

Kaspersky Anti-Virus 2012

**KASPERSKY** **Anti-Virus**

Felhasználói útmutató

ALKALMAZÁS VERZIÓJA: 12.0

Tisztelt Felhasználó!

Köszönjük, hogy termékünket választotta. Reméljük, hogy ez a dokumentáció hasznos lesz az Ön számára és választ ad az esetlegesen felmerült kérdései nagy részére.

Figyelmeztetés! Jelen dokumentum a Kaspersky Lab ZAO (a továbbiakban Kaspersky Lab) tulajdona: a dokumentum szerzői jogaira Oroszország szerzői jogi törvényei és nemzetközi megállapodások is vonatkoznak. A dokumentum vagy annak részeinek illegális másolása vagy terjesztése a hatályos törvények szerinti polgári, közigazgatási vagy büntetőjogi felelősségre vonást eredményezhet.

Az anyagok, beleértve a fordításokat is, sokszorosítása és terjesztése csak a Kaspersky Lab írásbeli hozzájárulásával végezhető.

A jelen dokumentum és a kapcsolódó ábrák kizárólag saját vagy tájékoztató – és nem kereskedelmi – célra használhatók fel.

A dokumentum előzetes értesítés nélkül módosulhat. A jelen dokumentum legújabb változata a Kaspersky Lab webhelyén, a <http://www.kaspersky.com/docs> címen tekinthető meg.

A Kaspersky Lab sem a dokumentumban található olyan anyagok tartalmáért, minőségéért, releváns voltáért és pontosságáért, amelyek jogait egy harmadik fél birtokolja, sem az ilyen dokumentumok használatából eredő esetleges károkért nem vállal felelősséget.

A jelen dokumentumban olyan bejegyzett védjegyek és szolgáltatási nevek szerepelnek, amelyek az illető tulajdonos tulajdonát képezik.

Dokumentum átdolgozásának dátuma: 2011.04.19

© 1997-2011 Kaspersky Lab ZAO. Minden jog fenntartva.

<http://www.kaspersky.hu>  
<http://support.kaspersky.com>

# TARTALOM

AZ ÚTMUTATÓRÓL .....	8
Ebben a dokumentumban.....	8
Egyezményes jelölések a dokumentumban.....	9
AZ ALKALMAZÁSSAL KAPCSOLATOS INFORMÁCIÓFORRÁSOK.....	11
Információforrások önálló kutatáshoz .....	11
A Kaspersky Lab alkalmazásainak fóruma .....	12
A kereskedelmi osztály elérhetősége .....	12
A Dokumentációfejlesztő csoport email elérhetősége .....	12
KASPERSKY ANTI-VIRUS .....	13
Újdonságok.....	13
Forgalmazási készlet.....	13
Regisztrált felhasználók számára biztosított szolgáltatások .....	14
Hardveres és szoftveres rendszerkövetelmények .....	14
AZ ALKALMAZÁS TELEPÍTÉSE ÉS ELTÁVOLÍTÁSA .....	15
Normál telepítési eljárás .....	15
1. lépés: Az alkalmazás új változatának keresése .....	16
2. lépés: Annak ellenőrzése, hogy a rendszer megfelel-e a telepítés követelményeinek.....	16
3. lépés: A telepítés típusának kiválasztása.....	16
4. lépés: A licencszerződés megtekintése .....	16
5. lépés: A Kaspersky Security Network adatgyűjtési nyilatkozat .....	16
6. lépés: Inkompatibilis alkalmazások keresése.....	17
7. lépés: A célmappa kiválasztása .....	17
8. lépés: A telepítés előkészítése.....	17
9. lépés: Telepítés.....	18
10. lépés: A telepítés befejezése .....	18
11. lépés: Alkalmazás aktiválása .....	18
12. lépés: Felhasználó regisztrálása .....	18
13. lépés: Az aktiválás befejezése .....	19
A Kaspersky Anti-Virus korábbi verziójának frissítése .....	19
1. lépés: Az alkalmazás új változatának keresése .....	19
2. lépés: Annak ellenőrzése, hogy a rendszer megfelel-e a telepítés követelményeinek.....	20
3. lépés: A telepítés típusának kiválasztása.....	20
4. lépés: A licencszerződés megtekintése .....	20
5. lépés: A Kaspersky Security Network adatgyűjtési nyilatkozat .....	20
6. lépés: Inkompatibilis alkalmazások keresése.....	21
7. lépés: A célmappa kiválasztása .....	21
8. lépés: A telepítés előkészítése.....	21
9. lépés: Telepítés.....	22
10. lépés: A varázsló bezárása .....	22
Nem szabványos telepítések .....	22
Első lépések .....	23
Az alkalmazás eltávolítása .....	23
1. lépés: Adatok mentése ismételt használathoz .....	23
2. lépés: Az alkalmazás eltávolításának megerősítése .....	23
3. lépés: Alkalmazás eltávolítása. Eltávolítás befejezése .....	24
AZ ALKALMAZÁS LICENCELÉSE .....	25
A végfelhasználói licencszerződésről .....	25
Az adatok feletti rendelkezés .....	25
A licenc.....	25
Az aktiváló kód .....	26

ALKALMAZÁS FELÜLETE.....	27
Az értesítési terület ikonja.....	27
A helyi menü.....	28
A Kaspersky Anti-Virus főablaka .....	29
Értesítési ablakok és felugró üzenetek .....	30
Az alkalmazás beállítási ablaka.....	31
A Kaspersky Gadget.....	32
Hírügynök .....	33
AZ ALKALMAZÁS ELINDÍTÁSA ÉS LEÁLLÍTÁSA .....	34
Az automatikus indítás engedélyezése és letiltása.....	34
Az alkalmazás kézi elindítása és leállítása .....	34
A SZÁMÍTÓGÉP VÉDELME NEK KEZELÉSE .....	35
A számítógép védelmével kapcsolatos problémák diagnosztizálása és megszüntetése.....	35
A védelem engedélyezése és letiltása.....	36
Védelem felfüggesztése és folytatása .....	37
TIPIKUS FELADATOK MEGOLDÁSA .....	38
Az alkalmazás aktiválásának módja .....	38
Licenc vásárlása vagy megújítása.....	39
Teendők az alkalmazás által megjelenített értesítésekkel .....	40
Az alkalmazás adatbázisainak és alkalmazásmóduljainak frissítése.....	40
Vírusok keresése a számítógép kritikus részein.....	40
Objektum (fájl, mappa, meghajtó) vírusellenőrzése.....	41
Vírusok keresése a számítógépen teljes vizsgálattal .....	42
Számítógép sebezhetőségének vizsgálata.....	42
Személyi adatok eltulajdonítás elleni védelme .....	43
Védelem adathalászat ellen.....	43
Védelem a billentyűzeten bevitt adatok elfogása ellen.....	43
Teendők vírus által fertőzöttnek vélt objektummal.....	44
Teendők vírus által fertőzöttnek vélt számítógéppel.....	45
Az alkalmazás által törölt vagy vírusmentesített fájl visszaállítása .....	46
Helyreállító-lemez létrehozása és használata .....	46
Helyreállító-lemez létrehozása.....	47
A számítógép indítása helyreállító-lemezről.....	49
Az alkalmazás működéséről szóló jelentés megtekintése .....	49
Az alkalmazás alapértelmezett beállításainak visszaállítása .....	49
A beállítások átvitele egy másik számítógépre telepített Kaspersky Anti-Virus alkalmazásba .....	50
Átkapcsolás a Kaspersky Anti-Virus alkalmazásról Kaspersky Internet Security alkalmazásra.....	51
Átkapcsolás a kereskedelmi változatra .....	51
Ideiglenes átkapcsolás a próbaverzióra.....	52
A Kaspersky Gadget használata .....	53
Alkalmazás reputációjának ellenőrzése.....	54
AZ ALKALMAZÁS SPECIÁLIS BEÁLLÍTÁSAI .....	55
Általános védelmi beállítások .....	55
A Kaspersky Anti-Virus elérésének korlátozása.....	56
Védelmi mód kiválasztása.....	56
Vizsgálat .....	56
Víruskeresés .....	57
Sebezhetőségi vizsgálat .....	63
Vizsgálati feladatok kezelése. Feladatkezelő.....	63
Frissítés.....	63
Frissítésforrás kiválasztása.....	64
Frissítés indítási ütemezésének létrehozása .....	66
Legutolsó frissítés visszagörgetése .....	66
Frissítések futtatása másik felhasználói fiókból .....	67
Proxy kiszolgáló használata.....	67

Fájl víruskereső .....	67
A Fájl víruskereső engedélyezése és letiltása .....	68
A Fájl víruskereső automatikus felfüggesztése .....	68
A Fájl víruskereső védelmi hatókörének létrehozása .....	69
Fájl biztonsági szint megváltoztatása és visszaállítása .....	70
Vizsgálati mód kiválasztása .....	70
Heurisztikus elemzés alkalmazása a Fájl víruskereső működése során .....	71
Fájlvizsgálati technológia kiválasztása .....	71
A fertőzött fájlokon végrehajtandó művelet módosítása .....	71
Összetett fájlok vizsgálata a Fájl víruskeresővel .....	71
Fájlvizsgálat optimalizálása .....	72
Levél víruskereső .....	72
A Levél víruskereső engedélyezése és letiltása .....	74
A Levél víruskereső védelmi hatókörének létrehozása .....	74
Email biztonsági szint megváltoztatása és visszaállítása .....	74
Heurisztikus elemzés alkalmazása a Levél víruskereső működése során .....	75
A fertőzött email üzeneteken végrehajtandó művelet módosítása .....	75
Mellékletek szűrése az email üzenetekben .....	75
Összetett fájlok vizsgálata a Levél víruskeresővel .....	76
Email vizsgálata a Microsoft Office Outlook programban .....	76
Email vizsgálata a The Bat! programban .....	76
Webes víruskereső .....	77
A Webes víruskereső engedélyezése és letiltása .....	78
A webes forgalom biztonsági szintjének megváltoztatása és visszaállítása .....	78
A webes forgalomban észlelt veszélyes objektumokon végrehajtandó művelet módosítása .....	79
URL-ek ellenőrzése a weboldalon .....	79
Heurisztikus elemzés alkalmazása a Webes víruskereső működése során .....	81
Veszélyes parancsfájlok blokkolása .....	81
Vizsgálatoptimalizáció .....	81
Megbízható címek listájának létrehozása .....	82
IM víruskereső .....	82
Az IM víruskereső engedélyezése és letiltása .....	83
IM víruskereső védelmi hatókörének létrehozása .....	83
URL-ek ellenőrzése az IM kliensekből érkező üzenetekben .....	83
Heurisztikus elemzés alkalmazása az IM víruskereső működése során .....	83
Proaktív védelem .....	84
A Proaktív védelem engedélyezése és letiltása .....	84
Megbízható alkalmazások csoportjának létrehozása .....	84
Veszélyes tevékenységek listájának használata .....	85
Alkalmazás veszélyes tevékenységére indított művelet módosítása .....	85
Rendszerfigyelő .....	85
A Rendszerfigyelő engedélyezése és letiltása .....	86
Veszélyes tevékenység mintázatának a használata (BSS) .....	86
Rosszindulatú programok által végzett műveletek visszagörgetése .....	86
Hálózati védelem .....	87
Titkosított kapcsolatok vizsgálata .....	87
A proxykiszolgáló beállítása .....	89
Figyelt portok listájának létrehozása .....	89
Megbízható zóna .....	90
Megbízható alkalmazások listájának létrehozása .....	91
Kizárási szabályok létrehozása .....	91
Teljesítmény és más alkalmazásokkal való kompatibilitás .....	92
Az észlelhető fenyegetéskategóriák kiválasztása .....	92
Energiatakarékosság .....	92
Fejlett vírusmentesítés .....	93
A számítógép erőforrásainak elosztása vírusellenőrzéskor .....	93

Feladatok futtatása a háttérben .....	93
Teljes képernyős mód. Játék profil.....	94
A Kaspersky Anti-Virus önvédelme .....	95
Az önvédelem engedélyezése és letiltása .....	95
Külső szolgáltatásvezérlés tiltása .....	95
Karantén és másolatok.....	95
Fájlok tárolása a karanténban és a másolattárolóban.....	96
Műveletek a karanténba helyezett fájlokkal .....	96
Műveletek a Másolattárolóban található objektumokkal .....	97
Karanténba helyezett fájlok vizsgálata frissítés után.....	98
További eszközök a számítógép jobb védelméhez .....	98
Személyes adatok törlése.....	99
Böngészőbeállítás biztonságos munkához .....	100
A varázslók által végzett módosítások visszagörgetése .....	101
Jelentések .....	102
Jelentés létrehozása a kijelölt védelmi összetevőhöz .....	102
Adatszűrés.....	103
Események keresése.....	103
Jelentés mentése fájlba .....	104
Jelentések tárolása .....	104
Az alkalmazás jelentéseinek törlése .....	104
Nem kritikus események rögzítése a jelentésbe .....	105
Jelentésértesítések konfigurálása.....	105
Az alkalmazás megjelenése. Aktív kezelőfelület-elemek kezelése.....	105
Értesítési ablakok átlátszósága.....	105
Az értesítési területen megjelenő alkalmazás ikon animációja .....	105
Szöveg a Microsoft Windows bejelentkezési képernyőjén .....	106
Értesítések.....	106
Értesítések engedélyezése és tiltása .....	106
Az értesítés módjának konfigurálása .....	107
Hírszolgáltatás letiltása .....	107
Kaspersky Security Network.....	107
A Kaspersky Security Networkben való részvétel engedélyezése és letiltása .....	108
A Kaspersky Security Networktel létrehozott kapcsolat ellenőrzése .....	108
AZ ALKALMAZÁS MŰKÖDÉSÉNEK TESZTELÉSE .....	109
Az EICAR tesztfájl .....	109
A z alkalmazás működésének ellenőrzése az EICAR tesztfájllal.....	109
Az EICAR tesztfájl típusai.....	110
KAPCSOLATFELVÉTEL A TERMÉKTÁMOGATÁSI SZOLGÁLTATÁSSAL .....	112
Terméktámogatás igénylése.....	112
A nyomkövető fájl és az AVZ parancsfájl segítségével .....	112
Jelentés készítése a rendszer állapotáról .....	113
Nyomkövetési fájl létrehozása .....	113
Adatfájlok küldése.....	113
AVZ parancsfájl végrehajtása .....	114
Terméktámogatás telefonon .....	114
Terméktámogatás igénylése a Saját Kaspersky fiókon keresztül .....	115
FÜGGELÉK.....	116
Az alkalmazás használata parancssorból.....	116
Alkalmazás aktiválása.....	117
Alkalmazás elindítása .....	117
Alkalmazás leállítása .....	117
Alkalmazás-összetevők és feladatok kezelése .....	118
Víruskeresés .....	119
Az alkalmazás frissítése.....	121

Legutolsó frissítés visszagörgetése .....	122
Védelmi beállítások exportálása .....	122
Védelmi beállítások importálása .....	122
Nyomkövetési fájl létrehozása .....	123
A Sűgó megtekintése .....	123
A parancssori felület visszatérési kódjai .....	124
Kaspersky Anti-Virus értesítések listája.....	125
Értesítések minden védelmi üzemmódban .....	125
Értesítések interaktív védelmi üzemmódban.....	129
SZÓJEGYZÉK .....	136
KASPERSKY LAB ZAO .....	145
A HARMADIK FÉLTŐL SZÁRMAZÓ KÓDRA VONATKOZÓ INFORMÁCIÓK .....	146
TÁRGYMUTATÓ.....	147

# AZ ÚTMUTATÓRÓL

Üdvözlük Önt a Kaspersky Lab szakemberei!

Ez az útmutató a Kaspersky Anti-Virus telepítését, beállítását és használatát mutatja be. Reméljük, hogy az útmutató információi segítenek abban, hogy az alkalmazással a maximális kényelemmel dolgozhasson.

Az útmutató célja:

- segít telepíteni, aktiválni és a használni a Kaspersky Anti-Virus alkalmazást;
- biztosítani az alkalmazással kapcsolatos kérdésekre vonatkozó információk gyors kereshetőségét;
- további információforrásokat adni az alkalmazáshoz és a Terméktámogatással való együttműködéshez.

Az alkalmazás megfelelő használatához rendelkeznie kell az alapvető számítógéphasználati ismeretekkel: ismernie kell a használt operációs rendszer kezelőfelületét, tudnia kell használni a rendszerre jellemző legfontosabb technikákat, az emailt és az internetet.

## EBBEN A RÉSZBEN:

Ebben a dokumentumban .....	<a href="#">8</a>
Egyezményes jelölések a dokumentumban .....	<a href="#">9</a>

## EBBEN A DOKUMENTUMBAN

Ez az útmutató az alábbi részekből áll.

### Az alkalmazással kapcsolatos információforrások

Ez a rész az alkalmazással kapcsolatos információforrásokat ismerteti, valamint felsorolja azokat a webhelyeket, ahol megvitathatja másokkal az alkalmazás működését.

### Kaspersky Anti-Virus

Ez a rész az alkalmazás funkcióit írja le, és rövid áttekintést nyújt az alkalmazás funkcióiról és összetevőiről. Megtudhatja, mely elemek vannak a forgalmazási csomagban és mely szolgáltatások érhetők el az alkalmazás regisztrált felhasználói számára. Ez a rész információkat tartalmaz a számítógépnek az alkalmazás telepítéséhez szükséges szoftveres és hardveres követelményeiről.

### Az alkalmazás telepítése és eltávolítása

Ez a rész tájékoztatást nyújt arról, hogyan kell telepíteni az alkalmazást a számítógépre, és hogyan távolítsa el azt.

### Az alkalmazás licencelése

Ez a rész tájékoztatást nyújt az alkalmazás aktiválásával kapcsolatos általános feltételekről. Olvassa el ezt a részt, hogy többet megtudjon a licencszerződés céljáról, a licenc típusairól, az alkalmazás aktiválási módjairól és a licenc megújításáról.

### Alkalmazás felülete

Ez a rész tájékoztatást nyújt az alkalmazás grafikus felületének alapvető elemeiről: az alkalmazás ikonjairól és az alkalmazás ikonjainak helyi menüjéről, a főablakról, a beállítási ablakról és az értesítési ablakokról.

### Az alkalmazás elindítása és leállítása

Ebben a részben az alkalmazás indításával és leállításával kapcsolatosan található információk.

## A számítógép védelmének kezelése

Ez a rész tájékoztatást nyújt a számítógép biztonságát veszélyeztető fenyegetések felismeréséről és a biztonsági szint beállításáról. Olvassa el ezt a részt, hogy többet megtudjon a védelem engedélyezéséről, letiltásáról és felfüggesztéséről az alkalmazás használata során.

## Tipikus feladatok megoldása

Ez a rész tájékoztatást nyújt arról, hogyan lehet megoldani a számítógép védelmével kapcsolatos leggyakoribb problémákat az alkalmazás segítségével.

## Az alkalmazás speciális beállításai

Ebben a részben az alkalmazás egyes összetevőinek beállítási módjairól talál részletes információkat.

## Az alkalmazás működésének tesztelése

Ez a fejezet azt mutatja be, miként ellenőrizhető, hogy az alkalmazás észleli a vírusokat és változataikat, és a megfelelő műveleteket végzi rajtuk.

## Kapcsolatfelvétel a terméktámogatási szolgáltatással

Ez a rész tájékoztatást nyújt arról, hogyan léphet kapcsolatba a Kaspersky Lab terméktámogatási szolgáltatásával.

## Függelék

Ebben a részben a dokumentum szövegét kiegészítő információk találhatók.

## Szójegyzék

Ez a rész a dokumentumban használt kifejezéseket és azok magyarázatát tartalmazza.

## Kaspersky Lab ZAO

Ez a rész a Kaspersky Labre vonatkozó információkat tartalmaz.

## A harmadik féltől származó kódra vonatkozó információk

Ez a rész tájékoztatást nyújt az alkalmazásban használt, harmadik féltől származó kódról.

## Tárgymutató

Ennek a résznek a segítségével gyorsan megtalálja a szükséges információkat a dokumentumon belül.

# EGYEZMÉNYES JELÖLÉSEK A DOKUMENTUMBAN

Az itt olvasható szöveget szemantikai elemek, figyelmeztetések, tippek és példák egészítik ki, amelyeket ajánlott alaposan elolvasni.

A szemantikai elemek kiemeléséhez egyezményes jelölések kerültek alkalmazásra. Az alábbi táblázat az egyezményes jelöléseket és használati példákat mutat.

1. táblázat. Egyezményes jelölések a dokumentumban

MINTASZÖVEG	EGYEZMÉNYES JELÖLÉSEK LEÍRÁSA
Megjegyezzük, hogy...	A figyelmeztetések piros színnel és bekeretezve láthatók. A figyelmeztetések olyan lehetséges szándékolatlan műveletekről nyújtanak információkat, amelyek adatvesztéshez, vagy a számítógép hibás működéséhez vezethetnek.
Javasolt a használata...	A megjegyzések be vannak keretezve. A megjegyzések tartalmazhatnak hasznos tippet, javaslatokat, adott értékeket, vagy az alkalmazás működésének fontosabb okait.

MINTASZÖVEG	EGYEZMÉNYES JELÖLÉSEK LEÍRÁSA
<b><u>Például:</u></b> ...	A példák sárga háttérrel kiemelt részekben jelennek meg, a Példa fejléc alatt.
<i>Frissítés – ez a...</i> <i>Az adatbázisok nem naprakészek</i> <i>esemény történik.</i>	Az alábbi szemantikai elemek a szövegben dőlt betűvel jelennek meg: <ul style="list-style-type: none"> <li>• új kifejezések;</li> <li>• alkalmazásállapotok és események nevei.</li> </ul>
Nyomja meg az <b>ENTER</b> gombot. Nyomja meg az <b>ALT+F4</b> billentyűkombinációt.	A billentyűzet gombjai félkövér betűkkel, nagybetűs formátumban szerepelnek a szövegben. A billentyűk nevének „plusz” („+”) szimbólummal való összekapcsolása a billentyűk kombinációját jelenti. Ezeket a billentyűket egyszerre kell megnyomni.
Kattintson az <b>Engedélyezés</b> gombra.	Az alkalmazás interfész elemeinek, például beviteli mezők, menüpontok és gombok nevei félkövér betűtípussal jelennek meg.
➡ <i>Feladat ütemezésének beállítása:</i>	Az utasítások bevezető kifejezései dőlt betűkkel vannak írva, és nyíl is jelöli őket.
Gépelje be a parancssorba a <code>help</code> kifejezést. Ekkor a következő üzenet jelenik meg: Specify the date in dd:mm:yy format (Adja meg a dátumot nn:hh:éé formátumban).	Az alábbi szövegtípusok jelennek meg speciális fontkészlettel: <ul style="list-style-type: none"> <li>• a parancssor szövege;</li> <li>• az alkalmazás által a képernyőn megjelenített üzenetek szövege;</li> <li>• adatok, melyeket a felhasználónak kell bevinnie.</li> </ul>
<A számítógép IP-címe>	A változók szögletes zárójelbe vannak írva. A változó helyett annak tényleges értékét kell beírni, a szögletes zárójelet pedig el kell hagyni.

# AZ ALKALMAZÁSSAL KAPCSOLATOS INFORMÁCIÓFORRÁSOK

Ez a rész az alkalmazással kapcsolatos információforrásokat ismerteti, valamint felsorolja azokat a webhelyeket, ahol megvitathatja másokkal az alkalmazás működését.

A kérdés fontosságának és sürgősségének függvényében kiválaszthatja a legmegfelelőbb információforrást.

## EBBEN A RÉSZBEN:

Információforrások önálló kutatáshoz.....	<a href="#">11</a>
A Kaspersky Lab alkalmazásainak fóruma.....	<a href="#">12</a>
A kereskedelmi osztály elérhetősége.....	<a href="#">12</a>
A Dokumentációfejlesztő csoport email elérhetősége.....	<a href="#">12</a>

## INFORMÁCIÓFORRÁSOK ÖNÁLLÓ KUTATÁSHOZ

Az alkalmazással kapcsolatban a következő forrásokból tájékozódhat:

- az alkalmazás weboldala a Kaspersky Lab webhelyén;
- az alkalmazás weboldala a Terméktámogatási szolgáltatás webhelyén (Tudásbázis);
- online súgó;
- a dokumentáció.

Ha egyedül nem tudja megoldani a felmerült problémát, javasoljuk, hogy lépjen kapcsolatba a Kaspersky Lab Terméktámogatási szolgáltatással (lásd: „Terméktámogatási szolgáltatás telefonon”, [114.](#) oldal).

A Kaspersky Lab webhelyén található információforrások használatához internetkapcsolat szükséges.

### Az alkalmazás weboldala a Kaspersky Lab webhelyén

A Kaspersky Lab webhelyén minden alkalmazáshoz külön oldal tartozik.

Ezek az oldalakon ([http://www.kaspersky.hu/termekek/kaspersky\\_anti-virus.html](http://www.kaspersky.hu/termekek/kaspersky_anti-virus.html)) általános információkat találhat az alkalmazásokról, azok funkcióiról és beállításairól.

A <http://www.kaspersky.hu> oldal egy az eStore-ra mutató URL-t is tartalmaz. Ott megvásárolhatja vagy megújíthatja az alkalmazást.

### Az alkalmazás weboldala a Terméktámogatási szolgáltatás webhelyén (Tudásbázis)

A Tudásbázisa Terméktámogatás Szolgáltatás webhely része, amely javaslatokat tartalmaz arra vonatkozóan, hogyan kell használni a Kaspersky Lab alkalmazásait. A Tudásbázis témák szerint csoportosítva tartalmazza a referenciacikkeket.

Az alkalmazás Tudásbázisban megtalálható oldalán (<http://support.kaspersky.com/kav2012>) olyan cikkeket olvashat, melyekben hasznos információkat, tanácsokat és a gyakran ismételt kérdésekre adott válaszokat talál az alkalmazás vásárlásával, telepítésével és használatával kapcsolatban.

A cikkekben olyan kérdésekre is választ találhat, amelyek kívül esnek a Kaspersky Anti-Virus hatókörén, és más Kaspersky Lab alkalmazásokra vonatkoznak. Emellett a Terméktámogatási szolgáltatás híreit is tartalmazhatják.

### Online súgó

Az alkalmazás online súgóját súgófájlok alkotják.

A helyi súgó információkat tartalmaz az alkalmazás egyes ablakairól, felsorolja és leírja a megfelelő beállításokat és feladatokat.

A teljes súgó részletes információkat nyújt a számítógép védelmének kezeléséről az alkalmazás segítségével.

### Dokumentáció

Az alkalmazás felhasználó útmutatója az alkalmazás telepítéséről, aktiválásáról és konfigurálásáról tartalmaz információkat, valamint az alkalmazás működési adatairól is. A dokumentum bemutatja az alkalmazás felhasználói felületét is, és megmutatja, hogyan végezhető el az alkalmazás használatakor felmerülő tipikus felhasználói feladatok.

## A KASPERSKY LAB ALKALMAZÁSAINAK FÓRUMA

Ha kérdése nem igényel azonnali választ, megbeszélheti azt a Kaspersky Lab szakértőivel és más felhasználókkal is a Fórum webhelyén (<http://forum.kaspersky.com>).

Ezen a fórumon izgalmas témákról olvashat, megjegyzéseket fűzhet a beszélgetésekhez és létrehozhat új témát.

## A KERESKEDELMI OSZTÁLY ELÉRHETŐSÉGE

Ha bármilyen kérdése van az alkalmazás kiválasztására, beszerzésére, illetve megújítására vonatkozóan, vegye fel a kapcsolatot az értékesítési osztály szakembereivel a következő módon:

- Hívja fel telefonon a moszkvai központunkat (<http://www.kaspersky.com/contacts>).
- Küldje el kérdését a [sales@kaspersky.com](mailto:sales@kaspersky.com) címre.

A szolgáltatás orosz és angol nyelvű.

## A DOKUMENTÁCIÓFEJLESZTŐ CSOPORT EMAIL ELÉRHETŐSÉGE

Ha fel szeretné venni a kapcsolatot a Dokumentációfejlesztő csoporttal, küldjön egy emailt a to [docfeedback@kaspersky.com](mailto:docfeedback@kaspersky.com) címre. Az üzenet tárgya a „Kaspersky Help Feedback: Kaspersky Anti-Virus” legyen.

# KASPERSKY ANTI-VIRUS

Ez a rész az alkalmazás funkcióit írja le, és rövid áttekintést nyújt az alkalmazás funkcióiról és összetevőiről. Megtudhatja, mely elemek vannak a forgalmazási csomagban és mely szolgáltatások érhetők el az alkalmazás regisztrált felhasználói számára. Ez a rész információkat tartalmaz a számítógépnek az alkalmazás telepítéséhez szükséges szoftveres és hardveres követelményeiről.

## EBBEN A RÉSZBEN:

Újdonságok .....	13
Forgalmazási készlet.....	13
Regisztrált felhasználók számára biztosított szolgáltatások.....	14
Hardveres és szoftveres rendszerkövetelmények .....	14

## ÚJDONSÁGOK

A Kaspersky Anti-Virus az alábbi új funkciókkal rendelkezik:

- A Kaspersky Anti-Virus főablakának továbbfejlesztett felülete gyors hozzáférést biztosít az alkalmazás funkcióihoz.
- Jobb lett a Karantén és másolatok (lásd [95.](#) oldal) működése: a két funkció két külön lapra lett szétválasztva, melyek saját hatókörrel rendelkeznek.
- Bekerült a csomagba a Feladatkezelő, ami leegyszerűsíti a feladatok kezelését a Kaspersky Anti-Virus-ban (lásd: „Vizsgálati feladatok kezelése. Feladatkezelő”, [63.](#) oldal).
- A Kaspersky Security Networkben (lásd [107.](#) oldal) való részvétel lehetővé teszi az alkalmazások és webhelyek reputációjának azonosítását a többi felhasználótól a világ minden részéből kapott adatok alapján.
- Ha a Webes víruskereső be van kapcsolva, külön engedélyezheti a heurisztikus elemzést a weboldalak adathalászati vizsgálatára (lásd: „Heurisztikus elemzés alkalmazása a Webes víruskereső működése során”, [81.](#) oldal). Az oldalak adathalászati ellenőrzésekor a heurisztikus elemzés attól függetlenül megtörténik, hogy a funkció be van kapcsolva a Webes víruskeresőben vagy sem.
- A Kaspersky Gadget új megjelenést kapott (lásd [32.](#) oldal).

## FORGALMAZÁSI KÉSZLET

Az alkalmazást az alábbi módokon vásárolhatja meg:

- **Dobozban.** Partnereink üzleteiben kerül forgalomba.
- **Az online áruházban.** A Kaspersky Lab online áruházában (például a <http://www.kaspersky.hu> weboldal eStore részében), vagy a partnervállalatok online áruházában kerül forgalomba.

Ha az alkalmazás dobozos verzióját vásárolja meg, az értékesítési csomag a következő elemeket tartalmazza:

- lezárt borítékban lévő telepítő CD, amely az alkalmazás és dokumentáció fájljait tartalmazza;
- rövid felhasználói útmutató egy aktiváló kóddal;
- licencszerződés, amely leírja azokat a feltételeket, amelyek szerint az alkalmazást használhatja.

Az értékesítési csomag tartalma az alkalmazás terjesztési régiójától függően eltérő lehet.

Ha a Kaspersky Anti-Virus alkalmazást egy online áruházban vásárolja meg, az alkalmazást az áruház weboldaláról másolhatja le. Az alkalmazás aktiválásához szükséges információkat fizetés után emailben küldjük el.

A vásárlással és az értékesítési csomaggal kapcsolatos további részletekről érdeklődjön a kereskedelmi osztályon.

## REGISZTRÁLT FELHASZNÁLÓK SZÁMÁRA BIZTOSÍTOTT SZOLGÁLTATÁSOK

Felhasználói licenc vásárlásakor Ön a Kaspersky Lab alkalmazások regisztrált felhasználójává válik, és a licenc teljes érvényességi időszakában az alábbi szolgáltatások előnyeit élvezheti:

- adatbázisok frissítése és új termékverziók biztosítása;
- tanácsadás telefonon vagy emailben a termék telepítésével, beállításával és használatával kapcsolatban;
- értesítések a Kaspersky Lab új alkalmazásainak kibocsátásával és új vírusok megjelenésével kapcsolatban. A szolgáltatás igénybevételéhez fel kell iratkoznia a Kaspersky Lab hírlevelére a Terméktámogatási szolgáltatás webhelyén.

Az operációs rendszerek működésével, valamint külső féltől származó szoftverekkel és technikákkal kapcsolatban nem vállalunk tanácsadást.

## HARDVERES ÉS SZOFTVERES RENDSZERKÖVETELMÉNYEK

A Kaspersky Anti-Virus megfelelő működéséhez a számítógépnek teljesítenie kell a következő követelményeket:

Általános követelmények:

- 480 MB szabad lemezterület a merevlemezen (380 MB a rendszermeghajtón).
- CD / DVD-ROM (a Kaspersky Anti-Virus CD-ről való telepítéséhez).
- Internetkapcsolat (az alkalmazás aktiválásához, valamint az adatbázisok és szoftvermodulok frissítéséhez).
- Microsoft Internet Explorer 6.0 vagy újabb.
- Microsoft Windows Installer 2.0.

Követelmények Microsoft Windows XP Home Edition (2. szervizcsomag vagy újabb), Microsoft Windows XP Professional (2. szervizcsomag vagy újabb) és Microsoft Windows XP Professional x64 Edition (2. szervizcsomag vagy újabb) esetén:

- Intel Pentium 800 MHz-es, 32 bites (x86) / 64 bites (x64) vagy gyorsabb processzor (vagy azzal kompatibilis);
- 512 MB szabad RAM.

Követelmények Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate, Microsoft Windows 7 Starter, Microsoft Windows 7 Home Basic, Microsoft Windows 7 Home Premium, Microsoft Windows 7 Professional, Microsoft Windows 7 Ultimate esetén:

- Intel Pentium 1 GHz-es, 32 bites (x86) / 64 bites (x64) processzor vagy gyorsabb (vagy azzal kompatibilis).
- 1 GB szabad RAM (32 bites operációs rendszer esetén); 2 GB szabad RAM (64 bites operációs rendszer esetén).

Követelmények netbookok esetében:

- Intel Atom 1,6 GHz vagy azzal kompatibilis processzor.
- Intel GMA950 videokártya legalább 64 MB videó RAM memóriával (vagy azzal kompatibilis).
- Legalább 10,1" képernyőméret.

# AZ ALKALMAZÁS TELEPÍTÉSE ÉS ELTÁVOLÍTÁSA

Ez a rész tájékoztatást nyújt arról, hogyan kell telepíteni az alkalmazást a számítógépre, és hogyan távolítsa el azt.

## EBBEN A RÉSZBEN:

Normál telepítési eljárás.....	15
A Kaspersky Anti-Virus korábbi verziójának frissítése .....	19
Nem szabványos telepítések .....	22
Első lépések.....	23
Az alkalmazás eltávolítása .....	23

## NORMÁL TELEPÍTÉSI ELJÁRÁS

A Kaspersky Anti-Virus a Telepítővarázsló segítségével interaktív módban fellepül a számítógépre.

A varázsló ablakok (lépések) sorozatából áll, amelyek között a **Vissza** és a **Tovább** gombokkal navigálhat. A használat befejezésekor a varázsló bezárására a **Befejezés** gomb szolgál. A varázslót bármelyik lépésnél leállíthatja a **Mégse** gombbal.

Ha az alkalmazás egynél több számítógépet véd (a számítógépek maximális száma a licenctől függ), minden számítógépre ugyanúgy kell fellepíteni. Ne feledje, hogy ebben az esetben – a licencszerződésnek megfelelően – a licenc időtartama az első aktiválás napjától kezdődik. Amikor aktiválja az alkalmazást a második és további számítógépeken, a licenc érvényességi ideje annyi lesz rövidebb, amennyi idő az első aktiválás óta eltelt. Így a licenc érvényességi ideje az alkalmazás összes telepített másolatánál egyszerre jár le.

- *A Kaspersky Anti-Virus számítógépre történő telepítése:*  
futtassa a .EXE kiterjesztésű telepítőfájlt a terméket tartalmazó CD-lemezről.

Az online letölthető Kaspersky Anti-Virus telepítő fájl telepítése megegyezik a telepítő CD-n találhatóéval.

## EBBEN A RÉSZBEN:

1. lépés: Az alkalmazás új változatának keresése .....	16
2. lépés. Annak ellenőrzése, hogy a rendszer megfelel-e a telepítés követelményeinek .....	16
3. lépés: A telepítés típusának kiválasztása .....	16
4. lépés: A licencszerződés megtekintése.....	16
5. lépés: A Kaspersky Security Network adatgyűjtési nyilatkozat.....	16
6. lépés: Inkompatibilis alkalmazások keresése.....	17
7. lépés: A célmappa kiválasztása .....	17
8. lépés: A telepítés előkészítése.....	17
9. lépés: Telepítés.....	18
10. lépés: A telepítés befejezése .....	18
11. lépés: Alkalmazás aktiválása .....	18
12. lépés: Felhasználó regisztrálása .....	18
13. lépés: Az aktiválás befejezése .....	19

## 1. LÉPÉS: AZ ALKALMAZÁS ÚJ VÁLTOZATÁNAK KERESÉSE

A telepítés előtt a telepítővarázsló a Kaspersky Lab frissítési kiszolgálóin ellenőrzi, hogy elérhető-e a Kaspersky Anti-Virus újabb verziója.

Ha nem talál újabb termékváltozatot a Kaspersky Lab frissítési kiszolgálóin, az aktuális változat telepítési varázslója indul el.

Ha a frissítési kiszolgálók a Kaspersky Anti-Virus újabb verzióját tartalmazzák, megjelenik egy felszólítás a letöltésére és telepítésére. Javasoljuk, hogy telepítse az alkalmazás új változatát, mert az további fejlesztéseket tartalmaz, így biztosíthatja a legmegbízhatóbb védelmet számítógépe számára. Ha a felhasználó nem fogadja el az újabb verzió letöltését, a telepítő varázsló az aktuális verziót indítja el. Ha a felhasználó úgy dönt, hogy telepíti az újabb verziót, a termékelosztási fájlok letöltődnek a számítógépre, és a telepítő varázsló ezt az új verziót indítja el. Az új verzió telepítési eljárásával kapcsolatos további információkért lásd a megfelelő dokumentációt.

## 2. LÉPÉS. ANNAK ELLENŐRZÉSE, HOGY A RENDSZER MEGFELEL-E A TELEPÍTÉS KÖVETELMÉNYEINEK

A Kaspersky Anti-Virus telepítése előtt a telepítő program ellenőrzi az operációs rendszert és a javítócsomagokat, hogy megfelelnek-e a termék telepítéséhez szükséges szoftverkövetelményeknek (lásd: „Hardveres és szoftveres rendszerkövetelmények”, [14.](#) oldal). Emellett ellenőrzi az alkalmazások telepítéséhez szükséges szoftverek és jogosultságok meglétét. Ha valamely fent ismertetett feltétel nem teljesül, a képernyőn megjelenik az erre utaló értesítés.

Ha a számítógép megfelel a feltételeknek, a varázsló olyan Kaspersky Lab alkalmazásokat kezd keresni, amelyek a Kaspersky Anti-Virus alkalmazással együtt futtatva ütközést okozhatnak. Ha ilyen alkalmazást talál, a telepítő felkéri, hogy távolítsa azt el manuálisan.

Ha a telepítő a Kaspersky Anti-Virus vagy Kaspersky Internet Security régebbi verziójára lel, a Kaspersky Anti-Virus 2012 által használt összes adat (aktiválási információk, alkalmazás beállításai stb.) mentésre kerül, az újonnan telepített alkalmazás pedig felhasználja ezeket.

## 3. LÉPÉS: A TELEPÍTÉS TÍPUSÁNAK KIVÁLASZTÁSA

Ennél a lépésnél kiválaszthatja a Kaspersky Anti-Virus legalkalmasabb típusú telepítését:

- *Normál telepítés.* Ezt a lehetőséget választva (a **Telepítési beállítások módosítása** négyzet nincs bejelölve) az alkalmazás teljes terjedelmében fellepül a számítógépre a Kaspersky Lab szakértői által ajánlott beállításokkal.
- *Egyéni telepítés.* Ebben az esetben (a **Telepítési beállítások módosítása** négyzet be van jelölve) Ön határozhatja meg a mappát, amelybe az alkalmazás telepítve lesz (lásd: „7. lépés: A célmappa kiválasztása”, [17.](#) oldal), és szükség esetén letilthatja a telepítési folyamat védelmét (lásd: „8. lépés: A telepítés előkészítése”, [17.](#) oldal).

A telepítés folytatásához kattintson a **Tovább** gombra.

## 4. LÉPÉS: A LICENSZERZŐDÉS MEGTEKINTÉSE

Ennél a lépésnél át kell olvasnia az Ön és a Kaspersky Lab között létrejött licencszerződést.

Figyelmesen olvassa el a szerződést, és ha annak minden feltételét elfogadja, kattintson az **Elfogadom** gombra. A telepítés folytatódik.

Ha nem fogadja el a licencszerződést, a **Mégse** gombra kattintva szakítsa meg az alkalmazás telepítését.

## 5. LÉPÉS: A KASPERSKY SECURITY NETWORK ADATGYŰJTÉSI NYILATKOZAT

Ebben a lépésben a telepítő felajánlja, hogy csatlakozzon a Kaspersky Security Network hálózatához. A programban való részvétel a számítógépen észlelt új fenyegetések, futó alkalmazások és letöltött aláírt alkalmazások adatainak és a rendszer adatainak elküldését jelenti a Kaspersky Lab részére. Garantáljuk, hogy az alkalmazás a személyes adatait nem küldi el.

Tekintse meg a Kaspersky Security Network Adatgyűjtési nyilatkozatot. A nyilatkozat teljes szövegének megtekintéséhez kattintson a **Teljes KSN szerződés** gombra. Ha egyet ért a nyilatkozat összes pontjával, jelölje be az **Elfogadom a Kaspersky Security Network részvételi feltételeit** négyzetet.

Kattintson a **Tovább** gombra, ha az egyéni telepítés (lásd: „3. lépés: A telepítés típusának kiválasztása”, 16. oldal) lehetőséget választotta. Normál telepítés esetén kattintson a **Telepítés** gombra. A telepítés folytatódik.

## 6. LÉPÉS: INKOMPATIBILIS ALKALMAZÁSOK KERESÉSE

Ennél a lépésnél az alkalmazás ellenőrzi, hogy a számítógépre telepített alkalmazások valamelyike nem inkompatibilis-e Kaspersky Anti-Virus alkalmazással.

Ha nincs ilyen alkalmazás, a varázsló automatikusan továbblép a következő lépésre.

Inkompatibilis alkalmazás észlelése esetén azok egy listában jelennek meg a képernyőn, és a telepítő kéri azok eltávolítását. Azokat az alkalmazásokat, amelyeket a Kaspersky Anti-Virus automatikusan nem képes eltávolítani, azokat kézzel kell. Az inkompatibilis alkalmazások eltávolításakor újra kell indítani az operációs rendszert, ami után a Kaspersky Anti-Virus telepítése automatikusan tovább folytatódik.

A telepítés folytatásához kattintson a **Tovább** gombra.

## 7. LÉPÉS: A CÉLMAPPA KIVÁLASZTÁSA

A telepítővarázsló ezen lépése csak az egyéni telepítés kiválasztása esetén jelenik meg (lásd a „3. lépés: A telepítés típusának kiválasztása” részt; 16. oldal). A normál telepítés során ez a lépés kimarad, az alkalmazás pedig az alapértelmezett mappába települ.

Ennél a lépésnél az alkalmazás felajánlja, hogy válassza ki a mappát, ahova a Kaspersky Anti-Virus telepítésre kerül. A következő útvonal az alapértelmezett:

- <lemez>\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 2012 – 32 bites rendszereknél;
- <lemez>\Program Files (x86)\Kaspersky Lab\Kaspersky Anti-Virus 2012 – 64 bites rendszereken.

A Kaspersky Anti-Virus másik mappába történő telepítéséhez adja meg a mappa elérési útját a beviteli mezőbe, vagy kattintson a **Tallózás** gombra, és válassza ki a mappát a megnyíló ablakban.

Ügyeljen az alábbi korlátozásokra:

- Az alkalmazás nem telepíthető hálózati meghajtóra, cserélhető meghajtóra és virtuális (SUBST paranccsal létrehozott meghajtóra) meghajtóra sem.
- Javasoljuk, hogy ne telepítse az alkalmazást abba a mappába, amely más fájlokat vagy mappákat tartalmaz, mert a telepítési mappa szerkesztésre való hozzáférése majd blokkolásra kerül.
- A telepítési mappa elérési útja nem lehet hosszabb 160 karakternél, és nem tartalmazhatja a /, ?, :, \*, ", >, < és | karaktereket.

Annak megállapítására, hogy van-e elegendő szabad hely a számítógépen az alkalmazás telepítésére, kattintson a **Lemezhely** gombra. A megnyíló ablakban megjelennek a lemezterületre vonatkozó információk. Az ablak bezárásához kattintson az **OK** gombra.

A telepítés folytatásához kattintson a **Tovább** gombra a varázsló ablakában.

## 8. LÉPÉS: A TELEPÍTÉS ELŐKÉSZÍTÉSE

A telepítővarázsló ezen lépése csak az egyéni telepítés kiválasztása esetén jelenik meg (lásd a „3. lépés: A telepítés típusának kiválasztása” részt; 16. oldal). Normál telepítés esetén ez a lépés kimarad.

Mivel számítógépe rosszindulatú programokkal fertőződhetett meg, amelyek hatnak a Kaspersky Anti-Virus telepítésére, a telepítési folyamatot védeni kell.

Alapértelmezésben a telepítési folyamat védelme engedélyezve van **Telepítési folyamat védelme** négyzet be van jelölve a Varázsló ablakában.

Javasolt törölni a négyzet bejelölését, ha az alkalmazás nem telepíthető (például távoli telepítés végrehajtásakor a Windows Távoli Asztal használatával). Ennek az engedélyezett védelem is lehet az oka.

Ebben az esetben meg kell szakítania és újra kell indítania a telepítést, majd be kell jelölnie a **Telepítési beállítások módosítása** négyzetet A telepítés típusának kiválasztása lépésben (lásd: „3. lépés: A telepítés típusának kiválasztása”, [16.](#) oldal), és amikor a Telepítés előkészítése lépéshez ér, törölje a **Telepítési folyamat védelme** négyzet bejelölését.

A telepítés folytatásához kattintson a **Telepítés** gombra.

Ha Microsoft Windows XP alatt futó számítógépre telepíti az alkalmazást, az aktív hálózati kapcsolatok megszakadnak. A megszakított kapcsolatok többsége rövid szünet után helyreáll.

## 9. LÉPÉS: TELEPÍTÉS

Az alkalmazás telepítése némi időt igénybe vesz. Várja meg, amíg befejeződik.

A telepítés befejezése után a varázsló automatikusan folytatja a következő lépéssel.

Ha a telepítéskor egy rosszindulatú program által okozott olyan hiba történik, amely megakadályozza víruskereső alkalmazások telepítését a számítógépre, a telepítő varázsló felajánlja, hogy töltsen le a *Kaspersky víruseltávolító eszközt* a fertőzés semlegesítésére.

Ha beleegyezik a segédprogram telepítésébe, a telepítő varázsló letölti azt a Kaspersky Lab kiszolgálóról, ami után a telepítés automatikusan megkezdődik. Ha a varázsló nem tudja letölteni a segédprogramot, az alkalmazás felajánlja, hogy töltsen le Ön manuálisan a megadott hivatkozásra kattintva.

Ha befejezte a segédprogram használatát, törölje le, és kezdje újra a Kaspersky Anti-Virus telepítését.

## 10. LÉPÉS: A TELEPÍTÉS BEFEJEZÉSE

A varázsló ezen ablaka tájékoztatja az alkalmazás sikeres telepítéséről. A Kaspersky Anti-Virus használatának megkezdéséhez jelölje be az **A Kaspersky Anti-Virus futtatása** négyzetet, majd kattintson a **Befejezés** gombra.

Előfordulhat, hogy újra kell indítania az operációs rendszert. Ha bejelölte az **A Kaspersky Internet Security 2012 futtatása** négyzetet, az alkalmazás az operációs rendszer újraindítása után automatikusan elindul.

Ha a varázsló bezárása előtt megszüntette a négyzet bejelölését, az alkalmazást manuálisan kell elindítania (lásd: „Az alkalmazás kézi elindítása és leállítása”, [34.](#) oldal).

## 11. LÉPÉS: ALKALMAZÁS AKTIVÁLÁSA

Az *Aktiválás* annak a licencnek az aktiválását jelenti, amellyel annak lejártáig az alkalmazás teljesen funkcionális verzióját használhatja.

Az alkalmazás aktiválásához internetkapcsolat szükséges.

A Kaspersky Anti-Virus a következő aktiválási módokat kínálja fel:

- **Kereskedelmi verzió aktiválása.** Válassza ezt a lehetőséget és adja meg az aktiváló kódot, ha megvásárolta a termék kereskedelmi verzióját.

Ha begépel a Kaspersky Internet Security aktiválási kódját a beviteli mezőbe, az aktiválás befejeztével megkezdődik az átváltás a Kaspersky Internet Security alkalmazásra.

- **Próbaverzió aktiválása.** Ezt az aktiválási módot akkor használja, ha a kereskedelmi verzió megvásárlása előtt telepíteni szeretné az alkalmazás próbaverzióját. Az alkalmazás próbaverziója esetén teljesen működőképes verziót használhat a licenc által biztosított korlátozott ideig. Ha a licenc lejár, másodszor már nem aktiválható.

## 12. LÉPÉS: FELHASZNÁLÓ REGISZTRÁLÁSA

Ez a lépés csak az alkalmazás kereskedelmi verziójának aktiválása után elérhető. Próbaverzió aktiválásakor a lépés kimarad.

Regisztrálnia kell magát, hogy a jövőben kapcsolatba léphessen a Kaspersky Lab Terméktámogatási szolgáltatásával.

Ha beleegyezik a regisztrációba, a megfelelő mezőkben adja meg a regisztrációs adatait, és kattintson a **Tovább** gombra.

### 13. LÉPÉS: AZ AKTIVÁLÁS BEFEJEZÉSE

A varázsló tájékoztatja Önt a Kaspersky Anti-Virus sikeres aktiválásáról. Ezenkívül megjelennek a licenccel kapcsolatos információk: licenc típusa (kereskedelmi vagy próba), lejárat dátum és a licenchez tartozó kiszolgálók száma.

Ha aktiválta az előfizetést, a licenc lejárat dátuma helyett az előfizetés állapotával kapcsolatos információ jelenik meg. Nyomja meg a **Befejezés** gombot a varázsló bezárásához.

## A KASPERSKY ANTI-VIRUS KORÁBBI VERZIÓJÁNAK FRISSÍTÉSE

Ha a Kaspersky Anti-Virus 2010 vagy 2011 már telepítésre került a számítógépre, frissítenie kell a Kaspersky Anti-Virus 2012-re. Ha rendelkezik a Kaspersky Anti-Virus 2010 vagy 2011 aktív licencével, nem kell aktiválnia az alkalmazást: a Telepítővarázsló automatikusan átveszi a Kaspersky Anti-Virus 2010 vagy 2011 licencadatait, és azt felhasználva telepíti az alkalmazást.

A Kaspersky Anti-Virus a Telepítővarázsló segítségével interaktív módban fellepül a számítógépre.

A varázsló ablakok (lépések) sorozatából áll, amelyek között a **Vissza** és a **Tovább** gombokkal navigálhat. A használat befejezésekor a varázsló bezárására a **Befejezés** gomb szolgál. A varázslót bármelyik lépésnél leállíthatja a **Mégse** gombbal.

Ha az alkalmazás egynél több számítógépet véd (a számítógépek maximális száma a licenctől függ), minden számítógépre ugyanúgy kell fellepíteni. Ne feledje, hogy ebben az esetben – a licencszerződésnek megfelelően – a licenc időtartama az első aktiválás napjától kezdődik. Amikor aktiválja az alkalmazást a második és további számítógépeken, a licenc érvényességi ideje annnyival lesz rövidebb, amennyi idő az első aktiválás óta eltelt. Így a licenc érvényességi ideje az alkalmazás összes telepített másolatánál egyszerre jár le.

➔ **A Kaspersky Anti-Virus számítógépre történő telepítése:**

futtassa a .EXE kiterjesztésű telepítőfájlt a terméket tartalmazó CD-lemezről.

Az online letölthető Kaspersky Anti-Virus telepítő fájl telepítése megegyezik a telepítő CD-n találhatóéval.

#### EBBEN A RÉSZBEN:

1. lépés: Az alkalmazás új változatának keresése .....	<a href="#">19</a>
2. lépés: Annak ellenőrzése, hogy a rendszer megfelel-e a telepítés követelményeinek .....	<a href="#">20</a>
3. lépés: A telepítés típusának kiválasztása .....	<a href="#">20</a>
4. lépés: A licencszerződés megtekintése .....	<a href="#">20</a>
5. lépés: A Kaspersky Security Network adatgyűjtési nyilatkozat .....	<a href="#">20</a>
6. lépés: Inkompatibilis alkalmazások keresése .....	<a href="#">21</a>
7. lépés: A célmappa kiválasztása .....	<a href="#">21</a>
8. lépés: A telepítés előkészítése .....	<a href="#">21</a>
9. lépés: Telepítés .....	<a href="#">22</a>
10. lépés: A varázsló bezárása .....	<a href="#">22</a>

## 1. LÉPÉS: AZ ALKALMAZÁS ÚJ VÁLTOZATÁNAK KERESÉSE

A telepítés előtt a telepítővarázsló a Kaspersky Lab frissítési kiszolgálóin ellenőrzi, hogy elérhető-e a Kaspersky Anti-Virus újabb verziója.

Ha nem talál újabb termékváltozatot a Kaspersky Lab frissítési kiszolgálóin, az aktuális változat telepítési varázslója indul el.

Ha a frissítési kiszolgálók a Kaspersky Anti-Virus újabb verzióját tartalmazzák, megjelenik egy felszólítás a letöltésére és telepítésére. Javasoljuk, hogy telepítse az alkalmazás új változatát, mert az további fejlesztéseket tartalmaz, így biztosíthatja a legmegbízhatóbb védelmet számítógépe számára. Ha a felhasználó nem fogadja el az újabb verzió letöltését, a telepítő varázsló az aktuális verziót indítja el. Ha a felhasználó úgy dönt, hogy telepíti az újabb verziót, a termékelosztási fájlok letöltődnek a számítógépre, és a telepítő varázsló ezt az új verziót indítja el. Az új verzió telepítési eljárásával kapcsolatos további információkért lásd a megfelelő dokumentációt.

## 2. LÉPÉS. ANNAK ELLENŐRZÉSE, HOGY A RENDSZER MEGFELEL-E A TELEPÍTÉS KÖVETELMÉNYEINEK

A Kaspersky Anti-Virus telepítése előtt a telepítő program ellenőrzi az operációs rendszert és a javítócsomagokat, hogy megfelelnek-e a termék telepítéséhez szükséges szoftverkövetelményeknek (lásd: „Hardveres és szoftveres rendszerkövetelmények”, [14.](#) oldal). Emellett ellenőrzi az alkalmazások telepítéséhez szükséges szoftverek és jogosultságok meglétét. Ha valamely fent ismertetett feltétel nem teljesül, a képernyőn megjelenik az erre utaló értesítés.

Ha a számítógép megfelel a feltételeknek, a varázsló olyan Kaspersky Lab alkalmazásokat kezd keresni, amelyek a Kaspersky Anti-Virus alkalmazással együtt futtatva ütközést okozhatnak. Ha ilyen alkalmazást talál, a telepítő felkéri, hogy távolítsa azt el manuálisan.

Ha a telepítő a Kaspersky Anti-Virus vagy Kaspersky Internet Security régebbi verziójára lel, a Kaspersky Anti-Virus 2012 által használt összes adat (aktiválási információk, alkalmazás beállításai stb.) mentésre kerül, az újonnan telepített alkalmazás pedig felhasználja ezeket.

## 3. LÉPÉS: A TELEPÍTÉS TÍPUSÁNAK KIVÁLASZTÁSA

Ennél a lépésnél kiválaszthatja a Kaspersky Anti-Virus legalkalmasabb típusú telepítését:

- *Normál telepítés.* Ezt a lehetőséget választva (a **Telepítési beállítások módosítása** négyzet nincs bejelölve) az alkalmazás teljes terjedelmében feltelepül a számítógépre a Kaspersky Lab szakértői által ajánlott beállításokkal.
- *Egyéni telepítés.* Ebben az esetben (a **Telepítési beállítások módosítása** négyzet be van jelölve) Ön határozhatja meg a mappát, amelybe az alkalmazás telepítve lesz (lásd: „7. lépés: A célmappa kiválasztása”, [17.](#) oldal), és szükség esetén letilthatja a telepítési folyamat védelmét (lásd: „8. lépés: A telepítés előkészítése”, [17.](#) oldal).

A telepítés folytatásához kattintson a **Tovább** gombra.

## 4. LÉPÉS: A LICENCSZERZŐDÉS MEGTEKINTÉSE

Ennél a lépésnél át kell olvasnia az Ön és a Kaspersky Lab között létrejött licencszerződést.

Figyelmesen olvassa el a szerződést, és ha annak minden feltételét elfogadja, kattintson az **Elfogadom** gombra. A telepítés folytatódik.

Ha nem fogadja el a licencszerződést, a **Mégse** gombra kattintva szakítsa meg az alkalmazás telepítését.

## 5. LÉPÉS: A KASPERSKY SECURITY NETWORK ADATGYŰJTÉSI NYILATKOZAT

Ebben a lépésben a telepítő felajánlja, hogy csatlakozzon a Kaspersky Security Network hálózatához. A programban való részvétel a számítógépen észlelt új fenyegetések, futó alkalmazások és letöltött aláírt alkalmazások adatainak és a rendszer adatainak elküldését jelenti a Kaspersky Lab részére. Garantáljuk, hogy az alkalmazás a személyes adatait nem küldi el.

Tekintse meg a Kaspersky Security Network Adatgyűjtési nyilatkozatot. A nyilatkozat teljes szövegének megtekintéséhez kattintson a **Teljes KSN szerződés** gombra. Ha egyet ért a nyilatkozat összes pontjával, jelölje be az **Elfogadom a Kaspersky Security Network részvételi feltételeit** négyzetet.

Kattintson a **Tovább** gombra, ha az egyéni telepítés (lásd: „3. lépés: A telepítés típusának kiválasztása”, [16.](#) oldal) lehetőséget választotta. Normál telepítés esetén kattintson a **Telepítés** gombra. A telepítés folytatódik.

## 6. LÉPÉS: INKOMPATIBILIS ALKALMAZÁSOK KERESÉSE

Ennél a lépésnél az alkalmazás ellenőrzi, hogy a számítógépre telepített alkalmazások valamelyike nem inkompatibilis-e Kaspersky Anti-Virus alkalmazással.

Ha nincs ilyen alkalmazás, a varázsló automatikusan továbblép a következő lépésre.

Inkompatibilis alkalmazás észlelése esetén azok egy listában jelennek meg a képernyőn, és a telepítő kéri azok eltávolítását. Azokat az alkalmazásokat, amelyeket a Kaspersky Anti-Virus automatikusan nem képes eltávolítani, azokat kézzel kell. Az inkompatibilis alkalmazások eltávolításakor újra kell indítani az operációs rendszert, ami után a Kaspersky Anti-Virus telepítése automatikusan tovább folytatódik.

A telepítés folytatásához kattintson a **Tovább** gombra.

## 7. LÉPÉS: A CÉLMAPPA KIVÁLASZTÁSA

A telepítővarázsló ezen lépése csak az egyéni telepítés kiválasztása esetén jelenik meg (lásd a „3. lépés: A telepítés típusának kiválasztása” részt; [16.](#) oldal). A normál telepítés során ez a lépés kimarad, az alkalmazás pedig az alapértelmezett mappába települ.

Ennél a lépésnél az alkalmazás felajánlja, hogy válassza ki a mappát, ahova a Kaspersky Anti-Virus telepítésre kerül. A következő útvonal az alapértelmezett:

- <lemez>\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 2012 – 32 bites rendszereknél;
- <lemez>\Program Files (x86)\Kaspersky Lab\Kaspersky Anti-Virus 2012 – 64 bites rendszereken.

A Kaspersky Anti-Virus másik mappába történő telepítéséhez adja meg a mappa elérési útját a beviteli mezőbe, vagy kattintson a **Tallózás** gombra, és válassza ki a mappát a megnyíló ablakban.

Ügyeljen az alábbi korlátozásokra:

- Az alkalmazás nem telepíthető hálózati meghajtóra, cserélhető meghajtóra és virtuális (SUBST paranccsal létrehozott meghajtóra) meghajtóra sem.
- Javasoljuk, hogy ne telepítse az alkalmazást abba a mappába, amely más fájlokat vagy mappákat tartalmaz, mert a telepítési mappa szerkesztésre való hozzáférése majd blokkolásra kerül.
- A telepítési mappa elérési útja nem lehet hosszabb 160 karakternél, és nem tartalmazhatja a /, ?, :, \*, ", >, < és | karaktereket.

Annak megállapítására, hogy van-e elegendő szabad hely a számítógépen az alkalmazás telepítésére, kattintson a **Lemezhely** gombra. A megnyíló ablakban megjelennek a lemezterületre vonatkozó információk. Az ablak bezárásához kattintson az **OK** gombra.

A telepítés folytatásához kattintson a **Tovább** gombra a varázsló ablakában.

## 8. LÉPÉS: A TELEPÍTÉS ELŐKÉSZÍTÉSE

A telepítővarázsló ezen lépése csak az egyéni telepítés kiválasztása esetén jelenik meg (lásd a „3. lépés: A telepítés típusának kiválasztása” részt; [16.](#) oldal). Normál telepítés esetén ez a lépés kimarad.

Mivel számítógépe rosszindulatú programokkal fertőződhetett meg, amelyek hatnak a Kaspersky Anti-Virus telepítésére, a telepítési folyamatot védeni kell.

Alapértelmezésben a telepítési folyamat védelme engedélyezve van **Telepítési folyamat védelme** négyzet be van jelölve a Varázsló ablakában.

Javasolt törölni a négyzet bejelölését, ha az alkalmazás nem telepíthető (például távoli telepítés végrehajtásakor a Windows Távoli Asztal használatával). Ennek az engedélyezett védelem is lehet az oka.

Ebben az esetben meg kell szakítania és újra kell indítania a telepítést, majd be kell jelölnie a **Telepítési beállítások módosítása** négyzetet A telepítés típusának kiválasztása lépésben (lásd: „3. lépés: A telepítés típusának kiválasztása”, [16.](#) oldal), és amikor a Telepítés előkészítése lépéshez ér, törölje a **Telepítési folyamat védelme** négyzet bejelölését.

A telepítés folytatásához kattintson a **Telepítés** gombra.

Ha Microsoft Windows XP alatt futó számítógépre telepíti az alkalmazást, az aktív hálózati kapcsolatok megszakadnak. A megszakított kapcsolatok többsége rövid szünet után helyreáll.

## 9. LÉPÉS: TELEPÍTÉS

Az alkalmazás telepítése némi időt igénybe vesz. Várja meg, amíg befejeződik.

A telepítés befejezése után a varázsló automatikusan folytatja a következő lépéssel.

Ha a telepítéskor egy rosszindulatú program által okozott olyan hiba történik, amely megakadályozza víruskereső alkalmazások telepítését a számítógépre, a telepítő varázsló felajánlja, hogy töltsen le a *Kaspersky víruseltávolító eszközt* a fertőzés semlegesítésére.

Ha beleegyezik a segédprogram telepítésébe, a telepítő varázsló letölti azt a Kaspersky Lab kiszolgálóról, ami után a telepítés automatikusan megkezdődik. Ha a varázsló nem tudja letölteni a segédprogramot, az alkalmazás felajánlja, hogy töltsen le Ön manuálisan a megadott hivatkozásra kattintva.

Ha befejezte a segédprogram használatát, törölje le, és kezdje újra a Kaspersky Anti-Virus telepítését.

## 10. LÉPÉS: A VARÁZSLÓ BEZÁRÁSA

A varázsló ezen ablaka tájékoztatja az alkalmazás sikeres telepítéséről. A Kaspersky Anti-Virus használatának megkezdéséhez jelölje be az **A Kaspersky Anti-Virus futtatása** négyzetet, majd kattintson a **Befejezés** gombra.

Előfordulhat, hogy újra kell indítania az operációs rendszert. Ha bejelölte az **A Kaspersky Internet Security 2012 futtatása** négyzetet, az alkalmazás az operációs rendszer újraindítása után automatikusan elindul.

Ha a varázsló bezárása előtt megszüntette a négyzet bejelölését, az alkalmazást manuálisan kell elindítania (lásd: „Az alkalmazás kézi elindítása és leállítása”, [34.](#) oldal).

## NEM SZABVÁNYOS TELEPÍTÉSEK

Ez a fejezet ismerteti azokat a telepítési módszereket, amelyek a normál telepítéstől vagy a előző verzióról történő frissítéstől eltérnek.

### A Kaspersky Anti-Virus telepítése és későbbi aktiválása egy Kaspersky Internet Security aktiváló kóddal

Ha a Kaspersky Anti-Virus telepítése során az aktiválási lépésnél a Kaspersky Kaspersky Internet Security aktiváló kódját írja be, elindul a frissítési folyamat, amely a Kaspersky Anti-Virus alkalmazást a Kaspersky Internet Security alkalmazással váltja le.

Ha a Kaspersky Anti-Virus telepítése során az aktiválási lépésnél az **Aktiválás később** lehetőséget választja, majd a Kaspersky Internet Security aktiváló kódjával aktiválja az alkalmazást, szintén elkezdődik a frissítési folyamat, amely a Kaspersky Anti-Virust a Kaspersky Internet Security alkalmazással váltja le.

### A Kaspersky Anti-Virus 2012 telepítése a Kaspersky Internet Security 2010-re vagy 2011-re

Ha olyan számítógépen indítja el a Kaspersky Anti-Virus 2012 telepítését, amelyiken már aktív licenccel működik a Kaspersky Internet Security 2010 vagy 2011, a telepítővarázsló a licenc adatait felhasználva az alábbi műveletek valamelyikének kiválasztását kéri:

- A Kaspersky Internet Security 2010 vagy 2011 meglévő licencének felhasználása. Ebben az esetben elkezdődik a frissítési folyamat, melynek végén a Kaspersky Internet Security 2012 lesz feltelepítve a számítógépre. Addig használhatja a Kaspersky Internet Security 2012 alkalmazást, amíg a Kaspersky Internet Security 2010 vagy 2011 licence érvényes.
- A Kaspersky Anti-Virus 2012 telepítésének a folytatása. Ebben az esetben a telepítés a normál telepítési eljárás szerint, az alkalmazás aktiválásával kezdve zajlik le.

## ELSŐ LÉPÉSEK

Az alkalmazás a telepítés után készen áll a használatra. A számítógép megfelelő védelmének biztosításához ajánlott közvetlenül a telepítés és a konfigurálás után elvégezni a következő műveleteket:

- Alkalmazás adatbázisainak frissítése (lásd: „Az alkalmazás adatbázisainak és alkalmazásmóduljainak frissítése”, [40.](#) oldal).
- Számítógép vizsgálata vírusok (lásd: „Vírusok keresése a számítógépen teljes vizsgálattal”, [42.](#) oldal) és sebezhetőségek (lásd: „Számítógép sebezhetőségének vizsgálata”, [42.](#) oldal) tekintetében.
- A számítógép védelmi állapotának ellenőrzése és szükség esetén a védelmi problémák megszüntetése.

## AZ ALKALMAZÁS ELTÁVOLÍTÁSA

A Kaspersky Anti-Virus eltávolítása után számítógépe és a személyes adatai védtelenek lesznek!

A Kaspersky Anti-Virus eltávolítása a telepítővarázsló segítségével történik.

### ➤ A varázsló elindítása:

a **Start** menüben válassza ki a **Programok** → **Kaspersky Anti-Virus 2012** → **Kaspersky Anti-Virus 2012 eltávolítása** elemet.

### EBBEN A RÉSZBEN:

1. lépés: Adatok mentése ismételt használathoz .....	<a href="#">23</a>
2. lépés: Az alkalmazás eltávolításának megerősítése .....	<a href="#">23</a>
3. lépés: Alkalmazás eltávolítása. Az eltávolítás befejezése .....	<a href="#">24</a>

## 1. LÉPÉS: ADATOK MENTÉSE ISMÉTELT HASZNÁLATHOZ

Ezen a ponton megadhatja, hogy az alkalmazás által használt adatok közül melyeket szeretne megtartani ismételt felhasználásra az alkalmazás következő telepítésekor (pl. az alkalmazás újabb verziójának telepítésekor).

Alapértelmezésben az alkalmazás teljesen el lesz távolítva a számítógépről.

### ➤ Adatok mentése ismételt használathoz:

1. Válassza az **Alkalmazásobjektumok mentése** lehetőséget.
2. Jelölje be a menteni kívánt adattípusok melletti négyzeteket:
  - **Aktiválási adatok** - az alkalmazás jövőbeni aktiválását a jelenlegi licenc használata révén szükségtelenné tevő adatok, feltéve, hogy a következő telepítésig a licenc érvényessége még nem jár le.
  - **Karanténba helyezett és a Másolatok mappában levő fájlok** – az alkalmazás által ellenőrzött és a karanténba vagy a másolattárolóba helyezett fájlok.
  - **Alkalmazás működési beállításai** – az alkalmazás beállításainak konfigurálásakor kiválasztott értékei.
  - **iChecker adatok** – a víruskeresésen már átesett objektumok adatait tároló fájlok.

## 2. LÉPÉS: AZ ALKALMAZÁS ELTÁVOLÍTÁSÁNAK MEGERŐSÍTÉSE

Mivel az alkalmazás eltávolítása veszélyezteti a számítógép és személyes adatai biztonságát, meg kell erősítenie az alkalmazás eltávolítására irányuló szándékát. Ehhez kattintson az **Eltávolítás** gombra.

Az alkalmazás eltávolításának leállításához a **Mégse** gombra kattintva bármikor megszakíthatja ezt a műveletet.

### **3. LÉPÉS: ALKALMAZÁS ELTÁVOLÍTÁSA. ELTÁVOLÍTÁS BEFEJEZÉSE**

A varázsló ennél a lépésnél távolítja el az alkalmazást a számítógépről. Várja meg, amíg az eltávolítás befejeződik.

Az alkalmazás eltávolításakor előfordulhat, hogy újra kell indítania az operációs rendszert. Ha visszavonja az azonnali újraindítást, az eltávolítás befejezése áttevődik arra az alkalomra, amikor az operációs rendszer újraindul, vagy a számítógépet kikapcsolja és bekapcsolja.

# AZ ALKALMAZÁS LICENCELÉSE

Ez a rész tájékoztatást nyújt az alkalmazás aktiválásával kapcsolatos általános feltételekről. Olvassa el ezt a részt, hogy többet megtudjon a licencszerződés céljáról, a licenc típusairól, az alkalmazás aktiválási módjairól és a licenc megújításáról.

## EBBEN A RÉSZBEN:

A végfelhasználói licencszerződésről.....	<a href="#">25</a>
Az adatok feletti rendelkezés .....	<a href="#">25</a>
A licenc.....	<a href="#">25</a>
Az aktiváló kód .....	<a href="#">26</a>

## A VÉGFELHASZNÁLÓI LICENCszerződésről

A végfelhasználói licencszerződés egy jogi megállapodás Ön és a Kaspersky Lab ZAO között, amely meghatározza, hogy milyen feltételek szerint használhatja az alkalmazást.

**Az alkalmazás használatba vétele előtt olvassa át figyelmesen a végfelhasználói licencszerződés feltételeit.**

A végfelhasználói licencszerződés feltételeit a Kaspersky Lab alkalmazás telepítése során elolvashatja.

A végfelhasználói licencszerződés feltételeinek elfogadását az alábbiak jelzik:

- A telepítő CD dobozának felnyitása (csak akkor, ha dobozolt alkalmazást vásárolt egy üzletben vagy egy partnernél).
- Az alkalmazás telepítésekor a végfelhasználói licencszerződés szövege elfogadásának megerősítése esetén.

Ha nem fogadja el a végfelhasználói licencszerződés feltételeit, a telepítést meg kell szakítania.

## AZ ADATOK FELETTI RENDELKEZÉS

A végfelhasználói licencszerződés feltételeit elfogadva a valós idejű védelem szintjének növelése érdekében Ön abba is beleegyezik, hogy a feldolgozott objektumok ellenőrzőösszeg adatait a rendszer automatikus módban (MD5) elküldje. Ebből az információból határozható meg az URL-ek reputációja, és statisztikai adatokat nyújt a levélszemét elleni védelemhez. A begyűjtött információk nem tartalmaznak személyes adatokat és egyéb bizalmas információt. A beérkezett információkat a Kaspersky Lab a hatályos rendelkezések értelmében védi. További részletekért látogasson el a webhelyre: <http://support.kaspersky.com>.

## A LICENC

A *licenc* alkalmazás időben korlátozott használati joga, amelyet a licencszerződés alapján kap. A licenc egy egyedi aktiválókódot tartalmaz a Kaspersky Anti-Virus alkalmazáshoz.

A licenc az alábbi szolgáltatások igénybevételére jogosít:

- Az alkalmazás használata egy vagy több eszközön.

Az eszközök számát, amelyeken az alkalmazást használhatja, a licencszerződés tartalmazza.

- A Kaspersky Lab Terméktámogatási szolgáltatása.
- A Kaspersky Lab vagy partnerei által nyújtott szolgáltatások teljes körű igénybevétele a licenc érvényességi ideje alatt (lásd: „Regisztrált felhasználók számára biztosított szolgáltatások”, [14.](#) oldal).

A szolgáltatások köre, valamint az alkalmazás érvényességi ideje az alkalmazás aktiválásához használt licenc típusától függ.

A következő licenctípusok választhatók:

- *Próba*– korlátozott érvényességi idejű ingyenes licenc, amely lehetővé teszi, hogy megismerkedjen az alkalmazással.

Ha letölti az alkalmazást a <http://www.kaspersky.hu> weboldalról, automatikusan egy próbalicenc tulajdonosává válik. A próbalicenc lejáratát után a Kaspersky Anti-Virus minden funkciója le lesz tiltva. Az alkalmazás további használatához meg kell vásárolnia egy kereskedelmi licencet.

- *Kereskedelmi* – korlátozott érvényességi idejű fizetett licenc, amelyet az alkalmazás megvásárlásakor kap.

A kereskedelmi licenc lejáratát után az alkalmazás korlátozott üzemmódban fut. Továbbra is kereshet vírusokat a számítógépen, és használhatja az alkalmazás egyéb összetevőit, de csak a licenc lejáratát előtt telepített adatbázisokkal. A Kaspersky Anti-Virus további használatához újítsa meg a kereskedelmi licencet.

Javasoljuk, hogy legkésőbb az érvényes licenc lejáratának napján újítsa meg a licencet annak érdekében, hogy a számítógépe a lehető legteljesebb vírusvédelemben részesüljön.

## AZ AKTIVÁLÓ KÓD

Az *Aktiváló kód* egy a Kaspersky Anti-Virus kereskedelmi licencének megvásárlásakor kapott kód. A kód az alkalmazás aktiválásához szükséges.

Az aktiváló kód egy latin karakterekből álló alfanumerikus karaktorsor xxxxx-xxxxx-xxxxx-xxxxx formátumban.

Az aktiváló kódot az alábbi módok valamelyikén kapja meg, az alkalmazás beszerzési módjától függően:

- Ha a Kaspersky Anti-Virus dobozolt változatát vásárolta meg, az aktiváló kód a dokumentációban, vagy a telepítő CD-t tartalmazó dobozon található.
- Ha a Kaspersky Anti-Virus alkalmazást online boltban vásárolta meg, az aktiváló kódot arra az email címre küldjük el, amelyet a termék vásárlásakor megadott.

A licenc érvényességi időszaka abban a pillanatban kezdődik el, amikor aktiválta az alkalmazást. Ha a Kaspersky Anti-Virus több eszközön aktiválható licencét vásárolta meg, a licenc érvényességi időszaka abban a pillanatban kezdődik el, amikor az első ilyen eszközön aktiválta az alkalmazást.

Ha az aktiválás után elvesztette, vagy véletlenül törölte az aktiváló kódot, küldjön egy kérést a Kaspersky Lab Terméktámogatási szolgáltatásának a Saját Kaspersky fiókból (lásd: „Terméktámogatás igénylése a Saját Kaspersky fiókon keresztül”, [115.](#) oldal).

Ha elvégezte az alkalmazás aktiválását a kóddal, kap egy *kliensazonosítót*. A kliensazonosító annak a felhasználónak az azonosítója, aki ingyenes támogatást kaphat telefonon vagy a Saját Kaspersky fiók segítségével (lásd: „Terméktámogatás igénylése a Saját Kaspersky fiókon keresztül”, [115.](#) oldal).

# ALKALMAZÁS FELÜLETE

Ez a rész tájékoztatást nyújt az alkalmazás grafikus felületének alapvető elemeiről: az alkalmazás ikonjairól és az alkalmazás ikonjainak helyi menüjéről, a főablakról, a beállítási ablakról és az értesítési ablakokról.

## EBBEN A RÉSZBEN:

Az értesítési terület ikonja .....	<a href="#">27</a>
A helyi menü .....	<a href="#">28</a>
a Kaspersky Anti-Virus főablaka .....	<a href="#">29</a>
Értesítési ablakok és felugró üzenetek.....	<a href="#">30</a>
Az alkalmazás beállítási ablaka .....	<a href="#">31</a>
A Kaspersky Gadget .....	<a href="#">32</a>
Hírügynök.....	<a href="#">33</a>

## AZ ÉRTEŚÍTESI TERÜLET IKONJA

Közvetlenül az alkalmazás telepítése után a Microsoft Windows tálca értesítési területén megjelenik az alkalmazás ikonja.






A Microsoft Windows 7 operációs rendszer esetében az alkalmazás ikonja alapértelmezésben el van rejtve, de az alkalmazás könnyebb eléréséhez megjelenítheti azt (lásd az operációs rendszer dokumentációját).

Az ikon funkciói a következők:

- Az alkalmazás működésének jelzése.
- A helyi menü, az alkalmazás főablaka és a hírek ablak megnyitása.



### Az alkalmazás működésének jelzése

Ez az ikon az alkalmazás működését jelzi. Ezenkívül tájékoztat a védelem állapotáról és megjeleníti az alkalmazás által éppen végrehajtott alapvető funkciókat:

-  – email üzenet vizsgálata;
-  – webes forgalom ellenőrzése;
-  – adatbázisok és alkalmazásmodulok frissítése;
-  – a frissítések életbe léptetéséhez újra kell indítani a rendszert;
-  – az alkalmazás egyik összetevőjének működésében hiba lépett fel.


Az ikon alapértelmezésben animált: például az email üzenet vizsgálata közben egy kicsi levél szimbólum villog az alkalmazás ikonja előtt; frissítés közben egy forgó földgömb látható. Az animációt ki is kapcsolhatja (lásd: „Értesítési ablakok átlátszósága”, [105.](#) oldal).

Az animáció letiltása esetén az ikon az alábbi formákban jelenhet meg:

-  (színes szimbólum) – egy vagy több védelmi összetevő be van kapcsolva;
-  (fekete-fehér szimbólum) – minden védelmi összetevő ki van kapcsolva.

### A helyi menü és az alkalmazás ablakainak elérése.

Az ikon segítségével (a jobb gombbal kattintva) megnyithatja a helyi menüt ([28.](#) oldal) és (a bal egérgombbal) az alkalmazás főablakát (lásd: „A Kaspersky Anti-Virus főablaka”, [29.](#) oldal).

Ha friss Kaspersky Lab-hírek érhetőek el, a Microsoft Windows tálca értesítési területén megjelenik a  ikon. Kattintson kétszer az ikonra a Hírügynök megnyitásához (lásd: „Hírügynök”, [33.](#) oldal).

## A HELYI MENÜ

A helyi menü segítségével gyorsan végezhet különböző műveleteket az alkalmazáson.

A Kaspersky Anti-Virus menüje az alábbi pontokat tartalmazza:

- **Feladatkezelő** – megnyitja a **Feladatkezelő** ablakát.
- **Frissítés** – az alkalmazás adatbázisainak és moduljainak a frissítése.
- **Virtuális billentyűzet** – megjeleníti a Virtuális billentyűzetet.
- **Kaspersky Anti-Virus** – megnyitja az alkalmazás főablakát.
- **Védelem felfüggesztése / Védelem folytatása** – ideiglenesen letiltja / engedélyezi a valós idejű védelmi összetevőket. Ez a menüpont nincs hatással az alkalmazás frissítéseire, sem a víruskeresés végrehajtására.
- **Beállítások** – megnyitja az alkalmazás beállításait tartalmazó ablakot.
- **Névjegy** – megnyitja az alkalmazással kapcsolatos információkat tartalmazó ablakot.
- **Hírek** – megnyitja a Hírügynök ablakát (lásd: „Hírügynök”, [33.](#) oldal). Ez a menüelem akkor látható, ha vannak olvasatlan hírek.
- **Kilépés** – bezárja a Kaspersky Anti-Virus alkalmazást (az elem kiválasztása esetén az alkalmazás kikerül a számítógép RAM memóriájából).



1. ábra: A helyi menü

Ha a helyi menü megnyitásakor víruskeresési feladat vagy frissítés fut, akkor annak neve és (százalékos) készültségi állapota megjelenik a helyi menüben. Ha kiválaszt egy olyan menüelemet, amelyik egy feladat nevét tartalmazza, átválthat a főablakra a feladat futtatásának eredményeit tartalmazó jelentés megtekintéséhez.

### ➔ A helyi menü megnyitásához

vigye az egeret az alkalmazás ikonja fölé a tálca értesítési területén, majd kattintson rá a jobb egérgombbal.

A Microsoft Windows 7 operációs rendszer esetében az alkalmazás ikonja alapértelmezésben el van rejtve, de az alkalmazás könnyebb eléréséhez megjelenítheti azt (lásd az operációs rendszer dokumentációját).

## A KASPERSKY ANTI-VIRUS FŐABLAKA

A alkalmazás főablaka a felhasználói felület azon elemeit tartalmazza, amelyekkel elérhetők az alkalmazás fontosabb funkciói.

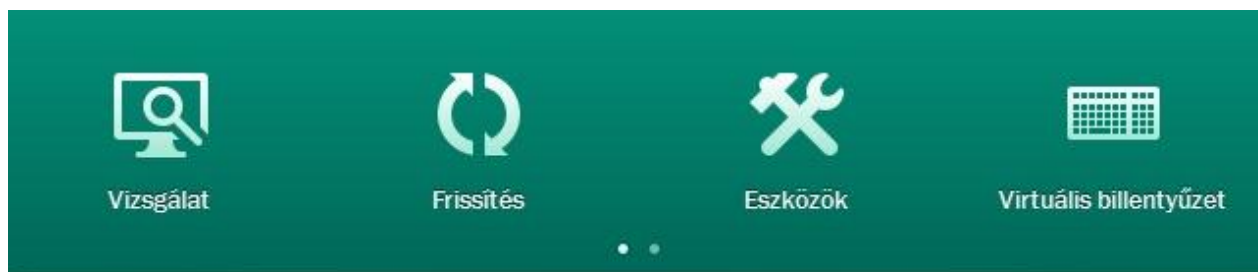
A főablak két részre osztható:

- Az ablak felső része információkat a számítógép védelmének állapotáról tartalmaz információkat.



2. ábra: A főablak felső része

- Az ablak alsó részében gyorsan válthat az alkalmazások fő funkcióinak használatára (például víruskeresési feladatok futtatása, adatbázisok és a szoftvermodulok frissítése).



3. ábra: A főablak alsó része

Ha kiválasztja valamelyik részt az ablak alsó részében, megnyílik az ahhoz tartozó funkció. Az ablak bal felső sarkában található **Vissza** gomb segítségével visszatérhet a funkcióválasztáshoz.

Az alábbi gombokat és hivatkozásokat is használhatja:

- **Cloud védelem** – váltás a Kaspersky Security Networktel kapcsolatos információkra ([107.](#) oldal).
- **Beállítások** – az alkalmazás beállítási ablakának megnyitása (lásd: „Az alkalmazás beállítási ablaka”, [31.](#) oldal).
- **Jelentések** – az alkalmazás működéséről tájékoztató jelentések megjelenítése.
- **Hírek** – a hírek megtekintése a Hírügynök ablakban (lásd: „Hírügynök”, [33.](#) oldal). A hivatkozás azt követően jelenik meg, hogy az alkalmazás megkapta az első híreket.
- **Súgó** – a Kaspersky Anti-Virus súgórendszerének megtekintése.
- **Saját Kaspersky fiók** – a felhasználó saját fiókjának megtekintése a Terméktámogatási szolgáltatás webhelyén.
- **Támogatás** – a rendszerrel kapcsolatos információkat és a Kaspersky Lab információforrásaira mutató hivatkozásokat tartalmazó ablak megnyitása (Terméktámogatási szolgáltatás webhelye, fórum).
- **Licenc kezelése** – a Kaspersky Anti-Virus aktiválási és licencmegújítási ablakának megnyitása.

➔ Az alkalmazás főablakát a következő műveletekkel nyithatja meg:

- A bal egérgombbal az alkalmazás ikonjára kattintva a tálca értesítési területén.

A Microsoft Windows 7 operációs rendszer esetében az alkalmazás ikonja alapértelmezésben el van rejtve, de az alkalmazás könnyebb eléréséhez megjelenítheti azt (lásd az operációs rendszer dokumentációját).

- A **Kaspersky Anti-Virus** elem kiválasztásával a helyi menüből (lásd: „A helyi menü”, 28. oldal).
- A Kaspersky Anti-Virus ikonra kattintva a Kaspersky Gadget közepén (csak Microsoft Windows Vista és Microsoft Windows 7 esetén).

## ÉRTEŚITĒSI ABLAKOK ÉS FELUGRÓ ÜZENETEK

A Kaspersky Anti-Virus *értesítési ablakkal* és a tálca értesítési területén az alkalmazás ikonja fölött megjelenő *felugró üzenetekkel* értesíti Önt a működése során előforduló fontos eseményekről.

*Értesítési ablakok* akkor jelennek meg, amikor a Kaspersky Anti-Virus egy eseménnyel kapcsolatban több műveletet is elvégezhet: például rosszindulatú objektum észlelése esetén blokkolhatja a hozzáférést, törölheti, de megpróbálhatja vírusmentesíteni is. Az alkalmazás felkéri, hogy válasszon az elérhető műveletekből. Az értesítési ablak csak akkor tűnik el, ha Ön kiválaszt egy műveletet.



4. ábra: Az Értesítések ablak

*Felugró üzenetek* akkor jelennek meg, ha a Kaspersky Anti-Virus olyan eseményről szeretné informálni Önt, amely nem igényli a beavatkozását. Néhány felugró üzenet olyan hivatkozást tartalmaz, amelyet az alkalmazás által javasolt művelethez használhat: például egy adatbázisfrissítés futtatása vagy alkalmazás aktiválásának elindítása). A felugró üzenetek a feltűnésük után hamarosan automatikusan el is tűnnek.



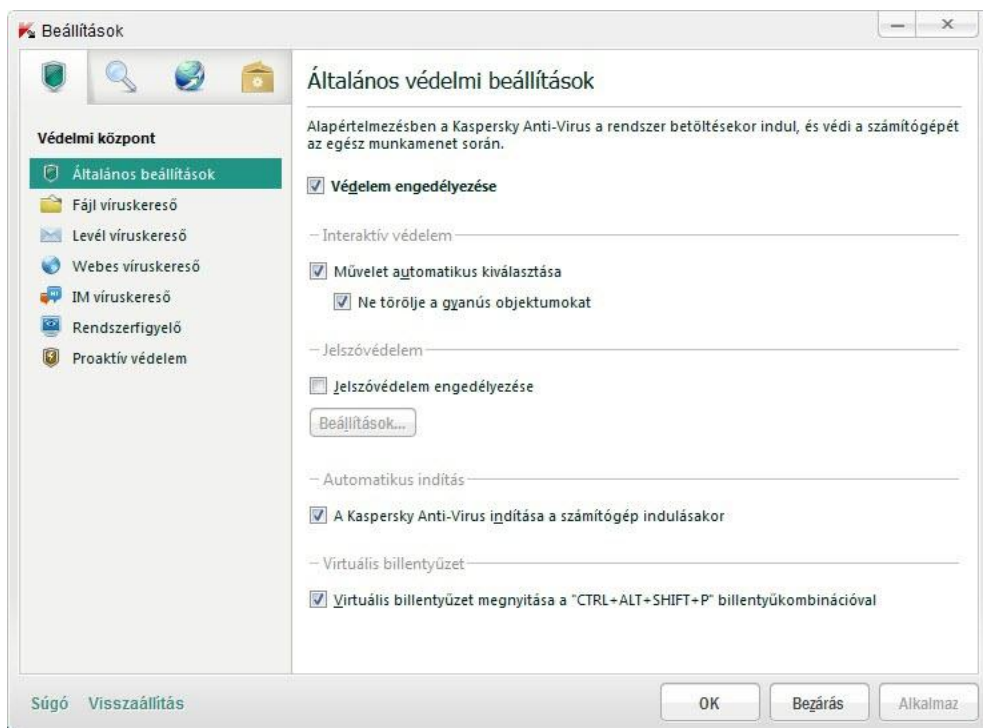
5. ábra: Felugró üzenet

Az eseményeknek a számítógép biztonsága szerinti fontossága alapján az értesítések és a felugró ablakok három csoportba sorolhatók:

- **Kritikus értesítések** – olyan eseményekről tájékoztatnak, melyek kritikus fontosságúak a számítógép biztonsága szempontjából, például egy rosszindulatú objektum észleléséről vagy a rendszerben észlelt veszélyes tevékenységről. A kritikus értesítések ablakai és felugró üzenetei piros színűek.
- **Fontos értesítések** – olyan eseményekről tájékoztatnak, melyek potenciálisan fontosak a számítógép biztonsága szempontjából, például egy potenciálisan fertőzött objektum észleléséről vagy a rendszerben észlelt gyanús tevékenységről. A fontos értesítések ablakai és felugró üzenetei sárga színűek.
- **Információs értesítések** – olyan eseményekről tájékoztatnak, melyek nem kritikus fontosságúak a számítógép biztonságára nézve. Az információs értesítések ablakai és felugró üzenetei zöld színűek.

## AZ ALKALMAZÁS BEÁLLÍTÁSI ABLAKA

A Kaspersky Anti-Virus beállítási ablakában (más néven „beállítási ablak”) konfigurálható a teljes alkalmazás, az egyes védelmi összetevők, a vizsgálati és frissítési feladatok, valamint egyéb speciális konfigurációs feladatok (lásd: „Az alkalmazás speciális beállításai”, 55. oldal).



6. ábra: Az alkalmazás beállítási ablak

Az alkalmazás beállításainak megadására szolgáló ablak két részből áll:

- a bal oldalon választhatja ki az alkalmazás összetevőjét, feladatokat vagy egyéb beállítani kívánt elemet;
- a jobb oldal tartalmazza azokat a kezelőszerveket, amelyekkel beállítható az ablak bal oldalában kiválasztott elem.

Az összetevők, feladatok és más elemek az ablak bal oldalán a következő részekben vannak összegyűjtve:



– Védelmi központ;



– Vizsgálat;




– Frissítés;



– Speciális beállítások.

A Védelem felfüggesztése ablakot az alábbi módszerek egyikével nyithatja meg:

- a **Beállítások** hivatkozásra kattintva az alkalmazás főablakának felső részén (lásd: „A Kaspersky Anti-Virus főablaka”, [29.](#) oldal);
- a **Beállítások** elem kiválasztásával a helyi menüből (lásd: „A helyi menü”, [28.](#) oldal);
- a  **Beállítások** ikonra kattintva a Kaspersky Gadget felületen (csak Microsoft Windows Vista és Microsoft Windows 7 operációs rendszereknél). A beállítási ablak megnyitására szolgáló funkciót hozzá kell rendelni a gombhoz (lásd: „A Kaspersky Gadget használata”, [53.](#) oldal).

## A KASPERSKY GADGET

Ha a Kaspersky Anti-Virus alkalmazást Microsoft Windows Vista vagy Microsoft Windows 7 alatt használja, akkor a Kaspersky Gadget alkalmazást (a továbbiakban *gadget*) is használhatja. A Kaspersky Gadget gyors hozzáférést biztosít az alkalmazás fő funkcióihoz (például védelmi állapot jelzése, objektumok vírusellenőrzése, alkalmazás működési jelentései stb.).

Ha a Kaspersky Anti-Virus alkalmazást Microsoft Windows 7 alá telepítette, a Kaspersky Gadget automatikusan megjelenik az asztalon. Ha az alkalmazást Microsoft Windows Vista alá telepítette, az eszközt manuálisan kell felvennie a Microsoft Windows Oldalsávra (lásd az operációs rendszer dokumentációját).





7. ábra: A Kaspersky Gadget

## HÍRÜGYNÖK

A *Hírügynök* segítségével informálja Önt a Kaspersky Lab a Kaspersky Anti-Virus összetevővel kapcsolatos fontos eseményekről és a számítógépet érő fenyegetések elleni védelemről.

Az alkalmazás a tálca értesítési területén megjelenített speciális ikonnal és felugró üzenetben értesíti a hírekről (lásd alább). Az alkalmazás főablakában az olvasatlan hírek számával kapcsolatos információ is megjelenik. Egy hírek ikon jelenik meg a Kaspersky Anti-Virus gadget felületén.

A híreket az alábbi módokon olvashatja el:

- a  ikonra kattintva a tálca értesítési területén;
- kattintson a felugró hírek üzenet **Hírek olvasása** hivatkozására;
- a **Hírek** hivatkozásra kattintva az alkalmazás főablakában;
- a Gadget közepén megjelenő  ikonra kattintva, amely akkor jelenik meg, amikor új hír érkezik (csak Microsoft Windows Vista és Microsoft Windows 7 esetén).

A Hírügynök megnyitásának fent ismertetett módszerei csak akkor működnek, ha vannak olvasatlan hírek.

Ha nem szeretne híreket kapni, letilthatja a hírszolgáltatást.

# AZ ALKALMAZÁS ELINDÍTÁSA ÉS LEÁLLÍTÁSA

Ebben a részben az alkalmazás indításával és leállításával kapcsolatosan találhatók információk.

## EBBEN A RÉSZBEN:

Az automatikus indítás engedélyezése és letiltása .....	<a href="#">34</a>
Az alkalmazás kézi elindítása és leállítása.....	<a href="#">34</a>

## AZ AUTOMATIKUS INDÍTÁS ENGEDÉLYEZÉSE ÉS LETILTÁSA

Az alkalmazás automatikus indítása azt jelenti, hogy az operációs rendszer betöltődése után elindul a Kaspersky Anti-Virus. Ez az alapértelmezett indítási mód.

- *Az alkalmazás automatikus indításának letiltása vagy engedélyezése:*
  1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
  2. A megnyíló ablak bal oldalának **Védelmi központ** részben válassza ki az **Általános beállítások** összetevőt.
  3. Az alkalmazás automatikus indításának kikapcsolásához szüntesse meg **A Kaspersky Anti-Virus indítása a számítógép indulásakor** négyzet bejelölését az **Automatikus indítás** részben az ablak jobb oldalán. Jelölje be a négyzetet az alkalmazás automatikus indításához.

## AZ ALKALMAZÁS KÉZI ELINDÍTÁSA ÉS LEÁLLÍTÁSA

A Kaspersky Lab szakemberei nem javasolják a Kaspersky Anti-Virus leállítását, mert ekkor veszélybe kerül a számítógép és a személyes adatok védelme. Javasoljuk, hogy az alkalmazás védelmét annak bezárása nélkül ideiglenesen szüneteltesse.

A Kaspersky Anti-Virus alkalmazást manuálisan kell elindítani, ha kikapcsolta az alkalmazás automatikus indítását (lásd: „Automatikus indítás be- és kikapcsolása”, [34.](#) oldal).

- *Az alkalmazás kézi elindításához*  
a **Start** menüben válassza ki a **Programok** → **Kaspersky Anti-Virus 2012** → **Kaspersky Anti-Virus 2012** elemet.
- *Az alkalmazás bezárásához*  
válassza ki a tálca értesítési területén található alkalmazásikon jobb kattintással elérhető helyi menüjének **Kilépés** elemét.

A Microsoft Windows 7 operációs rendszer esetében az alkalmazás ikonja alapértelmezésben el van rejtve, de az alkalmazás könnyebb eléréséhez megjelenítheti azt (lásd az operációs rendszer dokumentációját).

# A SZÁMÍTÓGÉP VÉDELMÉNEK KEZELÉSE

Ez a rész tájékoztatást nyújt a számítógép biztonságát veszélyeztető fenyegetések felismeréséről és a biztonsági szint beállításáról. Olvassa el ezt a részt, hogy többet megtudjon a védelem engedélyezéséről, letiltásáról és felfüggesztéséről az alkalmazás használata során.

## EBBEN A RÉSZBEN:

A számítógép védelmével kapcsolatos problémák diagnosztizálása és megszüntetése .....	<a href="#">35</a>
A védelem engedélyezése és letiltása .....	<a href="#">36</a>
Védelem felfüggesztése és folytatása .....	<a href="#">37</a>

## A SZÁMÍTÓGÉP VÉDELMÉVEL KAPCSOLATOS PROBLÉMÁK DIAGNOSZTIZÁLÁSA ÉS MEGSZÜNTETÉSE

A számítógép védelmével kapcsolatos problémákat a számítógép védelmi állapotának ikonja jelzi az alkalmazás főablakának bal oldalán (lásd: „A Kaspersky Anti-Virus főablaka”, [29.](#) oldal). A jelző egy monitor alakú ikon, amelynek színe a számítógép védelmi állapotától függően változik: a zöld szín azt jelenti, hogy a számítógép védelem alatt áll, a sárga szín védelemmel kapcsolatos problémákra utal, a piros szín pedig a számítógép biztonságát súlyosan veszélyeztető fenyegetésre utal.



8. ábra: A védelem állapotjelzője

A felmerült problémák és biztonsági fenyegetések azonnali orvoslása javasolt.

A jelző ikonjára kattintva az alkalmazás főablakában megnyílik a **Biztonsági problémák** ablak (lásd az alábbi ábrát), amely részletes információt tartalmaz a számítógép védelmének állapotáról, valamint az észlelt problémák és fenyegetések megszüntetésének lehetőségeiről.



9. ábra: A Biztonsági problémák ablak

A védelem problémái kategóriák szerint vannak csoportosítva. Minden probléma mellett fel vannak sorolva a megoldásához használható műveletek.

## A VÉDELEM ENGEDÉLYEZÉSE ÉS LETILTÁSA

Alapértelmezésben a Kaspersky Anti-Virus az operációs rendszer betöltődésekor indul el, és a kikapcsolásáig folyamatosan védi a számítógépet. Minden védelmi összetevő működik.

Az Kaspersky Anti-Virus által nyújtott védelmet teljesen vagy részlegesen is letilthatja.

A Kaspersky Lab szakemberei ugyanakkor erősen javasolják, hogy ne tiltsa le a védelmet, mert az a számítógép fertőzéséhez és adatvesztéshez vezethet. Javasoljuk, hogy csak függesse fel a számítógép védelmét a szükséges időtartamra (lásd: „Védelem felfüggesztése és folytatása”, [37.](#) oldal).

Az alábbi jelek utalnak arra, hogy a védelem szünetel, vagy le van tiltva:

- inaktív (szürke) alkalmazás ikon a tálca értesítési területén (lásd: „Az értesítési terület ikonja”, [27.](#) oldal);
- a biztonságjelző piros színe az alkalmazás főablakának felső részén.

Ebben az esetben a védelmet a védelmi komponensek tekintetében kell megvizsgálni. A védelmi összetevők letiltása vagy felfüggesztése nincs hatással a víruskeresési feladatokra és a Kaspersky Anti-Virus frissítéseire.

Engedélyezheti vagy letilthatja a védelmet vagy az alkalmazás egyes összetevőit is az alkalmazás beállítási ablakában (lásd: „Az alkalmazás beállítási ablaka”, [31.](#) oldal).

➤ *A védelem teljes letiltása vagy engedélyezése:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. A megnyíló ablak bal oldalának **Védelmi központ** részben válassza ki az **Általános beállítások** összetevőt.
3. Szüntesse meg a **Védelem engedélyezése** négyzet bejelölését, ha le szeretné tiltani a védelmet. Jelölje be a négyzetet, ha engedélyezni szeretné a védelmet.

➤ *Egy védelmi összetevő letiltása vagy engedélyezése:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldali részének **Védelmi központ** részében válassza ki az engedélyezni vagy letiltani kívánt összetevőt.
3. Az ablak jobb oldalán szüntesse meg az **<Összetevő neve> engedélyezése** négyzet bejelölését, ha le szeretné tiltani ezt az összetevőt. Jelölje be a négyzetet, ha engedélyezni szeretné az összetevő működését.

## VÉDELEM FELFÜGGESZTÉSE ÉS FOLYTATÁSA

A védelem felfüggesztése valamennyi védelmi összetevő ideiglenes kikapcsolását jelenti.

Az alábbi jelek utalnak arra, hogy a védelem szünetel, vagy le van tiltva:

- inaktív (szürke) alkalmazás ikon a tálca értesítési területén (lásd: „Az értesítési terület ikonja”, [27.](#) oldal);
- a biztonságjelző piros színe az alkalmazás főablakának felső részén.

Ebben az esetben a védelmet a védelmi komponensek tekintetében kell megvizsgálni. A védelmi összetevők letiltása vagy felfüggesztése nincs hatással a víruskeresési feladatokra és a Kaspersky Anti-Virus frissítéseire.

Ha a védelem felfüggesztésének pillanatában hálózati kapcsolatokat létesítettek, értesítés jelenik meg mindezen kapcsolatok bontásáról.

Ha Microsoft Windows Vista vagy Microsoft Windows 7 operációs rendszert futtató számítógépet használ, a védelmet a Kaspersky Gadget segítségével is felfüggesztheti. Ehhez hozzá kell rendelnie a védelem felfüggesztése funkciót a gadget egyik gombjához (lásd: „A Kaspersky Gadget használata”, [53.](#) oldal).

➤ *A számítógép védelmének felfüggesztése:*

1. Nyissa meg a **Védelem felfüggesztése** ablakot az alábbi módszerek egyikével:
  - válassza a **Védelem felfüggesztése** elemet az alkalmazás ikonjának helyi menüjéből (lásd: „A helyi menü”, [28.](#) oldal);
  - kattintson a **Védelem felfüggesztése** ikonra a Kaspersky Gadget felületen (csak Microsoft Windows Vista és Microsoft Windows 7 operációs rendszereknél).
2. A **Védelem felfüggesztése** ablakban adja meg, hogy mennyi idő elteltével folytatódjon a védelem:
  - **Felfüggesztés a megadott időre** – a védelem az alábbi legördülő listából kiválasztott idő leteltekor lesz újra engedélyezve.
  - **Felfüggesztés újraindításig** – a védelem az alkalmazás vagy az operációs rendszer újraindításakor lesz újra engedélyezve (feltéve, hogy az alkalmazás automatikus indítása be van állítva (lásd: „Az automatikus indítás engedélyezése és letiltása”, [34.](#) oldal)).
  - **Felfüggesztés** – a védelem akkor lesz újra engedélyezve, ha Ön dönt a védelem folytatásáról (lásd alább).

➤ *A számítógép védelmének folytatásához:*

válassza a **Védelem folytatása** elemet az alkalmazás ikonjának helyi menüjéből (lásd: „A helyi menü”, [28.](#) oldal).

A számítógép védelmének folytatására ezt a módszert akkor használhatja, ha korábban a **Felfüggesztés**, a **Felfüggesztés a megadott időre** vagy **Felfüggesztés újraindításig** lehetőségeket valamelyikét választotta.

# TIPIKUS FELADATOK MEGOLDÁSA

Ez a rész tájékoztatást nyújt arról, hogyan lehet megoldani a számítógép védelmével kapcsolatos leggyakoribb problémákat az alkalmazás segítségével.

## EBBEN A RÉSZBEN:

Az alkalmazás aktiválásának módja.....	<a href="#">38</a>
Licenc vásárlása vagy megújítása .....	<a href="#">39</a>
Teendők az alkalmazás által megjelenített értesítésekkel.....	<a href="#">40</a>
Az alkalmazás adatbázisainak és alkalmazásmóduljainak frissítése .....	<a href="#">40</a>
Vírusok keresése a számítógép kritikus részein .....	<a href="#">40</a>
Objektum (fájl, mappa, meghajtó) vírusellenőrzése .....	<a href="#">41</a>
Vírusok keresése a számítógépen teljes vizsgálattal .....	<a href="#">42</a>
Számítógép sebezhetőségének vizsgálata .....	<a href="#">42</a>
Személyi adatok eltulajdonítás elleni védelme .....	<a href="#">43</a>
Teendők vírus által fertőzöttnek vélt objektummal .....	<a href="#">44</a>
Teendők vírus által fertőzöttnek vélt számítógéppel .....	<a href="#">45</a>
Az alkalmazás által törölt vagy vírusmentesített fájl visszaállítása .....	<a href="#">46</a>
Helyreállító-lemez létrehozása és használata .....	<a href="#">46</a>
Az alkalmazás működéséről szóló jelentés megtekintése.....	<a href="#">49</a>
Az alkalmazás alapértelmezett beállításainak visszaállítása.....	<a href="#">49</a>
A beállítások átvitele egy másik számítógépre telepített Kaspersky Anti-Virus alkalmazásba.....	<a href="#">50</a>
Átkapcsolás a Kaspersky Anti-Virus alkalmazásról Kaspersky Internet Security alkalmazásra .....	<a href="#">51</a>
A Kaspersky Gadget használata .....	<a href="#">53</a>
Alkalmazás reputációjának ellenőrzése .....	<a href="#">54</a>

## AZ ALKALMAZÁS AKTIVÁLÁSÁNAK MÓDJA

Az *Aktiválás* annak a licencnek az aktiválását jelenti, amellyel annak lejártáig az alkalmazás teljesen funkcionális verzióját használhatja.

Ha nem aktiválta az alkalmazást a telepítés során, azt később is megteheti. Az alkalmazás aktiválására a tálca értesítési területén megjelenő Kaspersky Anti-Virus üzenetek emlékeztetik.

➤ *A Kaspersky Anti-Virus aktiváló varázslójának futtatásához tegye a következőket:*

- Kattintson az **Aktiválás** hivatkozásra a Kaspersky Anti-Virus értesítési ablakában, amely a tálca értesítési területén jelenik meg.
- Kattintson az **Adja meg itt az aktiváló kódot** hivatkozásra az alkalmazás főablakának alsó részén. A megnyíló **Licenc kezelése** ablakban kattintson az **Alkalmazás aktiválása** gombra.

Az alkalmazás aktiváló varázsló használata során számos beállítás értékét meg kell adnia.

### 1. lépés: Aktiváló kód beírása

Írja be az aktiváló kódot a megfelelő mezőbe, és kattintson a **Tovább** gombra.

## 2. lépés: Aktiválás kérése

Ha az aktiválási kérés küldése sikeres, a varázsló automatikusan a következő lépéssel folytatja.

## 3. lépés: A regisztrációs adatok megadása

A felhasználó regisztrálására a Terméktámogatási szolgáltatás eléréséhez van szükség. A nem regisztrált felhasználók csak minimális támogatást kapnak.

Adja meg a regisztrációs adatokat, és kattintson a **Tovább** gombra.

## 4. lépés: Aktiválás

Ha az aktiválási sikeres, a varázsló automatikusan a következő lépéssel folytatja.

## 5. lépés: Varázsló befejezése

Ez az ablak az aktiválás eredményeivel kapcsolatos információkat mutatja: a használt licence típusát és lejáratának dátumát.

Nyomja meg a **Befejezés** gombot a varázsló bezárásához.

# LICENC VÁSÁRLÁSA VAGY MEGÚJÍTÁSA

Ha licenc nélkül telepítette a Kaspersky Anti-Virus alkalmazást, a telepítés után megvásárolhatja. Licenc vásárlásakor kap egy aktiváló kódot, amivel aktiválhatja az alkalmazást (lásd: „Az alkalmazás aktiválásának módja”, [38.](#) oldal).

Ha a licenc lejár, megújíthatja. Vásárolhat egy új licencet a jelenlegi aktiváló kód érvényességi időszakának lejáta előtt. Ehhez hozzá kell adnia egy új kódot tartalék aktiváló kódként. Amikor az aktuális licenc érvényességi ideje lejár, a Kaspersky Anti-Virus automatikusan a tartalék aktiváló kóddal lesz aktiválva.

### ► *Licencvásárlás:*

1. Nyissa meg az alkalmazás főablakát.
2. Kattintson a főablak alján a **Licenc kezelése** hivatkozásra a **Licenc kezelése** ablak megnyitásához.
3. A megnyíló ablakban kattintson a **Aktiváló kód vásárlása** gombra.  
Megnyílik az eStore weboldal, ahol megvásárolhatja a licencet.

### ► *Tartalék aktiváló kód hozzáadása:*

1. Nyissa meg az alkalmazás főablakát.
2. Kattintson a főablak alján a **Licenc kezelése** hivatkozásra a **Licenc kezelése** ablak megnyitásához.  
Megnyílik a **Licenc kezelése** ablak.
3. A megnyíló ablak **Új aktiváló kód** részben kattintson az **Aktiváló kód beírása** gombra.  
Megnyílik az Alkalmazás aktiválása varázsló.
4. Írja be az aktiváló kódot a megfelelő mezőkbe, és kattintson a **Tovább** gombra.  
Ekkor a Kaspersky Anti-Virus ellenőrzésre elküldi az adatokat az aktiválási kiszolgálóra. Ha az ellenőrzés sikeres, a Varázsló automatikusan továbblép a következő lépésre.
5. Válassza az **Új kód** lehetőséget, majd kattintson a **Tovább** gombra.
6. Ha végzett a Varázslóval, kattintson a **Befejezés** gombra.

## TEENDŐK AZ ALKALMAZÁS ÁLTAL MEGJELÉNÍTETT ÉRTESEKSEL

A feladatsáv értesítési területén megjelenő alkalmazásértesítések informálják Önt az alkalmazás működése során előforduló, figyelmet igénylő eseményekről. Attól függően, hogy az esemény mennyire érinti a számítógép biztonságát, az alábbi értesítések valamelyike jelenik meg:

- **Kritikus értesítések** – olyan eseményekről tájékoztatnak, melyek kritikus fontosságúak a számítógép biztonsága szempontjából, például egy rosszindulatú objektum észleléséről vagy a rendszerben észlelt veszélyes tevékenységről. A kritikus értesítések ablakai és felugró üzenetei piros színűek.
- **Fontos értesítések** – olyan eseményekről tájékoztatnak, melyek potenciálisan fontosak a számítógép biztonsága szempontjából, például egy potenciálisan fertőzött objektum észleléséről vagy a rendszerben észlelt gyanús tevékenységről. A fontos értesítések ablakai és felugró üzenetei sárga színűek.
- **Információs értesítések** – olyan eseményekről tájékoztatnak, melyek nem kritikus fontosságúak a számítógép biztonságára nézve. Az információs értesítések ablakai és felugró üzenetei zöld színűek.

Ha ilyen értesítés jelenik meg a képernyőn, választania kell egyet a javasolt opciók közül. Alapértelmezésben az optimális beállítás az, amelyet a Kaspersky Lab szakértői ajánlanak.

## AZ ALKALMAZÁS ADATBÁZISAINAK ÉS ALKALMAZÁSMODULJAINAK FRISSÍTÉSE

Alapértelmezés szerint a Kaspersky Anti-Virus automatikusan ellenőrzi, hogy vannak-e frissítések a Kaspersky Lab frissítéskiszolgálóján. Ha a kiszolgálón megtalálhatók a legújabb frissítések, a Kaspersky Anti-Virus a háttérben letölti és telepíti azokat. A Kaspersky Anti-Virus frissítését manuálisan bármikor elindíthatja.

A frissítések Kaspersky Lab kiszolgálóiról való letöltéséhez kapcsolódnia kell az Internetre.

### ➤ *Frissítés indítása a helyi menüből:*

válassza ki a **Frissítés** elemet az alkalmazás ikonjának a helyi menüjéből.

### ➤ *Frissítés indítása az alkalmazás főablakában:*

1. Nyissa meg az alkalmazás főablakát, és válassza ki a **Frissítés** részt az ablak alsó részén.
2. A megnyíló **Frissítés** ablakban kattintson a **Frissítés futtatása** gombra.

## VÍRUSOK KERESÉSE A SZÁMÍTÓGÉP KRITIKUS RÉSZEIN

A kritikus területek vizsgálata az alábbi objektumok vizsgálatát jelenti:

- az operációs rendszer indulásakor betöltődő objektumok;
- rendszermemória;
- a lemez indítószektorai;
- felhasználó által felvettobjektumok (lásd: „Vizsgálendő objektumok listájának létrehozása”, [59.](#) oldal).


A kritikus területek vizsgálatát az alábbi módok valamelyikén kezdheti el:

- egy korábban létrehozott parancsikkal (lásd [63.](#) oldal).
- az alkalmazás főablakából (lásd: „A Kaspersky Anti-Virus főablaka”, [29.](#) oldal).

### ➤ *Vizsgálat indítása parancsikkal:*

1. Nyissa meg a Microsoft Windows Explorer ablakát, és keresse meg a mappát, ahova a parancsikont létrehozta.
2. Kattintson duplán a parancsikonra a vizsgálat elindításához.

➤ *A vizsgálat indítása az alkalmazás főablakában:*

1. Nyissa meg az alkalmazás főablakát, és válassza ki a **Vizsgálat** részt az ablak alsó részén.
2. A megnyíló **Vizsgálat** ablak **Kritikus területek vizsgálata** részében kattintson a  gombra.

## OBJEKTUM (FÁJL, MAPPA, MEGHAJTÓ) VÍRUSELLENŐRZÉSE

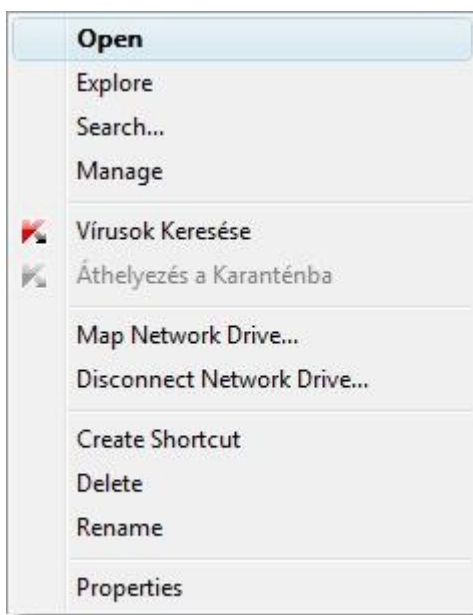
Objektum vírusellenőrzésére az alábbi módszerek használhatók:

- az objektum helyi menüjének használatával;
- az alkalmazás főablakából (lásd: „A Kaspersky Anti-Virus főablaka”, [29.](#) oldal);
- a Kaspersky Anti-Virus gadget használatával (csak Microsoft Windows Vista és Microsoft Windows 7 operációs rendszereknél).

➤ *Víruskeresés indítása az objektum helyi menüjéből:*

1. Nyissa meg a Microsoft Windows Explorer ablakát, és keresse meg az ellenőrizendő objektum mappáját.
2. Jobb kattintással nyissa meg az objektum helyi menüjét (lásd az alábbi ábrát), és válassza a **Vírusok keresése** elemet.

A feladat végrehajtásának előrehaladása és eredménye a **Feladatkezelő** ablakban jelenik meg.

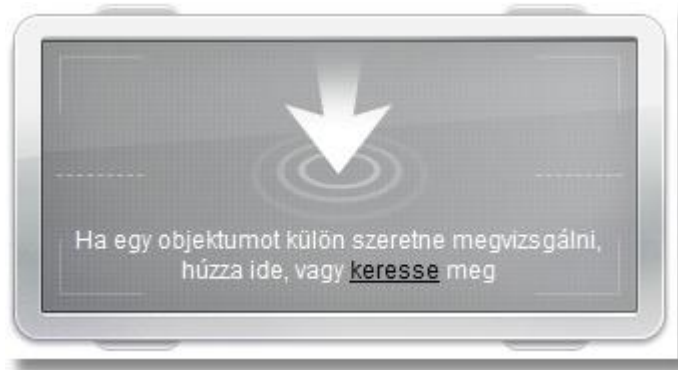


10. ábra: Objektum helyi menüje Microsoft Windows alatt

➤ *Objektum vizsgálatának indítása az alkalmazás főablakából:*

1. Nyissa meg az alkalmazás főablakát, és válassza ki a **Vizsgálat** részt az ablak alsó részén.
2. Határozza meg a megvizsgálandó objektumot az alábbi módszerek egyikével:
  - Kattintson a **keresse** hivatkozásra az ablak jobb alsó részében az **Egyedi vizsgálat** ablak megnyitásához, majd jelölje be a négyzeteket a vizsgálandó mappák és meghajtók mellett.  
Ha a megjelenő ablak nem tartalmaz vizsgálandó objektumot:
    - a. Kattintson a **Hozzáadás** gombra.
    - b. A megnyíló **Objektumok kijelölése vizsgálatra** ablakban jelöljön ki egy vizsgálandó objektumot.
  - A megvizsgálandó objektumot húzza át a főablak kijelölt területére (lásd az alábbi ábrát).

A feladat végrehajtásának előrehaladása a **Feladatkezelő** ablakban jelenik meg.



11, ábra: A Vizsgálat ablaknak az a része, amelybe át kell áthúznia a vizsgálandó objektumot

➤ **Objektum víruskeresése a Gadget segítségével:**

húzza a vizsgálandó objektumot a Gadgetre.

A feladat végrehajtásának előrehaladása a **Feladatkezelő** ablakban jelenik meg.

## VÍRUSOK KERESÉSE A SZÁMÍTÓGÉPEN TELJES VIZSGÁLATTAL


A teljes vizsgálat az alábbi módszerek valamelyikével indítható:

- egy korábban létrehozott parancsikonnal (lásd [63.](#) oldal);
- az alkalmazás főablakából (lásd: „A Kaspersky Anti-Virus főablaka”, [29.](#) oldal).

➤ **A teljes vizsgálat elindítása parancsikonnal:**

1. Nyissa meg a Microsoft Windows Explorer ablakát, és keresse meg a mappát, ahova a parancsikont létrehozta.
2. Kattintson duplán a parancsikontra a vizsgálat elindításához.

➤ **A teljes vizsgálat indítása az alkalmazás főablakában:**

1. Nyissa meg az alkalmazás főablakát, és válassza ki a **Vizsgálat** részt az ablak alsó részén.
2. A megnyíló **Vizsgálat** ablak **Teljes vizsgálat** részében kattintson a  gombra.

## SZÁMÍTÓGÉP SEBEZHETŐSÉGÉNEK VIZSGÁLATA

A *Sebezhetőségek* a szoftver kód olyan védtelen részei, amelyeket a betolakodók szándékosan felhasználhatnak saját céljaikra, például a védtelen alkalmazásokban használt adatok lemásolására. A számítógép sebezhetőségének vizsgálata segíti felfedni a számítógép védelmének hiányosságait. Javasolt az észlelt sebezhetőségek megszüntetése.


A következő módszerekkel végezhetők a sebezhetőségi vizsgálatok:

- az alkalmazás főablakából (lásd: „A Kaspersky Anti-Virus főablaka”, [29.](#) oldal);
- egy korábban létrehozott parancsikonnal (lásd [63.](#) oldal).

➤ **A feladat elindítása parancsikonnal:**

1. Nyissa meg a Microsoft Windows Explorer ablakát, és keresse meg a mappát, ahova a parancsikont létrehozta.
2. Kattintson duplán a parancsikontra a rendszer átvizsgálásához.

➤ **A feladat indítása az alkalmazás főablakában:**

1. Nyissa meg az alkalmazás főablakát, és válassza ki a **Vizsgálat** részt az ablak alsó részén.
2. A megnyíló **Vizsgálat** ablak **Sebezhetőségi vizsgálat** részében kattintson a  gombra.

## SZEMÉLYI ADATOK ELTULAJDONÍTÁS ELLENI VÉDELME

A Kaspersky Anti-Vírus segítségével megvédheti az alábbi személyes adatait az eltulajdonítás ellen:

- jelszavak, felhasználói nevek és más regisztrációs adatok;
- bankszámla és bankkártya számok.

A személyes adatai védelmét a Kaspersky Anti-Vírus következő összetevői és eszközei segítik:

- Adathalászat-blokkoló. Az adathalászattal összefüggő adatlopások ellen biztosít védelmet.
- Virtuális billentyűzet. Meggátolja a billentyűzeten keresztül bevitt adatok elfogását.

### EBBEN A RÉSZBEN:

Védelem adathalászat ellen .....	<a href="#">43</a>
Védelem a billentyűzeten bevitt adatok elfogása ellen .....	<a href="#">43</a>

## VÉDELEM ADATHALÁSZAT ELLEN

Az adathalászat elleni védelem a Webes víruskereső és az IM víruskereső összetevőbe épített adathalászat elleni védelem biztosítja. A Kaspersky Lab javasolja, hogy mindegyik védelmi összetevőnél engedélyezze az adathalászati ellenőrzést.

➤ *Az adathalászat elleni védelem engedélyezése a Webes víruskereső futtatásakor:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Webes víruskereső** összetevőt.
3. Kattintson a **Beállítások** gombra az ablak jobb oldali részében.
4. Megnyílik a **Webes víruskereső** ablaka.
5. A megnyíló ablak **Általános** lapjának **Kaspersky URL-tanácsadó** részben jelölje be a **Weboldalak adathalászati ellenőrzése** négyzetet.

➤ *Az adathalászat elleni védelem engedélyezése az IM víruskereső futtatásakor:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki az **IM víruskereső** összetevőt.
3. Az ablak jobb oldali részében, a **Vizsgálatmódok** részben jelölje be az **URL-ek ellenőrzése az adathalászat URL-ek adatbázisában** négyzetet.

## VÉDELEM A BILLENTYŰZETEN BEVITT ADATOK ELFOGÁSA ELLEN

Az Interneten dolgozva gyakran előfordulhat, hogy meg kell adnia személyes adatait, vagy felhasználónevét és jelszavát. Erre például akkor lehet szükség, ha felhasználói fiókot hoz létre egy webhelyen vagy internetes boltban, vagy Internetes bankolási szolgáltatást használ.

Fennáll annak a veszélye, hogy személyes adatait billentyűzetfigyelők vagy billentyűzetnaplózók elfogják. Ezek olyan programok, amelyek a billentyűleütéseket regisztrálják.

A Virtuális billentyűzet megelőzi a billentyűzeten keresztül bevitt adatok elfogását.

A Virtuális billentyűzet nem képes személyes adatai védelmére, ha a webhely, amely az ilyen adatokat kéri előzőleg lett törve, mert ekkor az információk közvetlenül a behatolóhoz jutnak.

Kémprogramként besorolt számos alkalmazás képes képernyőfelvételeket készíteni, amelyeket aztán a behatolóknak továbbít további elemzésre, és a felhasználó személyes adatainak eltulajdonítására. A Virtuális billentyűzet megelőzi a megadott adatok képernyőképek alkalmazásával történő elfogását.


A Virtuális billentyűzet a személyes adatok elfogását csak Microsoft Internet Explorer, Mozilla Firefox és Google Chrome böngészők használata esetén képes megelőzni.

A Virtuális billentyűzet az alábbi funkciókkal rendelkezik:

- A Virtuális billentyűzet gombjait az egérrel nyomhatja meg.
- A valódi billentyűzetektől eltérően a Virtuális billentyűzeten sajnos nem lehet egyszerre több gombot lenyomni. Ezért billentyűkombinációk (pl. **Alt+F4**) használatához előbb meg kell nyomnia az első gombot (pl. **ALT**), majd pedig a másodikat (pl. **F4**), végül ismét az első gombot. A gombra történő második kattintás ugyanazt jelenti, mint a gomb felengedése a valódi billentyűzeten.
- A Virtuális billentyűzet beviteli nyelve a beállítások függvényében a **CTRL+SHIFT** billentyűkombináció (a **SHIFT** gombot a jobb egérgombbal kell megnyomni) vagy a **CTRL+BAL ALT** billentyűkombináció (a **BAL ALT** gombot a jobb egérgombbal kell megnyomni) segítségével váltható.

A Virtuális billentyűzetet következő módok valamelyikével nyithatja meg:

- az alkalmazás ikonjának helyi menüjéből;
  - az alkalmazás főablakából;
  - Microsoft Internet Explorer, Mozilla Firefox vagy Google Chrome böngészőablakból;
  - billentyűzetkombináció segítségével.
- ➔ *A Virtuális billentyűzet megnyitása az alkalmazásikon helyi menüjéből:*  
válassza ki a **Virtuális billentyűzet** elemet az alkalmazás ikonjának a helyi menüjéből.
- ➔ *A Virtuális billentyűzet megnyitása az alkalmazás főablakából:*  
az alkalmazás főablakának alsó részén válassza ki a **Virtuális billentyűzet** elemet.
- ➔ *A Virtuális billentyűzet megnyitása a böngésző ablakából:*

kattintson a  **Virtuális billentyűzet** gombra a Microsoft Internet Explorer, Mozilla Firefox vagy Google Chrome eszköztárában.

- ➔ *A Virtuális billentyűzet megnyitása a számítógép billentyűzetének segítségével:*  
nyomja meg a **CTRL+ALT+SHIFT+P** kombinációt.

## TEENDŐK VÍRUS ÁLTAL FERTŐZÖTTNEK VÉLT OBJEKTUMMAL

Ha egy objektumot fertőzöttnek vél, először vizsgálta meg a Kaspersky Anti-Virus programmal (lásd: „Objektum (fájl, mappa, meghajtó) vírusellenőrzése”, [41.](#) oldal).

Ha az alkalmazás megvizsgálta egy objektumot, és abban nem jelezte rosszindulatú objektumok jelenlétét, ugyanakkor Ön ennek ellenkezőjét feltételezi, a következő műveleteket hajthatja végre:

- Az objektum áthelyezése a *Karanténba*. A karanténba helyezett objektumok nem jelentenek veszélyt a számítógépre. Az adatbázisok frissítése után a Kaspersky Anti-Virus valószínűleg már képes lesz egyértelműen azonosítani, és megszüntetni a fenyegetést.
- Az objektum elküldése *Víruslaboratóriumba*. A Víruslaboratórium specialistái megvizsgálják az objektumot. Ha kiderül, hogy vírussal fertőzött, az új vírus leírása bekerül az adatbázisokba, amelyet az alkalmazás frissítéskorlátolt (lásd: „Az alkalmazás adatbázisainak és alkalmazásmoduljainak frissítése”, [40.](#) oldal).

Fájlt az alábbi két módszerrel helyezhet a Karanténba:

- a **Karantén** ablakban található **Áthelyezés a Karanténba** gombra kattintva;
- a fájl helyi menüjének használatával.

- *Áthelyezés a Karanténba a Karantén ablakból:*
  1. Nyissa meg az alkalmazás főablakát.
  2. Az ablak alsó részén válassza ki a **Karantén** részt.
  3. A **Karantén** lapon kattintson az **Áthelyezés a Karanténba** gombra.
  4. A megnyíló ablakban válassza ki a karanténba helyezendő fájlt.
- *Fájl karanténba helyezése a helyi menü használatával:*
  1. Nyissa meg a Microsoft Windows Intézőt, és keresse meg a Karanténba helyezendő fájl mappáját.
  2. A helyi menü megnyitásához kattintson az egér jobb gombjával a fájlra, és válassza az **Áthelyezés a Karanténba** parancsot.
- *Fájl elküldése a Víruslaboratóriumba:*
  1. Lépjen a Víruslaboratórium kérési weboldalára (<http://support.kaspersky.com/virlab/helpdesk.html>).
  2. Kérése elküldéséhez kövesse az oldalon megjelenő utasításokat.

## TEENDŐK VÍRUS ÁLTAL FERTŐZÖTTNEK VÉLT SZÁMÍTÓGÉPPEL

Ha azt gyanítja, hogy az operációs rendszer rosszindulatú programok tevékenysége vagy rendszerhiba miatt megsérült, használja a *Microsoft Windows hibaelhárítás* lehetőséget a rosszindulatú objektumok nyomainak eltávolításához a rendszerből. A Kaspersky Lab azt javasolja, hogy a számítógép vírusmentesítése után futtassa ezt a varázslót, hogy a fertőzés által jelentett minden fenyegetés el legyen hárítva és az okozott kár ki legyen javítva.

A Microsoft Windows hibaelhárítás ellenőrzi a rendszert módosítások és meghibásodások (például fájlkiterjesztések módosítása, hálózati környezet vagy vezérlőpult blokkolása) tekintetében. A módosításokat és meghibásodásokat okozhatja rosszindulatú program tevékenysége, érvénytelen rendszerkonfiguráció, rendszerhibák vagy rendszeroptimalizáló alkalmazások hibás működése is.

Az ellenőrzés végeztével a varázsló elemzi az adatokat, és meghatározza, hogy van-e azonnali beavatkozást igénylő rendszerkárosodás. Az ellenőrzés alapján létrehozza a problémák megszüntetéséhez szükséges műveletek listáját. A varázsló a műveleteket az észlelt probléma súlyosságának megfelelően kategóriákba rendezi.

- *A Rendszer-visszaállítás varázsló elindítása:*
  1. Nyissa meg az alkalmazás főablakát (lásd [29.](#) oldal).
  2. Az ablak alsó részén válassza ki az **Eszközök** részt.
  3. A megnyíló ablak **Microsoft Windows hibaelhárítás** részében kattintson az **Indítás** gombra.

Megnyílik a Microsoft Windows hibaelhárítás ablaka.

A varázsló ablakok (lépések) sorozatából áll, amelyek között a **Vissza** és a **Tovább** gombokkal navigálhat. A használat befejezésekor a varázsló bezárására a **Befejezés** gomb szolgál. A varázslót bármelyik lépésnél leállíthatja a **Mégse** gombbal.

### 1. lépés: Rendszer-helyreállítás indítása

Ellenőrizze, hogy a **Rosszindulatú programok tevékenysége okozta problémák keresése** lehetőség van kiválasztva, majd kattintson a **Tovább** gombra.

### 2. lépés: Problémák keresése

A varázsló megkeresi a problémákat és sérüléseket, amelyeket aztán ki kell javítani. A keresés befejeztével a varázsló automatikusan folytatja a következő lépéssel.

### 3. lépés: Hibaelhárítási műveletek kiválasztása

A rendszer az előző lépésben talált sérüléseket veszélytípusok szerint csoportosítja. A Kaspersky Lab valamennyi sérüléscsoport esetében megjeleníti a sérülés kijavításához ajánlott műveletsort. Három műveletcsoportot különböztetünk meg:

- *Az Erősen javasolt műveletek* a biztonságot súlyosan fenyegető problémákat szüntetik meg. Javasolt az ebbe a csoportba tartozó összes művelet elvégzése.
- *A Javasolt műveletek* a potenciális fenyegetést jelentő problémákat szüntetik meg. Javasolt az ebbe a csoportba tartozó összes művelet elvégzése is.
- *A További műveletek* a rendszer olyan sérüléseinek a megszüntetésében nyújtanak segítséget, amelyek aktuális veszélyt ugyan nem jelentenek, de a számítógép jövőbeni biztonsága érdekében célszerű beavatkozások.

A műveletek megtekintéséhez egy csoporton belül kattintson a + ikonra a csoport nevével balra.

Ha azt szeretné, hogy a varázsló egy bizonyos műveletet hajtson végre, jelölje be a négyzetet az alkalmazás nevével balra. Alapértelmezésben a varázsló minden javasolt és erősen javasolt műveletet végrehajt. Ha valamelyik műveletet nem kívánja végrehajtani, szüntesse meg a mellette levő négyzet bejelölését.

**Nyomatékosan javasoljuk, hogy ne szüntesse meg az alapértelmezett bejelölt négyzetek jelölését, mert így a számítógép fenyegetéseknek lesz kitéve.**

Ha meghatározta az műveletek csoportját, amelyet a varázsló végre fog hajtani, kattintson a **Tovább** gombra.

### 4. lépés: Problémák megszüntetése

A varázsló végrehajtja az előző lépésben kiválasztott műveletet. A problémák elhárítása időbe telhet. A hibaelhárítás befejezése után a varázsló automatikusan folytatja a következő lépéssel.

### 5. lépés: Varázsló befejezése

Nyomja meg a **Befejezés** gombot a varázsló bezárásához.

## AZ ALKALMAZÁS ÁLTAL TÖRÖLT VAGY VÍRUSMENTESÍTETT FÁJL VISSZAÁLLÍTÁSA

**A Kaspersky Lab nem javasolja törölt vagy vírusmentesített fájlok helyreállítását, mert a számítógépre fenyegetést jelenthetnek.**

Törölt vagy vírusmentesített fájl helyreállítása helyett használja az alkalmazás által a vizsgálatkor létrehozott biztonsági másolatot.

➔ *Az alkalmazás által törölt vagy vírusmentesített fájl visszaállítása:*

1. Nyissa meg az alkalmazás főablakát.
2. Az ablak alsó részén válassza ki a **Karantén** részt.
3. A **Tárolás** lapon válassza ki a kívánt fájlt a listából, és kattintson a **Visszaállítás** gombra.

## HELYREÁLLÍTÓ-LEMEZ LÉTREHOZÁSA ÉS HASZNÁLATA

A Kaspersky Anti-Virus telepítése és a számítógép első vizsgálatának végrehajtása után javasolt egy Helyreállító-lemez készítése.

A helyreállító-lemez egy alkalmazás, aminek a neve Kaspersky Rescue Disk, és cserélhető adathordozón (CD vagy USB flash meghajtó) található.

A Kaspersky Rescue Disk alkalmazást a későbbiekben olyan fertőzött számítógépek vizsgálatára és vírusmentesítésére használhatja, amelyek más módszerekkel (pl. egy víruskereső alkalmazás segítségével) nem vírusmentesíthetők.

## EBBEN A RÉSZBEN:

Helyreállító-lemez létrehozása .....	47
A számítógép indítása helyreállító-lemezzel .....	49

## HELYREÁLLÍTÓ-LEMEZ LÉTREHOZÁSA

A Helyreállító-lemez létrehozása egy lemezképnek (ISO-fájl) a Kaspersky Rescue Disk friss verziójával való létrehozásából és egy cserélhető hordozóra való kiírásából áll.

Az eredeti lemezképet letöltheti a Kaspersky Lab kiszolgálóról vagy átmásolhatja egy helyi forrásról is.

A Helyreállító-lemez a *Kaspersky Rescue Disk Létrehozási varázsló* segítségével hozható létre. A varázsló által létrehozott rescued.iso fájl a számítógép merevlemezére kerül mentésre:

- Microsoft Windows XP esetén a következő mappába: Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Data\Rdisk\;
- Microsoft Windows Vista és Microsoft Windows 7 esetén pedig a következő mappába: ProgramData\Kaspersky Lab\AVP12\Data\Rdisk\.

### ➔ *Helyreállító-lemez létrehozása:*

1. Nyissa meg az alkalmazás főablakát.
2. Az ablak alsó részén válassza ki az **Eszközök** részt.
3. A megnyíló ablak **Kaspersky Rescue Disk** részében kattintson a **Létrehozás** gombra.

Megnyílik a **Kaspersky Rescue Disk Létrehozási varázsló** ablaka.

A varázsló ablakok (lépések) sorozatából áll, amelyek között a **Vissza** és a **Tovább** gombokkal navigálhat. A használat befejezésekor a varázsló bezárására a **Befejezés** gomb szolgál. A varázslót bármelyik lépésnél leállíthatja a **Mégse** gombbal.

Tekintsük át részletesebben a varázsló lépéseit.

### 1. lépés: A varázsló indítása. Meglévő lemezkép keresése

A Varázsló első ablaka a Kaspersky Rescue Diskről tartalmaz információkat.

Ha a varázsló a megadott mappában (lásd fent) egy korábban létrehozott képfájlt észlel, akkor azt az első ablakban található **Meglévő ISO-lemezkép használata** négyzetet bejelölve eredeti lemezképként használhatja. Ha a négyzetet bejelöli, az észlelt fájlt eredeti ISO-képfájként felhasználva közvetlenül a **Lemezkép frissítéssel** lépéssel folytatja (lásd alább). Szüntesse meg a négyzet kijelölését, ha nem szeretné használni az észlelt lemezképet. A varázsló a **Lemezképforrás kiválasztása** ablakra lép.

### 2. lépés: Lemezképforrás kiválasztása

Ha a varázsló első ablakában bejelölte a **Meglévő ISO-lemezkép használata** négyzetet, akkor ez a lépés kimarad.

Ennél a lépésnél kell kiválasztania a lemezkép forrását a javasolt lehetőségek közül:

- Ha már rendelkezik a Helyreállító-lemez rögzített másolatával vagy a számítógépre vagy egy helyi hálózati erőforrásra mentett ISO-lemezképpel, válassza az **ISO-lemezkép másolása helyi vagy hálózati meghajtóról** opciót.
- Ha nem rendelkezik létrehozott ISO-lemezképfájjal és le kíván tölteni egyet a Kaspersky Lab kiszolgálójáról (a fájl méret kb. 175 MB), válassza az **ISO-lemezkép letöltése a Kaspersky Lab kiszolgálójáról** opciót.

### 3. lépés: Lemezkép másolása (letöltése)

Ha a varázsló első ablakában bejelölte a **Meglévő ISO-lemezkép használata** négyzetet, akkor ez a lépés kimarad.

Ha az előző lépésben az **ISO-lemezkép másolása helyi vagy hálózati meghajtóról** opciót választotta, kattintson a **Tallózás** gombra. Miután megadta a fájl elérési útját, kattintson a **Tovább** gombra. A lemezképfájl másolásának állapota megjelenik a Varázsló ablakban.

Ha az **ISO-lemezkép letöltése a Kaspersky Lab kiszolgálójáról** opciót választotta, azonnal megjelenik a lemezkép letöltésének állapota.

Az ISO-lemezkép másolásának vagy letöltésének befejeztével a Varázsló automatikusan a következő lépésre ugrik.

### 4. lépés: Az ISO-lemezkép frissítése

Az ISO-lemezkép fájl frissítése az alábbi műveletekből áll:

- a víruskereső adatbázisok frissítése;
- a konfigurációs fájlok frissítése.

konfigurációs fájlok határozzák meg, hogy a számítógép indítható-e a Varázsló által létrehozott tartalmat tartalmazó cserélhető hordozóról (például a Kaspersky Rescue Disk fájljait tartalmazó CD / DVD-lemezről vagy USB flash meghajtóról).

A víruskereső adatbázisok frissítésekor a Kaspersky Anti-Virus utolsó frissítésekor kapottak kerülnek felhasználásra. Ha az adatbázis nem naprakész, javasolt futtatni a frissítési feladatot, és újra elindítani a Kaspersky Rescue Disk Létrehozási varázslót.

Az ISO-fájl frissítésének megkezdéséhez kattintson a **Tovább** gombra. A feladat előrehaladása megjelenik a varázsló ablakában.

### 5. lépés: A lemezkép rögzítése adathordozóra

Ennél a lépésnél a Varázsló tájékoztatja a lemezkép sikeres létrehozásáról, és felkínálja annak rögzítését egy adathordozóra.

Adathordozó megadása a Kaspersky Rescue Disk rögzítéséhez:

- A lemezkép CD / DVD-lemezre való rögzítéséhez válassza a **Rögzítés CD-/DVD-lemezre** lehetőséget, és határozza meg a hordozót, amelyre a lemezképet rögzíteni szeretné.
- A lemezkép USB tárolóeszközeire való rögzítéséhez válassza a **Másolás USB tárolóeszközeire** opciót, és adja meg az eszközt, amelyre a lemezképet rögzíteni szeretné.

A Kaspersky Lab azt ajánlja, hogy ne másolja az ISO-lemezképet nem kifejezetten adattárolásra készített eszközökre, például okostelefonra, mobiltelefonra, PDA-ra vagy MP3-lejátszóra. Az ISO-lemezképek ezen eszközökre történő másolása az eszközök hibás működését okozhatja a későbbiekben.

- A lemezképnek a számítógép merevlemezére vagy egy a hálózaton át elérhető másik számítógép merevlemezére való rögzítéséhez válassza a **Lemezkép mentése fájlba egy helyi vagy hálózati meghajtón** opciót, és adja meg a mappát, amelybe rögzíteni szeretné a lemezképet, valamint az ISO-fájl nevét.

### 6. lépés: Varázsló befejezése

A használat befejezésekor a varázsló bezárására a **Befejezés** gomb szolgál. Ha a számítógép egy vírus vagy rosszindulatú program hatása miatt nem indítható be és a Kaspersky Anti-Virus nem futtatható normál módon, az újonnan létrehozott helyreállító-lemezt használhatja a számítógép indítására (lásd [49.](#) oldal).

## A SZÁMÍTÓGÉP INDÍTÁSA HELYREÁLLÍTÓ-LEMEZRŐL

Ha az operációs rendszer vírusátadás miatt nem indítható el, használja a Helyreállító-lemezt.

Az operációs rendszer indításához egy a Kaspersky Rescue Disk másolatát tartalmazó CD / DVD-lemezt vagy USB tárolóeszközt kell használnia (lásd: „Helyreállító-lemez létrehozása”, 47. oldal).

A számítógép nem minden esetben indítható cserélhető eszközről. Ezt az üzemmódot néhány régebbi számítógéptípus nem támogatja. Mielőtt leállítaná a számítógépet, hogy azután hordozható eszközről indítsa be, ellenőrizze, hogy a művelet végrehajtható-e.

➤ *A számítógép újraindítása a Helyreállító-lemezeiről:*

1. A BIOS beállításainál engedélyezze a CD / DVD-meghajtóról vagy USB tárolóeszközről történő indítást (részletes információkat a számítógép alaplapjának a dokumentációjában talál).
2. Helyezzen be egy CD / DVD-lemezt a fertőzött számítógép CD / DVD-meghajtójába vagy csatlakoztasson egy USB tárolóeszközt, amelyre felmásolta a Kaspersky Rescue Disket.
3. Indítsa újra a számítógépet.


A Helyreállító-lemez használatával kapcsolatos részletes információkért lásd a Kaspersky Helyreállító-lemez felhasználói útmutatóját.

## AZ ALKALMAZÁS MŰKÖDÉSÉRŐL SZÓLÓ JELENTÉS MEGTEKINTÉSE

A Kaspersky Anti-Virus összetevőinek működését jelentés rögzíti. A jelentésből statisztikai információkat kaphat az alkalmazás működéséről (megismerheti például, hogy hány rosszindulatú objektumot észlelt és semlegesített az alkalmazás a megadott időintervallumban, hányszor volt frissítve az alkalmazás ugyanezen időtartam alatt, hány levélszemét üzenetet észlelt stb.).

Ha Microsoft Windows Vista vagy Microsoft Windows 7 operációs rendszert futtató számítógépet használ, a jelentéseket a Kaspersky Gadget segítségével is megnyithatja. Ehhez úgy kell beállítani a Kaspersky Gadget összetevőt, hogy a jelentések ablak megnyitására szolgáló lehetőség legyen az egyik gombhoz rendelve (lásd: „A Kaspersky Gadget használata”, 53. oldal).

➤ *Az alkalmazás működéséről szóló jelentés megtekintése:*

1. Nyissa meg a **Jelentések** ablakot az alábbi módszerek egyikével:
  - kattintson a **Jelentések** hivatkozásra az alkalmazás főablakának felső részén;
  - kattintson a  **Jelentések** ikont tartalmazó gombra a Kaspersky Gadget felületen (csak Microsoft Windows Vista és Microsoft Windows 7 operációs rendszereknél).

A **Jelentések** ablak ábrák formájában jeleníti meg az alkalmazás működésével kapcsolatos jelentéseket.

2. Ha részletes jelentést szeretne (például az egyes összetevők működési jelentéseire kíváncsi), kattintson a **Részletes jelentés** gombra a **Jelentések** ablak alsó részén.

Megnyílik a **Részletes jelentés** ablak, ahol az adatok táblázatban jelennek meg. A jelentések kényelmesebb megtekintéséhez a bejegyzések számos módon sorba rendezhetők.

## AZ ALKALMAZÁS ALAPÉRTELMEZETT BEÁLLÍTÁSAINAK VISSZAÁLLÍTÁSA

Bármikor visszatérhet a Kaspersky Anti-Virus alkalmazás Kaspersky Lab által ajánlott alapértelmezett beállításaihoz. A beállítások visszaállításához használja az *Alkalmazásbeállító varázslót*.

Amikor a varázsló befejezi a tevékenységét, minden védelmi összetevőnél az **Ajánlott** biztonsági szint kerül beállításra. A javasolt biztonsági szint visszaállításakor az alkalmazás összetevőinek korábban megadott egyes beállításai menthetők.

➤ *Az alkalmazás alapértelmezett beállításainak visszaállítása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az Alkalmazásbeállító varázslót az alábbi módokon indíthatja el:
  - kattintson a **Visszaállítás** hivatkozásra az ablak alján;
  - válassza ki az ablak bal oldalán a **Speciális beállítások Beállítások kezelése** részét, majd kattintson az **Alapértelmezett beállítások visszaállítása** rész **Visszaállítás** gombjára.

Tekintsük át részletesebben a varázsló lépéseit.

### 1. lépés: A varázsló indítása

A varázsló elindításához kattintson a **Tovább** gombra.

### 2. lépés: Beállítások helyreállítása

A varázsló ezen ablaka azt jeleníti meg, hogy a Kaspersky Anti-Virus mely védelmi összetevőinek a beállítása különbözik az alapértéktől a felhasználó által történt módosítása miatt. Ha valamelyik összetevőnél speciális beállításokat adtak meg, akkor az is megjelenik az ablakban.

Jelölje be a megtartani kívánt beállítások melletti négyzetet, majd kattintson a **Tovább** gombra.

### 3. lépés: A visszaállítás befejezése

A használat befejezésekor a varázsló bezárására a **Befejezés** gomb szolgál.

## A BEÁLLÍTÁSOK ÁTVITELE EGY MÁSIK SZÁMÍTÓGÉPRE TELEPÍTETT KASPERSKY ANTI-VIRUS ALKALMAZÁSBA

Ha befejezte a termék konfigurálását, a beállításokat egy másik számítógépre telepített Kaspersky Anti-Virus alkalmazásban is használhatja. A művelet eredményeképpen a két számítógépre telepített alkalmazás konfigurációja teljesen azonos lesz. Ez a funkció hasznos lehet, ha például a Kaspersky Anti-Virus alkalmazást az otthoni és a munkahelyi számítógépére is telepíti.

Az alkalmazás beállításai egy speciális fájlba vannak elmentve, amely átvihető egy másik számítógépre.

A Kaspersky Anti-Virus beállításai három lépésben átvihetők egy másik számítógépre:

1. Az alkalmazás beállításainak konfigurációs fájlba mentése.
2. A konfigurációs fájl átvitele a másik számítógépre (például email vagy cserélhető adathordozó segítségével).
3. A konfigurációs fájlból származó beállítások alkalmazása a másik számítógépre telepített alkalmazáson.

➤ *A Kaspersky Anti-Virus aktuális beállításainak exportálása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán, a **Speciális beállítások** részben válassza ki a **Beállítások kezelése** alpontot.
3. Kattintson a **Mentés** gombra az ablak jobb oldali részében.
4. A megnyíló ablakban adja meg a konfigurációs fájl nevét és a mentés helyét.
5. Kattintson az **OK** gombra.

➤ *Az alkalmazás beállításainak importálása az elmentett konfigurációs fájlból:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán, a **Speciális beállítások** részben válassza ki a **Beállítások kezelése** alpontot.
3. Kattintson a **Betöltés** gombra az ablak jobb oldali részében.
4. A megnyíló ablakban válassza ki a fájlt, amelyből importálni kívánja a Kaspersky Anti-Virus beállításait.
5. Kattintson az **OK** gombra.

# ÁTKAPCSOLÁS A KASPERSKY ANTI-VIRUS ALKALMAZÁSRÓL KASPERSKY INTERNET SECURITY ALKALMAZÁSRA

A Kaspersky Anti-Virus a Kaspersky Internet Security alkalmazásra való váltást fájlletöltés és szoftvertelepítés nélkül teszi lehetővé.

*Kaspersky Internet Security* – az alkalmazás arra lett létrehozva, hogy átfogó védelmet biztosítson számítógépének. Számos fejlett funkciót tartalmaz, melyek a következő modulokba vannak beépítve:

- Alkalmazásfelügyelő;
- Szülői felügyelet;
- Tűzfal;
- Behatolásmegelőzési rendszer;
- Geo szűrő;
- Veszélyes webhelyek elérésének blokkolása;
- Hálózatfigyelő;
- Levélszemét-blokkoló;
- Reklámcsíkblokkoló;
- Személyes adatok törlése;
- Biztonságos futtatás.

Ideiglenesen átkapcsolhat a Kaspersky Internet Security próbaváltozatára, hogy megismerkedhessen a funkcióival, de rögtön annak kereskedelmi verzióját is használatba veheti.

Ha előfizetéses licencet használ vagy az alkalmazást az egyik speciális régióban használja, a Kaspersky Internet Security Önnél levő változata nem teszi lehetővé a váltást a próbaverzióra.

## EBBEN A RÉSZBEN:

Átkapcsolás a kereskedelmi változatra .....	<a href="#">51</a>
Ideiglenes átkapcsolás a próbaverzióra .....	<a href="#">52</a>

## ÁTKAPCSOLÁS A KERESKEDELMELI VÁLTOZATRA

Ha a Kaspersky Internet Security kereskedelmi verziójára szeretne váltani, mindössze a kereskedelmi változat aktiváló kódjára van szüksége, amellyel aktiválhatja azt (lásd: „Az alkalmazás aktiválásának módja”, [38.](#) oldal).

### ➤ *Aktiváló kód vásárlása a Kaspersky Internet Security alkalmazáshoz:*

1. Nyissa meg az alkalmazás főablakát.
2. Válassza ki a **Frissítés** részt az ablak alsó részén.
3. A megnyíló ablakban kattintson a **Aktiváló kód vásárlása** gombra.

Ezután a rendszer átirányítja az eStore webhelyre, ahol megvásárolhatja a Kaspersky Internet Security aktiváló kódját.

Az alkalmazás egy speciális régióban vásárolta meg, vagy előfizetéses licencet használ, a **Frissítés** rész nem található meg az alkalmazás főablakában.

## IDEIGLENES ÁTKAPCSOLÁS A PRÓBAVERZIÓRA

Ideiglenesen átválthat a Kaspersky Internet Security próbaverziójának használatára, hogy kipróbálhassa annak funkcióit. Ezt követően az alkalmazás további használatához licenctet is vásárolhat.

➤ *Ideiglenes átkapcsolás a Kaspersky Internet Security alkalmazásra:*

1. Nyissa meg az alkalmazás főablakát.
2. Válassza ki a **Frissítés** részt az ablak alsó részén.
3. A megnyíló ablakban kattintson a **Próbaverzió** gombra.

Megnyílik az Alkalmazásbeállító varázsló.

Az alkalmazás egy speciális régióban vásárolta meg, vagy előfizetéses licenctet használ, a **Frissítés** rész nem található meg az alkalmazás főablakában.

Az Alkalmazásbeállító varázsló használata során számos beállítás értékét meg kell adnia.

### 1. lépés: A Kaspersky Internet Security próbaverziója aktiválásának a kérése

Ha a Kaspersky Internet Security aktiválására irányuló kérés küldése sikeres, a varázsló automatikusan a következő lépéssel folytatja.

### 2. lépés: A frissítés elindítása

Ennél a lépésnél a varázsló egy üzenetet jelenít meg a képernyőn, ami a frissítés előkövetelményeinek meglétéről tájékoztatja. A varázsló folytatásához kattintson a **Tovább** gombra.

### 3. lépés: Inkompatibilis alkalmazások eltávolítása

Ennél a lépésnél a varázsló ellenőrzi, hogy a számítógépre telepített alkalmazások valamelyike nem inkompatibilis-e Kaspersky Internet Security-vel. Ha nincs ilyen alkalmazás, a varázsló automatikusan továbblép a következő lépésre. Ha észlel ilyen alkalmazást, a varázsló kilistázza azokat egy ablakban, és megkéri Önt az eltávolításukra.

Az inkompatibilis alkalmazások eltávolítását követően elképzelhető, hogy újra kell indítania az operációs rendszert. Az operációs rendszer újraindítása után automatikusan megnyílik a varázsló, és folytatja a frissítést.

### 4. lépés: Frissítés

Ennél a lépésnél a varázsló csatlakoztatja a frissítő modulokat, ami némi időt vehet igénybe. A folyamat befejezése után a varázsló automatikusan folytatja a következő lépéssel.

### 5. lépés: Az alkalmazás újraindítása

A alkalmazás frissítésének utolsó lépéseként újra kell indítania az alkalmazást. Ehhez kattintson a varázsló ablakában a **Befejezés** gombra.

### 6. lépés: Aktiválás befejezése

Az alkalmazás újraindítása után automatikusan megnyílik a varázsló. Ha a Kaspersky Internet Security próbaváltozatát sikeresen aktiválta, a varázsló ablaka információkat jelenít meg a próbaváltozat használatának hátralevő idejéről.

### 7. lépés: Rendszerelemzés

Ebben a fázisban kerülnek összegyűjtésre a Microsoft Windows alkalmazások adatai. Ezek az alkalmazások a megbízható alkalmazások listájára kerülnek, amelyekre nem vonatkoznak a rendszeren végzett műveleteiket érintő korlátozások.

Az elemzés befejezése után a varázsló automatikusan folytatja a következő lépéssel.

## 8. lépés: A frissítés befejezése

A használat befejezésekor a varázsló bezárására a **Befejezés** gomb szolgál.

Az alkalmazásban csak egyszer lehet a Kaspersky Internet Security próbaverziójára váltani.

# A KASPERSKY GADGET HASZNÁLATA

Ha a Kaspersky Anti-Virus alkalmazást Microsoft Windows Vista vagy Microsoft Windows 7 alatt használja, akkor a Kaspersky Gadget alkalmazást (a továbbiakban *gadget*) is használhatja. Ha a Kaspersky Anti-Virus alkalmazást Microsoft Windows 7 alá telepítette, a Kaspersky Gadget automatikusan megjelenik az asztalon. Ha az alkalmazást Microsoft Windows Vista alá telepítette, az eszközt manuálisan kell felvennie a Microsoft Windows Oldalsávra (lásd az operációs rendszer dokumentációját).

A Gadget színes visszajelzője a számítógép védeltségi állapotát ugyanúgy jelzi, mint az alkalmazás főablakában levő jelző (lásd: „A számítógép védelmével kapcsolatos problémák diagnosztizálása és megszüntetése”, 35. oldal). A zöld szín azt jelzi, hogy a számítógép teljesen védett, a sárga azt jelzi, hogy védeltségi problémák vannak, a vörös pedig azt, hogy a számítógép biztonsága súlyos veszélyben van. A szürke szín azt jelzi, hogy az alkalmazás leállt.

Az alkalmazásadatbázisok és szoftvermodulok frissítése közben egy forgó földgömb alakú ikon jelenik meg a gadget középső részén.


A Gadget segítségével a következő műveletek végezhetők el:

- a korábban felfüggesztett alkalmazás elindítása;
- az alkalmazás főablakának megnyitása;
- víruskeresés megadott objektumokon;
- a hírek ablakának megnyitása.

Konfigurálhatja a gadget gombjait, hogy további műveleteket indítsanak el:

- frissítés futtatása;
- az alkalmazás beállításainak a szerkesztése;
- az alkalmazás jelentéseinek a megtekintése;
- védelem felfüggesztése;
- Virtuális billentyűzet megnyitása;
- a Feladatkezelő ablak megnyitása.

### ➤ *Az alkalmazás elindítása a Gadget segítségével:*

kattintson a gadget közepén található  **Engedélyezés** ikonra.

### ➤ *Az alkalmazás főablakának a megnyitása a Gadget segítségével:*

kattintson a Gadget közepén található monitor ikonra.

### ➤ *Objektum víruskeresése a Gadget segítségével:*


húzza a vizsgálandó objektumot a Gadgetre.

A feladat végrehajtásának előrehaladása a **Feladatkezelő** ablakban jelenik meg.

### ➤ *A hírek ablakának a megnyitása a Gadget segítségével:*

kattintson a Gadget közepén az új hírek érkezésekor megjelenő  ikonra.

### ➤ *A Gadget konfigurálása:*

1. Nyissa meg a gadget beállítási ablakát a  ikonra kattintva, amely a gadget blokk jobb felső sarkában jelenik meg, ha fölé húzza a kurzort.
2. A gadget gombjait tartalmazó legördülő listából válassza ki az egyes gombokra való kattintáskor végrehajtandó műveleteket.
3. Kattintson az **OK** gombra.

## ALKALMAZÁS REPUTÁCIÓJÁNAK ELLENŐRZÉSE

A Kaspersky Anti-Virus lehetőséget biztosít az alkalmazások reputációjának ellenőrzésére az azt világszerte alkalmazó felhasználóktól. Az alkalmazás reputációjának ellenőrzéséhez az alábbiak szükségesek:

- a forgalmazó neve;
- a digitális aláírás adatai (akkor elérhető, ha létezik digitális aláírás);
- a csoporttal kapcsolatos információk, amibe a Kaspersky Security Network felhasználóinak többsége az alkalmazást besorolta;
- a Kaspersky Security Network szolgáltatás azon felhasználóinak száma, akik az alkalmazást használják (csak akkor elérhető, ha az alkalmazás a Kaspersky Security Network adatbázisában a Megbízható csoportba tartozik);
- az az időpont, amikor az alkalmazás ismertté vált a Kaspersky Security Network számára;
- azok az országok, amikben az alkalmazást széles körben használják.

Egy alkalmazás reputációjának ellenőrzéséhez a Kaspersky Anti-Virus telepítésekor el kell fogadnia arészvételt a Kaspersky Security Networkben (lásd [108.](#) oldal).

➔ *Alkalmazás reputációjának ellenőrzése:*

nyissa meg az alkalmazás végrehajtható fájljának helyi menüjét, és válassza ki a **Reputáció ellenőrzése a KSN-ben** elemet.

### LÁSD MÉG:

Kaspersky Security Network ..... [107](#)

# AZ ALKALMAZÁS SPECIÁLIS BEÁLLÍTÁSAI

Ebben a részben az alkalmazás egyes összetevőinek beállítási módjairól talál részletes információkat.

## EBBEN A RÉSZBEN:

Általános védelmi beállítások .....	<a href="#">55</a>
Vizsgálat.....	<a href="#">56</a>
Frissítés.....	<a href="#">63</a>
Fájl víruskereső .....	<a href="#">67</a>
Levél víruskereső .....	<a href="#">72</a>
Webes víruskereső .....	<a href="#">77</a>
IM víruskereső.....	<a href="#">82</a>
Proaktív védelem .....	<a href="#">84</a>
Rendszerfigyelő .....	<a href="#">85</a>
Hálózati védelem.....	<a href="#">87</a>
Megbízható zóna.....	<a href="#">90</a>
Teljesítmény és más alkalmazásokkal való kompatibilitás .....	<a href="#">92</a>
A Kaspersky Anti-Virus önvédelme .....	<a href="#">95</a>
Karantén és másolatok.....	<a href="#">95</a>
További eszközök a számítógép jobb védelméhez .....	<a href="#">98</a>
Jelentések .....	<a href="#">102</a>
Az alkalmazás megjelenése. Aktív kezelőfelület-elemek kezelése .....	<a href="#">105</a>
Értesítések .....	<a href="#">106</a>
Kaspersky Security Network .....	<a href="#">107</a>

## ÁLTALÁNOS VÉDELMI BEÁLLÍTÁSOK

Az alkalmazás beállítási ablakában, a **Védelmi központ** rész **Általános beállítások** alpontjában az alábbi műveletek végezhetők:

- az összes védelmi összetevő letiltása (lásd: „A védelem engedélyezése és letiltása”, [36.](#) oldal);
- az interaktív vagy az automatikus védelmi mód kiválasztása (lásd: „Védelmi mód kiválasztása”, [56.](#) oldal);
- felhasználói hozzáférés korlátozása az alkalmazáshoz jelszó beállításával (lásd: „A Kaspersky Anti-Virus elérésének korlátozása”, [56.](#) oldal);
- az alkalmazás operációs rendszerrel együtt történő automatikus beindulásának tiltása és engedélyezése (lásd: „Az automatikus indítás engedélyezése és letiltása”, [34.](#) oldal);
- egyéni billentyűkombináció engedélyezése a virtuális billentyűzet megjelenítéséhez a képernyőn (lásd: „Védelem a billentyűzeten bevitt adatok elfogása ellen”, [43.](#) oldal).

## EBBEN A RÉSZBEN:

A Kaspersky Anti-Virus elérésének korlátozása .....	<a href="#">56</a>
Védelmi mód kiválasztása.....	<a href="#">56</a>

## A KASPERSKY ANTI-VIRUS ELÉRÉSÉNEK KORLÁTOZÁSA

A számítógépet több felhasználó is használhatja, eltérő számítástechnikai ismeretekkel. A Kaspersky Anti-Virus és beállításainak korlátozás nélküli elérése miatt a számítógép védelme csökkenhet.

Az alkalmazáshoz történő hozzáférés korlátozása érdekében beállíthat egy jelszót, és megadhatja, hogy milyen műveletekhez legyen szükséges a jelszó megadása:

- az alkalmazás beállításainak módosítása;
- az alkalmazás bezárása;
- az alkalmazás eltávolítása.

**Legyen óvatos, ha jelszóval korlátozza a hozzáférést az alkalmazás eltávolításához. Ha elfelejti a jelszót, az alkalmazást nehéz lesz eltávolítani a számítógépről.**

➤ *A Kaspersky Anti-Virus hozzáféréseinek jelszavas védelme:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. A megnyíló ablak bal oldalának **Védelmi központ** részben válassza ki az **Általános beállítások** összetevőt.
3. Az ablak jobb oldalán a **Jelszóvédelem** részben jelölje be a **Jelszóvédelem engedélyezése** négyzetet, majd kattintson a **Beállítások** gombra.
4. A megnyíló **Jelszóvédelem** ablakban írjon be egy jelszót, és adja meg a hozzáférési korlátozással védeni kívánt területet.

## VÉDELMI MÓD KIVÁLASZTÁSA

A Kaspersky Anti-Virus alapértelmezetten *automatikus védelmi módban* fut. Az alkalmazás ebben az üzemmódban automatikusan a Kaspersky Lab által ajánlott műveleteket végzi a veszélyes eseményekre válaszul. Ha azt szeretné, hogy a Kaspersky Anti-Virus értesítse Önt minden a rendszerben megjelenő veszélyes és gyanús eseményekről és hagyja Önre a döntést az alkalmazás által javasolt műveletek között, engedélyezze az *interaktív védelmi módot*.

➤ *A védelmi mód kiválasztása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. A megnyíló ablak bal oldalának **Védelmi központ** részben válassza ki az **Általános beállítások** összetevőt.
3. Az **Interaktív védelem** részben jelölje be a kívánt védelmi mód melletti négyzetet, vagy szüntesse meg a jelölését:
  - az interaktív védelmi mód engedélyezéséhez szüntesse meg a **Művelet automatikus kiválasztása** négyzet bejelölését;
  - az automatikus védelmi mód engedélyezéséhez jelölje be a **Művelet automatikus kiválasztása** négyzetet.

Ha nem szeretné, hogy a Kaspersky Anti-Virus automatikus módban futva törölje a gyanús objektumokat, jelölje be a **Ne törölje a gyanús objektumokat** négyzetet.

## VIZSGÁLAT

A számítógép vizsgálata sebezhetőségek, vírusok és egyéb kockázatos programok szempontjából az egyik legfontosabb feladat, amelyet a számítógép biztonságának szavatolása érdekében el kell végezni.

Vírusok és egyéb kockázatos programok keresésének rendszeres futtatására a számítógépen azért van szükség, hogy kizárható legyen az olyan rosszindulatú programok terjedésének lehetősége, amelyeket a biztonsági összetevők nem észleltek, például az alacsony biztonsági szint miatt vagy egyéb okokból.

A sebezhetőségi vizsgálat az operációs rendszer biztonságának diagnosztikai elemzését végzi el, és észleli azokat a szoftverfunkciókat, amelyeket a támadók rosszindulatú objektumok terjesztésére és személyes adatok megszerzésére használhatnak fel.

Ez a rész információkat tartalmaz a vizsgálati feladatok jellemzőiről és beállításáról, a biztonsági szintekről, vizsgálatmódokról és a vizsgálati technológiákról.

**EBBEN A RÉSZBEN:**

Víruskeresés .....	<a href="#">57</a>
Sebezhetőségi vizsgálat.....	<a href="#">63</a>
Vizsgálati feladatok kezelése. Feladatkezelő .....	<a href="#">63</a>

**VÍRUSKERESÉS**

Vírusok és más kockázatos programok észleléséhez a Kaspersky Anti-Virusban az alábbi feladatok használhatók:

- **Teljes vizsgálat.** A teljes rendszer vizsgálata. Alapértelmezésben a Kaspersky Anti-Virus az alábbi objektumokat vizsgálja:
  - rendszermemória;
  - a rendszer indulásakor betöltött objektumok;
  - a rendszer biztonsági másolata;
  - email adatbázisok;
  - cserélhető meghajtók, merevlemezek és hálózati meghajtók.
- **Kritikus területek vizsgálata.** Alapértelmezésben a Kaspersky Anti-Virus megvizsgálja az operációs rendszer indulásakor betöltődő objektumokat.
- **Egyéni vizsgálat.** A Kaspersky Anti-Virus a felhasználó által kiválasztott objektumokat ellenőrzi. Az alábbi listából bármely objektumot megvizsgálhatja:
  - rendszermemória;
  - a rendszer indulásakor betöltött objektumok;
  - a rendszer biztonsági másolata;
  - email adatbázisok;
  - cserélhető meghajtók, merevlemezek és hálózati meghajtók;
  - bármely fájl vagy mappa, amit kiválaszt.

A Teljes vizsgálat és a Kritikus területek vizsgálata feladatok külön tulajdonságokkal rendelkeznek. Ezen feladatok esetében nem ajánlott a vizsgálandó objektumok listájának módosítása.

Minden vizsgálati feladat a meghatározott területen kerül végrehajtásra, és a korábban létrehozott ütemezés szerint indítható. Minden vizsgálati feladathoz tartozik egy biztonsági szint (beállítások kombinációja, amely meghatározza a vizsgálat mélységét). Alapértelmezésben az *aláírás mód* (amely az alkalmazás adatbázisait használja fel fenyegetések keresésére) mindig engedélyezve van. Ezenkívül különböző vizsgálatmódokat és technológiákat is alkalmazhat.

A teljes vizsgálat feladat vagy a kritikus területek vizsgálata feladat elindítása után a vizsgálat előrehaladása megjelenik a **Vizsgálat** ablakban, a futó feladat nevével jelzett részen, valamint a Feladatkezelő ablakban is (lásd: „Vizsgálati feladatok kezelése. Feladatkezelő”, [63.](#) oldal).

Fenyegetés észlelésekor a Kaspersky Anti-Virus a következő állapotok egyikét rendeli a talált objektumhoz:

- Rosszindulatú program (például *vírus* vagy *trójai*).
- *Potenciálisan fertőzött* (gyanús) állapot, ha a vizsgálat nem tudja eldönteni, hogy az objektum fertőzött-e. A fájl tartalmazhat a vírusokra jellemző kódrészletet vagy egy ismert vírus módosított kódját.

Az alkalmazás értesítést (lásd [106.](#) oldal) jelenít meg az észlelt fenyegetésről, és végrehajtja az előre meghatározott műveletet. Módosíthatja a fenyegetés észlelésekor végrehajtandó műveletet.

Ha automatikus módban dolgozik (lásd: „Védelmi mód kiválasztása”, [56.](#) oldal), veszélyes objektumok észlelésekor a Kaspersky Anti-Virus automatikusan végrehajtja a Kaspersky Lab szakértői által javasolt műveletet. A rosszindulatú objektumok esetében ez a művelet a **Vírusmentesítés. Törlés, ha a vírusmentesítés nem sikerül**, gyanús objektumoknál – **Áthelyezés a Karanténba**. Ha az alkalmazás interaktív módban (lásd: „Védelmi mód kiválasztása”, [56.](#) oldal) veszélyes objektumokat észlel, értesítést jelenít meg a képernyőn, melynek segítségével kiválaszthatja a kívánt műveletet az elérhető műveletek listájából.

Fertőzött objektum vírusmentesítésének megkezdése vagy törlése előtt a Kaspersky Anti-Virus létrehozza az objektum mentett másolatát, hogy később lehetőség legyen az objektum visszaállítására vagy vírusmentesítésére. A gyanús (potenciálisan fertőzött) objektumok a Karanténba kerülnek. Engedélyezheti a karanténba helyezett objektumok automatikus vizsgálatát minden frissítés után.

A vizsgálat eredményeivel és a feladat végrehajtása során történt eseményekkel kapcsolatos információkat a Kaspersky Anti-Virus egy jelentésben naplózza (lásd [102.](#) oldal).

## EBBEN A RÉSZBEN:

A biztonsági szint megváltoztatása és visszaállítása .....	<a href="#">58</a>
Vizsgálat indítási ütemezésének létrehozása .....	<a href="#">59</a>
Vizsgálendő objektumok listájának létrehozása .....	<a href="#">59</a>
Vizsgálatmód kiválasztása .....	<a href="#">60</a>
Vizsgálati technológia kiválasztása .....	<a href="#">60</a>
A fenygetés észlelésekor végrehajtandó műveletek módosítása .....	<a href="#">60</a>
Vizsgálat futtatása másik felhasználói fiókból .....	<a href="#">61</a>
A vizsgálendő objektumok típusának módosítása .....	<a href="#">61</a>
Összetett fájlok vizsgálata .....	<a href="#">61</a>
Vizsgálatoptimalizáció .....	<a href="#">62</a>
Cserélhető meghajtók vizsgálata csatlakoztatáskor .....	<a href="#">62</a>
Parancsikon létrehozása feladat indításához .....	<a href="#">63</a>

## BIZTONSÁGI SZINT MEGVÁLTOZTATÁSA ÉS VISSZAÁLLÍTÁSA

Az aktuális igényeinek függvényében kiválaszthatja valamelyik előre beállított biztonsági szintet vagy manuálisan módosíthatja a víruskeresés beállításait.

A víruskeresés beállításainak módosításakor az ajánlott értékek mindig visszaállíthatók. Ezek a beállítások a Kaspersky Lab által javasolt optimálisnak tekinthető beállítások, és az **Ajánlott** biztonsági szinten vannak csoportosítva.

### ➤ *Az létrehozott biztonsági szint módosítása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán található **Vizsgálat** részben válassza ki a kívánt feladatot (**Teljes vizsgálat, Kritikus területek vizsgálata** vagy **Egyéni vizsgálat**).
3. A **Biztonsági szint** részben állítsa be a kiválasztott feladat kívánt biztonsági szintjét, vagy kattintson a **Beállítások** gombra a víruskeresés beállításainak kézi módosításához.

A beállítások kézi módosítása esetén a biztonsági szint neve az **Egyéni** értékre módosul.

### ➤ *Alapértelmezett keresési beállítások visszaállítása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán található **Vizsgálat** részben válassza ki a kívánt feladatot (**Teljes vizsgálat, Kritikus területek vizsgálata** vagy **Egyéni vizsgálat**).
3. Kattintson a kiválasztott feladathoz tartozó **Alapértelmezett szint** gombra a **Biztonsági szint** részben.

## VIZSGÁLAT INDÍTÁSI ÜTEMEZÉSÉNEK LÉTREHOZÁSA

Ütemezés létrehozásával automatikusan indíthatja el a víruskeresési feladatokat: megadhatja a feladat futtatásának gyakoriságát, indítási időpontját (ha szükséges), valamint részletesebb beállításokat is.

Ha a feladat elindítása valamilyen okból (például a számítógép abban az időpontban nem volt bekapcsolva) nem volt lehetséges, beállíthatja a kimaradt feladatot úgy is, hogy automatikusan elinduljon, amint lehet. Lehetőség van a vizsgálat automatikus felfüggesztésére, ha a képernyővédő ki van kapcsolva vagy a számítógépet feloldották. Ez a funkció elhalasztja a feladat elindítását, amíg a felhasználó befejezi a munkát a számítógépen. Így a víruskeresési feladat munka közben nem foglalja le a rendszer erőforrásait.

A speciális Üresjárat vizsgálati mód (lásd: „Feladatok futtatása a háttérben”, [93.](#) oldal) lehetővé teszi, hogy az automatikus frissítés futtatására a számítógép üresjáratokor kerüljön sor.

### ➤ *Vizsgálati feladat ütemezésének módosítása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán található **Vizsgálat** részben válassza ki a kívánt feladatot (**Teljes vizsgálat**, **Kritikus területek vizsgálata** vagy **Sebezhetőségi vizsgálat**).
3. Kattintson a **Futásmód** gombra az ablak jobb oldali részében.
4. A megnyíló ablak **Futásmód** lapjának **Ütemezés** részén válassza ki az **Ütemezés szerint** elemet, és konfigurálja a víruskeresés futásmódját a **Gyakoriság** beállítás kívánt értékeinek megadásával.

### ➤ *Kihagyott feladat automatikus indításának engedélyezése:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán található **Vizsgálat** részben válassza ki a kívánt feladatot (**Teljes vizsgálat**, **Kritikus területek vizsgálata** vagy **Sebezhetőségi vizsgálat**).
3. Kattintson a **Futásmód** gombra az ablak jobb oldali részében.
4. A megnyíló ablak **Futásmód** lapjának **Ütemezés** részén válassza ki az **Ütemezés szerint** elemet, és jelölje be a **Kihagyott feladatok futtatása** négyzetet.

### ➤ *Víruskeresés futtatása csak akkor, ha a számítógép már nincs használatban:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán található **Vizsgálat** részben válassza ki a kívánt feladatot (**Teljes vizsgálat**, **Kritikus területek vizsgálata** vagy **Sebezhetőségi vizsgálat**).
3. Kattintson a **Futásmód** gombra az ablak jobb oldali részében.
4. A megnyíló ablak **Futásmód** lapjának **Ütemezés** részén válassza ki az **Ütemezés szerint** elemet, és jelölje be az **Ütemezett víruskeresés futtatása a képernyővédő bekapcsolódásakor vagy a számítógép lezárt állapotában** négyzetet.

## VIZSGÁLANDÓ OBJEKTUMOK LISTÁJÁNAK LÉTREHOZÁSA

Mindegyik víruskeresési feladat saját alapértelmezett objektumlistával rendelkezik. Ezek között az objektumok között lehetnek a számítógép fájlrendszerének az elemei, például logikai meghajtók és email adatbázisok, vagy más típusú objektumok, mint például hálózati meghajtók. Ez a lista szerkeszthető.

**Ha a vizsgálat hatóköre üres, vagy csak bejelöletlen objektumokat tartalmaz, nem indítható vizsgálati feladat.**

### ➤ *Az egyéni vizsgálat objektumlistájának létrehozása:*

1. Nyissa meg az alkalmazás főablakát.
2. Válassza ki a **Vizsgálat** részt az ablak alsó részén.
3. Az ablak alsó részén kattintson a **megadás** hivatkozásra a vizsgálandó objektumok listájának a megnyitásához.
4. A megnyíló **Egyéni vizsgálat** ablakban kattintson a **Hozzáadás** gombra.
5. A megnyíló **Objektumok kijelölése vizsgálatra** ablakban válassza ki a kívánt objektumot, és kattintson a **Hozzáadás** gombra. Miután felvette az összes szükséges objektumot, kattintson az **OK** gombra. Törölje az objektum neve melletti négyzet bejelölését, ha ki szeretné zárni az objektumot a vizsgálandó objektumok listájából.

A vizsgálni kívánt fájlokat akár be is húzhatja a **Vizsgálat** rész megjelölt területére.

➤ *Objektumok listájának létrehozása Teljes vizsgálat, Kritikus területek vizsgálata vagy Sebezhetőségi vizsgálat feladatokhoz:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán található **Vizsgálat** részben válassza ki a kívánt vizsgálati feladatot (**Teljes vizsgálat**, **Kritikus területek vizsgálata** vagy **Sebezhetőségi vizsgálat**).
3. Az ablak jobb oldali részén kattintson a **Vizsgálat hatóköre** gombra.
4. A megnyíló **Vizsgálat hatóköre** ablakban a **Hozzáadás**, **Szerkesztés** és **Törlés** gombok segítségével hozzon létre egy listát. Törölje az objektum neve melletti négyzet bejelölését, ha ki szeretné zárni az objektumot a vizsgálandó objektumok listájából.

A listában alapértelmezettként megjelenő objektumok nem szerkeszthetők és nem is törölhetők.

## VIZSGÁLATMÓD KIVÁLASZTÁSA

Víruskeresés során az alkalmazás mindig használja az *alírást-elemzést*: a Kaspersky Anti-Virus összehasonlíja a talált objektumot az adatbázis bejegyzéseivel.

A vizsgálat hatékonyságának növeléséhez további vizsgálatmódokat is engedélyezhet: a *heurisztikus elemzést* (azaz az objektum által a rendszerben végzett tevékenység elemzését) és a *rootkitek keresését* (eszközök, amelyek elrejtik a rosszindulatú programokat az operációs rendszerben).

➤ *A használandó vizsgálatmód kiválasztásához:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán található **Vizsgálat** részben válassza ki a kívánt feladatot (**Teljes vizsgálat**, **Kritikus területek vizsgálata** vagy **Egyéni vizsgálat**).
3. Kattintson a kiválasztott feladathoz tartozó **Beállítások** gombra a **Biztonsági szint** részben.
4. A megnyíló ablak **További** lapjának **Vizsgálatmódok** részében válassza ki a kívánt vizsgálatmódokat.

## VIZSGÁLATI TECHNOLÓGIA KIVÁLASZTÁSA

A vizsgálatmódok mellett speciális objektumvizsgálati technológiákat is használhat, amelyek az utolsó vizsgálatuk óta nem módosult fájlok kizárásával lehetővé teszik a víruskeresés sebességének növelését.

➤ *Az objektumvizsgálati technológiák beállítása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán található **Vizsgálat** részben válassza ki a kívánt feladatot (**Teljes vizsgálat**, **Kritikus területek vizsgálata** vagy **Egyéni vizsgálat**).
3. Kattintson a kiválasztott feladathoz tartozó **Beállítások** gombra a **Biztonsági szint** részben.
4. A megnyíló ablak **További** lapjának **Vizsgálati technológiák** részében válassza ki a kívánt értékeket.

## A FENYEGETÉS ÉSZLELÉSEKOR VÉGREHAJTANDÓ MŰVELETEK MÓDOSÍTÁSA

Fertőzött objektumok észlelése esetén az alkalmazás elvégzi a kijelölt műveletet.

➤ *A fenyegetés észlelésekor végrehajtandó művelet módosítása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán található **Vizsgálat** részben válassza ki a kívánt feladatot (**Teljes vizsgálat**, **Kritikus területek vizsgálata** vagy **Egyéni vizsgálat**).
3. Válassza ki a kívánt lehetőséget az ablak jobb oldalán található **Művelet fenyegetés észlelésekor** részben.

## VIZSGÁLAT FUTTATÁSA MÁSIK FELHASZNÁLÓI FIÓKBÓL

Alapértelmezett esetben a vizsgálati feladatok futtatása az Ön felhasználói fiókjából történik. Ugyanakkor előfordulhat, hogy egy feladatot egy másik felhasználói fiókból kell elindítania. Megadhatja, hogy melyik fiókot használja az alkalmazás a vizsgálati feladat futtatásakor.

➔ *Vizsgálat elindítása egy másik felhasználó fiókjában:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán található **Vizsgálat** részben válassza ki a kívánt feladatot (**Teljes vizsgálat**, **Kritikus területek vizsgálata** vagy **Sebezhetőségi vizsgálat**).
3. Kattintson a **Futásmód** gombra az ablak jobb oldali részében.
4. A megnyíló ablak **Futásmód** lapjának **Felhasználói fiók** részében jelölje be a **Feladat futtatása másként** négyzetet. Adja meg a felhasználónevet és a jelszót.

## A VIZSGÁLANDÓ OBJEKTUMOK TÍPUSÁNAK MÓDOSÍTÁSA

A vizsgálandó objektumok típusának megadásával meghatározható, hogy mely fájlformátumokat kívánja vizsgálatnak alávetni a kiválasztott víruskeresési feladat futtatásakor.

A fájl típusok kiválasztásakor a következőkre kell odafigyelnie:

- A rosszindulatú kódok behatolási és későbbi aktiválódási valószínűsége számos fájlformátum (például .txt) esetén meglehetősen alacsony. Más formátumok (például .exe, .dll, .doc) ugyanakkor végrehajtható kódot tartalmazhatnak. A rosszindulatú kódok behatolásának és aktiválódásának kockázata az ilyen fájlknál meglehetősen magas.
- A behatoló úgy is küldhet vírust a számítógépére, hogy egy végrehajtható fájl .txt kiterjesztésűre nevez át. Ha a fájl kiterjesztés alapján történő vizsgálatát választotta, az ilyen fájl kimaradnak a vizsgálatból. Ha a formátum alapján történő vizsgálat van kiválasztva, a Fájl víruskereső kiterjesztéstől függetlenül elemzi a fájl fejlécét, és felfedi, hogy a fájl valójában .exe fájl. Az ilyen fájlkat alapos ellenőrzésnek veti alá.

➔ *A vizsgálandó objektumok típusának módosítása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán található **Vizsgálat** részben válassza ki a kívánt feladatot (**Teljes vizsgálat**, **Kritikus területek vizsgálata** vagy **Egyéni vizsgálat**).
3. Kattintson a kiválasztott feladathoz tartozó **Beállítások** gombra a **Biztonsági szint** részben.
4. A megnyíló ablak **Hatókör** lapjának **Fájl típusok** részében válassza ki a kívánt beállítást.

## ÖSSZETETT FÁJLOK VIZSGÁLATA

A vírusok álcázásának gyakori módja az összetett fájlba, archívumokba, telepítőcsomagokba, beágyazott OLE-objektumokba és emailés fájlformátumokba való ágyazása. Az ilyen módon elrejtett vírusok felismeréséhez az összetett fájl ki kell csomagolni, ami jelentősen csökkenti a keresés sebességét.

Az összetett fájl minden típusához külön kiválaszthatja, hogy az alkalmazás minden fájl vizsgálgjon át vagy csak az új fájlkat. A kiválasztáshoz kattintson az objektum neve melletti hivatkozásra. Az érték módosításához kattintson rá a bal egérgombbal. Amennyiben csak az új és módosult fájl vizsgálatát választja (lásd [62.](#) oldal), az összes fájl vagy csak az új fájl vizsgálatának kiválasztását lehetővé tevő hivatkozások nem lesznek elérhetők.

Korlátozhatja a vizsgálandó összetett fájl maximális méretét. A megadottnál nagyobb méretű összetett fájl nem lesznek ellenőrizve.

**Az archívumokból kicsomagolt nagyméretű fájl ellenőrzése akkor is megtörténik, ha be van jelölve a **Ne bontsa ki a nagyméretű összetett fájlkat** négyzet.**

➔ *A vizsgálandó összetett fájl listájának módosítása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán található **Vizsgálat** részben válassza ki a kívánt feladatot (**Teljes vizsgálat**, **Kritikus területek vizsgálata** vagy **Egyéni vizsgálat**).
3. Kattintson a kiválasztott feladathoz tartozó **Beállítások** gombra a **Biztonsági szint** részben.
4. A megnyíló ablak **Hatókör** lapjának **Összetett fájl vizsgálat** részében válassza ki az összetett fájl azon típusait, amelyeket vizsgálni szeretne.

➤ *A vizsgálendő összetett fájlok maximális méretének beállítása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán található **Vizsgálat** részben válassza ki a kívánt feladatot (**Teljes vizsgálat, Kritikus területek vizsgálata** vagy **Egyéni vizsgálat**).
3. Kattintson a kiválasztott feladathoz tartozó **Beállítások** gombra a **Biztonsági szint** részben.
4. A megnyíló ablak **Hatókör** lapjának **Összetett fájlok vizsgálata** részében kattintson a **További** gombra.
5. A megnyíló **Összetett fájlok** ablakban jelölje be a **Ne bontsa ki a nagy méretű összetett fájlokat** négyzetet, és adja meg a maximális fájl méretet.

## VIZSGÁLATOPTIMALIZÁCIÓ

Lerövidítheti a vizsgálat időtartamát és felgyorsíthatja a Kaspersky Anti-Virus alkalmazást. Ez úgy érhető el, hogy az alkalmazás csak az új és a legutóbbi vizsgálat óta megváltozott fájlokat vizsgálja. Ez a mód az egyszerű és az összetett fájlokra egyaránt érvényes.

Időkorlátot is rendelhet bármelyik objektum vizsgálatához. Ha letelik a megadott időtartam, az objektum kizárásra kerül az aktuális vizsgálatból (kivéve az archívumokat és a több objektumból álló fájlokat).

➤ *Csak az új és módosított fájlok vizsgálata:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán található **Vizsgálat** részben válassza ki a kívánt feladatot (**Teljes vizsgálat, Kritikus területek vizsgálata** vagy **Egyéni vizsgálat**).
3. Kattintson a kiválasztott feladathoz tartozó **Beállítások** gombra a **Biztonsági szint** részben.
4. A megnyíló ablak **Hatókör** lapjának **Vizsgálatoptimalizáció** részében jelölje be a **Csak az új és módosult fájlok vizsgálata** négyzetet.

➤ *A vizsgálat időtartamának korlátozása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán található **Vizsgálat** részben válassza ki a kívánt feladatot (**Teljes vizsgálat, Kritikus területek vizsgálata** vagy **Egyéni vizsgálat**).
3. Kattintson a kiválasztott feladathoz tartozó **Beállítások** gombra a **Biztonsági szint** részben.
4. A megnyíló ablak **Hatókör** lapjának **Vizsgálatoptimalizáció** részében jelölje be a **Vizsgált objektumok kihagyása, ha a vizsgálatuk hosszabb, mint** négyzetet, és írja be egy fájl vizsgálatának időtartamát.

## CSERÉLHETŐ MEGHAJTÓK VIZSGÁLATA CSATLAKOZTATÁSKOR

Napjainkban egyre jelentősebb az olyan rosszindulatú objektumok száma, amelyek a hálózatokon és cserélhető meghajtókon való terjedésükhöz az operációs rendszerek sebezhetőségeit használják ki. A Kaspersky Anti-Virus lehetővé teszi a cserélhető meghajtók ellenőrzését azok számítógéphez való csatlakoztatásakor.

➤ *A cserélhető meghajtó csatlakoztatásakor való vizsgálatának beállítása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Válassza ki a **Vizsgálat** részt az ablak bal oldali részén, majd ott az **Általános beállítások** elemet.
3. A **Cserélhető meghajtók vizsgálata csatlakoztatásakor** részben válassza ki a műveletet, és az alatta levő mezőben adja meg a vizsgálendő meghajtó maximális méretét, ha szükséges.

## PARANCSIKON LÉTREHOZÁSA FELADAT INDÍTÁSÁHOZ

Az alkalmazás lehetővé teszi parancsikon létrehozását a teljes, gyors és sebezhetőségi vizsgálati feladatok gyors elindítása érdekében. Ezáltal a fő alkalmazásablak és a helyi menü megnyitása nélkül indíthatja el a kívánt vizsgálatot.

➤ *Parancsikon létrehozása vizsgálat elindításához:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Válassza ki a **Vizsgálat** részt az ablak bal oldali részén, majd ott az **Általános beállítások** elemet.
3. Az ablak jobb oldali részén, a **Vizsgálati feladatok gyors futtatása** részben kattintson a **Parancsikon létrehozása** gombra a kívánt feladat neve mellett (**Kritikus területek vizsgálata**, **Teljes vizsgálat** vagy **Sebezhetőségi vizsgálat**).
4. A megnyíló ablakban adja meg a parancsikon mentési helyét és nevét. A parancsikon alapértelmezésben a feladat nevével elnevezve a számítógép aktuális felhasználójának Sajátgép mappájába kerül.

## SEBEZHETŐSÉGI VIZSGÁLAT

Az operációs rendszerben a sebezhetőséget okozhatja például programozási hiba, nem biztonságos jelszó, vagy rosszindulatú program tevékenysége. Sebezhetőségi vizsgálat lefolytatásakor az alkalmazás számos biztonsági eljárást lefuttat, például megvizsgálja a rendszert, elemzi az operációs rendszer és a böngésző beállításait, sebezhető szolgáltatásokat keres.

A diagnosztika eltarthat egy ideig. Ha befejeződött, a talált problémák olyan nézőpontból kerülnek elemzésre, hogy azok milyen mértékű fenyegetést jelentenek a rendszerre.

Ha a sebezhetőségi vizsgálat elindult (lásd [42.](#) oldal), a végrehajtás folyamata a **Vizsgálat** ablakban (a **Sebezhetőségi vizsgálat** részben), valamint a Feladatkezelő ablakban is (lásd: „Vizsgálati feladatok kezelése. Feladatkezelő”, [63.](#) oldal).

A sebezhetőségi vizsgálat eredményéről a Kaspersky Anti-Virus jelentést készít (lásd [102.](#) oldal).

A víruskeresési feladatoknál látottakhoz hasonlóan a sebezhetőségi vizsgálati feladathoz is beállíthat indítási ütemezést, létrehozhatja a vizsgálandó objektumok listáját (lásd [59.](#) oldal), megadhat egy fiókot (lásd: „Vizsgálat futtatása másik felhasználói fiókból”, [61.](#) oldal) és létrehozhat egy parancsikont a feladat gyors futtatásához. A számítógépre telepített alkalmazások alapértelmezett módon már kijelölésre kerültek, mind vizsgálandó objektumok.

## VIZSGÁLATI FELADATOK KEZELÉSE. FELADATKEZELŐ

A Feladatkezelő információkat jelenít meg az utoljára végzett, vagy a jelenleg futó vizsgálatról (például víruskeresés, sebezhetőség vizsgálata, rootkit keresése, illetve fejlett vírusmentesítés).

A Feladatkezelővel megtekinteni egy feladat haladását és eredményét, vagy leállíthatja a feladatot. Egyes feladatoknál további lépések is rendelkezésre állnak (például a sebezhetőség vizsgálat befejezésekor megnyithatja az észlelt sebezhetőségek listáját, és kijavíthatja azokat).

➤ *A Feladatkezelő megnyitása:*

1. Nyissa meg az alkalmazás főablakát.
2. Válassza ki a **Vizsgálat** részt az ablak alsó részén.
3. A megnyíló **Vizsgálat** ablakban kattintson a **Feladatok kezelése** gombra az ablak jobb felső sarkában.

## FRISSÍTÉS

A Kaspersky Anti-Virus adatbázisainak és programmoduljainak frissítése biztosítja a számítógép védelmének naprakész állapotát. Nap mint nap jelentős számú új vírus, trójai és más típusú fenyegetés jelenik meg világszerte. A fenyegetésekről és a semlegesítésük módjáról a Kaspersky Anti-Virus adatbázisai tartalmaznak információkat. Az új fenyegetések időben történő észleléséhez rendszeres időközönként frissíteni kell az adatbázisokat és alkalmazásmodulokat.

A rendszeres frissítéshez aktív licenc szükséges. Ha nincs telepítve licenc, csak egyszer hajthatja végre a frissítést.

Frissítés végrehajtásakor az alkalmazás letölti és telepíti az alábbi objektumokat a számítógépre:

- Kaspersky Anti-Virus adatbázisok.

Az adatok védelmét a fenyegetésszignatúrákat, a hálózati támadások leírását, valamint az ezek leküzdésének módját tartalmazó adatbázisok biztosítják. A védelmi összetevők ezen információ segítségével keresik meg és vírusmentesítik a számítógépen található veszélyes objektumokat. Az adatbázisok óráról órára kiegészülnek az új fenyegetések adataival és az ellenük való védekezés módszereivel. Ezért erősen ajánlott az adatbázisok rendszeres frissítése.

A Kaspersky Anti-Virus adatbázisai mellett frissülnek azok a hálózati illesztőprogramok is, amelyek segítségével az alkalmazás összetevői nyomon követik a hálózati forgalmat.

- Alkalmazásmodulok.

A Kaspersky Anti-Virus adatbázisai mellett a programmodulok is frissíthetők. Az alkalmazásmodulok frissítése megszünteti a Kaspersky Anti-Virus alkalmazásban található sebezhetőségeket, és új funkciókkal bővíti az alkalmazást, illetve továbbfejleszti a meglévő funkciókat.

Frissítéskor az alkalmazás összehasonlítja a számítógépen található alkalmazásmodulokat és adatbázisokat a frissítési forráson található naprakész változatokkal. Ha az érvényes adatbázisok és alkalmazásmodulok különböznek az alkalmazás telepített verziójában megtalálhatóktól, a frissítés telepíti a hiányzó részeket a számítógépre.

**Ha az adatbázisok elavultak, a frissítőcsomag nagyméretű lehet, és jelentős internetforgalmat (több tíz MB) generálhat.**

A Kaspersky Anti-Virus a frissítés előtt biztonsági másolatokat készít az adatbázisokról arra az esetre, ha vissza szeretne térni az előző adatbázis-verzióra (lásd: „Legutolsó frissítés visszagörgetése”, [66.](#) oldal).

Az alkalmazás főablakának **Frissítés** része a Kaspersky Anti-Virus adatbázisainak aktuális állapotáról jelenít meg információkat.

A frissítés eredményeivel és a frissítési feladat végrehajtása során történt eseményekkel kapcsolatos információkat a Kaspersky Anti-Virus egy jelentésben naplózza (lásd [102.](#) oldal).

Kiválaszthat egy frissítésforrást (lásd: „Frissítésforrás kiválasztása”, [64.](#) oldal) és konfigurálhatja a frissítés automatikus elindítását.

## EBBEN A RÉSZBEN:

Frissítésforrás kiválasztása .....	<a href="#">64</a>
Frissítés indítási ütemezésének létrehozása.....	<a href="#">66</a>
Legutolsó frissítés visszagörgetése .....	<a href="#">66</a>
Frissítések futtatása másik felhasználói fiókból.....	<a href="#">67</a>
Proxykiszolgáló használata .....	<a href="#">67</a>

## FRISSÍTÉSFORRÁS KIVÁLASZTÁSA

A *Frissítésforrás* a Kaspersky Anti-Virus adatbázisainak és alkalmazásmoduljainak frissítéseit tartalmazó erőforrás.

Az elsődleges frissítésforrások a Kaspersky Lab frissítéskiszolgálói, amelyek az adatbázisok és a alkalmazásmodulok frissítéseit tárolják minden Kaspersky termékhez.

A frissítések kiszolgálókról való sikeres letöltéséhez a számítógépnek csatlakoznia kell az internethez. Alapértelmezés szerint az alkalmazás automatikusan észleli az internetkapcsolat beállításait. Ha proxykiszolgálóval csatlakozik az internethez, előfordulhat, hogy meg kell adnia a kapcsolat beállításait (lásd: „A proxykiszolgáló beállítása”, [89.](#) oldal).

A Kaspersky Anti-Virus frissítésekor az adatbázisok és programmodulok Kaspersky Lab kiszolgálóiról letöltött frissítéseit átmásolhatja egy helyi mappába (lásd: „Alkalmazás megosztott mappából való frissítése”, [65.](#) oldal), a hálózat többi számítógépe számára is hozzáférést biztosítva a frissítésekhez. Ezzel csökkenthető az internetes adatforgalom.

Ha nem éri el a Kaspersky Lab frissítéskiszolgálóit (például azért, mert a számítógép nem csatlakozik az internetre), felhívhatja a Kaspersky Lab központi irodáját (<http://www.kaspersky.com/contacts>), ahol megtudhatja, melyik Kaspersky Lab partnertől kaphatja meg a frissítéseket cserélhető meghajtón.

**Ha cserélhető adathordozón rendeli a frissítéseket, adja meg, hogy szüksége van-e az alkalmazásmodulok frissítéseire is.**

## FRISSÍTÉSFORRÁS HOZZÁADÁSA

Alapértelmezésben a frissítésforrások listája csak a Kaspersky Lab frissítéskiszolgálóit tartalmazza. Frissítésforrásként felvehet egy helyi mappát, vagy egy másik szervert. Ha több forrás van kiválasztva frissítésforrásként, a Kaspersky Anti-Virus egymás után próbál kapcsolatot létesíteni azokkal a lista első elemétől kezdve, és az első elérhető forrásról letölti a frissítéseket.

### ► *Frissítésforrás hozzáadása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Frissítés** részében válassza ki a **Frissítések beállítása** összetevőt.
3. Kattintson a **Frissítésforrás** gombra az ablak jobb oldali részében.
4. A megnyíló ablak **Forrás** lapján kattintson a **Hozzáadás** gombra a forrás kiválasztására szolgáló ablak megnyitásához.
5. A megnyíló **Frissítésforrás kiválasztása** ablakban válassza ki a frissítéseket tartalmazó mappát, vagy adja meg annak a kiszolgálónak a címét a **Forrás** mezőben, amelyről letölthetők a frissítések.

## A FRISSÍTÉSKISZOLGÁLÓ RÉGIÓJÁNAK KIVÁLASZTÁSA

Ha frissítési forrásként a Kaspersky Lab kiszolgálóit használja, a frissítések letöltéséhez kiválaszthatja az optimális helyen található kiszolgálót. A Kaspersky Lab kiszolgálói számos országban megtalálhatók.

A legközelebbi Kaspersky Lab frissítéskiszolgáló használata lehetővé teszi a frissítések letöltési időtartamának csökkentését és növeli a működési sebességet. Alapértelmezésben az alkalmazás az érvényes régióra vonatkozó információkat az operációs rendszer rendszerleíró adatbázisából szerzi. A régiót manuálisan is kiválaszthatja.

### ► *A kiszolgáló régiójának kiválasztása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Frissítés** részében válassza ki a **Frissítések beállítása** összetevőt.
3. Kattintson a **Frissítésforrás** gombra az ablak jobb oldali részében.
4. A megnyíló ablak **Forrás** lapjának **Területi beállítások** részében válassza a **Kijelölés a listáról** lehetőséget, majd válassza ki a legördülő listából az Önhöz legközelebb eső országot.

## ALKALMAZÁS MEGOSZTOTT MAPPÁBÓL VALÓ FRISSÍTÉSE

Az Internetes forgalom csökkentése érdekében az alkalmazás hálózatba kapcsolt számítógépeken való frissítése esetén beállíthatja, hogy a Kaspersky Anti-Virus frissítése megosztott mappából történjen. Ha így tesz, a hálózat egyik számítógépe letölti a kívánt frissítéseket tartalmazó frissítőcsomagot a Kaspersky Lab kiszolgálóról vagy egy másik webes erőforrásról. A beszerzett frissítések egy megosztott mappába kerülnek. A hálózat többi számítógépe ebből a mappából tölti le a Kaspersky Anti-Virus frissítéseit.

Ha vendég fiókkal jelentkezik be a Microsoft Windows 7-be, a frissítések nem lesznek a megosztott mappába másolva. A frissítések átmásolásához javasolt egy másik fiók alatt bejelentkezni a rendszerbe.

### ► *A frissítésterjesztési mód engedélyezése:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Frissítés** részében válassza ki a **Frissítések beállítása** összetevőt.
3. Jelölje be a **Frissítések másolása mappába** négyzetet a **További** részben, az alatta lévő mezőben pedig adja meg annak a nyilvános mappának az elérési útvonalát, amelybe a letöltött frissítések kerülnek. A mappát a **Tallózás** gombra kattintva választhatja ki.

➤ *Frissítések letöltése a számítógépre megosztott mappából:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Frissítés** részében válassza ki a **Frissítések beállítása** összetevőt.
3. Kattintson a **Frissítésforrás** gombra az ablak jobb oldali részében.
4. A megnyíló ablak **Forrás** lapján kattintson a **Hozzáadás** gombra a forrás kiválasztására szolgáló ablak megnyitáshoz.
5. A megnyíló **Frissítésforrás kiválasztása** ablakban válasszon ki egy mappát, vagy adja meg annak teljes elérési útvonalát a **Forrás** mezőben.
6. A **Forrás** lapon szüntesse meg a **Kaspersky Lab frissítéskiszolgálók** négyzet bejelölését.

## FRISSÍTÉS INDÍTÁSI ÜTEMEZÉSÉNEK LÉTREHOZÁSA

Ütemezés létrehozásával automatikusan indíthatja el a frissítési feladatot: megadhatja a gyakoriságot, az indítási időpontját (ha szükséges), valamint részletesebb beállításokat is.

Ha a feladat elindítása valamilyen okból (például a számítógép abban az időpontban nem volt bekapcsolva) nem volt lehetséges, beállíthatja a kimaradt feladatot úgy is, hogy automatikusan elinduljon, amint lehet.

A feladat automatikus indítását el is halaszthatja az alkalmazás elindulása után. Ne feledje, hogy az ütemezett feladatok futtatására csak akkor kerül sor, ha letelik a megadott időtartam a Kaspersky Anti-Virus elindulása után.

A speciális Üresjárat vizsgálati mód (lásd: „Feladatok futtatása a háttérben”, [93.](#) oldal) lehetővé teszi, hogy az automatikus frissítés futtatására a számítógép üresjáratokor kerüljön sor.

➤ *A frissítési feladat indítási ütemezésének beállítása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Frissítés** részében válassza ki a **Frissítések beállítása** összetevőt.
3. Kattintson a **Futásmód** gombra az ablak jobb oldali részében.
4. A megnyíló ablak **Futásmód** lapjának **Ütemezés** részén válassza ki az **Ütemezés szerint** elemet, és konfigurálja a frissítés futásmódját.

➤ *Kihagyott feladat automatikus indításának engedélyezése:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Frissítés** részében válassza ki a **Frissítések beállítása** összetevőt.
3. Kattintson a **Futásmód** gombra az ablak jobb oldali részében.
4. A megnyíló ablak **Futásmód** lapjának **Ütemezés** részén válassza ki az **Ütemezés szerint** elemet, és jelölje be a **Kihagyott feladatok futtatása** négyzetet.

➤ *Egy feladat futásának elhalasztására az alkalmazás indítását követően:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Frissítés** részében válassza ki a **Frissítések beállítása** összetevőt.
3. Kattintson a **Futásmód** gombra az ablak jobb oldali részében.
4. A megnyíló ablak **Futásmód** lapjának **Ütemezés** részében jelölje be az **Ütemezés szerint** négyzetet, és a **Futtatás elhalasztása az alkalmazások indítása után** mezőben adja meg az időtartamot, amennyivel el szeretné halasztani a feladat futtatását.


## LEGUTOLSÓ FRISSÍTÉS VISSZAGÖRGETÉSE

A Kaspersky Anti-Virus első frissítése után elérhetővé válik a korábbi adatbázisok visszagörgetésének lehetősége.

A frissítés visszagörgetése funkció akkor hasznos, ha az adatbázisok új verziója érvénytelen aláírást tartalmaz, amely miatt a Kaspersky Anti-Virus egy biztonságos alkalmazást blokkol.

A Kaspersky Anti-Virus adatbázisainak sérülése esetén a naprakész védelem biztosításához ajánlott elindítani a frissítést, és letölteni az adatbázisok érvényes változatait.

➤ *A korábbi adatbázisokra való visszagörgetéshez:*

1. Nyissa meg az alkalmazás főablakát.
2. Válassza ki a **Frissítés** részt az ablak alsó részén.
3. A megnyíló **Frissítés** ablakban kattintson a  gombra, és a megnyíló menüben válassza a **Visszagörgetés a korábbi adatbázisokra** elemet.

## FRISSÍTÉSEK FUTTATÁSA MÁSIK FELHASZNÁLÓI FIÓKBÓL

Alapértelmezett esetben a frissítési folyamat az Ön felhasználói fiókja alatt fut. Ugyanakkor előfordulhat, hogy a Kaspersky Anti-Virus frissítése olyan forrásból történik, amelyhez Önnek nincs hozzáférése (például egy a frissítéseket tartalmazó hálózati mappából), vagy nincs jogosultsága a proxykiszolgáló használatához. A Kaspersky Anti-Virus frissítéseit csak olyan fiókokon futtathatja, amelyek rendelkeznek ilyen jogosultsággal.

➤ *Frissítés elindítása egy másik felhasználó fiókjában:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Frissítés** részében válassza ki a **Frissítések beállítása** összetevőt.
3. Kattintson a **Futásmód** gombra az ablak jobb oldali részében.
4. A megnyíló ablak **Futásmód** lapjának **Felhasználói fiók** részében jelölje be a **Feladat futtatása másként** négyzetet. Adja meg a felhasználónevet és a jelszót.

## PROXY KISZOLGÁLÓ HASZNÁLATA

Ha proxykiszolgáló segítségével kapcsolódik az Internethez, azt a Kaspersky Anti-Virus megfelelő frissítéséhez újra be kell állítania.

➤ *Proxykiszolgáló beállítása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Frissítés** részében válassza ki a **Frissítések beállítása** összetevőt.
3. Kattintson a **Frissítésforrás** gombra az ablak jobb oldali részében.
4. A megnyíló ablak **Forrás** lapján kattintson a **Proxykiszolgáló** gombra.
5. A megnyíló **Proxykiszolgáló beállításai** ablakban adja meg a proxykiszolgáló beállításait.

## FÁJL VÍRUSKERESŐ

A Fájlfő víruskereső megakadályozza a számítógép fájlrendszerének megfertőződését. Az összetevő az operációs rendszer betöltődésekor indul el, a számítógép memóriájában marad, és vírusokat és egyéb kockázatos programokat keresve megvizsgálja a számítógépen és a csatlakoztatott meghajtókon megnyitott, mentett vagy futó fájlokat.

Létrehozhat egy védelmi hatókört és beállíthat egy biztonsági szintet (a vizsgálat alaposságát meghatározó beállítások).

Amikor a felhasználó vagy egy program megpróbál hozzáférni egy védett fájlhoz, a Fájlfő víruskereső megvizsgálja az iChecker és iSwift adatbázisokat, hogy azok tartalmazznak-e információt a fájlról, és a kapott információk alapján megállapítja, hogy a fájlt meg kell-e vizsgálni.

Alapértelmezésben az *aláírás-elemzés* – a fenyegetések keresésére az alkalmazás adatbázisainak bejegyzéseit használó mód – mindig engedélyezve van. Ezen kívül engedélyezheti a heurisztikus elemzést és különböző vizsgálati technológiákat is.

Ha egy fájlban fenyegetést észlel, a Kaspersky Anti-Virus a következő állapotok egyikét rendeli ahhoz:

- Az észlelt rosszindulatú program típusát meghatározó állapot (például *vírus*, *trója*).
- *Potenciálisan fertőzött* (gyanús) állapot, ha a vizsgálat nem tudja eldönteni, hogy a fájl fertőzött-e. A fájl valószínűleg egy vírus vagy egyéb rosszindulatú program tipikus kódrészletét vagy egy ismert vírus módosított kódját tartalmazza.

Ezután az alkalmazás egy értesítést (lásd [106.](#) oldal) jelenít meg a képernyőn az észlelt fenyegetésről, és végrehajtja a Fájlvíruskereső beállításaihoz megadott műveletet. Az alkalmazás által egy fenyegetés észlelésekor végrehajtandó műveletet (lásd [71.](#) oldal) módosíthatja.

Ha automatikus módban dolgozik (lásd: „Védelmi mód kiválasztása”, [56.](#) oldal), veszélyes objektumok észlelésekor a Kaspersky Anti-Virus automatikusan végrehajtja a Kaspersky Lab szakértői által javasolt műveletet. A rosszindulatú objektumok esetében ez a művelet a **Vírusmentesítés. Törlés, ha a vírusmentesítés nem sikerül**, gyanús objektumoknál – **Áthelyezés a Karanténba**. Ha az alkalmazás interaktív módban (lásd: „Védelmi mód kiválasztása”, [56.](#) oldal) veszélyes objektumokat észlel, értesítést jelenít meg a képernyőn, melynek segítségével kiválaszthatja a kívánt műveletet az elérhető műveletek listájából.

Fertőzött objektum vírusmentesítésének megkezdése vagy törlése előtt a Kaspersky Anti-Virus létrehozza az objektum mentett másolatát, hogy később lehetőség legyen az objektum visszaállítására vagy vírusmentesítésére. A gyanús (potenciálisan fertőzött) objektumok a Karanténba kerülnek. Engedélyezheti a karanténba helyezett objektumok automatikus vizsgálatát minden frissítés után.

## EBBEN A RÉSZBEN:

A Fájlvíruskereső engedélyezése és letiltása.....	<a href="#">68</a>
A Fájlvíruskereső automatikus felfüggesztése .....	<a href="#">68</a>
A Fájlvíruskereső védelmi hatókörének létrehozása .....	<a href="#">69</a>
Fájlvizsgálati mód megváltoztatása és visszaállítása .....	<a href="#">70</a>
Vizsgálati mód kiválasztása .....	<a href="#">70</a>
Heurisztikus elemzés alkalmazása a Fájlvíruskereső működése során .....	<a href="#">71</a>
Fájlvizsgálati technológia kiválasztása .....	<a href="#">71</a>
A fertőzött fájlok végrehajtandó művelet módosítása .....	<a href="#">71</a>
Összetett fájlok vizsgálata a Fájlvíruskeresővel .....	<a href="#">71</a>
Fájlvizsgálat optimalizálása .....	<a href="#">72</a>

## A FÁJLVÍRUSKERESŐ ENGEDÉLYEZÉSE ÉS LETILTÁSA

A Fájlvíruskereső alapértelmezett módon be van kapcsolva, és a Kaspersky Lab specialistái által javasolt beállítással működik. Szükség esetén letilthatja a Fájlvíruskeresőt.

### ► A Fájlvíruskereső letiltása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Fájlvíruskereső** összetevőt.
3. Az ablak jobb oldali részében szüntesse meg a **Fájlvíruskereső engedélyezése** négyzet bejelölését.

## A FÁJLVÍRUSKERESŐ AUTOMATIKUS FELFÜGGESZTÉSE

Erőforrás-igényes műveletek végzésekor felfüggesztheti a Fájlvíruskereső működését. A terhelés csökkentése és az objektumok gyors elérése érdekében beállíthatja az összetevő működésének felfüggesztését egy adott időpontban, illetve ha bizonyos programokkal dolgozik.

A Fájlvíruskereső felfüggesztése annak más alkalmazásokkal való ütközése esetén csak vészhelyzetben alkalmazható. Ha probléma lép fel az összetevő használata közben, keresse meg a Kaspersky Lab Terméktámogatási szolgáltatását (<http://support.kaspersky.com>). A terméktámogatási szakemberek segítenek megoldani a Kaspersky Anti-Virus és a számítógépen lévő többi alkalmazás egyidejű működtetésének problémáját.

- *Az összetevő felfüggesztése egy adott időpontban:*
  1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
  2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Fájl víruskereső** összetevőt.
  3. Az ablak jobb oldalán a **Biztonsági szint** részben kattintson a **Beállítások** gombra.
  4. A megnyíló ablak **További** lapjának **Feladat felfüggesztése** részében jelölje be az **Ütemezés szerint** négyzetet, majd kattintson az **Ütemezés** gombra.
  5. A **Feladat felfüggesztése** ablakban adja meg (24 órás óó:pp formátumban), hogy mennyi ideig legyen a védelem felfüggesztve (**Feladat felfüggesztése** és **Feladat folytatása** mezők).
- *Összetevő felfüggesztése meghatározott alkalmazások futtatásakor:*
  1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
  2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Fájl víruskereső** összetevőt.
  3. Az ablak jobb oldalán a **Biztonsági szint** részben kattintson a **Beállítások** gombra.
  4. A megnyíló ablak **További** lapjának **Feladat felfüggesztése** részében jelölje be **Az alkalmazás indításakor** négyzetet, és kattintson a **Kiválasztás** gombra.
  5. Az **Alkalmazások** ablakban hozza létre azon alkalmazások listáját, amelyek futtatása felfüggeszti az összetevőt.

## A FÁJL VÍRUSKERESŐ VÉDELMI HATÓKÖRÉNEK LÉTREHOZÁSA

A védelem hatóköre meghatározza a vizsgált fájlok helyét és típusát. Alapértelmezésben a Kaspersky Anti-Virus csak a merevlemezen, hálózati meghajtón vagy cserélhető adathordozón tárolt potenciálisan fertőzhető fájlokat vizsgálja.

- *A védelem hatókörének létrehozásához:*
  1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
  2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Fájl víruskereső** összetevőt.
  3. Kattintson a **Beállítások** gombra az ablak jobb oldali részében.
  4. A megnyíló ablak **Általános** lapján a **Fájltípusok** részben adja meg, hogy a Fájl víruskereső milyen típusú fájlokat vizsgáljon:
    - Ha minden fájlt vizsgálni kíván, válassza a **Minden fájl** lehetőséget.
    - Ha a fertőzés által leginkább veszélyeztetett formátumú fájlokat szeretné vizsgálni, válassza a **Formátum alapján vizsgált fájlok** lehetőséget.
    - Ha a fertőzés által leginkább veszélyeztetett kiterjesztésű fájlokat szeretné vizsgálni, válassza a **Kiterjesztés alapján vizsgált fájlok** lehetőséget.

A vizsgálandó fájl típus kiválasztásakor vegye figyelembe az alábbiakat:

  - A rosszindulatú kódok behatolási és későbbi aktiválódási valószínűsége számos fájlformátum (például .txt) esetén meglehetősen alacsony. Más formátumok (például .exe, .dll, .doc) ugyanakkor végrehajtható kódot tartalmazhatnak. A rosszindulatú kódok behatolásának és aktiválódásának kockázata az ilyen fájloknál meglehetősen magas.
  - Egy hacker vírust vagy egyéb kockázatot jelentő alkalmazást küldhet a számítógépére egy olyan futtatható fájlban, amelyet .txt kiterjesztésűre nevezett át. Ha a fájl kiterjesztés alapján történő vizsgálatát választotta, az ilyen fájlok kimaradnak a vizsgálatból. Ha a formátum alapján történő vizsgálat van kiválasztva, a Fájl víruskereső kiterjesztéstől függetlenül elemzi a fájl fejlécét, és felfedi, hogy a fájl valójában .exe fájl. Az ilyen fájlt alaposan megvizsgálja vírusok és egyéb, kockázatot jelentő alkalmazások szempontjából.
  5. A **Védelem hatóköre** listában hajtsa végre a következő műveletek valamelyikét:
    - Ha egy új objektumot szeretne felvenni a vizsgálandó objektumok listájára, kattintson a **Hozzáadás** hivatkozásra.
    - Ha meg szeretné változtatni egy objektum helyét, válasszon ki egyet a listából, és kattintson a **Szerkesztés** hivatkozásra.

Megnyílik az **Objektumok kijelölése vizsgálatra** ablakot.

- Ha törölni kíván egy objektumot a vizsgálandó objektumok listájáról, válasszon ki egyet a listáról, és kattintson a **Törlés** hivatkozásra.  
Megnyílik a törlést megerősítő ablak.
- 6. Hajtsa végre a következő műveletek valamelyikét:
  - Ha egy új objektumot kíván felvenni a vizsgálandó objektumok listájára, jelöljön ki egyet az **Objektumok kijelölése vizsgálatra** ablakban, és kattintson az **OK** gombra.
  - Ha meg szeretné változtatni az objektum helyét, szerkessze az elérési útvonalat az **Objektumok kijelölése vizsgálatra** ablak **Objektum** mezőjében, és kattintson az **OK** gombra.
  - Ha törölni kíván egy objektumot a vizsgálandó objektumok listájáról, kattintson az **Igen** gombra a törlést megerősítő ablakban.
- 7. Ha szükséges, ismételje meg a 6 - 7. lépést a vizsgálandó objektumok listáján objektumok hozzáadásához, áthelyezéséhez vagy törléséhez.
- 8. Törölje az objektum neve melletti négyzet bejelölését a **Védelem hatóköre** listán, ha ki szeretné zárni az objektumot a vizsgálandó objektumok listájából. Az objektum a vizsgálandó objektumok listáján marad, de a Fájlvíruskereső kizárja a vizsgálatból.

## FÁJL BIZTONSÁGI SZINT MEGVÁLTOZTATÁSA ÉS VISSZAÁLLÍTÁSA

Az aktuális igényeknek megfelelően kiválaszthatja az előre beállított fájl/memória biztonsági szintek egyikét, de egyéni beállításokat is megadhat a Fájlvíruskeresőhöz.

A Fájlvíruskereső beállításakor mindig visszaállíthatja az ajánlott beállításokat. Ezek a beállítások a Kaspersky Lab által javasolt optimálisnak tekinthető beállítások, és az **Ajánlott** biztonsági szinten vannak csoportosítva.

### ➤ Az előre beállított fájl biztonsági szint módosítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Fájlvíruskereső** összetevőt.
3. Az ablak jobb oldalán található **Biztonsági szint** részben állítsa be a kívánt biztonsági szintet, vagy a **Beállítások** gombra kattintva módosítsa kézzel a beállítást.

A beállítások kézi módosítása esetén a biztonsági szint neve az **Egyéni** értékre módosul.

### ➤ Az alapértelmezett fájl biztonsági szint visszaállítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Fájlvíruskereső** összetevőt.
3. Kattintson az **Alapértelmezett szint** gombra a **Biztonsági szint** részben az ablak jobb oldali részén.

## VIZSGÁLATI MÓD KIVÁLASZTÁSA

A *vizsgálati mód* egy olyan feltételt jelent, amely szerint a Fájlvíruskereső elkezd a fájlok vizsgálatát. A Kaspersky Anti-Virus alapértelmezésben okos módban fut. Ebben a fájlvizsgálati módban a Fájlvíruskereső a felhasználó által a fájlokon végrehajtott műveletek és az érintett fájlok típusa alapján hoz döntést a fájlvizsgálatra vonatkozóan. Ha például egy Microsoft Office fájlal dolgozik, a Kaspersky Anti-Virus a fájl első megnyitásakor és utolsó bezárásakor fogja megvizsgálni azt. E kettő között a fájl felülíró semmilyen művelet nem váltja ki a fájl átvizsgálását.

### ➤ A fájlvizsgálati mód módosítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Fájlvíruskereső** összetevőt.
3. Az ablak jobb oldalán a **Biztonsági szint** részben kattintson a **Beállítások** gombra.
4. A megnyíló ablak **További** lapjának **Vizsgálati mód** részében válassza ki a kívánt módot.

A vizsgálati mód kiválasztásakor vegye figyelembe a fájlok típusát, amelyekkel az idő nagy részében dolgozni fog.

## HEURISZTIKUS ELEMZÉS ALKALMAZÁSA A FÁJL VÍRUSKERESŐ MŰKÖDÉSE SORÁN

A Fájlvíruskereső működése közben mindig használja az *aláírás-elemzést*: a Kaspersky Anti-Virus összehasonlítja a talált objektumot az adatbázis bejegyzéseivel.

A védelem hatékonyságának javítása érdekében használhatja a *heurisztikus elemzést* (azaz, az objektum által a rendszerben végzett tevékenység elemzését). Az elemzés olyan új rosszindulatú objektumok észlelését teszi lehetővé, amelyek még nincsenek benne az adatbázisokban.

➤ *A heurisztikus elemzés engedélyezése:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Fájlvíruskereső** összetevőt.
3. Az ablak jobb oldalán a **Biztonsági szint** részben kattintson a **Beállítások** gombra.
4. A megnyíló ablak **Teljesítmény** lapjának **Vizsgálati módok** részében jelölje be a **Heurisztikus elemzés** négyzetet, és adja meg a vizsgálat részletességének szintjét.

## FÁJLVIZSGÁLATI TECHNOLOGIA KIVÁLASZTÁSA

A heurisztikus elemzés mellett, speciális technológiákat is használhat, amelyek az utolsó vizsgálat óta nem módosult fájlok kizárásával lehetővé teszik a fájlvizsgálat teljesítményének optimalizálását.

➤ *Az objektumvizsgálati technológiák beállítása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Fájlvíruskereső** összetevőt.
3. Az ablak jobb oldalán a **Biztonsági szint** részben kattintson a **Beállítások** gombra.
4. A megnyíló ablak **További** lapjának **Vizsgálati technológiák** részében válassza ki a kívánt értékeket.

## A FERTŐZÖTT FÁJLOKON VÉGREHAJTANDÓ MŰVELET MÓDOSÍTÁSA

Fertőzött objektumok észlelése esetén az alkalmazás elvégzi a kijelölt műveletet.

➤ *Fertőzött objektumokon elvégzendő művelet módosítása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Fájlvíruskereső** összetevőt.
3. Válassza ki a kívánt lehetőséget az ablak jobb oldalán található **Művelet fenyegetés észlelésekor** részben.

## ÖSSZETETT FÁJLOK VIZSGÁLATA A FÁJLVÍRUSKERESŐVEL

A vírusok álcázásának gyakori módja az összetett fájlalba, archívumokba, telepítőcsomagokba, beágyazott OLE-objektumokba és emailés fájlformátumokba való ágyazása. Az ilyen módon elrejtett vírusok felismeréséhez az összetett fájl ki kell csomagolni, ami jelentősen csökkenti a keresés sebességét.

Az összetett fájl minden típusához külön kiválaszthatja, hogy az alkalmazás minden fájl vizsgálatát át vagy csak az új fájlakat. A kiválasztáshoz kattintson az objektum neve melletti hivatkozásra. Az érték módosításához kattintson rá a bal egérgombbal. Amennyiben csak az új és módosult fájlok vizsgálata vizsgálatmódot választja, az összes fájl vagy csak az új fájlok vizsgálatának kiválasztását lehetővé tevő hivatkozások nem lesznek elérhetők.

A Kaspersky Anti-Virus alapértelmezés szerint csak a beágyazott OLE objektumokat vizsgálja.

Nagyméretű összetett fájl vizsgálatkor előfordulhat, hogy előzetes kicsomagolásuk hosszú időt vesz igénybe. Ez az időtartam csökkenthető, ha engedélyezi az összetett fájl kibontását a háttérben, ha azok mérete meghalad egy bizonyos fájl méretet. Ha egy ilyen fájl használata közben az alkalmazás rosszindulatú objektumot észlel, értesítést jelenít meg.

Korlátozhatja a vizsgálandó összetett fájl maximális méretét. A megadottnál nagyobb méretű összetett fájlok nem lesznek ellenőrizve.

Az archívumokból kicsomagolt nagyméretű fájlok ellenőrzése akkor is megtörténik, ha be van jelölve a **Ne bontsa ki a nagyméretű összetett fájlokat** négyzetet.

➤ *A vizsgálandó összetett fájlok listájának módosítása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Fájl víruskereső** összetevőt.
3. Az ablak jobb oldalán a **Biztonsági szint** részben kattintson a **Beállítások** gombra.
4. A megnyíló ablak **Teljesítmény** lapjának **Összetett fájlok vizsgálata** részében válassza ki az összetett fájlok azon típusát, amelyet vizsgálni szeretne.

➤ *A vizsgálandó összetett fájlok maximális méretének beállítása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Fájl víruskereső** összetevőt.
3. Az ablak jobb oldalán a **Biztonsági szint** részben kattintson a **Beállítások** gombra.
4. A megnyíló ablak **Teljesítmény** lapjának **Összetett fájlok vizsgálata** részében kattintson a **További** gombra.
5. A megnyíló **Összetett fájlok** ablakban jelölje be a **Ne csomagoljon ki nagy összetett fájlokat** négyzetet, és adja meg a maximális fájl méretet.

➤ *Nagyméretű összetett fájlok kibontása a háttérben:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Fájl víruskereső** összetevőt.
3. Az ablak jobb oldalán a **Biztonsági szint** részben kattintson a **Beállítások** gombra.
4. A megnyíló ablak **Teljesítmény** lapjának **Összetett fájlok vizsgálata** részében kattintson a **További** gombra.
5. Az **Összetett fájlok** ablakban jelölje be az **Összetett fájlok kibontása a háttérben** négyzetet, és adja meg a minimális fájl méretet.

## FÁJLVIZSGÁLAT OPTIMALIZÁLÁSA

Lerövidítheti a vizsgálat időtartamát és felgyorsíthatja a Kaspersky Anti-Virus alkalmazást. Ez úgy érhető el, hogy az alkalmazás csak az új és a legutóbbi vizsgálat óta megváltozott fájlokat vizsgálja. Ez a mód az egyszerű és az összetett fájlokra egyaránt érvényes.

➤ *Csak az új és módosított fájlok vizsgálata:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Fájl víruskereső** összetevőt.
3. Kattintson a **Beállítások** gombra az ablak jobb oldali részében.
4. A megnyíló ablak **Teljesítmény** lapjának **Vizsgálatoptimalizáció** részében jelölje be a **Csak az új és módosult fájlok vizsgálata** négyzetet.

## LEVÉL VÍRUSKERESŐ

A Levél víruskereső rosszindulatú objektumokat keres a bejövő és kimenő üzenetekben. Az összetevő az operációs rendszer elindulásakor betöltődik, és ettől kezdve folyamatosan fut, megvizsgálva az összes POP3, SMTP, IMAP, MAPI és NNTP protokollon, valamint a biztonságos (SSL) POP3 és IMAP kapcsolatokon küldött és fogadott emailt (lásd: „Titkosított kapcsolatok vizsgálata”, [87.](#) oldal).

Az összetevő működését a tálca értesítési területén található  alkalmazásikon jelzi. Az ikon mindig látható ha email átvizsgálására kerül sor.

A Levél víruskereső elfogja, és megvizsgálja a felhasználónak érkező, vagy általa küldött leveleket. Ha az üzenet nem tartalmaz biztonsági fenyegetést, a felhasználó elérheti azt.

Megadhatja a vizsgálandó üzenetek típusait, és kiválaszthatja a biztonsági szintet (lásd [74.](#) oldal) (a vizsgálat részletességét meghatározó konfigurációs beállításokat).

Alapértelmezésben az *aláírás-elemzés* – a fenyegetések keresésére az alkalmazás adatbázisainak bejegyzéseit használó mód – mindig engedélyezve van. Ezen kívül engedélyezheti a heurisztikus elemzést is. Engedélyezheti továbbá a mellékletek szűrését (lásd [75.](#) oldal), ami bizonyos típusú fájlok automatikus átnevezését vagy törlését teszi lehetővé.

Ha egy fájlban fenyegetést észlel, a Kaspersky Anti-Virus a következő állapotok egyikét rendeli ahhoz:

- Az észlelt rosszindulatú program típusát meghatározó állapot (például *vírus, trójai*).
- *Potenciálisan fertőzött* (gyanús) állapot, ha a vizsgálat nem tudja eldönteni, hogy a fájl fertőzött-e. A fájl valószínűleg egy vírus vagy egyéb rosszindulatú program tipikus kódrészletét vagy egy ismert vírus módosított kódját tartalmazza.

Ezután az alkalmazás blokkolja az emailt, egy értesítést (lásd [106.](#) oldal) jelenít meg a képernyőn az észlelt fenyegetésről, és végrehajtja a Levél víruskereső beállításában megadott műveletet. Módosíthatja a fenyegetés észlelésekor végrehajtandó műveleteket (lásd: „A fertőzött email üzeneteken végrehajtandó művelet módosítása”, [75.](#) oldal).

Ha automatikus módban dolgozik (lásd: „Védelmi mód kiválasztása”, [56.](#) oldal), veszélyes objektumok észlelésekor a Kaspersky Anti-Virus automatikusan végrehajtja a Kaspersky Lab szakértői által javasolt műveletet. A rosszindulatú objektumok esetében ez a művelet a **Vírusmentesítés. Törlés, ha a vírusmentesítés nem sikerül**, gyanús objektumoknál – **Áthelyezés a Karanténba**. Ha az alkalmazás interaktív módban (lásd: „Védelmi mód kiválasztása”, [56.](#) oldal) veszélyes objektumokat észlel, értesítést jelenít meg a képernyőn, melynek segítségével kiválaszthatja a kívánt műveletet az elérhető műveletek listájából.

Fertőzött objektum vírusmentesítésének megkezdése vagy törlése előtt a Kaspersky Anti-Virus létrehozza az objektum mentett másolatát, hogy később lehetőség legyen az objektum visszaállítására vagy vírusmentesítésére. A gyanús (potenciálisan fertőzött) objektumok a Karanténba kerülnek. Engedélyezheti a karanténba helyezett objektumok automatikus vizsgálatát minden frissítés után.

Ha a vírusmentesítés sikeres, az email elérhetővé válik. Ha a vírusmentesítés sikertelen, a fertőzött objektumot az alkalmazás törli az emailből. A Levél víruskereső az email tárgyához hozzáad egy szöveget, amely értesíti a felhasználót, hogy az email üzenetet a Kaspersky Anti-Virus feldolgozta.

A Microsoft Office Outlook programhoz egy integrált bővítmény használható az email kliens finombeállítására.

Ha The Bat! levelezőklienset használ, a Kaspersky Anti-Virus más víruskereső alkalmazásokkal együtt is használható. Ez esetben az email forgalmat feldolgozó szabályok közvetlenül a The Bat! rendszeren belül kerülnek konfigurálásra, és magasabb prioritást élveznek, mint a Kaspersky Anti-Virus hasonló beállításai.

Más elterjedt levelezőprogramok esetén, mint például Microsoft Outlook Express/Windows Mail, Mozilla Thunderbird, Eudora és Incredimail, a Levél víruskereső az emaileket SMTP, POP3, IMAP és NNTP protokollokon vizsgálja.

**Felhívjuk a figyelmét arra, hogy Thunderbird levelezőkliens használata esetén az IMAP-on keresztül kapott email üzenetekben nem lehet víruskeresést végezni, ha az üzeneteket a **Beérkezett üzenetek** mappából szűrő helyezi át.**

## EBBEN A RÉSZBEN:

A Levél víruskereső engedélyezése és letiltása .....	<a href="#">74</a>
A Levél víruskereső védelmi hatókörének létrehozása .....	<a href="#">74</a>
Email biztonsági szint megváltoztatása és visszaállítása .....	<a href="#">74</a>
Heurisztikus elemzés alkalmazása a Levél víruskereső működése során .....	<a href="#">75</a>
A fertőzött email üzeneteken végrehajtandó művelet módosítása .....	<a href="#">75</a>
Mellékletek szűrése az email üzenetekben .....	<a href="#">75</a>
Összetett fájlok vizsgálata a Levél víruskeresővel .....	<a href="#">76</a>
Email vizsgálata a Microsoft Office Outlook programban .....	<a href="#">76</a>
Email vizsgálata a The Bat! programban .....	<a href="#">76</a>

## A LEVÉL VÍRUSKERESŐ ENGEDÉLYEZÉSE ÉS LETILTÁSA

A Levél víruskereső alapértelmezett módon be van kapcsolva, és a Kaspersky Lab specialistái által javasolt beállítással működik. Szükség esetén letilthatja a Levél víruskeresőt.

### ➤ A Levél víruskereső letiltása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Levél víruskereső** összetevőt.
3. Az ablak jobb oldali részében szüntesse meg a **Levél víruskereső engedélyezése** négyzet bejelölését.

## A LEVÉL VÍRUSKERESŐ VÉDELMI HATÓKÖRÉNEK LÉTREHOZÁSA

A védelem hatóköre magában foglalja a vizsgálandó email típusát, a Kaspersky Anti-Virus által ellenőrzött forgalmú protokollokat és a Levél víruskereső rendszerbe történő integrálásának beállításait.

Alapértelmezésben a Kaspersky Anti-Virus a Microsoft Office Outlook és a The Bat! programokba van integrálva, és vizsgálja a bejövő és kimenő emaileket, valamint a POP3, SMTP, NNTP és IMAP email protokollok forgalmát.

### ➤ A kimenő üzenetek vizsgálatának letiltása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Levél víruskereső** összetevőt.
3. Kattintson a **Beállítások** gombra az ablak jobb oldali részében.
4. A megnyíló ablak **Általános** lapjának **Védelem hatóköre** részén kattintson a **Csak bejövő üzenetek** lehetőségre.

Ha csak bejövő üzenetek vizsgálatát választotta ki, akkor ajánlott a kimenő üzenetek vizsgálata a Kaspersky Anti-Virus első futtatásakor, mivel a számítógépe email férgekkel lehet fertőzve, amely az emailt használja a terjedéséhez. A kimenő levelek vizsgálatával elkerülheti az üzeneteknek a számítógépről történő ellenőrizetlen küldése miatt bekövetkező problémákat.

### ➤ A vizsgálandó protokollok és a Levél víruskeresőnek a rendszerbe történő integrálására vonatkozó beállítások kijelölése:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Levél víruskereső** összetevőt.
3. Kattintson a **Beállítások** gombra az ablak jobb oldali részében.
4. A megnyíló ablak **További** lapjának **Kapcsolat** részében válassza ki a kívánt beállításokat.

## EMAIL BIZTONSÁGI SZINT MEGVÁLTOZTATÁSA ÉS VISSZAÁLLÍTÁSA

Az aktuális igényeknek megfelelően kiválaszthatja az előre beállított email biztonsági szintek egyikét, de egyéni beállításokat is megadhat a Levél víruskeresőhöz.

**A Kaspersky Lab nem javasolja a Levél víruskereső beállításainak egyéni konfigurálását. Az esetek többségében elegendő kiválasztani egy másik biztonsági szintet.**

A Levél víruskereső beállításakor mindig visszaállíthatja az ajánlott beállításokat. Ezek a beállítások a Kaspersky Lab által javasolt optimálisnak tekinthető beállítások, és az **Ajánlott** biztonsági szinten vannak csoportosítva.

### ➤ Az aktuális email védelmi szint módosítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Levél víruskereső** összetevőt.
3. Az ablak jobb oldalán található **Biztonsági szint** részben állítsa be a kívánt biztonsági szintet, vagy a **Beállítások** gombra kattintva módosítsa kézzel a beállítást.

A beállítások kézi módosítása esetén a biztonsági szint neve az **Egyéni** értékre módosul.

➤ *Alapértelmezett levélvédelmi beállítások visszaállítása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Levél víruskereső** összetevőt.
3. Kattintson az **Alapértelmezett szint** gombra a **Biztonsági szint** részben az ablak jobb oldali részén.

## HEURISZTIKUS ELEMZÉS ALKALMAZÁSA A LEVÉL VÍRUSKERESŐ MŰKÖDÉSE SORÁN

A Levél víruskereső működése közben mindig használja az *aláírás-elemzést*: a Kaspersky Anti-Virus összehasonlítja a talált objektumot az adatbázis bejegyzéseivel.

A védelem hatékonyságának javítása érdekében használhatja a *heurisztikus elemzést* (azaz, az objektum által a rendszerben végzett tevékenység elemzését). Az elemzés olyan új rosszindulatú objektumok észlelését teszi lehetővé, amelyek még nincsenek benne az adatbázisokban.

➤ *A heurisztikus elemzés engedélyezése:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Levél víruskereső** összetevőt.
3. Az ablak jobb oldalán a **Biztonsági szint** részben kattintson a **Beállítások** gombra.
4. A megnyíló ablak **Általános** lapjának **Vizsgálatmódok** részében jelölje be a **Heurisztikus elemzés** négyzetet, és adja meg a vizsgálat részletességének szintjét.

## A FERTŐZÖTT EMAIL ÜZENETEKEN VÉGREHAJTANDÓ MŰVELET MÓDOSÍTÁSA

Fertőzött objektumok észlelése esetén az alkalmazás elvégzi a kijelölt műveletet.

➤ *Fertőzött email üzeneteken elvégzendő művelet módosítása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Levél víruskereső** összetevőt.
3. Válassza ki a kívánt lehetőséget az ablak jobb oldalán található **Művelet fenyegetés észlelésekor** részben.

## MELLÉKLETEK SZŰRÉSE AZ EMAIL ÜZENETEK BEN

Emailekkel terjedő rosszindulatú programok legtöbbször a mellékletekben bújnak meg. A szűrést az email üzenetek mellékleteinek típusa alapján is végezheti, ezáltal az adott típusú fájlokat a program automatikusan átnevezheti, vagy törölheti.

➤ *A mellékletek szűrésének beállítása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Levél víruskereső** összetevőt.
3. Kattintson a **Beállítások** gombra az ablak jobb oldali részében.
4. A megnyíló ablak **Mellékletszűrő** lapján válassza ki meg a mellékletek szűrési módját. Az utóbbi két lehetőség valamelyikének kiválasztása esetén elérhetővé válik a fájltypusok (kiterjesztések) listája, ahol kiválaszthatók a kívánt típusok, vagy maszk segítségével új típus is megadható.

Egy új típusú maszk hozzáadásához kattintson a **Hozzáadás** hivatkozásra, és adja meg a szükséges adatokat a megnyíló **Fájlnévmaszk beírása** ablakban.

## ÖSSZETETT FÁJLOK VIZSGÁLATA A LEVÉL VÍRUSKERESŐVEL

A vírusok álcázásának gyakori módja az összetett fájlalba, archívumokba, telepítőcsomagokba, beágyazott OLE-objektumokba és emailés fájlformátumokba való ágyazása. Az ilyen módon elrejtett vírusok felismeréséhez az összetett fájlt ki kell csomagolni, ami jelentősen csökkenti a keresés sebességét.

Bekapcsolhatja vagy kikapcsolhatja az összetett fájlok ellenőrzését, és beállíthat egy maximális mérethatárt az összetett fájlok vizsgálatához.

Ha a számítógépét nem védi semmilyen helyi hálózati szoftver (az internethez proxy vagy tűzfal használata nélkül csatlakozik), akkor nem ajánlott az összetett fájlok vizsgálatának letiltása.

➤ *Az összetett fájlok vizsgálatának beállítása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Levél víruskereső** összetevőt.
3. Kattintson a **Beállítások** gombra az ablak jobb oldali részében.
4. A megnyíló ablak **Általános** lapján adja meg a szükséges beállításokat.

## EMAIL VIZSGÁLATA A MICROSOFT OFFICE OUTLOOK PROGRAMBAN

A Kaspersky Anti-Virus telepítésekor egy speciális bővítmény telepítődik a Microsoft Office Outlook alkalmazásba is. Ennek segítségével gyorsan átválthat a Microsoft Office Outlookból a Levél víruskereső beállítására, és megadhatja, hogy keressen-e az email üzenetekben vírusokat és más rosszindulatú szoftvereket az üzenet fogadásakor, megnyitásakor vagy küldésekor.

A Levél víruskereső Microsoft Office Outlookból történő konfigurálása akkor lehetséges, ha bejelölte ezt a lehetőséget a Levél víruskereső védelmi hatókör beállításában.

➤ *Átváltás az email vizsgálati beállításokra a Microsoft Office Outlookban:*

1. Nyissa meg a Microsoft Office Outlook alkalmazás főablakát.
2. Az alkalmazás menüjéből válassza ki az **Eszközök** → **Beállítások** lehetőséget.
3. A megnyíló **Beállítások** ablakban válassza ki az **Email védelem** lapot.

## EMAIL VIZSGÁLATA A THE BAT! PROGRAMBAN

A The Bat! programban lévő vírusos email objektumokkal kapcsolatos műveletek meghatározása az alkalmazás saját eszközeivel történik.

A program figyelmen kívül hagyja a Levél víruskereső azon beállításait, amelyek meghatározzák, hogy a bejövő és kimenő üzeneteket meg kell-e vizsgálni, milyen műveleteket kell végrehajtani az emailben található veszélyes objektumokon, és milyen kizárásokat kell alkalmazni. Az egyetlen dolog, amelyet a The Bat! figyelembe vesz, az a mellékelt archívumok vizsgálata.

Az email védelmi beállítások az összes olyan a számítógépre telepített víruskereső összetevőre kiterjednek, amelyek együttműködnek a The Bat! alkalmazással.

Megjegyezzük, hogy a beérkező email üzeneteket először a Levél víruskereső ellenőrzi, és csak utána a The Bat! bővítmény. Rosszindulatú objektum észlelésekor a Kaspersky Anti-Virus azonnal értesíti a felhasználót az eseményről. Ha a Levél víruskereső értesítési ablakában a **Vírusmentesítés (Törlés)** műveletet választja ki, akkor a fenyegetés elhárítását célzó lépéseket a Levél víruskereső fogja megtenni. Ha az értesítési ablakban a **Kihagyás** lehetőséget választja, akkor a vírusmentesítést a The Bat! bővítmény fogja végezni. Email küldésekor az üzenetet először a bővítmény ellenőrzi, majd a Levél víruskereső.

A Levél víruskereső The Bat! alkalmazásból történő konfigurálása akkor lehetséges, ha bejelölte ezt a lehetőséget a Levél víruskereső védelmi hatókör beállításában.

Az email vizsgálati beállításoknak a The Bat! alkalmazásban történő konfigurálásához az alábbiakat kell beállítani:

- melyik levélfolyam (bejövő, kimenő) megvizsgálendő;
- mikor történjen az email objektumok vizsgálata (az üzenet megnyitásakor, vagy még mielőtt a merevlemezre kerül);
- milyen műveletet végezzen a levelezőkliens, amikor veszélyes objektumot észlel az email üzenetben. Ezek közül választhat:
  - **Megpróbálja vírusmentesíteni a fertőzött részeket** – ezen opció kiválasztásakor kísérlet történik a fertőzött objektum vírusmentesítésére; ha az nem vírusmentesíthető, akkor az objektum az üzenetben marad.
  - **Fertőzött részek törlése** – ezen opció kiválasztásakor az üzenetben lévő veszélyes objektum törölve lesz függetlenül attól, hogy az fertőzött vagy csak fertőzésgyanús.

A The Bat! program az alapbeállítása szerint minden fertőzött email objektumot vírusmentesítési kísérlet nélkül karanténba helyez.

A veszélyes objektumokat tartalmazó email üzeneteket a The Bat! bővítmény nem jelöli meg a tárgy speciális kiegészítésével.

➔ *Átkapcsolás az email vizsgálati beállításokra a The Bat! alkalmazáson belül:*

1. Nyissa meg a The Bat! alkalmazás főablakát.
2. A **Tulajdonságok** menüjében válassza a **Beállítások** elemet.
3. Válassza ki a **Vírusvédelem** elemet a beállítások fájában.

## WEBES VÍRUSKERESŐ

Amikor az Interneten dolgozik, a számítógépen tárolt adatok veszélyben vannak, mivel ki vannak téve a vírus és egyéb rosszindulatú programok általi fertőzés veszélyének. Ezek ingyenes alkalmazások letöltésekor hatolhatnak be a számítógépébe, illetve akkor is, amikor olyan webhelyeken tekint meg információkat, amelyeket látogatása előtt hackerek támadtak meg. A hálózati férgek még azelőtt behatolhatnak a számítógépébe, hogy megnyitna egy weboldalt vagy letöltene egy fájlt – ehhez elegendő, hogy a számítógépe létrehozza az internetkapcsolatot.

A Webes víruskereső megvédi számítógépe által HTTP-, HTTPS- és FTP-protokollokon keresztül fogadott és küldött információkat, és megelőzi a veszélyes parancsfájlok futtatását a számítógépen.

A Webes víruskereső csak figyelt portok listájában megadott portokon átmenő webes forgalmat figyeli. A Kaspersky Anti-Virus telepítőcsomagjában megtalálható az adatátvitelre leggyakrabban használt figyelt portok listája. Ha a figyelt portok listájában nem szereplő portokat használ, azokat hozzá kell adnia a figyelt portok listájához (lásd: „Figyelt portok listájának létrehozása”, [89.](#) oldal), hogy biztosítsa a rajtuk átmenő webes forgalom védelmét.

A Webes víruskereső speciális beállításkészletek alapján vizsgálja a webes forgalmat, melyek neve biztonsági szint. Ha a Webes víruskereső fenyegetést észlel, elvégzi az előírt műveletet. A rosszindulatú objektumokat a Kaspersky Anti-Virus adatbázisok és a heurisztikus algoritmus alapján is észleli a program.

A Kaspersky Lab azt javasolja Önnek, hogy saját maga ne konfigurálja a Webes víruskereső beállításait. Az esetek többségében elegendő kiválasztani a megfelelő biztonsági szintet.

### Webes forgalom vizsgálati algoritmus

A felhasználó vagy egy program által a HTTP-, HTTPS- vagy FTP-protokollon elért oldalt vagy fájlt a Webes víruskereső elfogja, és rosszindulatú kódot keres benne.

- Ha a felhasználó által elért weboldal vagy fájl rosszindulatú kódot tartalmaz, az elérését a rendszer blokkolja. Megjelenik egy értesítés, hogy a kért fájl vagy weboldal fertőzött.
- Ha a fájl vagy weboldal nem tartalmaz rosszindulatú kódot, a program azonnal engedélyezi a hozzáférést.

## Parancsfájlvizsgálati algoritmus

A Webes víruskereső az összes futó parancsfájlt elfogja és elemzi, hogy tartalmaznak-e rosszindulatú kódot:

- Ha egy parancsfájl rosszindulatú kódot tartalmaz, a Webes víruskereső blokkolja azt, és megjelenít egy értesítést a képernyőn.
- Ha nem talál rosszindulatú kódot, a parancsfájl lefuthat.

A Webes víruskereső csak a Microsoft Windows Script Host funkción alapuló parancsfájlokat képes elfogni.

### EBBEN A RÉSZBEN:

A Webes víruskereső engedélyezése és letiltása .....	<a href="#">78</a>
A webes forgalom biztonsági szintjének megváltoztatása és visszaállítása.....	<a href="#">78</a>
A webes forgalomban észlelt veszélyes objektumokon végrehajtandó művelet módosítása .....	<a href="#">79</a>
URL-ek ellenőrzése a weboldalakon .....	<a href="#">79</a>
Heurisztikus elemzés alkalmazása a Webes víruskereső működése során.....	<a href="#">81</a>
Veszélyes parancsfájlok blokkolása .....	<a href="#">81</a>
Vizsgálatoptimalizáció .....	<a href="#">81</a>
Megbízható címek listájának létrehozása.....	<a href="#">82</a>

## A WEBES VÍRUSKERESŐ ENGEDÉLYEZÉSE ÉS LETILTÁSA

A Webes víruskereső alapértelmezett módon be van kapcsolva, és a Kaspersky Lab specialistái által javasolt beállítással működik. Szükség esetén letilthatja a Webes víruskeresőt.

### ➤ A Webes víruskereső letiltása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Webes víruskereső** összetevőt.
3. Szüntesse meg a **Webes víruskereső engedélyezése** négyzet bejelölését az ablak jobb oldali részében.

## A WEBES FORGALOM BIZTONSÁGI SZINTJÉNEK MEGVÁLTOZTATÁSA ÉS VISSZAÁLLÍTÁSA

Az aktuális igényeknek megfelelően kiválaszthatja a webes forgalom egyik előre beállított biztonsági szintjeinek egyikét, de egyéni beállításokat is megadhat a Webes víruskeresőhöz.

A Webes víruskereső beállításakor mindig visszaállíthatja az ajánlott beállításokat. Ezek a beállítások a Kaspersky Lab által javasolt optimálisnak tekinthető beállítások, és az **Ajánlott** biztonsági szinten vannak csoportosítva.

### ➤ A webes forgalom biztonsági szintjének módosítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Webes víruskereső** összetevőt.
3. Az ablak jobb oldalán található **Biztonsági szint** részben állítsa be a kívánt biztonsági szintet, vagy a **Beállítások** gombra kattintva módosítsa kézzel a beállítást.

A beállítások kézi módosítása esetén a biztonsági szint neve az **Egyéni** értékre módosul.

### ➤ A webes forgalom biztonsági szintjének visszaállítása alapértelmezett értékre:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Webes víruskereső** összetevőt.
3. Kattintson az **Alapértelmezett szint** gombra a **Biztonsági szint** részben az ablak jobb oldali részén.

## A WEBES FORGALOMBAN ÉSZLELT VESZÉLYES OBJEKTUMOKON VÉGREHAJTANDÓ

### MŰVELET MÓDOSÍTÁSA

Fertőzött objektumok észlelése esetén az alkalmazás elvégzi a kijelölt műveletet.

A Webes víruskereső mindig blokkolja a veszélyes parancsfájlok műveleteit és felbukkanó üzenetben tájékoztatja a felhasználót az elvégzett műveletről. A veszélyes parancsfájllal kapcsolatos intézkedést nem tudja megváltoztatni, csak annyit tehet, hogy letiltja a parancsfájlok vizsgálatát (lásd: „Veszélyes parancsfájlok blokkolása”, [81.](#) oldal).

➔ *Észlelt objektumokkal kapcsolatban elvégzendő műveletek módosítása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Webes víruskereső** összetevőt.
3. Válassza ki a kívánt lehetőséget az ablak jobb oldalán található **Művelet fenyegetés észlelések** részben.

## URL-EK ELLENŐRZÉSE A WEBOLDALAKON

Weboldalak vizsgálata adathalászati szempontból az *adathalászati támadások* megakadályozása érdekében. Az adathalászati támadásokat általában állítólagos pénzügyi szervezetektől küldött üzenetekkel követik el, amelyek URL-eket tartalmaznak az ilyen szervezetek webhelyeire. Az email üzenet a felhasználót arról igyekszik meggyőzni, hogy kattintson az URL-re, és adja meg személyes adatait a megnyíló ablakban, például a bankkártyája számát, vagy online bankfiókjának felhasználónevét és jelszavát. Egy adathalászati támadás álcázható például egy banktól érkező levélnek is, amely a bank hivatalos webhelyére mutató linket tartalmaz. Ha a hivatkozásra kattint, a bank webhelyének pontos másolatára jut. A böngésző címsorában a valódi címet fogja látni még akkor is, ha ténylegesen egy hamisított webhelyen tartózkodik. Ettől a ponttól kezdve a webhelyen végzett minden műveletét rögzítik, és felhasználhatják a pénz megszerzéséhez.

Mivel adathalász helyekre mutató hivatkozást nem csak email üzenetben kaphat, hanem más módokon, például ICQ-üzenetben is, a Webes víruskereső a webes forgalom szintjén követi nyomon az adathalász helyek elérésének kísérletét, és blokkolja az ilyen helyek elérését.

A Kaspersky Anti-Virus adatbázisai mellett a heurisztikus elemzés (lásd [81.](#) oldal) is használható a weboldalak vizsgálatra adathalászati szempontból.

### EBBEN A RÉSZBEN:

URL-ek ellenőrzésének engedélyezése és letiltása .....	<a href="#">79</a>
A Kaspersky URL-tanácsadó használata .....	<a href="#">79</a>

## URL-EK ELLENŐRZÉSÉNEK ENGEDÉLYEZÉSE ÉS LETILTÁSA

➔ *URL-ek ellenőrzésének engedélyezése a gyanús és adathalász webcímek adatbázisainak használatával:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Webes víruskereső** összetevőt.
3. Kattintson a **Beállítások** gombra az ablak jobb oldali részében.  
Megnyílik a **Webes víruskereső** ablaka.
4. Az **Általános** lap **Kaspersky URL-tanácsadó** részében jelölje be az **URL-ek ellenőrzése a gyanús URL-ek adatbázisában** és a **Weboldalak adathalászati ellenőrzése** négyzeteket.

## A KASPERSKY URL-TANÁCSADÓ HASZNÁLATA

A Kaspersky URL-tanácsadó a Microsoft Internet Explorer, Mozilla Firefox és Google Chrome böngészőkben bővítményként van jelen.

A Kaspersky URL-tanácsadó megvizsgálja a weboldalon található összes URL-t olyan szempontból, hogy rajta van-e a gyanús URL-ek listáján. Emellett ellenőrzi őket abból a szempontból is, hogy adathalász weboldalakra mutatnak-e, és az ilyeneket kiemeltté teszi.

Létrehozhatja webhelyek olyan listáját, amelyen az összes URL-t ellenőrizni kell, de ellenőrizheti a listán szereplőkön kívüli URL-eket is, ellenőrizheti a csak a keresési eredményben szereplő URL-eket, vagy megadhat webhelykategóriákat, amelyeken található URL-eket ellenőrizni kell.

A Kaspersky URL-tanácsadót az alkalmazás beállítási ablakán kívül magában a Kaspersky URL-tanácsadónak a webböngészőből elérhető beállítási ablakában is konfigurálhatja.

➤ *Azoknak a webhelyeknek a megadása, amelyeken ellenőrizni kell az URL-eket:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Webes víruskereső** összetevőt.
3. Kattintson a **Beállítások** gombra az ablak jobb oldali részében.
4. Megnyílik a **Webes víruskereső** ablaka.
5. A **Kaspersky URL-tanácsadó** rész **Biztonságos szörfölés** lapján jelölje be az **URL-ek ellenőrzése** négyzetet.
6. Azoknak a webhelyeknek a kijelölése, amelyeken a hivatkozásokat ellenőrizni kell:
  - a. Ha szeretne létrehozni egy listát azokról a webhelyekről, amelyeken az összes URL-t ellenőrizni kell, jelölje ki a **Csak a listán szereplő webhelyek** lehetőséget, majd kattintson a **Megadás** gombra. A megnyíló **Ellenőrzött URL-ek** ablakban hozza létre az ellenőrizendő webhelyek listáját.
  - b. Ha az összes webhely összes URL-jét ellenőriztetni kívánja a megadottakon kívül, válassza a **Mind, kivéve a kizárásokat** lehetőséget, és kattintson a **Kizárások** gombra. A megnyíló **Kizárások** ablakban hozza létre azoknak a webhelyeknek a listáját, amiken nem szeretné ellenőriztetni az URL-eket.

➤ *URL-ek ellenőrzése csak a keresési eredményekben:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Webes víruskereső** összetevőt.
3. Kattintson a **Beállítások** gombra az ablak jobb oldali részében.
4. Megnyílik a **Webes víruskereső** ablaka.
5. A **Kaspersky URL-tanácsadó** rész **Biztonságos szörfölés** lapján jelölje be az **URL-ek ellenőrzése** négyzetet, majd kattintson a **Beállítások** gombra.
6. A megnyíló **Kaspersky URL-tanácsadó beállításai** ablak **Ellenőrzési mód** részében jelölje be a **Csak a keresési eredményekben szereplő URL-ek** lehetőséget.

➤ *Azon webhelyek kategóriájának kijelölése, melyek URL-jeit nem kell megvizsgálni:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Webes víruskereső** összetevőt.
3. Kattintson a **Beállítások** gombra az ablak jobb oldali részében.
4. Megnyílik a **Webes víruskereső** ablaka.
5. A **Kaspersky URL-tanácsadó** rész **Biztonságos szörfölés** lapján jelölje be az **URL-ek ellenőrzése** négyzetet, majd kattintson a **Beállítások** gombra.
6. A megnyíló **Kaspersky URL-tanácsadó beállításai** ablak **Webhely-kategóriák** részében jelölje be az **Információk megjelenítése webhely tartalom kategóriákról** négyzetet.
7. A kategóriák közül jelölje be a négyzetet azok mellett, amelyek URL-jeit nem kell ellenőrizni.

➤ *A Kaspersky URL-tanácsadó beállítási ablakának megnyitása a webböngészőből:*

kattintson a Kaspersky Anti-Virus ikonra a böngésző eszköztárában.

## HEURISZTIKUS ELEMZÉS ALKALMAZÁSA A WEBES VÍRUSKERESŐ MŰKÖDÉSE SORÁN

A védelem hatékonyságának javítása érdekében használhatja a *heurisztikus elemzést* (azaz, az objektum által a rendszerben végzett tevékenység elemzését). Az elemzés olyan új rosszindulatú objektumok észlelését teszi lehetővé, amelyek még nincsenek benne az adatbázisokban.

Ha a Webes víruskereső fut, külön engedélyezheti a heurisztikus elemzést a webes forgalom vizsgálatában, valamint az adathalász weboldalak ellenőrzésekor.

➤ *A heurisztikus elemzés engedélyezése a webes forgalom vizsgálata során:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Webes víruskereső** összetevőt.
3. Kattintson a **Beállítások** gombra az ablak jobb oldali részében.  
Megnyílik a **Webes víruskereső** ablaka.
4. Az **Általános** lap **Heurisztikus elemzés** részében jelölje be a **Heurisztikus elemzés használata** négyzetet, és állítsa be a vizsgálat részletességének a szintjét.

➤ *A heurisztikus elemzés engedélyezése az adathalász weboldalak ellenőrzésekor:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Webes víruskereső** összetevőt.
3. Kattintson a **Beállítások** gombra az ablak jobb oldali részében.  
Megnyílik a **Webes víruskereső** ablaka.
4. A **Kaspersky URL-tanácsadó** rész **Általános** lapján kattintson a **További** gombra.
5. A megnyíló **Adathalászat-blokkoló beállítások** ablakban jelölje be a **A Heurisztikus elemző használata a weboldalak adathalászati ellenőrzésére** négyzetet, és állítsa be a vizsgálat részletességi szintjét.

## VESZÉLYES PARANCSFÁJLOK BLOKKOLÁSA

A Webes víruskereső a Microsoft Internet Explorerben feldolgozott mindenparancsfájlt és minden egyéb WSH-parancsfájlt megvizsgál (JavaScript, Visual Basic Script stb.), amelyet a számítógépen végzett munka során Ön elindít. Ha a parancsfájl fenyegetést jelent a számítógépre, akkor blokkolásra kerül.

➤ *A veszélyes parancsfájlok blokkolásának tiltása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Webes víruskereső** összetevőt.
3. Kattintson a **Beállítások** gombra az ablak jobb oldali részében.  
Megnyílik a **Webes víruskereső** ablaka.
4. Az **Általános** lap **További** részében törölje a **Veszélyes parancsfájlok blokkolása a Microsoft Internet Explorerben** négyzet bejelölését.

## VIZSGÁLATOPTIMALIZÁCIÓ

A Webes víruskereső az internetről jövő objektumtöredékek gyorsítótárzását használja a rosszindulatú kódok észlelési hatékonyságának növeléséhez. A gyorsítótárzás használatával a Webes víruskereső csak akkor vizsgálja meg az objektumokat, miután azok teljesen megérkeztek a számítógépre.

A gyorsítótárzás növeli az objektumok feldolgozásához és a felhasználónak való továbbküldéséhez szükséges időt. A gyorsítótárzás problémát okozhat nagy objektumok másolásakor és feldolgozásakor, mert a HTTP-ügyféllel való kapcsolaton időtűllépés következik be.

Megoldhatja ezt a problémát, ha korlátozza az Internetről származó objektumok töredékeinek gyorsítótárzását. Bizonyos idő letelte után az objektum minden töredéke vizsgálat nélkül továbbítódik a felhasználóhoz. A másolás befejezésekor az objektum egésze lesz megvizsgálva. Ez lehetővé teszi az objektumok felhasználóhoz való továbbításához szükséges idő csökkentését, és megoldja a kapcsolat megszakadásával kapcsolatos problémákat. Az Internetes biztonsági szint nem csökken.

A webes forgalom gyorsítótárazásának időtartamára vonatkozó korlátozások megemlése javítja a víruskeresés hatékonyságát, de lassíthatja az objektumok elérési idejét.

➤ *A fájl-törédekek gyorsítótárazási időkorlátjának módosítása vagy eltávolítása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Webes víruskereső** összetevőt.
3. Kattintson a **Beállítások** gombra az ablak jobb oldali részében.  
Megnyílik a **Webes víruskereső** ablaka.
4. Az **Általános** lap **További** részében jelölje be a **Forgalom gyorsítótárazási idejének korlátozása 1 másodpercre a vizsgálat optimalizálása érdekében** négyzetet.

## MEGBÍZHATÓ CÍMEK LISTÁJÁNAK LÉTREHOZÁSA

A Webes víruskereső nem ellenőrzi az adatforgalmat veszélyes objektumok után, ha az megbízható URL-ről érkezik.

➤ *Megbízható webcímek listájának létrehozása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Webes víruskereső** összetevőt.
3. Kattintson a **Beállítások** gombra az ablak jobb oldali részében.  
Megnyílik a **Webes víruskereső** ablaka.
4. A **Megbízható URL-ek** lapon jelölje be a **Ne vizsgálja a megbízható URL-ekről érkező webes forgalmat** négyzetet.
5. Hozzon létre egy listát olyan webhelyekről/weboldalokról, amelyek tartalmában megbízik. Ehhez tegye a következőt:
  - a. Kattintson a **Hozzáadás** gombra.  
Megnyílik a **Címmezsk (URL)** ablak.
  - b. Adja meg a webhely / weboldal címét, vagy webhely / weboldal címmezskjét.
  - c. Kattintson az **OK** gombra.  
Megjelenik egy új bejegyzés a megbízható URL-ek listáján.
6. Szükség esetén ismétlje meg a lépéseket a-tól c-ig.

## IM VÍRUSKERESŐ

Az IM víruskereső az azonnali üzenő kliensek (*internetes üzenetküldők*) forgalmát vizsgálja.

Az IM üzenetek gyanús webhelyekre, valamint a hackerek által adathalászati támadásokhoz használt webhelyekre mutató hivatkozásokat tartalmazhatnak. A rosszindulatú programok IM klienseket felhasználva küldenek levélszemetet tartalmazó üzeneteket és hivatkozásokat a programoknak (vagy magukat a programokat), amelyek kilopatják a felhasználói azonosító számokat és jelszavakat.

A Kaspersky Anti-Virus számos azonnali üzenetküldő biztonságos működését képes biztosítani, többek között az ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, Mail.Ru Agent és IRC alkalmazásokét.

Bizonyos IM kliensek, például a Yahoo! Messenger és a Google Talk biztonságos kapcsolatot használnak. Az ilyen programok forgalmának vizsgálatához engedélyeznie kell a titkosított kapcsolatok vizsgálatát (lásd [87.](#) oldal).

Az IM víruskereső elfogja az üzeneteket és megvizsgálja azokat veszélyes objektumok vagy URL-ek tekintetében. Megadhatja a vizsgálandó üzenetek típusát és a vizsgálati módokat.

Ha egy üzenetben a rendszer fenyegetést észlel, az IM víruskereső az üzenetet lecseréli egy a felhasználónak címzett figyelmeztető üzenetre.

Az IM klienseken keresztül továbbított fájlokat a Fájlvíruskereső összetevő (lásd [67.](#) oldal) ellenőrzi, amikor menteni próbálják azokat.

**EBBEN A RÉSZBEN:**

Az IM víruskereső engedélyezése és letiltása.....	<a href="#">83</a>
IM víruskereső védelmi hatókörének létrehozása .....	<a href="#">83</a>
URL-ek ellenőrzése az IM kliensekből érkező üzenetekben .....	<a href="#">83</a>
Heurisztikus elemzés alkalmazása az IM víruskereső működése során .....	<a href="#">83</a>

**AZ IM VÍRUSKERESŐ ENGEDÉLYEZÉSE ÉS LETILTÁSA**

Alapértelmezésben az IM víruskereső engedélyezve van és normál módban működik. Szükség esetén letilthatja az IM víruskeresőt.

➔ *Az IM víruskereső letiltása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki az **IM víruskereső** összetevőt.
3. Szüntesse meg az **IM víruskereső engedélyezése** négyzet bejelölését az ablak jobb oldali részében.

**IM VÍRUSKERESŐ VÉDELMI HATÓKÖRÉNEK LÉTREHOZÁSA**

A védelem hatóköre a vizsgálandó üzenetek típusát jelenti. A Kaspersky Anti-Virus alapértelmezésben a bejövő és kimenő üzeneteket egyaránt vizsgálja. Ha biztos abban, hogy az elküldött üzenetei nem tartalmazhatnak rosszindulatú objektumokat, letilthatja a kimenő forgalom vizsgálatát.

➔ *A kimenő üzenetek vizsgálatának letiltása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki az **IM víruskereső** összetevőt.
3. Az ablak jobb oldalának **Védelem hatóköre** részében válassza ki a **Csak bejövő üzenetek** lehetőséget.

**URL-EK ELLENŐRZÉSE AZ IM KLIENSEKBŐL ÉRKEZŐ ÜZENETEKBE**

➔ *Gyanús és adathalász URL-ekről származó üzenetek vizsgálata:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki az **IM víruskereső** összetevőt.
3. Az ablak jobb oldalán található **Vizsgálatmódok** részben jelölje be az **URL-ek ellenőrzése a gyanús URL-ek adatbázisában** és az **URL-ek ellenőrzése az adathalász URL-ek adatbázisában** négyzetet.

**HEURISZTIKUS ELEMZÉS ALKALMAZÁSA AZ IM VÍRUSKERESŐ MŰKÖDÉSE SORÁN**

A védelem hatékonyságának javítása érdekében használhatja a *heurisztikus elemzést* (azaz, az objektum által a rendszerben végzett tevékenység elemzését). Az elemzés olyan új rosszindulatú objektumok észlelését teszi lehetővé, amelyek még nincsenek benne az adatbázisokban.

A heurisztikus elemzés használata esetén az IM kliensek üzeneteiben található minden parancsfájl védett környezetben kerül végrehajtásra. Ha a parancsfájl műveletei a rosszindulatú programok műveleteire hasonlítanak, akkor az objektum valószínűleg rosszindulatú vagy gyanús. A heurisztikus elemzés alapértelmezésben engedélyezett.

➔ *A heurisztikus elemzés engedélyezése:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki az **IM víruskereső** összetevőt.
3. Az ablak jobb oldali részében, a **Vizsgálatmódok** részben jelölje be a **Heurisztikus elemzés** négyzetet, és állítsa be a vizsgálat kívánt intenzitási szintjét.

## PROAKTÍV VÉDELEM

A Proaktív védelem a Kaspersky Anti-Virus adatbázisaiban még nem szereplő új fenyegetések ellen védi a számítógépet.

A Proaktív védelem működése proaktív technológiákon alapul. A proaktív technológiák segítségével még azelőtt semlegesíthető az új fenyegetés, hogy bármilyen kárt tenne számítógépében. A kódokat a Kaspersky Anti-Virus adatbázisaiban bejegyzései alapján elemző reaktív technológiákkal ellentétben a megelőző technológiák a programok által végrehajtott művelet sorok alapján ismerik fel a számítógépen található fenyegetéseket. Ha a tevékenységelemzés során bármiféle gyanú merül fel a művelet sorral kapcsolatban, a Kaspersky Anti-Virus blokkolja az illető alkalmazás működését.

Ha például a rendszer olyan programot észlel, amely hálózati erőforrásokra, az indítómappába vagy a rendszerleíró adatbázisba másolja magát, valószínűsíthető, hogy féregről van szó.

Veszélyes művelet sorok lehetnek a HOSTS fájl módosítására irányuló kísérletek, illesztőprogramok rejtett telepítése stb. Lehetősége van a veszélyes tevékenységek monitorozásának kikapcsolására (lásd [85.](#) oldal) vagy a monitorozás szabályainak szerkesztésére (lásd [85.](#) oldal).

A Proaktív védelem számára létrehozhatja a megbízható alkalmazások csoportját (lásd [84.](#) oldal). Az ilyen alkalmazások tevékenységéről nem kap értesítést.

Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64, Microsoft Windows 7 és Microsoft Windows 7 x64 alatt a felügyelet nem érint minden eseményt. Ez a nevezett operációs rendszerek jellegzetességeiből adódik. Például az összetevő nem felügyeli teljes körűen az adatok küldését megbízható alkalmazásokon keresztül, valamint a gyanús rendszertevékenységeket sem.

### EBBEN A RÉSZBEN:

A Proaktív védelem engedélyezése és letiltása .....	<a href="#">84</a>
Megbízható alkalmazások csoportjának létrehozása .....	<a href="#">84</a>
Veszélyes tevékenységek listájának használata .....	<a href="#">85</a>
Alkalmazás veszélyes tevékenységére indított művelet módosítása .....	<a href="#">85</a>

## A PROAKTÍV VÉDELEM ENGEDÉLYEZÉSE ÉS LETILTÁSA

A Proaktív védelem alapértelmezett módon be van kapcsolva, és a Kaspersky Lab specialistái által javasolt beállítással működik. A Proaktív védelmet szükség esetén letilthatja.

### ➤ A Proaktív védelem letiltása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Proaktív védelem** összetevőt.
3. Szüntesse meg a **Proaktív védelem engedélyezése** négyzet bejelölését az ablak jobb oldali részében.

## MEGBÍZHATÓ ALKALMAZÁSOK CSOPORTJÁNAK LÉTREHOZÁSA

Létrehozhatja a megbízható alkalmazások egy csoportját, amelynek a tevékenységét nem felügyeli a Proaktív védelem. Alapértelmezésben a megbízható alkalmazások listája a digitális aláírással rendelkező alkalmazásokat és a Kaspersky Security Network adatbázisában megbízhatóként jelölt alkalmazásokat tartalmazza.

### ➤ A megbízható alkalmazások csoport beállításainak módosítása:

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Proaktív védelem** összetevőt.
3. Az ablak jobb felén, a **Megbízható alkalmazások** részben végezze el az alábbi műveleteket:
  - Ha azt kívánja, hogy a hitelesített digitális aláírással rendelkező alkalmazások szerepeljenek a megbízható alkalmazások csoportjában, jelölje be az **Alkalmazások digitális aláírással** négyzetet.
  - Ha azt kívánja, hogy a Kaspersky Security Network adatbázisa által megbízhatónak tartott alkalmazások szerepeljenek a megbízható alkalmazások csoportjában, jelölje be a **Megbízható a Kaspersky Security Network adatbázisában** négyzetet.

## VESZÉLYES TEVÉKENYSÉGEK LISTÁJÁNAK HASZNÁLATA

A veszélyes tevékenységekre jellemző műveletek listája nem szerkeszthető. Azonban megtagadhatja a kiválasztott veszélyes tevékenység felügyeletét.

- ◆ *Adott veszélyes tevékenység figyelésének kikapcsolása:*
  1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
  2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Proaktív védelem** összetevőt.
  3. Kattintson a **Beállítások** gombra az ablak jobb oldali részében.
  4. A megnyíló **Proaktív védelem** ablakban törölje a bejelölést azon tevékenységtípus mellett, amelyiket nem kívánja figyelni.

## ALKALMAZÁS VESZÉLYES TEVÉKENYSÉGÉRE INDÍTOTT MŰVELET MÓDOSÍTÁSA

A veszélyes tevékenységekre jellemző műveletek listája nem szerkeszthető. Ugyanakkor megváltoztathatja azt a műveletet, amelyet a Kaspersky Anti-Virus végez, amikor egy alkalmazás veszélyes tevékenységét észleli.

- ◆ *A Kaspersky Lab alkalmazás által a másik alkalmazás veszélyes tevékenységére válaszul indított művelet megváltoztatása:*
  1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
  2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Proaktív védelem** összetevőt.
  3. Kattintson a **Beállítások** gombra az ablak jobb oldali részében.
  4. A megnyíló **Proaktív védelem** ablak **Esemény** részében válassza ki azt az eseményt, amelyre vonatkozóan a szabályt módosítani kívánja.
  5. Adja meg a kiválasztott esemény beállításait a **Szabályleírás** részben lévő hivatkozások segítségével. Például:
    - a. Kattintson az előre beállított művelet hivatkozására és a megnyíló **Válasszon műveletet** ablakban válassza ki a kívánt műveletet.
    - b. Kattintson a **Be / Ki** hivatkozásra annak meghatározásához, hogy a feladat elvégzésekor készüljön-e jelentés.

## RENDSZERFIGYELŐ

A Rendszerfigyelő a számítógépen futó alkalmazások műveleteiről gyűjt adatokat, és információkat nyújt a többi összetevőnek a védelem fokozása érdekében.

A Rendszerfigyelő által összegyűjtött információk alapján a Kaspersky Anti-Virus visszagörgetheti a rosszindulatú programok által végrehajtott műveleteket.

A rosszindulatú programok által végrehajtott műveletek visszagörgetését az alábbi védelmi összetevők kezdeményezhetik:

- Rendszerfigyelő – a veszélyes tevékenység mintázata alapján;
- Proaktív védelem;
- Fájl víruskereső;
- víruskeresés végrehajtásakor.

Ha a rendszerben gyanús eseményt észlelt, a Kaspersky Anti-Virus védelmi összetevői további információkat kérhetnek a Rendszerfigyelőtől. A Kaspersky Anti-Virus interaktív védelmi módjában (lásd: „Védelmi mód kiválasztása”, [56.](#) oldal) megtekintheti a Rendszerfigyelő összetevő által összegyűjtött és a veszélyes tevékenységgel kapcsolatos előzményeket tartalmazó jelentés formájában bemutatott adatokat. Ezek az adatok segítenek dönteni, amikor ki kell választani egy műveletet az értesítési ablakban. Ha az összetevő rosszindulatú programot észlel, az értesítési ablak (lásd [126.](#) oldal) felső részében megjelenik a Rendszerfigyelő jelentéséhez vezető hivatkozás a művelet kiválasztására vonatkozó felkéréssel.

**EBBEN A RÉSZBEN:**

A Rendszerfigyelő engedélyezése és letiltása .....	<a href="#">86</a>
Veszélyes tevékenység mintázatának a használata (BSS).....	<a href="#">86</a>
Rosszindulatú programok által végzett műveletek visszagörgetése .....	<a href="#">86</a>

**A RENDSZERFIGYELŐ ENGEDÉLYEZÉSE ÉS LETILTÁSA**

A Rendszerfigyelő alapértelmezett módon be van kapcsolva, és a Kaspersky Lab specialistái által javasolt beállítással működik. A Rendszerfigyelőt szükség esetén letilthatja.

**Javasoljuk, hogy ha nem feltétlenül szükséges, ne tiltsa le az összetevőt, mert ez elkerülhetetlenül hatással van a Proaktív védelem és más olyan védelmi összetevők hatékony működésére, amelyek az észlelt potenciális fenyegetés azonosítására a Rendszerfigyelő által gyűjtött adatokat használják.**

◆ **A Rendszerfigyelő letiltása:**

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Rendszerfigyelő** összetevőt.
3. Az ablak jobb oldalán szüntesse meg a **Rendszerfigyelő engedélyezése** négyzet bejelölését.

**VESZÉLYES TEVÉKENYSÉG MINTÁZATÁNAK A HASZNÁLATA (BSS)**

A veszélyes tevékenység mintázatai (BSS – Behavior Stream Signatures) a veszélyesnek minősített alkalmazások jellemző műveletsoarait tartalmazzák. Ha egy alkalmazás aktivitása megegyezik a veszélyes tevékenység mintázatával, a Kaspersky Anti-Virus végrehajtja az előírt műveletet.

A valós idejű hatékony védelem érdekében a Kaspersky Anti-Virus gyarapítja a Rendszerfigyelő által használt veszélyes tevékenységek mintáit az adatbázis frissítései során.

Ha a Kaspersky Anti-Virus automatikus üzemmódban fut, a Rendszerfigyelő alapértelmezésben karanténba helyezi az alkalmazást, ha a tevékenysége megfelel a veszélyes tevékenység mintázatának. Ha interaktív módban fut, a Rendszerfigyelő rákérdez az elvégzendő műveletre. Megadhatja, hogy milyen műveletet végezzen az összetevő, ha egy alkalmazás tevékenysége megfelel a veszélyes tevékenység mintázatának.

Annak figyelése mellett, hogy az alkalmazás tevékenysége pontosan megfelel-e a veszélyes tevékenység mintázatának, a Rendszerfigyelő az olyan részleges egyezést is figyeli, amelyet a heurisztikus elemzés gyanúsak talál. Gyanús aktivitás észlelése esetén a Rendszerfigyelő a működési módjától függetlenül figyelmeztetést ad.

◆ **Annak megadása, hogy milyen műveletet végezzen az összetevő, ha egy alkalmazás tevékenysége megfelel a veszélyes tevékenység mintázatának:**

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Rendszerfigyelő** összetevőt.
3. Az ablak jobb oldalán található **Heurisztikus elemzés** részben jelölje be a **Veszélyes tevékenység frissíthető mintázatának használata (BSS)** négyzetet.
4. Kattintson a **Válasszon műveletet** elemre, és válassza ki a legördülő listából a kívánt műveletet.

**ROSSZINDULATÚ PROGRAMOK ÁLTAL VÉGZETT MŰVELETEK VISSZAGÖRGETÉSE**

Használhatja a rosszindulatú programok által a rendszerben végzett műveletek visszagörgetésére szolgáló lehetőséget. A visszagörgetés lehetővé tételéhez a Rendszerfigyelő naplózza a programok tevékenységét. A Rendszerfigyelő által a visszagörgetésekhez tárolt információk mennyiségét korlátozhatja.

A Kaspersky Anti-Virus alapértelmezésben automatikusan végrehajtja az adott műveletek visszagörgetését, ha a védelmi összetevő rosszindulatú tevékenységet észlel. Ha interaktív módban fut, a Rendszerfigyelő rákérdez az

elvégzendő műveletre. Meghatározhatja az egy rosszindulatú program által végrehajtott művelet visszagörgethetősége esetén végrehajtható műveletet.

A rosszindulatú programok műveleteinek visszagörgetése szigorúan meghatározott adatcsoportot érint. Ez semmilyen negatív következménnyel nem jár az operációs rendszer vagy a számítógép adatainak integritására nézve.

➤ *A rosszindulatú program által végrehajtott művelet visszagörgethetősége esetén végrehajtható művelet kiválasztása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Rendszerfigyelő** összetevőt.
3. Az ablak jobb oldalán, a **Rosszindulatú műveletek visszagörgetése** részben válassza a **Válasszon műveletet** lehetőséget, és a legördülő listából válassza ki a kívánt műveletet.

➤ *A Rendszerfigyelő által a visszagörgetésekhez tárolt információk mennyiségének korlátozása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Védelmi központ** részében válassza ki a **Rendszerfigyelő** összetevőt.
3. Az ablak jobb oldalán, a **Rosszindulatú műveletek visszagörgetése** részben jelölje be az **A visszagörgetéshez tárolt adatok korlátozása** négyzetet, és adja meg azt a maximális adatmennyiséget, amelyet a Rendszerfigyelő tárolhat a visszagörgetésekhez.

## HÁLÓZATI VÉDELEM

A Kaspersky Anti-Virus eszközei és beállításai együttesen biztosítja a hálózati tevékenységek biztonságát és felügyeletét.

Az alábbi rész részletes információkat nyújt a hálózati kapcsolatok ellenőrzéséről, a proxykiszolgáló beállításairól és a hálózati portok figyeléséről.

### EBBEN A RÉSZBEN:

Titkosított kapcsolatok vizsgálata .....	<a href="#">87</a>
A proxykiszolgáló beállítása .....	<a href="#">89</a>
Figyelt portok listájának létrehozása .....	<a href="#">89</a>

## TITKOSÍTOTT KAPCSOLATOK VIZSGÁLATA

Az SSL-/TLS-protokollokkal való kapcsolódás védi az adatcserére szolgáló csatornát az interneten. Az SSL / TLS protokollok használata esetén elektronikus tanúsítványok segítségével azonosíthatók az adatcserét végző felek, kódolhatók a továbbított adatok, és biztosítható azok épsége az átvitel során.

A protokollnak mindezeket a tulajdonságait a számítógépes betörők rosszindulatú programok terjesztésére használják fel, hiszen a legtöbb víruskereső alkalmazás nem ellenőrzi az SSL-/TLS-forgalmat.

A Kaspersky Anti-Virus a titkosított kapcsolatokat a Kaspersky Lab tanúsítványával vizsgálja.

Ha a kiszolgálóhoz való csatlakozás közben az alkalmazás érvénytelen tanúsítványt észlel (például ha a tanúsítványt egy behatoló kicserélte), egy a képernyőn megjelenő értesítés a tanúsítvány elfogadását vagy visszautasítását kéri.

Ha biztos benne, hogy a webhellyel a kapcsolat az érvénytelen tanúsítvány ellenére is mindig biztonságos, a webhelyet felveheti a megbízható URL-ek listájára. A Kaspersky Anti-Virus a továbbiakban nem fogja vizsgálni a titkosított kapcsolatot ezzel a webhellyel.

A Tanúsítványtelepítő varázsló segítségével telepítheti a titkosított kapcsolatok félig interaktív módban való vizsgálatához szükséges tanúsítványt Microsoft Internet Explorer, Mozilla Firefox (ha nincs elindítva) és Google Chrome böngészőkhöz, emellett utasításokat kaphat arra vonatkozóan, hogyan telepítheti a Kaspersky Lab tanúsítványát Opera böngészőhöz.

- *A titkosított kapcsolatok vizsgálatának engedélyezése és a Kaspersky Lab tanúsítványának telepítése:*
  1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
  2. Az ablak bal oldalán a **Speciális beállítások** részben válassza ki a **Hálózat** összetevőt.
  3. A megnyíló ablakban jelölje be a **Titkosított kapcsolatok vizsgálata** négyzetet. Ha először engedélyezi a beállítást, automatikusan elindul a Tanúsítványtelepítő varázsló.
  4. Ha a varázsló nem indul el, kattintson a **Tanúsítvány telepítése** gombra. Ekkor elindul egy varázsló, amely végigvezet a Kaspersky Lab tanúsítványának sikeres telepítéséhez szükséges lépéseken.

## EBBEN A RÉSZBEN:

Titkosított kapcsolatok vizsgálata a Mozilla Firefox böngészőben .....	<a href="#">88</a>
Titkosított kapcsolatok vizsgálata az Opera böngészőben.....	<a href="#">88</a>

## TITKOSÍTOTT KAPCSOLATOK VIZSGÁLATA A MOZILLA FIREFOX BÖNGÉSZŐBEN

A Mozilla Firefox böngésző nem használ Microsoft Windows tanúsítványtárolást. Az SSL-kapcsolatok Firefox használata melletti vizsgálatához manuálisan kell telepíteni a Kaspersky Lab tanúsítványát.

Használhatja a Tanúsítványtelepítő varázslót, ha a böngésző nincs elindítva.

- *A Kaspersky Lab tanúsítványának telepítése:*
  1. A böngésző menüjében válassza az **Eszközök**→**Beállítások** elemet.
  2. A megnyíló ablakban válassza a **További** részt.
  3. A **Tanúsítványok** részben válassza a **Biztonság** lapot, és kattintson a **Tanúsítványkezelő** gombra.
  4. A megnyíló ablakban válassza ki a **Hitelesítésszolgáltatók** lapot, majd kattintson a **Visszaállítás** gombra.
  5. A megnyíló ablakban válassza ki a Kaspersky Lab tanúsítványát. A Kaspersky Lab tanúsítványának elérési útvonala a következő:  
`%AllUsersProfile%\Application Data\Kaspersky Lab\AVP12\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.`
  6. A megnyíló ablakban a négyzetek bejelölésével válassza ki azokat a műveleteket, amelyeket a telepített tanúsítvánnyal vizsgálni szeretne. A tanúsítvány adatainak megtekintéséhez kattintson a **Megtekintés** gombra.
- *A Kaspersky Lab tanúsítványának kézi telepítése a Mozilla Firefox 3.x verziójához:*
  1. A böngésző menüjében válassza az **Eszközök**→**Beállítások** elemet.
  2. A megnyíló ablakban válassza a **További** részt.
  3. A **Titkosítás** lapon kattintson a **Tanúsítványkezelő** gombra.
  4. A megnyíló ablakban válassza ki a **Hitelesítésszolgáltatók** lapot, majd kattintson az **Importálás** gombra.
  5. A megnyíló ablakban válassza ki a Kaspersky Lab tanúsítványát. A Kaspersky Lab tanúsítványának elérési útvonala a következő:  
`%AllUsersProfile%\Application Data\Kaspersky Lab\AVP12\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.`
  6. A megnyíló ablakban a négyzetek bejelölésével válassza ki azokat a műveleteket, amelyeket a telepített tanúsítvánnyal vizsgálni szeretne. A tanúsítvány adatainak megtekintéséhez kattintson a **Megtekintés** gombra.

Ha a számítógépén Microsoft Windows Vista vagy Microsoft Windows 7 fut, a Kaspersky Lab tanúsítványának elérési útvonala a következő: `%AllUsersProfile%\Kaspersky Lab\AVP12\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.`

## TITKOSÍTOTT KAPCSOLATOK VIZSGÁLATA AZ OPERA BÖNGÉSZŐBEN

Az Opera böngésző nem használ Microsoft Windows tanúsítványtárolást. Ha Opera használata mellett vizsgál SSL-kapcsolatokat, manuálisan kell telepítenie a Kaspersky Lab tanúsítványt.

➤ *A Kaspersky Lab tanúsítványának telepítése:*

1. A böngésző menüjében válassza az **Eszközök**→**Beállítások** elemet.
2. A megnyíló ablakban válassza a **További** részt.
3. Az ablak bal oldali részén válassza a **Biztonság** lapot, majd kattintson a **Tanúsítványok kezelése** gombra.
4. A megnyíló ablakban válassza ki a **Szállítók** lapot, majd kattintson az **Importálás** gombra.
5. A megnyíló ablakban válassza ki a Kaspersky Lab tanúsítványát. A Kaspersky Lab tanúsítványának elérési útvonala a következő:  
`%AllUsersProfile%\Application Data\Kaspersky Lab\AVP12\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.`
6. A megnyíló ablakban kattintson a **Telepítés** gombra. A Kaspersky Lab tanúsítványa telepítésre kerül. A tanúsítvány adatainak megtekintésére és a műveletek kiválasztására, amelyekre a tanúsítványt használni fogja, jelölje ki a listából a tanúsítványt, és kattintson a **Megtekintés** gombra.

➤ *A Kaspersky Lab tanúsítványának telepítése Opera 9.x verzióhoz:*

1. A böngésző menüjében válassza az **Eszközök**→**Beállítások** elemet.
2. A megnyíló ablakban válassza a **További** részt.
3. Az ablak bal oldali részén válassza a **Biztonság** lapot, majd kattintson a **Tanúsítványok kezelése** gombra.
4. A megnyíló ablakban válassza ki a **Hitelesítésszolgáltatók** lapot, majd kattintson az **Importálás** gombra.
5. A megnyíló ablakban válassza ki a Kaspersky Lab tanúsítványát. A Kaspersky Lab tanúsítványának elérési útvonala a következő:  
`%AllUsersProfile%\Application Data\Kaspersky Lab\AVP12\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.`
6. A megnyíló ablakban kattintson a **Telepítés** gombra. A Kaspersky Lab tanúsítványa telepítésre kerül.

Ha a számítógépén Microsoft Windows Vista vagy Microsoft Windows 7 fut, a Kaspersky Lab tanúsítványának elérési útvonala a következő: `%AllUsersProfile%\Kaspersky Lab\AVP12\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.`

## A PROXYKISZOLGÁLÓ BEÁLLÍTÁSA

Ha a számítógép proxykiszolgálón keresztül csatlakozik az internethez, szükség lehet a kapcsolat beállításainak szerkesztésére. A Kaspersky Anti-Virus ezeket a beállításokat több védelmi összetevőnél, valamint az alkalmazás adatbázisainak és moduljainak frissítésekor is használja.

Ha a hálózat nem szabványos portot használó proxykiszolgálót tartalmaz, a port számát fel kell venni a figyelt portok listájára (lásd: „Figyelt portok listájának létrehozása”, [89.](#) oldal).

➤ *Proxykiszolgálóval rendelkező kapcsolat beállításai:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán a **Speciális beállítások** részben válassza ki a **Hálózat** összetevőt.
3. Kattintson a **Proxykiszolgáló beállításai** gombra a **Proxykiszolgáló** részben.
4. A megnyíló **Proxykiszolgáló beállításai** ablakban adja meg a proxykiszolgálóhoz való kapcsolódás beállításait.

## FIGYELT PORTOK LISTÁJÁNAK LÉTREHOZÁSA

Az olyan védelmi összetevők, mint a Levél víruskereső, a Webes víruskereső és az IM víruskereső (lásd [77.](#) oldal) figyelik a bizonyos protokollokkal bizonyos nyitott TCP portokon átmenő adatforgalmat. Például, a Levél víruskereső az SMTP-kapcsolaton küldött adatokat, míg a Webes víruskereső a HTTP-, HTTPS- és FTP-kapcsolatok adatátvitelét ellenőrzi.

Engedélyezheti az összes vagy csak a kiválasztott hálózati portok figyelését. Ha úgy állítja be a terméket, hogy csak bizonyos portokat figyeljen, létrehozhatja azoknak az alkalmazásoknak a listáját, amelyek esetében minden port figyelendő. Javasoljuk, hogy bővítse ki a listát az FTP-kapcsolaton adatátvitelt folytató alkalmazások felvételével.

➤ *Port hozzáadása a megfigyelt portok listájához:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldali részén, a **Speciális beállítások** részben válassza ki a **Hálózat** alpontot.
3. A **Figyelt portok** részben jelölje ki a **Csak a kijelölt portok figyelése** elemet, majd kattintson a **Kiválasztás** gombra.  
Megnyílik a **Hálózati portok** ablak.
4. A **Hálózati port** ablak megnyitásához, majd a portszám és a leírás megadásához kattintson az ablak felső részén a portok listája alatt található **Hozzáadás** hivatkozásra.

➤ *Port kizárása a megfigyelt portok listájáról:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldali részén, a **Speciális beállítások** részben válassza ki a **Hálózat** alpontot.
3. A **Figyelt portok** részben jelölje ki a **Csak a kijelölt portok figyelése** elemet, majd kattintson a **Kiválasztás** gombra.  
Megnyílik a **Hálózati portok** ablak.
4. Az ablak felső részén a portok listájában szüntesse meg a kizárandó port leírása melletti négyzet jelölését.

➤ *Azon alkalmazások listájának létrehozása, amelyeknél minden portot figyelni szeretne:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldali részén, a **Speciális beállítások** részben válassza ki a **Hálózat** alpontot.
3. A **Figyelt portok** részben jelölje ki a **Csak a kijelölt portok figyelése** elemet, majd kattintson a **Kiválasztás** gombra.  
Megnyílik a **Hálózati portok** ablak.
4. Jelölje be **A megadott alkalmazások figyelése minden porton** négyzetet, és az alkalmazások listájában jelölje be annak az alkalmazásnak a neve melletti négyzetet, amelyiknek az összes portját meg kívánja figyelni.
5. Ha a kívánt alkalmazás nincs a listán, az alábbi módon veheti fel rá:
  - a. Kattintson a **Hozzáadás** hivatkozásra az alkalmazáslista alatt a menü megnyitásához, és válasszon egy elemet:
    - Egy alkalmazás végrehajtható fájlja helyének megadásához válassza a **Tallózás** gombot, és adja meg a fájl helyét a számítógépen.
    - Válassza az **Alkalmazások** opciót egy alkalmazás kiválasztásához a jelenleg futó alkalmazások listájából. A megnyíló **Alkalmazás kiválasztása** ablakban válassza ki a kívánt alkalmazást.
  - b. Az **Alkalmazás** ablakban adja meg a kiválasztott alkalmazás leírását.

## MEGBÍZHATÓ ZÓNA

A *Megbízható zóna* egy objektumlista, amelynek elemeit az alkalmazásnak nem kell figyelnie. Más szóval a Kaspersky Anti-Virus védelmi hatókörére vonatkozó kizárások egy csoportja.

A Megbízható zóna létrehozása a megbízható alkalmazások listája (lásd: „Megbízható alkalmazások listájának létrehozása”, 91. oldal) és a kizárási szabályok (lásd: „Kizárási szabályok létrehozása”, 91. oldal) alapján történik, figyelembe véve a feldolgozott objektumok és a számítógépre telepített alkalmazások tulajdonságait. Adott objektumok megbízható zónába történő felvételére azért lehet szükség, mert például a Kaspersky Anti-Virus blokkolhat olyan objektumhoz / alkalmazáshoz való hozzáférést is, amely egyébként teljesen ártalmatlan.

Például, ha úgy gondolja, hogy a Microsoft Windows Notepad által használt objektumok ártalmatlanok és nem igényelnek vizsgálatot, így megbízva ebben az alkalmazásban, a Notepadet felveheti a megbízható alkalmazások listájára, hogy kizárja az objektumok vizsgálatából.

Egyes veszélyesnek minősített tevékenységek biztonságosak lehetnek bizonyos alkalmazások esetében. Például a billentyűzetkiosztást automatikusan váltó alkalmazások (mint például a Punto Switcher) rendszeresen megszakítják a billentyűzeten keresztüli szövegbevitelt. Az ilyen alkalmazások specifikációnak figyelembe vételéhez és aktivitásuk monitorozásának a letiltásához célszerű ezeket a megbízható alkalmazások közé sorolni.

Ha egy alkalmazást felvett a megbízhatóak listájára, annak fájl és hálózati tevékenysége (még ha gyanús is) felügyelet nélkül folyhat, csak úgy, mint az alkalmazás rendszerleíró adatbázis elérésére irányuló próbálkozásai is. A víruskereső

ugyanekkor átvizsgálja a futtatható fájlt és a megbízható alkalmazás folyamatait, ahogy előtte is. Az alkalmazásnak a víruskeresésből történő kizárásához kizárási szabályokat kell használnia.

A megbízható alkalmazások víruskeresésből való kizárásával elkerülhetők olyan problémák, amelyek az adott alkalmazás más alkalmazásokkal való esetleges inkompatibilitásából ered (pl. a hálózati forgalom kettős vizsgálata harmadik fél számítógépén a Kaspersky Anti-Virus alkalmazással és más víruskereső programmal is), és ezenkívül növeli a számítógép teljesítményét, ami kiszolgáló alkalmazásoknál kritikus lehet.

Cserébe a megbízható zóna kizárási szabályai biztonságosabbá teszik a kockázatos programokkal végzett munkát. Az ilyen alkalmazások nem rendelkeznek rosszindulatú funkciókkal, de egy rosszindulatú program külső összetevőként felhasználhatja azokat. Ebbe a kategóriába tartoznak például a távoli rendszer-felügyeleti programok, IRC-kliensek, FTP-szerverek, különböző segédprogramok, amelyek folyamatokat állítanak le vagy rejtenek el, billentyűzetfigyelők, jelszófeltörők, automata tárcsázók stb. Az ilyen alkalmazásokat a Kaspersky Anti-Virus blokkolhatja. A blokkolás elkerülésére kizárási szabályok konfigurálhatók.

A **Kizárási szabály** egy olyan feltételkészlet, ami a Kaspersky Anti-Virus által nem vizsgálandó objektumot határoz meg. Minden egyéb esetben az objektumot a vonatkozó védelmi beállítások szerint az összes védelmi komponens átvizsgálja.

A megbízható zóna kizárási szabályait olyan alkalmazás-összetevők használhatják, mint például a Fájl víruskereső (lásd: „Fájl víruskereső”, [67.](#) oldal), Levél víruskereső (lásd: „Levél víruskereső”, [72.](#) oldal) Webes víruskereső (lásd: „Webes víruskereső”, [77.](#) oldal), vagy víruskeresési feladat futtatásakor kerülhetnek használatba.

## EBBEN A RÉSZBEN:

Megbízható alkalmazások listájának létrehozása .....	<a href="#">91</a>
Kizárási szabályok létrehozása .....	<a href="#">91</a>

## MEGBÍZHATÓ ALKALMAZÁSOK LISTÁJÁNAK LÉTREHOZÁSA

A Kaspersky Anti-Virus alapértelmezés szerint átvizsgálja a megnyitott, futó vagy bármilyen programfolyamat által mentett objektumokat, és monitorozza az összes alkalmazás tevékenységét és az általuk generált hálózati forgalmat. Ha egy alkalmazást hozzáad a megbízható alkalmazások listájához, a Kaspersky Anti-Virus kizárja azt a vizsgálatból.

### ➤ *Alkalmazás hozzáadása a megbízható listára:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Speciális beállítások** részében válassza ki a **Fenyegetések és kizárások** alpontot.
3. A megnyíló **Kizárások** részben kattintson a **Beállítások** gombra.
4. A megnyíló ablak **Megbízható alkalmazások** lapján kattintson a **Hozzáadás** gombra az alkalmazás kiválasztására szolgáló menü megnyitásához.
5. A megnyíló menüben válasszon egy alkalmazást az **Alkalmazások** listából, vagy a **Tallózás** gombot megnyomva adja meg kívánt alkalmazás végrehajtható fájljának elérési útvonalát.
6. A megnyíló **Alkalmazás kizárásai** ablakban jelölje be a négyzeteket az alkalmazás azon tevékenységtípusai mellett, amelyeket ki szeretne zárni a vizsgálatból.

## KIZÁRÁSI SZABÁLYOK LÉTREHOZÁSA

Ha a Kaspersky Anti-Virus által olyannak ismert alkalmazásokat használ, amelyeket a behatolók a számítógép vagy a felhasználó adatainak a károsítására használhatnak, azt javasoljuk, hogy konfiguráljon rájuk kizárási szabályokat.

### ➤ *Kizárási szabály létrehozása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Speciális beállítások** részében válassza ki a **Fenyegetések és kizárások** alpontot.
3. A megnyíló **Kizárások** részben kattintson a **Beállítások** gombra.
4. A megnyíló ablak **Kizárási szabály** lapján kattintson a **Hozzáadás** hivatkozásra.
5. A megnyíló **Kizárási szabály** ablakban végezze el a kizárási szabály szerkesztését.

## TELJESÍTMÉNY ÉS MÁS ALKALMAZÁSOKKAL VALÓ KOMPATIBILITÁS

A Kaspersky Anti-Virus teljesítményét az észlelt fenyegetések köre, valamint az energia és a számítástechnikai erőforrások felhasználása határozza meg.

A Kaspersky Anti-Virus lehetővé teszi a különböző kategóriájú fenyegetések kiválasztását (lásd: „Az észlelhető fenyegetéskategóriák kiválasztása”, [92.](#) oldal), amelyet az alkalmazásnak észlelnie kell.

Az energiafogyasztás nagy fontossággal bír a hordozható számítógépeknél. A számítógép vírusellenőrzése és a Kaspersky Anti-Virus adatbázisainak a frissítése jelentős erőforrásigénnyel bír. A Kaspersky Anti-Virus speciális laptop üzemmódja (lásd: „Energiatakarékosság”, [92.](#) oldal) lehetővé teszi az ütemezett vizsgálatok és frissítések automatikus késleltetését, ha a gép akkumulátorról működik, így meghosszabbítva az üzemidőt, míg az Üresjárat vizsgálat üzemmód (lásd: „Feladatok futtatása a háttérben”, [93.](#) oldal) segítségével akkor futtathatók nagy erőforrás-igényű feladatok, amikor a gép éppen nincs használatban.

A számítógép erőforrásainak fogyasztását tekintve a Kaspersky Anti-Virus hatással lehet más alkalmazások teljesítményére is. A CPU és a lemez alrendszer több program egyidejű működése által okozott fokozott terhelésének csökkentése érdekében a Kaspersky Anti-Virus szüneteltetheti a vizsgálati feladatokat, és átadhatja az erőforrásokat a többi alkalmazásnak (lásd: „A számítógép erőforrásainak elosztása vírusellenőrzéskor”, [93.](#) oldal).

Játék profil (lásd [94.](#) oldal) üzemmódban az alkalmazás automatikusan letiltja a Kaspersky Anti-Virus tevékenységével kapcsolatos értesítéseket, ha a másik alkalmazás teljes képernyős üzemmódban fut.

Ha a rendszerbe aktív fertőzés kerül, a speciális vírusmentesítési eljárás a számítógép újraindítását igényli, ami szintén hatással lehet más alkalmazások teljesítményére. Szükség esetén letilthatja a fejlett vírusmentesítő technológiát (lásd [93.](#) oldal), hogy elkerülhető legyen a gép szándékolatlan újraindítása.

### EBBEN A RÉSZBEN:

Az észlelhető fenyegetéskategóriák kiválasztása .....	<a href="#">92</a>
Energiatakarékosság .....	<a href="#">92</a>
Fejlett vírusmentesítés .....	<a href="#">93</a>
A számítógép erőforrásainak elosztása vírusellenőrzéskor .....	<a href="#">93</a>
Feladatok futtatása a háttérben.....	<a href="#">93</a>
Teljes képernyős mód. Játék profil.....	<a href="#">94</a>

## AZ ÉSZLELHETŐ FENYEGETÉSKATEGÓRIÁK KIVÁLASZTÁSA

A Kaspersky Anti-Virus az általa észlelt fenyegetéseket különböző attribútumok alapján kategóriákba rendezi. Az alkalmazás mindig keresi a vírusokat, Trójai programokat és rosszindulatú eszközöket. Ezek a programok jelentős károkat okozhatnak a számítógépen. A számítógép még megbízhatóbb védelme érdekében kibővítheti az észlelt fenyegetések listáját úgy, hogy engedélyezi az olyan legális alkalmazások tevékenységének a felügyeletét, amelyeket a behatoló felhasználhat a számítógéphez és a felhasználói adatokhoz való hozzáféréshez.

♦ *Az észlelhető fenyegetések kategóriájának a kiválasztása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Speciális beállítások** részében válassza ki a **Fenyegetések és kizárások** alpontot.
3. Az ablak jobb oldalán kattintson **A következő típusú veszélyek észlelése engedélyezett** lista alatt található **Beállítások** gombra.
4. A megnyíló **Fenyegetések** ablakban jelölje be a négyzeteket az észlelni kívánt fenyegetéskategóriák mellett.

## ENERGIATAKARÉKOSSÁG

A hordozható számítógépeken energiatakarékossági okból elhalasztható a víruskeresés és az ütemezett frissítési feladat végrehajtása. Szükség esetén manuálisan frissítheti a Kaspersky Anti-Virus alkalmazást, vagy elindíthatja a víruskeresést.

- *Az energiatakarékos mód engedélyezése akkumulátoros üzem mellett:*
  1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
  2. Az ablak bal oldalán, a **Speciális beállítások** részben válassza ki az **Energiatakarékosság** alpontot.
  3. Az ablak jobb oldali részén jelölje be az **Ütemezett vírusvizsgálatok blokkolása, ha a számítógép akkumulátorról üzemel** négyzetet.

## FEJLETT VÍRUSMENTESÍTÉS

A mai rosszindulatú programok a legalacsonyabb szinteken juthatnak be az operációs rendszerekbe, ezáltal a törlésük gyakorlatilag lehetetlen. Ha a rendszerben rosszindulatú tevékenységet észlel, a Kaspersky Anti-Virus a speciális Fejlett vírusmentesítés technológia alkalmazását ajánlja fel, melynek segítségével megszüntethető a fenyegetés, és törölhető a számítógépről is.

A fejlett vírusmentesítési eljárás végén az alkalmazás újraindítja a számítógépet. A számítógép újraindítása után ajánlott a teljes víruskeresést (lásd: „Vírusok keresése a számítógépen teljes vizsgálattal”, [42.](#) oldal) lefuttatni.

- *A Fejlett vírusmentesítési technológia alkalmazásának beállítása a Kaspersky Anti-Virus alkalmazásban:*
  1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
  2. Az ablak bal oldali részén, a **Speciális beállítások** részben válassza ki a **Kompatibilitás** alpontot.
  3. Jelölje be a **Fejlett vírusmentesítő technológia engedélyezése** négyzetet.

## A SZÁMÍTÓGÉP ERŐFORRÁSAINAK ELOSZTÁSA

### VÍRUSELLENŐRZÉSKOR

A vizsgálat végrehajtása növeli a processzor és a lemezes alrendszerek terhelését, ami lassítja a többi alkalmazást. Ilyen esetben a Kaspersky Anti-Virus alapértelmezésben szünetelteti a víruskeresési feladatot és átengedi a rendszer erőforrásait a felhasználó alkalmazásai számára.

Azonban sok alkalmazás azonnal elindul és a háttérben fut, amint a processzor rendelkezésre áll. Annak érdekében, hogy a vizsgálat ne függjön ezen alkalmazások működésétől, nem szabad a rendszer erőforrásait átengedni nekik.

- *Ahhoz, hogy a Kaspersky Anti-Virus felfüggeszesse a vizsgálati műveleteket, ha azok lassítják más alkalmazások működését:*
  1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
  2. Az ablak bal oldali részén, a **Speciális beállítások** részben válassza ki a **Kompatibilitás** alpontot.
  3. Jelölje be az **Erőforrások adása más alkalmazásoknak** négyzetet.

## FELADATOK FUTTATÁSA A HÁTTÉRBE

A számítógép erőforrásaira jutó terhelés optimalizálásához engedélyezheti, hogy a Kaspersky Anti-Virus a rootkitek keresését a háttérben futtassa, a nagy erőforrás-igényű műveleteket pedig a számítógép üresjáratában indítsa el.

A rootkitek rendszeres keresése akkor fut, amikor Ön is dolgozik a számítógépen. A keresés maximum 5 percig tart, és csak minimális mértékben veszi igénybe az erőforrásokat.

A számítógép üresjáratában az alábbi feladatok futhatnak:

- víruskereső adatbázisok és programmodulok automatikus frissítése;
- rendszermemória, indítási objektumok és rendszerpartíciók vizsgálata.

Az Üresjárat vizsgálat feladatai akkor indulnak el, ha a számítógépet a felhasználó blokkolta, vagy amikor a képernyővédő már legalább 5 perce üzemel.

Ha számítógépe akkumulátorról üzemel, üresjáratban nem indul el feladat.

Amikor a feladatok a háttérben futnak, az előrehaladásuk megjelenik a Feladatkezelő ablakban (lásd: „Vizsgálati feladatok kezelése. Feladatkezelő”, [63.](#) oldal).

**EBBEN A RÉSZBEN:**

Rootkitek keresése a háttérben.....	<a href="#">94</a>
Üresjárat vizsgálat.....	<a href="#">94</a>

**ROOTKITEK KERESÉSE A HÁTTÉRBE**

Alapértelmezésben a Kaspersky Anti-Virus rendszeresen végrehajtja a rootkitek keresését. Szükség esetén letilthatja a rootkitek keresését.

➤ *A rendszeres rootkit-keresés letiltása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Válassza ki a **Vizsgálat** részt az ablak bal oldali részén, majd ott az **Általános beállítások** alpontot.
3. Az ablak jobb oldalán törölje a **Rootkitek rendszeres vizsgálata** négyzet jelölését.

**ÜRESJÁRATI VIZSGÁLAT**

Az Üresjárat vizsgálat első lépése annak ellenőrzése, hogy az adatbázisok és program modulok naprakészek-e. Ha a vizsgálat után frissítés szükséges, elindul az automatikus frissítési feladat. A második lépésben az alkalmazás azt ellenőrzi, hogy mikor futott utoljára az Üresjárat vizsgálat. Ha még egyáltalán nem futott, már legalább 7 napja nem futott, esetleg a futása megszakadt, az alkalmazás megvizsgálja a rendszermemóriát, az indítási objektumokat és a rendszerleíró adatbázist.

Az Üresjárat vizsgálat a heurisztikus elemzés alapos szintjén fut, ami növeli a fenyegetések észlelésének valószínűségét.

Ha a felhasználó visszatér a munkájához, az Üresjárat vizsgálat működése automatikusan félbeszakad. Megjegyezzük, hogy az alkalmazás emlékszik arra az állapotra, ahol a működését félbeszakították, így ennél a pontnál folytatja majd a működését.

Ha az Üresjárat vizsgálat futása frissítőcsomag letöltése közben lett megszakítva, a letöltés legközelebb előlről kezdődik el.

➤ *Az Üresjárat vizsgálat letiltása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Válassza ki a **Vizsgálat** részt az ablak bal oldali részén, majd ott az **Általános beállítások** alpontot.
3. Az ablak jobb oldalán törölje az **Üresjárat vizsgálat végrehajtása** négyzet bejelölését.

**TELJES KÉPERNYŐS MÓD. JÁTÉK PROFIL**

Bizonyos teljes képernyős módban futó programok (különösen a számítógépes játékok) kevésbé kompatibilisek a Kaspersky Anti-Virus néhány funkciójával: a felugró értesítések megjelenítése például nem kívánatos ebben a módban. Ezek az alkalmazások elég gyakran jelentős rendszer-erőforrásokat igényelnek, és a Kaspersky Anti-Virus bizonyos feladatainak futtatása lelassíthatja a teljesítményüket.

Annak érdekében, hogy a teljes képernyős alkalmazások elindítása előtt ne kelljen minden alkalommal kézzel letiltani az értesítéseket és felfüggeszteni a feladatokat, a játék profil segítségével lehetőség van a beállítások ideiglenes szerkesztésére a Kaspersky Anti-Virus alkalmazásban. Amikor a Játék profil aktív, a teljes képernyős üzemmódra való váltáskor a termék összetevőinek beállításai automatikusan megváltoznak, hogy a rendszer működése ebben a módban optimális legyen. A teljes képernyős módból való kilépéskor a termék beállításai visszatérnek a teljes képernyős mód előtt használt értékekre.

➤ *A játék profil engedélyezése:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalán, a **Speciális beállítások** részben válassza ki a **Játék profil** alpontot.
3. Jelölje be a **Játék profil használata** négyzetet, és adja meg a játék profil szükséges beállításait az alatta levő **Profil beállításai** részben.

## A KASPERSKY ANTI-VIRUS ÖNVÉDELME

Mivel a Kaspersky Anti-Virus biztosítja a számítógép védelmét a rosszindulatú programok ellen, a számítógépbe behatoló kártevők megpróbálják blokkolni a Kaspersky Anti-Virus működését, akár az alkalmazás törlését is megkísérelhetik a számítógépről.

A számítógép biztonsági rendszerének stabil teljesítményét a Kaspersky Anti-Virus alkalmazásba beépített önvédelmi funkciók és távoli hozzáférés elleni védelem biztosítják.

A Kaspersky Anti-Virus önvédelme meggátolja az alkalmazás merevlemezen található fájljainak, a memóriában futó folyamatainak, és a rendszerleíró adatbázis bejegyzéseinek törlését vagy módosítását a számítógépen. A távoli hozzáférés elleni védelem blokkolja az alkalmazás szolgáltatásainak vezérlésére irányuló távoli próbálkozásokat.

A 64 bites operációs rendszert és a Microsoft Windows Vistát futtató számítógépeken a Kaspersky Anti-Virus önvédelme csak a helyi merevlemezeken található saját fájlok és a rendszerleíró adatbázis bejegyzések törlés és módosítás elleni védelmére terjed ki.

### EBBEN A RÉSZBEN:

Az önvédelem engedélyezése és letiltása.....	<a href="#">95</a>
Külső szolgáltatásvezérlés tiltása.....	<a href="#">95</a>

## AZ ÖNVÉDELME ENGEDÉLYEZÉSE ÉS LETILTÁSA

Alapértelmezésben a Kaspersky Anti-Virus önvédelme engedélyezett. Az önvédelmet szükség esetén letilthatja.

➔ *A Kaspersky Anti-Virus önvédelmének letiltása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. A megnyíló ablak bal oldalának **Speciális beállítások** részében válassza ki az **Önvédelem** alpontot.
3. Az ablak jobb oldalán szüntesse meg az **Önvédelem engedélyezése** négyzet jelölését.

## KÜLSŐ SZOLGÁLTATÁSVEZÉRLÉS TILTÁSA

A külső szolgáltatásvezérlés tiltása alapértelmezésben engedélyezett. A tiltást szükség esetén feloldhatja.

Távoli adminisztrációs alkalmazások (például RemoteAdmin) használatakor ezeket a programokat fel kell vennie a Megbízható alkalmazások listájára (lásd: „Megbízható zóna”, [90.](#) oldal), ha a külső szolgáltatásvezérlés engedélyezve van, és engedélyezze számukra a **Ne figyelje az alkalmazástevékenységet** opciót.

➔ *Külső szolgáltatásvezérlés tiltásának feloldása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. A megnyíló ablak bal oldalának **Speciális beállítások** részében válassza ki az **Önvédelem** alpontot.
3. A **Külső vezérlés** részben szüntesse meg a **Külső szolgáltatásvezérlés tiltása** négyzet jelölését.

## KARANTÉN ÉS MÁSOLATOK

*Karantén* különleges tárterület a vélhetően vírussal fertőzött és az észlelésük időpontjában nem vírusmentesíthető fájlok tárolására.

A potenciálisan fertőzött objektumot a víruskeresés vagy a Fájl víruskereső, Levél víruskereső és Proaktív védelem észlelheti és helyezheti karanténba.

A fájlok a következő esetekben kerülnek a karanténba:

- A fájl kódja egy ismert, de részlegesen módosult fenyegetésre hasonlít, vagy a rosszindulatú programokéhoz hasonló szerkezete van, de nem szerepel az adatbázisban. Ebben az esetben a fájl a Fájl víruskereső vagy a Levél víruskereső futtatása, vagy egy víruskeresés során végrehajtott heurisztikus elemzést követően a Karanténba kerül. A heurisztikus elemzés ritkán okoz hibás riasztásokat.
- Az objektum által végrehajtott műveletek sorozata gyanúsnak mutatkozik. Ebben az esetben a fájl a Karanténba kerül, de csak azután, hogy a Proaktív védelem összetevő elemezte a viselkedését.

A Karanténba került fájlok nem jelentenek fenyegetést. Ahogy múlik az idő, információk jelennek meg az új fenyegetésekről és azok semlegesítéséről, amik alapján a Kaspersky Anti-Virus vírusmentesítheti a Karanténba mentett fájlokat.

*Másolattároló* azon fájlok másolatainak tárolására szolgál, amelyek a vírusmentesítés során töröltek vagy módosultak.

## EBBEN A RÉSZBEN:

Fájlok tárolása a karanténban és a másolattárolóban .....	<a href="#">96</a>
Műveletek a karanténba helyezett fájlokkal .....	<a href="#">96</a>
Műveletek a Másolattárolóban található objektumokkal .....	<a href="#">97</a>
Karanténba helyezett fájlok vizsgálata frissítés után .....	<a href="#">98</a>

## FÁJLOK TÁROLÁSA A KARANTÉNBAN ÉS A MÁSOLATTÁROLÓBAN

Az objektumok maximális tárolási időtartama alapértelmezett esetben 30 nap. Ezután az objektumok törölve lesznek. Megszüntetheti a tárolás időtartamának korlátozását vagy módosíthatja az objektumok tárolásának maximális idejét.

Emellett megadhatja a Karantén és másolatok maximális méretét is. A maximális méret elérésekor a Karantén és másolatok tartalmát felülírják az új objektumok. Alapértelmezés szerint a maximális méret korlátozása le van tiltva.

### ➤ *Az objektumok maximális tárolási idejének módosítása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Speciális beállítások** részében válassza ki a **Jelentések és tárolók** alpontot.
3. Az ablak jobb oldali részében, a **Karanténba és másolattárolóba helyezett objektumok tárolása** részben jelölje be az **Objektumok tárolása – legfeljebb** négyzetet, és adja meg a karanténba helyezett objektumok maximális tárolási idejét.

### ➤ *A Karantén és a Másolatok maximális méretének beállítása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Speciális beállítások** részében válassza ki a **Jelentések és tárolók** alpontot.
3. Az ablak jobb oldali részében, a **Karanténba és másolattárolóba helyezett objektumok tárolása** részben jelölje be a **Maximális méret** négyzetet, és adja meg a Karantén és a Másolatok maximális méretét.

## MŰVELETEK A KARANTÉNBAN HELYEZETT FÁJLOKKAL

A Kaspersky Anti-Virus karanténja segítségével az alábbi műveletek végezhetők:

- gyanítottn fertőzött fájlok karanténba helyezése;
- a Karanténban lévő fájlok vizsgálata a Kaspersky Anti-Virus adatbázisainak aktuális verziójával;
- a fájlok visszaállítása az eredeti mappába, ahonnan a Karanténba kerültek;
- kiválasztott fájlok törlése a Karanténból;
- fájlok elküldése a Karanténból a Kaspersky Lab részére kutatási célokra.

A következő módszerekkel helyezhet át fájlokat a Karanténba:

- a **Karantén** ablakban található **Áthelyezés a Karanténba** gombra kattintva;
- a fájl helyi menüjének használatával.

- *Áthelyezés a Karanténba a Karantén ablakból:*
  1. Nyissa meg az alkalmazás főablakát.
  2. Az ablak alsó részén válassza ki a **Karantén** részt.
  3. A **Karantén** lapon kattintson az **Áthelyezés a Karanténba** gombra.
  4. A megnyíló ablakban válassza ki a karanténba helyezendő fájlt.
- *Fájl karanténba helyezése a helyi menü használatával:*
  1. Nyissa meg a Microsoft Windows Intézőt, és keresse meg a Karanténba helyezendő fájl mappáját.
  2. A helyi menü megnyitásához kattintson az egér jobb gombjával a fájlra, és válassza az **Áthelyezés a Karanténba** parancsot.
- *Karanténba helyezett fájl vizsgálata:*
  1. Nyissa meg az alkalmazás főablakát.
  2. Az ablak alsó részén válassza ki a **Karantén** részt.
  3. A **Karantén** lapon jelölje ki a vizsgálandó fájlt.
  4. Kattintson a **Vizsgálat** gombra.
- *Karanténba helyezett objektum visszaállítása:*
  1. Nyissa meg az alkalmazás főablakát.
  2. Az ablak alsó részén válassza ki a **Karantén** részt.
  3. A **Karantén** lapon jelölje ki a visszaállítandó fájlt.
  4. Kattintson a **Visszaállítás** gombra.
- *Karanténba helyezett objektum törlése:*
  1. Nyissa meg az alkalmazás főablakát.
  2. Az ablak alsó részén válassza ki a **Karantén** részt.
  3. A **Karantén** lapon jelölje ki a törlendő fájlt.
  4. A helyi menü megnyitásához kattintson jobb gombbal a fájlra, és válassza a **Törlés** elemet.
- *Karanténba helyezett objektumok elküldése a Kaspersky Lab részére elemzésre.*
  1. Nyissa meg az alkalmazás főablakát.
  2. Az ablak alsó részén válassza ki a **Karantén** részt.
  3. A **Karantén** lapon jelölje ki a kutatási célra elküldendő fájlt.
  4. A helyi menü megnyitásához kattintson az egér jobb gombjával a fájlra, és válassza a **Küldés elemzésre** parancsot.

## MŰVELETEK A MÁSOLOTTÁROLÓBAN TALÁLHATÓ OBJEKTUMOKKAL

A Kaspersky Anti-Virus másolattárolója segítségével az alábbi műveletek végezhetők:

- fájlok visszaállítása megadott vagy az eredeti mappába, ahonnan a fájl elkerült, amint azt a Kaspersky Anti-Virus feldolgozta;
  - a Másolattárolóban található kijelölt vagy összes fájl törlése.
- *Objektum visszaállítása a Másolattárolóból:*
    1. Nyissa meg az alkalmazás főablakát.
    2. Az ablak alsó részén válassza ki a **Karantén** részt.
    3. A **Tárolás** lapon jelölje ki a visszaállítandó fájlt.
    4. Kattintson a **Visszaállítás** gombra.

➤ *Fájl törlése a Másolattárolóból:*

1. Nyissa meg az alkalmazás főablakát.
2. Az ablak alsó részén válassza ki a **Karantén** részt.
3. A **Tárolás** lapon jelölje ki a törlendő fájlt.
4. A helyi menü megnyitásához kattintson jobb gombbal a fájlra, és válassza a **Törlés** elemet.

➤ *Az összes fájl törlése a Másolattárolóból:*

1. Nyissa meg az alkalmazás főablakát.
2. Az ablak alsó részén válassza ki a **Karantén** részt.
3. A **Tárolás** lapon kattintson a **Tárhely kiürítése** gombra.

## KARANTÉNBBA HELYEZETT FÁJLOK VIZSGÁLATA FRISSÍTÉS UTÁN

Ha az alkalmazás megvizsgált egy fájlt, és nem tudta pontosan megállapítani, hogy milyen rosszindulatú program fertőzte meg, a fájl a Karanténba kerül. Az adatbázisok frissítése után a Kaspersky Anti-Virus valószínűleg már képes lesz egyértelműen azonosítani, és megszüntetni a fenyegetést. Engedélyezheti a karanténba helyezett objektumok automatikus vizsgálatát minden frissítés után.

Javasoljuk, hogy rendszeresen nézze át a karanténba helyezett fájlokat. A vizsgálat hatására az állapotuk módosulhat. Néhány fájl visszakerülhet a korábbi helyére, velük tovább folytathatja a munkát.

➤ *A karanténba helyezett fájlok frissítés utáni vizsgálatának engedélyezése:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Frissítés** részében válassza ki a **Frissítések beállítása** összetevőt.
3. Jelölje be a **Karantén újbóli vizsgálata frissítés után** négyzetet a **További** részben.

## TOVÁBBI ESZKÖZÖK A SZÁMÍTÓGÉP JOBB VÉDELMEHEZ

A Kaspersky Anti-Virus részét képező következő varázslók és eszközök a számítógép biztonságával kapcsolatos speciális problémák megoldására szolgálnak:

- A Kaspersky Rescue Disk Létrehozási varázsló ISO lemezképet készít, és cserélhető adathordozóra írja a Kaspersky Rescue Disk tartalmát, amely lehetővé teszi a rendszer működőképességének visszaállítását egy vírustámadás után, ha az alkalmazást betölti a cserélhető adathordozóról. A Kaspersky Rescue Disk akkor használandó, ha a fertőzés olyan szintű, hogy lehetetlennek bizonyul a számítógép vírusmentesítése víruskereső alkalmazásokkal vagy rosszindulatú programot eltávolító eszközökkel.
- A Személyes adatok törlése varázsló a felhasználó tevékenységének nyomait keresi meg és törli a rendszerben, valamint az operációs rendszer olyan beállításait, amelyek lehetővé teszik a felhasználó tevékenységével kapcsolatos adatok gyűjtését.
- A Rendszer-visszaállítás varázsló a rosszindulatú programok nyomainak eltüntetésére és az általuk okozott rendszerkárosodás kijavítására szolgál.
- A Böngészőbeállítás varázsló elemzi és behangolja a Microsoft Internet Explorer beállításait, hogy megszüntesse a potenciális sebezhetőségeket.

A Varázslók (kivéve a Kaspersky Rescue Disk Létrehozási varázsló) által talált problémák csoportosítva kerülnek megjelenítésre, az általuk az operációs rendszerre jelentett fenyegetés típusának megfelelően. A Kaspersky Lab minden problémacsoportra olyan műveletkészletet kínál, melyek segítik megszüntetni a sebezhetőséget és a rendszerbeállításokban észlelt gyenge pontokat. Három problémacsoport, és ennek megfelelően három hozzájuk tartozó műveletcsoport különböztethető meg:

- *Az Erősen javasolt műveletek* a biztonságot súlyosan fenyegető problémák elhárításában nyújtanak segítséget. A fenyegetés megszüntetése érdekében javasolt az ebbe a csoportba tartozó összes művelet azonnali elvégzése.
- *A Javasolt műveletek* a potenciális fenyegetést jelentő problémák megszüntetésében nyújtanak segítséget. A védelem optimális szintjének biztosítása érdekében javasolt az ebbe a csoportba tartozó összes művelet elvégzése is.

- A *További műveletek* segítenek a rendszer olyan sérüléseinek a megszüntetésében, melyek aktuális veszélyt ugyan nem jelentenek, de a számítógép jövőbeni biztonsága érdekében célszerű beavatkozások. Ezen műveletek végrehajtása biztosítja a számítógép átfogó védelmét. Azonban egyes esetekben ezek a felhasználói beállítások (például a sütik) törléséhez vezethetnek.

## EBBEN A RÉSZBEN:

Személyes adatok törlése .....	<a href="#">99</a>
Böngészőbeállítás biztonságos munkához .....	<a href="#">100</a>
A varázslók által végzett módosítások visszagörgetése.....	<a href="#">101</a>

## SZEMÉLYES ADATOK TÖRLÉSE

A számítógép használata közben a rendszer rögzíti a felhasználó műveleteit. Az elmentett adatok között megtalálhatók a felhasználók által beírt keresési kulcsszavak és meglátogatott webhelyek, elindított programok, megnyitott és elmentett fájlok, a Microsoft Windows rendszer-eseménynapló, ideiglenes fájlok stb.

A felhasználók tevékenységére vonatkozó fenti információk bizalmas adatokat (például jelszavakat) tartalmazhatnak, és előfordulhat, hogy behatók számára is hozzáférhetők. A felhasználóknak gyakran nincsenek megfelelő ismereteik arról, hogy miként akadályozható meg az ezekből a forrásokból származó információk eltulajdonítása.

A Kaspersky Anti-Virus alkalmazásnak részét képezi a Személyes adatok törlése varázsló. Ez a varázsló megkeresi a rendszerben a felhasználói tevékenységre utaló nyomokat, valamint az operációs rendszer azon beállításait, amelyek a felhasználói tevékenység rögzítésében játszanak szerepet.

Ne feledje, hogy a felhasználó tevékenységével kapcsolatos adatokat a rendszer folyamatosan gyűjti. Rögzíti minden fájl elindítását és minden dokumentum megnyitását. A Microsoft Windows rendszernaplója sok, a rendszerben zajló eseményt feljegyez. A Személyes adatok törlése varázsló olyan tevékenységnyomokat is találhat, amelyek a varázsló előző futtatásakor nem törődtek. Előfordulhat, hogy egyes fájlok, például a Microsoft Windows naplófájlla, használatban vannak, amikor a varázsló megpróbálja törölni őket. E fájlok törlése érdekében a varázsló a rendszer újraindítását kéri. Az újraindítás során azonban ugyanezek a fájlok ismét létrejöhetnek, és a varázsló ismét tevékenységnyomként azonosíthatja őket.

A varázsló ablakok (lépések) sorozatából áll, amelyek között a **Vissza** és a **Tovább** gombokkal navigálhat. A használat befejezésekor a varázsló bezárására a **Befejezés** gomb szolgál. A varázslót bármelyik lépésnél leállíthatja a **Mégse** gombbal.

➤ *A felhasználó tevékenységnyomainak eltávolítása a rendszerből:*

1. Nyissa meg az alkalmazás főablakát.
2. Az ablak alsó részén válassza ki az **Eszközök** részt.
3. A megnyíló ablak **Személyes adatok törlése** részében kattintson az **Indítás** gombra.

Tekintsük át részletesebben a varázsló lépéseit.

### 1. lépés: A varázsló indítása

Ellenőrizze, hogy a **Felhasználói tevékenység nyomait kereső diagnosztika futtatása** négyzet be van jelölve, majd kattintson a **Tovább** gombra a varázsló elindításához.

### 2. lépés: Aktivitás nyomainak keresése

A varázsló rosszindulatú programok tevékenységének nyomait keresi a számítógépen. A keresés időt vesz igénybe. A keresés befejeztével a varázsló automatikusan folytatja a következő lépéssel.

### 3. lépés: A Személyes adatok törlése varázsló műveleteinek kiválasztása

A keresés befejeződése után a varázsló megjeleníti az észlelt aktivitásnyomokat és az eltávolításukra javasolt műveleteket.

A műveletek megtekintéséhez egy csoporton belül kattintson a + ikonra a csoport nevéől balra.

Ha azt szeretné, hogy a varázsló egy bizonyos műveletet hajtson végre, jelölje be a négyzetet az alkalmazás nevéől balra. Alapértelmezésben a varázsló minden javasolt és erősen javasolt műveletet végrehajt. Ha valamelyik műveletet nem kívánja végrehajtani, szüntesse meg a mellette levő négyzet bejelölését.

**Nyomatékosan javasoljuk, hogy ne szüntesse meg az alapértelmezetten bejelölt négyzetek jelölését, mert így a számítógép fenyegetéseknek lesz kitéve.**

Ha meghatározta az műveletek csoportját, amelyet a varázsló végre fog hajtani, kattintson a **Tovább** gombra.

#### 4. lépés: Személyes adatok törlése

A varázsló végrehajtja az előző lépésben kiválasztott műveletet. A tevékenységek nyomainak eltüntetése eltarthat egy ideig. Bizonyos nyomok eltüntetéséhez szükség lehet a számítógép újraindítására. A varázsló értesítést jelenít meg erről.

A tisztítás befejeztével a varázsló automatikusan folytatja a következő lépéssel.

#### 5. lépés: Varázsló befejezése

Ha szeretné minden alkalommal automatikusan eltüntetni a felhasználói tevékenység nyomait, amikor a Kaspersky Anti-Virus befejezi munkát, a varázsló utolsó képernyőjén jelölje be a **Mindig törölje az aktivitás nyomait a Kaspersky Anti-Virus bezárásakor** négyzetet. Ha a tevékenység nyomait manuálisan szeretné eltüntetni a varázsló használatával, ne jelölje be ezt a négyzetet.

Nyomja meg a **Befejezés** gombot a varázsló bezárásához.

## BÖNGÉSZŐBEÁLLÍTÁS BIZTONSÁGOS MUNKÁHOZ

A Microsoft Internet Explorer böngésző bizonyos esetekben speciális elemzést és beállítást igényel, mert a felhasználó által vagy alapértelmezésként beállított értékek biztonsági problémákat okozhatnak.

Néhány példa a böngésző által használt objektumokról és paramétereikről, valamint arról, hogyan jelenthetnek potenciális biztonsági problémát:

- **Microsoft Internet Explorer gyorsítótár.** A gyorsítótár az internetről letöltött adatokat tartalmazza, amelyeket így legközelebb nem kell letölteni. Ez lerövidíti a weboldalak letöltési idejét, és csökkenti az internetes forgalmat. Emellett a gyorsítótár személyes adatokat is tartalmaz és lekövethetővé teszi, hogy milyen webhelyeket látogatott a felhasználó. Egyes rosszindulatú objektumok a lemez vizsgálata során a gyorsítótárat is végigpásztázzák, és megszerezhetik például a felhasználó email címét. Javasoljuk, hogy a védelem javítása érdekében a böngésző bezárásakor mindig törölje a gyorsítótár tartalmát.
- **Az ismert fájltypusok kiterjesztésének megjelenítése.** A fájlnevek kényelmes szerkesztéséhez letilthatja a kiterjesztések megjelenítését. Ugyanakkor bizonyos esetekben hasznos, ha láthatók a fájlkiterjesztések. Számos rosszindulatú program fájlneve olyan szimbólumok kombinációját tartalmazza, amelyek egy további fájlkiterjesztésként jelennek meg a tényleges kiterjesztés előtt (pl.: example.txt.com). Ha a valódi fájlkiterjesztés nem jelenik meg, a felhasználók csak a fájlnev hamis kiterjesztést tartalmazó részét látják, így a rosszindulatú objektumot ártalmatlan fájlként azonosítják. A védelem javítása céljából javasolt engedélyezni az ismert formátumú fájlok kiterjesztéseinek megjelenítését.
- **Megbízható webhelyek listája.** A helyes működésük érdekében bizonyos webhelyeket hozzá kell adni a megbízható helyek listájához. Ugyanakkor a rosszindulatú objektumok behatolók által létrehozott webhelyek hivatkozásait adhatják hozzá a listához.

**A böngésző biztonságos futtatásra történő beállítása bizonyos webhelyek látogatásánál problémákat okozhat (például, ha azokon ActiveX elemek találhatók). A problémát megoldhatja, ha ezeket a webhelyeket a megbízható zónához adja.**

A böngésző elemzését és konfigurálását a Böngészőbeállítás varázsló végzi. A varázsló ellenőrzi, hogy telepítve vannak-e a böngésző legutóbbi frissítései és biztosítja, hogy a böngésző aktuális beállításai ne tegyék sebezhetővé a rendszert a rosszindulatú exploitokkal szemben. A varázsló befejezése után az elkészült jelentést el lehet küldeni a Kaspersky Lab részére elemzés céljából.

A varázsló ablakok (lépések) sorozatából áll, amelyek között a **Vissza** és a **Tovább** gombokkal navigálhat. A használat befejezésekor a varázsló bezárására a **Befejezés** gomb szolgál. A varázslót bármelyik lépésnél leállíthatja a **Mégse** gombbal.

Zárja be az összes Microsoft Internet Explorer ablakot az elemzés elindítása előtt.

➤ *Böngészőbeállítás biztonságos munkához:*

1. Nyissa meg az alkalmazás főablakát.
2. Az ablak alsó részén válassza ki az **Eszközök** részt.
3. A megnyíló ablak **Böngészőbeállítás** részében kattintson az **Indítás** gombra.

Tekintsük át részletesebben a varázsló lépéseit.

### 1. lépés: A varázsló indítása

Ellenőrizze, hogy a **Diagnosztika futtatása Microsoft Internet Explorerre** opció van kiválasztva, és kattintson a **Tovább** gombra a Varázsló elindításához.

### 2. lépés: Microsoft Internet Explorer beállításainak elemzése

A varázsló elemzi a Microsoft Internet Explorer beállításait. A böngésző beállításáiban szereplő problémák keresése időbe telhet. A keresés befejeztével a varázsló automatikusan folytatja a következő lépéssel.

### 3. lépés: Műveletek kiválasztása a böngésző beállításához

A keresés befejeződése után a varázsló megjeleníti az észlelt problémákat és az eltávolításukra javasolt műveleteket.

A műveletek megtekintéséhez egy csoporton belül kattintson a + ikonra a csoport nevéől balra.

Ha azt szeretné, hogy a varázsló egy bizonyos műveletet hajtson végre, jelölje be a négyzetet az alkalmazás nevéől balra. Alapértelmezésben a varázsló minden javasolt és erősen javasolt műveletet végrehajt. Ha valamelyik műveletet nem kívánja végrehajtani, szüntesse meg a mellette levő négyzet bejelölését.

**Nyomatékosan javasoljuk, hogy ne szüntesse meg az alapértelmezetten bejelölt négyzetek jelölését, mert így a számítógép fenyegetéseknek lesz kitéve.**

Ha meghatározta az műveletek csoportját, amelyet a varázsló végre fog hajtani, kattintson a **Tovább** gombra.

### 4. lépés: Böngészőbeállítás

A varázsló végrehajtja az előző lépésben kiválasztott műveletet. A böngésző beállítása eltarthat egy ideig. A konfigurálás befejezése után a varázsló automatikusan folytatja a következő lépéssel.

### 5. lépés: Varázsló befejezése

Nyomja meg a **Befejezés** gombot a varázsló bezárásához.

## A VARÁZSLÓK ÁLTAL VÉGZETT MÓDOSÍTÁSOK VISSZAGÖRGETÉSE

A Személyes adatok törlése varázsló (lásd: „Személyes adatok törlése”, [99.](#) oldal), Rendszer-visszaállítás varázsló (lásd: „Teendők vírus által fertőzöttnek vélt számítógéppel”, [45.](#) oldal), Böngészőbeállítás varázsló (lásd: „Böngészőbeállítás biztonságos munkához”, [100.](#) oldal) által végzett néhány módosítás visszagörgethető.

➤ *A varázslók által végzett módosítások visszagörgetése:*

1. Nyissa meg az alkalmazás főablakát, és válassza ki az **Eszközök** részt az ablak alsó részén.
2. Kattintson az ablak jobb oldalán található **Indítás** gombra annak a varázslónak a nevét tartalmazó részen, amelynek módosításait vissza kívánja görgetni:
  - **Személyes adatok törlése**– a Személyes adatok törlése varázsló által korábban végzett módosításokat görgeti vissza;
  - **Microsoft Windows hibaelhárítás**– a Microsoft Windows hibaelhárítás által korábban végzett módosításokat görgeti vissza;
  - **Böngészőbeállítás**– a Böngészőbeállítás varázsló által korábban végzett módosításokat görgeti vissza.

Tekintsük át közelebbről a varázslók lépéseit a módosítások visszagörgetése közben.

## 1. lépés: A varázsló indítása

Válassza a **Módosítások visszagörgetése** lehetőséget, majd kattintson a **Tovább** gombra.

## 2. lépés: Módosítások keresése

A Varázsló megkeresi a korábban végzett és visszagörgethető módosításokat. A keresés befejeztével a varázsló automatikusan folytatja a következő lépéssel.

## 3. lépés: Módosítások kiválasztása visszagörgetéshez

A keresés befejeztével a varázsló információt nyújt a fellelt módosításokról.

A varázsló visszagörgetni kívánt korábbi módosításai kijelölésére jelölje be a módosítás neve mellett balra található négyzetet.

Amikor végzett a visszagörgetni kívánt műveletek kiválasztásával, kattintson a **Tovább** gombra.

## 4. lépés: Módosítások visszagörgetése

A varázsló visszagörgeti az előző lépésben kijelölt műveleteket. A visszagörgetés befejeztével a varázsló automatikusan a következő lépéssel folytatja.

## 5. lépés: Varázsló befejezése

Nyomja meg a **Befejezés** gombot a varázsló bezárásához.

# JELENTÉSEK

A Kaspersky Anti-Virus védelmi összetevőinek tevékenysége és a víruskeresési feladatok jelentésekben kerülnek naplózásra.

### EBBEN A RÉSZBEN:

Jelentés létrehozása a kijelölt védelmi összetevőhöz .....	<a href="#">102</a>
Adatszűrés .....	<a href="#">103</a>
Események keresése .....	<a href="#">103</a>
Jelentés mentése fájlba.....	<a href="#">104</a>
Jelentések tárolása .....	<a href="#">104</a>
Az alkalmazás jelentéseinek törlése .....	<a href="#">104</a>
Nem kritikus események rögzítése a jelentésbe .....	<a href="#">105</a>
Jelentésértesítések konfigurálása .....	<a href="#">105</a>

## JELENTÉS LÉTREHOZÁSA A KIJELÖLT VÉDELMI ÖSSZETEVŐHÖZ

Részletes jelentést kaphat a Kaspersky Anti-Virus védelmi összetevőinek működése, illetve a feladatok végrehajtása közben bekövetkezett eseményekről.

A jelentések kényelmes kezeléséhez meghatározhatja az adatok megjelenítésének módját a képernyőn: különböző paraméterek szerint csoportosíthatja az eseményeket, kiválaszthatja a jelentés időtartamát, oszlopok vagy fontosság szerint sorba rendezheti a eseményeket és elrejtheti az egyes oszlopokat.

➔ *Adott védelmi összetevőről vagy feladatról szóló jelentés létrehozása:*

1. Nyissa meg az alkalmazás főablakát.
2. Kattintson az ablak felső részén található **Jelentések** hivatkozásra.
3. A megnyíló **Jelentések** ablakban kattintson a **Részletes jelentés** gombra.
4. A megnyíló **Részletes jelentés** ablakban válassza ki az összetevőt vagy a feladatot, amelyhez a jelentést létre szeretné hozni. A **Védelmi központ** elem kiválasztásakor minden védelmi összetevőről készül jelentés.

## ADATSZŰRÉS

A Kaspersky Anti-Virus jelentéseiben található eseményeket a jelentések oszlopaiban levő egy vagy több érték alapján szűrheti, de összetett szűrési feltételeket is meghatározhat.

### ➤ *Események szűrése érték alapján:*

1. Nyissa meg az alkalmazás főablakát.
2. Kattintson az ablak felső részén található **Jelentések** hivatkozásra.
3. A megnyíló **Jelentések** ablakban kattintson a **Részletes jelentés** gombra.
4. A megnyíló **Részletes jelentés** ablak jobb oldalán vigye az egérmutatót az oszlop fejlécének bal felső sarkába, majd kattintson a szűrési menü megnyitásához.
5. A szűrési menüben válassza ki az értéket, amely alapján az adatokat szűrni szeretné.
6. Ha szükséges, ismételje meg az eljárást egy másik oszlop esetében is.

### ➤ *Összetett szűrési feltétel megadása:*

1. Nyissa meg az alkalmazás főablakát.
2. A jelentések ablakának megnyitásához kattintson a **Jelentések** hivatkozásra az ablak felső részén.
3. A megnyíló ablak **Jelentés** lapján kattintson a **Részletes jelentés** gombra.
4. A megnyíló **Részletes jelentés** ablakban kattintson a jobb egérgombbal a jelentés megfelelő oszlopának fejlécére a helyi menü megjelenítéséhez, majd válassza az **Egyéni** lehetőséget.
5. A megnyíló **Egyéni szűrő** ablakban adja meg a kívánt szűrési feltételeket:
  - a. Határozza meg a lekérdezés határfeltételeit az ablak jobb oldalán.
  - b. Az ablak bal oldali részén a **Feltétel** legördülő listából válassza ki a szükséges határfeltételeket (pl. nagyobb vagy kisebb, egyenlő vagy nem egyenlő a lekérdezés határfeltételeinél megadott értékkel).
  - c. Szükség esetén a logikai konjunkció (logikai ÉS) vagy diszjunkció (logikai VAGY) műveletek segítségével második feltételt is meghatározhat. Ha azt szeretné, hogy a lekérdezett adatok mindkét megadott feltételt kielégítsék, válassza az **És** lehetőséget. Ha a kettő közül egy feltétel elegendő, akkor válassza a **Vagy** lehetőséget.

## ESEMÉNYEK KERESÉSE

A kereső sorban megadott kulcsszó vagy a speciális keresőablak segítségével megkeresheti a kívánt eseményeket a jelentésekben.

### ➤ *Esemény megtalálása a keresősor segítségével:*

1. Nyissa meg az alkalmazás főablakát.
2. Kattintson az ablak felső részén található **Jelentések** hivatkozásra.
3. A megnyíló **Jelentések** ablakban kattintson a **Részletes jelentés** gombra.
4. Adja meg a kulcsszót a megnyíló **Részletes jelentés** ablak jobb oldalán található keresősorban.

### ➤ *Esemény megtalálása a keresőablak segítségével:*

1. Nyissa meg az alkalmazás főablakát.
2. Kattintson az ablak felső részén található **Jelentések** hivatkozásra.
3. A megnyíló **Jelentések** ablakban kattintson a **Részletes jelentés** gombra.
4. A megnyíló **Részletes jelentés** ablakban kattintson a jobb egérgombbal a jelentés megfelelő oszlopának fejlécére a helyi menü megjelenítéséhez, majd válassza a **Keresés** lehetőséget.
5. A megnyíló **Keresés** ablakban adja meg a keresési feltételeket:
  - a. A **Karaktorsorozat** mezőbe írja be a kulcsszót, amely szerint keresni szeretne.
  - b. Az **Oszlop** legördülő listából válassza ki az oszlop nevét, amelyben a megadott kulcsszó alapján keresni szeretne.
  - c. Szükség esetén jelölje be a további keresési beállítások melletti négyzeteket.

6. Indítsa el a keresést a következő módszerek egyikével:
- Ha olyan eseményt keres, amely megfelel a megadott keresési feltételeknek, és a listán bejelölt esemény után következik, kattintson a **Következő keresése** gombra.
  - Ha az összes olyan eseményt keresi, amely megfelel a megadott keresési feltételeknek, kattintson az **Összes megjelölése** gombra.

## JELENTÉS MENTÉSE FÁJLBA

A jelentés szövegfájlba menthető.

### ▶ *Jelentés mentése fájlba:*

1. Nyissa meg az alkalmazás főablakát.
2. Kattintson az ablak felső részén található **Jelentések** hivatkozásra.
3. A megnyíló **Jelentések** ablakban kattintson a **Részletes jelentés** gombra.
4. A megnyíló **Részletes jelentés** ablakban hozza létre a kívánt jelentést, és kattintson a **Mentés** hivatkozásra a menteni kívánt fájl helyének kiválasztásához.
5. A megnyíló ablakban válassza ki azt a mappát, amelyikbe a jelentésfájlt menteni kívánja, és adja meg a fájl nevét.

## JELENTÉSEK TÁROLÁSA

A jelentések tárolásának időtartama alapértelmezésben 30 nap. Ezután a jelentés törölve lesz. Megszüntetheti a tárolás időtartamának korlátozását vagy módosíthatja a jelentések tárolásának maximális idejét.

Megadhatja továbbá a jelentésfájl maximális méretét is. Alapértelmezés szerint a maximális méret 1024 MB. A maximális méret elérésekor a fájl tartalmát felülírják az új rekordok. Törölheti a jelentés méretkorlátozását vagy megadhat más értéket is.

### ▶ *A jelentések maximális tárolási idejének módosítása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Speciális beállítások** részében válassza ki a **Jelentések és tárolók** alpontot.
3. A megnyíló ablak **Jelentések tárolása** részében jelölje be a **Jelentések tárolása legfeljebb** négyzetet, és adja meg a jelentések tárolásának maximális időtartamát.

### ▶ *A jelentés maximális fájl méretének beállítása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Speciális beállítások** részében válassza ki a **Jelentések és tárolók** alpontot.
3. Az ablak jobb oldalán, a **Jelentések tárolása** részben jelölje be a **Maximális fájl méret** négyzetet, és adja meg a jelentésfájl maximális méretét.

## AZ ALKALMAZÁS JELENTÉSEINEK TÖRLÉSE

Törölheti azokat a jelentéseket, amelyek olyan adatokat tartalmaznak, amelyekre már nincs szüksége.

### ▶ *Az alkalmazás jelentéseinek törlése:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Speciális beállítások** részében válassza ki a **Jelentések és tárolók** alpontot.
3. Az ablak jobb oldalán, a **Jelentések törlése** részben kattintson az **Adatok törlése** gombra.
4. A megnyíló **Jelentések törlése** ablakban jelölje be a törölni kívánt jelentéskategóriák négyzeteit.

## NEM KRITIKUS ESEMÉNYEK RÖGZÍTÉSE A JELENTÉSBE

Alapértelmezésben a termék nem rögzíti a naplóban a nem kritikus eseményeket, valamint a rendszerleíró adatbázis és a fájlrendszer eseményeit. Az ilyen eseményeket saját maga rögzítheti a jelentésben.


➤ *Nem kritikus események felvétele a jelentésbe:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Speciális beállítások** részében válassza ki a **Jelentések és tárolók** alpontot.
3. Az ablak jobb oldali részében jelölje be a **Nem kritikus események naplózása** négyzetet.

## JELENTÉSÉRTESÍTÉSEK KONFIGURÁLÁSA

Ütemezést hozhat létre, amely szerint a Kaspersky Anti-Virus tájékoztatja a jelentés készülségéről.

➤ *A jelentés elkészültéről tájékoztató értesítés konfigurálása:*

1. Nyissa meg az alkalmazás főablakát.
2. Kattintson az ablak felső részén található **Jelentések** hivatkozásra.
3. A megnyíló **Jelentések** ablakban kattintson a  gombra.
4. A megnyíló **Értesítések** ablakban adja meg az ütemezési beállításokat.

## AZ ALKALMAZÁS MEGJELENÉSE. AKTÍV KEZELŐFELÜLET-ELEMEK KEZELÉSE

A Kaspersky Anti-Virus segítségével módosíthatja a Microsoft Windows bejelentkezési képernyőjén megjelenő szöveg és az aktív interfész elemek (az értesítési területen megjelenő alkalmazás ikon, értesítési ablakok és felugró üzenetek) beállításait.

### EBBEN A RÉSZBEN:

Értesítési ablakok átlátszósága .....	<a href="#">105</a>
Az értesítési területen megjelenő alkalmazás ikon animációja .....	<a href="#">105</a>
Szöveg a Microsoft Windows bejelentkezési képernyőjén .....	<a href="#">106</a>

## ÉRTESÍTÉSI ABLAKOK ÁTLÁTSZÓSÁGA

➤ *Az értesítés ablakok átlátszóvá tétele:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldali részén, a **Speciális beállítások** részben válassza ki a **Megjelenés** alpontot.
3. Az **Ikon a tálca értesítési területén** részben jelölje be a **Félig átlátszó ablakok engedélyezése** négyzetet.

## AZ ÉRTESÍTÉSI TERÜLETEN MEGJELENŐ ALKALMAZÁS IKON ANIMÁCIÓJA

Frissítés vagy vizsgálat során az értesítési területen az alkalmazás ikon animáltan jelenik meg.

Alapértelmezésben az értesítési területen megjelenő alkalmazás ikon animációja engedélyezve van.

➤ *Az alkalmazás ikon animációjának letiltása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldali részén, a **Speciális beállítások** részben válassza ki a **Megjelenés** alpontot.
3. Az **Ikon a tálca értesítési területén** részben szüntesse meg a **Tálcaikon animálása feladatok végrehajtásakor** négyzet bejelölését.

## SZÖVEG A MICROSOFT WINDOWS BEJELENTKEZÉSI KÉPERNYŐJÉN

Alapértelmezésben, ha a Kaspersky Anti-Virus engedélyezve van, és védi a számítógépét, a „Kaspersky Lab védelem” felirat jelenik meg a bejelentkező képernyőn a Microsoft Windows betöltésekor.

A „Kaspersky Lab védelem” felirat csak a Microsoft Windows XP rendszerben jelenik meg.

➤ *A felirat megjelenítésének engedélyezése a Microsoft Windows betöltésekor:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldali részén, a **Speciális beállítások** részben válassza ki a **Megjelenés** alpontot.
3. Az **Ikon a tálca értesítési területén** részben szüntesse meg az **A „Kaspersky Lab védelem” felirat megjelenítése a Microsoft Windows bejelentkező képernyőjén** négyzet bejelölését.

## ÉRTEŚITÉSEK

A Kaspersky Anti-Virus alapértelmezett módon a működésében észlelt minden eseményről értesíti Önt. Ha további művelet szükséges, értesítési ablakok jelennek meg a képernyőn (lásd: „Értesítési ablakok és felugró üzenetek”, [30.](#) oldal). Az alkalmazás hangjelzéssel, email üzenetekkel és a tálca értesítési területén felugró üzenetekkel értesíti azon eseményekről, amelyek nem igénylik művelet kiválasztását (lásd: „Értesítési ablakok és felugró üzenetek”, [30.](#) oldal).

A Kaspersky Anti-Virus tartalmazza a Hírügynök (lásd [33.](#) oldal) funkciót, mellyel a Kaspersky Lab értesíti Önt a különböző hírek megjelenéséről. Ha nem szeretne híreket kapni, letilthatja a hírszolgáltatást.

### EBBEN A RÉSZBEN:

Értesítések engedélyezése és tiltása .....	<a href="#">106</a>
Az értesítés módjának konfigurálása .....	<a href="#">107</a>
Hírszolgáltatás letiltása .....	<a href="#">107</a>

## ÉRTEŚITÉSEK ENGEDÉLYEZÉSE ÉS TILTÁSA

A Kaspersky Anti-Virus alapértelmezésben számos módszert alkalmaz az Ön értesítésére az alkalmazás működésével kapcsolatos fontos eseményekről (lásd: „Az értesítés módjának konfigurálása”, [107.](#) oldal). Az értesítések letilthatók.

Függetlenül attól, hogy az értesítéseket engedélyezte vagy letiltotta, a Kaspersky Anti-Virus működésével kapcsolatos események egy működési jelentésben naplózásra kerülnek (lásd [102.](#) oldal).

Ha letiltja az értesítéseket, az nem érinti az értesítési ablakok megjelenítését. Ha minimalizálni szeretné a képernyőn megjelenő értesítések számát, alkalmazza az automatikus védelmi módot (lásd: „Védelmi mód kiválasztása”, [56.](#) oldal).

➤ *Az értesítések letiltásához tegye a következőket:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Speciális beállítások** részében válassza ki az **Értesítések** alpontot.
3. Az ablak jobb oldalán szüntesse meg az **Eseményértesítések engedélyezése** négyzet jelölését.

## AZ ÉRTEŚÍTÉS MÓDJÁNAK KONFIGURÁLÁSA

Az alkalmazás az eseményekről az alábbi módszerekkel értesíti Önt:

- felugró üzenet formájában a tálca értesítési területén;
- hangos értesítések;
- email üzenetek.

Az egyes eseménytípusokra egyedi értesítéseket is konfigurálhat.

A kritikus értesítésekkel és az alkalmazás működési hibáira vonatkozó értesítésekkel alapértelmezés szerint hangjelzés is együtt jár. A hangeffektusok forrásául a Microsoft Windows hangsémái szolgálnak. A beállított sémát módosíthatja, de le is tilthatja a hangjelzéseket.

Ha azt szeretné, hogy a Kaspersky Anti-Virus email értesítést küldjön, végezze el az email beállításokat az értesítés elküldéséhez.

### ► *Értesítési módszerek kiválasztása az egyes eseménytípusokhoz:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Speciális beállítások** részében válassza ki az **Értesítések** alpontot.
3. Az ablak jobb oldali részében jelölje be az **Eseményértesítések engedélyezése** négyzetet, majd kattintson a **Beállítások** gombra.
4. A megnyíló **Értesítések** ablakban jelölje be a négyzeteket aszerint, hogy milyen értesítést szeretne kapni az egyes eseményekről: emailben, felugró üzenetként vagy hangjelzéssel.

### ► *Az értesítések kézbesítésével kapcsolatos email beállítások módosításához végezze el az alábbiakat:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Speciális beállítások** részében válassza ki az **Értesítések** alpontot.
3. Az ablak jobb oldali részében jelölje be az **Email értesítések engedélyezése** négyzetet, majd kattintson a **Beállítások** gombra.
4. A megnyíló **E-mail értesítési beállítások** ablakban adja meg az értesítések emailben történő küldésének beállításait.

### ► *Értesítések hangsémájának a beállítása:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Speciális beállítások** részében válassza ki az **Értesítések** alpontot.
3. Az ablak jobb oldalán szüntesse meg a **Hangos értesítések engedélyezése** négyzet jelölését.

Ha a Microsoft Windows hangsémáját kívánja használni a Kaspersky Anti-Virus eseményeivel kapcsolatos értesítésekhez, kattintson **A Windows alapértelmezett hangsémájának használata** négyzetre. Ha a négyzet nincs bejelölve, a Kaspersky Anti-Virus korábbi verzióinak a hangsémáját használja az alkalmazás.

## HÍRSZOLGÁLTATÁS LETILTÁSA

### ► *Hírek letiltása az alkalmazás beállítási ablakából:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldali részén, a **Speciális beállítások** részben válassza ki a **Megjelenés** alpontot.
3. Az ablak jobb oldalán szüntesse meg a **Hírértesítések engedélyezése** négyzet jelölését.

## KASPERSKY SECURITY NETWORK

A számítógép védelme hatékonyságának növeléséhez a Kaspersky Anti-Virus a felhasználóktól a világ minden tájáról kapott adatokat használja. A Kaspersky Security Network feladata ezen adatok gyűjtése.

A Kaspersky Security Network (KSN) online szolgáltatások olyan infrastruktúrája, amely hozzáférést nyújt az Kaspersky Lab online tudásbázisához, ahonnan információkat szerezhet fájlok, webes erőforrások és szoftverek hírnevéről. A

Kaspersky Security Network adatait felhasználva a Kaspersky Anti-Virus válaszüzenete új típusú fenyegetésekkel találkozáskor rövidül, egyes védelmi összetevők teljesítménye nő, a vakriasztások kockázata pedig csökken.

A felhasználók részvétele a Kaspersky Security Networkben lehetővé teszi a Kaspersky Lab számára, hogy valós idejű információkat gyűjtsön össze az új fenyegetések típusairól és forrásairól, módszereket fejleszthessen a semlegesítésükre, és csökkentse a téves riasztások számát.

Emellett a Kaspersky Security Networkben való részvétellel hozzáférhetnek a különböző alkalmazások és webhelyek reputációjával kapcsolatos információkhoz is.

Ha csatlakozik a Kaspersky Security Networkhez, a Kaspersky Anti-Virus a számítógép védelme közben összegyűjtött statisztikákat automatikusan elküldi a Kaspersky Labnak.

Személyes adatok nem kerülnek összegyűjtésre, felhasználásra vagy tárolásra.

A Kaspersky Security Network szolgáltatásban a részvétel önkéntes. A részvételről a Kaspersky Anti-Virus telepítéskor dönthet, de a döntését később bármikor megváltoztathatja.

### EBBEN A RÉSZBEN:

A Kaspersky Security Networkben való részvétel engedélyezése és letiltása .....	<a href="#">108</a>
A Kaspersky Security Networkkel létrehozott kapcsolat ellenőrzése .....	<a href="#">108</a>

## A KASPERSKY SECURITY NETWORKBEN VALÓ RÉSZVÉTEL ENGEDÉLYEZÉSE ÉS LETILTÁSA

### ➤ *Csatlakozás a Kaspersky Security Networkhez:*

1. Nyissa meg az alkalmazás beállításait tartalmazó ablakot.
2. Az ablak bal oldalának **Speciális beállítások** részében válassza ki a **Visszajelzések** alpontot.
3. Az ablak jobb oldalán jelölje be a **Beleegyezek a részvételbe a Kaspersky Security Networkben** négyzetet.

## A KASPERSKY SECURITY NETWORKKEL LÉTREHOZOTT KAPCSOLAT ELLENŐRZÉSE

A Kaspersky Security Networkkel létrehozott kapcsolat a következő okok miatt szakadhat meg:

- a számítógépe nem csatlakozik az internethez;
- nem vesz részt a Kaspersky Security Networkben;
- a Kaspersky Anti-Virus licence korlátozott.

### ➤ *A Kaspersky Security Networkkel létrehozott kapcsolat ellenőrzése:*

1. Nyissa meg az alkalmazás főablakát.
2. Kattintson a **Cloud védelem** gombra az ablak felső részén.
3. A megnyíló ablak bal oldalán megjelenik a Kaspersky Security Network kapcsolat állapota.

# AZ ALKALMAZÁS MŰKÖDÉSÉNEK TESZTELÉSE

Ez a fejezet azt mutatja be, miként ellenőrizhető, hogy az alkalmazás észleli a vírusokat és változataikat, és a megfelelő műveleteket végzi rajtuk.

## EBBEN A RÉSZBEN:

Az EICAR teszt fájl.....	<a href="#">109</a>
Az alkalmazás működésének ellenőrzése az EICAR teszt fájllal .....	<a href="#">109</a>
Az EICAR teszt fájl típusai .....	<a href="#">110</a>

## AZ EICAR TESZTFÁJL

Az *EICAR teszt fájl* segítségével ellenőrizheti, hogy az alkalmazás észleli-e a vírusokat és vírusmentesíti-e a fertőzött fájlokat. Az EICAR teszt fájllt a European Institute for Computer Antivirus Research (EICAR, magyarul: Európai Számítógépes Vírusvédelmi Kutatóintézet) fejlesztette ki vírusvédelmi termékek tesztelésére.

Az EICAR teszt fájl nem vírus. Az EICAR teszt fájl nem tartalmaz olyan programkódot, amely károsíthatja a számítógépet. Ugyanakkor a legtöbb víruskereső alkalmazás az EICAR teszt fájllt vírusként azonosítja.

Az EICAR teszt fájl nem a heurisztikus elemző működésének ellenőrzésére, vagy rendszerszintű rosszindulatú programok (rootkitek) keresésére szolgál.

**Ne használjon valódi vírusokat a vírusvédelmi alkalmazás működésének tesztelésére! Ez károsíthatja a számítógépet.**

**Az EICAR teszt fájl használata után ne felejtse el visszaállítani a webes forgalom és fájlok vírusvédelmét.**

## A Z ALKALMAZÁS MŰKÖDÉSÉNEK ELLENŐRZÉSE AZ EICAR TESZTFÁJLLAL

Az EICAR teszt fájl segítségével tesztelheti az internetes forgalom biztonságát, a fájlok vírusvédelmét és a számítógép vizsgálatának hatékonyságát.

**Az EICAR teszt fájl használata után ne felejtse el visszaállítani a webes forgalom és fájlok vírusvédelmét.**

➤ *Az internetes forgalom biztonságának tesztelése az EICAR teszt fájllal:*

1. A teszt fájllt az EICAR hivatalos weboldaláról, a [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm) címről töltheti le.
2. Próbálja menteni az EICAR teszt fájllt a számítógép bármely mappájába.

A Kaspersky Anti-Virus tájékoztatja Önt, hogy fenyegetést észlelt a kért URL-címen, és blokkolja az objektum számítógépre mentését.

3. Szükség esetén az EICAR teszt fájl különböző változatait is használhatja (lásd: „Az EICAR teszt fájl típusai” , [110.](#) oldal).

➤ *A fájlok vírusvédelmének ellenőrzése EICAR tesztfájllal vagy annak módosított változatával:*

1. Függessze fel az internetes forgalom és a számítógépén lévő fájlok vírusvédelmét.  
Ha a védelem fel van függesztve, a számítógépben a rosszindulatú programok okozta kár megelőzése érdekében nem javasoljuk, hogy csatlakoztassa a számítógépet a helyi hálózatokra vagy cserélhető eszközöket használjon.
2. A tesztfájlt az EICAR hivatalos weboldaláról, a [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm) címről töltheti le.
3. Mentse az EICAR tesztfájlt a számítógép bármely mappájába.
4. Egészítse ki az egyik előtaggal az EICAR tesztfájl fejlécét (lásd: „Az EICAR tesztfájl típusai” , [110.](#) oldal).  
Ehhez használhatja bármilyen szöveg- vagy hipertextszerkesztőt, például a Notepad alkalmazást. A Notepad megnyitásához válassza ki a **Start** → **Programok** → **Kellékek** → **Notepad** menüpontot.
5. A kapott fájlt mentse az EICAR fájl módosítását jelző néven; ha például a DELE- előtagot adta hozzá, mentse a fájlt eicar\_dele.com néven.
6. Kapcsolja be az internetes forgalom és a számítógépén lévő fájlok vírusvédelmét.
7. Kísérlelje meg a mentett fájl futtatását.  
A Kaspersky Anti-Virus értesíti Önt a számítógép merevlemezén fellelt fenyegetésről, és elvégzi a fájlok vírusvédelmi beállításában megadott műveletet.

➤ *A víruskeresés ellenőrzése EICAR tesztfájllal vagy annak módosított változatával:*

1. Függessze fel az internetes forgalom és a számítógépén lévő fájlok vírusvédelmét.  
Ha a védelem fel van függesztve, a számítógépben a rosszindulatú programok okozta kár megelőzése érdekében nem javasoljuk, hogy csatlakoztassa a számítógépet a helyi hálózatokra vagy cserélhető eszközöket használjon.
2. A tesztfájlt az EICAR hivatalos weboldaláról, a [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm) címről töltheti le.
3. Egészítse ki az egyik előtaggal az EICAR tesztfájl fejlécét (lásd: „Az EICAR tesztfájl típusai” , [110.](#) oldal).  
Ehhez használhatja bármilyen szöveg- vagy hipertextszerkesztőt, például a Notepad alkalmazást. A Notepad megnyitásához válassza ki a **Start** → **Programok** → **Kellékek** → **Notepad** menüpontot.
4. A kapott fájlt mentse az EICAR tesztfájl módosítását jelző néven; ha például a DELE- előtagot adta hozzá, mentse a fájlt eicar\_dele.com néven.
5. Indítsa el a mentett fájl vizsgálatát.  
A Kaspersky Anti-Virus értesíti Önt a számítógép merevlemezén fellelt fenyegetésről, és elvégzi a víruskeresési beállításokban megadott műveletet.
6. Kapcsolja be az internetes forgalom és a számítógépén lévő fájlok vírusvédelmét.

## AZ EICAR TESZTFÁJL TÍPUSAI

Az alkalmazás működését az EICAR tesztfájl különböző változatainak létrehozásával ellenőrizheti. Az alkalmazás észleli a létrehozott EICAR tesztfájlt (vagy annak módosított változatát), és a vizsgálat eredményétől függően hozzárendel egy státuszt. Az alkalmazás végrehajtja a megadott műveleteket az EICAR tesztfájlon, ha kiválasztotta azokat az EICAR tesztfájl észlelő összetevő beállításainál.

A táblázat első oszlopában (lásd az alábbi táblázatot) láthatók az EICAR tesztfájl módosításához használható előtagok. A második oszlop tartalmazza az összes lehetséges állapotot, amelyet az alkalmazás a vizsgálat után a fájlhoz rendelhet. A harmadik oszlop azt a módot jelzi, ahogy az adott állapotú fájlt az alkalmazás kezeli.

2. táblázat. Az EICAR tesztfájl módosított változatai

Előtag	Fájl állapota	Fájl feldolgozásával kapcsolatos információk
Előtag nélküli, standard tesztvírus.	<b>Fertőzött.</b> A fájl egy ismert vírus kódját tartalmazza. A fájl nem vírusmentesíthető.	Az alkalmazás megállapította, hogy a fájl olyan vírust tartalmaz, amely nem vírusmentesíthető. A fertőzött fájlokhoz meghatározott művelet elvégzésre kerül a fájlra. Alapértelmezés szerint az alkalmazás megjelenít egy értesítést a képernyőn arról, hogy a fájlt nem lehet vírusmentesíteni.
CURE-	<b>Fertőzött.</b> A fájl egy ismert vírus kódját tartalmazza. A fájl vírusmentesíthető.	A fájl olyan vírust tartalmaz, amely vírusmentesíthető vagy törölhető. Az alkalmazás vírusmentesíti a fájlt; a „vírus” testét képező szöveget a CURE kifejezés váltja fel. Az alkalmazás megjelenít a képernyőn egy értesítést arról, hogy vírusmentesített fájlt észlelt.
DELE-	<b>Fertőzött.</b> A fájl egy ismert vírus kódját tartalmazza. A fájl nem vírusmentesíthető.	Az alkalmazás megállapította, hogy a fájl olyan vírust tartalmaz, amely nem vírusmentesíthető, és törli a fájlt. Az alkalmazás megjelenít a képernyőn egy értesítést arról, hogy a vírusmentesített fájlt törölte.
WARN-	<b>Potenciálisan fertőzött.</b> A fájl egy ismeretlen vírus kódját tartalmazza. A fájl nem vírusmentesíthető.	A fájl potenciálisan fertőzött. Az alkalmazás elvégzi a potenciálisan fertőzött fájlokhoz meghatározott műveletet a fájlra. Alapértelmezésben az alkalmazás megjelenít a képernyőn egy értesítést arról, hogy egy potenciálisan fertőzött fájlt észlelt.
SUSP-	<b>Potenciálisan fertőzött.</b> A fájl egy ismert vírus módosított kódját tartalmazza. A fájl nem vírusmentesíthető.	Az alkalmazás egy ismert vírus kódjának egy szakaszát tartalmazó részt talált a fájl kódjában. Egy potenciálisan fertőzött fájl észlelésekor az alkalmazás adatbázisai nem tartalmazzák a vírus teljes kódjának leírást. Az alkalmazás elvégzi a potenciálisan fertőzött fájlokhoz meghatározott műveletet a fájlra. Alapértelmezésben az alkalmazás megjelenít a képernyőn egy értesítést arról, hogy egy potenciálisan fertőzött fájlt észlelt.
CORR-	<b>Sérült.</b>	Az alkalmazás nem vizsgálja ezt a fájl típust, mert a szerkezete sérült (például a fájlformátum érvénytelen). A fájl feldolgozásával kapcsolatos információkat megtalálja az alkalmazás által végrehajtott műveletről készült jelentésben.
ERRO-	<b>Vizsgálathiba.</b>	Hiba történt a fájl vizsgálata közben. Az alkalmazás nem tudott hozzáférni a fájlhoz, mert a fájl integritása megsérült (például nincs meg a vége egy többkötetes archívumnak), vagy nincs hozzá kapcsolat (ha a fájl vizsgálata hálózati meghajtón zajlott). A fájl feldolgozásával kapcsolatos információkat megtalálja az alkalmazás által végrehajtott műveletről készült jelentésben.

# KAPCSOLATFELVÉTEL A TERMÉKTÁMOGATÁSI SZOLGÁLTATÁSSAL

Ebben a részben tudhatja meg, miként kérhet műszaki segítséget, és milyen feltételekkel kaphat segítséget a Terméktámogatási szolgáltatástól.

## EBBEN A RÉSZBEN:

Terméktámogatás igénylése .....	<a href="#">112</a>
A nyomkövető fájl és az AVZ parancsfájl segítségével .....	<a href="#">112</a>
Terméktámogatás telefonon.....	<a href="#">114</a>
Terméktámogatás igénylése a Saját Kaspersky fiókon keresztül.....	<a href="#">115</a>

## TERMÉKTÁMOGATÁS IGÉNYLÉSE

Ha nem talál megoldást a problémájára az alkalmazás dokumentációjában vagy az egyik alkalmazással kapcsolatos információforrásból (lásd: Az alkalmazással kapcsolatos információforrások", [11.](#) oldal), javasoljuk, hogy lépjen kapcsolatba a Kaspersky Lab Terméktámogatási szolgáltatásával. A terméktámogatási szolgáltatás szakemberei választ adnak minden, az alkalmazás telepítésére és használatára vonatkozó kérdésre. Ha a számítógép fertőzött, szakértőink segítenek a rosszindulatú programok által okozott problémák megoldásában.

Mielőtt felveszi a kapcsolatot a Terméktámogatási szolgáltatással, olvassa el terméktámogatási szabályokat (<http://support.kaspersky.com/support/rules>).

A Terméktámogatási szolgáltatással az alábbi módokon veheti fel a kapcsolatot:

- Telefonon. Ekkor konzultálhat az orosz nyelvű vagy nemzetközi Terméktámogatási szolgáltatás szakértőivel.
- Kérés küldésével a Kaspersky fiókból a Terméktámogatási szolgáltatás webhelyén. Ekkor egy űrlap kitöltésével léphet kapcsolatba szakértőinkkel.

A terméktámogatást csak a Kaspersky Anti-Virus kereskedelmi verziójának regisztrált felhasználójaként veheti igénybe. A Terméktámogatás nem érhető el az alkalmazás próbaverziójának használói számára.

## A NYOMKÖVETŐ FÁJL ÉS AZ AVZ PARANCSFÁJL SEGÍTSÉGÉVEL

Amikor értesíti a Terméktámogatási szolgáltatás szakembereit a tapasztalt problémáról, megkérhetik Önt, hogy hozzon létre egy jelentést, amely az operációs rendszer adatait tartalmazza, és küldje el a Terméktámogatási szolgáltatásnak. A Terméktámogatási szolgáltatás szakemberei azt is kérhetik, hogy hozzon létre egy *nyomkövető fájlt*. A nyomkövető fájl lehetővé teszi, hogy lépésről lépésre nyomon követhesse az alkalmazás parancsainak végrehajtását, és kiderítse, hogy az alkalmazás működésének melyik szakaszában történt a hiba.

Miután a Terméktámogatási szolgáltatás specialistái elemezték a beküldött adatokat, létrehoznak egy AVZ parancsfájlt, és elküldik Önnek. Az AVZ parancsfájl segítségével elemezheti a rosszindulatú kód aktív folyamatait, rosszindulatú kódot kereshet a rendszerben, vírusmentesítheti / törölheti a fertőzött fájlokat, és jelentéseket hozhat létre a rendszer átvizsgálásának eredményeiről.

## JELENTÉS KÉSZÍTÉSE A RENDSZER ÁLLAPOTÁRÓL

➤ *Jelentés készítése a rendszer állapotáról:*

1. Nyissa meg az alkalmazás főablakát.
2. Kattintson a **Támogatás** hivatkozásra a főablak alsó részén a **Támogatás** ablak megnyitásához, majd kövesse a **Támogatóeszközök** hivatkozást.
3. A megnyíló **Támogatóeszközök** ablakban kattintson a **Rendszerállapot-jelentés létrehozása** gombra.

A rendszerállapot jelentés HTML vagy XML formátumban készül, és a sysinfo.zip archívumba kerül mentésre. Ahogy az információk összegyűltek, megtekintheti a jelentést.

➤ *A jelentés megtekintéséhez:*

1. Nyissa meg az alkalmazás főablakát.
2. Kattintson a **Támogatás** hivatkozásra a főablak alsó részén a **Támogatás** ablak megnyitásához, majd kövesse a **Támogatóeszközök** hivatkozást.
3. A megnyíló **Támogatóeszközök** ablakban kattintson a **Megtekintés** gombra.
4. Nyissa meg a jelentésfájlokat tartalmazó sysinfo.zip archívumot.

## NYOMKÖVETÉSI FÁJL LÉTREHOZÁSA

➤ *Nyomkövetési fájl létrehozása:*

1. Nyissa meg az alkalmazás főablakát.
2. Kattintson a **Támogatás** hivatkozásra a főablak alsó részén a **Támogatás** ablak megnyitásához, majd kövesse a **Támogatóeszközök** hivatkozást.
3. A megnyíló **Támogatóeszközök** ablak **Nyomkövetések** részében található legördülő listájából válassza ki a nyomkövetési szintet.  
 Javasoljuk, hogy a nyomkövetés kívánt szintjét egyeztesse a terméktámogatási szolgáltatás egy szakemberével. Ha épp nem kaphat útmutatást a terméktámogatási szolgáltatás szakemberétől, állítsa be a szintet **500**-ra.
4. A nyomkövetési folyamat elindításához kattintson az **Engedélyezés** gombra.
5. Rekonstruálja a probléma fellépésekor fennálló helyzetet.
6. A nyomkövetési folyamat leállításához kattintson a **Letiltás** gombra.

Ezután feltöltheti a nyomkövetési eredményeket (lásd: „Adatfájlok küldése”, [113.](#) oldal) a Kaspersky Lab kiszolgálójára.

## ADATFÁJLOK KÜLDÉSE

Miután létrehozta a nyomkövető fájlokat és a rendszerállapot-jelentést, el kell azokat küldenie a Kaspersky Lab Terméktámogatási szolgáltatásának szakértőjéhez.

Az adatfájloknak a Terméktámogatási szolgáltatás kiszolgálójára való feltöltéséhez egy kérészámra van szüksége. Ez a szám a Saját Kaspersky fiókban érhető el a Terméktámogatási szolgáltatás webhelyén akkor, ha a kérése aktív.

➤ *Az adatfájlok feltöltése a Terméktámogatási szolgáltatás kiszolgálójára:*

1. Nyissa meg az alkalmazás főablakát.
2. Kattintson a **Támogatás** hivatkozásra a főablak alsó részén a **Támogatás** ablak megnyitásához, majd kövesse a **Támogatóeszközök** hivatkozást.
3. A megnyíló **Támogatóeszközök** ablak **Műveletek** részében kattintson az **Információk feltöltése a terméktámogatási szolgáltatás kiszolgálójára** gombra.  
 Megnyílik az **Információk feltöltése a terméktámogatási szolgáltatás kiszolgálójára** ablak.
4. Jelölje be a Terméktámogatási szolgáltatásnak elküldendő nyomkövető fájlok melletti négyzetet, majd kattintson a **Küldés** gombra.  
 Megnyílik a **Kérészám** ablak.

- Adja meg a kéréséhez a Terméktámogatási szolgáltatásnál megtalálható Saját Kaspersky fiókban hozzárendelt számot, majd kattintson az **OK** gombra.

A kiválasztott adatfájlokat a rendszer összecsomagolja, és elküldi a Terméktámogatási szolgáltatás kiszolgálójára.

Ha a Terméktámogatási szolgáltatás valamilyen okból nem elérhető, az adatfájlokat tárolhatja a saját számítógépén, és később is elküldheti a Saját Kaspersky fiókjából.

➔ *Adatfájlok mentése lemezre:*

- Nyissa meg az alkalmazás főablakát.
- Kattintson a **Támogatás** hivatkozásra a főablak alsó részén a **Támogatás** ablak megnyitásához, majd kövesse a **Támogatóeszközök** hivatkozást.
- A megnyíló **Támogatóeszközök** ablak **Műveletek** részében kattintson az **Információk feltöltése a terméktámogatási szolgáltatás kiszolgálójára** gombra.

Megnyílik az **Információk feltöltése a terméktámogatási szolgáltatás kiszolgálójára** ablak.

- Jelölje be a Terméktámogatási szolgáltatásnak elküldendő nyomkövető fájlok melletti négyzetet, majd kattintson a **Küldés** gombra.

Megnyílik a **Kérés szám** ablak.

- Kattintson a **Mégse** gombra, majd a megnyíló ablakban az **Igen** gombra kattintva erősítse meg a fájlok lemezre mentését.

Megnyílik az archívum mentése ablak.

- Adja meg az archívum nevét, és erősítse meg a mentést.

A létrehozott archívumot a Saját Kaspersky fiókjából elküldheti a Terméktámogatási szolgáltatásnak.

## AVZ PARANCSFÁJL VÉGREHAJTÁSA

A Kaspersky Lab szakemberei nem javasolják, hogy megváltoztassa a tőlük kapott AVZ parancsfájl szövegét. Ha a parancsfájl végrehajtásával kapcsolatban probléma merülne fel, forduljon a Terméktámogatási szolgáltatáshoz (lásd: „Terméktámogatás igénylése”, [112. oldal](#)).

➔ *Az AVZ parancsfájl futtatása:*

- Nyissa meg az alkalmazás főablakát.
- Kattintson a **Támogatás** hivatkozásra a főablak alsó részén a **Támogatás** ablak megnyitásához, majd kövesse a **Támogatóeszközök** hivatkozást.
- A megnyíló **Támogatóeszközök** ablakban kattintson az **AVZ parancsfájl végrehajtása** gombra.

A parancsfájl sikeres futtatása esetén a varázsló bezáródik. Ha hiba történik a parancsfájl futtatása közben, akkor a varázsló ezzel kapcsolatos hibaüzenetet jelenít meg.

## TERMÉKTÁMOGATÁS TELEFONON

Sürgős esetben hívja telefonon az orosz nyelvű vagy nemzetközi terméktámogatási szolgáltatást ([http://support.kaspersky.com/support/support\\_local](http://support.kaspersky.com/support/support_local)).

Mielőtt a Terméktámogatási szolgáltatás szakembereivel kapcsolatba lép, gyűjtse össze a számítógép és az arra telepített víruskereső alkalmazás adatait (<http://support.kaspersky.com/support/details>). Így szakembereink gyorsabban tudnak segíteni Önnek.

## TERMÉKTÁMOGATÁS IGÉNYLÉSE A SAJÁT KASPERSKY FIÓKON KERESZTÜL

A Saját Kaspersky fiók az Ön személyes területe (<https://my.kaspersky.com>) a Terméktámogatási szolgáltatás webhelyén.

Ha szeretne egy Saját Kaspersky fiókot, el kell végeznie a regisztrációs eljárást a regisztrációs oldalon (<https://my.kaspersky.com/registration>). Adja meg az email címét és egy jelszót a Saját Kaspersky fiókba való bejelentkezéshez.

A Saját Kaspersky fiókban az alábbi műveleteket végezheti el:

- kapcsolatba léphet a Terméktámogatási szolgáltatással és a Víruslaboratóriummal;
- email küldése nélkül léphet kapcsolatba a Terméktámogatási szolgáltatással;
- kövesse kérése státuszát valós időben;
- megtekintheti a Terméktámogatási szolgáltatáshoz intézett korábbi kéréseinek részletes történetét;
- másolatot kaphat a kulcsfájlról, ha elhagyta vagy törölte azt.

### Terméktámogatás emailben

Online kérést a Terméktámogatás Szolgáltatásnak orosz, angol, német, francia vagy spanyol nyelven küldhet.

Az online kérési űrlap mezőiben a következő adatokat kell megadnia:

- kérdés típusa;
- alkalmazás neve és verziószáma;
- kérdés leírása;
- felhasználói azonosító és jelszó;
- email cím.

A Terméktámogatási szolgáltatás egyik szakértője elküldi a választ a kérdésére a Saját Kaspersky fiókba, valamint az online kérdésben megadott email címre is.

### Online kérés a Víruslaboratóriumnak

Bizonyos kérdéseket a Víruslaboratóriumnak kell küldeni a Terméktámogatás szolgáltatás helyett.

A Víruslaboratóriumnak a következő típusú kéréseket küldheti el:

- *Ismeretlen rosszindulatú program* – azt gyanítja, hogy egy fájl vírusot tartalmaz, de a Kaspersky Anti-Virus nem azonosítja azt fertőzöttnek.  
A Víruslaboratórium szakértői elvégzik a küldött rosszindulatú kód elemzését. Ha egy addig ismeretlen vírust észlelnek, hozzáadják az adatbázishoz annak leírását, és az a víruskereső alkalmazások frissítésekor elérhetővé válik.
- *Téves riasztás* – a Kaspersky Anti-Virus vírusnak ismeri fel a fájlt, pedig Ön biztos benne, hogy a fájl nem fertőzött.
- *Egy rosszindulatú program leírására irányuló kérés* – leírást kaphat egy a Kaspersky Anti-Virus által észlelt vírusról a vírus nevének megadásával.

A Kaspersky Víruslaboratóriumnak címzett kéréseit a webes űrlapon (<http://support.kaspersky.com/virlab/helpdesk.html>) keresztül akkor is elküldheti, ha nincs Saját Kaspersky fiókja. Ezen az oldalon nem kell megadnia az alkalmazás aktiváló kódját.

# FÜGGELÉK

Ebben a részben a dokumentum szövegét kiegészítő információk találhatók.

## EBBEN A RÉSZBEN:

Az alkalmazás használata parancssorból .....	<a href="#">116</a>
Kaspersky Anti-Virus értesítések listája .....	<a href="#">125</a>

## AZ ALKALMAZÁS HASZNÁLATA PARANCSSORBÓL

A Kaspersky Anti-Virus program a parancssorból is használható. Ennek során az alábbi műveletek hajthatók végre:

- az alkalmazás aktiválása;
- az alkalmazás elindítása és leállítása;
- az alkalmazás összetevőinek elindítása és leállítása;
- a feladatok elindítása és leállítása;
- információk megjelenítése az összetevők és feladatok aktuális állapotáról és azok statisztikáiról;
- víruskeresési feladatok elindítása és leállítása;
- kiválasztott objektumok vizsgálata;
- adatbázisok és szoftvermodulok frissítése, frissítések visszagörgetése;
- biztonsági beállítások exportálása és importálása;
- súgó fájlok megnyitása a parancssori szintaxissal általánosan és egyedi parancsokhoz.

Parancssor szintaxisa:

```
avp.com <parancs> [options]
```

Az alkalmazás a parancssorból az alkalmazás telepítómappájából vagy az avp.com fájl teljes elérési útvonalának megadásával érhető el.

Az alkalmazás és összetevőinek a vezérlésére szolgáló parancsok listáját az alábbi táblázat tartalmazza.

<b>START</b>	Elindít egy összetevőt vagy egy feladatot.
<b>STOP</b>	Leállít egy összetevőt vagy egy feladatot. A parancsot csak akkor lehet végrehajtani, ha a Kaspersky Anti-Virus felhasználói felületén megadott jelszót beírja.
<b>STATUS</b>	Összetevő vagy feladat jelenlegi állapotának a megjelenítése a képernyőn.
<b>STATISTICS</b>	Összetevő vagy feladat statisztikájának a megjelenítése a képernyőn.
<b>HELP</b>	A parancsok listáját és azok szintaxis információit tartalmazza.
<b>SCAN</b>	Objektum vírusellenőrzése.
<b>UPDATE</b>	Elindítja az alkalmazás frissítését.
<b>ROLLBACK</b>	Visszagörgeti a Kaspersky Anti-Virus legutóbbi frissítését. A parancsot csak akkor lehet végrehajtani, ha a Kaspersky Anti-Virus felhasználói felületén megadott jelszót beírja.
<b>EXIT</b>	Bezárja az alkalmazást. A parancsot csak akkor lehet végrehajtani, ha a program felhasználói felületén megadott jelszót beírja.

<b>IMPORT</b>	Importálja az alkalmazás védelmi beállításait. A parancsot csak akkor lehet végrehajtani, ha a Kaspersky Anti-Virus felhasználói felületén megadott jelszót beírja.
<b>EXPORT</b>	Exportálja az alkalmazás védelmi beállításait.

Valamennyi parancshoz saját beállításkészlet tartozik.

### EBBEN A RÉSZBEN:

Alkalmazás aktiválása.....	<a href="#">117</a>
Alkalmazás elindítása.....	<a href="#">117</a>
Alkalmazás leállítása.....	<a href="#">117</a>
Alkalmazás-összetevők és feladatok kezelése .....	<a href="#">118</a>
Víruskeresés .....	<a href="#">119</a>
Az alkalmazás frissítése.....	<a href="#">121</a>
Legutolsó frissítés visszagörgetése .....	<a href="#">122</a>
Védelmi beállítások exportálása.....	<a href="#">122</a>
Védelmi beállítások importálása.....	<a href="#">122</a>
Nyomkövetési fájl létrehozása.....	<a href="#">123</a>
A Súly megtekintése .....	<a href="#">123</a>
A parancssori felület visszatérési kódjai.....	<a href="#">124</a>

## ALKALMAZÁS AKTIVÁLÁSA

A Kaspersky Anti-Virus alkalmazás kulcsfájl segítségével aktiválható.

Parancs szintaxisa:

```
avp.com ADDKEY <fájlnév>
```

Az alábbi táblázat a parancs lehetséges beállításait mutatja be.

<b>&lt;fájlnév&gt;</b>	Az alkalmazás-kulcsfájl neve *.key kiterjesztéssel.
------------------------	---

### **Például:**

```
avp.com ADDKEY 1AA111A1.key
```

## ALKALMAZÁS ELINDÍTÁSA

Parancs szintaxisa:

```
avp.com
```

## ALKALMAZÁS LEÁLLÍTÁSA

Parancs szintaxisa:

```
avp.com EXIT /password=<jelszó>
```

Az alábbi táblázat a paraméterek leírását tartalmazza.

<b>&lt;jelszó&gt;</b>	A felületen megadott alkalmazásjelszó.
-----------------------	--

Ne feledje, hogy ezt a parancsot nem hajthatja végre a jelszó megadása nélkül.

## ALKALMAZÁS-ÖSSZETEVŐK ÉS FELADATOK KEZELÉSE

Parancs szintaxisa:

```
avp.com <parancs> <profil|feladatnév> [/R[A]:<jelentésfájl>]
avp.com STOP <profil|feladatnév> /password=<jelszó> [/R[A]:<jelentésfájl>]
```

A parancsok és beállítások ismertetését az alábbi táblázat tartalmazza.

<b>&lt;parancs&gt;</b>	A Kaspersky Anti-Virus összetevőit és feladatait kezelheti a parancssorból az alábbi parancsokkal: START – védelmi összetevő vagy feladat elindítása. STOP – védelmi összetevő vagy feladat leállítása. STATUS – a védelmi összetevő vagy feladat aktuális állapotának megjelenítése. STATISTICS – védelmi összetevő vagy feladat működésével kapcsolatos statisztika megjelenítése a képernyőn. Ne feledje, hogy a STOP parancsot nem hajthatja végre a jelszó megadása nélkül.
<b>&lt;profil feladatnév&gt;</b>	A Kaspersky Anti-Virus bármilyen védelmi összetevőjét, összetevő modulját, igény szerinti vizsgálati vagy frissítési feladatát megadhatja a <b>&lt;profil&gt;</b> paraméter értékeként (a programban használt standard értékek az alábbi táblázatban láthatók). A <b>&lt;feladatnév&gt;</b> paraméter értéke bármely igény szerint vizsgálati vagy frissítési feladat neve lehet.
<b>&lt;jelszó&gt;</b>	A felületen megadott alkalmazásjelszó.
<b>/R[A]:&lt;jelentésfájl&gt;</b>	<b>/R:&lt;jelentésfájl&gt;</b> – csak a fontos események naplózása a jelentésben. <b>/RA:&lt;jelentésfájl&gt;</b> – az összes esemény naplózása a jelentésben. Megadhat abszolút vagy relatív elérési utat is a fájlhoz. Ha a beállítás nincs megadva, akkor a vizsgálat eredményei jelennek meg a képernyőn, és az összes esemény látható.

A **<profil>** beállításban meg kell adnia az alábbi táblázat valamelyik értékét.

<b>RTP</b>	Összes védelmi összetevő. Az <b>avp.com START RTP</b> parancs valamennyi védelmi összetevőt elindítja, ha a védelem teljesen ki van kapcsolva. Ha az összetevőt a parancssori <b>STOP</b> paranccsal kikapcsolták, az <b>avp.com START RTP</b> parancs nem fogja elindítani. Ennek elindításához az <b>avp.com START &lt;profil&gt;</b> parancsot kell használni, a megadott védelmi összetevő nevét a <b>&lt;profil&gt;</b> paraméterben megadva, például, <b>avp.com START FM</b> .
<b>pdm</b>	Proaktív védelem.
<b>FM</b>	Fájl víruskereső.
<b>EM</b>	Levél víruskereső.
<b>WM</b>	Webes víruskereső. A Webes víruskereső alösszetevőinek értékei: <b>httpscan (HTTP)</b> – a HTTP-forgalom vizsgálata; <b>sc</b> – parancsfájlok vizsgálata.
<b>IM</b>	IM víruskereső.
<b>Frissítő</b>	Frissítés.
<b>Visszagörgetés</b>	Legutolsó frissítés visszagörgetése.
<b>Scan_My_Computer</b>	Vizsgálat.

<b>Scan_Objects</b>	Objektumok vizsgálata.
<b>Scan_Quarantine</b>	Karantén vizsgálata.
<b>Scan_Startup (STARTUP)</b>	Objektumok vizsgálatának indítása.
<b>Scan_Vulnerabilities (SECURITY)</b>	Sebezhetőségi vizsgálat.

A parancssorban elindított összetevők és feladatok a felhasználói felületen megadott beállításokkal fognak futni.

#### **Példák:**

➤ *A Fájlvíruskereső engedélyezéséhez gépelje be az alábbi utasítást:*

```
avp.com START FM
```

➤ *A számítógép vizsgálatának a leállításához gépelje be az alábbi utasítást:*

```
avp.com STOP Scan_My_Computer /password=<jelszó>
```

## VÍRUSKERESÉS

Az adott területen történő víruskeresés és rosszindulatú objektum feldolgozás parancssorból történő elindítása általában így néz ki:

```
avp.com SCAN [<vizsgálandó objektum>] [<művelet>] [<fájltípusok>] [<kizárások>]
[<konfigurációs fájl>] [<jelentés beállítások>] [<speciális beállítások>]
```

Objektumok vizsgálatához az alkalmazásban létrehozott feladatok is használhatók, ha a parancssorból elindítja a szükségeset. A feladat a Kaspersky Anti-Virus interfészen megadott beállításokkal elindul.

Az alábbi táblázat a paraméterek leírását tartalmazza.

<b>&lt;vizsgálandó objektum&gt;</b> – ez a paraméter adja meg azon objektumok listáját, amelyekben a program rosszindulatú kódot keres.	
A paraméterben a mellékelt listából különféle értékek is megadhatók szóközzel elválasztva.	
<b>&lt;fájlok&gt;</b>	Vizsgálandó fájlok és mappák elérési útvonala. Megadhat abszolút vagy relatív elérési utat is a fájlhoz. A lista elemeit szóköz választja el. Megjegyzések: <ul style="list-style-type: none"> <li>• ha az objektum neve szóközt tartalmaz, akkor idézőjelek közé kell tenni;</li> <li>• ha a referencia adott mappára mutat, a mappában található összes fájl vizsgálatra kerül.</li> </ul>
<b>/MEMORY</b>	RAM objektumok.
<b>/STARTUP</b>	Indítási objektumok.
<b>/MAIL</b>	Levelező fiókok.
<b>/REMDRIVES</b>	Összes cserélhető meghajtó.
<b>/FIXDRIVES</b>	Összes belső meghajtó.
<b>/NETDRIVES</b>	Összes hálózati meghajtó.
<b>/QUARANTINE</b>	Karanténba helyezett objektumok.

/ALL	Teljes számítógép-vizsgálat.
/@:<filelist.lst>	<p>A vizsgálandó objektumok és könyvtárak listáját tartalmazó fájl elérési útvonala. Megadhat abszolút vagy relatív elérési utat is a listát tartalmazó fájlhoz. Az elérési utat akkor is idézőjelek nélkül kell megadni, ha az szóközt tartalmaz.</p> <p>Az objektumok listáját tartalmazó fájlnak szöveges formátumúnak kell lennie. Minden vizsgált objektumnak külön sorban kell szerepelnie.</p> <p>Javasolt a vizsgálandó objektumok abszolút elérési útját megadni. Relatív útvonal megadásakor az útvonalat az alkalmazás futtatható fájljához viszonyítva kell megadni, nem pedig a vizsgálandó objektumok listáját tartalmazó fájlhoz képest.</p>
<p><b>&lt;művelet&gt;</b> – ez a paraméter határozza meg, hogy milyen művelet történjen, ha a rendszer a vizsgálat során rosszindulatú objektumot talál. Ha nem adja meg ezt a paramétert, az alapértelmezett művelet az lesz, amelynek az értéke /i8.</p> <p>Ha automatikus mód üzemmódban dolgozik, veszélyes objektum észlelésekor a Kaspersky Anti-Virus automatikusan a Kaspersky Lab szakemberei által ajánlott műveletet fogja végrehajtani. A program mellőzi a <b>&lt;művelet&gt;</b> paraméter értékének megfelelő műveletet.</p>	
/i0	Az objektumon ne történjen semmilyen művelet; készüljön róla bejegyzés a jelentésben.
/i1	Fertőzött objektumok vírusmentesítése; kihagyás, ha a vírusmentesítés nem sikerül.
/i2	Fertőzött objektumok vírusmentesítése; kihagyás, ha a vírusmentesítés nem sikerül; nem törli a fertőzött objektumokat az összetett objektumokból; végrehajtható fejlécű (sfx archívumok) összetett objektumok törlése.
/i3	Fertőzött objektumok vírusmentesítése; kihagyás, ha a vírusmentesítés nem sikerül; összes összetett objektum teljes törlése, ha a fertőzött rész külön nem törölhető.
/i4	Fertőzött objektumok törlése. Összes összetett objektum teljes törlése, ha a fertőzött rész külön nem törölhető.
/i8	Fertőzött objektum észlelésekor a felhasználó megkérdezése a tevékenységről.
/i9	A vizsgálat befejeztével felhasználó megkérdezése a tevékenységről.
<p><b>&lt;fajltípusok&gt;</b> – ez a paraméter határozza meg a víruskeresés tárgyát képező fájl típusokat. Alapértelmezésben ez a paraméter nincs definiálva, a fertőzhető fájlok csak a tartalmuk alapján kerülnek vizsgálatra.</p>	
/fe	Fájlok vizsgálata csak kiterjesztés alapján.
/fi	Fájlok vizsgálata csak tartalom alapján.
/fa	Összes fájl vizsgálata.
<p><b>&lt;kizárások&gt;</b> – ez a paraméter definiálja a keresésből kizárandó objektumokat. A paraméterben a mellékelt listából különféle értékek is megadhatók szóközzel elválasztva.</p>	
-e:a	Az archívumokat nem vizsgálja.
-e:b	Az email adatbázisokat nem vizsgálja.
-e:m	Az egyszerű szöveges emaileket nem vizsgálja.
-e:<fájlmaszk>	A maszkhoz illő fájlokat nem vizsgálja.
-e:<másodperc>	Olyan objektumok kihagyása, amelyeknek a vizsgálata hosszabb ideig tart a <b>&lt;másodperc&gt;</b> paraméternél.
-es:<méret>	<p>Olyan objektumok kihagyása, amelyek mérete (MB-ban) meghaladja a <b>&lt;méret&gt;</b> beállításban megadott értéket.</p> <p>Ez a beállítás csak az összetett fájlokhoz (például archívumokhoz) érhető el.</p>

<b>&lt;konfigurációs fájl&gt;</b> – az alkalmazás víruskeresési beállításait tartalmazó konfigurációs fájl elérési útvonala. A konfigurációs fájl szöveg formátumú, és a víruskeresés parancssori paramétereit tartalmazza. Megadhat abszolút vagy relatív elérési utat is a fájlhoz. Ha ezt a paramétert nem adja meg, az alkalmazás interfészén megadott értékek kerülnek alkalmazásra.	
<b>/C:&lt;fájlnév&gt;</b>	A <b>&lt;fájlnév&gt;</b> konfigurációs fájlban megadott beállítási paraméterek használata.
<b>&lt;jelentés beállítások&gt;</b> – ez a paraméter határozza meg a vizsgálati eredmény jelentésének formátumát. Megadhat abszolút vagy relatív elérési utat is a fájlhoz. Ha a beállítás nincs megadva, akkor a vizsgálat eredményei jelennek meg a képernyőn, és az összes esemény látható.	
<b>/R:&lt;jelentésfájl&gt;</b>	A fontos eseményeket csak ebbe a fájlba naplózza.
<b>/RA:&lt;jelentésfájl&gt;</b>	A fájlba minden esemény bekerül.
<b>&lt;speciális beállítások&gt;</b> – a vizsgálati technológiák használatát definiáló beállítások.	
<b>/iChecker=&lt;be ki&gt;</b>	Az iChecker technológia engedélyezése ill. letiltása.
<b>/iSwift=&lt;be ki&gt;</b>	Az iSwift technológia engedélyezése ill. letiltása.

**Példák:**

- *A memória, az indító programok, a postafiókok, a My Documents és a Program Files mappa, valamint a test.exe fájl vizsgálatának a megkezdése:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files" "C:\Downloads\test.exe"
```

- *Az object2scan.txt fájlban felsorolt objektumok vizsgálata a scan\_setting.txt konfigurációs fájl alkalmazásával a feladatra. A scan\_setting.txt konfigurációs fájl használata. Amikor a vizsgálat befejeződött, az összes eseményt naplózó jelentés készítése:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

Konfigurációs mintafájl:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

## AZ ALKALMAZÁS FRISSÍTÉSE

A Kaspersky Anti-Virus modulok és az alkalmazás adatbázisainak parancssori frissítési szintaxisa a következő:

```
avp.com UPDATE [<frissítési_forrás>] [/R[A]:<jelentésfájl>] [/C:<fájlnév>]
```

Az alábbi táblázat a paraméterek leírását tartalmazza.

<b>&lt;frissítési_forrás&gt;</b>	A frissítések letöltéséhez a hálózati mappa HTTP- vagy FTP-kiszolgálója. A paraméter értékéül a frissítési forrás teljes elérési útvonalát vagy URL-jét kell megadni. Ha nem választ ki elérési utat, a frissítési forrást a rendszer az alkalmazás frissítési beállításából veszi.
<b>/R[A]:&lt;jelentésfájl&gt;</b>	<b>/R:&lt;jelentésfájl&gt;</b> – csak a fontos események naplózása a jelentésben. <b>/RA:&lt;jelentésfájl&gt;</b> – az összes esemény naplózása a jelentésben. Megadhat abszolút vagy relatív elérési utat is a fájlhoz. Ha a beállítás nincs megadva, akkor a vizsgálat eredményei jelennek meg a képernyőn, és az összes esemény látható.
<b>/C:&lt;fájlnév&gt;</b>	A Kaspersky Anti-Virus frissítési beállításait tartalmazó konfigurációs fájl elérési útvonala. A konfigurációs fájl egy egyszerű szöveg formátumú fájl, amely az alkalmazás frissítéséhez szükséges parancssori paraméterek listáját tartalmazza. Megadhat abszolút vagy relatív elérési utat is a fájlhoz. Ha ezt a paramétert nem adja meg, az alkalmazás interfészén megadott értékek kerülnek alkalmazásra.

**Példák:**

- *Az alkalmazás adatbázisainak frissítése, és minden esemény jelentésbe rögzítése:*

```
avp.com UPDATE /RA:avbases_upd.txt
```

➔ A Kaspersky Anti-Virus modulok frissítése az updateapp.ini konfigurációs fájl beállításai alapján:

```
avp.com UPDATE /C:updateapp.ini
```

Konfigurációs mintafájl:

```
"ftp://my_server/kav_updates" /RA:avbases_upd.txt
```

## LEGUTOLSÓ FRISSÍTÉS VISSZAGÖRGETÉSE

Parancs szintaxisa:

```
avp.com ROLLBACK [/R[A]:<jelentésfájl>] [/password=<jelszó>]
```

Az alábbi táblázat a paraméterek leírását tartalmazza.

<b>/R[A]:&lt;jelentésfájl&gt;</b>	<b>/R:&lt;jelentésfájl&gt;</b> – csak a fontos események naplózása a jelentésben. <b>/RA:&lt;jelentésfájl&gt;</b> – az összes esemény naplózása a jelentésben. Megadhat abszolút vagy relatív elérési utat is a fájlhoz. Ha a beállítás nincs megadva, akkor a vizsgálat eredményei jelennek meg a képernyőn, és az összes esemény látható.
<b>&lt;jelszó&gt;</b>	A felületen megadott alkalmazásjelszó.

Ne feledje, hogy ezt a parancsot nem hajthatja végre a jelszó megadása nélkül.

### Például:

```
avp.com ROLLBACK /RA:rollback.txt /password=<jelszó>
```

## VÉDELMI BEÁLLÍTÁSOK EXPORTÁLÁSA

Parancs szintaxisa:

```
avp.com EXPORT <profil> <fájlnév>
```

Az alábbi táblázat a parancs lehetséges beállításait mutatja be.

<b>&lt;profil&gt;</b>	Összetevő vagy feladat, amelyhez a beállításokat exportálja. A <b>&lt;profil&gt;</b> paraméternél az „Alkalmazás-összetevők és feladatok kezelése” Súgó részben felsorolt bármely értéket használhatja.
<b>&lt;fájlnév&gt;</b>	A Kaspersky Anti-Virus beállításainak exportálásához használni kívánt fájl elérési útvonala. Abszolút vagy relatív elérési útvonal is megadható. Ha nincs másik formátum megadva, vagy egyáltalán nincs semmilyen formátum megadva, a konfigurációs fájl bináris formátumban lesz elmentve (DAT), és segítségével az alkalmazásbeállítások később más számítógépekre importálhatók. A konfigurációs fájl szövegfájlként is menthető. Ehhez adja meg a .txt kiterjesztést a fájlnevben. Megjegyzés: a védelmi beállítások szövegfájlból nem importálhatók. A fájl csak a Kaspersky Anti-Virus működéséhez szükséges fő beállítások megadására használható.

### Például:

```
avp.com EXPORT RTP c:\settings.dat
```

## VÉDELMI BEÁLLÍTÁSOK IMPORTÁLÁSA

Parancs szintaxisa:

```
avp.com IMPORT <fájlnév>[/password=<jelszó>]
```

Az alábbi táblázat a parancs lehetséges beállításait mutatja be.

<b>&lt;fájlnév&gt;</b>	A Kaspersky Anti-Virus beállításainak importálásához használt forrásfájl elérési útvonala. Abszolút vagy relatív elérési útvonal is megadható.
<b>&lt;jelszó&gt;</b>	A Kaspersky Anti-Virus felhasználói felületén megadott jelszó. A biztonsági paraméterek csak bináris fájlból importálhatók.

Ne feledje, hogy ezt a parancsot nem hajthatja végre a jelszó megadása nélkül.

**Például:**

```
avp.com IMPORT c:\settings.dat /password=<jelszó>
```

## NYOMKÖVETÉSI FÁJL LÉTREHOZÁSA

Nyomkövetési fájl létrehozására akkor lehet szükség, ha problémák lépnek fel a Kaspersky Anti-Virus működésében. A fájl a probléma pontosabb diagnosztizálásában segít a Terméktámogatási szolgáltatás szakembereinek.

Nyomkövető fájl létrehozása csak egy adott probléma elhárításához ajánlott. A nyomkövetés gyakori bekapcsolása lelassíthatja a számítógépet, és felemésztheti a merevlemez tárhelykapacitását.

Parancs szintaxisa:

```
avp.com TRACE [file] [on|off] [<nyomkövetési_szint>]
```

Az alábbi táblázat a paraméterek leírását tartalmazza.

[on off]	Nyomkövetési fájl létrehozásának engedélyezése / letiltása
[file]	Nyomkövetés kimenete fájlba.
<nyomkövetési_szint>	A beállítás bármely egész szám lehet 0 (minimális szint, csak kritikus hibák) és 700 (maximális szint, összes üzenet) között. Ha a Terméktámogatási szolgálathoz fordul, megadják Önnek, hogy milyen nyomkövetési szintet kell beállítania. Ha nem adják meg a szintet, az ajánlott érték: 500.

**Példák:**

➔ *Nyomkövetési fájl létrehozásának letiltása:*

```
avp.com TRACE file off
```

➔ *Nyomkövetési fájl létrehozása a Terméktámogatásnak való elküldésre legfeljebb 500-as nyomkövetési szint mellett:*

```
avp.com TRACE file on 500
```

## A SÚGÓ MEGTEKINTÉSE

Az alábbi paranccsal jelenítheti meg a parancssor szintaxisának sűgóját:

```
avp.com [ /? | HELP ]
```

Adott parancs szintaxisának sűgóját az alábbi parancsokkal jelenítheti meg:

```
avp.com <parancs> /?
```

```
avp.com HELP <parancs>
```

## A PARANCSSORI FELÜLET VISSZATÉRÉSI KÓDJAI

Ez a rész a parancssori felület visszatérési kódjait tartalmazza (lásd alább a táblázatot). Az általános kódokat a parancssorból kiadott bármely parancs kiválthatja. A visszatérési kódok között vannak általános kódok és egy adott feladatra jellemző kódok is.

<b>ÁLTALÁNOS VISSZATÉRÉSI KÓDOK</b>	
<b>0</b>	A művelet sikeresen befejeződött.
<b>1</b>	Érvénytelen beállítási érték.
<b>2</b>	Ismeretlen hiba.
<b>3</b>	Hiba a művelet végrehajtása során.
<b>4</b>	Művelet törölve.
<b>VÍRUSKERESÉSI FELADAT VISSZATÉRÉSI KÓDJAI</b>	
<b>101</b>	Minden veszélyes objektum feldolgozva.
<b>102</b>	A program veszélyes objektumokat észlelt.

# KASPERSKY ANTI-VIRUS ÉRTEŚÍTÉSEK LISTÁJA

Ez a fejezet azokat az információkat ismerteti, amiket a Kaspersky Anti-Virus megjeleníthet a képernyőn.

## EBBEN A RÉSZBEN:

Értesítések minden védelmi üzemmódban.....	<a href="#">125</a>
Értesítések interaktív védelmi üzemmódban.....	<a href="#">129</a>

## ÉRTEŚÍTÉSEK MINDEN VÉDELMI ÜZEMMÓDBAN

Ez a fejezet azokat az információkat ismerteti, amik automatikus és interaktív védelmi módban jelennek meg (lásd: „Védelmi mód kiválasztása”, [56.](#) oldal).


## EBBEN A RÉSZBEN:

Speciális kezelés szükséges.....	<a href="#">125</a>
Cserélhető meghajtó csatlakoztatva .....	<a href="#">126</a>
Megbízhatatlan tanúsítvány észlelése.....	<a href="#">126</a>
Egy betolakodók által a felhasználó számítógépének vagy adatainak kihasználására alkalmas alkalmazást észlelt a rendszer.....	<a href="#">126</a>
Karanténba helyezett nem fertőzött fájl.....	<a href="#">127</a>
Új termékverzió kibocsátása .....	<a href="#">127</a>
Műszaki frissítés kibocsátása.....	<a href="#">127</a>
Műszaki frissítés letöltve .....	<a href="#">128</a>
A letöltött műszaki frissítés nem került telepítésre .....	<a href="#">128</a>
A licenc lejárt.....	<a href="#">128</a>
Javasoljuk, hogy a vizsgálat elindítása előtt frissítse az adatbázisokat.....	<a href="#">129</a>

## SPECIÁLIS KEZELÉS SZÜKSÉGES

Ha olyan fenyegetést észlel, amely jelenleg aktív a rendszerben (például a RAM vagy az indítási objektumok rosszindulatú folyamata), egy megjelenő üzenet speciális, fejlett vírusmentesítési eljárás végrehajtásának megerősítésére kéri.

Az értesítés a következő információkat tartalmazza:

- A fenyegetés leírása.
- A fenyegetés típusa és a rosszindulatú objektum neve, ahogy a Kaspersky Lab Virus Encyclopedia tartalmazza. A rosszindulatú objektum neve mellett megjelenik a  ikon. Az ikonra kattintva megnyílik az objektummal kapcsolatos információkat tartalmazó ablak. Az ablakban megjelenő [www.securelist.com](http://www.securelist.com) hivatkozásra kattintva eljuthat a Virus Encyclopedia webhelyére, ahol részletes információkhoz jut az objektum által jelentett fenyegetésről.
- A rosszindulatú objektum fájlneve és elérési útvonala.

Az alábbi műveletek közül választhat:

- **Igen, vírusmentesítés újraindítással**– a speciális vírusmentesítési eljárás végrehajtása (ajánlott). A vírusmentesítés alatt a megbízhatókon kívül az összes alkalmazás blokkolásra kerül. Ha a vírusmentesítés kész, az operációs rendszer újraindul, ezért azt javasoljuk, hogy mentsen minden változtatást, és zárjon be minden alkalmazást, mielőtt elkezdi a vírusmentesítést. A számítógép újraindítása után ajánlott a teljes víruskeresést lefuttatni.

- **Ne futtassa** – az észlelt objektum vagy folyamat a kijelölt művelet szerint kerül feldolgozásra.

Ha azt szeretné, hogy a hasonló esemény megtörténtekor mindig ugyanez a művelet kerüljön végrehajtásra, jelölje be az **Alkalmazás minden objektumra** négyzetet.

## CSERÉLHETŐ MEGHAJTÓ CSATLAKOZTATVA

Ha cserélhető lemezt csatlakoztat a számítógéphez, a képernyőn megjelenik egy értesítés.

Az alábbi műveletek közül választhat:

- **Gyors vizsgálat** – csak a potenciális fenyegetést jelentő fájlok vizsgálata a cserélhető meghajtón.
- **Teljes vizsgálat** – az összes fájl vizsgálata a cserélhető meghajtón.
- **Ne vizsgálja** – a cserélhető meghajtó nem kerül vizsgálatra.

Ha azt szeretné, hogy a jövőben minden csatlakoztatott cserélhető meghajtón a kijelölt művelet kerüljön végrehajtásra, jelölje be **Az ilyen esetekben mindig végezze el** négyzetet.

## MEGBÍZHATATLAN TANÚSÍTVÁNY ÉSZLELÉSE

A Kaspersky Anti-Virus egy telepített tanúsítvánnyal ellenőrzi az SSL-en keresztül létrehozott kapcsolat biztonságát. Egy értesítés jelenik meg a képernyőn, ha a kiszolgálóhoz való csatlakozási kísérlet közben az alkalmazás érvénytelen tanúsítványt érzékel (például ha a tanúsítványt egy behatoló kicserélte).

Az értesítés a következő információkat tartalmazza:

- a fenyegetés leírása;
- a tanúsítvány megtekintéséhez vezető hivatkozás;
- a hiba lehetséges oka;
- a webes erőforrás URL-je.

Az alábbi műveletek közül választhat:


- **Igen, elfogadom a megbízhatatlan tanúsítványt** – kapcsolódás folytatása a webes erőforráshoz.
- **Tanúsítvány elutasítása** – a webhelyhez való kapcsolódás megszakítása.

## EGY BETOLAKODÓK ÁLTAL A FELHASZNÁLÓ SZÁMÍTÓGÉPÉNEK VAGY ADATAINAK KIHASZNÁLÁSÁRA ALKALMAS ALKALMAZÁST ÉSZLELT A RENDSZER

Amikor a Tevékenységfigyelő a felhasználó számítógépének vagy adatainak kihasználására alkalmas alkalmazást észlel, megjelenik egy értesítés.

Az értesítés a következő információkat tartalmazza:

- A fenyegetés leírása.
- A betolakodó által a felhasználó számítógépének vagy adatainak kihasználására alkalmas alkalmazás típusa és neve.

Az alkalmazás neve mellett megjelenik a  ikon. Az ikonra kattintva megnyílik az alkalmazással kapcsolatos információkat tartalmazó ablak.

- A folyamat azonosítója és az alkalmazásfájl neve, valamint az elérési útja.
- Az alkalmazás vésznaplóját tartalmazó ablakra mutató hivatkozás.

Az alábbi műveletek közül választhat:

- **Engedélyezés** – a folyamat futásának engedélyezése.
- **Karantén** – az alkalmazás bezárása, az alkalmazásfájl áthelyezése a Karanténba, ahol már nem jelent fenyegetést a számítógép biztonságára.

A Karantén további vizsgálata során az objektum státusza megváltozhat. Például a program az objektumot fertőzöttnek azonosíthatja és feldolgozhatja a frissített adatbázis alapján. Vagy az objektum állapota a *nem fertőzött* értékre módosulhat, és ezután megtörténhet a visszaállítása.

A Karanténba helyezett fájl állapota a következő vizsgálatkor a *nem fertőzött* állapotra módosulhat, de erre legkorábban a Karanténba mozgatást követő harmadik napon kerülhet sor.

- **Alkalmazás megszakítása** – megszakítja az alkalmazás végrehajtását.
- **Hozzáadás a kizárásokhoz** – az alkalmazás a jövőben mindig végezhet hasonló tevékenységet.

## KARANTÉNBA HELYEZETT NEM FERTŐZÖTT FÁJL

A Kaspersky Anti-Virus alapértelmezésben az adatbázis minden frissítésekor megvizsgálja a karanténba helyezett fájlokat. Ha egy karanténba helyezett fájl vizsgálata azt mutatja, hogy az nem fertőzött, a képernyőn megjelenik egy értesítés.

Az értesítés a következő információkat tartalmazza:

- javaslat a karanténba helyezett fájl visszaállítására;
- a fájl neve a mappa elérési útjával együtt, ahol a karantén előtt tárolódott.

Az alábbi műveletek közül választhat:

- **Visszaállítás** – a fájl helyreállítása a karanténból történő eltávolítással és az eredeti mappába való visszahelyezéssel.
- **Mégse** – a fájl bent marad a karanténban.

## ÚJ TERMÉKVERZIÓ KIBOCSÁTÁSA

Ha ki lett bocsátva a Kaspersky Anti-Virus egy új változata és elérhetővé válik a Kaspersky Lab kiszolgálóin, a képernyőn megjelenik egy értesítés.

Az értesítés a következő információkat tartalmazza:

- hivatkozás az új termékverzió részletes adatait tartalmazó ablakhoz;
- a telepítőcsomag mérete.

Az alábbi műveletek közül választhat:

- **Igen, letöltés** – az alkalmazás új termékverziójának a letöltése a kijelölt mappába.
- **Nem** – a telepítőcsomag letöltése megszakad.

Ha nem szeretné, hogy a későbbiekben az értesítés az új termékverzióról megjelenjen a képernyőn, jelölje be a **Nem kérek információt a frissítésről** négyzetet.

## MŰSZAKI FRISSÍTÉS KIBOCSÁTÁSA

Ha ki lett bocsátva a Kaspersky Anti-Virus egy műszaki frissítése és elérhetővé válik a Kaspersky Lab kiszolgálóin, a képernyőn megjelenik egy értesítés.

Az értesítés a következő információkat tartalmazza:

- az alkalmazás számítógépre telepített verziójának a száma;
- az alkalmazás számítógépre telepített verziójának a száma a várható műszaki frissítés után;
- hivatkozás a műszaki frissítés részletes adatait tartalmazó ablakhoz;
- a frissítési fájl mérete.

Az alábbi műveletek közül választhat:

- **Igen, letöltés** – a frissítési fájl letöltése a kijelölt mappába.
- **Nem** – a frissítés letöltése megszakad. Ez a lehetőség akkor elérhető, ha a **Nem kérek információt a letöltésről** négyzetet bejelölte (lásd alább).

- **Nem, emlékeztessen később**– az azonnali letöltés visszavonásra kerül, a frissítésről később emlékeztető érkezik. Ez a lehetőség akkor elérhető, ha a **Nem kérek információt a letöltésről** négyzetet nem jelölte be (lásd alább).

Ha nem szeretné, hogy a későbbiekben ez az értesítés megjelenjen a képernyőn, jelölje be a **Nem kérek információt a frissítésről** négyzetet.

## MŰSZAKI FRISSÍTÉS LETÖLTVE

Ha a Kaspersky Anti-Virus műszaki frissítése sikeresen letöltődött a Kaspersky Lab kiszolgálóiról, a képernyőn megjelenik egy értesítés.

Az értesítés a következő információkat tartalmazza:

- az alkalmazás számítógépre telepített verziójának a száma a műszaki frissítés után;
- hivatkozás a frissítő fájlhoz.

Az alábbi műveletek közül választhat:

- **Igen, telepítés** – a frissítés telepítése.

A frissítés telepítése után az operációs rendszert újra kell indítani.

- **Telepítés elhalasztása** – a telepítés megszakítása későbbi végrehajtásra.

## A LETÖLTÖTT MŰSZAKI FRISSÍTÉS NEM KERÜLT TELEPÍTÉSRE

Ha a Kaspersky Anti-Virus műszaki frissítése letöltésre került de még nem települt a számítógépre, a képernyőn megjelenik egy értesítés.

Az értesítés a következő információkat tartalmazza:

- az alkalmazás számítógépre telepített verziójának a száma a műszaki frissítés után;
- hivatkozás a frissítő fájlhoz.

Az alábbi műveletek közül választhat:

- **Igen, telepítés** – a frissítés telepítése.

A frissítés telepítése után az operációs rendszert újra kell indítani.

- **Telepítés elhalasztása** – a telepítés megszakítása későbbi végrehajtásra.

Ha nem szeretné, hogy a későbbiekben ez a frissítési értesítés megjelenjen a képernyőn, jelölje be a **Ne kérdezzen rá, amíg nem érhető el új verzió** négyzetet.

## A LICENC LEJÁRT

Ha a próbalicenc lejár, a Kaspersky Anti-Virus megjelenít egy értesítést.

Az értesítés a következő információkat tartalmazza:

- a próbaidőszak hossza;
- információk az alkalmazás tevékenységének eredményéről (hivatkozást is tartalmazhat további részletekhez).

Az alábbi műveletek közül választhat:

- **Igen, vásárlás**– ezt a lehetőséget kiválasztva megnyílik egy böngészőablak, és betöltődik az eStore weboldal, ahol megvásárolhatja a kereskedelmi licencet.
- **Mégse**– az alkalmazás használatáról való lemondás. Ezt a lehetőséget választva az alkalmazás fő funkciói (víruskeresés, frissítés, valós idejű védelem stb.) leállnak.

## JAVASOLJUK, HOGY A VIZSGÁLAT ELINDÍTÁSA ELŐTT FRISSÍTSE AZ ADATBÁZISOKAT

Ha az adatbázisok első frissítése előtt vagy alatt indít vizsgálati feladatot, értesítés jelenik meg a képernyőn.

Az értesítés javaslatot tartalmaz az adatbázisok frissítésére, vagy arra, hogy várja meg a vizsgálat a frissítés befejeződését.

Az alábbi műveletek közül választhat:

- **Adatbázisok frissítése a vizsgálat előtt** – adatbázisok frissítésének elindítása, ami után a vizsgálati feladat automatikusan elkezdődik. Ez a művelet nem választható ki, ha már az adatbázisok első frissítése előtt elindította a vizsgálatot.
- **Vizsgálat megkezdése a frissítés után** – várakozás az adatbázisok frissítésének befejeződésére, majd a vizsgálat automatikus elindítása. Ez a művelet nem választható ki, ha már az adatbázisok első frissítése alatt elindította a vizsgálatot.
- **Vizsgálat megkezdése most** – vizsgálat megkezdése az adatbázisok frissítésének befejeződése előtt.

## ÉRTEŚÍTÉSEK INTERAKTÍV VÉDELMI ŰZEMMÓDBAN

Ez a fejezet azokat az információkat ismerteti, amik interaktív védelmi módban jelennek meg (lásd: „Védelmi mód kiválasztása”, [56.](#) oldal).

### EBBEN A RÉSZBEN:


Gyanús / rosszindulatú objektum észlelése .....	<a href="#">129</a>
Észlelt sebezhetőség .....	<a href="#">130</a>
Veszélyes aktivitás észlelése a rendszerben .....	<a href="#">131</a>
Betolakodó által a felhasználó számítógépének vagy adatainak kihasználására alkalmas alkalmazás által végzett módosítások vizsgálórgéte .....	<a href="#">131</a>
Rosszindulatú alkalmazás észlelése .....	<a href="#">131</a>
Egy betolakodók által kihasználásra alkalmas alkalmazást észlelt a rendszer .....	<a href="#">132</a>
Gyanús / rosszindulatú hivatkozás észlelése .....	<a href="#">133</a>
Veszélyes objektum észlelése az adatforgalomban .....	<a href="#">133</a>
Adathalász webhely elérési kísérletének észlelése .....	<a href="#">133</a>
A rendszerleíró adatbázis elérésére irányuló próbálkozás észlelése .....	<a href="#">134</a>
Az objektum nem vírusmentesíthető .....	<a href="#">134</a>
Rejtett folyamat észlelése .....	<a href="#">135</a>

## GYANÚS / ROSSZINDULATÚ OBJEKTUM ÉSZLELESE

A Fájll víruskereső, Levél víruskereső vagy egy víruskeresés futása közben értesítés jelenik meg a képernyőn az alábbi objektumok valamelyikének észlelésekor:

- rosszindulatú objektum;
- ismeretlen vírus kódját tartalmazó objektum;
- ismeretlen vírus módosított kódját tartalmazó objektum.

Az értesítés a következő információkat tartalmazza:

- A fenyegetés leírása.
- A fenyegetés típusa és a rosszindulatú objektum neve, ahogy a Kaspersky Lab Virus Encyclopedia tartalmazza. A rosszindulatú objektum neve mellett megjelenik a  ikon. Az ikonra kattintva megnyílik az objektummal kapcsolatos információkat tartalmazó ablak. Az ablakban megjelenő [www.securelist.com](http://www.securelist.com) hivatkozásra kattintva eljuthat a Virus Encyclopedia webhelyére, ahol részletes információkhoz jut az objektum által jelentett fenyegetésről.
- A rosszindulatú objektum fájlneve és elérési útvonala.

Az objektumhoz választhat egyet az alábbi műveletek közül:

- **Vírusmentesítés** – megkísérli vírusmentesíteni a rosszindulatú objektumot. Ez a lehetőség javasolt, ha a fenyegetés ismert.  
Az objektumról annak vírusmentesítése előtt biztonsági másolat készül.
- **Karantén** – az objektum áthelyezése a Karanténba, ahol már nem jelent veszélyt a számítógépre. Ez a lehetőség akkor javasolt, ha sem a fenyegetés, sem pedig az objektum vírusmentesítésének módja nem ismert.  
A Karantén további vizsgálata során az objektum státusza megváltozhat. Például a program az objektumot fertőzöttnek azonosíthatja és feldolgozhatja a frissített adatbázis alapján. Vagy az objektum állapota a *nem fertőzött* értékre módosulhat, és ezután megtörténhet a visszaállítása.

A Karanténba helyezett fájl állapota a következő vizsgálatkor a *nem fertőzött* állapotra módosulhat, de erre legkorábban a Karanténba mozgatást követő harmadik napon kerülhet sor.

- **Törlés** – törli az objektumot. Az objektumról annak törlése előtt biztonsági másolat készül.
- **Kihagyás / Blokkolás** – az objektum elérésének blokkolása további műveletek nélkül, az erre vonatkozó információ rögzítése a jelentésben.  
A jelentés ablakban visszatérhet a kihagyott objektumok feldolgozására. Az emailekben észlelt objektumok feldolgozása ugyanakkor nem halasztható el.


Jelölje be az **Alkalmazás minden objektumra** négyzetet a kiválasztott művelet alkalmazásához a védelmi összetevő vagy feladat aktuális munkamentében észlelt minden azonos típusú fenyegetésre. Az aktuális munkamenet az összetevő elindítása és leállítása, vagy a Kaspersky Anti-Virus újraindítása, illetve a víruskeresés elindítása és befejezése között eltelt időtartamot jelenti.

Ha biztos benne, hogy az észlelt objektum nem rosszindulatú, akkor javasoljuk, hogy vegye azt fel a megbízható zónába, így a program nem fog ismételt hamis pozitív jelzést adni az objektum használatakor.

## ÉSZLELT SEBEZHETŐSÉG

Sebezhetőség észlelése esetén egy értesítés jelenik meg a képernyőn.

Az értesítés a következő információkat tartalmazza:

- A sebezhetőség leírása.
- A sebezhetőség Kaspersky Lab Virus Encyclopedia adatbázisban szereplő nevét. A név mellett megjelenik a  ikon. Az ikonra kattintva megnyílik a sebezhetőséggel kapcsolatos információkat tartalmazó ablak. Az ablakban megjelenő [www.securelist.com](http://www.securelist.com) hivatkozásra kattintva eljut a Virus Encyclopedia webhelyére, ahol részletes információkhoz juthat a sebezhetőségről.
- A sebezhető objektum fájlneve és elérési útvonala.


Az objektumhoz választhat egyet az alábbi műveletek közül:

- **Igen, javítás** – a sebezhetőség megszüntetése.
- **Kihagyás** – nincs művelet a sebezhető objektummal.

## VESZÉLYES AKTIVITÁS ÉSZLELÉSE A RENDSZERBEN

Ha a Proaktív védelem veszélyes alkalmazási tevékenységet észlel a rendszerben, megjelenik egy értesítés.

Az értesítés a következő információkat tartalmazza:

- A fenyegetés leírása.
- A fenyegetés típusa és a rosszindulatú objektum neve, ahogy a Kaspersky Lab Virus Encyclopedia tartalmazza.  
A rosszindulatú objektum neve mellett megjelenik a  ikon. Az ikonra kattintva megnyílik az objektummal kapcsolatos információkat tartalmazó ablak. Az ablakban megjelenő [www.securelist.com](http://www.securelist.com) hivatkozásra kattintva eljuthat a Virus Encyclopedia webhelyére, ahol részletes információkhoz jut az objektum által jelentett fenyegetésről.
- A folyamat azonosítója és az alkalmazásfájl neve, valamint az elérési útja.

Az alábbi műveletek közül választhat:

- **Engedélyezés** – a folyamat futásának engedélyezése.
- **Karantén** – az alkalmazás bezárása, az alkalmazásfájl áthelyezése a Karanténba, ahol már nem jelent fenyegetést a számítógép biztonságára.

A Karantén további vizsgálata során az objektum státusza megváltozhat. Például a program az objektumot fertőzöttnek azonosíthatja és feldolgozhatja a frissített adatbázis alapján. Vagy az objektum állapota a *nem fertőzött* értékre módosulhat, és ezután megtörténhet a visszaállítás.

A Karanténba helyezett fájl állapota a következő vizsgálatkor a *nem fertőzött* állapotra módosulhat, de erre legkorábban a Karanténba mozgatást követő harmadik napon kerülhet sor.


- **Alkalmazás megszakítása** – megszakítja az alkalmazás végrehajtását.
- **Hozzáadás a kizárásokhoz** – az alkalmazás a jövőben mindig végezhet hasonló tevékenységet.

Ha biztos benne, hogy az észlelt program nem veszélyes, akkor ajánlott felvenni azt a megbízható zónába, hogy a Kaspersky Anti-Virus annak észlelésekor ne adjon ismételt hamis pozitív jelzést.

## BETOLAKODÓ ÁLTAL A FELHASZNÁLÓ SZÁMÍTÓGÉPÉNEK VAGY ADATAINAK KIHASZNÁLÁSÁRA ALKALMAS ALKALMAZÁS ÁLTAL VÉGZETT MÓDOSÍTÁSOK VISSZAGÖRGETÉSE

Javasoljuk, hogy végezze el a betolakodó által a felhasználó számítógépének vagy adatainak kihasználására alkalmas alkalmazás által végzett módosítások visszagörgetését (elvetését). Amikor egy ilyen objektum beszünteti a tevékenységét, egy értesítés jelenik meg a képernyőn, ami a módosítások visszagörgetésére szólítja fel.

Az értesítés a következő információkat tartalmazza:

- Ez a betolakodó által a felhasználó számítógépének vagy adatainak kihasználására alkalmas alkalmazás által végzett módosítások visszagörgetését kéri.
- Az alkalmazás típusa és neve.  
Az alkalmazás neve mellett megjelenik a  ikon. Az ikonra kattintva megnyílik az alkalmazással kapcsolatos információkat tartalmazó ablak.
- A folyamat azonosítója és az alkalmazásfájl neve, valamint az elérési útja.

Az alábbi műveletek közül választhat:


- **Átugrás** – a változások visszagörgetésének a megszakítása.
- **Igen, visszagörgetés** – az alkalmazás által végzett módosítások visszagörgetésére.

## ROSSZINDULATÚ ALKALMAZÁS ÉSZLELÉSE

Ha a Rendszerfigyelő olyan alkalmazást észlel, amelynek a működése pontosan megfelel a rosszindulatú alkalmazásokénak, a képernyőn megjelenik egy értesítés.

Az értesítés a következő információkat tartalmazza:

- A fenyegetés leírása.
- A rosszindulatú alkalmazás típusa és neve.

Az alkalmazás neve mellett megjelenik a  ikon. Az ikonra kattintva megnyílik az alkalmazással kapcsolatos információkat tartalmazó ablak.

- A folyamat azonosítója és az alkalmazásfájl neve, valamint az elérési útja.
- Az alkalmazás vésznaplóját tartalmazó ablakra mutató hivatkozás.

Az alábbi műveletek közül választhat:

- **Engedélyezés** – a folyamat futásának engedélyezése.
- **Karantén** – az alkalmazás bezárása, az alkalmazásfájl áthelyezése a Karanténba, ahol már nem jelent fenyegetést a számítógép biztonságára.

A Karantén további vizsgálata során az objektum státusza megváltozhat. Például a program az objektumot fertőzöttnek azonosíthatja és feldolgozhatja a frissített adatbázis alapján. Vagy az objektum állapota a *nem fertőzött* értékre módosulhat, és ezután megtörténhet a visszaállítása.

A Karanténba helyezett fájl állapota a következő vizsgálatkor a *nem fertőzött* állapotra módosulhat, de erre legkorábban a Karanténba mozgatást követő harmadik napon kerülhet sor.


- **Alkalmazás megszakítása** – megszakítja az alkalmazás végrehajtását.
- **Hozzáadás a kizárásokhoz** – az alkalmazás a jövőben mindig végezhet hasonló tevékenységet.

## EGY BETOLAKODÓK ÁLTAL KIHASZNÁLÁSRA ALKALMAS ALKALMAZÁST ÉSZLELT A RENDSZER

Ha a Fájl víruskereső, a Levél víruskereső vagy a víruskereső feladat olyan alkalmazást észlel, amelyet a betolakodó felhasználhat, megjelenik egy értesítés.

Az értesítés a következő információkat tartalmazza:

- A fenyegetés leírása.
- A fenyegetés típusa és az objektum neve, ahogy a Kaspersky Lab Virus Encyclopedia tartalmazza.

Az objektum neve mellett megjelenik a  ikon. Az ikonra kattintva megnyílik az objektummal kapcsolatos információkat tartalmazó ablak. Az ablakban megjelenő [www.securelist.com](http://www.securelist.com) hivatkozásra kattintva eljuthat a Virus Encyclopedia webhelyére, ahol részletes információkhoz jut a fenyegetésről.

- Az objektumfájl neve és elérési útja.

Az objektumhoz választhat egyet az alábbi műveletek közül:

- **Karantén** – az objektum áthelyezése a Karanténba, ahol már nem jelent veszélyt a számítógépre. Ez a lehetőség akkor javasolt, ha sem a fenyegetés, sem pedig az objektum vírusmentesítésének módja nem ismert.

A Karantén további vizsgálata során az objektum státusza megváltozhat. Például a program az objektumot fertőzöttnek azonosíthatja és feldolgozhatja a frissített adatbázis alapján. Vagy az objektum állapota a *nem fertőzött* értékre módosulhat, és ezután megtörténhet a visszaállítása.

A Karanténba helyezett fájl állapota a következő vizsgálatkor a *nem fertőzött* állapotra módosulhat, de erre legkorábban a Karanténba mozgatást követő harmadik napon kerülhet sor.

- **Törlés** – törli az objektumot. Az objektumról annak törlése előtt biztonsági másolat készül.
- **Archívum törlése** – jelszóval védett archívum törlése.
- **Kihagyás / Blokkolás** – az objektum elérésének blokkolása további műveletek nélkül, az erre vonatkozó információ rögzítése a jelentésben.

A jelentés ablakban visszatérhet a kihagyott objektumok feldolgozására. Az emailekben észlelt objektumok feldolgozása ugyanakkor nem halasztható el.

- **Hozzáadás a kizárásokhoz** – kizárási szabály létrehozása ehhez a fenyegetéstípushoz.

Jelölje be az **Alkalmazás minden objektumra** négyzetet a kiválasztott művelet alkalmazásához a védelmi összetevő vagy feladat aktuális munkamenetében észlelt minden azonos típusú fenyegetésre. Az aktuális munkamenet az összetevő elindítása és leállítása, vagy a Kaspersky Anti-Virus újraindítása, illetve a víruskeresés elindítása és befejezése között eltelt időtartamot jelenti.

Ha biztos benne, hogy az észlelt objektum nem rosszindulatú, akkor javasoljuk, hogy vegye azt fel a megbízható zónába, így a program nem fog ismételten hamis pozitív jelzést adni az objektum használatakor.

## GYANÚS / ROSSZINDULATÚ HIVATKOZÁS ÉSZLELÉSE

Ha a Kaspersky Anti-Virus gyanús vagy rosszindulatú tartalommal rendelkező webhely megnyitási kísérletét észleli, a képernyőn megjelenít egy értesítést.

Az értesítés a következő információkat tartalmazza:

- a fenyegetés leírása;
- a webhelyet betöltő alkalmazás (böngésző) neve;
- a gyanús vagy rosszindulatú tartalommal rendelkező webhely URL-je vagy weblapja.

Az alábbi műveletek közül választhat:

- **Engedélyezés** – a webhely letöltése folytatódhat.
- **Blokkolás** – a webhely letöltése blokkolódik.

Jelölje be az **Alkalmazás minden objektumra** négyzetet a kiválasztott művelet alkalmazásához a védelmi összetevő vagy feladat aktuális munkamenetében észlelt minden azonos típusú fenyegetést jelentő webhelyre. A jelenlegi munkamenet az az időszak, amely az összetevő elindításától annak leállításáig, vagy a Kaspersky Anti-Virus újraindításáig tart.

## VESZÉLYES OBJEKTUM ÉSZLELÉSE AZ ADATFORGALOMBAN

Ha a Webes víruskereső rosszindulatú objektumot észlel a forgalomban, a képernyőn megjelenik egy speciális értesítés.

Az értesítés a következő információkat tartalmazza:

- A fenyegetés vagy az alkalmazás által végzett műveletek leírása.
- A műveletet végző alkalmazás neve.
- A fenyegetés típusa és a rosszindulatú objektum neve, ahogy a Kaspersky Lab Virus Encyclopedia tartalmazza.

A rosszindulatú objektum neve mellett megjelenik a ⓘ ikon. Az ikonra kattintva megnyílik az objektummal kapcsolatos információkat tartalmazó ablak. Az ablakban megjelenő [www.securelist.com](http://www.securelist.com) hivatkozásra kattintva eljuthat a Virus Encyclopedia webhelyére, ahol részletes információkhoz jut az objektum által jelentett fenyegetésről.

- Objektum helye (URL).

Az alábbi műveletek közül választhat:

- **Engedélyezés** – az objektum letöltése folytatódhat.
- **Blokkolás** – az objektum letöltését a webes forrásból a rendszer blokkolja.

Jelölje be az **Alkalmazás minden objektumra** négyzetet a kiválasztott művelet alkalmazásához a védelmi összetevő vagy feladat aktuális munkamenetében észlelt minden azonos típusú fenyegetésre. A jelenlegi munkamenet az az időszak, amely az összetevő elindításától annak leállításáig, vagy a Kaspersky Anti-Virus újraindításáig tart.

## ADATHALÁSZ WEBHELY ELÉRÉSI KÍSÉRLETÉNEK ÉSZLELÉSE

Ha a Kaspersky Anti-Virus olyan weboldal elérési kísérletét érzékeli, amely adathalász webhelyhez tartozik vagy tartozhat, a képernyőn megjelenít egy speciális értesítést.

Az értesítés a következő információkat tartalmazza:

- a fenyegetés leírása;
- webhely URL-je.

Az alábbi műveletek közül választhat:

- **Engedélyezés** – a webhely letöltése folytatódhat.
- **Blokkolás** – a webhely letöltése blokkolódik.

Jelölje be az **Alkalmazás minden objektumra** négyzetet a kiválasztott művelet alkalmazásához a Kaspersky Anti-Vírus aktuális munkamenetében észlelt minden azonos típusú fenyegetést jelentő webhelyre. A jelenlegi munkamenet az az időszak, amely az összetevő elindításától annak leállításáig, vagy a Kaspersky Anti-Vírus újraindításáig tart.

## A RENDSZERLEÍRÓ ADATBÁZIS ELÉRÉSÉRE IRÁNYULÓ PRÓBÁLKOZÁS ÉSZLELÉSE

Ha a Proaktív védelem a rendszerleíró kulcsok elérésére irányuló kísérletet észlel, megjelenik egy értesítés.

Az értesítés a következő információkat tartalmazza:

- az elérni kívánt rendszerleíró kulcsot;
- a rendszerleíró kulcsok elérésére irányuló kísérletet kezdeményező folyamat fájlnevét és elérési útvonalát.

Az alábbi műveletek közül választhat:

- **Engedélyezés** – engedélyezi a veszélyes művelet egyszeri végrehajtását;
- **Blokkolás** – egyszer blokkolja a veszélyes műveletet.


Jelölje be a **Szabály létrehozása** négyzetet, ha a kiválasztott művelet a rendszerleíró kulcsokhoz való hozzáférésre irányuló minden kísérletre alkalmazni szeretné.

Ha biztos benne, hogy a rendszerleíró adatbázist elérni kívánó alkalmazás nem veszélyes, vegye azt fel a megbízható alkalmazások közé.

## AZ OBJEKTUM NEM VÍRUSMENTESÍTHETŐ

Bizonyos esetekben egy objektum nem minden vírusmentesíthető: például, ha a fájl oly mértékben károsodott, hogy az alkalmazás nem képes eltávolítani belőle a rosszindulatú kódot, majd helyreállítani az integritását. A kezelési eljárás nem alkalmazható a rosszindulatú objektumok több típusára, például a trójaiakra. Ha egy objektum nem vírusmentesíthető, egy értesítés jelenik meg a képernyőn.

Az értesítés a következő információkat tartalmazza:

- A fenyegetés leírása.
- A fenyegetés típusa és a rosszindulatú objektum neve, ahogy a Kaspersky Lab Virus Encyclopedia tartalmazza.  
A rosszindulatú objektum neve mellett megjelenik a  ikon. Az ikonra kattintva megnyílik az objektummal kapcsolatos információkat tartalmazó ablak. Az ablakban megjelenő [www.securelist.com](http://www.securelist.com) hivatkozásra kattintva eljuthat a Virus Encyclopedia webhelyére, ahol részletes információkhoz jut az objektum által jelentett fenyegetésről.
- A rosszindulatú objektum fájlneve és elérési útvonala.

Az alábbi műveletek közül választhat:

- **Törlés** – törli az objektumot. Az objektumról annak törlése előtt biztonsági másolat készül.
- **Kihagyás / Blokkolás** – az objektum elérésének blokkolása további műveletek nélkül, az erre vonatkozó információ rögzítése a jelentésben.

A jelentés ablakban visszatérhet a kihagyott objektumok feldolgozására. Az emailekben észlelt objektumok feldolgozása ugyanakkor nem halasztható el.


- **Hozzáadás a kizárásokhoz** – kizárási szabály létrehozása ehhez a fenyegetéstípushoz.

Jelölje be az **Alkalmazás minden objektumra** négyzetet a kiválasztott művelet alkalmazásához a védelmi összetevő vagy feladat aktuális munkamenetében észlelt minden azonos típusú fenyegetésre. Az aktuális munkamenet az összetevő elindítása és leállítása, vagy a Kaspersky Anti-Vírus újraindítása, illetve a víruskeresés elindítása és befejezése között eltelt időtartamot jelenti.

## REJTETT FOLYAMAT ÉSZLELÉSE

Ha a Proaktív védelem a háttérben rejtett folyamatot észlel, a képernyőn megjelenik egy értesítés.

Az értesítés a következő információkat tartalmazza:

- A fenyegetés leírása.
- A fenyegetés Kaspersky Lab Virus Encyclopedia adatbázisban szereplő típusa és neve.  
A név mellett megjelenik a  ikon. Az ikonra kattintva megnyílik a fenyegetéssel kapcsolatos információkat tartalmazó ablak. Az ablakban megjelenő [www.securelist.com](http://www.securelist.com) hivatkozásra kattintva eljut a Virus Encyclopedia webhelyére, ahol részletes információkhoz juthat a fenyegetésről.
- A folyamatfájl neve és elérési útja.

Az alábbi műveletek közül választhat:

- **Karantén** – a folyamat lezárása és a folyamatfájl áthelyezése a Karanténba, ahol már nem jelent fenyegetést a számítógép biztonságára.

A Karantén további vizsgálata során az objektum státusza megváltozhat. Például a program az objektumot fertőzöttnek azonosíthatja és feldolgozhatja a frissített adatbázis alapján. Vagy az objektum állapota a *nem fertőzött* értékre módosulhat, és ezután megtörténhet a visszaállítása.

A Karanténba helyezett fájl állapota a következő vizsgálatkor a *nem fertőzött* állapotra módosulhat, de erre legkorábban a Karanténba mozgatót követő harmadik napon kerülhet sor.

- **Megszakítás** – megszakítja a folyamatot.
- **Engedélyezés** – a folyamat végrehajtása engedélyezésre kerül.

Ha azt szeretné, hogy a kiválasztott művelet legyen alkalmazva a Proaktív védelem működésének aktuális munkamenetébe észlelt összes ilyen típusú fenyegetésre, jelölje be az **Alkalmazás minden ilyen esetben** négyzetet. A jelenlegi munkamenet az az időszak, amely az összetevő elindításától annak leállításáig, vagy a Kaspersky Anti-Virus újraindításáig tart.

Ha biztos benne, hogy az észlelt folyamat nem veszélyes, akkor ajánlott felvenni azt a megbízható zónába, hogy a Kaspersky Anti-Virus annak észlelésekor ne adjon ismételt hamis pozitív jelzést.

# SZÓJEGYZÉK

## A

### **A KASPERSKY LAB FRISSÍTÉSKISZOLGÁLÓI**

A Kaspersky Lab azon HTTP- és FTP-kiszolgálóinak listája, amelyekről az alkalmazás letölti a számítógépre az adatbázisokat és a modulfrissítéseket.

### **ADATBÁZIS-FRISSÍTÉS**

A Kaspersky Lab alkalmazások által végrehajtott egyik funkció, melynek révén a tartalom mindig naprakészen tartható. A frissítés során a rendszer a Kaspersky Lab frissítéskiszolgálóiról letölti az adatbázisokat a számítógépre, és automatikusan csatlakoztatja azokat az alkalmazáshoz.

### **ADATBÁZISOK**

A Kaspersky Lab szakemberei által létrehozott adatbázisok, amelyek a számítógép biztonságát veszélyeztető összes jelenleg létező fenyegetés részletes leírását tartalmazzák, a felismerésükre és vírusmentesítésükre szolgáló módszerekkel együtt. Az adatbázisokat a Kaspersky Lab új fenyegetések megjelenésekor folyamatosan frissíti.

### **ADATHALÁSZ WEBCÍMEK ADATBÁZISA**

A Kaspersky Lab szakértői által adathalászként megjelölt webcímek listája. Az adatbázis rendszeresen frissül, és a Kaspersky Lab alkalmazás részét képezi.

### **ADATHALÁSZAT**

Ez olyan internetes visszaélés, amely során bizalmas információk, leggyakrabban pénzügyi adatok megszerzése céljából kap a károsult email üzenetet.

### **ADMINISZTRÁCIÓS KISZOLGÁLÓI TANÚSÍTVÁNY**

Az Adminisztrációs konzol csatlakoztatásakor és a felhasználói számítógépekkel való adatcsere alkalmával az adminisztrációs kiszolgáló általi hitelesítést lehetővé tevő tanúsítvány. Az Adminisztrációs kiszolgálói tanúsítvány létrehozására az Adminisztrációs kiszolgáló telepítésekor kerül sor, és az az %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert mappában van tárolva.

### **AJÁNLOTT SZINT**

A Kaspersky Lab szakértői által ajánlott, az alkalmazás beállításain alapuló biztonsági szint, amely optimális védelmet biztosít a számítógépnek. A program alapértelmezés szerint ezt a szintet alkalmazza.

### **AKTÍV LICENC**

Valamely Kaspersky Lab alkalmazás futtatásához jelenleg használt licenc. A licenc meghatározza az összes funkcióra kiterjedő használati jogosultság lejáratát és az alkalmazásra vonatkozó licencirányelveket. Az alkalmazás legfeljebb egy aktív állapotú licencet tartalmazhat.

### **ALHÁLÓZATI MASZK**

Az alhálózati maszk (vagy hálózati maszk) és a hálózati cím határozzák meg a számítógépek címét egy hálózatban.

### **ALKALMAZÁS AKTIVÁLÁSA**

Az alkalmazás átkapcsolása teljes funkcionalitású üzemmódba. Az alkalmazás aktiválásához licenc szükséges.

### **ALKALMAZÁSBEÁLLÍTÁSOK**

Az összes feladattípusra jellemző alkalmazás-beállítások, amelyek az alkalmazás egészének működését szabályozzák, például a teljesítményre, a jelentésekre vagy a másolattárolóra vonatkozó beállítások tekintetében.

### **ALKALMAZÁSMODULOK**

A Kaspersky Lab telepítőcsomagjában található fájlok, amelyek a fő funkciók végrehajtásáért felelősek. Az alkalmazás által végrehajtott összes feladattípusnak (valós idejű védelem, kézzel indított keresés, frissítések) egy bizonyos végrehajtható modul felel meg. A számítógép teljes körű vírusellenőrzésének a főablakból való futtatásakor a felhasználó a megfelelő modul végrehajtását kezdeményezi.

## ALTERNATÍV NTFS-ADATFOLYAMOK

Olyan NTFS-adatfolyamok (alternatív adatfolyamok), amelyek kiegészítő jellemzőket vagy fájlinformációkat tartalmaznak.

Az NTFS-fájlrendszer valamennyi fájlja adatfolyamok egy csoportja. Ezen adatfolyamok közül az egyik tartalmazza a fájl megnyitásakor megjelenő tartalmat, míg más adatfolyamok (ezeket alternatívnak nevezzük) metainformációkat tartalmaznak, és biztosítják az NTFS más rendszerekkel – például a Macintosh régebbi HFS (Hierarchical File System) rendszerével – való kompatibilitását. Az adatfolyamok létrehozhatók, törölhetők, külön tárolhatók, átnevezhetők, sőt, akár folyamatként futtathatók.

Az alternatív adatfolyamokkal a behatolók titkosan továbbíthatnak adatokat, vagy ellophatják azokat a számítógépekről.

## ARCHÍVUM

Egy vagy több olyan objektumot „tartalmazó” fájl, amelyek maguk is archívumok lehetnek.

## B

### BEMENETI/KIMENETI PORT

A processzorokban (például Intel) a hardverösszetevőkkel való adatcserére használatos. A bemeneti/kimeneti port egy bizonyos hardverösszetevőhöz tartozik, és az alkalmazások adatcseréje céljából igénybe vehetik.

### BIZTONSÁGI SZINT

A biztonsági szint az összetevők előre megadott beállításait jelenti.

### BLOKKOLT URL-EK LISTÁJA

Olyan webes maszkok és címek listája, amelyek elérését a Kaspersky Lab alkalmazás blokkolja. A címek listáját a felhasználó hozza létre az alkalmazás beállításakor.

### BOOT VÍRUS

A számítógép merevlemezének indítószektorait megfertőző vírus. A vírus arra kényszeríti a rendszert, hogy újraindításakor betöltse azt a memóriába, és az eredeti indítókód helyett a víruskódnak adja át a vezérlést.

## E

### ELÉRHETŐ FRISSÍTÉSEK

A Kaspersky Lab alkalmazásmódulokhoz rendelkezésre álló frissítések csoportja, egyebek mellett a bizonyos idő alatt összegyűlt kritikus frissítésekkel és az alkalmazás architektúrájának változásaival.

### ELFOGÓ

Az alkalmazás egyik alösszetevője, amely bizonyos email típusok átvizsgálásáért felelős. Az adott telepítésre jellemző elfogók összetétele attól függ, hogy milyen szerepkör vagy szerepkörök betöltésére telepítették az alkalmazást.

### ELLENŐRIZENDŐ WEBCÍMEK LISTÁJA

Olyan webes maszkok és címek listája, amelyekben a Kaspersky Lab alkalmazásnak kötelezően ellenőriznie kell a rosszindulatú objektumok jelenlétét.

### ENGEDÉLYEZETT URL-EK LISTÁJA

Olyan webes maszkok és címek listája, amelyek elérését a Kaspersky Lab alkalmazás nem blokkolja. A címek listáját a felhasználó hozza létre az alkalmazás beállításakor.

### ÉRTESÍTÉSI SABLON

A vírusellenőrzés által megtalált fertőzött objektumokról generált értesítés alapját képező sablon. Az értesítési sablon tartalmazza az értesítés módját, a terjedés módját és az elküldendő üzenetek szövegét szabályozó beállításokat.

## ESEMÉNY SÚLYOSSÁGI SZINTJE

Egy a Kaspersky Lab alkalmazás működése közben naplózott esemény leírása. Négy súlyossági szint különböztethető meg:

- **Kritikus esemény.**
- **Funkcionális hiba.**
- **Figyelmeztetés.**
- **Információs üzenet.**

Azonos eseménytípusoknak más-más súlyossági szintje lehet attól függően, hogy milyen szituációban fordulnak elő.

## F

### FÁJLMASZK

Helyettesítő karakterekkel megadott fájlnev és kiterjesztés. A fájlmaszkokban használt két szabványos helyettesítő karakter a \* és a ?: a \* tetszőleges számú karaktert, míg a ? egyetlen karaktert helyettesít. Ezekkel a helyettesítő karakterekkel bármilyen fájlt leírhat. Fontos megjegyezni, hogy a fájlnev és a kiterjesztés között mindig egy pont áll.

### FEJLÉC

Egy fájl vagy üzenet elején található adatok, amelyek a fájl (vagy üzenet) állapotáról és feldolgozásáról tartalmazznak alacsony szintű információkat. Az email üzenetek fejléce például a feladóról és a címzetről, valamint a dátumról tájékoztat.

### FELADAT

A Kaspersky Lab alkalmazásában feladatként végrehajtott funkciók, például: **Valós idejű védelem, Teljes számítógép vizsgálata, Adatbázis-frissítés.**

### FELADATBEÁLLÍTÁSOK

Az egyes feladattípusokra jellemző alkalmazásbeállítások.

### FERTŐZÖTT OBJEKTUM

Rosszindulatú kódot tartalmazó objektum. Az alkalmazás akkor észleli, ha az objektum kódjának egy része teljesen azonos egy ismert fenyegetés kódjának egy részével. A Kaspersky Lab nem javasolja az ilyen objektumok használatát, mert azok megfertőzhetik a számítógépet.

### FIGYELT OBJEKTUM

HTTP-, FTP- vagy SMTP-protokollal a tűzfalon keresztül továbbított fájl, amelyet elküldenek a Kaspersky Lab alkalmazásnak ellenőrzés céljára.

### FORGALOMVIZSGÁLAT

Az adatbázisok legfrissebb verziójából származó információk alapján történő valós idejű ellenőrzés az összes protokollon (például HTTP, FTP stb.) keresztül továbbított objektumok körében.

### FRISSÍTÉS

A Kaspersky Lab frissítéskiszolgálóiról származó új fájlok (adatbázisok vagy alkalmazásmodulok) hozzáadása vagy korábbi fájlok helyetti beillesztése.

### FRISSÍTŐCSOMAG

A szoftver frissítésére szolgáló fájlcsomag. A program az internetről tölti le, majd telepíti a számítógépre.

## GY

### GYANÚS OBJEKTUM

Egy ismert vírus módosított kódját vagy egy vírus kódjára hasonlító, de a Kaspersky Lab által még nem ismert kódot tartalmazó objektum. A gyanús objektumok észlelése a heurisztikus elemző segítségével történik.

## GYANÚS ÜZENET

Olyan üzenet, amely nem tekinthető egyértelműen levélszemétnek, de a vizsgálat során gyanúsnak bizonyult (pl. bizonyos típusú levelek és reklámüzenetek).

## GYANÚS WEBCÍMEK ADATBÁZISA

Olyan webcímekek listája, amelyeknek tartalma potenciálisan veszélyesnek tekinthető. A listát a Kaspersky Lab szakértői hozták létre. Rendszeresen frissül, és a Kaspersky Lab alkalmazáscsomag részét képezi.

## H

### HÁLÓZATI PORT

TCP és UDP paraméter, amely IP formátumban meghatározza mindazon adatsomagok célhelyét, amelyek hálózaton keresztül kerülnek továbbításra egy gazdaszámítógéphez, és lehetővé teszi az egyetlen gazdaszámítógépen futó különböző programok számára, hogy egymástól függetlenül fogadjanak adatokat. Mindegyik program az egy bizonyos porton keresztül érkező adatokat dolgozza fel (azt is szokták mondani, hogy a program „figyeli” a portot).

Egyes gyakori hálózati protokollokhoz leggyakrabban szabványos portszámok vannak megadva (a webkiszolgálók például többnyire a 80-as TCP-porton keresztül fogadják a HTTP-kérelmeket); általában azonban egy adott program bármely porton keresztül használhatja bármelyik protokollt. Lehetséges értékek: 1 és 65 535 között.

### HARDVERPORT

Egy számítógép valamely hardverösszetevőjén található csatlakozó, amelybe kábel vagy csatlakozódugó illeszthető (LPT-port, soros port, USB-port).

### HEURISZTIKUS ELEMZŐ

A Kaspersky Lab alkalmazás adatbázisa segítségével nem azonosítható fenyegetések észlelésére létrehozott technológia. Lehetővé teszi a gyaníthatóan ismeretlen vírussal vagy egy ismert vírus új változatával fertőzött objektumok felismerését.

A heurisztikus elemző használatával akár a fenyegetések 92%-a is felismerhető. A mechanizmus elég hatékony és csak nagyon ritkán vezet hamis pozitív riasztáshoz.

A heurisztikus elemző által felismert fájlokat a program gyanúsnak tekinti.

## I

### ICHECKER TECHNOLÓGIA

Az iChecker technológia növeli a víruskeresések sebességét azáltal, hogy kizárja a keresésből a legutóbbi ellenőrzés óta változatlan objektumokat, feltéve, hogy közben az ellenőrzési paraméterek (vírusadatbázis, beállítások) sem változtak meg. Az egyes fájlokra vonatkozó információkat egy speciális adatbázis tárolja. A technológia a valós idejű védelemben és a kézzel indított ellenőrzések során egyaránt szerepet játszik.

Tegyük fel például, hogy a Kaspersky Lab alkalmazás már megvizsgált egy archívumot, és azt nem fertőzöttnek értékelte. Az alkalmazás legközelebb átugorja ezt az archívumot, kivéve ha azt módosították vagy a vizsgálati beállítások megváltoztak. Ha az archívumot új objektummal bővítette, módosította a keresési beállításokat, vagy frissítette a vírusadatbázist, az archívum ismét ellenőrzésre kerül.

Az iChecker technológia korlátai:

- a technológia nagyméretű fájlokkal nem használható, mert a fájl vírusellenőrzése rövidebb időt vesz igénybe, mint annak megvizsgálása, hogy módosították-e a legutóbbi vírusellenőrzés óta;
- a technológia csak néhány formátumot támogat (**EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR**).

### INDÍTÁSI OBJEKTUMOK

Az operációs rendszer és a számítógépre telepített szoftverek megfelelő elindításához és működéséhez szükséges programok csoportja. Ezen objektumok végrehajtására az operációs rendszer minden indításakor sor kerül. Bizonyos vírusok kifejezetten az ilyen objektumokat fertőzik meg, amivel például blokkolhatják az operációs rendszer elindulását.

## INDÍTÓSEKTOR

Az indítószektor a számítógép merevlemezének, egy hajlékony lemeznek vagy más adattároló eszköznek egy speciális területe. A lemez fájlrendszeréről tartalmaz információkat, és az itt tárolt rendszerindító program hajtja végre az operációs rendszer indítását.

Az úgynevezett boot-vírusok ezeket az indítószektorokat fertőzik meg. A Kaspersky Lab alkalmazás segítségével az indítószektorok is ellenőrizhetők, és fertőzés észlelése esetén vírusmentesíthetők.

## INKOMPATIBILIS ALKALMAZÁS

Olyan, harmadik fél által készített vírusvédelmi alkalmazás vagy olyan Kaspersky Lab alkalmazás, amely nem támogatja a Kaspersky Anti-Virus általi felügyeletet.

## INTERNETPROTOKOLL (IP)

Az internet alapprotokollja, amely kifejlesztése óta, vagyis 1974 óta változatlan. Olyan alapvető műveleteket hajt végre, mint a számítógépek közötti adattovábbítás, és a magasabb szintű protokolloknak (például TCP vagy UDP) is alapjául szolgál. Felügyeli a kapcsolódási és hibafeldolgozási funkciókat is. Az olyan technológiák, mint a NAT vagy a maszkolás révén elrejthető számos olyan magánhálózat, amely kisszámú (vagy akár egyetlen) IP-címet használ, és így lehetővé válik a folyamatosan növekvő internet igényeinek kielégítése a viszonylag korlátozott IPv4 címtér segítségével.

## ISMERETLEN VÍRUS

Olyan új vírus, amelyről az adatbázisok nem tartalmaznak információkat. Az alkalmazás általában a heurisztikus elemző segítségével észleli az objektumokban található ismeretlen vírusokat, és az ilyen objektumokat potenciálisan fertőzőtként jelöli meg.

## K

### KARANTÉN

Egy bizonyos mappa, amelybe a számítógép vizsgálata során vagy a valós idejű védelem által felismert potenciálisan fertőzött objektumok kerülnek.

### KASPERSKY SECURITY NETWORK

A Kaspersky Security Network (KSN) online szolgáltatások olyan infrastruktúrája, amely hozzáférést nyújt az Kaspersky Lab online tudásbázisához, ahonnan információkat szerezhet fájlok, webes erőforrások és szoftverek hírnevéről. A Kaspersky Security Network adatait felhasználva a Kaspersky Anti-Virus válaszsideje új típusú fenyegetésekkel találkozva rövidül, egyes védelmi összetevők teljesítménye nő, a vakriasztások kockázata pedig csökken.

### KÉT HÁLÓZATI ADAPTERREL ELLÁTOTT ÁTJÁRÓ

Olyan számítógép, amely két hálózati adapterrel rendelkezik (amelyek más-más hálózathoz kapcsolódnak), és a hálózatok között adatforgalmat bonyolít le.

### KIZÁRÁS

A kizárás egy olyan objektum, amelyre a Kaspersky Lab alkalmazás ellenőrzése nem terjed ki. Az ellenőrzésből kizárhatók bizonyos fájlformátumok, fájlmaszkok, de kizárhatók bizonyos területek (például mappák vagy programok), alkalmazásfolyamatok vagy objektumok is a Virus Encyclopedia besorolása szerinti fenyegetéstípusok alapján. Minden feladathoz hozzárendelhető egy bizonyos kizáráscsoport.

### KULCSFÁJL

A kulcsfájl egy .key kiterjesztéssel ellátott fájl, a felhasználó személyes „kulcsa”, amely a Kaspersky Lab alkalmazás használatához szükséges. Ha az alkalmazást a Kaspersky Lab forgalmazóitól vásárolta meg, a kulcsfájl a termék részét képezi. Ha online módon szerezte be, akkor pedig emailen kerül kiküldésre.

### KULCSFÁJLOK FEKETELISTÁJA

A feketelistán levő Kaspersky Lab kulcsfájlokkal kapcsolatos információkat tartalmazó adatbázis. A feketelista fájl tartalma a termék adatbázisaival együtt frissül.

**L****LICENC ÉRVÉNYESSÉGI IDEJE**

Az az időszak, amelyben a Kaspersky Lab alkalmazás valamennyi funkcióját használni tudja. A licenc érvényességi ideje általában a telepítés napjától számított egy év. A licenc lejártá után az alkalmazás korlátozott funkciókkal tovább használható. Az alkalmazás adatbázisai nem frissíthetők.

**M****MEGBÍZHATÓ FOLYAMAT**

Programfolyamat, amelynek a fájlműveleteit a Kaspersky Lab alkalmazása nem figyeli valós idejű védelemmel. Más szóval a megbízható folyamat által futtatott, megnyitott vagy mentett objektumok nem kerülnek ellenőrzésre.

**MEGBÍZHATÓ URL-EK LISTÁJA**

Azon webes erőforrások maszkjainak és címeinek listája, amelyek tartalmában a felhasználó megbízik. A Kaspersky Lab alkalmazása nem vizsgálja a rosszindulatú objektumok jelenlétét a lista elemeihez tartozó weboldalakon.

**MEMÓRIAFÁJL-KIÍRATÁS**

Egy folyamat munkamemóriájának vagy a rendszer teljes RAM-jának tartalma egy meghatározott időpontban.

**NY****NYOMKÖVETÉSEK**

Az alkalmazás futtatása hibakeresés módban; az alkalmazás minden egyes parancs végrehajtása után leáll, és megjelenik a lépés eredménye.

**O****OBJEKTUM BLOKKOLÁSA**

Objektumokhoz való hozzáférés megtagadása külső alkalmazásokból. A blokkolt objektum nem olvasható, nem hajtható végre, nem módosítható és nem törölhető.

**OBJEKTUM TÖRLÉSE**

Objektumok feldolgozási módja, amely annak fizikai törlésével végződik az eredeti helyéről (merevlemez, mappa, hálózati erőforrás). Javasoljuk ezen módszer alkalmazását azokra a veszélyes objektumokra, amelyek valamilyen okból nem vírusmentesíthetők.

**OBJEKTUMOK KARANTÉNBA HELYEZÉSE**

A potenciálisan fertőzött objektumok egyik feldolgozási módszere a fájlhoz való hozzáférés blokkolásával és az eredeti helyről a Karantén mappába való áthelyezésével, ahol az objektum titkosított formában – és ezáltal a fertőzés veszélyét kizáró módon – tárolódik.

**OBJEKTUMOK VÍRUSMENTESÍTÉSE**

A fertőzött objektumok feldolgozására használt módszer, amely az adatok teljes vagy részleges helyreállítását eredményezi, vagy eldönti, hogy az objektum nem vírusmentesíthető. Az objektumok vírusmentesítése az adatbázis bejegyzései alapján történik. A vírusmentesítés során részleges adatvesztés történhet.

**OBJEKTUMOK VÍRUSMENTESÍTÉSE ÚJRAINDÍTÁSKOR**

Olyan fertőzött objektumok esetén alkalmazott feldolgozási módszer, amelyeket a vírusmentesítés időpontjában más alkalmazások használnak. A művelet során a program másolatot készít a fertőzött fájlról, vírusmentesíti a létrehozott másolatot, majd a következő rendszerindításkor lecseréli az eredeti fertőzött fájlt a vírusmentesített másolatra.

**OBSZCÉN ÜZENET**

Sértő kifejezéseket tartalmazó email.

## OLE OBJEKTUM

Csatolt objektum vagy más fájlba beágyazott objektum. A Kaspersky Lab alkalmazása lehetővé teszi a víruskeresést az OLE-objektumokban. Ha például beilleszt egy Microsoft Office Excel táblázatot egy Microsoft Office Word dokumentumba, a program OLE-objektumként vizsgálja meg a táblázatot.

## P

### PARANCSFÁJL

A parancsfájl egy kis számítógépes program vagy egy program független eleme (funkciója), amely általában egy-egy apró feladat végrehajtására szolgál. Leggyakrabban hiperszövegbe ágyazott programokkal együtt kerül alkalmazásra. A parancsfájlok például akkor futnak le, amikor megnyit egy adott webhelyet.

Ha be van kapcsolva a valós idejű védelem, az alkalmazás figyel a parancsfájlok elindulását, elfogja és vírusellenőrzésnek veti alá azokat. A parancsfájl végrehajtása a vizsgálat eredményétől függően blokkolható vagy engedélyezhető.

### POTENCIÁLISAN FERTŐZÖTT OBJEKTUM

Egy ismert vírus módosított kódját vagy egy vírus kódjára hasonlító, de a Kaspersky Lab által még nem ismert kódot tartalmazó objektum. A potenciálisan fertőzött fájlok észlelése a heurisztikus elemző segítségével történik.

### POTENCIÁLISAN MEGFERTŐZHETŐ OBJEKTUM

Olyan objektum, amelyet szerkezetéből vagy formátumából adódóan a behatolók a rosszindulatú objektumok mentésére és terjesztésére szolgáló „tárolóként” használhatnak fel. Ezek általában futtatható fájlok, például .com, .exe, .dll stb. kiterjesztéssel. A rosszindulatú kódok ilyen fájlokba történő behatolásának kockázata meglehetősen magas.

### PROTOKOLL

Az ügyfél és a kiszolgáló közötti interakció irányítására szolgáló, egyértelműen definiált és szabványosított szabályrendszer. Néhány általánosan ismert protokoll és szolgáltatás: HTTP (WWW), FTP és NNTP (hírek).

### PROXYKISZOLGÁLÓ

A felhasználók által más hálózati szolgáltatásokhoz intézett közvetett kérélmeket lehetővé tevő számítógépes hálózati szolgáltatás. A felhasználó először egy proxykiszolgálóhoz csatlakozik, majd lekér egy olyan erőforrást (pl. egy fájlt), amely egy másik kiszolgálón található. Ezután a proxykiszolgáló vagy csatlakozik a megadott kiszolgálóhoz, és beszerzi tőle a kért erőforrást, vagy saját gyorsítótárából adja át az erőforrást (ha a proxy saját gyorsítótárral rendelkezik). Egyes esetekben a proxykiszolgáló bizonyos okokból módosítani tudja a felhasználó kérését vagy a kiszolgáló válaszát.

## R

### ROOTKIT

Alkalmazás vagy alkalmazások csoportja, amelyet egy behatoló vagy rosszindulatú program rendszerben található nyomainak álcázására fejlesztettek ki.

A Windows-alapú rendszereknél a rootkit általában olyan programot jelent, amely behatol a rendszerbe és elfogja a rendszerfunkciókat (Windows API). Az alacsony szintű API funkciók elfogása és módosítása révén ezek a programok nagyon kifinomult módon rejtik el jelenlétüket a rendszerben. Emellett egy rootkit általában más folyamatokat, a merevlemezen található fájlokat és mappákat, valamint rendszerleíró kulcsokat is elrejthet, ha ez van megadva a konfigurációjában. Számos rootkit saját illesztőprogramjait és szolgáltatásait is telepíti a rendszerbe (ezek szintén „láthatatlanok”).

## S

### SOCKS

Proxykiszolgálói protokoll, amelynek segítségével pont-pont kapcsolat hozható létre a belső és a külső hálózat számítógépei között.

### SÜRGŐS FRISSÍTÉSEK

A Kaspersky Lab alkalmazás moduljainak kritikus frissítései.

**T****TARTOMÁNYNÉV SZOLGÁLTATÁS (DNS)**

A gazdaeszköz (számítógép vagy más hálózati eszköz) nevét IP-címmé átalakító elosztott rendszer. A DNS szolgáltatás TCP/IP-hálózatokban működik. A DNS fordított irányú kérelmek tárolására és feldolgozására is alkalmas, és meghatározhatja a gazdaeszköz nevét az IP-cím alapján (PTR rekord). A DNS nevek feloldását általában nem a felhasználók, hanem hálózati alkalmazások végzik el.

**TELEPÍTÉS BEJELENTKEZÉSI PARANCSFÁJL HASZNÁLATÁVAL**

A Kaspersky Lab alkalmazásainak távoli telepítésére szolgáló módszer, amellyel a távoli telepítési feladat hozzárendelhető egy egyéni felhasználói fiókhoz (vagy több felhasználói fiókhoz). Ha egy felhasználót regisztrálnak egy tartományban, a rendszer megkísérli telepíteni az alkalmazást azon az ügyfélszámítógépen, amelyen a felhasználót regisztrálták. Ezt a módszert az alkalmazások Microsoft Windows 98 / Me operációs rendszereket futtató számítógépekre való telepítéséhez ajánlott használni.

**TÉVES RIASZTÁS**

Az az eset, amikor a Kaspersky Lab alkalmazása egy nem fertőzött objektumot fertőzöttnek tekint, mivel a kódja hasonló egy vírus kódjához.

**TOVÁBBI LICENC**

Olyan licenc, amelyet egy Kaspersky Lab alkalmazás használata érdekében nyilvántartásba vettek, de nem aktiváltak. A további licenc az aktív licenc lejárta után lép érvénybe.

**TÖMÖRÍTETT FÁJL**

Olyan fájlarchívum, amely a benne található kitömörítő programmal és utasításokkal segíti az operációs rendszert a végrehajtásban.

**V****VALÓS IDEJŰ VÉDELEM**

Az alkalmazás egyik működési módja, amelyben a rosszindulatú kódok objektumokban való keresése valós időben történik.

Az alkalmazás észlel az objektumok megnyitására (olvasás, írás vagy végrehajtás) irányuló minden kísérletet, és elvégzi az objektumok ellenőrzését. A nem fertőzött objektumokat átadja a felhasználónak, a fenyegetéseket tartalmazó vagy potenciálisan ilyennek vélt objektumokat pedig a beállításoknak megfelelően feldolgozza (vírusmentesítés, törlés vagy karanténba helyezés).

**VÉDELEM ÁLLAPOTA**

Az aktuális védelmi állapot, amely összefoglalja a számítógép biztonsági fokát.

**VESZÉLYES OBJEKTUM**

Vírust tartalmazó objektum. Ezekhez az objektumokhoz nem ajánlott hozzáférni, mert a számítógép fertőződését eredményezhetik. Ha fertőzött objektumot észlel, ajánlott azt vírusmentesíteni valamelyik Kaspersky Lab alkalmazással, vagy törölni, ha ez sikertelen.

**VÍRUSAKTIVITÁSI KÜSZÖB**

Egy bizonyos eseménytípus adott időszakon belüli maximális megengedett előfordulási száma, amelynek a túllépése esetén túlzott vírusaktivitásról és a víruskitörés veszélyéről beszélhetünk. Ennek a jellemzőnek víruskitörések alkalmával van kiemelt jelentősége; segítségével a rendszergazda időben reagálhat az esetlegesen fenyegető víruskitörésekre.

**VÍRUSKITÖRÉS**

Egy számítógép vírussal való megfertőzésére irányuló szándékos kísérletek sorozata.

**VÍRUSKITÖRÉS-SZÁMLÁLÓ**

A fenyegető víruskitörésekről generált értesítések alapját képező sablon. A víruskitörés-számláló tartalmazza a vírusaktivitási küszöböt, a terjedés módját és az elküldendő üzenetek szövegét meghatározó beállításokat.

## **VISSZAÁLLÍTÁS**

Egy eredeti objektum karanténból vagy másolattárolóból való áthelyezése arra a tárolási helyre, ahol az a karanténba helyezés, a vírusmentesítés, a törlés vagy a felhasználó által meghatározott mappába való áthelyezés előtt volt.

# KASPERSKY LAB ZAO

A Kaspersky Lab szoftvereit nemzetközi szinten is elismerik a vírusok, rosszindulatú programok, levélszemét, hálózati és hackertámadások és más fenyegetések elleni védelemben nyújtott teljesítményéért.

2008-ban a Kaspersky Lab bekerült a világ négy legnagyobb, a végfelhasználók számára adatvédelmi szoftvereket gyártó vállalata közé (IDC Worldwide Endpoint Security Revenue by Vendor). A COMCON „TGI-Russia 2009” felmérése szerint Oroszországban a Kaspersky Lab a számítógépes védelmi rendszerek első számú választása az otthoni felhasználók között.

A Kaspersky Labet 1997-ben alapították Oroszországban. Ma már egy moszkvai székhelyű nemzetközi cégcsoport, melynek öt regionális részlege a cég Oroszországban, Nyugat- és Kelet-Európában, a Közel-Keleten, Afrikában, Észak- és Dél-Amerikában, Japánban, Kínában és az ázsiai csendes-óceáni térség más országaiban végzett tevékenységét irányítja. A vállalat több, mint 2000 képzett szakembert alkalmaz.

**Termékek.** A Kaspersky Lab termékei minden rendszer számára védelmet nyújtanak, az otthoni számítógépektől a nagy vállalati hálózatokig.

Az egyéni felhasználók számára készített termékek között megtalálhatók az asztali, hordozható és kézisámítógépekre, valamint okostelefonokra és más mobileszközökre fejlesztett víruskereső alkalmazások.

A Kaspersky Lab munkaállomások, fájl- és webkiszolgálók, levelező átjárók és tűzfalak védelmét ellátó szoftvereket is fejleszt. A Kaspersky Lab központositott kezelőrendszerével együtt ezek a megoldások hatékony automatizált védelmet nyújtanak a cégek és szervezetek számára a számítógépes fenyegetések ellen. A Kaspersky Lab termékeit a legnagyobb tesztlaboratóriumok minősítették, számos számítógépes alkalmazásfejlesztő szoftvereivel kompatibilisek, és számos hardverplatformra optimalizálták működésüket.

A Kaspersky Lab vírusselemezői éjjel-nappal dolgoznak. Mindennap több ezer új számítógépes fenyegetést fedeznek fel, eszközöket fejlesztenek ezek felismerésére és ártalmatlanítására, és hozzáadják ezeket a Kaspersky Lab alkalmazásai által használt adatbázisokhoz. *A Kaspersky Lab víruskereső adatbázisai óránként frissülnek, a Levélszemét-blokkoló adatbázis pedig ötpercenként.*

**Technológiák.** Több, a modern víruskereső eszközök szerves részét képező technológiát eredetileg a Kaspersky Lab fejlesztett ki. Nem véletlen, hogy jó néhány fejlesztő a Kaspersky Anti-Virus kernelét használja saját termékeiben. Ilyenek többek között: SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Izrael), Clearswift (Egyesült Királyság), CommuniGate Systems (USA), Critical Path (Írország), D-Link (Tajvan), M86 Security (USA), GFI (Málta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), NETASQ (Franciaország), NETGEAR (USA), Parallels (Oroszország), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Tajvan). A vállalat számos innovatív technológiáját szabadalmaztatta.

**Eredmények.** Az évek során a Kaspersky Lab a számítógépes fenyegetések elleni küzdelemhez biztosított szolgáltatásaival díjak és egyéb elismerések százait nyerte el. 2010-ben például a Kaspersky Anti-Virus több kimagasló Advanced+ elismerést kapott az elismert osztrák vírusvédelmi laboratórium, az AV-Comparatives által végzett tesztorozatban. De a Kaspersky Lab számára a legnagyobb elismerést a felhasználók töretlen hűsége jelenti. A vállalat termékei és technológiái több, mint 300 millió felhasználót védenek, a vállalati ügyfeleinek száma pedig meghaladja a 200 000-et.

A Kaspersky Lab hivatalos honlapja:

<http://www.kaspersky.hu>

Vírus Encyclopedia:

<http://www.securelist.com>

Víruskereső laboratórium:

newvirus@kaspersky.com (csak a valószínűleg fertőzött fájlok küldésére tömörített formátumban)

<http://support.kaspersky.com/virlab/helpdesk.html> (a vírusselemezőinknek küldött kérdések számára)

A Kaspersky Lab webes fóruma:

<http://forum.kaspersky.com>

# A HARMADIK FÉLTŐL SZÁRMAZÓ KÓDRA VONATKOZÓ INFORMÁCIÓK

A harmadik féltől származó kódra vonatkozó információkat az alkalmazás telepítési mappájában található legal\_notices.txt fájl tartalmazza.

# TÁRGYMUTATÓ

## A

A helyi menü .....	28
Adathalász webcímek adatbázisa	
IM víruskereső .....	83
Webes víruskereső .....	79
Alapértelmezett beállítások visszaállítása .....	49
Alkalmazás elérésének korlátozása .....	56
Alkalmazás önvédelme .....	95
Az alkalmazás főablaka .....	29

## B

Biztonsági szint	
Fájl víruskereső .....	70
Levél víruskereső .....	78
Webes víruskereső .....	78
Böngészőbeállítás .....	100

## E

EICAR .....	109
Eltávolítás	
alkalmazás .....	23
Értesítések .....	40
értesítések emailben .....	107
értesítések típusai .....	107
hangjelzés letiltása .....	107
letiltás .....	106

## F

Fájl víruskereső	
biztonsági szint .....	70
felfüggesztés .....	68
heurisztikus elemzés .....	71
összetett fájlok vizsgálata .....	71
teendő fenyegetés esetén .....	71
védelem hatóköre .....	69
vizsgálati mód .....	70
vizsgálati technológia .....	71
vizsgálatoptimalizáció .....	72
Frissítés	
frissítés helyi mappából .....	65
frissítésforrás .....	64
legutolsó frissítés visszagörgetése .....	66
proxykiszolgáló .....	67
területi beállítások .....	65

## H

Hálózat	
figyelt portok .....	89
titkosított kapcsolatok .....	87
Helyreállító-lemez .....	46
Heurisztikus elemzés	
Fájl víruskereső .....	71
Levél víruskereső .....	75
Webes víruskereső .....	81

**I**

Ikon a tálca értesítési területén .....	27
IM víruskereső	
adathalász webcímek adatbázisa .....	83
védelem hatóköre .....	83

**J**

Jelentések	
események keresése .....	103
megtekintés .....	49
mentés fájlba .....	104
összetevő vagy feladat kiválasztása .....	102
szűrés .....	103

**K**

Karantén és másolatok .....	95
Kaspersky URL-tanácsadó	
Webes víruskereső .....	79

**L**

Levél víruskereső	
biztonsági szint .....	78
heurisztikus elemzés .....	75
mellékletek szűrése .....	75
összetett fájlok vizsgálata .....	76
teendő fenyegetés esetén .....	75
védelem hatóköre .....	74
Licenc	
alkalmazás aktiválása .....	38
Végfelhasználói licencszerződés .....	25
Licenc megújítása .....	39

**M**

Megbízható zóna	
kizárási szabályok .....	91
megbízható alkalmazások .....	91

**N**

Nyomkövetések	
nyomkövetési eredmények feltöltése .....	113
nyomkövetési fájl létrehozása .....	113

**P**

Proaktív védelem	
megbízható alkalmazások csoportja .....	84
veszélyes tevékenység figyelési szabálya .....	85
veszélyes tevékenységek listája .....	85

**S**

Számítógép hatékonysága .....	93
-------------------------------	----

**T**

Teendő fenyegetés esetén	
Fájl víruskereső .....	71
Levél víruskereső .....	75
víruskeresés .....	60
Webes víruskereső .....	79
Telepítési mappa .....	17

## Ü

Ütemezés	
frissítés .....	66
víruskeresés .....	59

## V

Valós idejű védelem engedélyezése / tiltása .....	36
Védelem hatóköre	
Fájl víruskereső .....	69
IM víruskereső .....	83
Levél víruskereső .....	74
Webes víruskereső .....	82
Virtuális billentyűzet .....	43
Vizsgálat	
az észlelt objektummal kapcsolatban elvégzendő művelet .....	60
biztonsági szint .....	58
fiók .....	61
kihagyott feladat automatikus indítása .....	59
összetett fájlok vizsgálata .....	61
sebezhetőségi vizsgálat .....	63
ütemezés .....	59
vizsgálandó objektumok típusa .....	61
vizsgálati technológiák .....	60
vizsgálatoptimalizáció .....	62

## W

Webes víruskereső	
adathalász webcímek adatbázisa .....	79
biztonsági szint .....	78
heurisztikus elemzés .....	81
Kaspersky URL-tanácsadó .....	79
teendő fenyegetés esetén .....	79
védelem hatóköre .....	82
vizsgálatoptimalizáció .....	81