Franciszek Wołowski
Janusz Zawiła-Niedźwiecki

Bezpieczeństwo systemów informacyjnych

Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi

Poradnik jest skierowany w pierwszej kolejności do administratorów bezpieczeństwa systemów informacyjnych, ale nie tylko.
Także do szeroko rozumianej kadry kierowniczej organizacji różnych branż, charakteru i wielkości oraz do specjalistów różnych profesji, którzy mogą się przyczyniać do zapewniania bezpieczeństwa w organizacjach. Rzecz bowiem w tym, że stan bezpieczeństwa budują wszyscy, a zburzyć go może nawet tylko jedna osoba.

edu-Libri

Redakcja merytoryczna i korekta: edu-Libri

Projekt okładki i stron tytułowych: GRAFOS

Wydawnictwo edu-Libri
ul. Zalesie 15, 30-384 Kraków
e-mail: edu-libri@edu-libri.pl

Skład i łamanie: GRAFOS
Druk i oprawa: Sowa Sp. z o.o.
Warszawa

ISBN 978-83-63804-00-8
ISBN e-book 978-83-63804-01-5 (PDF)
ISBN e-book 978-83-63804-02-2 (epub)

Spis treści

Najczęstszą przyczyną wystąpienia tego rodzaju incydentów jest słaby lub źle skonfigurowany system operacyjny, niekontrolowane wprowadzanie zmian, awarie sprzętu i oprogramowania umożliwiające dostęp do informacji osobom, które nie mają do nich praw.

Inne przypadki to:

- pozyskanie plików haseł,
- przepełnienie bufora w celu uzyskania dodatkowych przywilejów,
- wykorzystanie słabości protokołów w celu przejęcia lub oszukania połączeń sieciowych,
- powiększenie przywilejów ponad te, udzielone przez administratora,
- przełamanie ochrony fizycznej w celu nieuprawnionego dostępu do informacji,
- spadek wydajności spowodowany większą liczbą użytkowników, niż przewidziano,
- awaria sprzętu (naruszenie dostępności),
- zablokowanie systemu spowodowane brakiem umiejętności użytkowników,
- błąd (awaria) oprogramowania,
- atak (*malwa re* – naruszenie integralności i dostępności),
- włamanie i usunięcie danych (naruszenie integralności i dostępności),
- ujawnienie informacji, wykorzystanie w celach prywatnych (naruszenie poufności).

4.3. Procedury w zarządzaniu incydentami

Zarządzanie reakcją na incydent wchodzi w zakres zarządzania bezpieczeństwem a więc i w tym przypadku proces ten można przedstawić przy pomocy modelu PDCA – zwanym również cyklem Deminga (rys. 1.4). Tabela 4.1 przedstawia procedury w układzie modelu PDCA z uwzględnieniem specyfiki zarządzania incydentami.

4.3.1. Planowanie i przygotowanie

Od dokładności przeprowadzenia tego etapu zależy jakość realizowanych w przyszłości prac związanych z zarządzaniem incydentami. Po jego zakończeniu organizacja powinna być w pełni przygotowana do właściwego zarządzania incydentami. Na tym etapie podejmowane są następujące czynności:

- prace przygotowawcze,
- opracowanie polityki zarządzania incydentami naruszania bezpieczeństwa informacji,
- ustalenie postępowania z incydentami naruszania bezpieczeństwa informacji,

- aktualizacja polityki bezpieczeństwa informacji i procedur analizy ryzyka,
- powołanie Zespołu Reagowania na Incydenty (naruszania) Bezpieczeństwa Informacji – ZRIBI,
- powiązanie zarządzania incydentami z innymi obszarami zarządzania organizacją,
- powiązanie z zewnętrznymi organizacjami,
- organizacja wsparcia technicznego i organizacyjnego,
- opracowanie programu uświadamiania i szkolenia.

Tabela 4.1. Procedury w układzie modelu PDCA stosowane w procesach zarządzania incydentami

Planuj – Planowanie i przygotowanie (ustanowienie SZBI – *plan*)	Ustanowienie polityki bezpieczeństwa, jej celów, zakresu stosowania, procesów i procedur odpowiadających zarządzaniu ryzykiem oraz zwiększających bezpieczeństwo informacji, tak aby uzyskać wyniki zgodne z ogólnymi zasadami i celami organizacji.
Wykonaj – Stosowanie (wdrożenie i eksploatacja SZBI – *do*)	Wdrożenie i eksploatacja polityki bezpieczeństwa, zabezpieczeń, procesów i procedur. Wdrażanie procedur i innych zabezpieczeń zdolnych do zapewnienia natychmiastowego wykrycia i reakcji na incydenty związane z naruszeniem bezpieczeństwa.
Sprawdzaj – Przegląd (monitorowanie i przegląd SZBI – *check*)	Ocena lub nawet pomiar wykonania procesów w odniesieniu do polityki bezpieczeństwa, celów i praktycznych doświadczeń oraz przekazywanie kierownictwu wyników przeglądu. Realizowanie procedur monitorowania i przeglądu oraz innych zabezpieczeń w celu natychmiastowego identyfikowania naruszeń bezpieczeństwa i incydentów, zakończonych niepowodzeniem lub sukcesem.
Działaj – Doskonalenie (utrzymanie i doskonalenie SZBI – *act*)	Podejmowanie działań korygujących i prewencyjnych na podstawie wyników przeglądu realizowanego przez kierownictwo, tak aby osiągnąć stałe doskonalenie SZBI.

Źródło: opracowanie własne na podstawie: [ISO/IEC TR 18044:2004].

Prace przygotowawcze. Skuteczne i efektywne wprowadzenie w życie schematu zarządzania incydentami jest uwarunkowane podjęciem i zakończeniem z sukcesem kilku działań przygotowawczych, do których należy zaliczyć:

- sformułowanie polityki zarządzania incydentami oraz uzyskanie dla niej akceptacji najwyższego kierownictwa;
- opracowanie szczegółowego schematu zarządzania incydentami, który powinien uwzględniać:
  - skalę ważności incydentów, umożliwiającą ich formalny podział,

  - wzorce formularzy do zgłaszania i raportowania zdarzeń i incydentów, opis powiązanych z nimi procedur i działań z odniesieniami do procedur wykorzystywanych przez systemy i plan zapewniania ciągłości działania; jeśli to możliwe, to wszystkie formularze powinny być w formie elektronicznej z linkami do bazy zdarzeń/incydentów;
- operacyjne procedury dla ZRIBI ze zdefiniowaną odpowiedzialnością oraz przydzieleniem ról do konkretnym osobom w celu wykonywania takich czynności, jak np.:
  - zamykanie systemu, co w poszczególnych przypadkach powinno być poprzedzone uzgodnieniem tego z właścicielem biznesowym oraz z osobą odpowiedzialną za systemy teleinformatyczne,
  - pozostawienie działającego systemu,
  - uruchomienie procedur odtwarzania z kopii zapasowych, procedur planu zapewniania ciągłości działania oraz podjęcie działań wynikających z polityk bezpieczeństwa poszczególnych systemów,
  - zapewnianie bezpiecznego przechowywania śladów i dowodów (także w wersji elektronicznej), szczególnie w przypadku gdy niezbędne jest przeprowadzenie działań śledczych lub wewnętrznego postępowania wyjaśniającego,
  - wymiana informacji o incydentach z innymi osobami wewnątrz organizacji lub z osobami (organizacjami) trzecimi;
- testowanie użycia ustalonej procedury zarządzania incydentami oraz procesów i procedur ZRIBI;
- aktualizacja polityki bezpieczeństwa informacji, polityki analizy i zarządzania ryzykiem oraz polityk dedykowanych do poszczególnych systemów;
- zorganizowanie ZRIBI wraz z odpowiednim programem szkoleniowym dla jego członków;
- zapewnienie środków (szczególnie technicznych) wspierających zarządzanie incydentami, a co za tym idzie pracę ZRIBI;
- zaplanowanie, rozwój oraz realizację programu uświadamiającego i szkoleniowego dla wszystkich pracowników.

Opracowanie polityki zarządzania incydentami naruszania bezpieczeństwa informacji. Celem polityki jest wskazanie podstawowych zasad zarządzania incydentami naruszania bezpieczeństwa informacji w organizacji, które będą podstawą do opracowania i wdrożenia procesu zarządzania incydentami. Polityka powinna być zatwierdzona przez najwyższe kierownictwo organizacji, a fakt ten powinien być udokumentowany.

Polityka jest przeznaczona dla wszystkich osób posiadających uprawniony dostęp do zasobów informacyjnych organizacji. Powinna być dostępna dla każdego pracownika, współpracownika lub zleceniobiorcy organizacji oraz powinna być uwzględniona w programie uświadamiającym i szkoleniowym.

Polityka powinna:

- określać podstawy formalnoprawne;
- podkreślać znaczenie zarządzania incydentami dla organizacji;
- komunikować akceptację najwyższego kierownictwa dla polityki oraz systemu zarządzania incydentami;
- zawierać przegląd kwestii związanych z wykrywaniem, zgłaszaniem i gromadzeniem informacji o zdarzeniach oraz zdefiniowaniem, w jaki sposób mogą one być wykorzystane do określenia incydentów; przegląd ten powinien zawierać podsumowanie możliwych typów zdarzeń, sposobów wyjaśniania, zakresu raportowania (co, w jaki sposób, gdzie i do kogo przekazywać) oraz sposobu reagowania na nowe, nieznane dotąd, typy zdarzeń;
- określać modelowy przegląd oceny incydentu, ustalenie kto jest odpowiedzialny za jego zaistnienie, wskazanie co ma być zrobione, powiadomienie zainteresowanych stron i przełożonych;
- wskazywać, jak przeprowadzać podsumowanie działań, podjętych po potwierdzeniu faktu, że zdarzenie jest incydentem, co obejmuje:
  - ocenę pierwszej reakcji,
  - analizę śladów i dowodów,
  - komunikację ze wszystkimi zainteresowanymi stronami,
  - ocenę, czy przebieg incydentu jest kontrolowany,
  - wskazanie właściwej dalszej reakcji,
  - podjęcie działań kryzysowych,
  - określenie warunków informowania przełożonych,
  - wskazanie, kto jest odpowiedzialny za poszczególne działania;
- wskazywać potrzebę zadbania o to, aby:
  - wszystkie działania zostały właściwie zapisane w celu ich późniejszej analizy,
  - prowadzone było ciągłe monitorowanie w celu zapewnienia bezpieczeństwa zgromadzonych i przechowywanych śladów i dowodów (także w wersji elektronicznej), szczególnie w przypadku gdy będzie to wymagane do prowadzenia śledztwa lub wewnętrznego postępowania wyjaśniającego;
- określać działania podjęte po zamknięciu incydentu, włącznie z wnioskami wyciągniętymi z przebiegu i wyjaśniania incydentu oraz udoskonalaniem procesu zarządzania incydentami;
- wskazywać miejsce przechowywania dokumentacji zarządzania incydentami (włącznie z procedurami);
- określać, jak dokonywać przeglądów programu uświadamiającego i szkoleniowego w zakresie zarządzania incydentami;

- podawać podstawowe informacje o ZRIBI obejmujące:
  - strukturę organizacyjną ZRIBI wraz z identyfikacją kluczowego personelu oraz określeniem, kto jest odpowiedzialny za:
    - ◇ powiadamianie o incydentach najwyższego kierownictwa organizacji,
    - ◇ gromadzenie informacji i podejmowanie działań,
    - ◇ kontakty (kiedy to konieczne) z organizacjami lub organizacjami zewnętrznymi;
  - precyzyjne określenie, czym zajmuje się ZRIBI i z jakiego upoważnienia działa; minimum to zdefiniowanie misji, zakresu zadań, sponsora i uprawnień ZRIBI:
    - ◇ jasne i jednoznaczne określenie misji i celu funkcjonowania ZRIBI, które powinno skupić się na najważniejszych jego działaniach (m.in. wspieranie, ocenianie, reagowanie i zarządzanie reakcją na incydent, aż do ostatecznego wyjaśnienia jego przyczyn);
    - ◇ definicję zakresu działania ZRIBI, który zwykle obejmuje wszystkie systemy przetwarzania informacji; w szczególnych przypadkach organizacja może ograniczać ten zakres, ale powinno to być jasno określone (co jest objęte zakresem, a co zostało wyłączone) i odpowiednio udokumentowane;
    - ◇ wskazanie osoby z najwyższego kierownictwa, która odpowiada za finansowanie prac ZRIBI i autoryzuje jego działania.

Wiedza na ten temat pozwala pracownikom organizacji zrozumieć podstawy działania i umocowanie ZRIBI, co z kolei umożliwia zbudowanie zaufania do ZRIBI. Przed opublikowaniem tych informacji należy dokonać ich weryfikacji z prawnego punktu widzenia. Należy wziąć pod uwagę fakt, że w niektórych przypadkach ujawnienie uprawnień danego członka ZRIBI może go narazić na naciski wynikające z podległości służbowej.

Postępowanie z incydentami naruszania bezpieczeństwa informacji. Ustalenie modelu właściwego postępowania z incydentami może polegać na opracowaniu szczegółowej dokumentacji opisującej procesy i procedury takiego postępowania oraz sposoby komunikowania o incydentach. Dokumenty te są używane w przypadku wykrycia zdarzenia i służą za poradnik w zakresie:

- reagowania na zdarzenia,
- ustalenia, czy zdarzenie jest incydentem,
- zarządzania incydentami aż do ostatecznego ich wyjaśnienia,
- wdrażania zidentyfikowanych udoskonaleń.

Dokumentacja zarządzania incydentami jest przeznaczona dla wszystkich pracowników organizacji, w szczególności:

- osób odpowiedzialnych za wykrywanie i zgłaszanie zdarzeń, ocenę i reagowanie na zdarzenia i incydenty,
- osób zaangażowanych w działania podjęte po fazie wyjaśniania incydentu, w doskonalenie procesu zarządzania incydentami i samego systemu, perso-

nelu wspierającego działania operacyjne, ZRIBI, kierownictwa organizacji, działu prawnego, rzecznika biura prasowego itp.,

- firm trzecich, organizacji gospodarczych i urzędów.

Dokumentacja zarządzania incydentami powinna zawierać wymienione poniżej elementy.

- Przegląd polityki zarządzania incydentami.
- Przegląd całego systemu zarządzania incydentami.
- Szczegółowe procesy i procedury oraz informacje o narzędziach i klasyfikacji incydentów są związane z:
  - wykrywaniem i opiniowaniem występowania zdarzeń,
  - zbieraniem informacji o zdarzeniach,
  - przeprowadzaniem oceny zdarzeń, wykorzystywaniem klasyfikacji zdarzeń i incydentów oraz ustalaniem, czy zdarzenie można uznać za incydent,
  - fazą „przeglądania" (w przypadku gdy incydenty są potwierdzone),
  - komunikowaniem wystąpienia incydentu lub przekazaniem informacji o incydencie wewnątrz organizacji oraz organizacjom trzecim,
  - podejmowaniem natychmiastowej reakcji zgodnie z analizą i potwierdzoną oceną stopnia ważności incydentu, która może obejmować aktywację procedur odtworzenia i kontakty między osobami zaangażowanymi w reakcję,
  - przeprowadzaniem analizy śladów i dowodów, a jeśli to konieczne, dokonaniem zmiany kategorii lub stopnia ważności incydentu,
  - podejmowaniem decyzji, czy przebieg incydentu ma być kontrolowany,
  - rozpoczęciem innych wymaganych działań (np. ułatwiających odtworzenie systemu po awarii lub zniszczeniu),
  - podejmowaniem działań kryzysowych, jeśli przebieg incydentu nie jest kontrolowany (np. powiadomienie straży pożarnej, uruchomienie planu ciągłości działania),
  - powiadamianiem przełożonych w celu podjęcia dalszej oceny lub decyzji,
  - zapewnianiem, że wszystkie działania są właściwie zapisane w celu ich późniejszej analizy,
  - aktualizacją bazy zdarzeń/incydentów.
- Szczegóły klasyfikacji (skali ważności) zdarzeń i incydentów oraz związanych z nimi wskazówek.
- Wytyczne do podejmowania decyzji, czy wymagane jest zawiadomienie przełożonych w poszczególnych fazach procesu, oraz powiązane z wytycznymi procedury. Każda osoba oceniająca zdarzenie lub incydent powinna wiedzieć, bazując na poradach zawartych w dokumentacji postępowania z incydentami, kiedy w normalnych przypadkach informować przełożonych i których. Należy rozważyć to, że może mieć miejsce nieprzewidywalny lub mało ważny incydent, który w przypadku podjęcia niewłaściwej reakcji lub

jej braku może doprowadzić do sytuacji kryzysowej. Poradnik powinien definiować zdarzenia i typy incydentów, typy zgłoszeń do wyższego kierownictwa i określać, kto może zgłaszać.

- Procedury zapewniające, że wszystkie działania są właściwie zapisane, we właściwej formie, a analiza zapisów jest przeprowadzana przez odpowiedni personel.
- Procedury i mechanizmy zapewniające właściwe zarządzanie zmianami w zakresie śledzenia zdarzeń i incydentów oraz aktualizacji raportowania o incydentach oraz samego systemu zarządzania incydentami.
- Procedury analizy śladów i dowodów.
- Procedury korzystania z systemów wykrywania włamań IDS, zapewniające, że spełnione są wymagania prawne i regulacyjne.
- Schemat struktury organizacyjnej.
- Warunki powoływania i zakres odpowiedzialności ZRIBI (jako całości oraz poszczególnych jego członków).
- Ważne dane kontaktowe (numery telefonów, adresy e-mail).

Dokumentacja postępowania z incydentami powinna określać zarówno natychmiastową, jak i długoterminową reakcję na incydenty. Wszystkie incydenty wymagają bowiem jak najszybszej oceny potencjalnych negatywnych skutków w krótkiej i długiej perspektywie czasu. Dodatkowo, w przypadku wystąpienia zupełnie nieprzewidzianych wcześniej incydentów, podjęcie reakcji może oznaczać konieczność zastosowania rozwiązań tymczasowych (*ad hoc*). Nawet w takich sytuacjach opis sposobu postępowania z incydentami powinien podawać ogólne wytyczne co do kroków, jakie trzeba wykonać.

Po wystąpieniu incydentu należy podjąć takie czynności, dzięki którym w sposób systematyczny i dokładny można będzie ustalić przyczyny jego zaistnienia oraz które pozwolą przygotować właściwą dokumentację. Ułatwi ona i usprawni działania w tym zakresie w przyszłości. Do najważniejszych czynności należą:

- przeprowadzenie (jeśli to wymagane) dodatkowej analizy śladów i dowodów,
- identyfikacja i udokumentowanie wniosków wynikających z incydentu,
- przeglądanie i identyfikacja usprawnień rozwiązań bezpieczeństwa informacji,
- ocena efektywności procesów i procedur w trakcie odtwarzania stanu wyjściowego, oraz wskazywanie możliwości doskonalenia rozwiązań zarządzania incydentami,
- aktualizacja bazy zdarzeń/incydentów.

Stosownie do wniosków wynikających z incydentów, należy dążyć do wprowadzenia udoskonaleń, mając w szczególności na względzie:

- rezultaty analizy i ich odniesienia do dotychczasowego systemu zarządzania ryzykiem,
- zasady zarządzania incydentami (np. procesy, procedury, formularze, struktura organizacyjna),

- ogólny poziom bezpieczeństwa wynikający z wdrożenia nowych lub ulepszonych zabezpieczeń.

W organizacji potrzebne są udokumentowane i sprawdzone procedury, które powinny między innymi:

- określać osoby odpowiedzialne,
- dotyczyć śladów i dowodów związanych z incydentem oraz działań kryzysowych,
- być zgodne z polityką oraz dokumentacją zarządzania incydentami.

ZRIBI powinien zagwarantować publiczny dostęp do porad oraz rezultatów z analizy incydentów, w czytelnej i zrozumiałej dla wszystkich pracowników postaci. Niektóre z tych procedur mogą być opatrzone klauzulą „poufne". Zwłaszcza powinno to dotyczyć informacji szczegółowych o zastosowanych zabezpieczeniach, sposobach śledzenia zdarzeń i sposobach reakcji na zaistniałe incydenty. Ma to na względzie ochronę przed możliwością manipulacji wewnątrz organizacji, jak również wrogimi działaniami z zewnątrz.

Treść procedur zależy od kilku czynników:

- typu incydentu,
- typu produktu,
- natury poszczególnych zdarzeń i incydentów,
- typu zasobów,
- środowiska przetwarzania.

Procedura powinna określać podejmowane kroki i osobę (lub osoby), która ma je podejmować. W procedurze powinny być wykorzystane doświadczenia wewnętrzne i zewnętrzne. Procedury są opracowywane przede wszystkim dla znanych typów zdarzeń i incydentów, ale również dla nieznanych. Dla nieznanych typów zdarzeń i incydentów określa się:

- tryb ich zgłaszania,
- czas niezbędny na uzyskanie aprobaty najwyższego kierownictwa, na tyle krótki, aby uniknąć jakiegokolwiek opóźnienia w podjęciu reakcji,
- delegowanie uprawnień do podejmowania decyzji w sytuacjach nadzwyczajnych lub kryzysowych.

Należy zaplanować regularne kontrole oraz testowanie procesu i procedur, tak aby było możliwe ujawnienie i wskazanie potencjalnych wad oraz problemów, mogących wystąpić w trakcie zarządzania zdarzeniami lub incydentami. Jakakolwiek zmiana, która wynika z przeglądu dokonanego po wyjaśnieniu zdarzenia lub incydentu, powinna być drobiazgowo i dokładnie sprawdzona oraz testowana przed wprowadzeniem w życie.

Polityka bezpieczeństwa informacji i polityka zarządzania ryzykiem. Włączenie kwestii zarządzania reakcją na incydent do polityki bezpieczeństwa informacji, polityki zarządzania ryzykiem oraz polityk poszczególnych systemów:

- zapewnia skuteczne zarządzanie reakcją na incydent, w tym właściwe zgłaszanie incydentów;

- podkreśla rolę kierownictwa organizacji we właściwym przygotowaniu reagowania na incydenty;
- zapewnia spójność polityk i procedur;
- umożliwia spójne zaplanowanie systematycznego i racjonalnego trybu reagowania na incydenty, co ogranicza ich niekorzystne skutki.

Wszystkie wymienione polityki powinny być aktualne i wyraźnie odnosić się do polityki zarządzania reakcją na incydent. Dodatkowo wymagają one określenia mechanizmów przeglądania w celu zagwarantowania, że wszelkie informacje pochodzące z wykrywania, zgłaszania, monitorowania lub rozwiązywania incydentów, są wykorzystywane do aktualizowania zasad zarządzania i polityk bezpieczeństwa poszczególnych systemów.

Utworzenie Zespołu Reagowania na Incydenty (naruszania) **Bezpieczeństwa Informacji (ZRIBI).** Powołanie ZRIBI oznacza wskazanie personelu uprawnionego do oceniania, reagowania i wyciągania wniosków z incydentów, a także do koordynacji postępowania będącego reakcją na incydent oraz zapewniania komunikacji między zainteresowanymi stronami. Dobrze zorganizowana działalność ZRIBI może w dużym stopniu przyczynić się do zmniejszenia strat materialnych i finansowych, jak również utrzymywania właściwego wizerunku i reputacji organizacji.

ZRIBI to grupa odpowiednio wyszkolonych i zaufanych osób (członków organizacji), która jest w stanie zapewnić właściwą reakcję na incydent naruszenia bezpieczeństwa informacji, wspomagana czasem przez zewnętrznych ekspertów, np. reprezentujących uznane zespoły reagowania, CERT itp. Przy powoływaniu tego zespołu należy pamiętać że:

- właściwa wielkość, struktura i skład ZRIBI powinny odpowiadać rozmiarowi i strukturze organizacji;
- jakkolwiek ZRIBI może stanowić wydzielony zespół lub jednostkę organizacyjną, to jego członkowie mogą mieć także i inne obowiązki;
- w wielu przypadkach ZRIBI jest zespołem zadaniowym, zbierającym się na wezwanie, kierowanym przez osobę z najwyższego kierownictwa, która w razie potrzeby będzie wspierana przez specjalistów od obszarów wiedzy powiązanych z typem incydentu;
- w zależności od wielkości organizacji jedna osoba może spełniać więcej niż jedną rolę w ZRIBI.

Członkami ZRIBI mogą, a nawet powinny być osoby pracujące w różnych jednostkach organizacyjnych. Muszą one być łatwo osiągalne, dlatego też ich dane kontaktowe (oraz osób ich zastępujących) powinny być łatwo dostępne w organizacji. np. zawarte w dokumentacji reagowania na incydent, procedurach i formularzach.

Osoba kierująca pracami ZRIBI (zwykle jest to kierownik ZRIBI) powinna:

- mieć upoważnienie (pełnomocnictwo) do podejmowania natychmiastowych decyzji, dotyczących postępowania z incydentami;
- mieć specjalną, oddzielną od codziennej (tzw. biznesowej), drogę kontaktu z najwyższym kierownictwem;

- upewnić się, że wszyscy członkowie ZRIBI są wystarczająco kompetentni, a ich wiedza i umiejętności są stale aktualizowane i rozwijane;
- uczynić odpowiedzialną za wyjaśnianie każdego incydentu najbardziej właściwą (ze względu na wiedzę, umiejętności i doświadczenie) osobę w ZRIBI.

Powiązania zarządzania incydentami z innymi obszarami zarządzania. Kierownik i członkowie ZRIBI muszą mieć odpowiednie pełnomocnictwo, aby móc reagować na incydenty. Jednak działania, które mogą przynieść niepożądane efekty dla całej organizacji (finansowe lub związane z wizerunkiem), powinny być uzgadniane z najwyższym kierownictwem. Z tego powodu istotne jest wskazanie w dokumentacji reagowania na incydent przełożonego, którego kierownik ZRIBI informuje o poważnych incydentach.

Ważną sprawą jest również współpraca z mediami. Procedury określające i precyzujące odpowiedzialność za współpracę z mediami powinny być zaakceptowane przez najwyższe kierownictwo i udokumentowane. Powinny one precyzować:

- kto w organizacji odpowiada na pytania mediów,
- w jaki sposób osoba lub jednostka organizacyjna odpowiedzialna w organizacji za współpracę z mediami współpracuje ze ZRIBI.

Powiązanie z organizacjami zewnętrznymi. Efektywne i skuteczne wyjaśnianie oraz naprawianie sytuacji powstałych w wyniku incydentu wymaga nawiązywania odpowiednich kontaktów i współpracy między ZRIBI a:

- współpracownikami z organizacji zewnętrznych i zleceniobiorcami,
- zespołami ZRIBI innych organizacji lub organizacjami zajmującymi się tematyką incydentów (np. CERT, FIRST),
- organizacjami związanymi z przestrzeganiem prawa (np. policja),
- służbami ratowniczymi (np. straż pożarna, pogotowie ratunkowe),
- organami administracji państwowej i samorządowej,
- mediami (prasa, radio, telewizja),
- partnerami biznesowymi,
- klientami,
- społeczeństwem.

Przygotowanie wsparcia technicznego i organizacyjnego. Duży wpływ na szybkie i efektywne reagowanie na incydenty ma stosowanie środków technicznych i organizacyjnych, do których można zaliczyć:

- dostęp do aktualnego rejestru aktywów organizacji oraz do informacji na temat ich wpływu na funkcje biznesowe;
- dostęp do dokumentacji opisującej strategię oraz planów zapewniania ciągłości działania;
- udokumentowane i opublikowane procesy komunikowania się;
- wykorzystanie bazy zdarzeń/incydentów oraz środków technicznych w celu szybkiego wypełniania i aktualizacji bazy, analizowania zawartych tam informacji i podjęcia postępowania reakcji na incydent;

- zapewnienie ciągłości działania bazy zdarzeń/incydentów.

Środki techniczne wykorzystywane w celu szybkiego wypełniania bazy zdarzeń/incydentów, analizowania zawartych w niej informacji oraz ułatwienia reagowania na incydenty powinny zapewniać:

- szybkie pozyskiwanie informacji niezbędnych do zgłaszania zdarzeń i incydentów;
- powiadamianie wybranych wcześniej pracowników lub organizacji zewnętrznej za pomocą określonych środków (np. poczta elektroniczna, faks, telefon) wymagających zarządzania rzetelną bazą kontaktów oraz ułatwiających komunikację i transmisję informacji do poszczególnych osób w bezpieczny sposób;
- podejmowanie środków ostrożności proporcjonalnych do oszacowanego ryzyka, tak aby zagwarantować, że komunikacja elektroniczna nie będzie mogła być podsłuchana, nawet podczas ataku na system;
- zapewnienie gromadzenia informacji o systemach oraz przetwarzanych przez nie danych;
- udzielanie odpowiedzi na pytania o odpowiedniość zastosowanych mechanizmów kryptograficznej kontroli integralności oraz o to, czy i jakie części systemu oraz jakie dane zostały zmienione;
- zachowywanie, archiwizację i zabezpieczanie zebranych informacji (np. przez dodanie podpisów cyfrowych do dzienników zdarzeń (tzw. logów) oraz śladów i dowodów przed ich składowaniem na nośnikach jednokrotnego zapisu – CD/DVD– ROM);
- możliwość sporządzenia wydruku newralgicznych danych, włączając te, które pokazują rozwój incydentu oraz kroki procesu reakcji na incydent;
- odtworzenie i przywrócenie (w powiązaniu z planem zapewniania ciągłości działania) systemu do normalnego stanu pracy przy wykorzystaniu:
  - procedur tworzenia kopii zapasowych,
  - pewnych kopii zapasowych,
  - testowania kopii zapasowych,
  - kontroli złośliwego kodu,
  - stosowania oryginalnych nośników z systemami i aplikacjami,
  - samoinicjujących nośników,
  - pewnych i zaktualizowanych poprawek (tzw. łat) systemów i aplikacji.

Wszystkie środki techniczne powinny być starannie dobrane, prawidłowo wdrożone i regularnie testowane (włącznie z testami kopii zapasowych).

Należy zauważyć, że opisane środki techniczne nie obejmują tych, które są wykorzystywane bezpośrednio do wykrywania incydentów oraz automatycznego powiadamiania.

Opracowanie programu uświadamiania i programu szkoleń. Zarządzanie reakcją na incydent jest procesem, który wymaga nie tylko środków technicznych, ale przede wszystkim ludzi. Powinno być ono wspierane przez osoby odpowiednio

przeszkolone w zakresie ochrony informacji. Świadomość zadań oraz uczestnictwo w szkoleniach wszystkich pracowników organizacji są bardzo ważne dla odniesienia sukcesu w zarządzaniu incydentami. Z tego powodu zarządzanie reagowaniem na incydenty obejmuje promocję wiedzy o polityce bezpieczeństwa jako części korporacyjnego programu uświadamiającego i szkoleniowego. Program uświadamiający i związane z nim materiały muszą być dostępne dla wszystkich pracowników, włączając w to osoby nowo zatrudnione, współpracowników i zleceniobiorców. Powinien istnieć specjalny program szkoleniowy dla członków ZRIBI, grup wsparcia technicznego oraz dla administratorów systemów i osób związanych z ochroną informacji. Należy pamiętać, że każda z grup zaangażowanych bezpośrednio w zarządzanie reagowaniem na incydenty może wymagać szkoleń na różnym poziomie, w zależności od typu, częstotliwości oraz znaczenia ich powiązania z zarządzaniem reakcją na incydent. Szkolenia powinny obejmować:

- podstawowe zasady zarządzania reakcją na incydent, włącznie z jego zakresem oraz przepływem informacji na temat zdarzeń i incydentów,
- sposób opisywania zdarzeń i incydentów,
- zabezpieczenia poufności źródeł informacji,
- schemat poziomu świadczonych usług,
- przypadki, gdy osoby lub komórki organizacyjne będące źródłami informacji o zdarzeniach i incydentach powinny być powiadamiane o rezultatach,
- wyjaśnienie ograniczeń nakładanych przez umowy o zachowaniu poufności,
- kompetencje poszczególnych osób i jednostek organizacyjnych w zakresie zarządzania reakcją na incydenty oraz zasady raportowania o nich,
- informacje o tym, kto i w jaki sposób otrzymuje raporty na temat incydentów.

W niektórych przypadkach może być wymagane, aby w wyraźny sposób zaznaczyć informacje na temat zarządzania incydentami w innych programach szkoleniowych (np. dla kadry zarządzającej lub dotyczących ogólnej tematyki bezpieczeństwa organizacji). Takie podejście może wydatnie przyczynić się do podniesienia efektywności i skuteczności programu szkoleniowego dla poszczególnych grup pracowników.

Przed operacyjnym wykorzystaniem dokumentacji zarządzania reakcją na incydent wszystkie zaangażowane w to osoby muszą poznać procedury wykrywania oraz opisywania zdarzeń i incydentów, a wybrane osoby powinny posiąść dogłębną wiedzę na temat wszystkich związanych z tym procesów. Następstwem powinny być regularne szkolenia, które dodatkowo powinny być wsparte przez szkolenia specjalistyczne oraz ćwiczenia symulujące sytuacje potrzeby wsparcia dla członków ZRIBI, administratorów i pracowników związanych z bezpieczeństwem informacji.

4.3.2. „Stosowanie" − wdrożenie i eksploatacja

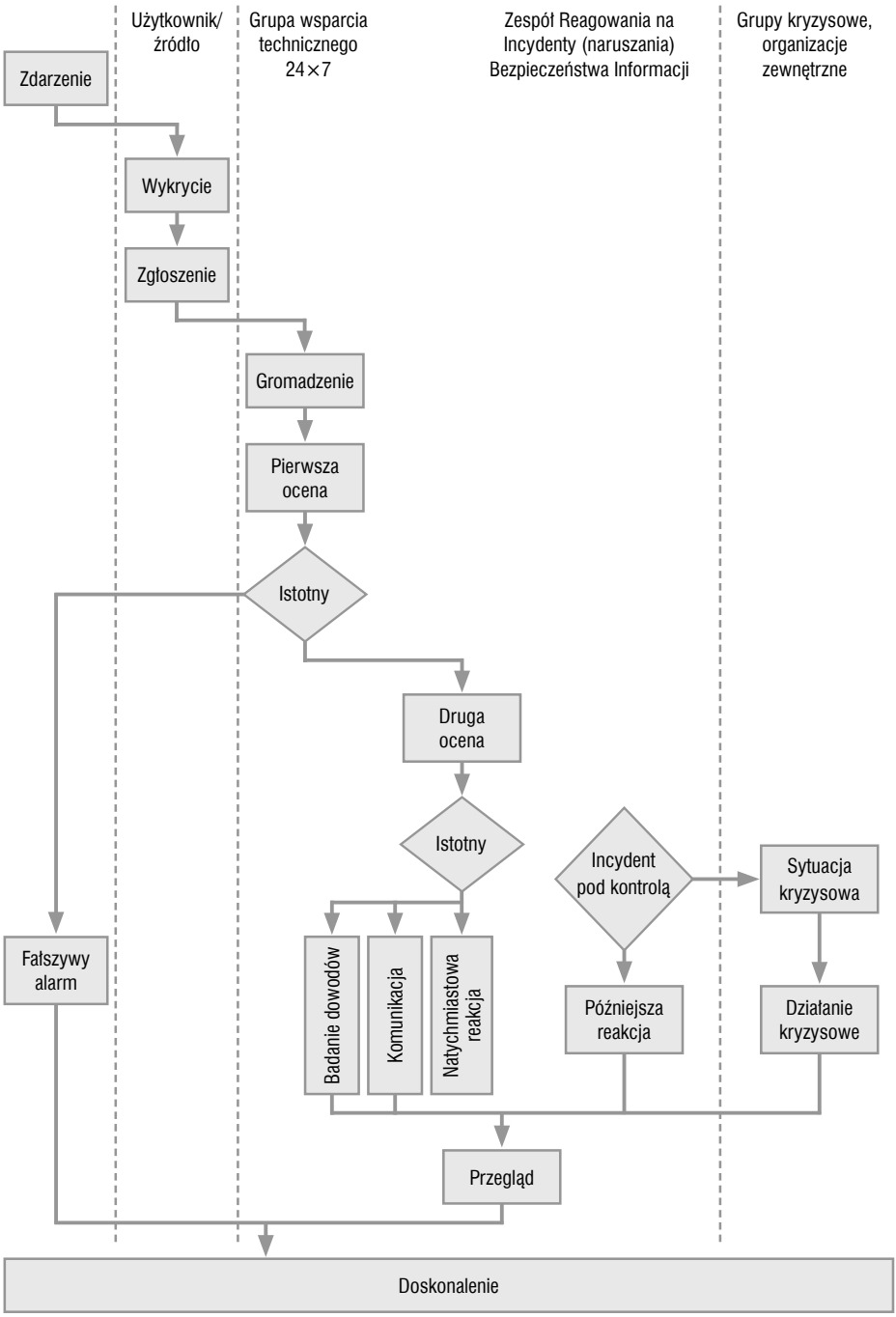
Zgodnie z rysunkiem 1.4 i tabelą 4.1 „stosowanie" to faza, która obejmuje wdrożenie systemu zarządzania incydentami i jego eksploatację. W niniejszym podroz-

dziale zawarto przegląd kluczowych procesów realizowanych w ramach systemu zapewniania bezpieczeństwa informacji, omówiono procesy wykrywania, dokumentowania i zgłaszania zdarzeń naruszania bezpieczeństwa informacji, oceny zdarzenia/incydentu i podejmowania decyzji w przypadku wystąpienia incydentu naruszenia bezpieczeństwa informacji, jak również reagowania na zdarzenia naruszające ochronę informacji, w tym analizę kryminalistyczną.

Do kluczowych działań procesu zapewniania bezpieczeństwa informacji zalicza się:

- wykrywanie i zgłaszanie faktów wystąpienia zdarzeń naruszenia bezpieczeństwa informacji;
- gromadzenie danych o tych zdarzeniach;
- ocenę zdarzenia naruszenia bezpieczeństwa przez ZRIBI, w celu potwierdzenia, że zdarzenie naruszenia bezpieczeństwa informacji jest incydentem; a jeśli jest, to następstwem tego powinno być natychmiastowe rozpoczęcie analizy śladów i dowodów oraz podjęcie działań informowania o zdarzeniu;
- reagowanie na incydenty naruszenia bezpieczeństwa informacji, tj. dokonanie przez ZRIBI przeglądu danych o incydencie w celu określenia, czy przebieg incydentu jest kontrolowany, a jeśli tak, to uruchomienie odpowiednich działań oraz zapewnienie, że wszystkie informacje są przygotowane do przeprowadzenia przeglądu stanu po incydencie; jeśli zaś uznaje się, że incydent nie jest kontrolowany, to uruchomienie działań związanych z zaistniałym kryzysem oraz zaangażowanie do nich odpowiednich pracowników (np. osób odpowiedzialnych za plan ciągłości działania);
- informowanie o incydencie naruszenia bezpieczeństwa informacji, przekazanie wyższemu szczeblowi decyzyjnemu informacji o zdarzeniu naruszenia bezpieczeństwa informacji do dalszej oceny lub podjęcia decyzji, zagwarantowanie, że wszystkie zainteresowane strony, a w szczególności członkowie ZRIBI, właściwie zarejestrowali swoje działania związane ze stwierdzeniem naruszenia bezpieczeństwa informacji w celu ich późniejszej analizy; zapewnienie, że ślady i dowody (szczególnie w formie elektronicznej) są bezpiecznie gromadzone i przechowywane, a zachowanie bezpieczeństwa jest ciągle monitorowane, co ma szczególne znaczenie w przypadku prowadzenia dochodzenia lub wewnętrznego postępowania wyjaśniającego;
- zapewnienie, że kontrola zmian jest prowadzona i obejmuje śledzenie incydentów, aktualizację opisów incydentów, a baza zdarzeń/incydentów jest aktualna;
- komunikację wewnątrz i na zewnątrz organizacji.

Wszystkie zgromadzone informacje, które odnoszą się do zdarzeń i incydentów, powinny być przechowywane w bazie danych zarządzanej przez ZRIBI. Informacje zgłaszane w trakcie wszystkich faz procesu powinny być możliwie jak najbardziej kompletne i aktualne, aby umożliwić właściwą ocenę sytuacji oraz podejmowanie decyzji i działań (rys. 4.1).



Rysunek 4.1. Przepływ informacji w procesie zarządzania incydentami

Źródło: opracowanie własne na podstawie: [ISO/IEC TR 18044:2004].

Cele kolejnych faz procesu, po wykryciu, opisaniu i zgłoszeniu zdarzenia są następujące:

- wyznaczenie osób do oceniania sytuacji, podejmowania decyzji i zarządzania incydentami;
- dostarczenie każdej zaangażowanej w ten proces osobie opisu zadań dotyczących przeglądania i dokonywania poprawek w przekazanym raporcie, szacowania strat i powiadamiania właściwego personelu;
- wykorzystanie wytycznych opisujących sposób przygotowywania szczegółowej dokumentacji dotyczącej zdarzeń, a jeśli zdarzenie zostanie zakwalifikowane jako incydent, to także dokumentacji dotyczącej podjęcia kolejnych działań i aktualizacji bazy zdarzeń/incydentów.

Wymienione wskazówki mogą dotyczyć:

- wykrywania, opisywania i zgłaszania incydentów;
- oceniania i podejmowania decyzji co do tego, czy zdarzenie może być sklasyfikowane jako incydent;
- reagowania na incydenty, czyli:
  - natychmiastowych reakcji;
  - dokonywania przeglądu w celu określenia, czy przebieg incydentu jest kontrolowany;
  - późniejszych reakcji polegających na:
    - ◇ działaniach kryzysowych,
    - ◇ analizie śladów i dowodów,
    - ◇ powiadamianiu zainteresowanych,
    - ◇ wytycznych co do dalszej eksploatacji,
    - ◇ rejestrowania działań.

Wykrywanie i zgłaszanie występowania zdarzeń naruszania bezpieczeństwa informacji. Zdarzenia mogą być wykrywane przez osoby, które zauważą coś niepokojącego, lub przez urządzenia albo środki techniczne (np. detektory wykrywania pożaru/dymu, systemy antywłamaniowe, zapory ogniowe, systemy IDS, narzędzia antywirusowe), które przesyłają sygnały alarmowe.

Niezależnie od źródła wykrycia zdarzenia naruszenia bezpieczeństwa informacji każda osoba powiadomiona o tym fakcie lub taka, która sama zauważyła coś niezwykłego, jest odpowiedzialna za zainicjowanie dalszego postępowania i za poinformowanie innych. Istotne jest, aby cały personel był świadomy możliwości zaistnienia naruszenia bezpieczeństwa informacji oraz miał dostęp do wytycznych opisujących zgłaszanie różnych typów zdarzeń.

Osoba zgłaszająca zdarzenie powinna wypełnić odpowiedni formularz, podając jak najwięcej dostępnych informacji. Istotne są nie tylko dokładność i kompletność informacji, niekiedy przede wszystkim czas.

Kiedy zawodzą domyślne drogi zgłaszania incydentów (np. poczta elektroniczna, strony WWW), a szczególnie w sytuacji kiedy system jest zaatakowany,

a formularze zgłoszenia mogą być przeglądane i czytane przez osoby nieuprawnione, należy wykorzystać zapasowe środki powiadamiania.

W wielu przypadkach, zanim zdarzenie zostanie zgłoszone w celu podjęcia działań przez grupę wsparcia technicznego, może ono być rozwiązane przez użytkowników, jeśli są odpowiednio przygotowani do takiej sytuacji.

Należy zagwarantować, aby zdarzenia związane z naruszaniem bezpieczeństwa informacji oraz wady systemów informacyjnych były zgłaszane w sposób umożliwiający szybkie podjęcie działań korygujących. Powinny zostać wdrożone formalne procedury zgłaszania zdarzeń naruszenia bezpieczeństwa. Wszyscy pracownicy, a także wykonawcy i użytkownicy systemów informacyjnych reprezentujący stronę trzecią powinni być uświadomieni w zakresie procedur zgłaszania różnych typów zdarzeń oraz słabości, które mogą mieć wpływ na bezpieczeństwo aktywów organizacji. Zaleca się ponadto, aby byli zobowiązani do niezwłocznego zgłaszania w wyznaczonym, zawsze dostępnym punkcie kontaktowym wszystkich zdarzeń związanych z bezpieczeństwem informacji oraz podatnościami zasobów na naruszenia tego bezpieczeństwa.

Procedury zgłaszania powinny określać:

- proces zwrotnego informowania zgłaszających zdarzenia naruszenia bezpieczeństwa o wynikach postępowania ze zdarzeniem, a co najmniej zgłoszeniem;
- formularze zgłaszania zdarzeń naruszania bezpieczeństwa informacji, pomagające zgłaszającym utrwalić wszystkie niezbędne fakty;
- poprawne zachowanie w przypadku takich zdarzeń obejmujące:
  - obowiązek natychmiastowego zanotowania wszystkich ważnych szczegółów (np. typu niezgodności lub naruszenia, błędu działania, wiadomości z ekranu, dziwnego zachowania);
  - zakaz podejmowania jakichkolwiek własnych działań i natychmiastowe zgłoszenie incydentu do punktu kontaktowego;
- elementy procesu dyscyplinarnego postępowania z pracownikami, wykonawcami i użytkownikami reprezentującymi stronę trzecią, którzy naruszają bezpieczeństwo.

W środowiskach, gdzie występuje poważne ryzyko wrogiej ingerencji, można wprowadzić specjalny rodzaj sygnału alarmowego „działanie pod przymusem" (jest to metoda tajnego informowania, że podejmowane działania są wykonywane „pod przymusem" np. terrorysty). Zaleca się, aby procedury obsługi zgłoszenia alarmu pod przymusem odzwierciedlały wskazywaną sytuację wysokiego ryzyka.

Przy zachowaniu należytej staranności w odniesieniu do poufności, analizy incydentów związanych z naruszeniem bezpieczeństwa informacji mogą być wykorzystane do podnoszenia świadomości użytkowników jako przykład tego, co może się zdarzyć, jak reagować na takie incydenty oraz jak ich unikać w przyszłości. Aby móc poprawnie postępować ze zdarzeniami związanymi z bezpieczeństwem informacji oraz incydentami naruszania tego bezpieczeństwa, niezbędnym może okazać się gromadzenie materiału dowodowego tak szybko, jak to możliwe.

Awarie lub inne nienormalne zachowania systemu informacyjnego mogą wskazywać na atak lub rzeczywiste naruszenie bezpieczeństwa i należy je zawsze zgłaszać jako zdarzenia związane z bezpieczeństwem informacji.

Wszyscy pracownicy, wykonawcy i użytkownicy reprezentujący stronę trzecią, korzystający z systemów informacyjnych i usług powinni być zobowiązani do zgłaszania zaobserwowanych lub podejrzewanych niedoskonałości rozwiązań zapewniania bezpieczeństwa do kierownictwa albo bezpośrednio do swojego dostawcy usług, tak szybko, jak to możliwe, aby uniknąć incydentów związanych z naruszeniem bezpieczeństwa informacji. Mechanizm zgłaszania powinien być prosty, dostępny i osiągalny.

Nie należy, pod żadnym pozorem, próbować sprawdzać na własną rękę istnienia podejrzewanej słabości. Może to być zinterpretowane jako potencjalne niewłaściwe korzystanie z systemu i może spowodować szkody w systemie informacyjnym lub usłudze oraz pociągnąć za sobą konsekwencje prawne wobec osoby wykonującej takie próby.

Gromadzenie danych o naruszeniach bezpieczeństwa informacji. Jeśli działania podejmowane po wystąpieniu incydentu związanego z bezpieczeństwem informacji obejmują kroki prawne (natury cywilnoprawnej lub karnej), to zaleca się zgromadzenie, zachowanie i przedstawienie materiału dowodowego zgodnie z zasadami obowiązującymi w systemie prawnym. Zaleca się, przy zbieraniu i przedstawianiu materiału dowodowego, opracowanie i stosowanie procedur wewnętrznych na potrzeby postępowania dyscyplinarnego prowadzonego w organizacji.

W ogólnym przypadku zasady związane z materiałem dowodowym dotyczą:

- dopuszczalności materiału dowodowego, tj. czy materiał dowodowy może być wykorzystany w sądzie;
- wagi materiału dowodowego, tj. jego jakości i kompletności.

Dopuszczalność materiału dowodowego jest osiągana, gdy systemy informacyjne organizacji są zgodne z opublikowanymi normami lub ogólnie przyjętymi zasadami tworzenia takiego materiału dowodowego.

Z kolei waga materiału dowodowego jest odpowiednia, gdy zapewniona jest jakość i kompletność zabezpieczeń używanych do ochrony materiału dowodowego (tzw. proces zabezpieczania materiału dowodowego). Mówi się w takim przypadku o utrzymaniu mocnego śladu dowodowego. Na ogół można to uzyskać pod następującymi warunkami:

- dla dokumentów papierowych: oryginał jest bezpiecznie przechowywany wraz z informacją, kto znalazł dokument, gdzie, kiedy i kto był świadkiem tego zdarzenia, a każde śledztwo może wykazać, że oryginał nie został naruszony;
- dla dokumentów na nośnikach komputerowych zaleca się:
  - utworzenie obrazu lub kopii (zależnie od stosownych wymagań) wszelkich nośników wymiennych,
  - zapisanie informacji znajdujących się na dyskach twardych lub w pamięci komputera, aby zapewnić ich dostępność,

ZARZĄDZANIE

Franciszek Wołowski – absolwent Politechniki Śląskiej (1968) oraz Studium Podyplomowego Ekonometrii i Programowania Matematycznego Wyższej Szkoły Ekonomicznej w Katowicach.

Zajmuje się zarządzaniem bezpieczeństwem systemów informacyjnych, ryzykiem oraz zastosowaniami biometrii i kryptografii klucza publicznego (podpisu elektronicznego). Wykładowca na studiach podyplomowych w Politechnice Warszawskiej, Politechnice Lubelskiej oraz w Instytucie Orgmasz, jak również na szkoleniach organizowanych przez instytucje administracji publicznej. Prelegent na wielu konferencjach zawodowych poświęconych ryzyku i bezpieczeństwu oraz autor szeregu publikacji w specjalistycznych wydawnictwach, w tym współautor książki *Podpis elektroniczny w administracji i zarządzaniu* (2005).

Janusz Zawiła-Niedźwiecki – od kilkunastu lat pracownik naukowy Wydziału Zarządzania Politechniki Warszawskiej, wykładowca Collegium Civitas, członek Polskiej Komisji Akredytacyjnej. Redaktor naukowy książek *Informatyka gospodarcza* (4 tomy, 2010) i *Zarządzanie ryzykiem operacyjnym* (2008). Autor książki *Ciągłość działania organizacji* (2008) oraz kilkudziesięciu artykułów i referatów konferencyjnych naukowych i zawodowych z zakresu zarządzania ryzykiem, bezpieczeństwem i ciągłością działania.

Równocześnie menedżer praktyk, w przeszłości m.in. w NBP, Pol-Mot, Giełdzie Papierów Wartościowych, Fund Services, Grupie PZU, Komisji Nadzoru Finansowego, Urzędzie Komunikacji Elektronicznej. Obecnie doradca biznesowy w firmie Casus Unicus.

W roku 1998 jako dyrektor IT Giełdy laureat nagrody „Lider Informatyki" przyznawanej przez Computerworld. Członek założyciel polskiego oddziału stowarzyszenia ISACA, przewodniczący Rady Fundacji im. Prof. Kazimierza Bartla.