

mgr inż. Seweryn Szczupakowski
Szkoła Główna Handlowa
w Warszawie
email: szczupakowski@proton.me
ORCID: 0009-0003-8772-0106

Model dojrzałości ochrony know-how w praktyce MŚP: studium przypadków z projektu „Żagle Biznesu SGH”

Know-how protection maturity model in SME practice: Case studies from the “Żagle Biznesu SGH” project

Słowa kluczowe:
ochrona wiedzy, know-how,
sektor MŚP, zarządzanie
wiedzą, dojrzałość
organizacyjna

Streszczenie: Artykuł podejmuje problematykę ochrony know-how w sektorze MŚP, wskazując na istotną lukę między rozwiązaniami formalnymi a faktyczną praktyką organizacyjną. W gospodarce opartej na wiedzy zdolność do zabezpieczenia zasobów niematerialnych stanowi kluczowy czynnik przewagi konkurencyjnej, jednak w wielu przedsiębiorstwach pozostaje marginalizowana i traktowana jako koszt operacyjny. Celem artykułu jest wielowymiarowa diagnoza stopnia ustrukturyzowania systemów ochrony wiedzy oraz identyfikacja dysproporcji w stosowaniu poszczególnych mechanizmów zabezpieczających. Badanie empiryczne objęło 37 przedsiębiorstw uczestniczących w projekcie „Żagle Biznesu SGH” w latach 2021–2024. Analizę przeprowadzono, opierając się na autorskim, pięciowarstwowym modelu ochrony, integrującym wymiary: poznawczy, strategiczny, zasobowy, procesowy oraz sygnalizacyjny. Weryfikacja hipotez badawczych wykazała dominację instrumentów prawnych (np. umów NDA) nad rozwiązaniami organizacyjnymi (H1), a także istotne zróżnicowanie poziomu ochrony uzależnione od czynników zarządczych (H3). Wyniki badań wskazują na niski poziom świadomości ryzyka, niespójność kontroli dostępu oraz niedostatki w retencji wiedzy. Wnioski wskazują na konieczność ścisłej integracji rozwiązań prawnych z procedurami kontroli dostępu oraz systemowej kodyfikacji wiedzy krytycznej.

Keywords:

knowledge protection, know-how, SME sector, knowledge management, organizational maturity

Abstract: This article examines know-how protection in the SME sector, highlighting a significant gap between formal mechanisms and actual organizational practice. In a knowledge-based economy, the ability to secure intangible assets constitutes a key source of competitive advantage; however, it is still frequently marginalized and treated as an operational cost. The study aims to provide a multi-dimensional assessment of the level of structuring of knowledge protection systems and to identify disparities in the application of specific safeguards. The empirical research covered 37 enterprises participating in the “Żagle Biznesu SGH” project between 2021 and 2024. The analysis was conducted based on an original five-layer protection model integrating cognitive, strategic, resource, process, and signaling dimensions. Hypothesis testing confirmed the dominance of legal instruments (e.g., NDA) over organizational solutions (H1), as well as significant variation in the level of protection depending on managerial factors (H3). The findings indicate a low level of risk awareness, inconsistent in access control, and deficiencies in knowledge retention. The results indicate the need for closer integration of legal mechanisms with access control procedures and for the systematic codification of critical knowledge.

JEL:

D83, L26, O34

Wprowadzenie

Współczesne uwarunkowania gospodarcze, charakteryzujące się nasilającą się konkurencją, skracaniem cykli życia produktów oraz postępującą cyfryzacją procesów biznesowych, prowadzą do redefinicji źródeł przewagi konkurencyjnej przedsiębiorstw. Coraz większego znaczenia nabiera zdolność organizacji do efektywnego zarządzania wiedzą, jej interpretowania oraz ochrony. Know-how, rozumiane jako specyficzna, często niejawną formą wiedzy zakorzeniona w rutynach operacyjnych i kompetencjach zespołowych, stanowi jeden z kluczowych, a zarazem najtrudniejszych do zabezpieczenia zasobów przedsiębiorstwa. Jego niematerialny charakter oraz silne powiązanie z kapitałem ludzkim sprawiają, że tradycyjne instrumenty ochrony prawnej okazują się często niewystarczające.

Pomimo rosnącej świadomości znaczenia kapitału intelektualnego, praktyka gospodarcza – szczególnie w sektorze małych i średnich przedsiębiorstw (MŚP) – ujawnia istotne luki w systemach ochrony wiedzy. Działania w tym obszarze mają często charakter fragmentaryczny i reaktywny, a nakłady na bezpieczeństwo informacji są postrzegane raczej jako koszt niż inwestycja strategiczna. Ochrona know-how nie ogranicza się jednak wyłącznie do zabezpieczeń przed zagrożeniami zewnętrznymi, lecz obejmuje również tworzenie wewnętrznych struktur umożliwiających kontrolowany przepływ

informacji, precyzyjne definiowanie uprawnień dostępu oraz ograniczanie ryzyka utraty wiedzy w związku z odejściem kluczowych pracowników.

Celem artykułu jest diagnoza stopnia ustrukturyzowania systemów ochrony know-how w przedsiębiorstwach sektora MŚP oraz identyfikacja rozbieżności pomiędzy deklarowaną wagą tego zagadnienia a rzeczywistą praktyką organizacyjną. Analiza obejmuje również ocenę użyteczności zintegrowanego, wielowarstwowego podejścia do ochrony zasobów niematerialnych.

Uzasadnienie podjęcia problemu badawczego wsparte rezultatami przeglądu literatury przedmiotu

Ewolucja podejścia do zarządzania strategicznego, koncentrująca się na wewnętrznym potencjale organizacji, znajduje swoje podstawy w teorii zasobowej (Resource-Based View – RBV). W jej ramach przedsiębiorstwo ujmowane jest jako wiązka zasobów, których unikalna konfiguracja determinuje możliwości rynkowe. Wskazuje się, że wartość zasobu nie wynika z samego faktu jego posiadania, lecz z możliwości jego wykorzystania oraz realokacji w odpowiedzi na zmiany otoczenia [Wernerfelt, 1984, s. 171–174]. Rozwinięciem tej perspektywy było sformułowanie warunków trwałej przewagi konkurencyjnej, obejmujących wartość, rzadkość, trudność imitacji oraz brak substytutów zasobów strategicznych [Barney, 1991, s. 99–120]. Ujęcie to zostało następnie uzupełnione o znaczenie mechanizmów izolacji, zabezpieczających zasoby przed replikacją przez konkurentów [Peteraf, 1993, s. 182–186].

Wiedza organizacyjna w szczególności sposób spełnia kryteria zasobu strategicznego, co znalazło wyraz w podejściu opartym na wiedzy (Knowledge-Based View – KBV). Organizacja ujmowana jest tu jako społeczny mechanizm tworzenia i replikacji wiedzy, oparty na zbiorowych rutynach i wspólnych kodach interpretacyjnych, co ogranicza możliwość jej transferu i imitacji [Kogut, Zander, 1992, s. 383–392]. Charakter wiedzy, w tym jej złożoność i podatność na kodyfikację, wpływa bezpośrednio na tempo replikacji zdolności organizacyjnych oraz możliwości ich ochrony [Zander, Kogut, 1995, s. 76–92].

Równolegle rozwijano podejścia uwzględniające poznawcze uwarunkowania procesu decyzyjnego. Zwraca się uwagę, że uproszczenia poznawcze i heurystyki stosowane przez menedżerów wpływają na sposób interpretacji informacji, co może prowadzić do niedoszacowania ryzyka oraz ignorowania słabych sygnałów zagrożeń [Schwenk, 1984, s. 113–121]. W kontekście ochrony wiedzy oznacza to, że nawet posiadanie odpowiednich zasobów i procedur nie gwarantuje ich właściwego wykorzystania.

Istotne znaczenie dla zarządzania wiedzą ma również jej dynamiczny charakter. Wiedza ujmowana jest jako proces ciągłej konwersji pomiędzy wymiarem jawnym i ukrytym, realizowany poprzez interakcje społeczne [Nonaka, 1994, s. 14–37]. Wiedza ukryta,

choć stanowi naturalną barierę imitacyjną, pozostaje jednocześnie trudna do formalnej kontroli. Podkreśla się również znaczenie wiedzy zbiorowej, zakorzenionej w praktykach i kontekstach organizacyjnych, jako fundamentu odrębności przedsiębiorstwa [Spender, 1996, s. 45–62].

Perspektywą integrującą ujęcie zasobowe i procesualne jest koncepcja dynamicznych zdolności, definiowana jako zdolność do integrowania, rekonfigurowania i adaptowania kompetencji w warunkach zmienności otoczenia [Teece i in., 1997, s. 516–525]. Jej zastosowanie do problematyki ochrony wiedzy implikuje odejście od statycznego rozumienia zabezpieczeń na rzecz ciągłego dostosowywania praktyk ochronnych.

Uzupełnieniem powyższych rozważań jest teoria sygnalizacji, wskazująca na znaczenie komunikowania jakości działań organizacji w warunkach asymetrii informacyjnej. Mechanizmy ochrony wiedzy mogą pełnić funkcję sygnałów świadczących o dojrzałości zarządczej oraz odpowiedzialności operacyjnej, redukując postrzegane ryzyko współpracy [Connelly i in., 2011, s. 45–48].

Przegląd literatury ujawnia istotną lukę badawczą. Dotychczasowe prace koncentrują się na pojedynczych instrumentach ochrony wiedzy – takich jak ochrona własności intelektualnej, kontrola dostępu, kodyfikacja czy zabezpieczenia techniczne – analizowanych w izolacji od siebie. Brakuje natomiast zintegrowanego ujęcia relacji pomiędzy świadomością ryzyka, praktykami organizacyjnymi oraz ich sygnalizacją rynkową, w szczególności w zakresie mechanizmów sprzężeń zwrotnych pomiędzy warstwami systemu ochrony.

W odpowiedzi na zidentyfikowaną lukę badawczą w artykule przyjęto model pięciowarstwowy ochrony wiedzy organizacyjnej, integrujący wymiary poznawcze, strategiczne, zasobowe, procesowe i sygnalizacyjne. Model ten stanowi kompleksową ramę analityczną:

1. Warstwa poznawcza (Awareness)

Odnosi się do stopnia, w jakim decydenci dostrzegają i identyfikują zagrożenia dla integralności wiedzy oraz rozumieją konsekwencje jej utraty. Opiera się na zdolności do przewyższania uproszczeń poznawczych w ocenie ryzyka.

2. Warstwa strategiczna (Strategic Alignment)

Obejmuje dopasowanie celów i środków ochrony do profilu ryzyka branżowego oraz specyfiki działalności. Zakłada świadomy wybór strategii adekwatnej do otoczenia.

3. Warstwa zasobowa (Resource Deployment)

Dotyczy alokacji środków finansowych, ludzkich i technicznych niezbędnych do wdrożenia i utrzymania systemów ochrony (np. infrastruktura IT, personel).

4. Warstwa procesowa (Process Implementation)

Koncentruje się na rutynach, procedurach i mechanizmach operacyjnych, poprzez które wiedza jest przechowywana, dystrybuowana i kontrolowana (np. polityki dostępu, kodyfikacja wiedzy).

5. Warstwa sygnalizacyjna (Signaling)

Odnosi się do komunikowania dojrzałości proceduralnej organizacji w otoczeniu rynkowym, co sprzyja budowaniu zaufania i redukcji asymetrii informacyjnej.

Pięć warstw stanowi zintegrowaną całość, a model zakłada występowanie sprzężeń zwrotnych pomiędzy nimi.

Sprzężenia:

1 warstwa poznawcza → 3 warstwa zasobowa

Wysoka świadomość wartości i ryzyka know-how zwiększa skłonność decydentów do alokowania zasobów na działania ochronne.

1 warstwa poznawcza → 4 warstwa procesowa

Wyższa świadomość ryzyka przekłada się na wdrażanie konkretnych procedur (np. zasada need-to-know, retencja wiedzy, kodyfikacja), bo to warstwa poznawcza uruchamia motywację i priorytetyzację działań.

1 warstwa poznawcza → 5 warstwa sygnalizacyjna

Wysoka świadomość wartości know-how i ryzyka sprzyja podejmowaniu działań formalnych i komunikacyjnych (np. standardy współpracy, NDA jako sygnał), co zwiększa skłonność do sygnalizowania dojrzałości ochrony na zewnątrz.

2 warstwa strategiczna → 4 warstwa procesowa

Przyjęta strategia ochrony determinuje architekturę procesów (np. kodyfikacja vs. ograniczanie dyfuzji), bezpośrednio wpływając na sposób organizacji kontroli i retencji wiedzy.

3 warstwa zasobowa → 1 warstwa poznawcza

Wdrożenie narzędzi i ról ochronnych zwiększa widoczność zagrożeń i incydentów, co zwrótnie podnosi świadomość ryzyka na poziomie zarządczym.

3 warstwa zasobowa → 5 warstwa sygnalizacyjna

Alokacja zasobów ochronnych (IT, role, budżet) umożliwia wiarygodną sygnalizację dojrzałości ochrony know-how wobec interesariuszy zewnętrznych.

4 warstwa procesowa → 1 warstwa poznawcza

Funkcjonujące procedury ochrony ujawniają realne luki i incydenty, co zwrótnie podnosi świadomość zagrożeń i ogranicza ich poznawcze niedoszacowanie.

4 warstwa procesowa → 2 warstwa strategiczna

Efekty wdrożenia procedur (skuteczność, kosztochłonność, opór organizacyjny) prowadzą do rewizji założeń strategicznych i ponownego dopasowania środków ochrony.

5 warstwa sygnalizacyjna → 1 warstwa poznawcza

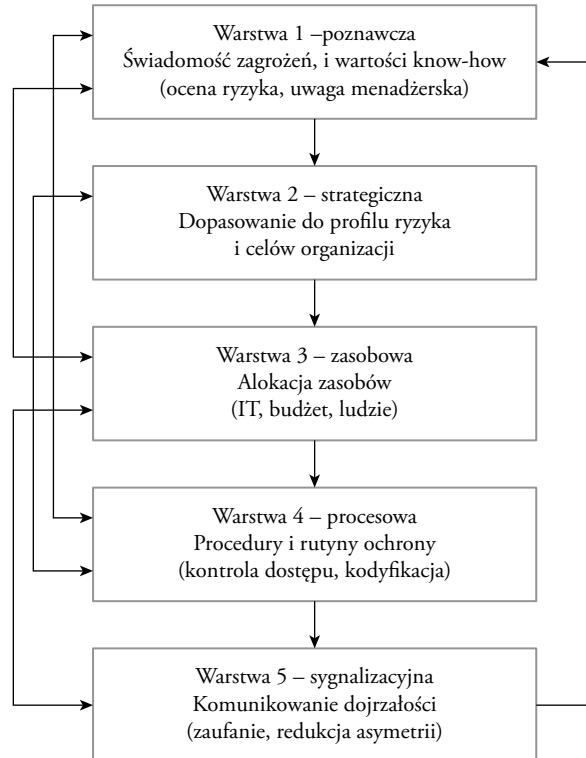
Sygnalizacja dojrzałości ochrony (np. formalne standardy, widoczne praktyki) wywołuje rynkową walidację i presję interesariuszy, co zwrótnie wzmacnia świadomość zagrożeń w organizacji.

5 warstwa sygnalizacyjna → 3 warstwa zasobowa

Presja rynkowa i kontraktowa wynikająca z sygnalizacji dojrzałości wymusza dalsze inwestycje w zasoby ochronne, wzmacniając zaplecze systemu.

Na rysunku 1 przedstawiono graficzną reprezentację modelu oraz relacje sprzężeń zwrotnych.

Rysunek 1. Graficzna prezentacja modelu oraz sprzężeń zwrotnych



Źródło: opracowanie własne.

Określenie celu oraz zakresu przeprowadzonych badań

Opierając się na przyjętym w części teoretycznej ujęciu zasobowym oraz podejściu akcentującym rolę wiedzy w tworzeniu przewagi konkurencyjnej, celem artykułu jest diagnoza stopnia ustrukturyzowania i spójności rozwiązań służących ochronie know-how w przedsiębiorstwach sektora MŚP, a także identyfikacja najczęściej występujących luk w tym obszarze. Ochronę know-how rozumie się jako zbiór rozwiązań formalnych i organizacyjnych, których funkcją jest ograniczanie ryzyka nieuprawnionego ujawnienia, utraty lub niekontrolowanego rozpowszechniania zasobów wiedzy o znaczeniu gospodarczym.

Cel badania ma charakter poznawczo-aplikacyjny. W wymiarze poznawczym obejmuje rekonstrukcję faktycznie stosowanych instrumentów ochrony, wykraczającą poza deklaracje respondentów. Wymiar aplikacyjny polega na sformułowaniu wniosków praktycznych dotyczących obszarów, w których rozwiązania formalnoprawne okazują się niewystarczające bez wsparcia odpowiednich mechanizmów zarządczych. Dotyczy to zwłaszcza kontroli dostępu do zasobów wiedzy, dokumentowania procedur oraz zarządzania ryzykiem personalnym.

Zakres analizy obejmuje lata 2021–2024, odpowiadające kolejnym edycjom projektu badawczego. Badaniem objęto 37 przedsiębiorstw należących do sektora MŚP. Zakres przedmiotowy analizy obejmuje praktyki ochrony know-how rekonstruowane na podstawie raportów eksperckich, ze szczególnym uwzględnieniem identyfikacji kluczowych zasobów wiedzy, zasad dostępu do nich oraz sposobów ograniczania ryzyka w relacjach z otoczeniem.

Wskazanie postawionych hipotez badawczych

Analiza literatury przedmiotu oraz przyjęte ramy teoretyczne wskazują, że ochrona know-how nie stanowi obszaru homogenicznego, lecz jest kształtowana przez współwystępowanie rozwiązań formalnych i praktyk organizacyjnych. W celu uporządkowania relacji między założeniami teoretycznymi a analizą empiryczną sformułowano następujące hipotezy badawcze o charakterze diagnostycznym:

H1: W badanych przedsiębiorstwach z sektora MŚP rozwiązania o charakterze formalnym, takie jak regulacje wewnętrzne, zapisy umowne, są identyfikowane i stosowane częściej niż rozwiązania organizacyjne związane z porządkowaniem procesów oraz kontrolą dostępu do informacji.

Hipoteza ta zakłada występowanie asymetrii między popularnością instrumentów formalnoprawnych a poziomem dojrzałości procesowej przedsiębiorstw.

H2: Wyższy poziom formalizacji procesów zarządczych współwystępuje ze stosowaniem bardziej rozbudowanego zestawu rozwiązań służących ochronie wiedzy.

Hipoteza zakłada występowanie dodatniej zależności między ogólnym poziomem dojrzałości zarządczej organizacji a stopniem zaawansowania jej systemu ochrony know-how.

H3: Poziom i struktura stosowanych praktyk ochrony know-how są silnie zróżnicowane w obrębie badanej grupy i nie zależą wyłącznie od wielkości przedsiębiorstwa ani od jego branży.

Oznacza to, że zróżnicowanie podejścia do ochrony know-how wynika w znacznym stopniu z czynników zarządczych, takich jak poziom świadomości kadry kierowniczej i kultura organizacyjna, a nie tylko z uwarunkowań strukturalnych.

Opis zastosowanej metody badawczej

Weryfikację modelu teoretycznego oraz identyfikację praktyk ochrony wiedzy przeprowadzono na podstawie materiału empirycznego zgromadzonego w ramach projektu „Żagle Biznesu SGH”, realizowanego w latach 2021–2024. Badaniem objęto 37 przedsiębiorstw sektora MŚP reprezentujących zróżnicowane branże, w tym usługi, produkcję i technologie. Podstawową metodą badawczą była analiza treści raportów eksperckich sporządzonych na podstawie pogłębionych wywiadów z przedstawicielami przedsiębiorstw oraz przeglądu dokumentacji wewnątrzorganizacyjnej. Każdy raport zawierał odrębną sekcję poświęconą systemom zarządzania wiedzą i środkom jej ochrony, co zapewniło porównywalność analizowanych danych.

W celu operacjonalizacji pięciowarstwowego modelu teoretycznego wyodrębniono siedem kryteriów badawczych stanowiących empiryczne wskaźniki dojrzałości systemu ochrony know-how:

- a) ochrona praw własności intelektualnej (IP) – rejestracja znaków i patentów oraz polityka praw autorskich (wskaźnik warstwy strategicznej i sygnalizacyjnej);
- b) umowy o poufności (NDA) – stosowanie klauzul poufności w relacjach wewnętrznych i zewnętrznych (wskaźnik warstwy sygnalizacyjnej i poznawczej);
- c) kontrola dostępu – zarządzanie uprawnieniami do zasobów fizycznych i cyfrowych (wskaźnik warstwy zasobowej i procesowej);
- d) infrastruktura IT – techniczne środki bezpieczeństwa, takie jak tworzenie kopii zapasowych, szyfrowanie i rejestrowanie zdarzeń (wskaźnik warstwy procesowej oraz dynamicznych zdolności);
- e) baza wiedzy – stopień sformalizowania i kodyfikacji wiedzy w postaci instrukcji i procedur (wskaźnik warstwy procesowej i zasobowej);
- f) świadomość zagrożeń i ryzyka – zdolność identyfikacji zagrożeń dla integralności zasobów wiedzy (wskaźnik warstwy poznawczej);
- g) retencja wiedzy – mechanizmy zatrzymania wiedzy w organizacji, w tym procesy *onboarding* i sukcesji (wskaźnik warstwy procesowej).

Każde z kryteriów oceniano na czterostopniowej skali porządkowej:

- 0 punktów – brak działań lub działania o nieskoordynowanym charakterze;
- 1 punkt – działania incydentalne, o niskim stopniu sformalizowania;
- 2 punkty – częściowa formalizacja i ograniczony zakres stosowanych praktyk;
- 3 punkty – pełne wdrożenie, systematyczność oraz powiązanie z innymi procesami.

Zastosowana skala umożliwiła obliczenie syntetycznego indeksu dojrzałości, którego maksymalna wartość wynosi 21 punktów, oraz typologizację badanych przedsiębiorstw. Indeks pełni funkcję wskaźnika orientacyjnego (*proxy*) zaawansowania systemu ochrony know-how. Szczegółową charakterystykę kryteriów oceny przedstawiono w tabeli 1.

Tabela 1. Skala oceny dojrzałości systemu ochrony know-how w przedsiębiorstwach sektora MŚP

Kryterium oceny	0 punktów	1 punkt	2 punkty	3 punkty
Ochrona praw własności intelektualnej	Brak formalnych działań w zakresie IP	Pojedyncze, incydentalne działania, np. rejestracja znaku towarowego	Częściowa strategia IP i ograniczony zakres ochrony	Spójna i świadomie realizowana strategia IP, zintegrowana z działalnością przedsiębiorstwa
Umowy o poufności (NDA)	Brak umów o poufności	NDA stosowane wybiórczo lub deklaratorywnie	NDA stosowane systematycznie, lecz bez kontroli ich egzekwowania	NDA zintegrowane z procedurami ochrony wiedzy i kontrolą dostępu
Kontrola dostępu do wiedzy	Brak ograniczeń dostępu	Ograniczenia nieformalne lub fragmentaryczne	Sformalizowane zasady dostępu o częściowym zakresie	Spójna polityka dostępu oparta na zasadzie <i>need-to-know</i>
Infrastruktura IT wspierająca ochronę	Brak rozwiązań ochronnych	Podstawowe zabezpieczenia, np. tworzenie kopii zapasowych	Rozwiązania techniczne obejmujące szerszy zakres ochrony	Zintegrowana infrastruktura bezpieczeństwa IT
Kodyfikacja i baza wiedzy	Wiedza nieudokumentowana	Częściowa dokumentacja bez systematycznej aktualizacji	Uporządkowana baza wiedzy o ograniczonym zakresie	Systematyczna kodyfikacja i zarządzanie wiedzą
Świadomość zagrożeń i ryzyka	Brak identyfikacji zagrożeń	Intuicyjne postrzeganie zagrożeń	Okresowa refleksja nad zagrożeniami i ryzykiem	Systematyczna analiza ryzyka związanego z ochroną know-how
Retencja wiedzy	Brak mechanizmów retencji wiedzy	Działania doraźne	Częściowo sformalizowane praktyki	Spójne procedury sukcesji i <i>offboardingu</i>

Źródło: opracowanie własne na podstawie analizy raportów eksperckich projektu „Żagle Biznesu SGH”.

Rezultaty przeprowadzonych badań

Analiza materiału empirycznego zgromadzonego w grupie 37 przedsiębiorstw umożliwiła ocenę poziomu dojrzałości systemów ochrony wiedzy w siedmiu zdefiniowanych obszarach. Maksymalny możliwy do uzyskania wynik syntetyczny wynosił 21 punktów. Uzyskane rezultaty wskazują na znaczne zróżnicowanie badanej grupy oraz występowanie istotnych dysproporcji pomiędzy poszczególnymi obszarami ochrony know-how.

Ochrona własności intelektualnej

W obszarze formalnej ochrony własności intelektualnej odnotowano jeden z najniższych wyników ogółem – średnio 0,86 pkt. Zaledwie cztery przedsiębiorstwa wdrożyły kompleksową strategię ochrony własności intelektualnej obejmującą zgłoszenia patentowe, rejestrację wzorów przemysłowych oraz znaków towarowych. W przypadku niemal połowy badanych przedsiębiorstw (18) nie stwierdzono żadnych formalnych działań w tym zakresie.

Część przedsiębiorstw uzasadniała ten stan ograniczoną innowacyjnością oferowanych rozwiązań lub specyfiką modelu biznesowego, charakteryzującego się niskimi barierami wejścia. Wśród przedsiębiorstw podejmujących aktywność w tym obszarze dominowała rejestracja znaków towarowych. Zidentyfikowano również przypadki celowego nieujawniania szczegółów technicznych, określanego jako strategia „milczenia”, zamiast ich formalnej rejestracji. Rozwiązanie to rzadko wynikało ze świadomej przyjętej polityki ochrony, a częściej z ograniczonych zasobów lub niewystarczającej wiedzy.

Umowy o poufności

Stosowanie umów o zachowaniu poufności (NDA) stanowiło najbardziej rozpowszechniony mechanizm ochrony know-how w badanej grupie (średni wynik wyniósł 1,86 pkt). Tylko cztery przedsiębiorstwa całkowicie zrezygnowały z tego instrumentu. W 11 przypadkach stwierdzono jego pełne wdrożenie, obejmujące wszystkich pracowników oraz kluczowych kontrahentów, a także powiązanie umów o poufności z zakazami konkurencji i systemem kontroli ich przestrzegania.

Wyniki te potwierdzają hipotezę dotyczącą dominacji rozwiązań formalnoprawnych nad rozwiązaniami organizacyjnymi. Umowy o poufności są postrzegane jako narzędzie relatywnie tanie i łatwe do wdrożenia. W wielu przypadkach ich stosowanie miało jednak charakter deklaracyjny i nie było powiązane z rzeczywistym monitorowaniem przepływu informacji.

Kontrola dostępu do wiedzy

Wdrażanie mechanizmów kontroli dostępu zgodnie z zasadą *need-to-know* miało charakter selektywny (średni wynik wyniósł 1,19 pkt). Jedynie pięć przedsiębiorstw wdrożyło sformalizowaną politykę dostępu połączoną z regularnymi audytami uprawnień. W 12 przedsiębiorstwach nie zidentyfikowano żadnych ograniczeń dostępu – każdy pracownik miał dostęp do całości zasobów wiedzy organizacji.

Dziewięć przedsiębiorstw stosowało nadawanie ról w systemach informatycznych, takich jak CRM, jednak rozwiązania te rzadko były wspierane spójną procedurą zarzą-

dzania tożsamością i uprawnieniami. Wyniki wskazują zatem na występowanie luki w warstwie procesowej. Pomimo wykorzystywania narzędzi technicznych przedsiębiorstwa często nie definiowały precyzyjnych reguł dostępu do kluczowych aktywów wiedzy.

Infrastruktura IT

Poziom zabezpieczeń technicznych oceniono jako umiarkowany (średni wynik wyniósł 1,46 pkt). Najwyższe oceny uzyskały przedsiębiorstwa wykorzystujące zaawansowane rozwiązania, takie jak systemy SIEM i SOAR, szyfrowanie danych oraz regularne testy penetracyjne. Najlicniejsza grupa (14 przedsiębiorstw) opierała ochronę na standardowych funkcjonalnościach usług chmurowych oraz systemach tworzenia kopii zapasowych.

Siedem przedsiębiorstw nie zadeklarowało żadnych sformalizowanych działań w obszarze bezpieczeństwa IT, co w warunkach postępującej cyfryzacji procesów stanowi poważne zagrożenie dla bezpieczeństwa zasobów wiedzy. Widoczna była tendencja do outsourcingu zabezpieczeń poprzez korzystanie z gotowych platform chmurowych. Rozwiązanie to przyczyniało się do podniesienia ogólnego poziomu ochrony w segmencie MŚP, choć nie zawsze oznaczało świadome i kompleksowe zarządzanie bezpieczeństwem informacji.

Baza wiedzy i kodyfikacja

Stopień sformalizowania wiedzy w postaci procedur i instrukcji był zróżnicowany (średni wynik wyniósł 1,35 pkt). Tylko sześć przedsiębiorstw posiadało w pełni ustrukturyzowaną cyfrową bazę wiedzy, np. w systemach typu Confluence, oraz regularnie ją aktualizowało. W 10 przypadkach wiedza miała charakter całkowicie rozproszony i nieudokumentowany, określany jako „plemienny”, co uzależniało funkcjonowanie organizacji od konkretnych pracowników.

Kodyfikacja wiedzy była najczęściej wymuszana przez czynniki zewnętrzne, takie jak wymogi certyfikacji ISO, lub konieczność skalowania działalności. W mniejszych przedsiębiorstwach dominował natomiast ustny przekaz wiedzy.

Świadomość zagrożeń i ryzyka

Najniższy wynik w całym badaniu odnotowano w obszarze świadomości zagrożeń i ryzyka (średnia wyniosła 0,78 pkt). Aż 17 przedsiębiorstw nie wykazało refleksji nad możliwością utraty wiedzy, koncentrując się wyłącznie na bieżącej działalności operacyjnej. Tylko trzy podmioty prowadziły systematyczną analizę ryzyka i posiadały zdefiniowane scenariusze awaryjne.

Wynik ten wskazuje na deficyt w poznawczej warstwie modelu. Kadra menedżerska często nie dostrzegała zagrożenia do momentu wystąpienia incydentu, np. odejścia kluczowego pracownika do przedsiębiorstwa konkurencyjnego. Niska świadomość zagrożeń i ryzyka stanowi barierę dla wdrażania bardziej zaawansowanych rozwiązań w pozostałych warstwach modelu.

Retencja wiedzy i sukcesja

Zarządzanie retencją wiedzy również stanowiło obszar niewystarczająco rozwinięty (średni wynik wyniósł 0,97 pkt). W 18 przedsiębiorstwach nie stwierdzono żadnych mechanizmów ograniczających ryzyko utraty wiedzy w wyniku rotacji personelu. Jedynie pięć organizacji wdrożyło kompleksowe programy sukcesji i offboardingu, połączone z procedurami przekazywania obowiązków (*handover*).

W większości przypadków odejście pracownika wiązało się z bezpowrotną utratą części kapitału intelektualnego przedsiębiorstwa. Dominowało podejście reaktywne, a procesy onboardingu koncentrowały się na aspektach administracyjnych, a nie na merytorycznym transferze know-how.

Typologia przedsiębiorstw

Syntetyczna analiza wyników pozwoliła wyodrębnić cztery typy organizacji w badanej próbie:

- „Nieświadomi” – przedsiębiorstwa uzyskujące od 0 do 5 pkt; 7 podmiotów bez systemowych rozwiązań ochrony wiedzy, funkcjonujących przede wszystkim na podstawie wzajemnego zaufania.
- „Formaliści” – przedsiębiorstwa uzyskujące od 6 do 10 pkt; 7 podmiotów koncentrujących się na aspektach prawnych, takich jak NDA i ochrona własności intelektualnej, przy jednoczesnym zaniedbaniu procesów organizacyjnych.
- „Pragmatycy” – przedsiębiorstwa uzyskujące od 11 do 15 pkt; 17 podmiotów wdrażających wybrane rozwiązania punktowe, głównie w obszarze IT i kontroli dostępu, lecz nieposiadających spójnej strategii ochrony wiedzy.
- „Liderzy ochrony” – przedsiębiorstwa uzyskujące powyżej 15 pkt; 6 podmiotów charakteryzujących się zintegrowanym podejściem, łączącym wymiary formalno-prawny, techniczny i organizacyjny.

Wnioski empiryczne, teoretyczne i rekomendacje praktyczne

Przeprowadzone badanie potwierdziło użyteczność przyjętego modelu pięciowarstwowego jako narzędzia diagnostycznego oraz umożliwiło pozytywną weryfikację sformułowanych hipotez badawczych.

W odniesieniu do hipotezy H1 wyniki wskazują na asymetrię w strukturze stosowanych zabezpieczeń. Instrumenty formalnoprawne, zwłaszcza umowy o zachowaniu poufności (NDA), były wykorzystywane najczęściej, osiągając średni wynik 1,86 pkt, podczas gdy rozwiązania organizacyjne, takie jak sformalizowana kontrola dostępu i procedury retencji wiedzy, pozostawały na znacznie niższym poziomie rozwoju. Oznacza to, że przedsiębiorstwa sektora MŚP chętniej sięgały po narzędzia jednorazowe i zewnętrzne niż podejmowały wysiłek budowy wewnętrznych procesów zarządzania wiedzą.

Hipoteza H2 również znalazła potwierdzenie. Organizacje o wyższym stopniu formalizacji procesów biznesowych, przejawiającym się m.in. posiadaniem certyfikatów jakości lub wykorzystywaniem systemów CRM, osiągały wyższe wyniki w zakresie ochrony know-how. Wynik ten wskazuje na współwystępowanie dojrzałości procesowej i wyższego poziomu ochrony informacji.

Weryfikacja hipotezy H3 ujawniła znaczne zróżnicowanie badanej grupy. Wyodrębnienie czterech typów organizacji – „Nieświadomych”, „Formalistów”, „Pragmatyków” i „Liderów” – potwierdza, że poziom ochrony wiedzy zależy w znacznym stopniu od czynników zarządczych, zwłaszcza od świadomości kadry kierowniczej, a nie wyłącznie od wielkości przedsiębiorstwa lub jego branży.

Wnioski teoretyczne

Na poziomie teoretycznym badanie wskazuje, że skuteczna ochrona wiedzy wymaga integracji wymiaru prawnego, technicznego i organizacyjnego. Zastosowanie wyłącznie instrumentów formalnoprawnych, bez ich powiązania z procedurami i rozwiązaniami technicznymi, nie zapewnia spójnego systemu ochrony know-how.

Model pięciowarstwowy pozwala uchwycić zarówno formalne instrumenty ochrony, jak i procesy organizacyjne, zasoby techniczne oraz poznawcze uwarunkowania zarządzania wiedzą. Jego wartość polega przede wszystkim na umożliwieniu diagnozy obszarów niedorozwoju oraz porównania poziomu dojrzałości systemów ochrony w badanych przedsiębiorstwach.

Rekomendacje praktyczne

W świetle uzyskanych wyników rekomenduje się:

- a) powiązanie umów o zachowaniu poufności z procedurami kontroli dostępu oraz monitorowania obiegu informacji;
- b) systematyczne budowanie świadomości wartości know-how i zagrożeń związanych z jego utratą;
- c) kodyfikację wiedzy o znaczeniu krytycznym dla funkcjonowania przedsiębiorstwa;
- d) wdrożenie formalnych procedur retencji, sukcesji i offboardingu;
- e) okresowy przegląd uprawnień dostępowych oraz aktualizację procedur ochrony wiedzy;
- f) uwzględnianie ochrony know-how w procesach onboardingu, aby transfer wiedzy od początku zatrudnienia był elementem zarządzania zasobami ludzkimi.

Ograniczenia badania

Zaproponowany model ma charakter diagnostyczny i porównawczy, a nie efektywnościowy. Nie służy zatem do bezpośredniego pomiaru skuteczności poszczególnych zabezpieczeń ani do oceny, czy zastosowane rozwiązania faktycznie zapobiegły wystąpieniu incydentów związanych z utratą lub ujawnieniem wiedzy.

Model ma również charakter statyczny i opiera się na próbie obejmującej przedsiębiorstwa uczestniczące w projekcie „Żagle Biznesu SGH”, co ogranicza możliwość pełnej generalizacji wyników. Ponadto model nie uwzględnia wprost różnic sektorowych i kulturowych, które mogą modyfikować znaczenie poszczególnych warstw ochrony wiedzy.

Podsumowanie

Ochrona know-how w przedsiębiorstwach sektora MŚP stanowi wielowymiarowe wyzwanie, wykraczające poza aspekty czysto prawne i technologiczne. Przeprowadzona analiza wykazała, że kluczową barierą w budowaniu skutecznych systemów ochrony nie jest brak zasobów finansowych, lecz niska świadomość zagrożeń i ryzyka oraz niewystarczający stopień formalizacji procesów wewnętrznych.

Zaproponowany model pięciowarstwowy umożliwia precyzyjną identyfikację luk w systemie ochrony wiedzy, a także może stanowić podstawę projektowania dedykowanych do potrzeb przedsiębiorstwa strategii doskonalenia. Jego zastosowanie pozwala analizować ochronę know-how jako układ wzajemnie powiązanych rozwiązań prawnych, organizacyjnych, technicznych i zarządczych, a nie jako zbiór pojedynczych instrumentów.

Dalsze badania powinny koncentrować się na ocenie skuteczności poszczególnych mechanizmów integracyjnych oraz na analizie wpływu kultury organizacyjnej na spójność i odporność systemu ochrony wiedzy. Zasadne byłoby również przeprowadzenie badań podłużnych, pozwalających określić, w jaki sposób zmienia się poziom dojrzałości systemów ochrony know-how wraz z rozwojem przedsiębiorstwa oraz formalizacją jego procesów zarządczych.

Bibliografia

- Barney J.B. [1991], Firm Resources and Sustained Competitive Advantage, *Journal of Management*, vol. 17(1), s. 99–120.
- Connelly B.L., Certo S.T., Ireland R.D., Reutzel C.R. [2011], Signaling Theory: A Review and Assessment, *Journal of Management*, vol. 37(1), s. 39–67.
- Kogut B., Zander U. [1992], Knowledge of the Firm, Combinative Capabilities, and the Replication of Technology, *Organization Science*, vol. 3(3), s. 383–397.
- Nonaka I. [1994], A Dynamic Theory of Organizational Knowledge Creation, *Organization Science*, vol. 5(1), s. 14–37.
- Peteraf M.A. [1993], The Cornerstones of Competitive Advantage: A Resource-Based View, *Strategic Management Journal*, vol. 14(3), s. 179–191.
- Schwenk C.R. [1984], Cognitive Simplification Processes in Strategic Decision-Making, *Strategic Management Journal*, vol. 5(2), s. 111–128.
- Sponder J.-C. [1996], Making Knowledge the Basis of a Dynamic Theory of the Firm, *Strategic Management Journal*, vol. 17 (S2), s. 45–62.
- Teece D.J., Pisano G., Shuen A. [1997], Dynamic Capabilities and Strategic Management, *Strategic Management Journal*, vol. 18(7), s. 509–533.
- Wernerfelt B. [1984], A Resource-Based View of the Firm, *Strategic Management Journal*, vol. 5(2), s. 171–180.
- Zander U., Kogut B. [1995], Knowledge and the Speed of the Transfer and Imitation of Organizational Capabilities: An Empirical Test, *Organization Science*, vol. 6(1), s. 76–92.

