1. SYSTEM INFORMATYCZNY

1.1. Definicja systemu informatycznego

System informatyczny to (przykłady definicji):

- system przetwarzania informacji wraz ze związanymi z nim ludźmi oraz zasobami technicznymi i finansowymi, który dostarcza i rozprowadza informacje [PKN],
- uporządkowany zestaw wzajemnie powiązanych składników: kadry, danych, procesów, sprzętu, oprogramowania i sieci komputerowej, współpracujących w celu wykonania założonych funkcji, pozwalających na rozwiązanie występujących problemów i osiągnięcie założonych celów w danej dziedzinie przedmiotowej [Wrycza],
- zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych [ustawa ODO],
- wyodrębniona część systemu informacyjnego, która jest z punktu widzenia przyjętych celów skomputeryzowana [Kisielnicki, Sroka].

Definicja:

***System informatyczny to celowo skomputeryzowana część systemu informacyjnego*.**

1.2. Model systemu informatycznego

System informatyczny (SI) dowolnej organizacji to zbiór elementów:

SI = {P, I, T, O, M, R, N}, gdzie:

P - personel systemu

$$P = \{P_Z, P_I, P_U\}$$

P_Z - personel szczebla zarządzającego i kierowniczego.

P_I - personel informatyczny.

P_U - pozostali użytkownicy systemu informatycznego.

I - dane i informacje

$$I = \{I_E, I_P, I_M\}$$

I_E - zasoby informacyjne w postaci elektronicznej.

I_P - zasoby informacyjne w postaci papierowej.

I_M - zasoby informacyjne w pamięci osób.

M - zbiór metainformacji

$$M = \{M_E, M_P, M_M\}$$

M_E - metainformacje w postaci elektronicznej.

M_P - metainformacje w postaci papierowej.

M_M - metainformacje zgromadzone w pamięci osób.

T - zbiór urządzeń i narzędzi technologii informatycznej

$$T = \{T_S, T_O, T_K\}$$

T_S - sprzęt (urządzenia komputerowe).

T_O - oprogramowanie.

T_K - telekomunikacja.

O - zbiór stosowanych rozwiązań organizacyjnych

$$O = \{ O_S, O_Z, O_R, O_P, O_{B,} ...\}$$

O_S - strategia rozwoju systemu informatycznego.

O_Z - zarządzenia, rozporządzenia i wytyczne regulujące kwestie związane z utworzeniem, funkcjonowaniem i rozwojem systemu informatycznego.

O_R - regulaminy dotyczące zasad użytkowania systemu.

O_P - procedury ochronne i procedury awaryjne.

O_B - dokument polityki bezpieczeństwa.

R - relacje pomiędzy elementami systemu informatycznego

$$R = \{R_{P-P}, R_{P-T}, R_{T-I}, R_{P-I}\}$$

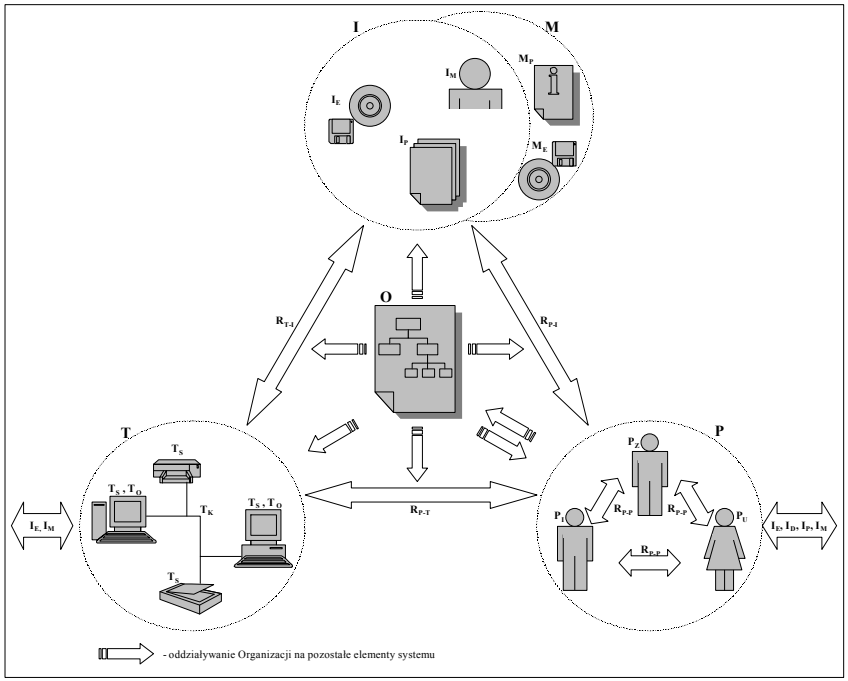
R_{P-P} - relacje pomiędzy personelem systemu.

R_{P-T} - relacje pomiędzy personelem systemu a urządzeniami technologii informatycznej.

R_{T-I} - relacje pomiędzy urządzeniami a zasobami informacyjnymi.

R_{P-I} - relacje pomiędzy personelem a zasobami informacyjnymi.

N - infrastruktura i otoczenie systemu informatycznego



Rys. 1. Model systemu informatycznego przedsiębiorstwa
Źródło: opracowanie własne

1.3. Zasoby systemu informatycznego

Definicja:

Zasoby SI, to wszystko to, co ma dla systemu i instytucji wartość **[PN-I-13335].**

Kategorie zasobów SI:

- zasoby informacyjne - dane i informacje (I) oraz metainformacje (M) - w postaci elektronicznej, papierowej i przechowywane w pamięci osób,
- zasoby ludzkie - personel systemu (P),
- zasoby materialne - urządzenia i narzędzia technologii informatycznej (T) oraz infrastruktura (N),

- zasoby niematerialne - relacje pomiędzy elementami systemu informatycznego (R), zbiór stosowanych rozwiązań organizacyjnych (O) oraz zadowolenie klientów, dobre imię, reputacja.

1.4. Wartość zasobów systemu informatycznego

- Określenie *wartości* zasobów jest niezbędne do wyznaczenia ich *wymagań ochronnych.*
- Nie należy na ochronę zasobu przeznaczać więcej niż jest on warty.
- W przypadku większości zasobów materialnych, można za ich *wartość minimalną* przyjąć ich wartość księgową (rynkową).
- Zasoby niematerialne, informacyjne lub ludzkie zazwyczaj nie mają określonej wartości rynkowej i trudno ją w ogóle oszacować.
- Określenie *rzeczywistej wartości zasobu*, nawet materialnego, zależy od wielu innych czynników.
- Należy pamiętać, że czym innym jest sama wartość zasobu, a czym innym są dodatkowe *straty* spowodowane np. jego utratą.
- Często lepiej posługiwać się pojęciem *straty* spowodowanej uszkodzeniem, zniszczeniem lub naruszeniem bezpieczeństwa zasobu.
- Można próbować ustalić dla zasobu *maksymalną stratę*, jaką spowoduje naruszenie jego bezpieczeństwa.

Podczas określenia wartości zasobu, należy uwzględnić przede wszystkim:

- wartość rynkową zasobu,
- straty wynikające z nieosiągniętych zysków,
- koszty straconego czasu,
- koszty napraw i wymian.

W praktyce zamiast wyznaczania wartości zasobów określa się ich *ważność* (znaczenie), przyjmując za kryterium wpływ na funkcjonowanie systemu.

Bezpośrednio ze znaczeniem zasobów związane są ich *wymagania ochronne*.

Zazwyczaj stosuje się czterostopniową hierarchię ważności zasobów:

- *zasoby strategiczne* - decydują o realizacji strategii, a niekiedy i przetrwaniu przedsiębiorstwa; wymagania ochronne *bardzo wysokie* (podlegają szczególnej ochronie),
- *zasoby krytyczne* - warunkują bieżące, sprawne funkcjonowanie przedsiębiorstwa; wymagania ochronne *wysokie* (chronione w sposób racjonalny i selektywny),
- *zasoby autoryzowane* - podlegają ochronie na podstawie ogólnie obowiązujących przepisów - wymagania ochronne *umiarkowane* (chronione w sposób standardowy),
- *zasoby powszechnie dostępne* - ogólnie dostępne; wymagania ochronne - *brak* (słabo chronione lub nie chronione).

Określenie *ważności zasobów* i ich *wymagań ochronnych* nie jest wystarczające do określenia *zabezpieczeń*, jakie należy w stosunku do nich zastosować. O tym decyduje jeszcze *ryzyko* wystąpienia potencjalnych zagrożeń oraz *podatność* zasobów.

2. POJĘCIE BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO

2.1. Bezpieczeństwo systemu informatycznego - definicja

Pojęcie „bezpieczeństwo" należy do sfery subiektywnych odczuć i może być postrzegane w różny sposób.

Słowniki języka polskiego podają, że:

- *bezpieczeństwo to stan niezagrożenia, spokoju, pewności* [Szymczak],
- *bezpieczeństwo to pojęcie trudne do zdefiniowania. Sytuacja, w której istnieją formalne, instytucjonalne, praktyczne gwarancje ochrony* [Smolski i in.].

W terminologii informatycznej bezpieczeństwo to (przykłady definicji):

- *bezpieczeństwo to* ***miara*** *zaufania, że system i jego dane pozostaną nienaruszone* [Adamczewski],
- *bezpieczeństwo komputerowe to stan, w którym komputer jest bezpieczny, jego użytkownik może na nim polegać, a zainstalowane oprogramowanie działa zgodnie ze stawianymi mu oczekiwaniami* [Garfinkel, Spafford],
- *bezpieczeństwo systemów informatycznych polega na ochronie informacji, systemów lub usług przed katastrofami, błędami i manipulacjami, a także na minimalizowaniu prawdopodobieństwa i skutków wystąpienia przypadków naruszenia bezpieczeństwa oraz sprowadza się do zachowania poufności, integralności i dostępności zasobów i usług systemu* [Boran].

Definicja:

Bezpieczeństwo systemów informatycznych to wszystkie aspekty związane z definiowaniem, osiąganiem i utrzymywaniem poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności systemu **[PN-I-13335-1].**

Atrybuty bezpieczeństwa SI:

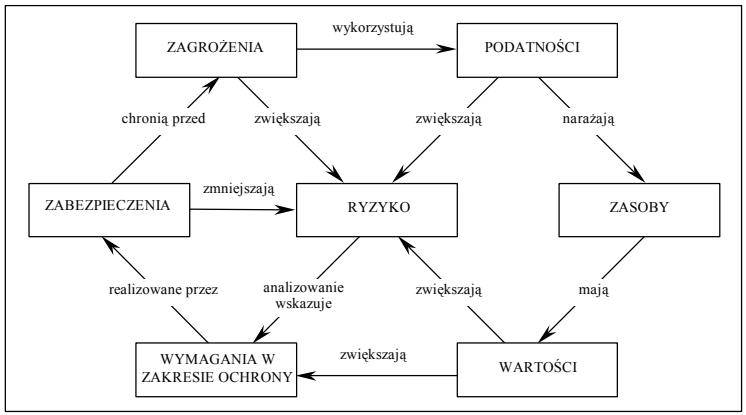
- *poufność* (ang. *confidentiality*) - oznacza, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom (podmiotom, procesom).
- *integralność systemu* (ang. *system integrity*) - oznacza, że system realizuje swoją zamierzoną funkcję w nienaruszony sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej. *Integralność danych* (ang. *data integrity*) - oznacza, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
- *dostępność* (ang. *availability*) - oznacz że, system (informacje) jest dostępny i możliwy do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot.
- *rozliczalność* (ang. *accountability*) - oznacza, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
- *autentyczność* (ang. *authenticity*) - oznacza, że tożsamość podmiotu (użytkownika, procesu, systemu) lub zasobu jest taka, jak deklarowana.
- *niezawodność* (ang. *reliability*) - oznacza spójne, zamierzone zachowanie i skutki.

2.2. Elementy bezpieczeństwa systemu informatycznego

Podatność zasobów i ryzyko wystąpienia zagrożeń

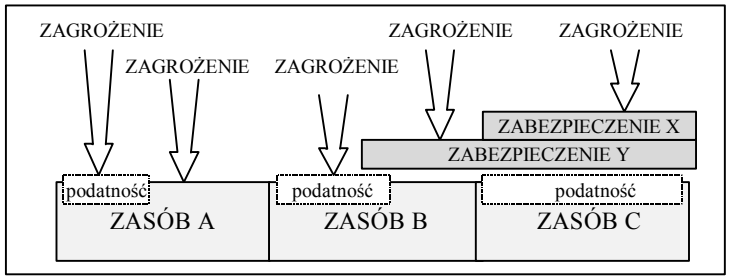
Na rzeczywisty poziom bezpieczeństwa SI i jego zasobów wpływa także:

- *zagrożenie* (ang. *threat*), czyli potencjalna przyczyna niepożądanego incydentu, którego skutkiem może być szkoda dla systemu. Niektóre zagrożenia mogą mieć wpływ na większą liczbę zasobów i powodować różne skutki w zależności od tego, których zasobów dotknęły.
- *podatność* (ang. *vulnerability*) jest to słabość zasobu lub grupy zasobów, która może być wykorzystana przez zagrożenie. Podatność zasobów oznacza ich słabość, ale sama w sobie nie powoduje szkody. Jest jedynie warunkiem, który może umożliwić zagrożeniu oddziaływanie na zasoby.
- *ryzyko* (ang. *risk*) jest to prawdopodobieństwo, że określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów, aby spowodować ich zniszczenie lub straty.



Rys. 2. Zależności pomiędzy podstawowymi elementami wpływającymi na bezpieczeństwo SI
Źródło: opracowanie własne na podstawie [PN-I-13335-1]

Z punktu widzenia bezpieczeństwa najbardziej interesująca jest relacja: **zagrożenia - zabezpieczenia - podatności - zasoby**.



Rys. 3. Zależności pomiędzy zagrożeniami a zasobami oraz ich zabezpieczeniami i podatnościami
Źródło: opracowanie własne

Możliwe są tutaj sytuacje:

- zasób jest chroniony całkowicie (zasób C), częściowo (zasób B) lub w ogóle (zasób A),
- na zasób oddziałuje jedno lub kilka zagrożeń, które mogą wykorzystywać jego podatność lub nie (zasób A),
- podatności zasobów mają różną wielkość (por. podatność zasobu A i zasobu C),
- zasób jest chroniony przez zabezpieczenie częściowo (zasób B i zabezpieczenie Y) lub całkowicie (zasób C i zabezpieczenie Y),
- zasób może być chroniony przez kilka zabezpieczeń (zasób C).

Przyczyny podatności na zagrożenia zasobów SI

- niemożność zobaczenia „gołym okiem" danych elektronicznych - sprawia, że trudno je śledzić oraz bezpośrednio kontrolować.
- szybkość i automatyzacja przetwarzania danych - utrudnia bieżące wykrycie ewentualnej pomyłki, przekłamania lub modyfikacji oraz zmniejsza wpływ człowieka na wynik przetwarzania.

- transmisja siecią danych - podczas tego procesu dane są narażone na przechwycenie, modyfikację, utratę integralności lub zniszczenie.
- niewielki rozmiar urządzeń i nośników danych - sprzyja ich kradzieży i uszkodzeniu.
- łatwość uszkodzenia - urządzenia i nośniki danych są mało odporne na uszkodzenia mechaniczne, ładunki elektrostatyczne, ogień i wodę.
- dokładna wiedza środowiska informatycznego (np. programistów) na temat zasad działania SI - świadomość istnienia braków, błędów lub nieudokumentowanych funkcji systemu w połączeniu z chęcią jej wykorzystania, sprzyja nadużyciom bardzo trudnym do wykrycia.
- brak określonych uprawnień i odpowiedzialności - sytuacje, w których zasoby są wykorzystywane przez wielu użytkowników, ale żaden z nich nie jest osobiście za nie odpowiedzialny, sprzyjają nadużyciom.
- brak standardowych mechanizmów ochrony zasobów - powoduje, że zasoby nie są bezpieczne w sytuacji, gdy ktoś uzyska do nich dostęp.
- brak wiedzy, świadomości, umiejętności i odpowiednich przyzwyczajeń użytkowników w zakresie bezpieczeństwa - pomimo coraz prostszej obsługi programów i urządzeń nadal zdarzają się przypadki nieprawidłowego z nich korzystania, popełniania błędów i nieprzestrzegania zasad bezpieczeństwa.

Następstwa wystąpienia zagrożeń

Następstwem zagrożeń są szkody (straty) spowodowane wystąpieniem niepożądanego incydentu i mogą mieć one charakter:

- czasowy (np. chwilowa niedostępność systemu),
- stały (np. zniszczenie zasobów).