7. ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO

7.1. Zabezpieczenia systemu informatycznego i ich funkcje

Zabezpieczenia systemu informatycznego to *wszystkie środki (praktyki, procedury, mechanizmy), które chronią przed zagrożeniem, redukują podatność zasobów na zagrożenia, ograniczają następstwa wystąpienia zagrożeń, wykrywają niepożądane incydenty i ułatwiają odtwarzanie stanu sprzed wystąpienia zagrożenia* [PN-I-13335-1].

Funkcje zabezpieczeń:

- zapobieganie,
- ograniczanie,
- wykrywanie,
- odstraszanie,
- poprawianie,
- odtwarzanie,
- monitorowanie,
- uświadamianie.

7.2. Podział zabezpieczeń

Zabezpieczenia można podzielić na:

- ***zabezpieczenia fizyczne*** (infrastrukturalne) - to przeciwdziałanie zagrożeniom wynikającym z bezpośredniego kontaktu nieuprawnionych osób, sił przyrody i zdarzeń losowych z systemem informatycznym (np.

systemy przeciwpożarowe, systemy alarmowe i antywłamaniowe, klimatyzacja pomieszczeń),

- ***zabezpieczenia techniczne*** - to zastosowanie dodatkowych urządzeń i oprogramowania zabezpieczającego (np. programów firewall, programów antywirusowych, programów szyfrujących, urządzeń archiwizujących dane) oraz odpowiednie użytkowanie urządzeń i programów działających w SI,
- ***zabezpieczenia organizacyjne*** - to odpowiednia organizacja formuły zarządzania SI (np. odpowiedni przydział obowiązków i odpowi edzialności, kontrole przeciwpożarowe, sprawdzanie logów systemowych, bezpieczne niszczenie zużytych nośników danych),
- ***zabezpieczenia personalne*** - to odpowiednie zarządzanie zasobami ludzkimi (np. właściwy dobór pracowników, ich szkolenia i uświadamianie w zakresie bezpieczeństwa),
- ***procedury ochronne i awaryjne*** (podgrupa zabezpieczeń organizacyjnych) - to odpowiednie przygotowanie procedur, które ustalają, w jaki sposób użytkownik powinien postępować w określonych sytuacjach, aby nie dopuścić do wystąpienia zagrożeń lub ograniczyć ich ewentualne skutki (np. profilaktyka antywirusowa, procedury przeciwpożarowe).

7.3. Zabezpieczenia fizyczne

Zabezpieczenia fizyczne polegają na:

- ***organizacji stref bezpieczeństwa*** - celem jest zapobieganie nieuprawnionemu dostępowi do pomieszczeń i ingerencji w zasoby SI,
- ***zabezpieczaniu urządzeń i nośników danych*** - w celu przeciwdziałania utracie, uszkodzeniu lub innemu naruszeniu bezpieczeństwa zasobów SI.

7.3.1. Organizacja stref bezpieczeństwa

Organizacja stref bezpieczeństwa polega na:

1. Utworzeniu fizycznego obwodu zabezpieczającego wyposażonego w punkty kontroli wejścia (np. recepcja, portiernia, drzwi otwierane za pomocą karty magnetycznej).

2. Fizycznemu zabezpieczeniu wejścia poprzez:

- umożliwienie wejścia wyłącznie osobom upoważnionym (np. sprawdzanie wchodzących gości i rejestrowanie czasu ich wejścia i wyjścia),
- zabronienie wnoszenia urządzeń rejestrujących (np. aparatów fotograficznych, magnetofonów, kamer),
- wymaganie od personelu noszenia identyfikatorów.

3. Zabezpieczeniu biur, pomieszczeń i urządzeń

Przede wszystkim należy uwzględnić szereg czynników, takich jak:

- nieuprawniony dostęp, podsłuch, podgląd i emisję ujawniającą,
- konsekwencje uszkodzeń wskutek zdarzeń losowych i sił wyższych,
- konsekwencje uszkodzeń w wyniku ludzkiej działalności,
- odpowiednie regulacje i standardy z dziedziny BHP,
- zagrożenia bezpieczeństwa ze strony sąsiednich pomieszczeń (np. zalanie).

W ramach zabezpieczania zaleca się:

- zamykanie drzwi i okien w momencie opuszczania pomieszczeń,
- stosowanie ochrony okien (np. krat, folii antywłamaniowych),
- stosowanie regularnie testowanych systemów alarmowych, chroniących wszystkie zewnętrzne drzwi i okna oraz obszary bezobsługowe (np. pomieszczenia dla urządzeń komputerowych),

- składowanie materiałów niebezpiecznych i łatwopalnych w bezpiecznej odległości od pomieszczeń,
- zapewnienie prawidłowej wentylacji i klimatyzacji pomieszczeń,
- fizyczne oddzielenie urządzeń zarządzanych przez przedsiębiorstwo od urządzeń zarządzanych przez osoby trzecie.

4. Odpowiedniej organizacji pracy w strefach bezpieczeństwa, tak aby były one zabezpieczone przed osobami nie będącymi pracownikami (np. osobami wykonującymi prace zlecone, klientami, pracownikami firm trzecich).

7.3.2. Zabezpieczanie urządzeń

Zabezpieczanie urządzeń polega na:

1. Odpowiednim rozmieszczeniu i ochronie urządzeń

Zaleca się m.in.:

- rozlokowanie urządzeń tak, aby zminimalizować niepożądany dostęp do nich,
- zabezpieczenie urządzeń przed wpływem szkodliwych czynników, takich jak np. woda, kurz, ogień, drgania, środki chemiczne,
- wprowadzenie ograniczeń dotyczących jedzenia, picia i palenia tytoniu w pobliżu urządzeń komputerowych,
- monitorowanie warunków środowiskowych w celu wykrycia czynników, które mogą negatywnie wpływać na działanie urządzeń (np. pomiar temperatury, wilgotności),
- w środowiskach przemysłowych stosowanie odpowiednich urządzeń lub środków ochronnych (np. osłony na klawiatury),
- rozważenie wpływu katastrofy w pobliskich pomieszczeniach (np. awaria instalacji wodnej) lub sąsiednich budynkach (np. pożar) na bezpieczeństwo.

2. Zabezpieczeniu zasilania

Aby zasilać urządzenia zgodnie z ich wymaganiami, należy stosować m.in.:

- zasilacze awaryjne (UPS),
- filtry przeciwzakłóceniowe,
- automatyczne bezpieczniki zapobiegające przeciążeniu linii,
- system piorunochronów,
- generatory awaryjne.

3. Zapewnieniu bezpieczeństwa okablowania

W tym celu zalecane jest:

- poprowadzenie okablowania w sposób niedostępny (np. w ścianach, pod podłogą) lub jego ochronę za pomocą innych środków (np. rur, rynienek),
- oddzielenie kabli zasilających od telekomunikacyjnych (dla uniknięcia interferencji),
- zamykanie szafek i skrzynek przyłączeniowych,
- kontrolę okablowania i wyszukiwanie nieuprawnionych, podłączonych urządzeń,
- dublowanie okablowania.

4. Odpowiedniej konserwacji urządzeń

Zaleca się m.in.:

- konserwowanie urządzeń zgodnie z zaleceniami producenta,
- naprawianie i serwisowanie urządzeń tylko przez uprawniony personel,
- rejestrowanie wszystkich awarii, działań prewencyjnych oraz napraw,
- stosowanie odpowiednich zabezpieczeń przy wysyłaniu urządzeń do konserwacji poza siedzibą przedsiębiorstwa (np. usuwanie danych, ochronę podczas transportu).

5. Zabezpieczaniu urządzeń i dokumentów poza systemem

Uwaga: Używanie urządzeń dokumentów poza SI powinno być zatwierdzone przez kierownictwo, a użytkownik powinien zagwarantować im poziom bezpieczeństwa nie mniejszy niż podczas pracy w systemie.

Zaleca się m.in.:

- niepozostawianie urządzeń i dokumentów bez nadzoru w miejscach publicznych (np. w samochodzie),
- przewożenie ich jako bagażu podręcznego i, w miarę możliwości, maskowanie podczas podróży,
- przestrzeganie zaleceń producentów dotyczących ochrony urządzeń (np. przed polem elektromagnetycznym, temperaturą, wilgocią),
- odpowiednie zabezpieczanie dokumentów i urządzeń w domu (np. przed dziećmi),
- ubezpieczenie urządzeń wykorzystywanych poza przedsiębiorstwem.

6. Bezpiecznym zbywaniu urządzeń (przekazywaniu do ponownego użycia)

Uwaga: W SI urządzenia komputerowe lub ich elementy (np. nośniki danych) zmieniają często swoje przeznaczenie, lokalizację lub właściciela, może wówczas dojść do ujawnienia nieuprawnionym osobom informacji zawartych w ich pamięci. Dlatego należy pamiętać, aby takie informacje usunąć wcześniej na trwałe z urządzeń.

7.4. Zabezpieczenia techniczne

Do zabezpieczeń technicznych (sprzętowych i programowych) zalicza się przede wszystkim:

- systemy tworzenia kopii zapasowych i odtwarzania danych,
- programy antywirusowe i narzędziowe,
- zwielokrotnienie urządzeń i danych,
- programowe i sprzętowe systemy uwierzytelniania użytkowników (np. hasła, karty identyfikacyjne),
- narzędzia kryptograficzne (np. szyfrowanie przechowywanych danych, szyfrowanie transmisji w sieci, używanie podpisów cyfrowych),
- systemy monitorowania zachowania użytkowników (np. systemy wykrywania włamań) i filtrowania przesyłanych danych (np. systemy firewall).

7.4.1. Kopie zapasowe

Uwaga: kopie tworzone są nie tylko na wypadek utraty danych w wyniku awarii, ale także na wypadek wystąpienia błędu w oprogramowaniu, zarażenia systemu wirusem, uszkodzenia urządzenia, jego kradzieży czy błędnego działania samego użytkownika.

Zaleca się, m.in.:

- regularne sporządzanie kopii istotnych danych i oprogramowania,
- przechowywanie kopii z dala od przynależnego komputera (najlepiej w innym budynku) w celu ochrony przed różnego rodzaju zdarzeniami (np. pożarem),
- utrzymywanie kilku generacji kopii danych,
- zapewnienie kopiom właściwego bezpieczeństwa,

- regularne sprawdzanie poprawności odczytu nagranych kopii,
- regularne testowanie procedur odtwarzania danych.

Uwaga: Najprostszą metodą sporządzania kopii jest ręczne kopiowa nie plików na nośniki (np. dyski CD-R), lecz jest to rozwiązanie doraźne i możliwe do zaakceptowania tylko w przypadku pojedynczych komputerów. Większe systemy należy zaopatrzyć w urządzenia do **automatycznego zapisywania i odtwarzania danych z kopii** oraz opracować **procedury** postępowania i określić **odpowiedzialne za to osoby**.

W zależności od ilości i znaczenia danych w SI, należy ustalić:

- pliki podlegające kopiowaniu (np. tylko pliki z danymi, wszystkie pliki),
- rodzaj tworzonych kopii zapasowych (np. kopie normalne, przyrostowe, różnicowe),
- częstotliwość lub porę tworzenia kopii (np. na bieżąco, co godzinę, codziennie, co tydzień),
- okres przechowywania kopii (liczbę kopii wstecz),
- rodzaj nośnika do sporządzania kopii (np. taśma, dysk CD-RW, dysk twardy),
- osoby odpowiedzialne za nadzorowanie procesu tworzenia kopii, sprawdzania ich poprawności i testowania procedur odtwarzania danych.

Rodzaje kopii zapasowych:

- *kopia normalna* - kopiowanie wszystkich wybranych plików i oznaczeniu każdego z nich jako zarchiwizowanego. Zaleta: łatwe odzyskiwanie danych (wymagany tylko nośnik z najświeższymi danymi). Wada: długi czas tworzenia kopii.

- *kopia przyrostowa* - kopiowanie jedynie tych plików, które powstały lub zostały zmienione od czasu utworzenia ostatniej przyrostowej lub normalnej kopii, oraz na oznaczeniu ich jako zarchiwizowanych. Zaleta: skrócenie czasu tworzenia kopii. Wada: przed zrobieniem pierwszej kopii przyrostowej należy utworzyć normalną kopię. Do odtworzenia danych konieczne jest posiadanie, w chronologicznym porządku, ostatnio utworzonej kopii normalnej oraz wszystkich kolejnych kopii przyrostowych.
- *kopia różnicowa* - kopiowanie jedynie tych plików, które zostały utworzone lub zmienione od czasu utworzenia ostatniej kopii normalnej lub przyrostowej. Podczas wykonywania kopii różnicowej kopiowane pliki nie są oznaczane jako zarchiwizowane. Zaleta: skrócenie czasu tworzenia kopii. Wada: przed utworzeniem pierwszej kopii różnicowej zalecane jest wykonanie pełnej kopii normalnej. Do odtworzenia danych konieczne jest posiadanie ostatniej kopii normalnej oraz ostatniej kopii różnicowej.

7.4.2. Ochrona przed wirusami

Ochrona przed wirusami komputerowymi polega na:

- profilaktyce antywirusowej,
- usuwaniu wirusów i skutków ich wystąpienia.

Uwaga: *Profilaktyka antywirusowa* obejmuje wszystkie działania, które mają na celu niedopuszczenie do zarażenia systemu wirusem komputerowym, zgodnie z zasadą, że „lepiej zapobiegać zarażeniu niż leczyć".

7.4.2.1. Profilaktyka antywirusowa

W profilaktyce antywirusowej należy:

- korzystać z oprogramowania,
- regularnie aktualizować bazę wirusów,

- regularnie tworzyć kopie zapasowe posiadanego oprogramowania i danych oraz chronić je przed zarażeniem,
- unikać programów i dokumentów z niepewnego źródła - np. nieznanych stron internetowych, plików otrzymanych pocztą elektroniczną,
- zachować ostrożność przy otwieraniu załączników poczty elektronicznej, szczególnie w przypadku listów od nieznanych nadawców,
- posiadać zabezpieczoną przed zapisem i wolną od wirusów dyskietkę systemową (dysk CD) z aktualnym programem antywirusowym.

7.4.2.2. Usuwanie wirusów

Podczas usuwania wirusa należy:

- wyłączyć komputer, aby nie dopuścić do dalszych destrukcyjnych działań wirusa. Jeżeli istnieje podejrzenie, że jest to robak internetowy, należy odłączyć także kabel sieci komputerowej.
- zaopatrzyć się w aktualną wersję programu antywirusowego, uruchomić system operacyjny z dyskietki startowej (dysku CD) i przeprowadzić skanowanie systemu.
- po zidentyfikowaniu wirusa przez program antywirusowy należy uzyskać jak najwięcej informacji na jego temat (np. o skutkach zarażenia, sposobie przenoszenia, metodzie usunięcia).
- w zależności od rodzaju wirusa dalsze postępowanie jest zróżnicowane - może się okazać, że program antywirusowy usunie wirusa lub też konieczne będzie ponowne instalowanie systemu i odtwarzanie danych.

7.4.2.3. Moduły oprogramowania antywirusowego:

Do modułów oprogramowania antywirusowego zlicza się:

- skaner plików - umożliwia skanowanie systemu plików w wybranym przez użytkownika momencie,

- skaner rezydentny - „w tle” kontroluje wszystkie wykonywane operacje,
- terminarz - określa kiedy skaner plików ma się automatycznie uruchomić i sprawdzić system,
- moduł aktualizujący - automatycznie pobiera bieżące bazy wirusów z serwera producenta.

7.4.2.4. Metody wykrywania wirusów:

Podstawowe metody wykrywania wirusów to:

- monitorowanie pracy uruchomionych programów - moduł śledzi wszystkie uruchomione programy i stara się zablokować te, które próbują wykonać operacje zagrażające bezpieczeństwu systemu (np. zmiana sektora MBR) lub przypominają swoim działaniem znane już typy wirusów. Po zablokowaniu podejrzanej operacji, o potencjalnym zagrożeniu informowany jest użytkownik, który sam musi zdecydować o dalszym działaniu programu. Zaleta: możliwość wykrycia, na podstawie zachowania, nieznanego jeszcze wirusa. Wada: fałszywe alarmy.
- wyszukiwanie wzorców wirusów - poszukiwanie w systemie (np. w pamięci operacyjnej, plikach) ciągów bajtów będących wzorcami znanych wirusów. Zaleta: duża skutecznością w przypadku znanych wirusów. Wada: nieskuteczność w wykrywaniu nowych wirusów.
- generowanie i sprawdzanie sum kontrolnych plików - utworzenie bazy danych zwierającej tzw. *sumy kontrolne plików*. Następnie sumy są ponownie obliczane i porównywana z wartością z bazy. Różne sumy kontrolne tego samego pliku świadczą o jego modyfikacji. Zaleta: duża skuteczność oraz możliwość wykrywania nieznanych wirusów. Wada: nieskuteczność w przypadku kiedy suma kontrolna zostanie obliczona dla zainfekowanego pliku.

7.4.3. Zwielokrotnianie urządzeń i danych

- celem zwielokrotniania jest zapobieganie sytuacjom, w których uszkodzenie pojedynczego elementu powoduje niedostępność całego systemu,
- powielane są elementy krytyczne lub najczęściej ulegające awariom,
- zwielokrotnianie możliwe jest dzięki:
  - spadkowi cen urządzeń,
  - opracowaniu mechanizmów samoanalizy (np. technologia SMART),
  - opracowaniu mechanizmów pozwalających na odłączanie i zastępowanie uszkodzonych elementów podczas pracy systemu (np. macierze dyskowe, dyski SATA).

7.4.4. Dobór i ochrona haseł

Uwierzytelnianie można podzielić na trzy metody:

- na podstawie wiedzy,
- na podstawie fizycznego posiadania,
- na podstawie cech indywidualnych.

Zagadnienie: *Przestrzeń haseł*

Przestrzeń haseł S o długości k znaków stworzonych z alfabetu N znaków wynosi $S = N^k$ i oznacza liczbę wszystkich możliwych do utworzenia haseł o długości k ze zbioru N znaków. Nawet dla niewielkich k i N przestrzeń S przyjmuje relatywnie dużą wartość. Niestety, użytkownicy często nie wiedzą nawet, z ilu oraz z jakich znaków może się składać ich hasło. Efektem jest tworzenie krótkich haseł w oparciu o 26 liter alfabetu - wtedy liczba wszystkich możliwych haseł o długości do 8 znaków wynosi 2,17E+11. Liczba ta wydaje się ogromna, ale ponieważ w takiej sytuacji użytkownik często tworzy hasła będące wyrazami lub nazwami własnymi, to hasła te są podatne

na *ataki słownikowe*. Uwzględnienie cyfr i dużych liter (dodatkowe 36 znaków) zwiększa liczbę możliwych haseł oraz zmniejsza ryzyko ataku słownikowego. Ponadto w niektórych systemach można używać znaków: !@#$%^&*()_-+=[]|\;:,.~' i spacji. Te dodatkowe znaki zwiększają przestrzeń haseł oraz podnoszą stopień ich trudności i odporność na ataki słownikowe.

7.4.4.1. Prawidłowy wybór hasła

Zasady tworzenia haseł - dobre hasło **powinno**:

- być trudne do odgadnięcia i łatwe do zapamiętania,
- być odpowiednio długie (min. 6 znaków),
- zawierać wielkie i małe litery, cyfry oraz znaki dodatkowe (np. „!", „_"),
- dać się szybko wprowadzić z klawiatury (aby nikt nie mógł go podejrzeć),
- **nie zawierać** danych związanych z użytkownikiem lub jego bliskimi, nazw znanych postaci (np. aktorów, piosenkarzy, sportowców), nazw własnych, prostych ciągów znaków z klawiatury (np. *qwerty*, *123456*).

W celu utworzenia dobrego hasła można, np.:

- połączyć kilka krótkich wyrazów i oddzielić je jakimś znakiem (np. *tajne&haslo*),
- kilkakrotnie powtórzyć ten sam wyraz (np. *tajnetajne*),
- umieścić w haśle jakiś akronim znany tylko użytkownikowi (np. *nwjwh - nie wiem jakie wybrać hasło*),
- zastąpić litery znakami o „podobnym wyglądzie" (np. litera „O" na cyfrę „0", „S" na „$"; „a" na „@"; „i" na „1"; „G" na „6"),
- wprowadzić cyfry z wciśniętym klawiszem Shift (np. *!(%#* to liczba *1953*).

7.4.4.2. Dbanie użytkownika o bezpieczeństwo własnych haseł

Tabela 9. Sytuacje zagrażające bezpieczeństwu haseł

Rodzaj sytuacji	Charakterystyka
zapisywanie haseł	zapisane hasło powinno wyglądać jak nic nie znaczący tekst; razem z nim nie należy zapisywać nazwy użytkownika, komputera ani numeru IP, a kartki nie wolno przechowywać obok komputera.
używanie tylko jednego hasła	korzystając z kilku systemów (kont) często użytkownicy stosują w nich jedno „standardowe" hasło. Tymczasem bezwzględna zasada mówi, że nie wolno używać tego samego hasła, szczególnie jeśli systemy posiadają odmienny poziom bezpieczeństwa lub należą do różnych organizacji.
korzystanie z „niepewnych" komputerów	na komputerze, co do bezpieczeństwa którego użytkownik nie ma pewności, nie należy korzystać z usług wymagających podawania hasła, gdyż istnieje niebezpieczeństwo, że na komputerze uruchomiony jest rezydentny program zapisujący kody klawiszy.
nietypowe zachowania systemu	użytkownik powinien zachować ostrożność w sytuacji, kiedy podczas pracy z systemem pojawi się nietypowy komunikat proszący o powtórne podanie hasła. Może to być efekt działania programu przechwytującego podstępem hasło użytkownika.
udostępnianie hasła innym osobom	należy mieć świadomość tego, że osoba, której umożliwiono dostęp do zasobów, może nawet przypadkowo naruszyć ich bezpieczeństwo.
korzystanie z opcji „zapisywania haseł"	opcję tę należy stosować tylko wtedy, gdy zabezpieczony jest fizyczny dostęp do komputera, ponieważ w wielu przypadkach zapisywane hasło nie jest wystarczająco mocno utajnione. Istnieje prawdopodobieństwo, że intruz, mając dostęp do komputera, skopiuje plik z hasłami i je rozszyfruje, lub zainstaluje na swoim komputerze ten sam program, podmieni pliki i bez łamania hasła będzie mógł pracować z systemem. Może także na miejscu skorzystać z komputera i programów.
korzystanie z usług przesyłających niezaszyfrowane dane	stanowi to dla użytkownika zagrożenie ze względu na dużą łatwość przechwycenia jego hasła lub danych. Rozwiązaniem jest korzystanie z usług, które dokonują szyfrowania transmisji (np. protokół SSh - Secure Shell).
niezmienienie hasła po utworzeniu (odblokowaniu) konta	czasami użytkownicy przed założeniem konta muszą złożyć o nie pisemny wniosek, na którym podają m.in. swoje tymczasowe hasło. Niestety, często hasło to nie zostaje później zmienione. Należy pamiętać, że do wniosków mogą mieć dostęp niepowołane osoby. Potencjalne zagrożenie stanowi także sytuacja, w której użytkownik zapomni swojego hasła i poprosi administratora o jego zmianę. Zdarza się, że administrator nadaje zawsze jedno hasło, które mogą znać także inne osoby.
niekontrolowanie dostępu do konta	większość systemów rejestruje najważniejsze zdarzenia, m.in. zapisuje informacje o logowaniu na konta (czas, adres komputera). Użytkownik powinien okresowo sprawdzać te informacje, ponieważ w ten sposób może zauważyć logowanie, które nie należy do niego (miało miejsce o nietypowej porze lub z nietypowego miejsca).

Źródło: opracowanie własne

7.4.5. Narzędzia kryptograficzne

Kryptologia - nauka zajmująca się zagadnieniami szyfrów:

- kryptografia - ochrona (utajnianie) danych za pomocą szyfrów,
- kryptoanaliza - bada metody kryptograficzne, przede wszystkim stara się wykazać ich słabość i znaleźć sposób ich złamania.

Uwaga: W praktyce nie istnieje efektywny algorytm *bezwarunkowo bezpieczny*, czyli taki, który generuje tekst zaszyfrowany nie zawierający wystarczającej informacji do tego, by jednoznacznie określić odpowiadający mu tekst jawny, niezależnie od ilości dostępnego tekstu zaszyfrowanego. Wyjątkiem jest algorytm z kluczem jednorazowym (*one-time pad*).

Stosowane algorytmy to algorytmy *obliczeniowo bezpieczne*, czyli spełniające jeden lub oba warunki:

- koszt złamania szyfru przewyższa wartość informacji zaszyfrowanej,
- czas złamania szyfru przekracza użyteczny „czas życia" informacji.

7.4.5.1. Wybór narzędzi kryptograficznych

Za bezpieczne narzędzia kryptograficzne uznaje się te, które:

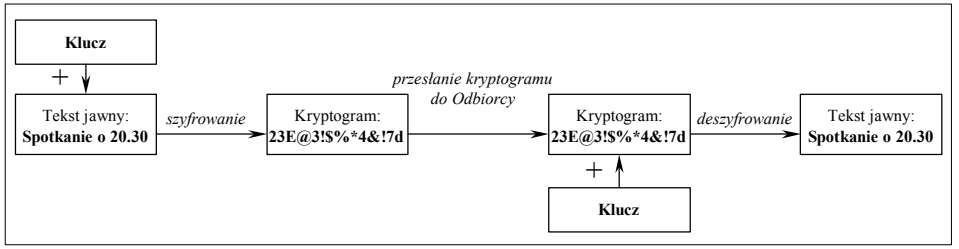
- są oferowane przez znane firmy o niezaprzeczalnej reputacji,
- posiadają certyfikaty odpowiednich instytucji kontrolnych,
- realizują powszechnie znane i przetestowane rozwiązania, tzn.
  - szczegółowy opis zastosowanej metody kryptograficznej został podany do publicznej wiadomości,
  - metoda wzbudziła powszechne zainteresowanie środowisk nauki i biznesu,

  - nad metodą były przeprowadzane intensywne badania mające na celu jej złamanie lub udowodnienie bezpieczeństwa.

7.4.5.2. Metody szyfrowania

7.4.5.2.1. Szyfrowanie symetryczne

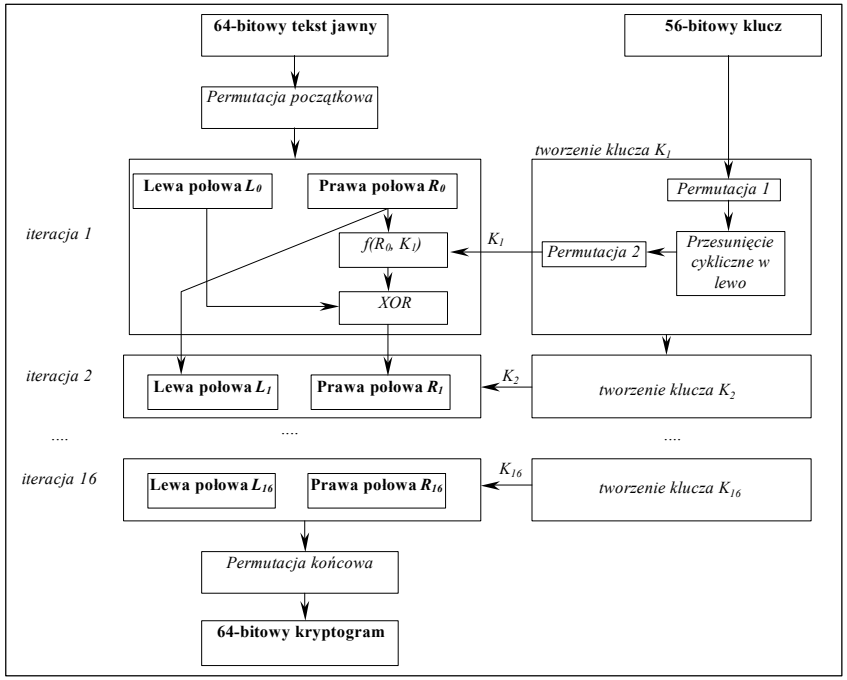
Schemat działania: Nadawca przekształca (za pomocą operacji podstawienia i permutacji) *tekst jawny* za pomocą odpowiedniego *klucza* do postaci zaszyfrowanej - tzw. *kryptogramu*. Odbiorca może odszyfrować kryptogram przekształcając go w tekst jawny za pomocą *tylko tego samego* klucza.



Rys. 5. Schemat szyfrowania symetrycznego
Źródło: opracowanie własne

Przykład: Zasada działania algorytmu DES:

- szyfrowanie i deszyfrowanie składa się z 16 rund,
- tekst jawny ma długość 64 bitów,
- klucz ma długość 56 bitów,
- w trakcie każdej rundy dokonywane są te same operacje, ale na wynikach z poprzedniej rundy i specjalnym podkluczu generowanym z 56-bitowego klucza (Rys. 6).



Rys. 6. Schemat szyfrowania algorytmem DES
Źródło: opracowanie własne na podstawie [Denning 1993; Kutyłowski, Strothmann 2000]

Przykład algorytmów symetrycznych:

- DES (*Data Encryption Standard*) - najbardziej znanym algorytm symetryczny, opracowany przez IBM (projekt *Lucifer*, 1971 r.), zgłoszony do konkursu (1973 r.), zmodyfikowany przez NSA (*National Security Agency*) i zaakceptowany (1977 r.), jako federalny standard szyfrowania danych o charakterze niemilitarnym (do 2000 r.).
- AES (*Advanced Encryption Standard*) - w ogłoszonym konkursie (1997 r.) na nowy standard szyfrowania mający zastąpić DES, zwycięzcą (2000 r.) został belgijski algorytm o nazwie *Rijndael* i od 2001 r. jest nowym standardem szyfrowania danych (specyfikacja udostępniona w FIPS197).
- Triple-DES (trzykrotny DES, 3DES) - opracowany w celu zwiększenia odporności szyfrowania algorytmem DES. Zasada działania polega na

trzykrotnym szyfrowaniu tekstu jawnego algorytmem DES przy zastosowaniu dwóch kluczy.

- IDEA (*International Data Encryption Algorithm*) - opracowany w latach 90-tych, jako konkurencja dla DES (uważano, że wielkość kluczy DES jest zbyt mała, a konieczność uzyskania licencji utrudnia jego stosowanie). Opatentowany w Europie i bezpłatny do celów niekomercyjnych.
- RC2, RC4 (*Rivest's Cipher*) - algorytmy autorstwa R. Rivesta; ich szczegóły nie zostały oficjalnie podane. Są to szyfry o zmiennej długości klucza (od 1 do 2048 bitów). Posiadają specjalny status eksportowy, dzięki czemu uzyskanie zezwolenia na eksport jest prostsze pod warunkiem ograniczenia długości klucza (z kluczem do 40 bitów można wykorzystywać je bez ograniczeń). RC4 jest algorytmem powszechnie wykorzystywanym przez przeglądarki (zazwyczaj klucze o długości 40 lub 128 bitów).

7.4.5.2.2. Szyfrowanie asymetryczne (z kluczem publicznym)

Historia:

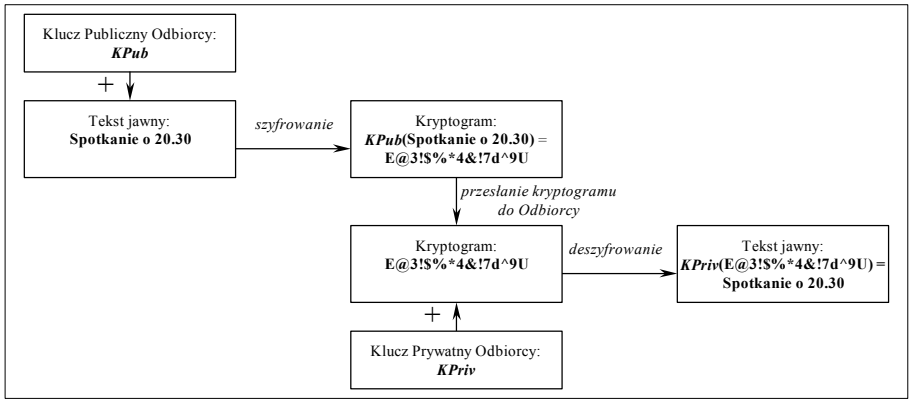
Pomysł na szyfrowanie asymetryczne rozwinięto i opublikowano, zanim jeszcze okazało się, że ma ono praktyczne zastosowanie. Koncepcję szyfrowania asymetrycznego publicznie zaprezentowali w 1976 roku W. Diffie i M. Hellman. Metoda ta stanowiła radykalną zmianę w porównaniu ze stosowanymi w przeszłości, gdyż opierała się na funkcjach matematycznych oraz, co ważniejsze, była asymetryczna. Asymetria oznacza fakt posługiwania się dwoma oddzielnymi kluczami zamiast jednym. Zastosowanie dwóch kluczy ma duży wpływ na poufność, uwierzytelnianie i dystrybucję kluczy.

Schemat działania: Użytkownik posiada parę kluczy: prywatny (*KPriv*) - znany tylko sobie oraz publiczny (*KPub*) - udostępniany każdemu, kto chce z

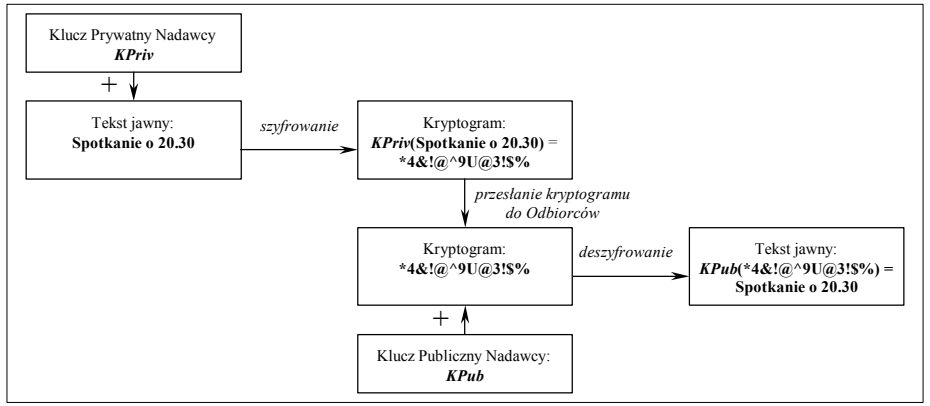
niego korzystać. Tekst zaszyfrowany jednym kluczem może być odszyfrowany *tylko* drugim kluczem,

Zastosowanie szyfrowania z kluczem publicznym:

- szyfrowanie korespondencji - Nadawca przesyła wiadomość do Odbiorcy tak, aby nikt inny nie mógł jej odczytać: Nadawca szyfruje wiadomość kluczem publicznym Odbiorcy (*KPub*) i przesyła kryptogram do Odbiorcy (Rys. 7).
- uwierzytelnianie - Nadawca rozsyła komunikat tak, aby wszyscy mieli pewność, że to on jest jego autorem: Nadawca szyfruje komunikat swoim kluczem prywatnym (*KPriv*) i rozsyła go wszystkim zainteresowanym Odbiorcom (Rys. 8).



Rys. 7. Schemat szyfrowania asymetrycznego
Źródło: opracowanie własne



Rys. 8. Schemat uwierzytelniania przy pomocy szyfrowania asymetrycznego
Źródło: opracowanie własne

Najbardziej znanym algorytmem asymetrycznym jest RSA - opublikowany w 1978 r. przez naukowców z MIT R. Rivesta, A. Shamira i L. Adlemana. Jego sytuacja jest dosyć nietypowa - w USA jest on opatentowany (firma *RSA Data Security*). Na rynku europejskim można z niego korzystać bez ograniczeń, ponieważ został on opublikowany jeszcze przed jego opatentowaniem w USA.

Uwaga: Z szyfrowaniem asymetryczny wiąże się kilka nieporozumień, dlatego należy pamiętać, że:

- szyfrowanie asymetryczne nie jest bardziej odporne na złamanie niż szyfrowanie symetryczne,
- szyfrowanie asymetryczne nie jest techniką ogólnego zastosowania, która sprawi, że szyfrowanie symetrycznie przestanie być stosowane,
- dystrybucja kluczy w przypadku szyfrowania asymetrycznego nie jest trywialna (w porównaniu z symetrycznym) i wymaga odpowiednich procedur,
- szyfrowanie asymetryczne wymaga więcej mocy obliczeniowej niż szyfrowanie symetryczne.

Przykład:

Prędkość szyfrowania i deszyfrowania algorytmem RSA jest znacznie niższa niż algorytmem IDEA - od 100 do 1000 razy (w zależności od długości klucza). Dlatego np. program PGP (*Pretty Good Privacy*) korzysta z algorytmu RSA, ale nie szyfruje nim całego dokumentu tylko wygenerowaną losowo 128-bitową liczbę, którą używana następnie jako klucz szyfrowania algorytmem IDEA właściwego dokumentu. Deszyfracja polega na odszyfrowaniu algorytmem RSA klucza IDEA, a następnie przy jego pomocy reszty dokumentu.

7.4.5.3. Jednokierunkowe funkcje mieszające

Jednokierunkowa funkcja mieszająca (ang. *on-way hash-function*) *H*, to funkcja spełniająca następujące warunki:

- dla każdego *x* łatwo jest obliczyć *H(x)*,
- *H(x)* ma stałą długość dla wszystkich wartości *x*,
- dla danego *y* znalezienie *x* takiego, że *H(x) = y* jest praktycznie niemożliwe.

Zastosowanie jednokierunkowych funkcji mieszających:

- potwierdzanie istnienia dokumentu bez tymczasowego wyjawiania jego treści,
- zabezpieczanie przed zmianami - zagwarantowanie, że w pliku nie było żadnych zmian (wartość funkcji mieszającej dołączana do pliku to tzw. MAC - *Message Authentification Code*),
- przechowywanie haseł - zamiast przechowywać hasło w postaci zaszyfrowanej, przechowuje się tylko wartość funkcji mieszającej.

Najpopularniejszym algorytmem mieszającym jest MD5 (*Message Digest*) zaprojektowany przez R. Rivesta. MD5 jest podstawą dla algorytmu SHA (*Secure Hash Algorithm*) - standardowej funkcji mieszającej (128-bitowej) zaakceptowanej przez NIST.

7.4.5.4. Podpis cyfrowy

Cechy podpisu cyfrowego:

- bardzo duża trudność podrobienia - jedynie osoba X może utworzyć podpis osoby X,
- niemożność skopiowania podpisu z jednego dokumentu do drugiego.

Schemat działania: Podpis cyfrowy realizuje się jako szyfrowanie kluczem prywatnym *KPrv* wartości jednokierunkowej funkcji mieszającej otrzymanej z listu *L*, czyli *KPrv(H(L))*, tzn.:

- osoba A posiada klucz prywatny *KPrv*, a jej klucz publiczny *KPub* i algorytm asymetryczny jest powszechnie znany. Znana jest także postać jednokierunkowej funkcji mieszającej *H*.
- osoba A oblicza wartość funkcji *H* dla listu *L* - czyli *H(L)*,
- osoba A szyfruje kluczem prywatnym wartość *H(L)* - czyli generuje kryptogram *KPrv(H(L))*. Kryptogram *KPrv(H(L))* jest podpisem i jest prezentowany z oryginalnym listem *L*.
- osoba B pragnąca przekonać się, czy list *L* jest faktycznie podpisany przez osobę A - deszyfruje kryptogram kluczem publicznym osoby A, tzn. oblicza *KPub(KPrv(H(L)))*. W rezultacie tego otrzymuje wartość funkcji *H(L)*. Następnie sama oblicza wartość funkcji *H(L)* i porównuje obie wartości.

Infrastruktura zarządzania kluczami publicznymi PKI (*Public Key Infrastructure*) składa się z trzech głównych elementów:

- Organ Rejestracji (*Registration Authority*) - weryfikuje dane użytkownika i dokonuje jego rejestracji,
- Organ Certyfikacji (*Certification Authority*) - identyfikuje wnioskujących i wydaje certyfikaty,
- Repozytorium kluczy, certyfikatów i list unieważnionych certyfikatów.

Użytkownik po zarejestrowaniu się otrzymuje klucz prywatny i publiczny oraz możliwość dostępu do kluczy publicznych innych zarejestrowanych użytkowników.

7.4.6. Systemy firewall

Firewall to system (program, urządzenie) umożliwiający prowadzenie kontroli komunikacji pomiędzy siecią lokalną (komputerem) a siecią o niższym stopniu zaufania (np. Internetem).

Zadania systemu firewall:

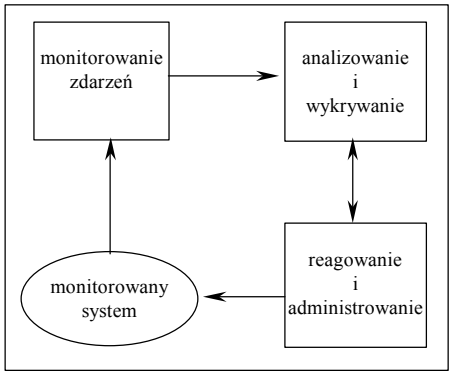
- wykrywanie i eliminowanie prób ataków (np. *spoofing*, DoS, *port scan*),
- kontrolowanie połączeń sieciowych (przechwytywanie pakietów i sprawdzanie czy połączenie sieciowe jest dozwolone),
- ograniczanie liczby dostępnych usług (np. telnet, ftp, irc),
- kontrolowanie dostępu do usług sieciowych na podstawie uwierzytelnienia użytkownika,
- kontrolowanie dostępu do usług i zasobów sieciowych w oparciu o pewne reguły (np. określenie czasu),

- zabezpieczanie przesyłanych informacji - tworzenie wirtualnych sieci prywatnych VPN (*Virtual Private Network*),
- wyłączanie potencjalnie groźnych programów zamieszczonych w serwisach sieciowych (np. programów Java, JavaScript, ActiveX, VisualBasicScript),
- kontrola antywirusowa przesyłanych plików (załączników poczty elektronicznej, plików transmitowanych poprzez ftp),
- ukrywanie wewnętrznej struktury sieci (wykorzystywanie mechanizmu NAT - *Network Address Translation*).
- monitorowanie stanu komunikacji sieciowej (np. obciążenia routera) i równoważenie obciążenia serwerów,
- rejestrowanie zdarzeń.
- dzienni, IS

7.4.7. Systemy wykrywania włamań

Systemów wykrywania włamań - IDS (*Intrusion Detection Systems*) - to kompleksowe narzędzia służące do monitorowania i wykrywania ataków na sieć komputerową.

7.4.7.1. Zasada działania systemów IDS



Rys. 9. Schemat wykrywania ataków użytkownika
Źródło: opracowanie własne

Metody wykrywania ataków:

- metoda sygnatur anormalnego zachowania - porównanie zachowania użytkownika z sygnaturami znanych technik i sposobów ataków,
- metoda profilu normalnego zachowania - monitorowanie zdarzeń generowanych przez użytkownika, analizowanie ich i wykrywanie odbiegających od przyjętej dla niego normy.

7.4.7.2. Monitorowanie zdarzeń

Dane uzyskane podczas monitorowania zapisywane są w *rejestrze zdarzeń*.
Rejestracji powinna podlegać niemal każda operacja użytkownika, a w szczególności:

- częstotliwość otwierania oraz czas trwania sesji usług sieciowych (np. ftp, telnet, ssh),
- próby połączenia się z innymi komputerami lub logowanie się na konta innych użytkowników systemu,
- praca z systemem w godzinach pozasłużbowych,

- miejsca, skąd następuje połączenie z systemem,
- częstotliwość dokonywania zmian katalogu (przeglądanie zasobów),
- modyfikowanie i próby usunięcia plików (logów) systemowych,
- częstotliwość nieudanych operacji w systemie (np. próby uruchamiania programów, odczytywania plików, do których nie ma uprawnień),
- operacje na plikach i katalogach (np. kopiowanie, zmiana praw dostępu),
- uruchamianie programów wywołujących błędy systemu operacyjnego lub błędy innych programów,
- próby wykonania poleceń systemowych, które mają wpływ na bezpieczeństwo systemu i jego zasobów (np. polecenia chmod, chown),
- uruchamianie programów spoza listy akceptowanego oprogramowania.

Analiza zachowania użytkownika

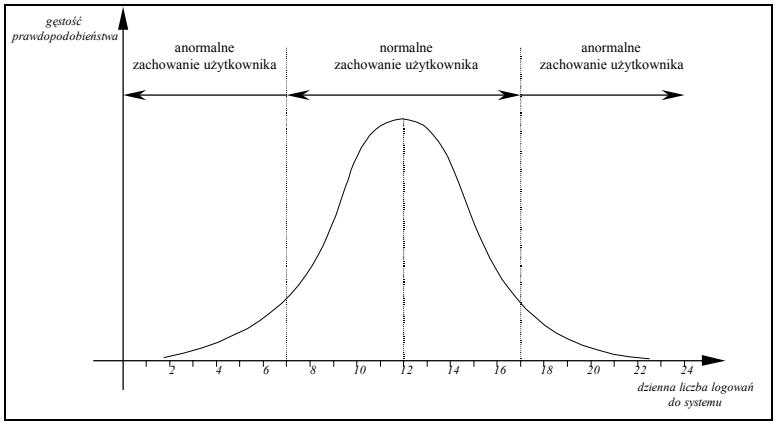
Uwaga: Schemat postępowania zakłada, że zachowanie atakującego różni się od normalnego zachowania użytkownika, a „odstępstwo od normy" da się zmierzyć i na podstawie uzyskanej różnicy (między zachowaniem normalnym a aktualnym) wyciągnąć wniosek o naruszeniu bezpieczeństwa.

Najpierw należy skonstruować tzw. *profil normalnego zachowania użytkownika* - wzorzec (model matematyczny).
Zbudowanie profilu wymaga:

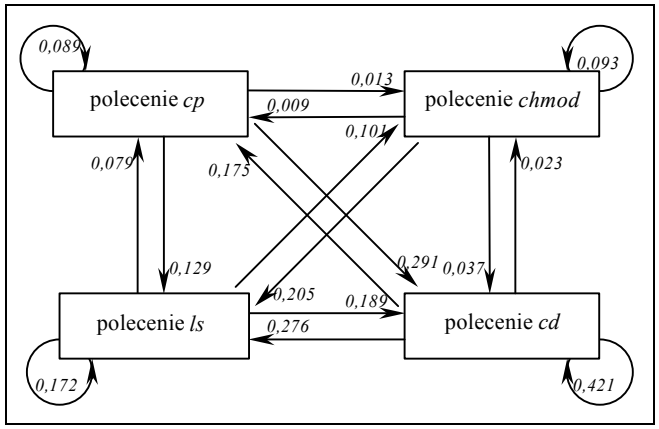
- uwzględnienia charakteru i potrzeb systemu,
- ustalenia *wartości początkowych* profilu.

Do budowy profilu normalnego, analizy i podejmowania decyzji o naruszeniu bezpieczeństwa, wykorzystuje się najczęściej modelowanie zachowania:

- za pomocą narzędzi statystyki matematycznej - parametry profilu traktowane są jako zmienne, a obliczane miary (np. wartość oczekiwana, odchylenie standardowe, korelacje, zmienność w czasie) pozwalają stwierdzić nieprawidłowości w jego zachowaniu (Rys. 10),
- za pomocą modelu Markowa - polega na ustaleniu prawdopodobieństwa przejść pomiędzy kolejno wykonywanymi przez niego operacjami, np. kolejność uruchamianych programów i wydawanych poleceń (Rys. 11).



Rys. 10. Przykładowy rozkład zachowania użytkownika
Źródło: opracowanie własne



Rys. 11. Przykładowe prawdopodobieństwa przejść przy wykonywaniu poleceń użytkownika
Źródło: opracowanie własne

7.4.7.3. Trudności w budowie systemów IDS

Problemy w budowie i funkcjonowaniu systemów IDS:

- trudności z wykrywaniem ataków użytkowników, którzy już w momencie tworzenia profilów normalnego zachowania dopuszczali się nadużyć,
- trudności z wykrywaniem ataków użytkowników, którzy stopniowo dopuszczają się nadużyć (profil jest aktualizowany z ich uwzględnieniem),
- trudności z ustaleniem wartości progowych, po przekroczeniu których sytuację należy uznać za anormalną,
- obciążenie systemu informatycznego przez rozbudowany system wykrywania ataków lub podczas pracy dużej liczby użytkowników,
- możliwość zablokowania lub obniżenia sprawności systemu poprzez umyślne generowanie zachowań anormalnych,
- wykrywanie ataku po jego wystąpieniu, tzn. kiedy szkoda została już wyrządzona (np. system wykrył atak po skasowaniu plików).

7.5. Zabezpieczenia organizacyjne

Zabezpieczenia organizacyjne to zabezpieczenia wynikające z odpowiedniej organizacji korzystania i obsługi systemu informatycznego, zalicza się do nich, m.in.:

- system kontroli (np. kontrole wewnętrzne, kontrole legalności oprogramowania, kontrole przeciwpożarowe, kontrole BHP),
- zasady użytkowania programów i urządzeń komputerowych,
- zarządzanie nośnikami danych,
- ubezpieczenia (np. od wypadków losowych, kradzieży),
- ogólne zasady bezpieczeństwa.

7.5.1. System kontroli

Kontrole wewnętrzne w zakresie bezpieczeństwa SI to zestaw środków, których celem jest zapewnienie odpowiedniego funkcjonowania i bezpieczeństwa SI poprzez *nadzorowanie* i *sprawdzanie*, czy przestrzegane są ustalone reguły postępowania.

7.5.2. Zasady użytkowania programów i urządzeń komputerowych

7.5.2.1. Naprawy, przeglądy i czyszczenie urządzeń komputerowych

- Prace konserwacyjne mają duże znaczenie, jako ochrona przed awariami.
- W systemie informatycznym należy prowadzić dokumentację (dziennik obsługi) zawierającą informacje o tym, co i kiedy było kontrolowane, naprawiane, i jakie usterki zostały usunięte.

Przy naprawach i konserwacjach należy, m.in.:

- poinformować z wyprzedzeniem użytkowników o terminie przeprowadzania prac,
- zadbać o to, aby technicy (serwisanci) wylegitymowali się na żądanie,
- zadbać o to, aby technicy (serwisanci) mieli ograniczony dostęp do danych,
- po zakończeniu prac uzupełnić stosowną dokumentację (należy zapisać nazwiska techników, zakres prac, czas ich realizacji, itp.),
- po zakończeniu prac dokładnie sprawdzić naprawiane (konserwowane, czyszczone) urządzenia, a wszelkie operacje testowe anulować.

7.5.2.2. Przeglądy i kontrole legalności oprogramowania

W systemie należy:

- opracować zasady zatwierdzania, instalowania i użytkowania programów,
- opracować listę programów dopuszczonych do użytku,
- zakazać i uniemożliwić korzystanie z nielegalnego oprogramowania.

7.5.3. Zarządzanie nośnikami danych

Zarządzanie nośnikami danych obejmuje:

- właściwe postępowanie z używanymi nośnikami (przechowywanie, oznakowanie, inwentaryzowanie, porządkowanie, transportowanie),
- odpowiednie niszczenie niepotrzebnych nośników.

7.5.4. Ubezpieczenia

Celem wykupienia ubezpieczeń jest uzyskanie gwarancji, że w przypadku wystąpienia następstw zagrożeń, poniesione straty zostaną choć w pewnym stopniu zrekompensowane.

Podstawowe rodzaje ubezpieczeń SI:

- ubezpieczenia urządzeń elektronicznych - od szkód materialnych wynikających z utraty, uszkodzenia lub zniszczenia wskutek nieprzewidzianej i niezależnej od ubezpieczającego przyczyny, a w szczególności spowodowanych przez:
  - działanie ludzi (niewłaściwe użytkowanie, nieostrożność, celowe zniszczenie przez osoby trzecie, kradzież z włamaniem),
  - działanie ognia, eksplozji, implozji, bezpośredniego uderzenia pioruna, upadku statku powietrznego, wiatru, wody (np. zalanie, powódź),
  - wady produkcyjne, wady materiałowe, nieodpowiednie napięcie, skutek wyładowań atmosferycznych, itp.
- ubezpieczenia od kradzieży z włamaniem i rabunku mienia - chronią m.in. środki obrotowe (urządzenia, narzędzia, towary, materiały, itp.), wyposażenie, gotówkę.
- ubezpieczenia od skutków działania żywiołów - chronią mienie (budynki, instalacje, urządzenia, maszyny, towary, wartości pieniężne, itp.) od szkód powstałych w wyniku ognia, uderzenia pioruna, eksplozji, upadku statku powietrznego oraz akcji ratowniczej prowadzonej w związku z tymi zdarzeniami. Zakres można rozszerzyć o dalsze zdarzenia (np. huragan, deszcz, powódź, trzęsienie ziemi, uderzenie pojazdu).

7.5.5. Ogólne zasady bezpieczeństwa

Do ogólnych zasad bezpieczeństwa należy przede wszystkim *zasada czystego biurka* (w odniesieniu do dokumentów i nośników danych) oraz *zasada czystego ekranu* urządzeń komputerowych. Zgodnie z nimi zaleca się m.in.:

- przechowywanie w zamykanych szafach (pojemnikach ochronnych, sejfach) dokumentów papierowych i nośników danych, kiedy nie są one używane,

- zamykanie (najlepiej w szafie pancernej lub sejfie) danych niezbędnych do prowadzenia działalności,
- niepozostawianie bez nadzoru komputerów zalogowanych do sieci,
- zabezpieczanie komputerów za pomocą haseł lub innych środków,
- ochronę wysyłanej i odbieranej poczty oraz faksów,
- zabezpieczenie kserokopiarek przed nieuprawnionym użyciem,
- niezwłoczne zabieranie wydruków ze współdzielonych drukarek.

7.6. Zabezpieczenia personalne

7.6.1. Zarządzanie zasobami ludzkimi w zakresie bezpieczeństwa SI

7.6.1.1. Nabór pracowników

Podczas naboru nowych pracowników należy przeprowadzić weryfikację polegającą m.in. na:

- sprawdzeniu kompletności i dokładności życiorysu kandydata,
- sprawdzeniu podanych informacji o wykształceniu i posiadanych kwalifikacjach,
- żądaniu i sprawdzeniu jego referencji.

Uwaga: Problemy osobiste lub problemy finansowe pracowników mają bardzo duży wpływ na ich postępowanie.
Należy zwracać uwagę na zmiany zachowania, stylu życia, nieobecności, oznaki stresu lub depresji pracowników.

7.6.1.2. Umowa o zachowaniu poufności

Podpisanie z pracownikiem umowy o zachowanie poufności informacji nie tylko zobowiązuje go do zachowania tajemnicy, ale także zwraca jego uwagę na to, że informacja posiada wartość i nie można jej ujawniać.

7.6.1.3. Określanie zakresu uprawnień, obowiązków i odpowiedzialności

Przy ustalaniu uprawnień użytkownika powinna obowiązywać zasada *minimalnych przywilejów*, tzn. użytkownik otrzymuje tylko takie przywileje, jakie są mu niezbędne do wykonania zadań i tylko na taki czas, jaki jest do tego potrzebny. Brak przywilejów ogranicza rozmiar ewentualnych szkód spowodowanych celowym i przypadkowym działaniem.

7.6.2. Szkolenie i uświadamianie użytkowników

Szkolenia powinny być przeprowadzane z zakresu:

- użytkowania urządzeń i oprogramowania - użytkownicy, którzy wiedzą, jak korzystać z systemu, popełniają mniej błędów i efektywniej pracują,
- bezpieczeństwa - zrozumienie znaczenia bezpieczeństwa oraz umiejętność postępowania po wystąpieniu zagrożeń zwiększa poziom bezpieczeństwa SI.

Uwaga: Szkolenie pracowników to jedna z bardziej efektywnych metod ochrony, ale bardzo kosztowna.
Szkolenie (uświadamianie) to proces ciągły - nowi użytkownicy wymagają przeszkolenia, a pozostali pracownicy - okresowego przypomnienia.

7.6.3. Zaangażowanie użytkowników w bezpieczeństwo SI

Od użytkowników SI oczekuje się, m.in.:

- zgłaszania przypadków naruszenia bezpieczeństwa,
- zgłaszania słabości systemu ochrony,

- zgłaszania niewłaściwego funkcjonowania oprogramowania i urządzeń.

7.7. Procedury ochronne i awaryjne

Procedury dotyczące bezpieczeństwa SI dzieli się na:

- procedury ochronne (zabezpieczające) - np. procedury fizycznego zabezpieczania systemu, tworzenia kopii zapasowych, postępowania ze zużytymi nośnikami, doboru i ochrony haseł, profilaktyki antywirusowej.
- procedury awaryjne - np. procedury postępowania po wykryciu ataku na sieć komputerową, po zarażeniu wirusem, po wystąpieniu awarii urządzeń, po wystąpieniu katastrofy naturalnej.

Celem procedur awaryjnych jest, m.in.:

- usunięcie (zablokowanie, wyeliminowanie) zagrożenia,
- niedopuszczenie do dalszego naruszania bezpieczeństwa,
- zminimalizowanie powstałych już następstw,
- umożliwienie funkcjonowania systemu,
- przywrócenie systemu do stanu sprzed naruszenia bezpieczeństwa,
- wyjaśnienie przyczyn wystąpienia incydentu,
- pomoc w zabezpieczeniu systemu przed innymi incydentami tego typu.

Procedury awaryjne dzieli się na procedury:

- postępowania po wykryciu incydentu (tzw. *procedury obsługi incydentu*),
- kontynuowania działania systemu informatycznego po wystąpieniu incydentu,
- odtwarzania systemu po wystąpieniu incydentu,
- wyjaśniające wystąpienie incydentu.

Procedury odtwarzania systemu informatycznego określają m.in.:

- plan odtwarzania systemu informatycznego,
- odpowiedzialność personalną za uruchomienie i nadzorowanie odtwarzania,
- odpowiedzialność personalną za poszczególne działania odtwarzające,
- opis działań odtwarzających.

Celem procedur wyjaśniających wystąpienie incydentu jest uzyskanie odpowiedzi na następujące pytania:

- co się wydarzyło (rodzaj incydentu) i kiedy,
- co było przyczyną wystąpienia incydentu,
- czy personel działał zgodnie z planem,
- czy potrzebne informacje były dostępne w odpowiednim czasie,
- jakie są propozycje personelu w zakresie modyfikacji zabezpieczeń przed przyszłymi wystąpieniami incydentu.

8. ZARZĄDZANIE BEZPIECZEŃSTWEM SI

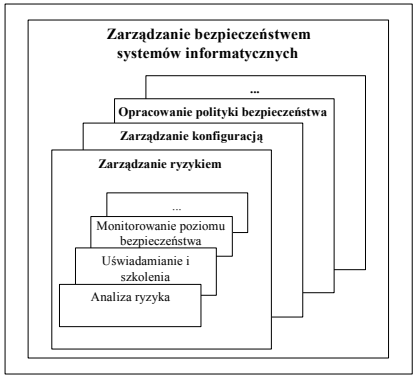
8.1. Zarządzanie bezpieczeństwem a polityka bezpieczeństwa SI

8.1.1. Zarządzanie bezpieczeństwem SI w przedsiębiorstwie

Definicja: *Zarządzanie bezpieczeństwem SI to proces, który ma na celu doprowadzenie do osiągnięcia i utrzymania odpowiedniego poziomu bezpieczeństwa systemu informatycznego* [PN-I-13335-1; PrPN-I-13335-2].

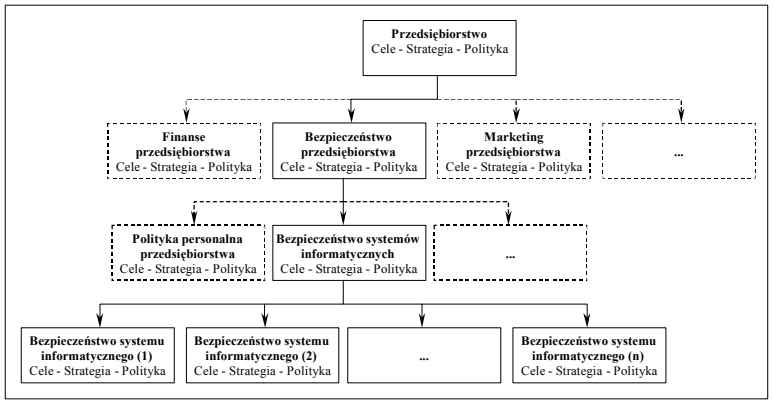
Zarządzanie bezpieczeństwem SI jest procesem trwałym, w skład którego wchodzą inne procesy, takie jak (Rys. 12):

- opracowanie polityki bezpieczeństwa SI,
- identyfikacja ról i odpowiedzialności w SI przedsiębiorstwa,
- zarządzanie ryzykiem,
- zarządzanie konfiguracją,
- zarządzanie zmianami,
- planowanie awaryjne i planowanie odtwarzania po katastrofach,
- wyspecyfikowanie, wybór i wdrożenie zabezpieczeń,
- szkolenia i uświadamianie w zakresie bezpieczeństwa,
- działania bieżące - czyli m.in.: eksploatacja zabezpieczeń, audyt bezpieczeństwa, monitorowanie, wykrywanie i reagowanie na incydenty.



Rys. 12. Procesy zarządzania bezpieczeństwem systemów informatycznych wg ISO/IEC TR 13335
Źródło: opracowanie własne na podstawie [PN-I-13335-1]

W praktyce, efektywne zarządzanie bezpieczeństwem SI możliwe jest tylko wtedy, gdy bezpieczeństwo stanie się integralną częścią ogólnego zarządzania przedsiębiorstwem (Rys. 13).



Rys. 13. Hierarchia celów, strategii i polityk w przedsiębiorstwie
Źródło: opracowanie własne na podstawie [PN-I-13335-1; PrPN-I-13335-2]

8.1.2. Polityki bezpieczeństwa w przedsiębiorstwie

Definicja: *Polityka bezpieczeństwa systemu informatycznego to zasady, zarządzenia i procedury, które określają, jak zasoby są zarządzane, chronione i dystrybuowane w instytucji i jej systemach informatycznych* [PN-I-13335-1].

Polityka bezpieczeństwa powinna odzwierciedlać stanowisko najwyższego kierownictwa i zawierać szczegóły dotyczące zarówno wymagań w zakresie bezpieczeństwa, jak i wykorzystanych zabezpieczeń.

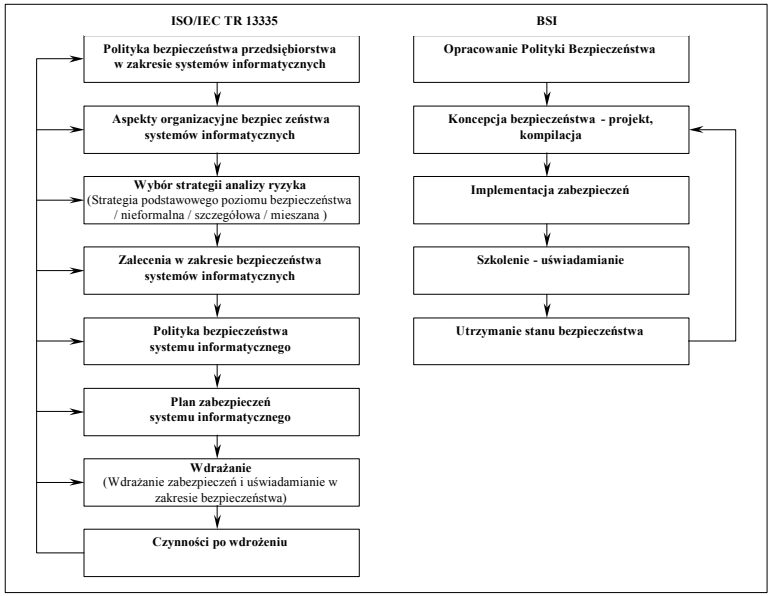
8.1.3. Krytyczne czynniki zarządzania bezpieczeństwem

Dla skutecznego zarządzania bezpieczeństwem SI krytyczne są następujące czynniki [PN-ISO/IEC 17799]:

- opracowanie polityki bezpieczeństwa odzwierciedlającej cele przedsiębiorstwa,
- zarządzanie bezpieczeństwem zgodnie z kulturą przedsiębiorstwa,
- przypisanie pracownikom odpowiedzialności za bezpieczeństwo systemu,
- zauważalne wsparcie i zaangażowanie kadry kierowniczej,
- właściwe zrozumienie wymagań ochronnych i prawidłowa ocena ryzyka,
- propagowanie zasad bezpieczeństwa wśród kierownictwa i pracowników,
- rozpowszechnianie wytycznych dotyczących polityki bezpieczeństwa wśród wszystkich pracowników i kontrahentów,
- zapewnienie odpowiednich szkoleń i uświadamiania pracowników,
- monitorowanie stanu bezpieczeństwa i przekazywanie propozycji ulepszeń.

8.2. Etapy zarządzania bezpieczeństwem SI

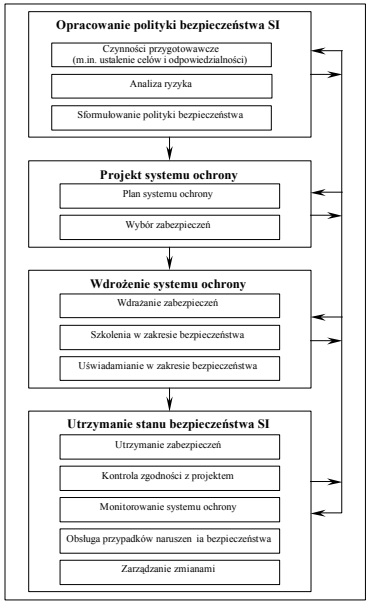
Proces zarządzania bezpieczeństwem SI przedstawiany jest z różną szczegółowością (Rys. 14).



Rys. 14. Etapy zarządzania bezpieczeństwem systemów informatycznych wg ISO/IEC TR 13335 i BSI
Źródło: opracowanie własne na podstawie [PrPN-I-13335-2; BSI ITBPM]

Zasadniczo składa się on z czterech głównych etapów (pomiędzy którymi zachodzą sprzężenia zwrotne - Rys. 15):

- opracowanie polityki bezpieczeństwa systemu informatycznego,
- zaprojektowanie systemu ochrony,
- wdrożenie systemu ochrony,
- utrzymanie stanu bezpieczeństwa systemu informatycznego.



Rys. 15. Etapy zarządzania bezpieczeństwem systemów informatycznych
Źródło: opracowanie własne

8.2.1. Opracowanie polityki bezpieczeństwa systemu informatycznego

8.2.1.1. Czynności przygotowawcze

8.2.1.1.1. Inicjatywa zarządzania bezpieczeństwem SI i zaangażowanie kierownictwa

Uwaga: Zanim zostaną rozpoczęte właściwe działania zmierzające do zarządzania bezpieczeństwem, koniecznie jest przekonanie do nich kierownictwa. Zadanie to może być łatwiejsze lub trudniejsze, w zależności od tego, kto jest pomysłodawcą i jakie są tego powody.

Bardzo ważną sprawą dla całego procesu zarządzania bezpieczeństwem SI jest więc odpowiednie **zaangażowanie kierownictwa** wszystkich szczebli, od którego oczekuje się, m.in.:

- zrozumienia potrzeb przedsiębiorstwa w zakresie bezpieczeństwa SI,
- demonstrowania zaangażowania w sprawy bezpieczeństwa SI,
- odpowiedniego poziomu świadomości w zakresie bezpieczeństwa SI,
- gotowości do zaspokojenia potrzeb wynikających z zarządzania bezpieczeństwem SI (np. przydzielanie środków finansowych i zasobów na rzecz działań w tym zakresie).

8.2.1.1.2. Odpowiedzialność za politykę bezpieczeństwa

Uwaga: Polityka bezpieczeństwa SI musi mieć swojego *właściciela*.

- wyznaczenie właściciela polityki należy do obowiązków kierownictwa przedsiębiorstwa,
- właściciel polityki nie musi być jej autorem (choć byłoby to korzystne),
- właściciel polityki to pracownik przedsiębiorstwa, który odpowiada za jej opracowanie, wdrożenie i późniejszą realizację,
- właściciel polityki zazwyczaj pełni funkcję *kierownika ds. bezpieczeństwa*,
- kierownictwo wraz właścicielem polityki ustala jej główne cele.

Uwaga: W praktyce, niewiele przedsiębiorstw ma wystarczające zaplecze personalne do opracowania polityki bezpieczeństwo, dlatego wyznaczony właściciel polityki musi korzystać z usług konsultantów zewnętrznych.

8.2.1.1.3. Cele polityki bezpieczeństwa

Cele polityki muszą wynikać z celów nadrzędnych (np. celów biznesowych), którymi najczęściej są:

- zagwarantowanie prawnych wymagań ochrony informacji (np. ochrona danych rachunkowych, ochrona danych osobowych, ochrona informacji niejawnych),

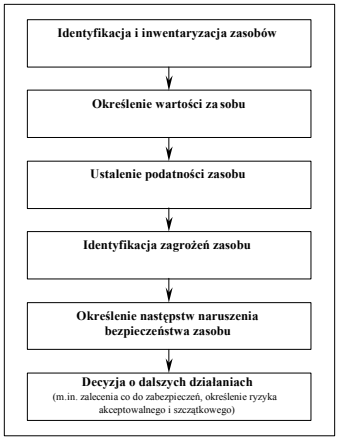
- zagwarantowanie bezpieczeństwa zasobów systemu, a w szczególności przetwarzanej informacji (tzn. zagwarantowanie jej poufności, integralności i dostępności),
- zagwarantowanie bezpieczeństwa publicznego i prestiżu przedsiębiorstwa,
- zagwarantowanie ciągłości funkcjonowania przedsiębiorstwa,
- osiągnięcie redukcji kosztów.

8.2.1.2. Analiza ryzyka

8.2.1.2.1. Cele i etapy analizy ryzyka

Definicja: *Analiza ryzyka w kontekście bezpieczeństwa systemów informatycznych to analiza wartości zasobów, ich zagrożeń i podatności.*

Od sposobu jej przeprowadzenia zależy ocena sytuacji w zakresie bezpieczeństwa i późniejszy wybór zabezpieczeń. Przebieg pełnej analizy ryzyka składa się z kilku etapów (Rys. 16), Niektóre z nich, w zależności od przyjętej strategii, mogą być pominięte.



Rys. 16. Etapy analizy ryzyka
Źródło: opracowanie własne

Celem analizy ryzyka jest dostarczenie m.in.:

- informacji o wartości i wymaganiach ochronnych analizowanych zasobów,
- informacji o podatności zasobów,
- informacji o potencjalnych zagrożeniach zasobów i ich poziomie ryzyka,
- informacji o następstwach naruszenia bezpieczeństwa zasobów,
- zaleceń co do *ryzyka akceptowalnego* i *ryzyka szczątkowego* zasobów,
- zaleceń co do wyboru zabezpieczeń,
- informacji o korzyściach wynikających z wdrożenia zabezpieczeń.

Uwaga: Zalecenia i informacje dostarczone przez analizę powinny być przyjęte i zatwierdzone przez kierownictwo, jako punkt wyjścia do dalszych działań (m.in. opracowania planu systemu ochrony).

Uwaga: Poddanie analizie wszystkich zasobów SI jest kosztowne i czasochłonne. Ponadto, nie zawsze istnieje potrzeba przeprowadzenia tak szczegółowej analizy, dlatego w praktyce występują różne jej strategie.

8.2.1.2.2. Strategie analizy ryzyka

Najczęściej wykorzystywane strategie analizy ryzyka to:

- strategia podstawowego poziomu bezpieczeństwa,
- nieformalna analiza ryzyka,
- szczegółowa analiza ryzyka,
- strategia mieszana.

Tabela 10. Porównanie strategii analizy ryzyka

	Strategia podstawowego poziomu bezpieczeństwa	Nieformalna analiza ryzyka	Szczegółowa analiza ryzyka	Strategia mieszana
czas przeprowadzania analizy	krótki / średni	krótki	długi	średni
koszt analizy	mały / średni	mały	wysoki	średni
zaangażowanie zasobów	małe / średnie	małe	wysokie	średnie
zasoby podlegające identyfikacji	wybrane	brak	wszystkie	wybrane
poziom bezpieczeństwa	podstawowy	niski	wysoki	podstawowy

Źródło: opracowanie własne

Strategia podstawowego poziomu bezpieczeństwa

Polega na doborze zabezpieczeń, które pozwalają osiągnąć podstawowy poziom bezpieczeństwa SI. Podczas jej realizacji należy:

- sporządzić listę zasobów (w oparciu o katalog modułów wzorcowych),
- zapoznać się z ich potencjalnymi zagrożeniami (w oparciu o katalog zagrożeń),
- przypisać wymagania ochronne do poszczególnych zasobów,
- wybrać zestaw zabezpieczeń odpowiedni dla zasobów i ustalonego dla nich poziomu bezpieczeństwa (w oparciu o katalog zabezpieczeń).

Uwaga: Wzorcowe katalogi zasobów, zagrożeń i zabezpieczeń dostępne są w publikacjach poświęconych wykorzystaniu podstawowego poziomu

bezpieczeństwa (np. [BSI ITBPM; PN-ISO/IEC 17799]). Można także skorzystać z doświadczeń innych przedsiębiorstw, podobnych do analizowanego pod względem celów, wielkości, rodzaju działalności i budowy systemu informatycznego.

Zalety strategii podstawowego poziomu:

- redukcja czasu i wysiłku poświęconego na wybór zabezpieczeń,
- niewielkie zaangażowanie zasobów systemu,
- łatwa przenośność rozwiązań pomiędzy różnymi systemami,
- łatwa porównywalność rozwiązań przyjętych w różnych przedsiębiorstwach.

Wady:

- nieodpowiednia (niewystarczająca lub zbyt restrykcyjna) ochrona zasobów systemu w przypadku błędnego ustalenia ich wymagań ochronnych,
- ewentualne trudności z zarządzaniem bezpieczeństwem w przypadku istotnych zmian w systemie (np. jego rozwoju lub aktualizacji).

Nieformalna analiza ryzyka

Analiza nieformalna przeprowadzana jest przez osobę (np. konsultanta zewnętrznego), która dzięki swojej wiedzy i doświadczeniu potrafi określić wartość zasobów, ich podatność oraz zidentyfikować ryzyko.

Zalety nieformalnej analizy ryzyka:

- oszczędność czasu potrzebnego na przeprowadzenie analizy,
- niewielki koszt analizy (w porównaniu np. z analizą szczegółową).

Wady:

- większe prawdopodobieństwo nieuwzględnienia niektórych rodzajów ryzyka oraz pominięcia zasobów,
- duży wpływ subiektywnych poglądów i nastawienia osoby analizującej na wynik analizy,
- brak szczegółowego uzasadnienia wyboru konkretnych zabezpieczeń,
- trudności w zarządzaniu bezpieczeństwem w przypadku istotnych zmian w systemie (np. jego rozwoju), które mogą spowodować konieczność przeprowadzenia powtórnej analizy.

Uwaga: Pomimo wad, ta analiza jest często wystarczająca dla małych przedsiębiorstw.

Szczegółowa analiza ryzyka

Szczegółowa analiza ryzyka jest przeprowadzana dla całego SI i polega ona na identyfikacji i określenia wartości wszystkich zasobów oraz oceny ich podatności i zagrożeń.

Zalety szczegółowej analizy ryzyka:

- określenie poziomu bezpieczeństwa dla każdego zasobu SI,
- dostarczenie dodatkowych informacji dla innych procesów w przedsiębiorstwie (np. zarządzania zmianami).

Wady:

- wysoki koszt wynikający m.in. z jej dużej czaso- i pracochłonności,
- konieczność posiadania przez osoby przeprowadzające analizę szczegółowej wiedzy o konkretnych rozwiązaniach występujących w systemie.

Strategia mieszana

Strategia mieszana polega na wyodrębnieniu części systemu o wysokim stopniu ryzyka (lub zawierającej zasoby krytyczne) i przeprowadzeniu dla niej szczegółowej analizy ryzyka. Dla reszty systemu realizowana jest strategia podstawowego poziomu bezpieczeństwa lub analiza nieformalna.

Zaleta strategii mieszanej: mniejszy koszt i krótszy czas jej realizacji (w porównaniu z analizą szczegółową).

Wada: nieodpowiednia analiza dla części systemu w przypadku niewłaściwego wyodrębnienia obszarów o wysokim stopniu ryzyka.

Uwaga: Strategia może być z powodzeniem wykorzystana zamiast analizy szczegółowej (mniejsze koszty i porównywalna skuteczność).

8.2.1.3. Sformułowanie polityki i opracowanie dokumentu polityki bezpieczeństwa SI

Uwaga: Analiza ryzyka powinna dostarczyć niezbędnej wiedzy na temat ryzyka zasobów systemu, możliwości jego zaakceptowania lub sposobów jego ograniczenia i eliminowania. Na jej podstawie kierownictwo musi opracować i przyjąć treść polityki bezpieczeństwa, która powinna zostać zawarta w *dokumencie polityki bezpieczeństwa*.

Dokument ten, to spisane zasady, rozporządzenia i procedury stanowiące politykę bezpieczeństwa SI. Powinien on być zatwierdzony przez kierownictwo oraz udostępniony wszystkim pracownikom.

Dokument polityki bezpieczeństwa powinien zawierać, m.in.:

- definicję bezpieczeństwa SI oraz cele, zakres i znaczenie bezpieczeństwa,

- przyjętą hierarchię ważności zasobów (np. strategiczne, krytyczne, autoryzowane, powszechnie dostępne) i klasyfikację wymagań ochronnych zasobów (np. bardzo wysokie, wysokie, umiarkowane, brak),
- wyjaśnienie polityki bezpieczeństwa, jej zasad i standardów,
- oświadczenie o intencjach kierownictwa i ich poparciu dla polityki,
- określenie ogólnych i szczegółowych obowiązków oraz odpowiedzialności w zakresie zarządzania bezpieczeństwem,
- odsyłacze do dokumentacji uzupełniającej politykę (np. do procedur).

Uwaga: Należy pamiętać o roli sprzężeń zwrotnych, które występują na każdym etapie zarządzania bezpieczeństwem - ostateczny kształt dokumentu polityki powstaje dopiero po wyborze i wdrożeniu zabezpieczeń.

8.2.2. Projekt systemu ochrony

8.2.2.1. Plan systemu ochrony

Uwaga: W praktyce nie jest możliwe wykorzystanie wszystkich dostępnych zabezpieczeń, gdyż doprowadziłoby to do powstania systemu ochrony drogiego, zbyt restrykcyjnego i niezdolnego do właściwego funkcjonowania.

Definicja: *Plan systemu ochrony to dokument określający działania (w krótkim, średnim i długim okresie czasu), które należy podjąć oraz związane z nimi koszty i obciążenia, które należy ponieść - aby wdrożyć politykę bezpieczeństwa SI.*

Plan ochrony powinien zawierać przede wszystkim:

- kompleksowy projekt systemu ochrony, tzn. m.in.:
  - wybrane zabezpieczenia dostosowane do wymagań ochronnych zasobów, oszacowanego ryzyka i innych czynników,

  - koszty zakupu i wdrożenia zabezpieczeń,
  - oszacowane ryzyko szczątkowe po wdrożeniu zabezpieczenia,
  - szczegółowy *plan wdrożenia* zabezpieczeń,
  - działania kontrolne podczas wdrażania systemu ochrony (np. przypisanie odpowiedzialności),
- wymagania w zakresie uświadamiania i szkolenia personelu,
- wymagania dotyczące opracowania procedur ochronnych i awaryjnych.

8.2.2.2. Wybór zabezpieczeń

Wybierając zabezpieczenia techniczne (programowe i sprzętowe) należy zapoznać się z ich specyfikacją i warunkami zakupu, uwzględniając, m.in.:

- zgodność zabezpieczeń (urządzeń, programów) z przyjętą specyfikacją (np. spełnianie planowanych funkcji, odpowiednia cena),
- zgodność zabezpieczeń z innymi elementami SI (np. systemem operacyjnym, programami, urządzeniami),
- warunki zakupu,
- warunki gwarancji,
- koszty dodatkowe (np. koszt instalacji, konfiguracji, serwisowania),
- łatwość obsługi zabezpieczenia,
- łatwość wdrożenia zabezpieczeń,
- dostępność usług serwisowych,
- markę producenta zabezpieczeń.

8.2.3. Wdrożenie sytemu ochrony

Uwaga: Równolegle z wdrażaniem powinny się odbywać szkolenia i uświadamianie użytkowników, ponieważ ich przyzwyczajeń, na ogół, nie da się zmienić z dnia na dzień.

8.2.3.1. Wdrażanie zabezpieczeń

Podczas wdrażania należy zwrócić uwagę m.in. na to, czy:

- koszty wdrażania zabezpieczeń nie przekroczyły zatwierdzonego poziomu,
- zabezpieczenia są właściwie wdrażane (zgodnie z ich wymaganiami i przyjętym planem),
- zabezpieczenia są od początku właściwie eksploatowane i administrowane.

Uwaga: Większość zabezpieczeń technicznych musi być uzupełniona przez zabezpieczenia organizacyjne, personalne i procedury ochronne, które należy wdrażać równolegle z nimi.

Po zakończeniu wdrożenia powinien się rozpocząć formalny proces zatwierdzenia (akredytacji) wdrożonych zabezpieczeń, po którym wydaje się zezwolenie na rozpoczęcie działania danego zabezpieczenia.

8.2.3.2. Szkolenia w zakresie bezpieczeństwa

Podczas gdy uświadamianie w zakresie bezpieczeństwa odnosi się do wszystkich użytkowników, szczegółowe szkolenia są niezbędne dla:

- personelu odpowiedzialnego za zarządzanie bezpieczeństwem SI, a w szczególności dla osoby pełniącej funkcję kierownika ds. bezpieczeństwa,
- personelu odpowiedzialnego za rozwój i funkcjonowanie SI.

Cykl szkoleń powinien obejmować m.in.:

- zasady funkcjonowania zabezpieczeń,
- zasady obsługi i utrzymania zabezpieczeń.

8.2.3.3. Uświadamianie w zakresie bezpieczeństwa

Uwaga: Program uświadamiania powinien obejmować całe przedsiębiorstwo - od najwyższych szczebli kierowniczych do szeregowych pracowników.
Krytycznym czynnikiem jest uświadomienie kierownictwa, ponieważ do jego obowiązków należy nadzorowanie, kontrolowanie i dalsze uświadamianie podległego im personelu.

Program uświadamiania powinien zawierać przede wszystkim:

- podstawowe potrzeby ochrony,
- cele polityki bezpieczeństwa systemów informatycznych,
- podstawowe pojęcia związane z bezpieczeństwem SI (np. podatność zasobów, zagrożenia, ryzyko, zabezpieczenia),
- następstwa wystąpienia zagrożeń i naruszenia bezpieczeństwa,
- funkcjonowanie systemu ochrony w przedsiębiorstwie,
- obowiązki i odpowiedzialność właścicieli zasobów,
- potrzebę kontroli i postępowań wyjaśniających naruszenia bezpieczeństwa,
- konsekwencje nieautoryzowanego działania (w tym sankcje dyscyplinarne).

Należy pamiętać, że uświadamianie:

- należy tak przeprowadzić, aby zmotywować pracowników i zapewnić ich akceptację w zakresie wspólnej odpowiedzialności za bezpieczeństwo,
- musi mieć wpływ na postępowanie pracowników, dlatego ich zachowanie i korzystanie z zabezpieczeń powinno być monitorowane, aby m.in. określić skuteczność programu uświadamiania,
- jest procesem ciągłym i nigdy nie może być uznane za zakończone.

8.2.4. Utrzymanie stanu bezpieczeństwa systemu informatycznego

Uwaga: Utrzymania uzyskanego poziomu bezpieczeństwa SI należy rozpocząć bezpośrednio po wdrożeniu systemu ochrony.
Niestety, istnieje tendencja do „zapominania" o zabezpieczeniach, które już zostały wdrożone. Tymczasem, naturalne jest starzenie się zabezpieczeń i spadek ich skuteczności w czasie.

Ze względu na dynamiczny rozwój TI oraz pojawiające się nowe zagrożenia i zabezpieczenia, należy śledzić wydarzenia w tej dziedzinie, m.in. poprzez:

- czytanie publikacji poświęconych tematyce informatycznej, a w szczególności zagadnieniom bezpieczeństwa,
- przeglądanie serwisów internetowych z zakresu bezpieczeństwa SI,
- uczestnictwo w grupach dyskusyjnych o tematyce bezpieczeństwa (np. pl.comp.security, pl.comp.networking, pl.comp.os.ms-windows),
- przeglądanie serwisów internetowych producentów oprogramowania i urządzeń wykorzystywanych w systemie informatycznym,
- utrzymanie kontaktów ze specjalistami do spraw bezpieczeństwa i podejmowanie z nimi współpracy.

8.2.4.1. Utrzymanie zabezpieczeń

Uwaga: Wszystkie zabezpieczenia, ze względu na ich starzenie się, potrzebują odpowiedniego utrzymania.
W związku z tym należy:

- wyznaczyć osoby do obsługi zabezpieczeń i ustalić ich odpowiedzialność,
- poddawać zabezpieczenia okresowej kontroli,
- uaktualniać i modyfikować zabezpieczenia,
- kontrolować w jaki sposób zmiany w SI wpływają na zabezpieczenia,

- zwracać uwagę na to, czy postęp technologiczny nie powoduje pojawienia się nowych zagrożeń lub podatności chronionych zasobów.

8.2.4.2. Kontrola zgodności z projektem systemu ochrony

Wdrożone zabezpieczenia muszą być zgodne z opracowanym projektem, dlatego należy przeprowadzać kontrolę zgodności, tzw. *audyt bezpieczeństwa*.

Kontrola zgodności (audyt) powinna:

- umożliwić sprawdzenie, czy zabezpieczenia wdrożone są prawidłowo, funkcjonują poprawnie oraz czy personel odpowiednio je użytkuje,
- być przeprowadzana systematycznie w określonych odstępach czasu oraz, dodatkowo, podczas dokonywania zmian w SI (np. podczas rozwoju systemu, przy wycofywaniu z eksploatacji jego elementów),
- być przeprowadzana przez personel zewnętrzny lub wewnętrzny (tzw. *audytorów*),
- polegać na wykorzystaniu list kontrolnych skonstruowanych w oparciu o projekt systemu ochrony,
- doprowadzić, po wykryciu niezgodności, do opracowania planu czynności naprawczych, jego wdrożenia oraz weryfikacji wyników.

8.2.4.3. Monitorowanie systemu ochrony

Uwaga: System informatyczny i używane w nim zabezpieczenia powinny być na bieżąco monitorowane w celu kontroli poprawności ich działania, upewnienia się, czy zmiany w środowisku nie wpłynęły na ich efektywność oraz czy zapewniona jest odpowiednia rozliczalność zasobów i procesów.

W określonym zakresie monitorowanie systemu wykonywane jest:

- automatycznie przez odpowiednie narzędzia (np. systemy IDS, firewalle),

- tradycyjnie - przez personel odpowiedzialny za bezpieczeństwo systemu.

8.2.4.4. Obsługa przypadków naruszenia bezpieczeństwa

Uwaga: W każdym SI, pomimo systemu ochrony, występowanie przypadków naruszenia bezpieczeństwa (incydentów) jest nieuniknione (np. brak prądu, awaria urządzeń), dlatego jedynym wyjściem jest minimalizacja skutków wystąpienia incydentu i przeciwdziałanie dalszym jego następstwom.

Dlatego w systemie powinny być opracowane *procedury awaryjne*, które w przypadku naruszenia bezpieczeństwa, krok po kroku, pozwolą użytkownikowi wykonać działania minimalizujące skutki wystąpienia incydentu.

W systemie należy przede wszystkim:

- posiadać szczegółowe procedury odpowiednie dla incydentów najczęściej spotykanych w SI oraz procedury ogólne dla danych typów zagrożeń,
- umieścić procedury w miejscu dostępnym dla każdego, kto może ich potrzebować,
- przeszkolić personel, tak aby umiał zidentyfikować rodzaj incydentu i potrafił bezzwłocznie zastosować odpowiednią procedurę,
- na bieżąco aktualizować i dostosowywać procedury.

8.2.4.5. Zarządzanie zmianami w SI i jego zabezpieczeniach

Głównym celem bezpieczeństwa w zarządzaniu zmianami jest zagwarantowanie, aby zmiany nie obniżały bezpieczeństwa SI, dlatego każda wprowadzana zmiana powinna być:

- rozpatrzona pod kątem jej wpływu na bezpieczeństwo systemu,
- uzgodniona i zaakceptowana przez osobę odpowiedzialną za bezpieczeństwo SI,

- odnotowana w dokumentacji systemu informatycznego,
- uwzględniana w związanych z nią dokumentach (np. procedurach ochronnych i awaryjnych).

Uwaga: W wypadku zakupu nowych urządzeń i programów niekiedy wymagane jest, aby przeprowadzony została ich *autoryzacja* polegająca na pisemnym potwierdzeniu przez osobę odpowiedzialną za bezpieczeństwo, że nowy element został sprawdzony pod kątem jego przeznaczenia, zgodności z systemem i wymogami bezpieczeństwa.

8.3. Wybrane aspekty zarządzania bezpieczeństwem systemów informatycznych

8.3.1. Zasady zarządzania bezpieczeństwem systemów informatycznych

Zasady bezpieczeństwa, to ogólne i uniwersalne wytyczne, których należy przestrzegać zarządzając bezpieczeństwem (Tabela 11, Tabela 12, Tabela 13).

Tabela 11. Zasady zarządzania bezpieczeństwem SI dotyczące użytkowników

Zasada	Charakterystyka
Zasada przywilejów koniecznych	Każdy użytkownik otrzymuje tylko przywileje (prawa), które są mu niezbędne do wykonywania jego obowiązków. Zasada powinna obowiązywać wszystkich, włącznie z kierownictwem i administratorami systemu. Opiera się ona na założeniu, że wszystko, co nie jest dozwolone, jest zabronione, w związku z czym pierwotnie użytkownicy nie mają żadnych uprawnień, a wszystkie prawa przydzielane są im w miarę potrzeb. Na bieżąco muszą być też odbierane uprawnienia, które nie są im już potrzebne. Zmniejsza to zagrożenia (przypadkowe i umyślne) ze strony użytkowników.
Zasada wiedzy koniecznej	Każdy użytkownik posiada wyłącznie wiedzę niezbędną do realizacji powierzonych mu zadań. Brak szerszej wiedzy na temat systemu stanowi jego dodatkowe zabezpieczenie i utrudnia nieuprawnione działania (np. przeprowadzenie ataku).
Zasada obecności koniecznej	W określonych pomieszczeniach przebywać mogą wyłącznie te osoby, których obecność jest tam konieczna, oraz które posiadają w związku z tym stosowne upoważnienia.
Zasada indywidualnej odpowiedzialności	Poszczególni użytkownicy mają przypisaną odpowiedzialność za ochronę zasobów. Zakres obowiązków, odpowiedzialności i ewentualnych konsekwencji powinien być ściśle i jednoznacznie określony, aby nie wywoływał nieporozumień.
Zasada słabości człowieka	Najsłabszym elementem każdego systemu informatycznego jest człowiek. To jego działania są najbardziej nieprzewidywalne i powodują wiele zagrożeń, dlatego ważne jest ciągłe podnoszenie umiejętności użytkowników oraz zwracanie im uwagi na rolę, jaką pełnią w jego funkcjonowaniu.
Zasada wspólnego zaangażowania (pracy zbiorowej)	Wszyscy użytkownicy systemu powinni być zaangażowani w prace związane z zarządzaniem jego bezpieczeństwem. Zaangażowanie daje im świadomość własnego wkładu w bezpieczeństwo i wzmacnia poczucie odpowiedzialność za jego stan.

Źródło: opracowanie własne

Tabela 12. Zasady zarządzania bezpieczeństwem SI dotyczące polityki bezpieczeństwa

Zasada	Charakterystyka
Zasada nieosiągalności całkowitego bezpieczeństwa	Całkowite bezpieczeństwo SI jest nieosiągalne. Chęć osiągnięcia takiego bezpieczeństwa przejawia się wdrażaniem wielu zabezpieczeń, które zmniejszają efektywność systemu i zwiększają koszty. Dlatego należy zawsze uwzględniać ryzyko szczątkowe, które pozostaje po wprowadzeniu zabezpieczeń.
Zasada tymczasowości i koniecznej elastyczności zabezpieczeń	Opracowanie systemu ochrony nie jest aktem jednorazowym. Wdrożone zabezpieczenia wymagają ciągłego kontrolowania i modernizacji. Jakiekolwiek zmiany w systemie lub jego otoczeniu muszą znaleźć swoje odbicie w systemie ochrony, który powinien zostać do nich dostosowany.
Zasada usług koniecznych	System powinien realizować tylko te usługi, które są niezbędne z punktu widzenia potrzeb przedsiębiorstwa. Wszystkie inne powinny być wyłączone. Zmniejszenie liczby dostępnych usług powoduje ograniczenie potencjalnych zagrożeń.
Zasada równowagi (minimalnych kosztów)	W zarządzaniu bezpieczeństwem ważne jest zachowanie równowagi pomiędzy kosztami zabezpieczeń a wartością zasobu, dlatego koszt zabezpieczenia zasobu nie powinien przekraczać jego wartości. Należy jednak unikać minimalizacji kosztów, która mogłaby doprowadzić do zbyt słabego zabezpieczenia zasobów.
Zasada konieczności stosowania norm, standardów i „dobrej praktyki”	Pozwala ona osiągnąć korzyści, do których zalicza się przede wszystkim oszczędność czasu i redukcję kosztów wynikającą z wykorzystania już sprawdzonych, zintegrowanych i przenośnych rozwiązań.
Zasada pełnej świadomości	Zasada ta podkreśla, że lepiej mieć niezabezpieczony system, ale posiadać pełną świadomość tego faktu, niż nie mieć go, ale sądzić, że jest zabezpieczony. Często użytkownicy nieświadomie zakładają, że ich działania nie zaszkodzą bezpieczeństwu, w związku z czym nie zachowują odpowiedniej ostrożności.

Źródło: opracowanie własne

Tabela 13. Zasady zarządzania bezpieczeństwem SI dotyczące systemu ochrony

Zasada	Charakterystyka
Zasada „najsłabszego ogniwa łańcucha”	System informatyczny jest tak mocny, jak mocny jest jego najsłabszy element. Oznacza to, że nawet jedno nieodpowiednie zabezpieczenie może osłabić cały system. Jest to szczególnie ważne np. w przypadku ataków wykorzystujących luki w zabezpieczeniach.
Zasada stałej gotowości systemu ochrony	System ochrony powinien być stale przygotowany do odparcia ewentualnych zagrożeń. Nie powinno się dopuszczać do sytuacji, w których - choćby przez pewien czas - zasoby systemu pozbawione są ochrony (np. na skutek tymczasowego wyłączenia zabezpieczeń).
Zasada dopasowania	System ochrony musi być indywidualnie dopasowany do SI i uwzględniać jego specyficzne wymagania. Zaadoptowanie rozwiązań z innych przedsiębiorstw jest możliwe, ale należy uwzględnić przy tym specyfikę systemu docelowego. Wymaga to przeprowadzenia analizy, która wykaże, czy adaptowanie systemu ochrony nie będzie droższe, niż opracowanie go od początku.
Zasada asekuracji zabezpieczeń	Ochrona kluczowych i cennych zasobów SI nie powinna opierać się tylko na jednym zabezpieczeniu, nawet jeżeli jest ono uznane za niezawodne. W takim wypadku konieczne jest zastosowanie kilku zabezpieczeń chroniących zasób niezależnie od siebie.
Zasada kompleksowej ochrony	System ochrony musi być odpowiednio i kompleksowo zaprojektowany i wdrożony. Nie powinno się konstruować systemu ochrony fragmentarycznie i niezależnie od siebie, gdyż wzrasta wtedy ryzyko pominięcia i pozostawienia zasobów bez zabezpieczenia.

Źródło: opracowanie własne

8.3.2. Ograniczenia w zarządzaniu bezpieczeństwem SI

Uwaga: Podczas każdego etapu zarządzania bezpieczeństwem SI można napotkać na ograniczenia, które utrudniają, ograniczają lub uniemożliwiają jego realizację.

Do najczęściej spotykanych należą ograniczenia:

- finansowe - kiedy przedsiębiorstwa nie stać na zarządzanie bezpieczeństwem w takim zakresie, w jakim jest to wymagane,
- osobowe - kiedy brakuje osób, które potrafiłyby zainicjować, opracować i koordynować proces zarządzania bezpieczeństwem lub brak jest poparcia użytkowników dla zarządzania bezpieczeństwem,
- organizacyjne - kiedy brak jest odpowiednich rozwiązań organizacyjnych,

- środowiskowe - kiedy środowisko, w jakim funkcjonuje przedsiębiorstwo, jest przeszkodą dla skutecznego zarządzania bezpieczeństwem,
- czasowe - kiedy czynnik czasu negatywnie wpływa na proces zarządzania bezpieczeństwem,
- prawne - kiedy uwarunkowania prawne, którym podlega przedsiębiorstwo uniemożliwiają efektywne zarządzanie bezpieczeństwem,
- techniczne - kiedy nie ma odpowiednich środków technicznych potrzebnych do zarządzania bezpieczeństwem,
- kulturowe i społeczne - kiedy uwarunkowania kulturowe i społeczne użytkowników utrudniają odpowiednie zarządzanie bezpieczeństwem.

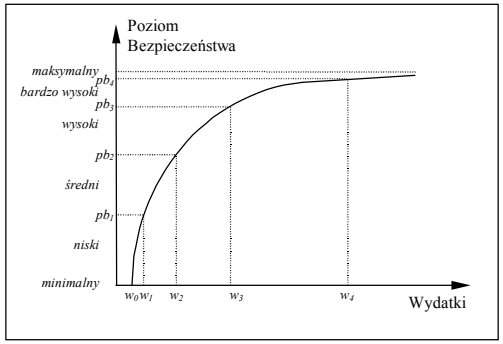
8.3.3. Wydatki na zarządzanie bezpieczeństwem SI

8.3.3.1. Wydatki na bezpieczeństwo a jego poziom

Zależność między poziomem osiągniętego bezpieczeństwa a przeznaczonymi na nie wydatkami nie jest liniowa.

Główne relacje pomiędzy osiągniętym poziomem bezpieczeństwa a wydatkami przedstawiają się następująco (Rys. 17):

- osiągnięcie nawet minimalnego poziomu bezpieczeństwa wymaga poniesienia pewnych wydatków (w_0),
- w systemie o niskim poziomie bezpieczeństwa nawet niewielkie zwiększenie wydatków (z w_1 do w_2) znacząco podnosi ten poziom (z pb_1 do pb_2),
- w systemie o wysokim poziomie bezpieczeństwa nawet znaczne zwiększenie wydatków (z w_3 do w_4) w nieznacznym stopniu podnosi poziom bezpieczeństwa (z pb_3 do pb_4),
- maksymalny poziom bezpieczeństwa jest w praktyce nieosiągalny.



Rys. 17. Zależność między poziomem bezpieczeństwa a wydatkami na bezpieczeństwo
Źródło: opracowanie własne

8.3.3.2. Poziom i struktura wydatków na bezpieczeństwo SI

Wyniki badań wskazują, że na rynku europejskim wydatki na bezpieczeństwo SI stanowią około 5% ogólnej kwoty przeznaczonej na technologię informatyczną. Na rynku amerykańskim ich udział wynosi około 7%.

Według tych samych badań, 63% ankietowanych twierdzi, że potrzebne są dalsze inwestycje w bezpieczeństwo, 32% uważa je za odpowiednie, a 5% sądzi, że wydatki na bezpieczeństwo można obniżyć.

Struktura wydatków jest następująca:

- zabezpieczenia techniczne - 36%,
- wynagrodzenie specjalistów - 23%,
- konsulting - 11%,
- opracowanie strategii - 9%,
- szkolenia - 9%.

8.3.3.3. Zwrot z inwestycji w bezpieczeństwo

Ochronę systemu informatycznego należy traktować, jako inwestycję, niestety, najczęściej wykorzystywany wskaźnik zwrotu z inwestycji ROI (*Return on*

Investment) - nie może być wykorzystany ze względu na trudną do oszacowania wartość zysku, jaką przyniesie wdrożenie zabezpieczeń.

Zaproponowany wskaźnik *zwrot z inwestycji w bezpieczeństwo* - ROSI (*Return on Security Investment*) można obliczyć następująco:

$$ROSI = R – (ALE)$$, gdzie:

R – roczne koszty odzyskania poniesionych strat,

ALE (*Annual Loss Expectancy*) - roczne spodziewane straty, tzn.:

$$ALE = T + (R - E)$$, gdzie:

T – koszt zabezpieczeń (koszt inwestycji),

E – oszczędności wynikające z prewencji.

Jednak w przypadku tego wskaźnika, kwantyfikacja niektórych składowych jest także bardzo trudna (np. spodziewane straty wynikające z utraty zaufania kontrahentów), dlatego otrzymywane wyniki mają charakter orientacyjny.

8.3.4. Stan bezpieczeństwa SI w świetle światowych badań

Wg raportu firmy Ernst & Young, pt. *Światowe badania dotyczące bezpieczeństwa informacji*:

- największą przeszkodą w osiągnięciu zadowalającego poziomu bezpieczeństwa jest brak wystarczających środków finansowych oraz zmieniające się priorytety wykorzystania zasobów.
- uzyskanie środków finansowych na bezpieczeństwo wymaga dokładnego uzasadnienia celowość wydatków. Dużym problemem jest przekonanie zarządu o wadze bezpieczeństwa informacji.
- pomimo powszechnego poglądu o dużym znaczeniu analizy ryzyka, jedynie 27% przedsiębiorstw stwierdziło, że jednym z trzech czynników

decydujących o rozpatrywaniu nowych rozwiązań w zakresie bezpieczeństwa były zalecenia wynikające z analizy ryzyka.

- niewiele przedsiębiorstw stosuje kompleksowe podejście do zagadnienia bezpieczeństwa (tzn. obejmujące analizę możliwości, zagrożeń i korzyści). Podejście do kwestii bezpieczeństwa ma z reguły charakter reaktywny.
- istnieje duża rozbieżność pomiędzy wysoką oceną wagi bezpieczeństwa, a relatywnie niską samooceną dotyczącą rzeczywistego jej stanu.
- największe nakłady ponoszone są na zakup technologii oraz narzędzi informatycznych (w raporcie sugeruje się, że większe korzyści przyniosłoby przeniesienie części wydatków na kwestie związane z kapitałem ludzkim).
- największe zagrożenie nadal stanowią wirusy komputerowe. Wymieniane są także zagrożenia pochodzące z wewnątrz przedsiębiorstw, takich jak np. niezgodne z zasadami wykorzystywanie SI przez pracowników.