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 1

1.1. Co zawiera?

Dokument zawiera podstawowe informacje na temat technicznych i organizacyjnych aspektów ochrony infrastruktury krytycznej (IK). Może on posłużyć jako zestaw konkretnych wskazówek dotyczących budowy i funkcjonowania systemu ochrony IK. Dodatkowo w dokumencie można znaleźć ocenę skuteczności poszczególnych metod zapewnienia bezpieczeństwa, jak również propozycję strategii implementacji, która zapewni, że będzie ona najbardziej efektywna.

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, może jednak posłużyć jako rozbudowana lista kontrolna tego, jak należy zorganizować system ochrony IK.

Przypisanie niektórych środków i zasad ochrony IK do konkretnych obszarów bezpieczeństwa często nie jest oczywiste i jednoznaczne (występują środki, które mogą być przypisane w różnych obszarach). Podział dokonany w dokumencie służy jedynie opisowi i nie może być traktowany jako ostateczny.

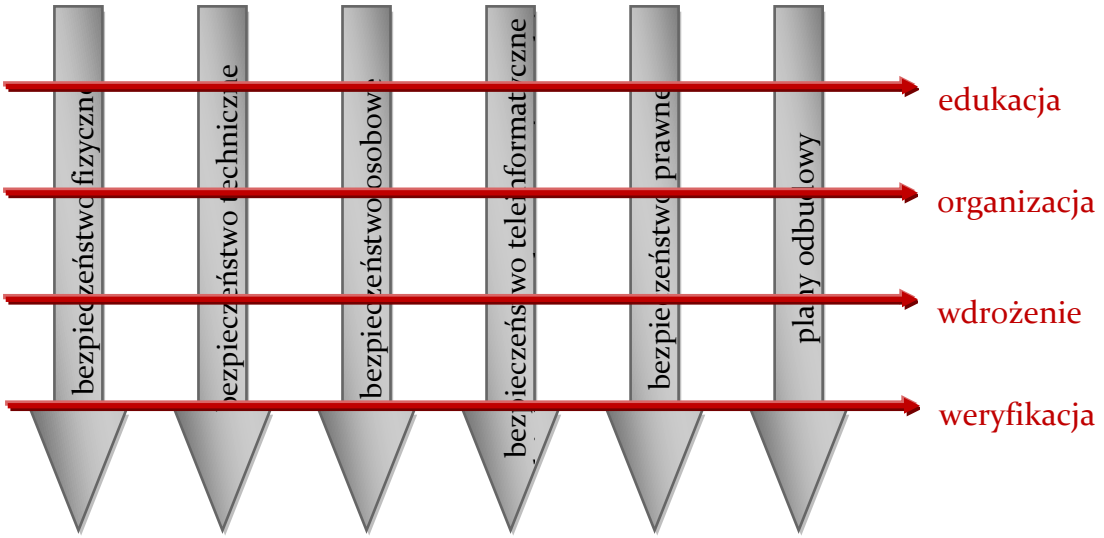
Biorąc pod uwagę, że adresatami niniejszego załącznika są zarówno podmioty stosujące różne rodzaje ochrony ze względów biznesowych oraz takie, które po raz pierwszy zetkną się z takimi zagadnieniami, w przedłożonym materiale zastosowano poziom szczegółowości adekwatny do wszystkich jego adresatów.

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 organizacji.

Bez względu na to, jakie rodzaje ochrony zostaną wybrane i wprowadzone w życie w organizacji, cztery elementy mają znaczenie we wdrożeniu wszystkich ich rodzajów:

(1) Prowadzenie działań edukacyjnych.
(2) Właściwa struktura organizacyjna pionu zarządzania bezpieczeństwem.
(3) Wybór strategii wdrożenia.
(4) Weryfikacja przyjętych rozwiązań i ich aktualizacja.



Rys. 1. 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,
- 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:

Rys. 2. 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.

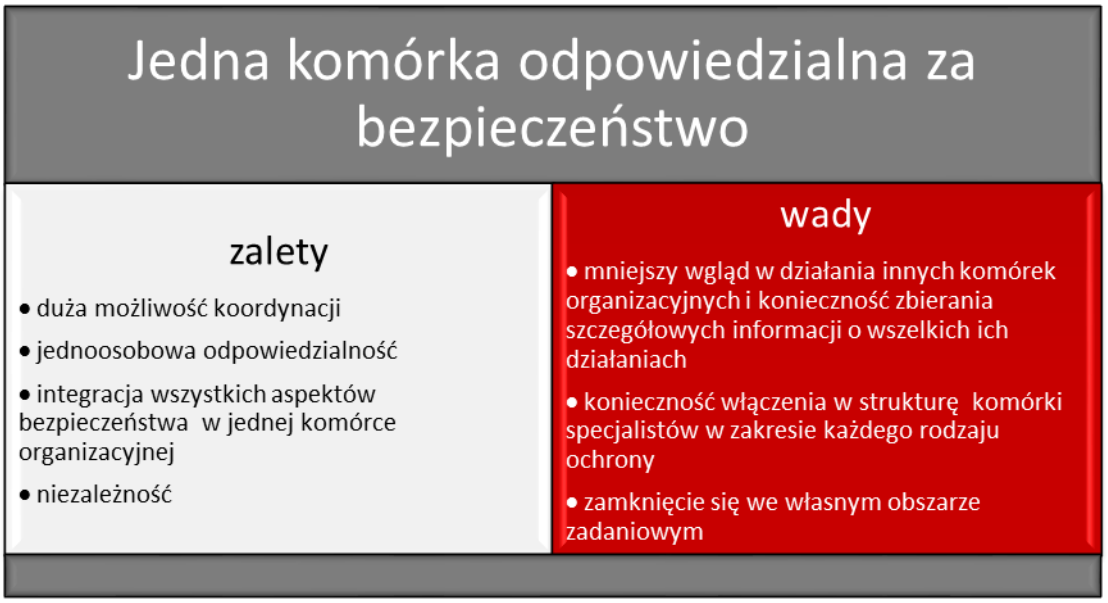
Działania edukacyjne są podstawowym elementem budowy kultury bezpieczeństwa organizacji. Kultura bezpieczeństwa oznacza współodpowiedzialność członków organizacji za bezpieczeństwo, przejawiające się obserwacją, informowaniem o możliwości jego zagrożenia (brak tolerancji dla zaniechań) i dążeniem do jego poprawy. Kultura bezpieczeństwa obejmuje system wartości, wzorce zachowań oraz wiedzę członków organizacji wraz z ich stosunkiem do tych elementów.

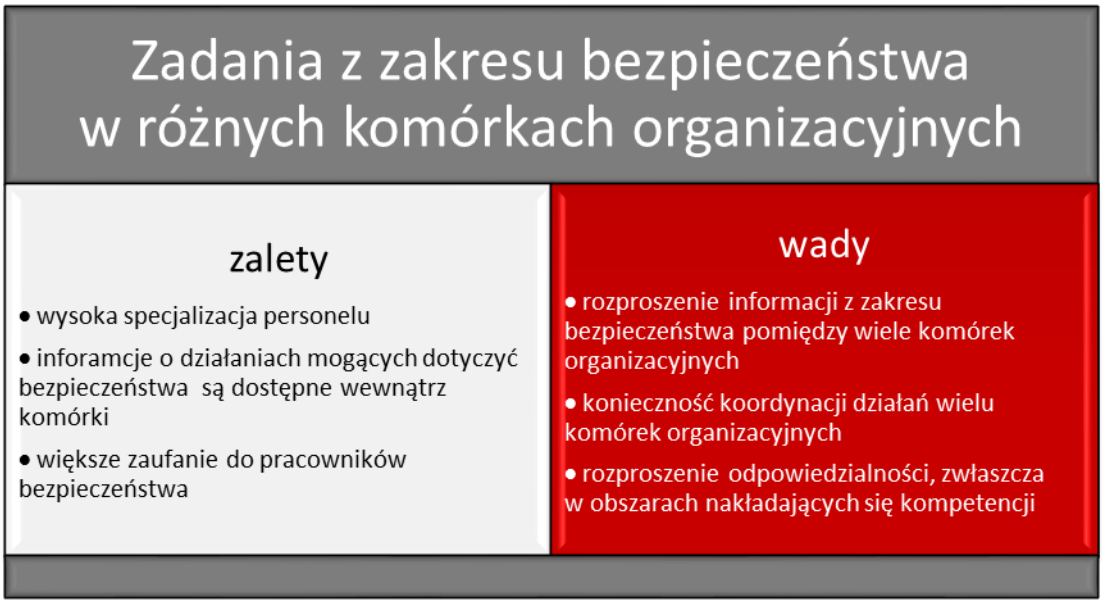
Należy także rozważyć przygotowanie dedykowanego materiału szkoleniowego podnoszącego świadomość Kierownictwa organizacji. Bez zbudowania odpowiedniego wsparcia ze strony Kierownictwa trudno będzie osiągnąć zakorzenienie systemu bezpieczeństwa w organizacji: problemy z budżetem, a przede wszystkim brak przekonania do konieczności budowy systemu zarządzania bezpieczeństwem mogą znacznie ograniczyć efektywność systemu w organizacji. Stąd konieczność przygotowania materiałów edukacyjno-szkoleniowych także dla Kierownictwa organizacji. Należy także zachęcać Kierownictwo do udziału w bezpośrednich działaniach promujących system zarządzania bezpieczeństwem w organizacji – „przykład idzie z góry", a więc Kierownictwo w swoich działaniach powinno dawać przykład przestrzegania zasad bezpieczeństwa wprowadzonych w organizacji, a także nawiązywać do systemu zarządzania bezpieczeństwem w komunikacji z załogą (spotkania, newslettery, itp.).

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. Poniżej przedstawiono przykładowe zestawienie wad i zalet obydwu modeli.

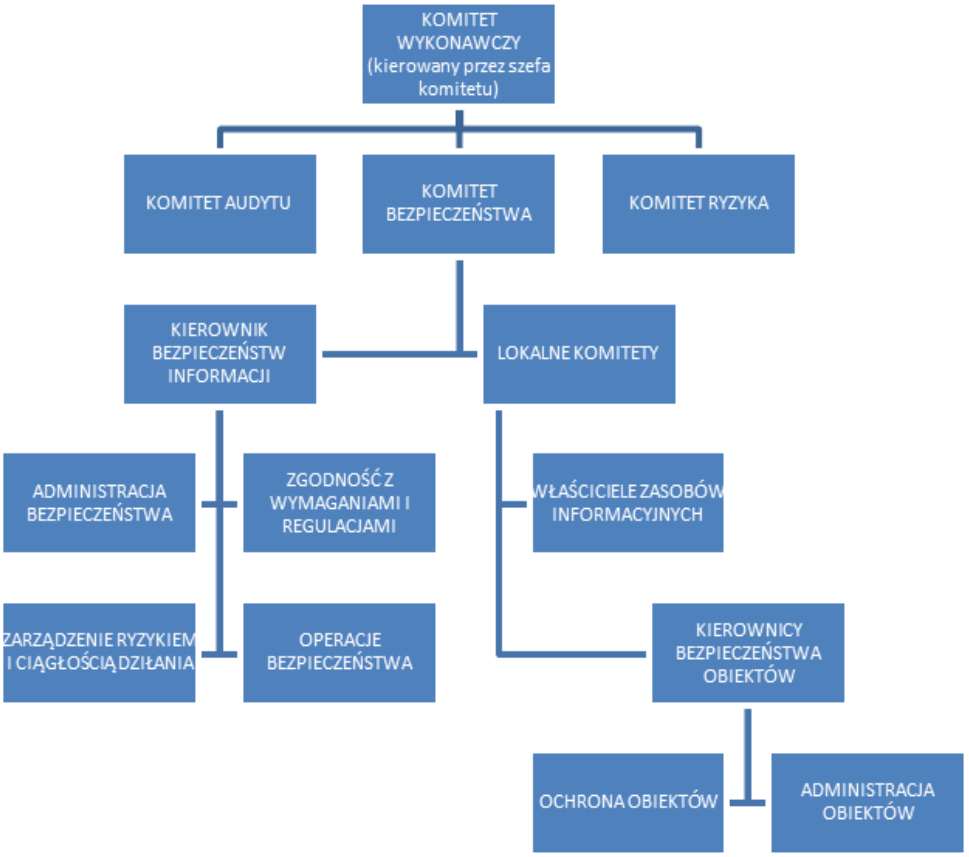




Wybór konkretnego modelu zależy od przyjętego w organizacji stylu zarządzania, wymagań i możliwości organizacyjno-finansowych.

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 27002:2014.

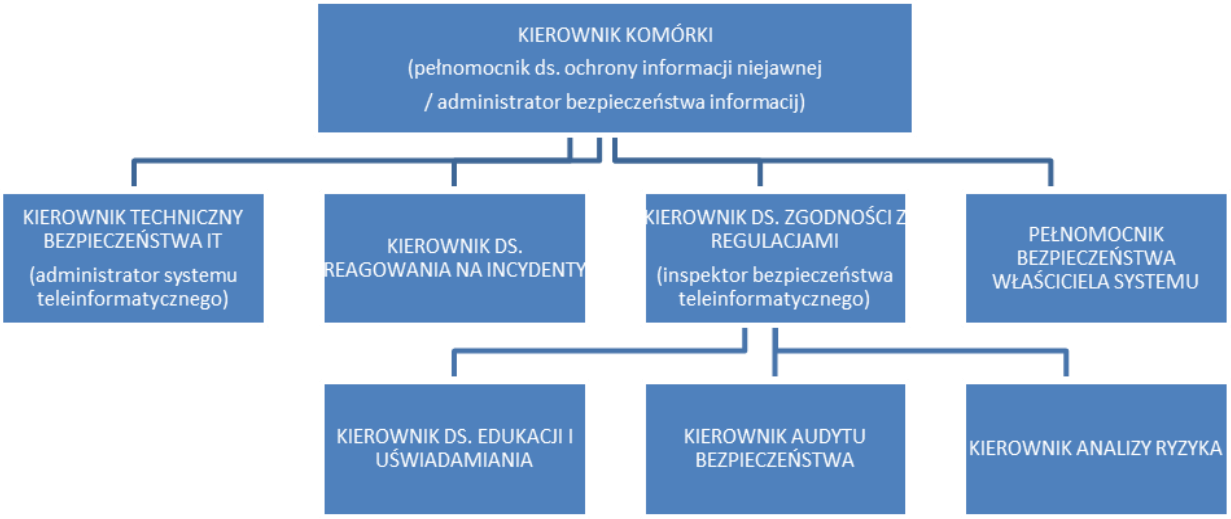


Rys. 3. Przykładowa struktura organizacyjna pionu bezpieczeństwa teleinformatycznego.

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 29 sierpnia 1997 r. o ochronie danych osobowych.



Rys. 4. Struktura organizacyjna komórki zapewnienia bezpieczeństwa teleinformatycznego.

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[1].

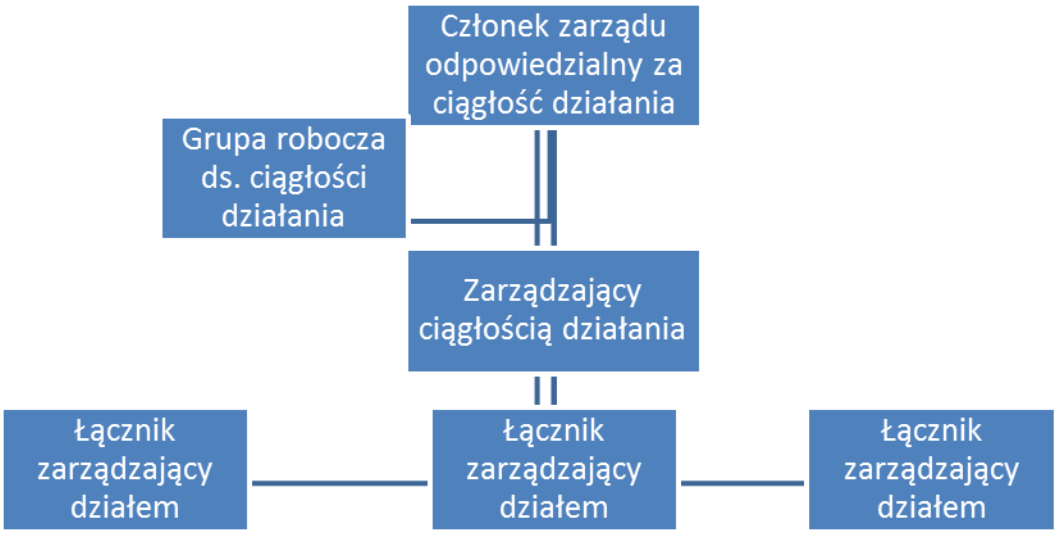
Tabela 1 Opis stanowisk wynikających z właściwych ustaw

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
KIEROWNIK DO	Tak	Nadzór i kontrola nad prawidłowym zaprojektowaniem,	N/D

[1] 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
SPRAW ZGODNOŚCI Z REGULACJAMI (obligatoryjne)		wdrożeniem i utrzymaniem zasad i mechanizmów zapewniających bezpieczeństwo teleinformatyczne	
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 22301:2012) dotyczącej zarządzania ciągłością działania organizacji.



Rys. 5. Przykładowa struktura organizacji ciągłości działania[2].

[2] John Sharp – The Route Map to Business Continuity Management. Meeting the Requirements to BS 25999 – British Standard Institution 2008.

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).

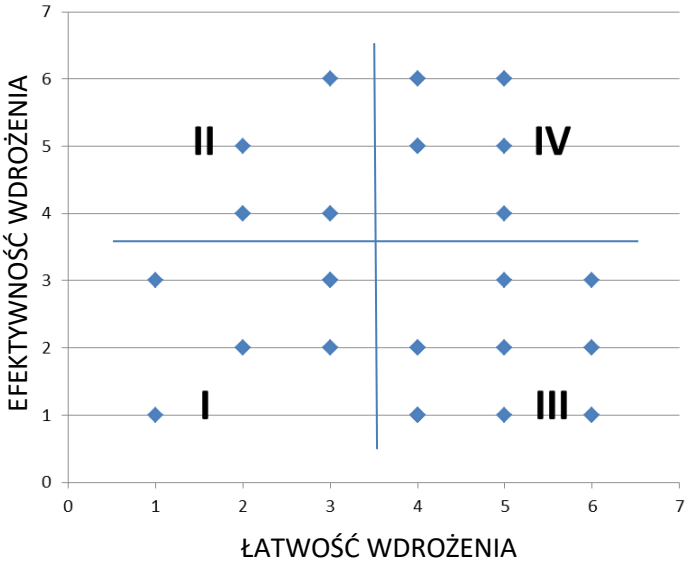
W oparciu o powyższe wartościowanie jesteśmy w stanie stworzyć graficzną reprezentację wartości wskaźników dla wszystkich proponowanych zasad i technik bezpieczeństwa. Dzieląc obszar pokazujący poziom efektywności i łatwość wdrożenia na ćwiartki, otrzymujemy przypisanie poszczególnych zasad bezpieczeństwa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



Rys. 6. 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 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 2 Przykładowa tabela oceny zasad

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 w przedsiębiorstwie politykami bezpieczeństwa. W odróżnieniu od projektów i programów, które nieodłącznie wiążą się ze zmianami w środowisku teleinformatycznym, 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 teleinformatyczne, np. wspólne bazy danych. Obecnie, w celu 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 (takie jak sterowniki PLC). 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[3] 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,

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

- test systemu,
- przegląd procedur,
- 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 3 Przykładowe ataki na infrastrukturę krytyczną

Rodzaj naruszenia	Czas/miejsce	Opis
Zamach terrorystyczny	19.04.1995 Oklahoma City USA	Eksplozja ciężarówki wypełnionej 2300 kg ANFO[4] 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.

[4] 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.

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. z 2014 r. poz. 1099 oraz z 2015 r. poz. 1505). 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 praktyka jest podział terenu, na którym zlokalizowana jest IK na strefy ochrony[5] i zaprojektowanie ich zgodnie z zasadą ochrony w głąb (ochrona powłokowa). Niekiedy wyróżnia się także strefę zewnętrzną poza obiektem.

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

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 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 przeszukania 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. nr 166 poz. 1128).

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*[6]

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.

[6] 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:

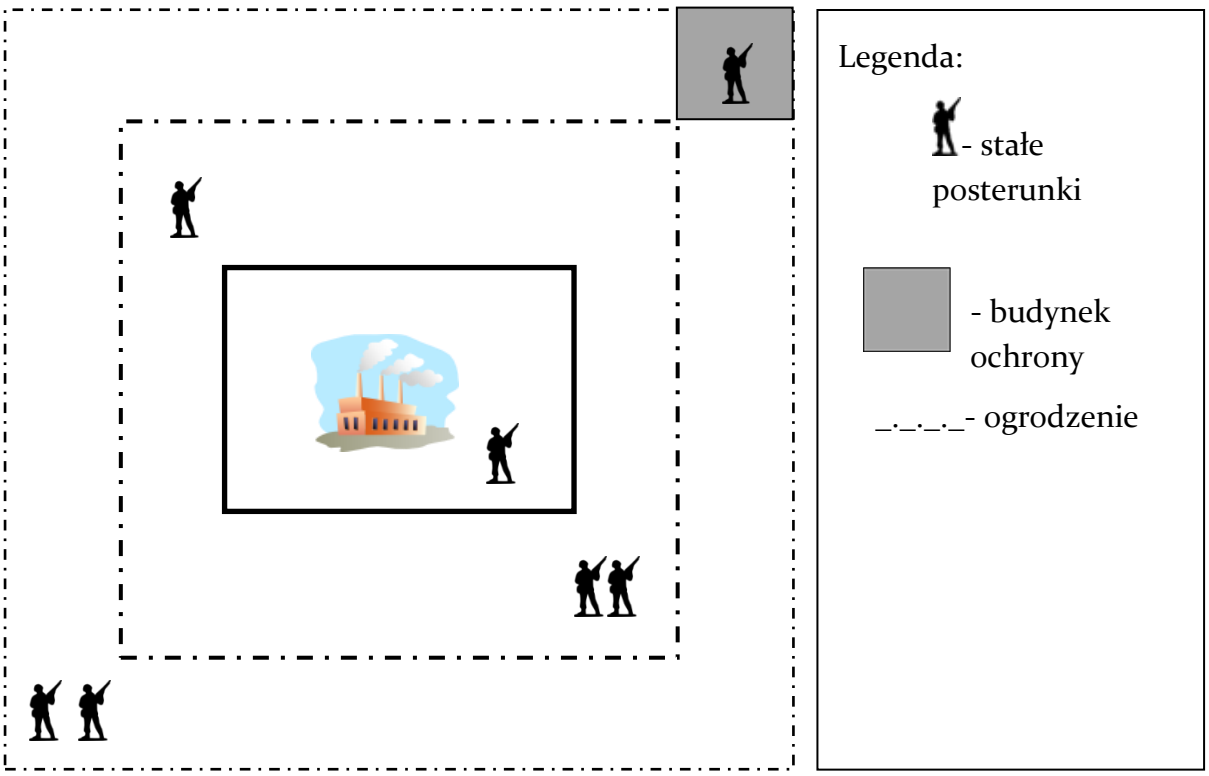
- wielowarstwowa ochrona,
- wielowarstwowy system wykrywania,
- stałe posterunki ochronne.

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.



Rys. 7. Ilustracja funkcjonowania modelu statycznego.

Model ruchomy:

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

Główne cechy:

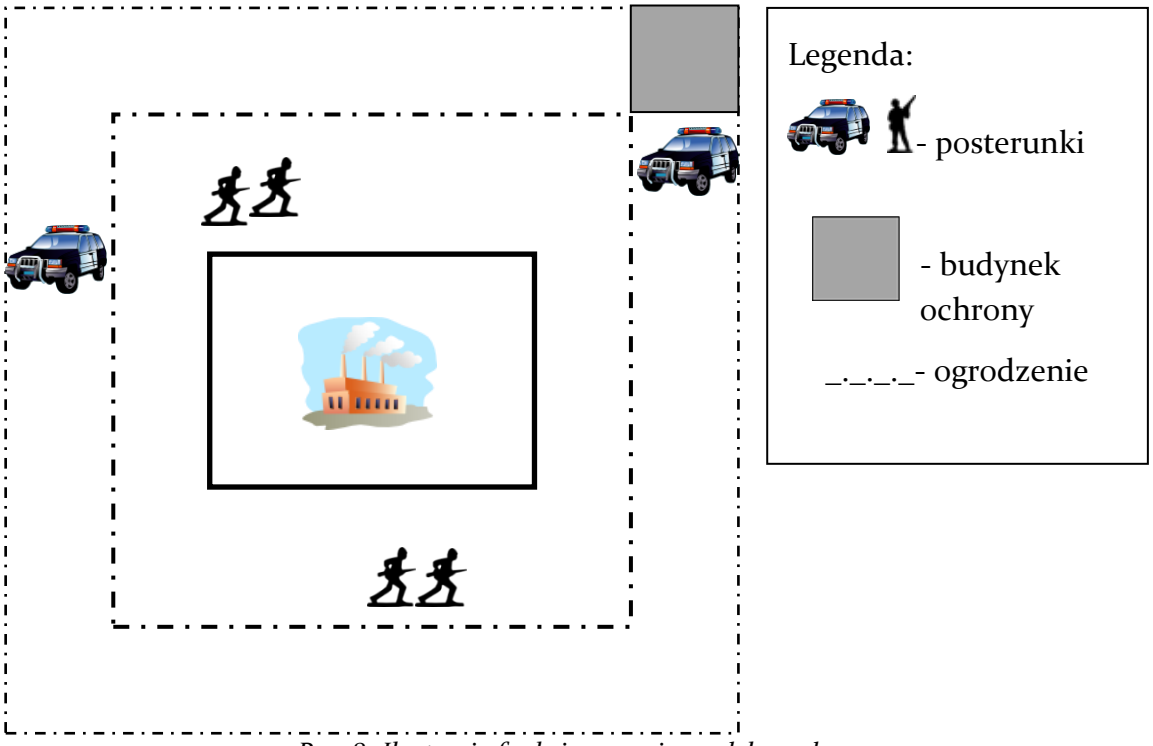
- używane są różne systemy elektroniczne uzupełniające działania służb ochrony,
- służba ochrony może się swobodnie poruszać po całym obiekcie.

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.



Rys. 8. Ilustracja funkcjonowania modelu ruchomego.

Model mieszany:

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

Główne cechy:

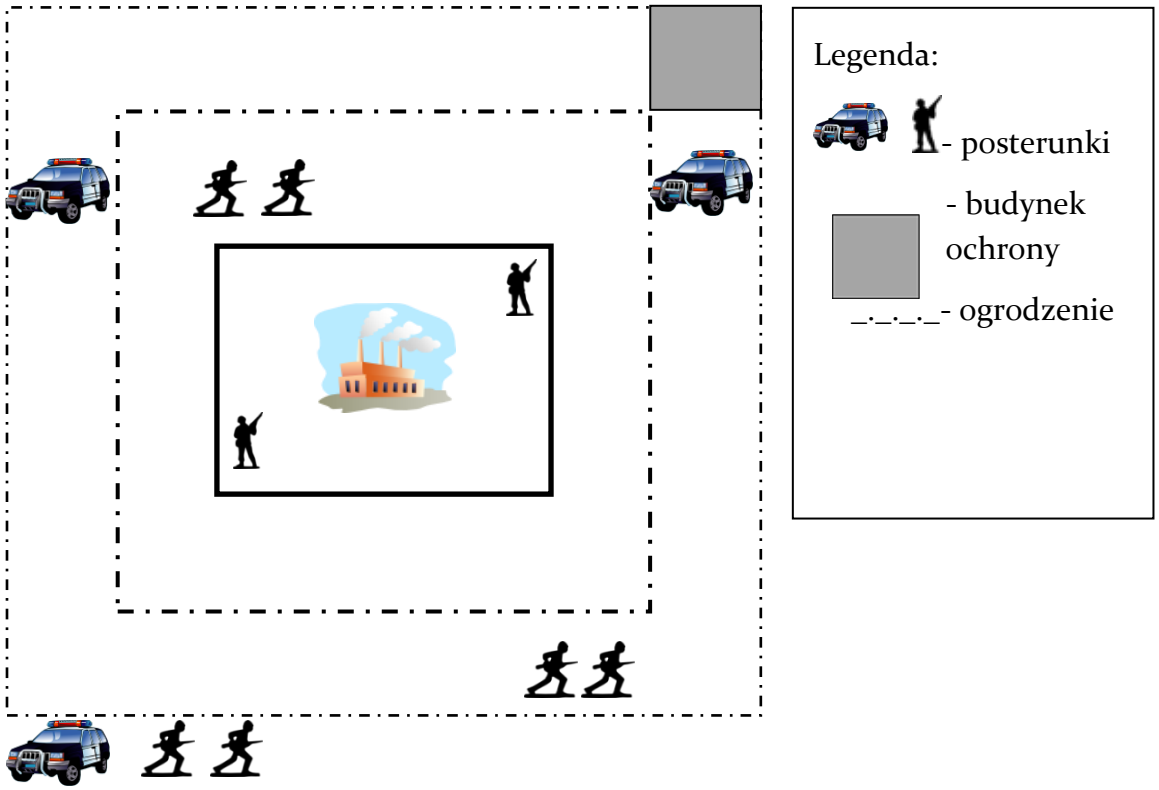
- wielowarstwowa ochrona,
- zgrane elementy ochrony statycznej z ruchomymi patrolami,
- stałe posterunki ochronne.

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.



Rys. 9. 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 (ustawa o ochronie osób i mienia, zasady interwencji, użycia środków przymusu bezpośredniego oraz broni 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, które regulują wewnętrzne przepisy. Na czas pobytu w obiekcie powyższe osoby powinny deponować broń i urządzenia w pomieszczeniu depozytowym nadzorowanym przez podmioty realizujące ochronę fizyczną infrastruktury krytycznej.

2.5.3. *Techniczne środki zapewnienia bezpieczeństwa fizycznego*[7]

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.

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

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.
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)[8]

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,
- 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)[9].

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.

---

[8] 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.

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

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. nr 166 poz. 1128),
  - 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. 19.06.2012 r. 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 kategorię B2 zgodnie z rozporządzeniem Ministra Kultury z 16.09.2002 *w sprawie postępowania z dokumentacją, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych*. (Dz. U. 2002 nr 167 poz. 1375).

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, by wszystkie wdrażane zabezpieczenia spełniały zalecenia zapisane w odpowiednich, najaktualniejszych normach. Przykładowe grupy norm będące w użyciu w 2015 r.:

- 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,
- System dozorowe CCTV stosowane w zabezpieczeniach – normy PN-EN 62676,
- Drzwi, okna, ściany osłonowe, kraty i żaluzje - Odporność na włamanie– norma PN-EN 1627.

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 analizą zagrożeń może być nieefektywny.
8. Fizyczne ataki na infrastrukturę krytyczną często prowadzą do ogromnych strat.

2.6. Zapewnienie bezpieczeństwa technicznego

Zapewnienie bezpieczeństwa technicznego to zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie zaburzenia realizowanych procesów technologicznych.

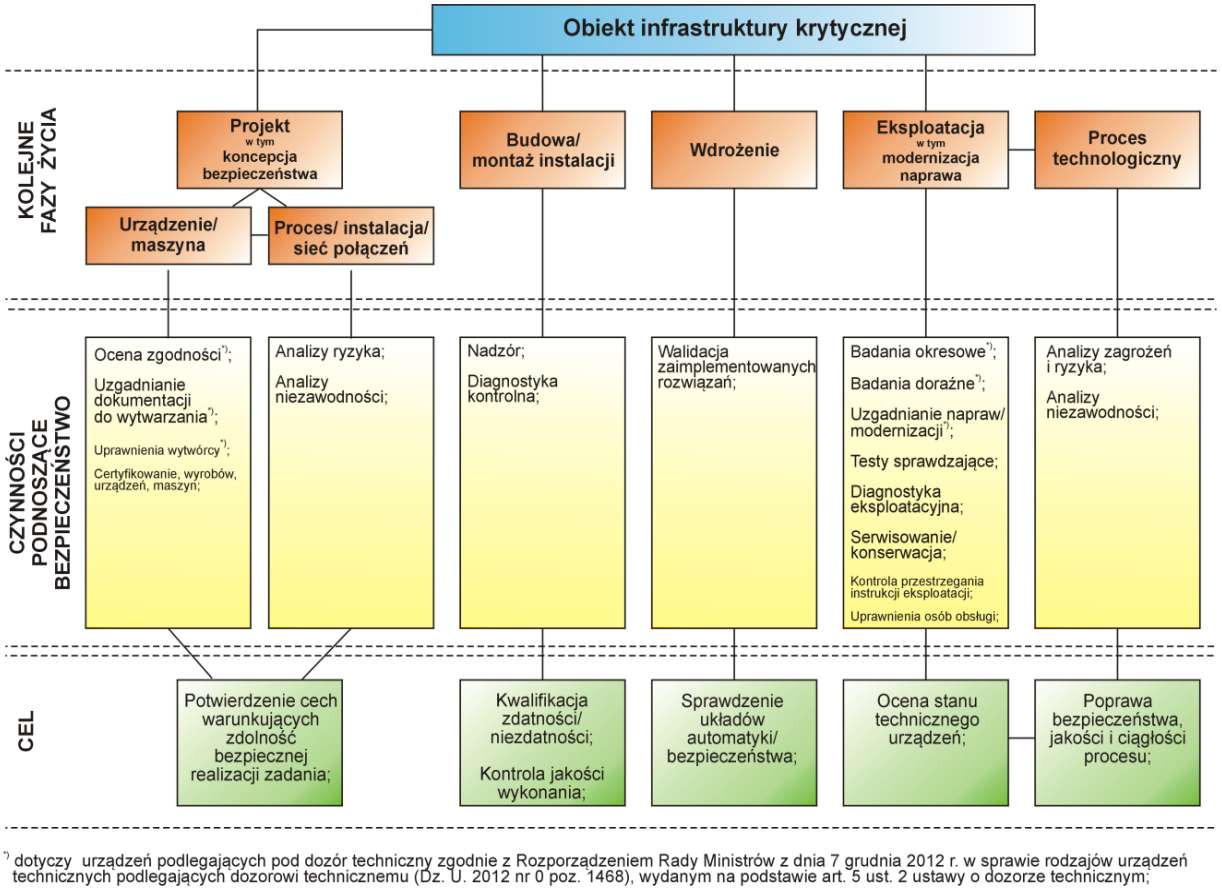
Podstawowym i najskuteczniejszym sposobem zapewnienia bezpieczeństwa technicznego IK jest przestrzeganie mających zastosowanie do danej infrastruktury aktów prawnych, norm oraz reżimów eksploatacyjnych. Zaniechania lub wyłączenia ze stosowania są najczęstszymi przyczynami zakłócenia funkcjonowania infrastruktury.

Bezpieczeństwo obiektów technicznych infrastruktury krytycznej zależy od procesów realizowanych w ramach danego obiektu, dotyczy wszystkich jego etapów cyklu życia, wymaga zaangażowania pracowników wszystkich szczebli i związane jest z zasadami oraz praktykami bezpieczeństwa:

- technicznego,
- pożarowego,
- chemicznego,
- 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,
- PN-N 18001 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 22313:2012 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.



Rys. 10. Wybrane czynności podnoszących bezpieczeństwo obiektów technicznych infrastruktury krytycznej w kolejnych fazach życia[10].

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!

[10] Źródło: UDT.

2.6.1. Cztery podstawowe elementy zapewnienia bezpieczeństwa technicznego

System odporny na zakłócenia powinien cechować się:

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

Zależnie od sytuacji i eksploatacyjnego znaczenia urządzeń wchodzących w skład systemu, 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 4 Pomiar dostępności[11]

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.

[11] 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.

średni czas postoju powinien być szacowany już od momentu uszkodzenia do momentu przywrócenia systemu do określonego stanu Często zdarza się, że czas ten liczony jest dopiero od momentu 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).**

systemów zasilania w energię elektryczną[12]

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

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

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[13].

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

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 długoeksploatowanych 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 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 2015 r. poz. 1422),
- Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 7 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz. U. Nr 109, poz. 719),
- 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. 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[14]

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**[15]**,** 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:

- 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 samotestowania[16].

---

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

[15] 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.

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

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 5*):

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

Tabela 5 Bezpieczeństwo a trzy niezależne warstwy ochrony[17]

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 skutkami awarii**	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 systemy zrzutu awaryjnego, zawory bezpieczeństwa systemy detekcji wycieku gazu i pożaru bariery, obudowy, tace i in.
Poziom ochrony przeciwdziałającej tzw. warstwa łagodzenia	systemy gaśnicze i neutralizacji (np. instalacje wodne, pianowe, kurtyny wodne, hydranty), personel i ratownicy na obiektach (np. ratownictwo chemiczne)

[17] Źródło: Opracowanie UDT.

TEORIA	PRAKTYKA
Cel: przeciwdziałanie skutkom awarii dla ludzi i środowiska	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 budowlane wraz ze związanymi z nimi urządzeniami budowlanymi należy, biorąc pod uwagę przewidywany okres użytkowania, projektować i budować w sposób określony w przepisach, w tym techniczno-budowlanych, oraz zgodnie z zasadami wiedzy technicznej, zapewniając m.in.:

(1) spełnienie wymagań podstawowych dotyczących:
   a) bezpieczeństwa konstrukcji,
   b) bezpieczeństwa pożarowego,
   c) bezpieczeństwa użytkowania,
   d) odpowiednich warunków higienicznych i zdrowotnych oraz ochrony środowiska,
   e) ochrony przed hałasem i drganiami,
   f) odpowiedniej charakterystyki energetycznej budynku oraz racjonalizacji użytkowania energii;
(2) warunki użytkowe zgodne z przeznaczeniem obiektu, 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;
(3) możliwość utrzymania właściwego stanu technicznego;
(4) ochronę ludności, zgodnie z wymaganiami obrony cywilnej;
(5) ochronę obiektów wpisanych do rejestru zabytków oraz obiektów objętych ochroną konserwatorską;
(6) odpowiednie usytuowanie na działce budowlanej;
(7) warunki bezpieczeństwa i ochrony zdrowia osób przebywających na terenie budowy.

Obiekty budowlane 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 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 m² oraz innych obiektów budowlanych o powierzchni dachu przekraczającej 1000 m²; 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 wszelkiego rodzaju zagrożeń. W praktyce najczęściej przeprowadza się ewakuację osób poszkodowanych lub bezpośrednio zagrożonych (także zagrożonego mienia) po wystąpieniu zdarzenia niebezpiecznego. Ewakuacja może mieć również charakter prewencyjny, tzn. może być prowadzona z terenów i obiektów, w przypadku zbliżającego się zagrożenia, np. związanego z rozprzestrzenianiem się zaistniałych zdarzeń niebezpiecznych lub groźbą prowadzenia działań militarnych, w przypadku zagrożeń wojennych. 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 oraz praktyczne sposoby jej sprawdzania określane są w instrukcji bezpieczeństwa pożarowego.

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.

Najważniejsze rekomendacje dotyczące zapewnienia bezpieczeństwa technicznego:

1. Podstawowym sposobem zapewnienia bezpieczeństwa technicznego IK jest przestrzeganie mających zastosowanie do danej infrastruktury aktów prawnych, norm oraz reżimów eksploatacyjnych.
2. 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.
3. 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.
4. Dla obiektów, w których zlokalizowane są elementy infrastruktury krytycznej należy przyjmować najwyższe wymagania dotyczące niezawodności zasilania i dostępu do mediów.
5. Zapewnienie możliwości kontynuacji działalności w lokalizacji zapasowej jest najlepszym sposobem zapewnienia ciągłości działania.

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[18].

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.

[18] 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. W przypadku gdy przepisy prawa na to pozwalają, należy żądać zaświadczenia lub oświadczenia o niekaralności.

2.7.3. *Postępowanie w stosunku do zatrudnionych*

Priorytetem w zapewnieniu bezpieczeństwa osobowego jest dokładne sprawdzenie pracownika 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*[19]

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) kolorem, w celu szybkiego rozpoznania każdego nielegalnie przebywającego w danym obszarze pracownika i podjęcia odpowiednich kroków. Tam, gdzie ma to uzasadnienie,

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

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.

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

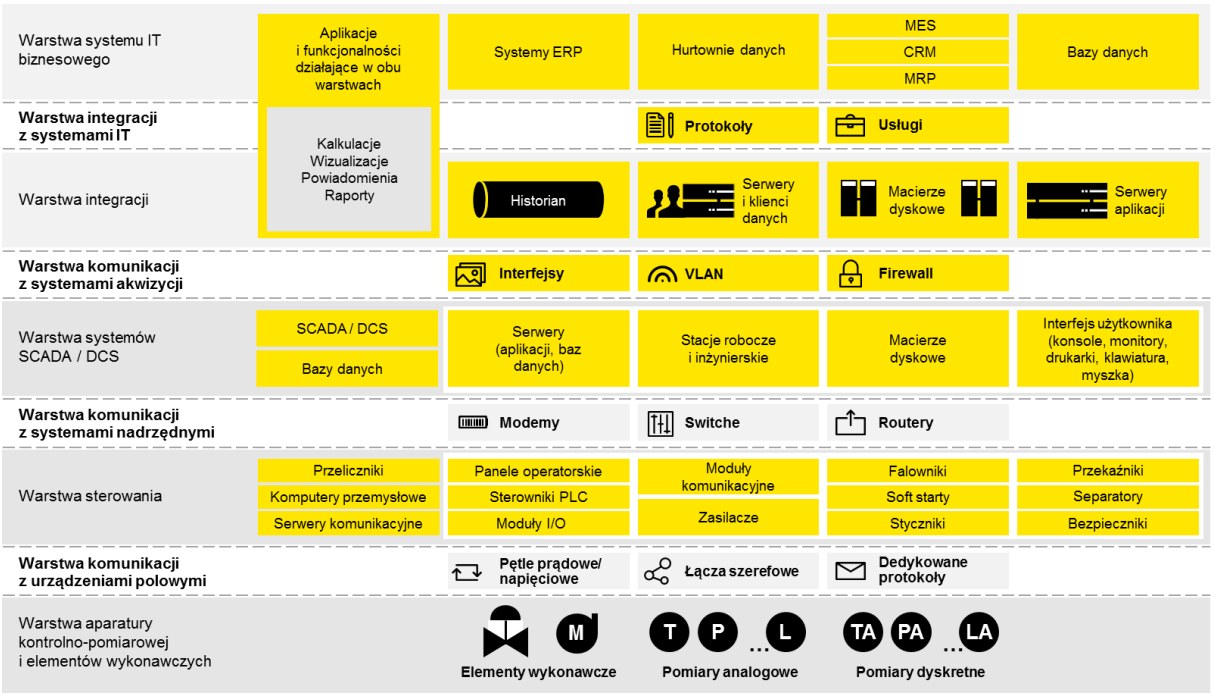
Zapewnienie bezpieczeństwa teleinformatycznego infrastruktury krytycznej to zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie nieautoryzowanego oddziaływania na aparaturę kontrolną oraz systemy i sieci teleinformatyczne, włączając 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[20] 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.

[20] 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*.

2.8.1. Środowisko systemów i sieci teleinformatycznych operatorów infrastruktury krytycznej

Środowisko teleinformatyczne operatorów IK można przedstawić w postaci modelu warstwowego, którego najwyższą warstwę stanowią klasyczne systemy IT, a najniższą aparatura kontrolno-pomiarowa oraz elementy wykonawcze oddziałujące na procesy technologiczne. W zależności od systemu IK, środowisko teleinformatyczne operatora może składać się z jednej lub więcej warstw. Model warstwowy środowiska systemów i sieci teleinformatycznych przedstawia poniższy rysunek:



Rys. 11. Model warstwowy środowiska teleinformatycznego infrastruktury krytycznej[21].

Najwyższa warstwa prezentowanego modelu (warstwa systemów IT) występuje u praktycznie wszystkich operatorów IK. Szczególnie istotna jest ona dla operatorów takich systemów jak sieci teleinformatyczne, sieci energetyczne, czy system finansowy. Znaczenie systemów i sieci IT będzie w ciągu najbliższych lat stale rosło dla wszystkich systemów IK.

Pozostałe (niższe) warstwy występują u operatorów infrastrukturalno-przemysłowych (np. w sektorze ropy i gazu, energii elektrycznej, wodnokanalizacyjnym). Warstwą, która jest najbliżej infrastruktury i procesu przemysłowego jest warstwa aparatury kontrolno-pomiarowej i elementów wykonawczych. Komunikuje się ona z warstwą sterowania, która zawiera urządzenia (często programowalne) zbierającą dane o stanie procesu przemysłowego i realizujące na tej podstawie odpowiednie algorytmy sterowania. Sygnały wyjściowe z tych urządzeń przekazywane są na elementy

[21] EY OT Advisory.

wykonawcze (takie jak pompy czy zawory) bezpośrednio oddziałujące na procesy przemysłowe. Informacje z urządzeń warstwy sterowania komunikują się z również z warstwą systemów nadrzędnych, takich jak SCADA czy DCS. Systemy te pełnią rolę interfejsu użytkownika dla operatorów i pozwalają na monitorowanie oraz sterowanie (również zdalne) stanem procesu technologicznego. Gromadzeniem danych, zaawansowaną analityką oraz raportowaniem i udostępnianiem informacji do systemów IT zajmują się systemy warstwy integracji (np. specjalistyczne, przemysłowe bazy danych, tzw. Historiany).

2.8.2. *Przykłady cyberataków na infrastrukturę krytyczną*

O tym, że cyberatak na IK nie jest zagrożeniem czysto teoretycznym, świadczy wiele przykładów z przeszłości potwierdzających takie możliwości. Poniżej krótko zostały przedstawione niektóre z nich.

Tabela 6 Lista przykładowych cyberataków

Cyberatak	Czas, miejsce	Sektor	Opis
Worcester Air Traffic Communications Attack	1997, Stany Zjednoczone	Transport lotniczy	Atakujący doprowadził do wyłączenia na lotnisku w Worcester linii telefonicznych obsługujących wieżę kontrolną, służby ochrony lotniska, lotniskowej straży pożarnej, służby pogodowej. Również unieruchomiony został system oświetlenia pasa startowego[22].
System dostawy wody pitnej	1999, Australia	Dostawa wody	Przykład sabotażu przeprowadzony przez byłego pracownika firmy, który doprowadził do dezaktywacji systemu alarmowego, co w konsekwencji wprowadziło zakłócenia w dostawie pitnej wody, w tym jej zanieczyszczenie. Cyberatak był zemstą za odmówienie zatrudnienia. System

[22] http://gspp.berkeley.edu/iths/Tsang_SCADA%20Attacks.pdf

Cyberatak	Czas, miejsce	Sektor	Opis
			obsługiwany był drogą radiową[23].
System sygnalizacji kolei CSX	2003, Stany Zjednoczone	Transport kolejowy	Robak internetowy SoBig zainfekował system komputerowy obsługujący ruch kolejowy kompanii CSX, obsługującej 23 stany amerykańskie. Awaria spowodowała odwołania pociągów i opóźnienia w transporcie kolejowym[24].
Zanik dostawy prądu w pn.-wsch. części Ameryki Północnej	2003, Stany Zjednoczone, Kanada	Dostawa energii elektrycznej	Awaria dostawy prądu dotyczyła obszaru zamieszkałego przez około 50 mln osób na terytorium dwóch krajów. Niektóre analizy tej awarii wskazały na jej powiązanie z wystąpieniem w tym samym okresie robaka internetowego Blaster, który mógł zakłócić system alarmujący o awarii. Całkowity koszt strat wyniósł między 4 a 10 mld dolarów amerykańskich.
System filtracji wody	2006, Stany Zjednoczone	Dostawa wody	Atakujący przejął kontrolę nad głównym komputerem zarządzającym systemem filtracji wody. Używał go do rozsyłania spamu oraz przetrzymywania pirackiego oprogramowania. Atakujący najpierw włamał się na podłączony do Internetu komputer pracownika firmy obsługującej system, a następnie w sposób zdalny zainstalował

[23] http://217.148.85.64/UserFiles/File/TNO-DV%202008%20C096_web.pdf

[24] http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=13100807

Cyberatak	Czas, miejsce	Sektor	Opis
			wirusa i oprogramowanie szpiegujące na głównym serwerze obsługującym system filtracji[25].
Atak na rurociąg	2008, Turcja	Przesył ropy	Hakerzy wyłączyli systemy alarmowe rurociągu wraz z wszelkimi systemy komunikacji oraz wywołali w rurociągu znaczny wzrost ciśnienia co doprowadziło do eksplozji. W wyniku ataku na systemy alarmowe oraz komunikacji, pracownicy bezpieczeństwa odpowiedzialni za monitoring rurociągu o całym wydarzeniu dowiedzieli się z przeszło 40 minutowym opóźnieniem i to nie poprzez informacje wygenerowaną automatycznie z systemu, a od pracownika, który zobaczył płomienie.
Wirus Stuxnet	2010, Iran	Energia atomowa	Wirus Stuxnet w sposób dedykowany zaatakował systemy obsługujące irańskie elektrownie atomowe. Cyberatak był bardzo precyzyjny i spowodował poważne kłopoty w funkcjonowaniu elektrowni[26].

[25] http://blogs.abcnews.com/theblotter/2006/10/hackers_penetra.html

[26] http://www.us-cert.gov/control_systems/pdf/ICSA-10-272-01.pdf

Cyberatak	Czas, miejsce	Sektor	Opis
Atak na hutę	2014, Niemcy	Metalurgia	Atakujący skutecznie uzyskali dostęp do sieci biznesowej wykorzystując pocztę korporacyjną, a następnie uzyskali dostęp do sieci produkcyjnej. Po przejęciu kontroli nad systemami przemysłowymi atakujący dokonali ataku na systemy nadzorujące bezpieczne wygaszenie pieca hutniczego. W rezultacie doszło do nieplanowanego wyłączenie pieca i sporych zniszczeń[27].

Cyberataki na systemy IK stały się częścią konfliktów cybernetycznych cyberprzestrzeni, w tym konfliktów między państwami. Z racji trudności, jakie niesie ze sobą precyzyjna identyfikacja źródeł cyberataków w sieci, lub celowe ich rozproszenie, trudno jest jednoznacznie udowodnić zaangażowanie się państw w cyberataki sieciowe. Niemniej jednak analiza cyberataków z ostatnich lat wskazuje na możliwość takich powiązań, choć należy jasno zaznaczyć, że powiązania te nie zostały w sposób oficjalny potwierdzone.

[27] http://www.wired.com/2015/01/german-steel-mill-hack-destruction/

2.8.3. Zasady bezpieczeństwa teleinformatycznego IK

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[28]:

- 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[29].

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**.

Należy zwrócić uwagę, iż systemy zlokalizowane na różnych warstwach modelu środowiska teleinformatycznego zaprezentowanego na rys. 9 mają różne priorytety do cech bezpieczeństwa. O ile systemy warstw IT ze swojej natury przetwarzają dużą ilość informacji wrażliwych (w tym danych osobowych) wymagających ochrony przed dostępem przez osoby nieuprawnione, tak dla systemów automatyki na pierwszy plan wysuwają się zagadnienia związane z zapewnieniem ciągłości dostępu do informacji i zapewnienia ich integralności. Systemy automatyki bardzo rzadko zawierają dane, które można uznać za wrażliwe z punktu widzenia przechowywanych informacji.

Rozwój technologii, w tym technologii sieciowych, jest bardzo dynamiczny. Jednym z priorytetów tego rozwoju jest minimalizacja kosztów obsługi IK. Dlatego coraz

---

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

[29] 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.

częściej w jej obsłudze stosuje się rozwiązania przynajmniej w części bazujące na systemach standardowych. Również zdalne zarządzanie tymi systemami jest jednym z priorytetów. Obydwa te czynniki, tj. stosowanie uniwersalnych rozwiązań i funkcjonowanie systemów sterowania w strukturze ogólnodostępnej sieci Internet, wpływają na wzrost ryzyka zakłócenia funkcjonowania IK, w szczególności przez zwiększenie podatności na zagrożenie w postaci dedykowanego sieciowego cyberataku z zewnątrz lub narażenie się na oddziaływanie negatywnych zjawisk sieciowych, takich jak rozprzestrzeniające się wirusy, robaki sieciowe czy ograniczenie dostępu do sieci. Systemy nadzorujące przebieg procesów technologicznych lub produkcyjnych (np. klasy: SCADA – Supervisory Control And Data Acquisition, DCS – Distributed Control Systems) działają na standardowych, popularnych platformach systemów Windows, Unix, Linux. Dlatego cyberataki sieciowe wykorzystujące słabości systemów operacyjnych dotyczą również działających na nich systemów przemysłowych.

Najprostszym i najbardziej efektywnym sposobem ustalenia zakresu ochrony IK jest skorzystanie z istniejących standardów opisujących metody zapewnienia bezpieczeństwa teleinformatycznego. Jednym z najbardziej rozpowszechnionych i kompletnych standardów z tej dziedziny jest standard ISO/IEC 27002. Jest to standard opublikowany przez Międzynarodową Organizację ds. Standaryzacji (ISO – International Organisation for Standarisation) i Międzynarodową Komisję Elektrotechniczną (IEC – International Electrotechnical Comission)[30]. Standard ten przedstawia najlepsze praktyki i rekomendacje z dziedziny bezpieczeństwa teleinformatycznego, właśnie zgodnie z zaprezentowanym wcześniej modelem CIA. Standard ISO/IEC zawiera 14 podstawowych obszarów organizacji bezpieczeństwa teleinformatycznego w organizacji:

(1) Polityki bezpieczeństwa informacji;
(2) Organizacja bezpieczeństwa informacji;
(3) Bezpieczeństwo zasobów ludzkich;
(4) Zarządzanie aktywami;
(5) Kontrola dostępu;
(6) Kryptografia;
(7) Bezpieczeństwo fizyczne i środowiskowe;
(8) Bezpieczna eksploatacja;
(9) Bezpieczeństwo komunikacji;
(10) Pozyskiwanie, rozwój i utrzymanie systemów;
(11) Relacje z dostawcami;
(12) Zarządzanie incydentami związanymi z bezpieczeństwem informacji;
(13) Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania;
(14) Zgodność.

[30] Norma ta pochodzi od standardu brytyjskiego z tej dziedziny, tj. British Standard 7799.

Ponadto, istnieje szereg standardów opracowanych specjalnie dla obszaru systemów automatyki przemysłowej, uwzględniających wymagania bezpieczeństwa teleinformatycznego specyficzne dla tego obszaru. Do najbardziej popularnych standardów należą:

IEC 62443 / ISA 62433 (wcześniej ISA 99) – stanowi zbiór standardów zawierających rekomendacje co do zakresu i realizacji programów poprawy bezpieczeństwa w przedsiębiorstwach będących operatorami przemysłowych systemów sterowania, wskaźników dla oceny stanu bezpieczeństwa w organizacji, definicji pojęć z zakresu bezpieczeństwa. Standardy z rodziny ISA 62433 są na bieżąco rozwijane, na chwilę obecną wiele z nich funkcjonuje jedynie jako wersje robocze.

NIST 800-82 – zawiera wiele rekomendacji z zakresu bezpieczeństwa teleinformatycznego systemów automatyki, w tym w szczególności w obszarze architektury sieci i separacji sieci IK od pozostałych sieci przedsiębiorstwa.

NERC CIP – amerykański standard poświęcony bezpieczeństwu teleinformatycznemu infrastruktury krytycznej w segmencie energetyki. Zgodność ze standardem jest obowiązkowa dla operatorów elektrowni oraz dostawców energii elektrycznej w USA.

API-1164 „Pipeline SCADA Security" – zbiór zasad dla bezpieczeństwa systemów ICS opracowany przez American Petroleum Institute specjalnie dla sektora rafineryjnego. Wytyczne w nim zawarte mogą być jednak z powodzeniem zastosowane w systemach przemysłowych innych sektorów.

TIA-942 – amerykański standard opisujący minimalne wymagania dla infrastruktury telekomunikacyjnej i centrów przetwarzania

ISO/IEC 24762 – podstawowe praktyki, które są zalecane do rozważenia zarówno przez wewnętrznych, jak i zewnętrznych dostawców usług odtwarzania techniki teleinformatycznej po katastrofie.

Na poziomie Unii Europejskiej warto zaznaczyć działalność ENISA (ENISA ang. – European Agency for Network and Information Security), czyli agencji Wspólnoty zajmującej się kwestiami bezpieczeństwa teleinformatycznego. ENISA wydała na przełomie 2011 oraz 2012 „Protecting Industrial Control Systems – Recommendations for Europe and Member States", dokument który opisuje ówczesną sytuację bezpieczeństwa systemów przemysłowych oraz 7 głównych kroków jak podnieść poziom bezpieczeństwa w takim środowisku.

Pomimo dostępności i użycia uniwersalnych standardów bezpieczeństwa teleinformatycznego, rozważyć należy posiadanie własnych regulacji ustalających konieczne do stosowania w organizacji standardy bezpieczeństwa.

Rys. 12. Obszary tematyczne standardu ISO/IEC 27002.

Najistotniejszymi elementami zapewnienie bezpieczeństwa teleinformatycznego IK są:

(1) Współpraca sektorowa;

(2) Plany awaryjne i ciągłości działania;

(3) Bezpieczeństwo oprogramowania;

(4) Kontrola dostępu;

(5) Ochrona stacji roboczych;

(6) Bezpieczeństwo sieci bezprzewodowych;

(7) Monitoring zagrożeń;

(8) Reakcja na incydenty.

2.8.3.1. *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[31]. 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 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 tego typu współpracy sektorowej można podać holenderską inicjatywę sektora finansowego o nazwie FI-ISAC[32] oraz amerykański ISAC sektora informatycznego – IT-ISAC[33].

[31] Te informacje ze względu na wysokie wymagania dotyczące poufności mogą być wymieniane w sposób anonimowy.

[32] http://www.samentegencybercrime.nl/Informatie_knooppunt/Sectorale_ISACs/FIISAC?p=content W serwisie można odnaleźć również wiele innych tego typu inicjatyw sektorowych.

[33] https://www.it-isac.org/

2.8.3.2. *Plany awaryjne infrastruktury IT (procedury odtworzenia)*[34]

Plany awaryjne zapewniające odtworzenie i ciągłość działania infrastruktury IT powinny być przygotowywane i utrzymane wg przedstawionego schematu.

Rys. 13. 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).

[34] Rozwiązania dotyczące planów awaryjnych mogą zostać użyte także w innych rodzajach zapewnienia bezpieczeństwa.

- **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 co najmniej 3 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.

2.8.3.3. *Bezpieczeństwo oprogramowania*

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,
- współpraca z dostawcą oprogramowania.

Rys. 14. Podstawowe elementy bezpieczeństwa oprogramowania.

2.8.3.4. *Kontrola dostępu*

Kontrola dostępu do zasobów jest podstawowym sposobem Zapewnienie 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 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:

(1) **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[35].

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.

(2) **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*)[36].

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

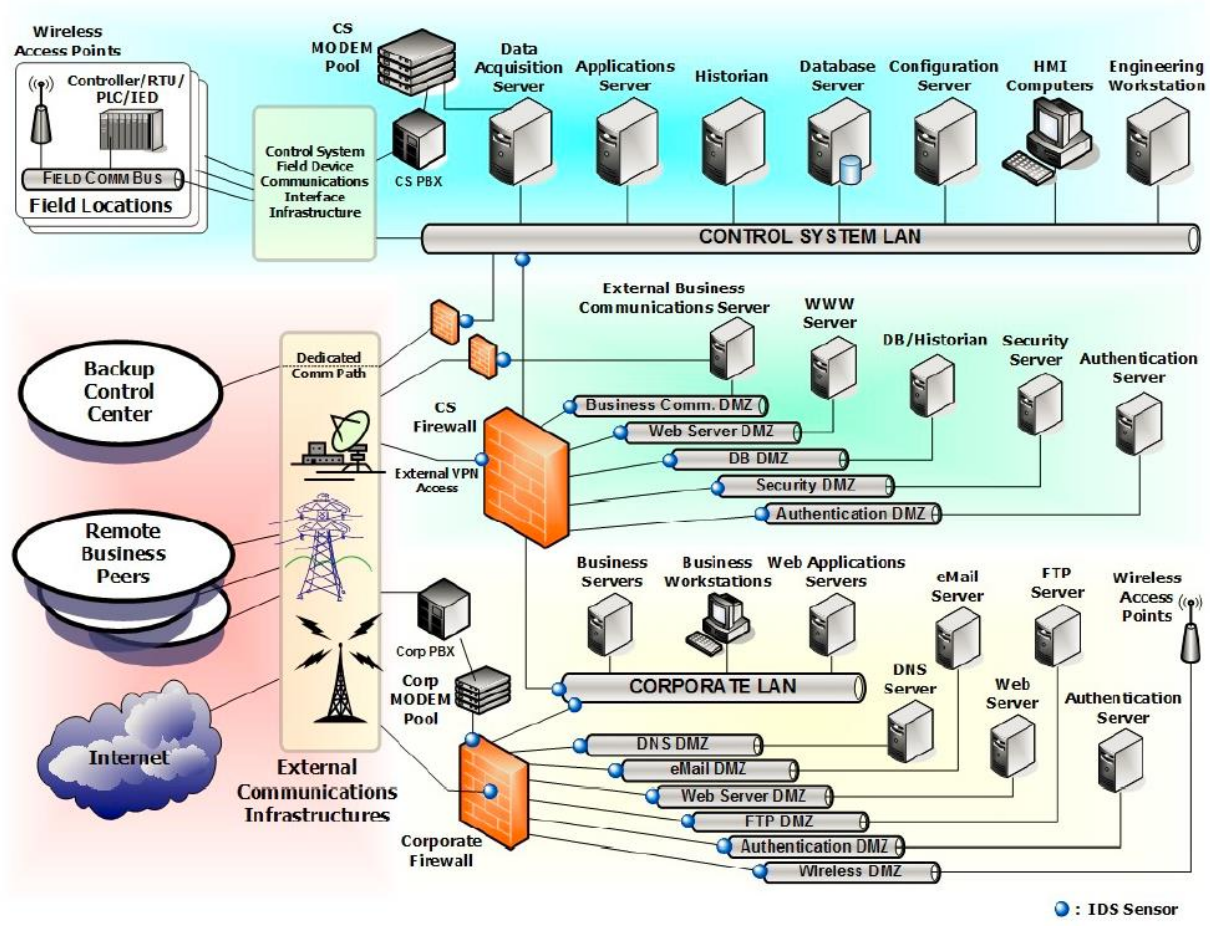
Zarówno przy pomocy wirtualnych sieci lokalnych, jak i firewallingu, możemy stworzyć rozwiązanie polegające na separacji sieci bezpośrednio obsługującej IK organizacji. Jako sieć bezpośrednio obsługującą IK rozumiemy tę część sieci organizacji, w której przetwarzane są kluczowe dane i obsługiwane są 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).

---

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

[36] 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



Rys. 15. Model segmentacji sieci[37].

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.

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

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

(4) **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 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 haseł jednorazowych, np. z wcześniej wygenerowanej listy lub z zastosowaniem połączenia hasła składającego się z części stałej i części dynamicznej (np. generowanej przez token).

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.

(1) **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[38]. Idea „czarnej listy" polega na wskazaniu tych adresów (e-mail, IP, 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.

(2) **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.

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

2.8.3.5. *Ochrona stacji roboczych*

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:

(1) **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[39] (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[40]. Jeśli jednak taka ocena nie jest dostępna, to możliwe jest przeprowadzenie jej samemu, np. z wykorzystaniem kalkulatora CVSS[41].

[39] http://www.first.org/cvss/cvss-guide.html

[40] Np. CISCO http://www.cisco.com/web/about/security/intelligence/Cisco_CVSS.html

[41] Np. udostępnianego przez NIST http://nvd.nist.gov/cvss.cfm?calculator

(2) ***Firewalling***

Zasady, które należy wykorzystywać przy ochronie stacji roboczych przez stosowanie zapory ogniowej, nie różnią się zasadniczo od tych opisywanych wcześniej[42]. 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.

(3) **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:

- 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 w celu poprawienia jego kamuflażu) jest bardzo duża[43]. Dlatego w praktyce nie jest możliwe skuteczne wykrycie wszystkich istniejących w sieci wirusów. Nie zmienia to oczywiście konieczności używania odpowiedniego oprogramowania.

[42] Patrz rozdział 2.8.3.4 Kontrola dostępu.

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

(4) ***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.

2.8.3.6. *Bezpieczeństwo automatyki przemysłowej (PLC, RTU, HMI, komponenty SCADA/DCS)*

Do warstwy sterowania modelu środowiska systemów teleinformatycznych przedstawionego w rozdziale 2.8.1. 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.

(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 infrastruktury krytycznej 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) **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.

(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.

(4) **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.

2.8.3.7. *Bezpieczeństwo sieci bezprzewodowych*

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.

2.8.3.8. *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 WEP (*Wired Equivalent Privacy*) and WPA/WPA2 (*Wi-Fi Protected Access*). Standardy WPA2 są standardami bezpieczniejszymi i one są rekomendowane.

(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[44] pozwoli na wykrywanie nieuprawnionych prób dostępu.

2.8.3.9. *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[45],
- w przypadku niekorzystania z sieci bezprzewodowych powinni oni wyłączać bezprzewodową kartę sieciową zainstalowaną w urządzeniu przenośnym.

---

[44] Patrz rozdział 2.8.3.10 Monitoring zagrożeń.

[45] Patrz punkt 2.8.3.4 Kontrola dostępu (dostęp z zewnątrz).

2.8.3.10. *Monitoring zagrożeń*

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 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 doporowadzić 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[46].

[46] 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[47], 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).

[47] 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.

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.

2.8.3.11. *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,

- 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.

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[48].

Plany reakcji powinny uwzględniać komunikację z podmiotami zewnętrznymi, w tym Policja i inne służby, dostawcy usług sieciowych, CERTy 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

[48] http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

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 CERT Polska/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.

2.8.3.12. *Reakcja na incydenty*

Istotną kwestią organizacyjną jest powołanie w strukturach organizacji zespołu do spraw reagowania na przypadki naruszania bezpieczeństwa teleinformatycznego zwanego CERT[49] (ang. *Computer Emergency Response Team*) lub CSIRT (*Computer Security Incident Response Team*). Komórka taka, jak pokazano w przykładzie w rozdz. 2.2, 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 CERT z najważniejszymi i najbardziej aktualnymi zjawiskami w dziedzinie bezpieczeństwa teleinformatycznego i praktycznej wiedzy dotyczącej nadużyć w sieci i sposobów im zapobiegania.

[49] Zestaw materiałów dotyczących tego, jak stworzyć zespół CERT, można znaleźć na stronie: http://www.terena.org/activities/tf-csirt/starter-kit.html

Jak zbudować zespół typu CERT[50]

Rys. 16. Etapy tworzenia zespołu CERT.

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 CERT

W kroku drugim należy szczegółowo zaplanować strategię stworzenia CERT. Jaka grupa osób będzie go tworzyła? Jak będzie wyglądało poparcie od zarządu? Jak poinformować o istnieniu i zadaniach takiego zespołu pozostałych członków organizacji?

Krok III – Zebranie kluczowej informacji

Jest to bardzo istotny krok, w trakcie którego dowiadujemy się o szczegółowych oczekiwaniach wobec przyszłego CERT. 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:

[50] Propozycja bazuje na rekomendacjach przygotowanych przez CERT Coordination Center: http://www.cert.org/csirts/Creating-A-CSIRT.html

- obszar działania (tzw. *constituency*) zespołu, czyli to, jakiej grupie użytkowników sieci CERT będzie świadczył swoje usługi,
- zdefiniowanie misji i celów działania,
- ustalenie zakresu świadczonych usług reaktywnych, proaktywnych i konsultacyjnych[51],
- ustalenie modelu organizacyjnego dla powstającego zespołu,
- ustalenie potrzebnych zasobów (osobowych i technicznych),
- ustalenie źródeł budżetowania dla zespołu CERT.

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 CERT

Rozpoczęcie działań operacyjnych wiąże się z zatrudnieniem personelu CERT, 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.

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 CERT, wykorzystanie organizacyjnego intranetu).

Krok VIII – Ocena efektywności działania CERT

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 lub

[51] Listę uznanych serwisów CERT można znaleźć na stronie: http://www.cert.org/csirts/services.html

wywiad z zainteresowanymi odbiorcami usług CERT, 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.

2.8.3.13. *Określenie obszaru działania*

Jednym z podstawowych zadań na początku funkcjonowania zespołu CERT jest określenie obszaru działania (tzw. constituency). Obszar działania wskazuje na to jakie zasoby i gdzie rozmieszczone, są obiektem odpowiedzialności CERT-u w kontekście reagowania na incydenty, z którymi są związane. Najbardziej powszechnym i najbardziej precyzyjnym określeniem obszaru działania jest wskazanie zakresu adresacji IP lub wskazanie numeru systemu autonomicznego (tzw. numeru AS). Również często występującym opisem obszaru działania jest wskazanie adresu domenowego podlegającego ochronie przez zespół CERT. Innym, mniej precyzyjnym, wskazaniem jest opis tekstowy – np.: „wszyscy zasoby informatyczne organizacji X". Nie daje on precyzyjnej odpowiedzi technicznej na pytanie o jakie zasoby chodzi, dlatego jeśli to możliwe to należy takiego wskazania omijać i posługiwać się precyzyjnymi wskaźnikami (adresy IP, numery AS, nazwy domenowe). Określony obszar działania CERT powinien być informacją jawną i umieszczoną w informacjach publicznych o zespole (np.: RFC2350[52]).

2.8.3.14. *Podstawowe modele organizacyjne dla zespołów CERT*

Istnieją trzy podstawowe modele organizacyjne zespołów CERT: scentralizowany, rozproszony i wirtualny. Zespół scentralizowany odpowiada w swojej strukturze najbardziej powszechnemu modelowi zwartej komórki organizacyjnej umiejscowionej w strukturze organizacyjnej firmy/organizacji. Model wirtualny polega na sformułowaniu zespołu, który składa się ze specjalistów na co dzień pracujących w różnych komórkach organizacyjnych, ale wypełniających zadania związane z reagowaniem na incydenty. Tacy specjaliści zazwyczaj tylko część swojego czasu poświęcają na zadania związane z reagowaniem na incydenty. Taki zespół pracuje ze sobą głównie zdalnie. Trzecią formą, bardzo często występującą wśród operatorów infrastruktury krytycznej, jest zespół o strukturze rozproszonej. Mimo tego, że członkowie takiego zespołu całość swojego etatu poświęcają na reagowanie na incydenty, to są oni zazwyczaj fizycznie odseparowani od siebie. Ta separacja jest naturalną konsekwencją fizycznej infrastruktury, co właśnie w przypadku infrastruktury krytycznej bardzo często ma miejsce.

[52] www.ietf.org/rfc/rfc2350.txt

2.8.3.15. *Zakres usług świadczonych przez zespół CERT*

Wachlarz usług jakie może świadczyć zespół CERT-owy jest bardzo szeroki. Jednocześnie dobór tych usług jest niezwykle ważny, gdyż w sposób jednoznaczny identyfikuje to czym zespół CERT będzie, a czym nie będzie się zajmował. Dlatego proces wyboru usług jest jednym z najważniejszych etapów tworzenia zespołu CERT-owego (patrz rozdział „Reakcja na incydenty", Jak zbudować zespół typu CERT, Krok IV – Zaprojektowanie wizji działania).

Usługi CERT-owe dzieli się na trzy zasadnicze grupy.

Tabela 7 Rodzaje usług typu CERT

USŁUGI CERT		
USŁUGI REAKCYJNE	USŁUGI PREWENCYJNE	USŁUGI ZARZĄDZNIA JAKOŚCIĄ BEZPIECZEŃSTWA
- **alertowanie I ostrzeganie** - **obsługa incydentów** - **obsługa słabości systemowych** - **analiza złośliwego oprogramowania**	- ogłoszenie komunikatów bezpieczeństwa - monitoring technologii bezpieczeństwa - ocena i audyt bezpieczeństwa - konfiguracja i utrzymanie narzędzi bezpieczeństwa, aplikacji i infrastruktury - rozwój narzędzie bezpieczeństwa - usługi wykrywania zagrożeń - dystrybucja informacji związanej z bezpieczeństwem	- analiza ryzyka - planowanie ciągłości działania - konsultacje z zakresu bezpieczeństwa - budowanie świadomości - szkolenie z zakresu bezpieczeństwa - ocena produktów lub ich certyfikacja

- usługi reakcyjne

Te usługi są podstawowym zestawem, bez których zespół CERT nie może istnieć. Najważniejsza z nich to oczywiście obsługa incydentów. Bardzo ważne jest również prowadzenie skutecznego powiadamiania o zaistniałych atakach, tak aby właściciele

zaatakowanych systemów mogli w porę na nie zareagować, gdyż nie zawsze zespół CERT będzie w stanie wykonać wszystkie konieczne działania operacyjne.

- usługi prewencyjne

Te działania mają zarówno charakter organizacyjny jak i ściśle techniczny. W ramach działań prewencyjnych prowadzi się stały monitoring technologiczny związany z pojawiającymi się zagrożeniami i technologiami bezpieczeństwa, jak również prowadzi się działania techniczne związane z wykrywaniem ataków, np.: z wykorzystaniem systemów typu IDS (ang. Intrusion Detection System - systemy wykrywania ataków) i IPS (ang. Intrusion Prevention System – systemy odpierania ataków).

- usługi zarządzania jakością bezpieczeństwa

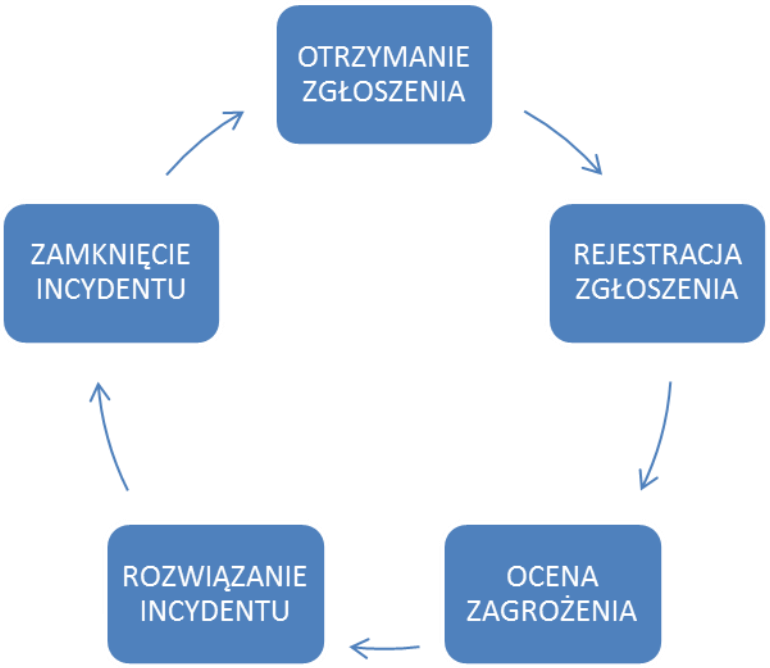
Ta grupa zwiera najrzadziej stosowane przez CERT-y usługi. Niemniej jednak w niektóre z nich CERT-y powinny się aktywnie angażować, korzystając ze swoich unikalnych doświadczeń związanych z zarządzaniem incydentami. W szczególności doświadczenia te są do wykorzystania w programach poprawiających świadomość bezpieczeństwa w organizacji oraz w szkoleniach, w szczególności dla personelu technicznego.

Planując i weryfikując zakres usług świadczonych przez CERT-y warto zadać trzy pytania:

- Jakie usługi zdaniem członków CERT powinny być świadczone przez zespół dla członków „constituency”?
- Jakie usługi zdaniem członków „constituency” powinny być świadczone przez CERT?
- W jakim stopniu zespół i jego członkowie jest przygotowany merytorycznie i technologicznie do świadczenia poszczególnych usług?

Odpowiedzi na te pytania powinny zdecydowanie ułatwić decyzje związane z wyborem usług oraz wskazać kierunki rozwoju i pozyskiwania kompetencji członków CERT, co stanowić może przy okazji program szkoleniowy lub program rekrutacji.

2.8.3.16. *Obsługa incydentów w przypadku posiadania w strukturze organizacji zespołu CERT*



Rys. 17. Fazy obsługi incydentu naruszającego bezpieczeństwo teleinformatyczne.

Procedura obsługi incydentów może być bardziej lub mniej skomplikowana. Dobrym rozwiązaniem jest rozpoczęcie działania ze stosunkowo prostą procedurą, która będzie rozwijana i udoskonalana wraz z rozwojem zespołu. Docelowa kompletna procedura powinna zawierać następujące fazy obsługi incydentu[53]:

- otrzymanie zgłoszenia o potencjalnym incydencie,
- rejestracja zgłoszenia (najlepiej z wykorzystaniem systemu wsparcia obsługi incydentów[54]),
- ocena zagrożenia związanego ze zgłoszeniem (co pozwala na nadanie odpowiedniego priorytetu obsługi):
  - weryfikacja słuszności zgłoszenia jako incydentu,

[53] Opracowane na podstawie dokumentu wydanego przez Europejską Agencję Bezpieczeństwa Sieci i Informacji ENISA – *Good Practice Guide for Incident Management* http://www.enisa.europa.eu/.../cert/.../incident-management/...practice...incident-management/.../fullReport

[54] Jednym z bardziej rozpowszechnionych systemów obsługi incydentów jest RTIR – *Request Tracker for Incident Response* http://bestpractical.com/rtir/

  - wstępna klasyfikacja incydentu[55],
  - ostateczne ustalenie priorytetu obsługi,
  - przypisanie obsługi incydentu do odpowiedniej osoby/osób,
- rozwiązanie incydentu, które odbywa się w cyklu:
  - analiza danych,
  - ustalenie metod rozwiązania,
  - propozycja zadań do realizacji,
  - wykonanie zadań,
  - usunięcie incydentu i przywrócenie sprawności działania,
- zamknięcie incydentu, czyli:
  - końcowe informacje dla zainteresowanych stron,
  - końcowa klasyfikacja,
  - archiwizacja danych związanych z incydentem,
  - analiza po zakończeniu incydentu,
  - propozycja działań naprawczych.

2.8.3.17. *Obsługa incydentu w przypadku nieposiadania w strukturze organizacji zespołu CERT*

W przypadku nieposiadania w strukturach organizacji zespołu CERT, w działaniach związanych z reagowaniem na incydenty w szczególny sposób bazujemy na wsparciu zewnętrznym. W takiej sytuacji incydent jest obsługiwany przez CERT zewnętrzny zgodnie z obszarem działania CERT zewnętrznego (ang. *constituency*).

Oprócz formalnie działających zespołów CERT wielu operatorów telekomunikacyjnych i innych instytucji posiada w swoich strukturach zespoły bezpieczeństwa, które mają za zadanie obsługiwać incydenty pojawiające się w sieciach należących do tych operatorów i instytucji.

Zgłoszenia incydentów powinny się odbywać zgodnie ze wskazanym w tabeli poniżej obszarem działania. Jednym ze sposobów odnalezienia odpowiedniego CERT lub instytucji związanej z danym adresem IP jest skorzystanie z bazy udostępnionej przez organizację RIPE: www.ripe.net lub narzędzia udostępnionego na stronach zespołu CERT Polska – IP digger: www.cert.pl.

[55] Jednym z bardziej rozpowszechnionych systemów klasyfikacji incydentów jest klasyfikacja wypracowana w ramach projektu eCSIRT.net http://www.ecsirt.net/cec/service/documents/wp4-clearinghouse-policy-v12.html#HEAD6

Tabela 8 Przykłady zespołów CERT działających w Polsce

ZESPÓŁ	ADRESS WWW	OBSZAR DZIAŁANIA
CERT.GOV.PL	http://cert.gov.pl/	Sieci domeny gov.pl, z wyłączeniem sieci instytucji wojskowych.
PIONIER-CERT	https://cert.pionier.gov.pl/	Sieć PIONIER i jednostki do niej podłączone. Sieć PIONIER: AS13293, AS8501 Sieci członków Konsorcjum PIONIER (w szczególności): AS9112, AS8364, AS8286, AS8267, AS8323, AS12324, AS12346, AS8256, AS8865, AS12423, AS15798, AS15373, AS5550, AS12831, AS9103, AS13065, AS8326, AS12618, AS8970, AS15851.
CERT Polska	http://www.cert.pl/	Sieci nieobjęte obszarem działania innych CERT, należące do domeny .pl
MIL CERT[56]	http://www.srnik.wp.mil.pl/pl/index.html	Domeny mon.gov.pl i wp.mil.pl oraz pozostałe domeny lub ich części wykorzystywane przez resort obrony narodowej.
CERT Orange Polska	http://www.cert.orange.pl/	Minimalizacja zagrożeń telekomunikacyjnych w sieciach Orange Polska S.A. Sieci związane z następującymi systemami autonomicznymi: AS5617, AS29535, AS33900, AS43447, AS12743.
ComCERT.PL	https://www.comcert.pl/	Sieci i usługi objęte usługą reagowania na incydenty przez ComCERT.PL, należące do klientów ComCERT.
Allegro CERT	http://cert.allegrogroup.com	Sieci związane z następującymi systemami autonomicznymi: AS 31621, AS 42656.

[56] Nazwa skrótowa – oficjalna nazwa zespołu CERT działającego przy Ministerstwie Obrony Narodowej to Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych.

ZESPÓŁ	ADRESS WWW	OBSZAR DZIAŁANIA
CERT Energa		193.243.142.0/23, 193.200.50.88/29, 213.192.66.0/29, 91.224.29.0/29, 109.197.58.56/30, 91.206.245.72/29, 83.3.240.208/29, 80.53.130.192/29, 213.172.175.228/30, 81.15.226.96/29, 37.123.206.232/29, 83.16.246.188/30, 79.187.125.144/30, 80.52.213.8/29, 83.15.123.0/30, 95.50.185.4/30, 79.188.89.168/30, 79.188.89.140/30, 83.3.149.220/30, 79.190.167.156/30, 83.12.178.124/30, 79.188.201.28/30, 83.12.46.204/30, 83.12.21.224/29, 83.3.77.72/30, 83.14.26.216/30, 79.189.162.100/30, 83.18.8.4/30, 91.212.231.96/30, 80.55.146.168/30, 83.13.48.112/30, 83.13.54.232/30, 83.13.168.148/30, 79.187.90.80/30.

2.8.3.18. *Klasyfikacja incydentów*

Istnieje wiele klasyfikacji incydentów. Środowisko CERT-ów jak do tej pory nie wypracowało jednej, powszechnej klasyfikacji stosowanej przez wszystkie lub chociażby większość zespołów. Są jednak klasyfikacje, które spośród wielu zyskały dużą popularność. Jedną z nich, która również często zaczęła być stosowana w Polsce[57], jest klasyfikacja wypracowana w trakcie projektu eCSIRT.net[58]. Zawiera ona osiem głównych grup incydentów oraz dwadzieścia pięć podgrup. Główne grupy są następujące:

- obraźliwe i nielegalne treści,
- złośliwe oprogramowanie,
- gromadzenie informacji,
- włamania,
- próby włamań,
- dostępność zasobów,
- ataki na bezpieczeństwo informacji,
- oszustwa komputerowe.

Zespół typu CERT powinien poważnie rozważyć stosowanie klasyfikacji (powyższej lub innej[59]). Systematyczne stosowanie klasyfikacji daje szansę na analizę trendów, optymalizowanie działań zespołu oraz jest bardzo dobrym systemem raportowania prac zespołu.

---

[57] Klasyfikację opartą na tym modelu stosuje między innymi zespół CERT.GOV.PL

[58] www.ecsirt.net/cec/service/documents/wp4-clearinghouse-policy-v12.html#HEAD6

[59] Więcej na temat innych klasyfikacji, oraz metod ich używania, można znaleźć w publikacji ENISA – „Good Practice Guide for Incident Management", rozdział 8.7.1 – Existing Taxonomies.

Najważniejsze rekomendacje dotyczące zapewnienia bezpieczeństwa teleinformatycznego

1. Wykorzystuj istniejące normy i standardy.
2. Regularnie szkól personel.
3. Wymieniaj doświadczenia i informacje o zagrożeniach z innymi organizacjami.
4. Twórz i testuj plany awaryjne.
5. Zarządzaj zmianą oprogramowania (testowanie, aktualizacja, audyt kodu).
6. Przydzielaj uprawnienia wyłącznie na podstawie faktycznych potrzeb.
7. Wykorzystuj oprogramowanie zabezpieczające przed kodem złośliwym włamaniami i wyciekiem informacji.
8. Chroń dostęp do narzędzi administratorskich, programistycznych oraz ograniczaj dostęp do kodów źródłowych.
9. Monitoruj ruch sieciowy.
10. Zabezpieczaj dane przesyłane publicznymi sieciami.
11. Stwórz własny lub w przypadku ataku teleinformatycznego korzystaj z usług istniejących Zespołów Reagowania na Incydenty Komputerowe.

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 Skarbu Państwa oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych (Dz. U. Nr 65, poz. 404).

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) Przy wyborze usługodawcy należy brać pod uwagę jego bieżącą sytuację finansowo-ekonomiczną oraz badać strukturę właścicielską, łącznie z identyfikacją beneficjentów rzeczywistych.

(3) Każda relacja z nowym partnerem powinna rozpocząć się od zawarcia umowy o zachowanie poufności. Umowa taka powinna gwarantować realne sankcje w przypadku jej naruszenia.

(4) 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).

(5) 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"[60] do kodów źródłowych oraz środowiska rozwojowego danej aplikacji.

(6) Docelowa umowa powinna zawierać precyzyjny opis przedmiotu umowy tak, aby zminimalizować ryzyko obszarów, które nie zostały przypisane wyraźnie do jednej ze stron.

(7) 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.

(8) Definicje awarii lub błędów używane w umowach powinny uwzględniać zjawiska wynikające z wykrycia nowych podatności oprogramowania.

(9) Umowa powinna zawierać zasady usuwania zgłoszonych błędów, w postaci tzw. umowy Service Level Agreement (SLA) zawierającej wskaźniki dotyczące procedur współpracy, terminowości usuwania zgłoszonych błędów jak i sankcji za ich nieusunięcie.

(10) Umowy serwisowe z producentami oprogramowania powinny zawierać dodatkowe SLA dotyczące usuwania wykrytych podatności, których wykorzystanie może powodować ryzyko zakłócenia funkcjonowania IK.

[60] 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.

(11) 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.

(12) 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.

(13) 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.

(14) 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.

(15) 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.

(16) Umowa powinna zawierać zasady zlecania podwykonawcom poszczególnych czynności wraz z wymogiem stosowania równorzędnych zabezpieczeń, jak wynikających z zawartej umowy głównej.

(17) 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 oraz ISO IEC 24762 – wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie.

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.

3. Szacowanie ryzyka

Jedną z zasad NPOIK jest zasada proporcjonalności i działań opartych na ocenie ryzyka. 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. Z punktu widzenia Programu jest to element kluczowy, determinujący i uzasadniający działania podejmowane w celu obniżenia ryzyka zakłócenia funkcjonowania IK. Ocena ryzyka powinna być podstawą określenia standardów ochrony IK i ustalenia priorytetów działań.

Przed rozpoczęciem jakichkolwiek analiz związanych z ryzykiem (wpływem niepewności na cel) należy wziąć pod uwagę dwa zagadnienia. Po pierwsze należy pamiętać, że szacowanie ryzyka jest pojęciem kompleksowym.

Zgodnie z normą PN-ISO 31000 na szacowanie ryzyka składają się:

1) identyfikacja zagrożeń,
2) analiza ryzyka,
3) ewaluacja ryzyka.

Dodatkowo trzeba mieć na względzie, że Narodowy Program Ochrony Infrastruktury Krytycznej zwraca uwagę operatorów na sześć obszarów bezpieczeństwa (zapewnienie bezpieczeństwa fizycznego, technicznego, osobowego, teleinformatycznego, prawnego oraz tzw. plany odbudowy), z których każdy wiąże się ze specyficznym dla siebie ryzykiem i do analizy każdego z tych obszarów podejść należy z jednakową starannością. Ponadto uwzględnić należy ryzyko, które dla zdecydowanej większości operatorów jest najistotniejsze, a mianowicie ryzyko biznesowe.

Najlepszym wspólnym mianownikiem dla przeprowadzenia spójnej analizy 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 jednostce. 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 poniesie organizacja w przypadku wystąpienia 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							

Rys. 18. – przykładowa tabela BIA.

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),
2) zasoby materiałowe (jakiego sprzętu, jakich materiałów używa do realizacji danej czynności),
3) zasoby informacyjne (co muszę wiedzieć, by wykonać czynność),
4) zasoby finansowe (ile 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.

Narodowy Program Ochrony Infrastruktury Krytycznej 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 powoduje szkody, ale jest warunkiem lub zbiorem warunków, które mogą umożliwić zagrożeniu oddziaływanie na organizację. Podatność może pochodzić ze źródeł zarówno wewnętrznych, jak i zewnętrznych i istnieć tak długo, dopóki w samej organizacji nie nastąpią zmiany powodujące jej zmniejszenie lub usunięcie (np. dziura w dachu – dopóki nie pojawią się opady może nie mieć wpływu na organizację). Wskazanie ich w etapie szacowania ryzyka jest najłatwiejsze, a jest w zarządzaniu ryzykiem nieuniknione, ponieważ podatności sugerują bezpośrednie sposoby na postępowanie z ryzykiem – jakie zabezpieczenia należy wprowadzić.

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 (przypisania określonym wartościom prawdopodobieństwa, podatności i skutków skal np. 1–6) 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, 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 będą szczegółowe, a ich autorzy konsekwentni.

4. 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