T.C.

MİLLÎ EĞİTİM BAKANLIĞI

Hayat Boyu Öğrenme Genel Müdürlüğü

BİLİŞİM TEKNOLOJİLERİ ALANI

SİBER TEHDİT İSTİHBARATI (Cyber Threat Intelligence) KURS PROGRAMI

Ankara, 2017

İÇİNDEKİLER

PROGRAMIN ADI

Siber Tehdit İstihbaratı (Cyber Threat Intelligence) Kurs Programı

PROGRAMIN DAYANAĞI

1. 24.06.1973 tarihli ve 14574 sayılı Resmî Gazete' de yayımlanan, 1739 sayılı Millî Eğitim Temel Kanunu,
2. 14.09.2011 tarihli ve 28054 sayılı Resmî Gazete' de yayımlanan, 652 sayılı Millî Eğitim Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname,
3. 21.5.2010 tarihli ve 27587 sayılı Resmî Gazete' de yayımlanan Yaygın Eğitim Kurumları Yönetmeliği,
4. Talim ve Terbiye Kurulu Başkanlığının 20.04.2016 tarih ve 19 sayılı kararı ile kabul edilen, Yaygın Eğitim Kurumları Çerçeve Kurs Programı,
5. 27.4.2012 tarihli ve 28276 sayılı Resmî Gazete' de yayımlanan Bilgisayar Donanım Elemanı 4. Seviye Ulusal Meslek Standardı,
6. 16.10.2012 tarihli ve 28443 sayılı Resmî Gazete' de yayımlanan Bilgi İşlem Destek Elemanı 4. Seviye Ulusal Meslek Standardı,
7. 16.10.2012 tarihli ve 28443 sayılı Resmî Gazete' de yayımlanan Sistem İşletmeni 4. Seviye Ulusal Meslek Standardı,
8. 16.10.2012 tarihli ve 28443 sayılı Resmî Gazete' de yayımlanan Veri Giriş Elemanı 4. Seviye Ulusal Meslek Standardı,
9. 23.05.2007 tarihli ve 26530 sayılı Resmî Gazete' de yayımlanan 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
10. 05.11.2013 tarihli ve 28812 sayılı Resmî Gazete' de yayımlanan Yazılım Geliştirici 4. Seviye, 5. Seviye ve 6. Seviye Ulusal Meslek Standardı,
11. 30.11.2007 tarihli ve 26716 sayılı Resmî Gazete' de yayımlanan "İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik",
12. 26.02.2013 tarih ve 28571 sayılı Resmi Gazete' de yayımlanan Web ve Çoklu Ortam Geliştiricisi 4. Seviye ve 5. Seviye Ulusal Meslek Standardı,
13. Talim ve Terbiye Kurulu Başkanlığının 27.09.2005 tarih ve 329 sayılı kararı ile onaylanan Bilgi ve İletişim Teknolojisi Dersi Öğretim Programı,
14. Talim ve Terbiye Kurulu Başkanlığının 31.08.2016 Tarih ve 65 sayılı Kararı ile kabul edilen, Bilgisayar Bilimi Dersi (Kur 1, Kur 2) Öğretim Programı,

15. Talim ve Terbiye Kurulu Başkanlığının 08.02.2011 tarih ve 10 sayılı “Meslekî ve Teknik Eğitim Okul ve Kurumlarının 50 Alanına Ait Haftalık Ders Çizelgeleri ile Çerçeve Öğretim Programlarında Değişiklik Yapılması” konulu kararı.

PROGRAMA GİRİŞ KOŞULLARI

1. Türkiye Cumhuriyeti vatandaşı olmak,
2. Okuryazar olmak,
3. Genel bilgisayar kullanımı bilgisine sahip olduğunu belgelendirmek,
4. ***(Değ: 15.03.2022 / 45686018 Makam Onayı)*** 14 yaşını doldurmuş olmak.

EĞİTİMCİLERİN NİTELİĞİ

Talim ve Terbiye Kurulu Başkanlığınca yayımlanan Öğretmenlik Alanları, Atama ve Ders Okutma Esaslarına göre atanan;

a. Bilişim Teknolojileri Alan öğretmenleri,
b. Bilişim Teknolojileri Alan öğretmenliği mezunları,
c. Fakülte ve yüksekokulların Bilişim Teknolojileri alanından mezun olup öğretmenlik formasyonuna sahip olanlar

görev almalıdır.

PROGRAMIN AMAÇLARI

Siber Tehdit İstihbaratı (Cyber Threat Intelligence) Kurs Programını bitiren bireylerin;

1. İstihbarat terimlerini kavraması,
2. İstihbarat alanlarını kavraması,
3. İstihbarat toplama yöntemlerini kavraması,
4. Toplanan istihbaratı analiz edebilmesi,
5. İstihbarata karşı koyma faaliyetleri konusunda bilinçlenmesi,
6. Yabancı istihbarat servislerinin çalışma yöntemlerini kavraması,
7. Siber sızma ve karşı koyma yöntemlerini örneklerle açıklaması,
8. Siber istihbarat ve siber tehdit istihbaratı arasındaki farkları sıralaması,
9. Siber istihbarata karşı koyma yöntemlerini kavraması,
10. Servislerin haber toplama yöntemlerini kavraması,
11. Servis haber toplama özelliklerini sıralaması,
12. Otomatik zafiyet tarama yazılımlarını kullanması,

13. Parola kırma saldırılarına karşı korunma yöntemlerini kavraması,

14. Kablosuz ağ kırma yöntemlerinden korunması,

15. Ağ zehirleme terimini kavraması,

16. Adli bilişim, siber olay ve zararlı yazılım analizi yapması,

17. Web uygulamaları veritabanına izinsiz erişimleri engellemeye yönelik tedbirleri alması,

18. Güvenli yazılım geliştirmesi,

19. Adli bilişim işlemlerini gerçekleştirmesi,

20. Siber olayları analiz etmesi,

21. Zararlı yazılımları analiz etmesi,

22. Tersine mühendislik uygulamalarını gerçekleştirmesi,

23. Güvenli mobil uygulamaları geliştirmesi,

24. Bilişimle ilgili kanun ve yönetmelikleri kavraması

amaçlanmaktadır.

PROGRAMIN UYGULANMASIYLA İLGİLİ AÇIKLAMALAR

Siber Tehdit İstihbaratı (Cyber Threat Intelligence) Kursu aşağıda belirtilen hususlar çerçevesinde uygulanır:

1. Günümüzde mobil cihazların yaygınlaşmasıyla siber ortamda gerçekleşen faaliyetler kişilerin ve ülkelerin mahremiyetine ve güvenliğine zarar verecek boyutlara ulaşmıştır. İnternet ve sosyal medya üzerinden gerçekleştirilen dolandırıcılık, istismar ve siber saldırılar, kişiler ve ülkeler için tehdit haline gelmektedir. Bu program, bu konuda önleyici faaliyetlerde bulunarak tedbirler almak amacıyla hazırlanmıştır.

2. Siber uzay üzerinden Türkiye Cumhuriyeti'ne karşı ulusal tehditlerin artmasıyla birlikte, siber saldırılara karşı etkin bir mücadele vermek için gerekli insan kaynağının oluşturulması gerekliliği doğmaktadır. Bu konuda uzman nitelikli insan kaynağının oluşturulması için, bireylere kritik altyapılara karşı siber tehdit oluşturan hedeflere yönelik, defansif ve ofansif siber güvenlik faaliyetlerinin, teorik ve uygulamalı olarak verilmesi gerekmektedir.

3. Bu programla; siber uzayda karşılaşılan tehditler ve bu tehditlere karşı alınabilecek önlemler hakkında gerekli olan bilgi kaynağının oluşturulması amaçlanmaktadır. Kamu kurum ve kuruluşlarının bilişim, bilgi güvenliği ve ileri elektronik teknolojileri konularındaki istek ve ihtiyaçları doğrultusunda, gerek kamu gerekse de özel kurumların kritik

altyapılarının korunması için gerekli insan kaynağının yetiştirilmesi programın bir diğer amacıdır. Programın sonunda katılımcı siber uzay üzerinden gelen saldırıları tespit edip, önleyecek bilgi ve beceriye sahip olacaktır.

4. Programın uygulanmasında ağırlıklı olarak grupla öğrenmeyi destekleyici yöntem ve teknikler ile uygulamaya dayalı yöntem ve teknikler kullanılır. Uygulamalar mümkünse yuvarlak masalarda, grup çalışmalarına ve sunumları dinlemeye uygun bir ortamda gerçekleştirilir.
5. Kurs Programı, Millî Eğitim Bakanlığında görevli uzman, alan öğretmenleri ve alan uzmanları ile iş birliği içinde hazırlanmıştır.
6. Program, Hayat Boyu Öğrenme Genel Müdürlüğüne bağlı eğitim kurumlarında veya kurumlarca uygun görülen eğitim-öğretime elverişli diğer ortamlarda uygulanabilir.
7. Program kursiyerlerin, analitik zekâ, yaratıcı düşünce, yüksek sorumluluk bilinci, profesyonel disiplin, araştırma yöntemlerini kullanma, gelişim ve değişime açıklık, takım çalışmasına yatkınlık, bilgi işleme ve analiz etmek, yüksek teknik bilgiye ve tecrübeye erişmek ve ketumiyet becerilerini geliştirmek amacıyla hazırlanmıştır.
8. Kurs programının amaçları ve içeriği yoluyla kursa katılan bireylere aşağıda tabloda verilen değerlerin kazandırılması ve bu yolla bireylerin geliştirilmesi hedeflenmiştir.

DEĞERLER
Çalışkanlık
Empati
Sorumluluk
Saygı
Hoşgörü
Başarı

6. Programın uygulanmasında hayat boyu rehberlik hizmeti sunan eğiticiler, kursiyerlerin kişisel ve mesleki nedenlerle yeterliliklerinin değişmesi ve gelişmesine katkıda bulunacak bir rehber niteliğinde olmalıdır.

9. Program süresince bireylerin merak uyandırma ve planlama, araştırma ve keşfetme, çözümleme ve derinleştirme, paylaşma ve yaşantıya uygulama etkinliklerini gerçekleştirmeleri sağlanarak bireyin öğrenmeye etkin katılımı desteklenmelidir. Sınıf, işletme, kütüphane vb. ortamlarda; bilgisayar donanımları, Internet ortamı, Televizyon, VCD, DVD, projeksiyon vb. görsel ve işitsel materyaller kullanılarak konu ile ilgili sunumlar yapılmalıdır.
10. Bireysel öğretimi destekleyecek şekilde; gösteri, anlatım, grup çalışması, araştırma, uygulama vb. yöntem ve teknikleri uygulanabilir.
11. Kurs içeriğinin, bireyler tarafından daha iyi öğrenilmesi ve bilgilerin kalıcı olması açısından, çevrede bulunan, üniversitelerin ilgili bölümleri, dernek ve sivil toplum örgütleri, işletmeler, diğer alan öğretmenleri ile işbirliği yapılabilir.

PROGRAMIN KREDİSİ

Genel kurs programlarında kredilendirme yapılmamaktadır.

PROGRAM SÜRESİ VE İÇERİĞİ

Kurs programının süresi; günde en fazla 8 ders saati uygulanacak şekilde toplam 144 (Yüz kırk dört) saattir.

Konular	Süre (Ders Saati)
Temel İstihbarat	8
İstihbarata Karşı Koyma	8
Siber İstihbarat	8
Siber İstihbarata Karşı Koyma	8
Siber Güvenlik ve Bilgi Güvenliğine Giriş	8
Hedef Sistemler Hakkında Bilgi Toplama	8
Otomatik Zafiyet Tarama ve Değerlendirme, Parola Kırma Saldırıları	8
Ağ Zehirleme, Kablosuz Ağ Saldırıları, DDoS, Sosyal Mühendislik Saldırıları	8
Web Uygulaması ve Veri tabanına İzinsiz Erişim ve Güvenlik	24
Güvenli Yazılım Geliştirme	8
Adli Bilişim, Siber Olay Analizi, Zararlı Yazılım Analizi	16
Tersine Mühendislik	8
Güvenli Mobil Uygulama Geliştirme	16
Bilişim Hukuku	8
TOPLAM	**144**

İÇERİK

1. TEMEL İSTİHBARAT

1.1 İstihbaratın tanımı,

1.2 İstihbarat çarkı,

1.3 İstihbaratın temel ilkeleri,

1.4 Alanlarına göre istihbarat,

1.5 Ölçeklerine göre istihbarat,

1.5.1 Stratejik istihbarat,

1.5.2 Taktik (Cari) istihbarat,

1.5.3 Operasyonel istihbarat,

1.6 İstihbarat analizi,

1.7 Psikolojik istihbarat,

2. İSTİHBARATA KARŞI KOYMA

2.1 İKK ve Koruyucu Güvenliğin kapsamı, içeriği, temel kavramları,

2.2 Yabancı istihbarat servislerinin ve uzantılarının çalışma usûl ve yöntemleri,

2.3 Servislerin ve bağlantılı unsurların sebep olduğu tehditler, güvenlik sorunları,

2.4 Tehditlere karşı bireysel ya da kurumsal açıdan karşı koyma teknikleri,

2.5 İstihbarat faaliyetleri,

2.6 Kontrespiyonaj safhaları,

- 2.6.1 İnsana dayalı istihbarat,
- 2.6.2 Konum istihbaratı,
- 2.6.3 Görüntü istihbaratı,
- 2.6.4 Açık kaynak istihbaratı,
- 2.6.5 Sinyal istihbaratı,
- 2.6.6 Haberleşme istihbaratı,
- 2.6.7 Elektronik istihbarat,

2.7 Kontrterörizm,

2.8 Kontrsübversiyon,

2.9 Kontrsabotaj.

3. SİBER İSTİHBARAT

3.1 Siber istihbaratın tanımı,

3.2 Siber istihbarat ve siber tehdit istihbaratı arasındaki farklar,

3.3 Siber istihbarat toplama yöntemleri,

3.4 Siber tradecraft (espiyonaj yöntemleri),

3.5 Siber istihbarat faaliyetleri,

3.6 Siber uzayın tanımı,

3.7 Terör örgütlerinin siber uzaydaki faaliyetleri,

3.8 Siber savaş,

3.9 Siber saldırılar,

3.10 APT saldırılarının siber istihbarat faaliyetleri kapsamında kullanımı,

3.11 Yaşanmış siber istihbarat olayları,

3.12 Balküpü sistemleri ve siber balküpü sistemleri operasyonları,

4. SİBER İSTİHBARATA KARŞI KOYMA

4.1 Siber İKK'nın tanımı,

4.2 İKK ve koruyucu güvenlik,

4.3 Kompartımantasyon ilkesinin siber uzayda kullanımı,

4.4 Siber uzayda iz bırakmadan gezinme ve anonim kalma,

4.5 Sosyal medyadaki tehlikelerden korunma,

4.6 Güvenli ve gizli mesajlaşma,

4.7 Web üzerinden maske hikâye oluşturmak,

4.8 Siber uzayda maske hikâye kullanımı,

4.9 Defansif ve Ofansif Siber İKK metodolojileri,

4.10 İç hukuk tehditleri,

4.11 Siber Kontrterörizm.

5. SİBER GÜVENLİK VE BİLGİ GÜVENLİĞİNE GİRİŞ

5.1 Hacker, hacker türleri ve motivasyonları,

5.2 Deep Web,

5.3 Sızma ve zafiyet analizi testi,

5.4 Sızma testi türleri ve metodolojileri,

5.5 Sızma testi proje yönetimi,

5.6 Sızma testlerinde kullanılan araçlar,

5.7 Sızma testi raporu,

5.8 Siber güvenlik kavramı,

5.9 Siber saldırılar ve kaynakları,

5.10 Bilgi güvenliği kavramı,

5.11 Bilgi güvenliği yönetim sistemi,

5.12 Risk analizi ve yönetimi,

5.13 Güvenlik çözümleri,

5.14 Zararlı yazılımlar,

5.15 Hizmet dışı/dağıtık hizmet dışı bırakma (DoS/DDoS) saldırıları,

5.16 APT (Gelişmiş Siber Tehdit) saldırıları,

5.17 Web uygulama saldırıları,

5.18 Sosyal mühendislik,

5.19 Son Kullanıcı Farkındalığı,

- 5.19.1 Kullanıcı kimlik tespiti,
- 5.19.2 Bilgisayarda donanım ve yazılım değişiklikleri yapma,
- 5.19.3 Dizüstü bilgisayar kullanımı,
- 5.19.4 Yazıcı kullanımı,
- 5.19.5 Taşınabilir medya kullanımı,
- 5.19.6 Zararlı yazılımdan korunma,
- 5.19.7 İnternet erişim güvenliği,
- 5.19.8 E-posta güvenliği,
- 5.19.9 Yedekleme,
- 5.19.10 Dosya erişim ve paylaşımı.

6. HEDEF SİSTEMLER HAKKINDA BİLGİ TOPLAMA

6.1. Hedef sistem hakkında temel bilgi toplama,

6.1.1. Aktif bilgi toplama yöntemleri,

6.1.2. Pasif bilgi toplama yöntemleri,

6.2. Bir IP adresi üzerindeki sitelerin tespit edilmesi,

6.3. Siteye ait geçmiş içeriğin incelenmesi,

6.4. Bir alan adına ait alt alan adlarının tespit edilmesi,

6.5. Hedef alana ait e-posta adreslerinin tespit edilmesi,

6.6. Arama motorlarını kullanarak bilgi toplama,

6.7. Shodan arama motoruyla bilgi toplama,

6.8. Hedefteki güvenlik sistemlerinin tespit edilmesi,

6.9. DNS protokolü ile bilgi toplama,

6.10. DNS Zone transferi kontrolü,

6.11. DNS sunucu sürüm bilgisinin tespit edilmesi,

6.12. SMTP ile iç ağ IP yapısının tespit edilmesi,

6.13. Nmap kullanarak canlı (açık) sistemlerin tespit edilmesi,

6.14. Nmap kullanarak TCP/UDP port taramasının yapılması,

6.15. Nmap ile çalışan servislerin sürümlerinin tespit edilmesi,

6.16. Nmap ile belirli IP aralığındaki belirli port aralığını tarama,

6.17. Sahte IP/tuzak sistemler kullanarak port tarama,

6.18. Nmap'te NSE kullanarak güvenlik açığı tespit etme,

6.19. SYN proxy kullanan sistemlere yönelik port tarama,

6.20. Nmap kullanarak işletim sistemi belirleme,

6.21. Nmap NSE ile SMB dosya paylaşımlarını tespit etmek,

6.22. Nmap GUI/Zenmap kullanarak port tarama,

6.23. Web sunucu bilgilerinin keşfedilmesi,

6.24. Web uygulamasına ait alt dizin ve dosyaların keşfi,

6.25. Hata mesajlarından bilgi toplama,

6.26. Fotoğraflardan bilgi toplama,

6.27. Hepsi bir arada bilgi toplama aracı Maltego kullanımı.

7. OTOMATİK ZAFİYET TARAMA VE DEĞERLENDİRME, PAROLA KIRMA SALDIRILARI

7.1. Otomatik zafiyet tarama yazılımlarının kullanımı,

7.2. Keşfedilen zafiyetlerin değerlendirilmesi,

7.3. Etki alanı sızma testleri,

7.4. Yetki yükseltme yöntemleri,

7.5. Parola kırma saldırıları,

8. AĞ ZEHİRLEME, KABLOSUZ AĞ SALDIRILARI, DDoS, SOSYAL MÜHENDİSLİK SALDIRILARI

8.1. ARP/DNS/DHCP zehirleme,

8.2. Kablosuz ağ kırma,

8.3. Kablosuz ağ güvenliği,

8.4. DoS/DDoS saldırıları ve güvenliği,

8.5. Sosyal mühendislik kavramı,

8.6. Sosyal mühendislik saldırıları.

9. WEB UYGULAMASI VE VERİTABANI İZİNSİZ ERİŞİM VE GÜVENLİK

9.1. Web teknolojileri,

9.2. OWASP,

9.3. En tehlikeli web güvenlik zafiyetleri,

- 9.3.1. SQL Injection,
- 9.3.2. Cross Site Scripting,
- 9.3.3. Cross Site Request Forgery,
- 9.3.4. Local/Remote File Inclusion,
- 9.3.5. Remote Code/Command Injection,
- 9.3.6. Dosya yükleme istismarı,
- 9.3.7. Dosya ve dizin yolları keşfi.

10. GÜVENLİ YAZILIM GELİŞTİRME

10.1. Girdi doğrulamaları,

10.2. Beyaz & Kara liste,

10.3. Oturum yönetimi,

10.4. HTTP Only,

10.5. Güvenli çerez,

10.6. Yetkilendirme.

11. ADLİ BİLİŞİM, SİBER OLAY ANALİZİ, ZARARLI YAZILIM ANALİZİ

11.1. Adli bilişime Giriş,

11.2. Disk/Image Digital Forensics,

11.3. Memory Digital Forensics,

11.4. Siber olaylara müdahale uygulamaları,

11.5. Basit zararlı yazılım analizi,

12. TERSİNE MÜHENDİSLİK

12.1. Tersine mühendislik nedir?

12.1.1. Yazılım tersine mühendisliği,

12.1.2. Reversing uygulamaları,

12.2. Zararlı yazılım,

12.3. Kullanılan şifreleme algoritmaları,

12.4. Düşük seviye yazılımlar (Python),

12.5. Yazılım mimarisi,

12.6. Modüller,

12.7. Veri yönetimi,

12.8. Değişkenler,

12.9. Kullanıcı işlemleri,

12.10. Stack, Heaps,

12.11. Uygulama Programlama Arayüzü,

12.12. Win32 API,

12.13. Win64 API,

12.14. Native API,

12.15. Girdi-Çıktı işlemleri,

12.16. Reversing araçları,

12.17 Çevrimdışı kod analizi,

12.18. Canlı kod analizi,

12.19. Disassemblers,

12.20. IDA Pro,

12.21. ILDasm,

12.22. Hata ayıklayıcılar,

12.22.1. OllyDbg,

12.22.2. Kullanıcı hata ayıklama, WinDbg,

12.23. Çekirdek mod hata ayıklama,

12.24. Sistem izleme yazılımları,

12.25. Çalıştırılabilir dumping araçları,

12.26. Tersine zararlı yazılım,

12.27. Zararlı yazılım türleri,

12.28. Çalıştırılabilir bir dosyayı unpack etme,

12.29. Ağ faaliyet izlenimi,

12.30. IRC kanala katılma süreci,

12.31. Hata ayıklayıcı kullanımı,

12.32. Python ile IDA üzerinde işlemler.

13. GÜVENLİ MOBİL UYGULAMA GELİŞTİRME

13.1. iOS uygulama geliştirme,

13.1.1. Objective C,

13.1.2. Temel yapılar ve kavramlar,

13.1.3. XCode geliştirme ortamı,

13.1.4. Uygulama dizin altyapısı,

13.1.5. Günlük işlemleri,

13.1.6. Hata ayıklama işlemleri,

13.2. Android uygulama geliştirme,

13.2.1 Temel yapılar ve kavramlar,

13.2.2. APK dosya yapısı,

13.2.3. Günlük işlemleri,

13.2.4. Hata ayıklama işlemleri.

14. BİLİŞİM HUKUKU

14.1. 5070 Sayılı Elektronik İmza Kanunu,

14.2. 5237 Sayılı Türk Ceza Kanunu (TCK),

14.3. 5271 Sayılı Ceza Muhakemesi Kanunu (CMK),

14.4. 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,

14.5. 5809 Sayılı Elektronik Haberleşme Kanunu,

14.6. 5846 Sayılı Fikir Ve Sanat Eserleri Kanunu,

14.7. Siber Suçlarla İlgili Uluslararası Alanda Hukuki Düzenlemeler,

14.8. Birleşmiş Milletler'in Siber Suçlarla Mücadelesi,

14.9. Ekonomik İşbirliği ve Kalkınma Örgütü'nün siber suçlarla mücadelesi,

14.10. G-8 ülkelerinin siber suçlarla mücadelesi,

14.11. NATO'nun siber suçlarla mücadelesi,

14.12. Siber güvenlik anlaşmaları,

14.13. Avrupa Konseyi Siber Suçlar Sözleşmesi'nin,

14.14. 6698 Sayılı Kişisel Verilerin Korunması Kanunu,

14.15. Siber Güvenlik Kurulu ve görevleri,

14.16. Sibr güvenlik stratejileri ve eylem planları.

ÖLÇME VE DEĞERLENDİRMEYLE İLGİLİ ESASLAR

1. Değerlendirme, Yaygın Eğitim Kurumları Yönetmeliği esaslarına göre belirlenmelidir.
   - Kursiyerin kendi kendine yaptığı tüm öğrenim faaliyetler,
   - Kursiyerin performansına dayalı olarak gerçekleştirilecek sınavlar,
   - Kursiyere kurs sonunda uygulanan yazılı sınavlar,

   100 puan üzerinden değerlendirilir.

2. Değerlendirme; ders öğretmeni tarafından yazılı, sözlü, uygulamalı sınavlar veya varsa ödev ya da projelere göre yapılır. Birden fazla sınav şekli ile sınavı yapılan dersin puanı veya notu, bu sınavların aritmetik ortalaması ile belirlenir. Bu puan veya not, kursun başarı puan ya da notu olarak değerlendirilir.
3. Programların özelliğine göre sınavlar ve başarı değerlendirmesi bilişim teknolojisi kullanılarak da yapılabilir.
4. Kursiyerlerin sağlık durumları veya bedensel engelleri nedeniyle bazı derslerdeki sınavlar, durumlarına uygun sınav yöntemiyle yapılır.

PROGRAMIN UYGULANMASINDA KULLANILACAK ÖĞRETİM ARAÇ-GEREÇLERİ

1. Ders kitabı olarak, Millî Eğitim Bakanlığının yayınlamış olduğu materyaller kullanılmalıdır.
2. Programın uygulama sürecinde; kaynak ders kitapları, bireysel öğrenme materyalleri ve kaynak ders kitaplarının bulunmaması durumunda öğretmen/öğretici tarafından hazırlanan ders notlarından yararlanılabilir.
3. Programın uygulanabilmesi için Bilişim Teknolojileri alanı standart donanımları ve programın gerektirdiği diğer donanımlar kullanılacaktır. Yararlanılacak araç ve gereçlerden bazıları şunlardır: Bilgisayar donanımları, Internet ortamı, televizyon, VCD, DVD, projeksiyon, kitap, dergi, sunu, film vb. görsel ve işitsel araç gereçlerden yararlanılabilir.

BELGELENDİRME

Kursu başarı ile tamamlayanlara kurs bitirme belgesi düzenlenir.