Łukasz Siemieniuk, Adam Gardocki*, Nina Siemieniuk**

WYBRANE ASPEKTY BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH W FINANSACH I RACHUNKOWOŚCI

Wprowadzenie

Współcześni menedżerowe zmuszeni są do szybkiego przesyłania informacji, kontrolowania decyzji finansowych i efektywnego zarządzania firmą. W związku z tymi aspektami niezbędne jest posiadanie odpowiedniego systemu informatycznego, który zaspokoi wszystkie oczekiwania. System informatyczny musi również zapewniać poczucie bezpieczeństwa, które jest jednym z kluczowych aspektów funkcjonowania przedsiębiorstwa. Przy wyborze systemu finansowo-księgowego bezpieczeństwo jego funkcjonowania jest jednym z najważniejszych elementów, na które powinno się zwracać uwagę. Wielopoziomowa struktura systemu bezpieczeństwa jest w stanie ograniczyć ryzyko utraty, nieupoważnionej edycji lub nadpisania, a nawet utraty danych. Szybkiemu rozwojowi technologii informacyjnych towarzyszy coraz większe zagrożenie bezpieczeństwa, wynikające ze wzrastającej złożoności systemów informatycznych. W konsekwencji występuje trudność objęcia wszystkich danych ochroną – niezbędny jest również nadzór nad bezpieczeństwem w systemach finansowo-księgowych. Skomplikowana struktura systemów finansowo-księgowych oraz trudność w zapewnieniu ich bezpieczeństwa to jedne z największych problemów współczesnych przedsiębiorców.

Głównym celem publikacji jest omówienie głównych aspektów bezpieczeństwa systemów finansowo-księgowych. Szczególną uwagę w publikacji zwrócono na wiarygodność takiego oprogramowania oraz skuteczność w ochronie danych i poufnych informacji przedsiębiorstwa.

* *Uniwersytet w Białymstoku, Wydział Ekonomii i Zarządzania, Katedra Finansów, Rachunkowości i Informatyki.*

Bezpieczeństwo systemów informatycznych jako element strategii przedsiębiorstwa

Istota bezpieczeństwa systemów informatycznych

Bezpieczeństwo systemów informatycznych wraz z rozwijającą się technologią informacyjną wymaga coraz większego udziału przedsiębiorstw w zapewnianiu ochrony na tej płaszczyźnie[1].

Pod pojęciem bezpieczeństwa informacji rozumie się[2]:

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

Ważnym elementem strategii przedsiębiorstwa jest kwestia bezpieczeństwa informacji, za którą – na poziomie operacyjnym oraz podczas wdrożenia odpowiednich procedur i zabezpieczeń – powinno odpowiadać kierownictwo. Musi ono być świadome, że polityka bezpieczeństwa to zarówno ochrona danych firmy, zgodność z przepisami, jak i poufności i dostępności informacji w obszarach istotnych z punktu widzenia rentowności prowadzonego biznesu. Badania pokazują, że kadra zarządzająca przedkłada oszczędności ponad bezpieczeństwo informacji, przez co budżet przeznaczony na bezpieczeństwo w obszarze IT jest niewielki[3].

Według Ernst & Young najpoważniejszym problemem w zakresie bezpieczeństwa informacji jest brak wystarczającej liczby odpowiednio wykwalifikowanych pracowników zdolnych realizować działania w tym zakresie. Przedsiębiorcy niechętnie inwestują w zabezpieczenia, twierdząc że nie zostanie to docenione przez klientów oraz komfort użytkowania spadnie. Jedynym rozwiązaniem jest wprowadzenie nowych technologii, które podniosą wygodę użytkowania. Jednak wdrożenie ich w większości firm jest odkładane ze względu na zmniejszający się budżet przeznaczony na bezpieczeństwo informacji. Organizacja odniesie sukces tylko wtedy, gdy zrozumie, że ochrona informacji może przynieść wymierne korzyści przede wszystkim poprzez zapewnienie jej konkurencyjności[4].

---

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

[2] Ibidem, s. 43.

[3] 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.

[4] D. Książek, *Bezpieczeństwo informacji jako element strategii firmy,* (w:) *Wybrane problemy ...*, op. cit., s. 25-27.

Zastanawiając się nad bezpieczeństwem w sieci, należy zwrócić uwagę na model wdrażania chmury. W przypadku gdy używamy prywatnej chmury istniejące zabezpieczenia powinny być wystarczające, jednak gdy mamy do czynienia z chmurą publiczną istotną czynnością będzie zabezpieczenie połączenia z dostawcą i pamiętanie o następujących czynnościach[5]:

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

W przypadku zabezpieczenia 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 gdy używamy wirtualnej infrastruktury istnieją dwa poziomy, na których może wystąpić zagrożenie[6]:

- Poziom systemu operacyjnego, w 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. Tę platformę należy zabezpieczyć, ponieważ pozwala ona na szybkie tworzenie i usuwanie instalacji systemu operacyjnego.

Zagrożenia bezpieczeństwa systemów informatycznych w finansach i rachunkowości

W świecie realnym, jak i w rzeczywistości wirtualnej, występuje wiele zagrożeń; przy tej drugiej spotykamy niebezpieczeństwa wewnętrzne i zewnętrzne. Niebezpieczeństwo zewnętrzne, czyli ataki hakerów na dane przechowywane na komputerze, telefonie, tablecie, są w dzisiejszych czasach codziennością. Najczęściej jednak ofiarami ataków 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. Aby zapo-

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

biegać atakom hakerów, najważniejsze jest dążenie do wcześniejszej ochrony systemu, która uniemożliwi uzyskanie informacji osobom z zewnątrz.

Powyższe zagrożenie powstaje w wyniku bezpośredniego lub pośredniego ataku na informację przetwarzaną przez system lub usługę informatyczną, na przykład uszkodzenie, ujawnienie, modyfikację informacji lub jej dostępności[7]. Największym zagrożeniem dla bezpieczeństwa teleinformatycznego jest przede wszystkim utrata: poufności, integralności, autentyczności i niezawodności informacji oraz usług[8].

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.

Jednym z największych zagrożeń bezpieczeństwa wewnętrznego jest człowiek. Wiele się słyszy o utracie danych, włamaniu do systemu czy też ujawnieniu poufnych danych lub haseł. Coraz częściej w przedsiębiorstwach stosuje się politykę bezpieczeństwa, tak aby uniknąć zagrożenia. Mimo ludzkiej świadomości, nie zawsze człowiek stosuje się do danych zasad. Korzystając z przeglądarki internetowej, jesteśmy narażeni na ściągnięcie nieświadomie wirusa lub zostanie ofiarą ataku hackerskiego. Kolejnym przykładem zagrożenia bezpieczeństwa jest ujawnianie poufnych danych[9].

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[10]. 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 za uprawnionego użytkownika, lub w sposób pośredni, czyli atakuje system, wykorzystując wirusy lub konie trojańskie.

---

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

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

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

[10] M. Kopczewski, E. Czapik-Kowalewska, *Zagrożenia sieciowe a bezpieczeństwo informacyjne,* (w:) *Modele Inżynierii Teleinformatyki* Nr 6, (red.) A. Czajkowska, Wydawnictwo Uczelniane Politechniki Koszalińskiej, Koszalin 2011, s. 58.

Zabezpieczenia dotyczące systemów informatycznych wykorzystywanych w finansach i rachunkowości

Kontrole dostępu logicznego

Nowoczesne systemy informatyczne kompleksowo wspomagające procesy finansowo-księgowe, są ważnym narzędziem potrzebnym do sprawnego funkcjonowania przedsiębiorstwa. Firmy mogą prawidłowo funkcjonować wtedy i tylko wtedy, gdy ich informatyczne systemy finansowo-księgowe, z których korzystają, są bezpieczne[11]. Jako że omawiane systemy przechowują wrażliwe dane przedsiębiorstw, sposoby zabezpieczania znajdujących się w nich informacji musiały zostać uregulowane za pomocą przepisów prawnych. W Polsce kwestie zabezpieczeń systemów finansowo-księgowych reguluje przede wszystkim ustawa o rachunkowości[12]. Jako że omawiane systemy mogą także przechowywać i przetwarzać dane osobowe, sposoby ich zabezpieczenia podlegają również regulacjom zawartym w ustawie o ochronie danych osobowych z dnia 24 maja 2018 r., która w związku z wprowadzeniem rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych zastąpiła dotychczas obowiązujące przepisy[13].

Obecnie systemy ochrony danych nie ograniczają się jedynie do programów antywirusowych, a integrują się np. z przeglądarkami internetowymi, pocztą elektroniczną. Ważne jest, aby każdy system kontroli opierał się na przynajmniej dwóch warstwach ochronnych wdrożonych przy użyciu technologii odrębnych producentów. Powinna ona być podzielona na dwie części. Pierwszą jest kontrola wykonana przez serwer antywirusowy, druga natomiast przy użyciu skanera wykonującego kontrolę online[14]. Jednym z ważniejszym sposobów kontrolowania (zwłaszcza wśród firm zajmujących się rachunkowością) jest kontrola logicznego dostępu opierająca się na: powstrzymywaniu nieuprawnionych osób przed dostępem, a udzielanie dostępu jedynie uprawnionym w jak najwęższym możliwym stopniu i kontrolowaniu czynności przez nich wykonywanych. Aby odpowiednio realizować zabezpieczenia dostępu logicznego, jednostki gospodarcze powinny stosować: systemy zabezpieczeń programowo-sprzętowych, zabezpieczeń w systemie operacyjnym, zabezpieczeń

[11] 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.

[12] Ustawa o rachunkowości z dnia 29 września 1994 r. (tekst jedn. Dz.U. 2018 r., poz. 395).

[13] Ustawa o ochronie danych osobowych z dnia 24 maja 2018 r. (tekst jedn. Dz. U. 2018 r., poz. 1000).

[14] T. Muliński, *Zagrożenia bezpieczeństwa dla systemów…,* op. cit., s. 172.

aplikacyjnych oraz sieciowych. 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[15].

Zabezpieczenia sieci informatycznych

Zabezpieczenie sieci informatycznych jest ważnym aspektem zapewnienia bezpieczeństwa danych w systemach finansowo-księgowych. 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[16]. 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. Jest ona 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 zagrożonych usług Intranetu[17].

Równolegle z rozwojem informatycznych systemów finansowo-księgowych 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.[18] Jest to urządzenie, które składa się ze scalonych funkcji zapory sieciowej i innych systemów zabezpieczających.

---

[15] G. Michalczuk, Ł. Siemieniuk, *Problematyka bezpieczeństwa…,* op. cit., (w:) *Finansowe i pozafinansowe aspekty funkcjonowania podmiotów gospodarczych,* red. N. Siemieniuk, G. Michalczuk, E. Tokajuk, Wyd. Uniwersytetu w Białymstoku, Białystok 2014, s. 174-175.

[16] *Rodzaje i klasyfikacja włamań oraz ataków internetowych*, http://hackme.pl/articles.html?article_id=247 (dostęp 11.11.2017).

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

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

IPS jest to jeden z sposobów zabezpieczania sieci komputerowych zarówno przed atakami z zewnątrz, jak i wewnątrz. IPS służy do wykrywania ataków na systemy komputerowe oraz uniemożliwiania powodzenie takich ataków. IPS to połączenie podstawowych funkcji zapory sieciowej z funkcjami programów antywłamaniowych. Główną różnicą miedzy IPS a innymi formami zabezpieczeń jest nieustanne monitorowanie danych w sieci komputerowej firmy w celu wyszukiwania kodów, które mogłyby uszkodzić lub uniemożliwić korzystanie z sieci teleinformatycznej – bezpieczeństwo zewnętrzne. Kolejną ważną funkcją jest możliwość monitorowania i kontrolowania jakie ruchy są dokonywane przez wszystkie osoby, które są podłączone do sieci komputerowej – bezpieczeństwo wewnętrzne[19].

Kryptografia jako system szyfrowania danych

Kryptografia jest to dziedzina informatyki zajmująca się utajaniem danych przed niepożądanym dostępem poprzez szyfrowanie. Można ją stosować na wielu płaszczyznach, m.in. uwierzytelniania w systemach operacyjnych oraz aplikacjach, szyfrowania i uwierzytelniania transmisji bezprzewodowej. Na bezpieczeństwo współczesnych systemów kryptograficznych mają wpływ dwa czynniki[20]:

- długość klucza, która jest podstawą każdego systemu,
- moc kryptograficzna algorytmu – algorytm mocny to taki, który można poznać jedynie przy wypróbowaniu wszystkich możliwych kluczy.

W kryptografii wyróżnia się dwie kategorie szyfrowania: przestawieniowe i podstawieniowe. Metoda przestawieniowa polega na przypisaniu poszczególnym znakom używanym w treści komunikatu innych znaków z używanego zbioru. Szyfrowanie podstawieniowe zaś oznacza łączenie w pary poszczególnych znaków z innymi używanymi w komunikacie[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. W kryptografii symetrycznej występuje problem, który polega na bez-

[19] M. Wrzesień, Ł. Olejnik, P. Ryszawa, *IDS/IPS: Systemy wykrywania i zapobiegania włamaniom do sieci komputerowych*, (w:) *Przemysłowy Instytut Automatyki i Pomiarów PIAP w Warszawie*, „Pomiary Automatyka Robotyka" 2012, nr 7, s. 16-21.

[20] K. Rytelewska, T. Siemieniuk, *Problematyka zabezpieczenia…,* op. cit., (w:) *Systemy informatyczne …,* op. cit., s. 83.

[21] T. Muliński, *Zagrożenia bezpieczeństwa…,* op. cit., s. 176-177.

piecznym przekazaniu klucza między jednostkami. Nie należy to przekazywać poprzez kanał elektroniczny, gdyż mógłby on zostać przechwycony i wykorzystany przez niepożądane osoby. Za główne zalety tego rodzaju kryptografii można uznać to, iż algorytmy oparte na kluczach symetrycznych umożliwiają szybkie szyfrowanie danych, a same klucze są relatywnie krótkie. Niestety posiada ona również wady, m.in. 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 oraz IDEA[22].

W kryptografii asymetrycznej używa się klucza publicznego oraz prywatnego, który jest utajniony. Klucz publiczny może być powszechnie dostępny, przekazywany niezabezpieczonymi kanałami. Szyfrowanie przesyłki odbywa się za pomocą klucza publicznego, jednak wiadomość nie może być nim odszyfrowana. Niezbędne jest tutaj zastosowanie klucza prywatnego. Zaletą takiego systemu jest to, że liczba kluczy asymetrycznych oraz częstość ich wymieniania jest niższa niż w przypadku kluczy symetrycznych. Natomiast do wad można zaliczyć 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[23].

Podpis elektroniczny wykorzystuje szyfrowanie asymetryczne oraz jednokierunkową funkcję skrótu. Ma on postać kilkunastu bajtów i potwierdza integralność przesyłki oraz autorstwo wiadomości[24].

Podsumowanie

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. Systemy informatyczne wykorzystywane w większości przedsiębiorstw, zapewniają ciągłość pracy w każdej branży, ponadto ułatwiają procesy związane z obsługą finansów i rachunko-

[22] K. Rytelewska, T. Siemieniuk, *Problematyka zabezpieczenia …,* op. cit., (w:) *Systemy informatyczne …,* op. cit., s. 85-86.
[23] Ibidem, s. 86-87.
[24] Ibidem, s. 88.

wości 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.

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.

Kopczewski M., Czapik-Kowalewska E., *Zagrożenia sieciowe a bezpieczeństwo informacyjne*, (w:) *Modele Inżynierii Teleinformatyki* Nr 6, red. A. Czajkowska, Wydawnictwo Uczelniane Politechniki Koszalińskiej, 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.

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.

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

Wrzesień M., Olejnik Ł., Ryszawa P., *IDS/IPS: Systemy wykrywania i zapobiegania włamaniom do sieci komputerowych,* (w:) *Przemysłowy Instytut Automatyki i Pomiarów PIAP w Warszawie*, „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.

Ustawa o ochronie danych osobowych z dnia 24 maja 2018 r. (tekst jedn. Dz.U. z 2018 r., poz. 1000).

Ustawa o rachunkowości z dnia 29 września 1994 r. (tekst jedn. Dz.U. z 2018 r., poz. 395).

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_bezpieczeństwa_system%C3%B3w_komputerowych#Zagro.C5.BCenia_bezpiecze.C5.84stwa (dostęp 12.11.2017)

Rodzaje i klasyfikacja włamań oraz ataków internetowych, http://hackme.pl/articles.html?article_id=247 (dostęp 11.11.2017)

Streszczenie

Systemy informatyczne mają powszechne zastosowanie w przedsiębiorstwach, w szczególności w sferze finansów i rachunkowości. W związku z przechowywaniem i przetwarzaniem newralgicznych – z punktu widzenia strategii przedsiębiorstwa – danych, systemy te powinny być zabezpieczone w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym. Wewnętrzne i zewnętrzne zagrożenia systemów informatycznych wykorzystywanych w finansach i rachunkowości mogą być eliminowane poprzez zastosowanie zróżnicowanych metod zabezpieczeń, tj. kontrole dostępu, zabezpieczenia sieci czy kryptografii, jako metody szyfrowania danych. Stosowanie wspomnianych metod ochrony systemów rachunkowych jest kwestią indywidualną podmiotów gospodarczych, jednakże posiadanie luk w zabezpieczeniach powoduje większą podatność jednostek na ataki konkurencji, przez co przedsiębiorstwa mogą utracić swoją zdolność konkurencyjną na rynku. Głównym celem publikacji jest omówienie głównych aspektów bezpieczeństwa systemów finansowo-księgowych. Szczególną uwagę w publikacji zwrócono na wiarygodność takiego oprogramowania oraz skuteczność w ochronie danych i poufnych informacji przedsiębiorstwa.

SELECTED ASPECTS OF IT SYSTEMS SECURITY IN FINANCE AND ACCOUNTING

Summary

IT systems are widely used in enterprises, particularly in finance and accounting spheres. Due to the storage and processing of sensitive data in terms of the company's strategy, these systems should be secured in a way that prevents access to unauthorized persons. Internal and external threats to IT systems used in finance and accounting can be eliminated by using varied security methods, i.e. access controls, network security or cryptography as data encryption method. The use of such accounting systems protection methods is an individual matter of enterprises, however, having security holes results in greater susceptibility of individuals to competition attacks, which means that companies may lose their competitive ability on the market. The main purpose of the publication is to discuss the main aspects of the security of financial and accounting systems. Particular attention was paid to the reliability of such software and the effectiveness in data protection and company confidential information.