ACTA UNIVERSITATIS NICOLAI COPERNICI

DOI: http://dx.doi.org/10.12775/AUNC_ZARZ.2015.024 ZARZĄDZANIE XLII – NR 2 (2015)

Pierwsza wersja złożona 30.05.2015 ISSN 1689-8966
Ostatnia wersja zaakceptowana 24.09.2015

Dariusz Ceglarek[*]

PROCEDURY I NARZĘDZIA INFORMATYCZNE SŁUŻĄCE DO OCHRONY WŁASNOŚCI INTELEKTUALNEJ ORGANIZACJI OPARTEJ NA WIEDZY

Zarys treści: Artykuł omawia problematykę zarządzania wiedzą, w tym w szczególności wiedzą chronioną. Podejmuje problematykę metod ochrony własności intelektualnej oraz sposobu wyceny kosztów spowodowanych naruszeniami organizacyjnych zasobów własności intelektualnej. Artykuł przedstawia kategorie systemów informatycznych i stosowanych w nich mechanizmów ochrony kapitału intelektualnego, które zajmują się prawidłowym obiegiem informacyjnym, monitorowaniem informacji wchodzącej i wychodzącej z organizacji, a także skutecznym zabezpieczaniem informacji w formie elektronicznej. W artykule przedstawiono cechy system służący ochronie własności intelektualnej przechowywanej w publicznie dostępnych dokumentach tekstowych.

Słowa kluczowe: ochrona własności intelektualnej, kapitał intelektualny, systemy informatyczne.

Klasyfikacja JEL: M15; D23.

[*] Adres do korespondencji: Dariusz Ceglarek, Wyższa Szkoła Bankowa w Poznaniu, Wydział Finansów i Bankowości, Instytut Nauk Ekonomicznych, al. Niepodległości 2, 61-874 Poznań, e-mail: dariusz.ceglarek@wsb.poznan.pl.

WSTĘP

Zmiany zachodzące w organizacjach i ich otoczeniu wpływają na ewolucję poglądów na temat głównych czynników ich sukcesu i budowania trwałej przewagi konkurencyjnej na rynku. Organizacje skłaniają się do stosowania bardziej wyrafinowanych strategii i metod zarządzania, a także posiadania odpowiednich oraz unikatowych umiejętności i kompetencji. Proces globalizacji gospodarki, postęp technologiczny, szybki przepływ informacji itd. sprawiają, iż firmy konkurencyjne są często do siebie podobne w zakresie wykorzystywanych zasobów, współpracy z dostawcami, sposobów oddziaływania na klientów itd. Okazuje się, że tradycyjne źródła sukcesu, tj. produkt, proces technologiczny, dostęp do zasobów finansowych, tracą nieco na znaczeniu na rzecz niematerialnych zasobów przedsiębiorstwa, które stają się decydującymi z punktu widzenia konkurencyjności. Cechami decydującymi o sukcesie i uzyskaniu przewagi konkurencyjnej jest umiejętne przeprowadzenie procesów identyfikacji wiedzy oraz jej tworzenia i rozwijania w połączeniu z rozwijaniem kluczowych kompetencji oraz wykorzystanie wiedzy w praktyce. Zasoby informacyjne tworzące kapitał intelektualny, należy tak kształtować, aby w zwiększyć wartość rynkową przedsiębiorstwa, zdobyć przewagę konkurencyjną na rynku oraz utrzymać jak najlepsze relacje z klientami [Sroka, 2007].

Czynnikami, które stymulują powstawanie kapitału intelektualnego są czynności intelektualne związane z organizacyjnym nabywaniem wiedzy oraz inwencja związana z tworzeniem cennych i unikalnych relacji. W ramach zarządzania wiedzą organizacyjną postuluje się, aby korzystanie z zasobów wiedzy miało charakter powszechny. Jednakże wśród zasobów informacyjnych organizacji są informacje wrażliwe i wymagające ochrony przed dostaniem się w niepowołane ręce. Zatem zasoby wiedzy poddawane są rygorom odpowiedniej polityki bezpieczeństwa, co nie powinno dopuścić do wycieków informacyjnych lub innych form naruszenia własności intelektualnej organizacji. Ze względu na powszechne stosowanie przechowywania, przetwarzania i przesyłania informacji w formie elektronicznej, coraz częściej w celu ochrony korporacyjnych zasobów informacyjnych stosuje się specjalnie w tym celu skonstruowane systemy informatyczne.

Artykuł przedstawia zagadnienia wyceny organizacyjnych zasobów stanowiących własność intelektualną, kategorie strat finansowych dla organizacji, powstających w wyniku naruszeń bezpieczeństwa informacji oraz metody pomiaru kosztów spowodowanych naruszeniami bezpieczeństwa.

Artykuł podejmuje problematykę systemów informatycznych oraz stosowanych w nich mechanizmów, których zadaniem jest ochrona kapitału intelektualnego. Systemy te zajmują się prawidłowym obiegiem informacyjnym, monitorowaniem informacji wchodzącej i wychodzącej z organizacji, a także takim zabezpieczaniem danych w formie elektronicznej, żeby można było odkryć te, które w wyniku rozmaitych uchybień lub naruszeń wyciekły z organizacji. W artykule przedstawiono sposób działania systemów, które w sposób kompleksowy zapewniają bezpieczeństwo kapitału intelektualnego w przedsiębiorstwach oraz systemom używanym, gdy posiadająca wartość informacja jest informacją publiczną i której nie da się zabezpieczyć przed nieuprawnionym użyciem.

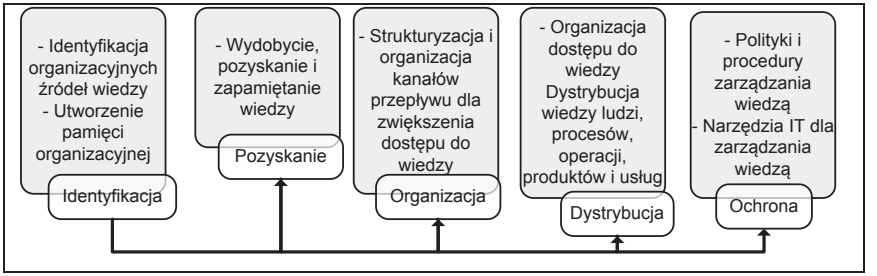
KAPITAŁ INTELEKTUALNY

Na kapitał intelektualny, który wchodzi w skład zasobów niematerialnych[1], składa się i kapitał strukturalny i kapitał ludzki. Kapitał ludzki tworzy przede wszystkim wiedza pracowników, ich umiejętności oraz podatność na tworzenie i wprowadzanie innowacji [Edvinsson, 2001]. Jak podaje *Brookings Institute*, w 1982 roku majątek niematerialny stanowił 38% średniej wartości rynkowej firm, a w 2002 roku wartość ta sięgnęła już 88%.

Właściwe zarządzanie kapitałem intelektualnym stanowi jedną z kluczowych kompetencji współczesnego przedsiębiorstw. Głównym celem zarządzania kapitałem intelektualnym jest rozpoznanie (identyfikacja) poszczególnych elementów aktywów niematerialnych, ich pomiar oraz odpowiednie wykorzystywanie i rozwijanie w celu osiągnięcia celów strategicznych przedsiębiorstwa (co ilustruje Rysunek 1).

Pojęcie własności intelektualnej zostało zdefiniowane przez WIPO (ang. *World Intellectual Propperty Organization*), a – zgodnie z polskim prawem – pod pojęciem własności intelektualnej należy rozumieć prawa związane z działalnością intelektualną w dziedzinie literackiej, artystycznej, naukowej i przemysłowej, obejmujące: prawo autorskie i prawa pokrewne z prawami autorskimi, prawa do baz danych, prawo własności przemysłowej dotyczące: wynalazków, wzorów użytkowych i wzorów przemysłowych, znaków towarowych czy oznaczeń geograficznych, topografii układów scalonych.

[1] Nazywane niekiedy aktywami niematerialnymi lub aktywami intelektualnymi.



Rysunek 1: Kluczowe procesy w zarządzaniu wiedzą

Źródło: Opracowanie własne na podstawie [Probst, 1999].

Ochrona prawna własności intelektualnej jest przedmiotem odpowiednich regulacji w każdym państwie. Polskie akty prawne, które regulują kwestie dotyczące własności intelektualnej, obejmują prawo autorskie i prawa pokrewne, ochronę baz danych, prawa własności przemysłowej i zwalczanie nieuczciwej konkurencji.

MECHANIZMY OCHRONY KAPITAŁU INTELEKTUALNEGO

Tabela 1 ilustruje sposoby ochrony określonych aspektów wytworów intelektualnych. Poza prawami autorskimi, które regulowane są przez Konwencję Berneńską, pozostałe prawa własności są ograniczone terytorialnie i z tego powodu muszą być rejestrowane i zabezpieczane na każdym rynku krajowym, na którym jest to potrzebne.

Tabela 1: Metody ochrony wytworów intelektualnych według ich kategorii

Kategoria własności intelektualnej	Sposób ochrony własności intelektualnej
Innowacyjne produkty i procesy biznesowe	Patent, sekret handlowy lub wzór użytkowy
Prace artystyczne, utwory literackie	Prawa autorskie lub pokrewne
Wzory, w tym wzory tekstylne	Wzory przemysłowe
Oprogramowanie komputerowe	Prawa autorskie i prawa pokrewne

Znaki charakterystyczne	Znaki towarowe i usługowe, oznaczenia handlowe i geograficzne
Układy scalone	Wzory projektowe, topografia układów scalonych
Oznakowanie dóbr o określonej jakości	Oznaczenia handlowe i geograficzne
Poufne informacje biznesowe i informacje handlowe o charakterze technicznym	Sekrety handlowe

Źródło: opracowanie własne na podstawie zaleceń WIPO2.

Poza własnością intelektualną podlegającą ochronie prawnej, organizacje posiadają wiedzę utajnioną (*know-how*) oraz wiedzę nie podlegającą rejestracji. Organizacje, starając się chronić korporacyjny kapitał intelektualny (tajemnice organizacji oraz poufne dane) przed zamierzonym lub przypadkowym wyciekiem, wykorzystują różne technologie i metody zabezpieczeń. Współcześnie funkcjonujące organizacje, poza danymi przechowywanymi w formie papierowej, w większości przechowują swoje zasoby informacyjne w postaci elektronicznej w pamięciach masowych i bazach danych. Utrata poufnych i firmowych danych jest drugim najpoważniejszym zagrożeniem tuż po zagrożeniu atakami wirusów. Powszechnym zjawiskiem jest to, że pracownicy nie posiadają rozeznania, jakiego rodzaju dane firmowe są poufne lub zastrzeżone oraz na jakich zasadach mogą być rozpowszechniane. Według powyższego raportu 80% wszystkich naruszeń bezpieczeństwa informacji odbywa się w sposób przypadkowy, niezamierzony [Haley, 2011]. W raporcie zatytułowanym *Wartość sekretów korporacyjnych* [Forrester, 2010] podaje, że w przemyśle opartym na wiedzy 70% korporacyjnego kapitału intelektualnego zawarta jest w wiedzy ukrytej, 62% w finansach i ubezpieczeniach. Utrata ukrytego kapitału intelektualnego może spowodować katastrofalne skutki dla przedsiębiorstwa.

Ochronie podlega również własność intelektualna znajdująca się w publicznie dostępnych w Internecie dokumentach. Ich stale rosnącej liczbie towarzyszy powszechne wykorzystanie treści zawartej w przechowywanych w nim dokumentach z naruszeniem własności intelektualnej, co stanowi naruszenie prawa własności intelektualnej wobec autorów pierwotnych dokumentów.

[2] WIPO IP Facts & Figures, http://www.wipo.int/edocs/pubdocs/en/wipo_pub_943_2014.pdf [dostęp: 27.05.2015].

Metody wyceny kapitału intelektualnego pozwalają na pomiar różnych składników kapitału intelektualnego, co prowadzi do wyrażenia zasobów niematerialnych w kategoriach pieniężnych. Do metod wartościowych zalicza się takie wskaźniki, jak: porównanie wartości rynkowej z księgową, wskaźniki oparte na relacji wartości rynkowej do kosztu odtworzenia aktywów, intelektualna wartość dodana [Pulic, 2004] czy kalkulowana wartość niematerialna [Steward, 1995].

Wśród metod opartych na porównaniu wartości rynkowej z księgową najprostszą jest miernik porównujący wartość rynkową przedsiębiorstwa z jego wartością księgową. Na potrzeby oceny kapitału intelektualnego przyjmuje się założenie, że wartość rynkowa przedsiębiorstwa stanowi sumę wartości księgowej oraz wartości kapitału intelektualnego. Ponadto zakładając, że wartość rynkowa zadłużenia przedsiębiorstwa jest w przybliżeniu równa wartości księgowej długu, wartość kapitału intelektualnego stanowi nadwyżkę wartości rynkowej kapitału własnego nad jego wartością księgową.

Wśród wielu różnych metod opracowanych do oszacowania wartości zasobów informacyjnych organizacji najbardziej popularne są metody oparte na wskaźnikach zwrotu z inwestycji ROI (ang. Return of Investment) oraz zwrotu z inwestycji ponoszonych na zapewnienie bezpieczeństwa ROSI (ang. *Return Of Security Investments*). Niektóre metody uwzględniają koszty tworzenia lub odtworzenia aktywów, natomiast, podczas gdy jeszcze inni próbują uchwycić wszystkie skutki zarówno po stronie przychodów jak i kosztów [Brotby, 2009].

POMIAR KOSZTÓW NARUSZEŃ WŁASNOŚCI INTELEKTUALNEJ

Wydatki organizacji na narzędzia ochrony własności intelektualnej stają się racjonalne, a ich wartość dobrze skalkulowana wtedy, gdy można określić wartość strat spowodowanych w wyniku naruszeń bezpieczeństwa (kosztów wygenerowanych z powodu ich zaistnienia).

Raporty szacujące straty w wyniku naruszeń bezpieczeństwa informacji i szerzej kapitału intelektualnego, które są tworzone przez różne instytucje i wyspecjalizowane ośrodki badawcze, opierają się na odmiennych metodach szacowania strat. Dlatego dla ustalenia skali strat w wyniku naruszeń własności intelektualnej potrzebne jest ustalenie w miarę możliwo-

ści uniwersalnych kategorii strat dla organizacji spowodowanych przez te naruszenia.

Naruszenie bezpieczeństwa w oczach inwestorów może być postrzegane jako czynnik, który spowoduje krótkookresowe i długookresowe straty i zredukuje oczekiwane przyszłe przepływy pieniężne. Zatem pomiar zmian wartości rynkowej firmy po ogłoszeniu naruszenia bezpieczeństwa może pomóc w oszacowaniu kosztów naruszenia.

Prawidłowe oszacowanie wartości aktywów informacyjnych organizacji z perspektywy ich bezpieczeństwa powinno uwzględniać wpływ następujących czynników [ISF Report, 2005]:

- skutki finansowe (ang. *financial impact*): utracone wpływy ze sprzedaży, utratę zamówień lub kontraktów, zmniejszenie wartości środków trwałych, pasywów, kar prawnych, wzrost nieprzewidzianych wydatków, obniżenie ceny akcji,
- skutki operacyjne (ang. *operational impact*): utrata kontroli zarządczej, utrata konkurencyjności utrata produktywności, utrata nowych przedsięwzięć, naruszenie standardów operacyjnych,
- skutki związane z klientami (ang. *customer-related impact*): opóźnione dostawy do klientów lub do klientów, utrata klientów, utrata zaufania przez kluczowe instytucje, naruszenie reputacji,
- skutki związane z pracownikami (ang. *employee-related impact*): mniejsza wydajność pracowników, zmniejszone morale, obrażenie ciała lub śmierć.

Wymienione powyżej skutki mogą mieć charakter materialny lub niematerialny. Wśród skutków stosunkowo łatwych do oszacowania jest np. zmniejszenie sprzedaży lub utrata produktywności. Inne koszty, takie jak utrata reputacji, mają charakter niematerialny i są trudne do oszacowania. Jednakże są one bardzo ważne dla prawidłowego pomiaru niezbędnych wydatków na zapewnienie bezpieczeństwa organizacji. Z tego powodu niektórzy badacze proponują dokonywanie pomiaru ukrytych kosztów poprzez utratę kapitalizacji rynkowej firm będących w obrocie publicznym.

Niektórzy badacze proponują oszacowanie rzeczywistego kosztu naruszenia bezpieczeństwa oparte na wycenie rynkowej firmy [Cavusoglu, 2004]. To podejście opiera się na hipotezie wydajnego rynku, na którym inwestorzy polegają na swojej zdolności do zrewidowania swoich oczekiwań w oparciu o nowe informacje w komunikatach od firmy. Oczekiwania inwestorów są odzwierciedlone w wartości firmy. Problemy bezpieczeństwa mogą sygnalizować uczestnikom rynku niewystarczające praktyki zapewniania bezpieczeństwa w firmie, co powoduje pytania inwestorów o długo-

terminowe wyniki i wycenę firmy. Naruszenia bezpieczeństwa mogą być postrzegane przez inwestorów jako czynnik, który może spowodować straty i zmniejszenie oczekiwanych przyszłych przepływów pieniężnych. Tak więc pomiar zmian w wartości rynkowej firmy po ogłoszeniu naruszenia bezpieczeństwa może pomóc ocenić koszty tego naruszenia.

Kluczowe zagadnienia w ramach utworzenia polityki bezpieczeństwa własności intelektualnej organizacji obejmuje:

- zdefiniowanie najbardziej wrażliwych danych, zdefiniowanie polityki bezpieczeństwa, utworzenie odpowiednich metryk,
- wdrożenie narzędzi monitorujących kanały komunikacyjne, zabezpieczenie dokumentów przy pomocy odpowiednich technik,
- egzekwowanie: poddanie kwarantannie podejrzanych informacji, zmniejszenie naruszeń polityki do akceptowalnego poziomu.

Narzędzia informatyczne służące do ochrony własności intelektualnej

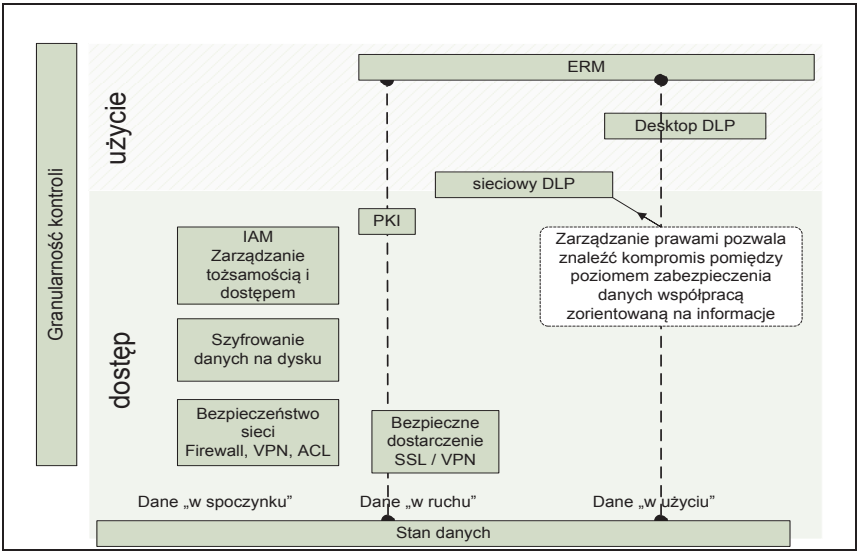
Dobór narzędzi informatycznych oraz wartość wydatków organizacji poniesionych na narzędzia ochrony własności intelektualnej zależeć powinien od wartości strat spowodowanych poprzez naruszenia własności intelektualnej. Metody oszacowania strat są nieodłącznie związane z metodami szacowania wartości aktywów informacyjnych organizacji.

Wśród narzędzi i systemów informatycznych, które chronią zasoby informacyjne organizacji, należy wyróżnić trzy kategorie systemów. Pierwszymi są systemy, które powstały po to, aby wspomagać tworzenie, transfer lub dystrybucję zasobów informacyjnych organizacji i w tym zakresie zapewniają ich bezpieczeństwo. Druga kategoria obejmuje takie systemy, które powstały, aby chronić zasoby informacyjne w wybranych aspektach bezpieczeństwa. Trzecia kategoria to systemy które utworzono, aby kompleksowo chronić zasoby informacyjne organizacji.

Do najbardziej popularnych informatycznych narzędzi wspomagających zarządzanie wiedzą należą: systemy zarządzania dokumentami (systemy archiwizujące, wyszukujące i udostępniające dokumenty), systemy workflow (wspomagające i ujednolicające procedury postępowania wewnątrz organizacji), systemy wspomagania pracy grupowej (ułatwiające komunikację pomiędzy pracownikami, co służy tworzeniu i transferowi wiedzy).

Do ochrony danych stosuje się rozmaite technologie, co pokazane zostało na Rysunku 2. Ta taksonomia pokazuje jak technologie stosowane do ochrony danych koncentrują się na bezpieczeństwie danych będących w specyficznym stanie: w spoczynku (dane przechowywane w zbiorach

danych), dane w ruchu (transferowane) oraz dane w użyciu (przetwarzane przez programy).



Rysunek 2. Kategorie narzędzi informatycznych do ochrony zasobów informacyjnych

Źródło: opracowanie własne na podstawie [Petrao, 2011].

Systemy zarządzania bezpieczeństwem dokumentów DSM (ang. *Document Management Systems*) to systemy zapewniające mechanizmy, dzięki którym autor informacji może się dzielić poufną informacją z innymi użytkownikami, bez utraty kontroli nad tą informacją. Zadania tych systemów obejmują zapobieganie ujawnieniu informacji poufnych, kontrolę uprawnień dostępu do dokumentu oraz rejestrowanie dostępu.

Do zapewnienia bezpieczeństwa gromadzonych w przedsiębiorstwie w formie elektronicznej dokumentów służą systemy zarządzania prawami do informacji ERM (ang. *Enterprise Rights Management*). Ich zadanie sprowadza się do ograniczania dostępu do dokumentów elektronicznych objętych różnymi formami utajnienia. Szczególnym przypadkiem zarządzania prawami do informacji są systemy zarządzania prawami cyfrowymi DRM stosowane do ochrony przed nieuprawnionym kopiowaniem dokumentów multimedialnych (zdjęć, filmów, muzyki), przeznaczonych do ochrony sprzedawanych na rynku plików multimedialnych.

Systemy ERM wykorzystują technologie zabezpieczania bezpieczeństwa poprzez szyfrowanie danych, co zapewnia bezpieczeństwo ich przechowywania, przesyłania oraz dostępu do nich (stosuje się tu również określenie, że dane są bezpieczne w stanie przechowywania, wtedy, kiedy są „w ruchu" oraz kiedy są „w użyciu"). Dokument jest rozszyfrowywany w momencie otwarcia przez osoby lub aplikacje uprawnione i posiadające odpowiedni klucz kryptograficzny. Dokumenty są odszyfrowywane w pamięci operacyjnej komputera na rzecz aplikacji, która ma za zadanie te dane przetwarzać. Jeśli dojdzie do skopiowania dokumentu poza uprawniony system, to będzie on nieczytelny bez odpowiedniego oprogramowania i klucza kryptograficznego.

Ponadto w systemach ERM[3] definiowane są czynności dozwolone do wykonania na określonych danych, takie jak: przyzwolenie lub zakaz drukowania, kopiowania do schowka, konwersji danych do innego formatu, wysłania pocztą elektroniczną itd. Stanowi to ochronę logiczną dokumentów elektronicznych za pomocą praw dostępu, która jest egzekwowana przez aplikację, wewnątrz której przetwarzane są dokumenty lub przez system operacyjny (dokumenty w plikach).

W celu kompleksowej ochrony informacji w organizacji stosuje się rozwiązania z rodziny DLP, które pozwalają nie tylko realizować szczegółową politykę bezpieczeństwa na oznaczonych danych, ale także na podstawie odpowiednich heurystyk, potrafią analizować treści danych będących w ruchu, najczęściej wysyłanych z przedsiębiorstwa. Są to najbardziej złożone systemy informatyczne zapewniające bezpieczeństwo kapitału intelektualnego wykonujące takie zadania, jak: analiza ruchu sieciowego, blokada określonych informatycznych kanałów komunikacyjnych, tworzenie i przechowywanie polityki bezpieczeństwa oraz monitorowanie urządzeń i pracowników mobilnych poprzez monitorowanie ich działań.

Najczęściej stosowane metody monitorowania bezpieczeństwa danych w systemach DLP polegają na: wyszukiwaniu poufnych informacji za pomocą wyrażeń regularnych, skanowaniu baz danych oraz wyszukiwaniu i łączeniu ze sobą określonych wzorców, wykorzystaniu techniki *fingerprinting* (tzw. odcisk palca dokumentu), dodawaniu metadanych do dokumentów, analizie fragmentów dokumentów, analizie behawioralnej, statystycznej oraz językowej.

Rozwiązania DLP umożliwiają zdefiniowanie zawartości, kontekstu, przeznaczenia danych, pozwalając zarządzać tym kto, jak i gdzie może

[3] Wiodące ERM.

przesyłać określone informacje, co pozwala zdefiniować szczegółową politykę przepływu danych w zależności od szczegółowych wymagań danej organizacji.

Znaczną część zasobów informacyjnych organizacji ma charakter informacji jawnej wyrażonej w postaci tekstowej, czyli takiej, której nie da się zabezpieczyć, gdyż wartość intelektualną posiada sama treść informacji. W świecie całkowicie opartym na wiedzy własność intelektualna znajduje się w rozmaitych opracowaniach o charakterze naukowym lub eksperckim. Zwiększająca się liczba incydentów polegających na niezgodnym z prawem wykorzystaniu własności intelektualnej ma związek z rosnącym, globalnym dostępem do informacji, co dotyczy również środowiska akademickiego w najbardziej wrażliwym dlań aspekcie – przywłaszczania osiągnięć naukowych.

Zaawansowane systemy informatyczne ochrony własności intelektualnej zawartej w tekstowych zasobach informacyjnych posługują się pojęciową reprezentacją wiedzy oraz stosują metody i mechanizmy powodujące, że sformułowane w różny sposób wypowiedzi w tekście dokumentów, które mają takie samo znaczenie informacyjne pod względem semantycznym, byłyby rozumiane przez utworzony system jako tożsame lub co najmniej jako bardzo podobne. Architekturę oraz dokładny sposób funkcjonowania takich systemów opisano w [Ceglarek, 2013].

Podstawowym zadaniem wykonywanym przez te systemy jest ustalanie czy dany dokument tekstowy nie zawiera zapożyczeń z innych dokumentów. Istotnym atrybutem jest zdolność systemu do poprawnego oznaczenia zapożyczeń w stosunku do rzeczywistej ich liczby i stopnia zapożyczenia. Wysoka precyzja systemu w tym znaczeniu mówi o niewielkiej liczbie przypadków fałszywie pozytywnych, natomiast duża pełność odpowiedzi oznacza, że system wykrył większość przypadków zapożyczeń występujących w analizowanym zbiorze dokumentów. Systemy te przetwarzają ogromne ilości informacji, co powoduje, że sposób indeksowania dokumentów z repozytoriów oraz stosowane algorytmy stanowią kluczowy czynnik ich wydajności.

WNIOSKI

W artykule został przedstawiony przegląd narzędzi i mechanizmów służących zarówno do ochrony własności intelektualnej organizacji przed dostaniem się w niepowołane ręce, jak i do ochrony przed niewłaściwym

użyciem publicznie dostępnych zasobów informacyjnych organizacji. Ochrona korporacji przed wyciekiem informacyjnym wymaga stosowania kompleksowych systemów zabezpieczających, posiadających wyspecjalizowane moduły ochronne, których zadaniem jest ochrona zasobów wiedzy korporacyjnej. Jest to ściśle powiązane i uzależnione od funkcjonującego w organizacji modelu biznesowego. W zależności od wymagań organizacji należy dobrać odpowiednie mechanizmy i technologie informatyczne, co pozwoli na zastosowanie właściwych polityk bezpieczeństwa, co spowoduje ich dopasowanie do wymagań danej organizacji. Elementy kapitału intelektualnego, które związane są z wiedzą jawną, również muszą być monitorowane.

LITERATURA

Aberdeen Group Report, "Thwarting Data Loss. *Best in Class Strategies for Protecting Sensitive Data",* Aberdeen Group Press 2007.

Brotby W.K., *Information security management metrics: a definitive guide to effective security monitoring and measurement*, Boca Raton, Auerbach Publications 2009.

Cavusoglu H., Mishra B., Raghunathan S., *A model for evaluating it security investments, Communication of ACM* 2004, 47(7), s. 87–92, ACM.

Ceglarek D., *Linearithmic Corpus to Corpus Comparison by Sentence Hashing Algorithm SHAPD2*, w: The 5th International Conference on Advanced Cognitive Technologies and Applications, Curran Associates, s. 141–146, Valencia (Spain), 2013.

Edvinsson L., Malone M.S., *Kapitał intelektualny,* PWN, Warszawa 2001.

Forrester Research Report, *The Value Of Corporate Secrets. How Compliance And Collaboration Affect Enterprise Perceptions Of Risk*, Forrester Research Inc., Cambridge 2010.

Haley K., *2011 Internet Security Threat Report Identifies Increased Risks for SMBs*, Symantec Report 2011.

ISF. The standard of good practice for information security. Technical report, Information Security Forum 2005.

Jaquith A., Balaouras S., Crumb A., *The Forrester Wave™: Data Leak Prevention Suites*, Q4 2010.

Meyer R., de Witt B., *Strategy-Process, Content, Context*, International Thompson Business Press, London 1998.

Petrao B., Managing the risk of information leakage, Continuity Central 2011.

Poore R.S., Valuing information assets for security risk management., Information Systems Security 2000*,* s. 13–23.

Probst G., Raub S., Romhard K., *Wissen Managen. Wie Unternehmen Ihre Wertvolle Ressource Optimal Nutzen*, Gabler, Frankfurt 1999.

Pulic A., *Intellectual Capital – Does it Create or Destroy Value?*, „Measuring Business Excellence" 2004, Vol. 8 (1).

Ricceri F., *Intellectual Capital and Knowledge Management. Strategic management of knowledge resources*, Routledge Francis & Taylor Group, New York 2008.

Sroka H., *Zarys koncepcji nowej teorii organizacji zarządzania dla przedsiębiorstwa e-gospodarki*, Wydawnictwo Akademii Ekonomicznej w Katowicach, Katowice 2007.

Stewart T.A., *Trying to Grasp the Intangible*, „Fortune" 1995, Vol. 132 (7), s. 158.

PROCEDURES AND IT TOOLS DEDICATED TO THE PROTECTION OF INTELLECTUAL PROPERTY OF KNOWLEDGE-BASED ORGANIZATION

Abstract: This paper presents the issues of knowledge management, in particular protected knowledge. It takes the problem of IT systems and mechanisms, whose function is to protect intellectual capital of an organization. These systems deal with the proper circulation of information, monitoring of incoming and outgoing information from the organization, as well as an effective securing information stored in electronic form in the corporate databases.

Keywords: IT systems, intellectual capital, intellectual property protection.