PRACE NAUKOWE AKADEMII EKONOMICZNEJ WE WROCŁAWIU
Nr 1139 — 2006
Rachunkowość a controlling

Katarzyna Szymczyk-Madej
Akademia Ekonomiczna w Krakowie

KONTROLA OGÓLNA I KONTROLA APLIKACJI W SYSTEMIE INFORMATYCZNYM RACHUNKOWOŚCI

1. Wstęp

Obecnie technologia informatyczna jest powszechnie stosowana w jednostkach gospodarczych, które w warunkach rosnącej konkurencji starają się wykorzystywać jej możliwości do uzyskania przewagi nad innymi jednostkami. System informatyczny (SI) przedsiębiorstwa odgrywa istotną rolę w efektywnym zarządzaniu i w znacznym stopniu warunkuje osiągnięcie zamierzonych rezultatów ekonomicznych. Wynika to przede wszystkim z tego, że podejmowanie racjonalnych decyzji jest możliwe tylko wówczas, gdy procesy decyzyjne opierają się na kompletnej, dokładnej i aktualnej informacji.

Niestety, rozwój technologii informatycznej, oprócz wniesienia szeregu pozytywnych zmian, doprowadził także do pojawienia się nowych zagrożeń. Jednostki gospodarcze, które zaprojektowały i wdrożyły własne systemy informatyczne, stanęły w obliczu konieczności zapewnienia im odpowiedniej ochrony. W podobnej sytuacji znalazły się również systemy informatyczne rachunkowości. Odpowiedzią na tę potrzebę stały się nowe rozwiązania stosowane w systemach kontroli wewnętrznej funkcjonujących w środowisku informatycznym. To właśnie zagadnienie zostało poruszone w niniejszym artykule.

2. Kontrola wewnętrzna w systemie rachunkowości

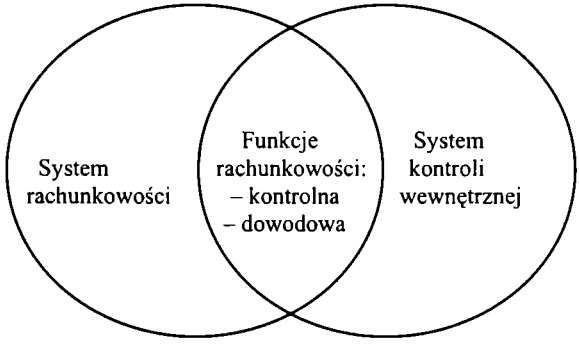
Związek między systemem rachunkowości a systemem kontroli wewnętrznej jest bardzo ścisły. Systemy te wzajemnie się przenikają i dostarczają obopólnych korzyści, których istota sprowadza się do stwierdzenia, że:

- kontrola wewnętrzna nie może być dobrze realizowana bez prawidłowo prowadzonej rachunkowości i prawidłowej sprawozdawczości finansowej,

– zapewnienie bieżącej, rzetelnej i prawidłowej rachunkowości jest jednym z celów kontroli wewnętrznej.

Związek ten ma charakter sprzężenia zwrotnego między jednym a drugim systemem. Oznacza to, że system rachunkowości tworzy warunki i dostarcza informacji niezbędnych do realizowania kontroli (np. kontroli majątku i kapitałów, kompletności dochodów i kosztów), dobrze zaś zorganizowana kontrola wewnętrzna zapewnia prawidłowe funkcjonowanie systemu rachunkowości.

Istotne znaczenie systemu rachunkowości dla kontroli wewnętrznej wynika z roli rachunkowości w funkcjonowaniu jednostki, a także z tego, że rachunkowość sama w sobie stanowi pewien sprawdzony od stuleci, kompleksowy, skuteczny i dobrze zorganizowany system kontrolny poszczególnych operacji gospodarczych, aktywów i pasywów oraz wyniku finansowego przedsiębiorstwa[1]. Z tego względu rachunkowość stanowi ważne źródło informacji kontrolnych i wiarygodny instrument kontroli wewnętrznej. Związek rachunkowości z kontrolą wewnętrzną przedstawiono na rys. 1.



Rys. 1. System rachunkowości a system kontroli wewnętrznej

Źródło: opracowanie własne na podstawie [12].

W rachunkowości prowadzonej przy użyciu komputera szczególną rolę odgrywają kontrole realizowane w środowisku informatycznym. Dzięki nim informacje dostarczane przez system rachunkowości są prawidłowe i mają wiarygodny charakter.

[1] Funkcja kontrolna rachunkowości ma zasadnicze znaczenie w ochronie majątku, a jej realizacja przejawia się w oddziaływaniu prewencyjnym, ingerencyjnym oraz interwencyjnym. Oddziaływanie prewencyjne – w formie czynności zachowawczych i zapobiegawczych – ogranicza rozmiary niegospodarności i przestępczości. Oddziaływanie ingerencyjne polega na współudziale rachunkowości z innymi organami kontroli wewnętrznej i zewnętrznej w ujawnianiu strat spowodowanych przestępczością, niedbalstwem i niegospodarnością, natomiast oddziaływanie interwencyjne – na włączaniu rachunkowości w tok zdarzeń związanych z przebiegiem procesów gospodarczych oraz na uczestniczeniu w sterowaniu tymi procesami (zob. [1]).

3. Kontrola wewnętrzna w środowisku informatycznym

Problematyka kontroli wewnętrznych w systemie informatycznym rachunkowości przedstawiona została w licznych publikacjach (zob. np. [3; 6; 7; 8; 13; 14; 15; 21; 23]). Wszyscy autorzy są zgodni, że jeżeli rachunkowość działa w środowisku informatycznym, to ze względu na specyficzne cechy tego środowiska[2] oraz powstanie większej liczby różnorodnych zagrożeń[3], system kontroli wewnętrznej musi ulec znacznej rozbudowie. Wynika to stąd, że chociaż ochrona przed zagrożeniami może być realizowana za pomocą zabezpieczeń technicznych[4], fizycznych[5], organizacyjnych[6] i personalnych[7], to konieczna jest jeszcze dodatkowa kontrola poprawności ich funkcjonowania.

---

[2] W przypadku prowadzenia rachunkowości z wykorzystaniem technologii informatycznej do podstawowych cech środowiska informatycznego, sprzyjających powstawaniu zagrożeń, należy zaliczyć m.in.:
- niemożność zobaczenia gołym okiem danych elektronicznych – utrudnia to ich śledzenie i bezpośrednią kontrolę, jak ma to miejsce w przypadku danych na papierze,
- szybkość przetwarzania danych – utrudnia wczesne wykrycie ewentualnej pomyłki lub fałszerstwa,
- transmisja danych siecią – sprawia, że dane te są narażone na przechwycenie lub utratę integralności,
- niewielki rozmiar nośników danych – sprzyja ich kradzieży lub uszkodzeniu,
- podatność na uszkodzenia – jest to spowodowane faktem, że urządzenia i nośniki danych są najczęściej mało odporne na uszkodzenia mechaniczne, ładunki elektrostatyczne, ogień i wodę,
- ujednolicenie i automatyczne przetwarzanie operacji księgowych przez programy – powoduje zmniejszenie wpływu człowieka na wynik przetwarzania, a tym samym błędy, które mogłyby być łatwo zauważone przy księgowaniu manualnym, pozostają często przez długi czas ukryte,
- dokładna znajomość personelu informatycznego (programistów, administratorów sieci), zasad działania i funkcjonowania systemu – sprzyja to trudnym do wykrycia nadużyciom (np. przeglądanie danych),
- brak standardowych mechanizmów ochrony w komputerach osobistych i wykorzystywanym oprogramowaniu,
- brak wiedzy, umiejętności i odpowiednich przyzwyczajeń użytkowników – sprawia, że mimo coraz prostszej i bardziej intuicyjnej obsługi programów nadal zdarzają się przypadki popełniania błędów.

[3] Zagrożenia te mogą być powodowane przez ludzi, powstawać w wyniku awarii, braków i uchybień organizacyjnych, a także być powodowane przez siły wyższe i zdarzenia losowe.

[4] Zabezpieczenia techniczne (sprzętowe i programowe) stanowią bardzo rozległą grupę zabezpieczeń, do których zalicza się przede wszystkim:
- systemy tworzenia kopii zapasowych i odtwarzania danych,
- programy antywirusowe i narzędziowe,
- zwielokrotnienie urządzeń i danych,
- programowe i sprzętowe systemy uwierzytelniania użytkowników (np. hasła, karty identyfikacyjne),
- narzędzia kryptograficzne (np. szyfrowanie przechowywanych danych, szyfrowanie transmisji w sieci, używanie podpisów cyfrowych),
- filtrowanie przesyłanych danych (np. systemy *firewall*).

[5] Ochrona fizyczna polega przede wszystkim na:
- organizacji stref bezpieczeństwa – czyli utworzeniu dookoła pomieszczeń przedsiębiorstwa obszaru bezpiecznego, zwanego strefą bezpieczeństwa, którego celem jest zapobieganie nieuprawnionemu dostępowi do pomieszczeń i ingerencji w znajdujące się tam zasoby,
- zabezpieczaniu urządzeń i nośników danych w celu przeciwdziałania utracie, uszkodzeniu lub innemu naruszeniu bezpieczeństwa zasobów systemu.

Zgodnie z ogólnym podziałem kontroli wewnętrznych w środowisku informatycznym można wyróżnić dwie ich kategorie [4]:
- kontrole ogólne (*general controls*) – przeprowadzane dla całego środowiska informatycznego, w tym także dla systemu informatycznego rachunkowości,
- kontrole aplikacji (*application controls*) – przeprowadzane dla konkretnego oprogramowania.

Kontrole ogólne i kontrole aplikacji są wzajemnie ze sobą powiązane. Kontrole ogólne przede wszystkim są niezbędne do zapewnienia prawidłowego działania całego systemu informatycznego i tym samym mają wpływ na skuteczność kontroli aplikacji. Oznacza to, że jeżeli kontrole ogólne nie są realizowane prawidłowo, to nie można polegać na kontrolach aplikacji. Wynika z tego, że nieprawidłowe kontrole ogólne podważają wiarygodność nawet silnych kontroli aplikacji. Oba rodzaje kontroli przedstawiono poniżej.

3.1. Kontrole ogólne

Celem kontroli ogólnych jest zapewnienie prawidłowego funkcjonowania i rozwoju całego środowiska informatycznego. Do kontroli ogólnych zaliczają się więc wszystkie działania (np. organizacja pracy, zachowanie użytkowników, rozporządzenia kierownictwa, szkolenie użytkowników, procedury postępowania, zakupy urządzeń i oprogramowania, zabezpieczanie zasobów itd.), które mają na celu zapewnienie prawidłowego funkcjonowania systemu informatycznego w przedsiębiorstwie.

Biorąc pod uwagę cel kontroli ogólnych, zalicza się do nich takie działania, jak:
- organizacja procesu przetwarzania, a szczególnie:
  - opracowanie odpowiedniej struktury organizacyjnej działu informatyki,
  - określenie udziału poszczególnych komórek organizacyjnych przedsiębiorstwa w procesie przetwarzania danych,

---

[6] Zabezpieczenia organizacyjne to zabezpieczenia wynikające z odpowiedniej organizacji korzystania i obsługi systemu informatycznego. Grupa tych zabezpieczeń jest bardzo zróżnicowana. Zalicza się do nich przede wszystkim:
- system kontroli (np. kontrole wewnętrzne, kontrole legalności oprogramowania, kontrole przeciwpożarowe, kontrole BHP),
- zasady użytkowania programów i urządzeń komputerowych,
- zarządzanie nośnikami danych,
- ubezpieczenia (np. od wypadków losowych, kradzieży),
- ogólne zasady bezpieczeństwa.

[7] Użytkownicy systemu mają duży wpływ na jego bezpieczeństwo i od ich postępowania zależy osiągnięty poziom bezpieczeństwa systemu. Dlatego w tym wypadku mechanizmów zabezpieczających nie można ograniczyć tylko do tych, które, wydawałoby się, bezpośrednio wpływają na bezpieczeństwo systemu, ale należy je rozciągnąć na cały obszar tzw. zarządzania personelem. Najważniejsze zagadnienia, na które w szczególności należy zwrócić uwagę, to: odpowiedni nabór pracowników na poszczególne stanowiska, przedzielanie im obowiązków, praw i odpowiedzialności nie pozostających ze sobą w sprzeczności, uświadamianie pracownikom wagi problemu bezpieczeństwa SI itp.

- odpowiednie rozdzielenie zadań[8] uczestników przetwarzania danych poprzez prawidłowe określenie ich uprawnień, obowiązków i odpowiedzialności,
- ustalenie przez kierownictwo odpowiednich środków nadzoru nad funkcjonowaniem działu informatyki i procesem przetwarzania danych,
- ustalenie przebiegu procesu przetwarzania,
- ustalenie harmonogramów przetwarzania;

- eksploatacja i wykorzystanie zasobów systemu, a zwłaszcza:
  - przestrzeganie procedur i zasad procesu przetwarzania,
  - kontrola dostępu do zasobów systemu,
  - prawidłowe użytkowanie programów i urządzeń komputerowych,
  - zarządzanie nośnikami danych;
- zagwarantowanie ciągłości i bezpieczeństwa procesu przetwarzania, a zwłaszcza:
  - przestrzeganie przez użytkowników ogólnych zasad bezpieczeństwa,
  - zabezpieczenie zasobów systemu przed nieupoważnionym dostępem,
  - tworzenie i przechowywanie kopii danych,
  - opracowanie i przestrzeganie procedur ochronnych i awaryjnych,
  - organizowanie szkoleń użytkowników w zakresie obsługi programów i urządzeń oraz szkoleń w zakresie ochrony i bezpieczeństwa systemu,
  - ubezpieczenie zasobów (np. urządzeń, oprogramowania, danych) od następstw wystąpienia zagrożeń (np. kradzieży, pożaru, zalania itp.);
- utrzymanie i rozwój systemu informatycznego, a zwłaszcza:
  - dbanie o prawidłowe funkcjonowanie programów i urządzeń komputerowych,
  - analizowanie potrzeb w zakresie rozwoju systemu informatycznego (np. zakup nowego oprogramowania, urządzeń, technologii przetwarzania danych),
  - dbanie o odpowiednią jakość urządzeń komputerowych i infrastruktury,
  - kontrolowanie efektywności systemu informatycznego,
  - ustalenie i realizowanie planu przeglądów, konserwacji i czyszczenia urządzeń komputerowych,
  - ustalenie i realizowanie planu i metody rozwoju systemu informatycznego[9];

---

[8] W literaturze przedmiotu zwraca się szczególną uwagę na rozdzielenie w systemie informatycznym użytkowników od osób odpowiedzialnych za jego funkcjonowanie, a zwłaszcza na rozdzielenie funkcji związanych z użytkowaniem systemu od funkcji jego zabezpieczania. Sposobem właściwego rozdzielenia niezgodnych funkcji jest przede wszystkim odpowiednia struktura organizacyjna działu informatyki. Podstawowy podział w ramach tego działu powinien dotyczyć tych, którzy tworzą system informatyczny, i tych, którzy go eksploatują. W strukturze pionu informatycznego zazwyczaj wyróżnia się następujące funkcje:
- projektowanie, programowanie oraz testowanie systemu,
- administrowanie bazami danych,
- administrowanie siecią,
- obsługa techniczna systemu,
- przetwarzanie danych,
- ochrona systemu.

[9] Plan rozwoju systemu informatycznego powinien przewidywać możliwy i pożądany rozwój:

- dokumentacja systemu informatycznego[10], a w szczególności:
  - dbanie o kompletność dokumentacji jako całości, tzn. obejmującej jego budowę, zasady funkcjonowania, wprowadzone zmiany itp.,
  - przechowywanie dokumentacji w bezpiecznym miejscu, do którego mają dostęp tylko upoważnione osoby,
  - dbanie o aktualizację dokumentacji,
  - zatwierdzanie przez kierownictwo zmian w dokumentacji,
  - udostępnienie użytkownikom tej części dokumentacji, która jest im niezbędna podczas wykonywanej pracy (np. dokumentacja programów, instrukcje obsługi urządzeń).

W jednostce powinny być wydzielone służby informatyczne do przeprowadzania kontroli ogólnych. Jeżeli jest to możliwe i opłacalne, powinna zostać powołana także osoba na stanowisko specjalisty do spraw bezpieczeństwa SI.

3.2. Kontrole aplikacji

Jak już wspomniano, oprócz kontroli ogólnych powinny być także przeprowadzane kontrole systemów użytkowych, czyli kontrole aplikacji. Ich celem jest przede wszystkim zagwarantowanie wiarygodności wykorzystywanego oprogramowania poprzez uzyskanie pewności, że dane i informacje przez nie wygenerowane są prawidłowe, tzn. że na etapie wprowadzania, przesyłania, przechowywania i generowania danych nie występują nieprawidłowości. Kontrole aplikacji obejmują:

- wprowadzanie danych (kontrola danych wejściowych),
- przetwarzanie danych (kontrola przetwarzanych danych),
- generowanie wyników (kontrola danych wyjściowych).

Kontrola przesyłania i przechowywania danych należy do zadań kontroli ogólnych, a zagwarantowanie poprawności przesyłania i przechowywania danych to element bezpieczeństwa systemu informatycznego.

3.2.1. Kontrola danych wejściowych

Należy przede wszystkim zaznaczyć, że przed rozpoczęciem wprowadzania danych konieczna jest weryfikacja użytkownika, który ten proces będzie realizował[11].

- urządzeń komputerowych,
- oprogramowania,
- personelu,
- technik i technologii informatycznych (rozwiązań dotyczących sieci komputerowych, systemów zarządzania bazami danych itp.).

[10] Należy podkreślić, że dokumentacja jest bardzo ważnym elementem systemu informatycznego rachunkowości, stanowi również przedmiot badania dla audytorów wewnętrznych i biegłych rewidentów.

[11] Weryfikacja użytkownika, czyli tzw. uwierzytelnianie, może się odbywać na poziomie systemu operacyjnego lub na poziomie samej aplikacji, do której wprowadzane są dane. Można wyróżnić trzy klasyczne

Jest to pierwszy i bardzo ważny etap kontroli[12]. Następnie, już podczas wprowadzania danych, mogą być przeprowadzone następujące rodzaje kontroli [7]:

- kontrola wartości (*total monetary amount*) – sprawdzenie, czy wartość wprowadzonych dokumentów[13] jest zgodna z wartością uzyskaną z innego źródła (np. przy wsadowym wprowadzaniu faktur zakupu ich wartość powinna odpowiadać wartości przedstawionej przez dostawcę np. na dokumencie przewozowym),
- kontrola ilości (*total items*) – sprawdzenie, czy liczba jednostek wprowadzonych do systemu z dokumentów jest zgodna z liczbą uzyskaną z innego źródła,
- kontrola liczby dokumentów (*total documents*) – sprawdzenie, czy liczba wprowadzonych do systemu dokumentów jest zgodna z liczbą dokumentów uzyskaną z innego źródła (np. podaną przez dostawcę),
- kontrola sum (*hash totals*) – sprawdzenie, czy sumy określonych pól (np. sumy liczby sztuk towarów) odpowiadają sumie ogólnej,
- kontrola kolejności (*sequence check*) – sprawdzenie, czy numeracja dokumentów jest ciągła,
- kontrola powtórzeń (*duplicate check*) – sprawdzenie, czy dokumenty nie zostały wprowadzone kilkakrotnie,
- kontrola limitów (*limit check*) – sprawdzenie, czy wprowadzona wartość nie przekracza określonego limitu[14],
- kontrola zakresu (*range check*) – sprawdzenie, czy dane mieszczą się w ustalonym zakresie (np. numer miesiąca od 1 do 12),
- kontrola poprawności danych (*validity check*) –sprawdzenie, czy wprowadzane dane są zgodne z założonymi kryteriami (np. płeć – K lub M),
- kontrola racjonalności (*reasonableness check*) – weryfikacja, czy wprowadzane dane mają sens[15],
- kontrola słownikowa (*table look-ups*) – sprawdzenie, czy wprowadzane dane pochodzą z określonego słownika danych,

---

sposoby uwierzytelniania: na podstawie wiedzy (użytkownik wie coś, co pozwala na jego uwierzytelnienie - np. zna hasło), na podstawie fizycznego posiadania (użytkownik posiada jakiś przedmiot, który jest podstawą jego uwierzytelnienia, np. kartę magnetyczną), na podstawie indywidualnych cech osoby (użytkownik poddaje się działaniu tzw. czujników biometrycznych, które sprawdzają jego indywidualne cechy, np. linie papilarne). Oczywiście, każdy z wymienionych sposobów ma wady i zalety, które decydują o jego popularności i zakresie zastosowań (zob. np. [18; 19]).

[12] Kontrole danych wejściowych mogą być przeprowadzane manualnie (kiedy użytkownik sam kontroluje wprowadzane dane) lub automatycznie (kiedy użytkownik określi wcześniej zestaw warunków, a procedury programu zgodnie z nimi kontrolują dane). Oczywiście, wykorzystując możliwości systemów informatycznych, dąży się do tego, aby jak największa liczba kontroli realizowana była automatycznie.

[13] W kontekście systemu informatycznego rachunkowości często obok pojęcia dane stosuje się pojęcie dokument, jako zbiór danych logicznie ze sobą powiązanych (np. faktura, nota odsetkowa, wyciąg bankowy).

[14] Dla klienta może być określony np. limit na dopuszczalną wielkość zakupu na kredyt kupiecki i program powinien kontrolować, czy nie został on przekroczony.

[15] Na przykład sprawdzenie, czy zlecenie na przewóz osób autokarem nie obejmuje większej liczby osób niż dopuszczalna liczba pasażerów w autokarze.

- weryfikacja cyfr kontrolnych (*check digit*) – sprawdzenie, czy wyliczona cyfra kontrolna jest zgodna z cyfrą dołączoną do danych (np. w numerach rachunków bankowych),
- kontrola kompletności (*completeness check*) – sprawdzenie, czy wszystkie wymagane pola mają wprowadzoną wartość,
- kontrola związków logicznych (*logical relationship link*) – sprawdzenie, czy wprowadzone dane mają sens w połączeniu z danymi, które już zostały wprowadzone lub przyjęte przez domniemanie (np. data wystawienia faktury nie może być późniejsza niż data jej zaksięgowania),
- kontrola poprawności podpisu cyfrowego (*electronic signature*) – sprawdzenie, czy podpis cyfrowy porcji danych jest prawdziwy (pozwala to potwierdzić integralność i wiarygodność danych).

Kontrole wprowadzanych danych są niezwykle istotne dla poprawności funkcjonowania systemu informatycznego rachunkowości. Wskazane jest, aby SIR automatycznie sprawdzał poprawność jak największej liczby danych. Istotne jest, aby sprawdzane były przynajmniej takie elementy, jak: istnienie konta w planie kont, status konta (aktywne/nieaktywne), uprawnienia użytkownika w zakresie dostępu do konta, dopuszczalność zaksięgowania danego rodzaju dokumentu na danym koncie, właściwość typu konta (rozrachunkowe, bilansowe), unikatowość symbolu dowodu, wypełnienie obligatoryjnych pól formularza (np. numer faktury, treść operacji), istnienie w bazie danych rekordów zawierających treść zgodną z zawartością pól referencyjnych formularza (np. porównanie nazwy kontrahenta z faktury z nazwą kontrahenta w bazie kontrahentów), dwustronność księgowania, zgodność sum Winien i Ma, zawieranie się księgowanej kwoty w dopuszczalnym zakresie, suma kontrolna dowodu, suma kontrolna paczki dowodów [16].

Jeżeli podczas kontroli wprowadzanych danych wykryte zostaną błędy, to w zależności od sposobu wprowadzania danych (bieżące, wsadowe) mogą być realizowane następujące działania:

- odrzucenie całej partii wprowadzanych danych,
- wstrzymanie wprowadzania danych, aż zostaną poprawione błędy,
- odrzucenie błędnych danych i dalsze wprowadzanie danych poprawnych.

3.2.2. Kontrola przetwarzania danych

Przetwarzanie danych powinno być kontrolowane, aby można było zapobiec nieautoryzowanej modyfikacji lub usunięciu danych. Podczas przetwarzania mają zastosowanie takie kontrole, jak:

- kontrola „drugiej ręki" – zatwierdzenie rozpoczęcia przetwarzania przez drugą osobę,
- powtórna autoryzacja – dodatkowa weryfikacja użytkownika przed rozpoczęciem przetwarzania (np. podanie dodatkowego hasła przed wykonaniem przelewu),

– przeliczanie ręczne – ręczne sprawdzenie niektórych danych (np. przy wypłacie gotówki w kasie kasjer ręcznie przelicza wypłacaną kwotę).

3.2.3. Kontrola danych wyjściowych

W przypadku danych wyjściowych należy przede wszystkim pamiętać, że dane te powinny być udostępniane wyłącznie upoważnionym osobom w ściśle określonych terminach i miejscach. Dlatego, poza kontrolami podczas wprowadzania danych, należy zwrócić uwagę na następujące zagadnienia:

– udostępnianie danych wyjściowych – sprawdzanie, czy tylko uprawnieni użytkownicy mają dostęp do tych danych,
– rejestrowanie przypadków udostępnienia danych wyjściowych, tzn. jakie dane, komu, kiedy, przez kogo i na jakiej podstawie zostały udostępnione.

Należy ponadto kontrolować i ograniczać ewentualną możliwość nieautoryzowanego uzyskania danych z aplikacji bez generowania danych wyjściowych[16].

4. Zakończenie

Podsumowując, należy stwierdzić, że kontrola ma zasadnicze znaczenie dla przetrwania i rozwoju przedsiębiorstwa. Pomaga lepiej przystosować się do zmiennych warunków rynkowych, umożliwia wykrywanie błędów, oszustw i niegospodarności, wpływa na podjęcie trafnych decyzji. Sprawność systemu kontroli zależy jednak od odpowiednio dobranych instrumentów kontrolnych. Narzędzia te mogą być bardzo zróżnicowane, gdyż system kontroli funkcjonuje często w otoczeniu zdywersyfikowanym pod względem kulturowym, prawnym, organizacyjnym, wielkości czy wreszcie wykorzystywanych technologii przetwarzania danych.

Kontrola wewnętrzna jest jednak tylko częścią procesu zarządzania i należy pamiętać, że nawet najlepszy system kontroli nie wystarczy, jeśli zarząd nie korzysta z generowanych przez niego informacji. Efektywność systemu kontroli osiąga się dzięki ludziom. To personel przedsiębiorstwa musi dostrzec potrzebę odpowiedniego projektowania, utrzymywania i monitorowania systemu kontroli. Jest to szczególnie istotne w warunkach dynamicznego rozwoju TI, kiedy wciąż pojawiają się nowe wyzwania, takie jak kontrola dostępu, ochrona danych, zabezpieczenia fizyczne czy wiele innych dotychczas nawet nierozpoznanych i niezdefiniowanych.

[16] Na przykład jeżeli w programie istnieje możliwość zaznaczenia i skopiowania danych (np. listy klientów) przy użyciu schowka do innego pliku, to należy uwzględnić, że może to zostać wykorzystane w sposób nieuprawniony. Podobnie sytuacja wygląda, jeżeli program tworzy tymczasowe pliki wynikowe, do których mają dostęp niepowołane osoby.

Literatura

[1] Burzym E., *Rachunkowość przedsiębiorstw i instytucji*, PWE, Warszawa 1980.
[2] Cadbury Report, Report of the Committee on the Financial Aspects of Corporate Governance, Gee and Co Ltd., Londyn December 1992.
[3] Ciesielczyk T., Watras G., *Kontrola wewnętrzna w środowisku informatycznym*, Prace Naukowe Akademii Ekonomicznej nr 872, AE, Wrocław 2000.
[4] COBIT 3rd Edition. IT Governance Institute 2002.
[5] Criteria of Control, Canadian Institute of Chartered Accountants, Toronto, December 1995.
[6] Czerwiński K., *Audyt wewnętrzny*, Wydawnictwo InfoAudit Sp. z o.o. , Warszawa 2004.
[7] Forystek M., *Audyt informatyczny*, Wydawnictwo InfoAudit Sp. z o.o. , Warszawa 2005.
[8] Idzikowska G., Owczarek Z., *Badanie kontroli wewnętrznej stosowanej przy zinformatyzowanej księgowośc – podstawowe problemy*, „Rachunkowość" 1998, Zeszyt Specjalny.
[9] Internal Control – Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission, Jersey City 1992.
[10] INTOSAI Auditing Standards, The International Organization of Supreme Audit Institutions, 1992.
[11] *Kontrola wewnętrzna – zintegrowana koncepcja ramowa*, Tłumaczenie PIKW, Fundacja Rozwoju Rachunkowości, Warszawa 1999.
[12] Krzywda D., *Istota i znaczenie współczesnej rewizji finansowej*, [w:] *Sprawozdawczość i rewizja finansowa w procesie podnoszenia kwalifikacji kadry menadżerskiej*, red. B. Micherda, AE, Kraków 2003.
[13] Kwasiborski A., *Kryteria oceny poprawności działania podsystemów rachunkowości informatycznej*, „Rachunkowość" 1998 nr 4-5.
[14] Messier W.T. jr., *Auditing. A Systematic Approach*, McGraw-Hill Companies, New York 1997.
[15] Ostaszewicz A., *Mikrokomputery i ich wpływ na rewizję finansową*, „Rachunkowość – Audytor" 2001 nr 3/8.
[16] *Rachunkowość*, red. M. Gmytrasiewicz, Wydawnictwo Prawnicze LexisNexis, Warszawa 2003.
[17] Rekomendacja H – dotycząca kontroli wewnętrznej w banku, Generalny Inspektorat Nadzoru Bankowego NBP, Warszawa 2002.
[18] Rozbicki L., Ryżko J., Sławiński J., *Systemy kontroli dostępu*, „Informatyka" 2000 nr 1.
[19] Ryżko J., *Zastosowanie metod biometrycznych w dziedzinie prawa i porządku*, „Informatyka" 2000 nr 10.
[20] Saunders E., *Audyt i kontrola wewnętrzna w przedsiębiorstwach*, Wydawnictwo EDUCATOR, Częstochowa 2002.
[21] Skowroński J., *Badanie ksiąg rachunkowości informatycznej*, „Rachunkowość" 1993 nr 3.
[22] Standardy, wytyczne i procedury audytowania i kontrolowania systemów informatycznych, The Information Systems Audit and Control Association 2002, http://www.isaca.org/.
[23] Stępniewski J., *Audyt i diagnostyka firmy*, AE, Wrocław 2001.

GENERAL CONTROL AND APPLICATION CONTROL IN AN ACCOUNTING INFORMATION SYSTEMS

Summary

Development of information technology (IT) and data storing devices as well as availability of Accounting Information Systems (AISs) on the Polish market have led not only to common utilization of IT in the field of book-keeping, but also to substantial changes in keeping and storing books. Variety of software packages, which are developed by applying the latest IT achievements, causes that AISs, which are utilized by business entities, function based upon various solutions.

Accounting Information Systems, however, have to fulfill many requirements. The basic of them are security and quality of data. Therefore, nowadays both general and application controls are introduced to AISs.