HAKEMLİ Denetişim
Ortak Aklın Harmanı
Kamu İç Denetçileri Derneği Meşrutiyet Caddesi Konur Sokak No: 36/6 Kızılay - ANKARA
www.kidder.org.tr/denetisim/ • denetisim@kidder.org.tr
ISSN 1308-8335
Yıl: 15, Sayı: 2024 Ek Sayı, 144-155, 2024

Konferans Bildirisi

KURUMSAL BİLGİ GÜVENLİĞİ YÖNETİMİNDE YAPAY ZEKÂ DESTEKLİ RİSK ANALİZİ

(ARTIFICIAL INTELLIGENCE SUPPORTED RISK ANALYSIS IN INSTITUTIONAL INFORMATION SECURITY MANAGEMENT)

Mustafa COŞAR[1]

ÖZ

Yaşamın giderek dijitalleştiği bilgi çağında, bilginin değeri ve önemi her geçen gün artmaktadır. Bilginin değerini ve önemini artırmanın esas yolu; onun gizliliği, güvenliği ve bütünlüğü unsurlarını korumaktan geçmektedir. Bu unsurların tümü pek çok bileşenin ve faktörün bir arada olduğu, sürekli ve çok yönlü etkileşimde bulundukları bir sistemi oluşturmaktadır. Bu sistemin yapısı gereği pek çok riski de beraberinde getirmektedir. Bu risklerin önceden belirlenmesi, hesaplanması ve analiz edilmesinde iyi bir risk yönetim anlayışına ihtiyaç vardır. Bilişim teknolojileri bu yönetim anlayışına destek olmak için pek çok yeni yöntem ve teknik ortaya koymaktadır. Yapay zekâ yöntem ve teknikleri buna örnek olarak verilebilir. Bilgi güvenliğini sağlama aşamasında ortaya çıkan açıkların, eksiklerin ve risklerin yapay zekâ ile önceden belirlenerek önlemlerin alınmasında önemli roller üstlendiği görülmektedir. Özellikle veri toplama, işleme ve karar verme süreçlerini kapsayan veri analitiği ile tahmin etme ve karar vermeyi kolaylaştırmaktadır. Ayrıca, veri iletimi ve erişimi sırasında oluşan anormal durumların tespitinde makine öğrenimi ve doğal dil işleme algoritmaları önemli başarılar elde etmektedir. Bu çalışma, kurumsal bilgi güvenliği yönetiminde yapay zekâ destekli risk analizine değinmektedir. Bu kapsamda kullanılan yapay zekâ uygulamalarının özellikleri açıklanırken, yapay zekâ destekli örnek bir risk analizi modelini oluşturulmuştur. Bu model içerisinde yapay zekâ yöntem, teknik ve araçları belirtilmiştir. Ayrıca, yapay zekânın, bilgi güvenliği alanında risk analizi süreçlerine entegrasyonu ve potansiyel faydaları üzerinde durulmaktadır. Çalışmada, önerilen modelde yer alan yapay zekâ tekniklerinin ve modellerinin risk analizi aşamalarına uygunluğu araştırılırken uygulama temelli ilişkilendirmeler yapılmıştır. Çalışmanın diğer bir amacı ise, geleneksel risk analizi yöntemlerine kıyasla yeni nesil bilişim teknolojileri desteğiyle oluşturulan yöntemlere yönelik farkındalığın artırılmasıdır.

Anahtar Kelimeler: Bilgi güvenliği, Bilgi güvenliği yönetimi, Yapay zekâ, Risk analizi

JEL Kodları: C80, D83, M10, O32

ABSTRACT

In the digital age where life is becoming increasingly digitalized, the value and importance of information are growing each day. The main way to enhance the value and importance of information is to preserve its elements of confidentiality, security, and integrity. These elements collectively form a system in which numerous components and factors interact continuously and in a multifaceted manner. Due to the structure of this system, it also brings along many risks. In order to identify, calculate, and analyse these risks beforehand, a strong understanding of risk management is required. Information technologies introduce various new methods and techniques to support this management approach. For example, artificial intelligence methods and techniques can be cited in this context. It is observed that artificial intelligence plays significant roles in pre-determining vulnerabilities, gaps, and risks emerging during the process of ensuring information security, enabling proactive measures to be taken. Particularly, data analytics encompassing data collection, processing, decision-making processes facilitate prediction and decision-making, while machine learning and natural language processing algorithms achieve notable successes in detecting abnormal situations during data transmission and access. This study delves into AI-supported risk analysis in corporate information security management. The characteristics of AI applications used within this scope are explained, and an AI-supported sample risk analysis model is developed. This model specifies AI methods, techniques, and tools. Furthermore, the integration of AI into risk analysis processes and its potential benefits in information security are emphasized. The study investigates the compatibility of AI techniques and models with

[1] Doktor Öğretim Üyesi, Hitit Üniversitesi, 0000-0001-6482-4592, mustafacosar@hitit.edu.tr

risk analysis stages in the proposed model, and application-based correlations are made. Another aim of the study is to enhance awareness about methods created with the support of next-generation IT technologies as compared to traditional risk analysis methods.

Keywords: *Information security, Information security management, Artificial intelligence, Risk analysis*

JEL Classification: *C80, D83, M10, O32*

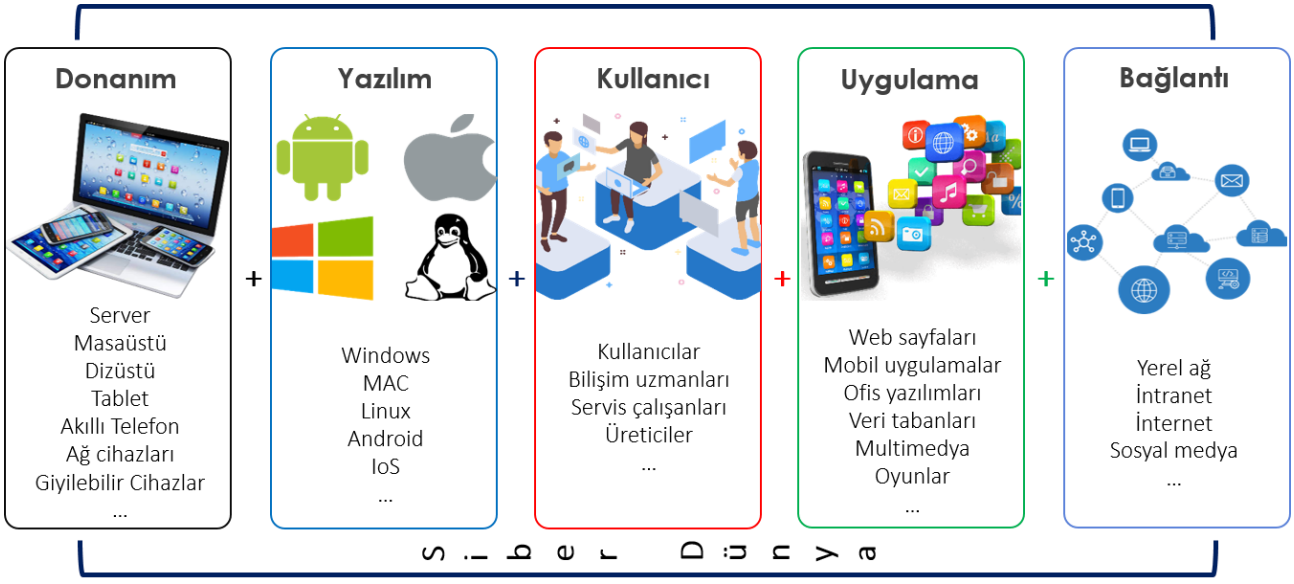
1. GİRİŞ

Son yıllarda, günlük yaşamın içerisindeki iş ve işlemlerin artan bir oranda dijitalleştiği görülmektedir. Dijitalleşme yaşam koşullarını hızlandırırken süreçlerin kolay ve verimli bir şekilde yürütülmesini sağlamaktadır. Ayrıca, kullanıcıların dijital sistemlere yer ve zaman bağımsız olarak daha özgürce erişimini sağlamaktadır. Buna karşın, artan oranda teknoloji okuryazarlığı düzeyine, ek maliyetlere ve güvenlik farkındalığına ihtiyaç duyulmaktadır.

Dijital sistemlerin kullanımı ve yaygınlaşması sonucunda hızlı, yüksek kapasiteli ve çok yönlü veri ve bilgi akışı olmaktadır. Bu da kişisel ve kurumsal kapsamda bilgi yönetimi ve bilgi güvenliği yönetimi unsurlarını ortaya çıkarmaktadır. Özellikle son zamanlarda karşılaşılan bilgi güvenliği zafiyetlerinin maddi ve manevi kayıplara yol açması, bu konunun daha karmaşık bir hal almasına ve daha fazla önem kazanmasına neden olmaktadır. Bu karmaşa teknolojik gelişmelerin hızlanması, kullanıcı sayısının artması ve uygulamaların çeşitlenmesiyle birlikte, bilgi güvenliği risklerinin sayısını ve karmaşıklığını da artırmaktadır. Bu karmaşanın çözümü aşamasında, geleneksel risk analizi yöntemlerinin yetersiz kaldığı ve yapay zekâ gibi yeni nesil potansiyel teknolojilerden bir çözüm arandığı görülmektedir.

Bilgi çağı insanlar ve dijital varlıklarla donatılmış siber bir dünya kavramını ortaya çıkarmıştır. Şekil 1'de bileşenleri resmedilen bu siber dünya, insanların ve sistemlerin birbirine bağlandığı, çok yönlü etkileşimlerin kurulduğu, sürekli veri üretilerek paylaşıldığı sınırsız bir dünya haline gelmiştir. Hatta bu dünyanın kendine has bir dili, kültürü ve yazılı olmayan yasaları oluşmaktadır. Bu dünyanın içerisinde yer alanlara yönelik sunduğu avantajların yanı sıra dezavantajları da ortaya çıkmaktadır.

Şekil 1. Siber Dünyayı Oluşturan Bileşenler



(Coşar, 2022a)

Bilgi güvenliği, bilginin yetkisiz erişimi, değiştirilmesi veya yok edilmesine yönelik olarak ortaya çıkabilen tehdit ve risklere karşı korunmasını kapsamaktadır. Bu amaçla koruma sürecine çeşitli teknolojiler, politikalar ve prosedürler eklenmektedir. Bilgi güvenliğinin benimsenmesi ve uygulanması pek çok boyutta ele alınmaktadır. Şekil 1'de özetlenmeye çalışılan bileşenlerin her biri için farklı boyutları ele almak gerekmektedir. Bu boyutların ilki kullanıcı boyutudur. Kullanıcıların bilgisi, alışkanlıkları, farkındalık düzeyleri ve sürece katılım oranları bilgi güvenliğinin temelini oluşturmaktadır

İkinci boyutu ise teknoloji boyutudur. Bu boyut bilişim teknolojilerinin donanım ve yazılım sistemlerini kapsamaktadır. Özellikle son yıllarda artan oranda kullanıma sahip olan mobil teknolojiler bu boyutun önemli bir parçasını oluşturmaktadır. Bu boyutun kullanıcılar boyutu ile doğrudan ilişkisi bilgi güvenliğini daha dikkatli bir şekilde ele almayı gerektirmektedir.

Bilişim teknolojilerinin yazılım ve donanım sistemlerinin günlük hayatı kolaylaştırmasının yanında elde edilen bilgilerin toplanması, sınıflandırılması, analiz edilmesi ve karar verme sürecinde kullanımını geliştirmektedir. Bu açıdan bakıldığında, veri derleme, değerlendirme ve analizi için çeşitli matematiksel ve istatistiksel yöntemler ve algoritmalar yardımıyla çıkarımda bulunma ortaya çıkmıştır.

Bu teknolojilere örnek olarak internet üzerinde arama motorları, son kullanıcıya dönük sohbet robot (chatbots) sistemleri, Internet of Things (IoT) sensörleri ile donatılmış akıllı ev aletleri, otonom araçlar ve son günlerde sıkça duyulan ChatGPT gibi kelime ve konu temelli yardımcı akıllı sistemler örnek gösterilebilir (Coşar, 2023a).

Bilgi güvenliği yönetimi süreçlerinde insan merkezli sistemlere ek olarak iyi birer veri analitiği ve öğrenme becerilerinin sonucunda doğruluğu yüksek tahmin geliştirme yeteneğine sahip yapay zekâ sistemlerinin yer alması mümkündür. Ancak, sistemin az ve düşük özellikteki mevcut verilerle yanlış çıkarımlarda bulunabileceği ya da ezber yaparak farklı durumlar için aynı sonuçları üretebileceği unutulmamalıdır.

Bu çalışma, kurumsal bilgi güvenliği yönetiminde yapay zekâ destekli risk analizinin modellemesini ve yürütülmesini incelemektedir. Yapay zekânın, bilgi güvenliği alanında risk analizi süreçlerine entegrasyonu ve potansiyel faydaları üzerinde durmaktadır. Entegrasyon sürecinde hangi yapay zekâ tekniklerinin ve modellerinin risk analizi aşamalarına uygunluğu araştırılırken uygulama temelli ilişkilendirmeler yapılmıştır. Çalışmanın diğer bir amacı ise, geleneksel risk analizi yöntemlerine kıyasla yapay zekâ tabanlı yöntemlerin sağladığı avantajları vurgulamak ve kurumsal bilgi güvenliği yönetimine katkı sağlamaktır. Bu makale giriş bölümünün ardından şu şekilde yapılandırılmıştır. Konunun kapsamını ilgilendiren kavramların ve terimlerin kavramsal çerçevesi ikinci bölümde açıklanmıştır. Üçüncü bölümde, bilgi güvenliği yönetiminde yapay zekâ destekli risk analizi modeli alan yazın desteği ile sunulmuştur. Son olarak, Sonuç ve Öneriler bölümü yer almaktadır.

2. KAVRAMSAL ÇERÇEVE

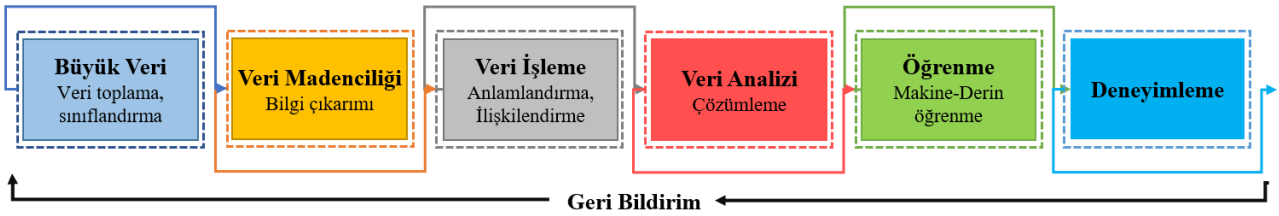
2.1. Yapay Zekâ

Bilişim teknolojilerinin son yıllarda adından en çok bahsedilen konularından birisi yapay zekâdır. Yapay zekâ veri analitiği ile makine öğrenme tekniklerinin bir araya gelerek bir sistemi öğrenen ve karar veren bir sistem haline getirmesidir. Yaşam koşullarının giderek hızlanması ve daha fazla kaynaktan yararlanma isteği insanların yerine düşünen ve kararlar veren sistemlerin varlığını tetiklemektedir. Bu tetikleme yapay zekâya sahip robotik sistemleri ortaya çıkarmaktadır.

Yapay zekânın oluşturulması ve geliştirilmesi için ilk olarak veriler üzerinde bazı işlemlerin yapılması gerekmektedir. Bu işlemler; verilerden büyük bir veri seti oluşturma, veri madenciliği yapma, veri işleme, veri analitiği ile çözümleme yapma ve sistemin öğrenme yöntemiyle yeni durumlara hazır hale gelmesi işlemleridir. Bu işlemlerin ardından veri analitiği algoritmaları, uzman sistemler, makine öğrenme ve derin öğrenme teknikleri, doğal dil işleme, görüntü işleme ve yapay sinir ağları gibi teknolojiler yardımıyla bu sistemin analiz yapmaya ve karar vermeye başlaması gelmektedir.

Yapay zekânın bir süreç olarak değerlendirilmesi sonucunda bazı bileşenlere sahip olduğu görülmektedir. Bu sürecin bilginin elde edilmesi ve tanımlanması ile başladığı, çözüm ve çıkarımda bulunulması ile sürdüğü söylenebilir. Şekil 2'de yapay zekânın bileşenlerinin bir süreç kapsamında değerlendirilerek resmedildiği görülmektedir.

Şekil 2. Yapay Zekâ Bileşenleri



(Coşar, 2023a)

Yapay zekâ terimi, insan zekâsına özgü olan bir dizi yüksek bilişsel fonksiyonları ve otonom davranışları bir bilgisayar sisteminin sergileyebilme yeteneği kazanması olarak tanımlanmaktadır (Yıldız ve Yıldırım, 2018). İnsana özgü olarak düşünülen bu yüksek bilişsel fonksiyonlar ise, ses ve görüntü algılama, nesneleri, olguları ve olayları düşünme, anlamlandırma, analiz etme, çıkarımda bulunma, öğrenme, problem çözme, deneyim kazanma ve karar verme olarak sıralanabilir (Coşar, 2023b).

Standart bilgisayar programları ile tam, doğru veri ve bilgilere dayalı pek çok problemin çözümü mümkündür. Bu tür problemlerde matematiksel ve mantıksal yöntemlerle sonuçlar elde edilebilir. Ancak, sınırlı ve kesin olmayan bilgiler ile bir problemi çözmek için zekâ destekli bazı algoritmalar gerekmektedir. Bu algoritmalar, alternatif sonuçlar içerisinden en uygun olanı ile bir karar verebilir.

Yapay zekâ, insan zekâsına benzer bir gelişim sürdürdüğü için insanın algılamasını ve öğrenmesini sağlayan bileşenlere sahiptir. Bu bileşenlerin başında, veri toplamak için ısı, ışık, ses, mesafe ve görüntü algılamayı sağlayan sensörler gelmektedir. Bunun yanı sıra, yapay zekâya sahip bir sisteme dışarıdan da veri girilebilmesi için depolama ünitelerine sahiptir. Bu bileşenler sayesinde elde ettiği veriler ile ilk kararlarını ve hareketlerini yapabilirler. Kendisinde bulunan ve çevreden elde ettikleri veriler bilgiye dönüşmek üzere temizleme, sınıflandırma, ilişkilendirme ve tanımlama aşamalarından geçerek kullanılmaya hazır hale gelir. Ardından nesneleri ve durumları, anlamlandırma, çözümleme ve öğrenme aşamaları gelmektedir. Bu süreç geçmiş deneyimlerden de beslenerek alternatif çözümler üretebilen sürekli öğrenen bir sistem haline gelebilmektedir.

2.2. Bilgi Güvenliği

Bilgi güvenliğini sağlamak için geleneksel yaklaşımların yanında çeşitli yeni nesil çözüm önerilerine ihtiyaç duyulmaktadır. Bu önerilerden birisi ise verilerin kaydedilmesi ve erişilmesi sürecinde merkezi sistem yerine dağıtık sistem mimarisinin kullanılmasıdır. Özellikle verilere erişim sırasında hız, kapasite ve güvenlik unsurları göz önüne alındığında yapay zekâ teknolojileri ve dağıtık sistemlerde blockchain teknolojisinin ismi tam da burada ön plana çıkmaktadır.

Bilgi güvenliğini sağlamanın temelinde bilginin gizlik düzeyini belirleme, bilginin saklandığı bilişim sistemlerinin güvenliğini sağlama ve bu sistemlere erişimi denetim altına alma ilkeleri gelmektedir. Şekil 3'te bilgi güvenliğini sağlama sürecinde etkili olan adımların bir süreç içerisinde ele alınması resmedilmiştir.

Şekil 3. Bilgi Güvenliğini Sağlama Adımları

(Coşar, 2022b)

Bilgi güveliğini sağlama görevi tüm paydaşları ilgilendiren bir yönetim süreci olduğundan farkındalık ve koordinasyon önemli ilkelerdir. Şekil 3'te yer alan bu adımlar yerinde, zamanında ve doğru bir şekilde yürütüldüğünde koordine edilmiş bir bilgi güvenliği yönetimi ortaya çıkmaktadır. Ayrıca, geçmişe dönük güvenlik ile ilgili olay/eylem arşivinin oluşturulması hafızanın diri tutulması için önemli görülmektedir.

2.3. Bilgi Güvenliği Yönetiminde Risk Analizi

Risk analizi, varlık ya da sisteme yönelik tehdit faktörlerinin belirlenmesini ve bu faktörlere ait risklerin olasılık ve etkilerine göre değerlendirilmesini içeren bir analizdir. Bu analiz süreci, riskin olasılık ve etkisinin belirlenmesi, olasılık ve etkinin boyutlarının hesaplanması, etkiyi azaltmak için önlemler alınması ve bu riskin tekrarlanmaması için deneyim kazanılmasına yardımcı olmaktadır. Tablo 1'de bilişim teknolojileri desteği ile yürütülen risk analizi model ve yöntemleri yer almaktadır.

Tablo 1. Bilişim Teknolojileri Destekli Risk Analizi Modelleri ve Yöntemleri

MODEL	ÖZELLİKLERİ	KAYNAK
TUAR	Riski ifade etmek için hata ağaçları ve bulanık mantık kullanan nicel bir araçtır.	Bilbao, 1992
RAMEX	Matematiksel veya istatistiksel araçlar kullanmayan nitel bir araçtır.	Kailey and Jarratt, 1995
Buddy System	Otomatik risk analizi ve yönetimi sağlayan bir yazılımdır.	Jenkins, 1998
COBRA	Yazılım tarafından desteklenen nitel risk analiz yöntemidir. Türkçe karşılığı; Danışma, Objektif ve İki İşlevli Risk Analizidir.	C&A Systems Security Limited, 2000
SPRINT	Belge tabanlı bir risk analizi yöntemidir.	ISF, 1997
ISO/IEC 15408	Hem nicel hem de nitel risk analiz yöntemidir. Bilgi güvenliği, siber güvenlik ve gizlilik koruması sunan sistem, BT güvenliği için değerlendirme ölçütleri içerir.	ISO/IEC 15408-1, 2022a
ISO/ IEC 27001	Bilgi güvenliği, siber güvenlik ve gizlilik koruması kılavuzudur. Bilgi güvenliği yönetim sistemleri için gereksinimler yer alır.	ISO/IEC 27001, 2022b
NIST 800-30 Special Publication	Bilgi teknolojilerine ilişkin diğer standartlar ve kılavuzlar içeren bir analiz rehberidir.	Stoneburner vd., 2002
CRAMM	Merkezi Bilgisayar ve Telekomünikasyon Ajansı Risk Analizi ve Yönetim. Standartlarla uyumlu nicel, yazılım tabanlı bir risk analiz yöntemidir.	CCTA, 2005
CORA	NIST 800-30 kılavuzuyla uyumlu nicel, yazılım tabanlı bir risk yönetim yazılımıdır.	Jacobson, 1996
OCTAVE	Operasyonel Olarak Kritik Tehdit ve Güvenlik Açığı Değerlendirmesi Modelidir.	Alberts vd., 2003
BPIRM	İş süreci bilgi risk yönetimidir.	Coles and Moulton, 2003
ISRAM	Information Security Risk Analysis Method (ISRAM) nicel, belge tabanlı bir risk analiz yöntemidir.	Karabacak ve Soğukpınar, 2005
RAIM	Gerçek zamanlı izleme, Anomali tespiti, Etki analizi ve Azaltma stratejileri olmak üzere dört bölümden oluşan bir SCADA güvenlik çerçevesidir.	Ten vd., 2008
I&C System of NPP	Nükleer santrallerinin enstrümantasyon ve kontrol sistemlerinin nicel ve nitel analizi birleştiren bir risk değerlendirme yöntemi	Tian, Li ve Huang, 2022

Alan ile ilgili ön literatür taraması sonucunda Tablo 1 oluşturulmuştur. Bu tabloda verilen akademik çalışmalar ve uluslararası uygulamalar, bilgi güvenliği yönetiminde ve risk analizinde kullanılmak üzere tasarlanmış önemli bazı standartları, modelleri ve yöntemleri özetlemektedir. Bunlara ek olarak (Kure vd. 2018) ISO 31000 ve IEC 31010 standartları risk yönetimi faaliyetleri için kılavuzlar sağlayan ve risk yönetimini stratejik planlama ve yönetim süreçleri de dahil olmak üzere genel organizasyonel süreçlerin ayrılmaz bir parçası olarak ele alan yaygın olarak kabul görmüş risk yönetimi standartlarıdır.

Şekil 4'te risk analizi yöntemleri bir ağaç modeli ile resmedilerek sunulmuştur. Risk analizi temelde beş farklı risk analizi yöntemine ayrılsa da bu yöntemlerin birbirlerine geçişli olduğu anlaşılmaktadır. Aslında, bu yöntemler daha çok üretim sistemleri ve fiziki varlıklar ile doğrudan ilişkili analiz yöntemleridir. Bilgi fiziki bir varlık olmasa da bu yöntemlerle

analizi edilebileceği düşünülmektedir. Bilgi her ne kadar fiziki bir varlık değilse de ilgili olduğu varlıkların fiziki olması, işlendiği ve kaydedildiği ortamların fiziki ortamlar olması bu analiz yöntemlerini çağrıştırmaktadır.

Risk analizi sürecinde riskin olasılığını ve oluşması durumunda oluşturduğu etkiyi belirlemek için bazı yöntemler önerilmektedir. Bunlardan ilk akla gelen risk matrisidir. Bu matrisler, L Tipi ve X Tipi olmak üzere iki farklı türde oluşturulmaktadır. Bu matrislerin her ikisinde de olayların risklerinin oluşması olasılığını ve oluştuktan sonraki etkilerini belirlemek için bir analiz yapılır. Bu analizin başarısı için, iyi bir paydaş analizine, sistem çözümlemesine ve neden-sonuç ilişkisine hâkim olmak gerekmektedir.

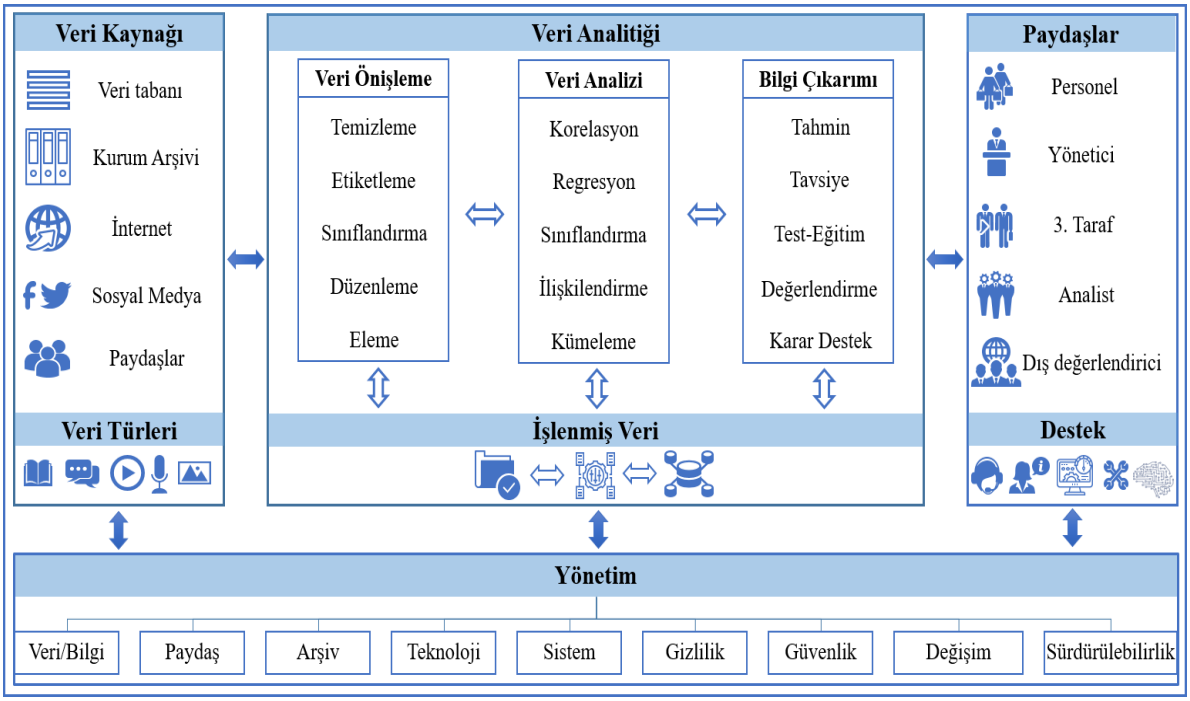
Şekil 4. Risk Analizi Yöntemleri

Bilgi güvenliği yönetiminde risk analizi süreçleri çalıştırılırken bilginin değeri ve önemi mutlaka ortaya konmalıdır. Bu değer ve önem ortaya çıktıktan sonra gizliliği, güvenliği, bütünlüğü ve erişim denetimi tam olarak sağlanabilir. Ayrıca, Şekil 3'te bilgi güvenliğini sağlama aşamalarında bilginin işlendiği ve saklandığı ortamın önemi bir kez daha ortaya çıkmaktadır. Bilgi bankaları ya da veri tabanları anlık olarak bilginin saklandığı ve işlendiği merkezlerdir. Bu merkezlere erişim denetimi sayesinde kimlerin hangi yetkilerle eriştiği ve ne tür işlemler yaptığı kayıt altına alınarak anlık ya da geçmişe dönük izlenebilir ve aksiyon alınabilir. Bu izleme ve denetim sürecine çok katmalı erişim güvenliği mekanizmaları da eklenerek sistem daha güvenli hale getirilebilir. Bu sayede bilgi bankalarında kullanıcı kaynaklı ortaya çıkabilecek gizlilik ve güvenlik ihlalleri önceden belirlenerek bazı riskler önlenmiş olur. Bu süreç, bilginin güvenliğini sağlama konusunda denetim döngüsü olarak hayata geçirilmelidir.

3. BİLGİ GÜVENLİĞİ YÖNETİMİNDE YAPAY ZEKÂ DESTEKLİ RİSK ANALİZİ

Yapay zekâ her alanda olduğu gibi bilgi güvenliği alanında da etkili uygulamalar yapmaktadır. Yapay zekâ sürecinin veriden başlayarak aksiyona geçmeye kadarki aşamalarda nasıl bir yol izlediği Şekil 5'te gösterilmiştir. Bu şekil Liu ve Yu (2023) öğrenim analitiğinde yapay zekânın kullanımını anlatan modelden esinlenerek bilgi güvenliği yönetiminde veri analitiğine yönelik olarak oluşturulmuştur.

Şekil 5. Kurumsal Bilgi Güvenliği Yönetiminde Veri Analitiği



Şekil 5'te veri kaynağı başlıklı kısımda, yapay zekânın var olmasının temeli olan verinin nerelerden üretildiği ve toplandığı yer almaktadır. Veri kaynağının en temel adresi kurumsal ver tabanları ve kurum arşivleridir. Bunun yanı sıra kurum ile ilgili olan internet ve sosyal medya ortamları önemli bir kaynak olmaktadır. Bu kaynaklar kurumun faaliyet alanı ile ilgili web sayfaları ve sosyal medya ortamları olabileceği gibi, ilişkili olduğu kişi ve kurumların ortamları da olabilir. Ayrıca, kurumun iş ve işleyişlerine etki eden paydaşların verileri de kaynak içerisinde yer almaktadır. Bu veriler genellikle; metin, resim, ses ve video türündeki verilerdir. İkinci başlık olan veri analitiği kısmında, veri önişleme, veri analizi ve bilgi çıkarımı süreçleri yer almaktadır. Veri önişleme süreci, veri kaynaklarından gelen verilerin eksik, hatalı ve tekrarlı olanların temizlenmesi ile başlamaktadır. Bu adımdan sonra veriler ne tür bir çıkarım için kullanılacaksa, etiketlenmeye başlar. Örneğin, müşteri yorumlarının işlendiği bir uygulamada, bir yoruma beş dereceli bir memnuniyet etiketlemesi yapılabilir. Bu etiketlemenin ardından tüm veriler bu örnekte olduğu gibi memnuniyet etiketi altında sınıflandırmaya alınır. Artık veriler, ilgi alanına ve çıkarım hedefine uygun olarak düzenlenmeye ve elemeye tabi tutulur. Ön işleme süreci doğru bir şekilde yürütüldüğünde veri seti artık matematiksel ve istatistiksel analizlere hazır hale gelmiş olur. Veri analizinde, problemin bağımlı ve bağımsız değişkenlerinin korelasyonuna, regresyonuna, sınıflandırmasına, ilişki düzeylerine ve kümelenme durumlarına bakılır. Bu aşamada lojistik regresyon, yapay sinir ağları, karar ağaçları ve destek vektör makineleri gibi yapay zekânın en bilinen algoritmalarından yararlanılır. Örneğin, ürün ilişkilendirmesi sayesinde, müşterinin bir ürünü alırken diğer hangi ürünleri aldığı bilgisi analiz edilebilir. Bu analiz için Apriori algoritması gibi birliktelik kuralları oluşturan algoritmalar tercih edilmektedir. Bu analizler sonucunda elde edilen bilgiler ve bulgular bilgi çıkarımı aşamasında tahmin, tavsiye ve değerlendirme amacıyla kullanılabilmektedir. Müşterinin siparişinde ilişkilendirme analizi ile elde edilen bilgilerle işletmenin stok tutma, reklam ve promosyon hazırlama gibi iş süreçlerini daha doğru yönetmesi sağlanabilir. Bu aşamalar sonucunda, öğrenen sistem artık gelecek veriler ve durumlar üzerine tahmin, tavsiye ve karar verme süreçlerini başlatabilir. Bu aşamaların sonunda, işlenmiş veriler dosyalarda ve veri tabanlarında raporlanmaya hazır halde tutulur.

Şekil 5'in üçüncü kısmında yapay zekâ sisteminin paydaşlarından bahsedilmiştir. Bu paydaşlar sistem içerisinde doğrudan ya da dolaylı olarak görev almaktadırlar. Bu paydaşlara örnek olarak; kurum personeli, kurumun ilişkili olduğu üçüncü taraflar, iç/dış değerlendiriciler, analistler, bilgi işlem uzmanları ve destek personeli yer almaktadır. Şekil 5'in en alt kısmında yer alan dördüncü kutuda ise yapay zekâ sisteminin yönetimi özetlenmiştir. Bu aşamada verinin ve bilginin oluşumu, saklanması ve iletimi ile ilgili tüm bileşenlerin yönetimi yer almaktadır. Özellikle teknolojinin seçimi ile sistem kurulumu ve yaşatılmasında yönetim anlayışına önemli görevler düşmektedir. Son olarak bu sistemin değişimi yakalayabilmesi ve sürdürülebilmesi için gelecek vizyonuna sahip bir bakış açısına sahip olması vurgulanmıştır. Kazan (2023) çalışmasında da vurguladığı gibi, değişime karşı direnç yönetimi aksatabileceği gibi bileşenler arasında uyumsuzluğa neden olarak başarıyı olumsuz etkileyebilir.

Şekil 6'da bilgi güvenliği yönetiminde risk analizi süreçlerine dahil edilen yapay zekâ yöntemleri, teknikleri ve araçlarının listelendiği bir model önerilmiştir. Aşamaların sektör ve kapasite temelli değişiklik gösterebileceği unutulmamalıdır. Ayrıca, bu yöntem, teknik ve araçların uygulama bazlı ele alınarak başarımı artırmak için bir kombinasyonu kullanılabileceği gibi bazı uygulamalarda farklı bir yöntem tercih edilebilir. Örneğin veri tabanlarına yapılan siber saldırıların önlenmesinde port analizi yapan tekniklerle protokol analizi yapan teknikler aynı anda kullanılabilir. Benzer bir şekilde bilginin şifrelenmesi sırasında yapay zekâ destekli kriptoloji yöntemlerinden sadece yapay sinir ağları tercih edilebilir. Bunun yanı sıra, Yapay zekâ uygulamalarında iç ve dış faktörler, veri setinin özellikleri ve veri setinin büyüklüğü başarımı doğrudan etkileyebilir. Ayrıca, Ağdeniz'in (2024) belirttiği gibi, yapay zekânın kullanımı sorasında ortaya çıkabilecek etik, yanlılık ve veri güvenliği gibi temel risklerin iyi analiz edilmesi gerekir.

Şekil 6. Kurumsal Bilgi Güvenliği Yönetiminde Risk Analizi Süreçlerinde Önerilen Yapay Zekâ Yöntemleri, Teknikleri ve Araçları

Şekil 6'da önerilen modelde risklerin tahmini ve belirlenmesi için bilgi kaynaklarının bir envanterinin oluşturulması ilk aşamadır. Bu aşamada, bilişim teknolojilerinin bileşenleri olan donanım ve yazılım sistemlerinin ve bilişim sistemleri içerisinde saklanan bilgilerin envanterinin oluşturulması yer almaktadır. Cibaroğlu ve Yalçınkaya (2019), bilgi kaynaklarının envanteri oluşturulurken bilgi yönetimi ve arşivleme süreçlerinde Çok Katmanlı Algılayıcı (Multi Layer Perception - MLP) algoritmasının %84 başarı oranına eriştiğini belirtmektedirler. Avusturalya Maliye Bakanlığı'nın e-posta sunucularında bulunan e-postaların yapay zekâ yöntemleri ile sınıflandırılması uygulaması örnek bir uygulama olarak verilmektedir. Yaşayan bir sistemde anlık risklerin tanımlanması ve tespiti önemli bir aşamadır. Şekil 5'te ikinci aşama olan risklerin tanımlanmasında kullanılan yapay zekâ yöntemleri belirtilmiştir. Bu aşamada temel olan anormal durumların izlenmesi ve önlemesi için raporlanmasıdır. Öner vd. (2024) Destek Vektör Makinesi (Support Vector Machine) ve diğer derin öğrenme yöntemleriyle borsa işlemlerinde anomali tespiti çalışmalarında, anormal verileri tespitinde %86,4 oranında başarı elde etmişlerdir. Üçüncü aşama olan risklerin sınıflandırması aşamasında, riskin derecelendirilmesi ve ona uygun önlemlerin belirlenmesi yer almaktadır. Özellikle bankacılık ve finans sektörlerinde çok sık kullanılan kredi risk derecelendirme uygulamaları buna örnek olarak verilebilir. Bankaların kredi risk derecelendirme ve değerlendirmesi aşamasında yapay sinir ağları, lojistik regresyon, rastgele orman ve karar ağaçları gibi yapay zekâ modelleri ile başarılı sonuçlar elde edilmiştir (Mesri vd., 2021; Guo ve Zhou, 2022). Önlemlerin alınması ve denetlenmesi aşamalarında ise, daha önceki başarılı uygulamalardan elde edilen deneyimler, kurumsal bir kültür haline gelerek risk yönetimini birer karar destek sistemi ve uzman sistem görevi ile yürütebilmektedir.

Yönetim kavramı organizasyonu oluşturan tüm bileşenlerin koordinasyonunu sağlarken sevk ve idare edebilme yeteneği sağlamaktadır. Bu yeteneğin, tüm paydaşların memnuniyetini, verimliliğini ve başarısını artırması beklenmektedir. Bu kapsamda bilgi güvenliğinin yönetimine bakıldığında; bilginin oluşumunda, kullanımında, iletiminde ve saklanmasında gizliliği, güvenliği ve bütünlüğü ilkelerinin sağlanmasını akla gelmektedir. Bu ilkelerin sağlanması aşamalarında mutlaka riskler ortaya çıkmaktadır. Bu risklerin belirlenmesi, ölçülüp hesaplanması, analiz edilmesi ve değerlendirilmesi önemli bir başarı faktörüdür. Risk analizinde yapay zekâdan destek alarak insana yardımcı bir araç olarak ele alınması gerekmektedir. Çünkü yaşayan ve gelişen birden fazla faktörün etkileşimde olduğu bir sistemin insan kapasitesini aşan yönleri olacaktır. Bu yönlerin izlenmesi, denetlenmesi ve giderilmesinde robotik sistemlerden ve yapay zekâ araçlarından destek almak kaçınılmaz olacaktır.

Şekil 5 ve Şekil 6'da önerilen modelde yer alan süreçlerin yürütülmesinde özenle, titizlikle ve modern bir yönetim anlayışını benimsemek gerekmektedir. Bu yönetim anlayışında tüm bileşenlerin koordinasyonu sağlarken teknolojinin tüm olanaklarından yararlanmak ilk iş olmalıdır. Yapay zekâ bu olanakların en güncel olanlarından olduğu için yönetim için ideal bir yere sahiptir. Şekil 6'da görüldüğü gibi veri ve bilginin olduğu her aşamada mutlaka bir yapay zekâ yöntemi, tekniği ve aracı devreye girmektedir.

4. SONUÇ VE ÖNERİLER

Bilgi, fiziki olmadığı için ve değeri ancak kaybedilince anlaşılabilen bir varlık olduğu için tehdit ve risklere karşı neler yapılması gerektiği iyi bir risk analizi ve değerlendirmesi ile belirlenebilir. Kişilerin, kurumların ve devletlerin bilgi kayıplarına karşı zarara uğramamasının, güvenli bir şekilde faaliyetlerini sürdürebilmesinin, başarıya erişmesinin ve siber dünyanın şartlarına uyum sağlayarak ilerleyebilmesinin en önemli şartının bilgi güvenliğinin ve gizliliğinin sağlanması olduğu unutulmamalıdır.

İnsanların bilgilerini dijital dünyada çok çeşitli ve gelişmiş tehdit ve risklere karşı koruması alınan tüm önlemlere rağmen yetersiz kalmaktadır. Bu nedenle sürekli tetikte ve korku içerisinde siber dünyada dijital bir yaşam sürmek mümkün görünmemektedir. Bu nedenle yardımcı bazı teknolojilere ihtiyaç vardır. Bu teknolojilerin başında da yapay zekâ teknolojisi gelmektedir. Yapay zekâya sahip varlıkların insana özgü duyguları anlaması, öğrenmesi ve taklit etmesine doğru bir yolda ilerlenirken, insana özgü yeteneklere sahip robotik varlıkların temelleri atılmaktadır. Bu süreçte dikkat edilmesi gereken nokta ise kötü niyet ve özelliklerden arındırılmış yapay zekânın tasarımını, toplumsal kabulünü ve hukuksal zeminini biran önce oluşturmak olmalıdır.

Bilgi güvenliği yönetiminde izleme, tespit etme, önleme ve tepki verme faaliyetleri birbirleriyle ilişkili ve sürekli çalışan bilgi güvenliğini sağlama döngüsüdür. Bu döngünün her aşaması insan eliyle yürütülmesi oldukça zor süreçler içermektedir. Özellikle bilgi kaynaklarına erişim aşamasında anormal durumların izlenmesi ve tespit edilmesi dikkat, özen ve süreklilik gibi bazı yetenekler gerektirmektedir. Yapay zekâ sistemleri bu yetenekleri sergilemede oldukça etkili ve başarılı olmaktadır. Örneğin, kurumsal bir bilişim ağında anlık iletilen veri miktarları gigabaytlar ölçüsünde olabilmektedir. Bu denli yüksek miktarlardaki veriler içerisinde tehdit içeren anormal trafiğin belirlenerek engellenmesi ağın doğru, düzenli ve güvenli çalışmasını sağlamaktadır. Bunun için güvenlik duvarları gibi yapay zekâ destekli sistemler önerilmektedir.

Kurumsal bilgi güvenliği yönetiminde risk analizi süreçlerinde kurum yönetimine ve çalışanlarına oldukça fazla görevler düşmektedir. Bu görevlerin pek çoğu zaman ve emek yoğun süreçler içermektedir. Bu süreçlerde, özellikle bilişim teknolojilerinden yapay zekâ sistemleri, birer asistan görevi ile yer alırken başarılı sonuçlar üretmektedirler. Bu çalışmada, bilgi güvenliğine yönelik ortaya çıkan risklerin belirlenmesinden, derecelendirmesine, bu risklerin yönetiminden bertaraf edilmesine kadarki tüm aşamalarda yapay zekâ teknik ve yöntemlerinden oluşturulan bir model önerilmiştir. Model, veri setinin toplanması ve büyük verinin oluşturulması temeli üzerine kurulmuştur. Bu temelde doğal dil işleme gibi derin öğrenme teknikleriyle bilgi kaynaklarının ön işlemesi ve yapay sinir ağları gibi gelişmiş ağlar ile bilgilerin analiz edilmesi yer almaktadır. Elde edilen tahmin bulguları ile karar destek sisteminin çalıştırılarak yönetime destek olması sağlanmaktadır. Bu model sürekli çalıştırıldığında, deneyimlerinden de öğrenen bir model haline gelerek uzman bir sistem mimarisi oluşturmaktadır.

Yapay zekânın, insan yerini alarak çalışabildiği sektör ve işlerde başarılı sonuçlar elde edildiği bilinmektedir. Ancak, şeffaflık, gizlilik, mahremiyet, adalet, etik ve eşitlik gibi temel insan hakları ilkelerine karşı oluşabilecek ihlallerin önüne geçilmesi zorlaşmaktadır. Bu ihlallerin önlenmesi için bu çalışmada önerilen modelin merkezinde, bilgili ve tecrübeli yöneticiler ve bilişim personelinin yer alması sağlanmaktadır. Bu sayede model sürekli izlenmekte ve kontrol altında tutulmaktadır. Bu tür yapay zekâ modellerinin kullanımında, ulusal ve uluslararası işbirlikleri ve anlaşmalar ile teknolojik ve hukuki zemin hazırlanmalıdır. Bu kapsamda, 2018 yılında "Yapay Zekânın Gelişiminde Sorumluluk için Montreal Deklarasyonu" adı altında ortaklık bildirisi ile dijital teknoloji ve yapay zekânın toplumsal gelişimini ve çıkarlarını

belirleyen bazı ilke ve değerler ortaya konmuştur (Singil, 2022). Bu gibi örnek ilke ve anlaşmaların güncellenerek geliştirilmesi birey ve toplum yararı yanı sıra faydalı modellerin geliştirilmesi için önemli görülmektedir.

Yapay zekâ teknolojisi insanlığa her ne kadar olumlu katkılar sunsa da dünyayı ele geçirebileceği gibi olumsuz düşünceler de ortaya çıkmaktadır. Bir diğer düşünce ise; yapay zekâya sahip sistemler zeki olsalar bile insana özgü duygu ve davranışları sergileyebilecek kadar iyi bir ruha ve sempatiye sahip olamayacakları düşüncesidir. Bu tür olumsuz düşüncelere karşın son zamanlarda geliştirilen uygulamalardan olan, çocuklara ve yetişkinlere duygusal destek sunabilen asistan robotlar ve otonom karar veren sistemler bu görüşlerin yersiz olduğunu göstermektedir.

Yapay zekânın insanlar için bir fırsat mı yoksa tehdit mi olduğuna yine insanlar karar verecektir. Yapay zekâ sisteminin mimarisi insanda bulunan zafiyetler ve art niyetlerle donatılacak şekilde geliştirilirse, onu ilerde kontrolsüz, yanlış kararlar veren ve zararlı eylemlerde bulunan varlıklar haline getirebilir. Bu nedenle, geliştirme ve kullanma aşamasında etik ve hukuki sınırlar içerisinde bir gelişim planı hazırlanmalıdır. Ayrıca, insanların yapay zekâ sistemlerini işlerini ellerinden alacak, yaşamı tehlikeye sokacak birer düşman varlık gördükleri de bilinmektedir. Bu ön yargılara karşın, onları hayatı kolaylaştıracak yeni nesil teknolojik sistemler olarak görmeleri sağlanmalıdır. Çünkü yapay zekânın gelişmesi ve ilerlemesi için biran önce toplumsal bir uzlaşının sağlanması gerekmektedir. Bu uzlaşı için insanların geleceği şekillendirecek bilgi, birikim ve farkındalık düzeyine erişmesinin yolu açılmalıdır.

Bilişim teknolojilerinin geliştirilmesi ve kullanılmasında dikkat edilmesi gereken bir diğer konu ise gizlilik ve güvenlik konularıdır. Hangi yapay zekâ türü kullanılırsa kullanılsın mutlaka kişisel bilgi güvenliği ve siber güvenlik konularına dikkat edilmelidir. Unutulmamalıdır ki, teknolojik bir sistem başka bir sisteme bağlandığı anda iki yönlü veri iletimi söz konusudur. Bu iletimin başından sonuna kadar kontrollü, izinli ve yetkili bir erişim üzerinden sağlanmalıdır. Yapay zekâ sistemleri de bireysel veya kurumsal ağlar üzerinden bağlantı yapacağı için topladığı verilerin gizliliğini ve güvenliğini tehdit edebilir. Bu süreçte, yapay zekâ fayda sağlayan bir araç olmaktan çıkarak bir siber tehdit haline gelebilir. Sonuçta da bu araçtan elde edilebilecek tüm faydanın zarara dönüşmesi mümkündür.

Yapay zekâ ile ilgili önemli bir diğer konu ise enerji konusudur. Yapay zekâ ile çalışan sistemler en temelde veri ve enerji girdisine ihtiyaç duymaktadırlar. Dijital bir sistemde bu iki girdi elektrik enerjisine bağlıdır. Bu bağımlılık mevcut elektrik kapasitesinin aşılmasına ve maliyetlerinin yükselmesine neden olmaktadır. Yapay zekâ teknolojisinin gelecek vizyonu da göz önüne alınarak çevreci teknolojiler ile enerji üretiminin desteklenmesi yenilenebilir enerji kaynaklarının kullanımının yaygınlaştırılması gerekmektedir.

Siber uzayda iş ve işlemlerini yürüten ve kullanıcı olarak yer alan insanın dijital varlıklarını güvenli bir şekilde barındırabilmesi için tehdit ve risklere karşı temel önlemleri alması gerekir. Bunun için hem kendisinin hem de kurumların bilgi güvenliği unsurları hakkında temel düzeyde farkındalıklarının olması gerekmektedir. Ayrıca, mevcut risklerin belirlendiği ve azaltıldığı şeffaf ve korunaklı ortamların oluşması için siber dünyanın tüm bileşenlerinin etkin bir şekilde rol alması gerekmektedir. Bunun için iyi bir risk analizi sürecinin ele alınması gerekmektedir.

Siber dünyanın görünen kısmından daha çok deepweb ve darknet gibi görünmeyen ve karanlık bölgelerinin olduğu unutulmamalıdır. Önemli ve değerli bilgilerin bu bölgelerden gelebilecek tehditlere karşı daha fazla korunması gerektiği unutulmamalıdır. Bunun için sahip olunan bilginin değeri ve önemi tam olarak ortaya konmalıdır. Bu değer ve öneme haiz bir risk hesabı ve değerlendirmesi yapılması gerekmektedir. Özellikle kişisel ve kurumsal hassas verilerin kaydedildiği ve paylaşıldığı ortamların iyi seçilmesi ve buna göre hareket edilmesi önemli görülmektedir. Bu kapsamda bilgi teknolojileri okuryazarlığının artırılması ve tüketici konumundan üretici konumuna geçerek teknolojiye yön veren bir düzeye erişmek gerekmektedir.

Bilgi güvenliği yönetimi sürecinde tehdit ve risklerin azaltılması için ilk olarak, yeni çıkan teknolojilerin kullanılmadan önce tüm özelliklerinin incelenmesi ve analizinin yapılması olmalıdır. Ardından, fayda maliyet analizi ile teknolojinin getirileri ve götürüleri hesaplanmalıdır. Sonrasında ise, teknolojinin uygulaması aşamasında temel güvenlik politikaları belirlenerek bir kullanım yönergesi devreye alınmalıdır. Son olarak, izleme ve önlem alma prensipleri ile proaktif bir güvenlik mekanizması geliştirilmelidir.

Coşar (2022b) bireysel ve kurumsal anlamda siber dünya ile etkileşime girildiğinde tehdit ve risklere karşı temel düzeyde de olsa farkındalık düzeyinin geliştirilmesi gerektiğini vurgulamaktadır. Bu temel düzeyin dijital okuryazarlık ile başlayarak, donanım, yazılım ve bağlantı güvenliği ile devam etmesi gerekmektedir. Ayrıca, oluşan riskli durumlarla baş edebilmek için bazı teknolojik bilgi ve becerilere sahip olunması gerektiğini de ileri sürmektedir. Bilgi güvenliği farkındalık düzeyinin geliştirilmesi ve güncel tutulması için kamu spotları, bilgilendirici animasyon ve videolar faydalı olabilir. Ayrıca, her kullanıcının dijital bilgi kapasitesini ve kaynaklarını ölçen ve değerlendiren uygulamalar geliştirilebilir. Bu uygulamalar birey ve kurumların siber zafiyetlerini, ihmallerini ve risklerini ortaya koyarak ön savunma mekanizmalarını geliştirebilir.

Kaynakça

Ağdeniz, Ş. (2024). Güvenilir Yapay Zeka ve İç Denetim. *Denetişim* (29), 112-126. https://doi.org/10.58348/denetisim.1384391

Alberts, C., Dorofee, A., Stevens, J. & Woody, C. (2003). Introduction to the OCTAVE Approach. *Pittsburgh, PA, Carnegie Mellon University*, pp.72-74.

Bilbao, A. (1992, October). TUAR-A Model of Risk Analysis in The Security Field. In *Proceedings 1992 International Carnahan Conference on Security Technology: Crime Countermeasures* (pp.65-71). IEEE.

CCTA, U. (2005). CCTA Risk Analysis and Management Method CRAMM. *United Kingdom Central Computer and Telecommunication Agency*. User Guide.

Cibaroğlu, M. O. & Yalçınkaya, B. (2019). Belge ve Arşiv Yönetimi Süreçlerinde Büyük Veri Analitiği ve Yapay Zeka Uygulamaları. *Bilgi Yönetimi*, 2(1), 44-58. https://doi.org/10.33721/by.570634

C&A Systems Security Limited. (2000). COBRA Consultant Products for Windows Evaluation & User Guide (2000)

Coles, R. S., Moulton, R. (2003). Operationalizing IT Risk Management. *Computers & Security*, Volume:22, Issue:6, pp.487-493, https://doi.org/10.1016/S0167-4048(03)00606-0

Coşar, M. (2022a). Privacy and Security on Blockchain. In: *Blockchain Innovative Bossiness Processes and Long-Term Sustainability*, Eds: Mert G., Zeren S.K., Yılmaz O., Nobel Bilimsel, Edition 1, ISBN: 978-625-433-841-0, Ankara.

Coşar, M. (2022b). Siber Dünyanın Karanlık Yüzü: DeepWeb ve DarkNet. *Journal of Management Theory and Practices Research*, 3 (1), ss.58-71.

Coşar, M. (2023a). Tedarik Zinciri Yönetiminde Yapay Zekâ ve Robotik. Editör: Taşkın, B. & Çağlar, B., *Tedarik Zincirinde Dijital Dönüşüm*, (5. Bölüm, ss.69-93), 1. Baskı, Ekin Yayınevi. ISBN: 978-625-6952-95-9

Coşar, M. (2023b). Yapay Zekâ Türleri ve Bileşenleri. Editör: Kılıç, S. *Yapay Zekâ Teori ve Uygulamalar*, (7. Bölüm, ss.129-146), 1. Baskı, Nobel Bilimsel, ISBN: 978-625-393-169-8

Guo, W., Zhou, Z.Z. (2022). A comparative study of combining tree-based feature selection methods and classifiers in personal loan default prediction. *Journal of Forecasting*, 41, 1248-1313. https://doi.org/10.1002/for.2856

ISF. (1997). Simplified Practical Risk Analysis Methodology (SPRINT) User Guide. Information Security Forum (ISF)

Jenkins, B. D. (1998). Security Risk Analysis and Management. White Paper, *Countermeasures, Inc*. Internet, Erişim Adresi: https://home.nr.no/~abie/RA_by_Jenkins.pdf (Erişim Tarihi: 21 Haziran, 2024)

ISO. (2022a). ISO/IEC 15408-1:2022, Information security, cybersecurity and privacy protection — Evaluation criteria for IT security. International Standart Organization, Parts 1, Edition 4. Internet, Erişim Adresi: https://www.iso.org/standard/72891.html (Erişim Tarihi: 21 Haziran, 2024)

ISO. (2022b). ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Standart Organization, Edition 3, Internet, Erişim Adresi: https://www.iso.org/standard/27001 (Erişim Tarihi: 21 Haziran, 2024)

Jacobson, R.V. (1996). CORA Cost-of-Risk Analysis. In Proceedings of IFIP'96 WG11.2 Somos, Greece.

Kailay, M. P., Jarratt, P. (1995). RAMeX: A Prototype Expert System For Computer Security Risk Analysis and Management. *Computers & Security*, Volume:14, Issue:5, pp.449-463, https://doi.org/10.1016/0167-4048(95)00013-X

Karabacak, B., & Sogukpinar, I. (2005). ISRAM: Information Security Risk Analysis Method. *Computers & Security*, Volume:24, Issue:2, pp.147-159, https://doi.org/10.1016/j.cose.2004.07.004

Kazan, G. (2023). Tedarik Zinciri Yönetiminde İç Kontrol: Verimliliğin ve Risk Yönetiminin Artırılması. *Denetişim*, Cilt:28, ss.123-136, https://doi.org/10.58348/denetisim.1320143

Kure, H.I., Islam, S., Razzaque, M.A. (2018). An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System. *Applied Sciences,* Volume:8, No:6, 898, https://doi.org/10.3390/app8060898

Liu, M., Yu, D. (2023). Towards Intelligent E-learning Systems. *Education and Information Technologies*, Volume:28, pp.7845-7876, https://doi.org/10.1007/s10639-022-11479-6

Mesri, K., Tahseen, I., Ogla, R. (2021). Default on a credit prediction using decision tree and ensemble learning techniques. *Journal of Physics: Conference Series,* https://doi.org/10.1088/1742-6596/1999/1/012121

Öner, S. C., Şahan, H., Demirdağ M. & Bayrak, A. T. (2024, May). Anomaly Detection in Stock Market Transactions: A Comparison of Deep Learning Methods. 2024 32nd Signal Processing and Communications Applications Conference (SIU), Mersin, Turkiye, 2024, pp.1-4, https://doi.org/10.1109/SIU61531.2024.10601101.

Stoneburner, G., Goguen, A. & Feringa, A. (2002). Risk Management Guide for Information Technology Systems. *Nist Special Publication*, 800(30), National Institute of Standards and Technology (NIST), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30.pdf

Singil, N. (2022). Yapay Zekâ ve İnsan Hakları. *Public and Private International Law Bulletin*, Volume:42, Issue:1, ss.121-158, https://doi.org/10.26650/ppil.2022.42.1.970856

Ten, C. W., Liu, C. C., & Govindarasu, M. (2008, May). Cyber-vulnerability of Power Grid Monitoring and Control Systems. In *Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead* (pp. 1-3).

Tian, Y., Li, J. & Huang, X. (2022). A Cybersecurity Risk Assessment Method and its Application for Instrumentation and Control Systems in Nuclear Power Plants. *IFAC-PapersOnLine*, Volume 55, Issue 9, pp.238-243, https://doi.org/10.1016/j.ifacol.2022.07.042

Yıldız, M., Yıldırım, F.B. (2018). Yapay Zekâ ve Robotik Sistemlerin Kütüphanecilik Mesleğine Olan Etkileri. *Türk Kütüphaneciliği*, Cilt:32, Sayı:1, ss.26-32, http://doi.org/10.24146/tkd.2018.29