BEZPIECZEŃSTWO INFORMACJI, PROBLEMY KSZTAŁCENIA KADR

Serghei OHRIMENCO*

*Chief of the Laboratory of Information Security of the Academy of Economic Studies of Moldova

Streszczenie: W artykule poddano analizie niektóre aspekty bezpieczeństwa systemów informatycznych zgromadzone w trakcie kształcenia studentów w Mołdawskiej Akademii Ekonomicznej w zakresie ochrony informacji.

Słowa kluczowe: bezpieczeństwo informacyjne, systemy informatyczne, edukacja.

1. WPROWADZENIE

Rozwój informatycznych technologii komunikacyjnych radykalnie zmienia nasze codzienne życie, obecnie stał się on dominującym czynnikiem rozwoju społeczeństwa XXI wieku. Nowe technologie pozwalają na gromadzenie, przetwarzanie i przechowywanie ogromnej ilości różnorodnej informacji (naukowej, technicznej, medycznej i in.). Oczywiście taka sytuacja wymaga budowania systemów bezpieczeństwa informatycznego: przy czym bezbronność systemów nie jest skutkiem technicznych czy też technologicznych niedoskonałości a jest konsekwencją błędów przy korzystaniu z tych technologii. Oznacza to, że procedury bezpieczeństwa winny integrować nie tylko w technologiczne operacje, ale też w funkcjonowanie systemów informatycznych [1,4]. Obecnie waga problemów związanych z bezpieczeństwem systemów informatycznych nabrała dużego znaczenia zarówno w skali państwa, społeczeństwa jak i każdego człowieka. W większości państw bezpieczeństwo informacyjne rozpatruje się jako składową bezpieczeństwa narodowego na równi z takimi dziedzinami jak energetyka, zaopatrzenie w żywność itp., a więc wymaga się zapewnienia bezpieczeństwa systemów techniczno-produkcyjnych i społeczno-ekonomicznych o ogólno-społecznym przeznaczeniu. W związku z powyższym, na uwagę zasługuje problem przygotowania odpowiedniej kadry fachowców dla potrzeb bezpieczeństwa informatycznego. Ponadto, ciągle odczuwana jest potrzeba ustawicznego kształcenia kadr ze względu na fakt, że teoria i praktyka ochrony zasobów informacyjnych jest nieustannie doskonalona i rozwija się. W kształceniu kadr można wyróżnić dwa podstawowe poziomy: akademicki (wyższy: licencjat, magister, doktor) i specjalistyczny (kursy wiodących firm wyspecjalizowanych w technologiach informacyjnych) [2].

Pierwszy poziom oferuje studia w zakresie różnorodnych dyscyplin wiedzy, zakłada przyswojenie osiągnięć naukowo-technicznych i w rezultacie kształci specjalistę o wysokim poziomie wiedzy teoretycznej i praktycznej.

Drugi poziom proponuje przyswojenie niezbędnej wiedzy oraz jej uzupełnianie, aby sprostać wymaganiom rozwijających się technologii informacyjnych i odpowiednim standardom [5]. Przykładem może tu być system certyfikacji specjalistów ISACA, od CISA

(*Certified Information Systems Auditor*) do CISM (*Certified Information Security Manager*). Wymienione powyżej poziomy przygotowania nie są wzajemnie sprzeczne. Aktualnym zadaniem jest ich konwergencja tj. powiązanie przygotowania fundamentalnego i nowych osiągnięć w praktyce na bazie współdziałania.

Na wstępie należy określić pojęcie „bezpieczeństwa informacyjnego" (BI). W literaturze spotyka się i wykorzystuje różne określenia BI. Często termin bezpieczeństwo informacyjne rozpatruje się jak część składową ogólnego pojęcia systemu informatycznego (SI). Stosowane jest ono zamiennie z takimi pojęciami jak „bezpieczeństwo komputerowe" „bezpieczeństwo sieciowe, telekomunikacyjne, bezpieczeństwo danych, itd. Wydaje się, że, kategoria „BI" jest najbardziej ogólna, ponieważ obejmuje wszystkie procesy technologiczne od pozyskania, poprzez transmisję, przetwarzanie, do przechowywania informacji w SI. Taka treść pojęciowa wynika z określenia BI – jest to kompleks przedsięwzięć zapewniający bezpieczeństwo środowiska *informacyjnego*, a także jego formowanie, wykorzystywanie i rozwój w interesie obywateli, organizacji i państwa. [4].

Ogólnie BI obejmuje trzy składowe: ludzie, technologie i procesy, które są obiektem badań oraz oceny.

2. CELE I ZADANIA KSZTAŁCENIA

Podstawowym celem kształcenia w zakresie BI jest przekazywanie na bieżąco regulacji prawnych, organizacyjnych, technicznych, programów i innych i środków ochrony informacji. Na czoło wysuwają się tu następujące podstawowe zadania [3]:

- kształtowanie współczesnego podejścia do BI jak do systematycznej działalności praktyczno-naukowej, która nosi praktyczny charakter,
- formułowanie podstaw teoretycznych, fundamentalnych dla zarządzania SI i zasoba-mi, a także BI,
- przekazywanie wiedzy o współczesnych metodach i środkach ochrony informacji,
- nauka obsługi oraz korzystania z popularnych produktów i usług informatycznych w zakresie BI.

W rezultacie kształcenia student powinien:

- poznać podstawy prawne ochrony informacji, umieć posługiwać się metodami organizacyjnymi, technicznymi i informatycznymi ochrony informacji we współczesnych sieciach komputerowych oraz SI, a także standardami i modelami bezpieczeństwa, metodami identyfikacji użytkowników, metodami ochrony zasobów przed włamaniem, infrastrukturą systemów zbudowanych z wykorzystaniem dostępnych i utajnionych kluczy,
- posiąść umiejętność stosowania w praktyce nabytej wiedzy o metodach i środkach BI, dokonywać analiz porównawczych, wyboru odpowiednich środków i metod, ocenienia poziomu ochrony zasobów informacyjnych,

– ukształtować swoje wyobrażenie o podstawowych tendencjach i perspektywach rozwojowych metod i środków BI.

W odniesieniu do etapów cyklu życia systemów informatycznych, które obejmują projektowanie, konstruowanie, próby eksploatacyjne, specjalista winien umieć rozwiązywać następujące zadania:

– w ramach procesu projektowania systemu informatycznego i systemu ochrony zasobów informacyjnych przeprowadzić badanie obiektu zarządzania w celu określenia konieczności wykorzystywania specjalnych środków ochrony; wyspecyfikować potencjalne zagrożenia, oszacować i prognozować wielkości wskaźników bezpieczeństwa zasobów informacyjnych, uzasadnić poziom koniecznej ochrony i sposobów zabezpieczenia, dokonać wyboru środków wystarczających dla wypełnienia zadania ochrony zasobów, opracować rozwiązania projektowe systemów bezpieczeństwa informacji dla zarządzanego obiektu oraz rekomendacje dla ich realizacji, zaprojektować schematy technologiczne funkcjonowania obiektu i systemu informacyjnego, w zastosowaniu dla różnych reżimów pracy obiektu i systemu informacyjnego, opracować propozycje dla praktycznej realizacji projektu systemu BI,
– w ramach procesu realizacji projektu: opracować specyfikację środków ochrony, dokonywać zamówień, sprawdzania i instalacji, a także przeprowadzania odbioru i prób; nauczać i instruować użytkowników o właściwościach funkcjonowania środków ochrony informacji, zasad zachowania się personelu,
– w ramach procesu funkcjonowania: organizować monitoring funkcjonowania systemu BI; opracowywać i realizować scenariusze działania w nietypowych sytuacjach; gromadzić i przetwarzać statystycznie informację o funkcjonowaniu systemu BI; opracowywać rekomendacje dla doskonalenia funkcjonowania systemu informacyjnego i systemu bezpieczeństwa informacji, a także ich realizacji.

Dodatkowym celem przygotowania specjalistów jest formowanie podejścia kompleksowego. Obejmuje ono wszystkie poziomy działań dla zapewnienia bezpieczeństwa informacji a także wszystkie etapy cyklu życia systemu informacyjnego.

2. TREŚCI PROGRAMOWE KURSU

Program może obejmować następujące zagadnienia:

– prawne aspekty bezpieczeństwa informacyjnego,
– organizacja systemu bezpieczeństwa informacji,
– analiza zagrożeń i ocena ryzyka,
– standardy i sposoby oceny bezpieczeństwa informacji,
– opracowanie dokumentacji ochrony informacji.

2.1. OCHRONA PRAWNA BEZPIECZEŃSTWA INFORMACYJNEGO

Prawne uwarunkowania określają i wyznaczają relacje występujące przy gromadzeniu, przekazie, przetwarzaniu, przechowywaniu, aktualizacji, zakupie i sprzedaży informacji,

powstałych w procesie tworzenia, wdrożenia i eksploatacji systemów informacyjnych i innych systemów przetwarzania i przekazu informacji.

W pierwszej kolejności należy poddać analizie międzynarodowe ustawodawstwo międzynarodowe i krajowe. Regulujące wzajemne relacje w obszarze systemów informacyjnych i komunikacyjnych

2.2. ORGANIZACJA SYSTEMU OCHRONY INFORMACJI

Analizując podstawy budowy i funkcjonowania systemu ochrony informacji szczególny nacisk należałoby położyć na następujące zagadnienia:

1) polityka – zespół konstytutywnych reguł (zasad formalnych), wyznaczających funkcjonowanie mechanizmów ochrony informacji,
2) identyfikacja – umiejscowienie każdego z uczestników współdziałania informacyjnego,
3) autentyfikacja – zagwarantowanie, że uczestnik procesu wymiany informacji będzie zawsze identyfikowalny,
4) kontrola dostępu – ustanowienie zbioru reguł, które każdemu uczestnikowi procesu wymiany informacji reglamentują dostęp do zasobów,
5) autoryzacja – dobór uprawnień dla wybranego uczestnika wymiany informacji,
6) audyt i monitoring – przegląd przebiegu zdarzeń, które wystąpiły w procesie wymiany informacji (audyt dotyczy zdarzeń zaszłych, monitoring czasu rzeczywistego),
7) reagowanie na zdarzenia – zestaw procedur lub przedsięwzięć, które należy wdrożyć w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa informacji,
8) sterowanie konfiguracją – skonfigurowanie i utrzymywanie roboczego stanu pracy środowiska wymiany informacji zgodnie z wymaganiami bezpieczeństwa informacyjnego
9) zarządzanie użytkownikami – zapewnienie odpowiednich warunków pracy użytkownikom w środowisku wymiany informacji zgodnie z wymaganiami ochrony informacji,
10) zarządzanie ryzykiem – określenie relacji pomiędzy możliwymi stratami a przypadkami naruszenia bezpieczeństwa,
11) zapewnienie stabilności – utrzymanie dopuszczalnego środowiska wymiany informacji w minimalnym dopuszczalnym zakresie pracy,

2.3. ANALIZA ZAGROŻEŃ

Analiza zagrożeń ma znaczenie podstawowe. Powinna ona obejmować klasyfikację zagrożeń bezpieczeństwa informacji, a także umożliwić wyodrębnienie czynników przewidywalnych i losowych z uwzględnieniem ich charakteru i skutków, celów, miejsce powstawania, obiekt oddziaływania, i inne. Wydaje się, że główną uwagę należy zwrócić na zagrożenia przewidywalne. Całe spektrum zagrożeń należałoby rozpatrywać przez pryzmat wrażliwości technicznej i softwarowej pod kątem identyfikacji ryzyk i ich

sterowaniem, stworzenia możliwości modelowania sytuacji awaryjnych oraz przygotowania i wdrażania odpowiednich decyzji. Analizę ryzyka prowadzi się na modelu z uwzględnieniem możliwych zakłóceń działania a także potencjalnych strat.

2.4. NORMY I MIARY BEZPIECZEŃSTWA INFORMACYJNEGO

Kształcenie w tym zakresie obejmuje przekaz wiadomości o normach międzynarodowych, krajowych, przemysłowych i specyfikacjach w obszarze BI. Główną uwagę zwraca się na normy międzynarodowe ISO/IEC 15408-1999 ”Evaluation Criteria for IT Security” i związane z nimi technologie ISO/IEC 18045, ISO/IEC 17799 (poprzednia norma BS 7799-2:2002), ISO/IEC 21827, ISO 7498-2, BSI; COBIT, SAC, COSO, SAS 78/94 a także inne standardy zapewniające ocenę poziomu bezpieczeństwa informacyjnego.

Tematyka kształcenia w tym obszarze dotyczy:

- określenia celów ochrony informacji SI,
- budowy efektywnego systemu zarządzania bezpieczeństwem informacyjnym,
- określenia wielkości wskaźników (jakościowych i ilościowych) zapewniających realizację wyspecyfikowanych celów,
- wyboru narzędzi ochrony informacji oraz bieżącej oceny ochrony,
- wykorzystywania metodyk zarządzania BI poprzez odpowiednio dobrany system norm i miar, który zapewni ochronę informacji, a także pozwoli obiektywnie oceniać bezpieczeństwo informacji i zarządzać ochroną informacji.

Kolejność postępowania reguluje międzynarodowa norma ISO/IEC17799, BSI, COBIT, która uwzględnia następującą problematykę:

- działania organizacyjne dotyczące ochrony informacji,
- klasyfikacja i zarządzanie zasobami,
- bezpieczeństwo personelu,
- bezpieczeństwo fizyczne,
- zarządzanie komunikacją i procesami,
- kontrola dostępu,
- opracowanie i utrzymanie systemów obliczeniowych,
- polityka bezpieczeństwa,
- zarządzanie ciągłością biznesu,
- zgodność systemu z wymaganiami.

2.5. OPRACOWANIE DOKUMENTACJI ORGANIZACYJNEJ OCHRONY INFORMACJI

Jest to etap końcowy kształcenia, w którym integruje się nabytą wiedzę teoretyczną i praktyczną, omówioną poprzednio. Początkowym zadaniem jest opracowanie koncepcji zapewnienia BI konkretnego SI, w którym są przedstawione ogólne zasady i podejścia

zabezpieczenia informacji i zasobów informacyjnych. Zawartość tego dokumentu stanowią podstawę dla zbudowania pełnego systemu BI.

Przygotowanie materiałów metodologicznych obejmuje sformułowanie odpowiednich ograniczeń, wskazówek i instrukcji niezbędnych dla użytkowników obiektu. Do nich należą również zasady korzystania z urządzeń i technologii informatycznych, oprogramowania, sformułowania hasła użytkownika, scenariuszy zachowań w sytuacjach kryzysowych, itd.

Opracowanie projektów systemów BI przewiduje określenie celów i zadań ochrony informacji, identyfikację zagrożeń a także środków przeciwdziałania, ocenę ryzyka i potencjalnych strat. Projekt winien uwzględniać również aspekty efektywności ekonomicznej systemu ochrony informacji, odzwierciedlać relację „efektywność-wartość" zespołu przedsięwzięć w postaci wskaźników ilościowych i jakościowych względnych i bezwzględnych. Należą do nich takie jak liczba rozpoznawalnych zagrożeń, jakość przeciwdziałania zagrożeniom, koszty przywrócenia stanu normalnego po wystąpieniu zagrożenia, współczynnik zmniejszenia potencjalnych strat.

Przygotowanie zarządzeń dla oddziałów, odpowiadających za realizację planu organizacyjno – technicznego przedsięwzięć ukierunkowanych na kompleksowe zapewnienie bezpieczeństwa zarządzanego obiektu z wyodrębnieniem zadań i funkcji, odpowiedzialności personalnej oceny efektywności prac związanych z ochroną informacji zasobów

3. WNIOSKI

Podsumowując można stwierdzić, że przy kształceniu kadr w zakresie BI należy przyjąć następujące zasady podstawowe:

- zakres wiedzy teoretycznej powinien uwzględniać międzynarodowe standardy i odpowiadać wymaganiom dnia dzisiejszego,
- kształcenie należy ukierunkować na zdobycie wiedzy teoretycznej i praktycznej, pozwalającej na zapobieganie sytuacjom kryzysowym występującym w procesie funkcjonowania systemów informatycznych.

4. LITERATURA

[1] *Компьютерная преступность и информационная безопасность*.- Мн.: АРИЛ,, 2000

[2] Охрименко С., Саркисян А.: *Подготовка на магистри по новата специалност* «Информационна безопасност». Информационно осигуряване на бизнеса. Юбилейна Международна научна конференция. – Свищов, Стопанска Академия «Д.А.Ценов, 2006

[3] Разумов О.С., Благодатских В.А.: *Системные знания: концепция, методология, практика*. Финансы и статистика, Москва, 2006

[4] Черней Г.А., Охрименко С.А., Ляху Ф.С.: *Безопасность автоматизированных информационных систем*. Ruxanda, Кишинев 1996

[5] Council C.: *Implication for the Future of CobiT Systems in Higher Education: Putting Critical Research and Theory Into Practice*. Information Systems Control. Vol. 1, 2007

[6] ISO/IEC FDIS 27001. Information technology-Security techniques-Information security management systems-Requirements. 2005-05-14