2013

Narodowy Program Ochrony Infrastruktury Krytycznej

Załącznik 2

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

RCB
Rządowe Centrum Bezpieczeństwa

Spis treści

1. Jak korzystać z załącznika 2

1.1. Co zawiera

Dokument zawiera podstawowe informacje na temat technicznych i organizacyjnych aspektów ochrony infrastruktury krytycznej. Może on posłużyć jako zestaw konkretnych wskazówek dotyczących budowy i funkcjonowania systemu ochrony IK. Dodatkowo w dokumencie można znaleźć ocenę skuteczności poszczególnych metod ochrony 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 jej rodzajów często nie jest oczywiste i jednoznaczne (występują środki, które mogą być przypisane do kilku rodzajów ochron). Podział dokonany w dokumencie służy jedynie opisowi i nie może być traktowany jako ostateczny.

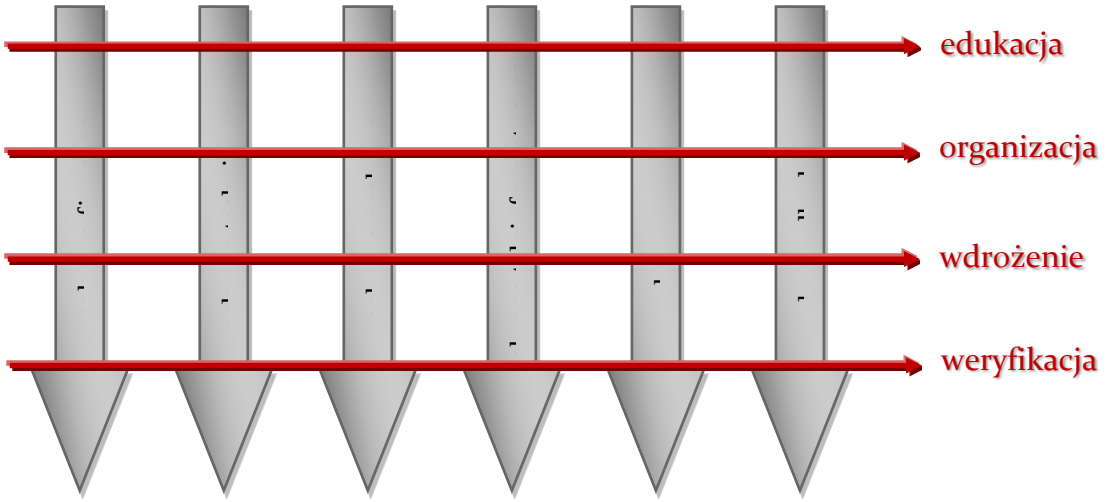
Biorąc pod uwagę, że adresatami niniejszego załącznika są zarówno podmioty stosujące różne rodzaje ochrony ze względów biznesowych oraz takie, które po raz pierwszy zetkną się z takim zagadnieniami, w przedłożonym materiale zastosowano poziom szczegółowości umożliwiający zastosowanie przez wszystkich 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 bezpieczeństwa.
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, niestety 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 stosunek pracowników do zasad bezpieczeństwa.
Działania edukacyjne powinny być prowadzone 2 etapowo:

- 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 na rozpowszechnianie periodyku jest przedstawienie go w formie krótkiego filmu.
- uświadamianie wizualne poprzez rozwieszanie w organizacji plakatów na temat zasad bezpieczeństwa.

PRZYKŁADY

Trzy podstawowe obszary edukacji na przykładzie ochrony teleinformatycznej wraz ze wskazaniem podobszarów szczególnej istotności:

rys. 2 - podstawowe obszary edukacji w zakresie ochrony teleinformatycznej

SUGESTIA

Działaniami edukacyjnymi należy objąć nie tylko personel, w zakresie obowiązków którego 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.

DOBRA PRAKTYKA

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.

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 ochrony) lub zadania z zakresu bezpieczeństwa mogą być przydzielone do komórek właściwych np. do spraw kadrowych (ochrona osobowa), teleinformatyki (ochrona teleinformatyczna) czy utrzymania infrastruktury (ochrona techniczna).
Obydwa modele mają swoje wady i zalety. Poniżej przedstawiono przykładowe zestawienie wad i zalet obydwu modeli.

Jedna komórka odpowiedzialna za bezpieczeństwo

zalety

- duża możliwość koordynacji
- jednoosobowa odpowiedzialność
- integracja wszystkich aspektów bezpieczeństwa w jednej komórce organizacyjnej

wady

- mniejszy wgląd w działania innych komórek organizacyjnych i konieczność zbierania szczegółowych informacji o wszelkich ich działaniach
- konieczność włączenia w strukturę komórki specjalistów w zakresie każdego rodzaju ochrony
- zamknięcie się we własnym obszarze zadaniowym

Zadania z zakresu bezpieczeństwa w różnych komórkach organizacyjnych

zalety

- wysoka specjalizacja personelu
- inforamcje o działaniach mogących dotyczyć bezpieczeństwa są dostępne wewnątrz komórki
- większe zaufanie do pracowników bezpieczeństwa

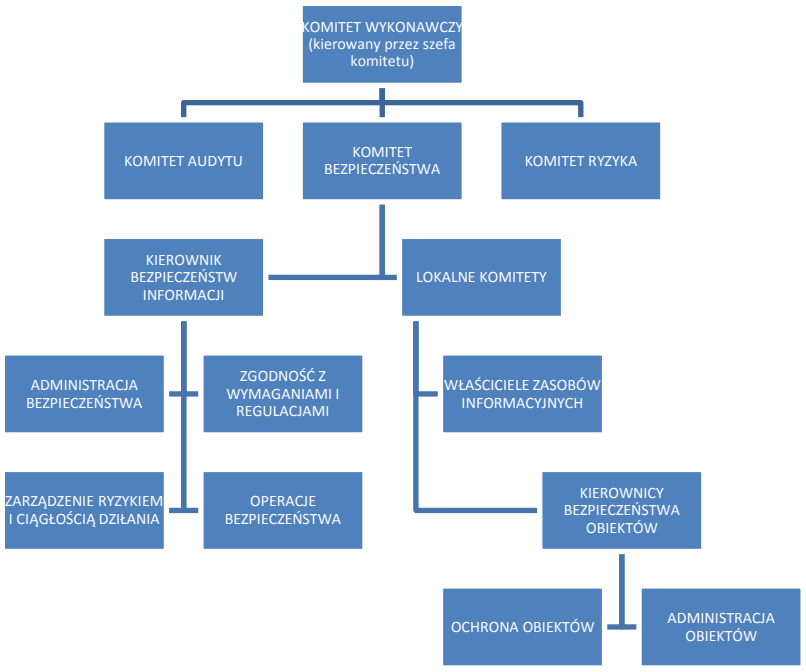
wady

- rozproszenie informacji z zakresu bezpieczeństwa pomiędzy wiele komórek organizacyjnych
- konieczność koordynacji działań wielu komórek organizacyjnych
- rozproszenie odpowiedzialnościzwłaszcza w obszarach nakładających się kompetencji

Wybór konkretnego modelu zależy od specyficznych potrzeb, wymagań i możliwości organizacyjno-finansowych organizacji.

Niezależnie od tego, skuteczność funkcjonowania wybranego modelu wymaga ścisłej współpracy pomiędzy 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.

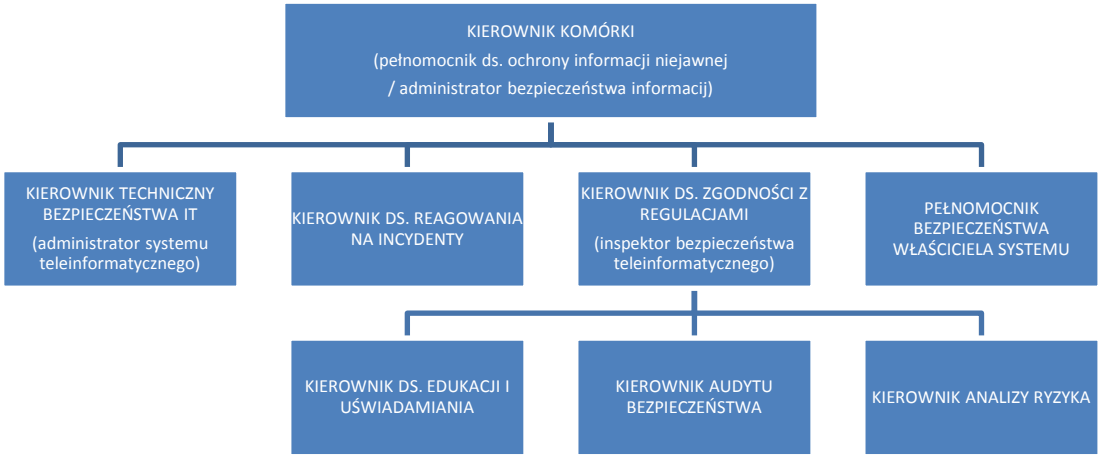
Jedną z metod podjęcia decyzji o kształcie struktury organizacyjnej jest przyjęcie istniejących modeli struktur organizacyjnych, np.: w zakresie ochrony teleinformatycznej zastosowanie zabezpieczeń zdefiniowanych w normie PN-ISO/IEC 17799:2007.



rys. 3 - struktura organizacyjna pionu bezpieczeństwa teleinformatycznego zgodna z normą PN-ISO/IEC 17799:2007

Powyższa struktura jest zalecana dla najbardziej rozbudowanych organizacji, posiadających również swoje regionalne przedstawicielstwa. Jest ona wskazana dla tych organizacji, które chcą zastosować kompletny zestaw zabezpieczeń opisanych w normie PN-ISO/IEC 17799:2007. Prostszy i bardziej praktyczny model oparty jest o dwie kategorie stanowisk (realizowanych funkcji): obligatoryjne i fakultatywne. 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 ochrony teleinformatycznej

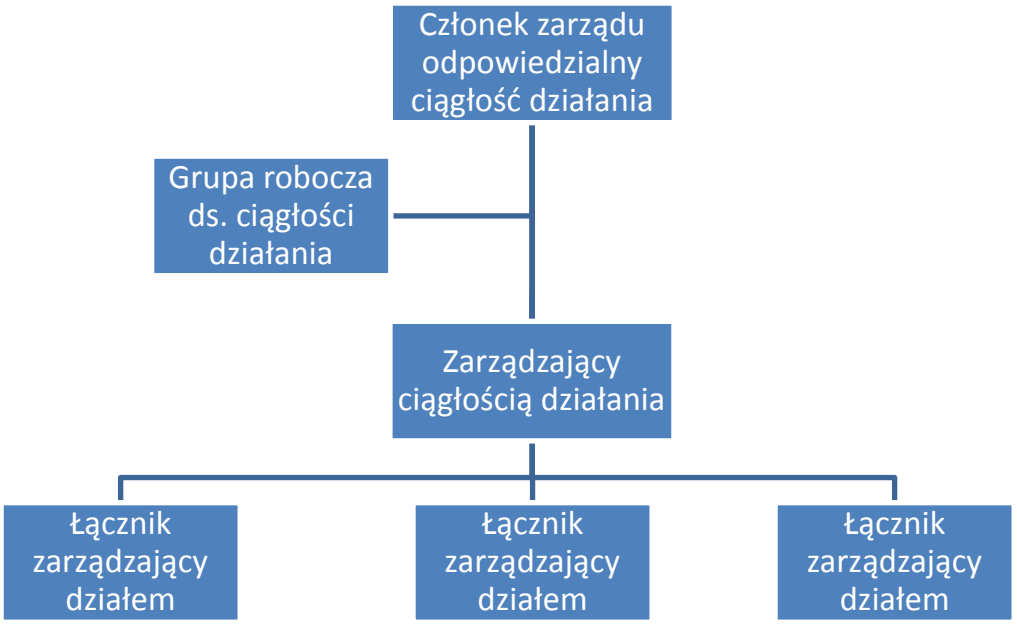
Poniższa tabela zawiera opis poszczególnych stanowisk wraz ze wskazaniem ich obligatoryjności lub fakultatywności, wskazaniem któremu ze stanowisk wymaganych w wspomnianych ustawach odpowiada dane stanowisko oraz wskazaniem, które z innych stanowisk przejmuje zadania danej funkcji w przypadku decyzji o rezygnacji z jej istnienia w strukturze organizacyjnej[1].

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 SPRAW ZGODNOŚCI Z REGULACJAMI (obligatoryjne)	Tak	Nadzór i kontrola nad prawidłowym zaprojektowaniem, wdrożeniem i utrzymaniem zasad i mechanizmów zapewniających bezpieczeństwo teleinformatyczne.	N/D
PEŁNOMOCNIK BEZPIECZEŃSTWA	Nie	Reprezentacja właściciela systemu, w celu kontroli tego, aby zasady bezpieczeństwa nie naruszały kluczowych	Kierownik ds. zgodności z

[1] W celu zapoznania się ze szczegółowym zakresem stanowisk wskazanych w „Ustawie o ochronie informacji niejawnej" oraz „Ustawie o ochronie danych osobowych", należy sięgnąć do tychże ustaw.

WŁAŚCICIELA SYSTEMU		funkcji prawidłowego funkcjonowania systemu zgodnie z zapotrzebowaniem biznesowym.	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 implementacji brytyjskiej normy BS 25999 dotyczącej zarządzania ciągłością działania organizacji[2].



rys. 5 - struktura organizacji ciągłości działania

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

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

[2] Przykład struktury i opisy na podstawie: John Sharp – The Route Map to Business Continuity Management. Meeting the Requirements to BS 2599 – British Standard Institution 2008

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. Niezależnie od tego 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:

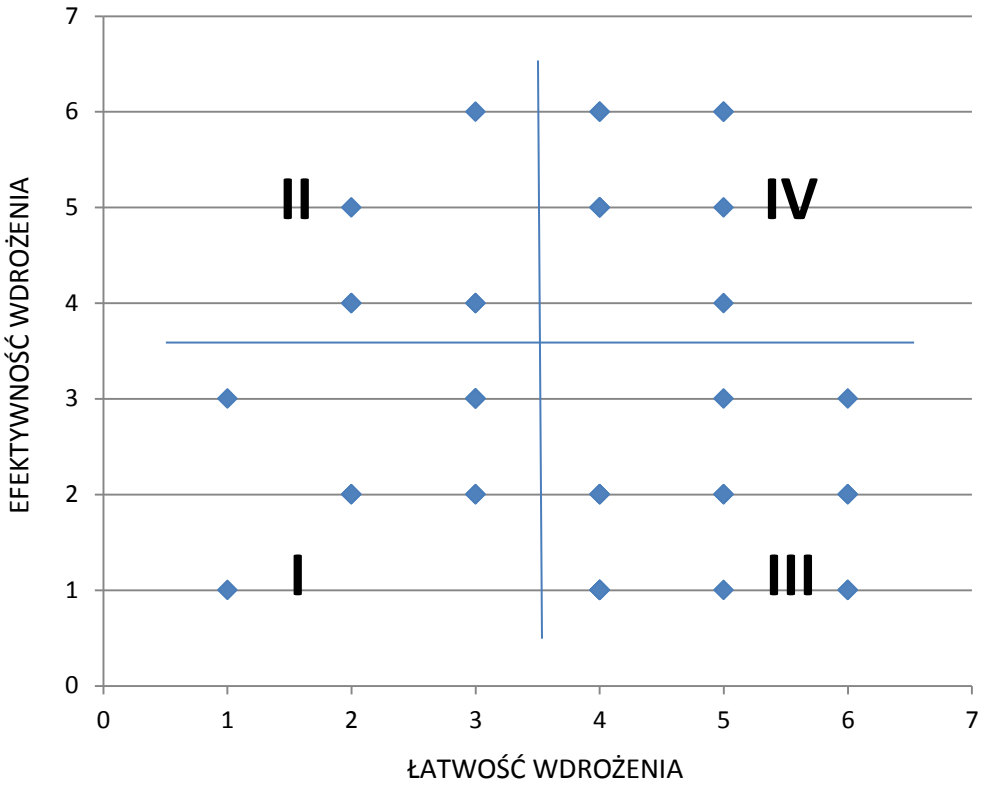
- opór pracowników;
- koszty utrzymania;
- koszty implementacji;

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



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.

SPOSOBY OCHRONY	WSKAŹNIK ŁATWOŚCI WDROŻENIA	WSKAŻNIK EFEKTYWNOŚCI	ETAP WDROŻENIA
OGOLNE			
Stanowiska i zakres odpowiedzialności			
Edukacja i uświadamianie			
OCHRONA FIZYCZNA			
Wydzielenie stref bezpieczeństwa			
Patrole wewnątrz obiektu			
OCHRONA TECHNICZNA			
Własne ujęcie wody			
Generatory prądotwórcze			
OCHRONA TELEINFORMATYCZNA			
Bezpieczeństwo oprogramowania			
Ochrona stacji roboczych			
OCHRONA OSOBOWA			
Wizualna identyfikacja pracowników organizacji			
Kontrola dostępu do stref bezpieczeństwa			
PLAN ODBUDOWY			
Testowania planu			

2.4. Weryfikacja przyjętych rozwiązań i ich aktualizacja

Podjęte przez organizację działania w celu wdrożenia wybranych rodzajów ochrony IK 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.

2.4.1. Ćwiczenia[3]

Ćwiczenia są jedynym sposobem, poza działaniem w warunkach rzeczywistych zagrożeń, na praktyczną weryfikację podjętych w zakresie ochrony IK działań. Dają możliwość rozwoju pracy zespołowej, podniesienia kompetencji, wzrostu zaufania do własnych możliwości oraz poziomu wiedzy.

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.

[3] bazowano na normie BS 25999-1:2006 Zarządzanie ciągłością działania część 1: Praktyczne porady

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.

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 poprzez 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 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.

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

2.5. Ochrona fizyczna

Ochrona fizyczna to zespół przedsięwzięć minimalizujących ryzyko zakłócenia funkcjonowania IK przez osoby, które znalazły się na terenie IK w sposób nieautoryzowany. Składają się na nią:

- ochrona osób, rozumiana jako działania mające na celu zapewnienie bezpieczeństwa życia, zdrowia i nietykalności osobistej,
- ochrona mienia czyli działania zapobiegające przestępstwom i wykroczeniom przeciwko mieniu, a także przeciwdziałające powstawaniu szkody wynikającej z tych zdarzeń,
- działania niedopuszczające do wstępu osób nieuprawnionych na teren chroniony.

Ochronę fizyczną prowadzi się przy wykorzystaniu wspomagających ją środków technicznych.

2.5.1. Przykłady fizycznych ataków i incydentów z udziałem infrastruktury krytycznej

Fizyczne ataki na infrastrukturę krytyczną oraz incydenty z jej udziałem nie należą wcale do rzadkości. Poniżej kilka przykładów takich ataków z ostatnich 15 lat.

Rodzaj ataku	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 Saudyjskiej	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

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

		ostrzelaniu przez strażników przed pokonaniem kolejnego ogrodzenia. Napastnicy byli dobrze przygotowani, uzbrojeni i wyposażeni. Wiadomości o ataku spowodowały wzrost cen ropy naftowej na rynku średnio o 2$.
Protest	03.07.2007 Bełchatów/Polska	Aktywiści Greenpeace 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. Następnie podłożyli materiały wybuchowe pod generatory prądotwórcze. W wyniku eksplozji dwa z trzech generatorów zostały uszkodzone. Sprawcy byli uzbrojeni w broń maszynową oraz granatniki przeciwpancerne

2.5.2. Działania organizacyjne i zapobiegawcze

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 2005 nr 145, poz. 1221 - j.t.). Zapewni to m.in. możliwość użycia, zgodnego z prawem, środków przymusu bezpośredniego przez osoby wykonujące tę ochronę. Wykonywanie zadań w obszarze ochrony fizycznej realizuje się poprzez zapewnienie ciągłej, 24-godzinnej ochrony fizycznej obiektów, urządzeń, instalacji i systemów IK.

Jednym z podstawowych sposobów na ochronę fizyczną IK jest podział terenu na którym zlokalizowana jest IK na strefy ochrony[5] (stref ograniczonego dostępu) i zaprojektowanie ich zgodnie z zasadą ochrony w głąb.

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.

Podział stref ochrony:
1 – specjalna strefa bezpieczeństwa
2 – strefa bezpieczeństwa
3 – strefa chroniona
4 – strefa kontrolowana

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

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

Należy wprowadzić procedury dotyczące:

(1) zasad wejścia do stref ochrony pracowników oraz pojazdów obsługujących oraz sposób poruszania się użytkowników po obiekcie obejmujące: dostęp do poszczególnych stref ochrony poprzez autoryzację przez system kontroli dostępu lub zgodnie z innymi zastosowanymi elementami rejestrowanej identyfikacji (klucze pobierane za potwierdzeniem/PIN), możliwość przeszukania itp.;

(2) zasad użycia elementów identyfikacji (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) wydawania identyfikatorów (przepustek) oraz nadawania uprawnień oraz ich zdejmowania użytkownikowi;

(4) zasad wejścia kontrahentów i wjazdu pojazdów do nich należących obejmujące: nadanie uprawnień na wejście i rejestrację kontrahentów, możliwość przeszukania, zasad poruszania się po obiekcie, jednoznaczną identyfikację osób (pojazdów, firm), identyfikację wizualną itp.;

(5) zasad wejścia gości i wjazdu pojazdów do nich należących obejmujące: nadanie uprawnień na wejście i rejestrację odwiedzających, zasady poruszania się po obiekcie, wizualną identyfikację;

(6) kontroli środków ochrony obejmujące: odpowiedzialnych za kontrole, odstępy czasu pomiędzy kontrolami, protokoły pokontrolne itp.;

(7) serwisowania technicznych środków ochrony fizycznej obejmujące: okresową obsługę zgodnie z dokumentacją techniczną, określone umownie czasy usuwania usterek itp.;

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

(9) sposobów reakcji ochrony na określone rodzaje zdarzeń.

Budując obiekt, który będzie wymagał ochrony należy mieć na uwadze zastosowanie urbanistycznych, architektonicznych i budowlanych rozwiązań podnoszących bezpieczeństwo oraz zapewnienie wytrzymałości i stabilności konstrukcji, ogrodzenia, możliwość podziału na strefy bezpieczeństwa i innych rozwiązań dla środków ochrony fizycznej.

Zauważalna obecność środków ochrony fizycznej i technicznej (płoty, siatki i ich zwieńczenia, kamery systemu telewizji przemysłowej, oświetlenie obecność pracowników ochrony) podświadomie zniechęca potencjalnych agresorów. Należy jednak mieć na uwadze, że nie wszystkie środki ochrony powinny być eksponowane, by nie narażać bezpieczeństwa informacji o budowie systemu ochrony fizycznej obiektu.

Należy dokonywać regularnych, okresowych przeglądów stanu zewnętrznego otoczenia chronionego obiektu (strefy ochrony) biorąc pod uwagę dostęp do obiektu i możliwości obserwacji wzrokowo - technicznej. W razie potrzeby należy dokonać regulacji terenu, usunięcia roślinności, drzew itp. wewnątrz i na zewnątrz obiektu.

Należy utworzyć centrum dowodzenia i koordynacji ochrony fizycznej w danej jednostce organizacyjnej i wyposażyć je w zintegrowany system informowania (CCTV, 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. Osoby posiadające uprawnienia do kontroli nad technicznymi środkami ochrony lub dokonywania w nich zmian powinny autoryzować dokonanie tych czynności poprzez połączenie 2 niezależnych unikalnych identyfikatorów (PIN-karty, PIN-biometria itp.)

2.5.3. Modele ochrony fizycznej[6]

Ochronę fizyczną można organizować w system posterunków (doraźnych lub stałych) oraz patroli. W trakcie ochrony 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 ochrony fizycznej, które można podzielić pod względem rozmieszenia i poziomu mobilności jednostek ochrony:

- model statyczny;
- model ruchomy;
- model mieszany.

Model Statyczny:

- celem tego typu modelu jest uniemożliwienie osobom postronnym zajęcie 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

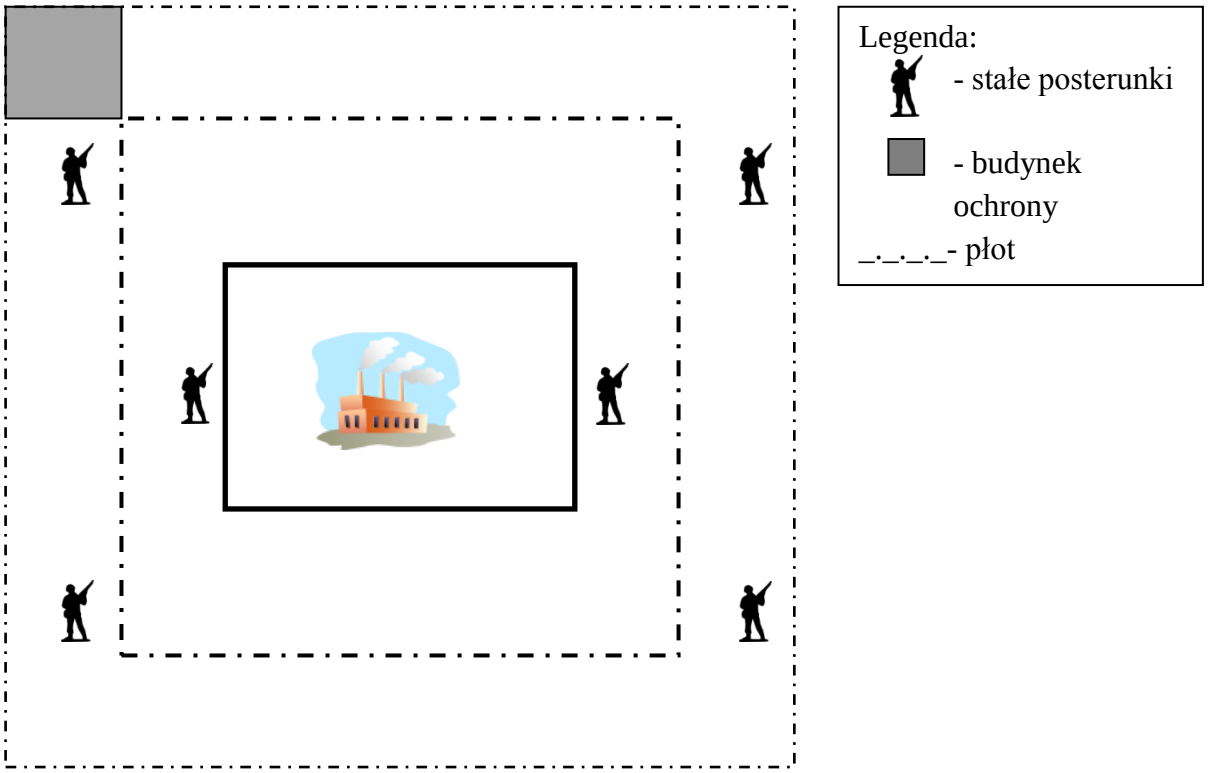
Zalety:

- 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.

[6] opracowano na podstawie prezentacji pana Richarda Thomsona - Chief Constable - Civil Nuclear Constabulary. Londyn 18 maja 2011 r.



rys. 6 - ilustracja funkcjonowania modelu statycznego

Model ruchomy :

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

Główne cechy:

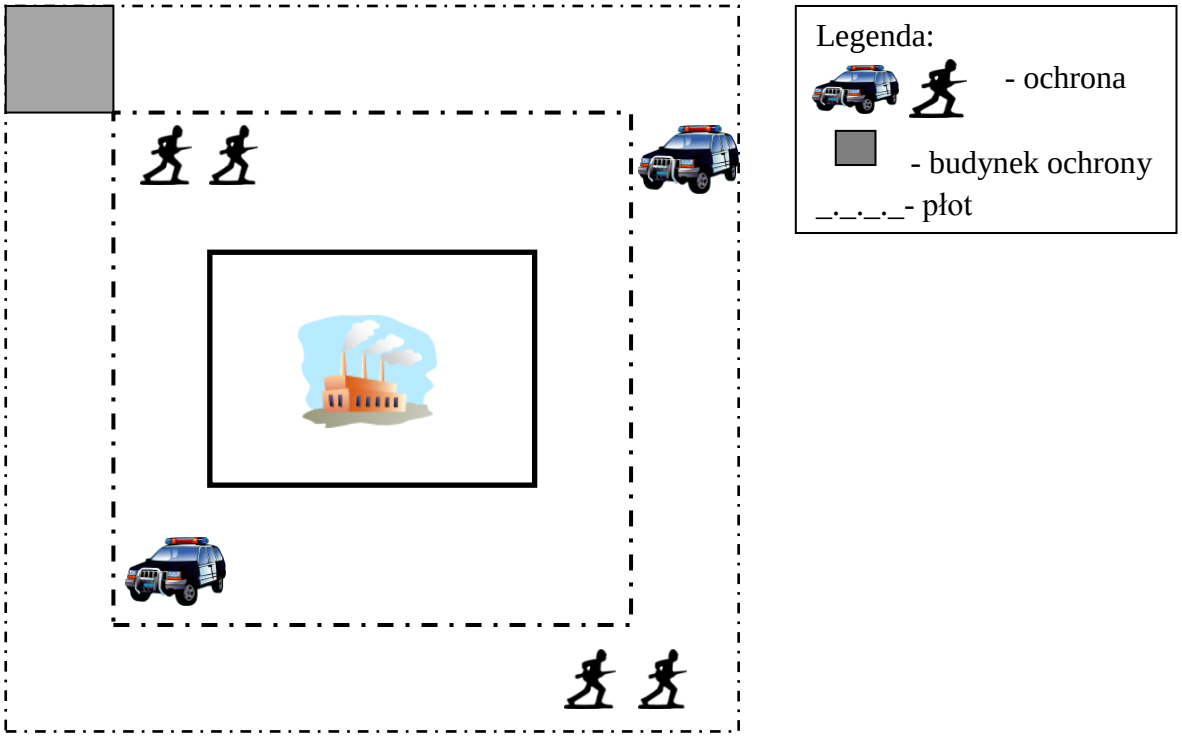
- używane są różne systemy elektroniczne uzupełniające działania służb ochrony,
- służba ochrony może się swobodnie poruszać po całym obiekcie.

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 poprzez ćwiczenia i szkolenia.



rys. 7 - ilustracja funkcjonowania modelu ruchomego

Model mieszany:

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

Główne cechy:

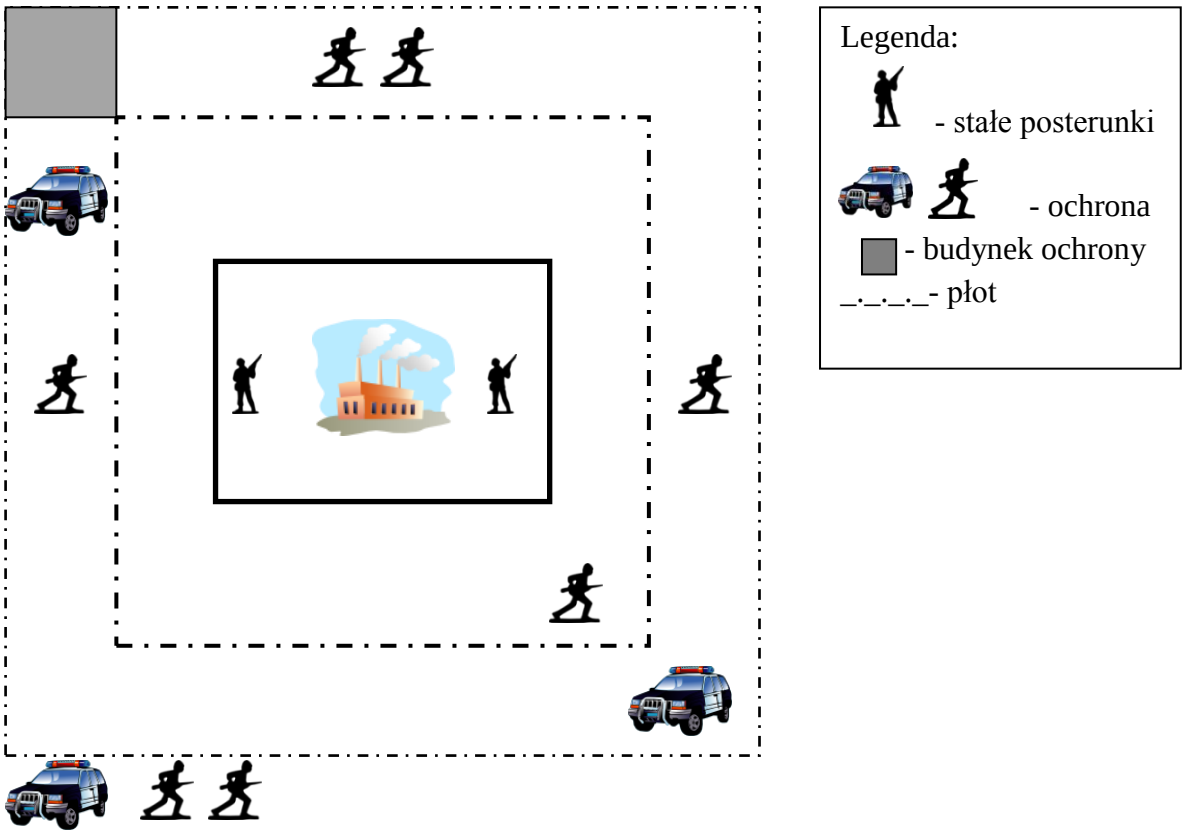
- wielowarstwowa ochrona,
- zgrane elementy ochrony statycznej z ruchomymi patrolami,
- stałe posterunki ochronne w strefie „zero".

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. 8 - ilustracja funkcjonowania modelu mieszanego

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

Pracownicy realizujący ochronę fizyczną IK, winni dokumentować zdarzenia i sytuacje mogące zagrażać bezpieczeństwu chronionego mienia.
Zakres działań w/w pracowników powinien również obejmować działania polegające na:

- ochronie elementów IK przed dostępem do nich osób nieuprawnionych,
- zapewnieniu bezpieczeństwa osób znajdujących się na terenie lub w granicach IK,
- zapobieganie przedostaniu się na teren IK paczek niewiadomego pochodzenia poprzez stosowanie prześwietlarek
- ochronie mienia IK przed kradzieżą, zniszczeniem lub uszkodzeniem,
- zapobieganie zakłóceniom porządku na terenie oraz powiadamianie właściwych przełożonych o zdarzeniach powodujących naruszenie porządku,
- przyjmowanie, przechowywanie i wydawanie depozytów (w tym broni),
- stały dozór sygnałów przesyłanych, gromadzonych i przetwarzanych w elektronicznych systemach ochrony,

- wykrywanie zagrożeń klęskami żywiołowymi, awariami technicznymi oraz podejmowanie i koordynowanie działań zmierzających do zapobiegania i przeciwdziałania ich skutkom, do czasu przybycia właściwych służb.

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, maski przeciwgazowe, hełmy i kamizelki kuloodporne, środki transportu oraz w miarę potrzeby inny sprzęt.

Operatorzy IK powinni zapewnić pracownikom ochrony możliwość stałego podnoszenia i doskonalenia umiejętności w zakresie:

1) techniki i taktyki posługiwania się bronią palną,
2) użycia środków przymusu bezpośredniego,
3) techniki i taktyki interwencji.

Należy również zwrócić uwagę na kwestię poruszania się po terenie IK, z bronią i amunicją. Należy wprowadzić zakaz wnoszenia na teren obiektów broni lub amunicji, urządzeń rejestrujących obraz typu aparaty fotograficzne, kamery itp. przez osoby nie posiadające 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 wewnętrzną ochronę infrastruktury krytycznej.

2.5.4. Techniczne środki ochrony fizycznej

Ogrodzenie, zapory mechaniczne, wejścia i wyjścia

Jeśli istniej 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 napastnika, w tym celu:

- wysokość ogrodzenia nad powierzchnią terenu powinna w maksymalny sposób utrudnić jego pokonanie ponad nim,
- dolna krawędź ogrodzenia powinna być zabetonowana lub w inny sposób trwale zamontowana w podłożu bądź osadzona w podmurówce,
- powinno być wyposażone w próg uniemożliwiający dokonanie podkopu,
- powinno być wyposażone w bariery wieńczące ogrodzenie z drutu kolczastego lub spirali 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 pomiędzy nimi.

Ogrodzenie powinno mieć możliwość współpracy z systemami telewizji przemysłowej, pozwalającymi na obserwację ogrodzenia zewnętrznego oraz wszystkich wejść i wyjść z stref ochrony, systemami wykrywania i sygnalizacji włamania, pozwalającymi na jak najwcześniejsze wykrycie prób sforsowania ogrodzenia zewnętrznego obiektu oraz oświetleniem.

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. Mogą one jednocześnie tworzyć atrakcyjne otoczenie.

Wejścia na teren IK dla ludzi (jeśli jest taka możliwość warto rozdzielić także 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 zamki kontrolowane przez system kontroli dostępu lub inną metodę identyfikacji wchodzących i kontroli ich praw dostępu (klucz, PIN). 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 ochrony fizycznej. W przypadku zmniejszenia liczby wejść/wyjść pamiętać jednak należy o wymogach związanych z ewakuacją.

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 odpowiednio wyposażone w podesty, lustra, kamery itp. miejsce do obsługi (kontrolę ładunku, sprawdzenie tożsamości osób i uprawnień do przebywania na terenie obiektu chronionego) pojazdów przez personel odpowiedzialny za ochronę. Miejsce to może być zaaranżowane w formie zatoczki lub śluzy itp.
Należy również zapewnić kontrolę w czasie ładowania i rozładunku towarów na terenie IK (nadzór osobowy, z wykorzystaniem kamer CCTV, itp.).

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.

SKD powinien być wprowadzony we wszystkich strefach ochrony i obejmować wszystkie (lub przynajmniej używane) wejścia dla ludzi i bramy wjazdowe dla pojazdów. Wybrane pomieszczenia wewnątrz stref ochrony powinny być wyposażone w zamki kontrolowane przez system kontroli dostępu lub inną metodę identyfikacji wchodzących i kontroli ich praw dostępu (klucz, PIN). SKD powinien być wspomagany systemem telewizji przemysłowej (CCTV).

SKD można zaprogramować w sposób zapobiegający powtórnemu udzieleniu prawa dostępu w jednym kierunku. Takie rozwiązanie skutecznie wymusza konieczność rejestracji wejścia i wyjścia ze strefy ochrony oraz zapobiega nieuzasadnionemu przepuszczaniu przez strefy ochrony osób nieupoważnionych. Obecność użytkownika w określonym obszarze w celu umożliwienia wejścia do innego obszaru powinna odbywać się poprzez system kontroli dostępu.

Zapewniając kontrolę wejść i osób wchodzących, nie należy zaniedbywać kontroli wyjść i osób wychodzących. Pozwala na to m.in. na monitorowanie ewakuacji np. w razie pożaru.

Telewizja przemysłowa CCTV

Telewizja przemysłowa CCTV (z ang. *closed-circuit television*) 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.

Telewizja przemysłowa sprawdza się w przypadku kiedy wybrane strefy, obszary lub pomieszczenia wymagają stałej kontroli i nadzoru. Zastosowanie telewizji przemysłowej pozwala na:

- prowadzenie działań ochronnych z oddalonych miejsc,
- identyfikację rodzaju zdarzenia,
- wykrycie i identyfikację osób oraz pojazdów,
- detekcję ruchu,
- zapis materiałów audio i wideo.

System CCTV składa się z następujących elementów:

- kamer stałych lub ruchomych (z opcją śledzenia),
- serwera wideo,
- rejestratora wideo,
- centrum monitoringu.

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 CCTV zainstalowany na 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 CCTV.

Z systemem CCTV powinno współpracować 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.

SSWiN oparte są na urządzeniach:

(1) wykrywających ruch w strefie objętej ich działaniem,
(2) sygnalizujących otwarcie drzwi,
(3) sygnalizujących wypełnienie otworów budowlanych (wejścia, okna, inne otwory),
(4) sygnalizujących uszkodzenie powierzchni szklanych,
(5) ostrzegających o zagrożeniach (przyciski alarmowe).

Systemem SWiN powinien być objęty obwód zewnętrznej strefy ochrony 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 alarmy sygnalizacji zagrożenia.

Archiwizacja zdarzeń powinna obejmować:
- system CCTV minimum 30 dni zapisu;
- systemy SKD oraz SSWiN do 5 lat.

Należy pamiętać, by wszystkie zabezpieczenia spełniały wymagania zapisane w odpowiednich normach. Przykładowe normy:
Systemy sygnalizacji włamania i napadu - norma PN-EN 50131
Systemy kontroli dostępu - norma PN-EN 50133
System telewizji przemysłowej - norma PL-EN 50132
Okna, drzwi, żaluzje – norma PN-ENV 1627:2006

2.6. Ochrona techniczna

Ochrona techniczna infrastruktury krytycznej to zespół przedsięwzięć i procedur mających na celu minimalizację ryzyka zakłócenia funkcjonowania infrastruktury krytycznej związanego z technicznymi aspektami budowy i eksploatacji obiektów, urządzeń, instalacji lub usług infrastruktury krytycznej.

Oznacza to, że ochrona techniczna IK obejmuje m.in.:

- sprawy związane ze zgodnością budynków, urządzeń, instalacji i usług z obowiązującymi przepisami i normami np. budowlanymi i przeciwpożarowymi;
- działania techniczne mające na celu zmniejszenie uzależnienia funkcjonowania IK od zewnętrznych usług;
- działania techniczne mające na celu zapewnienia ciągłości funkcjonowania IK.

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

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

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

1) okresowej, co najmniej raz w roku, polegającej na sprawdzeniu stanu technicznego:
   a) elementów budynku, budowli i instalacji narażonych na szkodliwe wpływy atmosferyczne i niszczące działania czynników występujących podczas użytkowania obiektu,
   b) instalacji i urządzeń służących ochronie środowiska,
   c) instalacji gazowych oraz przewodów kominowych (dymowych, spalinowych i wentylacyjnych);
2) okresowej, co najmniej raz na 5 lat, polegającej na sprawdzeniu stanu technicznego i przydatności do użytkowania obiektu budowlanego; kontrolą tą

powinno być objęte również badanie instalacji elektrycznej i piorunochronnej w zakresie stanu sprawności połączeń, osprzętu, zabezpieczeń i środków ochrony od porażeń, oporności izolacji przewodów oraz uziemień instalacji i aparatów;

3) okresowej, co najmniej dwa razy w roku, w terminach do 31 maja oraz do 30 listopada, w przypadku budynków o powierzchni zabudowy przekraczającej 2000 m^2 oraz innych obiektów budowlanych o powierzchni dachu przekraczającej 1000 m^2; osoba dokonująca kontroli jest obowiązana bezzwłocznie pisemnie zawiadomić właściwy organ o przeprowadzonej kontroli;
4) bezpiecznego użytkowania obiektu każdorazowo w razie wystąpienia czynników zewnętrznych oddziaływujących 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 zabezpieczenie 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 zainteresowane przyczynami lub skutkami 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.

Urządzenia techniczne stwarzające zagrożenie poprzez:

- rozprężanie gazów znajdujących się pod ciśnieniem różnym od atmosferycznego,
- wyzwolenie energii potencjalnej lub kinetycznej przy przemieszczaniu ludzi lub ładunków w ograniczonym zasięgu,
- rozprzestrzeniania się materiałów niebezpiecznych podczas ich magazynowania lub transportu

objęte są dozorem technicznym!

2.6.2. 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 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 budowlany 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, zwierząt oraz ratowanie 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 organizację ewakuacji ludzi oraz praktyczne sposoby jej sprawdzania określana jest w instrukcji bezpieczeństwa pożarowego.

2.6.3. 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 poprzez:

- zasilanie z dwóch niezależnych stacji transformatorowych, wodociągów i sieci łączności lub do transmisji danych. Przewody powinno umieścić się pod ziemią i doprowadzić do różnych miejsc w budynku;
- zasilanie instalacji strukturalnych poprzez urządzenia podtrzymująco – stabilizujące – pojemność baterii akumulatorów powinna być dobrana z uwzględnieniem wszystkich urządzeń obiektu wymagającego rezerwowania;
- zasilanie rezerwowe obiektu poprzez 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;

Zagadnienie wymagań dotyczących niezawodności zasilania i dostępu do mediów najlepiej rozpatrzyć już w proces 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.

2.6.4. Działania techniczne mające na celu zapewnienia 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. Tym niemniej to ocena ryzyka zakłócenia funkcjonowania IK powinna być podstawą decyzji, które elementy infrastruktury organizacji powinny zostać zdublowane. Redundancja powinna być zarówno logiczna jak i fizyczna.

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

2.7. Ochrona osobowa

Ochrona osobowa to zespół przedsięwzięć i procedur mających na celu minimalizację ryzyka związanego z osobami, które poprzez 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).

Należy pamiętać, że wiele aspektów ochrony osobowej jest nierozerwalnie związanych z innymi elementami systemu bezpieczeństwa IK takimi jak ochrona fizyczna czy teleinformatyczna.
Dopiero komplementarność wszystkich elementów zapewni satysfakcjonujący poziom ochrony IK przed zagrożeniami wewnętrznymi np.: rozczarowanymi pracownikami, prowokacjami dziennikarskimi, 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.

2.7.1. Postępowanie w trakcie zatrudniania

Podstawą skuteczności ochrony osobowej jest zebranie jak największej ilości 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.

2.7.1.1. 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, ma aktualną datę ważności. Obowiązkowo należy wymagać dokumentów trudnych do podrobienia takich jak: paszport, dowód osobisty czy prawo jazdy.

2.7.1.2. Kwalifikacje

Sprawdzenia kwalifikacji kandydata powinno opierać się o weryfikację informacji zawartych w dokumentach rekrutacyjnych (CV, formularze 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.

- **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. 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 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), 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.

2.7.1.3. 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.

2.7.2. *Postępowanie w stosunku do zatrudnionych*

Priorytetem w ochronie osobowej jest dokładne sprawdzenie pracownika jeszcze przed jego zatrudnieniem, nie wolno zaniedbywać jednak zasad bezpieczeństwa w stosunku do już zatrudnionych w organizacji.

2.7.2.1. 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 z organizacją lub 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.

2.7.2.2. Dostęp[7]

Jednym z podstawowych sposobów na ochronę osobową IK jest ograniczanie dostępu pracowników organizacji do wrażliwych miejsc lub zasobów znajdujących się 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.

[7] o zasadach i sposobach przyznawania i kontroli dostępu czytaj także w rozdz. 2.5.2 i 2.5.4

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.

2.7.2.3. 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, celem szybkiego rozpoznania każdego nielegalnie przebywającego w danym obszarze pracownika i podjęcia odpowiednich kroków. Tam gdzie ma to uzasadnienie należy wprowadzić dodatkowo odzież służbową lub inny sposób identyfikacji poprzez elementy ubioru (kolorowe kamizelki, kaski itp.).

Nie należy nosić identyfikatorów w widocznych miejscach poza obiektami IK. Utrudni to osobom niepowołanym poznanie wyglądu graficznego identyfikatorów.

2.7.3. 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 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.

2.7.4. Usługodawcy/podwykonawcy

Pracownicy podmiotów wykonujące pracę na zlecenie operatora IK powinny zostać zweryfikowane 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 wydać przepustki lub ustanowić prawa dostępu do sieci. Wszelkie prace mogące mieć negatywny wpływ na IK muszą być wykonywane pod nadzorem stałej kadry IK.

2.7.5. Postępowanie z odchodzącymi z pracy

Każdy z pracowników odchodzących z organizacji jest w posiadaniu mniej lub bardziej wrażliwej wiedzy, która może być wykorzystana w nielegalny sposób. 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 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.

2.8. Ochrona teleinformatyczna

Ochrona teleinformatyczna infrastruktury krytycznej to zespół przedsięwzięć, procedur mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK związanego z wykorzystaniem do jej użytkowania systemów i sieci teleinformatycznych.

Współcześnie, skuteczny cyberatak na IK może bezpośrednio grozić naruszeniem bezpieczeństwa państwa i jego obywateli. Infrastruktura krytyczna jest narażona na cyberataki zarówno profesjonalistów – cyberprzestępców, którzy mogą doprowadzić do zakłócenia jej funkcjonowania IK[8], jak również może zostać również „zaatakowana" w sposób niezamierzony, na przykład w wyniku awarii systemu lub niesprawności urządzeń lub programów ją obsługujących.

2.8.1. 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.

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[9].
System dostawy wody pitnej	1999, Australia	Dostawa wody	Przykład sabotażu przeprowadzony przez byłego pracownika firmy, który doprowadził do dezaktywacji

[8] 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*.

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

			system alarmowego, co w konsekwencji wprowadziło zakłócenia w dostawie pitnej wody, w tym jej zanieczyszczenie. Cyberatak był zemstą za odmówienie zatrudnienia. System obsługiwany był drogą radiową[10].
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[11].
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

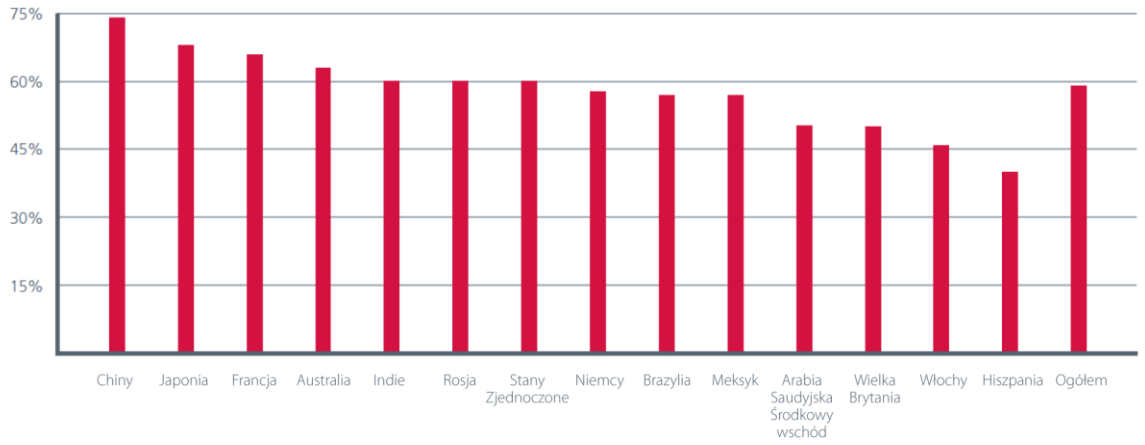
[10] http://217.148.85.64/UserFiles/File/TNO-DV%202008%20C096_web.pdf
[11] http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=131008o7

			komputer pracownika firmy obsługującej system, a następnie w sposób zdalny zainstalował wirusa i oprogramowanie szpiegujące na głównym serwerze obsługującym system filtracji[12].
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[13].

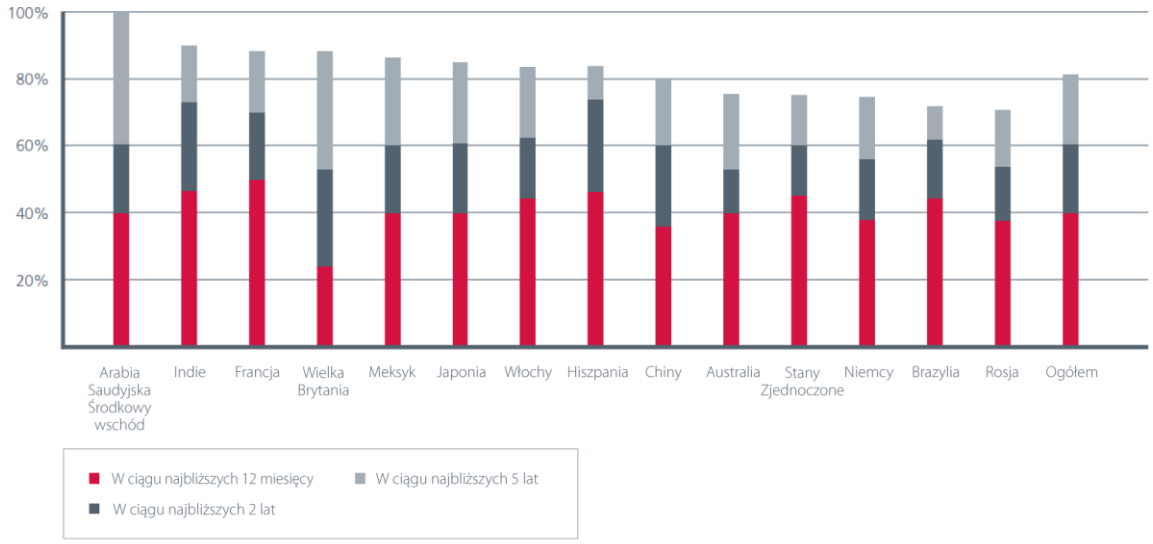
Cyberataki na systemy IK stały się częścią konfliktów cybernetycznych cyberprzestrzeni, w tym konfliktów pomiędzy państwami. Z racji trudności jakie niesie ze sobą precyzyjna identyfikacja źródeł cyberataków w sieci, lub celowe ich rozproszenie, trudno jest jednoznacznie udowodnić zaangażowanie się państw 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.

Niezależnie od powyższego wiele państw w sposób poważny rozpatruje taką możliwość, a nawet, co wskazują poniżej przywołane statystyki, wierzą że takie praktyki już mają miejsce. Wiele państw również zakłada, że tego typu cyberataki pojawią się w najbliższej przyszłości.

[12] http://blogs.abcnews.com/theblotter/2006/10/hackers_penetra.html
[13] http://www.us-cert.gov/control_systems/pdf/ICSA-10-272-01.pdf



rys. 9 - odsetek obywateli wierzących, że rządy innych państw były zaangażowane w cyberataki cybernetyczne na ich infrastrukturę krytyczną[14]



rys. 10 - odsetek obywateli oczekujących poważnych incydentów skierowanych przeciwko ich infrastrukturze krytycznej[15]

[14] In The Crossfire. Critical Infrastructure in the Age of Cyberwar - http://resources.mcafee.com/content/NACIPReport
[15] In The Crossfire. Critical Infrastructure in the Age of Cyberwar - http://resources.mcafee.com/content/NACIPReport

2.8.2. Zasady ochrony teleinformatycznej 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[16]:

- Poufność;
- Integralność;
- Dostępność.

Dodatkową niepowiązaną z poprzednimi istotną cechą bezpieczeństwa, na którą należy zwrócić uwagę jest rozliczalność, która zapewnia, że określone działania danego podmiotu, jest jednoznacznie przypisane temu podmiotowi.

Oznaczają one, że aby uznać system za odpowiednio zabezpieczony to 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.

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

Szczególnymi zagrożeniami dla tak rozumianego modelu bezpieczeństwa są:

- nieuprawniony dostęp do informacji i procesów jako naruszenie ich **poufności**;
- zmianę lub inne zakłócenie informacji i wykonywanych procesów jako naruszenie ich **integralności**;
- blokadę dostępu do informacji i procesów jako naruszenie ich **dostępności**.

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

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

przebieg procesów technologicznych lub produkcyjnych (ang. SCADA – Supervisory Control And Data Acquisition) są w praktyce systemami działającymi na platformach systemów Windows lub Linux. Dlatego cyberataki sieciowe wykorzystujące słabości systemowe tych systemów również dotyczą systemów SCADA na nich działających.

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 (ISO) i Międzynarodową Komisję Elektrotechniczną (IEC – International Electrotechnical Comission)[17]. Standard ten przedstawia najlepsze praktyki i rekomendacje z dziedziny bezpieczeństwa teleinformatycznego, właśnie zgodnie z zaprezentowanym wcześniej modelem C-I-A. Standard ISO/IEC zawiera 11 podstawowych obszarów organizacji bezpieczeństwa teleinformatycznego w organizacji:

i. Polityka bezpieczeństwa;
ii. Organizacja bezpieczeństwa informacji;
iii. Zarządzanie aktywami;
iv. Bezpieczeństwo zasobów ludzkich;
v. Bezpieczeństwo fizyczne i środowiskowe;
vi. Zarządzanie systemami i sieciami;
vii. Kontrola dostępu;
viii. Zarządzanie ciągłością działania;
ix. Pozyskiwanie, rozwój i utrzymanie systemów informatycznych;
x. Zarządzanie incydentami związanymi z bezpieczeństwem informacji;
xi. Zgodność z wymaganiami prawnymi i własnymi standardami.

Polskim odpowiednikiem ISO/IEC 17799:2005 jest opublikowana 9 stycznia 2007 roku norma PN-ISO/IEC 17799:2007 (wcześniej znana jako PN-ISO/IEC 17799:2003)[18]

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

[17] Norma ta pochodzi od standardu brytyjskiego z tej dziedziny, tj. British Standard 7799
[18] O bezpieczeństwie systemów SCADA można przeczytać również w: NIST SP 800-82 „Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems" (NIST 800-82) oraz ANSI/ISA-TR99.00.01-2007 „Manufacturing and Control Systems Security".

rys. 11 - obszary tematyczne standardu ISO/IEC 27002

Najistotniejszymi elementami ochrony teleinformatycznej 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

2.8.2.1. 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. Nawet jeśli to stwierdzenie wyda się kontrowersyjne, to już na pewno kontrowersje te nie powinny dotyczyć IK. Dlatego niezwykle 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 pomiędzy 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[19]. 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 pomiędzy uczestnikami była wartościowa i aby nie były naruszone zasady zaufania i poufności, przede wszystkim poprzez 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:

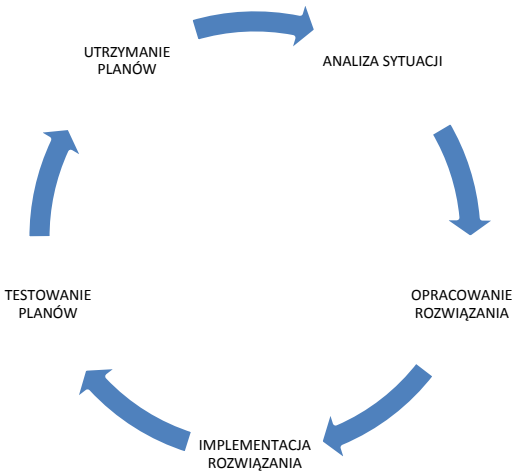
- Powiadomić innych członków o niebezpiecznej sytuacji;
- Uzyskać wsparcie merytoryczne w radzeniu sobie z sytuacją;
- Podjąć wspólne działania w celu osłabienia siły zagrożenia.

Jako dobre przykłady działania tego typu współpracy sektorowej można podać holenderską inicjatywę sektora finansowego o nazwie FI-ISAC[20] oraz amerykański ISAC sektora informatycznego – IT-ISAC[21].

[19] Te informacje ze względu na wysokie wymagania dotyczące poufności mogą być wymieniane w sposób anonimowy.
[20] http://www.samentegencybercrime.nl/Informatie_knooppunt/Sectorale_ISACs/FIISAC?p=content . W serwisie można odnaleźć również wiele innych tego typu inicjatyw sektorowych.
[21] https://www.it-isac.org/

2.8.2.2. Plany awaryjne[22]

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

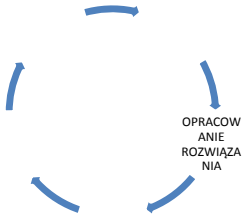


rys. 12 - cykl wdrożenia planów awaryjnych

- **Analiza sytuacji**

W tej fazie najważniejszym zadaniem jest ustalenie tych zasobów, które powinny być uwzględnione w planach awaryjnych. Jest to zadanie ściśle związane z oceną ryzyka. Tymi zasobami mogą być zarówno personel, infrastruktura fizyczna, infrastruktura techniczna, a także zasoby zewnętrzna, np: kluczowi dostawcy materiałów lub informacji koniecznej do podtrzymania procesu biznesowego. Również w tej fazie trzeba określić sytuacje kryzysowe, w których uruchamiane są plany awaryjne.

- **Opracowanie rozwiązania**



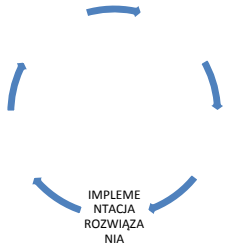
W fazie opracowania rozwiązania powstają szczegółowe plany, które odpowiadają na pytania: Kiedy? Kto? Co? W jaki sposób? Opracowując te plany trzeba pamiętać, że nie wszystkie sytuacje da się przewidzieć w fazie planowania. Dlatego oprócz szczegółowych gotowych planów powinien powstać mechanizm rozwiązania sytuacji, w której wystąpiło to czego nikt nie przewidział. Taki mechanizm przede wszystkim powinien zawierać

[22] rozwiązania dotyczące planów awaryjnych mogą zostać użyte także w innych rodzajach ochrony

reguły dotyczące tego jakie osoby (stanowiska) biorą udział w rozwiązaniu problemu i w jaki sposób podejmują one decyzję.

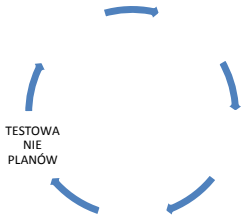
Ważnym elementem zabezpieczenia danych jest systematyczne tworzenie kopii zapasowych, których częstotliwość wykonywania powinna wynikać z analizy ryzyka oraz czasu dostępności do danych. Zakres wykonywania kopii zapasowych dla serwerów musi zawierać oprogramowanie systemowe (konfiguracja systemu), zainstalowane oprogramowanie użytkowe. Dla urządzeń sieciowych (routerów, switchy, zapór ognowych itp.) oznacza to zapisanie ich konfiguracji, a dla stacji roboczych przetwarzane informacje zgodnie ze zgłoszonym przez użytkownika zapotrzebowaniem.

- **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 obejmującej nie więcej niż 3 komórki organizacyjne. Natomiast test złożony powinien obejmować uruchomienie co najmniej 3 procedur awaryjnych na raz i swoim zasięgiem objąć maksymalnie największą liczbę komórek organizacyjnych firmy. 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"). Testy takie we wspomnianych obszarach pomagają utrwalić prawidłowe mechanizmy zachowań. Przykładowy scenariusz może uwzględniać:

- awarię głównego serwera pocztowego organizacji;

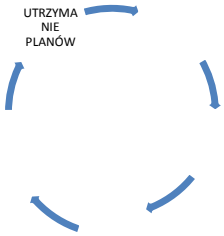
- atak wirusa unieruchamiającego komunikaty alarmowe przekazywane z systemu SCADA;
- awarię systemu kontroli fizycznej wejścia do budynku.

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**



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 odbywało 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.

2.8.2.3. 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. 13 - podstawowe elementy bezpieczeństwa oprogramowania

2.8.2.4. Kontrola dostępu

Kontrola dostępu do zasobów jest podstawowym sposobem ochrony systemu 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 zmianę zakresu dostępu na tzw. „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 poprzez system (jeżeli na to pozwala).

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

- **Kontrola dostępu poprzez 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[23]. Technikę tworzenia sieci wirtualnych można na przykład wykorzystać przy separacji logicznej kluczowych zasobów takich jak systemy SCADA.

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.

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

- **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 poprzez zestawienie szyfrowanego połączenia, tzw. wirtualnej sieci prywatnej (ang. Virtual Private Network)[24].

- **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. Dostęp do tej części sieci powinien odbywać się z wydzielonych fizycznie i logicznie urządzeń, poprzez poufne (szyfrowane) kanały komunikacji. W tej części sieci w sposób specjalny powinno być prowadzone monitorowanie ruchu sieciowego, a progi akceptacji dla zjawisk o charakterze anomalii powinny być ustawione na jak najniższym poziomie.

- **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 sie 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).

[24] 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

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.

- **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 jest stosować w przypadku ochrony przed złośliwym oprogramowanie instalującym się bez wiedzy użytkownika w trakcie odwiedzin zainfekowanej strony WWW[25]. Idea „czarnej listy" polega na wskazaniu tych adresów (e-mail, IP, domenowych), które nie są dozwolone w ruch przychodzącym. Wszystkie inne adresy będą dopuszczone. Natomiast „biała lista" zawiera te adresy, które będą akceptowane jako adresy źródłowe. Żadne inne adresy, które nie znajdują się na „białej liście" nie będą akceptowane. Oprócz wspomnianej możliwości wykorzystania tej techniki w ochronie komunikacji internetowej (spam, drive-by download), można ją również z powodzeniem wykorzystywać w zarządzaniu siecią wewnętrzną i zewnętrzną, w ustalaniu praw dostępu do poszczególnych aplikacji.

- **Serwer pośredniczący (ang. proxy serwer)**

Kolejną techniką kontroli dostępu jest użycie serwera pośredniczącego. Oprócz funkcji bezpieczeństwa może on również spełniać zadania poprawy efektywności ruchu, np.: poprzez 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. Serwer typu proxy może posłużyć również jako serwer „przesiadkowy" do autoryzacji użytkowników, w sytuacji kiedy autoryzacja ta ma pozwolić na dostęp do systemów IK. Dzięki temu nie ma konieczności łączenia się bezpośrednio z krytycznym serwerem co rodzi dodatkowe ryzyko.

[25] tzw. drive-by download (http://en.wikipedia.org/wiki/Drive-by_download)

- **Dostęp zdalny dodzwaniany (dial-up)**

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.

2.8.2.5. Ochrona stacji roboczych

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

- **Aktualizacja oprogramowania**

Najlepiej jeśli będzie się odbywała w sposób automatyczny. 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, często nie jest możliwe korzystanie z tej funkcji, a wprowadzenie zmiany w oprogramowaniu wiąże się z zastosowanie procedury zarządzania zmianą i przeprowadzeniem serii testów. Jest to

zrozumiałe, niemniej jednak wprowadza zwiększone ryzyko dla bezpiecznego funkcjonowania 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[26] (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[27]. Jeśli jednak taka ocena nie jest dostępna to możliwe jest przeprowadzenie jej samemu, np: z wykorzystaniem kalkulatora CVSS[28].

- **Firewalling**

Zasady, które należy wykorzystywać przy ochronie stacji roboczych poprzez stosowanie „zapory ogniowej" nie różnią się zasadniczo o tych opisywanych wcześniej[29]. Podstawową różnicą jest to, ze do ochrony stacji roboczych używamy tzw. osobistych „zapór ogniowych". Są one albo wbudowane w system operacyjny, albo są oddzielnym dedykowanym oprogramowaniem.

- **Ochrona przed złośliwym oprogramowaniem**

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

- 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

[26] http://www.first.org/cvss/cvss-guide.html
[27] np.: CISCO: http://www.cisco.com/web/about/security/intelligence/Cisco_CVSS.html
[28] np.: udostępnianego przez NIST: http://nvd.nist.gov/cvss.cfm?calculator
[29] Patrz rozdział 2.8.2.4 Kontrola dostępu

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 oprogramowani (lub chociażby nieznacznie modyfikowanego w celu poprawienia jego kamuflażu) jest bardzo duża[30]. Dlatego w praktyce nie jest możliwe skuteczne wykrycie wszystkich istniejących w sieci wirusów. Nie zmienia to oczywiście faktu konieczności używania odpowiedniego oprogramowania.

2.8.2.6. 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.

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.

2.8.2.7. Ochrona własnej sieci bezprzewodowej

Analizując bezpieczne korzystanie z sieci bezprzewodowych należy wziąć pod uwagę następujące filary bezpieczeństwa:

- **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.

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

- **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.

- **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.

- **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 uniknięcie dołączenia się do sieci nieautoryzowanych urządzeń sieciowych bez zastosowania specjalistycznych technik nielegalnego podszywania się pod wybrany adres MAC.

- **Fizyczne ograniczenie dostępu do sieci**

Poprawa bezpieczeństwa sieci bezprzewodowych w organizacji możliwa jest również poprzez 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[31] pozwoli na wykrywanie nieuprawnionych prób dostępu.

[31] Patrz rozdział 2.8.2.9 Monitoring zagrożeń

2.8.2.8. 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[32];
- w przypadku nie korzystania z sieci bezprzewodowych powinni oni wyłączać bezprzewodową kartę sieciową zainstalowaną w urządzeniu przenośnym.

2.8.2.9. 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.

[32] Patrz punkt 2.7.2.4 Kontrola dostępu (dostęp z zewnątrz)

2.8.2.9.1. 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 następuję 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 poprzez 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.

2.8.2.9.2.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;
- styku 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[33].

Oprócz samej implementacji systemów monitorujących, należy wypracować odpowiednią procedurę obsługi tych systemów. Najważniejsze elementy, które powinny znaleźć się w takiej procedurze[34] 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.

[33] w kwestii technik poprawy konfiguracji warto skorzystać z porad zamieszczonych w http://www.symantec.com/connect/articles/strategies-reduce-false-positives-and-false-negatives-nids

[34] 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

2.8.2.10. Reakcja na incydenty

Istotną kwestią organizacyjną jest powołanie w strukturach organizacji zespołu do spraw reagowania na przypadki naruszania bezpieczeństwa teleinformatycznego zwanego CERT[35] (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.

Jak zbudować zespół typu CERT[36]

rys. 14 - 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.

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

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

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 CERTu. Warto wtedy omówić te oczekiwania z kierującymi innymi komórkami (w szczególności dział IT, prawny i public relations). Pozwoli to między innymi na zaplanowanie koniecznych zasobów ludzkich i technicznych do funkcjonowania przyszłego zespołu. W trakcie tej fazy zbieramy również informacje na temat już istniejących zasad bezpieczeństwa w organizacji, w tym jak do tej pory (jeśli w ogóle) odbywało się reagowanie na incydenty. Pomocne również będą wszelkie schematy organizacyjne i organizacyjne procedury.

Krok IV – Zaprojektowanie wizji działania

Choć zadanie to brzmi ogólnikowo, to jest ono niezwykle ważne. Zdefiniowanie takich rzeczy jak:

- obszar działania (tzw. „constituency") zespołu, czyli to jakiej grupie użytkowników sieci CERT będzie świadczył swoje usługi;
- zdefiniowanie misji i celów działania;
- ustalenie zakresu świadczonych usług reaktywnych, proaktywnych i konsultacyjnych[37]
- 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 nowopowstającego 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

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

w obszarze działania na temat tego jak zachowywać się w przypadku stwierdzenia lub podejrzenia naruszenia bezpieczeństwa teleinformatycznego.

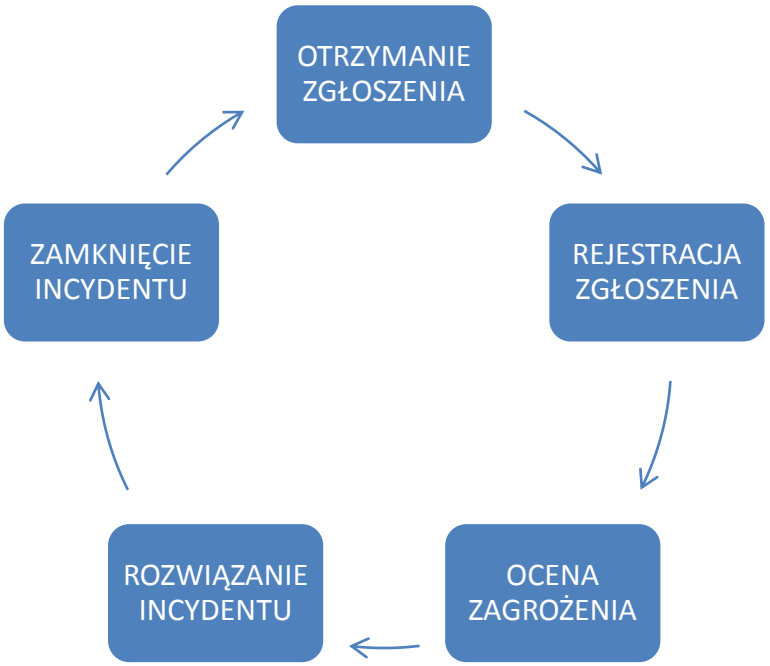
Krok VII – Ogłoszenie działań operacyjnych

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 wywiad z zainteresowanymi odbiorcami usług CERT, a także pewnymi miernikami, np: liczbą raportowanych i rozwiązywanych incydentów, czasem ich obsługi, zaimplementowaniu nowych narzędzi ochrony teleinformatycznej, które wynikają z wniosków z obsługi incydentów.

2.8.2.10.1. Obsługa incydentów w przypadku posiadania w strukturze organizacji zespołu CERT



rys. 15 - 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[38]:

- otrzymanie zgłoszenia o potencjalnym incydencie;
- rejestracja zgłoszenia (najlepiej z wykorzystaniem systemu wsparcia obsługi incydentów[39]);
- ocena zagrożenia związanego ze zgłoszeniem (co pozwala na nadanie odpowiedniego priorytetu obsługi):
  - weryfikacji słuszności zgłoszenia jako incydentu,
  - wstępna klasyfikacja incydentu[40],
  - ostateczne ustalenie priorytetu obsługi,
  - przypisanie obsługi incydentu do odpowiedniej osoby/osób;

[38] 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)

[39] Jednym z bardziej rozpowszechnionych systemów obsługi incydentów jest RTIR (Request Tracker for Incident Response - http://bestpractical.com/rtir/)

[40] 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

- rozwiązanie incydentu, które odbywa się w cyklu:
  - analiza danych,
  - ustalania 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.

2.8.2.10.2. 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 CERTu zewnętrznego (ang. constituency). W Polsce istnieje formalnie 5 zespołów CERTowych[41].

Oprócz formalnie działających zespołów CERTowych 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 CERTu 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.

[41] stan na marzec 2011 roku

Formalnie działające w Polsce zespoły CERT

ZESPÓŁ	ADRES WWW	OBSZAR DZIAŁANIA
CERT GOV PL	http://cert.gov.pl/	Sieci domeny gov.pl, z wyłączeniem sieci instytucji wojskowych.
CERT PIONIER	http://cert.pionier.gov.pl/	Podsieci Krajowej Szerokopasmowej Sieci Naukowej PIONIER (POL34/622). Sieci te wyszczególnione są na poniższej liście: AS13293, AS8501, AS8286, AS8267, AS8323, AS12324, AS12346, AS8256, AS8865, AS12423, AS15798, AS15373, AS9112, AS8364, AS5550, AS12831, AS9103, AS13065, AS8326, AS12618, AS8970, AS15851.
CERT PLIX	http://cert.plix.pl/	Sieci klientów węzła wymiany ruchu PLIX, wskazanych w wykazie na stronie: http://plix.pl/pl/member
CERT Polska	http://www.cert.pl/	Sieci nie objęte obszarem działania innych CERTów, należące do domeny .pl.
MIL CERT[42]		Sieci domeny mil.pl oraz gov.pl dla sieci instytucji wojskowych.
TP CERT	http://www.tp.pl/prt/tpcert	Społeczność internetowa Telekomunikacji Polskiej. Sieci związane z następującymi systemami autonomicznymi: AS 5617, 29535

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

2.9. Ochrona prawna

Ochrona prawna 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 ochronie prawnej mamy na myśli przede wszystkim narzędzia stosowane przez państwo, aby zabezpieczyć najważniejsze obiekty IK przed zagrożeniami. Oznacza to zastosowanie narzędzi prawnych niedopuszczających, poprzez 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.

Takie narzędzia 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).

Ochrona prawna 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, powalające na egzekwowanie dostępu do IK oraz zabezpieczenia się umowami z dostawcami mediów są przykładami dobrych praktyki w tym zakresie.

2.10. Plany odbudowy

Faza odbudowy jest ostatnim etapem ochrony infrastruktury krytycznej. 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 zawczasu przygotować stosowne plany.

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, 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),
- zaopatrzenia itp.

Należy zawczasu 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.

Wszystkie plany muszą uzyskać akceptacje kierownictwa i być dostępne dla wszystkich pracowników, na których zostały nałożone obowiązki w fazie 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. Plan dodatkowo powinien zawierać opisane okoliczności, w których może być użyty, procedury jego uruchamiania, sposób mobilizacji zespołu, miejsca spotkań oraz dane kontaktowe do osób kluczowych w fazie odbudowy IK.

Plany sporządzone powinny zostać w kilku egzemplarzach, a następnie rozdystrybuowane po wszystkich obiektach IK!

Dobór osób odpowiedzialnych za zarządzanie 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 powrotu IK do stanu sprzed katastrofy, jednocześnie wdrażając nowe rozwiązania celem zapewnienia jeszcze większego poziomu bezpieczeństwa.