CENTRUM EDUKACJI PIBR

rachunkowość - audytor
KWARTALNIK REDAGOWANY PRZY WSPÓŁPRACY KRAJOWEJ RADY BIEGŁYCH REWIDETÓW

Stosowanie procedur analitycznych do badania sprawozdań finansowych

Jak zbudować skuteczną ochronę wewnętrzną – spojrzenie praktyka

Waldemar K. Lachowski

SPIS TREŚCI

STOSOWANIE PROCEDUR ANALITYCZNYCH DO BADANIA SPRAWOZDAŃ FINANSOWYCH 3

JAK ZBUDOWAĆ SKUTECZNĄ OCHRONĘ WEWNĘTRZNĄ – SPOJRZENIE PRAKTYKA 22

STOSOWANIE PROCEDUR ANALITYCZNYCH DO BADANIA SPRAWOZDAŃ FINANSOWYCH

Korzystanie z procedur analitycznych może poprawić skuteczność i gospodarność (przez obniżenie kosztów) badania sprawozdania finansowego w nowych warunkach. W artykule przedstawiono przesłanki stosowania procedur analitycznych na różnych etapach badania: celowość, zakres, możliwość i obowiązek stosowania, możliwy do osiągnięcia poziom pewności, powiązanie z modelem ryzyka i istotnością.

Niektóre omawiane kwestie z konieczności będą stanowiły przypomnienie tego, co od lat funkcjonuje w praktyce krajowej. Inne zostaną opisane z uwzględnieniem wymogów nowych standardów badania. Nie zamierzam omawiać wszystkich przypadków korzystania z procedur analitycznych. Nie znaczy to jednak, że zostaną pominięte zagadnienia przez wielu uważane za trudne. Takie tematy, jak korzystanie z analizy regresji do gromadzenia dowodów badania czy z analizy dyskryminacyjnej do oceny zagrożeń dla kontynuacji działalności przez jednostkę zostaną zasygnalizowane w sposób niewymagający od czytelników specjalistycznej wiedzy.

W toku badania przeprowadza się wiele działań, które pojedynczo lub w połączeniu z innymi przyczyniają się do realizacji zadań cząstkowych i ogólnych nałożonych na biegłego rewidenta. Umożliwiają one wyrażenie miarodajnej opinii o sprawozdaniu finansowym (sf). Należą do nich procedury analityczne, które mogą być stosowane praktycznie na wszystkich etapach badania. Dotyczy to również poprzedzających je działań, warunkujących akceptację danego zlecenia.

Praktyka pokazuje, że nie zawsze prawidłowo rozumiane są cel i zakres stosowania procedur analitycznych. Wielu biegłych rewidentów nadal utożsamia je tylko z analizą wskaźnikową oraz tymi zapisami „starych" standardów badania[1], które dotyczyły ich wykorzystania do sporządzenia raportu towarzyszącego opinii. Nowe standardy nie wymagają już przygotowania takiego raportu. Mimo to – zgodnie z ich zapisami – procedury analityczne na pewnych etapach badania muszą, a na innych mogą być stosowane. Będzie o tym mowa dalej.

Znaczenie procedur analitycznych wzrosło w ostatnich 20 latach. Prawidłowość ta dotyczy wszystkich narzędzi dających możliwość wnioskowania – z większą lub mniejszą pewnością – o badanej zbiorowości na podstawie wybranej z niej reprezentacji (takich jak próbkowanie) lub obserwowanych w niej zależnościach (takich jak procedury analityczne). Wzrost roli procedur analitycznych nie jest więc przypadkowy. Zwiększenie wolumenu transakcji gospodarczych przeprowadzanych przez badane jednostki, korzystające z zaawansowanych technologii informatycznych do przetwarzania danych[2], przy jednoczesnej presji na ograniczenie czasu trwania

[1] Przez „stare" standardy badania rozumiem wcześniej obowiązujące normy i KSRF. Nowe standardy, będące głównym przedmiotem rozważań w artykule, to Krajowe Standardy Badania w brzmieniu MSB (dalej KSB), będące tłumaczeniami MSB w wersji przyjętej przez KRBR i zatwierdzonej przez KNA (dostępne na stronie internetowej: www.pibr.org.pl/pl/prawo#krajowe-standardy-rewizji-finansowej).

[2] System informatyczny rachunkowości jako skomputeryzowana, wydzielona część systemu informacyjnego danej jednostki coraz bardziej wpływa na prawidłowość i rzetelność jej ksiąg rachunkowych oraz sporządzanego na ich podstawie sf.

i kosztu badania, sprawiają, że coraz rzadziej można bezpośrednio sprawdzić, obliczyć i zmierzyć wszystko, co jest lub co powinno się znaleźć w sf.

Jak się wydaje, została osiągnięta granica możliwości stosowania wielu tradycyjnych procedur szczegółowych[3] w odniesieniu do coraz większej liczby badanych jednostek. Tendencja ta będzie się nasilać, a tym samym wzrośnie znaczenie procedur analitycznych jako narzędzia badania. Wyciągnięte na ich podstawie wnioski nadal będą łączone z wynikami innych procedur (np. testami operacyjnej skuteczności procedur kontrolnych lub próbkowania), ale coraz częściej ich wyniki będą traktowane jako główne dowody badania.

Zarysowane tendencje stanowią zagrożenie dla biegłych rewidentów i firm audytorskich nadmiernie przywiązanych do wcześniejszej praktyki badania sf. Trwanie w przeszłości i negowanie rzeczywistości nie ma większego sensu. Lepszy efekt można osiągnąć, „otwierając się" na możliwości, jakie oferują nowe techniki i narzędzia. Ważne jest, by nadążać za zmianami zachodzącymi w jednostkach i środowisku, w jakim one funkcjonują, bo inaczej świadczenie odpowiedniej jakości usług badania nie będzie możliwe lub opłacalne. Korzystanie z nowych technik i narzędzi (lub chociażby zmiana celu i zakresu stosowania dotychczasowych) jest zasadne tym bardziej, że na ogół nie wymagają one dużych nakładów.

POJĘCIE „PROCEDUR ANALITYCZNYCH" I ICH PRZEBIEG NA RÓŻNYCH ETAPACH BADANIA

Termin „procedury analityczne" jest różnie rozumiany, warto go zatem uściślić. W myśl KSB 520.4[4] chodzi o ocenę informacji finansowych przez analizę możliwych do przyjęcia, uwiarygodnionych wcześniej przez biegłego rewidenta wzajemnych relacji między danymi finansowymi oraz niefinansowymi (takimi jak zależność między ilością sprzedanych produktów a wynikiem na sprzedaży). W zakres tych procedur wchodzi także wyjaśnianie stwierdzonych odchyleń, wahań i zależności znacząco odbiegających od oczekiwanych, niespójności z innymi posiadanymi informacjami oraz przyjętymi wcześniej założeniami.

Procedury analityczne stosuje się na każdym etapie badania, gdyż wspomagają realizację różnych celów biegłego rewidenta. Dotyczy to w szczególności:

- wstępnego zdobywania wiedzy o jednostce oraz identyfikacji i oceny ryzyka,
- gromadzenia dowodów badania,
- wykonywania procedur końcowych.

[3] Jako głównego źródła dowodów badania.

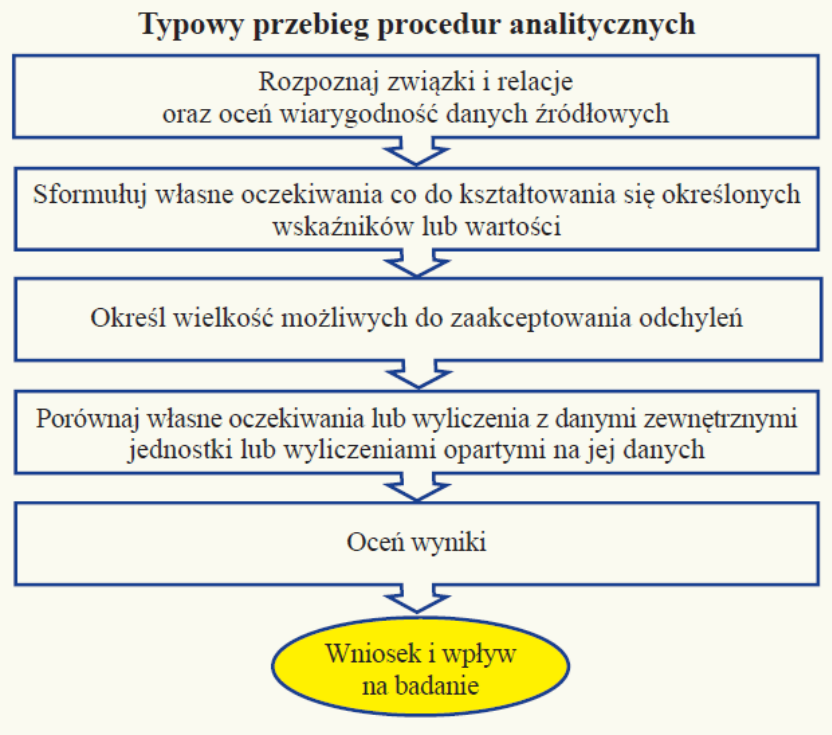
[4] KSB 520 Procedury analityczne.

W trakcie badania przeprowadzanego zgodnie z KSB[5] istnieje obowiązek stosowania procedur analitycznych na etapach a i c. Można też korzystać z nich dużo wcześniej, bo już na etapie akceptacji klienta – stanowią wówczas pomoc przy ocenie ryzyka zlecenia. Poprawia to gospodarność pracy biegłego rewidenta, gdyż wyniki zastosowania procedur analitycznych, po niezbędnej aktualizacji i ew. rozszerzeniu zakresu, mogą być później uznane za realizację części wymogów dotyczących podstawy formułowania strategii i planu badania (etap planowania).

Procedury analityczne stanowią ważne narzędzie badania ukierunkowanego na ryzyko. Stosując je, wykorzystuje się zależności, trendy i powtarzalność relacji zachodzących między danymi finansowymi i niefinansowymi. Ich użyteczność przejawia się przede wszystkim w tym, że pozwalają zidentyfikować obszary obarczone wyższym ryzykiem zniekształcenia sf oraz zwiększają efektywność badania. Mogą być stosowane do badania większości istotnych sald bilansu oraz grup transakcji dzięki występowaniu w miarę stałych relacji między danymi.

Nawet jeśli biegły rewident nie uzna procedur analitycznych za możliwą lub właściwą alternatywę dla badań szczegółowych (lub ich uzupełnienie), to zwykle przyczyniają się one do ukierunkowania jego pracy na obszary obarczone największym ryzykiem.

Procedury analityczne na różnych etapach badania przedstawiono na rysunku poniżej.



[5] Zagadnienia związane z wykorzystaniem procedur analitycznych jako sposobu zdobywania wiedzy o badanej jednostce oraz identyfikacji i oceny ryzyka wchodzą w zakres KSB 315 *Identyfikacja i ocena ryzyk istotnego zniekształcenia dzięki zrozumieniu jednostki i jej otoczenia*. Przedmiotem wspomnianego wcześniej KSB 520 *Procedury analityczne* jest ich wykorzystanie jako procedur wiarygodności oraz jako jednej z obowiązkowych końcowych procedur badania, umożliwiających sformułowanie ogólnego wniosku co do sf. KSB 330 *Postępowanie biegłego rewidenta w odpowiedzi na ocenę ryzyka* zawiera wymogi i wytyczne dotyczące rodzaju, czasu przeprowadzenia oraz zakresu procedur badania w reakcji na ocenione ryzyko. Zgodnie z tym standardem procedurami takimi mogą być również analityczne procedury wiarygodności. KSB 500 *Dowody badania* określa wymogi i wytyczne dotyczące stosowania procedur badania, które należy przeprowadzić w trakcie weryfikowania informacji wykorzystywanych do analitycznych procedur wiarygodności. KSB 240 *Odpowiedzialność biegłego rewidenta podczas badania sprawozdań finansowych dotycząca oszustw* wskazuje na rolę procedur analitycznych przy rozpatrywaniu ryzyka oszustwa.

Jak wynika z rysunku, procedury analityczne są oparte na ocenie związków istniejących między danymi podlegającymi analizie i porównaniu ich z oczekiwaniami co do wyników oraz możliwych relacji i trendów. W razie stwierdzenia istotnych, nietypowych lub nieoczekiwanych rezultatów trzeba je uwzględnić przy rozpoznawaniu ryzyka istotnego zniekształcenia oraz dodatkowo zweryfikować. Należy zacząć od próby uzyskania wiarygodnego wyjaśnienia od pracowników i kierownictwa badanej jednostki. Nie można jednak na tym poprzestać. Wymagane jest zgromadzenie dowodów potwierdzających racjonalność uzyskanych wyjaśnień.

Niekiedy biegły rewident może uznać, że przeprowadzenie wyłącznie procedur analitycznych jest odpowiednie do oszacowanego ryzyka wystąpienia istotnego zniekształcenia w grupie transakcji, jeżeli wstępny szacunek ryzyka potwierdzą dowody uzyskane drogą badań skuteczności działania kontroli wewnętrznej. W innych przypadkach biegły może zdecydować, że właściwe będą tylko badania szczegółowe lub że najlepszą reakcją na oszacowane ryzyko będzie połączenie badań szczegółowych z procedurami analitycznymi.

Chcąc wykorzystać procedury analityczne do gromadzenia dowodów badania, warto się posłużyć zmodyfikowanym modelem zależności składników ryzyka badania[6], w którym ryzyko przeoczenia zostało podzielone na 2 nowe kategorie:

$$RB = RN \times RK \times RPA \times RPS$$

lub

$$RB = RIZ \times RPA \times RPS$$

$$\text{Wymagany poziom RPA} = \frac{RB}{RN \times RK \times RPS} \text{ lub } = \frac{RB}{RIZ \times RPS}$$

gdzie:

RB	– ryzyko badania,
RN	– ryzyko nieodłączne,
RK	– ryzyko kontroli,
RPA × RPS = RP	– ryzyko przeoczenia,
RPA	– ryzyko nieskuteczności procedur analitycznych w wykrywaniu nieprawidłowości,
RPS	– ryzyko nieskuteczności procedur szczegółowych w wykrywaniu nieprawidłowości,
RIZ	– ryzyko istotnego zniekształcenia = RN × RK.

Fakt, że procedury analityczne na różnych etapach badania przebiegają wg podobnego schematu, nie oznacza, że nie ma między nimi różnic. Są one znaczące, a diabeł – jak zwykle – tkwi w szczegółach. Dotyczy to zarówno celu i sposobu korzystania z procedur analitycznych, sformułowania oczekiwań, wielkości akceptowalnych odchyleń, jak i możliwego do osiągnięcia poziomu pewności.

W tabeli na następnej stronie zamieszczono podstawowe informacje dotyczące stosowania procedur analitycznych na różnych etapach badania.

[6] Dla biegłego rewidenta model ryzyka badania jest przede wszystkim narzędziem planowania, a nie oceny jego rezultatów. Dlatego posługuje się nim w sposób logiczny, a nie statystyczny. Opisowa ocena poziomów ryzyka typu „wysokie" czy „niskie" jest z tego punktu widzenia wystarczająco precyzyjna. Jeżeli biegły posługuje się procentową oceną ryzyka, nie jest to równoważne ze stosowaniem przez niego rachunku prawdopodobieństwa.

PROCEDURY ANALITYCZNE NA RÓŻNYCH ETAPACH BADANIA

Etap	Cel i sposób stosowania	Obowiązek/możliwość stosowania w myśl KSB Możliwy do osiągnięcia poziom pewności Obowiązek sformułowania oczekiwań co do wielkości akceptowalnych odchyleń przed przeprowadzeniem procedury
Akceptacja nowego zlecenia, klienta lub kontynuacji relacji z nim	Wstępna analiza ryzyka zlecenia; wsparcie decyzji co do akceptacji lub odrzucenia konkretnego zlecenia bądź kontynuowania relacji z klientem	Możliwość Niski Nie
Planowanie	Jedna z czterech (pozostałe to zapytania, inspekcja i obserwacja) wymaganych przy każdym badaniu procedur zdobywania wiedzy o jednostce i środowisku, w jakim działa; służy identyfikacji i ocenie ryzyka oraz pomaga określić rodzaj, czas i zakres dalszych procedur rewizyjnych	Obowiązek Niski Nie
Badanie zasadnicze – reakcja rewizyjna na poziomie stwierdzeń	Jedna z dwóch (obok procedur szczegółowych) dostępnych biegłemu rewidentowi technik gromadzenia dowodów badania drogą bezpośredniej weryfikacji wiarygodności stwierdzeń; stosowanie w tym celu procedur analitycznych jest wskazane w przypadku badania stosunkowo licznych zbiorowości, w których występują powtarzalne relacje i współzależności między danymi finansowymi i niefinansowymi; zwykle dla zwiększenia pewności są łączone w badanie określonych zbiorowości; stosowane łącznie z innymi procedurami	Możliwość Średni lub wysoki Tak
Zakończenie badania	Na końcowym etapie badania, przed wydaniem opinii biegły rewident ma obowiązek zaprojektowania i przeprowadzenia procedury analitycznej, mającej formę ogólnego przeglądu; wyniki przeglądu powinny potwierdzać wnioski sformułowane podczas badania poszczególnych części lub elementów sf; mają one pomóc w sformułowaniu ogólnego wniosku, czy obraz przekazywany przez sf jest zgodny z posiadaną przez biegłego rewidenta wiedzą o jednostce i środowisku, w jakim ona działa; na tym etapie badania biegły powinien już rozumieć i umieć wyjaśnić wszystkie istotne zmiany, trendy i relacje występujące w zbadanym sf; jeżeli wynik analiz jest niezgodny z oczekiwaniami, to wymagane jest przeprowadzenie dodatkowych procedur wyjaśniających	Obowiązek Niski lub średni Nie

Tabela pokazuje zawarte wprost w treści KSB oczekiwania co do przydatności zastosowanych procedur dla rozpoznania nietypowych transakcji, zdarzeń, kwot i trendów. Mogą one wskazywać na ryzyka, które w razie ich realizacji wpłyną negatywnie na sf.

Wybór właściwych w danych okolicznościach technik i narzędzi analitycznych oraz poziomów ich zastosowania[7] jest kwestią osądu zawodowego. Nie oznacza to jednak dowolności – osąd musi być racjonalny. W szczególności uwzględnienia wymaga poziom pewności możliwej do osiągnięcia za pomocą poszczególnych technik i narzędzi analizy danych. Kwestie z tym związane zostaną omówione dalej.

POZIOM PEWNOŚCI MOŻLIWY DO UZYSKANIA DZIĘKI PROCEDUROM ANALITYCZNYM

Biegły rewident musi być zawsze świadomy ryzyka, że nawet bezbłędnie przeprowadzone procedury analityczne mogą potwierdzić oczekiwane wartości lub wielkości, mimo że w rzeczywistości saldo, grupa transakcji lub pozycja są obarczone istotnym błędem. Stopień pewności, jaki można uzyskać, stosując procedury analityczne, zależy przede wszystkim od dokładności i prawidłowości ustalenia przez biegłego rewidenta wartości oczekiwanych oraz progu akceptowalnych odchyleń. Istnieje zależność między tymi zmiennymi. Jeśli potrzebny jest większy stopień pewności, większa musi być też dokładność wyliczeń oczekiwanych wartości lub wielkości oraz mniejsza skłonność (próg) do akceptacji odchyleń. Co do zasady próg taki nie powinien być wyższy od istotności przyjętej do badania danego obszaru.

RYZYKO OSZUSTWA

Ujawnienie nietypowych lub nieoczekiwanych powiązań może sygnalizować zniekształcenie spowodowane oszustwem. KSB 240.22[8] wyraźnie wskazuje, że dotyczy to zwłaszcza kont przychodów. W odniesieniu do przychodów istnieje zatem obowiązek stosowania procedur analitycznych i oceny przyczyn ew. nietypowych lub nieoczekiwanych powiązań. Trzeba również pamiętać, że zgodnie z KSB 240.26 szczególnej uwagi biegłego rewidenta w toku każdego badania wymaga ryzyko oszustwa przy ujmowaniu przychodów (przez domniemanie istnienia znaczącego ryzyka). Podobna jest sytuacja w razie ew. ujawnienia, w wyniku zastosowania procedur analitycznych, zagrożeń dla kontynuacji działalności.

Dokładność wyliczeń zależy przede wszystkim od:

- wiarygodności przyjętych do kalkulacji danych źródłowych (im jest ona wyższa, tym większy stopień pewności można uzyskać),
- stopnia szczegółowości (np. dane zagregowane, szczegółowe, dzienne, miesięczne, roczne),

[7] Chodzi głównie o poziom szczegółowości danych podlegających analizie. Ta sama procedura zastosowana do danych szczegółowych (np. miesięczne koszty w podziale na kategorie i miejsca powstawania) da zwykle biegłemu rewidentowi większą pewność, że nie nastąpiły zniekształcenia, niż gdy analizie będą podlegać dane zagregowane (np. łączne koszty roczne).

[8] Pojęcie to opisano szerzej w dalszej części.

- przewidywalności danej pozycji (np. pozycje rachunku zysków i strat uważa się z reguły za bardziej przewidywalne niż salda bilansowe),
- rodzaju zastosowanej techniki analitycznej (np. analiza wskaźnikowa, test racjonalności, analiza regresji).

Nie wszystkie dane nadają się do badania przy zastosowaniu procedur analitycznych. Podstawowymi kryteriami, jakimi trzeba się tu kierować, są wiarygodność danych źródłowych oraz racjonalność założenia istnienia w danym okresie w miarę stałych relacji między analizowanymi zmiennymi (np. wielkością sprzedaży a średnim saldem należności z tytułu dostaw i usług). Jeżeli są co do tego wątpliwości, prawdopodobieństwo wyciągnięcia na podstawie analizy właściwych wniosków jest niskie. Procedura wstępna powinna zatem polegać na próbie potwierdzenia wiarygodności danych źródłowych, np. dzięki upewnieniu się, że podstawowe dane wartościowe czy ilościowe da się uzgodnić z kontami analitycznymi, syntetycznymi lub rejestrami. Zawsze trzeba też skorygować poddawane analizie dane oraz związane z nimi oczekiwania, eliminując z nich pozycje jednorazowe lub nietypowe, o których biegły rewident dowiedział się wcześniej, bo mogą one zniekształcić wyniki.

Chcąc poddać procedurom analitycznym dane lub informacje przygotowane przez klienta bądź pochodzące z jego systemu informacyjnego, warto też rozważyć możliwość i potrzebę przeprowadzenia testów kontrolnych w tym obszarze. Chodzi głównie o zebranie za ich pomocą dowodów potwierdzających poprawność oraz kompletność danych i informacji podlegających analizie. Im większe zaufanie do ich wiarygodności, tym bardziej zasadne jest poleganie na wynikach procedur analitycznych.

PRZYKŁAD

Badając przychody przez porównanie cen standardowych z wielkością sprzedaży, biegły rewident ocenia poprawność informacji o cenach oraz kompletność i poprawność danych dotyczących ilości sprzedanych produktów (towarów). Zwykle wykorzystuje on w tym celu informacje pozafinansowe lub dane planowane (budżetowe) dostarczane przez system informacyjny badanej jednostki. Uzyskiwanie dowodów badania dotyczących kompletności i poprawności informacji tworzonych przez ten system stanowi integralną część badania. Może ono przebiegać równolegle ze stosowaniem do tych informacji bieżących procedur rewizyjnych lub być elementem badania poprawności i skuteczności procedur kontrolnych stosowanych przez jednostkę do przygotowywania i przechowywania informacji.

Biegły rewident ocenia też, czy dane można zweryfikować na podstawie źródeł zewnętrznych (np. branżowych) lub czy podlegały one jakimkolwiek procedurom weryfikującym w bieżącym bądź poprzednim okresie.

Wyniki uzyskane na podstawie analizy danych o znacznym stopniu agregacji (np. roczna wielkość przychodów ze sprzedaży bez podziału na poszczególne miesiące i istotne kategorie) traktuje się jako wstępne wskazówki wymagające weryfikacji w toku dalszych prac. Z tego powodu zwykle nie nadają się one do gromadzenia dowodów badania. Ich stosowanie należy ograniczyć do etapu planowania i procedur końcowych badania, kiedy to nie jest wymagany wysoki poziom pewności.

Przeprowadzenie procedur analitycznych nie jest celem samym w sobie. Jeżeli nie można uzyskać wymaganego poziomu wiarygodności danych podlegających analizie, trzeba rozważyć stosowanie innych procedur. Oczywiście dotyczy to tylko przypadków, gdy przyczyny, z powodu których nie było możliwe lub zasadne przeprowadzenie procedur analitycznych, nie podważają całkowicie wiarygodności i skuteczności systemu kontroli wewnętrznej bądź jego kluczowych elementów z uwagi na możliwość sporządzenia sf odpowiedniej jakości.

TECHNIKI ANALIZY STOSOWANE DO FORMUŁOWANIA OCZEKIWAŃ

Procedury analityczne obejmują wiele technik analizy danych, które mogą być stosowane na różnych etapach badania. Do najczęściej wykorzystywanych zalicza się:

- analizę wskaźnikową,
- analizę trendu,
- analizę porównawczą,
- test racjonalności (zasadności[9]),
- analizę regresji.

Głównym elementem różnicującym te techniki – z uwagi na ich przydatność do badania – jest wspomniany już poziom precyzji (dokładności) obliczeń oczekiwanych wartości lub wielkości. Precyzja jest miarą bliskości oczekiwań biegłego rewidenta i wielkości lub wartości rzeczywiście ujętych w księgach rachunkowych. Skuteczność technik analitycznych w dużym stopniu zależy od ich precyzji i celu, jakiemu mają służyć. Im większa precyzja, tym większe prawdopodobieństwo, że ujawnione odchylenia i różnice świadczą o faktycznych zniekształceniach sf, a nie są wynikiem innych przyczyn. Istnieje również zależność między precyzją a istotnością (ilustruje to kolejny przykład). Dlatego biegły rewident musi ustalić poziom precyzji, z jakim powinna być określona wartość oczekiwana, aby wykryć zniekształcenia, które pojedynczo lub łącznie z innymi przewyższają poziom istotności.

Zgodnie z KSB 520.5 przy projektowaniu lub przeprowadzaniu analitycznych procedur wiarygodności trzeba ustalić wszelkie różnice – między kwotami rzeczywistymi a oczekiwanymi – które można zaakceptować bez dalszej analizy. Łatwo tu o popełnienie błędu wobec zawyżenia wielkości akceptowanych odchyleń. Ich graniczna wielkość powinna wynikać z zawodowego osądu uwzględniającego istotność, ryzyko, oczekiwany poziom pewności i cel procedury. Wszystkie te zmienne są wzajemnie powiązane. Im większy jest poziom ryzyka w danym obszarze, tym bardziej przekonujące dowody badania należy uzyskać. Można to osiągnąć m.in. przez obniżenie kwoty różnicy, uznanej za akceptowalną, bez konieczności dalszej analizy.

Kwota ta, jak już wspomniano, nie może być wyższa od tej, którą biegły rewident uważa za istotną. W praktyce za jej odpowiednik często się przyjmuje istotność wykonawczą. Nie jest to podejście właściwe w każdym przypadku. Im wyższy bowiem ma być poziom pewności, że wyniki uzyskane w wyniku procedur analitycznych są wiarygodne, tym wysokość akceptowanych odchyleń powinna

[9] Zwany coraz częściej w literaturze anglosaskiej „niestatystycznym modelowaniem prognostycznym".

być mniejsza od tego, co biegły rewident uważa za istotne. Ilustruje to uproszczony przykład na następnej stronie.

Analizując przykład, należy pamiętać, że wielkości (kwotowe lub procentowe) odchyleń, akceptowane bez potrzeby ich wyjaśniania, nie muszą być takie same w razie wykorzystywania różnych technik analitycznych, nawet jeżeli stosuje się je do badania tych samych zbiorowości. W tabeli zawarto główne elementy różnicujące poszczególne techniki analizy danych z punktu widzenia ich przydatności na poszczególnych etapach badania. W dalszej części artykułu zamieszczono ich szczegółowy opis wraz z przykładami zastosowania.

PRZYDATNOŚĆ POSZCZEGÓLNYCH TECHNIK ANALITYCZNYCH NA RÓŻNYCH ETAPACH BADANIA

Technika analizy danych	Największa przydatność	Ilość zmiennych możliwych do uwzględnienia podczas analizy	Możliwy do uzyskania poziom pewności	Możliwość statystycznej oceny poprawności wyników
Analiza wskaźnikowa	Planowanie/ procedury końcowe	Jedna lub kilka	Niski	Nie
Analiza trendu	Planowanie/ procedury końcowe	Zwykle jedna	Niski	Nie
Analiza porównawcza	Planowanie/ procedury końcowe	Jedna lub kilka	Niski	Nie
Test racjonalności	Planowanie/badanie zasadnicze	Jedna lub kilka	Średni lub wysoki	Nie
Analiza regresji	Badanie zasadnicze	W teorii nieograniczona, w praktyce 5–10	Wysoki	Tak

Analiza wskaźnikowa polega na obliczaniu określonych mierników (wskaźników) na podstawie danych finansowych, niefinansowych lub mieszanych zawartych w sf (bądź stanowiących podstawę ich sporządzenia), porównywaniu ich w czasie i na wybrany moment oraz wyciąganiu na tej podstawie wniosków. Wskaźniki obrazują relacje ekonomiczne, zachodzące między wzajemnie powiązanymi wielkościami. Trzeba jednak pamiętać, że samo obliczenie wskaźników nie jest tożsame z przeprowadzeniem przez biegłego rewidenta procedur analitycznych. Konieczne jest uzupełnienie o próbę wyjaśnienia znaczących odchyleń od wielkości oczekiwanych oraz uwzględnienie wyników analizy w dalszym badaniu.

Analiza wskaźnikowa jest jedną z najbardziej rozpowszechnionych (co nie znaczy najlepszych) technik analizy danych, stosowanych podczas badania. Pozwala ona na syntetyczną ocenę różnych aspektów działalności gospodarczej badanej jednostki. Uważa się ją za rozwinięcie tzw. wstępnej analizy sf[10], służącej poznaniu jednostki i zidentyfikowaniu ryzyk. Dzięki swobodzie doboru

[10] Przez to pojęcie rozumie się zwykle analizę pionową (struktury) i poziomą (dynamiki) bilansu oraz rachunku zysków i strat.

wskaźników[11] istnieje możliwość jej dostosowania do potrzeb biegłego rewidenta i specyfiki danej jednostki.

Prawidłowa analiza powinna się opierać na użyciu wielu powiązanych ze sobą wskaźników jednocześnie, a nie na wybiórczej analizie kilku wybranych wskaźników. Warunkiem prawidłowej interpretacji danego wskaźnika jest zrozumienie jego treści, określonej sposobem jego obliczenia, oraz świadomość istnienia ograniczeń z nim związanych. Przedmiotem analizy stosowanej w toku badania sf są zazwyczaj 4 główne kategorie wskaźników charakteryzujących:

- **płynność (zdolność do terminowego regulowania bieżących zobowiązań)** – analiza dostarcza informacji o posiadanych przez jednostkę źródłach dopływu środków pieniężnych, które mogą być w każdej chwili przeznaczone na spłatę zobowiązań,
- **aktywność gospodarcza (obrotowość)** – analiza rotacji wybranych składników aktywów trwałych i obrotowych; określa efektywność wykorzystania posiadanych przez jednostkę zasobów do wypracowania przychodów ze sprzedaży,
- **zadłużenie (wypłacalność)** – w toku analizy następuje weryfikacja struktury finansowania majątku jednostki pod względem zdolności do obsługi zadłużenia, a zwłaszcza zobowiązań długoterminowych, z istoty wykraczających poza ramy analizy płynności,
- **rentowność (zdolność posiadanych aktywów do wypracowania zysku)** – analiza stosowana do pomiaru relacji wielkości zysku, jaki wypracowuje jednostka, do jej przychodów oraz majątku lub kapitału zaangażowanego w działalność gospodarczą.

Wszystkie wymienione kategorie wskaźników najlepiej jest rozpatrywać łącznie, gdyż są ze sobą wzajemnie powiązane. Dobór danych i wskaźników charakteryzujących działalność jednostki nie może być stały. Celowe jest dostosowanie każdorazowo wskaźników do bieżącej sytuacji jednostki. Wymaga to rozwagi. Chodzi bowiem o taki zestaw wskaźników, który pozwoli w sposób syntetyczny określić obecną sytuację jednostki i trendy rozwojowe oraz wskazać na ew. zagrożenia dla kontynuowania przez nią działalności.

Większość wskaźników nie ma optymalnej wielkości. Dopiero odniesienie ich do odpowiednich pozycji bazowych, takich jak wskaźniki z poprzednich okresów lub średnie branżowe czy najlepsze w branży, umożliwia porównanie oraz w miarę obiektywną ocenę sytuacji ekonomiczno-finansowej badanej jednostki. Specyfika jej działalności ma tu ogromne znaczenie. Z góry można bowiem przewidzieć, jak będą się kształtowały niektóre wskaźniki. Przykładowo hipermarket będzie miał zwykle dużo gotówki w kasach, podczas gdy szybkość obrotu zapasu turbin wiatrowych będzie u ich producenta niewielka.

Dla ilustracji zamieszczam na następnej stronie fragment karty roboczej pochodzący z jednego z programów wspomagających pracę biegłego rewidenta w tym obszarze.

Główną zaletą analizy wskaźnikowej jest to, że ukazuje ona zmiany będące wynikiem decyzji gospodarczych podejmowanych w okresie sprawozdawczym oraz wpływu czynników niezależnych

[11] Metody obliczania wskaźników przez biegłych rewidentów nie regulują żadne standardy. W praktyce możliwe jest więc stosowanie różnych wzorów. Niektóre wskaźniki mają kilka nazw. Zdarza się, że wskaźniki określane jedną nazwą są obliczane na wiele różnych sposobów. Ze względu na ich powszechną dostępność (np. w internecie) w artykule nie podano żadnych przykładowych wzorów.

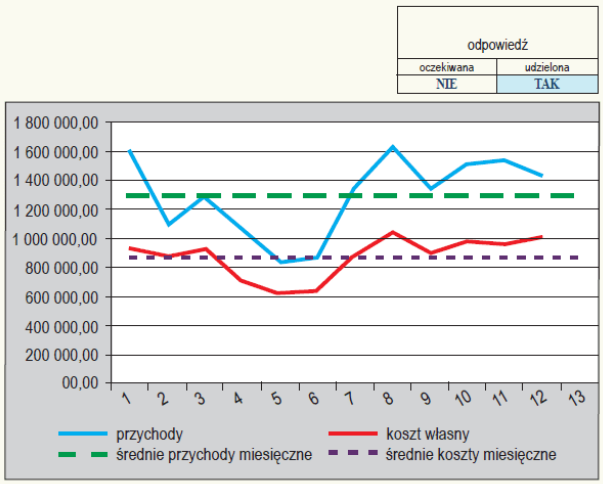
od kierownictwa danej jednostki. Jest to zarazem szybka i skuteczna metoda uzyskiwania wglądu w operacje gospodarcze i sposób funkcjonowania badanej jednostki.

Jej podstawowymi słabościami są: subiektywizm, fakt, że wymaga wyważonego doboru wskaźników, że interpretacja wyników nie może przebiegać w izolacji (należy ją uzupełnić i potwierdzić dzięki wynikom zastosowania innych procedur), że podstawą analizy jest głównie przeszłość badanej jednostki, dlatego jej przydatność np. do analizy zagrożeń dla kontynuacji działalności jest ograniczona. Wady analizy próbuje się minimalizować, stosując – przy akceptacji zlecenia i w toku samego badania – liniowe, wielowymiarowe analizy dyskryminacyjne, o czym będzie mowa w dalszej części artykułu.

c) czy występują „rozchwiane" marże w poszczególnych okresach miesięcznych w stosunku do średniej marży za rok

Rok objęty badaniem 2017	Przychody ze sprzedaży	Koszt własny sprzedaży	% uzyskanej marży	Odchylenie od średniej rocznej
styczeń	1 609 809,86	924 804,07	74,07	25,20
luty	1 084 988,57	879 038,90	23,43	−25,44
marzec	1 295 296,44	919 772,15	40,83	−8,04
kwiecień	1 044 404,23	695 944,66	50,07	1,20
maj	833 578,30	611 750,01	36,26	−12,61
czerwiec	868 520,29	627 384,04	38,44	−10,44
lipiec	1 351 559,19	891 917,85	51,53	2,66
sierpień	1 651 370,48	1 045 783,38	57,91	9,04
wrzesień	1 326 553,55	901 162,30	47,20	−1,67
październik	1 520 229,17	981 203,78	54,94	6,06
listopad	1 542 247,54	956 333,90	61,27	12,39
grudzień	1 422 403,00	1 010 739,75	40,73	−8,14
Razem	**15 550 960,62**	**10 445 834,79**	**40,87**	×

W przypadku wystąpienia istotnych różnic pomiędzy marżą roczną a marżą danego m-ca dokonać pogłębionych badań, ustalając przyczyny odchyleń oraz podjąć właściwą reakcję przez biegłego. Analizą można objąć plan miesięcznych przychodów i kosztów, porównując z wykonaniem, identyczną analizą można objąć rok poprzedni oraz obecny w układzie miesięcznym, stawiając pytania dotyczące przyczyn istotnych odchyleń.



Wnioski biegłego:

Analiza % uzyskanej marży, a także odchyleń od średniej marży rocznej wskazuje na duże rozbieżności pomiędzy poszczególnymi okresami miesięcznymi. Poziom marży wynosi od 74,07 do 23,43% (styczeń–luty). Przeprowadzić analizę przyczyn spadku sprzedaży w lutym. Wyjaśnić bardzo wysoki poziom marży w styczniu (brak kosztów ???). Sprawdzić ew. koszty sprzedaży w lutym i porównać do poprzednich lat kształtowanie się tych relacji. Jednostka charakteryzuje się sezonowością. W okresie letnim występuje zmniejszenie sprzedaży akcesoriów kominowych.

Źródło: APS-15, ARCHES Henryk Jankowiak.

Z analizą wskaźnikową ściśle się wiążą i są zwykle łączone w toku badania analiza trendu oraz analiza porównawcza. Celowo opisuję je oddzielnie, ponieważ stosuje się je nie tylko do wskaźników, lecz także do kluczowych mierników charakteryzujących jednostkę, wyrażonych w wielkościach absolutnych (np. suma bilansowa, aktywa netto, przychody ze sprzedaży, wynik finansowy netto). Analizie mogą podlegać ich dynamika oraz zmiany struktury (np. udział znaczących części majątku i zobowiązań w sumie bilansowej).

PRZYKŁAD

Firma audytorska bada sf jednostki kolejny rok. Za poprzedni okres wyrażono opinię bez zastrzeżeń. Jednostka prowadzi działalność poprzez sieć 5 marketów spożywczych działających na południu kraju. Wszystkie mają podobną ofertę asortymentową. Kluczowy biegły rewident objął analizą następujące dane dotyczące sprzedaży detalicznej (po zaokrągleniu):

Market	Sprzedaż w roku poprzednim po badaniu (tys. zł)	Sprzedaż w roku bieżącym przed badaniem (tys. zł)	Zmiana (tys. zł)	Zmiana (%)	Odchylenia wymagające wyjaśnienia zgodnie z przyjętym wcześniej poziomem akceptowalnych odchyleń (wartość lub %) wg wariantów postępowania biegłego rewidenta		
Lp.	A	B	B - A	(B - A) / A	W1	W2	W3
1	18 920	20 140	1 220	6,45	0	0	1
2	16 050	15 430	(620)	(3,86)	0	0	0
3	14 910	12 220	(2 690)	(18,04)	0	1	1
4	5 282	9 372	4 090	77,43	0	1	1
5	16 187	15 587	(600)	(3,71)	0	0	0
Razem	71 349	72 749	1 400	1,96	0	2	3

Wariant 1 (W1): Kluczowy biegły rewident zdecydował, że wyjaśnienia wymagają odchylenia wartościowe wyższe od istotności wykonawczej, ustalonej dla badania tego obszaru (Iw) lub wyższe niż 10% zmiany (rok do roku). Ten drugi wskaźnik został przyjęty, aby zidentyfikować nieoczekiwane odchylenia, nawet jeżeli wartościowo są one niższe od granicy istotności. Wskaźnik ten nie ma swojej optymalnej wielkości, więc należy go określić, kierując się osądem zawodowym. Iw ustalono na poziomie 70% istotności określonej dla całego sf (Io). Za podstawę ustalenia Io przyjęto 3% rocznych przychodów. Na tej podstawie przyjęte zostały następujące parametry (po zaokrągleniu) dla przeprowadzenia procedury: Io = 2180 tys. zł (72 749 tys. zł × 0,03); Iw = 1530 tys. zł (Io × 0,70).

W wyniku przeprowadzonych procedur analitycznych nie ujawniono odchyleń wymagających dalszej analizy, gdyż procedurze poddano tylko zagregowane dane roczne. W związku z tym ani zmiany wartościowe, ani procentowe nie przekroczyły akceptowalnych poziomów. Poziom pewności uzyskany przez biegłego rewidenta w wyniku przeprowadzenia tej procedury jest wyjątkowo niski. Nie powinno się jej zatem stosować ani na etapie planowania, ani do gromadzenia dowodów badania.

Wariant 2 (W2): Warunki wstępne jak w W1. Procedurę analityczną przeprowadzono na postawie danych rocznych pochodzących z każdego marketu. W jej wyniku ujawniono nieakceptowalne odchylenia (zawyżenia i zaniżenia przekraczające Iw i % zmiany) dotyczące marketów 3 i 4. Wymagają one dalszej analizy. Poziom pewności uzyskany przez biegłego rewidenta w wyniku przeprowadzenia tej procedury jest nadal niski, ale wyższy niż w W1. Procedura nie jest wystarczająco precyzyjna, aby ją wykorzystać do gromadzenia dowodów badania. Może natomiast być pomocna na etapie planowania.

Wariant 3 (W3): Warunki wstępne jak w W2. Biegły rewident, dla zwiększenia pewności wyników, postanowił jednak obniżyć wysokość akceptowalnych bez dalszej analizy odchyleń poniżej istotności wykonawczej. Nowa granica to 1200 tys. zł lub 8% zmiany (rok do roku). W wyniku przeprowadzenia procedury analitycznej ujawniono nieakceptowalne odchylenia dotyczące

marketów 1 (kryterium wartości) oraz 3 i 4 (kryteria wartości i zmiany). Poziom pewności uzyskany przez biegłego rewidenta jest wyższy niż w W2.

Procedura może być wykorzystywana do gromadzenia dowodów badania. Warto jednak rozszerzyć jej zakres. Wyjaśnienie odchyleń może polegać np. na powtórnym przeprowadzeniu procedur analitycznych, ale tym razem tylko w odniesieniu do 3 marketów i szczegółowych danych za poszczególne miesiące. Można również rozważyć bardziej precyzyjne określenie wartości oczekiwanych, np. dzięki porównaniu danych jednostki z wskaźnikami branżowymi[12], zastosowaniu analizy trendu, zaprojektowaniu testu racjonalności czy analizie regresji. Zawsze trzeba pamiętać, że nieakceptowalne różnice, których nie uda się racjonalnie wyjaśnić, muszą być w dalszym toku badania traktowane jak zniekształcenia.

Analiza trendu polega na porównaniu wskaźników lub innych wielkości obejmujących kilka lub kilkanaście okresów. Przy coraz szybszych zmianach otoczenia gospodarczego (co następowało w Polsce w ostatnich 20 latach) analizy trendu stosowane podczas rewizji finansowej są zwykle ograniczone do maksymalnie 3-letnich okresów. Wiąże się to również z ograniczonym dostępem biegłego rewidenta do danych historycznych i ich zwykle niską wiarygodnością.

Przedmiotem analizy może być również dynamika zmian porównywalnych wielkości ekonomicznych (np. wielkości przychodów ze sprzedaży). Przydatność tego rodzaju analizy dla biegłego rewidenta zależy przede wszystkim od jednorodności i zakresu porównywanych wielkości. Możliwe jest rozszerzenie zakresu analizy trendu przez powiązanie jej z opisaną dalej analizą regresji, co pozwala przewidzieć przyszłe kształtowanie się rozpatrywanych wielkości czy wartości. Może to być przydatne do oceny zasadności przyjętego przez kierownictwo danej jednostki założenia kontynuacji działalności jako podstawy sporządzenia badanego sf.

Analiza porównawcza polega na porównaniu obliczonych przez biegłego rewidenta wskaźników lub innych wielkości ze wskaźnikami bądź wielkościami dotyczącymi innych podmiotów działających w tej samej branży. Warunkami przydatności analizy są porównywanie danych za ten sam okres i identyczność obliczania zestawianych wskaźników lub wielkości. Uważa się, że ta technika analizy danych dostarcza dużo więcej istotnych informacji niż analiza trendu, ponieważ umożliwia wstępną ocenę sytuacji badanej jednostki na tle konkurencyjnych firm oraz ustalenie istotnych ryzyk, które inaczej można by przeoczyć.

PRZYKŁAD

Ustalenie, że zyskowność sprzedaży netto produktów (towarów) w badanej jednostce wynosi 15%, może doprowadzić biegłego rewidenta do całkowicie odmiennych wniosków, dotyczących rentowności działalności, jeżeli ustali na podstawie wiarygodnych danych branżowych, że średnia wysokość tego wskaźnika w innych podobnych podmiotach wynosi odpowiednio a) 7 lub b) 27%.

W pierwszym przypadku może to świadczyć zarówno o pozytywnej przewadze konkurencyjnej jednostki nad innymi jednostkami branży (np. przedmiotem sprzedaży są produkty lub towary o ponadprzeciętnej jakości, więc o wyższych wycenach), jak i o zniekształceniu sf wobec zaniżania

[12] Takimi jak wskaźnik LFL (*Like-for-Like*). Wskaźnik ten porównuje sprzedaż tych samych placówek dzisiaj i przed rokiem. Oznacza to, że do wyliczeń nie są brane sklepy, które otwarto w ciągu badanego roku lub nie funkcjonowały przez cały porównywany okres.

kosztów lub zawyżania przychodów. W drugim przypadku w grę wchodzą niekompletność przychodów, zawyżanie kosztów, nieatrakcyjność sprzedawanych produktów lub towarów, co może uzasadniać dokonanie odpisów aktualizujących wartość zapasów czy wprost wskazywać na problemy z kontynuacją działalności. Przyczyn może być wiele. Dlatego wszystkie znaczące odchylenia od oczekiwanych przez biegłego rewidenta wskaźników lub wielkości wymagają wyjaśnienia w toku badania.

Test racjonalności (zasadności) mimo braku podbudowy statystycznej umożliwia uzyskanie wysokiego poziomu pewności, że badana zbiorowość nie zawiera istotnego zniekształcenia. Technika ta polega na tym, że biegły rewident analizuje salda i obroty kont lub ich zmiany w różnych okresach sprawozdawczych, budując pewien logiczny model pozwalający – na podstawie znanych mu danych finansowych i/lub niefinansowych – określić oczekiwane wartości.

PRZYKŁAD

Biegły rewident uzyskał z działu kadr informację, że średnia miesięczna płaca wraz z narzutami wynosi w jednostce 7 tys. zł, a średnioroczne zatrudnienie pracowników to 90 osób. Racjonalnie spodziewany roczny koszt wynagrodzeń powinien być bliższy kwocie 7,6 mln zł (7 tys. zł × 90 × 12 mies.) niż np. 9 mln zł.

Podobnie będzie, jeżeli biegły zechce ustalić oczekiwaną wielkość przychodów z wynajmu powierzchni biurowej w kilku lokalizacjach. Może je obliczyć na podstawie zweryfikowanych danych niefinansowych odnoszących się do powierzchni budynków, średnich rynkowych stawek czynszu za 1 m2 w okolicy lokalizacji biur oraz uśrednionych danych dotyczących wynajętych powierzchni. Zawsze należy pamiętać, że sposób przeprowadzania testu racjonalności różni się w zależności od tego, czy ma on służyć identyfikacji i ocenie ryzyka (planowanie), czy bezpośrednio dostarczać dowodów wiarygodności określonych stwierdzeń. W tym drugim przypadku biegły powinien przed przeprowadzeniem procedury określić maksymalną wielkość odchylenia od wielkości oczekiwanej (kwotowo lub procentowo), które nie będzie wymagało dalszego wyjaśnienia i zostanie uznane za jeden z dowodów badania potwierdzających wiarygodność danego stwierdzenia (np. kompletności i dokładności kosztów wynagrodzeń lub ujęcia przychodów z wynajmu).

Jak wynika z przykładów, test racjonalności służy do subiektywnej oceny możliwego wpływu zjawisk i procesów ekonomicznych na poszczególne elementy sf. Nie zmienia to jednak faktu, że jest to technika bardzo przydatna w praktyce. Dla uzyskania wystarczającej pewności łączy się ją zwykle w toku badania z innymi procedurami nakierowanymi na dane zagadnienie.

Analiza regresji przeżywa obecnie swój renesans. Jest ona przykładem zastosowania metod statystycznych do rewizji finansowej. Regresja jest metodą umożliwiającą zbadanie i opisanie relacji zachodzących między różnymi poddanymi analizie wielkościami oraz wykorzystanie tej wiedzy do przewidywania nieznanych wartości jednych wielkości na podstawie znanych innych wielkości.

Regresja umożliwia warunkowe przewidzenie oczekiwanej wartości zmiennej losowej (tzw. zmienna objaśniana np. wielkość przychodów) dla znanej wartości innej zmiennej lub wektora zmiennych

losowych (tzw. zmienne objaśniające np. ilość sprzedanych produktów danej kategorii, średnia cena, wielkość zwrotów, udzielane rabaty, sezonowość sprzedaży, lokalizacja i wielkość odbiorców).

W praktyce stosowanie techniki regresji polega na sformułowaniu przez biegłego rewidenta wzoru matematycznego umożliwiającego obliczenie, jak powinny się kształtować określone wielkości i wartości w badanym sf. Technika ta ma tę przewagę nad innymi (np. testem racjonalności), że umożliwia zmierzenie w sposób naukowy prawdopodobieństwa pewności uzyskanych wyników.

Na potrzeby rewizji finansowej najczęściej stosuje się metody analizy, których przedmiotem są albo szeregi czasowe (np. prognoza wielkości sprzedaży na podstawie danych z kilku poprzednich lat), albo regresja wieloraka, nakierowana na ilościowe ujęcie związków między wieloma zmiennymi na jedną datę lub za okres (np. prognoza wielkości sprzedaży sieci supermarketów w danym roku przy znanej wielkości zapasów, liczbie pracowników, powierzchni sklepowej oraz ich lokalizacji).

Modele analizy oparte na regresji bywają włączane do skomplikowanych narzędzi (technik) wspomagających komputerowo badanie. Ich elementy stosuje się zwłaszcza przy badaniu sf dużych podmiotów z branży finansowej i ubezpieczeniowej. Trzeba przyznać, że poza największymi firmami audytorskimi stosowanie zaawansowanych metod analiz ma u nas na razie dość ograniczony zasięg, mimo że dysponując odpowiednim oprogramowaniem, można by je stosować do badania dużo większej liczby jednostek różnej wielkości. Dobre efekty daje także wykorzystanie arkusza kalkulacyjnego MS Excel[13].

PROCEDURY ANALITYCZNE A RYZYKO NIEMOŻNOŚCI KONTYNUOWANIA DZIAŁALNOŚCI

Ocena zagrożeń dla kontynuacji działalności ma decydujący wpływ na wycenę aktywów i pasywów w sf[14]. Zgodnie z KSB 570 Kontynuacja działalności biegły rewident powinien tak zaplanować i przeprowadzić badanie (w tym zdarzeń, które nastąpiły po dniu bilansowym), aby zebrać odpowiednie i wystarczające dowody badania, potwierdzające lub kwestionujące zasadność deklaracji kierownika jednostki o kontynuacji przez nią działalności. Ma on obowiązek wnikliwie rozpatrzyć jej zasadność, a zwłaszcza ocenić realność leżących u jej podstaw przesłanek. Przy dokonywaniu takiej oceny ważną rolę do odegrania mają procedury analityczne, które odpowiednio wcześnie zastosowane (najlepiej jeszcze na etapie akceptacji zlecenia, przed podpisaniem umowy o badanie) mogą oszczędzić wielu przykrych niespodzianek. Jest to więc także element oceny ryzyka zlecenia. Ew. problemy to brak zapłaty za badanie, negatywny wpływ na reputację firmy audytorskiej, zwiększona pracochłonność badania, trudności z utrzymaniem ryzyka badania na akceptowalnym poziomie czy nawet brak możliwość wyrażenia opinii.

[13] Można to zrobić na co najmniej 3 sposoby: przez narzędzie „Regresja" w dodatku „Analysis ToolPak", wykorzystując funkcję REGLINP albo pisząc samodzielnie odpowiednie formuły.

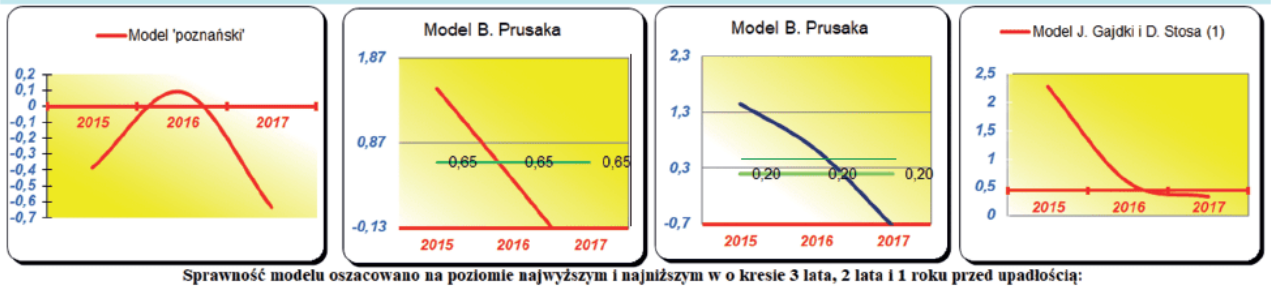
[14] Sf jednostek niekontynuujących działalności sporządza się wg innych zasad. W myśl art. 29 uor wycena aktywów następuje po cenach sprzedaży netto możliwych do uzyskania, nie wyższych od cen ich nabycia albo kosztów wytworzenia, pomniejszonych o dotychczasowe odpisy amortyzacyjne lub umorzeniowe, a także z tytułu trwałej utraty wartości, nie wyższych od ich wartości figurującej w księgach. Ponadto tworzy się rezerwę na przewidywane dodatkowe koszty i straty spowodowane zaniechaniem lub utratą zdolności do kontynuowania działalności.

Rekapitulacja przeprowadzonej analizy możliwości kontynuowania działalności wg przedstawionych powyżej modeli Z-scoringowych

Nazwa modelu		wynik przeprowadzonego testu za rok 2017	zastosowany wzorzec modelu
Ogólna konstrukcja modelu			Zi INE PAN =w0 + w1*x1+w2*x2+…wn*xn
szczegółowe	Zi=1	brak zagrożenia	Zi =1 INE PAN=5,577*Wsk.1+1,427*Wsk.2+0,154*Wsk.3+ 0,310* Wsk.4+ 1,937*Wsk.5+ 1,598*Wsk.6+ 3,203*Wsk.7+ 0,436*Wsk.8+ 0,192*Wsk.9+ 0,140*Wk.10+0,386*Wsk.11+ Log10Aktywów-9,832
szczegółowe	Zi=2	brak zagrożenia	Zi=2 INE PAN=5,837*Wsk.1+ 2,231*Wsk.2+ 0,222*Wsk.3+ 0,496*Wsk.4+ 0,945*Wsk.5 + 2,028* Wsk.6+ 3,472*Wsk.7+ 0,495*Wsk.8+ 0,166*Wsk.9+ 0,195*Wk.10+0,030*Wsk.11-0,392
szczegółowe	Zi=3	brak zagrożenia	Zi=3 INE PAN=5,896*Wsk.1+2,831*Wsk.2+0,539*Wsk.5+2,538*Wsk.6+ 3,655* Wsk.7+ 0,467*Wsk.8+ 0,179*Wsk.9+ 0,226*Wk.10+0,168*Wsk.11-0,678
szczegółowe	Zi=4	brak zagrożenia	Zi=4 INE PAN=6,028*Wsk.1+ 6,546*Wsk.2+ 1,546*Wsk.5+ 1,463*Wsk.6+ 3,585*Wsk.7+ 0,363*Wsk.9+0,172*Wk.10+0,114*Wsk.11-0,593
szczegółowe	Zi=5	brak zagrożenia	Zi=5 INE PAN =9,004*Wsk.2+1,177*Wsk.5+ 1,889*Wsk.6+3,134*Wsk.7+ 0,500*Wsk.9+0,160*Wk.10+0,749*Wsk.11-1,962
szczegółowe	Zi=6	brak zagrożenia	Zi=6 INE PAN =9,478* Wsk.2+3,613*Wsk.5+ 3,246*Wsk.7+0,455*Wsk.9+ 0,802*Wsk.11-2,478
szczegółowe	Zi=7	zagrożony upadłością	Zi=7 INE PAN = 9,498*Wsk.2+3,566*Wsk.5+ 2,903*Wsk.7+0,452*Wsk.9-1,498
Model B. Prusaka		zagrożony upadłością	ZBP2'=1,4383*x1+0,1878*x2+5,0229*x3-1,8713
Model B. Prusaka		zagrożony upadłością	ZBP1'=6,5245*x1+0,1480*x2+0,4061*x3+2,1754*x4-1,5685
Model 'poznański'		zagrożony upadłością	ZHCP =3,562*x1+1,588*x2+4,288*x3+6,719*xn-2,368
Model A. Holdy		prawdopodobieństwo upadłości bardzo duże	ZH1=0,605+6,81*10-1 PWP-1,96x*10-2 SZ+9,69*10-3ZM +6,72*10-4WOZO+1,57*10-1 RM
Model J. Gajdki i D. Stosa (1)		zagrożony upadłością	Z=0,20098985*x1+0,0013027*x2+0,7609754*x3+0,9659628*x4-0,341096*x5
Podsumowanie wyników		Wynik testu Strefa pośrednia = Zagrożenie upadłością	W wyniku przeprowadzenia testowania 12 modeli zagrożenia upadłością ustalono w 6 modelach.

Model B. Prusaka	Model B. Prusaka	Model 'poznański'	Model J. Gajdki i D. Stosa (1)
ZBP2'=1,4383*x1+ 0,1878*x2+5,0229*x3-1,8713	ZBP1'=6,5245*x1+0,1480*x2+ 0,4061*x3+2,1754*x4-1,5685	ZHCP =3,562*x1+1,588*x2+ 4,288*x3+6,719*xn-2,368	Z=0,20098985*x1+0,0013027*x2+0,760975 4*x3+0,9659628*x4-0,341096*x5

Oznaczone wykresy posiadają zdolność do sygnalizowania mogących pojawić się trudności na dwa lata przed upadłością w modelu ZBP2 a model ZBP1 nawet 3-4 lat przed upadłością, a model Z na 3 lata przed upadłością



Sprawność modelu oszacowano na poziomie najwyższym i najniższym w o kresie 3 lata, 2 lata i 1 roku przed upadłością:

92,36%	95,71%	94,29%	73,47 % do 84,25 %

Źródło: APS Analiza finansowa; wyd. ARCHES Henryk Jankowiak

Warto zwrócić uwagę, że na polskim rynku jest już sporo narzędzi wspomagających pracę biegłego rewidenta, także w zakresie procedur analitycznych. Dla ilustracji powyżej zamieszczam sporządzony za pomocą jednego z dostępnych na rynku programów komputerowych fragment analizy zagrożeń dla kontynuacji działalności. Program ten posługuje się ponad 20 różnymi modelami dostosowanymi do specyfiki krajowych jednostek produkcyjnych, handlowych oraz usługowych. Karty powstają automatycznie po wczytaniu danych finansowych za 3 kolejne okresy (analiza zawiera łącznie ponad 50 stron wydruku).

PROCEDURY ANALITYCZNE A WYKRYWANIE ZNIEKSZTAŁCEŃ SPOWODOWANYCH OSZUSTWEM

Wykrywanie oszustw nie jest bezpośrednim celem biegłego rewidenta przeprowadzającego badanie sf. To kierownictwo jednostki oraz osoby (organy) sprawujące nad nią nadzór są odpowiedzialne za zapobieganie oszustwom i błędom oraz ich wykrywanie. Nie znaczy to jednak, że w trakcie badania

zagadnienie to może pozostać poza strefą zainteresowań biegłego. Wręcz przeciwnie. KSB 200.5[15] jednoznacznie stanowi, że podstawą do wyrażenia opinii biegłego rewidenta jest uzyskanie przez niego wystarczającej pewności, czy sf jako całość nie zawiera istotnego zniekształcenia, niezależnie od tego, czy powstało ono w wyniku błędu, czy oszustwa. Dotyczy to więc zarówno przypadkowych, jak i zamierzonych nieprawidłowości.

Próby zatajenia faktów i dokonania oszustw trudniej wykryć niż przypadkowe błędy, gdyż zazwyczaj istnieje zmowa między zainteresowanymi osobami, a podejrzenia mogą sięgać nawet kierownictwa najwyższych szczebli.

Warto więc przypomnieć zapisy KSB 240[16]. Standard ten w sposób szczególny określa zadania w zakresie oceny ryzyka oszustwa i procedury z tym związane. Zgodnie z nimi biegły rewident powinien uwzględnić podczas badania ryzyko oszustwa. Każde badanie zaczyna się od identyfikacji ryzyk, na jakie narażona jest dana jednostka. Oddzielnego ustalenia wymagają czynniki wpływające na ryzyko działalności gospodarczej i ryzyko oszustwa. Dzieje się tak, bo szacowanie ryzyka działalności gospodarczej i reakcja na nie mogą się znacząco różnić od oszacowania i reakcji na ryzyko oszustwa.

Biegłego rewidenta powinny interesować te oszustwa – faktyczne lub domniemane – które są na tyle znaczące, że zniekształcają badane sf. W szczególności chodzi o zawłaszczenie majątku i oszukańczą sprawozdawczość finansową. Przypadki zawłaszczenia majątku są o wiele częstsze niż fałszowanie sf. Jeżeli jednak dochodzi do zafałszowań sf, wartość zniekształceń jest znacznie większa niż zawłaszczeń. Zależność taką potwierdzają od lat badania, co przekłada się na wskazówki dla oceny ryzyka oszustw i zawłaszczeń przez biegłego rewidenta. Jeżeli stwierdzi on istnienie czynników zwiększających ryzyko oszukańczej sprawozdawczości, to musi być świadomy, że ryzyko zniekształcenia sf jest nieporównanie większe niż wtedy, gdy czynniki ryzyka będą wskazywać na sprzeniewierzenia majątku.

Przez lata panowało przekonanie, że tradycyjne narzędzia analityczne, takie jak analiza wskaźnikowa, są mało skuteczne w wykrywaniu nieprawidłowości będących wynikiem celowych oszukańczych działań. Obecnie sytuacja jest inna. Rozbudowane modele wielowymiarowej analizy regresji, oparte na odpowiednio szczegółowych danych czerpanych wprost z systemu informacyjnego jednostki, umożliwiają niejako „przy okazji" realizacji swoich głównych zadań ujawnienie podejrzanych relacji czy trendów. Pojawiło się też sporo narzędzi od początku projektowanych z myślą o wykrywaniu manipulacji finansowych.

Część z nich została oparta na tzw. prawie Benforda[17], które dotyczy częstości występowania znaczących cyfr w zbiorach losowych. Wiele osób nie zdaje sobie sprawy, że w bardzo wielu zbiorach danych pewne cyfry występują częściej na pierwszej pozycji niż inne (patrz tabela).

---

[15] KSB 200 Ogólne cele niezależnego biegłego rewidenta oraz przeprowadzanie badania zgodnie z Międzynarodowymi Standardami Badania.

[16] KSB 240 Odpowiedzialność biegłego rewidenta podczas badania dotycząca oszustw.

17 Od F.A. Benforda, amerykańskiego inżyniera z General Electric. Prawidłowość wiązana powszechnie (niekoniecznie słusznie) wyłącznie z nim bywa też nazywana „prawem pierwszej cyfry". Artykuł dr. M. Folcika nt. wykorzystania tego prawa – przy zastosowaniu programu Excel – zamieszczono w „Rachunkowości" nr 11/2015.

PRZYBLIŻONE PRAWDOPODOBIEŃSTWO WYSTĘPOWANIA OKREŚLONEJ PIERWSZEJ CYFRY

Pierwsza cyfra	Rozkład Benforda (%)	Rozkład intuicyjny (%)
1	30,1	11,1
2	17,6	
3	12,5	
4	9,7	
5	7,9	
6	6,7	
7	5,8	
8	5,1	
9	4,6	

Jak wynika z tabeli, jedynka występuje jako pierwsza cyfra w 30,1% przypadków, a dla porównania cyfra 7 pojawia się tylko w 5,8% przypadków. Wniosek jest oczywisty: im mniejsza cyfra, tym większe prawdopodobieństwo, że pojawi się na początku liczby.

PRZYKŁAD

Mając dostęp do bazy danych badanej jednostki, zawierającej wszystkie transakcje w roku obrotowym, można stwierdzić w nich nieprawidłowości w rozkładzie pierwszej, ale też drugiej i kolejnych cyfr. Możliwe jest również przeprowadzenie testów sprawdzających częstotliwość występowania kilku cyfr jednocześnie na różnych miejscach oraz liczących sumę wszystkich transakcji dla danej kombinacji cyfr (przydatnych do zidentyfikowania pojedynczych nieprawidłowości o dużej wartości). Wszystkie wspomniane testy polegają na porównaniu rzeczywistej częstotliwość występowania cyfr z prognozowaną wg rozkładu Benforda.

Prawo Benforda dało producentom oprogramowania możliwość stworzenia narzędzi analizujących częstotliwość występowania cyfr w określonych zbiorach. Tego typu narzędzia[18] są stosowane do analizy naturalnych zbiorów, takich jak dane rachunkowe, podatkowe[19], ubezpieczeniowe i wielu innych, jako podstawa wykrywania nadużyć. W toku badania sf zaobserwowano szczególną

[18] Np. dostępna w Polsce wersja 9 programu IDEA umożliwia przeprowadzenie licznych testów danych na podstawie prawa Benforda. Analizy są przeprowadzane w sposób półautomatyczny z możliwością samodzielnego dostosowania parametrów programu do potrzeb użytkownika. Więcej informacji na ten temat na stronie internetowej: www.pbsg.pl/zastosowanie-prawa-benforda-w-analizie-danych.

[19] Za ich pomocą można np. ujawnić fikcyjne faktury ujęte jako koszt uzyskania przychodu. Kwoty na fakturach również podlegają prawu Benforda, więc ich zbyt „równomierne" rozłożenie jest stosunkowo łatwe do wykrycia.

przydatność tego prawa do testowania transakcji gotówkowych, zapisów na kontach należności, zapasów i zobowiązań. Za pomocą takich narzędzi można zidentyfikować manipulowanie czekami, błędną wycenę zapasów, wartości tuż poniżej limitów wymagających autoryzacji, podwójne płatności lub podwójne numery faktur i wiele innych nieprawidłowości.

Stosowanie narzędzi opartych na rozkładzie Benforda jest celowe w odniesieniu do stosunkowo dużych zbiorów danych (powyżej kilku tysięcy), w miarę możliwości wielocyfrowych. Przy badaniach sf bardzo małych jednostek ich przydatność jest więc niewielka.

Biegli rewidenci, którzy chcieliby zastosować takie narzędzia w praktyce, powinni pamiętać, że wspomniana prawidłowość jest obserwowana w wielu zbiorach, ale nie we wszystkich. W pewnych zbiorowościach ujawnienie częstotliwości występowania cyfr zgodnych z prawem Benforda będzie wskazywać na możliwość manipulacji. Dzieje się tak, bo dane o niewielkiej zmienności, w sposób sztuczny ograniczone lub o charakterze powtarzalnym, nie mają takiego rozkładu.

PODSUMOWANIE

Jak starałem się udowodnić, pojęcie „procedur analitycznych” jest szerokie. Są one stosowane do wielu obszarów i zagadnień. Mogą też być w różny sposób wykorzystywane na poszczególnych etapach badania.

Zmiany w otoczeniu wymuszają na biegłych rewidentach przesunięcie nacisku z prostych technik, takich jak analiza wskaźnikowa, na narzędzia oparte na prawach statystyki i rachunku prawdopodobieństwa, gdyż umożliwiają one precyzyjną ocenę uzyskanych wyników. Towarzyszący temu rozwój specjalistycznych narzędzi informatycznych pozwala na analizowanie ogromnych ilości danych szybciej i z coraz większą precyzją, pod warunkiem zdobycia przez biegłych nowej wiedzy i kompetencji.

JAK ZBUDOWAĆ SKUTECZNĄ OCHRONĘ WEWNĘTRZNĄ – SPOJRZENIE PRAKTYKA

W artykule przedstawiono ogólne przesłanki stosowania systemu ochrony (kontroli) wewnętrznej – zwłaszcza w małych przedsiębiorstwach – celowość, opłacalność, obszary, warunki sprawnego działania i ograniczenia.

Rozumienie pojęcia „kontrola wewnętrzna" w przedsiębiorstwach prywatnych wywołuje wiele nieporozumień. Bywa ono odmiennie rozumiane przez właścicieli, personel kierowniczy, pracowników różnych szczebli i strony trzecie. Sprawa jest ważna, ale często przedstawiana nieprawidłowo. Jest to jedno z tych pojęć, które obrosło nadmierną „naukowością", stając się niezrozumiałe dla większości zwykłych zjadaczy chleba. Warto więc przyjrzeć się tej tematyce bliżej i spojrzeć na nią w sposób praktyczny (użytkowy).

OCHRONA „SZYTA NA MIARĘ"

Już samo słowo „kontrola" odstrasza, a zarazem wprowadza w błąd. Sugeruje ingerencję z zewnątrz, coś narzuconego i niemile widzianego (kontrola wg słownika języka polskiego PWN to *sprawdzanie czegoś*, *zestawianie stanu faktycznego ze stanem wymaganym*, *nadzór nad kimś lub nad czymś*, *potocznie instytucja lub osoba sprawująca nad czymś nadzór*[20]). Tymczasem w przypadku kontroli wewnętrznej nie tyle chodzi o „kontrolę", co o zapewnienie ochrony interesów przedsiębiorcy oraz bezpieczeństwo (komfort) racjonalnego zarządzania.

Ochrona jest wewnętrzna, gdy sprawują ją osoby zatrudnione w jednostce[21].

Ochrona majątku i działań przedsiębiorstwa sprawowana siłami własnymi (wewnątrz) jest obiektywnie potrzebna. Nie chodzi tylko o bezpieczeństwo zasobów przedsiębiorstwa (właściciela). Jest to tylko jeden z powodów jej wprowadzenia. Główna przyczyna jest inna. Działalność gospodarcza wiąże się nieuchronnie z niepewnością i nieprzewidywalnością. Każde przedsiębiorstwo, prowadzące taką działalność, ma jakieś cele. Ich realizacji zagraża wiele czynników zewnętrznych lub wewnętrznych.

Przedsiębiorca może mieć wpływ na ograniczenie prawdopodobieństwa ich wystąpienia lub zmniejszenie ew. ich skutków[22], tworząc odpowiednie bariery ochronne. Praktycznie można uznać, że wszystkie działania podejmowane dla zapobiegania, ograniczenia prawdopodobieństwa zaistnienia lub zmniejszenia negatywnych skutków zrealizowania się ryzyka – a przez to przyczyniające się do osiągnięcia celów – są elementem ochrony wewnętrznej.

---

[20] Zob. sjp.pwn.pl/sjp/kontrola;2473611.html

[21] Lub grupie kapitałowej, której częścią jest jednostka.

[22] Skutki te nie zawsze muszą mieć czysto materialny charakter. Utrata reputacji (wiarygodności) jest zwykle dużo większym problemem dla przedsiębiorcy niż drobna kradzież w magazynie czy nieściągalność pojedynczej należności.

Analizując to zagadnienie, trzeba pamiętać, że przedsiębiorca chce przede wszystkim realizować swoje własne, a nie narzucone mu cele. Przykładowo dla większości przedsiębiorców celem nie jest „przestrzeganie prawa podatkowego" (jako cel samoistny), ale „bezpieczeństwo podatkowe", rozumiane jako zapewnienie, że nie poniosą negatywnych skutków jego niewłaściwej interpretacji lub naruszenia (np. kar, nieplanowanych wypłat wobec stwierdzenia zaległości, wstrzymania zwrotu VAT, tracenia czasu na odwołania itd.).

Podobnie autor nie spotkał jeszcze przedsiębiorcy, który bezinteresownie chciałby, aby jego „składane na zewnątrz" sprawozdania finansowe przedstawiały „rzetelny i jasny obraz sytuacji majątkowej, finansowej i wyniku działalności jednostki". Przedsiębiorca chce, aby przedkładane przez niego sprawozdanie finansowe nie zostało zakwestionowane. W wielu mniejszych firmach te same osoby są zarazem właścicielami, jak i zarządzającymi, i nie potrzebują formalnego potwierdzania (a tym bardziej kwestionowania) przez innych (np. biegłych rewidentów) wiarygodności sprawozdań finansowych. Bywa, że prawdziwy obraz pokazywany jest tylko w raportach wewnętrznych, które nie powstają z myślą o stronach trzecich i rzadko do nich trafiają. W praktyce chodzi więc głównie o to, aby jak najmniejszym kosztem zaspokoić potrzeby kredytodawców lub/i wymogi ustawowe i nie narazić się na ew. sankcje za ich nieprzestrzeganie.

Nie oznacza to oczywiście, że wymogi prawa nie mogą pokrywać się z potrzebami przedsiębiorców. Bardzo często występuje zbieżność interesów stron. To, czego przedsiębiorca na pewno nie potrzebuje, to „kontrola dla kontroli". Potrzebna mu jest rozsądna tzn. ani zbyt „sztywna", ani zbyt kosztowna ochrona (zapewnienie bezpieczeństwa). Jest ona tym bardziej skuteczna, im bardziej się z nią utożsamia (nie wystarczy jej „narzucić"). Patrząc na zagadnienie z perspektywy typowego (jeśli taki istnieje) małego przedsiębiorcy, chce on m.in. aby:

- jego pieniądze ulokowane w przedsiębiorstwie były bezpieczne i racjonalnie wykorzystywane,
- w firmie nie dochodziło do kradzieży, malwersacji, oszustw (zawinionych przez strony trzecie, jak i pracowników[23]),
- było zapewnione bezpieczeństwo podatkowe i księgowe,
- system informacyjny[24] działał poprawnie, przekazując na czas niezbędne do zarządzania i nadzorowania informacje o zagrożeniach, sytuacji majątkowej, finansowej i wynikach działalności.

Jak wynika z rozważań, ochrona przedsiębiorcy (a nie przedsiębiorstwa – ono stanowi tylko jedno z jego aktywów) jest wdrażana na skutek obiektywnego istnienia takiej potrzeby, z własnej inicjatywy; nie wynika z przepisów, bo nikogo nie powinno się na siłę uszczęśliwiać. Jeżeli państwo, samorząd lub ich organy próbują to robić, lepiej (uczciwiej) nazwać to wprost zleconą „kontrolą

[23] Badania ankietowe wśród członków amerykańskiego stowarzyszenia zrzeszającego ekspertów zajmujących się wykrywaniem tego typu przestępstw (ACFE) wykazały, że straty przedsiębiorstw w wyniku nadużyć pracowniczych szacuje się na 5% ich rocznych przychodów (w skali globalnej). Pierwszą przyczyną na liście słabości organizacyjnych, które przyczyniły się do faktycznie stwierdzonych przypadków nadużyć, był brak kontroli (ochrony) wewnętrznej w danym obszarze, a drugą – obejście istniejących czynności (procedur) kontrolnych. Stwierdzono również, że w mniejszych jednostkach dużo niższy jest wskaźnik wprowadzonych i działających mechanizmów nastawionych na zapobieganie i wykrywanie nadużyć, przez co – biorąc pod uwagę ich ograniczone zasoby – są one narażone na większe ryzyko niż duże firmy (zob. acfe.com/rttn2016.aspx).

[24] W tym jego część informatyczna.

zewnętrzną”[25]. Główne różnice między tak rozumianymi pojęciami z punktu widzenia przedsiębiorcy przedstawia tabela na następnej stronie.

KONTROLA ZEWNĘTRZNA A OCHRONA WEWNĘTRZNA

Wyszczególnienie	Kontrola zewnętrzna	Ochrona wewnętrzna
Realizowane cele	narzucone przez strony trzecie	określone przez przedsiębiorcę
Postrzeganie przez przedsiębiorcę	działanie na rzecz innych	działanie w swoim interesie
Narzędzia realizacji	ściśle określone przez innych	dowolnie określane przez przedsiębiorcę
Adresat procedur kontrolnych	przedsiębiorca	osoby pracujące na rzecz przedsiębiorcy i strony trzecie
Główny beneficjent	strony trzecie	przedsiębiorca
Wdrożenie	zwykle pełny system	system lub wybrane elementy
Stopień sformalizowania	znaczny	zależny od przedsiębiorcy
Obowiązek udokumentowania	istnieje zawsze	zależny od przedsiębiorcy
Koszt	niezależny od przedsiębiorcy	w znacznym stopniu zależny od przedsiębiorcy

Zorganizowanie – lub nie – ochrony i jej zakres oraz sposób funkcjonowania zależą przede wszystkim od właścicieli danego przedsiębiorstwa, jego kierownictwa i/lub organów nadzorczych. Nie musi być ona kosztowna, jeżeli zostaną wykorzystane proste narzędzia realizacji celów przedsiębiorcy i wbudowane w rozwiązania, które i tak muszą być stosowane (np. wystawianie faktur czy inkaso należności).

Budowa systemu ochrony musi być przemyślana z punktu widzenia możliwych alternatyw oraz relacji: koszt działania – osiągane korzyści. Niekoniecznie musi to być system kompletny, obejmujący wszystkie obszary działalności przedsiębiorstwa. Innej ochrony potrzebuje fabryka farmaceutyczna, a innej producent odzieży, inaczej chroni się zapasy, a inaczej prawidłowość obliczenia wynagrodzenia za pracę na akord. Ochrona jako system lub jego wybrane elementy musi być „szyta na miarę”. Wspólną cechą rozwiązań powinno być zawsze to, że mają chronić i wspomagać, a nie utrudniać realizację celów właściciela[26].

W artykule zostaną zaprezentowane przesłanki wymagające uwzględnienia przy budowie skutecznej ochrony wewnętrznej jako pełnego systemu lub wybranych jego elementów. Nie wyczerpuje on tematu i koncentruje się na mniejszych przedsiębiorstwach.

[25] Nawet jeżeli realizować ją muszą w praktyce pracownicy jednostki lub sam przedsiębiorca.

[26] Cele te nie zawsze muszą być tożsame z celami stron trzecich.

W szczególności chodzi o przybliżenie praktycznego, uniwersalnego i „przyziemnego" (w dobrym tego słowa znaczeniu) charakteru ochrony z punktu widzenia potrzeb mniejszych firm. Dlatego artykuł nie odnosi się wprost do takich koncepcji „kontroli wewnętrznej" jak model COSO, jego kolejne odmiany czy "ich wykorzystanie w trzech (lub pięciu) liniach obrony". To samo dotyczy możliwego cytowania licznych, powiązanych z tymi koncepcjami definicji. Autor starał się uwypuklić praktyczne aspekty i mechanizmy typowe dla mniejszych firm z punktu widzenia faktycznych (bez względu na to, jakie one są) potrzeb ich właścicieli lub działającego w ich imieniu kierownictwa.

Jeśli któryś z Czytelników po przeczytaniu artykułu powie, parafrazując Molierowskiego pana Jourdain: „U licha! Już od tylu lat zajmuję się ochroną wewnętrzną, nic o tym nie wiedząc"[27], zamysł autora zostanie zrealizowany.

CEL I PRZESŁANKI TWORZENIA SYSTEMU OCHRONY WEWNĘTRZNEJ

Każde przedsiębiorstwo prowadzące działalność gospodarczą jest narażone na różnego rodzaju ryzyko – zewnętrzne i wewnętrzne. Nie istnieje uniwersalny zbiór czynników ryzyka pasujących do każdego podmiotu. Na inne ryzyka jest narażony sklep, na inne bank, a na jeszcze inne fabryka czy hurtownia.

Niektóre czynniki ryzyka zewnętrznego mogą dotyczyć większości przedsiębiorstw (np. wzrost stawek podatkowych czy zmiana stóp procentowych). Inne dotyczą w szczególnym stopniu określonych podmiotów lub branż (np. Brexit wpłynie w większym stopniu na firmy handlujące whisky czy zapewniające przejazd do i z Wielkiej Brytanii niż na eksporterów mebli do Niemiec).

W odniesieniu do mniejszych jednostek o ograniczonych zasobach praktycznie zawsze należy brać pod uwagę niepewność co do możliwości kontynuacji działalności oraz ryzyko płynności, wynikające np. z nieuzyskania należnej zapłaty, utraty znaczących klientów bądź trudnych relacji z instytucjami finansującymi ich działalność.

Wewnętrzne czynniki ryzyka wiążą się głównie ze sposobem działania i organizacją przedsiębiorstwa. Zaliczyć do nich można: ustalenie nierealistycznych lub niewłaściwych celów strategicznych czy operacyjnych, wejście w nowe obszary działalności bez posiadania wystarczających zasobów, kompetencji i doświadczenia, zmiany oferty produktowej, zmiany i przekształcenia kapitałowe lub własnościowe, rodzaj dokonywanych transakcji, charakter i rodzaj świadczonych usług i produktów stanowiących przedmiot sprzedaży, strukturę organizacyjną, rotację kierownictwa lub kluczowego personelu, kompetencje pracowników i poziom kultury organizacyjnej, skuteczność wewnętrznych zasad promujących etyczne postępowanie i dobre praktyki.

O ile ryzyku zewnętrznemu trudno przeciwdziałać w sposób systematyczny, to ryzyko wewnętrzne można ograniczać. Ryzyku, które jest powtarzalne i znaczące, przedsiębiorstwa przeciwdziałają, organizując system ochrony wewnętrznej, mający na celu zmniejszenie prawdopodobieństwa realizacji ryzyka, a co najmniej ograniczenie negatywnych skutków jego ziszczenia się. Zawiera on w sobie określone polityki (zasady) działania i procedury, np. dotyczące ochrony majątku, fakturowania sprzedaży, akceptacji wydatków czy naboru pracowników. W założeniu mają one służyć osiągnięciu określonych celów – uniemożliwiać łatwe wyniesienie składnika zapasów lub

[27] W sztuce Moliera *Mieszczanin szlachcicem* wspomniany pan Jourdain mówi do nauczyciela filozofii: „Daję słowo, zatem ja już przeszło 40 lat mówię prozą, nie mając o tym żywnego pojęcia".

ruchomości, chronić przed udzieleniem nieuzasadnionych rabatów, nie dopuścić do nieracjonalnych wydatków itd.

Zanim przedsiębiorstwo zacznie budować kompleksowy system ochrony wewnętrznej lub tylko jego wybrane – z uwagi na znaczenie – elementy, warto zastanowić się, jakie istnieją zagrożenia i czy możliwa jest skuteczna i zarazem opłacalna ochrona przed nimi. W tym celu trzeba odpowiedzieć sobie na następujące pytania:

- Jakie są cele strategiczne i operacyjne przedsiębiorstwa?
- Jakie są główne zagrożenia dla ich realizacji?
- Jak i kiedy przedsiębiorstwo dowiaduje się o możliwych zagrożeniach?
- Na czym polega ryzyko, jakie niosą te zagrożenia i czy jest ono znaczące?
- Czy rozpoznane ryzyka dotyczą transakcji i zdarzeń następujących w skali roku często, czy rzadko?
- Jakie jest prawdopodobieństwo realizacji „czarnego scenariusza" (ziszczenie się ryzyka) i jego ew. skutki?
- Co można zrobić, aby przedsiębiorstwo (właściciela) zabezpieczyć przed ryzykiem?
- Czy ryzyko da się w części lub całości przenieść na strony trzecie (np. ubezpieczyciela)?
- Jaki poziom ryzyka można zaakceptować (uznać za niewymagający szczególnej ochrony)?
- Ile wynosiłby koszt ew. wewnętrznej i/lub zewnętrznej ochrony i czy nie przekroczyłby on korzyści?
- W jakich obszarach zabezpieczenia muszą być sztywne, a w jakich powinny być elastyczne?
- Czy potrzebne jest sformalizowanie mechanizmów zapewniających ochronę?
- Czy trzeba będzie i jak często weryfikować (aktualizować) sposób zaprojektowania, wdrożenie i operacyjną skuteczność działania ochrony (jako całości i/lub poszczególnych jej elementów)?

PRZYKŁAD

Jednym z podstawowych zagrożeń, przed jakim stoi większość przedsiębiorców, jest to, że za wykonane usługi lub dostarczone towary nie dostaną oni zapłaty. Wybór możliwych zabezpieczeń z tym związanych jest ogromny. Wymieńmy niektóre z nich:

- zapłata z góry lub znacząca zaliczka,
- limity kredytu kupieckiego (sprawdzani na bieżąco, bardziej wiarygodni odbiorcy mają wyższe limity),
- żądanie dodatkowego zabezpieczenia płatności (weksel, gwarancje bankowe, cesje, umowy, zastaw, hipoteka itd.),
- ubezpieczenie należności,

- faktoring.

Każde z tych zabezpieczeń (mechanizmów ochronnych) ma określony koszt. Dotyczy to również żądania zapłaty z góry. Z jednej strony redukuje się ryzyko niespłacenia transakcji praktycznie do zera, ale z drugiej maleje konkurencyjność firmy, a przez to liczba potencjalnych klientów. Przy doborze mechanizmów ochronnych warto więc pamiętać, aby były one racjonalne, gdyż zbytnia uciążliwość dla drugiej strony może spowodować rezygnację ze współpracy.

Przykładowe ogólne mechanizmy zabezpieczające[28] realizację celów przedsiębiorstwa (właściciela) spotykane w praktyce funkcjonowania podmiotów różnej wielkości to:

- nadzór właścicielski,
- nadzór kierowniczy (ochrona pionowa),
- ochrona funkcjonalna (pozioma),
- ochrona instytucjonalna,
- wspomaganie technicznymi zabezpieczeniami.

Pod pojęciem **nadzoru właścicielskiego** rozumie się ochronę (egzekwowanie praw własnościowych) wykonywaną w ramach powoływanych statutowo lub w umowie organów nadzoru nad jednostką, takich jak np. rada nadzorcza, komisja rewizyjna czy komitet audytu[29]. Tak rozumiany nadzór odnosi się tylko do relacji panujących pomiędzy właścicielami przedsiębiorstwa (nadzorujący) a najemnymi kierownikami (zarządzający) i pomija pozostałych interesariuszy. W Polsce – pomijając jednostki zainteresowania publicznego – w większości przypadków nadzór sprawowany nad przedsiębiorstwami ma charakter wewnętrzny i jest bardziej właścicielski aniżeli korporacyjny.

Ochrona wewnętrzna – jak już wspomniano – jest jedną z czynności zarządczych. W ramach **nadzoru kierowniczego** (ochrona pionowa) istnieje możliwość wydawania na bieżąco odpowiednich poleceń, pouczeń, korygowania decyzji itp. Bez (pionowej) ochrony wewnętrznej zarządzający każdego szczebla hierarchii organizacyjnej przedsiębiorstwa nie mieliby pewności, że nałożone przez nich na poszczególne podległe im osoby lub komórki zadania są wykonywane. Nie wiedzieliby też, jak są one wykonywane – czy w pełni zgodnie z poleceniem, z jakim skutkiem itp.

Natomiast przez **funkcjonalną (poziomą) ochronę** wewnętrzną rozumie się rozwiązanie, gdy w zakres czynności (funkcji) nieodzownych do realizacji zadań jednostki, wykonywanych przez poszczególnych jej pracowników, wchodzą także czynności ochrony. Np. operatywnym zadaniem pracownika jest wystawianie faktur, co stanowi warunek zainkasowania przez jednostkę należności za sprzedane wyroby, usługi czy towary. Na pracownika tego może być nałożone dodatkowe zadanie – kontroli, czy odbiorca nie zalega z zapłatą za poprzednią dostawę, a jeżeli tak, to czy o zwiększeniu zadłużenia wie właściwa osoba na stanowisku kierowniczym oraz czy ceny i warunki płatności wymagające wykazania w fakturze nie odbiegają od oferty (potwierdzenia zamówienia),

[28] W zestawieniu świadomie połączono mechanizmy prawne, ekonomiczne i techniczne dla pokazania różnorodności dostępnych narzędzi, które w różnych konfiguracjach mogą służyć realizacji celów przedsiębiorstwa (właściciela).

[29] Szczególnym rodzajem tak rozumianego nadzoru właścicielskiego jest dziś już zapomniana i występująca praktycznie wyłącznie w nielicznych pozostałych jeszcze przedsiębiorstwach państwowych kontrola społeczna (np. kontrola wykonywana przez związki zawodowe bądź radę pracowniczą).

a jeżeli tak, to czy odstępstwo to zostało autoryzowane (akceptowane) przez osobę do tego upoważnioną.

Cechą charakterystyczną tej formy ochrony jest wykonywanie jej na bieżąco, w czasie zamierzonych operacji gospodarczych (np. podczas kontroli wstępnej umów) lub w toku realizowania tych operacji (np. w czasie bieżącej kontroli dokumentów uprawniających do pobrania materiałów do produkcji).

Ochrona instytucjonalna w odróżnieniu od ochrony funkcjonalnej, sprawowanej systematycznie „przy okazji" wykonywania czynności operatywnych, polega na tym, że wyspecjalizowana komórka lub doraźnie powołany zespół zajmuje się sprawdzeniem. Przykładowo może to być:

- stanowisko lub komórka audytu (rewizji) wewnętrznego,
- stanowisko lub komórka inwentaryzacji ciągłej,
- straż przemysłowa lub inna forma ochrony.

W dalszej części artykułu pominięta zostanie kwestia audytu wewnętrznego, gdyż nie opłaca się go stosować w mniejszych przedsiębiorstwach.

Ostatnim z ogólnych mechanizmów ochronnych są tzw. techniczne zabezpieczenia. Często się o nich zapomina lub marginalizuje ich rolę, gdy mowa o ochronie wewnętrznej „w nowoczesnym wydaniu" – jest to podejście błędne. Nie straciły one nic na znaczeniu, mimo że ich wdrożenie i funkcjonowanie jest stosunkowo proste. Najbardziej wymyślny system ochrony nie działa bez fizycznych zabezpieczeń (nic nie zastąpi kłódki, solidnych drzwi, ogrodzenia, dobrego zamka w drzwiach do serwerowni, wnikliwej kontroli przy bramie, wagi, telewizji przemysłowej itd.). Z jednej strony potrafią one być bardzo skuteczne, z drugiej bez ich wdrożenia ubezpieczyciel nie wypłaci odszkodowania.

W dobie coraz większego skomplikowania procesów gospodarczych ochrona wewnętrzna jest niezbędna dla prawidłowego funkcjonowania każdego przedsiębiorstwa. W większych przedsiębiorstwach właściciele powierzają zwykle zarządzanie specjalnie w tym celu zaangażowanym fachowcom. Nie uczestniczą w bieżącym zarządzaniu, zostawiając sobie tylko funkcję nadzorczą. Przez to mniej widzą. Muszą chronić przedsiębiorstwo nie tylko przed negatywnym wpływem czynników zewnętrznych i wewnętrznych, ale również przed niekompetencją, a niekiedy nieuczciwością tych, którzy zarządzają ich majątkiem. Ochrona wewnętrzna musi więc być wieloszczeblowa oraz bardziej sformalizowana. Ma to wady i zalety. Z jednej strony trudniej jest na bieżąco panować nad ochroną zasobów majątkowych, przestrzeganiem przepisów i regulacji oraz prawidłowością wykonywania zadań, ale z drugiej stosuje się ułatwiający ją podział pracy, co wymaga jednak określenia zakresu czynności, obowiązków i odpowiedzialności każdego pracownika (stanowiska). Zasada komisyjności (zwana też „zasadą dwóch par oczu"), polegająca na wykonywaniu czynności przy udziale co najmniej dwóch osób, jest tu jednym z kluczowych mechanizmów zabezpieczających. Ochrona wewnętrzna stanowi w takiej jednostce nieodzowne narzędzie wspomagające właściciela w nadzorowaniu, a kierownictwo w zarządzaniu, podejmowaniu decyzji oraz zapobieganiu, wykrywaniu i korygowaniu błędów, nadużyć oraz innych nieprawidłowości.

Inaczej funkcjonuje ochrona w mniejszych przedsiębiorstwach. Te są zwykle bezpośrednio zarządzane przez właścicieli lub członków ich rodzin, bieżąco „pilnujących" swego biznesu (pańskie oko konia tuczy!). Zbędne jest im nadmierne formalizowanie i autokontrola. Dokumentacja

stosowanych procedur służących ochronie istnieje – jeżeli w ogóle – w formie szczątkowej. Podział obowiązków może być w małym przedsiębiorstwie trudny do realizacji ze względu na ograniczone zasoby ludzkie. Jednak nawet w nich warto zadbać, aby inicjacja, rejestracja i autoryzacja kluczowych transakcji była wykonywana przy udziale co najmniej dwóch osób (jedną z nich może być właściciel). Patrząc z zewnątrz, obecność silnie zaangażowanego w prowadzenie przedsiębiorstwa kierownika-właściciela może być zarówno mocną, jak i słabą stroną ochrony wewnętrznej.

WARUNKI SKUTECZNOŚCI OCHRONY WEWNĘTRZNEJ

Mniej lub bardziej sformalizowany system ochro-ny opłaca się zbudować w przedsiębiorstwie wtedy, gdy może on choć częściowo ochronić przed skutkami ryzyk uznanych za znaczące, których ziszczenie się – jeżeli się im nie zapobiegnie – jest wysoce prawdopodobne, a straty tym wywołane przewyższyłyby koszt ochrony. Musi więc być on jednocześnie i skuteczny, i opłacalny. Ilustruje to tabela:

WARUNKI OPTYMALIZACJI SYSTEMU OCHRONY WEWNĘTRZNEJ

Skuteczność	Przewaga korzyści nad kosztami
• ścisłe powiązanie z celami strategicznymi i operacyjnymi właściciela (przedsiębiorstwa) • jakość i siła środowiska – nastawienie właściciela, kierownictwa i pracowników do potrzeby wdrożenia i przestrzegania mechanizmów ochronnych • potwierdzona skuteczność rozpoznania znaczących ryzyk i przeciwdziałania im • zapobieganie powstaniu istotnych przypadkowych błędów, pomyłek i celowych oszustw • szybkie wykrycie istotnych błędów, pomyłek i nadużyć w przypadku ich wystąpienia • wdrożenie i bieżące śledzenie działań naprawczych, poprawiających funkcjonowanie i aktualizujących system ochrony wewnętrznej lub jego poszczególne elementy	• ukierunkowanie na znaczące, a nie wszystkie ryzyka • wbudowanie zabezpieczeń w to, co i tak istnieje w przedsiębiorstwie • koncentracja na procesach przebiegających w podmiocie w sposób ciągły i wielokrotny • zintegrowanie narzędzi ochrony tak, aby realizowały wiele zadań jednocześnie (np. przeciwdziałanie, wykrywanie, korygowanie) • wykorzystanie procedur kontrolnych i innych wbudowanych standardowo w systemy i aplikacje przez producentów oprogramowania • wykorzystanie wyników kontroli zewnętrznych • zapewnienie odpowiednich proporcji pomiędzy procedurami przebiegającymi z udziałem i bez udziału człowieka oraz mieszanymi • zapewnienie odpowiedniej proporcji pomiędzy procedurami wykrywającymi, prewencyjnymi (zapobiegawczymi) i korygującymi

Przeciwdziałać powinno się głównie takiemu ryzyku, do którego zaistnienia przedsiębiorstwo (właściciel) nie może dopuścić. Z drugiej strony nawet w małym przedsiębiorstwie powinny działać mechanizmy ochronne, nakierowane na tzw. węzłowe odcinki, których ew. nieprawidłowe funkcjonowanie może mieć szczególnie negatywne konsekwencje. Dotyczy to zarówno transakcji, jak i składników majątku.

Praktyka pokazuje, że do obszarów wymagających szczególnej uwagi – a więc i ochrony – w większości przedsiębiorstw (bez względu na ich wielkość) kwalifikują się takie powtarzalne transakcje, jak:

- sprzedaż (powstanie i rozliczenie należności) i rozchód wyrobów oraz towarów,
- zaopatrzenie (zakup i przychód materiałów, towarów i usług, zapłata lub powstanie zobowiązania),
- środki pieniężne (wpływ i wydatkowanie) oraz
- kadry i płace (w tym obliczenie wynagrodzeń i ich wypłata).

Te 4 obszary muszą być chronione, gdyż są niczym bramy do średniowiecznego miasta, najbardziej podatne na atak. Dlatego muszą być na tyle solidnie wykonane, aby nie wpuścić do środka nieprzyjaciela (tzn. nie dopuścić do realizacji znaczących zewnętrznych zagrożeń). Cały czas trzeba również pamiętać, że „wróg" może być ukryty wewnątrz i chcieć je otworzyć od środka. Mimo to „bramy" nie mogą być cały czas zamknięte lub nadmiernie szczelne, bo brak elastyczności uniemożliwia wykorzystanie szans pojawiających się co jakiś czas wewnątrz i na zewnątrz. Paradoksalnie obejście systemu ochrony nie zawsze musi być złe. Czasem jest to wprost jeden z warunków osiągnięcia sukcesu. Brama nie może uniemożliwiać opuszczenia miasta przez jego praworządnych mieszkańców.

Dla uznania danego ryzyka za znaczące, a więc takie, którego spełnieniu trzeba przeciwdziałać (lub łagodzić nieuniknione straty) drogą stworzenia odpowiedniego systemu ochronnego, pod uwagę bierze się jego istotę (np. gotówka jest o wiele bardziej narażona na kradzież niż majątek trwały), możliwy zasięg potencjalnych nieprawidłowości (np. brak dopływu środków ze sprzedaży lub utrata wiarygodności kredytowej mogą mieć negatywny wpływ na wiele dziedzin działalności przedsiębiorstwa) oraz prawdopodobieństwo wystąpienia i powtarzalność.

Ryzyko dotyczy oczywiście również nierutynowych lub specyficznych transakcji (np. połączenia spółek) czy innych zdarzeń nietypowych ze względu na to, że opiewają na wysoką kwotę, następują sporadyczne czy są skomplikowane (np. nabycie zorganizowanej części przedsiębiorstwa lub restrukturyzacja). Takie transakcje ze względu na swój charakter z reguły pozostają poza zasięgiem oddziaływania „normalnego" systemu ochrony wewnętrznej, choć oczywiście nie oznacza to, że przedsiębiorstwo, które dokonuje takiej transakcji, nie powinno zorganizować doraźnego nadzoru nad jej przebiegiem.

RYZYKO MOŻE MIEĆ TEŻ POZYTYWNE SKUTKI

Ochrona wewnętrzna nie polega wyłącznie na zapobieganiu ryzyku zaistnienia niepomyślnych zdarzeń. Część działań prowadzonych w warunkach niepewności i wiążące się z tym ryzyko prowadzi do pozytywnych rezultatów. Dlatego chodzi o znalezienie równowagi między unikaniem skutków ryzyka a możliwymi korzyściami, jakie ono niesie. To dzięki temu, że ludzie mają różną skłonność do akceptacji ryzyka, możliwe jest osiąganie ponadprzeciętnych zysków. Bank najbezpieczniejszy to zwykle ten, który oferuje depozytariuszom najniższe odsetki. Czasem mówi się, że zamiast minimalizować ryzyko należy maksymalizować okazje do osiągnięcia sukcesu. Rozpatrywanie ryzyka wyłącznie w płaszczyźnie zagrożeń może spowalniać lub blokować proces

decyzyjny i prowadzić do zaprzepaszczenia szans, np. poprzez nadmierne spowolnienie pewnych działań lub ich całkowite zaniechanie.

Nie zawsze ochrona musi stanowić pełen system, obejmujący wszystkie grupy powtarzalnych transakcji. W każdym przedsiębiorstwie występują różne ich grupy, ale wypracowanie procedur kontrolnych dla każdego ich rodzaju – z uwagi na niskie ryzyko (mała powtarzalność, niewielkie sumy, ograniczone skutki) – byłoby nieopłacalne. W przypadku funkcjonalnej ochrony wewnętrznej koszt jej działania odgrywa mniejszą rolę, bowiem w system zapewniający niezakłócone działanie przedsiębiorstwa, a więc taki, który musi działać w każdym przypadku, wbudowuje się „przy okazji" mechanizmy ochronne. Nie podraża to – praktycznie – kosztów przedsiębiorstwa.

Prawidłowo działający system ochrony wewnętrznej powoduje, że pracownicy sami nadzorują skuteczność zastosowanych procedur i korygują stwierdzone słabości. Działania realizowane na wszystkich szczeblach organizacyjnych i angażujące – choć w różnym stopniu – większość pracowników powinny sprzyjać zapewnieniu bezpiecznego i stabilnego funkcjonowania przedsiębiorstwa.

Jak już wspomniano, system ochrony wewnętrznej, a w jego ramach ogółu działających lub mających działać w przedsiębiorstwie mechanizmów (procedur), składa się zwykle z wielu, często wzajemnie powiązanych równoległych podsystemów, jak kontrola wydatków i wpływów środków pieniężnych, kontrola zakupów, przyjęcia dostaw i rozrachunków z dostawcami materiałów, towarów i usług, kontrola sprzedaży, wydania wyrobów, towarów, świadczonych usług i rozrachunków z odbiorcami, kontrola obecności zatrudnionych i obliczenie oraz wypłata wynagrodzeń oraz pochodnych od nich (składki ZUS, podatki itd.), kontrola kosztów podróży itd. Skuteczne działanie (lub nie) jednego podsystemu ochrony nie przesądza o sprawności działania innego.

Sposób zaprojektowania, wdrożenia i działania mechanizmów ochronnych różni się w zależności od wielkości, rodzaju prowadzonej działalności i złożoności przedsiębiorstwa oraz przedmiotu ochrony. Innego rodzaju podejście jest wskazane w przedsiębiorstwie prowadzącym sprzedaż detaliczną, gdy kluczowy jest obrót gotówkowy i towarowy w zakresie przyjęć, wydań oraz zarówno ochrony przed kradzieżą towarów, jak i inkasa czy odprowadzania gotówki, a inne w przedsiębiorstwie hurtu, gdy wzrasta znaczenie racjonalizacji stanu i asortymentu zapasu towarów, kontroli rozrachunków i ich zapłaty oraz zgodności dostaw z umowami i zasadami udzielania rabatów. Jeszcze innej ochrony wymaga produkcja budowlana czy wykonywanie napraw gwarancyjnych.

Punktem wyjścia budowy podsystemów ochrony wewnętrznej jest ustalenie, w jakich obszarach istnieje ryzyko powstawania błędów lub nadużyć, jakie wprowadzić procedury, aby im zapobiec oraz w jaki sposób kontrolować prawidłowość przebiegu poszczególnych transakcji. Stosowanie zbyt wielu lub zbyt szczegółowych procedur nadmiernie komplikuje cały proces (np. jeśli chodzi o obieg dokumentów) i nie ułatwia, lecz utrudnia ochronę.

ELEMENTY OCHRONY WEWNĘTRZNEJ

Wśród osób zajmujących się tą dziedziną panuje duża zgodność, że w pełni wdrożona w przedsiębiorstwie ochrona wewnętrzna jako system obejmuje zwykle 5 powiązanych ze sobą i wspomagających się składowych:

- środowisko,
- ocenę ryzyka,
- czynności kontrolne,
- informację i komunikację,
- monitorowanie i nadzór.

Przytoczony podział oraz stosowana terminologia mają charakter umowny, gdyż wiele elementów w praktyce wzajemnie się przenika. Przykładowo czynności kontrolne (potocznie zwane też „kontrolami") mogą jednocześnie dotyczyć jednego lub kilku elementów składowych systemu lub ich aspektów praktycznych (np. konkretnej procedury czy procesu).

Nie jest to również jedynie możliwy podział i dlatego nie musi odpowiadać sposobowi rozumienia i stosowania ochrony wewnętrznej przez dane przedsiębiorstwo oraz jego właścicieli. Nie podważa to jednak jego przydatności jako użytecznej podstawy do oceny, jak różne aspekty ochrony wewnętrznej mogą wpływać na realizację określonych celów.

Pod pojęciem **środowiska** rozumie się nastawienie właściciela, kierownictwa i pracowników do potrzeby zastosowania i przestrzegania mechanizmów ochronnych. Przykład musi przy tym iść z góry, inaczej personel nie traktuje poważnie systemu ochrony wewnętrznej. Ostentacyjne lekceważenie lub obchodzenie wcześniej wprowadzonych zasad i procedur przez przełożonych podważa sens ich przestrzegania i stosowania w oczach podwładnych.

Jakość i siła środowiska ochrony wewnętrznej ma podstawowe znaczenia dla skuteczności wykrywania błędów i zapobiegania oszustwom (odstraszania) oraz korygowania ich skutków. Uważa się, że środowisko jest najważniejszym elementem ochrony wewnętrznej bez względu na wielkość przedsiębiorstwa, ponieważ od niego zależy podejście do systemu ochrony. Jest fundamentem ochrony wewnętrznej, dyscyplinując i tworząc strukturę pod inne składowe systemu. Samo w sobie bezpośrednio nie zapobiega, nie wykrywa ani nie koryguje skutków błędów, oszustw czy innych nieprawidłowości. Może jednak znacząco wpływać na skuteczność działania innych składowych systemu. Uważa się, że środowisko ma dużo większe znaczenie niż np. faktycznie dokonywane czynności kontrolne, bo dopiero jego wysokie standardy sprzyjają wybraniu i stosowaniu najlepszych z możliwych zabezpieczeń.

Środowisko w mniejszym przedsiębiorstwie różni się od tego w większych podmiotach. Np. w mniejszych firmach do osób sprawujących nadzór nie należą zwykle osoby niezależne od zarządu (kierownictwa). W dużej ich części rolę nadzorczą może bezpośrednio sprawować właściciel-kierownik, pełniąc przy tym jeszcze wiele innych funkcji.

Ocena ryzyka wiąże się z jego rozpoznaniem (na czym polega), analizą prawdopodobieństwa wystąpienia oraz postępowaniem w warunkach niepewności, co dotyczy każdego przedsiębiorstwa. Ma ona dać odpowiedź na pytanie, co może pójść źle. Jak wspomniano, ocena ta koncentruje się głównie na niepewności dotyczącej realizacji celów przedsiębiorstwa (właściciela). Częste zmiany personelu, pojawianie się nowych produktów czy szybki rozwój działalności gospodarczej mogą oddziaływać negatywnie na ogólny poziom ryzyka, jeżeli system ochrony wewnętrznej nie nadąża za zmianami.

Ocena ryzyka – zarówno w dużym, jak i małym przedsiębiorstwie – obejmuje ocenę prawdopodobieństwa zaistnienia zdarzenia objętego ryzykiem, możliwych skutków oraz określenie sposobu reagowania na nie – chodzi zwłaszcza o reakcje kierownictwa. Może ono inicjować plany, programy lub działania jako reakcję na określone ryzyko lub też może zdecydować się na akceptację ryzyka ze względu na nadmierny koszt jego ograniczania lub bezsilność. Systematyczne procedury obserwacji zagrożeń są często wbudowane w zwykłe, powtarzalne działania przedsiębiorstwa i obejmują czynności wykonywane regularnie przez kierownictwo i nadzór.

W mniejszych przedsiębiorstwach rzadko istnieją sformalizowane systemy oceny ryzyka. Kierownictwo rozpoznaje je drogą bezpośredniego, osobistego zaangażowania w działalność, a kluczowe decyzje podejmuje, kierując się przede wszystkim intuicją i doświadczeniem (co nie zawsze przynosi zamierzone skutki).

Przez **czynności kontrolne** rozumie się zasady i procedury przyjęte przez dane przedsiębiorstwo i działające w obszarach narażonych na istotne ryzyko, które zapewniają realizację określonej polityki kierownictwa (właściciela). Przykładem mogą być kontrole mające na celu zapewnienie, że zakupy usług o wyższej cenie będą dokonywane po przeprowadzeniu odpowiednich procedur przetargowych lub nie nastąpią dostawy wyrobów bądź towarów na rzecz odbiorców zalegających z płatnościami dłużej niż 2 tygodnie.

Czynności kontrolne są jedynym „twardym" elementem systemu ochrony wewnętrznej. Nazywa się je tak, bo są zwykle widoczne, mierzalne, często udokumentowane – w przeciwieństwie np. do siły środowiska, w jakim funkcjonują mechanizmy ochronne.

Procedury kontrolne można podzielić na przeprowadzane na poziomie przedsiębiorstwa jako całości oraz poszczególnych transakcji (zdarzeń gospodarczych). Te drugie można dalej dzielić na zapobiegawcze (prewencyjne), wykrywające (i korygujące), kompensujące oraz sterujące. Czasem ze względu na znaczenie wyróżnia się jako oddzielną kategorię kontrole zabezpieczające przed oszustwami. Ich odpowiedniki w środowisku informatycznym – ze względu na swoje znaczenie – zostały opisane oddzielnie w dalszej części artykułu.

Sposób wykonywania czynności kontrolnych w mniejszych przedsiębiorstwach jest podobny do sposobu właściwego dla dużych przedsiębiorstw, ale sformalizowanie ich stosowania może się znacząco różnić, gdyż zastępuje je bezpośredni nadzór kierownika (będącego często również właścicielem), polegający na bieżącej obserwacji przychodów i kosztów oraz zatwierdzaniu wszystkich większych transakcji. Szczególną pieczę sprawuje on również nad wpływami i wydatkami pieniężnymi.

W tabeli pokazano przykłady procedur kontrolnych. Większość z nich jest stosowana zarówno w dużych, jak i małych przedsiębiorstwach. Mają one różny ciężar gatunkowy i częstotliwość, część wymaga udziału człowieka, inne przebiegają automatycznie, często nawet bez jego wiedzy[30]. Łączy je to, że stworzono je, aby służyły określonym celom i przeciwdziałały określonym ryzykom.

30 Dotyczy to np. bardzo wielu mechanizmów kontrolnych wbudowanych w standardowe systemy finansowo-księgowe przez producentów oprogramowania.

PRZYKŁADOWE CZYNNOŚCI KONTROLNE

Lp.	Procedura	Podstawowy cel	Częstotliwość
1.	Po włączeniu komputera wymagane jest wprowadzenie hasła; zmianę hasła co 2 tygodnie system wymusza automatycznie	Ograniczenie ryzyka spowodowanego dostępem do systemu osób nieuprawnionych oraz naruszenia zasad bezpieczeństwa integralności* danych	Zawsze, gdy komputer jest włączany; zmiana hasła co 2 tygodnie
2.	Dowody księgowe podlegają przed wprowadzeniem do ksiąg rachunkowych kontroli formalnej, rachunkowej i merytorycznej	Niedopuszczenie do ujęcia w księgach rachunkowych dokumentu wadliwego; nie chodzi tu tylko o zgodność z wymogami uor**, ale o dobrze rozumiany interes przedsiębiorstwa i jego właścicieli***	Współmierna do liczby dokumentów
3.	Inwentaryzacja zapasów drogą spisu z natury	Upewnienie się, że zapasy ujęte w księgach rachunkowych faktycznie istnieją i nie utraciły swojej przydatności lub wartości odzyskiwalnej	Raz w roku lub raz na 2 lata, bądź ciągła, zależnie od potrzeb może nastąpić częściej, niż wymagają tego przepisy
4.	Niezależna od sprzedawców weryfikacja cen stanowiących przedmiot sprzedaży oraz oferowanych bonifikat, rabatów i opustów	Upewnienie się, że przychody nie są uszczuplane drogą udzielania nienależnych zniżek; może to być zarówno skutkiem przypadkowych błędów i pomyłek, jak i celowych działań poszczególnych sprzedawców	Zależnie od decyzji kierownictwa
5.	Wymóg dodatkowej autoryzacji sprzedaży na kredyt po przekroczeniu określonego limitu wartościowego lub ilościowego	Ograniczenie ryzyka sprzedaży, za którą przedsiębiorstwo nie otrzyma zapłaty	Zawsze, gdy wartość lub ilość zamierzonej sprzedaży przekroczy określone wcześniej limity samodzielnej autoryzacji danego pracownika
6.	Automatyczna blokada dostępu do konta internetowego po 3-krotnym wpisaniu przez klienta sklepu internetowego błędnego hasła	Ograniczenie ryzyka spowodowanego dostępem do zewnętrznej części systemu informatycznego przedsiębiorstwa osób nieuprawnionych oraz wysyłki na ich rzecz towarów, za które przedsiębiorstwo nie otrzyma zapłaty	Zawsze, gdy błędne hasło zostanie 3-krotnie wprowadzone do systemu
7.	Moduł finansowo-księgowy nie pozwoli wprowadzić do systemu krajowego numeru VAT, jeżeli nie składa się on z 10 cyfr	Każdemu wystawcy faktury powinno zależeć na unikaniu błędów przy wystawianiu faktur; nieprawidłowo wystawiona faktura stwarza problem dla odbiorcy i podważa wiarygodność (reputację) wystawcy	Zawsze, gdy wprowadza się nowy numer VAT do systemu
8.	Sprawdzenie samochodów dostawczych wjeżdżających i wyjeżdżających z magazynu	Ograniczenie ryzyka, że aktywa przedsiębiorstwa zostaną utracone, a stany księgowe nie będą zgodne z rzeczywistością	Zawsze, gdy samochód wjeżdża lub wyjeżdża z magazynu

* Przez integralność rozumie się stan, w którym żadne dane nie zostały zmienione, dodane lub usunięte bez zgody autoryzacyjnej wyznaczonej osoby.

** Zgodnie z art. 22 uor dowody księgowe powinny być rzetelne (tj. zgodne z rzeczywistym przebiegiem operacji gospodarczej, którą dokumentują), kompletne (tj. muszą zawierać co najmniej dane określone w art. 21) oraz wolne od błędów rachunkowych.

*** Co by było, gdyby bez sprawdzenia na kontach zobowiązań ujęto faktury dotyczące dostaw, które trafiły do innych podmiotów?

Mniejsze przedsiębiorstwa mogą uznać, że przeprowadzanie określonych czynności kontrolnych nie jest im potrzebne ze względu na bieżące działania kierownictwa. Np. należące wyłącznie do kierownictwa prawo przyznawania odbiorcom kredytów kupieckich oraz wyrażania zgody na znaczące zakupy może zapewniać silną kontrolę tego typu transakcji, zmniejszając lub czyniąc zbędną potrzebę przeprowadzania dodatkowych procedur. Działania kontrolne w mniejszym przedsiębiorstwie mogą się ograniczać do głównych cykli transakcji, takich jak sprzedaż – należności, zakupy – zobowiązania i koszty wynagrodzeń.

Składowa „informacja i komunikacja" łączy w sobie różne elementy systemu ochrony wewnętrznej. Jest to jego „krwioobieg". Zawiera identyfikację, gromadzenie i wymianę lub przekazywanie (wykorzystywanie) informacji o charakterze operacyjnym, finansowym czy mających na celu zapewnienie zgodności z przepisami prawa i innymi regulacjami. Łączy wykorzystanie informacji z komunikowaniem się wewnątrz i na zewnątrz przedsiębiorstwa. Założeniem jest, że informacja i komunikacja następuje w sposób ciągły i terminowy. Kierownictwo (właściciel) lub organy nadzorcze, które otrzymują wystarczająco szybko wiarygodne informacje, mają większą możliwość prawidłowego zarządzania, nadzorowania i kontrolowania działalności przedsiębiorstwa. Mogą również szybciej i skuteczniej reagować na ujawnione nieprawidłowości.

Komunikacja w mniejszym przedsiębiorstwie jest prostsza i łatwiejsza niż w większym ze względu na mniej liczne szczeble odpowiedzialności i większą dostępność kierownictwa. Porozumiewanie się następuje często w sposób niesformalizowany, bez szkody dla jego skuteczności.

Monitorowanie i nadzór dają możliwość ujawnienia potencjalnych i rzeczywistych przypadków nieprawidłowości i niedociągnięć działania systemu ochrony wewnętrznej. Szczególnym zagrożeniem są te nieprawidłowości, które mogą całkowicie uniemożliwić lub znacząco utrudnić realizację celów przedsiębiorstwa (właściciela). Dlatego monitorowanie i nadzór dotyczą przede wszystkim oceny odpowiedniości, wdrożenia i skuteczności działania mechanizmów ochronnych.

Kierownictwo przedsiębiorstwa może sprawować nadzór nad wybranymi obszarami poprzez bieżący monitoring, indywidualne oceny przeprowadzane co jakiś czas lub kombinację obu tych działań.

W mniejszych przedsiębiorstwach nadzór sprawuje często bezpośrednio właściciel-kierownik. Ma to z reguły charakter nieformalny i następuje równolegle do bieżącego zarządzania. Zwykle polega na stwierdzaniu znaczących odchyleń od założeń lub oczekiwań, ustalaniu przyczyn nieprawidłowości lub nieścisłości danych finansowych i niefinansowych oraz podejmowaniu w ich wyniku działań naprawczych.

OCHRONA WEWNĘTRZNA A STOSOWANIE TECHNOLOGII INFORMATYCZNYCH

Wobec powszechnego stosowania technologii informatycznych zarówno w dużych, jak i mniejszych przedsiębiorstwach niezbędne jest monitorowanie poprawności ich funkcjonowania. Zastosowanie

takich narzędzi z jednej strony daje liczne korzyści (oszczędność czasu, zdolność do tzw. samokontroli, możliwość przetworzenia ogromnej ilości danych itd.), z drugiej jednak rodzi zagrożenia i ryzyko. Podstawowe znaczenie mają tu kwestie bezpieczeństwa i nienaruszalności (integralności) danych oraz poprawnego funkcjonowania mimo ograniczonego śladu rewizyjnego.

Rewolucja technologiczna i tempo zmian w tym obszarze sprawia, że dostęp osób nieuprawnionych do systemu lub naruszenie zasad bezpieczeństwa danych mogą coraz częściej w sposób bezpośredni wpływać na działalność i sytuację finansową danego przedsiębiorstwa (czasem nawet na możliwość jej kontynuacji). Nie wszystkie zagrożenia występują w każdym z nich w podobnym stopniu. Warto jednak pamiętać, że dziś nawet mniejsze przedsiębiorstwa są zinformatyzowane w dużo większym stopniu niż jeszcze kilka lat temu, przez co są narażone na dużo większe ryzyko. Problem jest tym większy, że jak wynika z moich obserwacji, w mniejszych przedsiębiorstwach bardzo niska jest świadomość zagrożeń i ich skutków, co powoduje, że te przedsiębiorstwa nie są chronione tak jak powinny (nawet gdy koszt z tym związany byłby stosunkowo nieduży).

Ochrona przedsiębiorstwa (właściciela) wymaga wdrożenia odpowiednich procedur (kontroli) ogólnych i aplikacyjnych[31], które łącznie mają na celu zapewnienie bezpieczeństwa, kompletności i poprawności przetwarzania informacji wejściowych w wyjściowe oraz ich udostępniania wyłącznie zamierzonym użytkownikom. Ilustracją tego jest tabela na następnej stronie. Analizując jej treść, warto zwrócić uwagę, że niektóre z przedstawionych procedur mają charakter automatyczny i zostały wbudowane w oprogramowanie już przez ich producentów. To, czy będą one służyły do ochrony danego przedsiębiorcy, często zależy od tego, czy jest on ich świadomym użytkownikiem.

Przy projektowaniu procedur kontroli ogólnych i aplikacyjnych poza realizacją celów wewnętrznych pod uwagę powinny być brane wymogi prawne. Przykładowo uor określa wiele wymogów, jakie powinny spełniać księgi rachunkowe prowadzone za pomocą komputera. W mniejszych przedsiębiorstwach systemy informacyjne ze względu na prostsze procesy gospodarcze są przeważnie mniej skomplikowane (często stosuje się kupowane „z zewnątrz" gotowe oprogramowanie), ale ich rola jest równie znacząca.

Nawet gdy obsługa informatyczna – ze względu na uzasadnienie ekonomiczne lub brak niezbędnych kompetencji wewnątrz jednostki – została zlecona innej firmie i dotyczy standardowego oprogramowania, trzeba zadbać, aby ten jakże ryzykowny obszar funkcjonowania przedsiębiorstwa też podlegał bieżącemu monitorowaniu i nadzorowi.

[31] Kontrole ogólne dotyczące elementów środowiska ochrony, jako całości, są podobne do innych tego typu kontroli funkcjonujących na poziomie przedsiębiorstwa, z tą różnicą, że ich przedmiotem jest sposób zarządzania systemami i organizacja IT. Kontrole aplikacyjne dotyczą specyficznych czynności wykonywanych przez aplikacje i programy. Są one ważnym elementem kontroli procesów gospodarczych (takich jak np. funkcjonujące w obszarze sprzedaż – należności) i dotyczą sposobu przetwarzania określonych transakcji. Mogą następować automatycznie (są inicjowane i przebiegają w zasadzie bez udziału człowieka) lub być uruchamiane i przeprowadzane z przynajmniej częściowym udziałem ludzi.

PRZYKŁADY KONTROLI SYSTEMU IT

Typ kontroli	Kategoria kontroli	Przykłady procedury kontrolnej
Kontrole ogólne	Zarządzenie funkcją IT w jednostce	Osoba odpowiedzialna za IT ma obowiązek informowania kierownictwa o przebiegu realizacji obowiązków
	Rozdział obowiązków w ramach komórki IT	Odpowiedzialność za zakup, rozwijanie, wdrażanie, modyfikację i bieżące funkcjonowanie oprogramowania oraz za bezpieczeństwo danych została rozdzielona między różne osoby
	Kontrole dostępu	Fizyczne zabezpieczenie dostępu do komputerów i serwerów, rozwiązania typu *firewall* chroniące przed włamaniami do systemu przez łącza internetowe, hasła dostępu i inne procedury uwierzytelniające użytkownika, szyfrowanie danych
	Plany awaryjne	Regularnie sporządza się kopie zapasowe danych i przechowuje w bezpiecznym miejscu
Kontrole aplikacyjne	Kontrole na wejściu	Na ekranie komputera ukazują się kolejne okna z komunikatami i wymuszają wprowadzenie wymaganych danych
	Kontrole przetwarzania	Mechanizm wbudowany w oprogramowanie sprawdza, czy wszystkie wprowadzone do systemu dane zostały przetworzone; modyfikacje harmonogramu przetwarzania może przeprowadzić tylko ograniczony krąg odpowiedzialnych za to osób
	Kontrole na wyjściu	Upoważniona osoba z działu sprzedaży regularnie sprawdza prawidłowość przetworzenia znaczących transakcji

GRANICE SKUTECZNOŚCI OCHRONY WEWNĘTRZNEJ

Ochrona wewnętrzna jest pojęciem szerokim, obejmującym wiele obszarów i zagadnień. Może ona być w bardzo różny sposób wdrożona w danym przedsiębiorstwie. Aby spełniała swoje funkcje, muszą być zapewnione odpowiednie warunki, o których – częściowo – była już mowa. Pewnym rozsądnym minimum w mniejszym przedsiębiorstwie jest zadbanie o to, aby:

- istniała odpowiednia struktura organizacyjna, z czym wiąże się określenie zadań, uprawnień i odpowiedzialności poszczególnych osób lub komórek,
- wdrożone były odpowiednie mechanizmy, których celem jest utrzymanie w każdym czasie i okolicznościach ciągłości działania przedsiębiorstwa (w tym kluczowych operacji gospodarczych),
- ustalony został sposób autoryzacji (akceptacji) poszczególnych transakcji, a przede wszystkim dyspozycji powodujących zamierzony lub bieżący rozchód i przychód zasobów (składników aktywów),

- w miarę możliwości nastąpił taki podział wykonywanych czynności, aby jedna osoba nie mogła samodzielnie przeprowadzić całej transakcji i aby była w jej trakcie kontrolowana przez kogoś innego (choćby kierownika-
-właściciela),

- wykonywane czynności były dokumentowane i ewidencjonowane stosownie do potrzeb i wymogów prawa (dotyczy to również ew. dokumentowania samego systemu ochrony wewnętrznej lub jego wybranych składowych),

- zastosowano odpowiedni dobór (fachowość, uczciwość, sumienność) pracowników uczestniczących w sprawowaniu ochrony wewnętrznej,

- stosowane były fizyczne zabezpieczenia zasobów (ogrodzenie terenu, kontrola wejść i wyjść, zabezpieczenie magazynów, kas itp.), fizyczna kontrola obrotu składnikami majątkowymi (pomiar),

- uwzględniano ryzyko związane z wykorzystywaniem technologii informatycznych (choćby przy zastosowaniu najprostszych środków, takich jak regularne wymuszanie zmian haseł do systemu, stosowanie dobrych programów antywirusowych, regularne aktualizacje standardowego oprogramowania, ograniczenie dostępu do serwerowni, robienie regularnych kopii danych czy rozwiązania typu firewall),

- kierownictwo (właściciel) sprawowało nadzór nad działaniem całego systemu ochrony wewnętrznej, w tym okresowo weryfikowało, czy czynności służące ochronie są należycie wykonywane i podejmowało – w miarę potrzeby – działania usprawniające.

Przy wszystkich zaletach ochrony wewnętrznej i korzyściach, jakie ona przynosi, należy mieć także świadomość istnienia obiektywnych ograniczeń jej skuteczności. Powody tego są różne. Naturalne jest założenie, że koszt wdrożenia i stosowania ochrony wewnętrznej nie może przewyższać potencjalnej straty. Ochrona nie może też być zbyt sztywna. Realizacja celów i prowadzenie działalności gospodarczej wymaga wykorzystywania pojawiających się możliwości oraz akceptacji pewnego poziomu ryzyka.

Większość wbudowanych w system ochrony wewnętrznej mechanizmów zapobiegających (odstraszających), wykrywających lub korygujących jest nakierowana na operacje typowe i rutynowe (a nie wyjątkowe). Pewne transakcje lub zasoby w związku z tym są objęte w ograniczonym zakresie oddziaływaniem systemu.

Pamiętać również trzeba, że ochronę wewnętrzną sprawują lub nadzorują ludzie, a ci są omylni i potrafią nadużywać uprawnień. Zrozumienie celu i działania systemu przez personel realizujący jego funkcje może być niepełne, istota transakcji i sposób ich ochrony bywają błędnie rozumiane, a informacje prawidłowo dostarczane przez system informacyjny niewłaściwie wykorzystywane.

Przedsiębiorstwo się rozwija, następują w nim zmiany, tymczasem mechanizmy ochrony nie zawsze za nimi nadążają. Zmianom ulegają również znaczące ryzyka wraz ze zmieniającym się otoczeniem czy zmianami wewnątrz przedsiębiorstwa. Wszystko to sprawia, że skuteczność aktualnej koncepcji i działania ochrony wewnętrznej powinny podlegać okresowej ocenie dzięki wykorzystaniu odpowiednich narzędzi, takich jak np. audyty wewnętrzne i zewnętrzne, samoocena przeprowadzana przez kierownictwo (właściciela) czy analiza raportów odchyleń i wyjątków.

Zagrożenie stanowi to, że ocena nie zawsze następuje w porę, a nawet gdy następuje na czas, nie jest pozbawiona subiektywizmu.

Warto też pamiętać, że nawet najlepiej zaprojektowany i skuteczny system można obejść w wyniku działań kierownictwa lub zmowy pracowników. Istnieją duże i niestety uzasadnione wątpliwości co do skuteczności ochrony w zakresie zapobiegania i wykrywania przestępstw popełnianych przez personel kierowniczy oraz mniejsze – przez zwykłych pracowników.

Ograniczenie skuteczności ochrony wewnętrznej ma również charakter pierwotny, „wrodzony". Chodzi o to, że ochrona taka może i powinna wspomagać osiąganie celów, ale sama nie określa, jakie to cele. Rzadko są one stałe i niezmienne. Decyzja o tym, czy i jak działać, należy do kierownictwa (właścicieli) danego przedsiębiorstwa. Ochrona wewnętrzna stanowi jedynie bardziej lub mniej skuteczne narzędzie realizacji celów określonych przez kierownictwo i/lub właścicieli. Ma pomóc w zapewnieniu, że osoby odpowiedzialne za nadzór i podejmowanie decyzji otrzymują właściwe, przydatne i rzetelne informacje. Może śledzić i raportować rezultaty, jakie dały podjęte działania lub decyzje, a dostarczane informacje mogą powodować dalsze decyzje i działania kierownictwa i/lub właścicieli. Ochrona wewnętrzna nie może jednak zapobiec podjęciu strategicznych lub operacyjnych decyzji bądź działań, które okażą się niewłaściwe.

Mimo wspomnianych ograniczeń praktyka potwierdza, że dobrze zaprojektowana ochrona wewnętrzna sprawdza się, działając skutecznie i opłacalnie co najmniej w odniesieniu do typowych transakcji. Świadomość ograniczeń skuteczności ochrony wewnętrznej powinna jednak umożliwiać lepsze jej dostosowanie do potrzeb i możliwości danego przedsiębiorstwa oraz jego właścicieli[32].

[32] Szczegółowe rozważania dotyczące budowy wybranych elementów ochrony wewnętrznej zostaną przedstawione w kolejnych artykułach poświęconych tej tematyce.