YAPAY ZEKA TEMELLİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ YAKLAŞIMI

Cemal GEMCİ, Ömer Faruk BAY
Gazi Üniversitesi, Bilişim Enstitüsü
cgemci@gmail.com, omerbay@gazi.edu.tr

ABSTRACT

In this study an expert system solution created based on the ISO/IEC 27001 standard adopted particularly in Europe in the field of information security management systems. Knowledge base is composed according ISO/IEC 27001 standard and relevant standards. The expert system solution will evaluate the responses given by business owners or employees who have little knowledge of information technology. Proposed software solution in this study will alleviate the need for Small and Medium Size Enterprises (SMEs), which already experience a shortage of qualified employees, to employ staff or obtain consulting services at high costs.

Key words: Information security, Information Security Management System (ISMS), Risk Management, Artificial Intelligence, Expert Systems.

1. GİRİŞ

Bilgi önceki zamanlarda söylendiği gibi güç olmaktan çıkmış günümüzde bir varlık halini almıştır. Bilgi ve destek süreçleri, sistemler ve bilgisayar ağları artık önemli ticari varlıklardır. Günümüzde bilginin gizliliği, güvenilirliği ve elverişliliği; rekabet gücünü, nakit akışını, karlılığı, yasal yükümlülükleri ve ticari imajı korumak ve sürdürmek için zorunlu ve gereklidir.

CSI Survey 2007 [1] ye göre ABD de KOBİ ler bilgi güvenliğine büyük yatırımlar yapmış olmalarına rağmen sanal yollardan yılda ortalama 345.000 USD para kaybına uğramaktadırlar. Türkiye de henüz böyle bir gözlem çalışması yapılmamış olduğundan KOBİ lerin sanal kayıpları hakkında bilgi sahibi olunamamaktadır. Detayları ilerleyen paragraflarda verilecek olan KoçNet raporundan [2] da görüleceği üzere Türkiye de KOBİ lerin büyük bilişim güvenliği açıkları bulunmaktadır. Amerika ile Türkiye nin ekonomik büyüklükleri de göz önüne alındığında Türkiye de KOBİ lerin kayıpları hakkında bir fikir edinilebilir.

Bir ekonominin gerçek dinamosu olarak bilinen KOBİ lerin, Türkiye de bilgisayar kullanımlarına ilişkin KOSGEB veya başka bir devlet kuruluşu tarafından yapılmış bir çalışma bulunmamaktadır. Bu konuda yapılan en ciddi çalışma Microsoft Türkiye tarafından yaptırılan KOBİ araştırmasıdır [3]. Ocak 2003 sonunda tamamlan araştırma, 728 şirketin yöneticileriyle yüzyüze yapılan görüşmeler ile gerçekleştirilmiştir. Araştırmadan elde edilen bulguların önemli olanları aşağıda özetlenmiştir:

- Bilgisayar kullanan çalışan sayısı geçtiğimiz 3 yıl içinde % 58'den % 66'ya yükselmiştir.
- Internet kullanım oranı % 72'den % 80'e yükselmiştir.
- Web sitesi olan KOBİ oranı 1999 yılında % 37, 2000 yılında % 40, 2002 yılında ise % 53'e yükselmiştir.
- KOBİ'lerin % 53'ü işletmelerinde yerel ağ (LAN) kullanmaktadır. Yerel alan ağında sunucu kullanan işletme oranı % 47'den % 59'a yükselmiş bulunmaktadır.

Elde edilen sonuçları kısaca yorumlamak gerekirse PC penetrasyonu hala daha arzu edilen düzeyde değildir. KOBİ'lerde kullanılan yazılımlar ağırlıklı olarak kelime işlemciler ve muhasebe programları gibi temel yazılımlardır. KOBİ'lerin Internet'i vazgeçilmez bir unsur olarak görüp, şirket stratejileri arasında öncelikli bir yer vermediklerini web sitesi olan ve e-ticaret yapan şirket sayısının hala daha son derece az olmasından anlamak mümkündür.

Türkiye'de KOBİ'lerin kurumsal güvenliği durumunu ortaya koyan tek çalışma Koç.net'in Ağustos-Eylül 2003 tarihleri arasında yaptığı ücretsiz güvenlik denetimi kampanyası sonrasında yayınladığı rapordur [2].

Denetimi yapılan şirketlerle ilgili olarak aşağıdaki önemli bulgulara ulaşılmıştır:

- % 87'si farklı düzeylerde güvenlik riski taşımaktadır.
- % 56'sının web sunucu bilgileri kolaylıkla çalınabilir, ana sayfaları değiştirilebilir veya bir başka adrese yönlendirilebilir.
- % 28'inin güvenlik duvarları konfigurasyonu kötü olduğu için by-pass edilerek her türlü bilgiye erişilebilir.

Bu iki araştırmanın sonucundan da açıkca anlaşılacağı üzere Türkiye de KOBİ'lerin bilişim konusunda istekli ancak çok fazla bilinçli olmadıkları, bununla birlikte KOBİ'lerin bilişim teknolojilerine yatırım yapma konusunda çok isteksiz oldukları gözlemlenmektedir.

KOBİ lere bilgi güvenliği açısından bakıldığında birçoğunda hiç bir güvenlik tedbirinin alınmadığı gözlemlenmektedir. Oysaki Avrupa birliğine girme sürecinde olan Türkiye de sanayinin lokomotifi sayılan KOBİ'lerde bu bilgi güvenliği bilincin yerleşmesi Avrupa da ki emsalleriyle rekabet edebilme ve ürünlerini güvenli bir sanal ortamda tüm dünyaya pazarlayabilme olanağına kavuşturacaktır.

Ülkemizde Ocak 2008 tarihinde yürürlüğe giren olan BASEL-II uygulamasıyla bankalar kurumsallaşmış firmalara daha düşük faizle kredi vereceklerdir, henüz tam kurumsallaşmamış firmaların kredi maliyetleri ise daha yüksek olacaktır. Diğer taraftan KOBİ'lerin teknolojik düzeylerinin genellikle düşük olması, teknik ve ticari gelişmeleri izleyememeleri ve nitelikli eleman sıkıntısı çekmeleri, teknik seviyesi yüksek olan Basel-II sebebiyle insan kaynağına ve bilgi işlem alt yapı unsurlarına önemli düzeyde yatırım yapmaları kaçınılmazdır.

Bu çalışmada; bilgi teknolojilerine çok fazla harcama yapma arzusunda olmayan, yüksek maliyetlerinden dolayı kalifiye eleman bulunduramayan, çok az bilişim bilgisine sahip tecrübesiz eleman bulunduran Türk KOBİ 'lerine yönelik yapay zeka temelli bir bilgi güvenlik yönetim sistemi yapısı amaçlanmıştır.

Hedeflenen uzman sistem tamamlandığında KOBİ' lerin kendi kendilerine Bilgi Güvenliği Yönetim Sistemi (BGYS) oluşturmalarını ve idame etmelerine olanak sağlayacak ve KOBİ leri yüksek kalifiye eleman ve danışmanlık hizmet bedellerinden tasarruf etmelerini sağlayacaktır.

Bu çalışmanın birinci bölümünde önerilen çözümün gereksinimleri vurgulanmış, ikinci bölümünde bilgi güvenliği yönetim sistemi literatür taraması özetlenmiştir. Üçüncü bölümde metodlar ve yöntem anlatılmış, dördüncü bölümde önerilen sistemin detayları açıklanmış ve sonuç bölümünde ise elde önerilen çözümün getirdikleri tartışılmıştır.

2. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

1970 lerin başında ABD'de Department of Defense (Savunma Bakanlığı) Rand Report R-609 olarak da bilinen "Bilgisayar Sistemleri için Güvenlik Kontrolleri" başlıklı bir rapor yayınladı. Birçok bakımdan bu rapor bilgi güvenliğinin ilk tohumları sayılmaktadır.

Bilgi güvenliğini sağlamak, teknolojik çözümlerle birlikte sağlam bir güvenlik yönetim sisteminin kurulması ile mümkün olabileceğinin anlaşılmasıyla birlikte tüm dünyada farklı gruplar tarafından çalışmalar başlamıştır. Avrupa da 1990'lı yılların sonunda bir grup İngiliz bilişim güvenliği uzmanı tarafından küçük, orta ve büyük firmalar tarafından benimsenip kullanabilecekleri ISO/IEC 17799:2000 Bilgi Güvenliği Yönetim adıyla bir standart hazırlandı. BS 7799 Parti 2:2002 Bilgi Güvenliği Yönetim Sistemi Özellikleri (Specification for information security management systems) British Standard Institude (BSI) veya akredite belgelendirme kuruluşları tarafından BS 7799 adıyla belgelendirmeye esas bir standart halini almıştır. 15 Ekim 2005 tarihinde ISO/IEC 27001:2005 [4] Bilgi Güvenliği Yönetim Sistemi (Information security management systems) standardı uluslararası bir standart olarak yayınlandı. Bilgi Güvenliği Yönetim Sistemi konusunda yayınlanmış olan bu standart yayım tarihinden itibaren, BS 7799-2:2002'nin yerini almıştır.

Türk Standartlar Enstitüsü TS 13268-1, Bilgi Güvenliği Yönetim Sistemi Belgelendirmesi İçin Gereksinimler ve Hazırlık Klavuzu [5] hazırlayarak yayımlamıştır.

Ayrıca ISO/IEC 27001 standardın da, ISO_IEC_TR_13335-3:1998, Techniques for the Management of IT Security [6] ve ISO_IEC_TR_13335-4:2000, Selection of Sefaguards [7] ISO Teknik raporlarına atıfta bulunulmuştur. İngiliz Standart enstitüsü BSI tarafından ISO/IEC 17799 standardını açıklama maksadıyla; PD 3001- Preparing for BS 7799-2 Certification [8], PD 3002- Guide to BS 7799 Risk Assesment [9], PD 3003-Are you ready for a BS 7799-2 audit?[10], PD 3004-Guide to the implementation and auditing of BS 7799 controls [11], PD 3005-Guide on the selection of BS 7799-2 controls [12] dokümanları hazırlanmıştır.

Qingxiong Ma ile J. Michael Pearson 'un birlikte, ISO 17799 standardının 354 bilgi güvenliği uzmanının katılımıyla yaptıkları geçerlilik çalışmasının sonuçlarını açıkladıkları makalede [13] organizasyonlar için bilgiyi varlıklarını korumak için birçok standart ve yol haritası önerildiğini bunların arasında ISO 17799 en güvenilir uluslararası bilgi güvenliği standardı olduğunu belirtmişlerdir. Standardın bilgi güvenliğini sağlamak için hem emredici olduğunu hemde

organizasyona adapte edilecek prosedürlerin olduğunu ifade etmişlerdir.

Bilgi Güvenliği Yönetim Sistemi tüm yönetim sisteminin ticari risk yaklaşımı, gerçekleştirme, işletme, gözlemleme, idame ettirme ve geliştirmeye dayalı bir parçasıdır. Yönetim sistemi organizasyon, kuruluş yapısı, politikalar, planlanan faaliyetler, sorumluluklar, prosedürler ve kaynakları kapsar. Bilgi güvenliğinin kapsamı, organizasyonun ve organizasyondaki bilgi kaynaklarının büyüklüğüne bağlıdır. Bilgi güvenliği organizasyonun işletme ve iş kültürünün tümleşik bir parçası olmalıdır. Bilgi güvenliği teknik bir konu olmaktan ziyade temelde yönetimin konusudur. Bilgi güvenliği bir kez yapılacak bir iş olmayıp süreklilik gerektirmektedir. Günümüzde bilgi güvenliğini ihmal ederek faaliyetini sürdüren başarılı hiçbir organizasyon bulunmamaktadır.

3. UZMAN SİSTEMLER

"Bilgi Çağı" ve "Bilgi Toplumu" gibi terimlerin sıklıkla kullanıldığı günümüzde bilginin önemi daha açık bir şekilde ortaya çıkmaktadır. Bilginin önemi arttığı oranda o bilgiye ulaşabilmeyi sağlayan sistemlerin de önemi artmaktadır. Birçok organizasyon bilgiyi toplamak, organize etmek ve dağıtmak için bilgisayar destekli bilgi sistemlerini kullanmaktadır. Yönetim bilimleri tabiriyle işletmelerde "Yönetim Bilgi sistemi" kullanımı yaygınlaşmaktadır. Bunun yanı sıra işletmeler "Uzman Sistem" gibi farklı yönetim bilimi tekniklerini kullanmaktadırlar.

Turban [14] uzman sistemleri şu şekilde tanımlamıştır; "Uzman sistem uzmanlığı gerektiren problemleri çözmek için bilgisayar tarafından depolanan insan bilgisini kullanan bir sistemdir. Bu sistemler hem uzman olmayanlar tarafından problemlerin çözümü için kullanılır, hem de uzmanlar tarafından bilgili yardımcılar olarak kullanılır." Uzman Sistemlerin birçok farklı alandaki zor seviyede sayılabilecek problemleri başarılı bir şekilde çözüme kavuşturması, dikkat çekmelerindeki en önemli unsuru oluşturmuştur.
Uzman Sistemler, temelde uzman bir insan düzeyinde problem çözmede, insan bilgisini yoğun biçimde kullanan programlardır. İyi tasarlanmış sistemler belirli problemlerin çözümünde uzman insanların düşünme işlemlerini taklit ederler. Amaç uzman bir insan gibi veya ondan daha iyi bir Uzman Sistem geliştirebilmektir. Böyle bir sisteme sahip olmak kişiyi uzman yapmaz, fakat bir uzmanın yapacağı işin bir kısmını veya tamamını yapmasını sağlar. Uzman Sistemi oluşturan birimler ve işlevleri özetlenirse;

Bilgi tabanı: İlgili alana özel tecrübeye dayalı bilginin saklandığı veri tabanıdır. Kural ve Olgulardan meydana gelir. Olgular; nesneler arasındaki ilişki, sınırlama ve açıklamalardan oluşur. Kurallar ise; problem alanı ile ilgili kavramlar arasındaki mantıksal ilişkileri tanımlar.

Çıkarım mekanizması: Kuralları ve olguları okuyarak ne demek istediklerini anlar ve muhakeme fonksiyonunu icra eder.

Açıklama ünitesi: Muhakemenin nasıl yapıldığını açıklar. Ayrıca kullanıcı ile iletişim anında bazı sorular sorar ve kullanıcı da neden bu soruyu sorduğunu bilmek isterse açıklama ünitesi gerekli açıklamayı yapar.

Kullanıcı arabirimi: Kullanıcı ile sistem arasındaki iletişimi sağlar. Geneldee, Neden ve Nasıl sorularına cevap veren bir açıklama ünitesini içerir [15].

Çıkarım mekanizmasının yapılanması problem alanının özelliklerine, bilgi gösterim ve düzenleme biçimine bağlıdır. Kural esaslı sistemlerin çıkarım mekanizmasında çözüme ulaşmak için izlenen yol bakımından birbirinden ayrılan iki ana çıkarım algoritması vardır [16].

İleri zincirleme (forward-chaining) ; Tüme varım yaklaşımının uygulanmasıdır. Veri yöneliktir (data-driven) Kullanıcıdan alınan bilgilere kurallar sırasıyla uygulanarak sonuç bulunmaya çalışılır. Kullanıcı ile uzman sistem arasında problem çözümünün sonuna kadar bir etkileşim vardır. Bu etkileşim bilgi tabanındaki kural zinciri içerisinde gerçekleşir.

Geri zincirleme (backward-chaining) ; Tümden gelim yaklaşımının uygulanmasıdır. Diğer bir değişle sonuca yöneliktir (goal-driven). Sonuç bellidir sebep bulunmaya çalışılır. İşlem, verilen sonuç bulununcaya veya uygulanacak kural kalmayıncaya kadar devam eder.

Uzman sistem yazılımı geliştirilirken herhangi bir proglamlama dili yerine, uzman sistem kabuk programı kullanılması zaman ve iş gücünden önemli bir tasarruf sağlar [17].

4. UZMAN SİSTEM TABANLI BİLGİ GÜVENLİK YÖNETİM SİSTEMİ YAKLAŞIMI

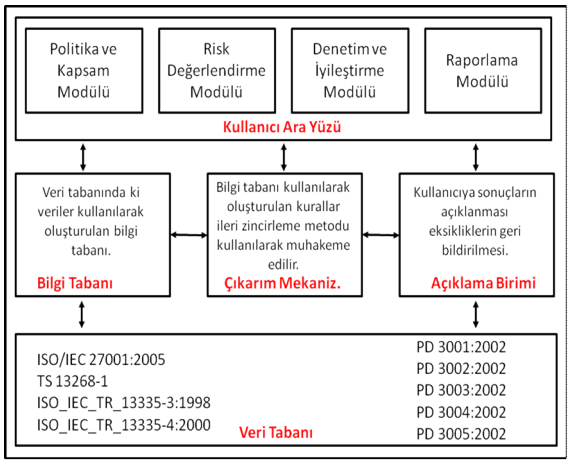
Bu çalışmada Türkiye de bilgi teknolojileri kullanımının gün geçtikçe arttığı ve bu konuda bilgi sahibi personelin çok az sayıda istihdam edildiği KOBİ lere yönelik bilgi güvenliği yönetim sisteminin kurulması ve sürdürülmesine ilişkin

yapay zeka temelli bir çözüm önerilmektedir. Çözüm olarak günümüz bilişim teknolojileri gereksinimlerine uygun ve sağlıklı bir bilgi güvenliği yönetim sistemi yaklaşımı sunan ISO/IEC 27001 standardı esas alınıp, uzman sistem geliştirme yöntemleri kullanılarak bir sistem geliştirilebilir.

Uygulamanın kullanıcısı olan KOBİ'lerin bilgisayar kullanım bilgisi seviyesi göz önüne alınarak visual bir platformda geliştirilmesi uygun olur. Bu nedenle uzman sistem kabuk programı seçilirken C, C++, Java uygulama geliştirme platformlarını destekleyen JESS, CLIPS, ACQUIRE vb. gibi bir kabuk seçilmelidir.

ISO/IEC 27001 standardına uygun BGYS kurulurken ilgili stantardlar kullanılarak bilgi tabanı ve bu bilgi tabanı kullanılarak kurallar oluşturulur. İleri zincirleme yöntemi kullanılarak, kullanıcı arayüzü yardımıyla oluşturulan kural tabanından koşullar kullanıcıya iletilir ve yanıtları alınarak sonuca ulaşılır. Kullanıcı istediğinde açıklama birimi yardımıyla sonuca nasıl ulaşıldığına dair açıklamaları alabilir.

Geliştirilen sistem ISO/IEC 27001 ve TS 13268-1 dokümanlarında belirtilen BGYS nin belgelendirilebilmesi için gereken koşulları sağlamalıdır. Önerilen sistemin mimari yapısı şekil-2 de gösterilmektedir.



Şekil 1. Uzman Sistem tabanlı BGYS yaklaşımı

Politika ve kapsam modulü: Bilgi güvenliği politikası ve BGYS kapsamının belirlenmesini kolaylaştıran modüldür. Kuruluşun bilgi güvenliği politikasında ifade edilmesi gereken hususlar Guidance requirements for certification dokümanında açıklanmıştır.

Risk Değerlendirme Modülü: Bilgi varlık envanterinin çıkartıldığı, varlıkların gizlilik, güvenilirlik ve erişilebilirlik değerlerine göre varlık değerlemesinin yapıldığı, varlıkların zafiyet ve tehditlerin tespit edildiği ve varlıkların korumalarının belirlendiği modüldür.
Varlık envanterinin nasıl çıkartılacağı ve bilgi varlıklarının değerlendirilmesinin nasıl yapılacağı Guide to BS 7799 Risk Assesment, ISO/IEC TR 13335-3 dokümanlarında ayrıntılı bir şekilde anlatılmıştır. ISO/IEC TR 13335-4 dokümanında ise varlıklara korumaların nasıl uygulanacağı anlatılmaktadır. Bu dokümanlardan yararlanılarak risk değerlendirme bilgi tabanı oluşturulur.

Denetim ve iyileştirme modülü: Bilgi güvenliği süreçlerinin etkin planlaması, işletilmesi ve kontrolü için prosedürler hazırlanır. ISO/IEC 27001 'in EK-A sında da hazırlanacak 10 başlık altında 133 adet kontrol maddesi verilmiştir. Bu kontrol maddelerinin organizasyon içerisinde nasıl uygulancağını açıklayan en az 10 prosedür ve bu prosedürlere uygun formlar, talimatlar hazırlanmalıdır. ISO/IEC 27001 'in EK-A sında belirtilen 133 kontrol maddesi kullanılarak bilgi tabanı oluşturulur.

Raporlama Modülü : BGYS faaliyetlerinin etkin işletilmesi ve gereksinimlere uygunluğun kanıtı olan kayıtların dokümante edilmesi modülüdür. Bu kayıtlar BGYS belgelendirmesinde istenmektedir.

Tüm sistemin kurallarının açıklanması bu makale boyutlarını aşacağından burada örnek iki kural tabanı gösterilmiştir.

Bilgi güvenliği politikası kontrol kural tabanı aşağıdaki gibi oluşturulabilir.

KURAL:1
IF
Organizasyonun bilgi varlıkları olası tehditlere karşı korunuyormudur **IS** TRUE
AND
Genel müdür onaylamışmıdır **IS** TRUE
AND
Bilginin gizliliği garanti edilmişmidir **IS** TRUE **AND**
Bilginin bütünlüğü sağlanmışmıdır **IS** TRUE
AND
Bilginin bulundurulabilirliği işin gereklerine göre sağlanmışmıdır **IS** TRUE
AND
Yasal yükümlülükler yerine getirilmişmidir **IS** TRUE
AND
İş sürekliliği planı güncelmidir **IS** TRUE
AND
Tüm personele bilgi güvenliği eğitimi verilmişmidir **IS** TRUE
AND
Bilgi güvenliği açıkları bilgi güvenliği yöneticisine bildirilimi **IS** TRUE

THEN
Bilgi güvenliği politikası uygundur.

Risk değerlendime kural tabanı aşağıdaki gibi olabilir;

KURAL:2
IF
Organizasyonun bilgi varlıkları envanteri çıkarılmışmıdır **IS** TRUE
AND
Bilgi varlıklarının risk değerlendirmesi yapılmışmıdır **IS** TRUE
AND
Bilgi varlıklarına tehditlere karşı kontroller uygulanarak risk seviyesi azaltılmışmıdır **IS** TRUE
AND
Yönetim kabul edilebilir risk seviyesini belirlemişmidir **IS** TRUE
AND
Uygulanabilirlik beyannamesi hazırlanmışmıdır **IS** TRUE
THEN
Risk değerlendirmesi uygundur.

Uzman sistemlerin en önemli özelliklerinden birisi olan açıklama birimi bu uygulamada organizasyonun kural tabanına verdiği yanıtları değerlendirerek eksiklikleri ve yapılması gerekenleri açıklığa kavuşturacaktır.

5. SONUÇLAR

Yapay zeka temelli bilgi güvenliği yönetim sistemi, ekonominin temel direkleri olarak nitelendirilen KOBİ lerin nitelikli eleman istihdamı ya da yüksek maliyetli danışmanlık hizmeti almaksızın, çok az bilişim teknolojisi bilgisiyle, ISO/IEC 27001 standardına uygun bilgi güvenliği yönetim sistemini oluşturup idame etmelerine olanak sağlayacaktır.

Bu çalışmada önerilen çözüm sayesinde KOBİ yöneticisi veya çalışanı, firması için ISO/IEC 27001 ye uygun bilgi güvenliği yönetim sisteminin oluşturulmasını uzman sistem yardımıyla kolayca gerçekleştirebilecektir.

Firmanın iş ve üretim süreçlerine uygun olarak BGYS gereksinimleri bir uzman sistem yardımıyla belirlenecek, firma yöneticileri bu gereksinimlerin bir kısmını kendileri yerine getirebilecek bir kısmında ise gerekli malzemenin tedariki yapılarak yerine getirilebilecektir. Bu da KOBİ lere büyük ekonomik kazançlar sağlayacaktır.

Önerilen BGYS'nin yazılım geliştirme aşaması devam etmektedir.

KAYNAKLAR

[1.] CSI, Computer Crime and Security Survey 2007, http://i.cmpnet.com/v2.gocsi.com/pdf/ CSISurvey2007.pdf, 13 Şubat 2008

[2.] KOÇ.NET Güvenlik Raporu, http://doctus.org/koc-net-guvenlik-raporu-24-t890. html,13 Şubat 2008

[3.] Microsoft KOBİ araştırması 2003 http://www.ilkeratalay.com/resources/kobiler2003.php, 13 Şubat 2008

[4.] ISO Standard, ISO/IEC 27001:2005, Information Security Management Systems.

[5.] Türk Standardı, TS 13268-1, Bilgi Güvenliği Yönetim Sistemi Belgelendirmesi İçin Gereksinimler ve Hazırlık Klavuzu.

[6.] ISO Technical Report, ISO_IEC_TR_ 13335-3:1998, Techniques for the Management of IT Security.

[7.] ISO Technical Report, ISO_IEC_TR_ 13335-4:2000, Selection of Sefaguards

[8.] BSI Preparing for BS 7799-2 Certification PD 3001:2002

[9.] BSI Guide to BS 7799 Risk Assesment PD 3002:2002

[10.] BSI Are you ready for a BS 7799- 2 audit? PD 3003:2002

[11.] BSI Guide to the implementation and auditing of BS 7799 controls, PD 3004:2002

[12.] BSI Guide on the selection of BS 7799-2 controls, PD 3005:2002

[13.] Qingxiong Ma Missouri State Universitesi ile J. Michael Pearson Southern Illinois Universitesi "Communications of the Association for Information Systems (Volume 15, 2005) 577-591"

[14.] Turban, E., Artificial intelligence, California State University, 1992.

[15.] Winstanley, G., Artificial Intelligence in Engineering, New York, 1991

[16.] Hotomaroğlu A.T. Bilgisayar destekli öğretim için uzman sistem tabanlı bir kabuk programın geliştirilmesi ve etkinliğinin değerlendirilmesi, Doktora tezi, Gazi Üniversitesi, 2002

[17.] Salim MD, Villavicencio A., & Timmerman Marc A. A Method for Evaluating Expert System Shells for Classroom Instruction, Journal of Industrial Technology, Volume 19, 2002.