezentować podobne tego typu zdarzenia, dla tego samego odcinka badawczego. Ważne jest, aby przy kwalifikacji zdarzenia awaryjnego do reprezentatywnych scenariuszy awaryjnych kierować się następującymi zasadami:

1. Metody rankingu dobierać według poziomu ryzyka lub poziomu zagrożeń.
2. Zasada łączenia podobnych zdarzeń, w których występują te same substancje i te same lub podobne warunki operacyjne.
3. Zasada wiarygodności oparta na możliwości wystąpienia danego zdarzenia awaryjnego.

Każde zdarzenie jest poddawane analizie określenia mechanizmu powstawania i rozwoju tego zdarzenia. Reprezentatywne zdarzenia awaryjne poddaje się analizom, najlepiej na zasadach „burzy mózgów", w celu wytypowania reprezentatywnych scenariuszy (zdarzeń) awaryjnych – RSA. W tym zakresie stosuje się różne techniki analityczne tj. drzewa błędu (FTA), drzewa zdarzeń (ETA) i metodę „bow-tie". Realizacja zadań w procesie analizy ryzyk daje wiedzę na temat: co się może wydarzyć, w jaki sposób do tego dojdzie i jakie będą skutki, co stanowi kluczową część procesu do przygotowania optymalizacji zarządzania ryzykiem. Do analizowania scenariuszy awaryjnych najbardziej polecaną metodą jest „bow-tie", gdyż:

- ilustruje zależności między zdarzeniami inicjującymi, zdarzeniami przejściowymi (warunkującymi i umożliwiającymi rozwój scenariusza), systemami bezpieczeństwa (barierami) realizującymi odpowiednie funkcje bezpieczeństwa i innymi czynnikami kontrolnymi,
- łączy metody drzewa błędów (FTA) i drzewa zdarzeń(ETA).

Etap analizy skutków i ich oceny nie zależy tylko od charakterystyk właściwości i uwolnienia substancji niebezpiecznych, ale również od szybkości i efektywności działania (przeciwdziałania) systemu zabezpieczeń, jakim są wewnętrzne rozwiązania techniczno – organizacyjne. Na proces skuteczności systemów przeciwdziałania ma również wpływ zidentyfikowanie czynników warunkujących niepożądane zdarzenie, np. charakterystyka źródła zapłonu, przestrzenie w których powstają efekty fizyczne, czy charakterystyka strukturalna obiektów, np. budowli lub budynków. Ustalenie wielkości skutków i zasięgu uwolnień (czyli stref zasięgu stref zagrożeń) to cel analizy efektów fizycznych i skutków, stanowiący wieloetapowy ciąg analiz i obliczeń oraz dyskusji zespołowej, aż do wskazania rekomendacji.

Celem zarządzania ryzykiem procesowym jest osiągnięcie kontroli nad czynnikami zagrożeń występujących w procesach, z udziałem substancji niebezpiecznych. Stąd

przyjęte wskaźniki lub kategorie ryzyka procesowego poddawane są ocenie w celu ustalenia dopuszczalności ryzyka. Wykorzystuje się do tego celu kryteria akceptacji ryzyka stosowane jako wytyczne lub zalecenia w danym kraju. Ponieważ w Polsce nie ma ustalonych wytycznych dotyczących kryteriów akceptacji ryzyka, stąd każdy operator samodzielnie podejmuje decyzje o ich stosowaniu. Przemysł kieruje się najczęściej kryteriami półilościowymi, stosując matrycę ryzyka, albo wykorzystuje stosowane kryteria ryzyka dostępne z innych państw europejskich lub USA o podobnych zakładach przemysłowych.

W przypadku nieakceptacji wyznaczonego poziomu ryzyka w porównaniu z wybranymi kryteriami akceptacji ryzyka, koniecznym jest uruchomienie kolejnego etapu prac, poprzez wprowadzenie propozycji dodatkowych środków zabezpieczeń i ochrony dla uzyskania, co najmniej dopuszczalnego poziomu ryzyka. Uzyskanie akceptowalnego poziomu ryzyka to jeden z ostatnich etapów prac, który zależy od procesów wcześniejszych i stanowi podstawę dla przedłożenia odpowiednich informacji i wniosków dla władz operatora IK oraz właścicieli i zarządzających ryzykiem i bezpieczeństwem poszczególnych zakładów, instalacji lub urządzeń w zakresie proponowanych decyzji strategicznych dotyczących zmian organizacyjnych, technicznych lub koniecznych nakładów finansowych.

2.6.7.3. *Ryzyko wybuchowe*

Ryzyko wybuchowe jest częścią składową ryzyka zawodowego, pracowniczego, obiektowego i technologiczno-procesowego, które najczęściej dotyczy następujących sektorów, w szczególności:

1) przemysłu chemicznego i petrochemicznego,
2) przemysłu wydobywczego,
3) przemysłu spożywczego,
4) przemysłu farmaceutycznego,
5) przemysłu drzewnego,
6) baz surowcowych, magazynowych i przeładunkowych,
7) energetyki,
8) transportu.

Przystępując do oceny ryzyka wybuchu, należy zidentyfikować w procesie analizowania źródeł i czynników zagrożeń wszystkie występujące substancje palne. Określenie właściwości substancji palnych i ich parametrów wybuchowości stanowi podstawę rozpoczęcia prac nad oceną ryzyka wybuchu i ma zasadnicze znaczenie w kolejnych etapach ich prowadzenia. Do istotnych parametrów wybuchowości można zaliczyć, w szczególności:

1. Minimalną energię zapłonu,
2. Maksymalne ciśnienie wybuchu,

3. Współczynniki wybuchowości dla pyłów oraz gazów i par cieczy,
4. Temperaturę zapłonu obłoku pyłu i zapłonu warstwy,
5. Temperaturę samozapłonu dla gazów i par cieczy,
6. Temperaturę zapłonu cieczy.

Powyższe parametry są wyjściowe do oszacowania ryzyka oraz potencjalnych skutków wybuchu, wskazania działań prewencyjnych, doboru urządzeń do pracy w danej strefie zagrożenia wybuchem oraz zaprojektowania systemu minimalizującego skutki wybuchu. Przy ocenie ryzyka wybuchu istotne jest podejście operatora IK do wybuchowości pyłów. Właściwości wybuchowe pyłów są zmienne i zależą od ich rozdrobnienia i wilgotności, co generuje dwie zasadnicze rodzaje konsekwencji:

1) dane uzyskane z własnych baz i literatury pozwalają jedynie określić wstępne zagrożenie, natomiast określenie parametrów wybuchowości próbek pyłu możliwe jest tylko w warunkach laboratoryjnych,
2) specyfika pyłu polega na tym, że pobrana próba z jednej części instalacji procesowej może nie mieć właściwości wybuchowych, natomiast z innej części tejże samej instalacji, może je nabyć np. w wyniku suszenia lub rozdrobnienia.

Kolejnym etapem jest wykonanie oceny ryzyka wybuchu, a na jej podstawie opracowanie dokumentu zabezpieczenia przed wybuchem (DZPW). Ocena ryzyka wybuchem służy po to aby wskazać przestrzenie, w których może występować lub pojawić się atmosfera wybuchowa, gdyż na ich podstawie operator IK, jako pracodawca, ma obowiązek podzielić przestrzenie zagrożone wybuchem na strefy, klasyfikując je na podstawie prawdopodobieństwa i czasu występowania atmosfery wybuchowej.

Ocena ryzyka wybuchu powinna być wykonana dla:

- normalnych warunków pracy, włącznie z konserwacją,
- uruchamiania i wycofywania z eksploatacji obiektów, instalacji i urządzeń,
- nieprawidłowego funkcjonowania, przewidywanych awarii,
- nieprawidłowego użycia, które można racjonalnie przewidzieć.

Dokument Zabezpieczenia Przed Wybuchem (DZPW) to kompletny, a zarazem najważniejszy dokument (według dyrektywy ATEX Users) jaki w świetle powinien posiadać każdy podmiot, na terenie którego występuje zagrożenie wystąpienia niekontrolowanego wybuchu, wywołanego obecnością palnych i wybuchowych pyłów, proszków, par, palnych cieczy, gazów, mgieł i mieszanin hybrydowych.

2.6.8. Najważniejsze rekomendacje dotyczące zapewnienia bezpieczeństwa technicznego:

1. Analiza zagrożeń i ocena ryzyka realizowana jest w procesie projektowania, budowy, oddania obiektu, instalacji lub urządzania do użytkowania oraz w procesie jego eksploatacji, napraw i serwisowania.
2. Błędy ludzkie są najczęstszymi przyczynami zakłócenia funkcjonowania infrastruktury.
3. Niepotrzebne remonty mogą okazać się szkodliwe, gdyż starając się przywrócić urządzenie do stanu idealnego, może wystąpić tzw. "efekt nowości", który oznacza, że wiele komponentów ulega awarii we wczesnym okresie eksploatacji.
4. W celu zapobiegania potencjalnym awariom oraz zapewnienia długoterminowej eksploatacji danego obiektu IK, wskazane jest sukcesywne prowadzenie kompleksowej oceny stanu technicznego w oparciu o analizy bezpieczeństwa oraz indywidualnie dedykowane programy badań i pomiarów.
5. Dla obiektów, w których zlokalizowane są elementy infrastruktury krytycznej należy przyjmować najwyższe wymagania dotyczące niezawodności zasilania i dostępu do mediów.
6. Osiągnięcie lub utrzymanie akceptowalnego poziomu bezpieczeństwa technicznego jest coraz bardziej pożądane nie tylko ze względu na przepisy prawne, ale ze względu na coraz większe znaczenie procesów zarządzania ryzykiem i kultury bezpieczeństwa. Dla wielu organizacji podniesienie poziomu bezpieczeństwa technicznego przekłada się na konkurencyjność w realizacji misji biznesowej i publicznej.
7. Wielu operatorów IK w ramach wzmocnienia swojej odporności, w tym w zakresie zabezpieczeń[28] technicznych, wdraża innowacyjne rozwiązania techniczno-organizacyjne, stosując wyższe wymagania i standardy bezpieczeństwa technicznego, niż wskazują przepisy krajowe lub międzynarodowe. Na poziom bezpieczeństwa technicznego mają także wpływ sprawdzone i zaimplementowane dobre praktyki polskie i zagraniczne wynikające z wiedzy i doświadczeń inżynierskich, branżowych, korporacyjnych lub rekomendacji niezależnych zespołów interdyscyplinarnych np. z zakresu zarządzania ryzykiem, działań antyterrorystycznych, systemów antydronowych, cyberbezpieczeństwa i bezpieczeństwa technologiczno-procesowego, energetycznego, budowlanego, hydrotechnicznego, przeciwpożarowego, ochrony środowiska lub bezpieczeństwa pracy, które po wdrożeniu stanowią standardy oczekiwanych wymagań w danej dziedzinie lub obszarze bezpieczeństwa.

[28] Zabezpieczenie to działania, systemy, wydzielone zasoby oraz zbiory przygotowanych zaleceń, zasad, procedur i instrukcji stosowanych w reakcji na rozpoznane zagrożenie w celu jego wyeliminowania (likwidacji) lub/i ograniczenia oddziaływania w sytuacji jego zmaterializowania.

8. Dobrą praktyką jest, że zespół realizujący ocenę ryzyka procesowego posiada swojego lidera i właściciela (zarządcę) instalacji oraz posiada strukturę i narzędzia do pracy, a także posiada stosowną liczbę i rodzaj ekspertów, którzy mają świadomość, że harmonogram prac jest spójny z planami prac innych zespołów dokonujących oceny ryzyk w obszarach bezpieczeństwa IK i działalności organizacji.

2.7. Zapewnienie bezpieczeństwa osobowego

Zapewnienie bezpieczeństwa osobowego to zespół przedsięwzięć i procedur mających na celu minimalizację ryzyka związanego z osobami, które przez autoryzowany dostęp do obiektów, urządzeń, instalacji i usług infrastruktury krytycznej, mogą spowodować zakłócenia w jej funkcjonowaniu.

Członkowie personelu związanego z obiektami, urządzeniami, instalacjami i usługami infrastruktury krytycznej oraz osoby czasowo przebywające w obrębie IK (usługodawcy, dostawcy, goście) mogą stanowić potencjalne zagrożenie dla jej funkcjonowania. Pozycja zajmowana w strukturze operatora IK determinuje poziom dostępu fizycznego do kolejnych stref bezpieczeństwa oraz dostęp do informacji wrażliwych, niekoniecznie niejawnych. Oba te przywileje mogą być nielegalnie wykorzystane i służyć zakłóceniu funkcjonowania IK lub działaniu na jej niekorzyść (dotyczy to także usługodawców, dostawców i gości).

Ponad 85 % nadużyć w firmach powodowanych jest przez ludzi z wewnątrz firmy[29].

Należy pamiętać, że wiele aspektów zapewnienia bezpieczeństwa osobowego jest nierozerwalnie związanych z innymi elementami systemu bezpieczeństwa IK, takimi jak zapewnienie bezpieczeństwa fizycznego czy teleinformatycznego. Dopiero komplementarność wszystkich elementów zapewni satysfakcjonujący poziom zapewnienia bezpieczeństwa IK przed zagrożeniami wewnętrznymi, np. rozczarowanymi pracownikami, prowokacjami, konkurencją czy przestępczością zorganizowaną.

Dla usystematyzowania informacji, tekst został podzielony na rozdziały odpowiadające kolejnym etapom działania z osobami mogącymi mieć negatywny wpływ na funkcjonowanie IK.

[29] Ernst & Young 9th International Fraud Survey – IX Badania Nadużyć Gospodarczych – Ryzyko Nadużyć na Rynkach Wschodzących.

2.7.1. Postępowanie w trakcie zatrudniania

Podstawą skuteczności zapewnienia bezpieczeństwa osobowego jest zebranie jak największej liczby informacji, możliwych do uzyskania w świetle obowiązującego prawa, o potencjalnym pracowniku już w procesie rekrutacji. Aby zoptymalizować czas, siły i środki wykorzystywane w postępowaniu rekrutacyjnym, należy przede wszystkim dokładnie sporządzić profil kandydata, a precyzyjne określenie zakresu obowiązków pozwoli ustalić poziom dostępu do stref, pomieszczeń, depozytorów itp., jaki będzie mu przyznany oraz jakimi informacjami wrażliwymi będzie dysponował.

Warto przeprowadzić ocenę ryzyka zakłócenia funkcjonowania IK, związanego z nielegalnym wykorzystaniem informacji lub praw dostępu dla różnych stanowisk w strukturze organizacji. Ocena ta będzie stanowić podstawę decyzji o szczegółowości postępowania sprawdzającego w procesie zatrudniania. Pozwoli także na lepsze określenie kryteriów, jakim powinien odpowiadać kandydat. Taką ocenę można wprowadzić i zakomunikować w formie skoordynowanej polityki zatrudniania w organizacji.

2.7.2. Ustalenie tożsamości

Warunkiem koniecznym do dalszego procedowania jest weryfikacja tożsamości kandydata. Nie należy podejmować dalszych czynności, jeśli istnieją jakiekolwiek zastrzeżenia co do jej poprawności!

Na tożsamość osoby składają się przymioty nadawane po narodzeniu (imię, nazwisko, data i miejsce urodzenia, imiona rodziców), indywidualne cechy biometryczne (biometria linii papilarnych, tęczówki, dłoni, twarzy, DNA) oraz elementy biografii (historia edukacji, zatrudnienia).

Sprawdzenie tożsamości powinno odbywać się przede wszystkim na podstawie przedstawionych oryginalnych dokumentów, zawierających imiona, nazwisko, datę urodzenia, adres, podpis posiadacza oraz zdjęcie. Należy sprawdzić, czy okazywany dokument jest wydany przez właściwy organ i ma aktualną datę ważności. Obowiązkowo należy wymagać dokumentów trudnych do podrobienia, takich jak: paszport, dowód osobisty czy prawo jazdy. Konieczne należy weryfikować autentyczność przedstawianych przez kandydata dokumentów. Pracownicy dokonujący takiej weryfikacji muszą posiadać odpowiednią wiedzę i umiejętności w celu przeprowadzenia takich sprawdzeń.

2.7.2.1. *Kwalifikacje*

Sprawdzenie kwalifikacji kandydata powinno opierać się o weryfikację informacji zawartych w dokumentach rekrutacyjnych (CV, formularze, świadectwa pracy, itp.). Pozwoli to ocenić wiarygodność i uczciwość kandydata oraz zdobyć informacje, które chciałby ukryć. Podobnie jak w przypadku ustalenia tożsamości, wszelkie dokumenty powinny być oryginalne. Weryfikacja prawdziwości przekazanych dokumentów powinna odbyć się podczas osobistego stawiennictwa kandydata w toku postępowania rekrutacyjnego po etapie preselekcji.

- **Wykształcenie**
  Należy porównać, czy zgadzają się informacje opisane w CV z przedstawianymi świadectwami, certyfikatami itp. Uwagę winno się zwrócić na nazwę szkoły, uczelni, firmy. Obecnie wiele podmiotów organizujących kursy czy szkolenia wykorzystuje nazwy podobne do wiodących i uznanych uczelni, aby w ten sposób przyciągnąć uczestników, nie gwarantując przy tym wysokiego poziomu kształcenia. Dodatkowo potwierdzić należy daty i dokładne nazwy kursów i otrzymanych tytułów. Dobrą praktyką jest wymaganie dokładnego planu takich kursów czy studiów, a w razie wątpliwości kontakt z uczelnią.
- **Doświadczenie**

  Podobną procedurę należy przeprowadzić przy sprawdzaniu doświadczenia zawodowego. Wymagać należy podania historii zatrudnienia z okresu co najmniej 3 lat (chyba, że z obowiązujących przepisów wynika inny okres). Zweryfikować należy czas zatrudnienia, stanowisko i wykonywane obowiązki. Poznanie powodu odejścia także będzie cenną informacją. Skontaktowanie się z poprzednimi pracodawcami jest o tyle wartościowe, że poza otrzymaniem informacji opisywanych powyżej, możliwe będzie też ustalenie innych umiejętności pracownika, takich jak współpraca w grupie czy sumienność wykonywanych obowiązków. Dlatego też warto rozważyć prośbę o referencje od bezpośredniego przełożonego.
- **Predyspozycje**

  Wykorzystując narzędzie badawcze, jakim są testy psychologiczne (w odniesieniu do stanowisk, co do których realizacja testów jest zasadna) i narzędzia psychometryczne, można ocenić osobowość kandydata, możliwości analityczne – predyspozycje do określonej pracy. Dodatkowo można przedstawić kandydatowi teoretyczny problem z zakresu jego potencjalnych obowiązków i zaproponować aby go rozwiązał. Pozwoli to poznać w pewnym stopniu metodykę jego działań, umiejętności tworzenia związków przyczynowo-skutkowych.

2.7.2.2. *Przeszłość kryminalna*

W przypadku rekrutacji na kluczowe stanowiska, połączone z dostępem do informacji niejawnych, postępowanie sprawdzające przeprowadzają właściwe służby ochrony państwa. Nie należy jednak zaniedbywać wewnętrznego procesu weryfikacji kandydata. Ułatwieniem w tym zakresie są obowiązujące przepisy prawa ujęte m.in. w ustawie o zarządzaniu kryzysowym, pozwalające żądać od pracownika (lub kandydata do pracy), przedłożenia informacji dotyczących karalności, w tym informacji, czy ich dane osobowe są zgromadzone w Krajowym Rejestrze Karnym.

2.7.3. *Postępowanie w stosunku do zatrudnionych*

Priorytetem w zapewnieniu bezpieczeństwa osobowego jest dokładne sprawdzenie pracownika (np. analiza złożonych dokumentów i weryfikacja ich autentyczności) jeszcze przed jego zatrudnieniem, nie wolno zaniedbywać jednak zasad bezpieczeństwa w stosunku do już zatrudnionych w organizacji. W trakcie zatrudnienia, w przypadku zmiany stanowiska pracy należy zweryfikować nadane osobie uprawnienia i dostosować je do obecnie zajmowanego stanowiska. Wszelkie uprawnienia, które posiadał pracownik w związku z poprzednio zajmowanym stanowiskiem powinny zostać cofnięte. Kluczowe znaczenie ma w tym przypadku **informacja z działu kadr o zmianie stanowiska** do pozostałych komórek organizacyjnych, w tym odpowiedzialnych za bezpieczeństwo. Wskazane jest także okresowe weryfikowanie niezbędności uprawnień przyznanych wszystkim osobom – pracownikom i podwykonawcom zewnętrznym.

2.7.3.1. *Niestandardowe zachowania*

Obserwacja zachowań pracowników jest jednym ze sposobów wykrycia potencjalnego zagrożenia wewnętrznego. Podkreślić należy jednak, że nie chodzi o wścibskość lub inwigilację, a jedynie ocenę możliwości wystąpienia takiego zagrożenia.

Zespół powinien być uwrażliwiony na zmiany zachowania i informować o tych, które mogą świadczyć o rozluźnieniu związku pracownika z organizacją lub jego problemy osobiste, takie jak:

- nadużywanie alkoholu,
- wypowiadanie poglądów aprobujących działania grup ekstremistycznych,
- zmiana wyznania, przynależności politycznej, społecznej,
- niewytłumaczalne zmiany w życiu osobistym,
- brak zainteresowania wykonywaną pracą, rozczarowanie,
- znamiona silnego stresu: agresja, choleryczne zachowanie,

- zmiana godzin pracy, przyzwyczajeń,
- niestandardowe zainteresowanie systemami bezpieczeństwa,
- brak przestrzegania procedur bezpieczeństwa,
- nieusprawiedliwione nieobecności.

Powyższa lista niestandardowych zachowań nie jest kompletna i nie może być jedynym kryterium do podjęcia kroków dyscyplinarnych. Może natomiast, razem z innymi przesłankami, stanowić podstawę do udzielenia danej osobie pomocy lub kontroli jej działalności w organizacji. Szczególnie wystąpienie całego szeregu przesłanek musi wzbudzić zainteresowanie osób odpowiedzialnych w organizacji za bezpieczeństwo.

2.7.3.2. *Dostęp*[30]

Jednym z podstawowych sposobów na zapewnienie bezpieczeństwa osobowego IK jest ograniczanie dostępu pracowników organizacji do wrażliwych miejsc lub zasobów znajdujących się na terenie organizacji, jak i w sieciach teleinformatycznych. Dostęp powinien być przyznawany tylko w zakresie i czasie potrzebnym do wykonywania swoich obowiązków służbowych. Próba dotarcia do zastrzeżonych stref, sieci lub zasobów może świadczyć o potencjalnym zagrożeniu ze strony pracownika.

Osoby odpowiedzialne za bezpieczeństwo w ustalonych odstępach czasu powinny:

- weryfikować prawa dostępu i w razie potrzeby je ograniczać,
- kontrolować, analizować i raportować wszelkie próby nieautoryzowanego dostępu do miejsc (pomieszczeń) oraz sieci i zasobów teleinformatycznych.

Pracownicy organizacji powinni być uczuleni na próby nieautoryzowanego dostępu wszelkich osób do zastrzeżonych miejsc oraz informować odpowiedzialne osoby o zauważonych tego typu próbach.

2.7.3.3. *Identyfikacja wizualna*

Identyfikacja wizualna pracowników organizacji oraz podwykonawców i gości jest najprostszym sposobem określenia przynależności do organizacji oraz potencjalnych uprawnień.

Każda osoba znajdująca się w obiekcie należącym do IK powinna nosić w widocznym miejscu identyfikator zawierający fotografię twarzy posiadacza. Identyfikator nie powinien jednak zawierać (ze względów bezpieczeństwa, np. po zgubieniu) informacji o przydzielonych mu prawach dostępu. Powinien za to być oznaczony odpowiednim dla strefy (budynku)

[30] O zasadach i sposobach przyznawania i kontroli dostępu czytaj także w rozdz. 2.5.1 i 2.5.3.

kolorem, w celu szybkiego rozpoznania każdego nielegalnie przebywającego w danym obszarze pracownika i podjęcia odpowiednich kroków. Tam, gdzie ma to uzasadnienie, należy wprowadzić dodatkowo odzież służbową lub inny sposób identyfikacji przez elementy ubioru (kolorowe kamizelki, kaski itp.). Wprowadzając odzież służbową należy pamiętać, że nie może to być jedyny sposób identyfikacji wizualnej zezwalający na dostęp do obiektu (osoba nosząca uniform z logo firmy niekoniecznie musi być tą, za którą się podaje).

Nie należy nosić identyfikatorów w widocznych miejscach poza obiektami IK. Utrudni to osobom niepowołanym poznanie wyglądu graficznego identyfikatorów. Osobom spoza organizacji nie należy również zezwalać na wynoszenie identyfikatorów poza obiekt.

2.7.4. Ochrona kluczowego personelu

W każdej organizacji są osoby posiadające newralgiczną (unikalną) wiedzę na temat jej funkcjonowania oraz doświadczenie i „pamięć instytucjonalną". Są one szczególnie cenne dla organizacji, a jednocześnie stanowią potencjalnie największe zagrożenie na wypadek działania na niekorzyść organizacji. W celu ochrony informacji mających istotne znaczenie dla pracodawcy zawierane są z nimi odrębne umowy o zakazie konkurencji w czasie trwania i po ustaniu stosunku pracy. Takie osoby powinny mieć zapewnione przez pracodawcę satysfakcjonujące warunki pracy, obejmujące wynagrodzenie, czas pracy i prestiż. Pracodawca powinien zapewnić także możliwość sukcesywnego podnoszenia kompetencji oraz wsparcie podmiotów zewnętrznych. Ochrona kluczowego personelu oznacza także bardziej restrykcyjne wymogi kontrolne w stosunku do tych osób. Należy także podjąć kroki dające możliwość zastępstwa o podobnych kwalifikacjach oraz uprawnieniach.

2.7.5. Usługodawcy/podwykonawcy

Pracownicy podmiotów, wykonujący pracę na zlecenie operatora IK, powinni zostać zweryfikowani w podobny sposób, jak w przypadku rekrutacji, a dodatkowo należy

sprawdzić, czy dany podwykonawca jest członkiem rozpoznawalnego i uznanego stowarzyszenia, posiada odpowiednie licencje, spełnia standardy jakości, posiada stabilność finansową itp.

Cenne są rekomendacje personalne, referencje od operatorów z tego samego systemu i przykłady już wykonanych prac, ale nawet gdy są one bardzo dobre, należy podać do wiadomości podwykonawcy, że są one weryfikowane.

Po ustaleniu zakresu usługi i ocenie ryzyka zakłócenia funkcjonowania IK powinno się ustalić poziom dostępów, przeprowadzić szkolenie informujące o występujących zagrożeniach i obowiązujących procedurach i dopiero wtedy wydać przepustki lub ustanowić prawa dostępu do sieci. Wszelkie prace mogące mieć negatywny wpływ na IK muszą być wykonywane pod nadzorem stałej kadry IK.

2.7.6. Postępowanie z odchodzącymi z pracy

Każdy z pracowników odchodzących z organizacji jest w posiadaniu mniej lub bardziej wrażliwej wiedzy, która może być wykorzystana ze stratą dla organizacji. Dlatego w każdym przypadku konieczna jest indywidualna ocena ryzyka związanego z możliwością ujawnienia informacji. Szacowanie powinno być oparte o kilka wytycznych. Pierwszym jest zajmowane stanowisko implikujące poziom dostępu do informacji. Drugim – powód odejścia z zakładu pracy (dobrowolny, dyscyplinarny, redukcja zatrudnienia, wygaśnięcie umowy). Dalej należy sprawdzić najbliższe plany pracownika, czy np. nowym miejscem zatrudnienia nie będzie firma konkurencyjna.

Postępowanie w okresie wypowiedzenia będzie wynikało z przeprowadzonej oceny ryzyka i będzie w głównej mierze oparte o ograniczenie dostępu w zależności od poziomu ryzyka, chyba że zwolnienie ma charakter natychmiastowy, wtedy należy odebrać pełny dostęp, a cały proces opuszczania miejsca pracy przeprowadzić pod nadzorem. Nie oznacza to jednak, że pracownikowi odchodzącemu dobrowolnie, na emeryturę należy pozostawić w okresie wypowiedzenia pełny dostęp. Decyzje w tym zakresie podejmuje w konkretnych sytuacjach pracodawca. Istnieje możliwość zwolnienia pracownika z obowiązku świadczenia pracy w okresie wypowiedzenia.

Opuszczający stanowisko pracownik powinien zwrócić:

- odzież firmową, w tym umundurowanie (jeśli występuje),
- identyfikatory, przepustki,
- służbowe telefony komórkowe,
- służbowe karty kredytowe,
- służbowe wizytówki,
- klucze do pomieszczeń,
- generatory kodów jednorazowych,
- należące do organizacji dokumenty,
- przenośne dyski danych, komputery.

Jednocześnie osoby odpowiedzialne za przyznawanie dostępu (fizycznego i teleinformatycznego) powinny:

- zablokować uprawnienia dostępu do systemów, w tym dezaktywować identyfikatory, karty dostępu, hasła,
- zmienić kody dostępu do drzwi, depozytorów,
- anulować karty kredytowe,
- przekazać pracownikom ochrony odpowiednio wcześniej informację o cofnięciu uprawnień pracownikowi.

W przypadku śmierci pracownika należy zastosować podobne czynności. Warto sprawdzić czy jest się w posiadaniu aktualnego kontaktu do rodziny, dzięki któremu możliwe będzie natychmiastowe odzyskanie ww. przedmiotów.

Należy rozważyć zmianę uprawnień dostępu (haseł, identyfikatorów, kart) do zasobów, danych, miejsc (stref), które odchodzący pracownik dzielił z innymi w ramach pracy zespołowej.

Aby podnieść świadomość operatorów IK o zagrożeniach wewnętrznych warto stworzyć na poziomie systemu IK (sektora) bazę danych informacji o zagrożeniach wewnętrznych i incydentach z udziałem pracowników, podwykonawców lub gości oraz mechanizm bezpiecznej wymiany tych informacji. Baza prowadzona na poziomie centralnym mogłaby zawierać informacje zebrane z poziomu sektorowego. Anonimowe przykłady mogą pomóc w przeprowadzeniu dokładniejszej oceny ryzyka i wdrożeniu efektywniejszych środków ochrony.

Bardzo duże znaczenie dla skutecznego procesu zapewnienia bezpieczeństwa osobowego ma profilaktyka przeciwdziałania nadużyciom. Działania operatora takie jak promowanie etyki zawodowej, polityka uczciwości we wszystkich działaniach firmy, etyczny przykład kierownictwa oraz skuteczne mechanizmy kontrolne skutecznie zmniejszają ryzyko popełnienia świadomego działania niepożądanego przez pracownika.

2.7.7. Najważniejsze rekomendacje dotyczące zapewnienia bezpieczeństwa osobowego:

1. Oceń ryzyko zakłócenia funkcjonowania IK dla konkretnych stanowisk w strukturze organizacji.
2. Poświęć dużo czasu na sprawdzenie wiarygodności i kompetencji nowego pracownika.
3. Uświadamiaj organizację, że zagrożeniem może być każdy pracownik.
4. Zidentyfikuj i stwórz odpowiednie warunki kluczowemu personelowi.
5. Informuj (dział kadr) pozostałych komórki organizacyjne, w tym odpowiedzialnych za bezpieczeństwo o zmianie przez pracowników zajmowanych przez nich stanowisk.
6. Nie zwlekaj z odebraniem praw dostępu pracownikom odchodzącym z organizacji.

2.8. Zapewnienie bezpieczeństwa teleinformatycznego

Zapewnienie bezpieczeństwa teleinformatycznego infrastruktury krytycznej to zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie nieautoryzowanego oddziaływania na aparaturę kontrolną oraz systemy i sieci teleinformatyczne, włączając w to akty szeroko rozumianej cyberprzestępczości i cyberterroryzmu a także przypadkowych (niecelowych) działań użytkowników.

Współcześnie skuteczny cyberatak na IK może bezpośrednio wpływać na bezpieczeństwo państwa i jego obywateli. Infrastruktura krytyczna jest narażona na cyberataki przeprowadzane zarówno przez początkujących[31] jak i wysoce wyspecjalizowanych cyberprzestępców, którzy mogą doprowadzić do zakłócenia jej funkcjonowania oraz na skutki zdarzeń losowych takich jak awarie systemów, niesprawności urządzeń lub programów ją obsługujących.

2.8.1. Bezpieczeństwo przetwarzania danych

2.8.1.1. *Rozwiązania on-premises*

Środowiska on-premises dotyczą przetwarzania danych, które odbywa się w środowiskach fizycznych lub wirtualnych, w serwerowniach własnych lub wynajętych, i nie wykorzystuje rozwiązań chmury publicznej. Model on-premises również podlega transformacji i odwołuje się także do takiego modelu przetwarzania, gdzie serwerownie czy same usługi serwerów fizycznych są wynajmowane od innych instytucji dla wybranych typów przetwarzania.

Często model on-premises w procesie przetwarzania wykorzystuje specyficzny sprzęt czy dedykowane rozwiązania (sprzęt połączony z wybranym oprogramowaniem i peryferiami), np. dostarczane tylko przez wąską grupę dostawców i o bardzo konkretnym przeznaczeniu, dla potrzeb bardzo specjalizowanych rozwiązań (np. sterowanie procesem przemysłowym lub wytwórczym).

W środowiskach on-premises aktualnie istnieje duży trend w kierunku automatyzacji i standaryzacji środowisk oraz wprowadzeniu pewnych procesów, obserwowanych dotychczas tylko w środowiskach chmury publicznej jak zarządzanie infrastrukturą poprzez kod czy rozliczanie kosztów środowisk. Wprowadzanie jednak tych procesów jest fragmentaryczne i bardzo płytkie ze względu na dużą heterogeniczność architektury, zakres wykorzystywanych rozwiązań fizycznych jak i technicznych jak

[31] Niestety często do przeprowadzenia ataku teleinformatycznego nie jest konieczna duża wiedza techniczna. Część ataków może zostać przeprowadzona z wykorzystaniem gotowych narzędzi programistycznych, a rola atakującego sprowadza się do wyboru metody ataku oraz celu. Atakujących w ten sposób nazywamy *script kiddies*.

również wysokie koszty wdrożeniowe związane choćby z dostępem do kompetencji na rynku.

Niezależnie od zmian rynkowych, zakłada się, że wszystkie opisane modele przetwarzania, również model on-premises, w długim horyzoncie czasu pozostaną na rynku, natomiast można obserwować zmiany w udziale każdego z tych modeli oraz dalej postępujący proces standaryzacji i automatyzacji środowisk on-premises.

2.8.1.2. *Rozwiązania wykorzystujące przetwarzanie w chmurze obliczeniowej*

Chmura obliczeniowa

W ciągu ostatnich dziesięciu lat coraz powszechniejsze zastosowanie ma model chmury obliczeniowej, zarówno dla rozwiązań IT, jak i w coraz większym stopniu dla rozwiązań automatyki przemysłowej i tzw. Internetu Rzeczy. Jej wykorzystanie zostało uwzględnione także dla rozwiązań wymagających szczególnych wymagań dotyczących bezpieczeństwa, jak usługi kluczowe lub przetwarzanie szczególnych kategorii danych osobowych.

Powszechnie wykorzystuje się definicję chmury obliczeniowej zaproponowaną w 2011 roku przez NIST[32], zarówno w dokumentach europejskich[33], jak i polskich[34].

chmura obliczeniowa – pula współdzielonych, dostępnych „na żądanie" przez sieci teleinformatyczne, konfigurowalnych zasobów obliczeniowych (np. sieci, serwerów, pamięci masowych, aplikacji, usług), które mogą być dynamicznie dostarczane lub zwalniane przy minimalnych nakładach pracy zarządczej i minimalnym udziale ich dostawcy.

Warto zwrócić uwagę na szczególne cechy chmury obliczeniowej:

- prekonfigurowane i standardowe zasoby obliczeniowe widoczne dla administratora jako oddzielny produkt,
- samodzielne, zdalne zarządzanie zasobami chmurowymi przez administratora, w tym uruchamianie lub zwalnianie zasobów, bez konieczności interakcji z dostawcą chmury,

32 NIST 800-145, https://www.nist.gov/publications/nist-definition-cloud-computing
33 Przykłady: European Commission Cloud Strategy z 16 maja 2019; European Banking Authority "EBA Guidelines on outsourcing arrangements" z 25 lutego 2019; Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (tzw. Dyrektywa NIS).
34 Przykłady: Uchwała nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa"; Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej z 23 stycznia 2020 r.

- standardowe umowy o świadczenie usług i modele kosztowe.

Powyższe cechy chmury obliczeniowej przybliżają ją do standardowego oprogramowania (tzw. „z półki"), które jest konfigurowalne, lecz nie jest modyfikowane przez użytkownika, a odróżniają od outsourcingu, w którym wszystkie elementy kontraktu i rozwiązania teleinformatycznego mogą być indywidualnie negocjowane i zmieniane, zaś modyfikacje są wprowadzane przez firmę świadczącą usługi outsourcingowe.

Cechami, które zachęcają do wykorzystania chmury obliczeniowej są przede wszystkim **skalowalność** zarówno poprzez uruchomienie bardzo dużych zasobów teleinformatycznych, jak i zwolnienie ich w przypadku braku potrzeby, a także **szybkość i łatwość wdrożenia**, model finansowy bazujący na kosztach, a nie na inwestycjach. W ostatnim czasie widać wyraźnie **cyberbezpieczeństwo** jako jedną z przyczyn migracji do chmury, gdyż dostawcy mają zazwyczaj znacząco większe środki i możliwości wdrożenia środków cyberochrony. Chmura zapewnia także możliwość łatwego uzyskania wysokiej odporności i możliwość utrzymania **ciągłości działania**. W dalszej części niniejszego rozdziału zamieszczone są zasady, którymi powinni kierować się wybierający rozwiązania bazujące na chmurze obliczeniowej.

Powyższy opis dotyczy publicznej chmury obliczeniowej, ale ma zastosowanie również w przypadku wprowadzenia modelu chmury prywatnej np. w grupie podmiotów lub chmury hybrydowej łączącej systemy w chmurze publicznej i chmurze prywatnej.

2.8.1.3. *Rozwiązania hybrydowe*

Wraz z wykorzystaniem przez instytucje IK zarówno środowisk on-premises (w różnej postaci) jak i środowisk chmury obliczeniowej, pojawiły się rozwiązania hybrydowe. Upraszczając, każde przetwarzanie danych, które w ramach jednego przedsiębiorstwa, odbywa się zarówno w środowiskach chmury obliczeniowej jak i w środowiskach on-premises można nazwać rozwiązaniem hybrydowym.

Na przykład systemy wewnętrzne, dziedzinowe dostarczane są w modelu on-premises, natomiast rozwiązania do współpracy z innymi podmiotami czy usługi powszechne, takie jak poczta elektroniczna, portale do wymiany danych i współpracy, dostarczane są w modelu usługowym („software as a service"). Rozwinął się również taki model przetwarzania, który w ramach jednego systemu informatycznego, posiada pewne zasoby w środowiskach chmury publicznej (np. system transakcyjny), natomiast dodatkowe funkcjonalności (np. analiza danych, hurtownia danych, raportowanie, monitoring bezpieczeństwa) odbywa się w modelu chmury publicznej. Rozwiązań tego typu jest więcej i w ostatnim czasie zaobserwować można wzrost tego typu projektów w obszarach: analizy danych również z użyciem sztucznej inteligencji, zbieraniu zdarzeń dotyczących IoT/OT, bezpieczeństwa czy ochrony danych poprzez dodatkowe

kopie zapasowe w środowiskach chmury. Wszędzie tam, gdzie rozbudowa systemu informatycznego może zostać zrealizowana przez wykorzystanie komponentu, usługi lub systemu dostępnego w środowiskach chmury publicznej, mowa o rozwiązaniach hybrydowych.

Rozwiązania hybrydowe wpływają również na współdzielenie i modyfikację najczęściej takich elementów środowiska teleinformatycznego jak:

1) Tożsamość użytkownika
2) Sieć
3) Systemy monitoringu
4) Systemy bezpieczeństwa
5) Systemy kopii zapasowych
6) Systemy współpracy i wymiany danych

Tych elementów może być oczywiście więcej, wymienione występują bardzo często w realizowanych projektach.

Dodatkowo, zagadnienie przetwarzania hybrydowego będzie zyskiwało na popularności nie tylko ze względu na wykorzystanie rozwiązań chmury publicznej, ale również ze względu na wykorzystanie rozwiązań innych dostawców (hosting, wynajem przestrzeni serwerowej, wynajem usług). Rozwiązania hybrydowe będą standardem przetwarzania danych i wpłyną na model bezpieczeństwa teleinformatycznego IK.

Wykorzystanie chmury obliczeniowej wymaga od operatora IK oceny ryzyka także w innym zakresie niż znanych z rozwiązań on-premises, w szczególności w przypadku korzystania z chmury publicznej. Ryzyko jest związane przede wszystkim z wykorzystaniem poddostawcy, na którego organizację i jej zmiany, infrastrukturę techniczną i personel operator IK ma ograniczony wpływ. Należy szczególnie podkreślić konieczność jednoczesnej i wspólnej oceny warunków prawno-kontraktowych, organizacyjnych i technicznych. Podstawowa lista zagadnień podlegających ocenie ryzyka została przedstawiona w rozdziale 2.8.3.2

2.8.2. *Zasady bezpieczeństwa teleinformatycznego IK*

2.8.2.1. *Poufność, dostępność i integralność informacji*

Istnieje wiele modeli identyfikacji cech, jakie powinien spełniać prawidłowo chroniony system teleinformatyczny. Jednym z bardziej znanych i najczęściej używanych jest system wskazujący na trzy najważniejsze cechy bezpieczeństwa informacji[35]:

[35] W terminologii anglojęzycznej system określany jest jako CIA (*Confidentiality, Integrity, Availability*).

- poufność,
- integralność,
- dostępność.

Oznaczają one, że aby uznać system za odpowiednio zabezpieczony, trzeba zapewnić, aby informacja w nim przetwarzana była traktowana poufnie, zgodnie z przyznanymi prawami dostępu, powinna ona zachować swoją integralność, tak, aby można było uznać ją za wiarygodną i nie powinny występować problemy z dostępem do tej informacji dla osób mających odpowiednie uprawnienia[36].

Powyższe cechy dotyczą oprogramowania, sprzętu i procesów komunikacji między jednym i drugim.

Szczególnymi zagrożeniami dla tak rozumianego modelu bezpieczeństwa są:

- nieuprawniony dostęp do informacji i procesów jako naruszenie ich **poufności**,
- zmiana lub inne zakłócenie informacji i wykonywanych procesów jako naruszenie ich **integralności**,
- blokada dostępu do informacji i procesów jako naruszenie ich **dostępności**.

Szybki rozwój technologii teleinformatycznych, nacisk na obniżanie kosztów oraz dostępność bogatej oferty standardowych produktów i usług chmury obliczeniowej skutkują ich zastosowaniem w systemach IK. Oznacza to, że podatności takich produktów stają się również istotne dla operatorów IK. Wymagane jest zatem podjęcie odpowiednich kroków organizacyjnych mających na celu odpowiedni dobór takich produktów i usług, jak również późniejsze zarządzanie usuwaniem podatności, w tym aktualizacje.

2.8.2.2. *Rozwiązania organizacyjne, technologiczne, kontraktowe i zasoby ludzkie*

Bezpieczeństwo systemów teleinformatycznych wymaga zapewnienia bezpieczeństwa na poziomie rozwiązań organizacyjnych, w sferze technicznej (logicznej) a także w obszarze zasobów ludzkich.

Do rozwiązań organizacyjnych tradycyjnie należy zaliczyć zabezpieczenia takie jak nadzór nad technologiami teleinformatycznymi w organizacji z hierarchią celów, raportowanie o wynikach realizowanych procesów, realizacja procedur, a także zbudowany w ramach organizacji katalog czynności z obszaru informatyki i cyberbezpieczeństwa. Rozwiązania organizacyjne mają postać polityk, procedur,

[36] Powyższe zasady zostały uwzględnione w Rozporządzeniu 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.

ocen, programów szkoleniowych skierowanych do pracowników oraz audytów bądź raportów zgodności.

Najważniejszym narzędziem w katalogu rozwiązań organizacyjnych jest Polityka bezpieczeństwa informacji. Polityka bezpieczeństwa informacji pozwala na efektywne i całościowe zarządzanie bezpieczeństwem danych, które zgromadzone są w organizacji, a w szczególności w jej systemach informacyjnych. Polityka bezpieczeństwa informacji powinna zawierać spisane cele, strategie oraz działania, które w jasny i ustrukturyzowany sposób określają, jak należy zarządzać zgromadzonymi danymi, jak je chronić i rozpowszechniać. Dokument powinien ułatwiać dokładne zrozumienie celu istnienia procedur bezpieczeństwa i ma za zadanie podnosić świadomość pracowników organizacji na temat zagrożeń bezpieczeństwa i związanego z nimi ryzyka.

Elementem bezpieczeństwa informacji jest zarządzanie aktywami. Celem realizowanych czynności powinno być zidentyfikowanie aktywów, określenie odpowiedzialności w zakresie ich ochrony, stosownie do ich krytyczności aktywów, a także przeciwdziałanie nieuprawnionemu ujawnieniu, modyfikacji, Istotnym czynnikiem w zarządzaniu ryzykiem jest częstotliwość jego szacowania oraz monitorowania.

Ostatnim komponentem zabezpieczeń organizacyjnych jest zarządzanie ryzykiem. Realizacja tej funkcji może być podyktowana misją organizacji, jej funkcjami biznesowymi czy też zdolnością do wykorzystania wyników monitorowania ryzyka w celu nabycia większej świadomości sytuacyjnej. Zwiększony poziom tej świadomości, w zakresie stanu bezpieczeństwa systemów informacyjnych organizacji oraz środowisk w jakich działają, pomaga organizacjom w lepszy sposób postrzegać i rozumieć ryzyko usunięcia czy zniszczenia aktywów informacyjnych.

Rozwiązania techniczne obejmują swoim zakresem każde przypadki zastosowania urządzenia, oprogramowania i konkretnej technologii w sferze specyfiki systemów informacyjnych podmiotów Infrastruktury Krytycznej, mogących realizować funkcje operacyjne, biznesowe, bezpieczeństwa (*safety*), ochrony fizycznej, reagowania kryzysowego. Kluczowym elementem w obszarze technologicznym jest bezpieczeństwo oprogramowania, definiowanie jako zapobieganie występowaniu błędów, które mogą pozwalać na przejęcie kontroli nad aplikacją, urządzeniem bądź systemem. Innym przykładem jest odporność systemu transmisyjnego na zakłócenia, czyli zabezpieczenie transmisji danych przed przechwyceniem lub zniekształceniem informacji. Innym rodzajem zabezpieczenia jest wprowadzanie monitorowania, który pracownik ma dostęp do poszczególnych kategorii informacji. Dzięki takiemu rozwiązaniu, w przypadku wycieku danych, organizacja może określić kto jest odpowiedzialny za dany wyciek oraz oszacować skalę zjawiska.

Przykładami zabezpieczeń technicznych są następujące rozwiązania:

1) IPS – Intrusion Prevention System

System IPS (ang. Intrusion Prevention Systems – IPS), czyli system zapobiegający włamaniom to rodzaj urządzenia sieciowego wykrywającego i blokującego ataki na systemy informacyjne. Działanie urządzenia polega na monitorowaniu kluczowych elementów systemu w poszukiwaniu niepożądanych zachowań i zdarzeń, takich jak robaki internetowe, trojany, oprogramowanie typu *spyware* lub *malware* oraz ich powstrzymywaniu. IPS może spowodować odłączenie sieci komputerowej lub przerwanie sesji użytkownika poprzez zablokowanie określonemu numerowi IP dostępu do zasobu lub usługi, niektóre rozwiązania pozwalają również narekonfigurację „zapory sieciowej" (ang. firewall) lub routera.

2) NGFW – Next Generation Firewall

"Zapora sieciowa" (ang. firewall) to rozwiązanie sprzętowe, obejmujące routery, serwery i oprogramowanie, ograniczające przepływ pakietów danych pomiędzy segmentami sieci komputerowej zgodnie z określoną polityką bezpieczeństwa. W przypadku Next Genaration Firewall tradycyjna technologia „zapory sieciowej" jest poszerzona o inne urządzenia sieciowe z funkcją filtrowania pakietów danych, w tym dokonujących pakietowej inspekcji danych (ang. DPI – deep packet inspection) oraz o systemy zapobiegające włamaniom IPS. Celem implementacji narządzi klasy NGFW jest realizacja inspekcji pakietów danych na większej liczbie warstw modelu OSI[37].

3) WAF - Web Application Firewall

Technologia aplikacyjnej „zapory sieciowej" to technologia umożliwiająca przepływy informacji między systemami komputerowymi, ale bez bezpośredniej możliwości wymiany pakietów danych. Technologia ta pozwala ograniczyć ryzyko związane z wymianą pakietów danych pomiędzy systemami wewnętrznymi i zewnętrznymii aplikacji hostowanych w sieci korporacyjnej. Aplikacyjna „zapora sieciowa" to urządzenie lub oprogramowanie umiejscowione na "utwardzonym" systemie operacyjnym np. Windows lub UNIX, funkcjonującą w aplikacyjnej warstwie modelu OSI. WAF analizuje przepływy informacji w oparciu o serwery proxy (serwery pośredniczące), obsługujące żądania klientów poprzez przesyłanie żądań do innych serwerów z własnym adresem sieciowym dla każdej usługi (np. FTP, Telnet czy http).

4) DLP – Data Leak Prevention

Oprogramowanie tego typu służy do ochrony danych przed wyciekiem, dotyczy to zarówno wycieków przypadkowych, wynikających na przykład z nieostrożności pracowników oraz działań celowych. Większość rozwiązań klasy DLP ułatwia lokalizację i katalogowanie informacji wrażliwych, monitoring i kontrolę przepływu informacji poprzez sieci korporacyjne oraz urządzenia końcowe. W tym celu

[37] Model referencyjny opisujący strukturę komunikacji w sieci komputerowej.

wykorzystywane są tzw. „crawlery”[38] przeszukujące zbiory danych, urządzenia sieciowe monitorujące ruch sieciowy, w tym dokonujące pakietowej inspekcji danych (ang. DPI – deep packet inspection), a także urządzenia monitorujące działania użytkowników końcowych na stacjach roboczych. Szczególnie istotne w przypadku rozwiązań klasy DLP jest przeprowadzenie szacowania bezpieczeństwa informacji, określenie wartości przetwarzanych informacji, a także ustanowienie polityk, reguł wykonywania operacji przez oprogramowanie i komponenty sprzętowe systemu klasy DLP.

5) **SIEM – Security Information and Event Management**

System SIEM to oprogramowanie przeznaczone do agregowania i analizowania znacznej liczby danych i informacji, zarówno z urządzeń końcowych, jak i z narzędzi do monitorowania sieci, takich jak „zapory sieciowe” czy systemy IPS. Systemy SIEM w sposób automatyczny agregują i korelują dane i logi związane ze zdarzeniami cyberbezpieczeństwa, w powiązaniu z analizą danych historycznych. Korelacja zdarzeń oznacza, że system SIEM umożliwia stworzenie jednego zdarzenia mającego charakter incydentu cyberbezpieczeństwa. Korelacja oparta na regułach pozwala określić wzorzec zdarzeń cyberbezpieczeństwa, natomiast korelacja oparta na statystykach pozwala zdefiniować poziom zagrożeń dla aktywów informacyjnych. Informacje z systemów mogą być wykorzystywane przez wewnętrzne zespoły typu CSIRT czy operacyjne centra bezpieczeństwa (ang. SOC – Security Operations Center).

6) **SOAR – Security Orchestration, Automation and Response**

SOAR to nowa, zyskująca coraz bardziej na znaczeniu technologia w bezpieczeństwie IT, szczególnie interesująca dla organizacji dysponujących własnym SOC (Security Operations Centre) lub aktywnie użytkujących system klasy SIEM. SOAR jest nową klasą systemów IT Sec, których zadaniem jest skuteczniejsze zarządzanie zdarzeniami cyberbezpieczeństwa występującymi w systemach IT/OT organizacji. Ich funkcjonalność sprowadza się zasadniczo do trzech obszarów: automatyzacja procesów reagowania na incydenty w oparciu o playbooki, automatyczne wzbogacanie zdarzeń cyberbezpieczeństwa o dodatkowe informacje w oparciu o różnorodne integracje oraz strukturyzacja procesów w oparciu o role i tickety.[39]

7) **EDR – Endpoint Detection and Response**

EDR to rodzaj narzędzia informatycznego monitorującego wykorzystywane w organizacji i jej sieci korporacyjnej urządzenia końcowe (np. telefon komórkowy, laptop, stacja robocza, urządzenie Internetu Rzeczy) celem zapobiegania zagrożeniom cyberbezpieczeństwa. Technologia EDR służy do identyfikowania podejrzanych zachowań i zaawansowanych trwałych zagrożeń cyberbezpieczeństwa na punktach

[38] Program zbierający informacje o strukturze danych, stronach i treściach.

[39] https://mediarecovery.pl/soar-czyli-wyzszy-poziom-soc/

końcowych w środowisku informatycznym oraz do odpowiedniego ostrzegania administratorów. Jest to realizowane poprzez zbieranie i agregowanie danych z punktów końcowych i innych źródeł. Te dane mogą, ale nie muszą, zostać wzbogacone o dodatkową analizę w chmurze. Rozwiązania EDR to przede wszystkim narzędzie ostrzegania, a nie warstwa ochrony, ale funkcje mogą być łączone w zależności od dostawcy. Dane mogą być przechowywane w scentralizowanej bazie danych lub przekazywane do narzędzia SIEM.

8) XDR – Extended Detection and Response

Rozszerzone możliwości wykrywania zagrożeń cyberbezpieczeństwa i reagowania na nie, określane skrótem XDR, to narzędzie w modelu Software-as-A-Service, które oferuje kompleksowe, zoptymalizowane zabezpieczenia, integrując produkty zabezpieczające oraz dane w uproszczone rozwiązania. W przeciwieństwie do systemów takich jak wykrywanie i reagowanie w punktach końcowych (EDR), system XDR rozszerza zakres zabezpieczeń, integrując ochronę z szerszą gamą produktów, w tym z punktami końcowymi organizacji, serwerami, aplikacjami w chmurze, pocztą e-mail. Dzięki temu system XDR łączy zapobieganie, wykrywanie, badanie i reagowanie, zapewniając widoczność, analizę, skorelowane alerty o incydentach i automatyczne reakcje w celu poprawy bezpieczeństwa danych i zwalczania zagrożeń cyberbezpieczeństwa[40].

Ponadto w obszarze technologicznym w sektorach przemysłowych należy uwzględnić takie czynniki jak odporność na warunki pracy i wpływ środowiska, a także niezawodność funkcjonowania w cyklu życia urządzenia, czyli czas do pierwszej awarii. Organizacja powinna dążyć do unifikacji i standaryzacji architektury rozwiązań, również poprzez modernizację lub wdrażanie nowych systemów w miejsce starszych, już wykorzystywanych. Pożądanym rozwiązaniem jest stopniowe wycofanie systemów informacyjnych, które z racji swojego wieku i długiej eksploatacji nie są objęte procesem aktualizacji, dostarczania poprawek bezpieczeństwa oraz tych, które są niekompatybilne z innymi systemami odpowiadającymi za bezpieczeństwo, mając na uwadze możliwe korzyści i straty wynikające z planowanej modernizacji. Powinno się także stosować uzupełniające środki bezpieczeństwa w starszych systemach, m.in. poprzez zapewnienie dodatkowych środków bezpieczeństwa fizycznego, takich jak środki ochrony przeciwpożarowej, systemy sygnalizacji włamania i napadu, kontroli dostępu, ochrony obwodowej, czy poprzez przeniesienie rozliczalności dostępu.

[40] https://www.microsoft.com/pl-pl/security/business/security-101/what-is-xdr

Rozwiązania kontraktowe związane są z wykorzystaniem zewnętrznych dostawców usług, w tym dostawców chmury publicznej, usług telekomunikacyjnych, w tym usług rozszerzonych (tzw. OTT) lub usług informatycznych, zarówno wdrożeniowych, jak i wsparcia technicznego. Organizacja, w celu uzyskania adekwatnego poziomu poufności, integralności i dostępności powinna sprawdzić warunki świadczenia usług (dla usług wystandaryzowanych) lub zapewnić odpowiednie zapisy w umowach (dla usług specyficznych dla odbiorcy). Pomocnym w ocenie może być zapewnienie potwierdzonej certyfikatami zgodności z normami.

Przykładowymi umowami mogą być warunki zapisane w tzw. umowach SLA (ang. Service Level Agreement) określające m.in. dostępność usługi, czas reakcji serwisowej lub zakres odpowiedzialności dostawcy/usługodawcy. Innym rodzajem są umowy określające warunki techniczne i organizacyjnej świadczenia usługi np. rolę dostawcy w procesie przetwarzania danych osobowych, zasady wykorzystania poddostawców, obecność planu ciągłości biznesowej czy zasady zarządzania personelem dostawcy. Istotne będą zasady postępowania z danymi organizacji przez dostawcę m.in. własność danych, standardowe zasady szyfrowania, procesu retencji i usuwania danych czy opis procesu zakończenia świadczenia usługi. Wśród norm towarzyszących stronie kontraktowej należy wymienić przede wszystkim ISO 27001, ISO 22301 lub ISO 9000.

W przypadku kiedy w ocenie organizacji standardowo dostarczane warunki świadczenia usług przez dostawców są niewystarczające, należy w pierwszej kolejności sprawdzić czy nie są dostępne rozszerzone usługi danego dostawcy, związane ze zmianami organizacyjnymi lub z zastosowaniem dodatkowych rozwiązań technicznych. Przykładem mogą być rozwiązania zwiększające dostępność (np. redundancja krytycznych elementów infrastruktury, dostępność specjalistów od wsparcia technicznego i możliwość podniesienia poziomu reakcji), bezpieczeństwo (np. inne metody szyfrowania, rozszerzony monitoring, dodatkowe narzędzia zarządzania danymi, narzędzia do zarządzania incydentami bezpieczeństwa, ale także wymaganie poświadczenia bezpieczeństwa dla inżynierów wsparcia), ciągłość działania itd.

Organizacja powinna również zatrudniać **specjalistów posiadających kwalifikacje** z różnych obszarów teleinformatyki i cyberbezpieczeństwa, przykładowo z obszaru planowania rozwoju rozwiązań teleinformatycznych, ich wdrażania, obsługi bądź monitorowania. Jednakże, szybkość zmieniających się technologii i pojawiających się nowych cyberzagrożeń powoduje, że osoby zajmujące się kwestią informatyki i cyberbezpieczeństwa powinny regularnie podnosić swoje kompetencje, a organizacja winna zapewnić swoim pracownikom zagwarantować odpowiednią ścieżkę rozwoju np. w postaci programu szkoleń. Program szkoleń był odpowiednio dostosowany

do potrzeb danego podmiotu, a także do poziomu dojrzałości organizacji i ilości wykorzystywanych systemów teleinformatycznych.

Z racji tego organizacja powinna dopasować program szkolenia do konkretnych stanowisk, nie tylko związanych stricte z cyberbezpieczeństwem, ponieważ oprócz automatyków czy administratorów systemów informacyjnych, ważne jest np. odpowiednie opracowanie opisu zamówień publicznych pod kątem zachowania standardów bezpieczeństwa i kompatybilności nowych urządzeń czy oprogramowania z już posiadanymi zasobami.

2.8.2.3. *Szkolenia i testy*

Testowanie systemów i komponentów odpowiedzialnych za realizację usług i procesów w ramach organizacji pozwala upewnić się, że spełniają one założenia ustanowione przez organizację oraz pozostałe określone wymogi związane z ich cyberbezpieczeństwem.

Jednym z nadrzędnych celów testowania systemów informacyjnych oraz komponentów jest wykrycie związanych z nimi podatności, aby móc podjąć działania zaradcze. Identyfikacja podatności może nastąpić w trakcie czynności takich, jak:

a) przeprowadzanie audytów i testów bezpieczeństwa, na które składają się: testy podatności, testy penetracyjne, audyty zgodności z wymaganiami norm bezpieczeństwa, audyty weryfikujące spełnienie wymagań bezpieczeństwa, ćwiczenia realizacji planów zapewnienia ciągłości działania oraz ćwiczenia typu *red teaming*, czyli kontrolowany atak na własną organizację,
b) przegląd systemu zarządzania bezpieczeństwem informacji i przegląd planów zapewnienia ciągłości działania,
c) przeprowadzanie modelowania zagrożeń i analizy ryzyka,
d) zarządzanie zdarzeniami bezpieczeństwa oraz proaktywne monitorowanie bezpieczeństwa systemów,
e) zarządzanie incydentami bezpieczeństwa (podatność jako przyczyna zgłoszonego incydentu bezpieczeństwa),
f) konsekwencja aktywnego poszukiwania informacji o podatnościach typu *zero-day* pasujących do bazy aktywów organizacji.[41]

Skanowanie podatności jest przeprowadzane w sposób zautomatyzowany i nie posiadają cechy bycia ukierunkowanymi na dedykowane, mniej znane autorskie systemy lub aplikacje. Skaner podatności pozwala uzyskać informacje o słabościach odnoszących się

[41] C. Banasiński, M. Rojszczak (red.), *Cyberbezpieczeństwo*, 2020, s. 152

do popularnych rozwiązań, ponieważ wykorzystuje on bazę znanych już podatności.[42].

Należy przy tym wyróżnić dwa rodzaje skanowania:

a) uwierzytelnione – realizowane z uwzględnieniem informacji dotyczących uwierzytelniania, dostępu itp.,
b) nieuwierzytelnione – wykonywane w taki sposób, jakby badana infrastruktura była nasłuchiwana z „zewnątrz"[43].

Testy penetracyjne również stanowią istotny element weryfikacji bezpieczeństwa systemów i komponentów, będąc kontrolowaną próbą przełamania ich zabezpieczeń. Działania realizowane w związku z nimi, symulują ataki hakerów czy crackerów, a ich celem jest ujawnienie podatności w danym systemie, która umożliwiłaby pokonanie zabezpieczeń, włamanie się lub przejęcie kontroli nad systemem. Badanie jego odporności na ataki, jest procesem złożonym z pięciu etapów:

I. Zdobycie informacji na temat badanego obiektu lub obszaru,
II. Skanowanie – przegląd urządzeniem elektronicznym badanego obiektu lub obszaru punkt po punkcie,
III. Enumeracja – zdobywanie informacji na temat systemów, na których bazuje usługa. Polega na nawiązaniu aktywnego połączenia oraz wysłaniu zapytania na temat zasobów systemu udostępniającego daną informację, z pominięciem weryfikacji uprawnienia audytora do otrzymania takich danych,
IV. Eksploracja, pozyskiwanie, ekstrakcja, drążenie i wydobywanie wiedzy z baz danych. Polega ono na sprawdzeniu możliwości ich pozyskania bez odpowiednich uprawnień,
V. Raportowanie mocnych i słabych stron testowanego systemu wraz z oceną krytyczności tych słabych.[44]

Można wyróżnić trzy typy wykonywanych testów penetracyjnych:

a) Black-Box – stanowi próbę przełamania zabezpieczeń bez jakiejkolwiek wiedzy na temat badanego systemu. Audytor posiada informacje jedynie na temat celu ataku, starając się przełamać zabezpieczenia, wiernie odwzorowując działania hakera,
b) Gray-Box – to próby przełamania zabezpieczeń z fragmentaryczną wiedzą w zakresie atakowanego systemu. Atakujący używa technik wykorzystywanych prze hakerów, lecz posiada także dodatkową wiedzę, aby dokładniej penetrować zabezpieczenia,

[42] *Ibidem*, s. 154.
[43] *Ibidem*. s. 155
[44] *Ibidem*, s. 156.

c) White-Box – atakujący ma kompletną wiedzę dotyczącą atakowanego systemu i stara się na tej podstawie przełamać zastosowane zabezpieczenia, w celu zdobycia jak najszerszych informacji o badanym systemie[45].

Testy tego typu pozwalają uzyskać wiele cennych informacji dotyczących bezpieczeństwa systemów poddawanych analizie, jak m.in.:

- potencjalny zbiór możliwych wektorów ataku,
- zidentyfikowane podatności wysokiego ryzyka, powstające w wyniku połączenia i wykorzystania w określonej kolejności luk niskiego ryzyka,
- zidentyfikowane luki, mogące być trudne lub niemożliwe do wykrycia za pomocą automatycznych narzędzi do skanowania pod kątem podatności sieci lub aplikacji,
- ocena skali potencjalnych strat biznesowych i operacyjnych w wyniku wystąpienia skutecznego ataku,
- zbadane zdolności sieciowych systemów ochrony do skutecznego wykrywania i reagowania na ataki,
- argumenty związane z koniecznością inwestowania w personel i technologie rozwiązań w zakresie cyberbezpieczeństwa.

W przypadku korzystania z rozwiązań chmurowych należy sprawdzić czy dostawca regularnie prowadzi i publikuje wyniki testów bezpieczeństwa ofertowanych rozwiązań lub platformy.

W przypadku ryzyka wewnętrznego bezpieczeństwa systemów informacyjnych występującego w organizacji, gdzie nie można zastosować zabezpieczeń technicznych ani wykorzystać narzędzi testowania, zasadne jest przygotowanie programu szkoleń i działań uświadamiających pracowników i specjalistów.

Podmiot powinien zagwarantować podobny poziom wiedzy bazowej wszystkich pracowników swojej organizacji w zakresie tematyki cyberbezpieczeństwa, a także prowadzić cykliczne szkolenia dla wszystkich zatrudnionych osób, aby regularnie budować świadomość cyberbezpieczeństwa w ramach swojej organizacji. Organizacja powinna również zidentyfikować różne grupy docelowe szkoleń – od podstawowych użytkowników systemów po osoby bezpośrednio zajmujące się bezpieczeństwem sieci i systemów IT i OT. Zakres szkoleniowy powinien być odpowiednio dopasowany w zależności od kompetencji potrzebnych do realizacji zadań na danym stanowisku.

[45] *Ibidem*, s. 157.

Pracownicy, w których zakresie obowiązków wymagana jest zaawansowana wiedza z zakresu cyberbezpieczeństwa, powinni mieć zapewniony dostęp do cyklicznych szkoleń i odpowiednich ścieżek rozwoju. W tym celu uzasadnione jest opracowanie odpowiedniego programu szkoleń dla specjalistów zajmujących się cyberbezpieczeństwem, aby poziom ich wiedzy był na wysokim poziomie, co będzie gwarancją lepszego przygotowania na wystąpienie potencjalnego cyberataku i odpowiedniej reakcji.

W celu utrzymania odpowiedniego poziomu wiedzy dotyczącej cyberbezpieczeństwa w organizacji, zaleca się przeprowadzanie cyklicznych szkoleń przypominających najważniejsze kwestie związane z cyberbezpieczeństwem. Z racji tego, że każdy najlepiej uczy się na swoich błędach, rekomenduje się również przeprowadzanie co jakiś czas praktycznych szkoleń, poprzez np. organizację wewnętrznych niezapowiedzianych ćwiczeń z wyłapywania kampanii phishingowych.

Organizacje winny brać aktywny udział w organizowanych krajowych ćwiczeniach cyberbezpieczeństwa, jak również, w ramach możliwości, w tych organizowanych na poziomie międzynarodowym.

Ćwiczenie i doskonalenie procedur przyczynia się do sprawniejszej reakcji na pojawiające się zagrożenie. Ponadto, umożliwia wymianę doświadczeń i dobrych praktyk z innymi podmiotami, a także przetestowanie swoich własnych zdolności. W takich ćwiczeniach zazwyczaj bierze udział wiele podmiotów z różnych sektorów – energii, finansów, transportu, dostawców usług cyfrowych itd. Co więcej, podczas ćwiczeń istnieje możliwość przetestowania ścieżki kontaktu z CSIRT poziomu krajowego czy CSIRT sektorowym.

2.8.3. Proces bezpieczeństwa teleinformatycznego

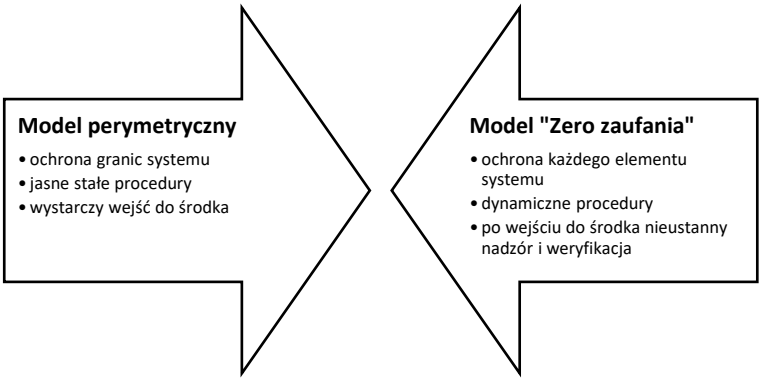
2.8.3.1. Strategia Zero Trust

Środowisko IT, zarówno w małych jak i w średnich organizacjach, jest coraz bardziej złożone. W jednej organizacji może funkcjonować wiele wewnętrznych sieci, usługi są często świadczone zdalnie z innej lokalizacji, upowszechnił się model pracy zdalnej. W sytuacji, w której trudno jest jednoznacznie określić zewnętrzne granice naszego środowiska IT, tradycyjny (tzw. perymetryczny) model zapewnienia cyberbezpieczeństwa przestał być wystarczający, po przełamaniu pierwszej bariery intruz może bowiem bez większych przeszkód poruszać się wewnątrz środowiska IT (ang. *lateral movment*).

Ochrona środowiska IT, szczególnie w przypadku operatorów IK, nie może więc obecnie sprowadzać się do ochrony brzegu sieci lub urządzenia końcowego przed niepożądanym działaniem z zewnątrz. Wzmocnienie technologiczne, dodawanie kolejnych rozwiązań

technicznych nie jest wystarczające. Towarzyszyć temu musi zmiana organizacji bezpieczeństwa.

Odpowiedzią na złożoność współczesnych środowisk IT jest nowy model cyberbezpieczeństwa znany jako „Zero Trust”[46]. Jest to agnostyczny technologicznie amerykański standard NIST (National Institute of Standards and Technology). **Jako jeden z Narodowych Standardów Cyberbezpieczeństwa opublikowanych przez Pełnomocnika Rządu ds. cyberbezpieczeństwa[47] model „Zero zaufania” jest rekomendowany dla operatorów IK we wszystkich systemach.**



Rysunek 12 Elementy modelu Zero Trust.

Model „Zero zaufania” jest skoncentrowany na ochronie danych i usług, ale powinien obejmować wszystkie zasoby organizacji (urządzenia, elementy infrastruktury, aplikacje, zasoby chmurowe i wirtualne) oraz podmioty (użytkowników końcowych, aplikacje oraz inne elementy zasilane danymi z zasobów).

„Zero zaufania” oznacza, że należy z góry założyć, że atakujący jest już obecny w środowisku organizacji, a sam fakt, że operator IK jest właścicielem środowiska nie oznacza wyższego poziomu ochrony niż w innych środowiskach. W tej sytuacji **rekomendowane jest przede wszystkim prowadzenie nieustannej oceny ryzyka dla swoich aktywów, ograniczanie do minimum dostępu do zasobów oraz ciągłe kontrolowanie tożsamości i stanu bezpieczeństwa użytkowników**, którym udostępnia się zasoby. Tożsamość w ostatnim czasie staje się kluczowym zasobem, który powinien podlegać szczególnej ochronie.

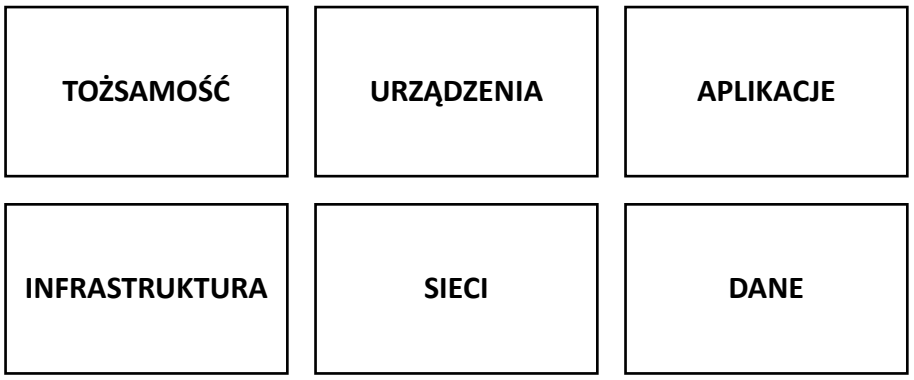
[46] NIST Special Publication 800-207 „Zero Trust Architecture”. 2020. Pełna wersja dostępna tu: https://doi.org/10.6028/NIST.SP.800-207

[47] https://gov.pl/attachment/8659d8de-6a83-4860-bcd1-d0648fbe9ead

Wszystkie działania powinny opierać się o następujące ogólne założenia:

1. **Wszystkie źródła danych i usługi obliczeniowe należy uznać za zasoby**, włącznie z urządzeniami prywatnymi (telefony, tablety, zegarki) – jeśli mają dostęp do zasobów.
2. Niezależnie od lokalizacji w sieci, **każda komunikacja musi być zabezpieczona**.
3. **Dostęp do zasobów powinien być przydzielany na zasadzie oddzielnej sesji**. Nie należy automatycznie udostępniać kolejnych zasobów.
4. **Dostęp do zasobów powinny określać dynamiczne zasady**, definiowane również na podstawie atrybutów innych niż tożsamość (np. dostęp do zasobów przez telefon komórkowy jest możliwy tylko wtedy, kiedy jest aktualny system operacyjny, dopuszczony do użytku, użytkownik potwierdzi tożsamość i sesja ma miejsce w godzinach pracy).
5. Należy prowadzić **ciągłą diagnostykę i monitoring wszystkich posiadanych i powiązanych zasobów**.
6. **Uwierzytelnianie i autoryzacja zasobów powinny przebiegać dynamicznie**, zależnie od bieżącego poziomu zaufania/zagrożenia – z wykorzystaniem systemów zarządzania tożsamością, wiarygodnością i dostępem (ICAM = Identity, Credential and Access Management) oraz systemów zarządzania zasobami.
7. Zalecane jest **gromadzenie jak największej ilości informacji o aktualnym stanie środowiska IT** i bieżące ich wykorzystywanie do oceny i poprawy stanu bezpieczeństwa.

Uogólniając, należy zapewnić ciągłą ochronę poniżej wskazanym elementom środowiska IT, uwzględniając fakt, że proces zapewnienia ich bezpieczeństwa powinien obejmować kwestie organizacyjne, techniczne i czynnik ludzki:



Rysunek 13 Podstawowe elementy środowiska IT.

Należy zwrócić uwagę, że podane wyżej zasady powinny odnosić się zarówno do zasobów własnych operatora, jak również do zasobów udostępnianych operatorowi w postaci usług np. hosting, kolokacja, chmura obliczeniowa. W dalszej części niniejszego rozdziału zostaną przedstawione zasady pozwalające operatorom IK zapewnić bezpieczeństwo w całym środowisku IT, we wskazanych powyżej obszarach.

Należy jednak podkreślić, że wdrożenie modelu „Zero zaufania" w organizacjach, w których wdrożone są rozwiązania polegające na ochronie granic systemu, powinno odbywać się stopniowo, z okresem przejściowym, w którym równolegle będą funkcjonować rozwiązania tradycyjne (perymetryczne), a środowisko i zasady pracy będą stopniowo modernizowane zgodnie z opisanymi powyżej zasadami. Wymaga to od organizacji określonego poziomu dojrzałości organizacyjnej, polegającej głównie na zidentyfikowaniu i skatalogowaniu aktywów, podmiotów, procesów biznesowych, przepływów sieciowych i map zależności.

REKOMENDACJA: Operatorzy IK powinni dążyć do szybkiego, choć stopniowego wdrażania zasad „zerowego zaufania" poprzez sukcesywne zmiany w procesach oraz rozwiązania technologiczne zapewniające ochronę najcenniejszych zasobów.

2.8.3.2. *Modele przetwarzania danych*

Wykorzystanie chmury obliczeniowej przez operatorów IK

Nowe rodzaje zagrożeń dla środowiska teleinformatycznego, w szczególności ataki sponsorowane przez państwa, a także doświadczenia wynikające z wojny w Ukrainie oraz zmiany legislacyjne w kilku krajach europejskich (Estonia, Litwa, Ukraina) pozwalają stwierdzić, że zastosowanie chmury obliczeniowej przez operatorów IK pozwoli na podniesienie bezpieczeństwa teleinformatycznego.

Operatorzy IK powinni przy tym kierować się poniższymi zaleceniami.

1. Wykorzystanie chmury jest dopuszczalne w środowisku teleinformatycznym operatorów IK. Dotyczy to zarówno rozwiązań bezpośrednio związanych z IK, jak i dla innych rozwiązań nie mających bezpośredniego powiązania z IK.
2. Ocenę możliwości wykorzystania chmury obliczeniowej należy przeprowadzić dla każdego nowego rozwiązania teleinformatycznego u operatora IK lub przy wymianie dotychczasowego rozwiązania na nowsze lub przy wdrożeniu jego nowszej wersji. **Zaleca się** także przeprowadzenie takiej oceny dla eksploatowanych rozwiązań pod kątem zwiększenia bezpieczeństwa teleinformatycznego.
3. Jeśli poziom zapewnienia bezpieczeństwa teleinformatycznego w chmurze publicznej jest wyższy niż dla innych rozwiązań, wówczas operator IK powinien

zastosować rozwiązanie chmurowe, w przeciwnym przypadku powinno zostać przygotowane uzasadnienie innego rozwiązania.

4. Ostateczną decyzję dotyczącą przetwarzania w chmurze podejmuje się po przeprowadzeniu oceny ryzyka, uwzględniającej klasyfikację i ocenę informacji przetwarzanych w chmurze, zapewnienie odpowiedniego poziomu ochrony danych w oparciu o ogólne i sektorowe przepisy ochrony danych oraz spełnienie wymagań właściwego regulatora, jeżeli ma to zastosowanie w przypadku operatora IK.
5. **Nie zaleca się** operatorom IK stosować chmury publicznej, jeśli:
   a. Dostawca chmury publicznej jest przedsiębiorstwem spoza UE lub NATO, lub jest własnością, bądź pozostaje pod kontrolą podmiotów spoza UE lub NATO. Prawo właściwe dla umowy z dostawcą chmury publicznej musi być prawem polskim lub innego kraju członkowskiego Unii Europejskiej.
   b. Dane nie pozostają wyłączną własnością i pod kontrolą operatora IK.
   c. Dane nie są szyfrowane zarówno w spoczynku, jak i podczas transmisji.
   d. Dostawca nie zapewnia wyboru lokalizacji danych (centrum lub centra przetwarzania danych, także w postaci tzw. regionu). Lokalizacja danych na terenie Polski jest zalecana w przypadku, kiedy bezpieczeństwo danych i możliwość przetwarzania są identyczne lub wyższe jak w przypadku lokalizacji na terenie krajów UE lub NATO.
   e. Dostawca dla konkretnej usługi chmurowej nie posiada systemu zarządzania bezpieczeństwem informacji opracowanego zgodnie z normą ISO 27001, wraz z ważnym certyfikatem wydanym przez akredytowany podmiot.
   g. Dostawca nie posiada planu ciągłości działania potwierdzonego ważnym certyfikatem zgodności z normą ISO 22301, którego zakres obejmuje konkretną usługę.
   h. Dostawca nie zapewnia kontraktowo standardowej dostępności rozwiązania chmurowego na poziomie co najmniej 99%.
   i. Dostawca nie przedstawia kontraktowo odpowiedzialności za swoich poddostawców (pod przetwarzających), a ich lista nie jest dostępna. Zaleca się wykorzystanie dostawców posiadających certyfikat ISO 27036.
   j. Dostawca nie zapewnia kontraktowo odpowiedzialności za swoich poddostawców (pod przetwarzających), a ich lista nie jest dostępna.
   k. Dostawca nie zapewnia kontraktowo procesu zgłaszania incydentów bezpieczeństwa.
   l. Dostawca nie zapewnia bezpośredniego wsparcia technicznego w Polsce.
6. **Zaleca się** by przy wyborze chmury obliczeniowej operator IK miał możliwość dodatkowo:
   a. Wyboru długości klucza szyfrującego oraz sposobu wyboru i przechowywania klucza.

b. Poprawy dostępności systemu teleinformatycznego w chmurze poprzez zastosowanie odpowiednich rozwiązań.
c. Zastosowania dedykowanego połączenia do chmury.
d. Skorzystania ze wsparcia technicznego osób posiadających poświadczenia bezpieczeństwa.
e. Dla usług chmury obliczeniowej, które mają być wykorzystywane przez operatora IK dostawca przedstawił także aktualne i wystawione przez akredytowane podmioty certyfikaty dla norm ISO 27017, ISO 27018, PN-EN 50600, SOC 1, SOC 2, NIST SP 800-53, NIST SP 800-207 lub równoważne.
f. W przypadku gdyby ocena ryzyka wskazywała, iż audyty niezależnych audytorów są niewystarczające to istnieje możliwość przeprowadzenia audytu u dostawcy.
g. Dla wybranych usług związanych z przetwarzaniem danych osobowych dostawca był związany odpowiednim kodeksem postępowania.

7. **Zaleca się** aby narzędzia administratora chmury pozwalały na wdrożenie polityk bezpieczeństwa, a w szczególności:
   a. Ochrony tożsamości poprzez wdrożenie wieloskładnikowego uwierzytelniania.
   b. Klasyfikacji danych.
   c. Ochrony przed przypadkowym lub celowym wyciekiem informacji poprzez wdrożenie narzędzi DLP (Data Loss Prevention).
8. Jeśli jest możliwe wykorzystanie Rządowej Chmury Obliczeniowej (RChO) to powinien być pierwszy wybór operatora IK.
9. Operator IK niezależnie od decyzji o wykorzystaniu chmury publicznej powinien przygotować **plan ewakuacji** systemów teleinformatycznych do chmury publicznej. W przypadku wykorzystywania chmury publicznej plan taki może ograniczyć się do przygotowania procesu przeniesienia systemu teleinformatycznego do innego centrum przetwarzania danych (lub regionu) tego samego dostawcy lub procesu zmiany dostawcy.

2.8.3.3. *Rodzaje zagrożeń*

Rozdział zawiera podzieloną na grupy aktywów przykładową listę podatności, wraz z odpowiadającym im zestawieniem potencjalnych zagrożeń, które w przypadku ich materializacji mogą mieć wpływ na ciągłość świadczenia usługi.

Grupy aktywów – lokalizacje fizyczne (budynki)

Podatności:

- Niestosowanie się użytkowników do zasad bezpiecznego korzystania z budynku i pomieszczeń.
- Niewłaściwe użytkowanie fizycznej kontroli dostępu (SKD, ochrona fizyczna).
- Lokalizacja w obszarze zagrożonym powodzią.
- Niestabilna sieć elektryczna.
- Nieodpowiednio zabezpieczone rozdzielnie.
- Zaniedbania w zakresie przeglądów i konserwacji urządzeń technicznych (zasilanie, klimatyzacja, itp.).
- W nieodpowiedni sposób prowadzone remonty i konserwacje.

Rodzaje zagrożeń i zabezpieczeń:

- Zniszczenia fizyczne
  a) Pożar - system wykrywania pożaru, system gaszenia, system suchogaszenia w serwerowni, zdublowany ośrodek obliczeniowy (serwerownia), biura zapasowe;
  b) Zalanie - lokalizacja pomieszczeń redukująca zagrożenie; zdublowany ośrodek obliczeniowy (serwerownia), biura zapasowe;
  c) Wybuch - ograniczenie ilości substancji wybuchowych, zdublowany ośrodek obliczeniowy (serwerownia), biuro zapasowe;
  d) Zamach terrorystyczny - kontrola dostępu, służby ochrony, nadzór wideo, zdublowany ośrodek obliczeniowy (serwerownia), biuro zapasowe;
  e) Silne promieniowanie / impuls elektromagnetyczny - w ograniczonym zakresie zdublowany ośrodek obliczeniowy (serwerownia), biuro zapasowe;
- Zjawiska naturalne
  a) Zjawiska sejsmiczne - w ograniczonym zakresie zdublowany ośrodek obliczeniowy (serwerownia), biuro zapasowe;
  b) Zjawiska atmosferyczne - konstrukcja i wyposażenie budynków, w ograniczonym zakresie zdublowany ośrodek obliczeniowy (serwerownia), biuro zapasowe;

c) Powódź - konstrukcja, wyposażenie i położenie budynków, w ograniczonym zakresie zdublowany ośrodek obliczeniowy (serwerownia), biuro zapasowe;
d) Osuwiska - konstrukcja, wyposażenie i położenie budynków, w ograniczonym zakresie zdublowany ośrodek obliczeniowy (serwerownia), biuro zapasowe;

- Awarie techniczne
  a) Utrata lub istotne ograniczenie dostaw wody - w ograniczonym zakresie zdublowany ośrodek obliczeniowy (serwerownia), biuro zapasowe;
  b) Utrata dostaw prądu - zasilanie gwarantowane, zasilanie z dwóch źródeł, agregaty prądotwórcze, zdublowany ośrodek obliczeniowy (serwerownia), biuro zapasowe;
  c) Awaria klimatyzacji - redundancja urządzeń; zdublowany ośrodek obliczeniowy (serwerownia), biuro zapasowe;
  d) Awaria urządzeń telekomunikacyjnych - redundancja urządzeń i łączy, zdublowany ośrodek obliczeniowy (serwerownia), biuro zapasowe.
- Niezamierzone, szkodliwe działania człowieka
  a) Przypadkowe odcięcie mediów (woda, prąd, łącza telekomunikacyjne) - redundancja urządzeń i łączy, zdublowany ośrodek obliczeniowy (serwerownia), biuro zapasowe.
- Celowe, szkodliwe działania człowieka
  b) Kradzież sprzętu - kontrola dostępu, służby ochrony, monitoring wizyjny, zdublowany ośrodek obliczeniowy (serwerownia), biuro zapasowe;
  c) Akty wandalizmu - konstrukcja i wyposażenie budynku, kontrola dostępu, służby ochrony, monitoring wizyjny, zdublowany ośrodek obliczeniowy (serwerownia), biuro zapasowe;
  d) Wymuszenie - kontrola dostępu, służby ochrony, nadzór wideo;
  e) Strajk służb odpowiedzialnych za utrzymanie i funkcjonowanie obiektów - w ograniczonym zakresie zdublowany ośrodek obliczeniowy (serwerownia), biuro zapasowe.

Grupy aktywów – infrastruktura techniczno-systemowa niezbędna do funkcjonowania systemów teleinformatycznych i aplikacji użytkowych

Podatności:

- Wrażliwość na czynniki środowiskowe (wilgoć, zbyt mała wilgotność, pył, zanieczyszczenia, itp.),
- Wrażliwość na promieniowanie elektromagnetyczne,
- Wrażliwość na wahania napięcia i częstotliwości,
- Brak lub opóźnione okresowe odtwarzania sprzętu,
- Niewłaściwe postępowanie z nośnikami pamięci,
- Brak skutecznej kontroli zmian konfiguracji,
- Brak staranności przy niszczeniu nośników,

- Nieodpowiednie zarządzanie infrastrukturą (nieużywane i nieodpowiednio zabezpieczone konta, włączone nieużywane usługi, niepotrzebnie otwarte porty, itp.),
- Niezabezpieczone okablowanie/łącza transmisji danych (w tym głowice telekomunikacyjne),
- Nieodpowiednio chroniony wrażliwy ruch,
- Występowanie pojedynczego punktu awarii,
- Brak lub słabe uwierzytelnienie (w tym słabe hasła kont uprzywilejowanych),
- Nadmierna ekspozycja usług,
- Niewłaściwe zasady nadawania uprawnień do zarządzania infrastrukturą,
- Działanie z nadmiernymi uprawnieniami,
- Niewłaściwie zabezpieczona struktura sieciowa,
- Brak separacji pomiędzy serwerami front-end i back-end (aplikacje - bazy danych),
- Nieodpowiednie zarządzanie siecią,
- Niezabezpieczona połączenia z siecią publiczną,
- Niezabezpieczenie lub niewłaściwe zabezpieczenie sieci Wi-Fi,
- Możliwość wpięcia do sieci LAN nieautoryzowanego urządzenia,
- Korzystanie ze sprzętu niewiadomego pochodzenia,
- Brak lub niewystarczające mechanizmy monitorowania działania infrastruktury,
- Brak lub niewłaściwe plany ciągłości działania,
- Brak lub nieaktualna lub niewystarczająca dokumentacja techniczna.

Rodzaje zagrożeń i zabezpieczeń:

- Zniszczenia fizyczne
    a) Wyładowanie elektrostatyczne – zerowanie, utrzymanie właściwej wilgotności (klimatyzacja z opcją nawilżania);
    b) Silne promieniowanie / impuls elektromagnetyczny - w ograniczonym zakresie redundancja urządzeń, zdublowany ośrodek obliczeniowy (serwerownia), biuro zapasowe;
    c) Silne promieniowanie cieplne - w ograniczonym zakresie redundancja urządzeń, zdublowany ośrodek obliczeniowy (serwerownia), biuro zapasowe;
    d) Zniszczenie fizyczne (np. upadek w trakcie czynności serwisowych, prac remontowych, itp.) - zasady BHP, w ograniczonym zakresie redundancja urządzeń, zdublowany ośrodek obliczeniowy (serwerownia), biuro zapasowe.
- Awarie techniczne
    a) Awaria całkowita urządzenia Redundancja urządzeń; zdublowany ośrodek obliczeniowy (serwerownia);
    b) Uszkodzenie modułu/komponentu urządzenia (w tym nośnika danych) - redundancja urządzeń, macierze dyskowe, kopie zapasowe, umowy

serwisowe, zdublowany ośrodek obliczeniowy (serwerownia), wirtualizacja;

c) Przerwa z zasilaniu - zasilanie gwarantowane, zasilanie awaryjne, agregat prądotwórczy, zdublowany ośrodek obliczeniowy (serwerownia),
d) Błędy w oprogramowaniu (firmware) - umowy serwisowe, zarządzanie podatnościami.

- Niezamierzone, szkodliwe działania człowieka
  a) Błędy konfiguracyjne - standardy konfiguracyjne, zarządzanie zmianą, testy, szkolenia;
  b) Błędy administratorów - standardy konfiguracyjne, zarządzanie zmianą, testy, szkolenia;
  c) Braki organizacyjne - źle zdefiniowana lub niezdefiniowana odpowiedzialność- procedury, polityki i zasady, audyt;
  d) Przypadkowy wyciek informacji - szyfrowanie nośników i urządzeń przenośnych, klasyfikacja informacji, systemy DLP, bezpieczny wydruk;
  e) Niewystarczająca dokumentacja techniczna - proces wyboru rozwiązania (ocena kompletności dokumentacji), testy, audyt;
  f) Brak wsparcia producenta/dostawcy - umowy serwisowe, unikanie niewspieranych technologii;
  g) Niewystarczające kompetencje administratorów - zasady rekrutacji, szkolenia, dokumentacja (instrukcje), standardy konfiguracyjne;
  h) Niewłaściwa architektura sieci - weryfikacja, testy bezpieczeństwa;
  i) Zastosowanie urządzeń nieadekwatnych do potrzeb - analiza potrzeb biznesowych, proces wyboru rozwiązania, testy;
  j) Niewystarczająca pojemność infrastruktury - zarządzanie pojemnością, wirtualizacja;
  k) Błędy monitorowania - określenie zakresu i częstotliwości monitorowania, systemy monitorowania i alarmowania;
  l) Udostepnienie możliwości zarządzania urządzeniem z sieci zewnętrznej - Polityki i zasady, konfiguracja sieci, sieciowe urządzenia zabezpieczające;
  m) Udostępnienie poświadczeń - polityki i zasady, rejestrowanie zdarzeń, mechanizmy zarządzania poświadczeniami.
- Celowe, szkodliwe działania człowieka
  a) Kradzież - kontrola dostępu, służby ochrony, monitoring wizyjny, zdublowany ośrodek obliczeniowy (serwerownia), biuro zapasowe;
  b) Podsłuch w tym przechwycenie komunikacji - architektura sieci, certyfikowane urządzenia, ekranowanie, konfiguracja sieci i urządzeń, sieciowe systemy zabezpieczające, szyfrowanie komunikacji;
  c) Działanie szkodliwego oprogramowania - sieciowe systemy zabezpieczające, oprogramowanie antywirusowe i antymalware, architektura sieci, zasada minimalnych uprawnień;
  d) Podmiana / rekonfiguracja oprogramowania - sieciowe systemy zabezpieczające, architektura sieci, zarządzanie zmianą, zasada minimalnych uprawnień, systemy centralnego zarzadzania, instalowania

oprogramowania, systemy centralnego zarządzania konfiguracją systemów;

e) Fałszowanie informacji Logowanie zdarzeń, kopie zapasowe, zdublowany ośrodek obliczeniowy (serwerownia), zasada minimalnych uprawnień;
f) Nadużycie praw dostępu - procedury i zasady, logowanie zdarzeń, monitoring, zarządzanie kontami uprzywilejowanymi,
g) Eskalacja uprawnień - zasada minimalnych uprawnień, zarządzanie podatnościami, regularne update-y i poprawki;
h) Wykorzystanie znanej podatności - zarządzanie podatnościami, sieciowe systemy zabezpieczające, architektura sieci, zasada minimalnych uprawnień;
i) Wymuszenie / socjotechnika - szkolenia, polityki i zasady, zasada minimalnych uprawnień, architektura sieci, sieciowe systemy zabezpieczające;
j) Spowodowanie niedostępności urządzenia (uszkodzenie, wyłączenie, DDoS) - Systemy antyDDoS na poziomie operatora łącz internetowych, operatorów CDN, zdublowane łącza, zdublowany ośrodek obliczeniowy (serwerownia), architektura sieci, zasada minimalnych uprawnień, system kontroli dostępu, służby ochrony;
k) Uszkodzenie okablowania - zdublowane łącza, zdublowany ośrodek obliczeniowy (serwerownia); architektura sieci, system kontroli dostępu, służby ochrony, monitoring wizyjny, systemy monitorowania infrastruktury;
l) Wykorzystanie publicznie dostępnych informacji - klasyfikacja informacji, procedury, polityki i zasady, sieciowe systemy zabezpieczające;
m) Przełamanie zabezpieczeń i pozyskanie informacji (konfiguracja urządzenia, struktura sieci wew., itp.) - sieciowe systemy zabezpieczające, architektura sieci, zasada minimalnych uprawnień, zarządzanie podatnościami, testy bezpieczeństwa, access listy.

Grupy aktywów – systemy i aplikacje

Podatności:

- Brak lub niewystarczające testowanie aplikacji
- Znane i nieusunięte podatności
- Nieaktualizowanie na bieżąco systemów i aplikacji
- Utrzymywanie aktywnej sesji przez czas dłuższy niż jest to wymagane
- Niewylogowanie ze stacji operatorskiej lub administracyjnej
- Brak lub niewystarczający poziom logowania zdarzeń
- Brak lub niewystarczająca kontroli spójności aplikacji i konfiguracji
- Niewłaściwe uprawnienia dostępu
- Niewłaściwe zarządzanie zmianą
- Niewłaściwa polityka hasłowa

- Nieprawidłowa konfiguracja
- Brak lub niewłaściwe mechanizmy uwierzytelniające
- Niezabezpieczona lub niewłaściwe zabezpieczone dane w bazach danych (w tym dane uwierzytelniające)
- Brak lub nieaktualna lub niewystarczająca dokumentacja techniczna
- Brak lub niewystarczające kopie zapasowe
- Uruchomione zbędne usługi
- Pozostawione aktywne niewykorzystywane konta
- Brak lub niewystarczająca kontrola nad rekonfiguracją systemów i aplikacji
- Brak lub niewystarczająca kontrola nad dostępem do danych

Rodzaje zagrożeń i zabezpieczeń:

- Awarie:
  a) Awaria systemu/aplikacji - zdublowany ośrodek obliczeniowy (serwerownia), architektura aplikacji (klaster/nadmiarowość), kopie zapasowe, wirtualizacja zasobów, testy aplikacji;
  b) Błędne działanie aplikacji w wyniku niezidentyfikowanego błędu - monitorowanie stanu działania aplikacji, testy aplikacji, zarządzanie zmianą;
  c) Nieakceptowalny czas odpowiedzi systemu/aplikacji (np. w wyniku przeciążenia) - monitorowanie stanu działania aplikacji, zarządzanie pojemnością, testy wydajnościowe i wysycenie aplikacji;
  d) Niewykonanie się kopii zapasowej - raportowanie systemu wykonywania kopii zapasowych, weryfikacja wykonania kopii.

- Niezamierzone, szkodliwe działania człowieka:
  a) Spowodowanie niedostępności systemu/aplikacji - zdublowany ośrodek obliczeniowy (serwerownia), architektura aplikacji (klaster/nadmiarowość), wirtualizacja zasobów,
  b) Błędy użytkowników - architektura i budowa aplikacji(walidacja danych wewnętrznych, system ról i uprawnień), szkolenia, dokumentacja użytkownika, testy,
  c) Nieprawidłowe skonfigurowanie systemu/aplikacji - dokumentacja aplikacji, monitorowanie stanu działania aplikacji, test aplikacji, zarządzanie zmianą, stosowanie wydzielonego środowiska developerskiego i testowego;
  d) Pozostawienie zidentyfikowanych podatności bez obsługi - zarządzanie podatnościami, dokumentacja aplikacji,
  e) Zastosowanie niezweryfikowanych komponentów systemów/aplikacji - architektura i budowa aplikacji, wymagania dotyczące aplikacji, procedury, polityki i zasady, testy aplikacji, stosowanie wydzielonego środowiska developerskiego i testowego,
  f) Ujawnienie danych autoryzacyjnych osobom nieuprawnionym - procedury, polityki i zasady, zasada minimalnych uprawnień,

g) Wprowadzenie niezweryfikowanej modyfikacji prowadzącej do powstania podatności - procedury, polityki i zasady, zasada minimalnych uprawnień, zarządzanie zmianą, testy aplikacji, dokumentacja aplikacji, stosowanie wydzielonego środowiska developerskiego i testowego,
h) Przypadkowe usunięcie kopii bezpieczeństwa - procedury, polityki i zasady, automatyzacja procesu wykonywania kopii bezpieczeństwa, duplikowanie kopii bezpieczeństwa.

- Celowe, szkodliwe działania człowieka
  a) Spowodowanie niedostępności systemu/aplikacji - zdublowany ośrodek obliczeniowy (serwerownia), architektura aplikacji (klaster), wirtualizacja zasobów sieciowe systemy zabezpieczające, polityki procedury i zasady, logowanie zdarzeń;
  b) Ograniczenie dostępności systemu / aplikacji - zdublowany ośrodek obliczeniowy (serwerownia), architektura aplikacji (klaster), wirtualizacja zasobów sieciowe systemy zabezpieczające, polityki procedury i zasady, logowanie zdarzeń;
  c) Usunięcie lub nieuprawniona modyfikacja danych - popie zapasowe, sieciowe systemy zabezpieczające architektura sieci i aplikacji, zasada minimalnych uprawnień, polityki procedury i zasady, logowanie zdarzeń, access listy;
  d) Nieuprawniona ekstrakcja danych - sieciowe systemy zabezpieczające architektura sieci i aplikacji, zasada minimalnych uprawnień, polityki procedury i zasady, logowanie zdarzeń, access listy;
  e) Zmiana konfiguracji systemu / aplikacji powodująca powstanie nowych podatności - sieciowe systemy zabezpieczające architektura sieci i aplikacji, zasada minimalnych uprawnień, polityki procedury i zasady, logowanie zdarzeń, zarządzanie podatnościami, testy aplikacji, access listy;
  f) Podniesienie uprawnień i wykonanie szkodliwych działań - sieciowe systemy zabezpieczające, architektura sieci i aplikacji, zasada minimalnych uprawnień, polityki procedury i zasady, logowanie zdarzeń, zarządzanie podatnościami, testy aplikacji, access listy;
  g) Instalacja szkodliwego oprogramowania (na stacji administracyjnej lub operatorskiej) - sieciowe systemy zabezpieczające, architektura sieci i aplikacji, zasada minimalnych uprawnień, monitoring, oprogramowania antymalware, logowanie zdarzeń, zarządzanie podatnościami, access listy
  h) Działanie szkodliwego oprogramowania Sieciowe systemy zabezpieczające, architektura sieci i aplikacji, zasada minimalnych uprawnień, oprogramowania antymalware, logowanie zdarzeń, zarządzanie podatnościami.

Grupy aktywów – Zasoby informacyjne, dane, dokumenty

Podatności:

- Niestosowanie się użytkowników do zasad postępowania z informacją
- Niewłaściwe zabezpieczenie informacji przed zniszczeniem lub dostępem osób nieuprawnionych
- Brak kopii zasobów informacyjnych (papierowych)
- Nieaktualizowanie dokumentacji
- Niepełna lub niewystarczająca a jakość informacji
- Niewystarczające zabezpieczenie danych na nośnikach danych
- Brak lub niewłaściwa realizacja kopii bezpieczeństwa
- Nieodpowiednie uprawnienia w zakresie dostępu do danych
- Brak autoryzacji środków przetwarzania informacji

Rodzaje zagrożeń i zabezpieczeń:

- Zagrożenia środowiskowe:

  a) Pożar - system wykrywania pożaru, system gaszenia (biuro) system suchogaszenia (serwerownia); zdublowany ośrodek obliczeniowy (serwerownia); biuro zapasowe, służby ochrony, szkolenia pracowników;
  b) Zalanie - lokalizacja pomieszczeń redukująca zagrożenie; zdublowany ośrodek obliczeniowy (serwerownia); biuro zapasowe.

- Awarie techniczne
  a) Uszkodzenie nośnika danych - redundancja nośników (RAID, macierze), kopie zapasowe;
  b) Awaria skutkująca tymczasową niedostępnością zasobów informacyjnych - zdublowany ośrodek obliczeniowy (serwerownia) (replikacja danych).

- Niezamierzone, szkodliwe działania człowieka
  a) Przypadkowe zniszczenie lub skasowanie - kopie zapasowe, zdublowany ośrodek obliczeniowy (serwerownia) (replikacja danych);
  b) Przypadkowe udostępnienie osobom nieuprawnionym - procedury, polityki i zasady;
  c) Zgubienie - kopie zapasowe, szyfrowanie danych, procedury, polityki i zasady;
  d) Przypadkowa modyfikacja (naruszenie integralności) - kopie zapasowe, zdublowany ośrodek obliczeniowy (serwerownia) (replikacja danych), zarządzanie zmianami.

- Celowe, szkodliwe działania człowieka
  a) Kradzież - kopie zapasowe, zdublowany ośrodek obliczeniowy (serwerownia) (replikacja danych), procedury, polityki i zasady;

b) Zniszczenie fizyczne - kopie zapasowe, zdublowany ośrodek obliczeniowy (serwerownia) (replikacja danych), procedury, polityki i zasady;
c) Modyfikacja informacji (danych) - kopie zapasowe, zdublowany ośrodek obliczeniowy (serwerownia) (replikacja danych), logowanie zdarzeń, procedury, polityki i zasady.

Grupy aktywów – Personel

Podatności:

- Nieobecność personelu
- Braki kadrowe
- Nieodpowiedzialność i niefrasobliwość personelu
- Nieodpowiednie procedury rekrutacji
- Niewystarczające szkolenia
- Niska świadomość z zakresu bezpieczeństwa
- Niepoprawne używanie sprzętu i aplikacji
- Brak mechanizmów monitorowania
- Brak lub niewystarczające zasady wykorzystania sprzętu i środków telekomunikacyjnych
- Podatność personelu na przekupstwo
- Nieprzestrzeganie zasad ochrony fizycznej

Rodzaje zagrożeń i zabezpieczeń:

- Czynniki zewnętrzne
  a) Choroba lub niedyspozycja – zastępowalność
  b) Niewystarczająca wiedza – szkolenia
  c) Braki kadrowe - polityka kadrowa, zarządzanie ryzykiem
- Czynniki wewnętrzne
  a) Brak motywacji - polityka kadrowa
  b) Konflikt interesów - procedury, polityki i zasady
  c) Sabotaż - system kontroli dostępu, służby ochrony, monitoring wizyjny, zasada minimalizacji uprawnień, systemy monitorowania, logowanie zdarzeń
  d) Strajk - zarządzanie ryzykiem

Grupy aktywów – Usługi

Podatności:

- Brak lub niewłaściwe procedury wyboru dostawców
- Brak wsparcia serwisowego
- Brak nadzoru nad realizacją usług zewnętrznych (serwisanci, dostawcy oprogramowania, serwis sprzątający)

- Brak lub niewystarczający poziom monitorowania działań dostawców zewnętrznych
- Brak lub niewłaściwe monitorowanie jakości świadczenia usług
- Brak lub niewłaściwe klauzule zabezpieczające w umowach na świadczenie usług
- Nieadekwatne uprawnienia dostawców usług zewnętrznych
- Brak odpowiednich ograniczeń w zakresie dostępu fizycznego (w tym brak nadzoru)
- Brak procedur awaryjnego wyboru dostawców alternatywnych
- Niewystarczający dostęp do części zamiennych

Rodzaje zagrożeń i zabezpieczeń:

- Niezamierzone szkodliwe działania:
  a) Utrata zdolności wykonawczych (np. zakończenie działalności, zmiana profilu, utrata kluczowego personelu - korzystanie ze sprawdzonych dostawców, zabezpieczające zapisy w umowach, monitorowanie jakości świadczenia usług, procedury awaryjnego wyboru nowego dostawcy;
  b) Ograniczenie zdolności wykonawczych (np. utrata części personelu, utrata istotnych kompetencji) - korzystanie ze sprawdzonych dostawców, zabezpieczające zapisy w umowach, monitorowanie jakości świadczenia usług, procedury awaryjnego wyboru nowego dostawcy;
  c) Niewystarczająca jakość świadczonej usługi - korzystanie ze sprawdzonych dostawców, zabezpieczające zapisy w umowach, monitorowanie jakości świadczenia usług, procedury awaryjnego wyboru nowego dostawcy;
  d) Brak dokumentacji wykonanej usługi - korzystanie ze sprawdzonych dostawców, zabezpieczające zapisy w umowach, monitorowanie jakości świadczenia usług.
- Celowe, szkodliwe działania:
  a) Celowa modyfikacja parametrów pracy systemów - korzystanie ze sprawdzonych dostawców, minimalizowanie uprawnień, monitorowanie pracy dostawców, testy;
  b) Celowa modyfikacja danych - korzystanie ze sprawdzonych dostawców, minimalizowanie uprawnień, monitorowanie pracy dostawców, testy;
  c) Nieprzestrzeganie warunków realizacji umowy - korzystanie ze sprawdzonych dostawców, zabezpieczające zapisy w umowach, monitorowanie jakości świadczenia usług, procedury awaryjnego wyboru nowego dostawcy;
  d) Wprowadzenie nieudokumentowanej funkcjonalności do aplikacji - korzystanie ze sprawdzonych dostawców, minimalizowanie uprawnień, monitorowanie pracy dostawców, testy;
  e) Kradzież informacji - korzystanie ze sprawdzonych dostawców, minimalizowanie uprawnień, monitorowanie pracy dostawców;

f) Kradzież sprzętu - korzystanie ze sprawdzonych dostawców, ograniczenie uprawnień dostępu, monitorowanie pracy dostawców;
g) Sabotaż - korzystanie ze sprawdzonych dostawców, minimalizowanie uprawnień, ograniczenie uprawnień dostępu, monitorowanie pracy dostawców, testy.

2.8.3.4. *Współodpowiedzialność za ciągłość procesu*

Bezpieczeństwo i zgodność (Security & Compliance) to wspólna odpowiedzialność dostawcy usług chmury obliczeniowej i klienta. Ten wspólny model dzielonej współodpowiedzialności pomaga zmniejszyć obciążenie operacyjne operatora IK, ponieważ dostawca usług chmury obliczeniowej działa, zarządza i kontroluje komponenty od systemu operacyjnego hosta i warstwy wirtualizacji aż po fizyczne bezpieczeństwo obiektów, w których działa dana usługa.

Operatorzy IK powinni dokładnie rozważyć i zrozumieć działanie usług, które wybierają, ponieważ ich obowiązki różnią się w zależności od rodzaju używanych usług, integracji tych usług z ich środowiskiem IT oraz obowiązujących przepisów i regulacji. Jest to również element bardzo istotny, jeśli chodzi o spojrzenie i planowanie w obszarze ciągłości działania i procesów, które będą przenoszone do chmury obliczeniowej, ponieważ różnią się one w sposób zasadniczy od tradycyjnego modelu on-premises.

W pewnym uproszczeniu przyjmuje się, że dostawca usług w chmurze obliczeniowej odpowiada za ochronę infrastruktury, na której działają te usługi. Ta infrastruktura składa się ze sprzętu, oprogramowania, sieci i obiektów obsługujących usługi w chmurze obliczeniowej.

Odpowiedzialność operatora IK jest określana przez rodzaj usług chmury obliczeniowej wybranych przez niego. Ten wybór niesie za sobą konsekwencje i determinuje ilość pracy konfiguracyjnej, którą operator musi wykonać w ramach swoich obowiązków związanych z obszarem bezpieczeństwem. Na przykład usługa sklasyfikowana jako infrastruktura jako usługa (IaaS – Infrastructure as a Service) jako taka wymaga od klienta wykonania wszystkich niezbędnych zadań związanych z konfiguracją zabezpieczeń i zarządzaniem. Operatorzy IK, którzy wdrażają taką usługę są odpowiedzialni za zarządzanie systemem operacyjnym hosta (w tym aktualizacjami i poprawkami bezpieczeństwa), wszelkimi aplikacjami lub narzędziami zainstalowanymi przez klienta na instancjach oraz konfigurację zapory sieciowej (firewall). W przypadku usług typu PaaS dostawca usług w chmurze obliczeniowej obsługuje warstwę infrastruktury, system operacyjny i platformę, a operator IK uzyskuje dostęp do punktów końcowych w celu przechowywania i pobierania danych. Co więcej klienci są odpowiedzialni za zarządzanie swoimi danymi (w tym wyborem

opcji szyfrowania), klasyfikowanie swoich zasobów i używanie narzędzi do stosowania odpowiednich uprawnień i zarządzania dostępem do nich.

Ten model współodpowiedzialności dostawca usług chmury obliczeniowej/operatora IK obejmuje również obszar zgodności i kontroli (compliance). Tak jak odpowiedzialność za obsługę środowiska IT jest dzielona pomiędzy dostawcę usług w chmurze obliczeniowej i jej operatorów, tak samo zarządzanie, obsługa i weryfikacja zgodności są współdzielone. Dostawca chmury obliczeniowej może pomóc odciążyć operatora zarządzając kontrolami związanymi z infrastrukturą fizyczną wdrożoną w swoim środowisku, które wcześniej mogły być zarządzane i leżały w gestii operatora. Ponieważ każde wdrożenie usługi w chmurze obliczeniowej jest inne, klienci mogą skorzystać z przeniesienia zarządzania pewnymi aspektami zgodności do dostawcy usług, co skutkuje (nowym) rozproszonym środowiskiem kontroli. Operatorzy IK mogą następnie wykorzystać dostępną im dokumentację kontroli i zgodności danego dostawcy chmury obliczeniowej, aby przeprowadzić wymagane procedury/audyty w obszarze ich oceny i weryfikacji.

W tej samej perspektywie należy spojrzeć na ciągłość procesu, który chcemy przenieść do chmury obliczeniowej. On również jest podzielony na część, za którą będzie odpowiedzialny dostawca usług w chmurze obliczeniowej i część, która będzie leżała w obszarze odpowiedzialności operatora. Będzie to również wynikiem tego jakiego rodzaju usługi w chmurze obliczeniowej będą wykorzystywane do jego realizacji. Po stronie dostawcy chmury obliczeniowej warto zwrócić uwagę na posiadanie certyfikatu ISO 22301 – Zarządzanie Ciągłością Działania jak również certyfikatu ISO 27001 z komponentami Business Continuity Management (BCM), Business Impact Analysis (BIA), Business Continuity Plan (BCP). Aby uzyskać bardziej szczegółowe informacje na temat działań podejmowanych przez dostawców usług w chmurze obliczeniowej w celu zapewnienia ciągłości działania warto zapoznać się również z raportami takimi jak C5 (Cloud Computing Compliance Controls Catalogue) czy też raportem SOC (Service Organizations Control) 2 typ 2.

Rekomendowane jest dla operatorów IK zweryfikowanie raportów i certyfikacji z obszaru ciągłości działania poprzez kontrolę raportów z atestacji dostawcy usług w chmurze obliczeniowej. Przykładowo, obszary na które powinniśmy zwrócić uwagę:

- Czy dostawca usług w chmurze obliczeniowej posiada program typu resiliency, który obejmuje procesy i procedury, za pomocą których identyfikuje, reaguje na poważne zdarzenie lub incydent, a także je usuwa;
- Czy plany awaryjne i podręczniki reagowania na incydenty są utrzymywane i aktualizowane w celu odzwierciedlenia pojawiających się zagrożeń

związanych z ciągłością działania i wniosków wyciągniętych z przeszłych incydentów;

- Czy plany odpowiedzi i reagowania zespołu serwisowego są testowane i aktualizowane w trakcie działalności, a plan odporności dostawcy chmury obliczeniowej jest testowany, weryfikowany i zatwierdzany corocznie przez kierownictwo wyższego szczebla;
- Czy dostawca chmury utworzył CSIRT (Computer Security Incident Response Team), który przyczynia się do skoordynowanego rozwiązywania konkretnych incydentów bezpieczeństwa i czy operatorzy dotknięci incydentami bezpieczeństwa są informowani w odpowiednim czasie i w odpowiedniej formie.

Istotnym elementem jest również zrozumienie poziomu dostępności nie tylko na poziomie samego regionu/stref dostępności danego dostawcy usług w chmurze obliczeniowej, ale poszczególnych usług i ich poziomu dostępności (służy do tego umowa SLA – Service Level Agreement). Informacje te powinny być standardowo dostępne na stronach internetowych dostawców usług w chmurze obliczeniowej.

W przypadku bardzo krytycznych obciążeń można rozważyć wdrożenie infrastruktury w wielu regionach z replikacją danych i ciągłymi kopiami zapasowymi, aby zminimalizować wpływ na ciągłość procesu. Należy wziąć pod uwagę, jak dostawca usług chmury obliczeniowej zaprojektował strefy dostępności w regionie i czy zachowana jest znacząca odległość między nimi i starannie zaplanowana lokalizacja, tak aby ewentualne katastrofy miały wpływ tylko na jedną strefę, a nie na inne.

2.8.4. Budowanie odporności

Cyberbezpieczeństwo jest często niesłusznie utożsamiane z ochroną urządzeń końcowych przez program antywirusowy. W rzeczywistości cyberbezpieczeństwo musi być budowane w każdym obszarze. Zgodnie z zasadą Zero Trust – odporność organizacji na zagrożenia teleinformatyczne powinna obejmować: tożsamość, dane, oprogramowanie, infrastrukturę, aplikacje oraz sieci. Ochrona tożsamości powinna obejmować silne uwierzytelnianie użytkowników, weryfikację wykorzystywanych przez niego urządzeń, weryfikację uprawnień (minimalne, niezbędne, nadawane tymczasowo) oraz weryfikację prowadzonej aktywności (pod kątem anomalii, w tym np. wycieków lub ekstrakcji danych).

Dodatkowo, w zakresie „white/black list", w dobie dynamicznych domen i zmiennej adresacji, zaproponowane rozwiązanie należy uznać za niewystarczające i wymagające rozbudowania o mechanizmy refutacyjne, bazujące na wykorzystaniu SI oraz współpracy firm, dostawców lub zespołów zajmujących się cyberbezpieczeństwem.

Szczególnym przypadkiem jest ochrona automatyki przemysłowej, która zostanie opisana w rozdziale 2.8.9.

2.8.4.1. *Urządzenia końcowe*

Powszechność dostępu do sieci Internet przez stacje robocze pracowników organizacji powoduje znaczny wzrost podatności na zagrożenia z niej pochodzące. Dlatego rekomendowanym rozwiązaniem jest rezygnacja z możliwości dostępu ze stacji roboczych pracowników, podłączonych do Internetu, do systemów obsługujących IK. Jednak jeśli jest taka konieczność, to w celu zmniejszenia tej podatności ochrona stacji roboczych, na których pracują pracownicy organizacji, w tym ci, którzy bezpośrednio obsługują IK, powinna być oparta o trzy podstawowe filary bezpieczeństwa:

Aktualizacja oprogramowania

Należy zwrócić uwagę, że oprócz powszechnej świadomości związanej z koniecznością aktualizacji oprogramowania systemów operacyjnych, konieczne jest również aktualizowanie aplikacji. Nie wszystkie systemy operacyjne i aplikacje posiadają możliwość automatycznej aktualizacji. Jeżeli możliwa jest automatyzacja danego oprogramowania (system operacyjny AV), jedną z dobrych praktyk jest uruchomienie własnego centrum aktualizacji. Daje to kontrolę nad instalacją aktualizacji i zmniejsza ryzyko instalacji aktualizacji prowadzącej do awarii oprogramowania. Dodatkowo, ze względu na konieczność zachowania prawidłowego działania aplikacji (np. w przypadku systemów automatyki), często nie jest możliwe korzystanie z tej funkcji, a wprowadzenie zmiany w oprogramowaniu wiąże się z zastosowaniem procedury zarządzania zmianą i przeprowadzeniem serii testów potwierdzających brak wpływu aktualizacji na funkcjonowanie systemu.

Częścią procedury zarządzania zmianą dotyczącą aktualizacji oprogramowania powinna być skrócona analiza ryzyka związana z pojawieniem się nowego zagrożenia. Pomocne przy tym może być zastosowanie standardu CVSS[48] (ang. *Common Vulnerability Scoring System*). Zastosowanie oceny zagrożenia słabości systemowej, z którą związana jest aktualizacja, z wykorzystaniem tego standardu, pozwala na zestandaryzowaną ocenę, która może być podstawą decyzji o aktualizacji. Niekiedy takiej oceny dokonują sami producenci[49]. Jeśli jednak taka ocena nie jest dostępna, to możliwe jest przeprowadzenie jej samemu, np. z wykorzystaniem kalkulatora CVSS[50].

[48] http://www.first.org/cvss/cvss-guide.html
[49] Np. CISCO http://www.cisco.com/web/about/security/intelligence/Cisco_CVSS.html
[50] Np. udostępnianego przez NIST http://nvd.nist.gov/cvss.cfm?calculator

Należy zwrócić uwagę na proces zarządzania aplikacjami na poziomie stacji roboczej poprzez odebranie uprawnień do samodzielnej instalacji oprogramowania lub udostępnienie wewnętrznych sklepów z oprogramowaniem umożliwiających samodzielną instalację, ale wyłącznie zatwierdzonego i/lub skonfigurowanego oprogramowania. Zaleca się również wdrożenie centralnego systemu do zarządzania aplikacjami lub dystrybucję skonfigurowanych aplikacji, w których użytkownik ma ograniczone możliwości zmiany ustawień.

Firewalling

Zasady, które należy wykorzystywać przy ochronie stacji roboczych przez stosowanie zapory ogniowej, nie różnią się zasadniczo od tych opisywanych wcześniej[51]. Podstawową różnicą jest to, że do ochrony stacji roboczych używamy tzw. osobistych zapór ogniowych. Są one albo wbudowane w system operacyjny, albo są oddzielnym dedykowanym oprogramowaniem.

Ochrona przed złośliwym oprogramowaniem

Uzupełnieniem dla aktualizacji oprogramowania i ochrony typu *firewalling* jest ochrona przed złośliwym oprogramowaniem. Jako złośliwe oprogramowanie (ang. *malware*) określa się wszelkiego rodzaju oprogramowanie ingerujące w funkcjonowanie komputera bez wiedzy jego właściciela. Wśród złośliwego oprogramowania można wyróżnić:

- Ransomware
- Wirusy komputerowe (ang. *computer virus*),
- Robaki internetowe (ang. *Internet worms*),
- Konie trojańskie (ang. *trojan horse*),
- Oprogramowanie szpiegujące (ang. *spyware*),
- Oprogramowanie kradnące tożsamość (ang. *crimeware*).

Może ono spełniać najróżniejsze funkcje, od prostego zbierania informacji o użytkowniku systemu do wykonywania działań przestępczych. W praktyce trudne jest rozróżnienie poszczególnych rodzajów złośliwego oprogramowania, zresztą coraz bardziej jest to bezcelowe, ponieważ coraz częściej poszczególne programy łączą w sobie złośliwe funkcje.

Ochroną przed złośliwym oprogramowaniem jest instalowanie odpowiedniego oprogramowania ochronnego. Oprogramowanie to w większości chroni przed znanymi złośliwymi programami. Należy jednak zwrócić uwagę na fakt, że liczba nowych rodzajów złośliwego oprogramowania (lub chociażby nieznacznie modyfikowanego

[51] Patrz rozdział 2.8.3.4 Kontrola dostępu.

w celu poprawienia jego kamuflażu) jest bardzo duża[52]. Dlatego w praktyce nie jest możliwe skuteczne wykrycie wszystkich istniejących w sieci wirusów. Nie zmienia to oczywiście konieczności używania odpowiedniego oprogramowania.

Należy pamiętać, że oprogramowanie antywirusowe chroni przed znanymi złośliwymi programami, które w dużej części bazuje na sygnaturach wirusów, choć ma wbudowane też mechanizmy heurystyczne czy funkcjonalności typu HIPS; warto uwzględnić również istniejące rozwiązania klasyEDR (Endpoint Detection and Response), które nie działają w oparciu o sygnatury, a w oparciu o zdarzenia na stacji końcowej, dzięki czemu mogą wykrywać nieznane zagrożenia.

2.8.4.2. *Dane*

Kontrola dostępu

Kontrola dostępu do zasobów jest podstawowym sposobem zapewnienia bezpieczeństwa teleinformatycznego. Główną zasadą, jaką należy się kierować przy ustalaniu zasad dostępu do zasobów, jest zasada „potrzeby dostępu do informacji" (ang. *need to know*). Według tej zasady należy przyznawać prawa dostępu do poszczególnych zasobów tylko i wyłącznie tym, dla których ten dostęp jest konieczny.

Istnieją dwie metody weryfikacji praw dostępu do systemu teleinformatycznego. Pierwsza polega na szczegółowym ponownym rozpatrzeniu praw dostępu. Warto uwzględnić w tej analizie częstotliwość dotychczasowego dostępu i rodzaj udostępnianych danych (czy pokrywają się one z rzeczywistymi potrzebami osób posiadających prawa dostępu). Zaletą tej metody jest systemowe podejście i pełne zachowanie ciągłości zadania. Wadą jest to, że najprawdopodobniej wiele prób odebrania dostępu napotka na poważny opór, związany z mniej lub bardziej prawdziwymi uzasadnieniami konieczności tego dostępu. Dlatego istnieje druga, bardziej radykalna metoda. Dostęp jest odbierany wszystkim użytkownikom systemu (być może oprócz tych oczywistych przypadków konieczności dostępu, jak dostęp dla księgujących rozliczenia do sytemu wprowadzania tych rozliczeń) i obserwuje się przypadki prób dostępu do systemu. Same te przypadki świadczą o potencjalnej konieczności dostępu do informacji. Należy je wtedy szczegółowo dodatkowo przeanalizować i podjąć ostateczną decyzję co do faktu dostępu i jego zakresu.

Jednym z największych zagrożeń jest przyznawanie praw dostępu lub zmiana zakresu dostępu tzw. na chwilę. Zazwyczaj podyktowane to jest rzeczywistą chwilową potrzebą, często też koniecznością dostępu z zewnątrz firmy (co na przykład w normalnej sytuacji uniemożliwiamy). Praktyka wskazuje, że często ten chwilowy

[52] Serwis internetowy Virus Total analizuje tygodniowo kilkadziesiąt tysięcy nowych plików ze złośliwym oprogramowaniem http://www.virustotal.com/stats.html

dostęp trwa znacznie dłużej. Dlatego należy go przede wszystkim unikać, a w uzasadnionych przypadkach przyznawania przyznawać wraz z czasowym ograniczeniem, kontrolowanym automatycznie przez system (jeżeli na to pozwala).

Poza opisanymi powyżej zasadami „potrzeby dostępu do informacji" powinno się stosować inne, bardziej techniczne, narzędzia kontroli dostępu:

Kontrola dostępu przez zapewnienie odpowiedniej architektury sieci

W szczególności chodzi o zastosowanie wirtualnych sieci lokalnych (ang. *Virtual Local Network*), czyli sieci komputerowych wydzielonych logicznie w ramach większej sieci fizycznej. Dzięki takiemu wydzieleniu możliwa jest separacja ruchu sieciowego, co jest ważną zasadą ochrony. Ważnymi dodatkowymi elementami bezpieczeństwa sieci wirtualnych jest zastosowanie kontroli ruchu na podstawie adresów MAC (ang. *Media Access Control*) oraz odpowiednią politykę filtracji pakietów IP[53].

Dobrą praktyką jest stosowanie zasad kontroli dostępu do sieci na podstawie „zdrowia komputera" tzn. czy jest wyposażony w najnowsze aktualizacje zgodne z założeniami administratora systemu. W przypadku, gdy komputer nie przechodzi prawidłowo weryfikacji, przekierowywany jest do innej podsieci, w której dokonywana jest automatyczna aktualizacja niezbędnych elementów oprogramowania.

Stosowanie informatycznej zapory ogniowej (ang. Firewalling)

Firewalling jest jedną z podstawowych technik bezpieczeństwa. Realizowany jest on w oparciu o odpowiednie oprogramowanie lub kompletne rozwiązanie w postaci dedykowanego urządzenia i oprogramowania. Dzięki zastosowaniu firewalla możemy chronić ruch wchodzący do sieci organizacji oraz ruch wychodzący z organizacji, za każdym razem wskazując tylko na ten, który jest przez nas dopuszczony. Inną istotną cechą, którą możemy realizować z wykorzystaniem firewalla, jest monitorowanie ruchu oraz identyfikacja i dopuszczanie do sieci uprawnionych użytkowników przez zestawienie szyfrowanego połączenia, tzw. wirtualnej sieci prywatnej (ang. *Virtual Private Network*)[54].

Dostęp z zewnątrz

Dostęp do zasobów organizacji z zewnątrz powinien odbywać się w sposób bezpieczny, pamiętając głównie o dostępie szyfrowanym (wybór protokołów i algorytmów szyfrujących powinien być dokonany na podstawie ich podatności na ataki

---

[53] Więcej na temat zasad bezpieczeństwa przy tworzeniu sieci wirtualnych można znaleźć w dokumencie „VLAN Security Guidlines" http://www.corecom.com/external/livesecurity/vlansec.htm

[54] Szczegółowe konfiguracje firewalla różnią się w zależności od jego rodzaju i producenta. Ogólne zasady dotyczące konfiguracji firewall można znaleźć na stronie http://msdn.microsoft.com/en-us/library/ms898965.aspx

kryptoanalityczne) i opartym o mocne uwierzytelnienie. W ten sposób tworzy się bezpieczny szyfrowany kanał komunikacji z zasobami firmy. Jednym z najlepszych sposobów mocnego uwierzytelnienia jest stosowanie uwierzytelniania wieloskładnikowego (MFA), najlepiej w postaci sprzętowych kluczy lub kluczy/tokenów aplikacyjnych.

Przy organizacji dostępu z zewnątrz warto również objąć specjalnym sposobem zabezpieczenia komunikacji dostęp dla firm serwisujących oprogramowanie i urządzenia. Tego typu dostęp jest bardzo często organizowany przez firmy zewnętrzne na ich warunkach. Niestety priorytetem przy tym dostępie jest organizowanie go tak, aby był jak najłatwiejszy dla serwisantów, bardzo często bez zwracania szczególnej uwagi na zasady bezpieczeństwa.

Szczególną uwagę należy zwrócić na zdalny dostęp (np. firm serwisujących) do aktywów systemów automatyki przemysłowej. Tego typu dostęp powinien być nadawany tylko w uzasadnionych przypadkach, każdorazowo rejestrowany oraz potwierdzony przez osobę odpowiedzialną za dany obszar / system. Kanał zdalnego dostępu powinien być zamykany po zakończeniu prac i otwierany ponownie jedynie w przypadku wystąpienia uzasadnionej potrzeby jego wykorzystania. Wszelkie prace prowadzone w ramach zdalnego dostępu powinny być rejestrowane i na bieżąco monitorowane.

W sieciach obsługujących IK nadal bardzo popularnym sposobem dostępu do urządzeń jest dostęp dodzwaniany (ang. *dial-up*). Korzystanie z tego typu dostępu nie jest najbezpieczniejszym sposobem i rekomendowane jest unikanie tego typu dostępu, niemniej jednak istnieją metody jego odpowiedniego zabezpieczenia w sytuacji konieczności użycia tej metody dostępu. W przypadku korzystania z dostępu dodzwanianego należy zwrócić uwagę na zapewnienie następujących zasad bezpieczeństwa:

- kontrolę danych logowania,
- kontrolę dostępu z wykorzystaniem odpowiednio mocnego hasła, w miarę możliwości hasła jednorazowego,
- systemu wykrywania połączeń z nieautoryzowanych źródeł i alarmowania o nich.

Tworzenie „czarnych list" i „białych list" (ang. blacklisting i whitelisting)

Jedną z możliwych do wyboru metod kontroli dostępu jest tworzenie „czarnych list" i „białych list". Wykorzystanie tych technik jest często w ochronie antyspamowej. Również można je stosować w przypadku ochrony przed złośliwym oprogramowaniem instalującym się bez wiedzy użytkownika w trakcie odwiedzin zainfekowanej strony www[55]. Idea „czarnej listy" polega na wskazaniu tych adresów (e-mail, IP,

[55] Tzw. *drive-by download* http://en.wikipedia.org/wiki/Drive-by_download

domenowych), które nie są dozwolone w ruchu przychodzącym. Wszystkie inne adresy będą dopuszczone. Natomiast „biała lista" zawiera te adresy, które będą akceptowane jako adresy źródłowe. Żadne inne adresy, które nie znajdują się na „białej liście", nie będą akceptowane. Oprócz wspomnianej możliwości wykorzystania tej techniki w ochronie komunikacji internetowej (spam, *drive-by download*), można ją również z powodzeniem wykorzystywać w zarządzaniu siecią wewnętrzną i zewnętrzną, w ustalaniu praw dostępu do poszczególnych aplikacji.

Serwer pośredniczący (ang. proxy serwer)

Kolejną techniką kontroli dostępu jest użycie serwera pośredniczącego. Oprócz funkcji bezpieczeństwa może on również spełniać zadania poprawy efektywności ruchu, np. przez pośredniczenie w dostępie do zasobów internetowych, które jeśli były wcześniej ściągane przez jednego użytkownika, to dla kolejnych są już udostępniane z serwera pośredniczącego, a nie z oryginalnego serwisu, co znacznie przyśpiesza transmisję danych. Natomiast podstawowymi funkcjami bezpieczeństwa dla serwera proxy jest możliwość kontroli ruchu, zanim zostanie on dostarczony do końcowego użytkownika (na przykład tak może się odbywać kontrola antywirusowa stron internetowych) oraz możliwość ukrywania (w przypadku takiej potrzeby) wybranych adresów IP z chronionej sieci

Szyfrowanie

Nieuprawniony dostęp do danych często jest wynikiem fizycznej kradzieży lub zgubienia urządzenia czy nośnika, na którym dane były przechowywane. Należy w związku z tym zadbać o to, aby wszelkie dane wrażliwe były utrwalane wyłącznie w postaci zaszyfrowanej. Dla urządzeń mobilnych, takich jak laptopy czy smartfony, najbardziej praktycznym i bezpiecznym rozwiązaniem jest skorzystanie z pełnego szyfrowania dysków. W praktyce rozwiązanie takie oznacza, że do zawartości dysku może mieć dostęp wyłącznie osoba dysponująca odpowiednim kluczem, hasłem lub kodem PIN. Dla takiego użytkownika dostęp odbywa się w sposób przezroczysty. Z drugiej strony, zdobycie dysku przez osobę nieposiadającą klucza (na przykład w następstwie kradzieży) umożliwia wyłącznie podejrzenie danych w postaci zaszyfrowanej. Pełne szyfrowanie dysku jest dostępne we wszystkich nowoczesnych systemach operacyjnych, często w postaci natywnego narzędzia (np. Bitlocker w Windows, Filevault w Mac OS) lub odpowiedniej opcji w panelu zabezpieczeń. Należy upewnić się, że dane rozwiązanie zostało poprawnie zastosowane. Oznacza to także, że wybrany został odpowiednio silny klucz, albo skomplikowane, trudne do odgadnięcia hasło bądź kod PIN. Jeśli mamy wybór, zawsze bezpieczniej jest używać haseł niż numerycznych kodów. Trzeba pamiętać, że kosztem zastosowania szyfrowania jest niewielki spadek wydajności systemu z powodu konieczności użycia dodatkowych zasobów, a także potrzeba odpowiedniego dbania o klucz szyfrujący.

Zasada szyfrowania danych obowiązuje także przy przechowywaniu ich poza urządzeniem – na dyskach przenośnych czy w chmurze. W takim przypadku należy w pierwszej kolejności rozważyć pełne szyfrowanie dysku, a jeśli jest to niemożliwe lub niepraktyczne, zaszyfrować konkretne pliki lub foldery.

2.8.5. Dostępność systemów i aplikacji. Kopie zapasowe

Operator IK powinien w sposób proporcjonalny i adekwatny zadbać o dostępność eksploatowanych systemów i aplikacji. Jednym z niezbędnych elementów tego procesu dla praktycznie wszystkich systemów jest uwzględnienie wykonywania kopii zapasowych. Działania można podzielić na część związaną z projektowaniem oraz na część związaną z eksploatowaniem systemów i aplikacji.

Dostępność (ang. *availability*[56]) można osiągnąć poprzez:

a. Eliminację pojedynczych punktów awarii (ang. *Single Point of Failure*), czyli części systemu teleinformatycznego, którego awaria powoduje zatrzymanie całości systemu.
b. Stosowanie redundancji na różnych poziomach (patrz dalej)[57].
c. Natychmiastowe usuwanie awarii przez obsługujących system. Jeśli w zdublowanym (redundantnym) systemie jeden z elementów jednej kopii ulegnie awarii to należy taką awarię natychmiast usunąć. Z punktu widzenia użytkownika systemu interwencja nie będzie widoczna. Przykładem może być wymiana dysku w macierzy RAID lub zmiana operatora telekomunikacyjnego.

Pomiar dostępności systemów lub ocenę dostępności systemów można prowadzić poprzez określenie SLA z pomocą procentu czasu dostępności. Poglądowe wartości przedstawia tabela poniżej:

Tabela 8 Poziomy dostępności w zależności od poziomu SLA

Poziom SLA	Niedostępność w skali roku	Niedostępność w ciągu dnia
99%	3,65 dnia	14,40 min
99,9%	8,77 h	1,44 min

[56] W języku polskim dwa całkowicie różne terminy są określane jako dostępność. Tu omawiamy pojęcie określone w jęz. angielskim jako „*availability*" czyli możliwość niezakłóconej eksploatacji systemu. Innym pojęciem jest „*accessibility*", które oznacza możliwość wykorzystania urządzenia/systemu/aplikacji przez wszystkich potencjalnych użytkowników, w tym w szczególności dla osób o różnym stopniu niepełnosprawności.

[57] Uwaga: bardzo często w literaturze traktuje się miejsce połączenia dwóch kopii systemów jako szczególny rodzaj pojedynczego punktu awarii, co oznacza, że właśnie ten fragment infrastruktury i aplikacji powinien być szczególnie starannie przygotowany.

99,95%	4,38 h	43,2 s
99,99%	52,6 min	8,64 s
99,999%	5,26 min	864 ms

Jest oczywiste, że wzrost wymagań związanych z dostępnością przekłada się na cenę rozwiązania, przy czym im wyższe wymagania tym wzrost przestaje być liniowy, a cena rośnie niezwykle szybko. Zaleca się staranne określenie parametru dostępności i adekwatności założonego parametru do potrzeb, ponieważ również dalsza eksploatacja i utrzymanie wysokiej dostępności może być niezwykle kosztowne.

Przy określaniu całkowitej dostępności należy pamiętać, że jest ona iloczynem wartości składowych tzn. jeśli mamy dwa elementy systemu, które trzeba rozpatrywać łącznie, pierwszy o dostępności 99,999%, a drugi o dostępności 99% to dostępność całego systemu wynosi tylko 98,99%. Stawia to pod znakiem zapytania architekturę systemu w sytuacji kiedy osiągnięta wysokim kosztem dostępność „pięciu dziewiątek" zostanie zniwelowana przez drugi komponent systemu.

W przypadku korzystania z zewnętrznych dostawców warto sprawdzić nie tylko deklarowaną (kontraktową) wartość dostępności, ale także – jeśli takie dane są dostępne – dotychczasową praktykę. Dla renomowanych dostawców rzeczywisty poziom dostępności powinien być wyższy od deklarowanego.

Dla oceny wprowadzania odpowiednich rozwiązań zwiększających odporność i dostępność systemów teleinformatycznych warto wykorzystać poniższą tabelę:

Tabela 9 Dobór rozwiązań w zależności od rodzaju awarii

Rodzaj awarii	Przykład	Przykłady rozwiązań
Awaria pojedynczego elementu systemu	Awaria dysku Awaria sterownika dysku	Wykorzystanie dysków o wysokim parametrze MTTF (niekiedy MTBF)[58] Macierz RAID Dublowanie sterowników
Awaria jednego systemu	Awaria serwera	Kopia systemu w tym

[58] MTTF – ang. Mean Time To Failure – średni czas pracy do awarii; MTBF – ang. Mean Time Between Failure, średni czas pomiędzy awariami. Dla serwerów zazwyczaj stosuje się dyski o podwyższonym parametrze MTTF/MTBF. Należy pamiętać, że jest to wartość statystyczna podawana przez producentów i nie chroni przed awarią.

		samym centrum przetwarzania
Awaria centrum przetwarzania	Blackout Awaria sieci dostępowej Lokalna katastrofa naturalna Lokalny atak terrorystyczny	Redundancja systemów zasilania Kilku dostawców sieci Kopia systemu w kilku centrach przetwarzania Ewakuacja do chmury publicznej (kopia chmurowa) – patrz p. 5.5
Katastrofa o wielkiej skali	Kryzys energetyczny w skali państwa Skoordynowane ataki terrorystyczne Wojna Katastrofa naturalna w wielkiej skali	Kopia chmurowa, w tym także poza granicami państwa, także: na innej płycie tektonicznej Ewakuacja do chmury publicznej

Ocena zagrożenia pozwoli na prawidłowe określenie docelowej dostępności i odporności systemu teleinformatycznego. Należy przy ocenie posłużyć się listą zagrożeń znajdującą się w rozdziale 2.8.3.3. Rodzaje zagrożeń.

Niezbędnym elementem planu uzyskania wysokiej odporności i dostępności systemów operatora IK jest przygotowanie procesu tworzenia kopii zapasowych (ang. *backup*). Przy planowaniu takiego procesu należy wziąć pod uwagę przedstawione wcześniej możliwości podniesienia dostępności oraz dwa parametry związane z wykonywaniem backupu.

a. RTO (ang. Recovery Time Objective) – maksymalny akceptowalny czas braku dostępności systemu
b. RPO (ang. Recovery Point Objective) – maksymalny akceptowalny czas, podczas którego dane wprowadzone do systemu zostały utracone

Należy przyjąć, że zapewnienie innymi środkami wysokiej odporności i dostępności systemu nie zwalnia operatora od wykonania kopii zapasowych. Ich wykonanie może być związane z wykorzystaniem infrastruktury własnej, infrastruktury hostowanej lub chmury publicznej.

Jako minimum zabezpieczenia należy przyjąć, że kopia zapasowa – bez względu na zastosowany nośnik - musi być fizycznie oddalona od systemu w zależności oceny niezbędnej ochrony fizycznej (por. tabela zagrożeń powyżej)! Analiza innych zagrożeń (por. rozdział 4.3) powinna doprowadzić do właściwego zabezpieczenia i przechowywania kopii zapasowych.

Dla celów archiwizacyjnych, jak i dla celów rozliczalności procesów, zarówno wynikających z przepisów prawa, jak i z wewnętrznych polityk retencji, operator IK powinien przygotować politykę tworzenia i przechowywania więcej niż jednej kolejnej kopii zapasowej.

Rekomendowane jest, aby w kontekście danych o krytycznym znaczeniu, należy zastosować dodatkowe metody składowania kopii zapasowych (np. w chmurze innego dostawcy lub on-premises).

2.8.6. Plan Ewakuacji do Chmury Obliczeniowej

Doświadczenia z wojny w Ukrainie wykazały, że informatyczne aktywa operatorów IK stały się obiektem hybrydowego ataku obejmującego m.in. zagrożenia cybernetyczne i fizyczne. Praktycznym rozwiązaniem była ewakuacja zasobów, danych i systemów do chmury obliczeniowej, w szczególności do chmury znajdującej się poza terytorium państwa. Liczne przykłady pokazały, że takie przeniesienie zasobów może zostać wykonane szybko i sprawnie, także w warunkach wojennych, choć przy braku wcześniejszego przygotowania rozwiązania techniczne nie będą optymalne i można napotkać wiele problemów. Aby proces ewakuacji został przeprowadzony sprawnie zaleca się przygotować Plan Ewakuacji poprzedzając go opisanym poniżej procesem przygotowawczym. **Plan Ewakuacji** do chmury obliczeniowej powinien być integralną częścią planu ochrony IK.

Operator IK przygotowując Plan Ewakuacji do Chmury Obliczeniowej w pierwszej kolejności powinien ocenić z jakiej chmury będzie mógł skorzystać, m.in. z chmury rządowej, chmury typu community lub chmury publicznej. W przypadku wyboru chmury innej niż chmura publiczna operator IK powinien uzgodnić z zarządzającymi chmurą formalne i fizyczne możliwości takiej migracji, tak aby niezbędne zasoby były dostępne dla tego operatora. Plan Ewakuacji w takim przypadku powinien być wspólnie przygotowany lub formalnie sprawdzony i potwierdzony przez zarządzających chmurą rządową lub chmurą typu community. W przypadku, kiedy ewakuacja do chmury rządowej lub chmury typu community nie będzie możliwa z przyczyn formalnych, organizacyjnych lub technicznych, należy przygotować plan ewakuacji do chmury publicznej. W dalszej części rozdziału omówiona została przede wszystkim zasady przygotowania Planu Ewakuacji do chmury publicznej ponieważ ocena możliwości i ocena dostawców chmury publicznej może być przygotowana przez

operatora IK bez konieczności współpracy z dostawcą lub – przy spełnieniu wszystkich kryteriów – do rzeczywistej ewakuacji może być wybranych kilku dostawców.

Korzyści związane z ewakuacją do chmury obliczeniowej:

a. Natychmiastowa dostępność – proces ewakuacji może zostać rozpoczęty natychmiast po rozpoznaniu zagrożenia lub po ogłoszeniu przez właściwe organy odpowiedniego alertu,
b. Bezpieczeństwo – renomowani dostawcy chmury obliczeniowych zapewniają bezpieczeństwo i ochronę często na wyższym poziomie niż ma to miejsce w infrastrukturze własnej operatorów IK,
c. Rozproszenie pod kontrolą operatora IK – można zdecydować w jakiej lokalizacji znajdą się poszczególne systemy i dane; nawet wykorzystanie jednej lokalizacji (jednego regionu) publicznej chmury obliczeniowej zwiększy bezpieczeństwo, jednak Plan Ewakuacji może przewidywać dalsze rozproszenie (w tym tworzenie celów pozornych), co stanie się dodatkowym utrudnieniem dla atakującego,
d. Wybór – operator może wybierać spośród wielu dostawców chmury publicznej; firmy chmurowe z państw NATO i UE, a także polskie firmy, które są liderami technologicznymi,
e. Skalowalność – zasoby dostawców chmur obliczeniowych znacznie przewyższają potrzeby wszystkich operatorów IK jednocześnie, [59]
f. Elastyczność i zarządzanie procesem ewakuacji – do decyzji operatora IK pozostaje co, w jaki sposób i na jak długo zostanie przeniesione do chmury publicznej.

Przygotowanie **Planu Ewakuacji** do chmury publicznej należy rozpocząć od przygotowania oceny możliwości oraz niezbędnych środków (proces przygotowawczy). W przypadku dostępności wystandaryzowanych i wstępnie przygotowanych materiałów, listy pytań i procedur należy z nich skorzystać.

Proces przygotowawczy – zasoby własne

a. Personel – należy co najmniej dokonać oceny:
   - zasobów własnych (personel, kwalifikacje) niezbędnych do przeprowadzenia ewakuacji,
   - możliwości pozyskania dodatkowego personelu zewnętrznego, zwłaszcza w sytuacji kryzysowej dotykającej jednocześnie większej liczby podmiotów,

[59] Przykładem skalowalności chmur obliczeniowych było przejście w czasie pandemii z pracy w zakładach i szkołach do pracy on-line. W ciągu dosłownie dni i tygodni całe branże przeniosły się z działaniami do chmury obliczeniowej. Szacuje się, że od marca do czerwca 2020 r. tylko w edukacji liczba osób codziennie korzystających z pracy i nauki on-line na platformach chmurowych wzrosła z kilkunastu tysięcy do ponad pięciu milionów!

- dostępności procesów podnoszenia kwalifikacji personelu w zakresie działania z chmurami obliczeniowymi,
- dostępności procesu podnoszenia kwalifikacji personelu odpowiedzialnego za bezpieczeństwo w zakresie bezpieczeństwa chmur obliczeniowych.

b. Aplikacje – należy co najmniej dokonać oceny warunków prawnych (w tym licencyjnych), organizacyjnych i technicznych:
   - możliwości migracji aktualnie wykorzystywanych aplikacji i systemów do technologii stosowanych w chmurze obliczeniowej (np. przeniesienie aplikacji do chmury prywatnej, konteneryzacja, także: migracja do chmury publicznej),
   - możliwości wdrażania nowych rozwiązań z wykorzystaniem technologii stosowanych w chmurze publicznej obliczeniowej, w tym w chmurze publicznej,
   - (jeśli rozwiązania chmurowe są już eksploatowane przez operatora) możliwości zmiany lokalizacji (zmiany regionu chmurowego) dla danej aplikacji i proces temu towarzyszący; należy zwrócić uwagę na potencjalną zmianę dostawcy np. dostawcy krajowego posiadającego centra przetwarzania danych wyłącznie na terenie RP na dostawcę międzynarodowego.

b. Dane – należy co najmniej dokonać oceny warunków prawnych, organizacyjnych i technicznych:
   - warunków przetwarzania w publicznej chmurze obliczeniowej, w szczególności dla danych osobowych,
   - dodatkowych zabezpieczeń danych przetwarzanych w publicznej chmurze obliczeniowej, m.in. wymaganych sposobów szyfrowania, wymaganych sposobów przechowywania kluczy,
   - dodatkowych zabezpieczeń w postaci chmurowych kopii zapasowych.

c. Uwierzytelnienie – należy co najmniej dokonać oceny:
   - możliwości ujednolicenia uwierzytelnienia dla aktualnego i chmurowego rozwiązania,
   - sprawdzenie możliwości wykorzystania wieloskładnikowego uwierzytelniania,
   - narzędzi monitorowania dostępu użytkowników.

d. Inne
   - wyłączyć z Planu Ewakuacji systemy przetwarzające informacje niejawne,[60]

[60] W aktualnym stanie prawnym nie jest możliwe przetwarzanie informacji niejawnych w publicznej chmurze obliczeniowej; należy jednak być gotowym do potencjalnego przeniesienia także systemów przetwarzających informacje ZASTRZEŻONE jeśli w warunkach zagrożenia prawo uległoby zmianie lub czasowemu zawieszeniu; warto dodać, że niektóre kraje UE dopuszczają przetwarzanie informacji niejawnych w chmurach publicznych po zweryfikowaniu aplikacji, określeniu wymagań organizacyjno-technicznych i nadaniu odpowiedniego certyfikatu.

- określić minimalny czas utrzymania zdublowanych zasobów w chmurze (służy do określenia potencjalnych kosztów utrzymania po ewakuacji),
- dokonać przeglądu i oceny aktualnych kontraktów serwisowych i suportowych z dostawcami technologii IT.

Proces przygotowawczy – ocena dostawców chmury publicznej

Operator IK dokonuje analizy ryzyka i oceny dostawców chmury publicznej. W przypadku dostępności rekomendacji[61] lub arkusza ryzyka i oceny wstępnie przygotowanego przez właściwego regulatora należy zastosować ten dokument lub weryfikując co najmniej pozycje zgodne z przedstawioną poniżej listą. Proces analizy ryzyka i oceny powinien być sformalizowany i udokumentowany. W przypadku braku rekomendacji właściwych dla sektora operator IK może korzystać z rekomendacji dostępnych dla innych sektorów, traktując je jako zbiór dobrych praktyk

Zaleca się tworzenie analizy w zespole złożonym z przedstawicieli działu IT, bezpieczeństwa, Inspektora Ochrony Danych, działu finansów oraz działu prawnego (m.in. dla celów określenia prawnego ryzyka ewakuacji do chmury zlokalizowanej w krajach trzecich). Należy pamiętać, że wymagania formalne związane z procesami ewakuacji do chmury obliczeniowej dotyczą sytuacji kryzysowej, a zatem mogą być inne niż nakładane na rozwiązanie chmurowe w normalnej sytuacji. Można przyjąć, że rozwiązanie chmurowe, które wypełniają kryteria dla normalnej sytuacji będą także odpowiadały wymaganiom kryzysowym.

Ocena ryzyka może być inna dla różnych systemów i aplikacji przy takiej samej informacji od dostawcy chmury obliczeniowej (przykład: lokalizacja centrum przetwarzania danych w kraju UE, który nie jest członkiem NATO np. w Austrii, może być dla pewnych scenariuszy istotniejsza, zaś lokalizacja CPD w kraju będącym członkiem NATO, który nie jest członkiem UE, np. Kanada, może być ważniejsza, jeśli ze względów bezpieczeństwa będzie wskazane stworzenie duplikatu aplikacji poza kontynentem europejskim).

Analiza oferty chmury publicznej

a. Dostawca udostępnia, także w formie elektronicznej, sformalizowaną umowę oraz inne dokumenty takie jak warunki korzystania z usług, regulaminy, certyfikaty zgodności z normami, raporty poaudytowe, itd.,
b. Dokumenty pozwalają na jednoznaczne określenie prawa właściwego dla umowy z dostawcą chmury publicznej,
c. Dokumenty pozwalają na jednoznaczny podział odpowiedzialności w zakresie bezpieczeństwa, ciągłości świadczenia usług, poziomu SLA,

[61] Przykładem rekomendacji regulatora, tu: dla sektora finansowego, może być „Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej" z 23 stycznia 2020 r.

d. Dokumenty lub narzędzia administratora[62] pozwalają na określenie lokalizacji centrum[63] przetwarzania danych dostawcy[64],
e. Dokumenty pozwalają na jednoznaczne określenie własności przetwarzanych danych w trakcie umowy, jak i po jej zakończeniu,
f. Dokumenty pozwalają na zapoznanie się z listą poddostawców (jeśli istnieją) oraz wskazują na sposób komunikacji w przypadku dodawania nowych poddostawców,
g. Dokumenty w sposób jednoznaczny wskazują, że możliwy jest audyt dostawcy, a także że dostawca regularnie poddaje się audytom wykonywanym przez niezależne firmy audytorskie, co potwierdzone jest odpowiednimi certyfikatami – zalecana jest weryfikacja zgodności z co najmniej następującymi normami:
    - ISO 27001 – zarządzanie bezpieczeństwem informacji,
    - ISO 27017 – rozszerzenie ISO 27001 dla chmury obliczeniowej,
    - ISO 27018 i/lub ISO 27701 – zarządzanie i ochrona danych osobowych w chmurze obliczeniowej,
    - ISO 22301 – zachowanie ciągłości świadczenia usługi,
    - SOC 1 i SOC 2,
    - ISO 50600 min. klasy 3 (wyposażenie i infrastruktura centrów przetwarzania danych) lub ANSI-TIA 942 co najmniej Tier 3[65],
    - (opcjonalnie) NIST 800-53 co najmniej R4[66].
h. Dostawca stosuje zasady ZeroTrust[67], w szczególności:
    - domyślną zasadę braku dostępu do informacji użytkownika chmury,
    - domyślną zasadę braku konta administratora w uruchamianych zasobach (dostęp jest udzielany na określony czas, w niezbędnym zakresie uprawnień),

[62] Wielu dostawców chmury publicznej umożliwia użytkownikom wybór centrum przetwarzania danych lub wybór regionu – ostateczna decyzja jest podejmowana przez samego użytkownika.

[63] Dostawcy chmury publicznej posługują się często określeniem „region", czyli obszar, na którym znajdują się co najmniej dwa (zazwyczaj trzy) centra przetwarzania danych, w których odbywa się przechowywanie i przetwarzanie danych; region chmury publicznej zazwyczaj pokrywa się z granicami państwa, chociaż w większych państwach często znajduje się więcej niż jeden region.

[64] Precyzyjne wskazanie adresu centrum/centrów przetwarzania danych jest rzadko udostępniane ze względów bezpieczeństwa – minimalnym wymaganiem jest wskazanie kraju, w którym znajduje się CPD lub region dostawcy chmury publicznej.

[65] Jeśli jest stosowane przez dostawców chmury obliczeniowej – jeśli nie należy zweryfikować stosowanie norm SOC 1 i SOC 2.

[66] Polskie Standardy Cyberbezpieczeństwa Chmury Obliczeniowej (SCCO) są *de facto* przetłumaczonymi na język polski zapisami normy NIST 800-53 R5.

[67] Porównaj punkt 4.1. Także: potencjalną weryfikacją jest posiadanie przez dostawcę normy NIST 800-207, jednak nie jest to jeszcze powszechnie stosowana norma, w szczególności w Europie (NIST są normami amerykańskimi).

- szyfrowanie danych, zarówno podczas przechowywania („at rest"), jak i przesyłu („in transit") – zalecane jest sprawdzenie dostępnych metod szyfrowania informacji,
- możliwość wprowadzenia wieloskładnikowego uwierzytelnienia
- ogranicza dostęp na poziomie sieci tylko do koniecznych połączeń,
- ogranicza dostęp na poziomie urządzeń tylko dla urządzeń dopuszczonych.

i. Dostawca (opcjonalnie) umożliwia połączenie z chmurą za pomocą dedykowanych łączy,
j. Dostawca posiada plan ciągłości świadczenia usługi,
k. Dostawca umożliwia i rekomenduje budowę dedykowanych planów ciągłości działania na poziomie aplikacji i rozwiązań,
l. Dostępne są do decyzji operatora IK metody i narzędzia podnoszące odporność systemu w chmurze (redundancje, duplikacje w różnych regionach),
m. Dostawca posiada oddział w Polsce (zalecane),
n. Dostawca oferuje usługi profesjonalne mogące wspierać proces ewakuacji,[68] w szczególności program wsparcia technicznego (zalecane),
o. Dostawca ma program podnoszenia kwalifikacji dostępny w Polsce tj. szkolenia, centra szkoleniowe, certyfikowani trenerzy, formalne certyfikaty (zalecane).

Rekomenduje się przygotowanie i włączenie do planu ochrony IK **Planu Ewakuacji do Chmury Publicznej**, zawierającego co najmniej:

a. Listę systemów i aplikacji, które powinny zostać przeniesione do chmury (zdublowane w chmurze) oraz danych z nimi związanych,
b. Określenie priorytetów (kolejności) ewakuacji systemów i aplikacji,
c. Określenie zakresu migracji dla poszczególnych pozycji z listy, od minimum chmurowego backupu (kopii danych), do pełnej funkcjonalności systemu lub aplikacji serwowanego z chmury (pełna ewakuacja),
d. (Jeśli niezbędne) Określenie dodatkowych narzędzi zwiększających odporność i bezpieczeństwo dla poszczególnych pozycji z listy,
e. Skład osobowy zespołu odpowiadającego za ewakuację ze wskazaniem ról i odpowiedzialności poszczególnych członków zespołu,

[68] Jeśli wymaga tego specyfika procesu ewakuacji dla niektórych systemów i aplikacji to zalecane jest zweryfikowanie posiadania przez dostawcę pracowników usług profesjonalnych z odpowiednimi poświadczeniami bezpieczeństwa, jak również posiadanie przez dostawcę świadectwa bezpieczeństwa przemysłowego.

f. W szczególności w zespole odpowiadającym za ewakuację musi zostać wskazana osoba (osoby) odpowiedzialne za kontakt z dostawcą publicznej chmury obliczeniowej i nadzorujące realizację zadań,
g. Listę personelu zewnętrznego niezbędnego lub zalecanego dla wykonania procesu ewakuacji, w tym w szczególności możliwość uzyskania profesjonalnego wsparcia ze strony dostawcy oraz dostawców dziedzinowych, jeśli jest taka konieczność,
h. Wstępny wybór krajów oraz regionów dostawcy chmurowego, do których przewiduje się ewakuację[69],
i. Wskazanie co najmniej dwóch dostawców chmury publicznej (pierwszy wybór, drugi wybór) wybranych na podstawie oceny dostawców wykonanej w fazie przygotowawczej,
j. Wstępne oszacowanie czasu i kosztów ewakuacji,
k. Oszacowanie potrzeb wewnętrznych w okresie 12 miesięcy od sporządzenia Planu mających na celu podniesienie pewności wykonania ewakuacji, w szczególności program podnoszenia kwalifikacji personelu, ćwiczenia ewakuacji, wskazanie systemów i aplikacji, które powinny zostać lepiej dostosowane do potrzeb ewakuacji, zmiana licencji dla oprogramowania (jeśli niezbędne), itd.

Dokumentacja z procesu przygotowawczego nie musi być włączona do **Planu Ewakuacji do Chmury Publicznej,** jednak powinna być dostępna dla celów powtórnej weryfikacji. Zaleca się wykonanie ćwiczenia polegającego na ewakuacji do chmury systemów nieprodukcyjnych. Zaleca się weryfikację i odnowienie Planu Ewakuacji nie rzadziej niż co dwa lata.

2.8.7. Oprogramowanie

Zasady zapewnienia bezpieczeństwa oprogramowania opierają się na uniwersalnych zasadach, które dotyczą również zapewnienia bezpieczeństwa dla innych zasobów teleinformatycznych, a przede wszystkim systemu operacyjnego.

Najważniejszymi elementami (filarami) zapewnienia bezpieczeństwa oprogramowania są:

- testowanie oprogramowania w wydzielonym środowisku, przed wdrożeniem produkcyjnym,
- aktualizacja systemu operacyjnego,
- aktualizacja oprogramowania,
- testowanie zmian wynikających z aktualizacji,
- audyt bezpieczeństwa kodu,

[69] W przypadkach kryzysowych właściwe organy państwa mogą wskazać preferowane kierunki ewakuacji.

- współpraca z dostawcą oprogramowania.

Rysunek 14 Podstawowe elementy bezpieczeństwa oprogramowania.

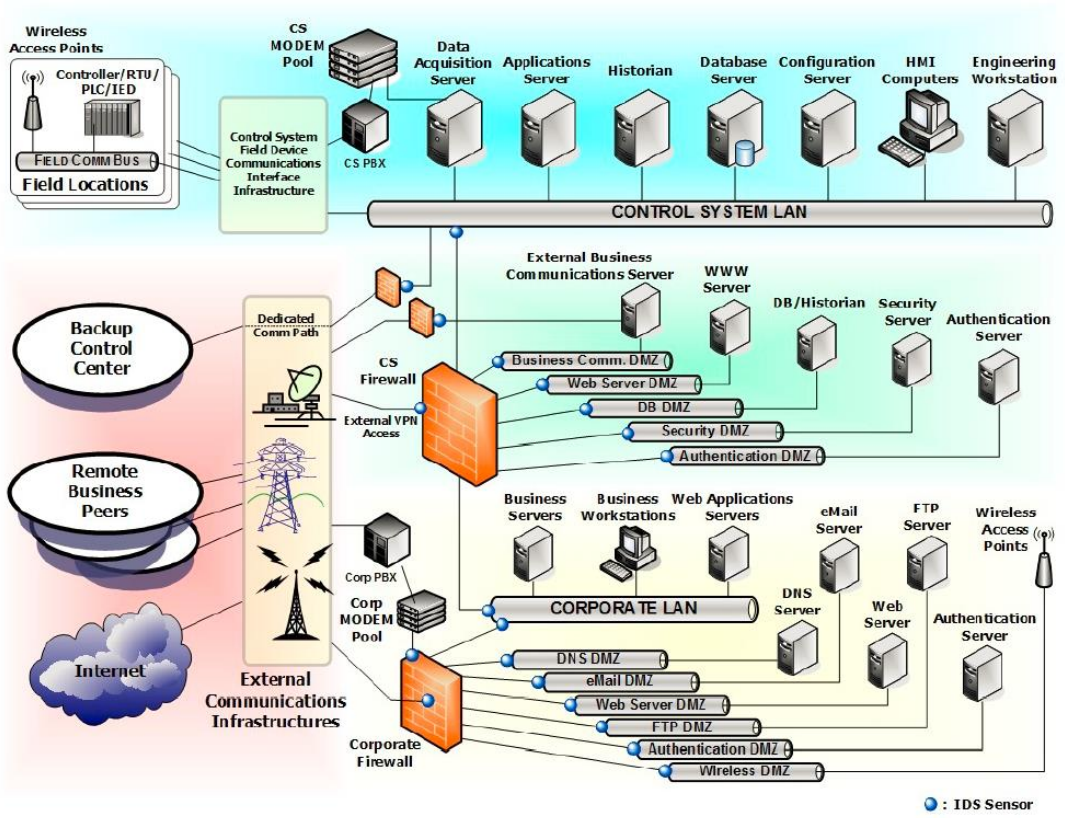
2.8.8. Infrastruktura

2.8.8.1. Sieci i architektura

Separacja sieci bezpośrednio obsługującej IK od podstawowej internetowej sieci organizacji (fizyczna i logiczna)

Zarówno przy pomocy wirtualnych sieci lokalnych, jak i firewallingu, możemy stworzyć rozwiązanie polegające na separacji sieci bezpośrednio obsługującej IK organizacji. Jako sieć bezpośrednio obsługującą IK rozumiemy tę część sieci organizacji, w której przetwarzane są kluczowe dane i obsługiwane są obiekty, urządzenia, instalacje stanowiące właściwą IK. Ta część sieci powinna podlegać szczególnej ochronie, dlatego w praktyce powinniśmy zastosować wszystkie z omawianych zabezpieczeń w sposób dodatkowy właśnie wobec tej części sieci. Konfiguracja tych zabezpieczeń powinna być realizowana na najwyższym i najbardziej restrykcyjnym poziomie.

W celu zapewnienia separacji sieci IK od pozostałych sieci organizacji, rekomenduje się implementację segmentacji sieci zgodnie z modelem przedstawionym poniżej (po dostosowaniu do potrzeb danej organizacji).



Rysunek 15 Model segmentacji sieci[70].

Powyższy model zakłada utworzenie odseparowanych od siebie stref bezpieczeństwa. Komunikacja pomiędzy strefami jest kontrolowana i ograniczona w stopniu odpowiadającym poziomowi bezpieczeństwa wymaganemu dla danej strefy. Systemy automatyki (rozumiane, jako systemy SCADA, DCS, urządzenia warstwy sterowania oraz aparatura kontrolno-pomiarowa) powinny być objęte najwyższym poziomem bezpieczeństwa ze względu na ich bezpośredni wpływ na ciągłość działania IK.

Pomiędzy sieciami IK, a pozostałymi sieciami należy umieścić dodatkowy, pośredniczący segment sieci (DMZ). Cały ruch do i z sieci IK powinien przebiegać z wykorzystaniem rozwiązań pośredniczących umieszczonych w tym segmencie (np. serwerów przesiadkowych, dedykowanych baz danych, serwerów plików). Jakiekolwiek bezpośrednie połączenia pomiędzy siecią IK a pozostałymi sieciami organizacji, z pominięciem segmentu DMZ powinny być blokowane.

Cały ruch sieciowy przepuszczany do segmentu DMZ oraz z tego segmentu do sieci aktywów IK powinien być ściśle kontrolowany w wykorzystaniem zapór ogniowych. Dodatkowo, w celu ochrony przed atakami oraz wykrywania złośliwego

[70] Publikacja NIST 800-82 Wer. 1.

oprogramowania, ruch w sieci powinien być kontrolowany z wykorzystaniem rozwiązań typu IDS/IPS.

2.8.8.2. *Sieci bezprzewodowe*

Sieci bezprzewodowe ze względu na łatwość budowy i konfiguracji oraz wygodę użycia są bardzo rozpowszechnione. Wykorzystanie sieci bezprzewodowych, bez zastosowania odpowiednich zabezpieczeń, niesie ze sobą duże zagrożenia, w szczególności możliwość:

- nielegalnego wykorzystania tych sieci do działań przestępczych,
- nieuprawnionego dostępu do informacji innych podmiotów.

Coraz powszechniej bezprzewodowa komunikacja znajduje zastosowanie w środowisku automatyki, szczególnie w przypadku opomiarowania obiektów, gdzie konieczne jest przesyłanie danych na duże odległości. Należy wtedy zwrócić szczególną uwagę na bezpieczeństwo przesyłanych danych, których przechwycenie lub w których ingerencja może mieć bezpośredni wpływ na proces technologiczny.

Warto również zwrócić uwagę, że bezpieczeństwo sieci bezprzewodowych powinniśmy rozpatrywać nie tylko z punktu widzenia własnych sieci, ale również sieci obcych, wykorzystywanych przez pracowników naszej organizacji.

Ochrona własnej sieci bezprzewodowej

Analizując bezpieczne korzystanie z sieci bezprzewodowych, należy wziąć pod uwagę następujące filary bezpieczeństwa:

(1) **Separacja ruchu z sieci bezprzewodowych**

Wyłączenie komunikacji z sieci bezprzewodowych do sieci obsługujących IK lub zasobów stanowiących IK jest skutecznym sposobem zmniejszenia ryzyka zakłócenia funkcjonowania IK.

(2) **Szyfrowanie komunikacji**

W sieciach bezprzewodowych powinno być stosowane szyfrowanie komunikacji. Najpopularniejszymi standardami szyfrowania są standardy WPA/WPA2/WPA3 (*Wi-Fi Protected Access*). Standardy WPA2 i WPA3 są standardami bezpieczniejszymi i one są rekomendowane. WPA3 wnosi szereg zmian w porównaniu do swoich poprzedników. Najważniejsze z nich to:

- Zmiana a w zasadzie całkowite zastąpienie TKIP/AES, szyfrowaniem SAE
- Praktycznie wyeliminowanie problemu ataku typu KRAK
- Szyfrowanie WPA 3 Enterprise 192 bit
- Szyfrowanie WPA 3 Personal 128bit

- Ochrona przed atakami Brute Force - Automatyczna blokada przy słownikowej próbie złamania hasła
- Zgodność z poprzednimi wersjami (WPA/WPA2)
- Możliwość korzystania z krótszych kluczy zabezpieczających

(3) **Rozgłaszanie identyfikatora sieciowego**

Podstawą cyberataku na sieć bezprzewodową jest wykrycie tej sieci, dlatego wyłączenie rozgłaszania tzw. SSID sieci (*service set identifier*), choć nie zapewni pełnego bezpieczeństwa, z pewnością utrudni skuteczny cyberatak.

(4) **Kontrola dostępu na podstawie adresu MAC**

Zezwolenie na dołączenie do sieci bezprzewodowej tylko tych urządzeń, których adres fizyczny MAC został wcześniej wpisany jako adres dozwolony. Pozwala to na zmniejszenie prawdopodobieństwa dołączenia się do sieci nieautoryzowanych urządzeń sieciowych bez zastosowania specjalistycznych technik nielegalnego podszywania się pod wybrany adres MAC.

(5) **Fizyczne ograniczenie dostępu do sieci**

Poprawa bezpieczeństwa sieci bezprzewodowych w organizacji możliwa jest również przez fizyczne ograniczenie dostępu do sieci tzn. takie kształtowanie sygnału radiowego, aby był on dostępny tylko i wyłącznie z wybranych lokalizacji. Należy unikać sytuacji, w której sygnał jest skierowany w głównej mierze na zewnątrz lokalizacji informacji. Prowadzenie odpowiedniego monitoringu zagrożeń[71] pozwoli na wykrywanie nieuprawnionych prób dostępu.

Bezpieczne korzystanie z sieci bezprzewodowej innych podmiotów

Oprócz zapewnienia bezpiecznego korzystania z własnej sieci bezprzewodowej ważne jest, aby korzystanie z sieci innych podmiotów również odbywało się w sposób bezpieczny. Z takich sieci korzystają głównie pracownicy, którzy w danej chwili znajdują się poza obszarem organizacji. Najlepszą praktyką jest, aby nie pozwalać na to, by w ten sposób dostawali się oni do sieci organizacji, w której znajduje się IK. Również jeśli korzystają oni z urządzeń przenośnych, które po podłączeniu do sieci lokalnej w organizacji, mają dostęp do krytycznych zasobów, to urządzenia te nie powinny mieć wcześniej dostępu do obcych sieci (zarówno bezprzewodowych, jak i stałych).

We wszystkich innych przypadkach, w których pozwalamy na dostęp do obcej sieci bezprzewodowej z urządzeń służbowych lub w celach służbowych, powinny obowiązywać pracowników następujące zasady:

- powinni oni korzystać tylko i wyłącznie ze znanych im sieci bezprzewodowych (np. znanego operatora telekomunikacyjnego),
- powinni oni korzystać tylko i wyłącznie z szyfrowanych sieci bezprzewodowych (WPA/WPA2),
- łączenie do zasobów organizacji (np. poczta elektroniczna) powinno się odbywać tylko i wyłącznie za pomocą wydzielonego, szyfrowanego kanału VPN[72],
- w przypadku niekorzystania z sieci bezprzewodowych powinni oni wyłączać bezprzewodową kartę sieciową zainstalowaną w urządzeniu przenośnym.

2.8.8.3. *Monitoring zdarzeń*

Niezależnie od tego, jak silnie będzie zabezpieczona nasza sieć teleinformatyczna, możliwość przeprowadzenia skutecznego cyberataku na nią zawsze istnieje. Dlatego organizacja powinna prowadzić stały monitoring zagrożeń.

Rodzaje systemów monitorujących

Następujące rodzaje urządzeń można wykorzystać do organizacji systemu monitoringu zagrożeń i wczesnej reakcji na ich wystąpienie:

- Systemy detekcji zagrożeń sieciowych IDS (ang. *Intrusion Detection System*)

  Są to systemy wykrywania cyberataków w czasie rzeczywistym. Wykrycie to następuje w oparciu o znany sieciowy wzorzec cyberataku (tzw. sygnaturę) lub wykrycie anomalii w ruchu sieciowym. Zaletą takich systemów jest to, że potrafią one wykryć cyberataki, które są w stanie przeniknąć przez zabezpieczenie typu zapora sieciowa, dzięki bardziej szczegółowej analizie pakietów sieciowych (np. robaki sieciowe, cyberataki na serwisy i aplikacje czy nieuprawnione próby logowania). Typowy system IDS składa się z systemu centralnego, jednej lub wielu sond oraz bazy danych, w której odbywa się przetwarzanie zebranych logów. Możliwe jest zastosowanie dwóch rodzajów systemów typu IDS:

  - HIDS (ang. *Host Based Intrusion Detection System*) – system wykrywania zagrożeń sieciowych przeznaczony dla wybranych urządzeń (np. kluczowych serwerów),
  - NIDS (ang. *Network Intrusion Detection System*) – system wykrywania zagrożeń sieciowych przeznaczony dla wybranych sieci (może być, np. zlokalizowany na styku sieci lokalnej z Internetem).
- System zapobiegania włamaniom IPS (ang. *Intrusion Prevention System*)

System taki jest podobnym systemem do IDS, z tym samym podziałem na systemy instalowane na konkretnym urządzeniu (HIPS) oraz w sieci (NIPS). Podstawowa

[72] Patrz punkt 2.8.3.4 Kontrola dostępu (dostęp z zewnątrz).

różnica polega na tym, że o ile IDS alarmuje o zagrożeniu, to system IPS jest w stanie podjąć aktywną akcję związaną z ochroną systemu, np. zablokować ruch z konkretnego adresu źródłowego.

Systemy IDS i IPS mogą być używane komplementarnie. W przypadku decyzji o używaniu obydwu systemów, dobrą praktyką jest umieszczanie systemu IPS na styku sieci, tak aby chronił on aktywnie przed najróżniejszymi nowymi cyberatakami, w tym cyberatakami, które dopiero co się w sieci pojawiły i nieznane są jeszcze ich sygnatury, a detekcja odbywa się przez wykrycie anomalii (tzw. *o-day attacks*). Natomiast system IDS może być używany głównie wewnątrz sieci, za zaporą ogniową tak, aby monitorował i alarmował o nadużyciach w sieci wewnętrznej bez aktywnego działania blokującego. Do rozważenia pozostaje również wdrożenie narzędzia klasy SIEM *(Security Information and Event Management*), zbierającego informacje ze wszystkich istotnych systemów, potrafiący korelować zdarzenia z różnych systemów i wykrywać anomalie zachowań.

Zasady monitoringu

Monitoring zagrożeń powinien zostać zorganizowany dla ochrony kluczowych zasobów firmy. Standardowe rozmieszczenie odpowiednich systemów monitorujących powinno obejmować następujące logiczne lokalizacje w sieci organizacji:

- styk z siecią Internet,
- styk z siecią, w której odbywa się zarządzanie (w ramach wewnętrznej organizacji),
- najważniejsze urządzenia obsługujące IK.

Oprócz niewątpliwych zalet działania systemów typu IDS, istnieją również jego wady. Jedną z najistotniejszych jest przekazywanie przez systemy monitorujące fałszywych alarmów. Wyróżnia się dwa rodzaje tych ataków:

- *false positive* – fałszywy alarm w sytuacji kiedy nie ma rzeczywistego zagrożenia,
- *false negative* – brak alarmu w sytuacji, w której istnieje rzeczywiste zagrożenie.

Zagadnienie fałszywych alarmów jest o tyle istotne, że ich masowe występowanie (chodzi tu głównie o alarmy typu *false positive*) może doprowadzić do ignorowania tego typu ataków i w konsekwencji braku reakcji na rzeczywisty cyberatak. Dlatego ważnym zadaniem przy korzystaniu z systemów monitoringu jest doprowadzenie ich konfiguracji do stanu, w którym tego typu błędów występuje jak najmniej[73].

[73] W kwestii technik poprawy konfiguracji warto skorzystać z porad zamieszczonych w http://www.symantec.com/connect/articles/strategies-reduce-false-positives-and-false-negatives-ids

Oprócz samej implementacji systemów monitorujących, należy wypracować odpowiednią procedurę obsługi tych systemów. Najważniejsze elementy, które powinny znaleźć się w takiej procedurze[74], to:

- zadbanie o to, aby wszelkie urządzenia sieciowe, które są monitorowane, jak również same systemy monitoringu miały ujednolicony czas zegara systemu operacyjnego,
- stałe kontrolowanie alarmów sygnalizujących zagrożenia,
- kontrola, czy wszystkie systemy, które tego wymagają, są objęte systemem monitoringu,
- dbanie o bezpieczeństwo urządzeń, na których odbywa się monitoring,
- przekazywanie alertów o szczególnie niebezpiecznych zagrożeniach do systemu obsługi incydentów.

Wykrywanie niepożądanego ruchu w sieci

Ze względu na ograniczoną skuteczność oprogramowania antywirusowego, w szczególności w zwalczaniu zagrożeń ukierunkowanych (np. APT), zaleca się monitorowanie ruchu sieciowego w poszukiwaniu charakterystyk aktywności złośliwego oprogramowania. Wykrycie ruchu do zidentyfikowanych „złych" obszarów sieci Internet pozwala na stwierdzenie z dużym prawdopodobieństwem, że w sieci doszło do infekcji – niezależnie od tego, jakie złośliwe oprogramowanie zostało użyte i czy jest ono wykrywane przez antywirusa. Podejrzanej aktywności można poszukiwać co najmniej na dwa sposoby – wśród zapytań DSN oraz w warstwie IP. W każdym przypadku barierą może okazać się ilość gromadzonego materiału. Niezbędne jest bowiem zapewnienie odpowiedniej przepustowości łącz oraz powierzchni dyskowej, odpowiednio dla przesyłania i przechowywania danych.

Monitorowanie zapytań DNS

Zapytania o konkretne nazwy domenowe wysyłane przez urządzenia w sieci lokalnej do serwera nazw mogą być porównywane z listami znanych złośliwych domen publikowanymi przez serwisy monitorujące zagrożenia oraz dostarczane w ramach usług bezpieczeństwa przez zewnętrzne podmioty. W przypadku wykrycia komunikacji z podejrzaną domeną można podjąć działania o różnym stopniu inwazyjności – od podniesienia alarmu w systemie monitorującym, przez zablokowanie rozwiązywania nazw (np. z wykorzystaniem DNS blackholingu), zablokowanie łączności (np. przez zmianę reguł firewalla) po przekierowanie łączności (np. do sinkhole'a).

[74] Dodatkowe informacje na temat zasad funkcjonowania procedur monitoringu i ich audytowania można znaleźć na stronie http://www.isaca.org/Knowledge-Center/Standards/Documents/ P3IDSReview.pdf

Wskazane jest także archiwizowanie zapytań DNS z sieci lokalnej, gdyż możliwość ich analizy jest nieocenioną pomocą w przypadku wykrycia intruza. Często wyłącznie na podstawie historycznych danych o zapytaniach DNS można ustalić w jaki sposób złośliwe oprogramowanie przedostało się po sieci i do jakich zasobów uzyskało dostęp.

DNSSEC (Domain Name System Security Extensions) to rozszerzenie protokołu DNS wzmacniające jego bezpieczeństwo. DNSSEC tworzy bezpieczny system nazw domen, wprowadzając podpisy kryptograficzne. Dodawane są one do już istniejących rekordów DNS. DNSSEC opiera się na kryptografii klucza publicznego, certyfikatach i podpisach cyfrowych. DNSSEC zapewnia dodatkowe uwierzytelnianie i integralność danych. Chroni przed zatruciem pamięci podręcznej oraz może chronić dodatkowe informacje za pomocą rekordów TXT. Wprowadzenie DNSSEC ma też przełożenie na problemy związane z atakami DDOS oraz może powodować problemy ze wdrożeniem podziału strefy. DNSSEC nie rozwiązuje problemów prywatności danych z DNS.

Monitorowanie ruchu IP

Do zbierania danych dotyczących całej komunikacji w warstwie IP z sieciami zewnętrznymi można zastosować mechanizm NetFlow, zbierający z urządzeń sieciowych informacje takie jak źródłowy i docelowy adres IP, port i protokół dla przechodzących przez to urządzenie pakietach. Rozwiązania zgodne z NetFlow wspierane są (pod różną nazwą) przez większość producentów urządzeń sieciowych, a do analizy zebranych w ten sposób danych można wykorzystać dedykowane – także darmowe – narzędzia. Należy zwrócić uwagę na to, że niektóre urządzenia (przynajmniej w domyślnej konfiguracji) nie analizują wszystkich pakietów, a jedynie pewną próbkę statystyczną. Dane próbkowane mogą być wystarczające na potrzeby monitorowania wolumenu ruchu w poszczególnych usługach, lecz zdecydowanie nie wystarczające do wykrywania złośliwych. połączeń. Podobnie jak w przypadku zapytań DNS, archiwizowanie danych NetFlow może być bardzo pomocne przy dochodzeniu w razie wystąpienia incydentu.

2.8.9. Bezpieczeństwo automatyki przemysłowej

Do warstwy sterowania modelu środowiska systemów teleinformatycznych należą urządzenia pobierające informacje z aparatury obiektowej (tj. z czujników, zabezpieczeń, mierników, sygnalizatorów) oraz bezpośrednio sterujące urządzeniami wykonawczymi (np. pompami, zaworami, napędami). Większość z tych urządzeń stanowi aktywa krytyczne z punktu widzenia wspieranych procesów i powinny podlegać szczególnej ochronie. Należy pamiętać, że za integralność dystrybuowanego przez dostawcę sterowników oprogramowania odpowiedzialność powinien ponosić dostawca.

2.8.9.1. Bezpieczeństwo sterowników PAC/PLC/RTU i innych urządzeń programowalnych

Sterowniki PLC (Programmable Logical Controller) to programowalne urządzenia wykorzystywane do sterowania i/lub monitorowania instalacji technologicznych. Sterowniki PLC mogą być łączone w większe systemy poprzez integrację z wykorzystaniem sieci przemysłowych. Sterowniki PLC najczęściej wymieniają dane z innymi sterownikami oraz nadrzędnymi systemami monitorowania i sterowania (np. systemy SCADA). Należy odnotować, że w ostatnim czasie obserwuje się ewolucję koncepcji sterowników PLC w stronę wspólnej platformy sprzętowej, realizującej znacznie więcej zadań niż tylko typowe algorytmy sterowania. Tego typu zaawansowane urządzenia są określane terminem PAC (Programmable Application Controller).

RTU (Remote Terminal Unit) podobnie jak sterowniki PLC przesyłają dane do systemów nadrzędnych (np. systemów SCADA). Najczęściej wykorzystywane są w energetyce i innych rozproszonych geograficznie systemach do przesyłania danych telemetrycznych.

Specyficznym obszarem zastosowań jednostek PLC/PAC/RTU są układy bezpieczeństwa, określane również jako system bezpieczeństwa SIS (Safety Instrumented System). Rolą układów bezpieczeństwa jest sprowadzenie procesu do stanu uznanego za bezpieczny na drodze, np. wyłączenia awaryjnego tzw. systemy ESD (Emergency Shut Down). Zaleca się, aby systemy takie funkcjonowały równolegle i całkowicie niezależnie od podstawowego układu sterownia i wykorzystywały dedykowane, specjalnie certyfikowane elementy.

Urządzenia PAC/PLC/RTU muszą być chronione przed nieupoważnionym dostępem fizycznym przez umieszczanie ich w zamykanych pomieszczeniach technicznych. Dostęp do pomieszczeń powinien być kontrolowany (proceduralnie lub z wykorzystaniem środków bezpieczeństwa technicznego). Urządzenia należy

umieszczać w zamykanych szafach elektrycznych wyposażonych w rozwiązania techniczne stabilizujące środowiskowe warunki pracy (np. wentylacja, klimatyzacja, grzałki) oraz zapewniające ochronę przed zakurzeniem.

Dostęp do programu urządzeń PAC/PLC/RTU powinien być chroniony z wykorzystaniem unikalnego hasła. Rekomenduje się użycie unikalnego hasła dla każdego urządzenia. Hasła powinny być okresowo zmieniane zgodnie z polityką bezpieczeństwa firmy. Zaleca się natychmiastową zmianę hasła po: zakończeniu etapu uruchomienia, zmianie obowiązków służbowych lub odejściu z firmy osób mających dostęp do programów urządzeń, podejrzeniu dostępu do hasła lub urządzenia przez osoby nieuprawnione. Szczególnie ważna jest zmiana haseł domyślnych producentów/dostawców. Używanie (pozostawienie) tych haseł stanowi podatność, która może zostać wykorzystana przez potencjalnych atakujących.

W celu przeprowadzania prac diagnostycznych lub zmian w konfiguracji urządzeń rekomenduje się wykorzystywanie dedykowanych do tego celu stacji inżynierskich (przenośnych – laptopy/programatory lub stacjonarnych – typu desktop). Komputery inżynierskie nie powinny być wykorzystywane w innych celach, w szczególności nie powinny być podłączane do sieci biurowej lub do sieci zewnętrznych. Przenoszenie plików na stacje inżynierskie powinno być realizowane tylko po wcześniejszym ich sprawdzeniu przez aktualne oprogramowanie antywirusowe. Rekomenduje się, aby pracownicy firm trzecich prowadzący prace serwisowe nie korzystali z własnych stacji inżynierskich (z uwagi na ograniczoną kontrolę nad ich bezpieczeństwem).

Operatorzy IK wykorzystującej sterowniki PAC/PLC/RTU powinni dążyć do zapewnienia sobie kompletu aktualnych kopii programów urządzeń:

- w wersjach edytowalnych z dostępem do wszystkich bloków programu (za wyjątkiem bloków predefiniowanych przez producenta urządzenia),
- zawierających komplet komentarzy programisty o poziomie szczegółowości wystarczającym na jednoznaczne zidentyfikowanie roli poszczególnych fragmentów programu,
- nazwami i opisami zmiennych,
- definicją konfiguracji sprzętowej.

Brak kopii programu zgodnej z wyżej wypisanymi wymaganiami zwiększa uzależnienie organizacji od dostawcy systemu automatyki i może znacznie zwiększać koszty i stopień złożoności ewentualnych zmian w algorytmie sterowania.

Wszelkie zmiany w programach urządzeń PAC/PLC/RTU należy przeprowadzać z zapewnieniem sobie możliwości szybkiego odtworzenia pierwotnej aplikacji. Przed uruchomieniem nowego programu rekomenduje się przeprowadzić testy funkcjonalne

na symulatorze lub w przeznaczonym do tego środowisku testowym. Powyższe uwagi odnoszące się do urządzeń PAC/PLC/RTU mają również zastosowanie do urządzeń polowych, typowo zarządzanych przez sterowniki programowalne. Dzieje się tak z uwagi na fakt, że coraz więcej falowników, zabezpieczeń silnikowych, rozproszonych układów wejść/wyjść oraz systemów pomiarowych umożliwia nie tylko prostą konfigurację, ale również zaprogramowanie określonych algorytmów działania na wypadek, np. utraty komunikacji ze sterownikiem nadrzędnym i konieczności zapewnienia autonomicznej pracy.

2.8.9.2. *Bezpieczeństwo urządzeń HMI*

W bezpośrednim sąsiedztwie instalacji technologicznych, często instalowane są lokalne pulpity operatorskie, stacje HMI (Human Machine Interface). Ich celem jest umożliwienie dalszego sprawowania nadzoru oraz sterowania procesem technologicznym w przypadku awarii łączy komunikacyjnych, a także usprawnienie prac serwisowych poprzez zapewnienie lokalnego dostępu do informacji o stanie procesu, instalacji i komponentów systemu automatyki. Umieszczane w miejscach rzadko uczęszczanych przez obsługę, stacje te mogą stanowić punkt nieupoważnionego dostępu do systemu automatyki.

Stacje HMI należy chronić przed nieupoważnionym dostępem fizycznym poprzez umieszczanie ich w zamykanych pomieszczeniach lub szafach obiektowych, do których dostęp jest ściśle kontrolowany. Urządzenia powinny być zabudowane w taki sposób, aby, aby operator lub inne osoby w pomieszczeniu miały dostęp jedynie do interfejsów użytkownika (ekranu, klawiatury, myszy itp.). Urządzenie powinny być zabezpieczone przed dostępem do portów fizycznych urządzenia.

Dla stacji HMI mają zastosowanie wszystkie rekomendacje, co do zabezpieczenia hasłami oraz zmianami wskazane w rozdziale poświęconym urządzeniom PAC/PLC/RTU.

Operatorzy infrastruktury krytycznej wykorzystujący stacje HMI powinni dążyć do zapewnienia sobie kompletu:

- aktualnych, edytowalnych kopii aplikacji HMI,

- instrukcji użytkownika, rozumianej zarówno jako instrukcja dla operatorów jak i część techniczną dla serwisu/inżynierów systemów sterowania, zawierające informacje o strukturze aplikacji.

2.8.9.3. *Bezpieczeństwo przemysłowych sieci sterowania*

W obszarze warstwy sterowania oraz AKPiA (Aparatury Kontrolno-Pomiarowej i Automatyki) wykorzystywane są specjalistyczne protokoły komunikacyjne. Część tych protokołów została zaprojektowana wiele lat temu, bez uwzględnienia wymagań

wynikających ze współczesnych zagrożeń teleinformatycznych. W protokołach tych występują znane podatności, które mogą zostać wykorzystane w celu zakłócenia działania lub przejęcia kontroli nad infrastrukturą krytyczną. Rekomenduje się zabezpieczanie przemysłowych sieci sterowania korzystających z protokołów o znanych podatnościach poprzez:

- ograniczenie dostępu fizycznego do infrastruktury sieciowej,
- ograniczenie dostępu logicznego poprzez wdrażanie właściwych mechanizmów bezpieczeństwa na wyższych warstwach modelu segmentacji sieci,
- tam, gdzie to możliwe oraz uzasadnione ekonomicznie (np. przewidywana jest wieloletnia eksploatacja systemu), należy rozważyć migrację do protokołów komunikacyjnych zapewniających wyższy poziom bezpieczeństwa.

Bezpieczeństwo stacji operatorskich systemów SCADA/DCS

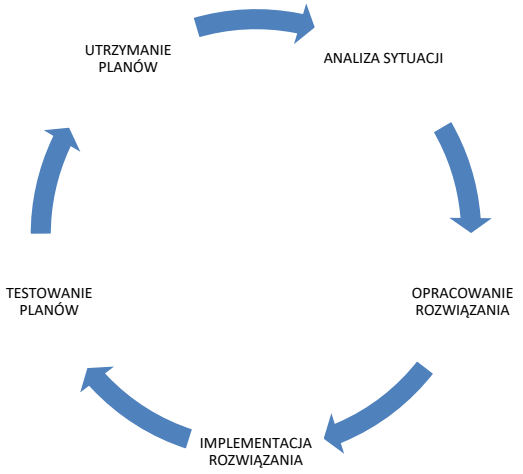
Przemysłowe systemy nadrzędnego monitorowania i sterowania, takie jak SCADA czy DCS, dla celów przechowywania i przetwarzania danych oraz realizacji interfejsu użytkownika, wykorzystują coraz częściej te same rozwiązania techniczne co pozostałe systemy IT (m. in.: serwery, stacje operatorskie, macierze dyskowe, standardowe systemy operacyjne, sieci TCP/IP). Zasady bezpieczeństwa dla tych rozwiązań zostały opisane we wcześniejszych rozdziałach. Należy jednak zwrócić uwagę, iż nastawienie na zapewnienie maksymalnej dostępności systemu wymusza w niektórych przypadkach inne podejście do praktycznej realizacji wymagań bezpieczeństwa, np. w przypadku, gdy systemy SCADA/DCS stanowią podstawową metodę nadzoru i kontroli nad procesem technologicznym, zabezpieczenie dostępu do stacji operatorskich hasłem może być niewskazane z uwagi na ryzyko błędu podczas wpisywania lub zapomnienia hasła przez operatora w sytuacji podwyższonego stresu. W takich przypadku takich systemów, wymagany poziom zabezpieczenia przed nieupoważnionym dostępem realizuje się poprzez restrykcyjne ograniczenie dostępu fizycznego do pomieszczenia sterowni.

Instalacja poprawki systemu operacyjnego, nawet odpowiedzialnej za usunięcie krytycznych błędów bezpieczeństwa nie może zostać zainstalowana na komponentach systemów odpowiedzialnych za nadzór i sterowanie procesami przemysłowymi o ile nie ma pewności, iż instalacja ta nie zakłóci funkcjonowania tego systemu. W takich przypadkach często wybiera się tymczasowe odłączenie fizyczne sieci systemu sterowania od innych sieci teleinformatycznej do czasu przetestowania działania poprawki przez producenta systemu sterowania lub na własnym środowisku testowym.

2.8.10. Plany awaryjne i procedury odtworzenia

2.8.10.1. Proces tworzenia i doskonalenia planów

Plany awaryjne zapewniające odtworzenie i ciągłość działania infrastruktury IT powinny być przygotowywane i utrzymane wg przedstawionego schematu.



Rysunek 16 Cykl wdrożenia planów awaryjnych.

Analiza sytuacji

W tej fazie najważniejszym zadaniem jest ustalenie zasobów, niezbędnych do sprawnego i bezpiecznego przełączenia/odtworzenia systemów IT. Jest to zadanie ściśle związane z oceną ryzyka, wymaganym czasem odtworzenia (RTO – recovery time objective) oraz akceptowalnym poziomem utraty danych (RPO – recovery point objective) – parametry RTO i RPO bezpośrednio wpływają na technologię tworzenia kopii zapasowych (backup). Tymi zasobami mogą być zarówno personel, infrastruktura techniczna, a także zasoby zewnętrzne, np. kluczowi dostawcy materiałów lub informacji koniecznej do podtrzymania procesów biznesowych i wsparcia. Również w tej fazie trzeba określić kryteria, przy których uruchamiane są plany awaryjne (wyznaczenie granicy pomiędzy planami awaryjnymi i zarządzaniem incydentem).

Opracowanie rozwiązania

W fazie opracowania rozwiązania powstają szczegółowe plany, które odpowiadają na pytania: kiedy? kto? co? w jaki sposób? Opracowując te plany, trzeba pamiętać, że nie wszystkie sytuacje da się przewidzieć w fazie planowania. Dlatego oprócz szczegółowych gotowych planów powinien powstać mechanizm rozwiązania sytuacji, w której wystąpiło to, czego nikt nie przewidział. Taki mechanizm przede wszystkim powinien zawierać reguły dotyczące tego, jakie osoby (stanowiska) biorą udział w rozwiązaniu problemu i w jaki sposób podejmują one decyzję.

Ważnym elementem zabezpieczenia danych jest systematyczne tworzenie kopii zapasowych, których częstotliwość wykonywania powinna wynikać z analizy ryzyka oraz czasu dostępności do danych. Zakres wykonywania kopii zapasowych dla serwerów musi zawierać oprogramowanie systemowe (konfiguracja systemu), zainstalowane oprogramowanie użytkowe. Dla urządzeń sieciowych (routerów, switchy, zapór ogniowych itp.) oznacza to zapisanie ich konfiguracji, a dla stacji roboczych przetwarzanie informacji zgodnie ze zgłoszonym przez użytkownika zapotrzebowaniem. Należy pamiętać, żeby kopie zapasowe nie były przechowane w tym samym miejscu co systemy, z których zostały wykonane (fizyczna utrata budynku, na przykład pożar, oznacz wtedy i utratę systemu, i utratę kopii zapasowej). Kopie zapasowe powinny być szyfrowane i okresowo testowane (czy nadal jest techniczna możliwość odczytu danych z nośnika).

Implementacja rozwiązania

Po tym, jak zostaną opracowane plany awaryjne, powinna nastąpić ich implementacja. Właściwym rozwiązaniem jest, aby wraz z implementacją nastąpiło przetestowanie zaplanowanych rozwiązań. Nie chodzi o pełne testy, tylko o to, aby sprawdzić, czy plany są kompletne, proceduralnie logiczne i możliwe do realizacji. Może tego dokonać zespół odpowiedzialny za implementację.

Testowanie planów

Właściwa weryfikacja planów odbywa się w fazie testów. W tym przypadku w testowaniu uczestniczą wszyscy zainteresowani. Testy te mogą być mniej lub bardziej złożone. Test prosty może składać się z uruchomienia pojedynczej procedury awaryjnej (test prosty może być realizowany samodzielnie przez jednostki IT bez udziału jednostek biznesowych). Natomiast test złożony powinien obejmować uruchomienie kilku procedur awaryjnych naraz i swoim zasięgiem objąć maksymalnie największą liczbę komórek organizacyjnych firmy (czynne zaangażowanie jednostek biznesowych w weryfikację jakości i poprawności odtworzenia systemów IT w lokalizacji zapasowej). W przypadku gdy nie jest możliwe przetestowanie określonego zakresu, rozwiązaniem mogą być testy polegające na przećwiczeniu teoretycznego planu, przy różnych scenariuszach.

W praktyce grupa zaangażowana w realizację planu realizuje wybrane scenariusze „na kartce papieru” (tzw. *table exercises*) lub na wydzielonym, odseparowanym środowisku testowym. Testy takie we wspomnianych obszarach pomagają utrwalić prawidłowe mechanizmy zachowań. Przykładowy scenariusz może uwzględniać:

- awarię głównego serwera pocztowego organizacji,
- atak wirusa unieruchamiającego komunikaty alarmowe przekazywane z systemu SCADA,
- awarię systemu kontroli fizycznej wejścia do budynku.

Jako wynik testowania sporządzany jest szczegółowy raport, który powinien zawierać informacje na temat:

- sytuacji awaryjnej,
- przebiegu testu,
- osiągniętych wyników w porównaniu z wynikami oczekiwanymi,
- analizy powodów różnic (jeśli wystąpiły),
- propozycji działań naprawczych (jeśli jest to konieczne).

Po zakończeniu testów następuje wdrożenie przedstawionych w raporcie propozycji działań naprawczych oraz ostateczne zatwierdzenie planów awaryjnych.

Utrzymanie planów

Utrzymanie planów awaryjnych składa się z dwóch głównych aktywności:

- szkolenia osób odpowiedzialnych za działania w trakcie sytuacji kryzysowej,
- testowania zatwierdzonych planów awaryjnych.

Wskazane jest, aby zarówno szkolenia, jak i testowanie, odbywały się co najmniej raz do roku.

Oczywiście w przypadku zajścia zmiany w środowisku, w jakim funkcjonuje organizacja, np. pojawienie się nowego systemu albo powołanie nowej komórki organizacyjnej, należy powtórzyć cały cykl stworzenia planów awaryjnych. Jeśli nie następują takie zmiany, warto powtarzać ten cykl co najmniej raz na 2 lata.

2.8.10.2. *Reakcja na incydenty*

Podstawowe rekomendacje w zakresie wykrywania i reagowania na ataki ukierunkowane (w tym APT).

Sprawna reakcja na zagrożenia jest kluczowym elementem, jeśli chodzi o przeciwdziałanie atakom ukierunkowanym, w tym APT (Advanced Persistent Threat). Poprzez atak ukierunkowany rozumiany jest atak na konkretną organizację lub osobę (lub też grupę organizacji/osób). Atak APT jest podzbiorem tej kategorii ataku i dotyczy zagrożeń (organizacji), które posiadają zaawansowane możliwości przeprowadzenia ataku - zarówno na poziomie technicznym jak i organizacyjnym, finansowym i rozwojowym - i posiadają jasno sprecyzowane długofalowe cele do których będą systematycznie dążyły.

Należy wyjść z założenia, że prędzej czy później dojdzie do udanego włamania do chronionej sieci. Ustanowienie pracy zespołu reagującego i jego planów powinno być poprzedzone analizą ryzyka, która skupi się przede wszystkim na określeniu, jakie są najważniejsze zasoby, które należy chronić a także określenie prawdopodobny ścieżek ataku na te zasoby. W szczególności warto zwrócić uwagę na różne metody socjotechniczne, które wraz z wykorzystaniem złośliwego oprogramowania mogą posłużyć do ataku na poszczególne osoby lub działy w firmie:

- spear phishing - atak ukierunkowany na konkretną organizację lub osobę/grupę osób, w którym atakujący wysyła korespondencję podając się za zaufaną instytucję lub nierzadko stojącą wysoko w hierarchii osobę z atakowanej organizacji; celem ataku jest nakłonienie ofiary do wykonania polecenia zawartego w wiadomości email (np. otwarcie załącznika lub odwiedzenie strony podanej w odnośniku), a w konsekwencji zarażenie jej złośliwym oprogramowaniem,
- clone phishing - klonowanie prawdziwej wiadomości e-mail. Przestępca może użyć wzoru podczas tworzenia nowej i załączyć zmienione linki prowadzące do złośliwej strony www. Ofiara ma pewność, że otrzymuje identyczną wiadomość od tego samego nadawcy,
- whaling - typ ataku spersonalizowanego, który ma za zadanie przechwycenie danych od osób zajmujących najwyższe stanowiska w firmie,
- brand phishing - oszuści podszywają się pod przedsiębiorstwo, świadczące usługi dla atakowanej firmy,
- waterholing, watering hole attack – atak ukierunkowany, polegający na zidentyfikowaniu przez atakującego stron odwiedzanych przez ofiary (np. strony podwykonawców, systemy dostarczające wiedzy), a następnie – przez osobny atak – umieszczenie na nich złośliwego kodu celem infekcji ofiar,
- spoofing - typ phishingu, który polega na fałszowaniu domen. Cyberprzestępca podszywa się pod istniejącą domenę, aby jego e-mail wyglądał jak oryginalna wiadomość od wybranej organizacji,
- Smishing - atak wykorzystujący wiadomości SMS, zawierające złośliwy link.

Wyznaczenie ścieżek potencjalnych ataków umożliwi uwzględnienie różnych metod detekcji ataku odpowiadających kolejnym etapom włamania. Warto w tym celu zapoznać się z pojęciem i metodyką "intrusion kill chain" wprowadzoną przez firmę Lockheed Martin[75].

[75] http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Rekomendacje:

- Nie należy klikać podejrzanych linków i plików do pobrania w wiadomościach. Należy zbadać wiarygodność danej wiadomości np. dzwoniąc do nadawcy, którego dotyczy e-mail.
- Wiadomość wydaje się pilna i wzbudza ciekawość? Nadawca kusi, że jest tylko 20 minut na odbiór nagrody lub rabatu? To jedna z socjotechnik, które mają zachęcić do szybkiego i nieprzemyślanego reagowania. Ogromna część ataków phishingowych ma za zadanie wzbudzenie silnych emocji.
- Przestępcy dbają o realistyczny wygląd swoich stron. Często są one łudząco podobne do oryginału, pod który się podszywają. Zielona kłódka obok adresu nie gwarantuje, że zapewnione jest bezpieczeństwo. Protokół HTTPS oznacza jedynie, że dane są bezpiecznie transmitowane, jednak nie gwarantuje wiarygodności samej witryny.
- Nie należy odpowiadać na mail, który wyda się podejrzany. Ignorować należy prośby o podanie loginu i hasła, danych osobowych lub skanu dowodu osobistego.
- Brak zaufania do wiadomości zawierających prośby o pieniądze – nawet od najbliższych współpracowników lub znajomych. Ich konto mogło zostać zhakowane i wykorzystane wbrew intencjom. Dotyczy to zwłaszcza sieci społecznościowych.

Plany reakcji powinny uwzględniać komunikację z podmiotami zewnętrznymi, w tym Policja i inne służby, dostawcy usług sieciowych, CSIRTy a także media. Warto uprzednio zweryfikować jakie są możliwości powyższych w zakresie niesienia pomocy i przygotować odpowiednie metody komunikacji.

Poprawna reakcja na dany incydent wymaga uzyskania przez podmiot dobrego obrazu sytuacyjnego funkcjonowania własnej sieci, w szczególności w kontekście zdarzeń bezpieczeństwa. Zaleca się przyjęcie postawy proaktywnej - tzn. aktywnego wyszukiwania potencjalnych problemów w sieci, tak aby móc zareagować na incydent już we wczesnej fazie jego rozwoju. Należy przyjąć założenie, że sieć może być skompromitowana już wcześniej i skupić się na wskaźnikach mogących świadczyć o obecności intruza wewnątrz sieci, np. o eksfiltrację danych. Podstawą jest logowanie ruchu w sieci w celu dalszej analizy (w tym także w celach analizy powłamaniowej). Zaleca się w tym wypadku jako minimum uwzględnienie mechanizmu netflow do zbierania i przechowywania całego ruchu sieciowego przez pewien czas (optymalnie przynajmniej rok) a także logowanie wszystkich zapytań na poziomie DNS.

W celu poprawy obrazu sytuacyjnego zaleca się zapoznanie i dostosowanie do rekomendacji dwóch raportów ENISA:

- Proactive Detection of Network Security Incidents https://www.enisa.europa.eu/activities/cert/support/proactive-detection
- Actionable Information for Security Incident Response https://www.enisa.europa.eu/activities/cert/support/actionable-information

Dokumenty te opisują metody, narzędzia i standardy wymiany informacji niezbędnego do tego, by proaktywnie wykrywać zagrożenia i wymienić się informacjami o nich.

Zaleca się również skorzystanie z istniejących mechanizmów wymiany danych o zagrożeniach wprowadzonych w Polsce. W szczególności wskazane jest dołączenie do istniejącego systemu agregującego sieciowe incydenty bezpieczeństwa dotyczące polskich podmiotów - platformy n6, stworzonej przez CSIRT NASK. W ramach tego systemu można bezpłatnie otrzymywać informacje o zagrożeniach wykrytych we własnych sieciach (w tym także informacji o atakach ukierunkowanych i APT), bez konieczności instalacji jakiegokolwiek oprogramowania lub sondy. Więcej informacji o tym systemie oraz jak do niego dołączyć znajduję się na stronie http://n6.cert.pl. Warto również rozważyć dołączenie do listy dyskusyjnej poświęconej projektowi - n6 forum.

2.8.11. Wsparcie działań w sytuacjach awaryjnych

2.8.11.1. Security Operation Centre

Istotną kwestią organizacyjną jest powołanie w strukturach organizacji zespołu do spraw reagowania na przypadki naruszania bezpieczeństwa teleinformatycznego zwanego SOC (ang. Security Operation Centre). Komórka taka nie jest obligatoryjna, niemniej jednak decyzję o jej powołaniu i funkcjonowaniu warto poważnie rozważyć. Praktyka pokazuje, że tego typu komórka, oprócz sprawowania powierzonych jej kluczowych zadań, tj. obsługi incydentów, również jest doskonałym wsparciem dla realizacji innych zadań, np. przeprowadzenia analizy ryzyka, audytu teleinformatycznego czy przeprowadzenia działań uświadamiająco-edukacyjnych. Jest to możliwe dzięki stałemu kontaktowi kadry SOC z najważniejszymi i najbardziej aktualnymi zjawiskami w dziedzinie bezpieczeństwa teleinformatycznego i praktycznej wiedzy dotyczącej nadużyć w sieci i sposobów im zapobiegania.

Jak zbudować SOC[76]

Rysunek 17 Etapy tworzenia SOC

Krok I – Uzyskanie poparcia zarządu organizacji

Podstawowym zadaniem, które stoi na początku drogi budowy zespołu reagującego, jest otrzymanie poparcia zarządu organizacji dla takiej inicjatywy. Jak w przypadku każdej nowej inicjatywy, brak takiego poparcia może odbić się negatywnie na jakości powstającej komórki.

Krok II – Stworzenie planu strategicznego

W kroku drugim należy szczegółowo zaplanować strategię stworzenia SOC. Jaka grupa osób będzie go tworzyła? Jak będzie wyglądało poparcie od zarządu? Jak poinformować o istnieniu i zadaniach takiego zespołu pozostałych członków organizacji?

[76] Propozycja bazuje na rekomendacjach przygotowanych przez CERT Coordination Center: http://www.cert.org/

Krok III – Zebranie kluczowej informacji

Jest to bardzo istotny krok, w trakcie którego dowiadujemy się o szczegółowych oczekiwaniach wobec przyszłego SOC. Warto wtedy omówić te oczekiwania z kierującymi innymi komórkami (w szczególności dział IT, prawny i public relations). Pozwoli to między innymi na zaplanowanie koniecznych zasobów ludzkich i technicznych do funkcjonowania przyszłego zespołu. W trakcie tej fazy zbieramy również informacje na temat już istniejących zasad bezpieczeństwa w organizacji, w tym, jak do tej pory (jeśli w ogóle) odbywało się reagowanie na incydenty. Pomocne również będą wszelkie schematy organizacyjne i organizacyjne procedury.

Krok IV – Zaprojektowanie wizji działania

Choć zadanie to brzmi ogólnikowo, to jest ono niezwykle ważne. Zdefiniowanie takich rzeczy jak:

- obszar działania (tzw. *constituency*) zespołu, czyli to, jakie SOC będzie realizował zadnia,
- zdefiniowanie misji i celów działania,
- ustalenie zakresu świadczonych usług reaktywnych, proaktywnych i konsultacyjnych[77],
- ustalenie modelu organizacyjnego dla powstającego zespołu,
- ustalenie potrzebnych zasobów (osobowych i technicznych),
- ustalenie źródeł budżetowania dla zespołu SOC.

Krok V – Poinformowanie i zebranie opinii na temat wizji działania

Dobrą praktyką przy tworzeniu zespołu jest sprawienie, aby szczegółowa informacja na temat wizji działania zespołu trafiła do zainteresowanych stron. Jest to skuteczne działanie nie tylko z punktu widzenia promocji i uzyskania przychylności dla nowo powstającego zespołu, ale również zebrania informacji na temat potencjalnych problemów i ryzyk związanych z funkcjonowaniem tak zaplanowanego zespołu.

Krok VI – Rozpoczęcie implementacji

Rozpoczęcie działań operacyjnych wiąże się z zatrudnieniem personelu, zakupem odpowiedniej infrastruktury, wstępnym ustaleniem procedur funkcjonowania, stworzeniem technicznego systemu wspierającego obsługę incydentów oraz przygotowaniem odpowiednich rekomendacji i wskazówek w obszarze działania na temat tego, jak zachowywać się w przypadku stwierdzenia lub podejrzenia naruszenia bezpieczeństwa teleinformatycznego.

---

[77] Listę uznanych serwisów CSIRT można znaleźć na stronie: http://www.cert.org/csirts/services.html

Krok VII – Ogłoszenie działań operacyjnych

Poinformowanie wszystkich zainteresowanych o rozpoczęciu funkcjonowania zespołu. Najlepiej, jeśli dokona tego osoba reprezentująca zarząd, co po raz kolejny potwierdzi jego poparcie dla tej inicjatywy. Wtedy też warto udostępnić wcześniej opracowane wskazówki i rekomendacje. Warto przy tym wszystkim skorzystać z atrakcyjnej formy przekazu (np. firmowa broszura, wywiad z kierownikiem zespołu SOC, wykorzystanie organizacyjnego intranetu).

Krok VIII – Ocena efektywności działania

Po odpowiednim okresie funkcjonowania zespołu (np. po 6 miesiącach) powinna nastąpić ocena tej funkcjonalności. Ocena ta pozwoli odpowiedzieć na to, czy warto było powoływać do życia taką komórkę i jeżeli odpowiedź jest twierdząca, to co ewentualnie warto poprawić w jej funkcjonowaniu. Aby odpowiedzieć na te pytania, można posłużyć się informacjami niemierzalnymi, takimi jak ankieta oceniająca, a także pewnymi miernikami, np. liczbą raportowanych i rozwiązywanych incydentów, czasem ich obsługi, zaimplementowaniu nowych narzędzi zapewnienie bezpieczeństwa teleinformatycznego, które wynikają z wniosków z obsługi incydentów.

2.8.11.2. *Współpraca sektorowa*

Znaczna część IK znajduje się w rękach sektora prywatnego. Często organizacje władające IK są na rynku komercyjnym konkurentami. Niemniej jednak zasada konkurencji nie powinna dotyczyć kwestii bezpieczeństwa. Dlatego wskazane jest, aby organizacje utrzymujące IK ze sobą współpracowały. Najlepiej jeśli ta współpraca realizowana jest w ramach poszczególnych sektorów, np. sektora energetycznego czy sektora bankowego.

Formuła współpracy sektorowej między zainteresowanymi organizacjami często określana jest angielskim terminem ISAC (Information Sharing and Analysis Center), czyli Centrum Analizy i Wymiany Informacji i najczęściej przyjmuje formę wirtualnej współpracy. W ramach takiego centrum wymieniana jest informacja o konkretnych zagrożeniach dla danego sektora, a nawet o przypadkach incydentów w poszczególnych organizacjach[78]. Pozwala to wszystkim uczestnikom inicjatywy na wykorzystanie tej praktycznej informacji w lepszym odparciu potencjalnego cyberataku lub poprawy poziomu bezpieczeństwa swoich zasobów. Najistotniejsze jest, aby informacja wymieniana między uczestnikami była wartościowa i aby nie były naruszone zasady zaufania i poufności, przede wszystkim przez zapewnienie odpowiedzialnej polityki personalnej wobec osób uczestniczących w wymianie

[78] Te informacje ze względu na wysokie wymagania dotyczące poufności mogą być wymieniane w sposób anonimowy.

informacji. W ramach istnienia centrum możliwe jest też podejmowanie wspólnych działań na rzecz poprawy bezpieczeństwa w całym sektorze. Jedną z ciekawszych i bardzo ważnych możliwości jest powołanie sieci informacji kryzysowej, która w przypadku wystąpienia szczególnie niebezpiecznej sytuacji dla jednego lub wielu członków centrum może szybko zadziałać, tak aby straty wynikające z wystąpienia sytuacji kryzysowej były jak najmniejsze. Dzięki takiej sieci można:

- powiadomić innych członków o niebezpiecznej sytuacji,
- uzyskać wsparcie merytoryczne w radzeniu sobie z sytuacją,
- podjąć wspólne działania w celu osłabienia siły zagrożenia.

Jako dobre przykłady działania współpracy sektorowej można podać inicjatywę Ministerstwa Klimatu i Środowiska – organu właściwego w sektorze energii tworzącego centrum analityczno-informacyjne (ISAC- Information Sharing and Analysis Center), a także holenderską inicjatywę sektora finansowego o nazwie FI- SAC[79] oraz amerykański ISAC sektora informatycznego – IT-ISAC[80].

2.8.11.3. *Zespoły reagowania na incydenty CSiRT*

W przypadku nieposiadania w strukturach organizacji zespołu SOC, w działaniach związanych z reagowaniem na incydenty w szczególny sposób bazujemy na wsparciu zewnętrznym. W takiej sytuacji incydent jest obsługiwany przez CSIRT zewnętrzny zgodnie z obszarem działania CSIRT zewnętrznego (ang. constituency).

Oprócz formalnie działających zespołów CSIRT wiele podmiotów posiada w swoich strukturach zespoły bezpieczeństwa, które mają za zadanie obsługiwać incydenty pojawiające się w sieciach należących do tych podmiotów, grup kapitałowych i instytucji.

Zgłoszenia incydentów powinny się odbywać zgodnie ze wskazanym w tabeli poniżej obszarem działania. Jednym ze sposobów odnalezienia odpowiedniego CSIRT lub instytucji związanej z danym adresem IP jest skorzystanie z bazy udostępnionej przez organizację RIPE: www.ripe.net.

[79] http://www.samentegencybercrime.nl/Informatie_knooppunt/Sectorale_ISACs/FIISAC?p=content
W serwisie można odnaleźć również wiele innych tego typu inicjatyw sektorowych.

[80] https://www.it-isac.org/

ZESPÓŁ	ADRES WWW	OBSZAR DZIAŁANIA
CSIRT GOV	http://csirt.gov.pl Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego	a) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1, 8 i 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, z wyjątkiem wymienionych w art. 26 ust. 5 i 6 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (UKSC); b) jednostki podległe Prezesowi Rady Ministrów lub przez niego nadzorowane; c) Narodowy Bank Polski; d) Bank Gospodarstwa Krajowego; e) inne niż wymienione w pkt a – d oraz będących w obszarze działania CSIRT MON podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym; f) podmioty, o których mowa w ust. 6, jeżeli incydent dotyczy systemów teleinformatycznych lub sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

ZESPÓŁ	ADRES WWW	OBSZAR DZIAŁANIA
CSIRT MON	https://csirt-mon.wp.mil.pl Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej	a) podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, w tym podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym; b) przedsiębiorcy o szczególnym znaczeniu gospodarczo-obronnym, w stosunku do których organem organizującym i nadzorującym wykonywanie zadań na rzecz obronności państwa w rozumieniu art. 5 pkt 3 ustawy z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców jest Minister Obrony Narodowej.
CSRIT NASK	http://www.cert.pl Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy	a) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 2–6, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, b) jednostki podległe organom administracji rządowej lub przez nie nadzorowane, z wyjątkiem jednostek, o których mowa w art. 26 ust. 7 pkt 2, UKSC c) instytuty badawcze, d) Urząd Dozoru Technicznego, e) Polską Agencję Żeglugi

ZESPÓŁ	ADRES WWW	OBSZAR DZIAŁANIA
		Powietrznej, f) Polskie Centrum Akredytacji, g) Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej, h) spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej, i) dostawców usług cyfrowych, z wyjątkiem wymienionych w art. 26 ust. 7 pkt 5 UKSC, j) operatorów usług kluczowych, z wyjątkiem wymienionych w ust. 5 i 7 UKSC, k) inne podmioty niż wymienione w lit. a–j oraz ust. 5 i 7 UKSC, l) osoby fizyczne;
CSIRT KNF	https://www.knf.gov.pl/dla_rynku/CSIRT_KNF Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego polskiego sektora finansowego	podmioty rynku finansowego uznane za Operatorów Usług Kluczowych (OUK) w rozumieniu UKSC

Tabela 10 Obszar działania poszczególnych CSIRT

2.8.12. Rekomendacje

Najważniejsze rekomendacje dotyczące zapewnienia bezpieczeństwa teleinformatycznego:

a) Wykorzystuj istniejące normy i standardy.
b) Regularnie szkól personel.
c) Wymieniaj doświadczenia i informacje o zagrożeniach z innymi organizacjami.
d) Twórz i testuj plany awaryjne.
e) Zarządzaj zmianą oprogramowania (testowanie, aktualizacja, audyt kodu).
f) Przydzielaj uprawnienia wyłącznie na podstawie faktycznych potrzeb.
g) Wykorzystuj oprogramowanie zabezpieczające przed kodem złośliwym włamaniami i wyciekiem informacji.
h) Chroń dostęp do narzędzi administratorskich, programistycznych oraz ograniczaj dostęp do kodów źródłowych.
i) Monitoruj ruch sieciowy.
j) Zabezpieczaj dane przesyłane publicznymi sieciami.
k) Stwórz własny SOC lub w przypadku ataku teleinformatycznego korzystaj z usług istniejących CSIRT poziomu krajowego.

2.9. Zapewnienie bezpieczeństwa prawnego

Zapewnienie bezpieczeństwa prawnego to zespół przedsięwzięć mających na celu minimalizację ryzyka związanego z działalnością osób fizycznych lub innych podmiotów gospodarczych (państwowych lub prywatnych), których działania mogą prowadzić do zakłócenia w funkcjonowaniu obiektów, urządzeń, instalacji i usług IK.

W zapewnieniu bezpieczeństwa prawnego mamy na myśli przede wszystkim narzędzia stosowane przez państwo, aby zabezpieczyć najważniejsze obiekty IK przed zagrożeniami. Oznacza to zastosowanie narzędzi prawnych niedopuszczających, przez możliwość kontroli i ewentualnego blokowania lub ograniczania decyzji zarządów, do np. wrogiego przejęcia, fuzji czy też sprzedaży niektórych elementów infrastruktury, której efektem mogą być zakłócenia w jej funkcjonowaniu.

Takich narzędzi dostarcza ustawa z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw aktywów państwowych oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych (Dz. U. 2020, poz. 2173).

Zapewnienie bezpieczeństwa prawnego w rozumieniu *Ustawy o szczególnych uprawnieniach...* ma zastosowanie jedynie w stosunku do podmiotów, których mienie zostało wykazane w jednolitym wykazie IK w systemie zaopatrzenia w energię, surowce energetyczne i paliwa.

Niezależnie od rozwiązań przyjętych przez państwo, należy podejmować wszelkie działania prawne minimalizujące ryzyko zakłócenia funkcjonowania IK. Zapewnienie sobie tytułu prawnego do nieruchomości, na której zlokalizowana jest IK, pozwalające na egzekwowanie dostępu do IK oraz zabezpieczenia się umowami z dostawcami mediów, są przykładami dobrych praktyk w tym zakresie.

2.9.1. Rekomendacje do umów zawieranych z podmiotami zewnętrznymi

(1) Operator IK powinien wdrożyć proces ciągłej oceny ryzyka prawnego wynikającego z umów zawieranych z dostawcami kluczowych usług i produktów.

(2) W sytuacjach korzystania przez operatorów IK ze wzorów wydawanych przez Prokuratorię Generalną RP można skorzystać z jej rekomendacji zawartych na stronie www.gov.pl [81] lub wynikających z bezpośredniej współpracy.

(1) [81] https://www.gov.pl/web/prokuratoria/rekomendacje-i-wzory-postanowien-umow2

(3) Przy wyborze usługodawcy należy brać pod uwagę jego bieżącą sytuację finansowo-ekonomiczną oraz badać strukturę właścicielską, łącznie z identyfikacją beneficjentów rzeczywistych.

(4) Każda relacja z nowym partnerem powinna rozpocząć się od zawarcia umowy o zachowanie poufności. Umowa taka powinna gwarantować realne sankcje w przypadku jej naruszenia.

(5) Szczególna uwaga powinna zostać poświęcona relacjom z dostawcami rozwiązań informatycznych lub produktów zawierających oprogramowanie komputerowe, które mogą mieć wpływ na zdolność operacyjną IK, w tym zwłaszcza systemów typu OT (np. SCADA/DCS).

(6) Każda zawierana umowa powinna zostać poddana analizie ryzyka pod kątem tzw. vendor lock (VL), czyli uzależnienia się od jednego dostawcy. VL zwykle związany jest z niekorzystnymi zapisami dotyczącymi własności intelektualnej w zakresie możliwości rozwoju lub korzystania z produktów (najczęściej oprogramowania) w przypadku upadłości dostawcy lub zerwania współpracy przez dostawcę. Rozwiązaniem rekomendowanym dla kluczowych, „szytych na miarę" systemów informatycznych jest przeniesienie autorskich praw majątkowych w zakresie pozwalającym na modyfikację oprogramowania lub zapewnienie długotrwałej licencji umożliwiającej samodzielny rozwój oprogramowania, w tym możliwości powierzenia go osobom trzecim. Należy rozważyć co najmniej wykorzystanie mechanizmów typu „escrow"[82] do kodów źródłowych oraz środowiska rozwojowego danej aplikacji.

(7) Docelowa umowa powinna zawierać precyzyjny opis przedmiotu umowy tak, aby zminimalizować ryzyko obszarów, które nie zostały przypisane wyraźnie do jednej ze stron.

(8) Umowa powinna zawierać opis oczekiwanego zakresu współpracy usługodawcy w tym osób trzecich działających na jego rzecz, współuczestniczących w świadczeniu usługi z operatorem IK w sytuacji usuwania awarii. Zakres ten powinien obejmować m.in.: udostępnianie określonej infrastruktury, personelu i gotowości tego personelu do działania.

(9) Definicje awarii lub błędów używane w umowach powinny uwzględniać zjawiska wynikające z wykrycia nowych podatności oprogramowania.

(10) Umowa powinna zawierać zasady usuwania zgłoszonych błędów, w postaci tzw. umowy Service Level Agreement (SLA) zawierającej wskaźniki dotyczące

[82] Dostęp poprzez escrow do kodów - zabezpieczenie interesów spółki polegające na powierzeniu stronie trzeciej kodów źródłowych danego rozwiązania informatycznego. W przypadku bankructwa dostawcy oprogramowania strona trzecia przekazuje kod źródłowy spółce.

procedur współpracy, terminowości usuwania zgłoszonych błędów jak i sankcji za ich nieusunięcie.

(11) Umowy serwisowe z producentami oprogramowania powinny zawierać dodatkowe SLA dotyczące usuwania wykrytych podatności, których wykorzystanie może powodować ryzyko zakłócenia funkcjonowania IK.

(12) W zależności od stwierdzonej istotności wpływu oprogramowania na funkcjonowanie IK, wskazane jest uregulowanie dostępu do kodu źródłowego operatorowi IK lub audytorowi wybranemu przez strony, zarówno w trakcie obowiązywania umowy jak i po jej zakończeniu.

(13) Umowa na dostawę lub obsługę serwisową oprogramowania powinna zawierać postanowienia dotyczące procedury zarządzania zmianami w tym oprogramowaniu oraz sposobu ustalania wynagrodzenia usługodawcy z tego tytułu.

(14) Umowa musi zawierać mechanizmy sankcyjne, nadające operatorowi IK uprawnienia finansowe (np. potrącenia, kary umowne) lub organizacyjne (np. rozwiązanie umowy) w przypadku naruszenia zobowiązań przez dostawcę.

(15) Umowa nie powinna zawierać postanowień całkowicie wyłączających odpowiedzialność dostawcy lub ograniczających jego odpowiedzialność do kwot nieodpowiadających ryzyku związanemu z dostarczeniem produktu lub usługi niespełniających warunków zamówienia.

(16) Umowa powinna posiadać sformalizowaną ścieżkę eskalacji w rozwiązywaniu problemów powstałych na gruncie realizacji umowy, w tym procedurę umożliwiającą podjęcie natychmiastowych działań w przypadku zagrożeń dla IK wynikających z ataków na infrastrukturę informatyczną.

(17) Umowa powinna zawierać zasady zlecania podwykonawcom poszczególnych czynności wraz z wymogiem stosowania równorzędnych zabezpieczeń, jak wynikających z zawartej umowy głównej.

- Umowa na dostawę oprogramowania systemów automatyki powinna zawierać zapisy zwiększające bezpieczeństwo przed zagrożeniami teleinformatycznymi, tj.: zobowiązanie dostawcy do sprawdzenia, czy dostarczane oprogramowanie nie posiada znanych luk bezpieczeństwa i poinformowania zamawiającego o ewentualnych, istniejących lukach,
- deklarację, iż architektura dostarczanego oprogramowania umożliwia usunięcie ewentualnych luk bezpieczeństwa, które zostaną wykryte w cyklu życia oprogramowania,
- załączony wykaz wszystkich komponentów dostarczanego oprogramowania,

– dodatkowo rekomendowane jest, aby do umowy załączone zostały deklaracje producentów oprogramowania co do stosowanych przez nich zasad usuwania wykrytych luk bezpieczeństwa, zasad informowania użytkowników o wykrytych lukach bezpieczeństwa oraz zasad dystrybucji poprawek.

2.10. Plany ciągłości działania i odbudowy

Działania podejmowane w ramach zapewnienia bezpieczeństwa fizycznego, technicznego, osobowego, teleinformatycznego czy prawnego są działaniami prewencyjnymi, które z założenia mają nie dopuścić do materializacji ryzyka zdarzenia kryzysowego. Pomimo prawidłowego wdrożenia programów ochrony nie jest możliwe 100% wyeliminowanie ryzyk związanych z przerwaniem realizacji procesów biznesowych. Dlatego należy opracować i wdrożyć plan(y) ciągłości działania.

Jedną z metod podjęcia decyzji o kształcie systemu siągłości działania jest zastosowanie istniejących standardów w tym zakresie. Przykładem jest norma ISO/IEC 22301 – wymagania dla systemu zarządzania ciągłością działania.

Plan ciągłości działania jest kompleksowym dokumentem (lub zestawem dokumentów) określającym organizację i sposób postępowania w ramach zaplanowanych działań będącymi reakcją na nagłe i niezależne od organizacji zdarzenie skutkujące przerwaniem realizacji procesów biznesowych. W skład planu BCP powinny wchodzić:

- plan zarządzania kryzysowego - opisujące zasady organizacji i postępowania jednostki kierującej i koordynującej działaniami podejmowanymi w ramach reakcji na zdarzenie kryzysowe,
- plany/procedury awaryjne (contingency plan) koncentrujące się na przywróceniu/wznowieniu działania procesów i zasobów po wystąpieniu awarii,
- plany/procedury odtworzenia utraconych zasobów (DRP – disaster recovery plan).

Przygotowanie planu BCP musi zostać poprzedzone analizą mającą na celu:

- identyfikację procesów biznesowych i zasobów z nimi związanych,
- określenie wpływu zdarzenia na funkcjonowanie organizacji (analiza BIA – Business Impact Analysis),
- zdefiniowanie parametrów odtworzenia i warunków aktywowania planu BCP z uwzględnieniem celów organizacji i dostępnych zasobów,
- określenie strategii przetrwania (deklaracja sposobu postępowania organizacji w przypadku wystąpienia sytuacji kryzysowej).

Po reakcji na incydent i zapewnieniu ciągłości działania kluczowych procesów, należy w jak najszybszym czasie przywrócić pełną (normalną) funkcjonalność infrastruktury krytycznej. Aby uczynić to w sposób sprawny i ograniczający koszty, należy wcześniej przygotować stosowne plany odbudowy (plany te mogą stanowić część planu ciągłości działania).

Skutki zagrożeń powinny zostać oszacowane na etapie oceny ryzyka. Pomimo tego nie ma możliwości przewidzenia wszystkich incydentów i ich wzajemnych oddziaływań, plany powinny być na tyle zwięzłe, na ile to możliwe. W małych organizacjach wystarczy pojedynczy plan obejmujący swoim zakresem wszelkie działania potrzebne do przywrócenia pełnej funkcjonalności infrastruktury krytycznej. W dużych organizacjach, zasadne jest podzielenie planu na części, z których każda szczegółowo przedstawia sposób powrotu do normalnego funkcjonowania obiektów, usług, urządzeń, instalacji w wyniku wystąpienia różnego rodzaju incydentów.

Rekomenduje się podział planów ze względu na strategię odbudowania zasobów:

- ludzkich (wiedza, umiejętności),
- lokalizacji (miejsca pracy),
- technologicznych (instalacje, wyposażenie),
- informacji (rzeczywistych, jak i wirtualnych: umowy, rejestr klientów),
- łańcucha dostaw itp.

Należy wcześniej zidentyfikować potencjalnych dostawców niezbędnych do odbudowy materiałów, produktów lub usług. Jeśli materiały, produkty lub usługi nie są dostępne na rynku „od ręki", wskazane jest zawarcie wstępnych umów umożliwiających uzyskanie pierwszeństwa w realizacji zamówień. W przypadku braku możliwości zawarcia umów z pierwszeństwem należy rozważyć (o ile istnieją techniczne i ekonomiczne możliwości) zmagazynowanie materiałów i produktów kluczowych dla odtworzenia należącej do organizacji IK. O ile jest to uzasadnione, należy zweryfikować jakie źródła finansowania mogą być użyte do odbudowy.

Wszystkie plany muszą uzyskać akceptację kierownictwa i być dostępne dla wszystkich pracowników, na których zostały nałożone obowiązki w fazie reagowania i zarządzania zdarzeniem kryzysowym, aktywowania i wdrożenia planu ciągłości działania oraz odbudowy. Upoważnienia do podejmowania decyzji czy wydatków powinny być jednoznacznie udokumentowane.

Plan powinien zawierać zhierarchizowane cele określające obszary odtwarzanych działalności i przewidywany czas, po którym powinno nastąpić wznowienie funkcjonowania do określonego poziomu. Sukcesywna realizacja celów zapewni powrót IK do stanu sprzed wystąpienia incydentu.

Dobór osób odpowiedzialnych za zarządzanie każdą fazą odbudowy jest kluczowy. Powinny być to osoby posiadające szeroką wiedzę na temat charakterystyki działania infrastruktury krytycznej, sprawne organizacyjnie, które po otrzymaniu powierzonych im zadań, na podstawie przygotowanych planów, opracują długofalową politykę zarządzania działaniami w sytuacji kryzysowej oraz powrotu IK do stanu sprzed katastrofy, jednocześnie wdrażając nowe rozwiązania w celu zapewnienia jeszcze większego poziomu bezpieczeństwa.

Przygotowując plany ciągłości działania i odbudowy, skuteczność procesu można podnieść przez zastosowanie następujących działań:

- uzyskanie i przechowanie w bezpiecznym miejscu planów IK, która musi być odbudowana po awarii – dostęp do planów sprzed awarii może znacznie skrócić proces odbudowy,
- ustalenie (weryfikacja) zasad i terminów wypłaty odszkodowań i ubezpieczenia za utracone elementy IK,
- przygotowanie strategii finansowania odbudowy pozostałej części IK (nie znajdującego pokrycia w odszkodowaniu i ubezpieczeniu),
- ustalenie (weryfikacja) zakresu zgód i zezwoleń, które trzeba będzie uzyskać na wypadek odbudowy infrastruktury,
- uzgodnienie z innymi operatorami IK pod kątem planowanych remontów i innych przestojów podobnej infrastruktury IK,
- określenie zasad, w tym częstotliwości, aktualizacji planów odbudowy,
- okresowe testowanie planów ciągłości działania i odbudowy przez porównanie ich zawartości z planami inwestycji realizowanych przez organizację (to porównanie ma na celu zidentyfikowanie innych istotnych elementów, które są częścią bieżącego planu inwestycyjnego, a mogłyby być dodane do planów odbudowy).

Dobrą praktyką jest integracja systemów zarządzania funkcjonujących w organizacji, m.in:

- Systemu Zarządzania Bezpieczeństwem Informacji;
- Systemu Zarządzania Ciągłością Działania;
- Systemu Zarządzania Usługami IT;
- Systemu Zarządzania Środowiskowego;
- Systemu Zarządzania Jakością.

2.10.1. Zawartość planu ciągłości działania

Organizacja powinna ustanowić udokumentowane procedury reagowania na incydent zakłócający działanie oraz procedury uwzględniające sposoby kontynuowania lub odtwarzania jej działalności w ustalonych ramach czasowych. Takie procedury powinny uwzględnić wymagania osób, które będą ich używać.

Plany ciągłości działania powinny wspólnie obejmować:

(1) Zdefiniowane role i odpowiedzialności osób i zespołów, mających uprawnienia w czasie trwania incydentu i po jego wystąpieniu;
(2) Proces wywołujący reakcję;
(3) Szczegóły zarządzania natychmiastowymi konsekwencjami incydentu, ze szczególnym uwzględnieniem:
    a. dobra poszczególnych osób,
    b. strategicznych, taktycznych i operacyjnych opcji reakcji na zakłócenia,
    c. zapobiegania dalszej stracie lub niedostępności działalności priorytetowych;
(4) Szczegóły dotyczące sposobu i okoliczności, w których organizacja będzie kontaktować się z pracownikami i członkami ich rodzin oraz z kluczowymi stronami zainteresowanymi, a także szczegóły dotyczące kontaktów w nagłych wypadkach;
(5) Sposób kontynuacji lub odtworzenia działalności priorytetowych przez organizację w ustalonych ramach czasowych;
(6) Szczegóły dotyczące kontaktów organizacji z mediami po wystąpieniu incydentu, w tym
    a. strategię komunikacyjną,
    b. preferowaną płaszczyznę komunikacji z mediami,
    c. wytyczne do lub wzór oświadczenia dla mediów,
    d. właściwych rzeczników prasowych;
(7) Proces wycofania planu w przypadku ustąpienia incydentu.

Każdy plan powinien definiować:

(1) Zamiar i zakres;
(2) Cele;
(3) Kryteria i procedury uruchomienia;
(4) Procedury wdrażania;
(5) Role, odpowiedzialności i uprawnienia;
(6) Wymagania i procedury komunikacyjne;
(7) Wewnętrzne i zewnętrzne powiązania i oddziaływania;
(8) Wymagania dotyczące zasobów oraz
(9) Przepływ informacji i procesy dokumentowania.

Zarówno plany ciągłości działania i odbudowy oraz ochrona osobowa, prawna, fizyczna, teleinformatyczna i techniczna, muszą być traktowane równorzędnie, jako kluczowe elementy zarządzania bezpieczeństwem. Zarządzanie bezpieczeństwem wymaga również interdyscyplinarnej wiedzy organizacyjnej, inżynierskiej i humanistycznej oraz skupienia na kompetencjach kierowniczych i pracowniczych we wszystkich jego najważniejszych procesach i usługach je wspomagających. Posiadanie wiedzy na temat zagrożeń, obszarów ich występowania i wzajemnych powiązań i współzależności, a także możliwości podejmowania działań prewencyjnych oraz w procesach zmaterializowania zagrożeń pozwala wszystkim pracownikom i interesariuszom na odpowiedzialne i trwałe budowanie bezpieczeństwa.

Celem opracowania, aktualizacji i stosowania każdego rodzaju planu opartego na zarządzaniu ryzykiem i skutecznym reagowaniu w przypadku wystąpienia incydentu jest wdrażanie przez organizację mechanizmów wzmacniających odporność na zdiagnozowane zagrożenia poprzez redukcje ryzyk do poziomów akceptowalnych i przygotowanie na zdarzenia mogące przynieść niepożądane straty.

3. Słownik skrótów

Lp.	Skrót	Wyjaśnienie	Polskie tłumaczenie
1	*APT*	Advanced Packaging Tool	System zarządzania pakietami
2	*BCP*	Business Continutity Plan	Plan ciągłości działania
3	*BIA*	Business Impact Analisys	Analiza wpływu na biznes
4	*CCTV*	Closed Circuit TeleVision	System telewizji przemysłowej
5	*CERT*	Computer Emergency Response Team	Zespół ds. reagowania na przypadki naruszenia bezpieczeństwa teleinformatycznego
6	*CSIRT*	Computer Security Incident Response Team	Zespół ds. reagowania na incydenty bezpieczeństwa teleinformatycznego
7	*DNS*	Domain Name System	System nazw domenowych
8	*DR*	Disaster Recovery	Przywracanie po awarii
9	*DRP*	Disaster Recovery Plan	Plan przywracania po awarii
10	*ENISA*	European Network and Information Security Agency	Europejska Agencja Bezpieczeństwa Sieci i Informacji
11	*IDS*	Intrusion Detection System	System wykrywania włamań
12	*IK*		Infrastruktura Krytyczna
13	*IPS*	Intrusion Prevention System	System zapobiegania włamaniom
14	*MTBF*	Mean Time Between Failure	Średni czas bezawaryjnej pracy
15	*MTTF*	Mean Time To Failure	Średni czas do wystąpienia usterki
16	*MTTR*	Mean Time To Repairs	Średni czas naprawy
17	*NPOIK*		Narodowy Program Ochrony Infrastruktury Krytycznej
18	*RBM*	Risk Based Maintenance	Utrzymanie oparte na ryzyku
19	*RCM*	Reliability Centered Maintenance	Utrzymanie oparte na niezawodności

Lp.	Skrót	Wyjaśnienie	Polskie tłumaczenie
20	*SCADA*	Supervisory Control And Data Acquisition	System sterowania i akwizycji
21	*SIEM*	Security Information and Event Management	Systemy zarządzania informacjami i zdarzeniami bezpieczeństwa
22	*SKD*		System Kontroli Dostępu
23	*SLA*	Service Level Agreement	Umowa o poziomie usług
24	*SSWiN*		Systemy Sygnalizacji Włamania i Napadu
25	*UDT*		Urząd Dozoru Technicznego
26	*WAN*	Wide Area Network	Sieć rozległa
27	*VLAN*	Virtual Local Area Network	Wirtualna sień lokalna
28	*VPN*	Virtual Private Network	Wirtualna Sieć Prywatna
29	*VL*	Vendor Lock	Uzależnienie od dostawcy
30	*VSS*	Video Surveillance System	System Dozoru Wizyjnego

Spis tabel i rysunków

Spis tabel

Spis rysunków