

Klasyfikacja informacji i danych prawnie chronionych oraz wymagania dotyczące środków informatycznych przeznaczonych do ich przechowywania i przetwarzania

Andrzej Adamczyk

ITTI Sp. z o. o.
e-mail: andrzej.adamczyk@itti.com.pl

Rafał Renk, Jakub Radziulis, prof. Witold Hołubowicz

Uniwersytet im. Adama Mickiewicza w Poznaniu
e-mail: rrenk@amu.edu.pl, radziuli@amu.edu.pl, holub@amu.edu.pl

Streszczenie

Na wstępie referatu zawarto krótkie wprowadzenie zawierające definicje i wyjaśnienia takich pojęć jak: dane, metadane, informacje, kontekst znaczeniowy, wiedza oraz określono cele ochrony informacji.

Następnie referat dokonuje przeglądu rodzajów informacji i danych prawnie chronionych, czyli takich, co do których zapisy o ochronie pojawiają się w aktach prawnych w Polsce. Dokonuje ich klasyfikacji w kontekście treści poszczególnych ustaw i rozporządzeń. Omówione zostały m.in. następujące kategorie danych i informacji: informacje niejawne (np. informacje zastrzeżone, poufne, tajne i ściśle tajne), dane osobowe, informacje stanowiące różnorodnego rodzaju tajemnice (np. tajemnicę państwową, służbową, pracodawcy, zawodową, przekazu i źródeł informacji, skarbową, lekarską, bankową, statystyczną, telekomunikacyjną i handlową).

Posługując się przedstawioną klasyfikacją danych i informacji prawnie chronionych, autorzy określają rolę tych elementów w kontekście formułowania podstawowych zasad ochrony w organizacji. Opis wykonany jest w kontekście założeń oraz

wymagań w odniesieniu do infrastruktury i systemów informatycznych służących przechowywaniu i przetwarzaniu tego rodzaju informacji.

Informacja o autorach

Andrzej Adameczyk w latach 1991-1993 studiował na Politechnice Poznańskiej na kierunku Telekomunikacja i Elektronika. W latach 1993-1996 kontynuował studia w EFP – Francusko-Polskiej Wyższej Szkole Technik Informatyczno-Komunikacyjnych w Poznaniu. W 1995 roku odbył półroczny staż w laboratorium LAAS-CNRS w Tuluzie we Francji. Stopień magistra inżyniera uzyskał w 1996 roku w dziedzinie systemów rozproszonych. Od 1996 roku pracował na stanowisku Kierownik Pracowni Systemów Informatycznych w Instytucie Technik Telekomunikacyjnych i Informatycznych (ITTI) w Poznaniu. W Zespole Systemów Informatycznych i Multimediów, pod kierownictwem prof. dr hab. inż. Czesława Jędrzejka, prowadził projekty w następujących dziedzinach: inżynieria oprogramowania, technologie inter- i intranetowe, aplikacje i systemy baz danych oraz technologia i metodyka zdalnego kształcenia multimedialnego. Koordynował projekty Piątego Programu Ramowego, programu Leonardo da Vinci i Phare. Przez rok kierował działaniami informatycznymi firmy ALMA S.A. na stanowisku Dyrektor Departamentu Systemów i Aplikacji. Obecnie w ITTI na stanowisku starszego konsultanta realizuje projekty związane z analizą, projektowaniem i budową systemów informatycznych oraz z zagadnieniami bezpieczeństwa informacji.

Rafał Renk jest absolwentem Akademii Techniczno-Rolniczej (ATR) w Bydgoszczy, którą ukończył w 1998 roku. W ATR pracował nad zagadnieniami związanymi z trójwymiarowymi światami wirtualnymi. Od 1998 roku jest pracownikiem ITTI, gdzie piastuje obecnie stanowisko dyrektora ds. rozwoju. Rafał Renk wykonywał oraz współkierował szeregiem projektów poruszających tematykę sieci telekomunikacyjnych w aspekcie technicznym i biznesowym oraz zagadnień informatycznych związanych z: inżynierią oprogramowania, technologiami internetowymi, aplikacjami i systemami baz danych oraz technologiami i metodykami zdalnego kształcenia multimedialnego wraz z systemami zdalnego nauczania oraz projektowania hurtowni danych. Projekty o tematyce telekomunikacyjnej dotyczyły zarówno rynku polskiego, jak i międzynarodowego, a ich tematyka obejmowała m.in. analizy rynkowe (w zakresie telefonii IP, transmisji danych itp.), tworzenie strategii budowy i rozbudowy sieci telekomunikacyjnych zarówno dostępowych jak i szkieletowych a także zagadnienia techniczne związane z VoIP, sieciami dostępowymi, sieciami szkieletowymi, protokołami i standardami technologii internetowych, strumieniowania, jakością usług w sieci IP oraz systemów zdalnego nauczania. Prace związane z systemami zdalnego nauczania obejmowały zagadnienia związane ze standaryzacją tego typu systemów oraz przeprowadzania i automatycznej oceny wyników egzaminów (wykorzystanie języka XML i ontologii). Rafał Renk jest również autorem bądź współautorem licznych publikacji i wystąpień na krajowych oraz zagranicznych konferencjach.

Jakub Radziulis jest absolwentem Akademii Techniczno-Rolniczej (ATR) w Bydgoszczy, którą ukończył w 2001 roku. W latach 2001-2003 był pracownikiem ITTI gdzie piastował stanowisko konsultanta. Od 2003 piastuje stanowisko asystenta na wydziale Fizyki UAM w Poznaniu w zakładzie Informatyki Stosowanej, pozostając jednocześnie w bliskiej współpracy z ITTI na stanowisku konsultanta. Na UAM Jakub Radziulis zajmuje się zagadnieniami dot. modelowania systemów informatycznych przy wykorzystaniu języka UML. Jako konsultant brał udział w projektach związanych z systemami informatycznymi, projektach telekomunikacyjnych związanych z sieciami IP oraz w projektach z zakresu bezpieczeństwa informacji. Projekty z zakresu bezpieczeństwa dotyczyły szerokiego spektrum aspektów takich, jak m.in. audyt bezpieczeństwa, analiza i ocena ryzyka, opracowanie procedur bezpieczeństwa, polityka bezpieczeństwa, opracowanie metod szkolenia jak i samych szkoleń. Projekty o tematyce telekomunikacyjnej dotyczyły wdrażania nowych usług multimedialnych opartych o wykorzystanie technologii VoIP oraz jakości usług w sieci IP. Prace związane z systemami informatycznymi obejmowały m.in. aplikacje zdalnego nauczania w tym zagadnienia tworzenia, rozbudowy, przygotowania materiałów autorskich. Jakub Radziulis brał także udział w pracach dotyczących analizy procesów, systemów informatycznych i usług. Zainteresowania autora dotyczą zagadnień bezpieczeństwa systemów teleinformatycznych oraz systemów telekomunikacyjnych.

Witold Hołubowicz jest absolwentem Wydziału Elektrycznego Politechniki Poznańskiej, gdzie uzyskał stopnie doktora i doktora habilitowanego. W latach 1987-89 był wykładowcą na Politechnice w Nowym Jorku, a w latach 1992-96 we Francusko-Polskiej Wyższej Szkole Nowych Technik Informatycznych i Komunikacyjnych (EFP) w Poznaniu. Od października 1996 r. jest profesorem na Wydziale Telekomunikacji i Elektrotechniki Akademii Techniczno-Rolniczej (ATR) w Bydgoszczy. Jest również profesorem i kierownikiem Zakładu Informatyki Stosowanej na Uniwersytecie A. Mickiewicza (od 2003 roku). Od 1996 r. jest także zawodowo związany z Instytutem Technik Telekomunikacyjnych i Informatycznych (ITTI) w Poznaniu, gdzie pełni obecnie funkcję prezesa zarządu. Jest również współtwórcą i przewodniczącym Komitetu Programowego Krajowej Konferencji Radiokomunikacji Ruchomej w Poznaniu (KKRR) w latach 1996-2000. Zainteresowania zawodowe Witolda Hołubowicza obejmują m.in. radiokomunikację (w tym technologie transmisji z poszerzonym widmem CDMA), aspekty techniczno-rynkowe sieci komunikacji ruchomej GSM i UMTS, aspekty usługowe sieci komórkowych i konwergentnych. Uczestniczył i kierował wieloma projektami naukowo-badawczymi i wdrożeniowymi, w tym również realizowanymi pod egidą Komisji Europejskiej. Witold Hołubowicz jest autorem ponad 100 publikacji zamieszczonych w czasopiśmie naukowych krajowych i zagranicznych oraz w materiałach konferencyjnych. Jest również współautorem 4 książek z zakresu łączności bezprzewodowej.

1.1. Wprowadzenie

Bezpieczeństwo informacyjne często odnosi się do zagadnień ochrony danych oraz ochrony informacji. Czy określenia te mogą być używane zamiennie? Czyżby ich sens był identyczny?

Na co dzień w pracy i w życiu prywatnym używamy wielu pojęć takich, jak: dane, informacje, kontekst, znaczenie, wiedza. Są to pojęcia których semantyka zmienia się w zależności od konkretnego przypadku, więc precyzyjna dyskusja wymaga ich ścisłego zdefiniowania. Taka systematyzacja pojęciowa jest konieczna, aby szczegółowo rozważać zagadnienia bezpieczeństwa informacyjnego. Poniżej omówione zostało znaczenie takich pojęć jak: dane, informacja, wiedza, mądrość, aby móc je rozróżnić.

1.2. Dane

Dane (ang. *data*) w ujęciu infologicznym Bo Sundgrena jest to wycinek rzeczywistości służący do opisu innego wycinka rzeczywistości. Dane mogą przyjmować różną postać: znaków, mowy, wykresów. Różne dane mogą przedstawiać tę samą informację. Dane są zatem pojęciem węższym od informacji, chociaż potocznie tych pojęć używamy zamiennie. [WIKI]

Układ danych przenoszący konkretną informację to komunikat. [WIKI]

Rozpatrując to zagadnienie bardziej szczegółowo dane to surowe, nie poddane analizie fakty, liczby i zdarzenia, z których można opracować informacje. Czyste, nie opracowane dane nie mają większego znaczenia praktycznego. Rozwój technologii i idąca w ślad za tym komputeryzacja przedsiębiorstw znacznie ułatwiają i przyspieszają proces zarządzania danymi. Z drugiej strony stanowią pokusę do gromadzenia zbyt wielu zbędnych danych.[HERACL]

Dane w systemie informatycznym to reprezentacja informacji zapisana w pewnym obszarze pamięci komputera. Dane mogą reprezentować pojedynczą informację np. imię lub nazwisko albo zespół powiązanych ze sobą informacji [WIEM]. Same dane jednak bez podania kontekstu ich wykorzystania niewiele znaczą dla użytkownika systemu informatycznego. Dopiero opisanie danych (określenie ich kontekstu) poprzez metadane nadaje znaczenie tym danym.

Jedną z najpopularniejszych definicji metadanych jest definicja określająca metadane jako „*dane o danych*” [KRMW98, Swet00]. Nie istnieje jednoznaczne rozróżnienie pomiędzy daną i metadaną. Metadane mogą stanowić dane dla kolejnych metadanych co prowadzi do budowy hierarchii metadanych (niekiedy tego rodzaju metadane określane są jako metametadane). Inną definicją metadanych jest definicja mówiąca, że metadane to: „*suma wszystkiego, co ktoś może powiedzieć o dowolnym obiekcie informacyjnym na dowolnym poziomie agregacji*” [Swet00]. Metadane wykorzystywane są w wielu dziedzinach m.in. w: zdalnym nauczaniu (w jego różnych aspektach m.in. opisie kursu, organizacji pytań itp.)¹, bibliotekach cyfrowych², sieci Internet³, systemach informacji przestrzennej GIS⁴, bazach chorób w medycynie, hurtowniach danych, wyszukiwarkach internetowych itp.

1.3. Informacja

W ujęciu infologicznym (Bo Sundgren 1973) informacja to treść komunikatu przekazywanego za pomocą danych. [WIKI]

Słowo „informacja” wywodzi się od łacińskiego *informare*, co znaczy „nadawać formę”. Jednym z nurtów związanych z informacją jest tzw. nurt „semantyczny” (semantic), koncentrujący

¹ np. specyfikacje konsorcjum IMS

² np. specyfikacja Dublin Core

³ specyfikacje grupy roboczej Semantic Web Activity w ramach organizacji W3C (m.in.: OWL, RDF)

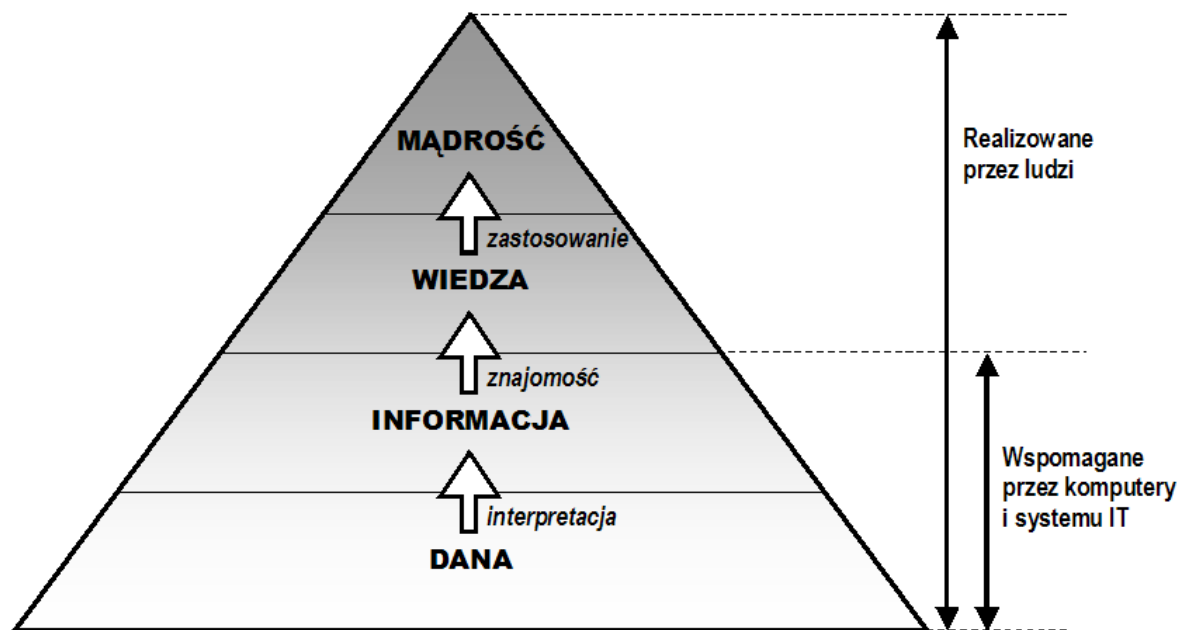
⁴ np. specyfikacje organizacji OpenGIS

się na znaczeniu informacji [3]. Zgodnie z nim, informacja dostarcza nowego punktu widzenia w interpretowaniu wydarzeń lub obiektów; sprawia, że to, co wcześniej było niewidoczne, zostało zauważone, rzuca nowe światło na pewne związki, których się nie spodziewaliśmy. Devenport i Prusak w podawanej przez siebie definicji traktują informację jako wiadomość, zwykle w formie dokumentu albo pod postacią komunikacji dźwiękowej lub wizualnej. Jak każda wiadomość, informacja ma nadawcę i odbiorcę, a jej podstawową rolą jest zmiana sposobu, w jaki odbiorca postrzega pewne rzeczy. Informacja ma przez to wpływ na jego osąd i zachowanie, co odróżnia ją od danych.

1.4. Wiedza

Wiedza jest pojęciem znacznie szerszym w stosunku do danych i informacji. Ma ona nadrzędną pozycję w stosunku do danych jak i informacji, choć na nich bazuje. Dane definiuje się jako niepołączone ze sobą fakty. Poprzez informację rozumiemy te dane, które zostały poddane kategoryzacji i klasyfikacji lub w inny sposób zostały uporządkowane. Natomiast wiedza oznacza uporządkowane i „oczyszczone” informacje. Powstaje ona dopiero po wyciągnięciu wniosków z dostępnych danych i informacji. Posiadanie bogatej wiedzy na dany temat prowadzi zaś do mądrości. Mądrość oznacza więc użycie wiedzy w praktyce.

Na rysunku Rys. 1 ukazano drogę od danych do mądrości.



Rys. 1. Wiedza a dane, informacje i mądrość [HERACL]

2. Prawna ochrona informacji i danych

Zatem czy otaczamy ochroną informację, czy raczej dane, a może wiedzę? W kontekście definicji tych pojęć należy stwierdzić, że chronić można, a nawet należy zarówno informację – poprzez działania na poziomie znaczeniowym – jak i dane, których interpretacja może prowadzić do pozyskania informacji. Mimo, że znaczenie obu terminów jest różne stanowią one wspólną wartość – zasób organizacji, tylko na różnych poziomach semantycznych.

Ochrona danych aby chronić informację, która z nich wynika. Ochrona zaś informacji podobnie jak zasobów fizycznych polega na zapewnieniu zgodności pomiędzy ich faktycznymi własnościami, a własnościami pożądanymi im przypisanymi. Do takich własności można zliczyć:

- dostępność,
- integralność,
- poufność.

Własności te wydają się niekiedy sprzeczne, jak np. zagwarantowanie „dostępności” i „poufności” określonej informacji. Kiedy jednak zdefiniujemy dla kogo informacja powinna być dostępna, a dla kogo niedostępna, zauważymy, że sprzeczności w tym stwierdzeniu być wcale nie musi. Przykładem takiej pozornej sprzeczności są ustawa o dostępie do informacji publicznej oraz ustawa o ochronie informacji niejawnych.

Jednym z aspektów ochrony informacji jest ochrona tajemnic. Dotyczy ona jedynie ochrony własności poufności informacji. Dowodzi tego definicja jaką podaje słownik języka polskiego. Według niego tajemnica to: ‘wiadomość, sprawa, fakt, których nie powinno się rozgłaszać, ujawniać ogółowi; sekret’. Mimo, że ochrona tajemnic to tylko jeden z aspektów ochrony informacji, akty prawne wyraźnie faworyzują ten rodzaj ochrony. Nie oznacza to, że nie istnieją wyjątki od tej reguły. Takim wyjątkiem może być ustawa o dostępie do informacji publicznej. Ustawa ta określa zasady ochrony dostępności do określonego rodzaju informacji.

Skupmy się jednak na tajemnicy. Prawodawstwo polskie odnosi się do wielu różnych rodzajów tajemnic. Trzeba jednak zaznaczyć, że mimo, że się do nich odnosi, to jednak często nie definiuje ich w sposób precyzyjny. W miarę jasna jest też definicja informacji niejawnych oraz danych osobowych, choć już interpretacja pojęcia zbiorów danych osobowych wzbudza liczne kontrowersje.

Jednak wydaje się, że jasność definicji tu się kończy zawartych w prawie. Istnieje wiele pojęć np. tajemnica przedsiębiorcy, tajemnica przedsiębiorstwa, tajemnica handlowa, których definicje jeżeli w ogóle istnieją nie są określają ich jednoznacznie. Taki stan rzeczy wymaga próby zebrania różnego rodzaju tajemnic prawnie chronionych i stworzenia ich systematyki.

3. Przegląd rodzajów informacji i danych prawnie chronionych

W niniejszym rozdziale zaproponowana została klasyfikacja informacji i danych prawnie chronionych. Klasyfikacji tej dokonano w oparciu o ponad 60 aktów prawnych. Informacje i dane prawnie chronione sklasyfikowano według następujących kryteriów:

- skutków naruszenia zasad ochrony np. utraty poufności wrażliwych danych,
- właściciela informacji chronionych,
- przedmiotu, który opisują lub którego dotyczą dane.

W kolejnych podrozdziałach pogrupowano tajemnicę w oparciu o wyżej wymienione kryteria podziału.

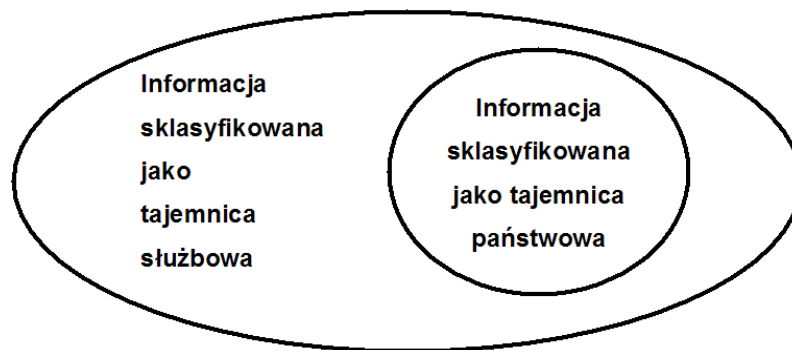
3.1. Klasyfikacja informacji chronionych według skutków naruszenia zasad ochrony

Jedna z najczęściej cytowanych ustaw – ustawa o ochronie informacji niejawnych próbuje zdefiniować rodzaje informacji w oparciu o skutek, jaki może przynieść ich odtajnienie (utrata ich poufności). W tym kontekście dokonuje podziału informacji niejawnych na informacje stanowiące tajemnicę służbową oraz tajemnicę państwową.

Tajemnica służbowa dotyczy informacji niejawnnej nie będącej tajemnicą państwową, uzyskaną w związku z czynnościami służbowymi albo wykonywaniem prac zleconych, której nieuprawnione ujawnienie mogłoby narazić na szkodę interes państwa, interes publiczny lub prawnie chroniony interes obywateli albo jednostki organizacyjnej (art. 2 pkt 2).

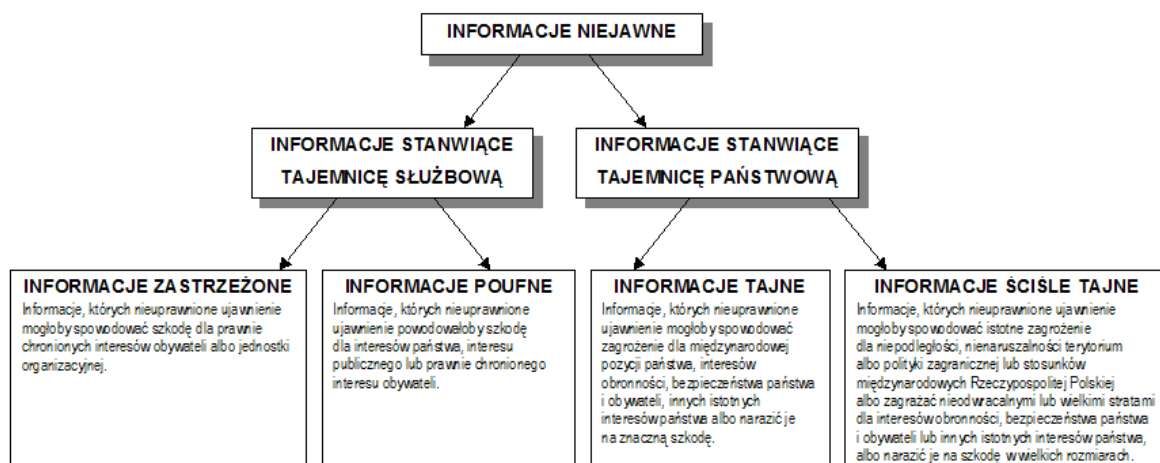
Tajemnica państwowa dotyczy informacji niejawnnej, której nieuprawnione ujawnienie może spowodować istotne zagrożenie dla podstawowych interesów Rzeczypospolitej Polskiej, a w szczególności dla niepodległości lub nienaruszalności terytorium, interesów obronności, bezpieczeństwa państwa i obywateli, albo narazić te interesy na co najmniej znaczną szkodę.

Praktycznie rzecz biorąc informacje sklasyfikowane jako tajemnica państwowa spełniają też kryteria klasyfikacji informacji służbowych. Dlatego stanowią ich podzbiór jak to zostało przedstawione na rysunku Rys. 2.



Rys. 2. Zależność pomiędzy informacjami określonymi jako tajemnica służbowa i państwowa

Ustawa idzie o krok dalej i definiuje informacje zastrzeżone oraz poufne, które objęte są tajemnicą służbową, zaś wśród informacji objętych tajemnicą państwową wyróżnia informacje tajne i ściśle tajne. Wymienione rodzaje informacji określonych przez ustawę wraz z definicjami przedstawia rysunek Rys. 3.



Rys. 3. Podział informacji według ustawy o ochronie informacji niejawnnych

Do tak zdefiniowanych informacji niejawnnych odnosi się wiele innych ustaw. Wymieniono je podkreślając ustawy odnoszące się do tajemnic państwowych (pozostałe odnoszą się do tajemnic służbowych):

- Ustawa o służbie wojskowej żołnierzy zawodowych art. 46,

- Ustawa o wynalazczości art. 59,
- Ustawa o państwowej Inspekcji pracy art. 24,
- Ustawa o społecznej inspekcji pracy art. 8,
- Prawo o ustroju sądów powszechnych art. 67,
- Ustawa o Rzeczniku Praw Obywatelskich art. 4,
- Ustawa o pracownikach samorządowych art. 15,
- Ustawa o Urzędzie Ochrony Państwa art. 17,
- Ustawa o Policji art. 27,
- Prawo o notariacie art. 15 i 18,
- Ustawa o Państwowej Straży Pożarnej art. 30,
- Ustawa o Służbie Więziennej art. 61,
- Ustawa o komercjalizacji i prywatyzacji przedsiębiorstw państwowych art. 62,
- Prawo energetyczne art. 28,
- Ustawa o świadku koronnym art. 23,
- Ustawa o komornikach sądowych i egzekucji art. 14 i 20,
- Ustawa o Biurze Ochrony Rządu art. 22,
- Ustawa o strażach gminnych art. 27,
- Ustawa o Narodowym Banku Polskim art. 55,
- Ustawa o Rzeczniku Praw Dziecka art. 5,
- Prawo własności przemysłowej Tyt. II dział II Roz. 4 oraz art. 270,
- Ustawa o prokuraturze art. 48,
- Ustawa o służbie medycyny pracy art. 11 ust. 3,
- Ustawa o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne art. 8 ust. 5 i art. 10 ust. 3,
- Prawo o ustroju sądów wojskowych art. 28 § 5,
- Ustawa o ogólnym bezpieczeństwie produktów art. 18 ust. 5,
- Ustawa o warunkach dopuszczalności i nadzorowaniu pomocy publicznej dla przedsiębiorców art. 38,
- Ustawa o przeciwdziałaniu wprowadzania do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł art. 6,
- Ustawa o Najwyższej Izbie Kontroli art. 73,
- Ustawa o Inspekcji Handlowej art. 16.

3.2. Klasyfikacja informacji chronionych według właściciela informacji

Przykładem mogą być tajemnice zawodowe. Tajemnice zawodowe często są skierowane do organizacji z określonego sektora gospodarczego. Wśród takich tajemnic wyróżniamy:

- tajemnica publicznego obrotu papierami wartościowymi inaczej zwana giełdową lub maklerską którą objęte są informacje związane z publicznym obrotem, jakich ujawnie-

nie mogłoby naruszyć interes uczestników tego obrotu na podstawie ustawy prawo o publicznym obrocie papierami wartościowymi art. 159 i następane,

- tajemnicę ubezpieczeniową na podstawie ustawy o działalności ubezpieczeniowej art. 9 i 37n,
- tajemnicę przekazu informacji na podstawie ustawy o łączności art. 29,
- tajemnicę bankową, którą objęte są wszystkie wiadomości dotyczące czynności bankowych i osób będących stroną umowy, uzyskane w czasie negocjacji oraz związane z zawarciem umowy z bankiem i jej realizacją, z wyjątkiem wiadomości, bez których ujawnienia nie jest możliwe należyte wykonanie zawartej przez bank umowy oraz dotyczące osób, które, nie będąc stroną umowy, dokonały czynności pozostających w związku z zawarciem takiej umowy na podstawie ustawy prawo bankowe art. 104 i następane oraz ustawy o Narodowym Banku Polskim art. 55,
- tajemnicę telekomunikacyjną na podstawie ustawy prawo telekomunikacyjne Roz. 5,
- tajemnicę lekarską, którą objęte są osoby wykonujące czynności lekarskie w zakresie zachowania w tajemnicy wszystkiego, o czym powezmą wiadomość w związku z wykonywaniem tych czynności, ponadto dane osobowe dotyczące dawcy i biorcy przeszczepu, na podstawie ustawy o zawodzie lekarza art. 40, ustawy o zwalczaniu chorób zakaźnych art. 6 ust. 1, ustawy o zawodach pielęgniarki i położnej art. 21, ustawy o ochronie zdrowia psychicznego Rozdz. VI i XVI, ustawy o służbie medycyny pracy art. 3 ust. 3 i art. 11 ust. 3, ustawy o pobieraniu i przeszczepianiu komórek, tkanek i narządów art. 12, ustawy o publicznej służbie krwi art. 13, ustawy o zakładach opieki zdrowotnej art. 18 oraz Kodeksu karnego art. 266 § 1,
- tajemnicę dziennikarską lub prasową, którą objęte są dane umożliwiające identyfikację autora materiału prasowego, listu do redakcji lub innego materiału o tym charakterze, jak również innych osób udzielających informacji opublikowanych albo przekazanych do opublikowania, jeżeli osoby te zastrzegły nieujawnienie powyższych danych oraz wszelkie informacje, których ujawnienie mogłoby naruszać chronione prawem interesy osób trzecich, na podstawie ustawy prawo prasowe art. 10 i art. 16 ust. 1 oraz Kodeksu karny art. 240,
- tajemnicą notarialną,
- tajemnicę adwokacką, którą objęte są wszelkie fakty, o których adwokat dowiedział się w związku z udzielaniem pomocy prawnej, na podstawie ustawy prawo o adwokaturze art. 3 i 6.

Wśród tajemnic zawodowych obowiązujących szeroko pojęty krąg odbiorców wyróżnić możemy:

- tajemnicę pracodawcy na podstawie Kodeksu pracy art. 100,
- tajemnicę skarbową, którą objęte są indywidualne dane zawarte w deklaracji oraz innych dokumentach składanych przez podatników, płatników lub inkasentów na podstawie ustawy o kontroli skarbowej art. 34 oraz ordynacji podatkowej Dział VII,
- tajemnicę przedsiębiorstwa lub przedsiębiorcy którą objęte są nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności na podstawie ustawy o zwalczaniu nieuczciwej konkurencji art. 11 ust.4 oraz ustawy o ochronie konkurencji i konsumentów art. 63,

- tajemnicę źródeł informacji na podstawie ustawy o prawie autorskim i prawach pokrewnych art. 84,
- tajemnicę statystyczną na podstawie ustawy o statystyce publicznej art. 12 oraz ustawy o narodowym spisie powszechnym ludności i mieszkań w 2002 r. art. 10,
- tajemnicę handlową na podstawie np. ustawy prawo energetyczne art. 28,
- pozostałe tajemnice zawodowe na podstawie ustawy prawo prasowe art. 15 ust. 2, ustawy o działalności ubezpieczeniowej art. 9 i 37n, ustawy prawo o notariacie art. 15 i 18, ustawy o izbach aptekarskich art. 21, ustawy z o biegłych rewidentach i ich samorządzie art. 4a, ustawy o doradztwie podatkowym art. 37, ustawy o funduszach inwestycyjnych art. 45, ustawy o organizacji i funkcjonowaniu funduszy emerytalnych art. 49, ustawy o komornikach sądowych i egzekucji art. 14 i 20, ustawy o giełdach towarowych Roz. 8, ustawy o rzecznikach patentowych art. 14, ustawy o służbie cywilnej art. 67, ustawy o sejmowej komisji śledczej art. 16, ustawy o wykonywaniu mandatu posła i senatora art. 19 oraz ustawy o gospodarce nieruchomościami art. 175.

Ponadto w ramach klasyfikacji zawartej w niniejszym rozdziale należy wspomnieć ochronę dostępności danych przetwarzanych w instytucjach administracji publicznej na podstawie ustawy o dostępie do informacji publicznej. Ten rodzaj ochrony również dotyczy informacji określonych w oparciu o ich właściciela. Prawo do informacji w zakresie określonym ustawą obejmuje m.in. uprawnienia do niezwłocznego uzyskania informacji publicznej, wglądu do dokumentów urzędowych, dostępu do posiedzeń kolegialnych organów władzy publicznej pochodzących z powszechnych wyborów.

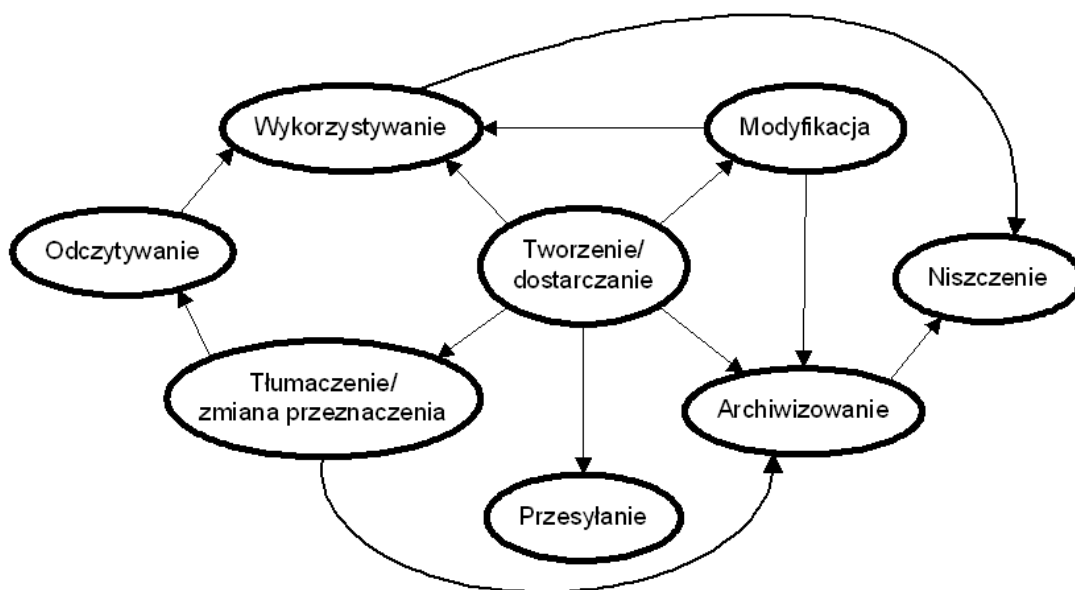
3.3. Klasyfikacja informacji chronionych według przedmiotu chronionego

Wśród danych i informacji prawnie chronionych określonych w oparciu o przedmiot ochrony wskazać można dane osobowe. Ustawa o ochronie danych osobowych definiuje je, jako: „wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej”.

4. Wymagania wynikające z regulacji prawnych

Zabezpieczenie dostępności i integralności informacji jest realizowane poprzez zapewnienie ich bezpieczeństwa (ang. *safety*). Natomiast poufność informacji dotyczy obszaru ochrony informacji (ang. *security*).

Zabezpieczenie informacji wiąże się z uzyskaniem odpowiedniego stanu odporności (niskiej podatności) informacji na wszelakie zagrożenia. Kierując się zasadą, że system jest tak odporny jak najmniej odporny jego element należy zwrócić uwagę na wszystkie procesy w całym cyklu życia informacji od jej powstania do zniszczenia. Procesy te przedstawia rysunek Rys. 4.



Rys. 4. Procesy przetwarzania informacji

Na każdym etapie „życia” bezpieczeństwa informacji zależy od bezpieczeństwa narzędzi oraz działań osób, które są zaangażowane w realizację poszczególnych procesów. Podatność tych osób i narzędzi na zagrożenia stanowi także zagrożenie dla samych informacji, bo może prowadzić do niepożądanych skutków. Oto typowe błędy prowadzące w konsekwencji do wystąpienia incydentów naruszenia bezpieczeństwa informacji na poszczególnych etapach „życia” informacji:

- tworzenie/dostarczanie – brak określenia listy odbiorców i klauzuli poufności,
- przesyłanie – brak szyfrowania kanału transmisyjnego,
- tłumaczenie/zmiana przeznaczenia – przekłamanie sensu informacji na skutek niezrozumienia przez tłumacza (naruszenie integralności informacji),
- odczytywanie – stworzenie kopii dokumentu z informacją dla własnej wygody, co zwiększa szansę na naruszenie jej poufności,
- wykorzystywanie – nielegalne wykorzystanie informacji do własnych celów np. utajonych informacji w trakcie procedury przetargowej,
- modyfikacja – nieautoryzowana modyfikacja w celu zafałszowania danych w wyniku wejścia nieuprawnionej osoby w posiadanie hasła zabezpieczającego przed modyfikacją,
- archiwizowanie – niewystarczające zabezpieczenie pomieszczeń archiwum lub trzymanie poufnych informacji w postaci kopii poza archiwum,
- niszczenie – brak procedury niszczenia wrażliwych danych i wyrzucanie dokumentów do śmietnika.

Zapewnienie bezpieczeństwa danym i informacją w całym cyklu ich życia wymaga dostosowania wielu procesów w organizacji. Procesy te obrazuje schemat na rysunku Rys. 3.



Rys. 5. Różnorakie aspekty utrzymania zgodności z przepisami

W zakresie zapewnienia odporności systemu, kryteria TCSEC [TCSEC] rozróżniają następujące elementy i wymagania:

- właściwa architektura systemu (np. ukrywanie przetwarzanych danych, wydzielenie jądra TCB),
- spójność systemu,
- testy zabezpieczeń,
- weryfikacja modelu systemu,
- analiza ukrytych kanałów,
- wiarygodne zarządzanie (np. rozdzielenie ról administratora),
- wiarygodny powrót do normalnego stanu,
- wiarygodna dystrybucja,
- zarządzanie konfiguracją.

5. Środki techniczne i organizacyjne bezpieczeństwa danych

W niniejszym rozdziale opisano wybrane środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i „rozliczalności” przetwarzanych danych. Na podstawie wymienionych informacji można stworzyć i wdrożyć instrukcje określające sposób zarządzania sys-

temem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem bezpieczeństwa informacji.

W dziedzinie doboru środków technicznych i organizacyjnych zapewnienia bezpieczeństwa danych i informacji należy kierować się określonymi zasadami. Warunkiem skutecznego funkcjonowania systemu ochrony informacji niejawnych jest stosowanie następujących zasad:

- zasada ograniczonego dostępu: informacje niejawne mogą być udostępnione wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy na zajmowanym stanowisku (tzw. zasada „need-to-know”). Stosowanie tej zasady ma zapewnić, że dostęp do informacji niejawnych jest determinowany zakresem obowiązków danego pracownika, co ogranicza do minimum liczbę osób, które zapoznają się z poszczególnymi informacjami;
- zasada udostępniania informacji niejawnych wyłącznie osobom gwarantującym ich ochronę przed nieuprawnionym ujawnieniem: warunkiem wykonywania obowiązków związanych z dostępem do informacji niejawnych jest uzyskanie odpowiedniego poświadczenia bezpieczeństwa (z wyjątkami określonymi w ustawie) oraz odbycie przeszkolenia w zakresie ochrony informacji niejawnych. Ma to zapewnić, że dostęp do informacji niejawnych uzyskują wyłącznie osoby dające rękojmię zachowania tajemnicy i znające zasady postępowania oraz odpowiedzialności karnej, dyscyplinarnej i służbowej za naruszenie przepisów w zakresie ochrony informacji;
- zasada podporządkowania środków ochrony klauzuli informacji: stosowane – w oparciu o przepisy ustawy oraz wydanych do niej aktów wykonawczych – środki ochrony fizycznej i zasady bezpieczeństwa obiegu dokumentów, muszą być adekwatne do klauzuli tajności wytwarzanych, przetwarzanych, przekazywanych i przechowywanych informacji. Dzięki temu dokumenty i materiały zawierające informacje niejawne tej samej wagi są we wszystkich instytucjach chronione w podobny sposób;
- zasada dostosowania zakresu środków ochrony fizycznej do uwarunkowań i specyfiki danej instytucji: zgodnie z ustawą zakres stosowania środków ochrony fizycznej musi jednocześnie:
 - odpowiadać klauzuli tajności i ilości informacji niejawnych (zasada podporządkowania środków ochrony klauzuli informacji) oraz poziomowi dostępu do takich informacji zatrudnionych osób,
 - uwzględniać wskazania służb ochrony państwa dotyczące w szczególności ochrony przed zagrożeniami ze strony obcych służb specjalnych.

Zasada ta uzupełnia poprzednią, stwarzając możliwość dostosowania zakresu i rodzaju środków ochrony do faktycznie występujących zagrożeń, w oparciu o fachową ocenę uprawnionych funkcjonariuszy służb ochrony państwa;

- zasada kontroli wytwórcy nad sposobem ochrony informacji: osoba, która jest upoważniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału (wytwórca), ma prawo do przyznania klauzuli tajności, która jednoznacznie określa środki ochrony danej informacji. Bez zgody tej osoby lub jej przełożonego klauzula tajności nie może być obniżona ani zniesiona. Celem takiego rozwiązania jest zapewnienie jednolitego sposobu ochrony informacji przez wszystkich odbiorców dokumentu lub materiału, zgodnego z dokonaną przez wytwórcę oceną zakresu szkód, które mogłyby za sobą pociągnąć jego nieuprawnione ujawnienie;
- zakaz zaniżania lub zawyżania klauzuli tajności: celem tej zasady jest stosowanie środków ochrony adekwatnych do wagi danej informacji, a w konsekwencji uniknięcie ponoszenia zbędnych kosztów związanych z zawyżaniem klauzuli tajności oraz koncen-

tracja środków na ochronie informacji wymagających specjalnych środków bezpieczeństwa;.

5.1. Środki organizacyjne

Wśród środków organizacyjnych zapewnienia bezpieczeństwa danych i informacji należy wymienić następujące zalecenia.

1. Dostęp do danych osobowych mogą mieć tylko i wyłącznie pracownicy posiadający pisemne, imienne upoważnienia podpisane przez Administratora Danych Osobowych.
2. Każdy z pracowników powinien zachować szczególną ostrożność przy przetwarzaniu, przenoszeniu wszelkich danych osobowych.
3. Należy chronić dane przed wszelkim dostępem do nich osób nieupoważnionych.
4. Pomieszczenia w których są przetwarzane dane osobowe muszą być zamykane na klucz.
5. Dostęp do kluczy powinni posiadać tylko upoważnieni pracownicy.
6. Dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy urzędu. W wypadku gdy jest wymagany poza godzinami pracy – możliwy jest tylko na podstawie pisemnego zezwolenia administratora danych osobowych.
7. Dostęp do pomieszczeń w których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy urzędu.
8. W przypadku pomieszczeń do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach TYLKO w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności.
9. Szafy w których przechowywane są dane osobowe muszą być zamykane na klucz.
10. Klucze do tych szaf powinni posiadać tylko upoważnieni pracownicy.
11. Szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych a następnie powinny być zamykane.
12. Dane osobowe w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych a następnie muszą być chowane do szaf.

5.2. Środki techniczne

Wśród środków technicznych zapewnienia bezpieczeństwa danych i informacji należy wymienić następujące zalecenia.

1. Dostęp do komputerów na których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy urzędu.
2. Stacje komputerowe na których przetwarzane są dane osobowe powinny mieć tak ustawione monitory aby osoby nieupoważnione nie miały wglądu w dane.
3. Każdy plik w którym są zawarte dane osobowe powinien być zabezpieczony hasłem jeśli nie jest to przetwarzanie danych w systemie informatycznym.
4. Po zakończeniu pracy komputery przenośne (np. typu notebook) zawierające dane osobowe powinny być zabezpieczone w zamykanych na klucz szafach.
5. Komputerów przenośnych (np. typu notebook) zawierających dane osobowe nie należy wносить poza budynek.
6. W wypadku potrzeby wyniesienia komputera przenośnego (np. typu notebook) zawierającego dane osobowe, wcześniej należy te dane przenieść na komputer stacjonarny w miejscu pracy.
7. Nie należy udostępniać osobom nieupoważnionym tych komputerów.
8. W przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami należy dokonać tego z zachowaniem szczególnej ostrożności.

9. Nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie) aby nie zostały na nich dane osobowe.
10. W wypadku niemożliwości skasowania danych z nośnika (płyta CD-ROM) należy taką płytę zniszczyć fizycznie.
11. W przypadku wykorzystania do przenoszenia dysków, dane należy kasować z tych dysków.
12. Niezabezpieczonych danych osobowych nie należy przysyłać drogą elektroniczną.
13. Sieć komputerowa powinna być zabezpieczona przed wszelkim dostępem z zewnątrz. Do zabezpieczenia sieci należy stosować:
 - a) firewall
 - b) adresowanie stacji roboczych tylko adresami prywatnymi, nierutowalnymi,
 - c) systemy wykrywania włamań IDS,
 - d) logowanie wszelkich zdarzeń w dziennikach systemowych na serwerach,
 - e) systemy antywirusowe,
 - f) zabezpieczenia skrzynek poczty elektronicznej hasłami „trudnymi” (8 znaków w tym litery, cyfry, znaki dodatkowe),
 - g) zabezpieczenie przed dostępem na zewnątrz ze stacji roboczych do innych usług niż WWW,
 - h) dostęp do poczty elektronicznej tylko na serwerach autoryzowanych przez urząd,
 - i) zabezpieczenia stacji roboczych poprzez hasła na BIOS, w systemach MS Windows 2000 i XP poprzez użytkowników i hasła,

Należy nadmienić, że wymienione środki są przykładowe i ich dobór jest bardzo zależny od wykorzystywanych architektur, sieci, technologii i technik przetwarzania danych.

6. Wnioski

W artykule dokonano próby klasyfikacji informacji i danych prawnie chronionych w Polsce oraz zaproponowano zestaw wymagań i zasad stosowania środków informatycznych przeznaczonych do ich przetwarzania oraz przechowywania. Ze względu na rozległość tematu w wielu miejscach ograniczono się do przykładów.

Bezpieczeństwo często jest definiowane jako brak niebezpieczeństwa. Można znaleźć tu analogię do zdrowia. Obowiązująca od wieków średnich definicja zdrowia, jako brak choroby jest dobrym przykładem słuszności takiego podejścia. Jednak Od lat 50-tych XX w. z inicjatywy Światowej Organizacji Zdrowia (ang. *World Health Organisation*) zwiększono wymogi, które należy spełnić, aby organizm nazwać zdrowym. Od tego czasu zdrowie definiuje się jako dobrostan organizmu, a więc nie tylko w wykorzystując relację negatywną. Można znaleźć podobny trend w dziedzinie bezpieczeństwa. Obecnie bezpieczeństwo nie polega tylko na uodpornianiu się na zagrożenia oraz niwelowania skutków ich realizacji. Dziś aby realizować politykę bezpieczeństwa należy stosować środki, które mają zapewnić sprawne i wydajne funkcjonowanie systemu bezpieczeństwa. Do takich środków należą działania w kierunku zapewnienia legalności, czyli zgodności z prawem oraz ogólnie obowiązującymi standardami. Dlatego stosowanie takich środków jak wdrażanie tajnych kancelarii i stref ochrony danych jest nie tylko potrzebne, aby nie narazić się na kary wynikające z nieprzestrzegania prawa, lecz jest niezbędne, by aktywnie wzmacniać odporność aby zagwarantować postęp w kierunku sprawnie i bezpiecznie funkcjonujących organizacji.

7. Bibliografia

- [HERACL] Loizos Heracleous, Better than the Rest: Making Europe the Leader in the Next Wave of Innovation and Performance, „Long Range Planning”, February 1998

- [WIEM] Internetowy portal wiedzy WIEM, <http://portalwiedzy.onet.pl/>
- [WIKI] Wolna encyklopedia Wikipedia, <http://pl.wikipedia.org/>
- [TCSEC] Trusted Computer Evaluation Criteria, Department of Defence Standard, USA, 1985
- [TAJZAW] Tajemnice zawodowe, http://www.t-j.cad.pl/index_pliki/tajemnice_zawodowe.htm