



Záróvizsga kérdéssor 2025
kibernetika szakirány részére
(nappali)

A tételsor:

- 1) A hacking büntetőjogi minősítésének lehetőségei.
- 2) A malware és túlterheléses támadások büntetőjogi minősítésének lehetőségei.
- 3) Az információs rendszer védelmét biztosító intézkedés kijátszása.
- 4) Személyes adattal visszaélés, a személyes adat és a különleges adat fogalma.
- 5) A kibertérben végrehajtott tiltott adatszerzés büntetőjogi szabályozása.
- 6) Ismertesse a kiberbűnözés elleni fontosabb nemzetközi normákat! (egyezmények, rendeletek, irányelvek).
- 7) Gyermekpornográfia és a gyermekek szexuális kizsákmányolása a kibertérben.
- 8) Az információs rendszer felhasználásával elkövetett csalás büntetőjogi szabályozása és elhatárolása a hagyományos csalástól.
- 9) A pénzmosás büntetőjogi szabályozása a kibertérben.
- 10) Az infokommunikáció és az infokommunikációs technológia fogalma, a kibernetika számára lényeges eszközök.
- 11) Infokommunikációs alapok (digitális, bináris, hexadecimális fogalmak használatuk)
- 12) Személyi számítógépek (asztali/desktop, laptop, tablet) felépítése (logikai felépítés, buszrendszerek, BIOS).
- 13) Adathordozók (memóriák és típusaik, jellemzőik).
- 14) Adathordozók (háttértárak és típusaik, jellemzőik).
- 15) Mobiltelefonok (operációs rendszerek, jellemző csatolók).
- 16) Fájlrendszerek (FAT felépítése és jellemzői, a többi rövid bemutatása).
- 17) Mutassa be a háttértártömbök szerepét, jelentőségét!
- 18) A vezetékes telefonhálózatok és azokból kinyerhető információk. A telefon-alközponti hálózatok és azokból kinyerhető információk.
- 19) A rádióhálózatok (RH, URH) és azokból kinyerhető információk. A műholdas rendszerek és azokból kinyerhető információk.
- 20) A mobiltelefon hálózatok és azokból kinyerhető információk. A mobilinternet hálózatok és azokból kinyerhető információk.
- 21) A felhő alapú rendszerek és azokból kinyerhető információk
- 22) A kibertérben felhasználható információgyűjtő eszközök és azokkal kinyerhető információk.
- 23) Ismertesse a számítógép hálózatok OSI modelljét, illetve az egyes rétegek legfontosabb feladatait!
- 24) Hasonlítsa össze a hálózati réteg összeköttetés alapú, illetve összeköttetés mentes szolgáltatását!
- 25) Milyen forgalomirányító algoritmusokat ismer?
- 26) Mit nevezünk torlódásnak? Hogyan védekezhetünk a torlódással szemben?
- 27) Hogyan épül fel egy IPV4-es cím?

B tételsor:

- 1) Azonosságok és különbségek a csalás és az online csalások elkövetési magatartásaiban.
- 2) A kriptovaluták lefoglalásának lényeges szabályai és ezek alkalmazása a gyakorlatban.
- 3) Milyen lehetőségei vannak a kriptovaluta tranzakciók nyomon követésére a bűnüldöző szervezeteknek? Térjen ki az egyes lehetőségek előnyeire és korlátjaira is!
- 4) Mutassa be a Dante és a Dénes rendszer működését, és szerepüket az online csalások visszaszorításában!
- 5) Mutassa be a készpénz kímélő fizetési rendszereket, és mutassa be a legújabb visszaélési lehetőségeket ezekkel kapcsolatban!
- 6) Mutassa be a magyar bankrendszer működését és a bűnüldöző szervezetekkel való együttműködés lehetőségeit és formáit!
- 7) Milyen főbb elkövetési módjai vannak a kibertérhez kapcsolódóan a pénzmosásnak és melyek a kapcsolódó kriminálmódszerei ajánlások?
- 8) Határozza meg az információbiztonság fogalmát, mutassa be alkalmazási területét! Határolja el az információ és az adat fogalmát!
- 9) Ismertesse a kiberfenyegetéseket és mutassa be röviden azok típusait!
- 10) Határozza meg a kibervédelem és az információbiztonság közötti különbséget!
- 11) Mi vagy ki fenyegetheti az adatot egy szervezeten belül? Határozza meg azokat a szegmenseket, amik hozzájárulnak annak sérülékenységéhez, fenyegetettségéhez!
- 12) Ismertesse a humán kockázatokat az információvédelem területén!
- 13) Mit jelent a gyermekkorúak és fiatalkorúak online szexuális kizsákmányolásának folyamatában a direkt és az indirekt kommunikáció?
- 14) Fejtse ki ismereteit a gyűlöletbeszédéről és az interneten terjedő agresszióról! Térjen ki a szélsőséges viselkedésekre és a radikalizáció felismerésére is!
- 15) Sorolja fel, majd magyarázza el az agresszióra épülő kiberdevianciák elkövetésének megjelenési formáit. Fejtse ki, hogy milyen online elkövetési mintázatokban jelenik meg a kényszerítés, a fenyegetés és megfélemlítés!
- 16) Magyarázza el, hogy mit jelent a flaming és az online karaktergyilkosság! Milyen társadalmi csoportokat érint leggyakrabban, milyen egyéni és társadalmi okok állnak a kriminális jelenség hátterében?
- 17) Milyen módszerekkel és milyen színtereken előzhető meg a gyermekkorúak és fiatalkorúak sérelmére irányuló szexuális online kizsákmányolás?
- 18) Ismertesse a kibertérben működő szervezett bűnözői csoportok jellemzőit (karakterisztikáját)! Mutassa be a lényeges eltéréseket a hagyományos, fizikai térben működő szervezett bűnözői csoportokhoz képest!
- 19) Ismertesse a kibertérben működő bűnözői csoportok Michael McGuire szerinti tipológiáját!
- 20) Mutassa be az IOCTA 2024 jelentésnek lényegesebb elemeit és megállapításait!
- 21) Mit jelent a hacktivizmus? Melyek a céljai, módszerei? Mutassa be a hacktivizmus korai időszakainak jellemzőit, a kiemelkedő hacktivisták projekteit, a hacktivizmus jogi megítélésért! Milyen összefüggés lehet a hacktivisták csoportok és az állami/titkosszolgálati szereplők között?
- 22) Ismertesse a surface, deep- és dark web jellemzőit, és az ezek közötti különbségeket, valamint a dark webhez történő hozzáférés fő kritériumait, és indokolja ezek alkalmazásának szükségességét!
- 23) Ismertesse a TOR project böngésző fő jellemzőit, mutassa be és részletezze a dark weben működő szervezett bűnözői csoportok sztenderdizált szervezeti szerepköreit!
- 24) Mutassa be a ransomware (zsarolóvírusok) támadások jellemzőit, bűnözők általi felhasználási területeit és a körforgását!

C tételsor (gyakorlati feladatok, számítógép használatával)

- 1) Futó Windows konfigurációban készítsen igazságügyi fizikai másolatot a vizsgáló által meghatározott állományra! Jelölje a jegyzőkönyvben szerepeltetni szükséges adatokat!
- 2) Triage program segítségével hozzon döntést arról, hogy a vizsgáló által rendelkezésre bocsátott számítógép kikapcsolható-e, vagy sem! Indokolja döntését és ismertesse, hogy milyen eljárást szükséges használni az adatok lefoglalásához!
- 3) Hajtson végre helyszíni digitális nyomrögzítési feladatot Triage program segítségével! Az eljárási cselekmény célja a vizsgáló által rendelkezésre bocsátott számítógépből kriptotárca privát kulcsának felkutatása.
- 4) Vizsgáló által megküldött email a vizsgáló rendelkezésre áll. Azonosítsa be és szabályszerűen rögzítse azokat a bűnyüggel releváns digitális nyomokat, amelyek egy BEC elkövetőjéhez elvezethetnek.
- 5) Vizsgáló által megküldött email a vizsgáló rendelkezésre áll. Az alábbi vizsgálati adatokat rögzítse egy adattáblában a későbbi feldolgozás érdekében:
 - email hitelesítő kulcs;
 - kézbesítési állapot útvonala;
 - üzenet azonosító;
 - kézbesítési információk elemzési eredménye.
- 6) A hallgató a PC munkaállomásán hozzon létre egy OSINT Level-1 eszközkészletet/munkakörnyezetet általa szabadon választott szoftver vagy egyéb megoldásokból az alábbi korlátozásokkal:
 - csak free vagy open source szoftver tölthető le amennyiben szükséges;
 - URL linkgyűjtemény egy dokumentumba rendezve vagy vágólapon nem elfogadott;
 - az információgyűjtés anonimizált és nem detektálható módon történhet;
 - legalább 7 komponensből álljon a kialakított eszközkészlet.
- 7) Vizsgáló által meghatározott Facebook profil kapcsolati adatait mentse le további kapcsolati adatelemzésre alkalmas módon!
- 8) A hallgató az e-mail fiókjába küldött URL linket vizsgálja meg az IT biztonsági rendszabályok betartásával. Az alábbi vizsgálati adatokat rögzítse egy adattáblában a későbbi feldolgozás érdekében:
 - vizsgálat találati arány,
 - SSL tanúsítvány,
 - fejlécben megjelölt szerver,
 - webrobot/bot szabályok vagy fenyegetettség,
 - HTTP fejléc kivonat,
 - archívum kimutatás.
- 9) A vizsgáló által rendelkezésre bocsátott képfájlokról hajtson végre elemzést az alábbi szempontok szerint:
 - minden elérhető adatot adjon meg a képről exportálva;
 - csak a bűnyüggel elemzés biztonsági rendszabályainak betartásával kinyert adat elemezhető-értékelhető;
 - a képek metaadatait dolgozza fel és a feladathoz rendelt adatállományban mutasson ki adatkapcsolatot;
 - a képek geolokációs adatait ábrázolja általa szabadon választott alkalmazásban.
- 10) Vizsgáló által rendelkezésre bocsátott "elkövetői" laptopon vizsgálja meg, hogy található-e dark web használatára utaló digitális nyom! Amennyiben igen, azt határolja be pontosan és a szemle jegyzőkönyvben dokumentálja!

- 11)A vizsgáztató által rendelkezésre bocsátott bekapcsolt mobiltelefon készüléket foglalja le szakszerűen a bizonyítékok integritásának fenntartásával! Az eljárást jegyzőkönyvezzé!
- 12)A vizsgáztató által átadott igazságügyi másolatból (lemezkép fájl) kíséreljen meg törölt képfájlokat helyreállítani és találat esetén elemezze azok metaadatait!
- 13)A vizsgáztató által átadott igazságügyi másolatból (lemezkép fájl) kísérelje meg a vizsgáztató által megadott hash függvény értékkel rendelkező fájlokat felkutatni!
- 14)Formázott külső adathordozó vizsgálatával (FTK Imager segítségével) igazolja vagy zárja ki, hogy a vizsgáztató által átadott fájlt tartalmazta-e az adathordozó!
- 15)Helyszíni kutatás során felkutatott kriptotárca privát kulcs alapján ellenőrizze, hogy az tartalmaz-e kriptovalutát! Amennyiben igen, akkor gondoskodjon annak biztosításáról!

