*Tomasz Siemieniuk**

BEZPIECZEŃSTWO INFORMATYCZNYCH SYSTEMÓW FINANSOWO - KSIĘGOWYCH

Wprowadzenie

Współcześni przedsiębiorcy zmuszeni są do szybkiego przesyłania informacji, kontrolowania spraw finansowych i efektywnego zarządzania firmą. W związku z tymi aspektami niezbędne jest posiadanie odpowiedniego systemu informatycznego, który zaspokoi wszystkie oczekiwania przedsiębiorcy.

Informatyczny system finansowo - księgowy musi również zapewniać poczucie bezpieczeństwa, które jest jedną z podstawowych wartości w życiu każdego człowieka, nie tylko przedsiębiorcy. Bezpieczeństwo informacyjne jest kluczowym i kosztownym celem każdego przedsiębiorstwa.

Przy wyborze informatycznych systemów finansowo - księgowych bezpieczeństwo ich funkcjonowania jest jednym z najważniejszych elementów, na które powinno się zwrócić uwagę. Dołożenie odpowiednich starań przy wyborze wyżej wymienionego systemu może usprawnić pracę firmy oraz zapobiec możliwości ponoszenia ewentualnych strat danych lub strat finansowych. Wielopoziomowa struktura systemu bezpieczeństwa jest w stanie ograniczyć ryzyko utraty, nieupoważnionej edycji lub nadpisania, a nawet wykradzenia danych.

Szybkiemu rozwojowi technologii towarzyszy coraz większe zagrożenie bezpieczeństwa, wynikające ze wzrastającej złożoności systemów informatycznych. W konsekwencji występuje trudność objęcia wszystkich danych ochroną - niezbędny jest również rozwój bezpieczeństwa w informatycznych systemach finansowo - księgowych.

Skomplikowana struktura informatycznych systemów finansowo - księgowych oraz trudność w zapewnieniu ich bezpieczeństwa to jedne z największych problemów współczesnych przedsiębiorców.

* *dr inż. Tomasz Siemieniuk - Wyższa Szkoła Finansów i Zarządzania w Białymstoku.*

Głównym celem publikacji jest analiza bezpieczeństwa informatycznych systemów finansowo-księgowych. Szczególną uwagę należy zwrócić na wiarygodność takiego oprogramowania oraz skuteczność w ochronie danych i poufnych informacji przedsiębiorstwa.

Celowi opracowania podporządkowano strukturę składającą się z czterech części.

Pierwsza część poświęcona jest bezpieczeństwie w cyberprzestrzeni, z wyszczególnieniem na takie aspekty jak: świadomość pracowników czy strategia firmy w sferze bezpieczeństwa. Omówione zostało bezpieczeństwo w sieci i na serwerach, gdzie wyszczególniono bezpieczeństwo danych na różnego rodzaju infrastrukturach systemu informatycznego.

Druga część publikacji dotyczy opisu zagrożeń zakłócających bezpieczeństwo systemów informatycznych. Uwzględnione również zostały źródła, z których mogą pochodzić te zagrożenia, jak również wyszczególnione aspekty z zakresu utraty dokumentacji elektronicznej, dostępu do niezabezpieczonego stanowiska komputerowego, ujawnienia haseł oraz instalacji nielegalnego oprogramowania.

Trzecia część opracowania to analiza wymogów ustawowych związanych z systemami księgowymi. W tej części pracy przedstawione zostaną wymogi Ustawy o Rachunkowości oraz innych dokumentów w zakresie bezpieczeństwa systemów księgowych.

W czwartej części zostały przedstawione zabezpieczenia systemów informatycznych wykorzystywanych w finansach i rachunkowości, takie jak: kontrole dostępu logicznego i zabezpieczenia sieci informatycznych. Ponadto została wskazana kryptografia jako element zabezpieczenia sieci teleinformatycznych. Całość kończy podsumowanie zagadnień i wnioski.

Bezpieczeństwo systemów informatycznych jako element strategii firmy

Bezpieczeństwo systemów informatycznych wraz z rozwijającą się technologią wymaga coraz to większego udziału przedsiębiorstw w zapewnienie sobie ochrony na tej płaszczyźnie. Proces integracji technologii informatycznych z telekomunikacją określa pojęcie teleinformatyka. Internet jako powszechne źródło wiedzy czy źródło komunikacji międzyludzkich jest ogólnie dostępny[1]. Umożliwia on bardzo szerokie spektrum wyboru narzędzi pomocnych do codziennego funkcjonowania, ale niestety posiada również ciemne strony jego

[1] T. Muliński, *Zagrożenia bezpieczeństwa dla systemów informatycznych e-administracji*, Wyd. CeDeWu.pl, Warszawa 2015, s. 41-42.

użytkowania. To, co się dzieje w globalnej sieci, jaką jest Internet w pewnym stopniu odzwierciedla to, do czego dochodzi w naszym ludzkim świecie, gdzie przestępczość widzimy na porządku dziennym. Mimo to, współczesny świat wiele zawdzięcza technologiom informatycznym, bez których osiągnięcie wysokiego rozwoju cywilizacyjnego byłoby wręcz niemożliwe. Bezpieczeństwo informacji możemy wyróżnić jako[2]:

a) Bezpieczeństwo systemu informatycznego – ma na celu zapobieganie możliwości odtworzenia informacji ze sprzętu teleinformatycznego czy bazy danych firmy, przez jakąkolwiek nieuprawnianą jednostkę;
b) Cyberbezpieczeństwo – można równie dobrze użyć określenia „bezpieczeństwo Internetu", które odnosi się do bezpieczeństwa w sektorze publicznym.

Bezpieczeństwo informatyczne ma szersze znaczenie niż bezpieczeństwo teleinformatyczne, ponieważ można zauważyć, że wykracza poza systemy informatyczne. W bezpieczeństwie teleinformatycznym podmiotem bezpieczeństwa jesteśmy my, jako ludzie. Natomiast przedmiotem jest system teleinformatyczny, który najprościej możemy zdefiniować jako: zespół urządzeń informatycznych, które współpracują ze sobą (przetwarzają, przechowują, wysyłają oraz odbierają dane) poprzez sieci telekomunikacyjne. Próby określenia bezpieczeństwa pojawiły się już w starożytności, jako jedna z podstawowych potrzeb człowieka, dlatego tak ważne jest dbanie o kształcenie i nieustanny rozwój na tej płaszczyźnie[3].

Ważnym elementem strategii firmy jest kwestia bezpieczeństwa informacji, za którą na poziomie operacyjnym oraz podczas wdrożenia odpowiednich procedur i zabezpieczeń, powinno odpowiadać kierownictwo. Organizacja odniesie sukces tylko wtedy, gdy zrozumie, że ochrona informacji może przynieść wymierne korzyści przede wszystkim poprzez zapewnienie jej konkurencyjności[4].

W momencie, kiedy zastanawiamy się nad bezpieczeństwem w sieci, należy zwrócić uwagę na to z jakim modelem wdrażania chmury mamy do czynienia. W przypadku, kiedy używamy prywatnej chmury istniejące zabezpieczenia powinny być wystarczające, jednak kiedy mamy do czynienia z chmurą

[2] T. Muliński, *Zagrożenia bezpieczeństwa dla systemów...*, op. cit., s. 43.
[3] Ibidem, s. 48-53.
[4] D. Książek, *Bezpieczeństwo informacji jako element strategii firmy,* (w:) *Wybrane problemy zarządzania bezpieczeństwem informacji,* red. J. Brdulak, P. Sobczak, Oficyna Wydawnicza Szkoły Głównej Handlowej w Warszawie, Warszawa 2014, s. 25-27.

publiczną istotną czynnością będzie zabezpieczenie połączenia z dostawcą i pamiętanie o następujących czynnościach[5]:

- zabezpieczenie transmisji danych do chmury,
- zabezpieczenie dostępu do zasobów w chmurze,
- zadbanie o dostępność zasobów chmury dla własnych klientów.

Można również zabezpieczyć naszą chmurę poprzez szyfrowanie połączeń czy cyfrowe podpisywanie danych. W sytuacji, kiedy mówimy o zabezpieczeniu serwerów, decydujące znaczenie ma używany model chmury. W sytuacji używania gotowej platformy, nad bezpieczeństwem czuwa dostawca, a użytkownik może się zabezpieczyć odpowiednią umową. W przypadku, kiedy używamy wirtualnej infrastruktury, istnieją dwa poziomy na których może wystąpić zagrożenie[6]:

- Poziom systemu operacyjnego, którym odpowiedzialność spada na klienta, w jego kwestii leży prawidłowa konfiguracja usług systemowych, instalacja poprawek oraz zarządzania kontami użytkowników;
- Poziom platformy wizualizacyjnej zarządzanej przez dostawcę. Tą platformę zależy zabezpieczyć, ponieważ pozwala ona na szybkie tworzenie i usuwanie instalacji systemu operacyjnego.

Przy transmisji danych wystarczy zabezpieczyć transmisję wewnątrz i na zewnątrz chmury przy pomocy odpowiedniego bezpieczeństwa protokołu, jednak kiedy mówimy o danych uśpionych zapewnienie bezpieczeństwa robi się bardziej skomplikowane. W przypadku chmury IaaS wystarczy zaszyfrować nieużywane dane i odszyfrować kiedy je przetwarzamy. W chmurze PaaS i SaaS dane nieużywane są indeksowane lub wyszukiwane. W przypadku chmury współdzielonej może dochodzić do sytuacji, np. poprzez błąd oprogramowania, że dane naszych klientów wykradnie inny użytkownik chmury. Najtrudniejsze do zapewnienia bezpieczeństwa są dane przetwarzane, które przed przetwarzaniem muszą być odkodowane. Podsumowując, podstawowym krokiem do zapewnienia bezpieczeństwa danym jest szyfrowanie przy pomocy bezpiecznych algorytmów, a następnie zapewnienie integralności danych. Mimo wszystko zapewnienie bezpieczeństwa danym jest jednym z największych wyzwań przy wdrażaniu chmury[7].

[5] P. Berliński, *Wyzwania związane z przetwarzaniem w chmurze,* (w:) *Wybrane problemy zarządzania …,* op. cit., s. 195-196.
[6] P. Berliński, *Wyzwania związane …*, op. cit., s. 197.
[7] Ibidem, s. 200-202.

Zagrożenia bezpieczeństwa informatycznego

Zarówno w życiu realnym, tak i w świecie wirtualnym występuje wiele zagrożeń, przy tym drugim napotkamy niebezpieczeństwa wewnętrzne i zewnętrzne. Niebezpieczeństwo zewnętrzne czyli ataki hakerów na nasze dane przechowywane na komputerze, telefonie, tablecie są w dzisiejszych czasach codziennością. Najczęściej jednak na ataki narażone są firmy, których dane i strategiczne kontakty są bardzo cenne. Obciążenie systemów informatycznych, tak aby uniemożliwić wykonywanie pracy to jedne z najlżejszych ataków, do cięższych należy całkowite zatrzymanie systemu lub całkowite odcięcie dostępności do systemów. Firmy starają się wprowadzać odpowiednie procedury i systemy, które mają utrudnić dostanie się do wnętrza firmy, jednak najczęściej wprowadzane są one dopiero po atakach hakerów. Podstawowe procedury to jak najszybsze zatrzymanie ataku i przywrócenie systemu do pracy. Żeby jednak zapobiegać atakom hakerów, najważniejsze jest dążenie do wcześniejszej ochrony systemu, które uniemożliwi uzyskanie informacji osobom z zewnątrz.

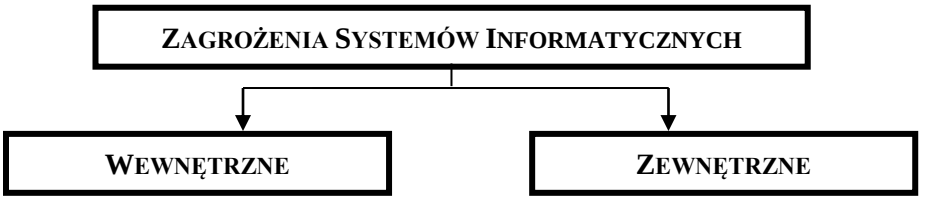
Zagrożenie może być potencjalną przyczyną niepożądanego incydentu, który może spowodować szkodę dla systemu bądź też instytucji wraz z jej zasobami. Szkoda ta powstaje w wyniku bezpośredniego lub pośredniego ataku na informację przetwarzaną przez system lub usługę informatyczną, na przykład uszkodzenie, ujawnienie, modyfikację informacji lub jej dostępności[8]. Największym zagrożeniem dla bezpieczeństwa teleinformatycznego jest przede wszystkim utrata: poufności, integralności, rozliczalności, autentyczności i niezawodności informacji oraz usług. Zagrożenia mogą być przypadkowe lub zamierzone, ludzkie lub środowiskowe. Norma dzieli je i wyszczególnia na zagrożenia: ludzkie zamierzone - przykładem może być podsłuch, modyfikacja informacji, kradzież; ludzkie przypadkowe czyli pomyłki i pominięcia oraz środowiskowe związane z trzęsieniem ziemi, pożarem czy też powodzią[9].

Przyczyn powstawania zewnętrznych zagrożeń dla bezpieczeństwa informacji powinniśmy szukać poza daną organizacją, natomiast wewnętrzne zagrożenia to te, których źródło jest umiejscowione wewnątrz organizacji użytkującej system informatyczny.

[8] J. Łuczak, M. Tyburski, *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC,* Wyd. Uniwersytetu Ekonomicznego w Poznaniu, Poznań 2009, s. 285.

[9] I. Wołłejko-Chwastowicz, *Wpływ porażek projektów IT na bezpieczeństwo,* (w:) *Wybrane problemy zarządzania …,* op. cit., s. 167.

Rysunek 1. **Podział zagrożeń pod względem lokalizacji ich źródła**



Źródło: opracowanie na podstawie: M. Pieniak, *Zagrożenia dla bezpieczeństwa informacji,* (w:) Wybrane problemy zarządzania bezpieczeństwem informacji, red. J. Brdulak, P. Sobczak, Oficyna Wydawnicza Szkoły Głównej Handlowej w Warszawie, Warszawa 2014, s. 29, 32.

Jednym z największych zagrożeń bezpieczeństwa wewnętrznego jest sam człowiek. Wiele się słyszy o utracie danych, włamaniu do systemu czy też ujawnieniu poufnych danych lub haseł. Coraz częściej w firmach stosuje się politykę bezpieczeństwa, tak aby uniknąć zagrożenia. Mimo ludzkiej świadomości, nie zawsze człowiek stosuje się do danych zasad. Najczęstszym problemem jest fakt, że ludzie pracują na swoich prywatnych komputerach, na których przechowują różnego rodzaju pliki, a nie zawsze robią kopię bezpieczeństwa, co może spowodować przede wszystkim utratę ważnych dokumentów, umów, swoich danych bądź też klienta. Korzystając również z przeglądarki internetowej, jesteśmy narażeni na ściągnięcie nieświadomie wirusa lub zostanie ofiarą ataku hackerskiego. Kolejnym przykładem zagrożenia bezpieczeństwa jest ujawnianie poufnych danych. Często ludzie bezmyślnie wyrzucają dokumenty nie zwracając uwagi, iż na nich są dane osobowe, które można wykorzystać w sposób niekoniecznie korzystny dla nich[10].

Zewnętrznymi zagrożeniami dla informacji są przede wszystkim hackerzy oraz cyberprzestępcy. Hackerstwo jest próbą uzyskania dostępu do systemu komputerowego z pominięciem uwierzytelniania. Ataki przeprowadzane są poprzez niechronione, otwarte porty, czyli kanały komunikacji komputera z Internetem[11]. Celem hackera jest głównie kradzież danych bądź celowe wyrządzanie szkód, najczęściej osoba, która padła ofiarą hackerstwa jest tego nieświadoma i przez długi czas nie zauważa niebezpiecznych skutków jego włamania. Hacker działa w sposób bezpośredni, łamiąc zabezpieczenia i podszywając się

[10] M. Pieniak, *Zagrożenia dla bezpieczeństwa informacji,* (w:) *Wybrane problemy zarządzania …,* op. cit., s. 30.

[11] M. Kopczewski, E Czapik-Kowalewska, *Zagrożenia sieciowe a bezpieczeństwo informacyjne,* Czasopismo Naukowego Koła Studentów Wydziału Elektroniki i Informatyki Politechniki Koszalińskiej „Omega", „Modele Inżynierii Teleinformatyki" , Koszalin 2011, nr 6, s. 58.

za uprawnionego użytkownika lub w sposób pośredni, czyli atakuje system wykorzystując wirusy lub konie trojańskie. Najczęściej hackerzy wolą zostać anonimowi, by móc dłużej korzystać z nieuprawnionego dostępu do danych lub podszywać się pod inne osoby. Każde włamanie jest niebezpieczne, ponieważ informacje pozyskane przez hackera są najczęściej dla właściciela cenniejsze od posiadanych dóbr materialnych. Uzyskane dane osobowe, loginy, hasła mogą zostać publicznie udostępnione i stać się następstwem kolejnych włamań. W celu uniknięcia bądź zapobiegania atakom hackerskim najlepiej jest przyswoić wiedzę na temat ochrony prawnej w Internecie oraz szukać pomocy u administratora serwera lub zgłosić przestępstwo na policję.

Zagrożenia bezpieczeństwa są wielorakie. Mogą być losowe lub celowe (pobudzane chęcią zysku). Mogą również wywodzić się z poza systemu lub z jego centrum. Duża część tych działań w świetle obecnego prawa rozpatrywana jest jako przestępstwo. Między innymi są to[12]:

- włamanie do systemu komputerowego,
- nieuprawnione pozyskanie informacji,
- destrukcja danych i programów,
- sabotaż systemu,
- piractwo komputerowe i kradzież oprogramowania,
- oszustwo komputerowe i fałszerstwo komputerowe,
- szpiegostwo komputerowe.

Zabezpieczenie informatyczne powinno być wieloetapowe i gruntowne, aby wyeliminować problemy łańcucha bezpieczeństwa, powinno zostać urzędowo sprecyzowane w formie procedur[13].

Jest wiele przypadków utraty danych elektronicznych. Mogą to być między innymi kradzieże, wadliwy sprzęt lub zarażenia wirusem. Zawsze trzeba pamiętać o dodatkowym zapisie w osobnym magazynie danych, np. dysku sieciowym. Kopie zapasowe powinny być wykonywane w różnych odstępach czasu. Informacje przechowywane w lokalnym urządzeniu sieciowym powinny być kodowane, opierając się na kluczu kryptograficznym. Dojście do tych informacji możliwe jest tylko poprzez podanie hasła. Kopie istotnych informacji powinny być sporządzane również poza przedsiębiorstwem[14].

---

[12] http://wazniak.mimuw.edu.pl/index.php?title=Bezpiecze%C5%84stwo_system%C3%B3w_komputerowych_-_wyk%C5%82ad_1%3AWprowadzenie_do_problematyki_bezpiecze%C5%84stwa_system%C3%B3w_komputerowych#Zagro.C5.BCenia_bezpiecze.C5.84stwa [dostęp 12.08.2022].

[13] Ł. Kaliś, *Praktyczne zalecenia w zarządzaniu bezpieczeństwem informacji,* (w:) *Wybrane problemy zarządzania …,* op. cit., s.105.

[14] Ł. Kaliś, *Praktyczne zalecenia w zarządzaniu…,* op. cit., s. 105-106.

Dostęp do stanowiska komputerowego powinien być tylko dla osób do tego powołanych, które mają wgląd w hasła i wszystkie ważne informacje[15]. Jednym z zagrożeń systemów informatycznych są niezabezpieczone hasła. Tworzenie bezpiecznych haseł oraz wymóg okresowej ich zmiany opisany jest w polityce bezpieczeństwa informacji. Według wytycznych, bezpieczne hasło powinno być zbiorem liter, które nie tworzą żadnego wyrazu słownikowego, a także hasło nie może być też nigdzie zapisywane, np. na kartce. Ponadto systemy z domyślnym hasłem powinny wymagać utworzenia nowego, trudnodostępnego hasła po pierwszym zalogowaniu użytkownika. Każde domyślne hasło powinno być niezwłocznie zastąpione nowym. Każde hasło dostępu powinno się zmieniać po około 1 miesiącu od jego ustawienia. Powinno także być łatwe do odgadnięcia, tj. ciąg liczb lub liter na klawiaturze oraz powinno wyróżniać się spośród innych haseł użytkownika.

Zaleca się także tworzenie oddzielnego konta, które nie ma praw administratora, w przypadku systemów operacyjnych na komputerach przenośnych. Każde hasło jest własnością danego użytkownika i nie może być nikomu ujawniane. Jest jednak wyjątek, w którym dopuszcza się ujawnienia hasła, ale tylko na polecenie przełożonego (ustne) lub członka zarządu. Po podaniu hasła użytkownik powinien je niezwłocznie zmienić na inne. Wszystkie tego typu sytuacje powinny być wyczerpująco opisane w procedurach[16].

Każdy sprzęt komputerowy podlega inwentaryzacji. To oznacza, że każdy komputer musi posiadać kartotekę urządzenia z jego podstawowymi danymi, m.in. nazwa urządzenia, dane personalne użytkownika, datę zakupu czy szczegółowy wykaz oprogramowania.

Istnieją takie pakiety programów, które pozwalają na zdalną inwentaryzację oprogramowania. Ponadto można za ich pomocą także śledzić zmiany w konfiguracji sprzętu. Takie pakiety tworzą kartotekę sprzętu i wykazu oprogramowania i budują ją najczęściej moduły, które można dodawać (podlega to opłacie) lub usuwać.

Każdy z pracowników powinien mieć ograniczony dostęp do niektórych stron www, w zależności od wykonywanych zadań. Program, który blokuje takie strony powinien przeprowadzać analizę danej otwartej strony internetowej, by zindeksować stronę i ewentualnie blokować niepożądane treści (np. strony erotyczne). Poza blokowaniem szkodliwych stron internetowych, komputery powinny posiadać blokadę zapisu danych na nośnikach zewnętrznych, np. USB[17].

[15] Ł. Kaliś, *Praktyczne zalecenia w zarządzaniu…,* op. cit., s. 106.
[16] Ibidem, s. 107-108.
[17] Ibidem, s. 107.

Dzisiejsze systemy ochrony oprogramowania przed zagrożeniami bezpieczeństwa stają się coraz bardziej rozbudowane i obejmują już nie tylko programy antywirusowe, ale także chronią powiązane przeglądarki internetowe czy programy do zarządzania pocztą elektroniczną. Ochrona bezpieczeństwa polega na skanowaniu podłączanych do komputera nośników wymiennych, częstej i systematycznej aktualizacji wirusów. Istnieją różne rodzaje oprogramowania do ochrony systemów teleinformatycznych i są nimi m.in. Avast, Kaspersky, Norton, czy Panda[18].

Programy te chronią systemy przed atakami zagrażającymi ich bezpieczeństwu. Ataki te polegają na wyszukiwaniu tzw. luk w oprogramowaniu, aplikacjach zainstalowanych na komputerze i systemach baz danych. Twórcy takich systemów ochrony systematycznie uaktualniają wersje swoich programów, które są dostosowywane do coraz nowszych słabości systemów operacyjnych, by w pełni mogły je zabezpieczać.

Źródeł zagrożeń w systemach informatycznych należy doszukiwać się w samych systemach i produktach firm takich jak Microsoft, Linux, czy Oracle. Najczęstszym źródłem zagrożeń są luki w zabezpieczeniach , które mogą zostać wykorzystywane w atakach na systemy informatyczne. To właśnie błędy i nieprawidłowości w działaniu produktów, aplikacji, czy programów są głównymi celami ataków[19].

Wymogi ustawowe związane z informatycznymi systemami finansowo - księgowymi

Zgodnie z Ustawą o rachunkowości prowadzenie ksiąg rachunkowych przy pomocy komputera zobowiązuje do[20]:

- prowadzenia wykazu zbiorów danych tworzących księgi rachunkowe na informatycznych nośnikach danych z określeniem ich struktury i wzajemnych powiązań;
- opisu systemu informatycznego, zawierającego wykaz programów, procedur lub funkcji, w zależności od struktury oprogramowania, wraz z opisem algorytmów i parametrów;
- stworzenia programowych zasad ochrony danych, w tym w szczególności metod zabezpieczenia dostępu do danych i systemu ich przetwarzania;
- określenia wersji oprogramowania i daty rozpoczęcia jego eksploatacji.

[18] T. Muliński, *Zagrożenia bezpieczeństwa dla systemów…,* op. cit., s. 172.
[19] Ibidem, s. 173-175.
[20] *Ustawa z dnia 29 września 1994r. o rachunkowości,* Dz. U. 2017, poz. 61 z późn. zm., Art. 10.

Ustawa przewiduje również, że jednostki, które prowadzą księgi rachunkowe przy użyciu komputera zobowiązane są do opisu systemu służącego ochronie danych[21]. Informatyczny system finansowo księgowy może być użytkowany, jeżeli spełni wymagania zawarte w ustawie.[22]

Zebrane dane podlegają okresowej archiwizacji z powodu zmniejszenia ryzyka wynikającego z możliwości utraty danych (np. awaria komputera, błąd przy wprowadzaniu danych). Aby zmniejszyć to ryzyko należy częściej archiwizować dane. Spora część przedsiębiorstw przeprowadza taką archiwizację po każdym skończonym dniu pracy.

Ważnym zagadnieniem jest także system bezpieczeństwa, który ma na celu ochronę danych i oprogramowania. Powinien zawierać następujące środki ostrożności[23]:

- system zabezpieczeń mechanicznych, który chroni komputer przed zniszczeniem;
- system zabezpieczeń systemu operacyjnego, który ogranicza dostęp poszczególnych osób do najważniejszych funkcji;
- program, który ciągle szkoli pracowników w kierunku bezpieczeństwa danych firmy;
- odpowiedni system i podział pracy w zależności od różnych opcji programów;
- podtrzymanie zabezpieczeń systemów komputerowych i ich ciągła kontrola.

Środkiem ochrony danych zapisywanych w księgach rachunkowych programów finansowo-księgowych jest[24]:

- użycie nośników danych, które są odporne na zagrożenia, a także ich zewnętrzna ochrona;
- regularne tworzenie kopii zapasowych zbiorów danych, które są zapisane na nośnikach komputerowych;
- korzystanie z odpowiednich rozwiązań programowych i organizacyjnych, które skupiają uwagę na ochronę danych przed zniszczeniem.

[21] *Ustawa z dnia 29 września 1994r. o rachunkowości*, op. cit., Art. 71.

[22] Ł. Siemieniuk, *System Symfonia jako przykład zintegrowanego systemu informatycznego w rachunkowości,* „Optimum. Studia ekonomiczne" 2011, nr 1, s. 219.

[23] G. Michalczuk, Ł. Siemieniuk, *Problematyka bezpieczeństwa komputerowych systemów finansowo-księgowych,* (w:) *Finansowe i pozafinansowe aspekty funkcjonowania podmiotów gospodarczych,* red. N. Siemieniuk, G. Michalczuk, E. Tokajuk, Wyd. Uniwersytetu w Białymstoku, Białystok 2014, s. 177-178.

[24] E. Karwowski, *Plan kont. Zasady rachunkowości z komentarzem,* Wyd. Ad. Drągowski, Warszawa 2001, s. 109.

Ochrona tajemnicy korespondencji jako czynnik zapewniający bezpieczeństwo

Powszechnym problemem w praktyce jest prywatna korespondencja pracownika wysyłana zarówno pocztą tradycyjna, jak i elektroniczną. Zgodnie z art. 23 Kodeksu cywilnego[25] tajemnica korespondencji stanowi dobra osobiste człowieka, które są pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach. Błędnie wskazuje się na ograniczenie praw pracownika w związku z łączącym go z pracodawcą stosunkiem pracy. Samo zaadresowanie listu oznacza, że jego treść została skierowana wyłącznie do określonego adresata. Jednakże, w niektórych przypadkach pracodawca ma prawo do kontroli korespondencji pracownika. Dzieje się tak w przypadku wyrażenia zgody pracownika na kontrolę korespondencji. W takiej sytuacji pracodawca nie narusza art. 23 kc. Inaczej dzieje się w przypadku korespondencji prowadzonej w ramach stosunku pracy. W tym przypadku wszystko, czego dokonał pracownik stanowi własność pracodawcy. Dotyczy to również korespondencji, której pracownik nie może skasować lub ukryć przed pracodawcą.

Ochrona korespondencji regulowana jest także w art. 267 kk[26]. Według tego artykułu podmiot, który bez uprawnienia uzyska dostęp do informacji dla niego nie przeznaczonej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch. Korespondencja nie podlega ochronie z art. 267 kk. w sytuacji gdy, pracownik prowadzi korespondencję służbową w imieniu pracodawcy.

Odmiennie kształtuje się sytuacja korespondencji, która dokonywana jest w sieci firmowej za pomocą serwera pocztowego administrowanego przez pracownika. W takim przypadku pracodawca ma dostęp do korespondencji bez przełamywania jakichkolwiek barier. Wobec tego korespondencja taka nie jest chroniona przepisami prawa karnego[27].

Zabezpieczenia dotyczące systemów informatycznych wykorzystywanych w finansach i rachunkowości

Nowoczesne systemy informatyczne kompleksowo wspomagające procesy zarządzania, w związku z rosnącą konkurencją rynkową, są ważnym narzędziem potrzebnym do sprawnego funkcjonowania przedsiębiorstwa. Obecnie

[25] *Kodeks cywilny z dnia 23 kwietnia 1964 r*. Dz. U. 1964 Nr 16, poz. 93 z późn. zm.

[26] *Kodeks karny z dnia 6 czerwca 1997 r.* Dz. U. 1997 Nr 88, poz. 553 z późn. zm.

[27] T. Kwiatkowski, *Prawna ochrona tajemnicy korespondencji elektronicznej w systemach informatycznych,* (w:) *Nowoczesne technologie informatyczne i ich wpływ na funkcjonowanie podmiotów gospodarczych,* red. N. Siemieniuk, Wyd. Wyższej Szkoły Finansów i Zarządzania, Białystok 2005, s. 51-56.

procesy przetwarzania i przesyłania informacji zostały niemal całkowicie zautomatyzowane. Firmy mogą prawidłowo funkcjonować wtedy i tylko wtedy, gdy systemy informatyczne, z których korzystają, są bezpieczne[28].

Jednym z ważniejszym sposobów kontrolowania jest kontrola logicznego dostępu, opierająca się na: powstrzymywaniu nieuprawnionych osób przed dostępem i udzielaniu dostępu jedynie uprawnionym w jak najwęższym możliwym stopniu i kontrolowaniu czynności przez nich wykonywanych. Z kolei zabezpieczenia programowo – sprzętowe odpowiadają za: szyfrowanie informacji, korzystanie zasilania awaryjnego oraz tworzenie kopii bezpieczeństwa. Zabezpieczenia w systemie operacyjnym dotyczą ograniczenia dostępu oraz niedopuszczenia do modyfikacji danych w sposób inny niż przewidziany w systemie. Zabezpieczenia aplikacyjne wyznaczają w jakim stopniu pracownik może mieć dostęp do danej aplikacji. Sieciowe zabezpieczenia to najogólniej mówiąc ochrona przed dostępem osobom nieuprawnionym do sieci komputerowej danej jednostki[29].

Zabezpieczenie sieci informatycznych jest ważnym aspektem zapewnienia bezpieczeństwa pracy. Na rynku występują programy, dzięki którym możemy dodatkowo zabezpieczyć nasze dane, w celu ochrony przed kradzieżą. Najczęstszymi formami ataków są: włamania do systemu, skanowanie hosta, ataki na serwer WWW, e-mail bombing oraz skanowanie firewalli. Bardzo niebezpieczne są również szkodliwe oprogramowania, takie jak: koń trojański, robak sieciowy, robaki skanujące losowo, robaki topologiczne, wirus komputerowy oraz mikrowirusy[30]. Bezpieczeństwo komputerowe postrzegane jest w trzech strefach: sprzętowej, programowej oraz proceduralnej.

Zapora sieciowa jest przykładem zabezpieczania sieci informatycznych przed ingerencją osób trzecich w dane jednostki gospodarczej. Jej główną funkcją jest zapobieganie niepewnych połączeń przychodzących. Zapora sieciowa jest pierwszym elementem, który staje na przeszkodzie wirusom oraz szkodliwym oprogramowaniom, jest to system, który blokuje transfer danych od jednostek nieznanych i niepewnych. Zalety korzystania z zapory sieciowej to kontrola dostępu do ważnych zasobów cyfrowych oraz ochrona zagrożo-

[28] K. Rytelewska, T. Siemieniuk, *Problematyka zabezpieczenia informacji w zintegrowanych systemach informatycznych,* (w:) *Systemy informatyczne a funkcjonowanie organizacji gospodarczych,* red. N. Siemieniuk, J. Sikorski, Wyd. Uniwersytetu w Białymstoku, Białystok 2011, s. 72-73.

[29] G. Michalczuk, Ł. Siemieniuk, *Problematyka bezpieczeństwa …,* op. cit., s. 174-175.

[30] *Rodzaje i klasyfikacja włamań oraz ataków internetowych,* http://hackme.pl/articles.html?article_id=247 [dostęp 11.08.2022].

nych usług Intranetu[31], czyli wewnętrznej sieci informatycznej, która ogranicza się do urządzeń w przedsiębiorstwie.

Ciągły postęp techniczny w świecie cyberprzestrzeni otwiera coraz to większe możliwości korzystania z urządzeń elektronicznych, jak i również Internetu, wraz z nieodzownymi jego elementami tj. programy i aplikacje, które są wykorzystywane przez przedsiębiorstwa. Równolegle z rozwojem systemów informatycznych narasta zagrożenie ich bezpieczeństwa. Działania hackerskie stają się coraz większym zagrożeniem. Wykradanie tajnych danych osobowych oraz finansowych firm to przykłady działań hackerskich. Niezbędna jest ochrona przeciw atakom hackerów. Przykładem systemu obronnego jest urządzenie UTM[32] (Unified Threat Management). Jest to urządzenie, które składa się ze scalonych funkcji zapory sieciowej i innych systemów zabezpieczających. System UTM cechuje się wysoką efektywnością z racji swojej budowy strukturalnej.

Obecnie istnieje wiele urządzeń UTM, które w zależności od wymagalności klienta, posiadają różnorodne funkcje. Do głównych funkcji urządzeń UTM zalicza się:

- zabezpieczenie antyspamowe,
- ochrona przed wirusami,
- funkcja router'a,
- filtr stron internetowych,
- funkcje systemów IPS,
- ochrona przed włamaniami.

IPS (Intrusion Prevention Systems) jest to jeden z sposobów zabezpieczania sieci komputerowych zarówno przed atakami z zewnątrz, jak i wewnątrz. Ważną funkcją IPS jest możliwość monitorowania i kontrolowania, jakie ruchy są dokonywane przez wszystkie osoby które są podłączone do sieci komputerowej - bezpieczeństwo wewnętrzne[33].

Kryptografia jest to dziedzina informatyki zajmująca się utajaniem danych przed niepożądanym dostępem poprzez szyfrowanie. Można ją stosować na wielu płaszczyznach, m.in. uwierzytelnianiu w systemach operacyjnych oraz aplikacjach, szyfrowaniu i uwierzytelnianiu transmisji bezprzewodowej.

[31] S. Wojciechowska-Filipek, Z. Ciekanowski, *Bezpieczeństwo funkcjonowania w cyberprzestrzeni jednostki organizacji państwa*, Wyd. CeDeWu.pl, Warszawa 2016, s. 140.

[32] J. M. Zaczek, *Ewolucja zagrożeń sieciowych motorem ewolucji sieciowych systemów bezpieczeństwa*, „Czasopismo techniczne. Nauki podstawowe" 2012, nr 109, s. 146.

[33] M. Wrzesień, Ł. Olejnik, P. Ryszawa, *IDS/IPS: Systemy wykrywania i zapobiegania włamaniom do sieci komputerowych*, „Pomiary Automatyka Robotyka" 2012, nr 7, s. 16-21.

W kryptografii można stosować szyfrowanie z kluczem symetrycznym i asymetrycznym. Kryptografia symetryczna opiera się na tzw. kluczu symetrycznym (tajnym), który jest narzędziem niezbędnym do szyfrowania i odszyfrowania wiadomości. Musi on być znany zarówno nadawcy, jak i odbiorcy przesyłki. Zaletami tego rodzaju kryptografii jest to, iż algorytmy oparte na kluczach symetrycznych umożliwiają szybkie szyfrowanie danych, a same klucze są relatywnie krótkie. Wadami natomiast jest, między innymi konieczność utrzymania klucza w tajemnicy między osobami komunikującymi się. Aby skomplikować odwzorowanie klucza, można zastosować dodatkowy element w postaci algorytmu (feistel cipher), który zmienia kolejność kodowanych bloków w szyfrogramie kryptografii symetrycznej. Algorytmami takimi są np. DES (Digidal Encription Standard) oraz IDEA (International Data Incription Algorithm) [34].

Z kolei kryptografia asymetryczna używa klucza publicznego oraz prywatnego, który jest utajniony. Klucz publiczny może być powszechnie dostępny. Szyfrowanie przesyłki odbywa się za pomocą klucza publicznego, jednak wiadomość nie może być nim odszyfrowana. W tym wypadku niezbędne jest zastosowanie klucza prywatnego. Zaletą tego podejścia jest fakt, że liczba kluczy asymetrycznych oraz częstość ich wymieniania jest niższa niż w przypadku kluczy symetrycznych. Wadami jest jego wielkość, która wielokrotnie przewyższa klucz symetryczny, a także jego prędkość kodowania, która z kolei jest znacznie niższa. Znalezienie funkcji deszyfrującej utrudniają algorytmy np. RSA, ElGamal, DSS (Digital Signature Standard) [35].

Podpis elektroniczny wykorzystuje szyfrowanie asymetryczne oraz jednokierunkową funkcję skrótu. Ma on postać kilkunastu bajtów i potwierdza integralność przesyłki oraz autorstwo wiadomości. Użycie podpisu elektronicznego nie stanowi niebezpieczeństwa dla poufności przesyłki. W węższym zakresie ma on na celu identyfikację osoby, która składa ten podpis. Natomiast w szerszym znaczeniu posiada następujące cechy[36]:

- integralność, czyli pewność wykrycia zmian w danych przesyłki podczas jej drogi;
- autentykacja, która umożliwia wysłanie przesyłki w czyimś imieniu, podając się za tą osobę;
- autoryzacja, autor nie może wyprzeć się zlecenia;
- umożliwienie weryfikacji podpisu elektronicznego przez niezależną osobę.

[34] K. Rytelewska, T. Siemieniuk, *Problematyka zabezpieczenia informacji …,* op. cit., s. 85-86.
[35] Ibidem, s. 86-87.
[36] Ibidem, s. 88.

Podsumowanie

Systemy informatyczne wykorzystywane są w większości przedsiębiorstw, zapewniają ciągłość pracy w każdej branży, ponadto ułatwiają procesy związane z obsługą finansów przedsiębiorstwa. Systemy te przetwarzają dane związane z finansami jednostki gospodarczej, dlatego zapewnienie ich bezpieczeństwa powinno być dla każdego podmiotu gospodarczego kwestią priorytetową.

Przy wyborze bezpiecznego systemu księgowo - finansowego należy zwrócić uwagę na takie aspekty jak posiadanie zabezpieczenia programowego, które zapewni bezpieczną obsługę danych. Sprzęt, z którego korzysta przedsiębiorstwo powinien posiadać odpowiednie oprogramowanie systemowe, natomiast sieć, powinna być chroniona przez różnego rodzaju zapory sieciowe.

System finansowo - księgowy nie tylko narażony jest na niebezpieczeństwo z zewnętrz, lecz także z wewnątrz, dlatego niezwykle ważna jest ochrona korespondencji oraz kontrola dostępu do baz danych przez osoby nieupoważnione. System ochrony danych to wielopoziomowa konstrukcja, którą należy zabezpieczyć na każdej płaszczyźnie, tak aby nie powstały w niej luki, przez które dane mogłyby ulec zniszczeniu.

Istnieje wiele legislacyjnych aktów, zawierających informacje dotyczące bezpieczeństwa ksiąg rachunkowych, generowanych przez system finansowo - rachunkowy przedsiębiorstwa. Podstawowym aktem definiującym te zagadnienie jest ustawa o rachunkowości, która dokładnie opisuje wszelkie zasady związane z przechowywaniem oraz przetwarzaniem danych systemów informatycznych.

Systemem finansowo - księgowym, który spełnia standardy bezpieczeństwa danych, jest Symfonia, oferowana przez firmę SAGE. Tworzenie kopii zapasowych baz danych, automatyczne uszeregowane archiwizowanie danych oraz tworzenie użytkowników, którym można podporządkować osobne hasła oraz loginy dostępu to podstawowe funkcje oferowane przez program w zakresie bezpieczeństwa informatycznego.

Zapewnienie bezpieczeństwa systemów finansowo - księgowych jest kwestią indywidualną każdego przedsiębiorstwa. Podmioty gospodarcze podejmują decyzje związane z bezpieczeństwem systemów informatycznych. Można uznać, że bezpieczeństwo systemów rachunkowych jest czynnikiem konkurencyjności przedsiębiorstwa na rynku. Odpowiednia ochrona danych uodparnia system jednostki gospodarczej na ataki ze strony konkurencji, dzięki czemu przedsiębiorstwo umacnia swoją pozycję na rynku.

Bibliografia

Finansowe i pozafinansowe aspekty funkcjonowania podmiotów gospodarczych, red. N. Siemieniuk, G. Michalczuk, E. Tokajuk, Wyd. Uniwersytetu w Białymstoku, Białystok 2014.

Karwowski E., *Plan kont. Zasady rachunkowości z komentarzem,* Wyd. Ad. Drągowski, Warszawa 2001.

Kodeks cywilny z dnia 23 kwietnia 1964 r. Dz. U. 1964 Nr 16, poz. 93 z późn. zm.

Kodeks karny z dnia 6 czerwca 1997 r. Dz. U. 1997 Nr 88, poz. 553 z późn. zm.

Kopczewski M., Czapik-Kowalewska E., *Zagrożenia sieciowe a bezpieczeństwo informacyjne,* Czasopismo Naukowego Koła Studentów Wydziału Elektroniki i Informatyki Politechniki Koszalińskiej „Omega", „Modele Inżynierii Teleinformatyki" Nr 6, Koszalin 2011.

Łuczak J., Tyburski M., *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC,* Wyd. Uniwersytetu Ekonomicznego w Poznaniu, Poznań 2009.

Muliński T., *Zagrożenia bezpieczeństwa dla systemów informatycznych e-administracji*, Wyd. CeDeWu.pl, Warszawa 2015.

Nowoczesne technologie informatyczne i ich wpływ na funkcjonowanie podmiotów gospodarczych, red. N. Siemieniuk, Wyd. Wyższej Szkoły Finansów i Zarządzania, Białystok 2005.

Rodzaje i klasyfikacja włamań oraz ataków internetowych, http://hackme.pl/articles.html?article_id=247 [dostęp 11.09.2022].

SAGE Symfonia, http://www.sage.com.pl/produkty/obszar-finansowo-ksiegowy/ksiegowosc/sage-symfonia-finanse-i%20ksiegowosc [dostęp 03.18.2022].

Siemieniuk Ł., *System Symfonia jako przykład zintegrowanego systemu informatycznego w rachunkowości,* „Optimum. Studia ekonomiczne" 2011 nr 1.

Systemy informatyczne a funkcjonowanie organizacji gospodarczych, red. N. Siemieniuk, J. Sikorski, Wyd. Uniwersytetu w Białymstoku, Białystok 2011.

Ustawa z dnia 29 września 1994r. o rachunkowości, Dz. U. 2017, poz. 61 z późn. zm.

Ustawa zasadnicza z dnia 2 kwietnia 1997 r. Dz. U. 1997 Nr 78, poz. 483 z późn. zm.

Wojciechowska-Filipek S., Ciekanowski Z., *Bezpieczeństwo funkcjonowania w cyberprzestrzeni jednostki organizacji państwa*, Wyd. CeDeWu.pl, Warszawa 2016.

Wprowadzenie do zagadnienia bezpieczeństwa systemów informatycznych, http://wazniak.mimuw.edu.pl/index.php?title=Bezpiecze%C5%84stwo_system%C3%B3w_komputerowych_-_wyk%C5%82ad_1%3AWprowadzenie_do_problematyki_bezpiecze%C5%84stwa_system%C3%B3w_komputerowych#Zagro.C5.BCenia_bezpiecze.C5.84stwa [dostęp 12.08.2022].

Wrzesień M., Olejnik Ł., Ryszawa P., *IDS/IPS: Systemy wykrywania i zapobiegania włamaniom do sieci komputerowych*, „Pomiary Automatyka Robotyka" 2012, nr 7.

Wybrane problemy zarządzania bezpieczeństwem informacji, red. J. Brdulak, P. Sobczak, Oficyna Wydawnicza Szkoły Głównej Handlowej w Warszawie, Warszawa 2014.

Zaczek J. M.*, Ewolucja zagrożeń sieciowych motorem ewolucji sieciowych systemów bezpieczeństwa*, „Czasopismo techniczne. Nauki podstawowe" 2012, nr 109.

Streszczenie

Przy wyborze informatycznych systemów finansowo - księgowych bezpieczeństwo ich funkcjonowania jest jednym z najważniejszych elementów, na które powinno się zwrócić uwagę. Dołożenie odpowiednich starań przy wyborze wyżej wymienionego systemu może usprawnić pracę firmy oraz zapobiec możliwości ponoszenia ewentualnych strat danych lub strat finansowych. Wielopoziomowa struktura systemu bezpieczeństwa jest w stanie ograniczyć ryzyko utraty, nieupoważnionej edycji lub nadpisania, a nawet wykradzenia danych.

Głównym celem publikacji jest analiza bezpieczeństwa informatycznych systemów finansowo-księgowych. Szczególną uwagę należy zwrócić na wiarygodność takiego oprogramowania oraz skuteczność w ochronie danych i poufnych informacji przedsiębiorstwa.

SECURITY OF IT FINANCIAL AND ACCOUNTING SYSTEMS

Summary

When choosing IT financial and accounting systems, the security of their operation is one of the most important elements that should be paid attention to. Applying appropriate efforts when choosing the above-mentioned system may improve the company's work and prevent the possibility of incurring possible data losses or financial losses. The multi-level structure of the security system is able to reduce the risk of loss, unauthorized editing or overwriting, or even theft of data.

The main purpose of the publication is to analyze the security of IT financial and accounting systems. Particular attention should be paid to the reliability of such software and the effectiveness in protecting company data and confidential information.