

**POUŽÍVATEL'SKÁ
PRÍRUČKA**

**KASPERSKY
INTERNET
SECURITY 2009**

Vážení používateľa produktu Kaspersky Internet Security 2009!

Ďakujeme, že ste si zvolili náš produkt. Dúfame, že vám táto dokumentácia pomôže pri práci a poskytne odpovede ohľadne tohto softvérového produktu.

Upozornenie! Tento dokument je vlastníctvom spoločnosti Kaspersky Lab a všetky práva k tomuto dokumentu sú vyhradené v súlade s autorským právom Ruskej federácie a medzinárodnými zmluvami. Nezákonné rozmnožovanie a šírenie tohto dokumentu alebo jeho častí vedie k občianskoprávnej, správnej alebo trestnoprávnej zodpovednosti podľa práva Ruskej federácie. Rozmnožovanie a šírenie akýchkoľvek materiálov, vrátane ich prekladu, je možné len s písomným súhlasom spoločnosti Kaspersky Lab. Tento dokument a súvisiace grafické prvky možno použiť len pre informáciu alebo na nekomerčné či osobné účely.

Tento dokument môže byť zmenený bez predchádzajúceho oznámenia. Najnovšiu verziu tohto dokumentu nájdete na webe spoločnosti Kaspersky Lab na adrese <http://www.kaspersky.com/docs>. Spoločnosť Kaspersky Lab v žiadnom prípade nezodpovedá za obsah, kvalitu, významnosť alebo presnosť materiálov použitých v tomto dokumente, ku ktorým majú práva tretie strany, ani za potenciálne škody spojené s použitím takýchto dokumentov.

Tento dokument obsahuje registrované a neregistrované ochranné známky. Všetky uvedené ochranné známky sú majetkom príslušných vlastníkov.

© Kaspersky Lab, 1996-2008

+7 (495) 645-7939,
Tel., fax: +7 (495) 797-8700,
+7 (495) 956-7000

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

Dátum revízie: 29 apríla 2008

OBSAH

ÚVOD	6
Získanie informácií o aplikácii	6
Zdroje informácií pre samostatné vyhľadávanie.....	6
Kontaktovanie oddelenia predaja	7
Kontaktovanie služby technickej podpory	7
Diskusia o aplikáciách spoločnosti Kaspersky Lab na webovom fóre	9
Novinky v produkte Kaspersky Internet Security 2009	9
Konceptia ochrany	11
Sprievodcovia a nástroje	12
Podporné funkcie	13
Heuristická analýza	14
Hardvérové a softvérové systémové požiadavky.....	15
HROZBY PRE BEZPEČNOSŤ POČÍTAČA.....	16
Škodlivé aplikácie.....	16
Škodlivé programy	17
Vírusy a červy.....	17
Trójske kone.....	20
Škodlivé utility.....	26
Potenciálne nežiaduce programy	30
Adware.....	31
Pornware.....	31
Iný riskware	32
Spôsoby detekcie napadnutých, podozrivých a potenciálne nebezpečných objektov.....	36
Internetové hrozby.....	36
Nevyžiadaná prichádzajúca pošta – Spam	37
Phishing	37
Útoky hackerov	38
Zobrazenie reklamných líšt.....	38
INŠTALÁCIA APLIKÁCIE NA POČÍTAČ	40
Krok 1. Vyhľadanie novej verzie aplikácie.....	41

Krok 2. Overenie, že systém spĺňa požiadavky na inštaláciu	42
Krok 3. Prívetacie okno sprievodcu	42
Krok 4. Zobrazenie licenčnej zmluvy	42
Krok 5. Výber typu inštalácie.....	43
Krok 6. Výber inštaláčnej zložky.....	43
Krok 7. Výber súčastí aplikácie na inštaláciu	44
Krok 8. Vyhľadanie iného antivírusového softvéru.....	45
Krok 9. Konečná príprava na inštaláciu	45
Krok 10. Dokončenie inštalácie	46
ROZHRANIE APLIKÁCIE.....	47
Ikona v oznamovacej oblasti	47
Miestna ponuka.....	48
Hlavné okno aplikácie.....	50
Upozornenie.....	53
Konfiguračné okno aplikácie	53
ZAČÍNAME.....	54
Výber typu siete	55
Aktualizácia aplikácie.....	56
Analýza bezpečnosti.....	56
Antivírusová kontrola počítača	57
Zapojenie sa do systému Kaspersky Security Network	57
Správa zabezpečenia	59
Pozastavenie ochrany	61
OVERENIE NASTAVENIA APLIKÁCIE.....	63
Testovací „vírus“ EICAR a jeho varianty	63
Testovanie ochrany dátového toku HTTP	66
Testovanie ochrany dátového toku SMTP	67
Overenie nastavenia súčasti File Anti-Virus.....	68
Overenie nastavenia úlohy antivírusovej kontroly.....	68
Overenie nastavenia súčasti Anti-Spam	69

KASPERSKY SECURITY NETWORK – VYHLÁSENIE O ZHROMAŽĎOVANÍ DÁT	70
KASPERSKY LAB	76
Ďalšie produkty spoločnosti Kaspersky Lab	77
Obráťte sa na nás	87
CRYPTOEX LLC	89
MOZILLA FOUNDATION	90
LICENČNÁ ZMLUVA	91

ÚVOD

V TOMTO ODDIELI:

Získanie informácií o aplikácii.....	6
Novinky v produkte Kaspersky Internet Security 2009	9
Koncepcia ochrany	11
Hardvérové a softvérové systémové požiadavky.....	15

ZÍSKANIE INFORMÁCIÍ O APLIKÁCIÍ

Pokiaľ máte akúkoľvek otázku týkajúcu sa nákupu, inštalácie alebo používania aplikácie, môžete na ňu ľahko dostať odpoveď.

Spoločnosť Kaspersky Lab má množstvo informačných zdrojov a vy si môžete zvoliť ten najvhodnejší podľa toho, aká je vaša otázka naliehavá a závažná.

ZDROJE INFORMÁCIÍ PRE SAMOSTATNÉ VYHLADÁVANIE

Môžete použiť systém nápovedy.

Systém nápovedy obsahuje informácie o správe bezpečnosti počítača: zobrazenie stavu ochrany, kontroly rôznych oblastí počítača a vykonávanie ďalších úloh.

Ak chcete otvoriť nápovedu, klepnite na odkaz **Nápoveda** v hlavnom okne aplikácie, alebo stlačte kláves <F1>.

KONTAKTOVANIE ODDELENIA PREDAJA

Ak máte otázku týkajúcu sa výberu či kúpy aplikácie alebo predĺženie obdobia jej používania, môžete sa telefonicky obrátiť na špecialistov obchodného oddelenia v hlavnom sídle našej spoločnosti v Moskve na čísle:

+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00.

Táto služba sa poskytuje v ruštine alebo angličtine.

Svoje otázky pre oddelenie predaja môžete zasielať na e-mailovú adresu sales@kaspersky.com.

KONTAKTOVANIE SLUŽBY TECHNICKEJ PODPORY

Pokiaľ ste si aplikáciu už zakúpili, môžete o nej získať informácie od služby technickej podpory telefonicky alebo cez internet.

Špecialisti technickej podpory odpovedia na vaše otázky týkajúce sa inštalácie a používania aplikácie, a pokiaľ bol váš počítač napadnutý, pomôžu vám odstrániť následky činnosti škodlivého softvéru.

Pred kontaktovaním služby technickej podpory si prosím prečítajte pravidlá podpory (<http://support.kaspersky.com/support/rules>).

E-mail s požiadavkou na službu technickej podpory (len pre registrovaných používateľov)

Otázky môžete špecialistom technickej podpory klásť tak, že vyplníte webový formulár (<http://support.kaspersky.com/helpdesk.html>).

Svoju otázku môžete poslať v ruštine, angličtine, nemčine, francúzštine alebo španielčine.

Ak chcete poslať e-mail s otázkou, musíte uviesť svoje **klientske číslo**, ktoré ste získali pri registrácii na internetovej stránke služby technickej podpory, spolu so svojím **heslom**.

Poznámka

Pokiaľ ešte nie ste registrovaným používateľom aplikácií spoločnosti Kaspersky Lab, môžete vyplniť registračný formulár (<https://support.kaspersky.com/en/PersonalCabinet/Registration/Form/>). Pri registrácii budete musieť uviesť aktivačný kód alebo názov súboru s kľúčom.

Odpoveď špecialistu technickej podpory na vašu požiadavku obdržíte pomocou služby **Personal Cabinet** (<https://support.kaspersky.com/en/PersonalCabinet>) a e-mailom na adresu, ktorú ste v požiadavke uviedli.

Vo webovom formulári čo najpodrobnejšie opíšte vzniknutý problém. Do povinne vyplňovaných polí zadajte tieto údaje:

- **Typ otázky.** Otázky, ktoré používatelia kladú najčastejšie, sú zoskupené do osobitných tém, napríklad „Product installation/removal problem“ (problém s inštaláciou/odstránením produktu) alebo „Virus scan/removal problem“ (problém s kontrolou/odstránením vírusov). Pokiaľ ste nenašli zodpovedajúcu tematickú skupinu, zvolte „General Question“ (všeobecná otázka).
- **Názov aplikácie a číslo verzie.**
- **Text otázky.** Opíšte čo najpodrobnejšie problém, ktorý nastal.
- **Klientske číslo a heslo.** Zadajte klientske číslo a heslo, ktoré ste obdržali pri registrácii na webe služby technickej podpory.
- **E-mailová adresa.** Špecialisti technickej podpory vám na túto adresu pošlú odpoveď na vašu otázku.

Technická podpora po telefóne

Ak máte problém, ktorý si vyžaduje rýchlu pomoc, môžete zatelefonovať najbližšej dostupnej službe technickej podpory. Nezapodnite prosím uviesť potrebné informácie (<http://support.kaspersky.com/support/details>), ak budete kontaktovať ruskú (http://support.kaspersky.com/support/support_local) alebo medzinárodnú (<http://support.kaspersky.com/support/international>) technickú podporu. Pomôžete tak našim špecialistom požiadavku čo najrýchlejšie spracovať.

DISKUSIA O APLIKÁCIÁCH SPOLOČNOSTI KASPERSKY LAB NA WEBOVOM FÓRE

Pokiaľ vaša otázka nevyžaduje rýchlu odpoveď, môžete ju prediskutovať so špecialistami spoločnosti Kaspersky Lab a ostatnými používateľmi antivírusových aplikácií spoločnosti Kaspersky Lab na našom webovom fóre, ktoré sa nachádza na adrese <http://forum.kaspersky.com>.

Na fóre si môžete prezrieť už skôr publikované témy, písať komentáre, vytvárať nové témy a použiť vyhľadávač.

NOVINKY V PRODUKTE KASPERSKY INTERNET SECURITY 2009

Produkt Kaspersky Internet Security 2009 predstavuje celkom nový prístup k zabezpečeniu dát. Hlavnou funkciou aplikácie je obmedzenie práv programov pristupovať k systémovým prostriedkom. To pomáha brániť nežiaducim akciám podozrivých a nebezpečných programov. Výrazne boli rozšírené schopnosti aplikácie chrániť dôverné dáta používateľa. Aplikácia teraz obsahuje sprievodcov a nástroje, ktoré značne uľahčujú vykonávanie konkrétnych úloh ochrany počítača.

Pozrime sa bližšie na nové funkcie aplikácie Kaspersky Internet Security 2009:

Nové funkcie ochrany

- Aplikácia Kaspersky Internet Security teraz zahŕňa súčasť Filtrovanie aplikácií, ktorá spoločne s proaktívnou ochranou a bránou firewall realizuje nový a univerzálny prístup na ochranu systému pred akoukoľvek hrozbou, vrátane existujúcich hrozieb i hrozieb, ktoré v tejto chvíli ešte nie sú známe. Vďaka zoznamom dôveryhodných aplikácií teraz Aplikácia Kaspersky Internet Security od používateľa vyžaduje výrazne menej vstupov.
- Kontrola a následná eliminácia zraniteľných miest operačného systému a softvéru udržuje vysokú úroveň zabezpečenia systému a bráni prenikaniu nebezpečných programov do vášho systému.
- Noví sprievodcovia – Analýza bezpečnosti a Konfigurácia prehliadača – uľahčujú kontrolu a elimináciu bezpečnostných hrozieb a zraniteľností

v aplikáciách inštalovaných na vašom počítači, v operačnom systéme a v nastavení prehliadača.

- Spoločnosť Kaspersky Lab teraz rýchlejšie reaguje na nové hrozby vďaka použitiu technológie Kaspersky Security Network, ktorá zhromažďuje údaje o nákazách počítačov používateľov a odosiela ich na servery spoločnosti.
- Nové nástroje – Sledovanie siete a Analýza sieťových balíčkov – uľahčujú zhromažďovanie a analýzu informácií o sieťových aktivitách na vašom počítači.
- Nový sprievodca – Obnovenie systému – pomáha opraviť poškodenie systému po útoku škodlivého softvéru.

Nové funkcie ochrany dôverných dát:

- Nová súčasť Filtrovanie aplikácií účinne monitoruje prístupy aplikácií k dôverným údajom, súborom a zložkám používateľa.
- Nový nástroj – Virtuálna klávesnica – zaisťuje bezpečnosť dôverných dát zadávaných z klávesnice.
- Štruktúra aplikácie Kaspersky Internet Security zahŕňa sprievodcu vymazávaním osobných údajov, ktorý z počítača odstráni všetky informácie o činnosti používateľa, ktoré by mohli byť zaujímavé pre votrelca (zoznam navštívených webových stránok, otvorené súbory, súbory cookie atď.).

Nové antispamové funkcie:

- Účinnosť filtrovania spamu pomocou súčasti Anti-Spam bola zlepšená vďaka použitiu serverových technológií Recent Terms.
- Rozširujúce moduly plug-in pre Microsoft Office Outlook, Microsoft Outlook Express, The Bat! a Thunderbird zjednodušujú proces konfigurácie nastavenia antispamu.
- Prepracovaná súčasť Rodičovská kontrola umožňuje účinne obmedziť nežiaduci prístup detí k niektorým internetovým zdrojom.

Nové ochranné funkcie na používanie internetu:

- Ochrana pred internetovými votrelcami bola zmodernizovaná vďaka rozšíreným databázam podvodných (phishing) stránok.
- Bola doplnená kontrola dátových tokov ICQ a MSN, ktorá zaisťuje bezpečné používanie internetových programov pre rýchle správy.

- Kontrola pripojenia Wi-Fi zaručuje bezpečnosť pri používaní bezdrôtových sietí.

Nové funkcie rozhrania programu:

- Nové rozhranie aplikácie odráža ucelený prístup k ochrane informácií.
- Vysoká informačná kapacita dialógových okien pomáha používateľovi rýchlo sa rozhodovať.
- Bola rozšírená funkcia správ a štatistických údajov o činnosti aplikácie. Pri práci so správami možno použiť filtre s flexibilným nastavením, vďaka ktorým je tento produkt nenahraditeľný pre profesionálov.

KONCEPCIA OCHRANY

Aplikácia Kaspersky Internet Security zaisťuje ochranu počítača pred známymi i novými hrozbami, útokmi hackerov a votrelcov, spamom a ďalšími nežiaducimi dátami. Jednotlivé typy hrozieb sa spracovávajú samostatnými súčasťami aplikácie. Vďaka tejto štruktúre je nastavenie flexibilné a súčasťou je možné ľahko konfigurovať, aby vyhovovali potrebám konkrétneho používateľa alebo celého podniku.

Produkt Kaspersky Internet Security zahŕňa:

- Monitorovanie činnosti aplikácií v systéme, ktoré aplikáciám bránia vo vykonávaní nebezpečných akcií.
- Súčasť ochrany pred škodlivým softvérom, ktoré poskytujú neustálu ochranu všetkých dátových prenosov a prístupových ciest do počítača.
- Súčasť na ochranu pri práci s internetom, ktoré zaisťujú ochranu počítača pred známymi sieťovými útokmi a útokmi votrelcov.
- Súčasť pre filtrovanie nežiaducich dát, ktoré pomáhajú šetriť čas, prenesené dáta i peniaze.
- Úlohy antivírusovej kontroly, ktoré kontrolujú prípadné vírusy v jednotlivých súboroch, zložkách, diskoch a oblastiach alebo vykonávajú kompletnú kontrolu počítača. Úlohy kontroly možno nakonfigurovať, aby zisťovali zraniteľnosti v aplikáciách, ktoré sú na počítači nainštalované.
- Aktualizácie, ktoré zaisťujú stabilitu vnútorných aplikačných modulov a taktiež slúžia na detekciu hrozieb, útokov hackerov a spamu.

- Sprievodca a nástroje, ktoré uľahčujú vykonávanie úloh v rámci činnosti aplikácie Kaspersky Internet Security.
- Podporné funkcie, ktoré poskytujú informačnú podporu pre prácu s aplikáciou a rozširovanie ich schopností.

SPRIEVODCOVIA A NÁSTROJE

Zaistenie bezpečnosti počítača je pomerne obtiažna úloha, ktorá vyžaduje znalosť vlastností operačného systému i spôsobov používaných na zneužitie jeho slabých miest. Navyše veľké množstvo a rôznorodosť informácií o zabezpečení systému robí analýzu a spracovanie ešte ťažšími.

Aplikácia Kaspersky Internet Security uľahčuje vykonávanie konkrétnych úloh zabezpečenia počítača pomocou radu sprievodcov a nástrojov:

- Sprievodca analýzou bezpečnosti vykonáva diagnostiku počítača a hľadá zraniteľnosti v operačnom systéme a v programoch, ktoré sú na počítači nainštalované.
- Sprievodca konfiguráciou prehliadača analyzuje nastavenia prehliadača Microsoft Internet Explorer a vyhodnocuje ich predovšetkým z hľadiska bezpečnosti.
- Sprievodca obnovením systému slúži na odstránenie následkov prítomnosti škodlivých objektov v systéme.
- Sprievodca vymazávaním osobných údajov vyhľadáva a eliminuje záznamy o činnosti používateľa v systéme a tiež nastavenia operačného systému, ktoré umožňujú zhromažďovať informácie o činnosti používateľa.
- Záchranný disk je určený na obnovenie funkcií systému potom, čo útok vírusu poškodil súbory operačného systému a systém nemožno spustiť.
- Analýza sieťových balíčkov zachytáva sieťové pakety a zobrazuje o nich podrobnosti.
- Sledovanie siete zobrazuje podrobnosti o sieťovej aktivite vášho počítača.
- Virtuálna klávesnica umožňuje zabrániť zachytenie dát zadávaných z klávesnice.

PODPORNÉ FUNKCIE

Aplikácia obsahuje celý rad podporných funkcií. Slúžia na to, aby aplikáciu udržiavali aktuálnu, rozšírili jej schopnosti a pomáhali vám pri jej používaní.

Kaspersky Security Network

Kaspersky Security Network – systém, ktorý automaticky odosiela správy o zistených a potenciálnych hrozbách do centralizovanej databázy. Databáza zaisťuje ešte rýchlejšiu reakciu na najbežnejšie hrozby a upozornenie používateľov na vírusové epidémie.

Licencia

Zakúpením aplikácie Kaspersky Internet Security uzatvárate so spoločnosťou Kaspersky Lab licenčnú zmluvu, ktorou sa po určené obdobie riadi používanie aplikácie, ako aj váš prístup k aktualizáciám databáz aplikácie a službám technickej podpory. Podmienky používania a ďalšie informácie potrebné na plnú funkčnosť aplikácie sú poskytované v súbore s kľúčom.

Pomocou funkcie **Licencia** môžete získať podrobnosti o licencii, ktorú používate, zakúpiť novú licenciu alebo obnoviť svoju pôvodnú licenciu.

Podpora

Všetci registrovaní používatelia aplikácie Kaspersky Internet Security môžu využívať naše služby technickej podpory. Ak chcete zistiť, kde presne môžete získať technickú podporu, použite funkciu Podpora.

Pomocou príslušných odkazov môžete navštíviť diskusné fórum používateľov produktov firmy Kaspersky Lab alebo vyplniť špeciálny online formulár na zaslanie správy o chybe technickej podpore či zaslanie spätnej väzby ohľadne aplikácie.

Taktiež máte prístup k online službe technickej podpory „Personal Cabinet“ a naši zamestnanci vám vždy radi poskytnú podporu pre aplikáciu Kaspersky Internet Security po telefóne.

HEURISTICKÁ ANALÝZA

Heuristiky sa používajú pri niektorých súčiastiach na ochranu v reálnom čase, ako napríklad File Anti-Virus, Mail Anti-Virus a Web Anti-Virus, a pri antivírusovej kontrole.

Kontrola pomocou metód signatúr s vopred vytvorenou databázou, ktorá obsahuje opis známych hrozieb a metód ich dezinfekcie, vám samozrejme poskytne konečnú odpoveď na otázku, či je kontrolovaný objekt škodlivý a do ktorej triedy nebezpečných programov patrí. Heuristická analýza sa na rozdiel od detekcie signatúr škodlivého kódu zameriava na zisťovanie určitého typického správania sa škodlivých programov, ktoré umožňuje skúmaný súbor posúdiť s určitou pravdepodobnosťou.

Výhodou heuristickej analýzy je, že pred kontrolou nemusíte aktualizovať databázu. Vďaka tomu sú nové hrozby zistené skôr, než sa s nimi stretnú analytici vírusov.

Existujú však metódy, ako heuristické postupy obísť. Jedným z takýchto obranných opatrení je zmrazenie aktivity škodlivého kódu vo chvíli, keď je zistená heuristická kontrola.

Poznámka

Použitie kombinácie rôznych metód kontroly zaisťuje väčšiu bezpečnosť.

V prípade možnej hrozby heuristický analyzátor simuluje beh objektu v zabezpečenom virtuálnom prostredí aplikácie. Pokiaľ je odhalená podozrivá aktivita, objekt sa považuje za škodlivý a na počítači nebude povolené jeho spustenie, alebo sa zobrazí správa s požiadavkou na ďalšie pokyny od používateľa:

- Presunúť novú hrozbu do Karantény, aby mohla byť skontrolovaná a spracovaná neskôr s použitím aktualizovaných databáz
- Odstrániť objekt
- Preskočiť (pokiaľ ste si istí, že je tento objekt neškodný).

Ak chcete použiť heuristickú metódu, zaškrtnite voľbu **Použiť heuristickú analýzu**. Na to posuňte posuvník do jednej z týchto polôh: Rýchla, Stredná, alebo Dôkladná. Úroveň podrobnosti kontroly umožňuje voliť kompromis medzi dôkladnosťou a teda kvalitou kontroly nových hrozieb a záťažou systémových prostriedkov i časom trvania kontroly. Čím vyššiu úroveň heuristickej analýzy nastavíte, tým viac systémových prostriedkov a času bude kontrola potrebovať.

Upozornenie!

Nové hrozby zistené pomocou heuristickej analýzy spoločnosť Kaspersky Lab rýchlo analyzuje a postupy pre ich dezinfekciu pridáva do aktualizácií databázy.

Pokiaľ pravidelne aktualizujete svoje databázy, získate optimálnu úroveň ochrany vášho počítača.

HARDVÉROVÉ A SOFTVÉROVÉ SYSTÉMOVÉ POŽIADAVKY

Na zaistenie normálnej funkcie aplikácie musí počítač spĺňať nasledujúce minimálne požiadavky:

Všeobecné požiadavky:

- 75 MB voľného miesta na pevnom disku.
- Jednotka CD-ROM (na inštaláciu aplikácie z inštaláčného CD).
- Myš.
- Prehliadač Microsoft Internet Explorer 5.5 alebo vyšší (na aktualizáciu databáz a softvérových modulov aplikácie prostredníctvom internetu).
- Inštaláčná služba Microsoft Windows Installer 2.0.

Microsoft Windows XP Home Edition (SP2 alebo vyšší), Microsoft Windows XP Professional (SP2 alebo vyšší), Microsoft Windows XP Professional x64 Edition:

- Procesor Intel Pentium 300 MHz alebo vyšší (alebo kompatibilný ekvivalent).
- 256 MB voľnej pamäte RAM.

Microsoft Windows Vista Starter x32, Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate:

- 32-bitový (x86) alebo 64-bitový (x64) procesor Intel Pentium 800 MHz alebo vyšší (alebo kompatibilný ekvivalent).
- 512 MB voľnej pamäte RAM.

HROZBY PRE BEZPEČNOSŤ POČÍTAČA

Vážnou hrozbu pre bezpečnosť počítača predstavujú škodlivé aplikácie. Hrozbou je tiež spam, podvody (phishing), útoky hackerov, adware a reklamné lišty. Tieto hrozby súvisia s používaním internetu.

V TOMTO ODDIELI:

Škodlivé aplikácie	16
Internetové hrozby	36

ŠKODLIVÉ APLIKÁCIE

Aplikácia spoločnosti Kaspersky Lab dokáže zistiť stotisíce škodlivých programov, ktoré sa vo vašom počítači môžu nachádzať. Niektoré z týchto programov predstavujú pre váš počítač väčšiu hrozbu, iné sú nebezpečné len za určitých podmienok. Potom, ako aplikácia zistí škodlivú aplikáciu, zaradí ju do kategórie a priradí jej úroveň nebezpečenstva (vysokú alebo strednú).

Analytici vírusov v spoločnosti Kaspersky Lab rozlišujú dve hlavné kategórie: *škodlivé programy a potenciálne nežiaduce programy*.

Škodlivé programy (pozrite na strane 17) (Malware) sú vytvorené so zámerom poškodiť počítač a jeho používateľa, napríklad odcudziť, zablokovať, pozmeniť či vymazať informácie alebo narušiť činnosť počítača či počítačovej siete.

Potenciálne nežiaduce programy (pozrite na strane 30) (PUPs) oproti škodlivým programom neslúžia len na páchanie škôd.

Vírusová encyklopédia (<http://www.viruslist.com/en/viruses/encyclopedia>) obsahuje podrobný opis týchto programov.

ŠKODLIVÉ PROGRAMY

Škodlivé programy boli vytvorené špeciálne na to, aby poškodzovali počítače a ich používateľov: odcudzili, blokovali, zmenili alebo mazali informácie, narušovali činnosť počítačov alebo počítačových sietí.

Škodlivé programy sa delia do troch podkategórií: *vírusy a červy*, *trójske kone* a *škodlivé utility*.

Vírusy a červy (pozrite na strane 17) (*Viruses_and_Worms*) dokážu sa samy kopírovať a kópie majú opäť schopnosť samy sa kopírovať. Niektoré sa spúšťajú bez toho, že by o tom používateľ vedel či sa na ich spúšťaní akokoľvek podieľal, iné potrebujú pre svoje spustenie aktivitu používateľa. Tieto programy vykonávajú svoju škodlivú činnosť, keď sú spustené.

Trójske kone (pozrite na strane 20) (*Trojan_programs*) oproti červom a vírusom sa samy nekopírujú. Preniknú do počítača napríklad prostredníctvom e-mailu alebo cez webový prehliadač, keď používateľ navštívi „infikovanú“ stránku. Na ich spustení sa musí podieľať používateľ a po spustení začnú vykonávať svoje škodlivé akcie.

Škodlivé utility (pozrite na strane 26) (*Malicious_tools*) sú vytvorené špeciálne na to, aby páchali škody. Na rozdiel od ostatných škodlivých programov však nevykonávajú škodlivú činnosť ihneď po spustení a môžu byť na používateľovom počítači bezpečne uložené a spúšťané. Tieto programy disponujú funkciami na vytváranie vírusov, červov a trójskych koní, organizovanie sieťových útokov na vzdialené servery, hackovanie počítačov alebo na iné škodlivé aktivity.

VÍRUSY A ČERVY

Podkategórie: vírusy a červy (*Viruses_and_Worms*)

Úroveň závažnosti: vysoká

Klasické vírusy a červy vykonávajú na počítači činnosti bez dovoľenia používateľa a môžu sa samy kopírovať, pričom kópie sa môžu opäť samy kopírovať.

Klasický vírus

Akonáhle klasický vírus prenikne do systému, infikuje súbor, aktivuje sa v ňom, vykoná svoju škodlivú akciu a potom pripojí svoje kópie k ďalším súborom.

Klasické vírusy sa množia len na lokálnych prostriedkoch určitého počítača, nemôžu samy preniknúť do iných počítačov. Iné počítače môžu napadnúť len v prípade, že pridajú svoju kópiu do súboru uloženého v zdieľanej zložke či na disku CD, alebo pokiaľ používateľ prepošle e-mailovú správu s infikovanou prílohou.

Kód klasického vírusu môže preniknúť do rôznych oblastí počítača, operačného systému alebo aplikácie. Podľa prostredia sa rozlišujú *súborové vírusy*, *vírusy v záväzacom sektore*, *skriptové vírusy* a *makrovírusy*.

Vírusy môžu infikovať súbory rôznymi spôsobmi. Prepisujúce vírusy zapíšu svoj kód tak, že nahradia kód súboru, ktorý infikujú, takže zničia obsah takéhoto súboru. Nakazený súbor prestane fungovať a nie je možné ho dezinfikovať. *Parazitujúce vírusy* pozmenia súbory a ponechajú ich plne alebo čiastočne funkčné. *Spríevodné vírusy* nemenia súbory, ale vytvoria ich duplikáty. Pri otvorení takéhoto nakazeného súboru sa spustí jeho duplikát, teda vírus. Existujú tiež odkazové vírusy (OBJ) vírusy infikujúce *objektové moduly*, vírusy infikujúce *knižnice prekladačov* (LIB), vírusy infikujúce *zdrojové texty programov* atď.

Červ

Kód sieťového červa sa po preniknutí do systému, podobne ako kód klasického vírusu, aktivuje a vykoná svoju škodlivú činnosť. Sieťový červ získal svoje meno podľa schopnosti preniesť sa z jedného počítača na iný, bez vedomia používateľa, a posielat tak svoje kópie rôznymi informačnými kanálmi.

Hlavný spôsob šírenia je najvýznamnejším atribútom, podľa ktorého sa rozlišujú rôzne typy červov. Nasledujúca tabuľka uvádza typy červov podľa spôsobu šírenia.

Tabuľka 1. Červy podľa spôsobu šírenia

TYP	NÁZOV	OPIS
IM-Worm	IM červy	<p>Tieto červy sa šíria prostredníctvom klientov IM (rýchlych správ), napríklad ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager alebo Skype.</p> <p>Zvyčajne takýto červ použije zoznam kontaktov na rozoslanie správ s odkazom na súbor so svojou kópiou umiestnený na webovej stránke. Keď používateľ stiahne a otvorí taký súbor, červ sa aktivuje.</p>

TYP	NÁZOV	OPIS
Email-Worm	E-mailové červy	<p>E-mailové červy infikujú počítače prostredníctvom e-mailu.</p> <p>Napadnutá správa obsahuje v prílohe súbor s kópiou červa, alebo odkaz na taký súbor nahraný na webovej stránke, ktorá môže byť napríklad hackerom pozmenená alebo priamo hackerovi patriť. Keď takú prílohu otvoríte, červ sa aktivuje; pokiaľ klepnete na odkaz, stiahnete a otvoríte súbor, červ tiež začne vykonávať svoju škodlivú činnosť. Potom sa bude naďalej množiť pomocou svojich kópií, ktoré vyhľadávajú ďalšie e-mailové adresy a pošlú na ne infikované správy.</p>
IRC-Worms	IM červy	<p>Červy tohto typu prenikajú do počítačov prostredníctvom IRC (Internet Relay Chat) – systémov služby používanej na komunikáciu s inými ľuďmi na internete v reálnom čase.</p> <p>Tento červ zverejní v internetovom chate súbor so svojou kópiou, alebo odkaz na taký súbor. Keď používateľ stiahne a otvorí taký súbor, červ sa aktivuje.</p>
Net-Worms	Sieťové červy (červy sídliace v počítačových sieťach)	<p>Tieto červy sa šíria prostredníctvom počítačových sietí.</p> <p>Na rozdiel od červov iných typov sa sieťové červy šíria bez účasti používateľa. Vyhľadávajú v lokálnych sieťach (LAN) počítača so zraniteľnými programami. Na tento účel červ rozosiela špeciálne sieťové pakety (exploity) obsahujúce jeho kód alebo jeho časť. Pokiaľ je v sieti zraniteľný počítač, takýto paket prijme. Akonáhle celý červ prenikne do počítača, aktivuje sa.</p>

TYP	NÁZOV	OPIS
P2P-Worm	Červy v sieťach na výmenu súborov	<p>Červy v sieťach na výmenu súborov sa šíria prostredníctvom príslušných peer-to-peer sietí, ako sú Kazaa, Grokster, EDonkey, FastTrack alebo Gnutella.</p> <p>Aby červ vnikol do siete na výmenu súborov, skopíruje sa do zložky na výmenu súborov, ktorá sa zvyčajne nachádza na používateľovom počítači. Sieť na výmenu súborov o tom zobrazí informáciu a používatelia môžu súbor na sieť „nájst“, stiahnuť ho a otvoriť ako každý iný súbor.</p> <p>Zložitejšie červy napodobňujú sieťové protokoly konkrétnej siete na výmenu súborov: poskytujú kladné odpovede na požiadavky na hľadanie a ponúkajú na stiahnutie svoje kópie.</p>
Červ	Iné červy	<p>Medzi ďalšie sieťové červy patria:</p> <ul style="list-style-type: none"> • Červy, ktoré šíria svoje kópie prostredníctvom sieťových prostriedkov. Pomocou funkcií operačného systému prechádzajú dostupné sieťové zložky, pripájajú sa k počítačom v globálnej sieti a pokúšajú sa otvoriť ich disky pre plný prístup. Na rozdiel od červov v počítačových sieťach musí používateľ otvoriť súbor s kópiou červa, aby sa červ aktivoval. • Červy, ktoré nepoužívajú žiadny zo spôsobov šírenia uvedených v tejto tabuľke (napríklad červy, ktoré sa šíria prostredníctvom mobilných telefónov).

TRÓJSKE KONE

Podkategórie: trójske kone (Trojan_programs)

Úroveň závažnosti: vysoká

Trójske kone na rozdiel od červov a vírusov nevytvárajú svoje kópie. Preniknú do počítača napríklad prostredníctvom e-mailu alebo cez webový prehliadač, keď používateľ navštívi „infikovanú“ stránku. Trójske kone sú spúšťané používateľom a pri spustení vykonávajú svoje škodlivé akcie.

Správanie sa rôznych trójskych koní sa na napadnutom počítači môže líšiť. Hlavnou funkciou trójskych koní je blokovať, pozmeňovať a mazať dáta, narušovať činnosť počítačov alebo počítačových sietí. Okrem toho môžu trójske kone prijímať a posilať súbory, spúšťať ich, zobrazovať správy, pristupovať k webovým stránkam, sťahovať a inštalovať programy a reštartovať napadnutý počítač.

Votrelci často používajú „sady“ pozostávajúce z rôznych trójskych koní.

Nasledujúca tabuľka opisuje typy trójskych koní a ich správanie sa.

Tabuľka 2. Typy trójskych koní podľa správania sa na napadnutom počítači

Typ	Názov	Opis
Trojan-ArcBomb	Trójske kone – archívne bomby	Archívy; pri rozbalení sa zväčšia na takú veľkosť, ktorá naruší činnosť počítača. Keď sa taký archív pokúsite rozbaľiť, počítač môže začať pracovať pomaly alebo „zamrznúť“ a disk sa môže zaplniť „prázdnyimi“ dátami. „Archívne bomby“ sú obzvlášť nebezpečné pre súborové a poštové servery. Pokiaľ sa na serveri používa systém automatického spracovania vstupných informácií, môže taká „archívna bomba“ server zastaviť.
Backdoor	Trójske kone pre vzdialenú administráciu	Tieto programy sa považujú medzi trójskymi koňmi za najnebezpečnejšie; funkčne pripomínajú komerčne dostupné programy pre vzdialenú administráciu. Tieto programy sa nainštalujú bez vedomia používateľa a útočníkovi umožnia vzdialenú správu počítača.

TYP	NÁZOV	OPIS
Trojan	Trójske kone	<p>Medzi trójske kone patria nasledujúce škodlivé programy:</p> <ul style="list-style-type: none"> • Klasické trójske kone, ktoré vykonávajú len hlavné funkcie trójskych koní: blokovanie, pozmeňovanie alebo mazanie dát, narušovanie činnosti počítačov alebo počítačových sietí. Nemajú žiadne ďalšie funkcie charakteristické pre ostatné typy trójskych koní opísaných v tejto tabuľke. • „Viacúčelové“ trójske kone, ktoré majú ďalšie funkcie charakteristické pre niekoľko typov trójskych koní.
Trojans-Ransoms	Trójske kone požadujúce výkupné	<p>Berú ako „rukojemníkov“ informácie na používateľovom počítači, ktoré pozmenia alebo zablokujú, alebo narušia činnosť počítača, takže používateľ nemôže dáta použiť. Útočník potom vyžaduje od používateľa výkupné výmenou za sľub, že pošle program, ktorý obnoví funkčnosť počítača.</p>
Trojans-Clickers	Klikacie trójske kone	<p>Tieto programy pristupujú z používateľovho počítača na webové stránky. Posielajú príkazy webovému prehliadaču alebo nahrádzujú webové adresy uložené v systémových súboroch.</p> <p>Pomocou týchto programov útočníci organizujú sieťové útoky a zvyšujú návštevnosť webových stránok, aby zvýšili počet zobrazení reklamných líšt.</p>

TYP	NÁZOV	OPIS
Trojans-Downloader s	Trójske kone – sťahovače	Pristupujú k webovej stránke útočníka, stiahnu z nej ďalšie škodlivé programy a tie nainštalujú na používateľov počítača. Názov súboru škodlivého programu na stiahnutie môžu obsahovať v sebe, alebo ho načítať z webovej stránky, ku ktorej pristupujú.
Trojan-Droppers	Trójske kone – inštalátory programov	Tieto trójske kone na pevný disk uložia a potom nainštalujú programy, ktoré obsahujú ďalšie trójske kone. Útočníci môžu pomocou trójskych koní – inštalátorov: <ul style="list-style-type: none"> • inštalovať škodlivé programy bez vedomia používateľa: trójske kone – inštalátory nezobrazujú žiadne správy, alebo zobrazujú falošné správy, napríklad oznámenie o chybe v archíve alebo o používaní nesprávnej verzie operačného systému; • chrániť iný známy škodlivý program pred odhalením: nie všetky antivírusové programy dokážu odhaliť škodlivý program umiestnený vo vnútri trójskeho koňa.
Trojans-Notifiers	Trójske kone – hlásiče	Oznamujú útočníkovi, že napadnutý počítač je pripojený, a potom odošlú útočníkovi informácie o tomto počítači, vrátane IP adresy, čísla otvoreného portu alebo e-mailovej adresy. S útočníkom komunikujú pomocou e-mailu, FTP, prístupom na webové stránky útočníka, alebo inými spôsobmi. Trójske kone – hlásiče sa často používajú v „sádach“ pozostávajúcich z rôznych trójskych koní. Hlásia útočníkovi, že ostatné trójske kone boli na používateľov počítač úspešne nainštalované.

TYP	NÁZOV	OPIS
Trojans-Proxies	Trójske kone – proxy servery	Umožňujú útočníkovi anonymne pristupovať k webovým stránkam pomocou používateľovho počítača a často sa používajú na rozosielanie spamu.
Trojans-PSWs	Trójske kone kradnúce heslá	<p>Trójske kone kradnúce heslá (Password Stealing Ware) kradnú používateľské účty, napríklad registračné informácie o softvéri. V systémových súboroch a v registri hľadajú dôverné informácie a posielajú ich svojmu tvorcovi pomocou e-mailu, FTP, prístupom na webové stránky útočníka, alebo inými spôsobmi.</p> <p>Niektoré z týchto trójskych koní spadajú do konkrétnych typov opísaných v tejto tabuľke. Sú to trójske kone, ktoré kradnú informácie o bankových účtoch (Trojans-Bankers), trójske kone, ktoré kradnú osobné údaje používateľov klientskych programov IM (Trojans-IMs), a trójske kone, ktoré kradnú dáta používateľom sieťových hier (Trojans-GameThieves).</p>
Trojans-Spies	Špehujúce trójske kone	Tieto programy sa používajú na špehovanie používateľa: zhromažďujú informácie o činnosti používateľa na počítači, napríklad zachycujú dáta, ktoré používateľ zadáva z klávesnice, robia snímky obrazovky a zhromažďujú zoznamy aktívnych aplikácií. Po prijatí tieto informácie odosielajú útočníkovi pomocou e-mailu, FTP, prístupom na webové stránky útočníka, alebo inými spôsobmi.

TYP	NÁZOV	OPIS
Trojans-DDoS	Trójske kone pre sieťové útoky	Z používateľovho počítača rozosielajú veľké množstvo požiadaviek na vzdialený server. Server potom vyčerpá svoje prostriedky na spracovanie požiadaviek a prestane fungovať (útok DoS (Denial-of-Service)). Tieto programy sa často používajú na nakazenie väčšieho počtu počítačov, aby z nich bolo možné na server útočiť.
Trojans-IMs	Trójske kone, ktoré kradnú osobné údaje používateľov klientskych programov IM	Tieto programy kradnú čísla a heslá používateľov klientov IM (programov pre rýchle zasielanie správ), napríklad ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager alebo Skype. Potom tieto informácie odošlú útočníkovi pomocou e-mailu, FTP, prístupom na webové stránky útočníka alebo inými spôsobmi.
Rootkits	Rootkity	Tieto programy maskujú iné škodlivé programy a ich činnosť, takže predlžujú čas existencie takýchto programov v systéme; skrývajú súbory alebo procesy v pamäti nakazeného počítača alebo kľúče registra spúšťané škodlivými programami, alebo maskujú výmenu dát medzi aplikáciami inštalovanými na používateľovom počítači a ostatnými počítačmi v sieti.
Trojans-SMS	Trójske kone – SMS správy	Tieto programy infikujú mobilné telefóny a odosielajú z nich textové správy (SMS) na čísla, ktoré sú pre používateľa napadnutého telefónu poplatné.
Trojans-GameThieves	Trójske kone, ktoré kradnú osobné údaje používateľov sieťových hier	Tieto programy kradnú informácie o používateľských účtoch používateľov sieťových hier; následne tieto informácie odošlú útočníkovi pomocou e-mailu, FTP, prístupom na webové stránky útočníka alebo inými spôsobmi.

Typ	Názov	Opis
Trojans-Bankers	Trójske kone, ktoré kradnú informácie o bankových účtoch	Tieto programy kradnú informácie o bankových účtoch alebo o účtoch elektronických / digitálnych peňazí; následne tieto údaje odošlú útočníkovi pomocou e-mailu, FTP, prístupom na webové stránky útočníka alebo inými spôsobmi.
Trojans-Mailfinders	Trójske kone, ktoré zhromažďujú e-mailové adresy	Tieto programy zhromažďujú z počítača e-mailové adresy a odosielajú ich útočníkovi pomocou e-mailu, FTP, prístupom na webové stránky útočníka alebo inými spôsobmi. Útočník môže zhromaždené adresy použiť na rozosielanie spamu.

ŠKODLIVÉ UTILITY

Podkategórie: škodlivé utility (Malicious_tools)

Úroveň závažnosti:stredná

Tieto utility sú navrhnuté špeciálne na to, aby páchali škody. Na rozdiel od ostatných škodlivých programov však nevykonávajú škodlivú činnosť ihneď po spustení a môžu byť na používateľovom počítači bezpečne uložené a spúšťané. Tieto programy disponujú funkciami na vytváranie vírusov, červov a trójskych koní, organizovanie sieťových útokov na vzdialené servery, hackovanie počítačov alebo na iné škodlivé aktivity.

Existuje veľa typov škodlivých utilít s rôznymi funkciami. Ich typy opisuje nasledujúca tabuľka.

Tabuľka 3. Škodlivé utility podľa funkcie

TYP	NÁZOV	OPIS
Constructor	Konštruktory	Konštruktory slúžia na vytváranie nových vírusov, červov a trójskych koní. Niektoré konštruktory majú štandardné rozhranie s oknami, ktoré umožňuje vybrať typ škodlivého programu, ktorý sa má vytvoriť, spôsob, aký má tento program použiť na ochranu proti ladeniu, a ďalšie vlastnosti.
Dos	Sieťové útoky	Z používateľovho počítača rozosiľajú veľké množstvo požiadaviek na vzdialený server. Server potom vyčerpá svoje prostriedky na spracovanie požiadaviek a prestane fungovať (útok DoS (Denial-of-Service)).

TYP	NÁZOV	OPIS
Exploit	Exploity	<p>Exploit je sada dát alebo programového kódu, ktorá využíva zraniteľné miesta aplikácie na vykonanie škodlivej akcie na počítači. Exploity napríklad môžu zapisovať a čítať súbory alebo pristupovať k „infikovaným“ webovým stránkam.</p> <p>Rôzne exploity používajú zraniteľné miesta rôznych aplikácií alebo sieťových služieb. Exploit sa prenáša po sieti na ďalšie počítače v podobe sieťového paketu, ktorý hľadá počítače so zraniteľnými sieťovými službami. Exploit obsiahnutý v súbore DOC používa zraniteľné miesta textových editorov. Keď používateľ otvorí infikovaný súbor, exploit môže začať vykonávať funkcie naprogramované útočníkom. Exploit obsiahnutý v e-mailovej správe hľadá zraniteľnosti v klientskych e-mailových programoch; škodlivú akciu môže vykonať, akonáhle používateľ v takomto programe otvorí infikovanú správu.</p> <p>Exploity sa používajú na šírenie sieťových červov (Net-Worm). Nukery („Exploit-Nuker“) sú sieťové pakety, ktoré počítače znefunkčnia.</p>
FileCryptors	Šifrovače súborov	Šifrovače súborov dešifrujú ostatné škodlivé programy, aby ich skryli pred antivírusovými aplikáciami.

TYP	NÁZOV	OPIS
Flooders	Programy používané na zahltenie sietí	<p>Rozosielajú sieťovými kanálmi obrovské množstvo správ. Medzi ne napríklad patria programy na zahlcovanie IRC.</p> <p>Tento typ škodlivého softvéru však nezahŕňa programy na zahltenie e-mailovej prevádzky alebo kanálov IM a SMS. Takéto programy sú v nasledujúcej tabuľke uvedené pod samostatnými typmi (Email-Flooder, IM-Flooder a SMS-Flooder).</p>
HackTools	Hackerské nástroje	<p>Hackerské nástroje sa používajú na hackovanie počítačov, na ktorých sú nainštalované, alebo na organizovanie útokov na iný počítač (napríklad na neoprávnené pridanie ďalších systémových používateľov alebo na vymazanie systémových protokolov, aby sa zamietli stopy ich prítomnosti v systéme). Zahŕňajú niektoré sniffery, ktoré vykonávajú škodlivé funkcie, napríklad zachytávajú heslá. Sniffery sú programy, ktoré umožňujú zobrazenie dátových tokov v sieti.</p>
not-virus:Hoax	Falošné programy	<p>Tieto programy strašia používateľa správami, ktoré sa podobajú vírusom: môžu „nájsť“ vírus v čistom súbore alebo zobraziť správu o formátovaní disku, ku ktorému nedôjde.</p>
Spoofers	Spoofery	<p>Tieto programy odosielajú správy a sieťové požiadavky s podvrhnutou adresou odosielateľa. Útočníci používajú spoofery napríklad preto, aby predstierali, že sú odosielateľom.</p>
VirTools	Nástroje na pozmeňovanie škodlivých programov	<p>Umožňujú pozmeniť iné škodlivé programy, aby ich skryli pred antivírusovými aplikáciami.</p>

TYP	NÁZOV	OPIS
Email-Flooders	Programy na zahlcovanie e-mailových adries	Tieto programy rozosiľajú značné množstvo správ na e-mailové adresy (zahltia ich). Kvôli obrovskému množstvu prichádzajúcich správ si používatelia nemôžu čítať legitímne prichádzajúce správy.
IM-Flooders	Programy na zahlcovanie IM programov	Tieto programy rozosiľajú veľké množstvo správ používateľom klientov IM (programov na rýchle zasielanie správ), napríklad ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager alebo Skype. Kvôli obrovskému množstvu prichádzajúcich správ si používatelia nemôžu čítať legitímne prichádzajúce správy.
SMS-Flooders	Programy na zahlcovanie pomocou textových správ (SMS)	Tieto programy rozosiľajú veľké množstvo textových správ na mobilné telefóny.

POTENCIÁLNE NEŽIADUCE PROGRAMY

Potenciálne nežiaduce programy, na rozdiel od škodlivých programov, nie sú určené len na to, aby spôsobili škodu. Môžu však oslabiť bezpečnosť počítača.

Potenciálne nežiaduce programy zahŕňajú adware, pornware a ďalšie *potenciálne nežiaduce programy*.

Adware (pozrite na strane 31) zobrazuje používateľovi reklamné informácie.

Pornware (pozrite na strane 31) zobrazuje používateľovi pornografické materiály.

Iný riskware (pozrite na strane 32) – často ide o užitočné programy používané mnohými používateľmi počítačov. Pokiaľ však útočník získa prístup k týmto programom, alebo ich nainštaluje na používateľov počítač, je možné použiť ich na narušenie bezpečnosti počítača.

Potenciálne nežiaduce programy sa inštalujú jedným z nasledujúcich spôsobov:

- Nainštaluje si ich používateľ, či už priamo alebo spolu s iným programom (dodávatelia softvéru napríklad ucinia adware súčasťou svojho freeware alebo shareware programu).
- Môžu ich tiež inštalovať votrelci, ktorí napríklad začlenia takéto programy do balíčka s ďalšími škodlivými programami, využijú „zraniteľnosť“ webového prehliadača alebo použijú trójske kone na ich stiahnutie a inštaláciu, keď používateľ navštívi „infikovanú“ stránku.

ADWARE

Podkategórie: Adware

Úroveň závažnosti: stredná

Adware zobrazuje používateľovi reklamné informácie. Zobrazuje reklamné lišty v rozhraní iného programu a presmerováva otázky vyhľadávania na reklamné webové stránky. Niektorý adware zhromažďuje a posiela svojmu tvorcovi marketingové informácie o používateľovi, napríklad ktoré stránky navštevuje a čo hľadá (na rozdiel od špehovacích trójskych koní tieto programy odosielajú informácie so súhlasom používateľa).

PORNWARE

Podkategórie: Pornware

Úroveň závažnosti: stredná

Používatelia zvyčajne inštalujú takéto programy sami, aby mohli hľadať alebo sťahovať pornografiu.

Votrelci tiež môžu nainštalovať tieto programy na používateľov počítač, aby sa používateľovi bez jeho súhlasu zobrazovali reklamy na komerčné pornografické servery a služby. Na inštaláciu používajú zraniteľné miesta v operačnom systéme alebo webovom prehliadači, prípadne trójske kone, ktoré sťahujú a inštalujú programy.

Existujú tri typy pornwaru, ktoré sa líšia podľa svojich funkcií. Tieto typy opisuje nasledujúca tabuľka.

Tabuľka 4. Typy pornwaru v závislosti od funkcie

Typ	Názov	Opis
Porn-Dialers	Automatické dialery	Tieto programy automaticky vytáčajú čísla telefónnych pornografických služieb (obsahujú uložené čísla týchto služieb); na rozdiel od trójskych koní – dialerov o svojej činnosti informujú používateľa.
Porn-Downloader s	Programy na sťahovanie súborov z internetu	Tieto programy sťahujú na používateľov počítač pornografické materiály; na rozdiel od trójskych koní – dialerov o svojej činnosti informujú používateľa.
Porn-Tools	Nástroje	Používajú sa na vyhľadávanie a zobrazovanie pornografie; tento typ zahŕňa špeciálnu nástrojovú lištu pre prehliadač a špeciálne prehrávače videa.

INÝ RISKWARE

Podkategórie: iný riskware

Úroveň závažnosti: stredná

Väčšina týchto programov je užitočná a používa ich mnoho používateľov. Patria medzi ne klienti IRC, dialery, programy na sťahovanie súborov, monitory aktivity počítačového systému, nástroje pre prácu s heslami, internetové servery služieb FTP, HTTP alebo Telnet.

Pokiaľ však útočník získa prístup k týmto programom, alebo ich nainštaluje na používateľov počítač, môže niektoré ich funkcie použiť na narušenie bezpečnosti počítača.

Iný riskware sa delí do kategórií podľa svojej funkcie. Ich typy opisuje nasledujúca tabuľka.

Tabuľka 5. Typy iného riskwaru podľa jeho funkcií

TYP	NÁZOV	OPIS
Client-IRC	Programy pre IRC	Používatelia inštalujú tieto programy, aby mohli komunikovať prostredníctvom IRC (Internet Relay Chat). Votrelci ich používajú na šírenie škodlivého softvéru.
Dialers	Programy na automatické vytáčanie	Tieto programy môžu „tajne“ nadviazať telefonické spojenie pomocou modemu.
Downloaders	Sťahovače	Tieto programy môžu tajne sťahovať súbory z webových stránok.
Monitors	Monitory	Tieto programy umožňujú sledovať činnosť počítačov, na ktorých sú nainštalované (sledovať výkon aplikácií, ako si vymieňajú dáta s aplikáciami na iných počítačoch atď.).
PSWTools	Nástroje na obnovu hesiel	Tieto programy sa používajú na zobrazenie a obnovenie zabudnutých hesiel. Keď ich votrelci nainštalujú na počítače používateľov, používajú ich presne na rovnaký účel.

TYP	NÁZOV	OPIS
RemoteAdmin	Programy na vzdialenú administráciu	<p>Tieto programy často používajú systémoví administrátori; vďaka nim majú prístup k rozhraniu vzdialeného počítača a môžu počítač monitorovať a spravovať. Keď votrelci inštalujú tieto programy na počítače používateľov, aby ich mohli sledovať a spravovať, sledujú presne tie isté ciele.</p> <p>Programy na vzdialenú administráciu typu riskware sa líšia od trójskych koní umožňujúcich vzdialenú administráciu, nazývaných zadné vrátka (backdoor). Trójske kone disponujú funkciami, ktoré im umožňujú nezávisle preniknúť do systému a nainštalovať sa; riskware takúto funkciu nemá.</p>
Server-FTP	FTP servery	Tieto programy fungujú ako FTP servery. Votrelci ich inštalujú na počítače používateľov, aby získali vzdialený prístup pomocou protokolu FTP.
Server-Proxy	Proxy servery	Tieto programy fungujú ako proxy servery. Votrelci ich inštalujú na počítače používateľov, aby mohli na účet používateľov rozosielať spam.
Server-Telnet	Servery služby Telnet	Tieto programy fungujú ako servery služby Telnet. Votrelci ich inštalujú na počítače používateľov, aby získali vzdialený prístup pomocou protokolu Telnet.
Server-Web	Webové servery	Tieto programy fungujú ako webové servery. Votrelci ich inštalujú na počítače používateľov, aby získali vzdialený prístup pomocou protokolu HTTP.

Typ	Názov	Opis
RiskTool	Nástroje pre miestny počítač	Tieto nástroje poskytujú používateľom ďalšie funkcie a používajú sa len v rámci používateľovho počítača (umožňujú skrývať súbory alebo okná aktívnych aplikácií, ukončovať aktívne procesy).
NetTool	Sieťové nástroje	Tieto nástroje ponúkajú používateľovi počítača, na ktorom sú nainštalované, ďalšie funkcie pre správu iných počítačov v rámci siete (reštartovať ich, nájsť otvorené porty, spúšťať programy inštalované na týchto počítačoch).
Client-P2P	Klientske programy sietí peer-to-peer	Tieto programy slúžia na používanie sietí peer-to-peer. Votrelci ich môžu použiť na šírenie škodlivého softvéru.
Client-SMTP	SMTP klienti	Tieto programy rozosiľajú e-mailové správy v skrytom režime. Votrelci ich inštalujú na počítače používateľov, aby mohli na účet používateľov rozosiľovať spam.
WebToolbar	Webové panely nástrojov	Tieto programy dopĺňajú vlastné panely nástrojov pre vyhľadávanie do panelov nástrojov iných aplikácií.
FraudTool	Podvrhnuté programy	Tieto programy sa maskujú ako iné skutočné programy. Napríklad existujú podvodné antivírusové programy; zobrazujú správy o zisťovaní škodlivého softvéru, ale nič nehľadajú ani nedezinfikujú.

SPÔSOBY DETEKcie NAPADNUTÝCH, PODOZRIVÝCH A POTENCIÁLNE NEBEZPEČNÝCH OBJEKTOV

Aplikácia spoločnosti Kaspersky Lab detekuje škodlivý softvér v objektoch pomocou dvoch metód: reaktívna (s použitím databáz) a proaktívna (s použitím heuristickej analýzy).

Databázy sú súbory so záznamami, ktoré sa používajú na zisťovanie prítomnosti statistícov známych hrozieb v detekovateľných objektoch. Tieto záznamy obsahujú informácie o riadiacich sekciách kódu škodlivého softvéru a algoritmy pre dezinfekciu objektov, v ktorých sa takýto softvér nachádza. Antivírusoví analytici spoločnosti Kaspersky Lab denne detekujú stovky nových škodlivých programov, vytvárajú záznamy s ich identifikáciou a tie pridávajú do aktualizácií databáz.

Pokiaľ aplikácia spoločnosti Kaspersky Lab v detekovateľnom objekte objaví časti kódu, ktoré sa podľa informácií v databáze plne zhodujú s riadiacimi sekciami kódu škodlivého softvéru, považuje objekt za napadnutý a pokiaľ sa zhodujú len čiastočne (podľa určitých podmienok), za podozrivý.

Pomocou proaktívnej metódy môže aplikácia odhaliť najnovší škodlivý softvér, o ktorom v databáze doteraz nie sú informácie.

Aplikácia spoločnosti Kaspersky Lab detekuje objekty obsahujúce nové škodlivé programy podľa ich správania. Nedá sa povedať, že by sa kód takého objektu plne alebo čiastočne zhodoval s kódom známeho škodlivého programu, ale obsahuje niektoré potupnosti príkazov, ktoré sú charakteristické pre škodlivý softvér, napríklad otvorenie súboru, zápis do súboru alebo presmerovanie vektorov prerušenia. Aplikácia napríklad zistí, že súbor je zrejme napadnutý neznámym vírusom v zavádzacom sektore.

Objekty zistené proaktívnou metódou sa nazývajú potenciálne nebezpečné.

INTERNETOVÉ HROZBY

Aplikácia spoločnosti Kaspersky Lab používa špeciálne technológie na prevenciu nasledujúcich hrozieb pre bezpečnosť počítača:

- spam – nevyžiadaná prichádzajúca pošta (pozrite oddiel „Nevyžiadaná prichádzajúca pošta – Spam“ na strane 37);
- phishing – podvody (na strane 37);
- útoky hackerov (na strane 38);
- zobrazenie reklamných líšt (na strane 38).

NEVYŽIADANÁ PRICHÁDZAJÚCA POŠTA – SPAM

Aplikácia spoločnosti Kaspersky Lab chráni používateľa pred spamom. Spam je nevyžiadaná prichádzajúca pošta, často reklamnej povahy. Spam zvyšuje záťaž prenosových kanálov a poštových serverov poskytovateľa. Prijemca platí za dátový tok vytvorený spamom a legitímna pošta cestuje pomalšie. Spam je preto v mnohých krajinách protizákonný.

Aplikácia spoločnosti Kaspersky Lab kontroluje prichádzajúce správy v programoch Microsoft Office Outlook, Microsoft Outlook Express a The Bat!, a pokiaľ zistí, že nejaká správa je spam, vykoná vami vybranú akciu, napríklad presunie takéto správy do osobitnej zložky alebo ich odstráni.

Aplikácia spoločnosti Kaspersky Lab detekuje spam s veľkou presnosťou. Používa niekoľko technológií na filtrovanie spamu: detekuje spam na základe adresy odosielateľa i slov a slovných spojení v predmete správy; detekuje grafický spam a používa samoučiace algoritmy na detekciu spamu podľa textu správ.

Antispamové databázy obsahujú „čierne“ a „biele“ zoznamy adries odosielateľov, a ďalej zoznamy slov a slovných spojení, ktoré súvisia s rôznymi kategóriami spamu, ako je reklama, zdravie a zdravotníctvo, hazardné hry atď.

PHISHING

Phishing je typ podvodnej činnosti na internete spočívajúci v „vylákaní“ čísiel kreditných kariet, čísel PIN a iných osobných údajov od používateľov s cieľom odcudzenia ich peňazí.

Phishing často súvisí s internetovým bankovníctvom. Útočníci vytvoria presnú kópiu banky, na ktorú miera, a potom jej menom rozosielajú správy jej klientom.

Oznamujú im, že v dôsledku zmeny alebo chyby softvéru internetového bankovníctva sa vymazali používateľské účty a používatelia musia na webe banky potvrdiť či zmeniť svoje údaje. Používateľ klepne na odkaz na web vytvorený útočníkmi a tu zadá svoje osobné údaje.

Antiphishingové databázy obsahujú zoznam adries URL webov, o ktorých je známe, že sa používajú na phishing.

Aplikácia spoločnosti Kaspersky Lab analyzuje prichádzajúce správy v programe Microsoft Office Outlook a Microsoft Outlook Express, a pokiaľ nájde odkaz na adresu URL, ktorá je v databázach, označí túto správu ako spam. Pokiaľ používateľ správu otvorí a pokúsi sa odkaz navštíviť, aplikácia túto webovú stránku zablokuje.

ÚTOKY HACKEROV

Sieťový útok je prienik do systému vzdialeného počítača s cieľom získania kontroly nad týmto systémom a spôsobenia jeho zlyhania alebo získania prístupu k chráneným informáciám.

Sieťové útoky vykonávajú buď útočníci (napríklad skenovanie portov, pokusy o uhádnutie hesla), alebo škodlivé programy, ktoré z účtu používateľa spúšťajú príkazy a prenášajú informácie svojmu „pánovi“ alebo vykonávajú iné funkcie súvisiace so sieťovým útokom. Sem spadajú niektoré trójske kone, útoky DoS, škodlivé skripty a niektoré typy sieťových červov.

Sieťové útoky sa v lokálnych aj globálnych sieťach šíria prostredníctvom zraniteľných miest v operačných systémoch a aplikáciách. Môžu sa prenášať ako jednotlivé dátové pakety IP v rámci sieťových spojení.

Aplikácia spoločnosti Kaspersky Lab zastaví sieťové útoky bez toho, že by narušila sieťové pripojenia. Používa špeciálne databázy pre bránu firewall. Tieto databázy obsahujú záznamy s charakteristikami dátových paketov IP rôznych hackerských programov. Aplikácia analyzuje sieťové spojenia a blokuje v nich tieto pakety IP, ktoré považuje za nebezpečné.

ZOBRAZENIE REKLAMNÝCH LÍŠŤ

Reklamné lišty alebo reklamy, ktoré odkazujú na web inzerenta, sa najčastejšie zobrazujú ako obrázky. Zobrazenie reklamných líšt na webovej stránke nepredstavuje hrozbu pre bezpečnosť počítača, ale napriek tomu sa považuje za narušenie normálnej činnosti počítača. Poblíkavanie reklamných líšt na

obrazovke zhoršuje pracovné podmienky a tým znižuje výkonnosť. Nepodstatné informácie používateľa rozptyľujú. Navštevovanie odkazov z reklamných líšt zvyšuje internetový dátový tok.

Mnoho organizácií v rámci svojich zásad zabezpečenia dát zakazuje zobrazovanie reklamných líšt v rozhraniach.

Aplikácia spoločnosti Kaspersky Lab blokuje reklamné líšty podľa adries URL webov, na ktoré líšta odkazuje. Používa aktualizovateľné antireklamné databázy, ktoré obsahujú zoznam adries URL ruských i zahraničných reklamných sietí. Aplikácia kontroluje odkazy v načítanej webovej stránke, porovnáva ich s adresami v databázach a pokiaľ konkrétny odkaz v niektorej z nich nájde, odstráni z webovej stránky odkaz na túto adresu a pokračuje v načítaní stránky.

INŠTALÁCIA APLIKÁCIE NA POČÍTAČ

Aplikácia sa na počítač inštaluje v interaktívnom režime pomocou sprievodcu inštaláciou aplikácie.

Upozornenie!

Pred inštaláciou odporúčame ukončiť všetky spustené aplikácie.

Ak chcete aplikáciu nainštalovať na svoj počítač, spustíte distribučný súbor (súbor s príponou *.exe).

Poznámka

Inštalácia aplikácie z inštalačného súboru stiahnutého z internetu je úplne totožná s inštaláciou z CD.

Sprievodca inštaláciou potom vyhľadá inštalačný balíček aplikácie (súbor s príponou *.msi), a pokiaľ taký súbor nájde, skúsi vyhľadať novšiu verziu na internetových serveroch spoločnosti Kaspersky Lab. Pokiaľ súbor inštalačného balíčka nebol nájdený, bude vám ponúknuté jeho stiahnutie. Po stiahnutí súboru sa spustí inštalácia aplikácie. Pokiaľ stiahnutie zrušíte, proces inštalácie aplikácie bude pokračovať v normálnom režime.

Inštalačný program je implementovaný ako sprievodca. Každé okno sprievodcu obsahuje sadu tlačidiel na riadenie procesu inštalácie. Nasleduje stručný opis ich účelu:

- **Ďalšie** – prijať akciu a prejsť k ďalšiemu kroku procesu inštalácie.
- **Predchádzajúce** – vrátiť sa k predchádzajúcemu kroku procesu inštalácie.
- **Storno** – zrušiť inštaláciu.
- **Dokončiť** – dokončiť inštaláciu aplikácie.

Ďalej nasleduje podrobný opis jednotlivých krokov inštalácie balíčka.

V TOMTO ODDIELI:

Krok 1. Vyhľadanie novej verzie aplikácie	41
Krok 2. Overenie, že systém spĺňa požiadavky na inštaláciu	42
Krok 3. Prívetivé okno sprievodcu.....	42
Krok 4. Zobrazenie licenčnej zmluvy.....	42
Krok 5. Výber typu inštalácie	43
Krok 6. Výber inštalačnej zložky	43
Krok 7. Výber súčastí aplikácie na inštaláciu.....	44
Krok 8. Vyhľadanie iného antivírusového softvéru.....	45
Krok 9. Konečná príprava na inštaláciu.....	45
Krok 10. Dokončenie inštalácie	46

KROK 1. VYHLADANIE NOVŠEJ VERZIE APLIKÁCIE

Pred inštaláciou aplikácie na váš počítač sprievodca kontaktuje aktualizáčn é servery spoločnosti Kaspersky Lab, aby skontroloval, či neexistuje novšia verzia inštalovanej aplikácie.

Pokiaľ na aktualizáčných serveroch spoločnosti Kaspersky Lab nie je novšia verzia nájdená, spustí sa sprievodca inštaláciou a nainštaluje aktuálnu verziu.

Pokiaľ je na severoch nájdená novšia verzia aplikácie, bude vám ponúknuté jej stiahnutie. Pokiaľ stiahnutie zrušíte, spustí sa sprievodca inštaláciou a nainštaluje aktuálnu verziu. Ak sa rozhodnete inštalovať novšiu verziu, inštalačné súbory sa stiahnu na váš počítač a automaticky sa spustí sprievodca inštaláciou, aby novšiu verziu nainštaloval. Podrobnosti o inštalácii novšej verzie nájdete v dokumentácii k príslušnej verzii aplikácie.

KROK 2. OVERENIE, ŽE SYSTÉM SPĺŇA POŹIADAVKY NA INŠTALÁCIU

Pred inštaláciou aplikácie na váš počítač sprievodca skontroluje, či operačný systém a inštalované opravy „service pack“ spĺňajú požiadavky na inštaláciu softvéru (pozrite oddiel „Hardvérové a softvérové systémové požiadavky“ na strane 15). Overí tiež, či sú na vašom počítači nainštalované potrebné programy a či na ňom máte práva potrebné na inštaláciu softvéru.

Pokiaľ niektoré požiadavky nie sú splnené, na obrazovke sa zobrazí príslušné upozornenie. Odporúčame pred inštaláciou aplikácie spoločnosti Kaspersky Lab nainštalovať potrebné programy a pomocou služby **Windows Update** nainštalovať potrebné aktualizácie.

KROK 3. PRIVÍTACIE OKNO SPRIEVODCU

Pokiaľ váš systém vo všetkom spĺňa požiadavky (pozrite oddiel „Hardvérové a softvérové systémové požiadavky“ na strane 15) a na aktualizáčnych serveroch spoločnosti Kaspersky Lab nebola nájdená novšia verzia aplikácie, alebo ste inštaláciu novej verzie zrušili, spustí sa sprievodca inštaláciou a nainštaluje aktuálnu verziu aplikácie. Potom sa na obrazovke zobrazí prvé dialógové okno sprievodcu inštaláciou, ktoré obsahuje informácie o spustení inštalácie aplikácie na váš počítač.

Ak chcete pokračovať v inštalácii, stlačte tlačidlo **Ďalšie**. Ak chcete inštaláciu zrušiť, stlačte tlačidlo **Storno**.

KROK 4. ZOBRAZENIE LICENČNEJ ZMLUVY

Nasledujúce dialógové okno sprievodcu obsahuje licenčnú zmluvu medzi vami a spoločnosťou Kaspersky Lab. Pozorne si ju prečítajte, a pokiaľ so všetkými podmienkami zmluvy súhlasíte, vyberte voľbu **S podmienkami licenčnej zmluvy súhlasím** a stlačte tlačidlo **Ďalšie**. Inštalácia bude pokračovať.

Ak chcete inštaláciu zrušiť, stlačte tlačidlo **Storno**.

KROK 5. VÝBER TYPU INŠTALÁCIE

V tomto kroku máte možnosť vybrať typ inštalácie, ktorý vám najviac vyhovuje:

- **Expresná inštalácia.** Ak vyberiete túto voľbu, na váš počítač sa nainštaluje celá aplikácia s nastavením ochrany, aké odporúčajú odborníci spoločnosti Kaspersky Lab. Po dokončení inštalácie sa spustí sprievodca konfiguráciou aplikácie.
- **Vlastná inštalácia.** V tomto prípade budete môcť vybrať súčasti aplikácie, ktoré chcete na počítač nainštalovať, určiť zložku, do ktorej sa aplikácia nainštaluje (pozrite oddiel „Krok 6. Výber inštalačnej zložky“ na strane 43), aktivovať aplikáciu a skonfigurovať ju pomocou špeciálneho sprievodcu.

Ak vyberiete prvú voľbu, sprievodca inštaláciou aplikácie prejde priamo ku kroku 8 (pozrite oddiel „Krok 8. Vyhľadanie iných antivírusových aplikácií“ na strane 45). Inak od vás bude v každom kroku inštalácie požadovaný vstup alebo potvrdenie.

KROK 6. VÝBER INŠTALAČNEJ ZLOŽKY

Poznámka

Tento krok sprievodcu inštaláciou sa vykoná len v prípade, že ste vybrali voľbu vlastnej inštalácie (pozrite oddiel „Krok 5. Výber typu inštalácie“ na strane 43).

V tomto kroku sa vám ponúkne možnosť určiť zložku v počítači, do ktorej sa aplikácia nainštaluje. Východisková cesta je:

- <jednotka> \ **Program Files \ Kaspersky Lab \ Kaspersky Internet Security 2009** – pre 32-bitové systémy.
- <jednotka> \ **Program Files (x86) \ Kaspersky Lab \ Kaspersky Internet Security 2009** – pre 64-bitové systémy.

Inú zložku môžete určiť tak, že stlačíte tlačidlo **Prechádzať** a vyberte zložku v štandardnom dialógovom okne pre výber zložiek, alebo zadáte cestu k zložke do vstupného poľa.

Upozornenie!

Pamätajte, že pokiaľ zadáte celú cestu k inštalačnej zložke ručne, jej dĺžka by nemala presiahnuť 200 znakov a cesta by nemala obsahovať špeciálne znaky.

Ak chcete pokračovať v inštalácii, stlačte tlačidlo **Ďalšie**.

KROK 7. VÝBER SÚČASTÍ APLIKÁCIE NA INŠTALÁCIU

Poznámka: Tento krok sprievodcu inštaláciou sa vykoná len v prípade, že ste vybrali voľbu vlastnej inštalácie (pozrite oddiel „Krok 5. Výber typu inštalácie“ na strane 43).

V prípade vlastnej inštalácie musíte vybrať súčasti aplikácie, ktoré chcete na svoj počítač nainštalovať. Štandardne sú na inštaláciu vybrané všetky súčasti aplikácie: súčasti na ochranu, kontrolu i aktualizáciu.

Pre rozhodovanie, ktoré súčasti nechcete inštalovať, použite stručné informácie o súčastiach. Získate ich tak, že vyberiete súčasť zo zoznamu a prečítate si o nej informácie v poli v spodnej časti. Informácie zahŕňajú stručný opis súčasti a voľné miesto na pevnom disku potrebné na jej inštaláciu.

Ak chcete zrušiť inštaláciu ľubovoľnej súčasti, otvorte miestnu ponuku klepnutím na ikonu vedľa názvu súčasti a vyberte položku **Súčasť nebude dostupná**. Pamätajte, že ak zrušíte inštaláciu nejakej súčasti, nebudete chránení proti mnohým nebezpečným programom.

Ak chcete vybrať súčasť na inštaláciu, otvorte miestnu ponuku klepnutím na ikonu vedľa názvu súčasti a vyberte položku **Súčasť sa nainštaluje na lokálny pevný disk**.

Po dokončení výberu súčasti na inštaláciu klepnite na tlačidlo **Ďalšie**. Ak sa chcete vrátiť k zoznamu súčastí, ktoré sa inštalujú štandardne, klepnite na tlačidlo **Vymazať**.

KROK 8. VYHLADANIE INÉHO ANTIVÍRUSOVÉHO SOFTVÉRU

Sprievodca v tomto kroku skúsi vyhľadať iné antivírusové programy, vrátane programov spoločnosti Kaspersky Lab, ktoré by mohli spôsobiť konflikt s inštalovanou aplikáciou.

Pokiaľ boli na vašom počítači takéto programy zistené, na obrazovke sa zobrazí ich zoznam. Pred pokračovaním v inštalácii budete mať možnosť ich odstrániť.

Pomocou ovládacích prvkov umiestených pod zoznamom nájdených antivírusových programov môžete zvoliť, či ich chcete odstrániť automaticky alebo ručne.

Pokiaľ zoznam zistených antivírusových programov zahŕňa aplikáciu spoločnosti Kaspersky Lab verzia 7.0, pri odoberaní aplikácie si uložte súbor s kľúčom použitý pre túto aplikáciu. Tento kľúč môžete použiť pre novú verziu aplikácie. Rovnako odporúčame uložiť objekty uložené v karanténe a v úložišti pre zálohovanie; tieto objekty sa automaticky presunú do karantény v novej verzii a po inštalácii ich budete môcť spravovať.

Pri automatickom odstránení verzie 7.0 program uloží informácie o jej aktivácii, ktoré sa potom použijú pri inštalácii verzie 2009.

Upozornenie!

Aplikácia podporuje súbory s kľúčmi pre verzie 6.0 a 7.0. Kľúče pre verziu 5.0 podporované nie sú.

Ak chcete pokračovať v inštalácii, stlačte tlačidlo **Ďalšie**.

KROK 9. KONEČNÁ PRÍPRAVA NA INŠTALÁCIU

V tomto kroku budete môcť vykonať konečnú prípravu na inštaláciu na váš počítač.

Pri počiatočnej a vlastnej inštalácii aplikácie (pozrite oddiel „Krok 5. Výber typu inštalácie“ na strane 43) odporúčame pri počiatočnej inštalácii ponechať zaškrtnuté políčko **Pred inštaláciou povoliť sebaobranu**. Ak je voľba ochrany

modulov povolená, zaistí správne vrátenie inštalácie späť, pokiaľ pri nej dôjde k chybe. Pri opakovanom pokuse o inštaláciu odporúčame zaškrtnutie tohto políčka zrušiť.

Poznámka

V prípade vzdialenej inštalácie aplikácie pomocou nástroja **Vzdialená pracovná plocha** odporúčame zrušiť zaškrtnutie políčka **Pred inštaláciou povoliť sebaobranu**. Ak je toto políčko zaškrtnuté, možno sa inštalácia nevykoná správne alebo sa nevykoná vôbec.

Ak chcete pokračovať v inštalácii, stlačte tlačidlo **Ďalšie**. Potom sa inštalačné súbory začnú kopírovať na váš počítač.

Upozornenie!

Pokiaľ balíček aplikácie obsahuje súčasti pre zachytávanie sieťovej prevádzky, pri inštalácii sa prerušia aktuálne sieťové spojenia. Väčšina ukončených pripojení bude po určitom čase automaticky obnovená.

KROK 10. DOKONČENIE INŠTALÁCIE

Okno **Inštalácia dokončená** obsahuje informácie o dokončení procesu inštalácie aplikácie na váš počítač.

Aby sa inštalácia správne dokončila, je potrebné reštartovať počítač; na obrazovke sa zobrazí príslušné oznámenie. Po reštarte systému sa automaticky spustí sprievodca konfiguráciou.

Pokiaľ pre dokončenie inštalácie netreba systém reštartovať, stlačením tlačidla **Ďalšie** spustíte sprievodcu konfiguráciou aplikácie.

ROZHRAINIE APLIKÁCIE

Aplikácia má pomerne jednoduché a ľahko použiteľné rozhranie. Táto kapitola podrobne opisuje jeho základné funkcie.

Okrem hlavného rozhrania program obsahuje moduly plug-in pre Microsoft Office Outlook (kontrola vírusov a spracovania spamu), Microsoft Outlook Express (Windows Mail), The Bat! (kontrola vírusov a spracovania spamu), Microsoft Internet Explorer a Prieskumníka Windows. Moduly plug-in rozširujú funkcie uvedených aplikácií a poskytujú schopnosť z rozhrania spravovať a konfigurovať súčasti Mail Anti-Virus a Anti-Spam.



V TOMTO ODDIELI:

Ikona v oznamovacej oblasti	47
Miestna ponuka	48
Hlavné okno aplikácie	50
Upozornenie	53
Konfiguračné okno aplikácie.....	53

IKONA V OZNAMOVACEJ OBLASTI

Ihneď po inštalácii aplikácie sa v oznamovacej oblasti hlavného panelu Microsoft Windows zobrazí ikona aplikácie.

Táto ikona je indikátorom činnosti aplikácie. Odráža stav ochrany a znázorňuje rôzne základné funkcie, ktoré aplikácia vykonáva.

Pokiaľ je ikona aktívna  (farebná), je spustená kompletná ochrana alebo niektoré jej súčasti. Pokiaľ je ikona neaktívna  (čiernobiela), boli všetka súčasti ochrany vypnuté.

Ikona aplikácie sa mení podľa vykonávanej operácie:



– prebieha kontrola e-mailu.



– aktualizujú sa databázy a programové moduly aplikácie.



– pre použitie aktualizácií je potrebné reštartovať počítač.




– došlo k chybe v niektorej súčasti aplikácie Kaspersky Internet Security.

Ikona tiež poskytuje prístup k základným prvkom rozhrania aplikácie: miestnej ponuke (pozrite oddiel „Miestna ponuka“ na strane 48) a hlavnému oknu aplikácie (pozrite oddiel „Hlavné okno aplikácie“ na strane 50).

Ak chcete otvoriť miestnu ponuku, klepnite pravým tlačidlom myši na ikonu aplikácie.

Ak chcete otvoriť hlavné okno aplikácie, poklepte na ikonu aplikácie. Hlavné okno sa vždy otvára v oddieli **Ochrana**.

Pokiaľ sú k dispozícii správy od spoločnosti Kaspersky Lab, objaví sa v oznamovacej oblasti hlavného panelu ikona správ . Poklepaním na ikonu sa novinky zobrazia vo výslednom okne.

MIESTNA PONUKA

Z kontextovej ponuky môžete spúšťať základné úlohy ochrany.

Ponuka aplikácie obsahuje nasledujúce položky:

- **Aktualizovať** – spustí aktualizáciu modulov a databáz aplikácie a nainštaluje aktualizácie na počítač.
- **Plná kontrola počítača** – spustí úplnú kontrolu počítača kvôli výskytu nebezpečných objektov. Skontrolujú sa objekty na všetkých jednotkách vrátane vymeniteľných pamätových médií.
- **Antivírusová kontrola** – výber objektov a spustenie antivírusovej kontroly. Vo východiskovom nastavení tento zoznam obsahuje niekoľko objektov, napríklad zložku **Moje dokumenty** a poštové schránky. Môžete doplniť zoznam výberom objektov určených na kontrolu a spustiť vyhľadávanie vírusov.

- **Sledovanie siete** – zobrazenie zoznamu nadviazaných sieťových spojení, otvorených portov a dátových tokov.
- **Virtuálna klávesnica** – prepnutie na virtuálnu klávesnicu.
- **Kaspersky Internet Security** – otvorenie hlavného okna aplikácie (pozrite oddiel „Hlavné okno aplikácie“ na strane 50).
- **Nastavenie** – zobrazenia a konfigurácia nastavenia aplikácie.
- **Aktivovať** – aktivácia aplikácie. Pre získanie štatútu registrovaného používateľa musíte aplikáciu aktivovať. Táto položka ponuky je k dispozícii, len ak aplikácia nie je aktivovaná.
- **O aplikácii** – zobrazí okno s informáciami o aplikácii.
- **Pozastaviť ochranu / Obnoviť ochranu** – dočasne vypne alebo zapne súčasť ochrany v reálnom čase. Táto voľba ponuky nemá vplyv na aktualizácie produktu alebo vykonávanie úloh antivírusovej kontroly.
- **Blokovať sieťovú prevádzku** – dočasne zablokuje všetky sieťové spojenia počítača. Ak chcete umožniť interakciu počítača so sieťou, vyberte túto položku z kontextovej ponuky znova.
- **Koniec** – zatvorí aplikáciu (ak vyberiete túto voľbu, aplikácia bude uvoľnená z pamäte RAM počítača).



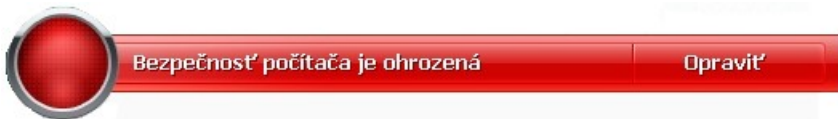
Obrázok 1: Miestna ponuka

Pokiaľ je vo chvíli, kedy otvárate miestnu ponuku, spustená úloha antivírusovej kontroly, v miestnej ponuke sa zobrazí jej názov a priebeh (dokončená časť v percentách). Výberom úlohy môžete prejsť do hlavného okna so správou o aktuálnych výsledkoch jej činnosti.

HLAVNÉ OKNO APLIKÁCIE

Hlavné okno aplikácie možno rozdeliť do troch častí:

- Horná časť okna ukazuje aktuálny stav ochrany počítača.



Obrázok 2: Aktuálny stav ochrany počítača

Sú tri možné stavy ochrany, každý z nich sa zobrazuje určitou farbou podobne ako na semafore. Zelená farba znamená, že ochrana počítača je na správnej úrovni, žltá a červená farba upozorňujú na rôzne bezpečnostné hrozby v nastavení alebo činnosti aplikácie. Okrem škodlivých programov hrozby tiež zahŕňajú zastarané databázy aplikácie, vypnuté súčasti ochrany, výber minimálnych nastavení aplikácie atď.

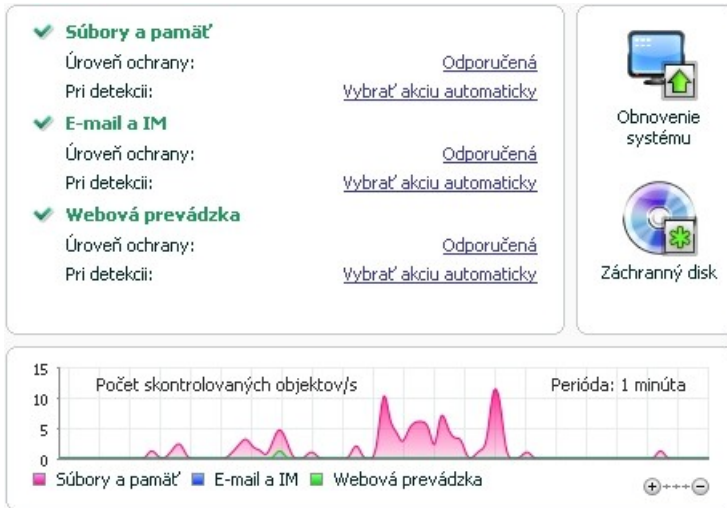
Pokiaľ sa objavia bezpečnostné hrozby, treba ich ihneď odstrániť. Pomocou odkazu **Opraviť teraz** (pozrite obrázok vyššie) o nich získate podrobné informácie a môžete ich rýchlo eliminovať.

- Ľavá časť okna – navigačná lišta – sa používa na rýchle prepnutie na ľubovoľnú funkciu aplikácie, na vykonanie antivírusovej kontroly, aktualizácie atď.



Obrázok 3: Ľavá časť hlavného okna

- Pravá časť okna obsahuje informácie o funkcii aplikácie vybranej v ľavej časti. Služi na konfiguráciu nastavenia tejto funkcie a ponúka nástroje na vykonanie úloh antivírusovej kontroly, stiahnutie aktualizácií atď.



Obrázok 4: Informačná časť hlavného okna

Môžete použiť tiež tlačidlá:

- **Nastavenie** – na prepnutie do nastavenia aplikácie.
- **Nápoveda** – na prepnutie do systému nápovedy aplikácie.
- **Zistené** – prepnutie na zoznam škodlivých objektov zistených v rámci činnosti ľubovoľnej súčasti alebo dokončenej antivírusovej kontroly a na zobrazenie podrobných štatistických údajov o výsledkoch činnosti aplikácie.
- **Správy** – prepnutie na zoznam udalostí, ku ktorým došlo počas činnosti aplikácie.
- **Podpora** – otvorenie okna s informáciami o systéme a s odkazmi na informačné zdroje spoločnosti Kaspersky Lab (stránky služby technickej podpory, fórum).

Poznámka

Vzhľad aplikácie môžete zmeniť vytvorením a použitím vlastnej grafiky a farebných schém.

UPOZORNENIE

Pokiaľ sa počas činnosti aplikácie vyskytnú určité udalosti, zobrazí sa na obrazovke nad ikonou aplikácie na hlavnom paneli Microsoft Windows špeciálne upozornenie formou prekryvných správ.

Podľa závažnosti udalosti vzhľadom na bezpečnosť počítača sa môžu zobrazit' nasledujúce typy upozornení:

- **Výstraha.** Došlo ku kritickej udalosti. V systéme bol napríklad zistený vírus alebo nebezpečná aktivita. Je potrebné, aby ste ihneď rozhodli, ako má aplikácia reagovať. Tento typ upozornenia má červenú farbu.
- **Upozornenie!** Došlo k potenciálne nebezpečnej udalosti. V systéme boli napríklad zistené potenciálne napadnuté súbory alebo podozrivá aktivita. Treba dať aplikácii pokyny v závislosti od toho, za akú nebezpečnú túto udalosť považujete. Tento typ upozornenia má žltú farbu.
- **Poznámka:** Toto upozornenie informuje o udalostiach, ktoré nie sú kritické. Tento typ správy napríklad obsahuje informácie o činnosti súčasti **Filtrovanie obsahu**. Informačné správy majú zelenú farbu.

KONFIGURAČNÉ OKNO APLIKÁCIE

Okno nastavenia aplikácie možno otvoriť z hlavného okna aplikácie (pozrite oddiel „Hlavné okno aplikácie“ na strane 50) alebo z miestnej ponuky aplikácie (pozrite oddiel „Miestna ponuka“ na strane 48). Ak chcete vyvolať toto okno, klepnite na odkaz **Nastavenie** v hornej časti hlavného okna aplikácie, alebo vyberte príslušnú voľbu z miestnej ponuky aplikácie.

Konfiguračné okno sa skladá z dvoch častí:

- Ľavá časť okna umožňuje prístup k rôznym súčastiam aplikácie, úlohám antivírusovej kontroly, úlohám aktualizácie atď.
- Pravá časť okna obsahuje zoznam nastavení súčastí, úlohy a pod. vybrané v ľavej časti okna.

ZAČÍNAME

Jedným z hlavných cieľov odborníkov spoločnosti Kaspersky Lab pri tvorbe aplikácie Kaspersky Internet Security bolo poskytnúť optimálnu konfiguráciu všetkých možností aplikácie. Skúsení i neskúsení používatelia tak môžu ihneď po inštalácii zaistiť ochranu svojho počítača bez toho, že by strávili hodiny nastavovaním.

Pre pohodlie používateľa sme spojili fázy predbežnej konfigurácie do jednotného sprievodcu počiatočným nastavením, ktorý sa spustí ihneď po nainštalovaní aplikácie. Podľa pokynov sprievodcu môžete aplikáciu aktivovať, konfigurovať nastavenie aktualizácií, obmedziť prístup k programu pomocou hesla a vykonať ďalšie nastavenie.

Počítač môže byť napadnutý škodlivým softvérom ešte pred inštaláciou aplikácie. Spustte kontrolu počítača (pozrite oddiel „Antivírusová kontrola počítača“ na strane 57), aby ste škodlivý softvér odhalili.

V dôsledku činnosti škodlivého softvéru a zlyhania systému môžu byť poškodené nastavenia vášho počítača. Spustte sprievodcu analýzou bezpečnosti, aby ste vyhládali zraniteľnosti inštalovaného softvéru a anomálie v nastavení systému.

Od okamihu inštalácie aplikácie môžu databázy, ktoré sú súčasťou balíčka databáz, zastarávať. Aktualizujte aplikáciu (pokiaľ aktualizácia neprebehla v sprievodcovi inštaláciou alebo automaticky ihneď po inštalácii aplikácie).

Súčasť Anti-Spam obsiahnutá v štruktúre aplikácie obsahuje samoučiaci algoritmus na detekciu nežiaducich správ. Spustte sprievodcu výukou súčastí Anti-Spam a skonfigurujte súčasť, aby pracovala s vašou korešpondenciou.

Po dokončení činností opísaných vyššie bude aplikácia pripravená začať činnosť. Na posúdenie úrovne ochrany počítača použite sprievodcu správou zabezpečenia (pozrite oddiel „Správa zabezpečenia“ na strane 59).

V TOMTO ODDIELI:

Výber typu siete.....	55
Aktualizácia aplikácie.....	56
Analýza bezpečnosti.....	56
Antivírusová kontrola počítača.....	57
Zapojenie sa do systému Kaspersky Security Network.....	57
Správa zabezpečenia	59
Pozastavenie ochrany.....	61

VÝBER TYPU SIETE

Po nainštalovaní aplikácie súčasť Firewall zanalyzuje aktívne sieťové spojenia na vašom počítači. Každému sieťovému spojeniu sa priradí status, ktorý určuje povolené sieťové aktivity.

Pokiaľ ste vybrali interaktívny režim činnosti aplikácie Kaspersky Internet Security, pri každom nadviazaní sieťového spojenia sa zobrazí upozornenie. V okne upozornenie teraz môžete vybrať status nových sietí:

- Verejná sieť – na pripojenie k sieťam, z ktorých nie je povolené pristupovať k vášmu počítaču zvonka. Z týchto sietí nie je taktiež povolený prístup k verejným zložkám a tlačiarňam. Tento status sa odporúča priradiť internetovým sieťam.
- Miestna sieť – na pripojenie k sieťam, z ktorých je povolený prístup k verejným zložkám a sieťovým tlačiarňam. Tento status sa odporúča priradiť chráneným miestnym sieťam, napríklad firemnej sieti.
- Dôveryhodná sieť – pri pripojení k týmto sieťam sú povolené všetky aktivity. Tento status sa odporúča priradiť len absolútne bezpečným oblastiam.

Aplikácia Kaspersky Internet Security obsahuje pre každý status sadu pravidiel, ktoré spravujú sieťové aktivity. Status siete môžete zmeniť aj neskôr po jej prvom zistení.

AKTUALIZÁCIA APLIKÁCIE

Upozornenie!

Na aktualizáciu aplikácie Kaspersky Internet Security je potrebné pripojenie k internetu.

Aplikácia Kaspersky Internet Security obsahuje databázy so signatúrami hrozieb, s príkladmi slovných spojení typických pre spam a s opismi sieťových útokov. V okamihu inštalácie aplikácie však môžu byť databázy zastarané, pretože spoločnosť Kaspersky Lab databázy i moduly aplikácie pravidelne aktualizuje.

V sprievodcovi nastavením aplikácie môžete zvoliť režim spúšťania aktualizácií. Aplikácia Kaspersky Internet Security pri východiskovom nastavení automaticky vyhľadáva aktualizácie na serveroch spoločnosti Kaspersky Lab. Pokiaľ sú na serveri nové aktualizácie, Kaspersky Internet Security ich stiahne a nainštaluje v tichom režime.

Odporúčame aplikáciu Kaspersky Internet Security ihneď po inštalácii aktualizovať, aby ste ochranu svojho počítača udržali v aktuálnom stave.

► *Ručná aktualizácia aplikácie Kaspersky Internet Security:*

1. Otvorte hlavné okno aplikácie.
2. V ľavej strane okna vyberte oddiel **Aktualizovať**.
3. Stlačte tlačidlo **Spustiť aktualizáciu**.

ANALÝZA BEZPEČNOSTI

Nežiaduce aktivity na vašom počítači, ktoré môžu byť výsledkom zlyhania systému alebo aktivácie škodlivého softvéru, môžu poškodiť nastavenie operačného systému. Okrem toho aplikácie inštalované na počítači môžu mať zraniteľné miesta, ktoré útočníci využívajú na páchanie škôd v počítači.

Aby ste tieto bezpečnostné problémy našli a odstránili, odborníci spoločnosti Kaspersky Lab odporúčajú po inštalácii aplikácie spustiť sprievodcu analýzou bezpečnosti. Sprievodca analýzou bezpečnosti vyhľadáva zraniteľnosti v inštalovaných aplikáciách a škody a anomálie v nastavení operačného systému a webového prehliadača.

► *Spustenie sprievodcu:*

1. Otvorte hlavné okno aplikácie.
2. V ľavej časti okna vyberte **Zabezpečenie systému**.
3. Spustíte úlohu **Analýza bezpečnosti**.

ANTIVÍRUSOVÁ KONTROLA POČÍTAČA

Autori škodlivého softvéru vyvíjajú veľké úsilie na zamaskovanie činnosti svojich programov, preto nemusíte prítomnosť škodlivých programov vo svojom počítači vôbec zaznamenať.

Po inštalácii na váš počítač aplikácia automaticky vykoná úlohu **Rýchla kontrola**. Táto úloha vyhľadáva a neutralizuje škodlivé programy vo vnútri objektov, ktoré sa načítajú pri spustení operačného systému.

Odborníci spoločnosti Kaspersky Lab tiež odporúčajú vykonať úlohu **Úplná kontrola**.

► *Spustenie / zastavenie úlohy antivírusovej kontroly:*

1. Otvorte hlavné okno aplikácie.
2. V ľavej časti okna vyberte oddiel **Kontrola (Úplná kontrola, Rýchla kontrola)**.
3. Klepnutím na voľbu **Spustiť kontrolu** spustíte kontrolu. Ak potrebujete úlohu zastaviť, stlačte tlačidlo **Zastaviť kontrolu** vo chvíli, keď úloha prebieha.

ZAPOJENIE SA DO SYSTÉMU KASPERSKY SECURITY NETWORK

Každý deň sa na svete objavuje veľké množstvo nových hrozieb. Aby sa zjednodušilo zhromažďovanie štatistických údajov o nových typoch hrozieb a ich zdroji a uľahčil vývoj spôsobov ich eliminácie, spoločnosť Kaspersky Lab vám umožňuje používať službu Kaspersky Security Network.

Pri používaní služby Kaspersky Security Network sa spoločnosti Kaspersky Lab odosielajú nasledujúce informácie:

- Jedinečný identifikátor, ktorý aplikácia priradila vášmu počítaču. Tento identifikátor charakterizuje nastavenie hardvéru vášho počítača a neobsahuje žiadne informácie.
- Informácie o hrozbách zistených súčasťami aplikácie. Štruktúra a obsah informácií závisí od typu zistenej hrozby.
- Informácie o systéme: verzia operačného systému, inštalované opravy „service pack“, služby a ovládače na stiahnutie, verzia prehliadača a poštového klienta, rozšírenie prehliadača, číslo inštalovanej aplikácie spoločnosti Kaspersky Lab.

Kaspersky Security Network tiež zhromažďuje rozšírené štatistické údaje, vrátane informácií o:

- spustiteľných súboroch a podpísaných aplikáciách stiahnutých na váš počítač,
- aplikáciách spustených na vašom počítači.

Štatistické informácie sa odosielajú po dokončení aktualizácie aplikácie.

Upozornenie!

Spoločnosť Kaspersky Lab zaručuje, že v rámci služby Kaspersky Security Network nedochádza k žiadnemu zhromažďovaniu ani šíreniu osobných údajov používateľov.

► Konfigurácia odosielania štatistických údajov:

1. Otvorte okno nastavenia aplikácie.
2. V ľavej časti okna vyberte oddiel **Spätná väzba**.
3. Zaškrtnutím políčka **Súhlasím so zapojením sa do systému Kaspersky Security Network** potvrdíte svoju účasť v systéme Kaspersky Security Network. Zaškrtnutím políčka **Súhlasím s posielaním rozšírených štatistík prostredníctvom frameworku systému Kaspersky Security Network** potvrdíte svoj súhlas s odoslaním rozšírených štatistických údajov.

SPRÁVA ZABEZPEČENIA

Problémy v ochrane počítača sa indikujú v hlavnom okne aplikácie zmenou farby ikony stavu ochrany a farby panelu, na ktorom sa ikona nachádza. Pokiaľ nastali v systéme ochrany problémy, odporúčame ich ihneď opraviť.



Obrázok 5: Aktuálny stav ochrany počítača

Zoznam problémov, ku ktorým došlo, ich opis a možné riešenia si môžete zobrazíť na karte **Stav** (pozrite nasledujúci obrázok), ktorá sa otvorí po klepnutí na odkaz **Opraviť teraz** (pozrite predchádzajúci obrázok).



Obrázok 6: Riešenie bezpečnostných problémov

Môžete si zobrazíť zoznam existujúcich problémov. Problémy sa zobrazujú podľa toho, aké dôležité je ich vyriešenie: najprv najkritickejšie problémy, čo sú problémy s červenou stavovou ikonou, potom menej dôležité problémy s žltou stavovou ikonou a nakoniec informatívne správy. Pri každom probléme je k dispozícii podrobný opis a nasledujúce akcie:

- **Ihneď odstrániť.** Pomocou príslušných tlačidiel môžete prejsť k oprave problému, čo je odporúčaná akcia.
- **Odložiť odstránenie.** Pokiaľ z nejakého dôvodu nie je možné problém okamžite odstrániť, môžete odstránenie odložiť a vrátiť sa k nemu neskôr. Na to použite tlačidlo **Skrýť správu**.

Všimnite si, že táto voľba nie je k dispozícii v prípade vážnych problémov. Medzi takéto problémy patria napríklad zistené a nedezinfikované škodlivé objekty, havárie jednej alebo niekoľkých súčastí, alebo poškodenie súborov aplikácie.

Aby sa skryté správy vo všeobecnom zozname znova objavili, zaškrtnite políčko **Zobraziť skryté správy**.

POZASTAVENIE OCHRANY

Pozastavenie ochrany znamená dočasné vypnutie všetkých súčastí ochrany na určitý čas.

► Pozastavenie ochrany počítača:

1. Vyberte položku **Pozastavenie ochrany** z **miestnej ponuky** aplikácie (pozrite oddiel „Miestna ponuka“ na strane 48).
2. V dialógovom okne **Pozastaviť ochranu**, ktoré sa zobrazí, vyberte čas, za aký má byť ochrana znova povolená:
 - **Za <časový interval>** – ochrana sa povolí po uplynutí zadaného časového intervalu. Pre výber časovej hodnoty intervalu použite rozbaľovaciu ponuku.
 - **Po reštarte** – ochrana sa obnoví po reštarte systému (za predpokladu, že je povolený režim spustenia aplikácie po zapnutí počítača).
 - **Ručne** – ochrana sa povolí až potom, keď ju ručne spustíte. Ak chcete ochranu povoliť, vyberte položku **Obnoviť ochranu** z miestnej ponuky aplikácie.

Pokiaľ dočasne vypnete ochranu, budú pozastavené všetky súčasti ochrany. To je indikované takto:

- Neaktívne (sivé) názvy vypnutých súčastí v oddieli **Ochrana** v hlavnom okne.
- Neaktívna (sivá) ikona aplikácie (pozrite oddiel „Ikona v oznamovacej oblasti“ na strane 47) na systémovej lište.
- Červená farba stavovej ikony a panelu hlavného okna aplikácie.

Pokiaľ boli pri pozastavenej ochrane nadviazané sieťové spojenia, zobrazí sa upozornenie na ich prerušenie.

OVERENIE NASTAVENIA APLIKÁCIE

Po nainštalovaní a konfigurácii aplikácie môžete skontrolovať správne nastavenie aplikácie pomocou testovacieho „vírusu“ a jeho rôznych foriem. Pre každú súčasť ochrany / protokol sa vykoná samostatný test.

V TOMTO ODDIELI:

Testovací „vírus“ EICAR a jeho varianty	63
Testovanie ochrany dátového toku HTTP	66
Testovanie ochrany dátového toku SMTP	67
Overenie nastavenia súčasti File Anti-Virus	68
Overenie nastavenia úlohy antivírusovej kontroly	68
Overenie nastavenia súčasti Anti-Spam	69

TESTOVACÍ „VÍRUS“ EICAR A JEHO VARIANTY

Tento testovací „vírus“ bol organizáciou **eicar** (European Institute for Computer Antivirus Research) vytvorený špeciálne pre testovanie antivírusových produktov.

Skúšobný „vírus“ NIE JE SKUTOČNÝ VÍRUS, pretože neobsahuje kód, ktorý by mohol poškodiť počítač. Väčšina výrobcov antivírusových programov ho však za vírus označuje.

Upozornenie!

Nikdy nepoužívajte na testovanie funkčnosti antivírusového programu skutočné vírusy!

Tento „vírus“ si môžete stiahnuť z oficiálnej webovej stránky organizácie EICAR na adrese: http://www.eicar.org/anti_virus_test_file.htm.

Poznámka

Než súbor stiahnete, musíte vypnúť antivírusovú ochranu, pretože inak by aplikácia identifikovala a spracovala súbor *anti_virus_test_file.htm* ako nakazený objekt prenášaný protokolom HTTP.

Nezabudnite ihneď po stiahnutí skúšobného „vírusu“ znova aktivovať antivírusovú ochranu.

Aplikácia identifikuje súbory stiahnuté z internetových stránok **EICAR** ako napadnutý objekt obsahujúci vírus, ktorý **nemožno dezinfikovať**, a vykoná akcie určené pre takýto objekt.

Na overenie činnosti aplikácie môžete tiež použiť modifikácie štandardného testovacieho „vírusu“. Ak to chcete vykonať, zmeňte obsah štandardného „vírusu“ tak, že k nemu pridáte jednu z predpôn (pozrite nasledujúcu tabuľku). Na úpravu testovacieho „vírusu“ môžete použiť ľubovoľný textový alebo hypertextový editor, napríklad **Microsoft Notepad**, **UltraEdit32** atď.

Upozornenie!

Správnu činnosť antivírusovej aplikácie možno pomocou upraveného „vírusu“ EICAR otestovať len v prípade, že ste antivírusové databázy naposledy aktualizovali 24. októbra 2003 alebo neskôr (október 2003, súhrnné aktualizácie).

V prvom stĺpci sú uvedené predpony, ktoré treba pridať na začiatok reťazca štandardného testovacieho „vírusu“. V druhom stĺpci sú uvedené všetky možné stavy, ktoré antivírusová aplikácia priradí objektu na základe výsledku kontroly. Tretí stĺpec obsahuje informácie, ako aplikácia spracováva objekty s príslušným stavom. Pamätajte, že akcie, ktoré sa majú s objektmi vykonať, sa určia v závislosti od hodnôt nastavenia aplikácie.

Po pridaní predpony k testovaciemu „vírusu“ uložte nový súbor pod iným názvom, napríklad: *ecar_dele.com*. Podobné názvy použite pre všetky upravené „vírusy“.

Tabuľka 6. Úpravy testovacieho „vírusu“

Predpona	Stav objektu	Informácie o spracovaní objektu
Žiadna predpona, štandardný testovací vírus	Napadnutý. Napadnutý objekt obsahuje kód známeho vírusu. Dezinfekcia nie je možná.	Aplikácia identifikuje objekt ako vírus, ktorý nemožno dezinfikovať. Pri pokuse o dezinfekciu objektu dôjde k chybe; vykoná sa akcia určená pre objekty, ktoré nemožno dezinfikovať.
CORR–	Poškodený.	Aplikácia mohla k objektu pristupovať, ale nemohla ho skontrolovať, pretože je poškodený (napríklad je porušená štruktúra súboru alebo je neplatný formát súboru). Informácie o spracovaní objektu možno nájsť v správe o činnosti aplikácie.
WARN–	Podozrivý. Podozrivý objekt obsahuje kód neznámeho vírusu. Dezinfekcia nie je možná.	Objekt bol vyhodnotený ako podozrivý na základe heuristickej analýzy kódu. V čase detekcie databázy antivírusu neobsahujú žiadny postup dezinfekcie tohto objektu. Akonáhle je taký objekt zistený, obdržíte upozornenie.
SUSP–	Podozrivý. Podozrivý objekt obsahuje upravený kód známeho vírusu. Dezinfekcia nie je možná.	Aplikácia rozpoznala čiastočnú zhodu nejakej sekcie kódu objektu so sekciou kódu známeho vírusu. V čase detekcie databázy antivírusu neobsahujú žiadny postup dezinfekcie tohto objektu. Akonáhle je taký objekt zistený, obdržíte upozornenie.

Predpona	Stav objektu	Informácie o spracovaní objektu
ERRO-	Chyba kontroly:	V priebehu kontroly objektu došlo k chybe. Aplikácii sa nepodarilo získať prístup k objektu: bola narušená integrita objektu (napríklad viacväzkový archív bez konca) alebo objekt nie je pripojený (pokiaľ sa kontrolovaný objekt nachádza na sieťovej jednotke). Informácie o spracovaní objektu možno nájsť v správe o činnosti aplikácie.
CURE-	Napadnutý. Napadnutý objekt obsahuje kód známeho vírusu. Možno dezinfikovať.	Objekt obsahuje vírus, ktorý sa dá dezinfikovať. Aplikácia vykoná dezinfekciu objektu; text tela „vírusu“ bude nahradený slovom CURE. Akonáhle je taký objekt zistený, obdržíte upozornenie.
DELE-	Napadnutý. Napadnutý objekt obsahuje kód známeho vírusu. Dezinfekcia nie je možná.	Aplikácia identifikuje objekt ako vírus, ktorý nemožno dezinfikovať. Pri pokuse o dezinfekciu objektu dôjde k chybe; vykoná sa akcia určená pre objekty, ktoré nemožno dezinfikovať. Akonáhle je taký objekt zistený, obdržíte upozornenie.

TESTOVANIE OCHRANY DÁTOVÉHO TOKU HTTP

- *Kontrolu zisťovania vírusov v dátovom toku prenášanom protokolom HTTP vykoná takto:*

Pokúste sa stiahnuť testovací „vírus“ z oficiálnych webových stránok organizácie EICAR na adrese: http://www.eicar.org/anti_virus_test_file.htm.

Pri pokuse o stiahnutie testovacieho „vírusu“ aplikácie Kaspersky Internet Security tento objekt zistí, identifikuje ho ako napadnutý objekt, ktorý nemožno dezinfikovať, a vykoná akciu určenú pre tento typ objektu v nastavení pre dátový tok HTTP. Pokiaľ sa pri východiskovom nastavení pokúsite stiahnuť skúšobný „vírus“, pripojenie k stránke bude ukončené a prehliadač zobrazí informačnú správu signalizujúcu, že tento objekt je napadnutý vírusom EICAR-Test-File.

TESTOVANIE OCHRANY DÁTOVÉHO TOKU SMTP

Na detekciu vírusov v dátových tokoch prenášaných protokolom SMTP môžete použiť e-mailový systém, ktorý pre prenos dát používa tento protokol.

Poznámka

Odporúčame otestovať, ako Kaspersky Internet Security spracováva prichádzajúce a odchádzajúce e-mailové správy, a to tak telo správy, ako aj jej prílohy. Vyhľadávanie vírusov v tele správy vyskúšate tak, že do tela správy skopírujete text štandardného testovacieho „vírusu“ alebo upraveného „vírusu“.

► Postupujte takto:

1. Pomocou e-mailového klienta nainštalovaného na svojom počítači vytvorte správu vo formáte **prostého textu**.

Poznámka

Správa obsahujúca testovací vírus sa neskontroluje, pokiaľ je vytvorená vo formáte RTF alebo HTML!

2. Skopírujte text štandardného alebo upraveného „vírusu“ na začiatok správy, alebo k správe pripojte súbor obsahujúci testovací „vírus“.
3. Pošlite správu administrátorovi.

Aplikácia zistí objekt a označí ho za napadnutý. Odoslanie správy obsahujúcej infikovaný objekt bude blované.

OVERENIE NASTAVENIA SÚČASTI FILE ANTI-VIRUS

- ▶ *Správnosť nastavenia súčasti File Anti-Virus (antivírusové kontroly súborov) overíte takto:*
 1. Vytvorte na disku zložku a skopírujte testovací vírus stiahnutý z oficiálnych webových stránok organizácie (http://www.eicar.org/anti_virus_test_file.htm) i úpravy testovacieho vírusu, ktoré ste vytvorili.
 2. Povoľte protokolovanie všetkých udalostí, aby sa do správy uložili údaje o poškodených objektoch a objektoch, ktoré neboli skontrolované kvôli chybám.
 3. Spustíte testovací „vírus“ alebo súbor s jeho modifikáciou.

Súčasť File Anti-Virus zachytí volanie súboru, súbor skontroluje a vykoná akciu určenú v nastavení. Výberom rôznych akcií, ktoré sa majú vykonať so zisteným objektom, môžete plne preveriť činnosť súčasti.

V správe o činnosti súčasti File Anti-Virus si môžete prezrieť informácie o výsledkoch činnosti súčasti.

OVERENIE NASTAVENIA ÚLOHY ANTIVÍRUSOVEJ KONTROLY

- ▶ *Správnosť nastavenia úlohy antivírusovej kontroly overíte takto:*
 1. Vytvorte na disku zložku a skopírujte testovací vírus stiahnutý z oficiálnych webových stránok organizácie (http://www.eicar.org/anti_virus_test_file.htm) i úpravy testovacieho vírusu, ktoré ste vytvorili.
 2. Vytvorte novú úlohu antivírusovej kontroly a ako objekt na kontrolu vyberte zložku, ktorá obsahuje sadu testovacích „vírusov“.

3. Povoľte protokolovanie všetkých udalostí, aby sa do správy uložili údaje o poškodených objektoch a objektoch, ktoré neboli skontrolované kvôli chybám.
4. Spustíte úlohu antivírusovej kontroly.

Keď je úloha antivírusovej kontroly spustená, pri zistení podozrivých alebo nakazených objektov sa vykonajú akcie zadané v nastavení úlohy. Výberom rôznych akcií, ktoré sa majú vykonať so zisteným objektom, môžete plne preveriť činnosť súčasti.

V správe o činnosti súčasti si môžete prezrieť úplné informácie o výsledkoch úlohy.

OVERENIE NASTAVENIA SÚČASTI ANTI-SPAM

Na overenie ochrany proti spamu môžete použiť testovaciu správu označenú ako SPAM.

Telo testovacej správy musí obsahovať tento riadok:

```
Spam is bad do not send it
```

Akonáhle počítač túto správu prijme, aplikácia ju skontroluje, priradí jej status spamu a vykoná akciu určenú pre objekty tohto typu.

KASPERSKY SECURITY NETWORK – VYHLÁSENIE O ZHROMAŽĎOVANÍ DÁT

ÚVOD

PROSÍM, POZORNE SI PREČÍTAJTE TENTO DOKUMENT. OBSAHUJE DÔLEŽITÉ INFORMÁCIE, KTORÉ BY STE MALI VEDIEŤ EŠTE PRED TÝM, NEŽ ZAČNETE VYUŽÍVAŤ NAŠE SLUŽBY ALEBO NÁŠ SOFTVÉR. AK BUDETE NAĎALEJ POUŽÍVAŤ SOFTVÉR A SLUŽBY SPOLOČNOSTI KASPERSKY LAB, BUDE TO POVAŽOVANÉ ZA VÁŠ SÚHLAS S TÝMTO VYHLÁSENÍM O ZHROMAŽĎOVANÍ DÁT SPOLOČNOSTÍ KASPERSKY LAB. Vyhradzuje si právo kedykoľvek zmeniť toto Vyhlásenie o zhromažďovaní dát umiestnením zmien na túto webovú stránku. Skontrolujte prosím nižšie uvedené dátum revízie, aby ste zistili, či sa vyhlásenie od chvíle, kedy ste ho naposledy čítali, nezmenilo. Používaním akejkoľvek časti služieb spoločnosti Kaspersky Lab po zverejnení aktualizovaného Vyhlásenia o zhromažďovaní dát potvrdzujete, že so zmenami súhlasíte.

Spoločnosť Kaspersky Lab a pridružené spoločnosti (ďalej spoločne nazývané „**spoločnosť Kaspersky Lab**“) vytvorili toto Vyhlásenie o zhromažďovaní dát, aby verejne informovali o svojich zásadách pri zhromažďovaní a šírení dát v súvislosti s produktmi Kaspersky Anti-Virus a Kaspersky Internet Security.

Slovo od spoločnosti Kaspersky Lab

Spoločnosť Kaspersky Lab usiluje o poskytovanie špičkových služieb všetkým svojim zákazníkom a plne chápe vaše obavy zo zhromažďovania dát. Sme si vedomí, že sa môžete pýtať, ako systém Kaspersky Security Network zhromažďuje a využíva informácie a dáta, a pripravili sme toto vyhlásenie, aby sme vás informovali o zásadách zhromažďovania dát, ktorými sa systém Kaspersky Security Network riadi („**Vyhlásenie o zhromažďovaní dát**“ alebo len „**Vyhlásenie**“).

Toto Vyhlásenie o zhromažďovaní dát obsahuje celý rad všeobecných i technických podrobností o opatreniach, ktoré činíme, aby sme rešpektovali vaše obavy zo zhromažďovania dát. Toto Vyhlásenie o zhromažďovaní dát sme usporiadali podľa hlavných procesov a oblastí, aby ste mohli rýchlo nájsť informácie, ktoré vás najviac zaujímajú. Hlavným princípom je, že splnenie vašich potrieb a očakávaní je základom všetkého, čo robíme – vrátane ochrany zhromaždených dát.

Dáta a informácie zhromažďuje spoločnosť Kaspersky Lab; ak máte po prečítaní tohto Vyhlásenia o zhromažďovaní dát nejaké otázky alebo ste znepokojení, pošlite prosím e-mail na adresu support@kaspersky.com.

Čo je Kaspersky Security Network?

Služba Kaspersky Security Network umožňuje používateľom bezpečnostných produktov spoločnosti Kaspersky Lab z celého sveta pomáhať s uľahčením identifikácie nových bezpečnostných rizík namierených na váš počítač a so skracovaním času potrebného na poskytnutie ochrany pred týmito rizikami. S cieľom identifikácie nových hrozieb a ich zdrojov, zlepšenia bezpečnosti používateľov a vylepšenia funkčnosti produktov systém Kaspersky Security Network zhromažďuje vybrané bezpečnostné a aplikačné dáta o potenciálnych bezpečnostných rizikách namierených na váš počítač a odosiela ich spoločnosti Kaspersky Lab na analýzu. **Tieto informácie neobsahujú žiadne informácie, podľa ktorých možno identifikovať osobu používateľa, a spoločnosť Kaspersky Lab ich využíva len na účel vylepšenia svojich bezpečnostných produktov a ďalšieho vývoja riešení namierených proti škodlivým hrozbám a vírusom. V prípade náhodného prenosu osobných údajov používateľa spoločnosť Kaspersky Lab tieto údaje uchováva a chráni v súlade s týmto Vyhlásením o zhromažďovaní dát.**

Účasťou v systéme Kaspersky Security Network vy i ostatní používatelia bezpečnostných produktov spoločnosti Kaspersky Lab z celého sveta významne prispievate k bezpečnejšiemu prostrediu na internete.

Právne otázky

Systém Kaspersky Security Network môže podliehať právnym predpisom niekoľkých jurisdikcií, pretože jeho služby možno používať v rôznych jurisdikciách, vrátane Spojených štátov amerických. Spoločnosť Kaspersky Lab vyzradí informácie, podľa ktorých možno identifikovať osoby, bez vášho súhlasu len v prípade, že to vyžaduje zákon, alebo v dobrej viere, že je to nevyhnutné na vyšetrovanie škodlivých činností namierených proti návštevníkom, hosťom, partnerom a majetku spoločnosti Kaspersky Lab alebo proti iným, alebo na ochranu pred takýmito činnosťami. Ako je uvedené vyššie, zákony týkajúce sa dát a informácií, ktoré systém Kaspersky Security Network zhromažďuje, sa v rôznych krajinách môžu líšiť. Napríklad niektoré informácie, podľa ktorých možno identifikovať osoby a ktoré sú zhromažďované v Európskej únii a ich členských štátoch, sú predmetom smerníc EÚ o osobných údajoch, súkromí a elektronických komunikáciách, predovšetkým smernice Európskeho parlamentu a Rady 2002/58/ES zo dňa 12. júla 2002 o spracovaní osobných údajov a ochrane súkromia v odvetví elektronických komunikácií a smernice Európskeho parlamentu a Rady 95/46/ES zo dňa 24. októbra 1995 o ochrane fyzických osôb v súvislosti so spracovaním osobných údajov o voľnom pohybe týchto údajov a následných právnych predpisov prijatých v členských štátoch EÚ, rozhodnutia Európskej komisie 2001/497/ES o štandardných zmluvných

doložkách (poskytovanie osobných údajov do tretích krajín) a následných právnych predpisov prijatých v členských štátoch ES.

Kaspersky Security Network riadne informuje dotknutých používateľov pri počiatocnom zhromažďovaní vyššie uvedených informácií o akomkoľvek poskytovaní týchto informácií, predovšetkým na účely rozvoja podnikania, a umožní týmto používateľom internetu online **vyjadriť súhlas** (v členských štátoch ES a ďalších krajinách vyžadujúcich udelenie súhlasu) alebo vyjadriť nesúhlas (vo všetkých ostatných krajinách) s komerčným využívaním týchto dát alebo prenosom týchto dát tretím stranám.

Policajné alebo súdne orgány môžu vyžadovať, aby spoločnosť Kaspersky Lab poskytla niektoré informácie, podľa ktorých je možné identifikovať osoby, príslušným štátnym orgánom. Ak budeme o to políciou alebo súdom požiadaní, po obdržaní príslušných dokumentov tieto informácie poskytneme. Spoločnosť Kaspersky Lab môže rovnako poskytnúť informácie policajným orgánom, aby v súlade s právnymi predpismi chránila svoje vlastníctvo a zdravie a bezpečnosť osôb.

Vyhlásenia orgánom na ochranu osobných údajov v členských štátoch budú vykonané podľa príslušných platných právnych predpisov členských štátov EÚ. Informácie o týchto vyhláseniach budú prístupné prostredníctvom služieb Kaspersky Security Network.

ZHROMAŽĎOVANÉ INFORMÁCIE

Dáta, ktoré zhromažďujeme

Služba Kaspersky Security Network bude zhromažďovať základné a rozšírené údaje o potenciálnych bezpečnostných hrozbách namierených na váš počítač a odosielat' ich spoločnosti Kaspersky Lab. Zhromažďované dáta zahŕňajú:

Základné dáta

- informácie o hardvéri a softvéri vášho počítača, vrátane operačného systému a inštalovaných opráv „service pack“, objektov jadra, ovládačov, služieb, rozšírenia prehliadača Internet Explorer, rozšírenia tlače, rozšírenia Prieskumníka Windows, stiahnutých programových súborov, aktívnych inštaláčnych prvkov, appletov ovládacieho panelu, záznamov hostiteľa a registra, IP adries, typov prehliadača, e-mailových klientov a čísla verzie produktu spoločnosti Kaspersky Lab, podľa ktorých všeobecne nemožno identifikovať osoby;
- jedinečný identifikátor, ktorý produkt spoločnosti Kaspersky Lab generuje na účel identifikácie jednotlivých počítačov bez toho, že by bolo nutné identifikovať používateľa, a ktorý neobsahuje žiadne osobné údaje;

- informácie o stave antivírusovej ochrany vášho počítača, a ďalej údaje o prípadných súboroch alebo činnostiach, pri ktorých je podozrenie na škodlivý softvér (napr. názov vírusu, dátum / čas zistenia, názvy / cesty a veľkosť napadnutých súborov, IP a port sieťového útoku, názov podozrivej aplikácie). Všimnite si prosím, že vyššie uvedené dáta neobsahujú informácie, podľa ktorých možno identifikovať osoby.

Rozšírené dáta

- informácie o digitálne podpísaných aplikáciách, ktoré používateľ stiahol (URL, veľkosť súboru, názov podpisujúceho);
- informácie o spustiteľných aplikáciách (veľkosť, atribúty, vytvorené dáta, informácie o PE záhlaví, región, názov, umiestnenie a použité komprimačné utility).

Zabezpečenie prenosu a uloženie dát

Spoločnosť Kaspersky Lab usiluje o ochranu bezpečnosti informácií, ktoré zhromažďuje. Zhromažďované informácie sú uložené na počítačových serveroch s obmedzeným a riadeným prístupom. Spoločnosť Kaspersky Lab prevádzkuje zabezpečené dátové siete, ktoré sú chránené bránami firewall a systémami ochrany hesla a sú v odvetví štandardom. Spoločnosť Kaspersky Lab používa širokú škálu bezpečnostných technológií a postupov, aby chránila zhromažené informácie pred hrozbami, ako sú neoprávnený prístup, použitie alebo vyradenie. Naše bezpečnostné zásady pravidelne preskúmavame a podľa potreby rozširujeme, a k údajom, ktoré zhromažďujeme, majú prístup len preverené osoby. Spoločnosť Kaspersky Lab robí opatrenia, aby zaistila, že sa s vašimi informáciami zaobchádza bezpečne a v súlade s týmto vyhlásením. Nemožno žiaľ zaručiť bezpečnosť žiadneho prenosu dát. Výsledkom toho je, že sa síce snažíme o ochranu vašich dát, ale nemôžeme zaručiť bezpečnosť žiadnych dát, ktoré nám zasielate alebo ktoré nám zasielajú naše produkty alebo služby, vrátane systému Kaspersky Security Network, a všetky tieto služby používate na vlastné nebezpečenstvo.

Zhromažené dáta môžu byť prenesené na servery spoločnosti Kaspersky Lab a spoločnosť Kaspersky Lab učinila potrebné opatrenia, aby zaistila, že sú zhromažené informácie, pokiaľ sú prenášané, patrične chránené. Dáta, ktoré zhromažďujeme, považujeme za dôverné informácie; sú teda predmetom našich bezpečnostných postupov a firemných zásad o ochrane a používaní dôverných informácií. Akonáhle sú zhromažené dáta prijaté spoločnosťou Kaspersky Lab, sú uložené na server s funkciami fyzickej a elektronickej bezpečnosti, ako je v odvetví obvyklé, vrátane použitia postupov prihlásenia / zadania hesla a elektronickej brán firewall navrhnutých na zablokovanie neoprávneného prístupu zvonku spoločnosti Kaspersky Lab. Dáta zhromažené v rámci systému Kaspersky Security Network, ktorých sa týka toto vyhlásenie, sú spracovávané a uložené v Spojených štátoch a prípadne iných jurisdikciách, ako aj v ďalších krajinách, kde spoločnosť Kaspersky Lab podniká. Všetci zamestnanci

spoločnosti Kaspersky Lab sú si vedomí našich bezpečnostných zásad. Vaše dáta sú prístupné len zamestnancom, ktorí ich potrebujú pre svoju prácu. Žiadne uložené dáta nie sú pridružené k žiadnym informáciám, podľa ktorých možno identifikovať osoby. Spoločnosť Kaspersky Lab nespája dáta uložené v systéme Kaspersky Security Network s žiadnymi údajmi, kontaktnými zoznamami alebo informáciami o predplatnom, ktoré spoločnosť Kaspersky Lab zhromažďuje pre propagačné či iné účely.

POUŽITIE ZHROMAŽDENÝCH DÁT

Ako využívame vaše osobné informácie

Spoločnosť Kaspersky Lab dáta zhromažďuje, aby mohla analyzovať a identifikovať zdroj potenciálnych bezpečnostných rizík a zlepšiť schopnosť svojich produktov odhaľovať škodlivé správanie, podvodné webové stránky, softvér na páchanie trestnej činnosti a ďalšie typy internetových bezpečnostných hrozieb, a v budúcnosti tak poskytna svojim zákazníkom najlepšiu možnú úroveň ochrany.

Vyzeradenie informácií tretím stranám

Spoločnosť Kaspersky Lab smie vyzeradiť akékoľvek zhromaždené informácie, pokiaľ ju o to v súlade s právnymi predpismi požiada polícia, alebo na základe predvolania či iného súdneho konania, alebo pokiaľ v dobrej viere veríme, že sme povinní tak konať, aby sme neporušili platný zákon, právny predpis, predvolanie alebo iný súdny proces či vynútiteľnú požiadavku štátnych orgánov. Spoločnosť Kaspersky Lab smie taktiež vyzeradiť informácie, podľa ktorých možno identifikovať osoby, pokiaľ máme dôvod sa domnievať, že vyzeradenie týchto informácií je nevyhnutné pre identifikáciu, kontaktovanie alebo žalovanie niekoho, kto môže porušovať toto Vyhlásenie alebo podmienky zmluvy so spoločnosťou Kaspersky Lab, alebo s cieľom ochrany našich používateľov i verejnosti, alebo v rámci zmlúv o utajení a licenčných zmlúv s určitými tretími stranami, ktoré nám pomáhajú pri vývoji, prevádzke a údržbe systému Kaspersky Security Network. Na podporu povedomia o internetových bezpečnostných hrozbách, ich detekcie a prevencie môže spoločnosť Kaspersky Lab zdieľať určité informácie s výskumnými organizáciami a inými dodávateľmi bezpečnostného softvéru. Spoločnosť Kaspersky Lab taktiež môže využívať štatistické údaje odvodené od zhromaždených informácií na sledovanie trendov v oblasti bezpečnostných rizík a zverejňovania správ o týchto trendoch.

Vaše možnosti

Účasť v systéme Kaspersky Security Network je dobrovoľná. Službu Kaspersky Security Network môžete aktivovať a deaktivovať kedykoľvek, a to tak, že navštívite nastavenie Spätná väzba na stránke možností vášho produktu spoločnosti Kaspersky Lab. Pamätajte však, že pokiaľ sa rozhodnete

neposkytovať požadované informácie alebo dáta, nemusíme byť schopní poskytnúť vám niektoré služby, ktoré od zhromažďovania týchto dát závisia.

Akonáhle servisné obdobie vášho produktu od spoločnosti Kaspersky Lab skončí, niektoré funkcie softvéru spoločnosti Kaspersky Lab môžu naďalej fungovať, ale informácie sa už nebudú automaticky odosielať spoločnosti Kaspersky Lab.

Vyhradzujeme si tiež právo zasielať používateľom občasné oznámenia, aby sme ich informovali o konkrétnych zmenách, ktoré môžu ovplyvniť možnosť používať naše služby, ktoré si predtým predplatili. Taktiež si vyhradzujeme právo kontaktovať vás, pokiaľ k tomu budeme prinútení v rámci súdneho konania, alebo pokiaľ došlo k porušeniu licenčnej, záručnej či kúpnej zmluvy.

Spoločnosť Kaspersky Lab si ponecháva tieto práva, pretože sa domnievame, že v niektorých krajných prípadoch môžeme potrebovať právo vás kontaktovať v právnych alebo iných záležitostiach, ktoré pre vás môžu byť dôležité. Tieto práva nám neumožňujú kontaktovať vás s cieľom propagácie nových alebo súčasných služieb, pokiaľ ste nás požiadali, aby sme tak nečinili, a tento typ komunikácie je ojedinelý.

ZHROMAŽĎOVANIE DÁT – SÚVISIACE OTÁZKY A SŤAŽNOSTI

Spoločnosť Kaspersky Lab prijíma podnety od používateľov týkajúce sa zhromažďovania dát a venuje im maximálnu pozornosť. Pokiaľ sa domnievate, že došlo k porušeniu tohto Vyhlásenia v súvislosti s vašimi informáciami alebo dátami, alebo máte iné súvisiace otázky či podnety, môžete spoločnosti Kaspersky Lab napísať alebo ju kontaktovať na e-mailovej adrese: support@kaspersky.com.

V správe opíšte čo najpodrobnejšie podstatu svojej otázky. Vašou otázkou alebo sťažnosťou sa budeme bezodkladne zaoberať.

Poskytovanie informácií je dobrovoľné. Zhromažďovanie dát môže používateľ kedykoľvek zakázať v časti „**Spätná väzba**“ na stránke „**Nastavenie**“ príslušného produktu spoločnosti Kaspersky Lab.

Copyright © 2008 Kaspersky Lab. Všetky práva vyhradené.

KASPERSKY LAB

Spoločnosť Kaspersky Lab, založená v roku 1997, sa stala uznávanou poprednou spoločnosťou v oblasti technológií informačnej bezpečnosti. Vyvíja široký rad programov pre zabezpečenie údajov a je dodávateľom vysoko účinných antivírusových, antispamových a antihackerských systémov.

Kaspersky Lab je medzinárodná spoločnosť. Sídli v Ruskej federácii a pobočky má vo Veľkej Británii, Francúzsku, Nemecku, Japonsku, USA (Kalifornii), krajinách Beneluxu, Číne, Poľsku a Rumunsku. Vo Francúzsku bola nedávno založená nová pobočka spoločnosti, Európske antivírusové výskumné stredisko. Sieť partnerov spoločnosti Kaspersky Lab je tvorená viac než 500 spoločnosťami na celom svete.

Dnes spoločnosť Kaspersky Lab zamestnáva viac než 450 vysoko kvalifikovaných špecialistov vrátane 10 držiteľov titulu MBA a 16 držiteľov titulu PhD. Vedúci odborníci sú členovia organizácie CARO (Computer Anti-Virus Researchers Organization).

Najväčšou devízou našej spoločnosti sú jedinečné znalosti a odborné skúsenosti našich špecialistov získané v priebehu štrnástich rokov neustávajúceho boja s počítačovými vírusmi. Vďaka dôkladnej analýze aktivít počítačových vírusov dokážu špecialisti našej spoločnosti predvídať nové trendy v oblasti škodlivého softvéru a poskytnúť našim používateľom včasnú ochranu proti novým typom útokov. Odolnosť proti budúcim útokom je základnou zásadou zabudovanou do všetkých produktov spoločnosti Kaspersky Lab. V poskytovaní antivírusovej ochrany svojim klientom sú produkty spoločnosti oproti ostatným predajcom vždy o krok napred.

Vďaka dlhoročnej tvrdej práci sa spoločnosť stala jedným zo špičkových vývojárov antivírusového softvéru. Spoločnosť Kaspersky Lab bola jednou z prvých firiem svojho druhu, ktorá vyvinula najvyššie štandardy antivírusovej ochrany. Hlavný produkt spoločnosti, aplikácia Kaspersky Anti-Virus, poskytuje komplexnú ochranu na všetkých úrovniach siete – pre pracovné stanice, súborové servery, poštové systémy, brány firewall, internetové brány a vreckové počítače. Naše pohodlné a jednoduché nástroje zaisťujú maximálny stupeň automatizácie antivírusovej ochrany počítačov a firemných sietí. Mnoho známych výrobcov používa jadro aplikácie Kaspersky Anti-Virus. Na zozname týchto spoločností sú napríklad Nokia ICG (USA), F-Secure (Fínsko), Aladdin (Izrael), Sybari (USA), G Data (Nemecko), Deerfield (USA), Alt-N (USA), Microworld (India) a BorderWare (Kanada).

Zákazníkom spoločnosti Kaspersky Lab je k dispozícii široká ponuka ďalších služieb, ktoré zaisťujú stabilnú prevádzku produktov spoločnosti a súlad so

špecifickými obchodnými požiadavkami. Navrhujeme, realizujeme a udržiavame komplexné antivírusové systémy pre veľké podniky. Antivírusová databáza spoločnosti Kaspersky Lab je aktualizovaná každú hodinu. Spoločnosť svojim používateľom poskytuje nonstop technickú podporu dostupnú v niekoľkých jazykoch.

V TOMTO ODDIELI:

Ďalšie produkty spoločnosti Kaspersky Lab	77
Obráťte sa na nás.....	87

ĎALŠIE PRODUKTY SPOLOČNOSTI KASPERSKY LAB

Kaspersky Lab's News Agent

Program News Agent sa používa na rýchle doručovanie noviniek spoločnosti Kaspersky Lab, na informácie o „vírusovej predpovedi počasia“ a o najnovších udalostiach. Aplikácia v stanovenom intervale načíta zoznam dostupných spravodajských kanálov a obsiahnutých informácií zo servera noviniek spoločnosti Kaspersky Lab.

Ďalej program News Agent umožňuje:

- vizualizovať „vírusovú predpoveď počasia“ na systémovej lište,
- prihlásiť alebo odhlásiť odber noviniek zo spravodajských kanálov spoločnosti Kaspersky Lab,
- prijímať novinky zo všetkých prihlásených kanálov v stanovenom intervale, ďalej môžete dostávať upozornenia na nové neprečítané správy,
- zobrazíť novinky v prihlásených kanáloch,
- zobrazíť zoznam kanálov a ich stav,
- otvoriť v prehliadači stránky s podrobnosťami noviniek.

News Agent beží v systéme Microsoft Windows a možno ho použiť ako samostatnú aplikáciu alebo ho zahrnúť do integrovaných riešení spoločnosti Kaspersky Lab.

Kaspersky® Online Scanner

Tento program je bezplatná služba poskytovaná návštevníkom webu spoločnosti, ktorá umožňuje vykonávať účinnú antivírusovú kontrolu počítača online. Kaspersky OnLine Scanner beží vo webovom prehliadači. Týmto spôsobom môže používateľ získať rýchlu odpoveď na svoje otázky týkajúce sa napadnutia škodlivým softvérom. V priebehu kontroly používateľ môže:

- vylúčiť z kontroly archívy a e-mailové databázy,
- zvoliť pre kontrolu štandardné alebo rozšírené databázy,
- uložiť výsledky kontroly do súboru vo formáte txt alebo html.

Kaspersky® OnLine Scanner Pro

Tento program je služba poskytovaná na základe predplatného. Je k dispozícii návštevníkom webu spoločnosti a umožňuje vykonávať účinnú antivírusovú kontrolu počítača a dezinfekciu napadnutých súborov online. Kaspersky On-Line Scanner Pro sa spúšťa priamo vo vašom prehliadači. V priebehu kontroly používateľ môže:

- vylúčiť z kontroly archívy a e-mailové databázy,
- zvoliť pre kontrolu štandardné alebo rozšírené databázy,
- dezinfikovať zistené napadnuté objekty,
- uložiť výsledky kontroly do súboru vo formáte txt alebo html.

Kaspersky Anti-Virus® Mobile

Kaspersky Anti-Virus Mobile zaisťuje antivírusovú ochranu mobilných zariadení s operačnými systémami Symbian OS a Microsoft Windows Mobile. Aplikácia umožňuje vykonávanie komplexných antivírusových kontrol, vrátane:

- používateľom vyžiadané kontroly pamäte mobilného zariadenia, pamäťových kariet, jednotlivých zložiek alebo súborov. Akonáhle je zistený napadnutý súbor, je umiestnený do karantény alebo vymazaný;
- ochrany v reálnom čase: skontrolujú sa všetky prichádzajúce alebo zmenené objekty, a ďalej súbory v okamihu pokusu o prístup k nim;
- ochrany proti sms a mms spamu.

Kaspersky Anti-Virus for File Servers

Tento produkt zaisťuje spoľahlivú ochranu súborových systémov na serveroch, ktoré bežia na systémoch Microsoft Windows, Novell NetWare a Linux, proti všetkým typom škodlivého softvéru. Štruktúra tohto softvérového produktu zahŕňa nasledujúce aplikácie spoločnosti Kaspersky Lab:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Windows Server.
- Kaspersky Anti-Virus for Linux File Server.
- Kaspersky Anti-Virus for Novell Netware.
- Kaspersky Anti-Virus for Samba Server.

Výhody a funkcie:

- *ochrana súborového systému serverov v reálnom čase*: všetky súbory servera sa kontrolujú pri pokuse o ich otvorenie alebo uloženie na server;
- *prevencia vírusových epidémií*;
- *kontroluje na vyžiadanie celý súborový systém alebo jednotlivé súbory a zložky*;
- *používa optimalizačné technológie* pri kontrole objektov v súborovom systéme servera;
- *obnova systému po infekcii*;
- *škálovateľnosť softvérového produktu* podľa dostupných systémových prostriedkov;
- *udržiavanie vyrovnaného zaťaženia systému*;
- *vytvorenie zoznamu dôveryhodných procesov*, ktorých aktivita na serveri nebude týmto produktom monitorovaná;
- *vzdialená správa produktu*, vrátane centralizovanej inštalácie, konfigurácie a správy;
- *ukladanie záložných kópií napadnutých a vymazaných objektov* pre prípad nutnosti ich obnovenia;
- *izolácia podozrivých objektov* v špeciálnom úložišti;
- *upozornenia na udalosti* v priebehu spracovania produktu sa zasielajú administrátorovi systému;

- *uchovávanie podrobných správ;*
- *automatická aktualizácia databáz softvérového produktu.*

Kaspersky Open Space Security

Kaspersky Open Space Security je softvérový produkt predstavujúci nový prístup k zabezpečeniu moderných firemných sietí akéhokoľvek rozsahu a zaisťujúci centralizovanú ochranu informačných systémov a podporu vzdialeným kanceláriám a mobilným používateľom.

Tento softvérový produkt zahŕňa štyri programy:

- Kaspersky Open Space Security.
- Kaspersky Business Space Security.
- Kaspersky Enterprise Space Security.
- Kaspersky Total Space Security.

Nižšie uvádzame podrobný opis všetkých jednotlivých produktov.

Kaspersky Work Space Security je produkt navrhnutý pre poskytovanie centralizovanej ochrany pracovných staníc vo firemnej sieti i mimo nej proti všetkým typom aktuálnych internetových hrozieb: vírusom, spywaru, útokom hackerov i spamu.

Výhody a funkcie:

- *komplexná ochrana proti vírusom, útokom hackerov a spamu;*
- *proaktívna ochrana pred novým škodlivým softvérom, o ktorom nie sú v databázach zatiaľ žiadne záznamy;*
- *osobná brána firewall so systémom detekcie prienikov a prevencie sieťových útokov;*
- *možnosť vrátiť späť škodlivé zmeny vykonané v systéme;*
- *ochrana proti útokom podvodníkov (phishing) a spamu;*
- *dynamická realokácia prostriedkov pri úplnej kontrole systému;*
- *vzdialená správa produktu, vrátane centralizovanej inštalácie, konfigurácie a správy;*
- *podpora pre Cisco® NAC (Network Admission Control);*
- *kontrola e-mailovej a internetovej prevádzky v reálnom čase;*

- *blokovanie pop-up okien a reklamných líšt na internete;*
- *zabezpečenie práce v sieťach všetkých typov vrátane Wi-Fi;*
- *nástroje pre vytvorenie záchranných diskov umožňujúcich obnovu po vírusovom útoku;*
- *rozvinutý systém správ o stave ochrany;*
- *automatické aktualizácie databáz;*
- *plnohodnotná podpora 64-bitových operačných systémov;*
- *optimalizácia softvéru pre laptopy (technológia Intel® Centrino® Duo pre mobilné PC);*
- *možnosť vzdialenej dezinfekcie (technológia Intel® Active Management, súčasť Intel® vPro™).*

Kaspersky Business Space Security zaisťuje optimálnu ochranu informačných zdrojov pred aktuálnymi internetovými hrozbami. Kaspersky Business Space Security chráni pracovné stanice a databázové servery proti všetkým typom vírusov, trójskych koní a červov, predchádza vírusovým epidémiám a zaisťuje bezpečnosť informácií i okamžitý prístup k sieťovým zdrojom pre používateľov.

Výhody a funkcie:

- *vzdialená správa produktu, vrátane centralizovanej inštalácie, konfigurácie a správy;*
- *podpora pre Cisco® NAC (Network Admission Control);*
- *ochrana pracovných staníc a súborových serverov pred všetkými typmi internetových hrozieb;*
- *použitie technológie iSwift pre zamedzenie opakovaných kontrol v rámci siete;*
- *distribúcia záťaže medzi jednotlivé procesory servera;*
- *izolácia podozrivých objektov v špeciálnom úložišti;*
- *možnosť vrátiť späť škodlivé zmeny vykonané v systéme;*
- *škálovateľnosť softvérového produktu podľa dostupných systémových prostriedkov;*
- *proaktívna ochrana pracovných staníc pred novým škodlivým softvérom, o ktorom neboli do databáz zatiaľ pridané žiadne záznamy;*

- kontrola e-mailovej a internetovej prevádzky v reálnom čase;
- osobná brána firewall so systémom detekcie prienikov a prevencie sieťových útokov;
- ochrana činnosti v bezdrôtových sieťach Wi-Fi;
- technológia sebaochrany antivírusu pred škodlivým softvérom;
- izolácia podozrivých objektov v špeciálnom úložišti;
- automatické aktualizácie databáz.

Kaspersky Enterprise Space Security

Tento softvérový produkt zahŕňa súčasti na ochranu pracovných staníc a tímových serverov proti všetkým typom najnovších internetových hrozieb, odstraňuje vírusy z e-mailových dátových tokov, zaisťuje bezpečnosť informácií a bezprostredný prístup používateľov k sieťovým prostriedkom.

Výhody a funkcie:

- ochrana pracovných staníc a serverov pred vírusmi, trójskymi koňmi a červami;
- ochrana poštových serverov Sendmail, Qmail, Postfix a Exim;
- kontrola všetkých správ na serveri Microsoft Exchange vrátane zdieľaných zložiek;
- kontrola správ, databáz a ostatných objektov serverov Lotus Domino;
- ochrana proti útokom podvodníkov (phishing) a spamu;
- ochrana proti hromadnému rozosielaniu pošty a vírusovým epidémiám;
- škálovateľnosť softvérového produktu podľa dostupných systémových prostriedkov;
- vzdialená správa produktu, vrátane centralizovanej inštalácie, konfigurácie a správy;
- podpora pre Cisco® NAC (Network Admission Control);
- proaktívna ochrana pracovných staníc pred novým škodlivým softvérom, o ktorom neboli do databáz zatiaľ pridané žiadne záznamy;

- *osobná brána firewall so systémom detekcie prienikov a prevencie sieťových útokov;*
- *bezpečná práca v bezdrôtových sieťach Wi-Fi;*
- *kontrola internetového dátového toku v reálnom čase;*
- *možnosť vrátiť späť škodlivé zmeny vykonané v systéme;*
- *dynamická realokácia prostriedkov pri úplnej kontrole systému;*
- *izolácia podozrivých objektov v špeciálnom úložišti;*
- *rozvinutý systém správ o stave systému ochrany;*
- *automatické aktualizácie databáz.*

Kaspersky Total Space Security

Toto riešenie kontroluje všetky prichádzajúce a odchádzajúce dátové toky – e-mail, web a všetku komunikáciu po sieti. Produkt zahŕňa súčasti na ochranu pracovných staníc a mobilných zariadení, zaisťuje okamžitý a bezpečný prístup používateľa k firemným informačným zdrojom a k internetu a zaručuje bezpečnú e-mailovou komunikáciu.

Výhody a funkcie:

- *komplexná ochrana pred vírusmi, útokmi hackerov a spamom na všetkých úrovniach firemnej siete, od pracovných staníc až po internetové brány;*
- *proaktívna ochrana pracovných staníc pred novým škodlivým softvérom, o ktorom neboli do databáz zatiaľ pridané žiadne záznamy;*
- *ochrana poštových serverov a zdieľaných serverov;*
- *kontrola webového dátového toku (HTTP / FTP) prichádzajúceho z lokálnej siete v reálnom čase;*
- *škálovateľnosť softvérového produktu podľa dostupných systémových prostriedkov;*
- *blokovanie prístupu z napadnutých pracovných staníc;*
- *prevencia vírusových epidémií;*
- *centralizované správy o stave ochrany;*

- *vzdialená správa produktu, vrátane centralizovanej inštalácie, konfigurácie a správy;*
- *podpora pre Cisco® NAC (Network Admission Control);*
- *podpora hardvérových proxy serverov;*
- *filtrovanie internetovej prevádzky podľa zoznamu dôveryhodných serverov, typov objektov a skupín používateľov;*
- *použitie technológie iSwift pre zamedzenie opakovaných kontrol v rámci siete;*
- *dynamická realokácia prostriedkov pri úplnej kontrole systému;*
- *osobná brána firewall so systémom detekcie prienikov a prevencie sieťových útokov;*
- *zabezpečená práca v sieťach všetkých typov vrátane Wi-Fi;*
- *ochrana proti útokom podvodníkov (phishing) a spamu;*
- *možnosť vzdialenej dezinfekcie (technológia Intel® Active Management, súčasť Intel® vPro™);*
- *možnosť vrátiť späť škodlivé zmeny vykonané v systéme;*
- *technológia sebaochrany antivírusu pred škodlivým softvérom;*
- *plnohodnotná podpora 64-bitových operačných systémov;*
- *automatické aktualizácie databáz.*

Kaspersky Security for Mail Servers

Softvérový produkt na ochranu poštových serverov a zdieľaných serverov pred škodlivým softvérom a spamom. Produkt zahŕňa aplikácie na ochranu všetkých populárnych poštových serverov: Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix a Exim a umožňuje určenie dedikovanej e-mailovej brány. Riešenie zahŕňa:

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.
- Kaspersky Anti-Virus for Lotus Notes/Domino.
- Kaspersky Anti-Virus for Microsoft Exchange.

- Kaspersky Anti-Virus® for Linux Mail Server.

Medzi schopnosti tohto programu patrí:

- *spoľahlivá ochrana pred škodlivým softvérom a potenciálne nebezpečnými programami;*
- *filtrovanie spamu;*
- *kontrola prichádzajúcich a odchádzajúcich e-mailových správ a príloh;*
- *antivírusová kontrola všetkých správ na serveri Microsoft Exchange vrátane zdieľaných zložiek;*
- *kontrola správ, databáz a ostatných objektov serverov Lotus Domino;*
- *filtrovanie správ podľa typov príloh;*
- *izolácia podozrivých objektov v špeciálnom úložišti;*
- *pohodlný systém správy softvérového produktu;*
- *prevencia vírusových epidémií;*
- *sledovanie stavu ochranného systému pomocou upozornenia;*
- *system správ o činnosti aplikácie;*
- *škálovateľnosť softvérového produktu podľa dostupných systémových prostriedkov;*
- *automatické aktualizácie databáz.*

Kaspersky Security for Gateways

Tento softvérový produkt zaisťuje bezpečný prístup k internetu všetkým zamestnancom spoločnosti, pretože automaticky odstraňuje škodlivý softvér a riskware z dátového toku prichádzajúceho do siete prostredníctvom protokolov HTTP/FTP. Riešenie zahŕňa:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Proxy Server.
- Kaspersky Anti-Virus for Microsoft ISA Server.
- Kaspersky Anti-Virus for Check Point FireWall-1.

Medzi schopnosti tohto programu patrí:

- *spoľahlivá ochrana pred škodlivým softvérom a potenciálne nebezpečnými programami;*
- *kontrola internetovej prevádzky (HTTP/FTP) v reálnom čase;*
- *filtrovanie internetovej prevádzky podľa zoznamu dôveryhodných serverov, typov objektov a skupín používateľov;*
- *izolácia podozrivých objektov v špeciálnom úložišti;*
- *pohodlný riadiaci systém;*
- *system správ o činnosti aplikácie;*
- *podpora hardvérových proxy serverov;*
- *škálovateľnosť softvérového produktu podľa dostupných systémových prostriedkov;*
- *automatické aktualizácie databáz.*

Kaspersky® Anti-Spam

Kaspersky Anti-Spam je prvý ruský softvérový balíček zaisťujúci ochranu pred spamom pre malé a stredne veľké spoločnosti. Tento produkt je kombináciou revolučných technológií lingvistickej analýzy textu, všetkých moderných metód filtrovania pošty (vrátane čiernej listiny DNS a formálnych atribútov správ) a unikátnej sady služieb, čo umožňuje používateľovi detekovať a odstrániť až 95 percent nežiaduceho dátového toku.

Kaspersky Anti-Spam je filter umiestnený na „vstupe“ do firemnej siete, ktorý kontroluje výskyt spamu v prichádzajúcich správach. Je kompatibilný s ktorýmkoľvek e-mailovým systémom používaným v sieti klienta a môže byť nainštalovaný na existujúci e-mailový server alebo na vyhradený server.

Vysoká účinnosť programu je zaručená každodennou automatickou aktualizáciou databáz na filtrovanie obsahu s použitím vzoriek zasielaných odborníkmi z lingvistického laboratória. Aktualizácie sa zverejňujú každých 20 minút.

Kaspersky Anti-Virus® for MIMESweeper

Kaspersky® Anti-Virus for MIMESweeper zaručuje rýchlu antivírusovú kontrolu dátového toku na serveroch, ktoré používajú systém Clearswift MIMESweeper for SMTP / Clearswift MIMESweeper for Exchange / Clearswift MIMESweeper for Web.

Táto aplikácia je realizovaná ako modul plug-in (rozširujúci modul) a vykonáva v reálnom čase antivírusovú kontrolu a spracovanie prichádzajúcich a odchádzajúcich e-mailových správ.

OBRÁŤTE SA NA NÁS

Ak máte otázky, môžete kontaktovať našich predajcov alebo priamo spoločnosť Kaspersky Lab. Konzultácie sú poskytované telefonicky alebo prostredníctvom e-mailu. Každú otázku vám plne a zrozumiteľne vysvetlíme.

Adresa:	Rusko, 123060, Moskva, 1-st Volokolamsky Proezd, 10, Building 1
Tel., Fax:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00
Podpora 24/7 pre prípad núdze	+7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08
Podpora pre používateľov firemných produktov:	+7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08 (od 10 do 19 hod.) http://support.kaspersky.com/helpdesk.html
Podpora pre firemných zákazníkov:	kontaktné informácie budú poskytnuté po zakúpení firemného produktu v závislosti od zakúpeného balíčka technickej podpory.
Webové fórum spoločnosti Kaspersky Lab:	http://forum.kaspersky.com
Antivírusové laboratórium:	newvirus@kaspersky.com (Ien pre posielanie nových vírusov v archívoch)
Tím pre vytváranie používateľskej dokumentácie	docfeedback@kaspersky.com (Ien pre zasielanie spätnej väzby k dokumentácii a systému nápovedy)

Oddelenie predaja:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00 sales@kaspersky.com
Všeobecné informácie:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00 info@kaspersky.com
WWW:	http://www.kaspersky.sk http://www.viruslist.com

CRYPTOEX LLC

Pre vytvorenie a kontrolu elektronického podpisu používa aplikácia Kaspersky Anti-Virus softvérovú knižnicu na zabezpečenie dát Crypto C vyvinutú spoločnosťou Crypto Ex LLC.

Crypto Ex je držiteľom licencie pre vývoj, výrobu a distribúciu komplexných šifrovacích systémov pre zaistenie bezpečnosti dát, ktoré nie sú súčasťou štátneho tajomstva, vydané Federálnou agentúrou pre vládne komunikácie a informácie (FSB – Federálna bezpečnostná služba).

Knižnica Crypto C je určená na použitie v systémoch komplexnej ochrany dôverných informácií triedy KS1 a získala certifikát o zhode FSB č. SF/114-0901 z 1. júla 2006.

Moduly tejto knižnice používajú šifrovanie a dešifrovanie dátových paketov s pevnou dĺžkou alebo dátových tokov na základe kryptografického algoritmu (GOST 28147-89), generovanie a overovanie elektronického podpisu na základe algoritmov (GOST R 34.10-94 a GOST 34.10-2001), hashovaciu funkciu (GOST 34.11-94), generovanie informácií kľúča pomocou programového generátora pseudonáhodných čísel. Ďalej spoločnosť CryptoEx LLC implementovala systém generovania informácií kľúča a simulačných vektorov (GOST 28147-89).

Moduly knižníc boli implementované s použitím programovacieho jazyka C (podľa normy ANSI C), možno ich integrovať do aplikácií ako staticky i dynamicky zavádzaný kód a možno ich spúšťať na platformách x86, x86-64, Ultra SPARC II a kompatibilných.

Moduly knižníc možno migrovať do nasledujúcich operačných prostredí: Microsoft Windows NT/XP/98/2000/2003, Unix (Linux, FreeBSD, SCO Open Unix 8.0, SUN Solaris, SUN Solaris pre Ultra SPARC II).

Web spoločnosti CryptoEx LLC: <http://www.cryptoex.ru>

E-mail: info@cryptoex.ru

MOZILLA FOUNDATION

Pri vývoji súčastí aplikácie bola použitá knižnica **Gecko SDK ver. 1.8**.

Tento softvér je použitý v súlade s podmienkami licencie MPL 1.1 (Mozilla Public License), <http://www.mozilla.org/MPL>.

Ďalšie podrobnosti o knižnici Gecko SDK nájdete na adrese: http://developer.mozilla.org/en/docs/Gecko_SDK.

© Mozilla Foundation

Web nadácie Mozilla Foundation: <http://www.mozilla.org>.

LICENČNÁ ZMLUVA

Štandardná licenčná zmluva s koncovým používateľom

UPOZORNENIE PRE VŠETKÝCH POUŽÍVATEĽOV: POZORNE SI PREČÍTAJTE NASLEDUJÚCU ZMLUVU („ZMLUVA“) O LICENCII K APLIKÁCII KASPERSKY INTERNET SECURITY („SOFTVÉR“) VYROBENEJ SPOLOČNOSŤOU KASPERSKY LAB („KASPERSKY LAB“).

V PRÍPADE ZAKÚPENIA TOHTO SOFTVÉRU PROSTREDNÍCTVOM INTERNETU KLEPNUTÍM NA TLAČIDLO SÚHLASU (AKO FYZICKÁ OSOBA ALEBO SAMOSTATNÁ ORGANIZAČNÁ JEDNOTKA) PRISTUPUJETE NA TÚTO ZMLUVU A SÚHLASÍTE, ŽE BUDETE TOUTO ZMLUVOU VIAZANÍ. POKIAĽ NESÚHLASÍTE SO VŠETKÝMI PODMIENKAMI TEJTO ZMLUVY, KLEPNITE NA TLAČIDLO OZNAČENÉ AKO NESÚHLAS S PODMIENKAMI TEJTO ZMLUVY A SOFTVÉR NEINŠTALUJTE.

POKIAĽ STE ZAKÚPILI TENTO SOFTVÉR NA FYZICKOM MÉDIU, OTVORENÍM OBALU DISKU CD (AKO FYZICKÁ OSOBA ALEBO SAMOSTATNÁ ORGANIZAČNÁ JEDNOTKA) SÚHLASÍTE, ŽE BUDETE ZMLUVOU VIAZANÍ. AK NESÚHLASÍTE SO VŠETKÝMI PODMIENKAMI TEJTO ZMLUVY, NEPORUŠUJTE OBAL DISKU CD-ROM, NESTAHUJTE, NEINŠTALUJTE A NEPOUŽÍVAJTE TENTO SOFTVÉR.

POKIAĽ IDE O SOFTVÉR SPOLOČNOSTI KASPERSKY LAB URČENÝ PRE INDIVIDUÁLNYCH SPOTREBITEĽOV A ZAKÚPENÝ ONLINE NA WEBE SPOLOČNOSTI KASPERSKY LAB ALEBO ICH PARTNEROV, V SÚLADE S PRÁVNymi PREDPISMI MÁ ZÁKAZNÍK LEHOTU ŠTRNÁSŤ (14) PRACOVNÝCH DNÍ OD DÁTUMU DODANIA PRODUKTU NA VRÁTENIE PRODUKTU PREDAJCOVI S CIEĽOM VÝMENY ALEBO VRÁTENIA PEŇAZÍ, ZA PODMIENKY, ŽE SOFTVÉR NIE JE ROZBALENÝ.

POKIAĽ IDE O SOFTVÉR SPOLOČNOSTI KASPERSKY LAB URČENÝ PRE INDIVIDUÁLNYCH SPOTREBITEĽOV NEZAKÚPENÝ ONLINE NA INTERNETE, NIE JE MOŽNÉ TENTO SOFTVÉR VRÁTIŤ ANI VYMENIŤ, POKIAĽ PARTNERSKÝ PREDAJCA PRODUKTU NESTANOVIL INAK. V TAKOM PRÍPADE NIE JE SPOLOČNOSŤ KASPERSKY LAB VIAZANÁ USTANOVENIAMÍ TOHTO PARTNERA.

NÁROK NA VRÁTENIE PRODUKTU A REFUNDÁCIU SA VZŤAHUJE LEN NA PŮVODNÉHO KUPCA.

Všetky odkazy na „Softvér“ v tomto dokumente zahŕňajú aj aktivačný kód softvéru, ktorý vám bude poskytnutý spoločnosťou Kaspersky Lab ako súčasť aplikácie Kaspersky Internet Security 2009.

1. *Udelenie licencie.* S výhradou zaplatenia príslušných licenčných poplatkov a s výhradou podmienok tejto Zmluvy vám spoločnosť Kaspersky Lab udeľuje nevýhradné a neprevoditeľné právo na používanie jednej kópie stanovenej verzie Softvéru a sprievodnej dokumentácie („Dokumentácia“) po dobu trvania tejto Zmluvy, a to výhradne pre interné účely vášho podnikania. Môžete nainštalovať jednu kópiu Softvéru na jednom počítači.

1.1 *Používanie.* Softvér je licencovaný ako jednotlivý produkt; nemôže byť používaný na viac než jednom počítači alebo viac než jedným používateľom súčasne, ak nie je v tejto časti uvedené inak.

1.1.1 Softvér je na počítači „používaný“, keď je zavedený do dočasnej pamäte (napr. pamäte RAM) alebo inštalovaný v trvalej pamäti (napr. na pevný disk, CD-ROM, alebo iné zariadenie na ukladanie dát) tohto počítača. Táto licencia oprávňuje na vytvorenie len takého počtu záložných kópií Softvéru, aký je potrebný na jeho zákonné používanie, a to výhradne na záložné účely, za predpokladu, že všetky také kópie budú obsahovať všetky majetkoprávne upozornenia k Softvéru. Budete viesť záznamy o počte a umiestnení všetkých kópií Softvéru a Dokumentácie a podniknete všetky primerané opatrenia na ochranu Softvéru pred neoprávneným kopírovaním alebo používaním.

1.1.2 Softvér chráni počítač proti vírusom a sieťovým útokom, ktorých signatúry sú obsiahnuté v databázach signatúr hrozieb a sieťových útokov, ktoré sú k dispozícii na aktualizáčnych serveroch spoločnosti Kaspersky Lab.

1.1.3 Pokiaľ predávate počítač, na ktorom bol Softvér nainštalovaný, zaistíte, aby všetky kópie Softvéru boli predtým vymazané.

1.1.4 Žiadnu časť tohto Softvéru nesmiete dekompilovať, spätne analyzovať, prevádzkať zo strojového kódu alebo inak prevádzkať do človekom čitateľnej podoby a nesmiete taký prevod dovoliť tretej strane. Informácie o rozhraní, potrebné na zaistenie spolupráce Softvéru s nezávisle vytvorenými počítačovými programami, budú poskytnuté spoločnosťou Kaspersky Lab na požiadanie po zaplatení primeraných nákladov a výdajov na získanie a poskytnutie takých informácií. V prípade, že spoločnosť Kaspersky Lab oznámi, že tieto informácie nemá v úmysle poskytnúť, a to z akéhokoľvek dôvodu, predovšetkým nákladov, smiete podniknúť kroky na zaistenie spolupráce len s použitím spätnej analýzy alebo dekompilácie Softvéru v rozsahu povolenom zákonom.

1.1.5 Nesmiete vykonávať opravy chýb alebo inak upravovať, prispôbovať alebo prekladať Softvér, vytvárať odvodené diela od Softvéru ani dovoliť tretej strane kopírovať Softvér (inak než je v tomto dokumente výslovne dovolené).

1.1.6 Nesmiete požičiavať, prenajímať alebo poskytovať na lízing Softvér žiadnej inej osobe ani preniesť či sublicencovať vaše licenčné práva na inú osobu.

1.1.7 Nesmiete poskytnúť aktivačný kód alebo súbor licenčného kľúča tretej osobe alebo umožniť tretej osobe prístup k aktivačnému kódu alebo licenčnému kľúču. Aktivačný kód a licenčný kľúč sa považujú za dôverné.

1.1.8 Spoločnosť Kaspersky Lab môže od používateľa požadovať, aby si nainštaloval najnovšiu verziu softvéru (najnovšiu verziu a najnovší balíček Maintenance Pack).

1.1.9 Tento Softvér nesmiete používať v automatických, poloautomatických ani ručných nástrojoch určených na vytváranie signatúr vírusov, rutín na zisťovanie vírusov a akýchkoľvek dát alebo kódov na zisťovanie škodlivého kódu alebo dát.

1.1.10 Máte právo poskytnúť spoločnosti Kaspersky Lab informácie o potenciálnych hrozbách a zraniteľnostiach zo svojho počítača, podrobnosti sú uvedené vo Vyhlásení o zhromažďovaní dát. Zhromažďované informácie sa vo všeobecnej podobe používajú len na účely vylepšovania produktov spoločnosti Kaspersky Lab.

1.1.11 Na účely uvedené v bode 1.1.10 bude Softvér automaticky zhromažďovať informácie o kontrolných súčtoch súborov, ktoré sú na počítači spúšťané, a odosielať ich spoločnosti Kaspersky Lab.

Podpora¹.

- (i) Spoločnosť Kaspersky Lab vám poskytne služby podpory („Služby podpory“) podľa nižšie uvedenej definície na obdobie, ktoré je určené v súbore licenčného kľúča a uvedené v okne „Služba“, a to od okamihu aktivácie a:
 - a) zaplataenia aktuálneho poplatku za poskytovanie služieb podpory a
 - b) úspešného vyplnenia formulára Support Services Subscription Form (prihláška k službám podpory) poskytnutého s touto Zmluvou alebo dostupného na webe spoločnosti Kaspersky Lab, ktorý vyžaduje zadanie aktivačného kódu taktiež poskytnutého

¹ Ak používate demonštračnú verziu softvéru, nemáte nárok na technickú podporu uvedenú v bode 2 tejto zmluvy ani právo predať kópiu, ktorá je vo vašom vlastníctve, tretím stranám.

Ste oprávnení používať softvér na demonštračné účely po dobu špecifikovanú v súbore licenčného kľúča počnajúc okamihom aktivácie (toto obdobie uvidíte v okne Služba grafického používateľského rozhrania softvéru (GUI)).

spoločnosťou Kaspersky Lab s touto Zmluvou. Rozhodnutie, či ste splnili túto podmienku poskytovania Služieb podpory, je výhradne na uvážení spoločnosti Kaspersky Lab.

Služby podpory budú prístupné po aktivácii Softvéru. Služba technickej podpory spoločnosti Kaspersky Lab je taktiež oprávnená požadovať od vás ďalšiu registráciu s cieľom pridelenia identifikátora na poskytovanie Služieb podpory.

Až do aktivácie Softvéru alebo získania identifikátora koncového používateľa (ID zákazníka) služba technickej podpory poskytuje asistenciu len pri aktivácii Softvéru a registrácii koncového používateľa.

- (ii) Poskytovanie Služieb podpory bude ukončené, pokiaľ ich neobnovíte raz ročne zaplatením ročného poplatku aktuálneho v tom období alebo úspešným opätovným vyplnením formulára Support Services Subscription Form.
- (iii) „Službami podpory“ sa rozumie:
 - (a) pravidelné aktualizácie antivírusovej databázy,
 - (b) aktualizácia databázy sieťových útokov,
 - (c) aktualizácia antispamovej databázy,
 - (d) aktualizácia softvéru zdarma vrátane aktualizovaných verzií;
 - (e) technická podpora prostredníctvom internetu a telefónu poskytovaná Predajcom a/alebo Distribútorom;
 - (f) aktualizácia funkcií zisťovania a dezinfekcie vírusov 24 hodín denne.
- (iv) Služby podpory sa poskytujú, len pokiaľ máte vo svojom počítači nainštalovanú najnovšiu verziu Softvéru (vrátane balíčkov Maintenance Pack) dostupnú na oficiálnom webe spoločnosti Kaspersky Lab (www.kaspersky.com).

3. *Vlastnícke práva.* Softvér je chránený autorským právom. Spoločnosť Kaspersky Lab a jej dodávateľa sú vlastníčkmi a držiteľmi všetkých práv, vlastníckych nárokov a podielov v Softvéri vrátane všetkých autorských práv, patentov, ochranných známk a ďalších práv vzťahujúcich sa na duševné vlastníctvo. Držba, inštalácia ani používanie Softvéru neprenáša na vás žiadne

nároky na duševné vlastníctvo Softvéru a nezískavate žiadne práva na Softvér okrem tých, ktoré sú výslovne v tejto Zmluve uvedené.

4. *Dôvernosť*: Súhlasíme s tým, že Softvér a Dokumentácia vrátane špecifického návrhu a štruktúry jednotlivých programov predstavujú dôverné vlastnícke informácie spoločnosti Kaspersky Lab. Tieto dôverné informácie nesmiete vyzradiť, poskytnúť alebo inak sprístupniť v ľubovoľnej forme tretej strane bez predchádzajúceho písomného súhlasu zo strany spoločnosti Kaspersky Lab. Musíte realizovať primerané bezpečnostné opatrenia na ochranu týchto dôverných informácií a bez obmedzenia vyššie uvedeného musíte vyvinúť maximálne úsilie o zachovanie bezpečnosti aktivačného kódu.

5. *Obmedzená záruka*.

- i) Spoločnosť Kaspersky Lab poskytuje záruku, že počas šiestich (6) mesiacov od prvého stiahnutia alebo inštalácie Softvéru zakúpeného na fyzickom médiu bude Softvér v podstatných rysoch pracovať v súlade s funkčnosťou opísanou v Dokumentácii, pokiaľ je obsluhovaný riadne a spôsobom uvedeným v Dokumentácii.
- ii) Preberáte všetku zodpovednosť za výber tohto Softvéru tak, aby spĺňal vaše požiadavky. Spoločnosť Kaspersky Lab nezaručuje, že Softvér a/alebo Dokumentácia budú týmto požiadavkám vyhovovať, ani že ich bude možné používať bez prerušení alebo chýb.
- iii) Spoločnosť Kaspersky Lab nezaručuje, že tento Softvér identifikuje všetky známe vírusy a nevyžiadajú poшту (spam), ani že tento Softvér príležitostne chybne neoznámi vírus v súbore, ktorý týmto vírusom nie je napadnutý.
- iv) Jediná náprava a úplná zodpovednosť spoločnosti Kaspersky Lab voči vám za porušenie záruky podľa odseku i) spočíva, podľa voľby spoločnosti Kaspersky Lab, v oprave, výmene alebo vrátení peňazí za Softvér, pokiaľ túto skutočnosť oznámite spoločnosti Kaspersky Lab alebo jej zmocnencovi v priebehu záručnej lehoty. Ste povinní poskytnúť všetky informácie, ktoré môžu byť dôvodne potrebné na spoluprácu s Dodávateľom na odstránenie chybných častí.
- v) Záruka podľa odseku i) neplatí v prípade, že a) uskutočnite alebo necháte uskutočniť akékoľvek úpravy tohto Softvéru bez súhlasu spoločnosti Kaspersky Lab, b) použijete Softvér spôsobom, na ktorý nebol určený, alebo c) použijete Softvér inak, než je povolené touto Zmluvou.

- vi) Záruky a podmienky stanovené v tejto Zmluve nahrádzajú všetky iné podmienky, záruky či iné ujednania týkajúce sa dodávky, domnejšej dodávky, nedodania alebo oneskorenia dodávky Softvéru alebo Dokumentácie, ktoré by sa, nebyť tohto odseku vi), uplatnili medzi spoločnosťou Kaspersky Lab a vami, alebo by inak vyplývali alebo boli začlenené do tejto Zmluvy alebo akejkoľvek vedľajšej zmluvy, či zákona, zvykového práva alebo *inak*, a ktoré sú týmto všetky vylúčené (predovšetkým vrátane predpokladaných podmienok, záruk alebo iných ujednaní týkajúcich sa uspokojivej kvality, vhodnosti na daný účel alebo používania s primeranou zručnosťou a starostlivosťou).

6. Obmedzenie zodpovednosti.

- i) Žiadne ustanovenie tejto Zmluvy nevylučuje ani neobmedzuje zodpovednosť spoločnosti Kaspersky Lab za a) prečin podvodu, b) smrť alebo zranenie osôb spôsobené porušením všeobecnej zákonnej povinnosti o poskytnutí starostlivosti alebo akýmkoľvek nedbalým porušením niektorej podmienky tejto Zmluvy, alebo c) akúkoľvek ďalšiu zodpovednosť, ktorá nemôže byť vylúčená zo zákona.
- ii) S výhradou vyššie uvedeného odseku i) spoločnosť Kaspersky Lab nenesie zodpovednosť (zo zmluvy, prečinu, nápravy alebo inak) za žiadne z nasledujúcich strát alebo škôd (bez ohľadu na to, či tieto straty alebo škody boli predvídané, predvídateľné, známe alebo iné):
- a) strata príjmu,
 - b) strata skutočných alebo predpokladaných ziskov (vrátane straty ziskov zo zmlúv),
 - c) strata z použitia peňazí,
 - d) strata predpokladaných úspor,
 - e) obchodná strata,
 - f) strata príležitosti,
 - g) strata dobrého mena firmy,
 - h) strata dobrej povesti,
 - i) strata, poškodenie alebo porušenie dát,

- j) akékoľvek nepriame alebo následné straty alebo škody spôsobené akýmkoľvek spôsobom (vrátane, pre vylúčenie pochybností, prípadov, kedy je strata alebo škoda typu uvedeného v ods. ii) písm. a) až ods. ii) písm. i)).
- iii) S výhradou vyššie uvedeného odseku i) zodpovednosť spoločnosti Kaspersky Lab (zo zmluvy, prečinu, nápravy alebo inak) vyplývajúca z dodávky Softvéru alebo v spojitosti s ňou za žiadnych okolností neprekročí sumu rovnú sume, ktorú ste za Softvér zaplatili.

7. Táto Zmluva obsahuje úplné ujednanie medzi oboma stranami s ohľadom na jej predmet a nahrádza všetky predošlé ujednania, záruky a sľuby medzi vami a spoločnosťou Kaspersky Lab, ústne alebo písomné, ktoré boli dané alebo môžu byť predpokladané z čohokoľvek napísaného alebo ústne oznámeného na rokovaníach s nami alebo našimi zástupcami pred touto Zmluvou, a všetky predošlé zmluvy medzi stranami, ktoré sa týkajú vyššie uvedených záležitostí, strácajú účinnosť Dňom platnosti.