INFORMACJA – JEJ ZNACZENIE I SPOSOBY OCHRONY. PERSPEKTYWA TECHNICZNA

Krzysztof Liderman

Wojskowa Akademia Techniczna

Streszczenie. Artykuł zawiera przegląd zagadnień związanych ze znaczeniem informacji dla funkcjonowania współczesnego państwa oraz zagadnień poprawnej ochrony takiej informacji.

1. Wstęp

Współczesne zaawansowane technologicznie społeczeństwa swój byt w dużym stopniu uzależniają od informacji i to głównie informacji przetwarzanej, przechowywanej i przesyłanej w systemach teleinformatycznych. Z tego powodu istotne staje się zagadnienie właściwej ochrony takiej informacji, a to z kolei wymaga sprecyzowania, dlaczego informacja powinna być chroniona. Informacja powinna być chroniona, ponieważ:

1. Jest ona towarem o znaczeniu strategicznym (dla kraju, firmy, konkretnego człowieka).
   Od zarania dziejów ci, którzy dysponowali właściwą informacją we właściwym czasie, wygrywali wojny oraz osiągali sukcesy rynkowe. Dlatego podobnie jak współcześnie rudy uranu czy nowe technologie, informacja jest towarem, który można kupić, dzięki któremu można osiągnąć określone korzyści i który trzeba chronić, mając na względzie własne interesy.
2. Jest podstawowym elementem procesów biznesowych.
   Podstawą działania prawie wszystkich współczesnych firm i organizacji, w tym organizacji takiej jak państwo, jest poprawny obieg informacji. Przerwanie tego obiegu lub sfałszowanie informacji powoduje straty, dla firmy kończące się często bankructwem, a dla państwa niepokojami społecznymi, zaburzeniami w gospodarce krajowej, gorszym postrzeganiem na forum międzynarodowym itd.
3. Służy do sterowania procesami w zautomatyzowanych procesach wytwórczych i usługowych o kluczowym znaczeniu dla gospodarki i społeczeństwa.
   Informacja może występować także w szczególnej postaci – informacji sterującej urządzeniami, zwykle czujnikami i mechanizmami wykonawczymi (w przedstawionej na rys. 2 klasyfikacji będą to systemy sterowania). Błędne sterowanie

takimi systemami może powodować katastrofy (np. ekologiczne) i wywoływać kryzysy na skalę lokalną, ogólnokrajową lub międzynarodową.

4. Tak nakazują przepisy obowiązującego prawa lub wynika to z zawartych umów. Ze względów przedstawionych w punktach 1 i 2 oraz z uwagi na ochronę dóbr osobistych obywateli, wszystkie cywilizowane kraje mają przepisy prawne wymuszające ochronę informacji przed nieuprawnionym dostępem, zapewnienie właściwego jej przetwarzania, przechowywania i przesyłania oraz określające zasady zbierania określonych kategorii informacji.

W dalszej części artykułu przedstawione są rozważania na temat informacji jako takiej (rozdz. 2), zagrożeń dla niej (rozdz. 3) oraz sposobach jej ochrony (rozdz. 3 i 4).

2. O informacji

Jak podano we wstępie, informacja była, jest i będzie towarem. Informacje mają jednak tę szczególną właściwość, odróżniającą je od innych towarów (przedmiotów materialnych, usług), że aby udzielić ich jednym (osobom), wcale nie trzeba odbierać ich innym. W konsekwencji ujawnienie informacji:

- może zostać niezauważone,
- zwykle samo w sobie nie powoduje straty.

Na wartość informacji, traktowanej jako pewien zasób[1] podlegający ochronie, wpływ będzie miała [3]:

- wiedza o istnieniu informacji,
- wiedza o ujawnieniu informacji i wiedza stron o ujawnieniu (oni wiedzą/nie wiedzą, że my wiemy, że znają nasze tajemnice),
- starzenie się informacji (utrata lub wzrost jej wartości z upływem czasu).

Ze względu na znaczenie dla użytkownika (ogólnie: podmiotu, w tym podmiotu gospodarczego) wszystkie wykorzystywane przez niego, jak również dotyczące go informacje można podzielić na *wrażliwe* i *niewrażliwe*. Informacje wrażliwe dla określonego podmiotu to te, które mogą zostać wykorzystane przeciwko jego interesom poprzez ujawnienie, nieudostępnienie oraz zmanipulowanie, jawne lub skryte.

Do wrażliwych zaliczają się zatem wszystkie informacje, które muszą być chronione, bo tak nakazują obowiązujące przepisy prawne (np. *Ustawa o ochronie danych osobowych*). Ale informacjami wrażliwymi będą też takie, których nakaz ochrony nie jest zawarty w żadnych regulacjach prawnych, a które organizacjom wytwarzającym je i przetwarzającym są zwykle wskazywane przez kompetentne organy – służby ochrony państwa lub wewnętrzne komórki bezpieczeństwa.

[1] W literaturze przedmiotu często zamiast „zasób" jest używany termin „aktywa".

Informacjami wrażliwymi mogą być też dane same w sobie niewrażliwe, ale które stają się takie w powiązaniu z innymi informacjami, pozwalając wyciągnąć prawidłowe wnioski np. o projektowanej fuzji firmy z zagranicznym partnerem. Przykładem mogą być informacje dotyczące spotkań kierownictwa firmy, zamówionych przez nią analiz firm trzecich, planów wyjazdów służbowych itd. Innym przykładem są informacje dotyczące życia osobistego czołowych przedstawicieli kierownictwa firmy, których ujawnienie mogłoby posłużyć do wywołania skandalu (i w efekcie np. do obniżenia notowań firmy na giełdzie, zerwania umów itp.) czy też do szantażowania określonych osób np. w celu ujawnienia przez nie innych informacji, tym razem strategicznych dla firmy.

Problem w praktyce ochrony informacji polega na tym, że najczęściej wymagana identyfikacja informacji wrażliwej ogranicza się do jej inwentaryzacji i przeglądu zasobów w ramach analizy ryzyka. Rzadko bierze się pod uwagę, że:

- oprócz identyfikacji informacji wrażliwych w organizacji trzeba je zlokalizować także poza nią,
- należy uwzględnić informacje pośrednie, pozwalające na wnioskowanie,
- powinno się zidentyfikować obieg informacji wrażliwej – to pozwala m.in. na opracowanie procedury lokalizacji jej „przecieków".

Sprawę komplikuje dodatkowo fakt, że [3]:

- prawa własności w wypadku informacji są często trudne do określenia,
- ustalenie wartości strat w wypadku ataków informacyjnych bywa trudne lub wręcz niemożliwe – dotyczy to np. utraty spodziewanych korzyści, wizerunku, przewagi konkurencyjnej itp.[2],
- lokalizacja wartościowych informacji bywa trudna.

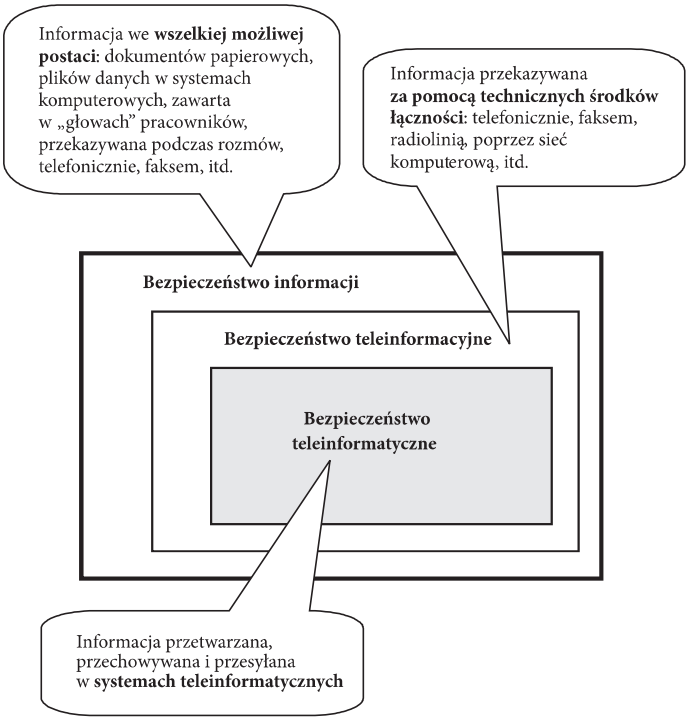
Z przedstawionych w tym rozdziale rozważań wynika ważny wniosek – osoby odpowiedzialne za ochronę informacji powinny dbać o ochronę informacji wrażliwych, a nie „danych osobowych" czy „informacji niejawnych". Wyżej wymienione kategorie informacji są tylko szczególnymi przypadkami informacji wrażliwej. Brak takiego podejścia do ochrony informacji jest zasadniczym błędem organizacyjnym, którego nie zniwelują żadne środki techniczne.

3. Podstawy ochrony informacji

Ochrona informacji jest zagadnieniem obszernym i generalnie wiąże się z tzw. **bezpieczeństwem informacyjnym**, obejmującym wszystkie formy (także werbalne) wymiany, przechowywania i przetwarzania informacji (patrz rys. 1). Tzw. bezpieczeństwo teleinformacyjne dotyczy węższego zakresu form wymiany, przechowywania

[2] Czasami jednak może być oczywiste, np. po oszustwie, szantażu lub przelaniu środków z konta organizacji.

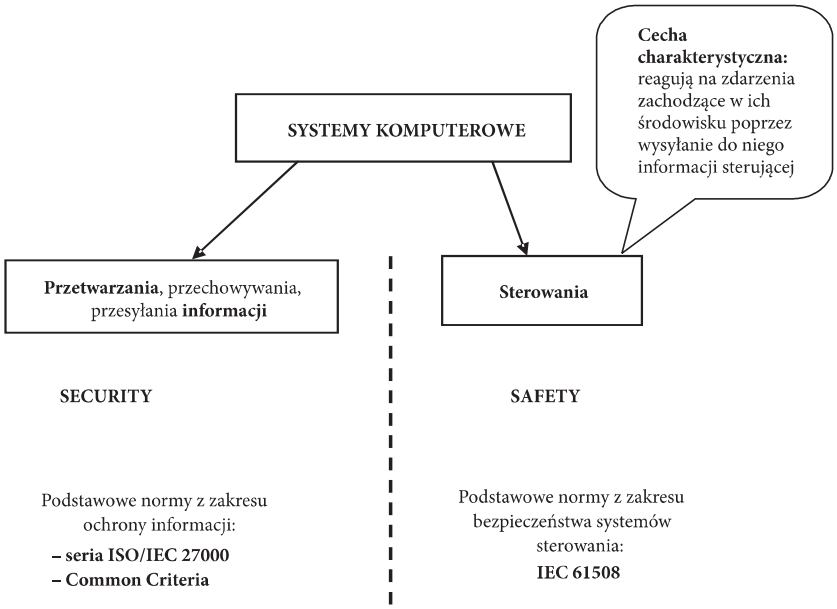
i przetwarzania informacji, ograniczonego do technicznych środków łączności (np. przez telefony stacjonarne i komórkowe, radiostacje, sieci i systemy komputerowe). Z kolei **bezpieczeństwo teleinformatyczne** dotyczy informacji przesyłanych, przechowywanych i przetwarzanych w sieciach i systemach teleinformatycznych.



Rys. 1. Kategorie bezpieczeństwa

W zależności od przeznaczenia i konstrukcji systemu teleinformatycznego (patrz rys. 2) rozróżnia się zwykle tzw. **bezpieczeństwo na zewnątrz** oraz **bezpieczeństwo do wewnątrz**. Termin bezpieczeństwo na zewnątrz określa ochronę przed **zagrożeniami dla środowiska** (w tym dla człowieka), w którym pracuje system komputerowy, spowodowanymi nieprawidłowym działaniem tego systemu. Dotyczy to głównie systemów sterowania (zwykle są to systemy czasu rzeczywistego), np. monitorujących stan pacjenta w szpitalu, kontrolujących działanie elektrowni jądrowej, nadzorujących ruch kolejowy, czy też systemów pokładowych, np. samolotów. W języku angielskim ogół zagadnień związanych z ochroną tego typu (w sensie niedopuszczania do katastrof) określa się zwykle terminem *safety*. Termin **bezpieczeństwo do wewnątrz** określa ochronę przed **zagrożeniami dla informacji** przechowywanej, przetwarzanej i przesyłanej w systemie teleinformatycznym.

Dotyczy to głównie sieci teleinformatycznych banków, firm, organizacji naukowych itd. W języku angielskim ogół zagadnień związanych z ochroną tego typu (w sensie niedopuszczania do utraty tajności, integralności, dostępności informacji) określa się zwykle terminem *security*. To rozróżnienie znajduje swoje odbicie w praktyce nie tylko w różnych unormowaniach (patrz rys. 2), ale także w strukturze cyklu życia systemów i sposobie ich wytwarzania i utrzymywania.



Rys. 2. Klasyfikacja systemów komputerowych

Proponuje się następującą definicję bezpieczeństwa informacji:

Definicja 1

Termin **bezpieczeństwo informacji** oznacza stopień uzasadnionego (np. analizą ryzyka i przyjętymi metodami postępowania z ryzykiem) zaufania, że nie zostaną poniesione potencjalne straty wynikające z niepożądanego (przypadkowego lub świadomego): ujawnienia, modyfikacji, zniszczenia lub uniemożliwienia przetwarzania informacji przechowywanej, przetwarzanej i przesyłanej w określonym systemie obiegu informacji.

Można zauważyć, że „bezpieczeństwo" nie jest ani obiektem, ani zdarzeniem, ani procesem – to imponderabilia z dziedziny psychologii. Decydujący wpływ na „zaufanie" ma siła ochrony (zabezpieczeń), z jaką chronimy podstawowe atrybuty informacji:

– *tajność* – informuje o stopniu (sile) ochrony informacji przed nieuprawnionym dostępem. Stopień ten jest uzgadniany przez podmioty dostarczające i otrzymujące informację (z tajnością jest ściśle związana dotycząca ludzi

poufność, czyli prawo jednostki do decydowania o tym, jakimi informacjami i z kim chce się podzielić i jakie jest skłonna przyjąć);
- *integralność* – informuje, czy dane i informacje są poprawne, nienaruszone i nie zostały poddane manipulacji;
- *dostępność* – informuje, czy dane, procesy i aplikacje są dostępne zgodnie z wymaganiami użytkownika (lub wymaganiami na system).

Przy projektowaniu systemu ochrony oraz analizie ryzyka należy brać pod uwagę wszystkie wymienione atrybuty oraz, w miarę potrzeb, inne związane z charakterem realizowanych zadań (np. rozliczalność, która umożliwia identyfikację użytkowników i wykorzystywanych przez nich usług; istotna dla skutecznej analizy powłamaniowej).

Należy zwrócić uwagę, że specjaliści od techniki komputerowej posługują się najczęściej pojęciem danych, a nie informacji. Przyjmuje się, że informacje przechowywane, przesyłane i przetwarzane w systemach komputerowych nazywa się „danymi". Jednak dla skutecznej ochrony danych/informacji, ze względu na przedstawione wcześniej zależności pomiędzy systemem informacyjnym a informatycznym, obecnie obowiązujący paradygmat w dziedzinie „bezpieczeństwa informacyjnego" brzmi: **chronimy „informacje" – „dane" są tylko ich szczególnym przypadkiem**.

Zagrożenia, przed którymi chroni się informację, można pogrupować następująco:

1. „Siły wyższe" (katastrofy naturalne, zmiany prawa, itp.).
2. Nieuprawnione i przestępcze działania ludzi[3]:
   a) kradzieże oraz zagubienia nosicieli informacji (sprzętu i dokumentów);
   b) podsłuchy różnego typu: pakiety w sieci (*sniffing*), emisja ujawniająca, fale głosowe („pluskwa");
   c) nieuprawnione działania personelu (w tym outsourcingowego i praktykantów);
   d) nieuprawnione działania osób postronnych (np. klientów, „hakerów").
3. Błędy ludzi uczestniczących w procesach przetwarzania, przesyłania i przechowywania informacji.
4. Błędy w organizacji przetwarzania, przesyłania i przechowywania informacji.
5. Awarie sprzętu i błędy w oprogramowaniu.

Wyżej wymienione grupy stanowią podstawowe **klasy zagrożeń**. Często popełnianym błędem podczas analizy stanu bezpieczeństwa jest postrzeganie zagrożeń wyłącznie przez pryzmat „ataków" (czyli zagrożeń z grupy 2d)[4].

[3] Nie każde działanie nieuprawnione (z punktu widzenia dysponenta systemu informacyjnego) jest działaniem przestępczym – przestępstwem jest tylko to, na co istnieje odpowiedni paragraf w *Kodeksie karnym*.

[4] Atakiem na system teleinformatyczny i informację w nim przetwarzaną nazywa się nieuprawnione, celowe działania ludzi mające na celu naruszenie tajności, integralności lub dostępności informacji.

Zagrożenie spowoduje szkody tylko wtedy, jeżeli istnieją wady lub luki, czyli tzw. **podatności** w strukturze fizycznej firmy, organizacji pracy, procedurach, obsadzie stanowisk pracy personelem, zarządzaniu i administrowaniu, sprzęcie lub oprogramowaniu, które mogą być wykorzystane przez zagrożenia do spowodowania szkód w systemie informatycznym lub działalności użytkownika. Związki pomiędzy zagrożeniami, podatnościami i szkodami można scharakteryzować następująco:

- Na zagrożenia nie mamy wpływu, ale zagrożenie nie zawsze musi się zrealizować – warunkiem koniecznym jest istnienie podatności.
- Na podatności mamy wpływ – możemy je minimalizować, stosując **zabezpieczenia**.
- Oprócz podatności, w zależności od typu zagrożenia, wiele innych czynników ma wpływ na **prawdopodobieństwo** jego realizacji.
- **Szkody**, które mogą powstać podczas realizacji zagrożenia, oraz **prawdopodobieństwo** jego realizacji (także w sensie potocznym „możliwości") określają **ryzyko**.

Na wspomniane zabezpieczenia składają się środki:

- fizyczne (np. sejf, płot, przegroda budowlana),
- techniczne (np. system alarmowy, system przeciwpożarowy, system nadzoru wizyjnego),
- osobowe (np. strażnik, portier),
- programowe (np. oprogramowanie antywirusowe)

oraz działania organizacyjne (np. szkolenia), stosowane w celu przeciwdziałania wykorzystaniu podatności przez zagrożenia. Odpowiednio zaimplementowane zabezpieczenia tworzą **system ochrony informacji**. Podział zabezpieczeń, w kontekście postępowania z ryzykiem, przedstawiony jest na rysunku 4.

Do podstawowych zasad organizacji pracy (czyli elementu ww. działań organizacyjnych), zapewniających ochronę informacji, należą zasady:

1. Wiedzy niezbędnej (pracownik ma wiedzieć o tym, co dzieje się w organizacji, dla której pracuje, tylko tyle, ile jest niezbędne do rzetelnego wypełniania przez niego obowiązków służbowych).
2. Minimalnego środowiska pracy (pracownik ma mieć dostęp tylko do tych pomieszczeń, urządzeń, narzędzi, usług i programów, które są niezbędne do rzetelnego wypełniania przez niego obowiązków służbowych)[5].
3. „Czystego biurka" i „czystego ekranu".
4. Separacji i rotacji obowiązków.
5. Dobrze opisanych reguł przetwarzania danych[6].

[5] Często spotykanym przypadkiem naruszania tej zasady jest przydzielanie wszystkim pracownikom nieograniczonego dostępu do Internetu.

[6] Pracownik nie będzie przetwarzał danych w sposób dowolny, tylko zgodnie z ustalonymi regułami, a wszelkie manipulacje na danych będą odnotowywane dla celów kontrolnych (tzw. audit-log).

Te zasady powinny być znane personelowi kierowniczemu (bo to on organizuje pracę) i stosowane oraz egzekwowane wszędzie tam, gdzie jest przetwarzana informacja wrażliwa.

4. Organizacja ochrony informacji

System ochrony informacji będzie skuteczny, jeżeli będzie systemem, a nie „workiem z zabezpieczeniami", tj. będzie **kompleksowy** i będą w nim wykorzystane w **spójny** sposób (tzn. niesprzeczny i niepozostawiający dziur) zabezpieczenia: organizacyjne i kadrowe, fizyczne i techniczne oraz sprzętowo-programowe zorganizowane w taki sposób, że zapewnią wykrycie naruszenia bezpieczeństwa i próby takich działań oraz skuteczną ochronę pomimo przełamania części zabezpieczeń, co oznacza ich zastosowanie według zasady obrony „w głąb".

Do podstawowych przedsięwzięć organizacyjnych związanych z budową i eksploatacją systemów ochrony informacji należą:

1. Wykonanie, jako podstawy budowy systemu ochrony informacji, analizy ryzyka związanego z wykorzystywaniem informacji w działalności biznesowej i właściwe zarządzanie tym ryzykiem.
2. Udokumentowanie systemu ochrony informacji.
3. Ocena stanu ochrony informacji (w tym tzw. audyt).
4. Zidentyfikowanie i stosowanie przepisów prawa oraz norm i standardów adekwatnych do dziedziny implementacji systemu ochrony.

Ze względu na ograniczone ramy niniejszej publikacji, w dalszej części rozdziału w skrócie przedstawione są tylko dwa pierwsze zagadnienia.

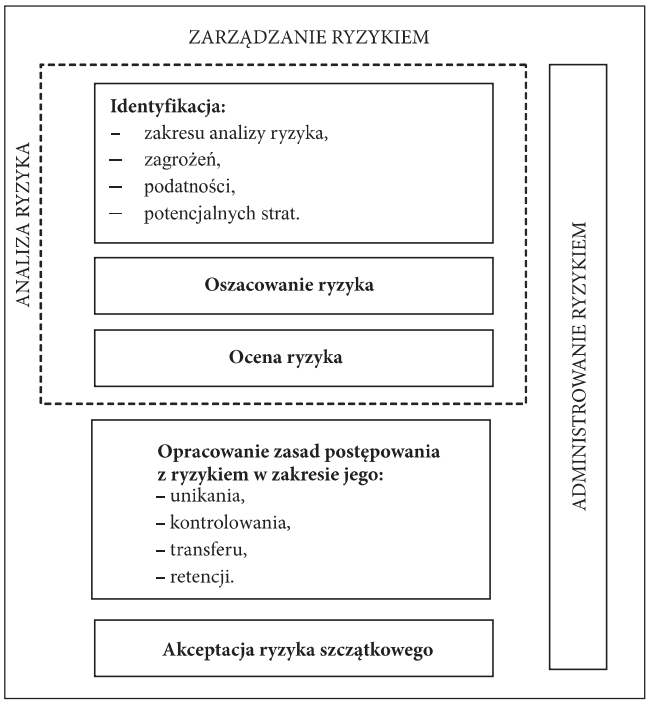
4.1. Zarządzanie ryzykiem

W tym artykule, gdzie rozważane są zagadnienia ochrony informacji, termin „ryzyko" oznacza miarę stopnia zagrożenia dla tajności, integralności i dostępności informacji wyrażoną jako złożenie prawdopodobieństwa (rozumianego również w sensie „możliwości") wystąpienia sytuacji stwarzającej takie zagrożenie i stopnia szkodliwości jej skutków (strat).

Na przestrzeni ostatnich 15 lat można było zaobserwować różne paradygmaty „postrzegania" działalności biznesowej. Lata 90. XX w. charakteryzuje postrzeganie jakości prowadzonej działalności biznesowej przez pryzmat jakości wytwarzanego i dostarczanego na rynek produktu (por. seria norm ISO/IEC 900x wydanych przed rokiem 2000). Przełom XX/XXI w. to postrzeganie jakości prowadzonej działalności biznesowej przez pryzmat jakość procesów wytwórczych (por. seria norm ISO/IEC 900x wydanych po roku 2000). Obecnie kształtuje się nowy paradygmat postrzegania „biznesu" – przez pryzmat ryzyka związanego z prowadzeniem działalności

biznesowej, w tym ryzyka związanego z obiegiem informacji i jej przetwarzaniem w systemach teleinformatycznych.

Zarządzanie ryzykiem [11] to systematyczne stosowanie polityki, procedur i praktyki zarządzania do zadań ustalania kontekstu ryzyka, jego identyfikowania, analizowania, wyznaczania, postępowania z ryzykiem oraz monitorowania i komunikowania ryzyka. Podstawowe elementy zarządzania ryzykiem ilustruje rysunek 3.



Rys. 3. Podstawowe elementy procesu zarządzania ryzykiem [1]

W praktyce stosowane są dwa podejścia do analizy ryzyka:

1. **Zasobowe** – identyfikowane są zasoby, które powinny być chronione; dla nich przeprowadza się analizę ryzyka. Sposób stosowany przy niewielkiej ilości zasobów, przy braku dobrze wyodrębnionych i nielicznych procesach[7].
2. **Procesowe** – identyfikowane są kluczowe i krytyczne procesy, dla nich przeprowadza się analizę ryzyka.

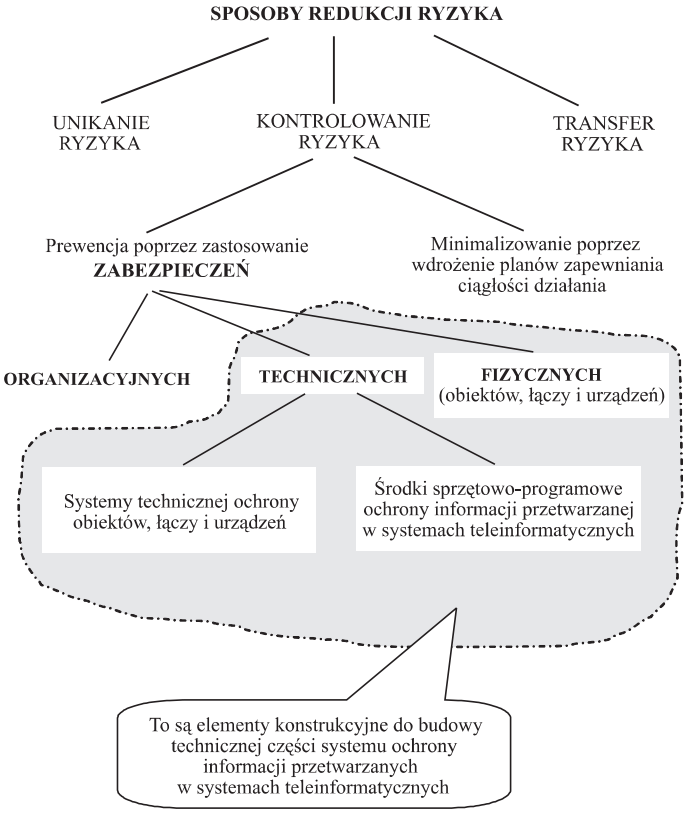
Do oszacowania ryzyka stosowane są dwie podstawowe metody:

1. Metoda **ilościowa**, gdzie operuje się miarą zdarzenia losowego – prawdopodobieństwem wyrażonym liczbą z przedziału [0, 1]. Metoda precyzyjna,

[7] Patrz *Szablon analizy i minimalizacji ryzyka* na www.ita.wat.edu.pl/Bezpieczeństwo.

ale w dziedzinie ochrony informacji rzadko stosowana ze względu na brak danych statystycznych.

2. Metoda **jakościowa**, gdzie operuje się opisowymi, arbitralnie dobieranymi miarami wyrażającymi możliwość zajścia zdarzenia losowego (np. możliwość zajścia zdarzenia WYSOKA, ŚREDNIA, NISKA). Metoda często stosowana w praktyce ochrony informacji. Wariantem analizy jakościowej jest oszacowanie częstościowe, gdzie podaje się możliwą liczbę badanych zdarzeń w pewnym okresie (np. roku).



Rys. 4. Sposoby redukcji ryzyka [1]

Podstawowe sposoby postępowania z ryzykiem są przedstawione na rysunku 4. Rysunek ten pokazuje też powiązania z różnymi typami zabezpieczeń, będącymi w tym kontekście środkami minimalizowania ryzyka. Dokładniejsze omówienie zagadnień zarządzania ryzykiem można znaleźć w [1].

4.2. Dokumentowanie systemu ochrony informacji

System ochrony informacji (w szczególności przetwarzanej w systemach komputerowych) może być w pełni udokumentowany przez następujące, opracowane i wdrożone dokumenty[8]:

- *Polityka bezpieczeństwa informacyjnego...* – zawiera najważniejsze, ogólne ustalenia najwyższego kierownictwa organizacji w zakresie ochrony informacji. Dokument ten powinien być **jawny** i dostępny wszystkim osobom, które zechcą się z nim zapoznać.
- *Plan bezpieczeństwa teleinformatycznego...* – zawiera szczegóły budowy systemu bezpieczeństwa teleinformatycznego[9]. Dokument ten powinien być **niejawny**, dostępny zgodnie z zasadą wiedzy niezbędnej.
- *Instrukcje bezpieczeństwa teleinformatycznego...* – zawierają zasady postępowania w zakresie bezpieczeństwa teleinformatycznego dla osób korzystających z systemów teleinformatycznych organizacji. Jest to dokument **do użytku wewnętrznego**, na jego podstawie prowadzone są szkolenia dla pracowników.
- *Plan zapewniania ciągłości działania...* – zawiera instrukcje i procedury postępowania w przypadku wystąpienia tzw. zdarzeń kryzysowych. Powinien to być dokument **do użytku wewnętrznego, podlegający specjalnej ochronie**.

„Wdrożone" oznacza, że dokumenty te są wprowadzone w organizacji odpowiednim zarządzeniem naczelnego kierownictwa oraz są wykonane odpowiednie czynności:

- **administracyjne**, jak np. szkolenia, zakupy czy zmiany w organizacji pracy;
- **techniczne**, jak np. instalacja sprzętu komputerowego i oprogramowania.

Spośród wymienionych, podstawowym dokumentem, którego znaczenie podkreślają różne normy i standardy oraz przepisy prawa (patrz np. *Ustawa* o *ochronie danych osobowych*), jest *Polityka bezpieczeństwa* (rys. 5). Dokument ten zawiera zapis **najważniejszych, ogólnych zamiarów działań najwyższego kierownictwa organizacji w zakresie bezpieczeństwa** informacji i jego **deklaracje** w zakresie zapewnienia odpowiedniego poziomu tego bezpieczeństwa w organizacji. Przeznaczony jest do **uzasadnienia zaufania** klientów i partnerów biznesowych do powierzenia swoich informacji tej organizacji oraz **stanowi podstawę do opracowania szczegółowych rozwiązań** organizacyjnych i technicznych w zakresie ochrony informacji. Dostępność takiego dokumentu w konkretnej organizacji:

---

[8] Dla audytora (często także dla biegłych sądowych i prokuratorów) to, co nie jest spisane, NIE ISTNIEJE!

[9] O ile *Polityka*… jest najczęściej kilkustronicowym dokumentem, to *Plan*… jest w praktyce zbiorem różnych dokumentów: dokumentacji powykonawczej sieci teleinformatycznej, sieci łączności i systemów alarmowych, regulaminów, schematów, procedur itp.

- świadczy o „należytej staranności" tej organizacji w zakresie ochrony informacji;
- stanowi podstawę zaufania potencjalnych klientów lub partnerów biznesowych do powierzenia swoich dóbr informacyjnych takiej organizacji;
- dla audytora stanowi dowód (audytowy), że koncepcja ochrony informacji jest przemyślana i spisana;
- dla inżynierów budujących system ochrony informacji zawiera podstawowe wytyczne (wymagania);
- dla pracowników uwikłanych w ochronę informacji stanowi podstawowy zbiór zasad pozwalających im na skuteczne pełnienie obowiązków służbowych;
- jest często wymagana przez przepisy prawa (np. *Ustawę o ochronie danych osobowych i stosowne rozporządzenie*).

5. Podsumowanie

Wysiłek administracji państwa w zakresie ochrony informacji najlepiej ilustrują dwa dokumenty: *Strategia* [4] i *Założenia* [5]. W [4] znajduje się rozdział 3.8 *Bezpieczeństwa informacyjne i telekomunikacyjne* (paragrafy 78-82[10]) oraz rozdział 4.3 *Podsystemy wykonawcze*, gdzie znajduje się paragraf 114 *Informatyzacja i telekomunikacja*. Podstawową wadą przywołanych zapisów, zdaniem piszącego te słowa, jest brak usystematyzowania problemów do rozwiązania oraz przesadne akcentowanie znaczenia bezpieczeństwa telekomunikacyjnego – oprócz tytułu, sformułowanie „bezpieczeństwo informacyjne" nigdzie w paragrafach 78-82 się nie pojawia. Obszerne omówienie *Strategii* można znaleźć np. w [2].

Drugi z przywołanych dokumentów [5] zawiera zarys podstaw, na których ma być budowany system ochrony „cyberprzestrzeni". Obecnie (listopad 2010) na etapie uzgodnień międzyresortowych znajduje się dokument *Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016*. Pomijając zasadniczą dla sprawy skutecznej ochrony ułomność definicji zamieszczonych na 6 stronie tego dokumentu (w tym kluczową definicję „cyberprzestrzeni"), w dokumencie proponuje się skoordynowanie przedsięwzięć natury legislacyjnej, organizacyjnej, edukacyjnej i technicznej obligatoryjnych dla organów władzy publicznej i operatorów infrastruktury krytycznej i dobrowolnych dla pozostałych podmiotów – użytkowników cyberprzestrzeni. Należy mieć nadzieję, że docelowa wersja ww. programu zostanie dobrze dopracowana, ponieważ w obecnej postaci, oprócz rozrostu biurokracji, nie rokuje innych „sukcesów".

[10] Godny uwagi jest zapis z paragrafu 79: *Priorytetem państwa będzie wspieranie narodowych programów i technologii informacyjnych*.

BIBLIOGRAFIA

1. K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, PWN, Warszawa 2008.
2. Z. Nowakowski, H. Szafran, R. Szafran, *Bezpieczeństwo w XXI wieku. Strategie bezpieczeństwa narodowego Polski i wybranych państw*, RS DRUK Drukarnia Wydawnictwo, Rzeszów 2009.
3. A.E. Patkowski, *Zagrożenia dla bezpieczeństwa informacji przetwarzanej w systemach teleinformatycznych. Wewnętrzne materiały szkoleniowe*, ITA WAT, Warszawa 2005.
4. *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2007.
5. *Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011. Założenia*, Warszawa, marzec 2009.
6. IEC 61508: *Functional Safety: Safety-Related Systems.*
7. PN-ISO/IEC-17799:2005: *Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji.*
8. PN-ISO/IEC 27001:2007: *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania.*
9. PN-ISO/IEC 27005:2010: *Technika Informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji.*
10. PN-ISO/IEC 15408-1:2002: *Technika informatyczna – Techniki zabezpieczeń – Kryteria oceny zabezpieczeń informatycznych* – Część 1: *Wprowadzenie i model ogólny.*
11. PN-ISO/IEC 15408-3:2002: *Technika informatyczna – Techniki zabezpieczeń – Kryteria oceny zabezpieczeń informatycznych* – Część 3: *Wymagania uzasadnienia zaufania do zabezpieczeń.*
12. PN-IEC 62198:2005: *Zarządzanie ryzykiem przedsięwzięcia – Wytyczne stosowania.*
13. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (DzU z dn. 21.05.07).
14. Komisja Wspólnot Europejskich, Bruksela, dnia 12.12.2006 KOM(2006) 786 wersja ostateczna: *Komunikat komisji w sprawie europejskiego programu ochrony infrastruktury krytycznej.*

Information – meaning and protection method in modern state. Technical perspective

Abstract. The paper includes a survey of issues connected to the meaning of information for functioning of a modern state, including issues related to proper protection of the information.