kaspersky

Kaspersky Basic | Standard | Plus | Premium

© 2022 AO Kaspersky Lab

Съдържание

Представяне на данни

Този раздел съдържа информация за конкретните данни, които предоставяте на Kaspersky, докато използвате приложението. Подразделът Записване на данни в отчета за работата на приложението съдържа данни, които се съхраняват локално на вашия компютър и не се изпращат на Kaspersky.

Предоставяне на данни според Лицензионното споразумение

Този раздел съдържа информация за специфични данни, които се предоставят на Kaspersky, ако сте инсталирали версията на приложението, която не е предназначена за употреба в Европейския съюз, Обединеното кралство, Бразилия или жители на Калифорния.

Данни за план Kaspersky Basic

Данни за план Kaspersky Standard

Данни за планове Kaspersky Plus и Kaspersky Premium

Kaspersky защитава получената информация според законовите изисквания и приложимите правила на Kaspersky. Данните се прехвърлят по шифровани канали.

За да подобри информираността на сигурността за нови заплахи и техните източници и за да подобри вашето ниво на защита на сигурността и работата на продукта, Притежателят на правата, с вашето съгласие, което е изрично потвърдено в Декларацията на събиране на данни на Kaspersky Security Network, има изрично право да получава такава информация. Може да изключите услугата Kaspersky Security Network по време на инсталиране. Освен това може да включвате и изключвате услугата Kaspersky Security Network по всяко време в прозореца с настройки на Софтуера.

Допълнително приемате и се съгласявате, че всяка информация, събрана от Притежателя на правата, може да се използва за проследяване и публикуване на отчети за тенденциите в рисковете за сигурността по ексклузивната преценка на Притежателя на правата.

Ако не желаете информацията, събрана от Софтуера, да бъде изпратена до Притежателя на правата, не трябва да включвате и/или изключвате услугата Kaspersky Security Network.

Предоставяне на данни според Лицензионното споразумение на територията на Европейския съюз, Обединеното кралство, Бразилия или от жители на Калифорния

Този раздел съдържа информация за специфични данни, които се предоставят на Kaspersky, ако сте инсталирали версията на приложението, която е предназначена за употреба в Европейския съюз, Обединеното кралство, Бразилия или жители на Калифорния. **Информацията, посочена в този раздел, не съдържа никакви лични данни на Потребителя и е необходима за работата на Софтуера на Притежателя на правата, освен ако изрично не е посочено друго**.

Вие се съгласявате, докато използвате софтуера, автоматично да предоставяте на Kaspersky следните данни за подобряване качеството на защитата в реално време, подобряване качеството на работата на софтуера и навременното откриване и коригиране на грешки, свързани с механизма за инсталиране, премахване и актуализиране на софтуера, отчитайки броя потребители:

Данни за планове Kaspersky Basic и Kaspersky Standard

Данни за планове Kaspersky Plus и Kaspersky Premium

За да се подобри качеството на защита на Потребителя, който извършва трансакции за плащане по интернет, вие се съгласявате да предоставяте автоматично на финансовия уеб сайт информация за името и версията на Софтуера и настройката за персонализиране на Софтуера, ИД на добавката на Софтуера в браузъра, използван за достъп до финансовия уеб сайт и ИД, който показва дали е използван защитен браузър или обикновен браузър.

Получената информация е защитена от Притежателя на правата по начина, описан от закона, и се изисква за работата на софтуера, предоставен за употреба по силата лицензa.

Kaspersky може да използва придобитите статистически данни въз основа на информацията, получена за наблюдаване на тенденциите в заплахите на компютърната сигурност, и да публикува отчетите от тези заплахи.

Предоставяне на данни на Kaspersky Security Network

Обхватът на данните, прехвърляни към Kaspersky Security Network, е описан в Декларацията на Kaspersky Security Network.

За да прегледате Декларацията на Kaspersky Security Network:

1. Отворете основния прозорец на приложението.
2. Щракнете върху бутона в долната част на прозореца на приложението.

   Отваря се прозорецът **Настройки**.
3. Отидете в **Настройки за защита** → **Kaspersky Security Network**.

   Отваря се прозорецът **Kaspersky Security Network**, който показва детайли на настройките за участие на Kaspersky Security Network и Kaspersky Security Network.
4. Щракнете върху връзката **Декларация за Kaspersky Security Network**, за да отворите текста на Декларация на Kaspersky Security Network.

Записване на данни в отчета за работата на приложението

Файловете с отчетите могат да съдържат лични данни, получени по време на работата на компонентите за защита, като например Защита на файлове, Защита за пощата, Безопасно сърфиране и Защита от спам.

Файловете с отчетите могат да съдържат следните лични данни:

- IP адрес на устройството на потребителя
- История на онлайн сърфирането
- Блокирани връзки
- История на съобщенията в социалните мрежи
- Версии на браузъра и операционната система
- Имена на бисквитки и други файлове и пътища до тях

- Имейл адрес, изпращач, тема на съобщението, текст на съобщението, потребителски имена и списък с контакти

Когато използвате компонентите Защита за деца, Умно домашно наблюдение, и Новини за сигурността, Вие подавате следните данни:

- ИД на Wi-Fi мрежа, състояние на Wi-Fi мрежа, ИД на устройство, хеш на MAC адреса на устройството, състояние на устройството;
- Информация за посетените уеб сайтове;
- Информация за броя пъти, които даден файл е бил стартиран на компютъра (популярност на файл).

Файловете с отчетите се съхраняват локално на вашия компютър и не се прехвърлят към Kaspersky. Път до файлове с отчети: %allusersprofile%\Kaspersky Lab\AVP21.8\Report\Database.

Отчетите се съхраняват в следните файлове:

- reports.db
- reports.db-wal
- reports.db-shm (не съдържа никакви лични данни)

Файловете с отчетите са защитени от неоторизиран достъп, ако самозащитата е активирана в Kaspersky. Ако самозащитата е изключена, файловете с отчетите не са защитени.

Запис на данни за техническата поддръжка

Приложението обработва и съхранява следните лични данни за допълнителен анализ от екипа за техническа поддръжка:

- Данни, които се показват в интерфейса на приложението:
  - Имейл адресът, използван за свързване към My Kaspersky
  - Адреси на уеб сайтове, които са били добавени към изключенията (показвани в компонентите Безопасно сърфиране, Защита от банери, Поверително сърфиране и Мрежа в прозореца Отчети)
  - Данни за лицензa

  Тези данни се съхраняват локално в непроменена форма и могат да бъдат преглеждани от всеки потребителски акаунт на компютъра.
- Данни за системната памет на процесите на приложението в момента, в който е създадено разтоварване на паметта.
- Данните, които се събират, когато се активират следи.

Тези данни се съхраняват локално в променена форма и могат да бъдат преглеждани от всеки потребителски акаунт на компютъра. Тези данни се прехвърлят към Kaspersky единствено с вашето съгласие, когато се свързвате с Екипа за техническа поддръжка. За да научите повече за тези данни, щракнете върху връзката **Декларация относно техническата поддръжка** в прозореца **Помощни инструменти**.

За използването на приложението в Европейския съюз, Обединеното кралство, Бразилия или жителите на Калифорния

Версиите на приложението, които Kaspersky и нашите партньори разпространяват в Европейския съюз, Обединеното кралство, Бразилия (както и версиите, предназначени за използване от жителите на Калифорния), отговарят на изискванията на регламентите, които управляват събирането и обработването на лични данни, които са установени в тези региони.

За да инсталирате приложението, трябва да приемете Лицензионното споразумение и условията на Политиката за поверителност.

В допълнение Съветникът за настройка ви подканя да приемете следните указания относно обработката на личните ви данни:

- Декларация на Kaspersky Security Network. Тази декларация позволява на експертите на Kaspersky веднага да получават информация за заплахите, засечени на вашия компютър, за приложенията, които са стартирани, и подписаните приложения, които са изтеглени, както и информация за операционната система, за да подобрят защитата ви.

- Декларация относно обработката на данни за маркетингови цели. Тази декларация ни позволява да създаваме по-ценни предложения за вас.

- Декларация относно обработката на данни при използване на Защита от спам. Тази декларация позволява на експертите на Kaspersky да получават данни, за да подобряват компонента Защита от спам.

Можете да приемете или отхвърлите Декларацията на Kaspersky Security Network и Декларацията относно обработката на данни за маркетингови цели по всяко време от прозореца **Настройки** → **Настройки за защита** → **Kaspersky Security Network**.

Относно решенията на Kaspersky

Нашите нови решения въплъщават нашата визия за съвременна киберсигурност. В допълнение към новите имена ще намерите чисто нов потребителски интерфейс и множество нови функционалности.

Решенията са представени от няколко плана. Плановете се различават по ниво на защита и по броя на функциите и услугите, предоставени на потребителите. Плановете съдържат както нови, така и изпитани във времето функции, които попадат в три категории.

Разгледайте достъпните за вас функции във всяка категория:

- Защита
- Производителност
- Поверителност

Сравнение на абонаментни планове

Приложението предлага четири абонаментни плана. Следващата таблица изброява функционалността на приложението, достъпна за всеки абонаментен план.

Абонаментни планове

Функционалност	Basic	Standard	Plus	Premium
My Kaspersky	✓	✓	✓	✓
Защита				
Бързо сканиране	✓	✓	✓	✓
Пълно сканиране	✓	✓	✓	✓
Сканиране по избор	✓	✓	✓	✓
Сканиране на сменяемо устройство	✓	✓	✓	✓
Сканиране във фонов режим	✓	✓	✓	✓
Сканиране за уязвимости	✓	✓	✓	✓
Защита на файлове	✓	✓	✓	✓
Безопасно сърфиране	✓	✓	✓	✓
Защита за пощата	✓	✓	✓	✓
Актуализиране на базата данни и модулите на приложенията	✓	✓	✓	✓
Отчети	✓	✓	✓	✓
Карантина	✓	✓	✓	✓
Отстраняване на неизправности на Microsoft Windows	✓	✓	✓	✓
Спешно възстановяване	✓	✓	✓	✓
Защита от експлойти	✓	✓	✓	✓

Системно наблюдение	✓	✓	✓	✓
Сканиране за слаби настройки	✓	✓	✓	✓
Защита от мрежови атаки	✓	✓	✓	✓
Проверка на уеб адреси	✓	✓	✓	✓
Разширение Kaspersky Protection	✓	✓	✓	✓
Предотвратяване на проникване		✓	✓	✓
Защитна стена		✓	✓	✓
Наблюдение на мрежата		✓	✓	✓
Умно домашно наблюдение			✓	✓
Антифишинг		✓	✓	✓
Новини за сигурността		✓	✓	✓
Производителност				
Бързо стартиране		✓	✓	✓
Ускоряване на компютъра		✓	✓	✓
Дубликати		✓	✓	✓
Големи файлове		✓	✓	✓
Неизползвани приложения		✓	✓	✓
Актуализация на приложения		✓	✓	✓
Текуща дейност		✓	✓	✓
Играл режим		✓	✓	✓
Режим "Не безпокой"		✓	✓	✓
Пестене на батерията		✓	✓	✓
Монитор за изправността на твърдия диск			✓	✓
Архивиране и възстановяване			✓	✓
Поверителност				
Проверка на изтичане на данни	един акаунт	един акаунт	✓	✓
Поверително сърфиране		✓	✓	✓
Безопасно плащане		✓	✓	✓
Управление на уеб камера и микрофон		✓	✓	✓
Откриване на преследвачески софтуер		✓	✓	✓
Инструмент за блокиране на инсталирането на нежелани приложения		✓	✓	✓
Програма за премахване на рекламен софтуер		✓	✓	✓
Защита от банери		✓	✓	✓
Почистване на следите от активността		✓	✓	✓
Kaspersky VPN			✓	✓

Диспечер на пароли			✓	✓
Унищожител за файлове			✓	✓
Тайно хранилище			✓	✓
Самоличност				
Портфейл за защита на самоличността				✓
Засичане на отдалечен достъп				✓
Премиум услуги за поддръжка				✓

Хардуерни и софтуерни изисквания

Общи изисквания

- 1500 MB свободно дисково пространство на твърдия диск
- Процесор, който поддържа набор инструкции SSE2 (с изключение на ARM).
- Интернет достъп (за инсталация и активация на приложението, за употреба от Kaspersky Security Network и за актуализация на модулите на приложението)
- Microsoft Windows® Installer 4.5 или по-нова версия
- Microsoft .NET Framework 4 или по-нова версия
- Microsoft .NET Desktop Runtime 5.x (5.0.10 или по-нова версия).
- Защита от достъп против достъп до уеб камерата се предоставя само за модели на съвместими уеб камери

Изисквания към операционната система

Операционна система	CPU	Свободна RAM памет	Ограничения
Microsoft Windows 11 Home (21H2, 22H2)	1 GHz или повече	4 GB (за 64-битова операционна система)	Подсистемата на Windows за Linux 2 (WSL2) не се поддържа.
Microsoft Windows 11 Enterprise (21H2, 22H2)			
Microsoft Windows 11 Pro (21H2, 22H2)			
Microsoft Windows 10 Home (версии: 1507, 1511, 1607, 1703, 1709, 1803, 1809, 1903, 1909, 2004, 20H2, 21H1, 21H2, 22H2)	1 GHz или повече	1 GB (за 32-битови операционни системи) или 2 GB (за 64-битови операционни системи)	
Microsoft Windows 10 Enterprise (версии: 1507, 1511, 1607, 1703, 1709, 1803, 1809, 1903, 1909, 2004, 20H2, 21H1, 21H2, 22H2)			
Microsoft Windows 10 Pro (версии: 1507, 1511, 1607, 1703, 1709, 1803, 1809, 1903, 1909, 2004, 20H2, 21H1, 21H2, 22H2)			

Microsoft Windows 8.1 (Service Pack 0 или по-нов, Windows 8.1 Update)	1 GHz или повече	1 GB (за 32-битови операционни системи) или 2 GB (за 64-битови операционни системи)	
Microsoft Windows 8.1 Pro (Service Pack 0 или по-нов, Windows 8.1 Update)			
Microsoft Windows 8.1 Enterprise (Service Pack 0 или по-нов, Windows 8.1 Update)			
Microsoft Windows 8 (Service Pack 0 или по-нов)	1 GHz или повече	1 GB (за 32-битови операционни системи) или 2 GB (за 64-битови операционни системи)	
Microsoft Windows 8 Pro (Service Pack 0 или по-нов)			
Microsoft Windows 8 Enterprise (Service Pack 0 или по-нов)			
Microsoft Windows 7 Starter (Service Pack 0 или по-нов)	1 GHz или повече	1 GB (за 32-битови операционни системи) или 2 GB (за 64-битови операционни системи)	
Microsoft Windows 7 Home Basic (Service Pack 0 или по-нов)			
Microsoft Windows 7 Home Premium (Service Pack 0 или по-нов)			
Microsoft Windows 7 Professional (Service Pack 0 или по-нов)			
Microsoft Windows 7 Ultimate (Service Pack 0 или по-нов)			

За да работят компонентите за безопасно сърфиране, защита от банери и безопасно плащане, услугата Base Filtering Engine (машина за основно филтриране) трябва да работи в операционната система.

Поддръжка на браузъри

Следните браузъри поддържат инсталирането на разширението Kaspersky Protection:

- Microsoft Edge 77.x – 104.x, базиран на Chromium;
- Mozilla™ Firefox™, версии 52.x – 105.x;
- Mozilla™ Firefox™ ESR 52.x, 60.x, 68.x, 78.x, 91.x, 102.x;
- Google Chrome™, версии 48.x – 105.x.

Следните браузъри поддържат екранна клавиатура и сканиране на шифровани връзки:

- Microsoft Edge 77.x – 104.x, базиран на Chromium;
- Mozilla Firefox версии 52.x – 105.x;
- Mozilla Firefox ESR 52.x, 60.x, 68.x, 78.x, 91.x; 102.x;
- Google Chrome 48.x – 105.x.

Следните браузъри поддържат режим на защитен браузър:

- Microsoft Internet Explorer 11.0;
- Microsoft Edge 77.x – 104.x, базиран на Chromium;
- Mozilla Firefox версии 52.x – 105.x;
- Mozilla Firefox ESR 52.x, 60.x, 68.x, 78.x, 91.x, 102.x;
- Google Chrome 48.x – 105.x;
- Yandex Browser 18.3.1 – 22.9.1 (с ограничения).

По-нови версии на браузърите могат да бъдат поддържани, ако браузърът поддържа съответната технология.

Kaspersky поддържа Google Chrome и Mozilla Firefox на 32-битови и 64-битови операционни системи.

Изисквания за таблети

- Microsoft Windows 8, Microsoft Windows 8.1, Microsoft Windows 10, Microsoft Windows 11;
- Процесор Intel® Celeron® с тактова честота от 1,66 GHz или по-бърз;
- 1000 MB свободна RAM памет.

Изисквания за минилаптопи

- Intel Atom™ CPU 1,60 GHz или по-бърз;
- 1024 MB свободна RAM памет;
- 10,1-инчов дисплей с екранна резолюция от 1024x768;
- Графичен процесор Intel GMA 950 или по-късна версия.

Изискванията за Kaspersky Password Manager са достъпни в помощните файлове на това приложение.

Съвместимост с други приложения на Kaspersky

Kaspersky е съвместимо със следните приложения на Kaspersky:

- Kaspersky Safe Kids 1.5
- Kaspersky Password Manager 10
- Kaspersky Software Updater 2.1
- Kaspersky Virus Removal Tool 2015, 2020
- Kaspersky VPN защитена връзка 4.0, 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8

Какво е новото в последната версия на приложението

Най-новата версия на приложението представя следните нови функции и подобрения:

- Функцията за защита на аудио потока вече се нарича „Mic control“ (Контрол на микрофона) и може да бъде открита в раздел „Webcam and Mic Control“ (Контрол на уеб камерата и микрофона) в раздел „Privacy“ (Поверителност).

- Функцията „Devices on My Network“ (Устройства в моята мрежа) вече се нарича „Smart Home Monitor“ (Интелигентен домашен монитор). Списъкът с типове устройства, които могат да бъдат добавяни от потребителя, е разширен.

- В Kaspersky Premium:

  - Подобрена е защитата при свързване с Wi-Fi мрежи. Приложението вече разпознава настройките на Wi-Fi мрежата, които не са достатъчно сигурни.

  - Добавена е функционалност за откриване на приложения за отдалечен достъп в компютъра.

- В нов прозорец се показва обяснение на начина на действие на автоматичното подновяване.

- Сценарият за преминаване към приложението на Kaspersky на други платформи е подобрен. Връзката вече не ви отвежда към My Kaspersky, а директно отваря прозорец за изтегляне на приложението в друга платформа.

- Коригирана е грешка, при която протоколът WPA3 се определя като несигурен.

- Подобрени са известията, свързани с необходимостта от рестартиране на компютъра.

Как работи абонаментът

Как работи платеният абонамент

Абонаментът се подновява автоматично в края на всеки период, освен ако не го анулирате. Към края на платения период ще получите електронно писмо с напомняне за предстоящото таксуване. Плащането за следващия период се извършва преди изтичането на текущия период, за да сте сигурни, че се радвате на непрекъсната защита от заплахи за киберсигурността. Ако абонаментът е успешно подновен, оставащите дни от текущия период се добавят към новия период.

Имайте предвид, че цената на абонамента може да варира. В момента на подновяване може да има специални оферти и отстъпки, които няма да повлияят на вашия абонамент.

Как работи безплатният абонамент

Безплатният пробен абонамент става активен незабавно, когато се абонирате. Няколко дни преди изтичане на пробния период ще получите напомняне за подновяване на абонамента. Ако не анулирате абонамента си по време на пробния период, след изтичане на пробния период, абонаментът автоматично се подновява за следващия период.

Ако има проблем с плащането

Ако по някаква причина Вашият абонамент не може да бъде автоматично подновен (Вашата банкова карта е изтекла, блокирана е или автоматичното подновяване е деактивирано), може да ви бъде предоставен гратисен период за подновяване на абонамента Ви, когато изтече; можете да използвате пълната функционалност на приложението без ограничения, докато гратисният период е активен. Ако не сте подновили абонамента си, приложението може да премине към режим с ограничена функционалност, когато гратисният период изтече. Продължителността на режима с ограничена функционалност зависи от вашия регион и лицензионните условия. За информация относно датата на изтичане на гратисния период и режима с ограничена функционалност вижте раздела Профил.

Относно абонаментите, закупени от доставчици на услуги

Можете да получите абонамент от доставчик на услуги (например от Вашия Интернет доставчик). Може да поставяте на пауза или да възобновявате своя абонамент, да го подновявате автоматично или да го отменяте. Можете да управлявате абонамента в акаунта си на уеб сайта на доставчика на услуги, който Ви е продал абонамента. В зависимост от доставчика на абонамента, наборът от опции за управление на абонамента може да варира.

За да активирате абонамента на вашето устройство, приложете кода за активиране, получен от вашия доставчик на услуги. В някои случаи кодът за активиране може да бъде изтеглен и приложен автоматично.

Ако друг абонамент вече е активен в приложението, когато получите абонамент от доставчик на услуги, приложението ще се използва с абонамента от доставчика на услуги. Вашият текущ абонамент може да се използва на друго устройство, докато изтече.

Абонаментът може да бъде неограничен (без дата на изтичане) или ограничен (например до една година). Неограничените абонаменти се подновяват автоматично, стига да е извършено навременното предплащане към доставчика на услуги. За да продължите да използвате приложението след изтичане на ограничен абонамент, трябва да извършите някои стъпки, за да го подновите.

Когато използвате приложението с абонамент, който сте получили от доставчик на услуги, не можете да добавите резервен код за активиране, за да продължите абонамента.

Ако не сте подновили абонамента или доставчикът на услуги не е могъл да поднови абонамента ви автоматично, след като изтече, може да ви бъде предоставен гратисен период за подновяване на абонамента. Функционалността на приложението остава достъпна по време на гратисния период. Приложението може да премине в режим с ограничена функционалност, когато гратисният период изтече. Ако доставчикът на услуги не предостави гратисен период или режим с ограничена функционалност, цялата функционалност на приложението спира да бъде достъпна, когато абонаментът изтече.

Относно абонаменти, закупени чрез App Store, Google Play или Huawei AppGallery

Ако сте закупили абонамент през App Store, Google Play или Huawei AppGallery, ще можете да видите подробности за абонамента в този магазин за приложения.

Как да купите абонамент

Има няколко начина за придобиване на абонамент за приложение:

Купете на уебсайта на Kaspersky

Можете да закупите абонамент за приложението на уебсайта на Kaspersky:

Купете Kaspersky Basic

Купете Kaspersky Standard

Купете Kaspersky Plus

Купете Kaspersky Premium

Kaspersky Premium не е налично в определени региони.

Купете с помощта на интерфейса на приложението

За да закупите абонамент на от интерфейса на приложението:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Профил**. Ако вашето устройство е свързано с акаунта ви в My Kaspersky, вашият имейл адрес се показва тук.
3. В информацията за абонамента щракнете върху **Купете сега**.

   Уеб сайтът на Kaspersky или един от нашите партньори се отваря в браузъра по подразбиране. Следвайте инструкциите на уеб сайта.

Покупка от партньор на Kaspersky

Можете да закупите абонамент от магазин на Kaspersky партньор.

Как да управлявате абонамента си от своя акаунт в My Kaspersky:

Необходим е *акаунт в My Kaspersky*, за да използвате приложението.

В зависимост от вашия абонамент, може да се наложи свързването на устройството, на което инсталирате приложението към вашия акаунт My Kaspersky, за да имате достъп до някои или всички функции на приложението.

Във вашия акаунт в My Kaspersky можете:

- Да преглеждате информация за абонаменти и техните дати на изтичане
- Отдалечено управление защитата на устройства.
- Безопасно да съхранявате и синхронизирате своите пароли и друга лична информация, ако използвате Kaspersky Password Manager.

- Да изтегляте закупени приложения.
- Свържете се с екипа за техническа поддръжка.
- Да научавате за нови приложения и специални оферти от Kaspersky.

За подробности относно цялата функционалност на акаунта в My Kaspersky вж. Помощ за My Kaspersky.

Как да свържете устройство към акаунт в My Kaspersky

Ако сте закупили абонамента си от уеб сайта на Kaspersky, по време на процеса на покупка е създаден акаунт. На имейл адреса, който сте посочили по време на покупката, беше изпратен имейл с връзката за създаване на парола.

Можете да влезете в акаунта си в My Kaspersky, като използвате своя имейл адрес и парола, или с акаунта ви за Google, Facebook или Apple. Ако вече имате акаунт, можете да конфигурирате бързо влизане с вашия акаунт в Google, Facebook или Apple в прозореца, използван за свързване на вашето устройство с вашия акаунт в My Kaspersky. Това е възможно, ако при създаването на вашия акаунт в My Kaspersky сте използвали имейл адреса от вашия акаунт в Google, Facebook или Apple.

Влизането с Facebook и Google не е налично в някои региони.

Ако все още нямате акаунт, можете да създадете такъв в процеса на свързване на устройството с вашия акаунт. Можете да използвате и идентификационни данни от други ресурси на Kaspersky, за да влезете във вашия акаунт.

За да свържете устройството си към акаунт в My Kaspersky:

1. Можете да свържете устройство към вашия акаунт:
   - В прозореца за връзка при активиране на приложението
   - В потребителския интерфейс на приложението, в раздел **Профил**.

     В блока **Вход в My Kaspersky** щракнете върху бутона **Влизане**.
   - На уебсайта на My Kaspersky
   - При активиране на определена функционалност на приложението
2. В прозореца за свързване на акаунта изберете метода на свързване, който намирате за най-удобен:
   - **Влезте с имейл адрес**. Въведете вашия имейл адрес в текстовото поле. На посочения имейл адрес е изпратено съобщение с връзка за създаване на парола.

     Ако сте конфигурирали двуетапна проверка в акаунта си в My Kaspersky, на телефона ви се изпраща текстово съобщение, съдържащо кода за потвърждение. В полето за въвеждане въведете кода за потвърждение и щракнете върху **Продължаване**.
   - **Влезте с акаунт в Google, Facebook или Apple**.

     a. Щракнете върху **Влезте с Google**, **Влезте с Facebook** или **Влезте с Apple**.

С това се отваря прозорец на браузъра; в този прозорец влезте в своя акаунт в Google, Facebook или Apple и разрешете на приложението да получи достъп до вашия имейл адрес.

Ако нямате акаунт в Google, Facebook или Apple, можете да си създадете такъв и да продължите с конфигурирането на бързо влизане в My Kaspersky.

Ако за вашия акаунт в My Kaspersky е конфигурирано потвърждаване в две стъпки, конфигурирайте бързо влизане в акаунта си на уебсайта на My Kaspersky, след което се върнете в приложението и влезте с Google, Facebook или Apple.

Ако използвате браузъра Microsoft Edge, за да конфигурирате влизането в My Kaspersky, ще ви е необходима версия на Microsoft Edge, базирана на Chromium 77.x или по-нова версия. Ако възникне грешка при установяване на връзка, изберете друг браузър като свой браузър по подразбиране, инсталирайте най-новата версия на браузъра Microsoft Edge или актуализирайте операционната система Microsoft Windows.

b. Върнете се в приложението и продължете със създаването на акаунта, като щракнете върху **Продължи**. Следвайте инструкциите на екрана.

Устройството ви ще се свърже с акаунта ви в My Kaspersky. Можете да зададете парола за своя акаунт и на уебсайта на My Kaspersky.

Обработка на данни при влизане в акаунта

При влизане във вашия акаунт в My Kaspersky с Google, Facebook или Apple, се обработват следните данни:

- Идентификатор на ресурса на притежателя на права
- Генерирана стойност за проверка на заявката
- Тип маркер
- URI номер, към който се изпраща отговорът на доставчика за удостоверяване

При влизане във вашия акаунт от уебсайт на доставчик на услуги чрез доставчици на удостоверителни услуги, се обработват следните данни:

- Идентификатор на ресурса на притежателя на права
- Маркер, използван за удостоверяване в инфраструктурата на доставчика на услуги
- Тип маркер
- Параметри, поискани от доставчиците на удостоверителни услуги
- URI номер, към който се изпраща отговорът на доставчика за удостоверяване

В някои региони приложението ви подканва да прочетете и приемете Декларацията относно обработката на данни за целите на използване на уеб портал. Ако приемате условията на декларацията, щракнете върху **Приемам**.

Как да отмените абонамента

Можете да анулирате абонамента си по всяко време. Анулираният абонамент не се подновява автоматично и вашите устройства остават защитени до изтичане на последния платен период.

За да избегнете ненужни разходи, трябва да анулирате абонамента си преди датата на плащане за следващия период. Имайте предвид, че плащането за следващия период се извършва преди изтичането на текущия период, за да сте сигурни, че защитата се поддържа без прекъсване.

Как да анулирате абонамента в Русия, Беларус, Абхазия, Армения, Азербайджан, Грузия, Южна Осетия, Киргизстан, Монголия, Таджикистан, Туркменистан, Узбекистан, Казахстан

За да отмените абонамента:

1. Проверете имейл адреса, който сте посочили при извършване на поръчката. В съобщението за потвърждение на поръчката или в съобщението за напомняне за подновяване на абонамента ще намерите връзка към акаунта си или връзка към вашата страница за управление на автоматичното подновяване.
2. Щракнете върху връзката.

   Във вашия браузър по подразбиране ще бъдете отведени до вашата персонализирана страница на уеб сайта на доставчика на плащане.
3. Можете да отмените абонамента си на страницата с информация относно подновяването.

   Абонаментът е отменен. На вашия имейл адрес се изпраща имейл за потвърждение на отмяната.

Как да анулирате абонамента в други страни

За да отмените абонамента:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Профил**.
3. В информацията за абонамента щракнете върху **Управление на акаунт**. Ако не сте свързали устройството си с акаунта си, щракнете върху **Влизане**.

   Отваря се прозорецът за влизане в My Kaspersky акаунт.
4. Във вашия акаунт в My Kaspersky отидете на **Абонаменти** раздел и щракнете върху панела за абонамент.

   Отваря се прозорец с подробности за абонамента.
5. Щракнете върху **Управление на абонамента**.

   В падащия списък изберете **Отмяна на абонамента**. Следвайте инструкциите на екрана.

Абонаментът е отменен.

Ако анулирате абонамента си след автоматично плащане за следващия период, абонаментът остава активен до изтичането на следващия период. Ако искате да отмените плащането за вече изтекъл период, можете да поискате възстановяване в съответствие с правилата за възстановяване на суми. Обикновено можете да получите възстановяване в рамките на 30 дни от плащането. За повече подробности относно условията и наличността за възстановяване, моля, свържете се с екипа за техническа поддръжка.

Когато поискате възстановяване, трябва да предоставите следната информация:

- Дата на покупката
- Вашето име и имейл адрес, посочени при извършване на покупката
- Номер на поръчката

След проверка на предоставената информация са необходими от 5 до 7 работни дни, за да получите средствата.

Как да зададете различен начин на плащане

Автоматичните такси за подновяване на абонамента използват начина на плащане, който сте избрали при закупуване на абонамента. Можете да зададете различен начин на плащане.

Как да зададете различен метод на плащане в Русия, Беларус, Абхазия, Армения, Азербайджан, Грузия, Южна Осетия, Киргизстан, Монголия, Таджикистан, Туркменистан, Узбекистан, Казахстан

За да зададете различен начин на плащане:

1. Проверете имейл адреса, който сте посочили при извършване на поръчката. В съобщението за потвърждение на поръчката или в съобщението за напомняне за подновяване на абонамента ще намерите връзка към акаунта си или връзка към вашата страница за управление на автоматичното подновяване.
2. Щракнете върху връзката.

   Във вашия браузър по подразбиране ще бъдете отведени до вашата персонализирана страница на уеб сайта на доставчика на плащане.
3. На страницата с информация за подновяване на абонамента променете начина на плащане и запазете промените.

Как да зададете различен начин на плащане в други държави

За да зададете различен начин на плащане:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Профил**.
3. В информацията за абонамента щракнете върху **Управление на акаунт**. Ако не сте свързали устройството си с акаунта си, щракнете върху **Влизане**.

   Отваря се прозорецът за влизане в My Kaspersky във вашия браузър по подразбиране.
4. Щракнете върху връзката с имейл адреса в горната дясна част на страницата.
5. В падащия списък изберете **Настройки на акаунта**.
6. Щракнете върху раздела **Начин на плащане**.
7. Щракнете върху  .

   В падащото меню изберете **Редактирай**.
8. Ще бъдете отведени до страницата за редактиране на метода на плащане на уеб сайта на нашия официален Nexway в нов прозорец на браузъра. Следвайте инструкциите на екрана, за да зададете различен начин на плащане.

Как да активирате абонамент на вашето устройство

В този раздел ще научите как да започнете да използвате приложения, след като сте закупили абонамент. За активиране е необходима интернет връзка.

Ако сте закупили абонамент от уебсайта на Kaspersky

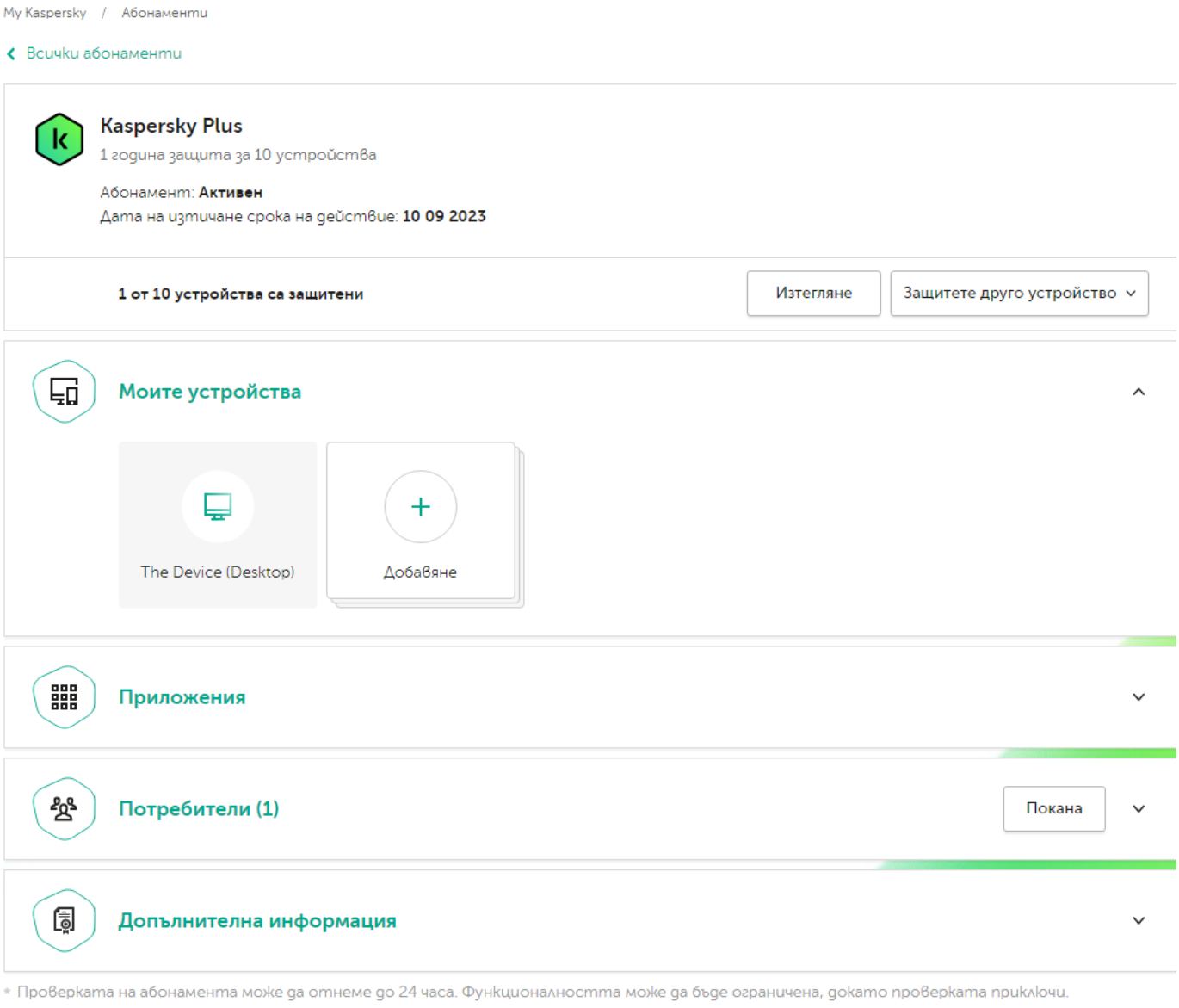
Ако сте закупили своя абонамент в онлайн магазина на Kaspersky, вашият My Kaspersky акаунт е създаден в хода на завършване на покупката. Изисква се акаунт в My Kaspersky за активиране на абонамент на различни устройства, както и за неговото управление. Можете да активирате абонамента си, като влезете в акаунта си в My Kaspersky от устройството, на което инсталирате приложението.

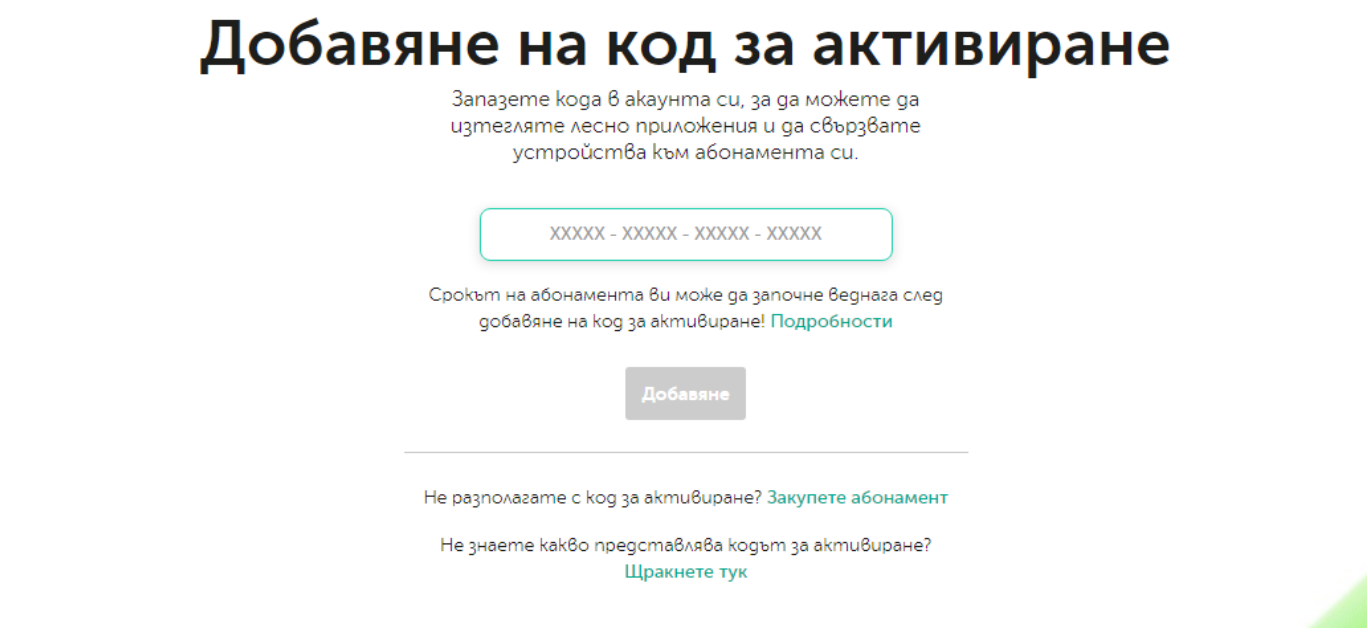
За да активирате абонамент на вашите устройства:

1. Проверете имейл адреса, който сте посочили при извършване на поръчката. Трябва да има две електронни писма от Kaspersky: разписка и инструкции за завършване на активирането на Вашия абонамент.

2. Щракнете върху връзката **Отидете на My Kaspersky** в имейла с инструкции, за да завършите създаването на акаунта си и да влезете.

3. В прозореца с информация за абонамент щракнете **Download,** за да изтеглите приложението на Вашето устройство.





4. Инсталирай приложението.

Когато инсталацията приключи успешно, приложението автоматично ще се свърже с вашия акаунт и ще бъде активирано според абонамента, който сте закупили.

Когато абонаментът бъде подновен, датата му на изтичане ще бъде актуализирана автоматично в рамките на 24 часа на всички устройства, които са активирани за този абонамент и са свързани с вашия акаунт My Kaspersky.

Ако закупите абонамент от онлайн магазина на Kaspersky, срокът на абонамента започва да тече от момента на покупката.

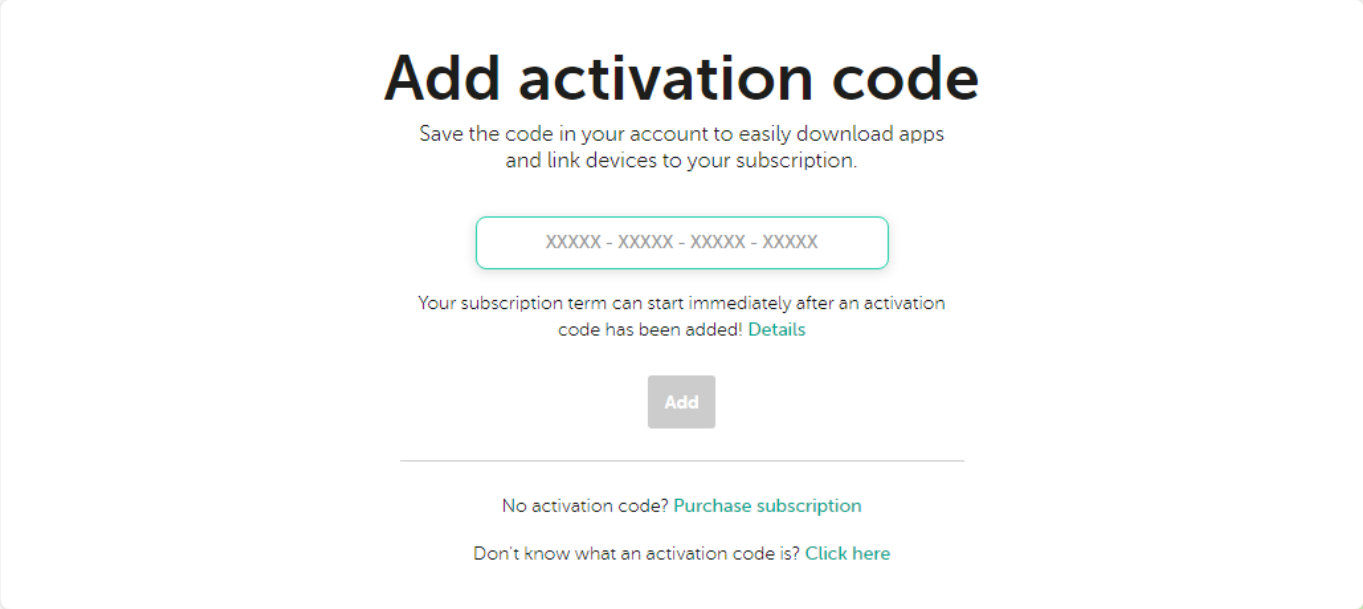
Ако сте закупили кутия или карта за активиране

Ако сте закупили кутия или карта за активиране в магазин, имате нужда от код за активиране, за да активирате приложението. Можете да намерите кода за активиране на кутията, в документацията или на гърба на картата. Кодът за активиране е уникална поредица от двадесет цифри и латински букви във формат xxxxx-xxxxx-xxxxx-xxxxx.

Отброяването за изтичане на абонамент, активиран с код за активиране, започва от датата, когато активирате приложението на първото устройство.

Ако сте закупили карта за активиране:

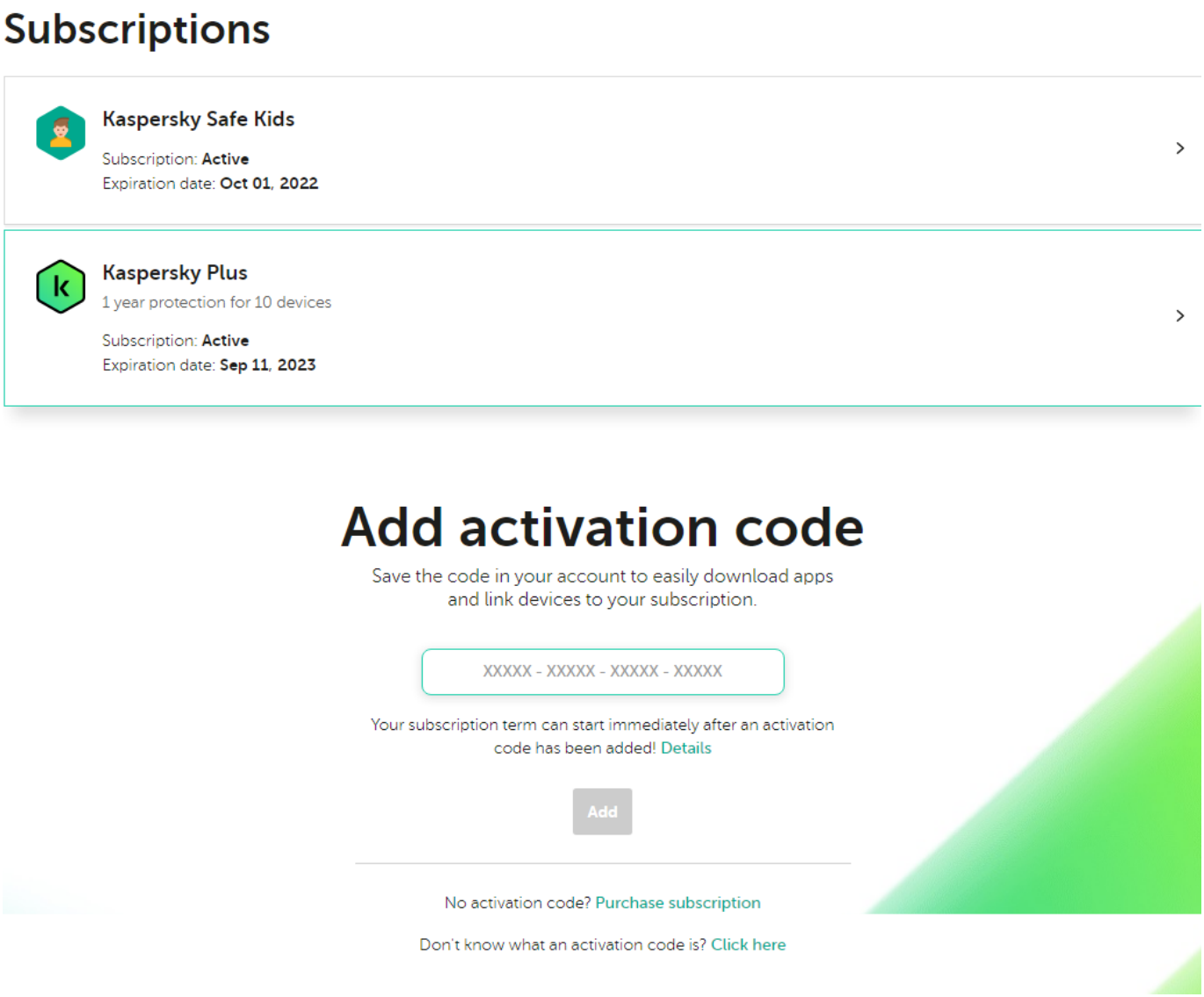
1. Отворете Уебсайт на My Kaspersky на устройството, което искате да защитите.
2. Създайте акаунт в My Kaspersky или влезте в съществуващ акаунт.
3. Под **Вече имате код за активиране?** в долната част на страницата въведете кода за активиране в полето за въвеждане.



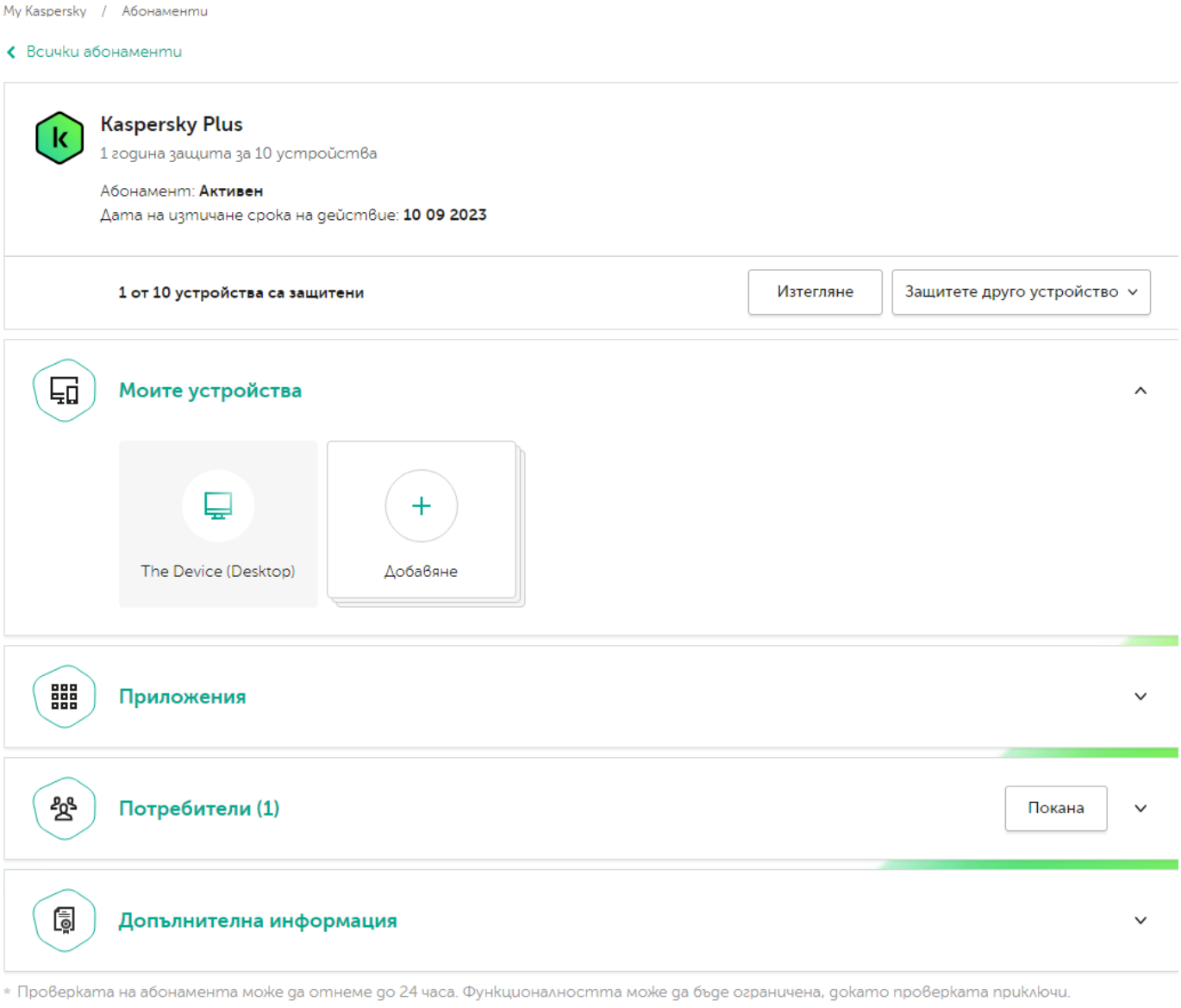
4. Щракнете върху бутона **Добави**.

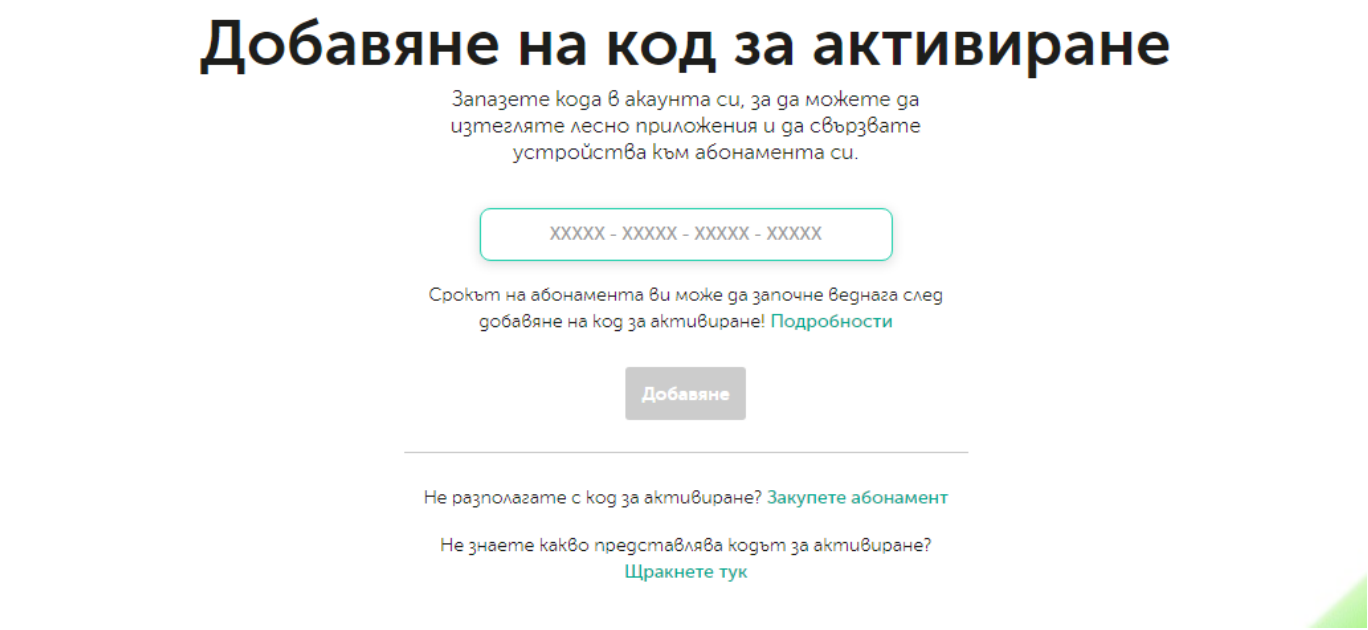
   Ако кодът за активиране е добавен успешно, разделът **Абонаменти** ще показва панела за абонаменти.

5. Щракнете върху панела за абонаменти.



6. В прозореца с информация за абонамент щракнете **Download,** за да изтеглите приложението на Вашето устройство.





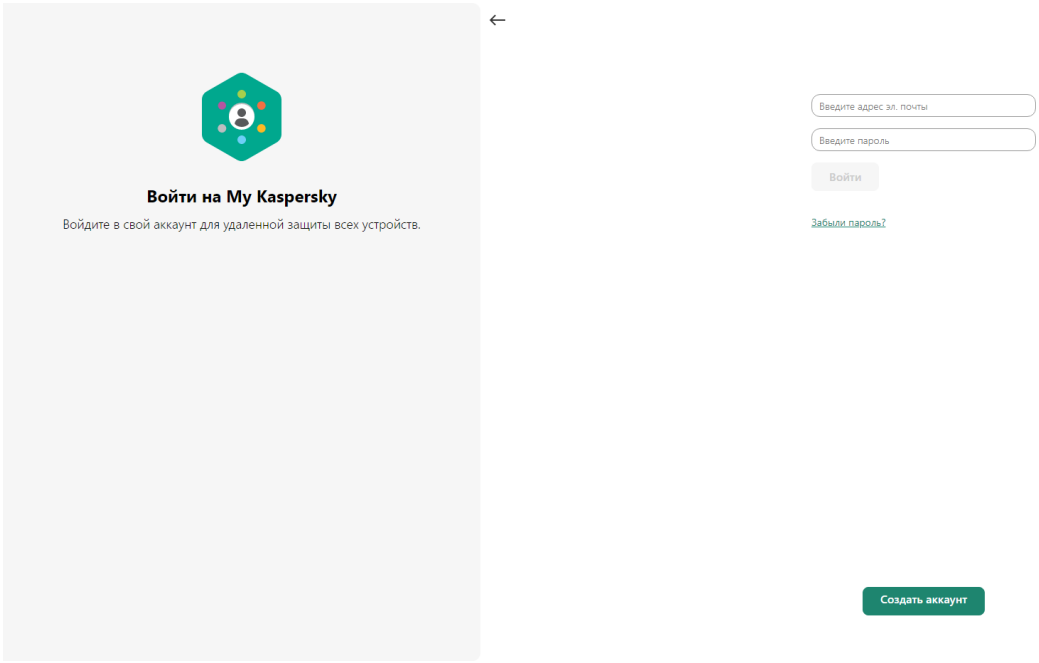
7. Инсталирай приложението.

   След като приложението бъде успешно инсталирано, то ще бъде активирано автоматично според условията на вашия абонамент.

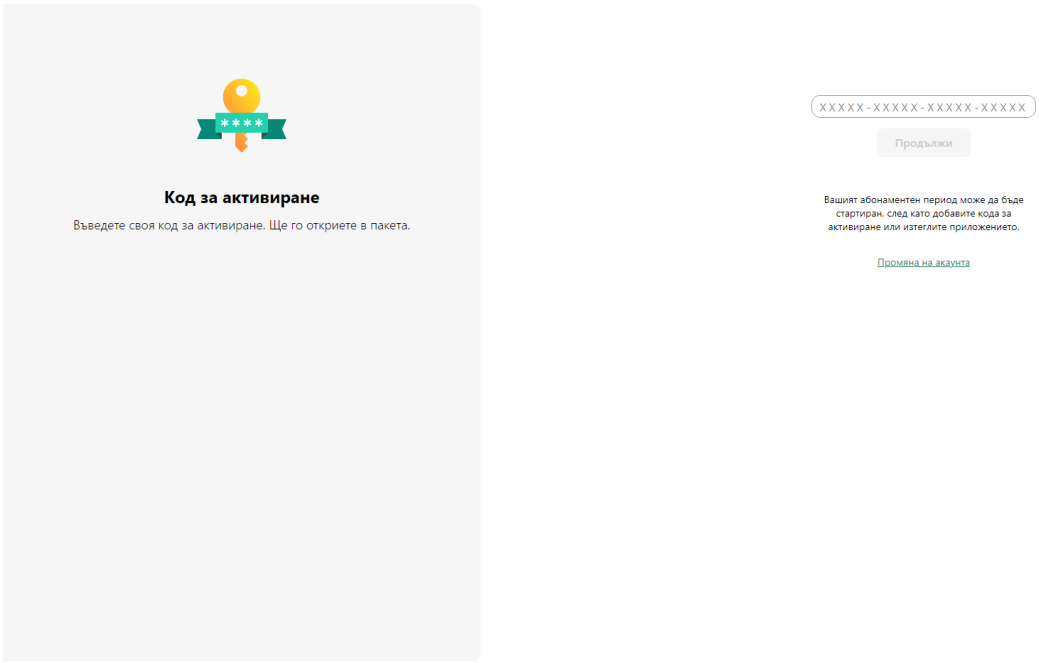
Ако сте закупили кутия с инсталационен диск:

1. Поставете диска в дисковото устройство.

2. В прозореца за връзка с акаунт в My Kaspersky създайте акаунт или влезте в съществуващ акаунт.

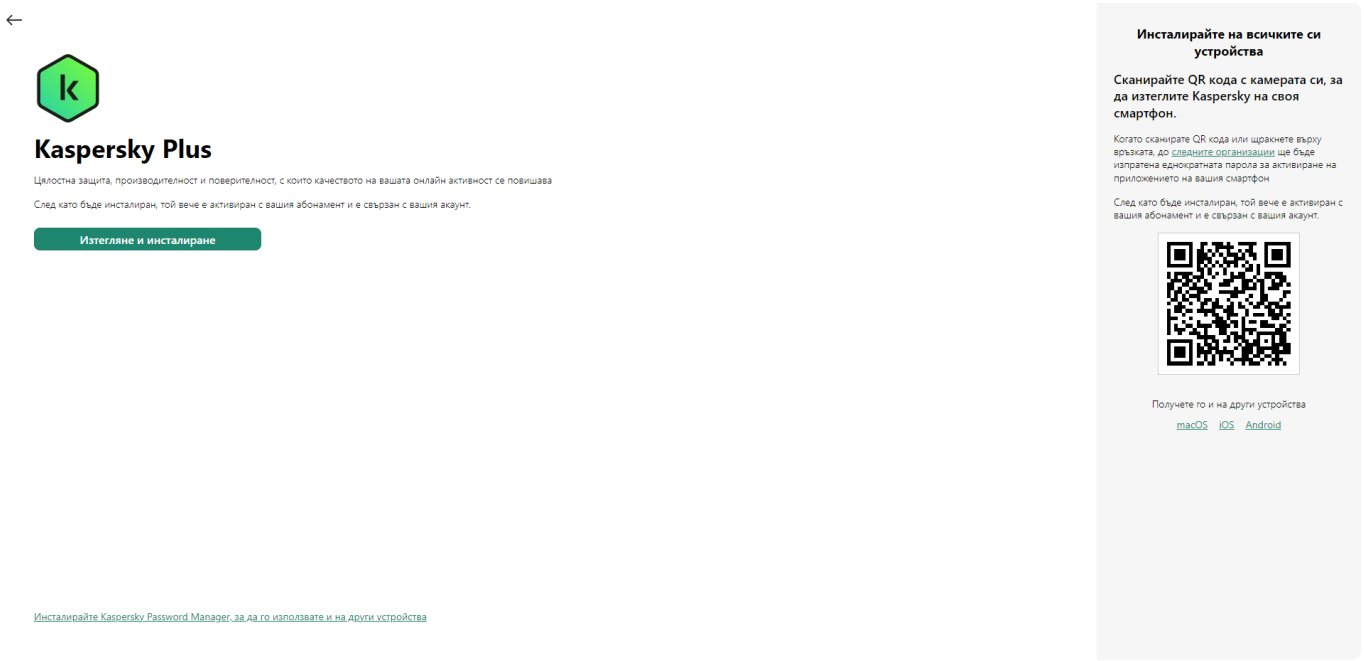


3. В прозореца с код за активиране въведете кода за активиране в текстовото поле и щракнете върху **Continue**.



Кодът за активиране се запазва във вашия акаунт под **Абонаменти**.

4. Щракнете върху **Изтегли и инсталирай**, за да изтеглите и инсталирате приложението на вашето устройство.



5. Инсталирай приложението.

   След като приложението бъде успешно инсталирано, то ще бъде активирано автоматично според условията на вашия абонамент.

Вашият код за активиране вече се съхранява във Вашия акаунт My Kaspersky. За да защитите ново устройство, влезте в акаунта и изтеглете приложението. Можете също така ръчно да въведете кода за активиране в приложението.

Активиране на вашия абонамент, ако приложението вече е инсталирано на вашето устройство

В този раздел ще научите как да подновите изтекъл абонамент, да добавите нов код за активиране към приложение, което има активен абонамент, за да се поднови автоматично и да преминете от пробния към платен абонамент.

Вашият абонамент е изтекъл

Ако имате активирано автоматично подновяване, абонаментът автоматично се подновява за още един срок без ваша намеса. Ако нямате активирано автоматично подновяване, трябва да подновите абонамента ръчно.

Ако подновите абонамента ръчно и преди това сте добавили резервен код за активиране в приложението, когато текущият абонамент изтече, приложението се активира автоматично с резервния код за активиране.

За да подновите абонамент:

1. Отворете основния прозорец на приложението.

2. Отидете в раздела **Профил**. Ако вашето устройство е свързано с акаунта ви в My Kaspersky, вашият имейл адрес се показва тук.

3. В информацията за абонамента щракнете върху **Поднови сега**.

   Уеб сайтът на Kaspersky eStore или един от нашите партньори се отваря в браузъра по подразбиране.

   По време на процеса на покупка въведете имейла, регистриран във вашия акаунт в My Kaspersky. Ако все още нямате акаунт, той ще бъде създаден с посочения имейл. След закупуване и свързване на приложението към вашия акаунт в My Kaspersky, абонаментът се активира автоматично на устройството в рамките на един час след подновяването.

Можете също да изпратите новия абонамент на устройства от вашия акаунт в My Kaspersky. За подробности относно изпращането на абонамент към устройство, свързано с вашия акаунт, вж Помощ за My Kaspersky.

Ако не сте подновили абонамента си, приложението може да премине към режим с ограничена функционалност.

Подновяване на абонамента с помощта на резервен код за активиране

Ако имате нов код за активиране, можете да го добавите към приложението, за да се използва като резервен код. Когато текущият абонамент изтече, приложението се активира автоматично с резервния код за активиране. По този начин можете да осигурите непрекъсната защита на вашето устройство.

Има случаи, когато **не можете** да добавите резервен код за активиране.

Добавянето на резервен код за активиране може да не е достъпно поради следните ограничения:

- Ако използвате автоматично подновен абонамент, не можете да добавите резервен код за активиране.
- Код за активиране на абонамент с автоматично подновяване не може да бъде добавен като резервен код за активиране.
- Ако използвате пробен абонамент, не можете да добавите резервен код за активиране.
- В приложението вече е зададен код за активиране като резервен код за активиране.
- Добавянето на резервен код не е възможно, ако текущият абонамент вече е изтекъл.
- Абонаментът все още не е достъпен във вашия регион.

За да добавите резервен код за активиране:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Профил**. Ако вашето устройство е свързано с акаунта ви в My Kaspersky, вашият имейл адрес се показва тук.
3. Под информация за абонамента щракнете върху трите точки и изберете **Въведете код за активиране**.
4. Въведете кода за активиране в полето за въвеждане и щракнете върху бутона **Запазване на код за активиране**.

   Резервният код за активиране ще се покаже в прозорец **Детайли за абонамента**.

Ако въведете резервен код за активиране, издаден за множество устройства, трябва да следвате стъпките, за да приложите резервния код на всички устройства, на които искате да подновите автоматично абонамента.

Ще бъде направен опит за активиране и пълна проверка на резервния код, когато текущият абонамент изтече или ако текущият абонамент бъде премахнат от устройството. Приложението проверява датата на изтичане на резервния код за активиране, максималния брой устройства, на които може да се използва абонаментът, както и съвместимостта на абонамента с инсталираната версия на приложението. По време на активиране на резервен код може да се изисква връзка с акаунта My Kaspersky.

Ако резервният код за активиране, който добавяте, вече е приложен на това или на друго устройство, датата, на която се активира с цел подновяване на абонамента чрез резервния код, е датата, на която приложението е било активирано с този код за първи път. За да подновите абонамента, добавете резервен код за активиране, чиято дата на изтичане е по-късна от датата на изтичане на абонамента, използван в момента от приложението.

Ако приложението не се активира автоматично с резервен код за активиране, можете да го активирате ръчно, като щракнете върху бутон **Опитайте отново**. Ако текущият абонамент е блокиран, можете да активирате приложението с помощта на резервен код за активиране, като щракнете **Активиране сега**.

Можете също да изпратите резервния код за активиране на устройства от вашия акаунт в My Kaspersky. За подробности относно изпращането на абонамент към устройство, свързано с вашия акаунт, вж Помощ за My Kaspersky.

Преминаване от пробен абонамент към платен абонамент

Когато безплатният пробен период изтече, абонаментът се подновява и активира без Вашето участие. Цената за подновяване на абонамента се таксува по избрания от Вас метод на плащане.

В някои региони автоматичното преминаване към платен абонамент може да не е налично. Ако не сте въвели данни за плащане за последващо подновяване, когато се абонирате за безплатния пробен период, ще трябва да закупите абонамент, за да сте сигурни, че Вашите устройства ще останат защитени.

За да превключите от пробен абонамент към платен:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Профил**. Ако вашето устройство е свързано с акаунта ви в My Kaspersky, вашият имейл адрес се показва тук.
3. В информацията за абонамента щракнете върху **Купете сега**.

   Уеб сайтът на Kaspersky или един от нашите партньори се отваря в браузъра по подразбиране. По време на процеса на покупка въведете имейла, регистриран във вашия акаунт в My Kaspersky.

Абонаментът, който сте закупили, се активира автоматично на Вашето устройство.

Как да инсталирате приложението

Приложението се инсталира на вашия компютър в интерактивен режим с помощта на Съветника за настройка и премахване.

Съветникът се състои от поредица от прозорци (стъпки). Броят и поредицата на стъпките в Съветника зависят от региона, в който инсталирате приложението. В някои региони Съветникът ви подканва да приемете допълнителни споразумения относно начина на обработване на личните ви данни. За да спрете дейността на съветника на която и да е стъпка на инсталацията, затворете прозореца на съветника.

Ако приложението ще се използва за защита на повече от един компютър (като максималният брой компютри е определен от условията на лицензионното споразумение), процедурата по инсталиране ще бъде идентична за всички компютри.

За да инсталирате приложението на вашия компютър,

- Ако използвате инсталационен диск, поставете диска в дисковото устройство и следвайте инструкциите на екрана.
- Ако сте изтеглили приложението от интернет, стартирайте го. Приложението се инсталира с помощта на стандартния Съветник за настройка. В този случай съветникът показва няколко допълнителни стъпки в инсталацията за някои езици на локализация.

Можете също да **инсталирате приложението от командния прозорец**.

Можете също да инсталирате приложението Kaspersky от командния прозорец.

> Определени команди могат да бъдат изпълнение единствено от администраторски акаунт.

Синтаксис на командния прозорец:

```
<path to the file of the installation package> [параметри]
```

За инсталиране на приложението от командния прозорец

1. Отворете командния прозорец като администратор.
2. Въведете пътя до инсталационния файл и командата за стартиране на инсталацията със съответните опции и свойства. Опциите и свойствата за инсталиране са описани по-долу.
3. Следвайте инструкциите на съветника за настройка.

Основни опции

Име на командата	Стойност	Например
`/сек`	Неинтерактивен (тих) режим: диалоговите прозорци не се показват по време на инсталацията.	`saas21.exe /s`
`/mybirthdate=YYYY-MM-DD`	Филтрирай по дата. Ако сте на възраст под 16 години, инсталацията не се извършва. Тази опция е: • Необходима за неинтерактивна инсталация • По избор за инсталиране на приложението в режим OEM	`saas21.exe /mybirthdate=1986-12-23`
`/l`	Избиране на езика, използван за инсталиране на многоезичната версия.	`saas21.exe /len-us`
`/t`	Папка, в която е записан регистрационният файл за инсталиране.	`saas21.exe /tC:\KasperskyLab`
`/p<property>=<value>`	Задава свойствата на инсталирането.	`saas21.exe /pALLOWREBOOT=1 /pSKIPPRODUCTCHECK=1`
`/h`	Показване на помощ.	`saas21.exe /h`

Допълнителни настройки

Име на командата	Стойност	Например
/x	Извадете продукта.	`saas21.exe /x`

Най-важни свойства за инсталиране

Име на командата	Стойност	Например
`ACTIVATIONCODE=<value>`	Въведете кода за активиране.	
`AGREETOEULA = 1`	Приемете	

	лицензионното споразумение с краен потребител	
`AGREETOPRIVACYPOLICY = 1`	Приемете политиката за поверителност.	
`JOINKSN_ENHANCE_PROTECTION=1`	Потвърдете съгласие за изпращане на лични данни за подобряване на основната функционалност на продукта.	
`JOINKSN_MARKETING = 1`	Потвърдете съгласие за изпращане на лични данни за маркетингови цели.	
`INSTALLDIR=<value>`	Задаване на местоположението на инсталацията.	`saas21.exe /p"INSTALLDIR=C:\Documents and Settings\saas21"`
`KLPASSWD = <value>`	Задайте паролата за различни функции на продукта. Ако стойността KLPASSWDAREA не е зададена, се използва обхватът на паролата по подразбиране: • Редактиране на настройките на приложението • Затваряне на приложението	`saas21.exe /pKLPASSWD=12345678`
`KLPASSWDAREA= [SET|EXIT|UNINST]`	Задайте обхвата на паролата, конфигурирана в KLPASSWD: • SET — Редактиране на настройките на приложението • EXIT — Затваряне на приложението • UNINST - Премахване на приложението. Това свойство може да има няколко стойности; в този случай стойностите трябва да бъдат разделени със знака за точка и запетая ";".	
`SELFPROTECTION=1`	Активирайте функцията за самозащита по време	`saas21.exe /pSELFPROTECTION=1`

	на инсталацията.	
`ALLOWREBOOT=1`	Позволяване на рестартиране, ако е необходимо.	`saas21.exe /pALLOWREBOOT=1`
`SKIPPRODUCTCHECK=1`	Не проверявайте за софтуер, който е несъвместим с Kaspersky.	`saas21.exe /pSKIPPRODUCTCHECK=1`
`-oembackupmode`	Не стартирайте приложението след инсталацията, ако Windows е стартиран в режим на одит.	`saas21.exe /s -oembackupmode`

Като зададете SKIPPRODUCTCHECK=1, вие поемате пълна отговорност за възможните последствия от несъвместимостта на Kaspersky с друг софтуер.

SKIPPRODUCTCHECK=1 ви позволява да игнорирате само приложения, които са премахнати ръчно.

Пример за съставна команда, която позволява рестартиране на компютъра по време на инсталацията и пропускане на проверката за несъвместим софтуер:

```
saas21.exe /pALLOWREBOOT=1 /pSKIPPRODUCTCHECK=1
```

Съветникът за инсталиране преминава през следните стъпки:

1. Стартиране на инсталирането

   По време на тази стъпка съветникът ще ви подкани да инсталирате приложението.

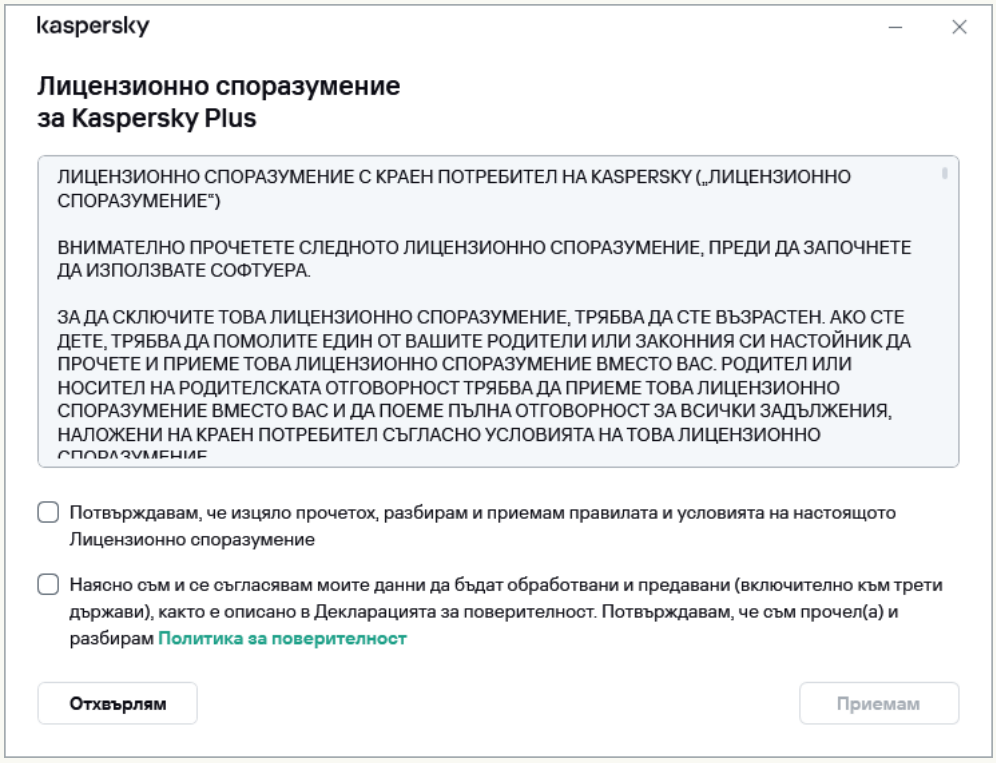
   В зависимост от типа инсталация и езика на локализация по време на тази стъпка съветникът може да ви подкани да прегледате лицензионното споразумение, сключено между вас и Kaspersky, и да ви попита дали искате да участвате в Kaspersky Security Network.

   Преглед на лицензионното споразумение

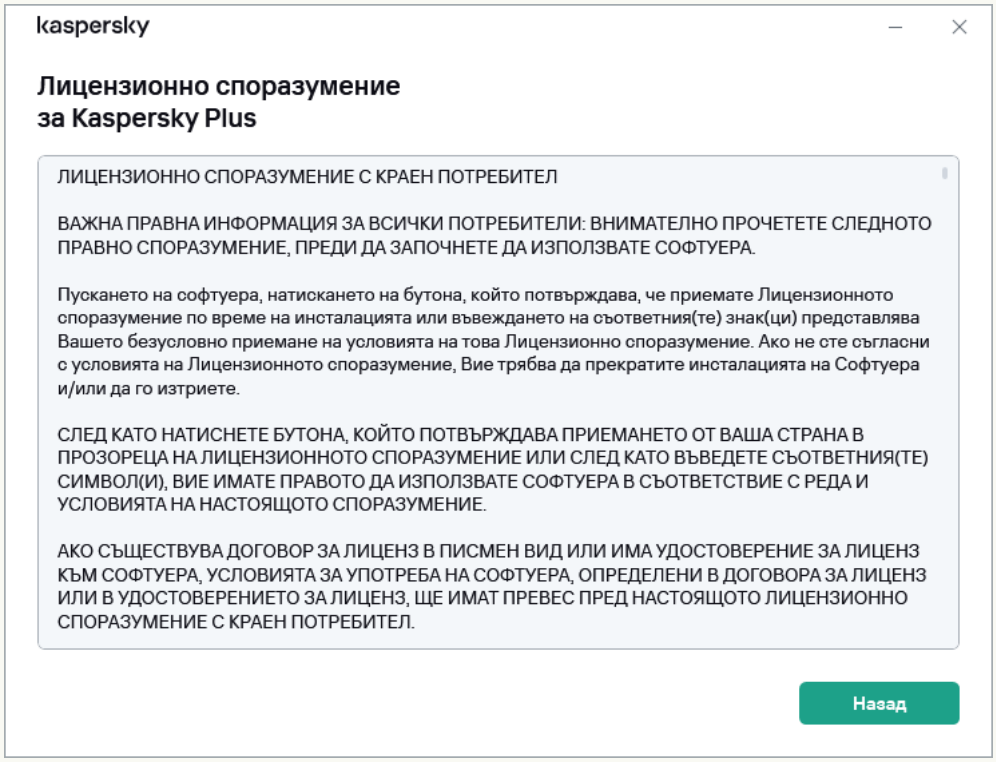
Тази стъпка на съветника се показва за някои езици на локализация при инсталиране на приложението от интернет.

По време на тази стъпка съветникът ви подканва да прегледате лицензионното споразумение, сключено между вас и Kaspersky.

Прочетете подробно лицензионното споразумение за краен потребител и ако сте съгласни с всички негови условия, щракнете върху **Продължаване** (този бутон се нарича **Приемам** в някои региони).



В някои версии на приложението Лицензионното споразумение с Крайния потребител може да се отвори, като се кликне върху връзката в Началния екран на Съветника. В този случай, в прозореца, **Назад** съдържащ текста на Лицензионното споразумение с Крайния потребител, е достъпен само бутонът. Като кликнете върху бутона **Инсталирай**, вие приемате условията на Лицензионното споразумение.



След това инсталацията на приложението на вашия компютър продължава.

Ако условията на лицензионното споразумение не се приемат, приложението няма да се инсталира.

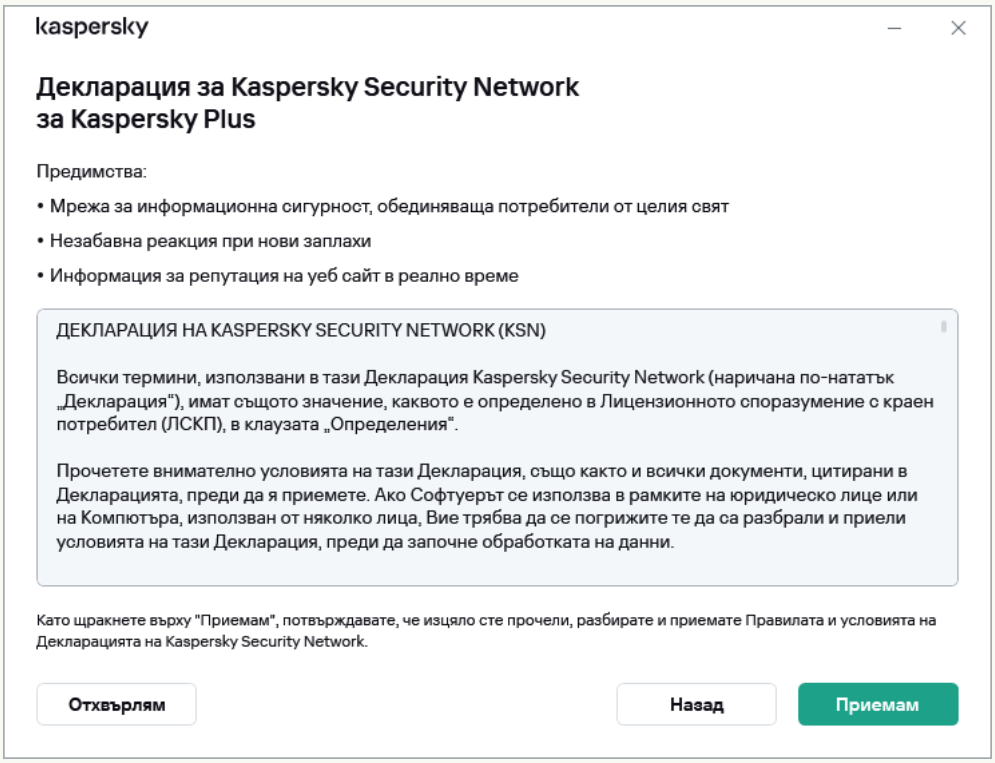
В някои региони също така трябва да приемете условията на Политиката за поверителност, за да продължите инсталацията на приложението.

Преглед на Декларацията на Kaspersky Security Network.

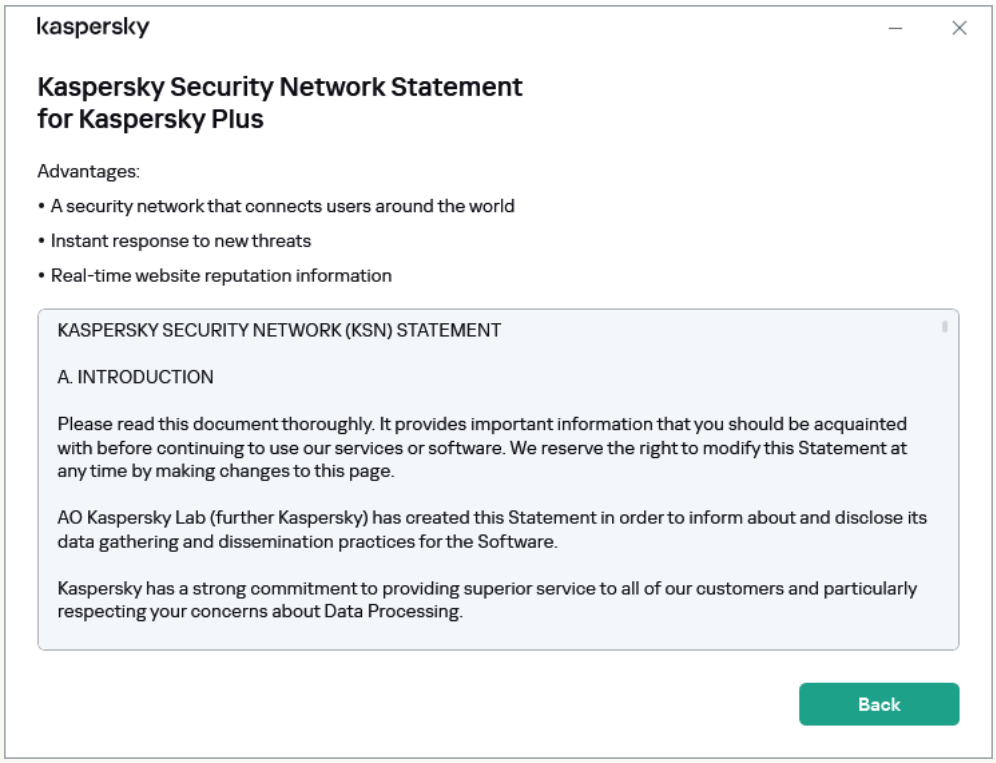
По време на тази стъпка съветникът ви кани да участвате в Kaspersky Security Network. Участието в програмата включва изпращане на информация за заплахи, откривани на вашия компютър, стартиране на приложения и изтеглени подписани приложения, както и информация за вашата операционна система, към АО Kaspersky Lab. Никакви лични данни, получени от вас, не се събират, обработват или съхраняват.

Прочетете Декларацията на Kaspersky Security Network и направете едно от следните действия:

- Ако приемате всички нейни условия, в прозореца кликнете върху **Приемам** бутона.
- Ако не искате да участвате в Kaspersky Security Network, щракнете върху бутона **Отхвърлям**.



В някои версии на приложения трябва да изберете квадратчето за отметка **Искам да участвам в Kaspersky Security NetworkWELCOME_CHECK_PRIVACY_POLICY_PART1 = Преглед на** на началния екран на съветника, за да приемете Декларацията на Kaspersky Security Network. Можете да прочетете декларацията, като щракнете върху връзката **Kaspersky Security Network**. След като прочетете споразумението, кликнете върху бутон **Назад**, за да продължите с инсталацията. Ако в квадратчето **Искам да участвам в Kaspersky Security NetworkWELCOME_CHECK_PRIVACY_POLICY_PART1 = Преглед на** е поставена отметка, вие приемате условията на Декларацията на Kaspersky Security Network, като щракнете върху бутона **Инсталирай**.



След като приемете или отхвърлите участието в Kaspersky Security Network, инсталацията на приложението продължава.

В някои версии на приложението Декларацията на Kaspersky Security Network включва информация относно обработването на лични данни.

2. Инсталиране на приложението

   Инсталирането на приложението може да отнеме известно време. Изчакайте да приключи. При завършване на инсталацията съветникът за инсталиране автоматично преминава към следващата стъпка.

   Проверки по време на инсталиране на приложението

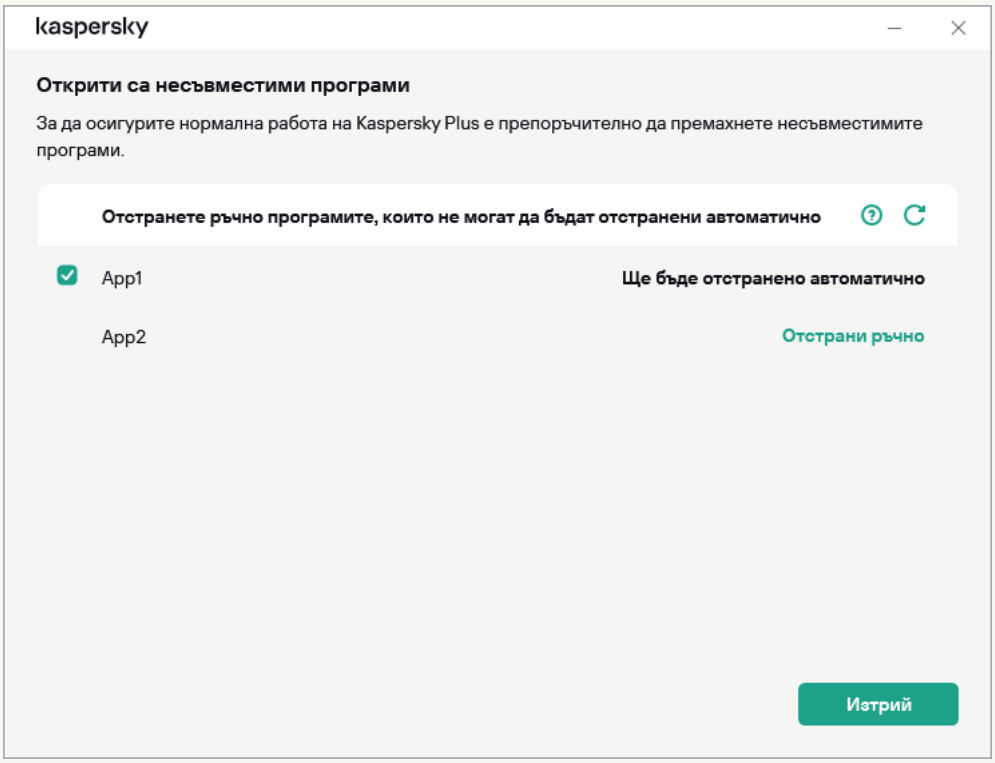
Приложението извършва няколко проверки по време на инсталацията. Тези проверки могат да открият следните проблеми:

- *Несъответствие на операционната система със софтуерните изисквания*. По време на инсталацията съветникът проверява следните условия:

  - Дали операционната система и сервизният пакет отговарят на софтуерните изисквания;
  - Всички изисквани приложения са налични;
  - Свободното дисково пространство е достатъчно за инсталация;
  - Потребителят, който инсталира приложението, има администраторски права.

  Ако някое от горепосочените изисквания не е покрито, се показва съответното известие.

- *Наличие на несъвместими приложения на компютъра*. Ако бъдат открити някакви несъвместими приложения, те се показват в списък на екрана и ще бъдете подканени да ги премахнете. Приложенията, които не могат да бъдат премахнати автоматично, трябва да бъдат премахнати ръчно, като кликнете върху бутон **Отстрани ръчно**.



Когато премахвате несъвместими приложения, ще трябва да рестартирате операционната система, след което инсталирането на Kaspersky продължава автоматично.

Инсталиране на Kaspersky Password Manager заедно с Kaspersky Plus или Kaspersky Premium

Преди да завърши инсталацията, Kaspersky Ви подканва да инсталирате Kaspersky Password Manager, за да защитите паролите си. Инсталацията на Kaspersky Password Manager може да продължи, след приключване на инсталацията на Kaspersky, няма отделно известие за завършване на инсталацията на Kaspersky Password Manager.

Kaspersky Password Manager не е включен в плановете Kaspersky Basic и Kaspersky Standard. Ако искате да използвате Kaspersky Password Manager за защита с парола, можете да го изтеглите и инсталирате като отделно приложение или да преминете към Kaspersky Plus.

3. Завършване на инсталирането

   По време на тази стъпка Съветникът ви информира за приключването на инсталацията на приложението.

   Всички необходими компоненти на приложението ще бъдат автоматично стартирани, след като инсталацията завърши.

   В някои случаи може да е необходимо да рестартирате операционната система, за да завършите инсталацията.

Заедно с приложението се инсталират добавки за браузъри, за да гарантират безопасно сърфиране в интернет.

Когато стартирате аудио и видео запис или възпроизвеждане за първи път след инсталацията на Kaspersky, възпроизвеждането или записът на аудио и видео може да прекъсне. Това се изисква, за да се активира функционалността, която контролира достъпа на приложения до звукозаписващи устройства. Системната услуга, която контролира аудио хардуер, се рестартира, когато Kaspersky стартира за първи път.

Kaspersky Plus или Kaspersky Premium се инсталира заедно с Kaspersky VPN Secure Connection, предназначено за установяване на защитена връзка чрез Виртуална частна мрежа (VPN). Може да премахнете Kaspersky VPN Secure Connection отделно от приложението Kaspersky. Ако използването на VPN е забранено във вашата страна, Kaspersky VPN Secure Connection не се инсталира.

Ако сте изтеглили приложението от Вашия My Kaspersky акаунт, след инсталиране приложението се активира автоматично с абонамента от Вашия акаунт.

Инсталиране върху други приложения на Kaspersky

Приложението може да се инсталира върху следните приложения на Kaspersky:

- Kaspersky Free
- Kaspersky Anti-Virus
- Kaspersky Internet Security
- Kaspersky Total Security
- Kaspersky Security Cloud

Когато инсталирате новото приложение, инсталираните по-рано Kaspersky Anti-Virus, Kaspersky Internet Security, Kaspersky Security Cloud, Kaspersky Total Security се премахват. Лицензът на премахнато приложение може да се използва за новото приложение на Kaspersky, с изключение на лицензия на Kaspersky Total Security. Настройките на премахнатите приложения се запазват.

Когато инсталирате новото приложение, инсталираното по-рано приложение Kaspersky Free се премахва. Настройките на Kaspersky Free не се записват.

Когато преминете от Kaspersky Total Security към Kaspersky Basic или Kaspersky Standard, резервните копия на файловете се запазват, но не се показват в тези приложения. Може да добавите резервните копия на файловете ръчно. Когато преминете от Kaspersky Total Security към Kaspersky Plus, копията на файловете се съхраняват и показват автоматично.

Разширение на браузъра Kaspersky Protection

За да може Kaspersky да поддържа напълно браузърите, разширението Kaspersky Protection трябва да бъде инсталирано и активирано в браузърите. Разширението Kaspersky Protection вгражда скрипт в уеб страницата, отворена в защитен браузър и в трафик. Приложението използва този скрипт, за да взаимодейства с уеб страницата и да пренася данни към банки, чиито уеб сайтове са защитени от компонента Безопасно плащане. Приложението защитава данните, предавани от скрипта с помощта на цифров подпис. Приложението може да вгради скрипта, без да използва разширението Kaspersky Protection.

Приложението подписва данни, предавани от скрипта с помощта на инсталираните антивирусни бази данни и заявки към Kaspersky Security Network. Приложението изпраща заявки към Kaspersky Security Network, независимо дали сте приели условията на Декларацията на Kaspersky Security Network или не.

Когато работите с браузъра, разширението Kaspersky Protection ви позволява:

Управление на Поверително сърфиране.

Управление на Защита от банери.

Да информирате за подозрения за фишинг.

Да докладвате подозрителен уебсайт за фишинг:

1. Уверете се, че сте на страницата, за която подозирате, че е фишинг страница.
2. В лентата с инструменти на браузъра щракнете върху **Kaspersky Protection**.
3. В менюто на разширението изберете **Информиране относно подозиран фишинг**.
4. Това отваря прозорец; уверете се, че в него е показан уеб адресът на уебсайта, за който подозирате, че е фишинг.
5. Щракнете върху **Информиране**.

Вашият доклад ще бъде доставен на Kaspersky Security Network.

Информация за проблема в уеб сайта

За да информирате за проблем в уеб сайта:

1. Уверете се, че сте на страницата, която искате да съобщите като проблемна.
2. В лентата с инструменти на браузъра щракнете върху **Kaspersky Protection**.
3. В менюто за разширение изберете **Информирайте ни за проблем с уеб сайт**.
4. Това отваря прозорец; уверете се, че прозорецът показва уеб адреса на уеб сайта.
5. Опишете проблема в текстовото поле.
6. Щракнете върху **Информиране**.

Съобщението е доставено.

Отваряне на Екранната клавиатура

Инсталиране на разширението Kaspersky Protection в Microsoft Edge, базиран на Chromium, Mozilla Firefox и Google Chrome

В браузърите Google Chrome и Mozilla Firefox разширението Kaspersky Protection се инсталира автоматично. Kaspersky Ви подканва да активирате разширението. В базирания на Chromium браузър Microsoft Edge разширението Kaspersky Protection също се инсталира автоматично, но приложението не ви подканва да активирате разширението. Трябва сами да предприемете стъпки за активиране на разширението.

Поддръжка на браузър Yandex

Когато използвате браузър Yandex, работят следните компоненти на приложението:

- Защитен браузър;
- Сканиране на уеб адреси
- Безопасно сърфиране;
- Антифишинг.

Компонентите Поверително сърфиране и Защита от банери работят, но не могат да бъдат конфигурирани в браузър Yandex.

Поддръжка на Internet Explorer

От приложението на Kaspersky, версия 4 нататък разширението Kaspersky Protection повече няма да поддържа браузъра Internet Explorer. Ако искате да продължите да използвате разширението Kaspersky Protection в Internet Explorer, може да се върнете към предишната версия на приложението.

Как да деинсталирате приложението

След премахване на приложението, вашият компютър и личните данни ще бъдат незащитени.

Приложението се премахва с помощта на съветника за инсталиране.

Как да деинсталирате приложението в Windows 7

За да стартирате съветника на компютър с Microsoft Windows 7 или по-ранни версии,

в менюто **Start** изберете **All applications** → **Kaspersky** → **Remove Kaspersky**.

За да деинсталирате приложението в Windows 8 или по-нова версия

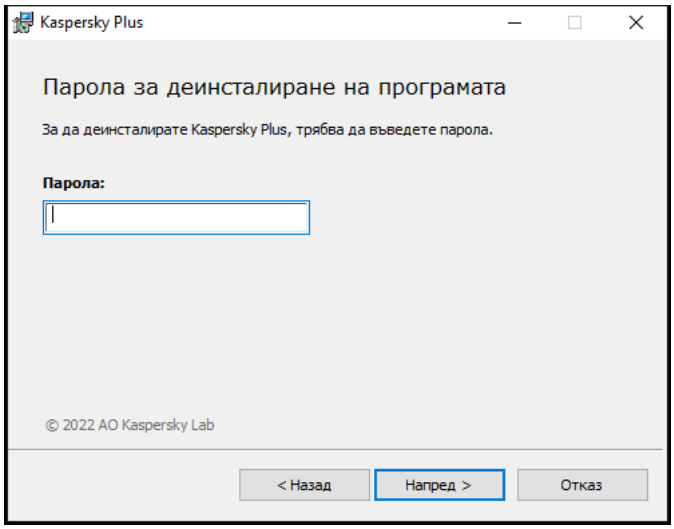
Как да стартирате съветника на компютър с Microsoft Windows 8 или по-нов:

1. Намерете инсталираното приложение, като използвате един от следните методи:
   - В Windows 8 кликнете върху бутона **Start** и намерете Kaspersky на екрана за бърз старт.
   - В Windows 10 и по-нова версия кликнете върху бутона **Старт** и намерете приложението в списъка или използвайте лентата за търсене.
2. Щракнете с десния бутон върху прекия път към приложението Kaspersky.
3. В контекстното меню изберете **Деинсталиране**.
4. В прозореца, който се отваря, изберете Kaspersky в списъка.
5. Щракнете върху бутона **Премахване** / **Редактиране** в горната част на списъка.

Ще се стартира съветникът за настройка на приложението.

Отстраняването включва следните стъпки:

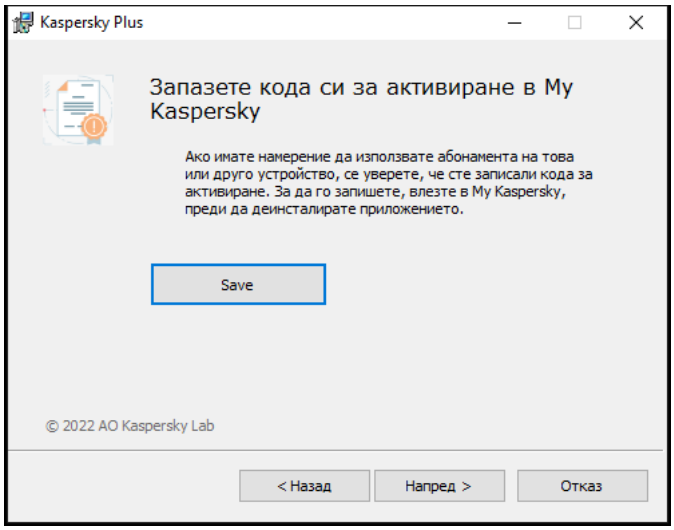
1. За да премахнете приложението, трябва да въведете паролата, за да осъществите достъп до настройките на приложението. Ако не можете да посочите паролата поради някаква причина, премахването на приложението ще бъде забранено. След като въведете паролата, щракнете **Потвърждение**.



Тази стъпка е налична само ако е била зададена парола за премахване на приложението.

2. Запазване на абонамента си от своя My Kaspersky акаунт.

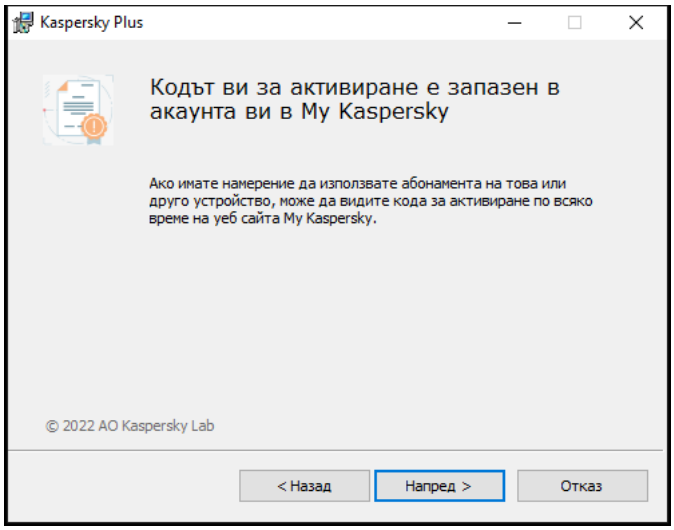
   На тази стъпка можете да посочите дали искате да запазите абонамента във Вашия My Kaspersky акаунт за бъдеща употреба.



   a. Ако искате да запазите абонамент, щракнете върху бутона **Save**.

   b. Щракнете **Напред >**.

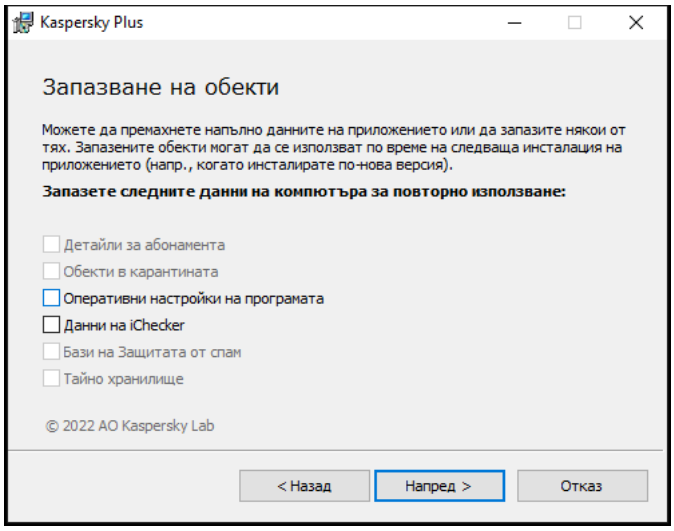
   Ще се покаже прозорецът със запазения абонамент.



   a. Щракнете **Напред >**.

3. Запис на данни за бъдеща употреба

   По време на тази стъпка може да посочите кои данни, използвани от приложението, искате да запазите за допълнителна употреба при следващото инсталиране на приложението (например когато инсталирате по-нова версия на приложението).



Може да запишете следните данни:

- **Детайли за абонамента** е набор от данни, които управляват необходимостта от активиране на приложението при бъдещо инсталиране, като ви позволяват да ги използвате с настоящия абонамент, докато той не изтече, преди да стартирате инсталирането.
- **Обекти в карантината** са файлове, сканирани от приложението и преместени в Карантина.

  След като приложението е премахнато от компютъра, файловете под карантина стават неналични. За да извършвате операции с тези файлове, приложението Kaspersky трябва да бъде инсталирано.

- **Оперативни настройки на програмата** са стойности на настройките на приложението, избрани при конфигуриране на приложението.

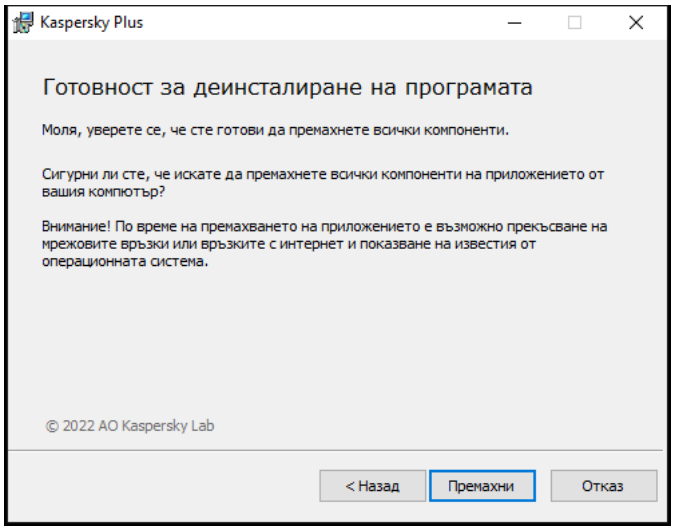
Освен това може да експортирате настройките на защитата в командния прозорец, като използвате следната команда: `avp.com EXPORT <file_name>`.

- **Данни на iChecker** са файлове, съдържащи информация за обекти, които вече са сканирани с помощта на технологията iChecker.
- **Бази на Защитата от спам** са бази данни с образци на спам съобщения, добавени от потребителя.
- **Тайно хранилище** са файлове, поставени в хранилището с помощта на функцията Тайно хранилище.

За да продължите с деинсталирането на приложението, щракнете **Напред >**.

4. Потвърждаване на премахването

   Тъй като премахването на приложението застрашава сигурността на вашия компютър и лични данни, ще бъдете помолени да потвърдите намерението си да премахнете приложението. За целта щракнете върху бутона **Премахни**.



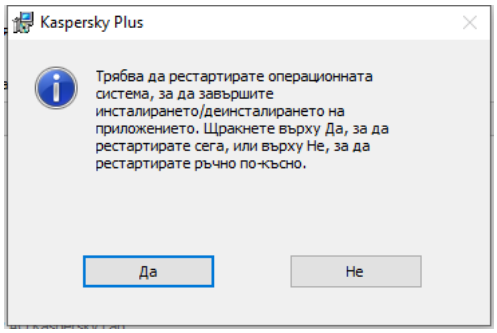
5. Завършване на премахването

   По време на тази стъпка Съветникът премахва приложението от вашия компютър. Изчакайте докато премахването завърши.

   > Тази функционалност може да не е налична в някои региони.

   По време на премахване на приложението трябва да рестартирате вашата операционна система. Ако отмените незабавното рестартиране, завършването на процедурата по премахване се отлага до рестартирането на операционната система или до изключване на компютъра и стартирането му.

6. За да рестартирате компютъра, щракнете **Да**.



Как да актуализирате приложението

Приложението се актуализира автоматично, ако изберете режим **Автоматично** актуализиране в прозореца за настройки за актуализиране (**Защита** → **Актуализация на антивирусните бази данни** → **График за актуализация на базите данни**).

Приложението автоматично се актуализира, ако инсталирате нова версия на приложението върху предишна.

Как да защитим повече устройства

Предлага се само в Kaspersky Standard, Kaspersky Plus и Kaspersky Premium.

Можете да използвате абонамента си, за да защитите всички устройства, работещи с операционни системи Microsoft Windows, Android, iOS и macOS. Точният брой устройства, на които можете да използвате абонамента, е посочен в свойствата на абонамента, когато правите покупката си.

Винаги можете да проверите колко устройства вече защитавате и колко още можете да защитите в раздела **Профил** на приложението и във вашия акаунт в My Kaspersky. Там ще намерите и лесни за използване инструменти за споделяне на Вашата защита с друго устройство.

За да споделите защита с помощта на тези инструменти, не е необходимо да помните кода за активиране, абонаментът се прехвърля през Вашия акаунт. Ако никога не сте влизали в акаунта си в My Kaspersky на съответното устройство, ще Ви помолим да го направите като част от процеса. След инсталацията Вашите приложения се активират автоматично с абонамента от Вашия акаунт.

За да споделите защита от вашето приложение:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Профил**.
3. Щракнете върху бутона +. При някои абонаменти текстът на бутона гласи **Защитаване на устройство**.
4. В прозореца **Защитете още устройства** изберете една от следните опции:

   - **Сканиране на QR код**

     В раздела **QR код** насочете камерата на телефона си към QR кода.

     На вашето мобилно устройство това отваря Google Play Store, App Store или Huawei AppGallery на страницата за изтегляне на приложението. След като изтеглите и инсталирате приложението, то автоматично ще се свърже към My Kaspersky и ще започне да защитава устройството ви.

     > Използвайки QR код на устройство с Android, вие се съгласявате да предоставите еднократна парола на Google Play, за да активирате приложението на вашия смартфон.

   - **Изпращане на връзка по имейл**

     a. Отидете на раздела **По имейл**.

     b. Щракнете върху връзката.

     Това отваря прозореца за влизане в My Kaspersky във вашия браузър по подразбиране.

     c. В прозореца **Изпрати по имейл** въведете имейл адреса в текстовото поле и щракнете върху **Изпрати**.

     d. Изтеглете приложението, като следвате връзката в имейла.

     След изтегляне и инсталиране приложението автоматично се свързва с вашия акаунт в My Kaspersky.

> За някои абонаменти може да бъде показана само общата информация за максималния брой устройства, които можете да защитите.

За да научите повече за дистанционното управление на защитата на устройството, отмяната на абонамента от потребител или от устройство, вижте Помощ на My Kaspersky.

Основна функционалност на приложението

В този раздел ще научите за основната настройка на приложението, включително конфигуриране на известия и потребителски интерфейс, както и как да коригирате проблемите със сигурността, които могат да възникнат.

Оценяване на състоянието на защита на компютъра и разрешаване на проблеми със сигурността

Проблеми с компютърната защита се обозначават с индикатор в горната част на основния прозорец на приложението. Зелено показва, че вашият компютър е защитен. Жълто показва, че има проблеми със защитата, а червено показва, че сигурността на вашия компютър е в сериозен риск. Съветваме ви да коригирате проблемите и заплахите за сигурността незабавно.

Може да отворите прозореца **Център за уведомяване**, като щракнете върху бутона **Детайли** в основния прозорец на приложението. Този прозорец предоставя детайлна информация за състоянието на защита на компютъра и предлага възможни действия за коригиране на проблемите и заплахите.

Проблемите със защитата са групирани по категории. За всеки проблем се показва списък с действия, които може да предприемете, за да разрешите проблема.

В раздела **Статус** се показва информация за състоянието на защитата на компютъра и състоянието на абонамента. Ако са открити проблеми, които трябва да бъдат отстранени, до известието се показва бутон **Поправи**; можете да отстраните проблемите със сигурността, като щракнете върху този бутон.

Разделът **Препоръки** изброява действия, които трябва да се извършат, за да се оптимизира работата на приложението и да се използва по-ефективно.

В раздела **Новини** се показват новини за киберсигурността.

Кликването върху **Покажи N игнорирани известия** показва известия, към които **Пропусни** е приложено действието. Игнорираните известявания не влияят на цвета на индикатора за защита в основния прозорец на приложението.

Как да отстраните проблеми със сигурността на компютъра си

За да отстраните проблеми със защитата на компютъра:

1. Отворете основния прозорец на приложението.
2. Щракнете върху връзката **Детайли** в горната част на основния прозорец на приложението, за да отидете в прозореца **Център за уведомяване**.
3. Отидете на раздел **Статус**. В този раздел се показват проблемите със сигурността на вашия компютър.
   - Изберете проблем от списъка и щракнете върху бутона за действие, например **Поправи**.
   - Изберете **Пропусни** от падащия списък, ако не искате да отстранявате този проблем сега. Можете да видите списъка с игнорирани известия по-късно, като кликнете върху бутона **Показване** на игнорирани известия.

4. Отидете на раздел **Препоръки**. В този раздел са показани препоръки, които не са задължителни, но ще ви помогнат да оптимизирате използването на приложението и да защитите по-добре компютъра си.

   a. Изберете предложение от списъка.

   b. Щракнете върху бутона до предложеното действие; например щракнете върху бутона **Включи** до предложението **Искате ли да се отървете от досадните изскачащи реклами?**.

5. Отидете на раздел **Новини**. В този раздел ще намерите новини за киберсигурността. Използвайте бутоните за навигация, за да прочетете следващия информационен елемент или да се върнете към предишната новина.

Новини за сигурността

Този раздел предоставя информация за новините за сигурността от Kaspersky.

За новините за сигурността

Всеки ден светът става свидетел все повече и повече на масови кражби на пароли, хакване на бази данни и измами с онлайн банкирането. Новините за сигурността на Kaspersky предоставят нова информация за такива престъпления и помага да предотвратите ситуации, в които бихте могли да станете жертва на хакери. За да се уверите, че новините за сигурността, които получавате, са особено подходящи за вас, приложението анализира информация за ресурсите, които посещавате, и приложенията, които стартирате. Тази информация се използва единствено за подбор на новини, които може да са важни или интересни за вас.

Новините за сигурността се показват в Центъра за уведомявания заедно с други новини от Kaspersky. Известията за новините за сигурността се появяват в зоната за известия на лентата на задачите. Прозорците с известията съдържат заглавната част на новините и кратка препоръка за разрешаване на проблем, описан в новините.

В зависимост от нивото на сериозност новините могат да бъдат следните типове:

- *Важни новини* – новини за събития, които поставят потенциална заплаха за вашата сигурност (например, новини за масова кражба на пароли за Facebook). Прозорците, които съдържат важни новини, са жълти.
- *Общи новини* – новини, които служат за информативни цели (например, новини за все по-честите случаи на пробиви в данните при онлайн банкирането, причинени от злонамерен софтуер с троянски кон). Прозорците, които съдържат общи новини, са зелени.

Ако известието за новините за сигурността се появи на екрана, може да преминете към пълния текст на новините, като щракнете върху бутона **Детайли** в изскачащия прозорец или може да затворите изскачащия прозорец. Може да прегледате пълния текст на новините по всяко време, като изберете съответните новини в списъка с новини в Центъра за уведомявания.

Ако не искате да получавате новини за сигурността на конкретно устройство, може да изключите показването на новините. Ако не искате да получавате новини на никое от вашите устройства, може да деактивирате получаването на новини в My Kaspersky.

Новините за сигурността не се показват през първия час работа на приложението, след като е инсталирано.

Как да активирате или деактивирате новините за сигурността

За да активирате или деактивирате новините за сигурността:

1. Отворете основния прозорец на приложението.
2. Щракнете върху в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.
3. Изберете раздела **Настройки на интерфейс**.

   Отваря се прозорецът **Настройки на интерфейс**.
4. В раздела **Рекламни материали** изпълнете едно от следните:

   - Ако искате да получавате новини за сигурността, изберете квадратчето за отметка **Получаване на информационни съобщения и реклами от Kaspersky**.
   - Ако не искате да получавате новини за сигурността, изчистете квадратчето за отметка **Получаване на информационни съобщения и реклами от Kaspersky**.

Как да активирате или деактивирате получаването на новини за сигурността в My Kaspersky

За да активирате или деактивирате получаването на новини за сигурността в My Kaspersky:

1. Отворете главната страница на My Kaspersky.
2. Щракнете върху бутона **Влизане** и въведете вашия имейл адрес, който сте посочили, когато сте създавали акаунта, и паролата.
3. Щракнете върху бутона .

   Отваря се прозорецът за преглед на известията.
4. Щракнете върху връзката **Настройки**, за да отидете в прозореца с настройки на известията.
5. Направете някое от следните действия:

   - Ако искате да активирате получаването на новини за сигурността, изберете квадратчето за отметка **Новини за сигурността**.
   - Ако искате да деактивирате получаването на новини за сигурността, изчистете квадратчето за отметка **Новини за сигурността**.

Дневник за дейността на приложението и подробен отчет

В главния прозорец можете да видите кратък преглед на всички действия, извършени от приложението по време на работа. Тази информация ви помага да разберете как точно приложението защитава вашето устройство и вашите данни.

За да видите времевата линия:

1. Отворете основния прозорец на приложението.

   В раздел **Начална страница** погледнете под **Времева линия**, за да видите кратка история на дейността на приложението.

2. За да видите историята на активността на приложението, щракнете върху **Преглед на всички**.

   Това отваря прозорец с подробно описание на действията, предприети от приложението, и времето, когато са настъпили събитията.

3. За да видите подробен отчет за приложението, щракнете върху **Покажи отчетите**.

   Това ви отвежда до прозорец **Отчети**.

Можете също да видите подробния отчет, като щракнете върху **Отчети** в раздела **Защита**. Прозорецът **Отчети** показва данни във формата на таблица. За удобен преглед на отчетите може да изберете различни опции за филтриране.

Как да конфигурирате интерфейса на приложението

Този раздел съдържа информация как да конфигурирате интерфейса на приложението.

Как да се конфигурират известията на приложението

Известията, които се появяват в областта за уведомяване в лентата на задачите ви информира за събития на приложението, които изискват вашето внимание. В зависимост от колко критично е събитието, може да получите следните типове известия:

- *Критичните известия* ви информират за събития, които имат критична важност за сигурността на компютъра, като например откриването на злонамерен обект или опасна активност на операционната система. Прозорците, използвани за критични известия и изскачащи съобщения, са червени.

- *Важните известия* ви информират за събития, които са потенциално важни за сигурността на компютъра, като например откриване на вероятно заразен обект или подозрителна активност в операционната система. Прозорците, използвани за важни известия и изскачащи съобщения, са жълти.

- *Информационните известия* ви информират за събития, които нямат критична важност за сигурността на компютъра. Прозорците, използвани за информационни известия и изскачащи съобщения, са зелени.

Ако дадено уведомление се покаже на екрана, трябва да изберете една от опциите, които са предложени на него. Оптималната опция е препоръчаната по подразбиране от експертите на Kaspersky.

Известието може да бъде затворено автоматично, когато компютърът се рестартира, когато приложението Kaspersky се затвори или е в режим на Свързаност и Готовност в Windows 8. Известията на Предотвратяване на проникване се затварят автоматично след 500 секунди. Известията за стартирането на приложението се затварят след 1 час. Когато известие се затвори автоматично, приложението Kaspersky извършва препоръчаното действие по подразбиране.

Щракнете върху връзките по-долу, за да научите как да конфигурирате известията на приложението.

Как да конфигурирате доставянето на известия

За да създадете правила за известия:

1. Отворете основния прозорец на приложението.
2. Щракнете върху ⚙ в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.
3. Изберете раздела **Настройки на интерфейс**.
4. В блока **Уведомления** щракнете върху връзката **Настройки за уведомяване**, за да продължите към прозореца с настройки на известията.
5. Изберете компонента от списъка вляво.

   Дясната част на прозореца показва списък със събития, които могат да настъпят по време на работата на този компонент.
6. Изберете събитие от списъка и поставете отметка в следните квадратчета:

   - **Запазване в локален доклад**. Когато настъпи събитието, информация за него ще бъде записана в доклада, който се съхранява на локалния компютър.
   - **Известяване на екрана**. Когато настъпи събитието, се показва изскачащо известие над иконата на приложението в областта за уведомяване в лентата на задачите.

   Може да използвате падащия списък в долния ляв ъгъл, за да посочите кои известия искате да запишете в локалния отчет:

   - **По подразбиране**. Когато е избрана тази опция, генерираният отчет ще запише събитията, избрани от експертите на Kaspersky.
   - **Ръчно**. Тази опция се избира автоматично, ако конфигурирате възможността ръчно да записвате събития в отчет.
   - **Критичен**. Когато е избрана тази опция, генерираният отчет ще запазва **Критични събития** (включително *събития, свързани с неизправността на Приложението* за **Системен одит** и **Предотвратяване на проникване** компонента).
   - **Важни**. Когато е избрана тази опция, генерираният отчет ще записва **Критични събития** (включително *Събития, свързани с неизправността на приложението* за компонента **Системен одит** и **Предотвратяване на проникване**) и **Предупреждения**.
   - **Информационно**. Когато е избрана тази опция, генерираният отчет ще записва всички събития.

Известия за всички промени, свързани със събитието **Приложението работи и обработва данни съгласно съответните закони и използва подходящата инфраструктура**, винаги се показват на екрана в областта на лентата на задачите. Изчистването на квадратчето за отметка не променя настройката.

[Как да конфигурирате доставянето на известия, съдържащи новини и специални оферти от Kaspersky](#)

Ако искате да останете информирани за последните новини за киберсигурността и да получавате специални оферти от Kaspersky:

1. Отворете основния прозорец на приложението.
2. Щракнете върху ⚙ в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.
3. Отидете в раздела **Настройки на интерфейс**.
4. В блока **Уведомления за новини** поставете отметка в квадратчето **Получаване на информационни съобщения и реклами от Kaspersky**, ако искате да получавате известия за новини за сигурността на компютъра.
5. В раздела **Рекламни материали** изпълнете едно от следните:

   - Поставете **Получаване на информационни съобщения и реклами от Kaspersky** отметка в квадратчето, ако искате да получавате известия за новини, свързани с компютърната сигурност.
   - Поставете отметка в квадратчето **Показване на информация за специални оферти**, ако искате да получавате най-добрите оферти, когато посещавате уеб сайтове на Kaspersky.
   - Поставете отметка в квадратчето **Получаване на информационни съобщения и реклами след изтичане на текущия период на абонамента**, ако искате да получавате известия за новините за сигурността от Kaspersky, след като вашият лиценз или абонамент изтече.

Как да активирате звуковете на известията

1. Отворете основния прозорец на приложението.
2. Щракнете върху ⚙ в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.
3. Изберете раздела **Настройки на интерфейс**.
4. В блока **Уведомления** поставете отметка в квадратчето **Активиране на звуковете на известия**.

   За да промените аудио сигнала по подразбиране на тип "квичене на прасе", напишете **IDKFA** в прозореца **Относно**.

Звуците на известията не се възпроизвеждат в Microsoft Windows 10.

Как да конфигурирате известявания, когато дадено дете използва приложението

Ако на Вашия компютър е инсталирана Kaspersky Safe Kids, можете да разрешите или забраните известявания от Kaspersky, когато дадено дете използва компютъра.

За да конфигурирате известията, когато дадено дете използва приложението:

1. Отворете основния прозорец на приложението.
2. Щракнете върху в долната част на главния прозорец.
   Отваря се прозорецът **Настройки**.
3. Отидете в раздела **Настройки на интерфейс**.
4. Изберете опция:
   - Изчистете квадратчето **Покажи известия в акаунтите на децата**, за да изключите известията от Kaspersky, когато дете използва приложението.
   - Изберете квадратчето **Покажи известия в акаунтите на децата**, за да включите известията от Kaspersky, когато дете използва приложението.

Подробности за конфигурирането на приложението Kaspersky, когато дадено дете използва компютър.

Как да промените темата на дизайна на приложението

Възможността да се променя темата на дизайна на приложението не е налична в някои региони.

За да промените темата на дизайна на приложението:

1. Отворете основния прозорец на приложението.
2. Щракнете върху в долната част на главния прозорец.
   Отваря се прозорецът **Настройки**.
3. Изберете раздела **Настройки на интерфейс**.
4. В блока **Дизайн на тема** изберете една от следните опции:
   - **Същото като операционната система**. Използва се текущата тема за дизайн на операционната система.
   - **Леко**. Използва се светлата тема за дизайн на приложението.
   - **Тъмна**. Използва се тъмната тема за дизайн на приложението.
   - **Използване на тема с персонализиран дизайн**, ако искате да използвате персонализирана тема за дизайн. Щракнете върху **Избор** и въведете пътя до ZIP архива или папката, съдържаща файловете с темата с персонализиран дизайн.

Темата на дизайна се прилага след рестартиране на приложението.

Как да конфигурирате иконата на приложението

В този раздел ще научите за конфигурирането на иконата на приложението на вашия работен плот и в областта за известяване.

Как да промените иконата на приложението

За да промените иконата на приложението:

1. Отворете основния прозорец на приложението.
2. Щракнете върху в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.
3. Изберете раздела **Настройки на интерфейс**.
4. В блока **Икона на приложението** изберете една от следните опции:

   - **Стандартна икона**. Когато е избрана тази опция, работният плот и областта за уведомяване ще показват стандартната икона на приложението.
   - **Midori Kuma**. Когато е избрана тази опция, работният плот и областта за уведомяване ще показват иконата, съдържаща изображение на мече-талисман, известно като Midori Kuma.

Ако искате да се върнете към традиционната икона на приложението K-letter, въведете **IDDQD** в прозореца **Относно**. За да приложите промените, трябва да рестартирате компютъра.

Как да промените иконата в областта за уведомяване в зависимост от състоянието на защита

За да промените иконата на приложението Kaspersky в областта за уведомяване в зависимост от състоянието на приложението:

1. Отворете основния прозорец на приложението.
2. Щракнете върху в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.
3. Изберете раздела **Интерфейс**.
4. В блока **Покажи статуса на приложението в областта за уведомления** изберете състояние и квадратче за отметка.

Когато приложението превключи към състояние, съответстващо на избраното, иконата на приложението в областта за уведомяване ще се промени.

Как да защитите с парола достъпа до функциите за управление на приложението

Един компютър може да бъде споделян с няколко потребители с различни нива на опит и компютърна грамотност. Неограничен достъп на различни потребители до приложението и неговите настройки може да компрометира нивото на сигурност на компютъра.

За да ограничите достъпа до приложението, може да определите администраторска парола за акаунта `KLAdmin`. Този потребител има неограничени права за управление и промяна на настройките на приложението, и за задаване на разрешения за достъп до приложението на други потребители. След като сте създали парола за `KLAdmin`, може да зададете разрешения за достъп до приложението на различни потребители или групи потребители.

За да създадете администраторска парола за `KLAdmin`:

1. Отворете основния прозорец на приложението.
2. Щракнете върху в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.
3. Изберете раздела **Настройки на интерфейс**.
4. Преместете превключвателя **Защита с парола** на **Вкл**.
5. В отворения прозорец попълнете полетата **Потребителско име** (препоръчва се KLAdmin), **Въвеждане на парола** и **Потвърждение на паролата**.

   Съвети за създаване на сигурна парола:

   - Паролата трябва да съдържа поне осем и не повече от 128 знака.
   - Паролата съдържа поне една цифра.
   - Паролата съдържа малки и главни букви.
   - Паролата трябва да съдържа поне един специален символ (например: ! @ # $ % ^ & *).
6. Щракнете върху **Запази**.

Забравена парола не може да бъде възстановена. Ако сте забравили своята парола, се свържете с екипа за техническа поддръжка, за да възстановите достъпа до настройките на приложението.

Потребителят `KLAdmin` може да задава разрешения на следните потребители и потребителски групи:

- Потребителска група `Всеки`. Тази група включва всички потребители на операционната система. Ако дадете на тази група разрешение да извършва конкретно действие, то потребителите в групата винаги ще имат разрешение да извършват това действие дори ако конкретен потребител или потребителска група, принадлежаща към потребителската група `Всеки`, няма индивидуално разрешение за извършване на действието. По подразбиране членовете на групата `Всеки` не могат да извършват никакви действия.
- `<system user>`. По подразбиране избраният потребител не може да извършва никакви действия. Това означава, че когато се опитвате да изпълните забранено действие, ще бъдете подканени на въведете

паролата на вашия KLAdmin акаунт.

Как да добавите потребител или потребителска група

1. В раздела **Настройки на интерфейс** в блока **Покажи статуса на приложението в областта за уведомления** щракнете върху бутона **Добави**.

   Отваря се прозорецът **Добавяне на разрешения за потребител или група**.

2. Щракнете върху връзката **Избиране на потребител или група**, за да отворите прозореца за избор на потребител или група от потребители на операционната система.

3. В полето за въвеждане на име на обект посочете името на потребителя или потребителската група (като например Администратор).

4. Щракнете **OK**.

5. В прозореца **Добавяне на разрешения за потребител или група** в блока **Разрешения** изберете квадратчетата за отметка до действията, които искате да разрешите за конкретен потребител или потребителска група.

Как да редактирате разрешения за потребител или потребителска група

В раздела **Настройки на интерфейс** в блока **Покажи статуса на приложението в областта за уведомления** изберете потребителя или потребителската група в списъка и щракнете върху бутона **Редактирай**.

Как да разрешите действие за отделен потребител или потребителска група

1. Отидете в прозореца **Добавяне на разрешения за потребител или група** за групата Всеки и махнете отметката от опцията, която разрешава това действие, ако е активирана.

2. Отидете в прозореца **Добавяне на разрешения за потребител или група** за избрания потребител и изберете квадратчето за отметка, за да разрешите това действие.

Как да забраните действие за отделен потребител или потребителска група

1. Отидете в прозореца **Добавяне на разрешения за потребител или група** за групата Всеки и махнете отметката от опцията, която разрешава това действие, ако е активирана.

2. Отидете в прозореца **Добавяне на разрешения за потребител или група** за избрания потребител и махнете отметката от опцията, която разрешава това действие.

Когато се опитате да извършите някакво действие от списъка в прозореца **Добавяне на разрешения за потребител или група**, приложението ще ви помоли да въведете парола. В прозореца за парола въведете потребителското име и парола за текущия потребителски акаунт. Действието ще се изпълни, ако посоченият акаунт има разрешение да извършва това действие. В прозореца за парола може да посочите интервала от време, през който потребителят няма да е необходимо да въвежда отново паролата.

В прозореца за парола можете да превключвате езика за въвеждане само с натискане на **ALT+SHIFT**. Всички други преки пътища няма да превключат езика за въвеждане, дори ако този пряк път е конфигуриран в операционната система.

Как да възстановите настройките по подразбиране на приложението

Може да възстановите по всяко време настройките, препоръчани от експертите на Kaspersky. Когато настройките се възстановят, нивото на защита **Оптимално** се задава за всички защитни компоненти.

За да възстановите настройките по подразбиране на приложението:

1. Отворете основния прозорец на приложението.
2. Щракнете върху в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.
3. Изберете раздела **Управление на настройките**.
4. Щракнете върху връзката **Възстанови**, за да стартирате Съветника за възстановяване на настройки.
5. Щракнете **Напред**.

   Прозорецът на Съветника показва напредъка на възстановяването на настройките на приложението до настройките по подразбиране, конфигурирани от експертите на Kaspersky.
6. След като процесът по възстановяване на настройките по подразбиране на приложението завърши, щракнете върху **Готово**.

Как да приложите настройките на приложението на друг компютър

След като конфигурирате Kaspersky по определен начин, после можете да приложите настройките на друг компютър. В резултат Kaspersky ще бъде конфигурирано идентично на двата компютъра.

Настройките на приложението Kaspersky са записани в конфигурационен файл, който може да преместите от единия компютър на другия.

Настройките на приложението Kaspersky се преместват от един компютър на друг в три стъпки:

1. Запишете настройките на приложението Kaspersky в конфигурационен файл.
2. Преместете конфигурационния файл на друг компютър (например по имейл или на сменяемо устройство).
3. Импортирайте настройките от конфигурационния файл в копието на приложението Kaspersky, което е инсталирано на другия компютър.

Как да експортирате настройките

Експортиране на настройките на Kaspersky:

1. Отворете основния прозорец на приложението.
2. Щракнете върху в долната част на главния прозорец.
   Отваря се прозорецът **Настройки**.
3. В прозореца **Настройки** изберете раздела **Управление на настройките**.
4. Изберете **Експорт**.
5. Отваря се прозорецът **Запази**.
6. Посочете име за конфигурационния файл и щракнете върху бутона **Запази**.

Настройките на приложението сега са записани в конфигурационния файл.

Освен това може да експортирате настройките на приложението Kaspersky в командния прозорец, като използвате следната команда: `avp.com EXPORT <file_name>`.

По време на експортирането на настройките на приложението Kaspersky, адресите на уеб сайтовете, които сте добавили към Безопасно плащане, се записват само за текущия потребител. По време на импортирането на настройките на друг компютър адресите на уеб сайтовете не се записват.

Как да импортирате настройките

За да импортирате настройки в приложението Kaspersky, инсталирана на друг компютър:

1. На другия компютър отворете основния прозорец на приложението на Kaspersky.
2. Щракнете върху бутона в долната част на прозореца.
   Отваря се прозорецът **Настройки**.
3. В прозореца **Настройки** изберете раздела **Управление на настройките**.
4. Изберете **Импорт**.
   Отваря се прозорецът **Отвори**.
5. Посочете конфигурационен файл и щракнете върху бутона **Отвори**.

Настройките се импортират в приложението Kaspersky, което е инсталирано на другия компютър.

Как да паузирате и възобновите защитата на компютъра

Преустановяване на защитата означава временно да деактивирате всички защитни компоненти за известно време.

Когато защитата е преустановена временно или приложението Kaspersky не работи, дейността на приложенията, които работят на Вашия компютър, се наблюдава. Информация за резултатите от наблюдението на дейността на приложенията се записва в операционната система. Когато приложението Kaspersky се стартира отново или защитата се възобнови, приложението използва тази информация да защитава компютъра Ви от злонамерени действия, които може да са изпълнени, когато защитата е била временно преустановена или когато приложението Kaspersky не е работило. Информацията за резултатите от наблюдението на дейността на приложенията се съхранява за неопределено време. Тази информация се изтрива, ако приложението Kaspersky се премахне от Вашия компютър.

За пауза на защитата на компютъра:

1. В контекстното меню на иконата на Kaspersky, намираща се в областта за уведомяване на лентата на задачите, изберете елемента **Pause protection**.

   Отваря се прозорецът **Пауза на защитата**.

2. В прозореца **Пауза на защитата** изберете интервала от време, след който защитата ще бъде възобновена:

   - **Пауза за** – защитата се активира след изтичане на интервала от време, избран от падащия списък.
   - **Пауза до рестартиране на приложението** – защитата се активира, след като приложението се активира отново или операционната система се рестартира (ако приложението стартира автоматично при стартиране).
   - **Пауза** – защитата ще се възобнови, когато решите да я възобновите.

3. Щракнете върху бутона **Пауза на защитата** и потвърдете избора си в прозореца, който се отваря.

Как да възобновите защитата на компютъра

За да възобновите защитата на компютъра:

В областта за уведомяване на лентата на задачите в контекстното меню на иконата на Kaspersky изберете **Resume protection**.

Оценяване на приложението Kaspersky

Може да оцените нашето приложение и да изпратите Вашата оценка на Kaspersky.

Известно време след инсталацията приложението ви предлага да оцените работата му.

За да оцените приложението:

1. В прозореца **Ние ценим вашето мнение** направете някое от следните неща:

- Ако сте готови да оцените Kaspersky, оценете приложението по 10-точковата скала.
- Ако не искате да оцените приложението, щракнете върху бутона ×, за да затворите прозореца за оценяване.

2. Щракнете върху бутона **Изпрати**.
3. Щракнете върху бутона **Затвори**, за да затворите прозореца.

Какви данни се прехвърлят при оценяване на приложението

В допълнение към оценката, Kaspersky обработва следната информация, която е необходима за анализиране на анкетата:

- Име и версия на приложението Kaspersky
- Версия на операционната система
- Регион за активиране и език на потребителския интерфейс на приложението Kaspersky
- Период на използване на приложението Kaspersky

Защита

Съвременните хакери стават все по-умни в стремежа си да проникнат в устройствата ви. Новите видове рансъмуер, фишинг и друг зловреден софтуер изискват нови решения за киберсигурност, които да ви изпреварят в нарастващите заплахи. Създадохме новото безплатно приложение на Kaspersky, за да ви помогнем да сте в крак със съвременните заплахи. Разберете какво можете да направите, за да се чувствате сигурни.

Сканиране на компютъра

По време на сканирането приложението търси заразени файлове и зловреден софтуер. Има няколко типа сканирания, които варират според продължителността и обхвата на търсенето.

- Пълно сканиране. Сканира всички области на компютъра. Това сканиране изисква много време, за да завърши.
- Бързо сканиране. Сканира обекти, които са заредени, когато операционната система стартира, както и системната памет и файлове за начално зареждане. Това сканиране не изисква много време, за да завърши.
- Сканиране по избор. Сканира избрания файл или папка.
- Сканиране на сменяеми устройства Сканиране на сменяеми устройства, като например твърди дискове и USB памет, свързани към компютъра.
- Незабавно сканиране на файлове. Тази опция сканира файлове от контекстното меню.
- Сканиране във фонов режим. Сканиране на системна памет, системния дял, стартиращи сектори и обекти на стартиране, както и търсене на комплекти за пълен достъп.
- Сканиране за уязвимости в приложения. Сканирайте компютъра за уязвимости в приложенията, които зловредният софтуер може да използва, за да зарази системата ви.

След като инсталирате приложението, ви препоръчваме да направите пълно сканиране на вашия компютър.

Как да стартирате Бързо сканиране

По време на бързо сканиране приложението сканира по подразбиране следните обекти:

- Обекти, заредени при стартиране на операционната система;
- Системна памет
- Стартиращи сектори на диска;

За да изпълните „Бързо сканиране“:

1. Отворете главния прозорец на приложението и извършете следните действия:

- Отидете в раздел **Начална страница** и щракнете върху бутона **Бързо сканиране**.
- Отидете на раздел **Защита**.
    1. В блока **Сканиране** щракнете върху бутона **Избор на сканиране**.
    2. Отваря се прозорецът **Сканиране**.
    3. В прозореца **Сканиране** изберете раздела **Бързо сканиране**.
    4. В раздела **Бързо сканиране** щракнете върху бутона **Стартирай сканиране**.

Приложението започва бързо сканиране на компютъра ви.

Как да стартирате Пълно сканиране

По време на пълно сканиране приложението сканира по подразбиране следните обекти:

- Системна памет
- Обекти, заредени при стартиране на операционната система;
- Резервно хранилище на системата;
- Твърди дискове и сменяеми дискове.

Препоръчваме да стартирате пълно сканиране незабавно след инсталиране на приложението на вашия компютър.

За да стартирате Пълно сканиране:

1. Отворете главния прозорец на приложението и отидете в раздела **Защита**.
2. В блока **Сканиране** щракнете върху бутона **Избор на сканиране**.

   Отваря се прозорецът **Сканиране**.
3. В прозореца **Сканиране** изберете раздела **Пълно сканиране**.
4. В падащия списък до бутона **Стартирай сканиране** изберете действието, което да се извърши след приключване на сканирането.
5. Щракнете **Стартирай сканиране**.

Приложението започва пълно сканиране на компютъра ви.

Как да стартирате Сканиране по избор

Сканиране по избор ви позволява да сканирате файл, папка или диск за вируси и други заплахи.

За стартиране на Сканиране по избор:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Защита**.
3. В блока **Сканиране** щракнете върху бутона **Избор на сканиране**.

   Отваря се прозорецът **Сканиране**.
4. В прозореца **Сканиране** изберете раздела **Сканиране по избор**.
5. Щракнете върху бутона **Избор** и посочете обекта в прозореца за избор на файла или папката, който се отваря.
6. Щракнете **Стартирай сканиране**.

Как да стартирате сканиране на сменяемо устройство

Сменяеми устройства, които свързвате към компютъра, могат да съдържат вируси или други прилежния, които представляват заплаха. Приложението Kaspersky сканира сменяемите устройства, за да предпази Вашия компютър от заразяване. Може да конфигурирате да се стартира ръчно или автоматично сканиране на сменяемо устройство, когато е свързано към компютъра. Автоматичното сканиране на сменяеми устройства е включено по подразбиране.

За да изпълните ръчно сменяемо устройство, сканирайте ръчно:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Защита**.
3. В блока **Сканиране** щракнете върху бутона **Избор на сканиране**.

   Отваря се прозорецът **Сканиране**.
4. В прозореца **Сканиране** изберете раздела **Сканиране на сменяемо устройство**.
5. В падащия списък изберете буквата на диска на външното устройство и щракнете върху бутона **Стартирай сканиране**.

Приложението ще започне сканиране на свързаното устройство.

Как да стартирате сканиране на файл или папка от контекстното меню

За да стартирате сканиране на файл или папка от контекстното меню

1. Щракнете с десния бутон на мишката върху файла или папката, които трябва да бъдат сканирани.
2. В контекстното меню, което се отваря, изберете **Сканирай за вируси**.

Приложението ще стартира сканиране на избрания файл или папка.

В Microsoft Windows 11 трябва да разширите контекстното меню на обект, за да видите командите за приложения.

Как да включите или изключите сканиране във фонов режим

Сканиране във фонов режим е автоматичен режим на сканиране, който не показва известия. Това сканиране изисква по-малко компютърни ресурси от други типове сканирания (например Пълно сканиране). Когато е в този режим, приложението сканира системната памет, системните обеми, сектори за начално стартиране и обекти на стартиране, и търсения за комплекти за пълен достъп.

Сканиране във фонов режим стартира в следните случаи:

- След актуализиране на базите данни и модулите за приложения
- 30 минути след пускането на приложението
- На всеки шест часа.
- Ако компютърът остане неактивен за пет или повече минути (след като скрийнсейвърът е стартиран).

Сканиране във фонов режим прекъсва, когато е изпълнено някое от следните условия:

- Компютърът става отново активен.
- Компютърът (лаптопът) преминава към режим на батерия.

Ако не е извършено фоново сканиране за повече от десет дни, сканирането не е спряно. Когато работи във фонов режим, приложението не сканира файлове, чието съдържание се намира в облачната услуга за съхранение OneDrive.

За да включите или изключите сканиране във фонов режим:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Защита**.
3. В блока **Сканиране** щракнете върху бутона **Избор на сканиране**.
   Отваря се прозорецът **Сканиране**.
4. Щракнете върху иконата в блока **Сканиране във фонов режим**.
   Отваря се прозорецът **Настройки за фоново сканиране**.
5. В прозореца **Настройки за фоново сканиране** преместете превключвателя на **Вкл**. или **Изкл**.

Как да създадете график за сканиране

За да създадете график за сканиране:

1. Отворете основния прозорец на приложението.

2. Отидете в раздела **Защита**.

3. В блока **Сканиране** щракнете върху бутона **Избор на сканиране**.

   Отваря се прозорецът **Сканиране**.

4. В прозореца **Сканиране** изберете типа сканиране и щракнете върху иконата .

5. В отворения прозорец щракнете върху връзката **График на сканиране**, за да преминете към прозореца **График на сканиране**.

6. В прозореца **График за сканиране** в списъка **Стартирай сканиране** изберете период, като например **Всеки ден** и посочете часа за стартиране на сканирането.

График за сканиране не може да бъде създаден за Сканиране от типа сканиране от Контекстно меню или Сканиране във фонов режим.

Как да търсите уязвимости в приложения, инсталирани на вашия компютър

Приложения, инсталирани на вашия компютър, могат да имат уязвимости, които да бъдат използвани от злонамерен софтуер. Сканирането на вашия компютър ще помогне да откриете тези уязвимости и да се предотврати заразяване на вашия компютър.

За да стартирате Сканиране за уязвимости в приложенията:

1. Отворете основния прозорец на приложението.

2. Отидете в раздела **Защита**.

3. В блока **Сканиране** щракнете върху бутона **Избор на сканиране**.

   Отваря се прозорецът **Сканиране**.

4. В прозореца **Сканиране** изберете раздела **Сканиране за уязвимости в приложения**.

5. Щракнете **Стартирай сканиране**.

Приложението започва да сканира компютъра ви за уязвимости в приложенията.

Как да изключите файл, папка или тип заплаха от сканиране

За да изключите файл, папка или тип заплаха от сканиране:

1. Отворете основния прозорец на приложението.

2. Щракнете върху в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.

3. Отидете в **Настройки за защита** → **Заплахи и изключения**.

4. Щракнете върху връзката **Управление на изключения**, за да отворите прозореца **Изключения**.

5. Щракнете **Добави**.

6. Добавете изключение по един от следните начини:

   - Щракнете върху **Преглед** и изберете папката или файла, който искате да изключите от сканиране. Щракнете **Избор**.
   - В полето **Файл или папка** въведете пълното име или маската на файла или папката.
   - В поле **Обект**, въведете пълното име или маската на типа на заплахата в съответствие с класификацията на Kaspersky на открития обект.
   - Ако попълните и двете полета, **Файл или папка** и **Обект**, посоченият файл или папка не се сканира за посочения тип заплаха.
   - В полето **Файлов хеш** въведете хеша, ако искате файловете да бъдат изключени от сканиране чрез техните хешове.

7. Премахнете отметките от квадратчетата за защитни компоненти, за които правилото за изключение не трябва да се прилага. Въведете коментар, ако желаете.

8. Изберете състоянието **Активен** на правилото и щракнете върху **Добави**.

Посочените обекти са изключени от сканиране.

Допълнителна информация за настройките в прозореца за Заплахи и изключения

Сканиране на файлове в облачното хранилище OneDrive

В Windows 10 RS3 или по-нова приложението не сканира файлове в облачната услуга за съхранение OneDrive. Ако приложението открие такива файлове по време на сканиране, то показва известие, че файловете в облачната услуга за съхранение не са били сканирани.

Следните компоненти не сканират файлове в облачната услуга за съхранение OneDrive:

- Пълно сканиране
- Сканиране по избор
- Бързо сканиране
- Сканиране във фонов режим.

Отчетът за работата на приложението съдържа списък с файлове в облачната услуга за съхранение OneDrive, които са били пропуснати по време на сканиране.

Файлове, изтеглени от облачната услуга за съхранение OneDrive на локален компютър, се сканират от компонентите за защита в реално време. Ако сканиране на файл се отложи и файлът е качен обратно в облачната услуга за съхранение OneDrive, преди да стартира сканирането, този файл може да бъде пропуснат по време на сканиране.

Когато се изпълняват приложения и скриптове, компонентите Предотвратяване на проникване и Системно наблюдение изтеглят приложения от облачната услуга за съхранение OneDrive на локалния компютър за сканиране.

За да се уверите, че файловете от OneDrive се показват в Explorer, включете функцията Файлове при поискване в клиентското приложение OneDrive. Ако сте свързани към интернет, може да ги използвате като всеки друг файл на компютъра.

Актуализиране на антивирусните бази данни и модулите за приложения

Този раздел съдържа информация за актуализациите на базата данни и модулите на приложението.

За актуализиране на бази данни и модули за приложения

Инсталационният пакет на приложението включва бази данни и модули на приложението. С тези бази данни:

- Приложението открива голяма част от заплахите с помощта на Kaspersky Security Network, което изисква интернет връзка.
- Приложението открива рекламен софтуер, програми за автоматично набиране и друг легален софтуер, който може да се използва от нарушители за повреждане на вашия компютър или лични данни.

За пълна защита препоръчваме да актуализирате антивирусните бази данни и модулите на приложенията, веднага след инсталиране на приложението.

Базите данни и модулите на програмите се актуализират на етапи:

1. Приложението започва да актуализира базите данни и модулите на приложенията според посочените настройки: автоматично, по график или при поискване. Приложението се свързва с източник на актуализация, който съхранява пакет за актуализиране на антивирусни бази данни и модули на приложението.
2. Приложението сравнява съществуващите бази данни, налични в източника на актуализация. Ако базите данни са различни, приложението изтегля липсващите части на базите данни.

Приложението използва след това актуализираните бази данни и модулите на приложенията, за да сканира компютъра за вируси и други заплахи.

Източници за актуализация

Може да използвате следните източници за актуализация:

- Сървъри за актуализации на Kaspersky
- HTTP или FTP сървър
- Мрежова папка

Специални съображения, свързани с актуализирането на антивирусните бази данни и модулите за прилагане

Актуализациите на антивирусните бази данни и модули на приложението са предмет на следните ограничения и специфики:

- Антивирусните бази данни се считат за остарели след един ден и изключително остарели след седем дни.
- За да изтеглите пакет с актуализации от сървърите на Kaspersky, е необходима интернет връзка.
- Актуализации на антивирусните бази данни и модулите на приложението не са налични в следните случаи:
  - Абонаментът е изтекъл и гратисният период или режимът с ограничена функционалност не е наличен.
  - Използва се интернет връзка с измерено потребление. Това ограничение важи за компютри с Microsoft Windows 8 или най-нови версии на тази операционна система, ако автоматични актуализации или планирани актуализации са активирани и е зададено ограничение на трафика за връзката с измерено потребление. Ако искате приложението да актуализира антивирусните бази данни и модулите за приложения в този случай, изчистете **Ограничаване на трафика при измервани връзки** в **Настройки → Настройки за защита → Разширени настройки → Настройки за мрежата**.
  - Приложението се използва при абонамент от доставчик на услуги и вие сте спрели абонамента си на уебсайта на доставчика на услуги.

Инсталиране на пакет с актуализации

Когато се получи пакет с актуализации (корекция), приложението го инсталира автоматично. За да завършите инсталацията на пакета с актуализации, трябва да рестартирате компютъра. Докато компютърът се рестартира, иконата на приложението в областта за уведомяване е червена, а прозорецът **Център за уведомяване** на приложението показва подкана за рестартиране на компютъра.

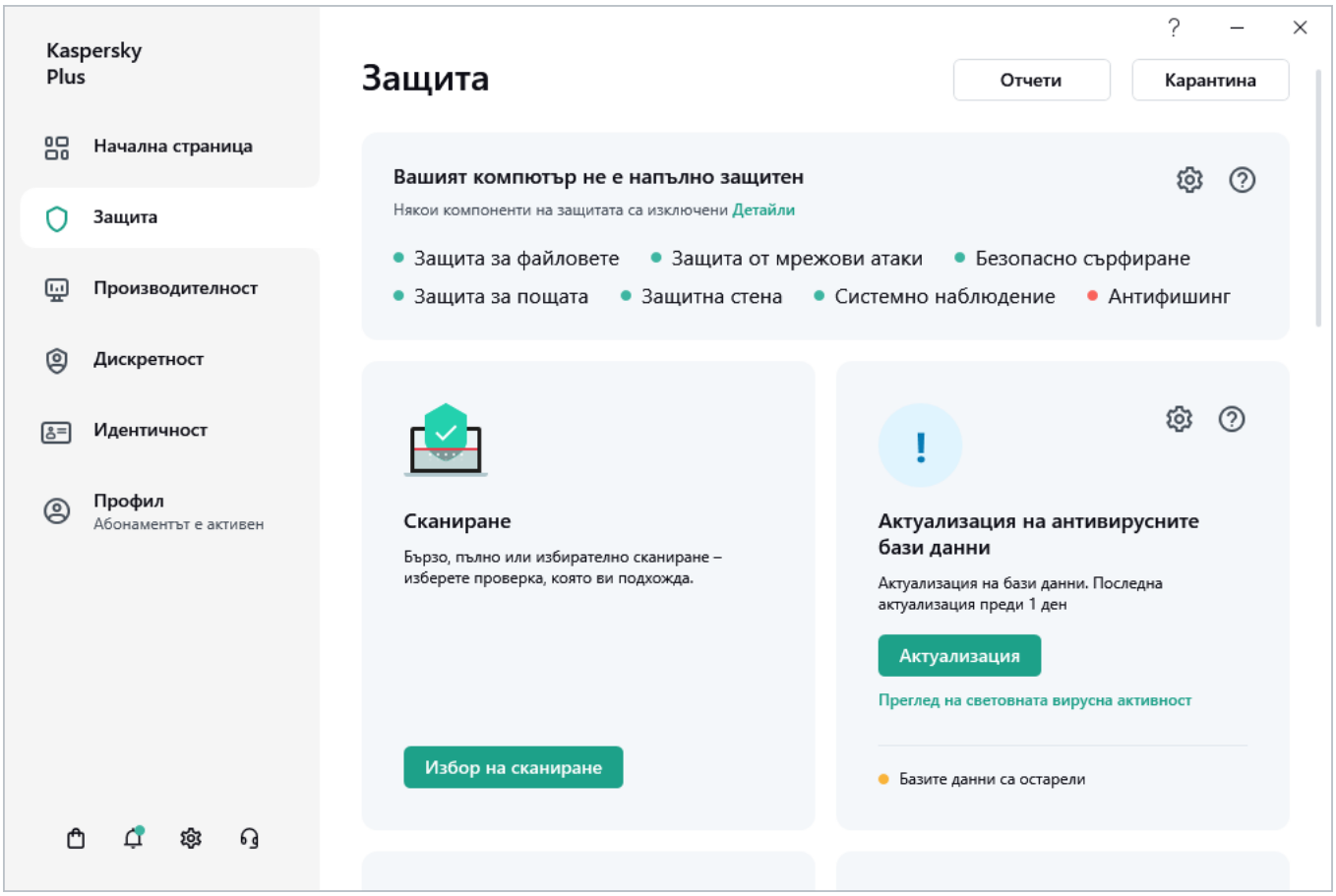
Как да стартирате актуализация на базите данни и модулите на приложението

По подразбиране, базите данни и модулите на приложенията се актуализират автоматично. Не е необходимо да извършвате някакви действия. Ако автоматичните актуализации са деактивирани, можете да актуализирате базите данни и модулите на приложението ръчно.

За да стартирате актуализация на базите данни и модулите на приложението:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Защита**.
3. В блока **Актуализация на антивирусните бази данни** щракнете върху бутона **Актуализация**.

Актуализация на антивирусна база данни



Предотвратяване на проникване

Приложението Kaspersky помага да се намали риска, свързан с използването на непознати приложения (като например риска от заразяване с вируси и друг злонамерен софтуер).

Приложението Kaspersky включва компоненти и инструменти, които позволяват проверката на репутацията на приложение и управление на действията му на Вашия компютър.

Относно Предотвратяване на проникване

Предлага се само в Kaspersky Standard, Kaspersky Plus и Kaspersky Premium.

Компонентът Предотвратяване на проникване предпазва приложения от изпълняване на действия, които може да са опасни за операционната система, и управлява достъпа до ресурсите на операционната система (включително файлови ресурси на отдалечени компютри) и личните ви данни.

Предотвратяване на проникване проследява действия, изпълнени в операционната система от приложения, инсталирани на компютъра, и ги регулира въз основа на правила. Тези правила ограничават подозрителна дейност на приложения, включително достъп на приложения до защитени ресурси, като файлове и папки, ключове от регистъра и мрежови адреси.

На 64-битови операционни системи правата на приложенията за следните действия не могат да бъдат конфигурирани:

- Директен достъп до физическата памет

- Управление на драйвер на принтер
- Създаване на услуга
- Четене на услуга
- Редактиране на услуга
- Реконфигуриране на услуга
- Управление на услуга
- Стартиране на услуга
- Премахване на услуга
- Достъп до вътрешни данни на браузъра
- Достъп до критични обекти на операционната система
- Достъп до хранилище на пароли
- Задаване на права за отстраняване на грешки
- Използване на програмни интерфейси на операционната система
- Използване на програмни интерфейси на операционната система (DNS)
- Използване на програмни интерфейси на други приложения
- Смяна на системни модули (KnownDlls)
- Стартиране на драйвери

На 64-битови Microsoft Windows 8 и Microsoft Windows 10 правата на приложенията за следните действия не могат да бъдат конфигурирани:

- Изпращане на съобщения в прозорци до други процеси
- Подозрителни операции
- Инсталиране на програми, записващи натискане на клавишите
- Прехващане на събития на входящи потоци
- Правене на екранни снимки

Мрежовата активност на приложенията се контролира от компонента Защитна стена.

Когато дадено приложение стартира на компютъра за първи път, Предотвратяване на проникване проверява безопасността на приложението и го задава към група (Сигурни, Несигурни, С големи ограничения или Със слаби ограничения). Групата определя правилата, които Kaspersky прилага за контролиране на активността на приложението.

Приложението Kaspersky задава приложения към надеждни групи (Сигурни, Несигурни, С големи ограничения или Със слаби ограничения) само ако е активиран Предотвратяване на проникване или Защитна стена, и когато и двата компонента са активирани. Ако и двата компонента са деактивирани, функционалността, която задава приложения към надеждни групи, не работи.

Може ръчно да редактирате правилата за контрол на програмите.

Правилата, които създавате за приложения, са наследени от дъщерни приложения. Например, ако забраните цялата мрежова активност за cmd.exe, тази активност също ще бъде забранена за notepad.exe, когато се стартира с помощта на cmd.exe. Когато приложение не е дъщерно на приложението, от което се стартира, правилата не се наследяват.

Как да промените настройките на Предотвратяване на проникване

Предлага се само в Kaspersky Standard, Kaspersky Plus и Kaspersky Premium.

За да промените настройките за Предотвратяване на проникване:

1. Отворете основния прозорец на приложението.
2. Щракнете върху в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.
3. Изберете раздела **Настройки за защита**.
4. Изберете компонента **Предотвратяване на проникване**.
5. В прозореца **Настройки на Предотвратяване на проникване** щракнете върху връзката **Управление на приложения**, за да отворите прозореца **Управление на приложения**.
6. Изберете приложението, което ви трябва в списъка, и щракнете два пъти върху името му, за да отворите прозореца **Правила за програмите**.
7. За да конфигурирате правилата за достъп на приложението до ресурси на операционната система:

   a. В раздела **Файлове и системен регистър** изберете съответната категория ресурси.

   b. Щракнете върху иконата в колоната с налично действие за ресурса (**Четене**, **Записване**, **Изтриване** или **Създаване**), за да отворите менюто. В менюто изберете съответния елемент (**Наследи**, **Разреши**, **Питай потребителя** или **Забрани**).
8. За да конфигурирате правата на приложението да извършва различни действия в операционната система:

   a. В раздела **Права** изберете съответната категория права.

   b. В колоната **Действие** щракнете върху иконата, за да отворите менюто, и изберете съответния елемент (**Наследи**, **Разреши**, **Питай потребителя** или **Забрани**).
9. За да конфигурирате правата на приложението да извършва различни действия в мрежата:

   a. В раздела **Мрежови правила** щракнете върху бутона **Добави**.

   Отваря се прозорецът **Мрежово правило**.

b. В прозореца, който се отваря, посочете необходимите настройки на правилата и щракнете върху **Запази**.

c. Задайте приоритет на новото правило. За целта изберете правилото и го преместете нагоре или надолу в списъка.

10. За да изключите определени действия на приложението от сканирането, в раздела **Изключения** изберете квадратчетата за отметка за действия, които не искате да бъдат контролирани.

11. Щракнете **Запази**.

    Всички изключения, създадени в правилата за Предотвратяване на проникване, са достъпни в прозореца на настройките на приложението Kaspersky в раздела **Заплахи и изключения**.

Предотвратяване на проникване мониторира и ограничава действията на приложението в съответствие с посочените настройки.

Проверка на репутацията на приложение

Kaspersky Ви позволява да проверявате репутацията на приложения с потребители по цял свят. Репутацията на дадено приложение обхваща следните критерии:

- Име на доставчика
- Информация за цифровия подпис (ако приложението е подписано цифрово)
- Информация за групата, към която е зададено приложението от Предотвратяване на проникване или повечето потребители на Kaspersky Security Network;
- Брой потребители на Kaspersky Security Network, които използват приложението (наличен, ако приложението е било включено в Надеждна група в базата данни на Kaspersky Security Network);
- Време, в което приложението става известно на Kaspersky Security Network;
- Страни, в които приложението е най-разпространено.

Проверката на репутацията на приложението е налична, ако сте приели да участвате в Kaspersky Security Network.

За да научите репутацията на дадено приложение:

Отворете контекстното меню на изпълнимия файл на приложението и изберете **Проверка на рейтинга в KSN**.

Отваря се прозорец с информация за репутацията на приложението в Kaspersky Security Network.

Сканиране за слаби настройки

В този раздел ще научите за слабите настройки на операционната система и как да търсите и поправяте слаби настройки в операционната система.

За слабите настройки на операционната система

Когато работите с компютър, настройките на операционната система могат да бъдат променяни в резултат на действията ви или действията на приложенията, които стартирате. Промяната на настройките на операционната система може да постави в риск сигурността на вашия компютър. Например ако в браузъра е активирано автоматично влизане с текущото потребителско име и парола, уеб сайт на трета страна може да прехване паролата ви.

Слабите настройки в операционната система могат да се разделят на два типа:

- *Критични настройки*. Такива настройки са приравнени към уязвимостите на операционната система.
- *Препоръчителни настройки*. Препоръчително е да поправите тези настройки, за да подобрите сигурността на операционната система.

По подразбиране приложението сканира за слаби настройки на операционната система поне веднъж дневно. Ако приложението открие слаби настройки в операционната система, ще ви подкани да ги поправите, за да възстановите сигурността на операционната система. За подробности относно всяка слаба настройка, кликнете върху връзката до съответната настройка в прозореца на приложението.

Може да щракнете върху връзката в прозореца за уведомяване, за да отидете в прозореца **Сканиране за слаби настройки**, който показва откритите в операционната система слаби настройки. Информация за слабите настройки също се показва в Центъра за уведомявания. Може да пристъпите към преглед и коригиране на слабите настройки от Центъра за уведомявания.

В прозореца **Сканиране за слаби настройки** може за извършвате следните действия:

- Коригиране на слаби настройки в операционната система.
- Игнорирай: оставете слабите настройки на операционната система непроменени.
- Отмени: възстановете коригираните преди това слаби настройки на операционната система до оригиналното им състояние.

Приложението идентифицира слабите настройки на операционната система за всички потребителски акаунти на вашия компютър. Може да поправите слабите настройки за други потребителски акаунти на компютъра само ако сте влезли в операционната система с администраторски акаунт.

> Ако не сте администратор на компютъра, може да игнорирате слабите настройки единствено за вашия собствен потребителски акаунт. Единствено администратор на компютъра може да игнорира слабите настройки на всички потребителски акаунти.

Можете ръчно да стартирате сканиране за слаби настройки или да изключите сканирането за слаби настройки.

Можете да управлявате отдалечено защитата на вашия компютър и да изпращате команда за коригиране на слаби настройки от My Kaspersky.

Как да намерите и коригирате слаби настройки в операционната система

За да откриете и поправите слаби настройки на операционната система:

1. Отворете основния прозорец на приложението.
2. Изберете раздел **Защита**.
3. В раздел **Защита** изберете **Сканиране за слаби настройки**.
4. Щракнете **Сканиране**.

   Извършва се сканиране на слаби настройки. След като сканирането завърши, ще видите резултатите от сканирането в раздела **Сканиране за слаби настройки**.
5. Щракнете върху **Преглед**, за да отидете в прозореца **Сканиране за слаби настройки**.
6. В прозореца **Сканиране за слаби настройки** изберете действие, което да предприемете за слабите настройки:

   - Открити слаби настройки. Направете някое от следните действия:
     - Щракнете върху бутона **Поправи всичко**, за да поправите всички слаби настройки.
     - Щракнете върху бутона **Поправи**, за да поправите слаба настройка.
     - Ако отворени приложения пречат на поправянето на слаба настройка, щракнете върху бутона **Изглед**, за да прегледате списъка с пречещи приложения.

       За да затворите приложения, които предотвратяват поправянето на настройката, направете някое от следните неща:

       - Щракнете върху бутона ✕ вдясно на името на пречещото приложения, за да го затворите нормално. Ако приложението открие незаписани промени, ще ви подкани да ги запишете.
       - Щракнете върху връзката **Форсирай затваряне**, за да затворите всички пречещи приложения, без да записвате данни.
     - В падащия списък до бутона **Поправи** изберете **Пропусни**, за да оставите слабата настройка непроменена.
     - В падащия списък до бутона **Поправи** изберете **Прочетете още**, за да видите информация за дадена слаба настройка на уеб сайта на Техническа поддръжка на Kaspersky.
   - Предишни поправени слаби настройки.
     - Щракнете върху бутона **Изпълни отмяна**, за да възстановите поправена настройка до оригиналното ѝ състояние.
     - В падащия списък до бутона **Изпълни отмяна** изберете **Прочетете още**, за да видите информация за дадена слаба настройка на уеб сайта на Техническа поддръжка на Kaspersky.
   - Игнорирани настройки. Щракнете върху връзката **Покажи всички** до съобщението **N игнорирани настройки**, за да отворите списъка със слаби настройки, които сте оставили непроменени, и щракнете

върху бутона **Поправи**.

Как да разрешите Сканиране за слаби настройки

За да забраните Сканиране за слаби настройки:

1. Отворете основния прозорец на приложението.
2. Щракнете върху в долната част на главния прозорец.
   Отваря се прозорецът **Настройки**.
3. Отидете в раздела **Настройки за производителност**.
4. Щракнете **Използване на ресурси на компютъра**.
5. Изчистете квадратчето **Сканиране за слаби настройки на операционната система**.

Приложението няма да сканира за слаби настройки на операционната система или да показва известявания за тях.

Наблюдение на мрежата

Предлага се само в Kaspersky Standard, Kaspersky Plus и Kaspersky Premium.

Наблюдение на мрежата ви позволява да преглеждате данните за мрежовата активност на вашия компютър в реално време, да блокирате мрежовата активност или да създавате правила за мрежа и пакети за приложения, инсталирани на вашия компютър.

За да отидете на настройките на мрежовия монитор:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Защита**.
3. В блока **Наблюдение на мрежата** щракнете върху бутона **Преглед**.

Отваря се прозорецът **Наблюдение на мрежата**.

В раздел **Мрежова активност** се показват всички активни в момента мрежови връзки. Той показва както входящите, така и изходящите връзки. Можете да използвате връзка **Блокирай цялата мрежова дейност** за блокиране на всички мрежови връзки.

В раздел **Отворени портове** се изброяват всички отворени мрежови портове. Можете също да използвате този раздел за създаване на мрежови и пакетни правила за приложения.

В раздел **Мрежов трафик** се показва обемът на входящия и изходящия мрежов трафик между Вашия компютър и други компютри във Вашата мрежа.

Раздел **Блокирани компютри** съдържа списък с IP адреси за отдалечени компютри, от които Защитата от мрежови атаки е открила опити за мрежова атака и е блокирала тяхната мрежова активност.

Умно домашно наблюдение

Този раздел съдържа информация как да използвате приложението Kaspersky, за да откриете кои устройства са свързани към Вашата кабелна Ethernet мрежа и Wi-Fi мрежата.

Относно компонента Умно домашно наблюдение

Предлага се само в Kaspersky Plus и Kaspersky Premium.

Хакерите биха могли потенциално да прехванат паролата ви или да влязат в домашната ви мрежа, за да се възползват от вашия интернет или да откраднат вашите данни. Приложението Kaspersky защитава Вашите кабелни Ethernet мрежи и Wi-Fi мрежи срещу неоторизирани свързвания.

Веднага след като потвърдите, че Вашата домашна мрежа е разпозната правилно, ние започваме да наблюдаваме свързаните към тази мрежа устройства и някои уязвимости, като например слаба парола за Wi-Fi или криптиране на рутера. Ако открием уязвимости или ново устройство в мрежата, което преди това не сте идентифицирали като известно устройство, ще Ви предупредим за това и ще Ви предложим препоръки, за да Ви позволим да предприемете стъпки за защита на Вашата домашна мрежа и устройствата, които я използват.

Известията за уязвимости на домашната мрежа са налични само в Kaspersky Premium. Известията за нови устройства, които се свързват с Вашата домашна мрежа, са налични в *Kaspersky Plus и Kaspersky Premium*.

Когато устройство се свързва към мрежата Ви, приложението Kaspersky показва съответно известие и Ви пита дали бихте желали да прегледате устройствата, свързани към тази мрежа:

- Ако сте съгласни, приложението Kaspersky показва списък с устройства, свързани към тази мрежа, и Ви уведомява, ако ново устройство се е свързало към нея.
- Ако откажете, приложението Kaspersky няма да Ви уведоми, когато връзка към тази мрежа се установи отново и няма да покаже списък с устройства, които са свързани.

Можете да деактивирате Smart Home Monitor. Когато изключвате компонента, приложението Kaspersky спира да Ви известява за връзките към Вашата мрежа.

За да научите други налични методи за безопасност за свързване към Wi-Fi мрежи, посетете уеб сайта за Техническа поддръжка.

Как да активирате или деактивирате Умно домашно наблюдение

За да активирате или деактивирате Умно домашно наблюдение:

1. Отворете основния прозорец на приложението.
2. Щракнете върху бутона в долната част на прозореца.

Отваря се прозорецът **Настройки**.

3. Изберете раздела **Настройки за защита**.

4. Изберете компонента Защитна стена.

5. Направете някое от следните действия:

   - За да включите Умно домашно наблюдение, изберете квадратчето за отметка **Показване на устройства, които са свързани с моите мрежи**.

   - За да изключите Умно домашно наблюдение, премахнете отметката от квадратчето **Показване на устройства, които са свързани с моите мрежи**.

Как да виждам устройствата в моята мрежа

Приложението Kaspersky показва следната информация за устройства, свързани с Вашата Wi-Fi мрежа или кабелна Ethernet мрежа:

- Име на устройство
- Производител на устройство
- Тип устройство (напр. компютър, мобилно устройство, маршрутизатор, игрова конзола или видео камера)
- Операционна система, инсталирана на устройството
- MAC адрес (уникален мрежови ИД на устройството)
- IP адрес на устройството
- Време, когато последно са откривани устройства с прекъсната връзка в мрежата
- Приложения на Kaspersky, инсталирани на Вашето устройство

За да видите устройства, които са свързани с вашата мрежа:

1. Отворете основния прозорец на приложението.
2. Направете някое от следните действия:
   - Отидете до блока **Защита** и щракнете върху бутон **Изглед** в раздел **Умно домашно наблюдение**.
   - В главния прозорец на приложението щракнете върху бутон **Изглед** в раздел **Умно домашно наблюдение**.
   - Щракнете върху връзка **<network name>**, която се показва в долната част на главния прозорец.

   Умно домашно наблюдение отваря се прозорец, показващ мрежата, към която е свързан Вашият компютър.
3. Изберете **Показване на информация за устройствата в тази мрежа на мобилните ми устройства** квадратчето за отметка, ако искате да прехвърлите информация за устройства, свързани към тази мрежа, към Вашите мобилни устройства.
4. За да видите устройствата, свързани към мрежата, щракнете **Да, покажи моите устройства**.

   Прозорецът **Умно домашно наблюдение** показва:
   - Устройства, които в момента са свързани към вашата мрежа.
   - Устройства, които са били свързани преди известно време към вашата мрежа.
   - Състояние на устройство в мрежата:
     - Свързаните устройства са оцветени в зелено;
     - Устройствата с прекъсната връзка са оцветени в сиво;
     - Новите устройства са обозначени като **нови**.

За да промените името на устройството:

1. Изберете съответното устройство от списъка с устройства в прозореца **Умно домашно наблюдение**.

   Отваря се прозорец, за да покаже информация за това устройство.
2. Въведете новото име на устройството в полето **Име на устройство**.

Как да промените типа устройство

1. Изберете съответното устройство от списъка с устройства в прозореца **Умно домашно наблюдение**.

   Отваря се прозорец, за да покаже информация за това устройство.

2. В прозореца **Тип устройство** щракнете върху връзката **Изберете тип**, за да отидете в прозореца **Тип устройство**.

3. В този прозорец изберете категория на устройството и въведете, например, **Домашни уреди** → **Хладилник**).

4. Щракнете **Запази**.

Как да отказвам достъп до мрежата на устройство

За да откажете достъп до мрежата на устройство:

1. Отворете основния прозорец на приложението.

2. Направете някое от следните действия:

   - Отидете до блока **Защита** и щракнете върху бутон **Изглед** в раздел **Умно домашно наблюдение**.

   - В главния прозорец на приложението щракнете върху бутон **Изглед** в раздел **Умно домашно наблюдение**.

   - Щракнете върху връзка **<network name>**, която се показва в долната част на главния прозорец.

3. В прозореца **Умно домашно наблюдение** изберете устройството, на което искате да прекъснете връзката.

   Отваря се прозорец с информация за това устройство, която включва информация за MAC адреса на устройството.

4. Запишете MAC адреса на устройството

5. Блокирайте MAC адреса на устройството в настройките на вашия браузър. Посетете уеб сайта на конкретния доставчик, за да видите Ръководството за потребителя за вашия маршрутизатор.

След като MAC адресът е блокиран, устройството няма да може да се свърже към вашата мрежа.

Как да изтривам от списъка мрежа без връзки

За да изтриете от списъка мрежа без връзки:

1. Отворете основния прозорец на приложението.

2. Направете някое от следните действия:

   - Отидете до блока **Защита** и щракнете върху бутон **Изглед** в раздел **Умно домашно наблюдение**.

- В главния прозорец на приложението щракнете върху бутон **Изглед** в раздел **Умно домашно наблюдение**.

3. Щракнете върху връзка **<network name>**, която се показва в долната част на главния прозорец.

   Това ви отвежда до прозорец **Умно домашно наблюдение**.

4. Щракнете върху стрелката в дясната част на списъка, за да го разширите и щракнете до мрежата, която искате да премахнете.

Мрежата ще бъде изтрита от списъка.

Как да изключа известията, когато устройства се свързват към моята мрежа

За да изключите известията, когато устройства се свързват към мрежата:

1. Отворете основния прозорец на приложението.

2. Направете някое от следните действия:

   - Отидете до блока **Защита** и щракнете върху бутон **Изглед** в раздел **Умно домашно наблюдение**.

   - В главния прозорец на приложението щракнете върху бутон **Изглед** в раздел **Умно домашно наблюдение**.

   - Щракнете върху връзка **<network name>**, която се показва в долната част на главния прозорец.

3. В прозореца **Умно домашно наблюдение** щракнете върху бутона ••• до мрежата и изберете елемента **Изключи известия**.

Приложението повече няма да Ви показва известия, ако към тази мрежа има свързани някакви устройства.

Също така може да изключите известията за избрана мрежа, когато приложението Kaspersky Ви показва известие, че дадено устройство се е свързало към тази мрежа. За да направите това щракнете върху връзката **Деактивиране на известията за тази мрежа** в прозореца за уведомявания.

Как да изпратите обратна връзка за Умно домашно наблюдение

За да изпратите обратна връзка до Kaspersky за работата на елемента за Умно домашно наблюдение:

1. Отворете основния прозорец на приложението.

2. Направете някое от следните действия:

   - Отидете до блока **Защита** и щракнете върху бутон **Изглед** в раздел **Умно домашно наблюдение**.

   - В главния прозорец на приложението щракнете върху бутон **Изглед** в раздел **Умно домашно наблюдение**.

   - Щракнете върху връзка **<network name>**, която се показва в долната част на главния прозорец.

3. В прозореца **Умно домашно наблюдение** щракнете върху бутона ••• и изберете елемента **Изпратете отзив**.

   Отваря се прозорецът **Помогнете ни да станем по-добри! Оставете отзив**.

4. Оценете компонента по 5-степенна скала, като изберете от 1 до 5 звезди.

5. Ако сте дали на компонента 3-5 звезди:

   a. Ако искате да добавите коментар към вашата обратна връзка, въведете го в полето **Детайли**.

   b. Изберете квадратчето за отметка **Съгласявам се да предоставя личните си данни (уникален идентификатор на моя компютър) за подобряване на софтуера и приемам условията на Политика за поверителност**.

6. Ако сте дали на компонента 1-2 звезди:

   a. Ако искате да уведомите Kaspersky за проблем с компонента Умно домашно наблюдение, изберете темата с най-близко значение от падащия списък **Тема**.

   Може да изберете една от следните опции от списъка:

   - **Неудобно за използване**. Изберете този елемент, ако изпитвате неудобства при използване на компонента Умно домашно наблюдение.
   - **Приложението отнема много време за търсене на устройства във мрежата**. Изберете този елемент, ако компонентът Умно домашно наблюдение работи твърде бавно.
   - **Приложението идентифицира неправилно устройствата във мрежата**. Изберете този елемент, ако приложението неправилно определя имената и/или типовете на устройствата, свързани към Wi-Fi мрежата или кабелната Ethernet мрежа.
   - **Твърде много известия за нови устройства във мрежата**. Изберете този елемент, ако приложението показва твърде много известия за нови устройства в Wi-Fi мрежата или кабелната Ethernet мрежа.
   - **Намалена производителност на компютъра**. Изберете този елемент, ако използването на компонента Умно домашно наблюдение забавя производителността на Вашия компютър.
   - **Невъзможно е да се конфигурира компонентът**. Изберете този елемент, ако изпитвате затруднения при конфигуриране на компонента Умно домашно наблюдение.
   - **Други**. Изберете този елемент, ако проблемът, който изпитвате, не се покрива от други елементи.

   b. Ако искате да добавите коментар към вашата обратна връзка, въведете го в полето **Детайли**.

   c. Изберете квадратчето за отметка **Съгласявам се да предоставя личните си данни (уникален идентификатор на моя компютър) за подобряване на софтуера и приемам условията на Политика за поверителност**.

7. Щракнете **Изпрати**.

Когато са изпратени тези данни, Kaspersky получава и обработва следната информация:

- Вашата обратна връзка, която съдържа оценка на работата на компонента, тема на проблема и коментари.
- Информация за и версия на операционната система.

- Информация за инсталираното приложение и неговата версия.

Kaspersky получава и обработва тази информация в шифрована форма, за да анализира грешките и да подобри работата на компонента Умно домашно наблюдение. Kaspersky не изисква от вас да предоставяте никаква лична информация, когато изпращате обратна връзка, и не събира такава информация. За детайли как се обработват личните данни, вижте Политика за поверителност на Kaspersky.

Премахване на вирус преди Kaspersky

Този раздел съдържа информация за възстановяване на операционната система, след като е била заразена със злонамерен софтуер.

Възстановяване на операционната система след заразяване

Ако подозирате, че операционната система е била повредена или променена поради дейност на злонамерен софтуер, използвайте *Съветника за отстраняване на неизправности на Microsoft Windows*, който изчиства системата от всякакви следи от злонамерени обекти. Kaspersky препоръчва да стартирате съветника, след като компютърът е бил дезинфектиран, за да се уверите, че всички заплахи и повреди, причинени от заразяванията, са коригирани.

Съветникът проверява дали има някакви промени в системата, които могат да включват блокиран достъп до мрежата, променени разширения на имена на файлове за известни формати, блокиран контролен панел и др. Има различни причини за тези различни видове повреди. Тези причини могат да включват дейност на злонамерен софтуер, неправилно конфигуриране на системата, системни грешки или неизправни приложения за оптимизиране на системата.

След като прегледът завърши, съветникът анализира информацията, за да оцени дали има повреда на системата, която изисква незабавно внимание. Базирано на прегледа, съветникът генерира списък с действия, които са необходими за отстраняване на повредата. Съветникът групира тези действия по категория според сериозността на откритите проблеми.

Отстраняване на неизправности на операционната система с помощта на съветника за отстраняване на неизправности на Microsoft Windows

За да стартирате Съветника за отстраняване на неизправности на Microsoft Windows:

1. Отворете основния прозорец на приложението.
2. Отидете в **Защита** → **Възстановяване след заразяване**.
3. Щракнете **Намиране на щета**.

   Отваря се прозорецът на съветника за отстраняване на неизправности на Microsoft Windows.

Съветникът се състои от серия страници (стъпки), които може да управлявате, като щраквате върху бутоните **Назад** и **Напред**. За да затворите съветника, след като приключи, щракнете върху бутона **Готово**. За да спрете Съветника във всеки етап, щракнете върху бутона **Отказ**.

Нека да прегледаме стъпките на Съветника в повече детайли.

Стартирай възстановяване на операционната система

a. Изберете една от двете опции за работата на Съветника:

- **Търсене на повреди, причинени от вредоносна програма**. Съветникът ще търси проблеми и възможни повреди.
- **Отмяна на промените**. Съветникът ще отмени корекциите, приложени на идентифицирани по-рано проблеми и повреди.

b. Щракнете **Напред**.

Търсене на проблеми

Ако сте избрали опцията **Търсене на повреди, причинени от вредоносна програма**, Съветникът търси проблеми и възможни повреди, които трябва да бъдат коригирани. Когато търсенето завърши, Съветникът преминава автоматично към следващата стъпка.

Изберете действия за коригиране на повредата

Всички повреди, открити на предишната стъпка, са групирани въз основа на типа опасност, която представляват. За всяка група повреди Kaspersky препоръчва набор от действия, за да отстраните повредата.

Има три групи:

- *Силно препоръчани действия* елиминират проблеми, които представляват сериозна заплаха за сигурността. Съветваме ви да отстраните всички повреди в тази група.
- *Препоръчани действия* целят да отстранят повреди, които може да представляват заплаха. Също така ви съветваме да отстраните повредата в тази група.
- *Допълнителни действия* коригират повреда на операционната система, която сега не е опасна, но може да представлява заплаха за сигурността на компютъра в бъдеще.

Разширете списъка на избраната група, за да видите повредата в групата.

За да накарате Съветника да коригира специфичен тип повреда, изберете квадратчето за отметка до описанието на повредата. По подразбиране Съветникът коригира повреда, която принадлежи към групите с препоръчани и силно препоръчани действия. Ако не желаете да се коригира специфичен тип повреда, махнете отметката от квадратчето до нея.

Силно се препоръчва да не премахвате отметката от квадратчетата, избрани по подразбиране, тъй като това ще остави компютъра ви уязвим на заплахи.

След като определите набора от действия за Съветника, които да извърши, щракнете върху бутона **Напред**.

Коригиране на повреда

Съветникът извършва действията, избрани по време на предишната стъпка. Коригирането на повредата може да отнеме известно време. След коригиране на повреда Съветникът автоматично преминава към следващата стъпка.

Завършване на съветника

Щракнете върху бутона **Готово**, за да излезете от съветника.

Аварийно възстановяване на операционната система

Kaspersky Rescue Disk е предназначено за аварийно възстановяване на операционната система. Може да използвате Kaspersky Rescue Disk за сканиране и дезинфектиране на заразени компютри, които не могат да бъдат дезинфектирани с други методи (например с антивирусни приложения).

Повече подробности за използването на Kaspersky Rescue Disk са налични на уеб сайта на Техническа поддръжка.

Как да възстановите изтрит или дезинфекциран файл

Архивните копия на изтрити или дезинфекцирани файлове се поставят в специална папка на вашия компютър, наречена *Карантина*. Резервни копия на файлове се съхраняват в специален формат, който не е опасен за вашия компютър. Можете да възстановите изтрит или дезинфекциран файл от резервното копие, съхранено в Карантина.

Препоръчваме ви да избягвате съхраняването на изтрити или дезинфектирани файлове, тъй като те могат да представляват заплаха за вашия компютър!

Приложението не дезинфекцира приложенията на Windows Store. Ако резултатите от сканирането показват, че такова приложение е опасно, то е изтрито от вашия компютър. Когато е изтрито приложение от Windows Store, приложението Kaspersky не създава негово резервно копие. За да възстановите такива обекти, трябва да използвате инструментите за възстановяване, включени в операционната система (за подробна информация вижте документацията за операционната система, инсталирана на вашия компютър) или да актуализирате приложенията чрез Windows Store.

За възстановяване на изтрит или дезинфектиран файл:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Защита**.
3. В горния десен ъгъл на прозореца на приложението щракнете върху бутона **Карантина**.

   Отваря се прозорецът **Карантина**.
4. В прозореца **Карантина**, който се отваря, изберете необходимия файл от списъка и щракнете върху бутона **Възстанови**.

Защита на имейл

Този раздел предоставя информация как да защитите имейла си от спам, вируси и други заплахи.

Конфигуриране на Защита за пощата

Приложението Kaspersky разрешава сканиране на имейл съобщения за опасни обекти с помощта на Защита за пощата. Защита за пощата стартира, когато операционната система е стартирана и остава постоянно в RAM паметта, сканирайки всички имейл съобщения, които са изпратени или получени по POP3, SMTP, IMAP и NNTP протоколи, както й чрез шифровани връзки (SSL) по POP3, SMTP и IMAP протоколи.

По подразбиране Защита за пощата сканира входящи и изходящи съобщения. Ако е необходимо, може да активирате само сканиране на входящи съобщения.

За да конфигурирате Защита за пощата:

1. Отворете основния прозорец на приложението.
2. Щракнете върху ⚙ в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.
3. Изберете раздела **Настройки за защита**.
4. В раздела **Настройки за защита** изберете прозореца Защита за пощата.

   Това ви отвежда до прозорец **Настройки на Защитата за пощата**.
5. Уверете се, че превключвателят в горната част на прозореца, който активира/деактивира Защита за пощата е активиран.
6. Изберете ниво на защита:

   - **Оптимално**. Когато е зададено това ниво на защита, Защита за пощата сканира входящите и изходящите съобщения и прикачени архиви и извършва евристичен анализ с ниво на детайл **Средно сканиране**.
   - **Ниско**. Ако изберете това ниво на защита, Защита за пощата сканира само входящи съобщения, без да сканира прикачени архиви.
   - **Изключително**. Когато е зададено това ниво на защита, Защита за пощата сканира входящите и изходящите съобщения и прикачени архиви и извършва евристичен анализ с ниво на детайл **Дълбоко сканиране**.
7. В раздела **Действие при откриване на заплаха** изберете действието, което искате Защита за пощата да извършва, когато бъде открит заразен обект (например дезинфектиране).

Ако не са открити заплахи в имейл съобщение или ако всички заразени обекти са успешно дезинфектирани, съобщението става достъпно за допълнителен достъп. Ако компонентът не успее да дезинфектира заразен обект, Защита за пощата го преименува или изтрива от съобщението и добавя известие към реда с тема на съобщението, че то е обработено от приложението Kaspersky. Преди да изтрие обект, приложението Kaspersky създава негово резервно копие и го поставя в Quarantine.

Когато надстройвате към по-нова версия на приложението, настройките на Защита за пощата, конфигурирани от потребителя, не се записват. Новата версия на приложението ще използва настройките по подразбиране на Защита за пощата.

Ако приложението Kaspersky открие паролата за архива в текстовото съобщение по време на сканиране, тя ще се използва за сканиране на съдържанието на този архив за злонамерен софтуер. Паролата не се записва. Архивът се разопакова преди сканиране. Ако приложението се срине при разопаковане на архива, може ръчно да изтриете файловете, които са разопаковани, в следния път: %systemroot%\temp. Файловете са с префикс PR.

Блокирай нежелан имейл (спам)

Ако получавате голямо количество нежелани съобщения (спам), ви препоръчваме да активирате компонента Защита от спам и да му зададете ниво на защита **Оптимално**.

За да активирате Защита от спам и зададете ниво на защита Оптимално:

1. Отворете основния прозорец на приложението.
2. Щракнете върху в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.
3. Изберете раздела **Настройки на поверителността**.
4. Изберете компонента Защита от спам.

   Прозорецът показва настройките на Защита от спам.
5. Активирайте Защита от спам с помощта на превключвателя.
6. В раздела **Ниво на защита** се уверете, че е зададено нивото на защита **Оптимално**.

Следните ограничения важат за Защита от спам:

- Компонентът Защита от спам може да анализира единствено съобщения, които са изтеглени изцяло от пощенски сървър, независимо от използвания протокол.
- Компонентът Защита от спам не проверява пощата, предадена с протокола MAPI.

Компонентът Защита от спам е деактивиран, когато надстройвате към по-скорошна версия на приложението. Може да активирате компонента ръчно.

В някои версии на приложението, за да активирате компонента Защита от спам, трябва да приемете условията на Декларацията относно обработката на данни за Защита от спам.

Участие в Kaspersky Security Network

Приложението Kaspersky използва защита в облака, за да направите защитата на Вашия компютър по-ефективна. Защитата в облака е въведена с помощта на инфраструктурата на Kaspersky Security Network, която използва данни, получени от потребители от целия свят.

Kaspersky Security Network (KSN) е базирана в облака база знания на Kaspersky с информация за репутацията на приложения и уеб сайтове. Използването на данни от Kaspersky Security Network гарантира по-бързи реакции на приложението Kaspersky на нови заплахи, подобрява работата на някои защитни компоненти и намалява вероятността за фалшиви тревоги.

Участието на потребители в Kaspersky Security Network позволява на Kaspersky да получава своевременно информация за типовете и източниците на нови заплахи, да разработва решения за неутрализирането им и да намали броя на фалшивите тревоги. Участието в Kaspersky Security Network ви дава достъп до статистика за репутацията на приложения и уеб сайтове.

Ако участвате в Kaspersky Security Network, Вие автоматично изпращате информация за конфигурацията на Вашата операционна система и времето за стартиране и завършване на процеси в приложението Kaspersky към Kaspersky.

Как да активирате или деактивирате участие в Kaspersky Security Network

Участието в Kaspersky Security Network е доброволно. Може да активирате или деактивирате използването на Kaspersky Security Network (KSN), когато инсталирате приложението Kaspersky и/или във всеки един момент след инсталиране на приложението.

За активиране или деактивиране на участие в Kaspersky Security Network:

1. Отворете основния прозорец на приложението.
2. Щракнете върху в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.
3. Отидете в **Настройки за защита** → **Kaspersky Security Network**.

   Отваря се прозорецът **Kaspersky Security Network**, който показва детайли на настройките за участие на Kaspersky Security Network и Kaspersky Security Network.
4. Активирайте или деактивирайте участие в Kaspersky Security Network с помощта на превключвателя в горната част на прозореца:

   - Ако искате да участвате в Kaspersky Security Network, задайте превключвателя на **Вкл**.

     Отваря се прозорец с текста на Декларацията на Kaspersky Security Network. Ако приемате условията на декларацията, щракнете върху **Съгласен/съгласна съм**.

   - Ако не искате да участвате в Kaspersky Security Network, задайте превключвателя на **Изкл**.

При някои версии на приложението Kaspersky, прозорецът **Kaspersky Security Network** показва **Декларация за Kaspersky Security Network** вместо информация за Kaspersky Security Network.

За да приемете Декларацията Kaspersky Security Network:

1. Щракнете върху бутона **Приемам** в раздела **Декларация за Kaspersky Security Network**.

   Отваря се Декларация на Kaspersky Security Network. Тази декларация позволява на експертите на Kaspersky веднага да получават информация за заплахите, засечени на вашия компютър, за приложенията, които са стартирани, и подписаните приложения, които са изтеглени, както и информация за операционната система, за да подобрят защитата ви.
2. Ако приемате условията на декларацията, щракнете върху бутона **Приемам**.

За да отхвърлите Декларацията на Kaspersky Security Network,

щракнете върху бутона **Отхвърлям** в раздела **Декларация за Kaspersky Security Network**.

Как да проверявате връзката към Kaspersky Security Network

Вашата връзка към Kaspersky Security Network може да се изгуби поради няколко причини:

- Вие не участвате в Kaspersky Security Network.
- Вашият компютър не е свързан с интернет.
- Сегашният статус на ключа не позволява свързване към Security Network. Например връзка към KSN може да не е налична поради следните причини:

- Приложението не е активирано.
- Лицензът или абонаментът е изтекъл.
- Идентифицирани са проблеми с лицензионния ключ (например ключът е добавен към списък с откази).

Текущото състояние на ключа се показва в My Kaspersky.

За да проверите връзката към Kaspersky Security Network:

1. Отворете основния прозорец на приложението.
2. Отидете в **Настройки за защита** → **Kaspersky Security Network**.

Прозорецът **Kaspersky Security Network** показва състоянието на вашата връзка към Kaspersky Security Network.

Защита с виртуализация на хардуер

В този раздел ще научите как да може да защитавате своя компютър с помощта на виртуализация на хардуер.

За защитата с виртуализация на хардуер

Когато приложението Kaspersky е инсталирано на 64-битов Microsoft Windows 8, Microsoft Windows 8.1 или Microsoft Windows 10, тя използва технология на софтуер за управление за допълнителна защита срещу сложен злонамерен софтуер, който може да прехване вашите лични данни с помощта на клипборд или фишинг.

Защитата с виртуализация на хардуер е активирана по подразбиране. Ако защитата е деактивирана ръчно, може да я активирате в прозореца с настройки на приложението.

На компютри с 64-битов Microsoft Windows 8, Microsoft Windows 8.1 или Microsoft Windows 10 защитата, осигурявана от виртуализацията с хардуер на Kaspersky (софтуер за управление) има следните ограничения:

- Тази функция не е налична, когато е стартиран софтуер за управление на трета страна, като например софтуера за управление, използван от софтуера за виртуализация VMware™. След като затворите софтуера за управление на трета страна, защитата срещу екранни снимки става отново налична.
- Функцията не е налична, ако CPU на вашия компютър не поддържа технологията за виртуализация с хардуер. За повече детайли дали вашият CPU поддържа виртуализация с хардуер вижте документацията, предоставена с вашия компютър или уеб сайта на производителя на CPU.
- Функцията не е налична, ако софтуер за управление на трета страна (като например софтуер за управление на VMware) работи, когато стартирате Защитен браузър.
- Функцията не е налична, ако виртуализацията с хардуер е деактивирана на вашия компютър. За детайли как да активирате виртуализацията с хардуер на вашия компютър вижте техническата документация на вашия компютър или посетете уеб сайта на производителя на вашия процесор.
- Функцията не е налична, ако Device Guard е активиран в операционната система Microsoft Windows 10.

- Функцията не е налична, ако Защита, базирана на виртуализация (VBS) е активирана в операционната система Microsoft Windows 10.

Как да активирате защита с виртуализация на хардуер

За да активирате защита с виртуализация на хардуер:

1. Отворете основния прозорец на приложението.
2. Щракнете върху в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.
3. Отидете на **Настройки за защита** → **Настройки на поверителността** → **Защитено въвеждане на данни**.
4. Поставете отметка в квадратчето до **Използвайте виртуализация на хардуера, ако има налична**. Това квадратче за отметка се показва, когато приложението е инсталирано на 64-битова версия на Windows 8, Windows 8.1 и Windows 10.
5. Изберете квадратчето за отметка **Използване на разширени функции на виртуализация на хардуера**, ако искате да включите виртуализация на хардуера, когато операционната система стартира.

Ако виртуализация на хардуера е деактивирана на вашия компютър, защитата с виртуализация на хардуер ще бъде деактивирана.

Защита с помощта на Интерфейс за сканиране срещу злонамерен софтуера (AMSI)

Този раздел Ви информира, че приложения на трети страни като Microsoft Office могат да изпращат скриптове към приложението Kaspersky, за да бъдат сканирани с интерфейса за сканиране срещу злонамерен софтуер (AMSI), и описва как да се изключи защитата с помощта на AMSI в приложението Kaspersky.

За защитата с помощта на интерфейс за сканиране срещу злонамерен софтуер

Интерфейсът за сканиране срещу злонамерен софтуер (AMSI) позволява на приложение на трета страна, което поддържа AMSI, да изпраща обекти (например скриптове на PowerShell) към приложението Kaspersky за допълнително сканиране и да получава резултатите от сканирането за тези обекти. Например приложения на Microsoft Office могат да бъдат такива приложения на трети страни. За повече информация за интерфейса AMSI вижте *Документация на Microsoft*.

Интерфейсът за сканиране срещу злонамерен софтуер позволява да се откриват единствено заплахи и да се уведомява приложение на трета страна за откритата заплаха. След получаване на известие за заплаха приложението на трета страна предотвратява злонамерени действия (например спиране).

Приложението Kaspersky може да отхвърли заявка от приложение на трета страна, ако например това приложение надвиши максималния брой разрешени заявки за даден период. В този случай приложението Kaspersky показва известие за отхвърлената заявка. Ако получите такова известие, не трябва да извършвате никакво действие.

Защитата с помощта на Интерфейс за сканиране срещу зловреден софтуер е налична в операционните системи Windows 10 Home / Pro / Education / Enterprise и Windows 11 Home / Pro / Enterprise.

Как да включите защитата с помощта на интерфейс за сканиране срещу злонамерен софтуер

За да включите защитата с помощта на интерфейс за сканиране срещу злонамерен софтуер:

1. Отворете основния прозорец на приложението.
2. Щракнете върху в долната част на главния прозорец.
   Отваря се прозорецът **Настройки**.
3. Отидете в **Настройки за защита** → **AMSI защита**.
4. В раздела **Скенер за скриптове** изберете квадратчето за отметка **Сканиране на скритове чрез Antimalware Scan Interface (AMSI)**.

Как да изключите скрипт от сканиране с помощта на интерфейс за сканиране срещу злонамерен софтуер

За да изключите скрипт от сканиране с помощта на интерфейс за сканиране срещу злонамерен софтуер:

1. Отворете основния прозорец на приложението.
2. Щракнете върху в долната част на главния прозорец.
   Отваря се прозорецът **Настройки**.
3. Отидете в **Настройки за защита** → **AMSI защита**.
4. В раздела **Скенер за скриптове** изберете квадратчето за отметка **Сканиране на скритове чрез Antimalware Scan Interface (AMSI)**.
5. Щракнете върху връзката **Управление на изключения**, за да отидете в прозореца **Изключения**.
6. В прозореца **Изключения** щракнете върху бутона **Добави**.
   Отваря се прозорецът **Добавяне на ново изключение**.
7. В полето **Файл или папка** посочете папката със скрипта.
8. В полето **Обект** посочете името на скрипта.

Също така може да добавите няколко файла от един и същ тип към изключенията с помощта на маска.

9. В раздела **Защитни компоненти** изберете квадратчето за отметка до компонента Защита на файлове.
10. Изберете състоянието **Активен**.

Посоченият обект няма да бъде сканиран с помощта на Antimalware Scan Interface.

Отдалечено управление на защитата на компютъра

Ако Вашият компютър има инсталирано Kaspersky и е свързан към My Kaspersky, може да управлявате защитата на този компютър отдалечено.

За да управлявате отдалечено защитата на компютъра, влезте във вашия акаунт в My Kaspersky и отидете в раздела **Устройства**.

В раздела **Устройства** може да:

- Преглеждате списък с проблеми в защитата на компютъра и да ги коригирате отдалечено
- Сканирате компютъра за вируси и други заплахи
- Актуализирай базата данни и модулите на приложенията
- Конфигуриране на компоненти на Kaspersky

Ако е стартирано сканиране на компютъра от My Kaspersky, Kaspersky обработва обекти, които са открити автоматично без ваше участие. При откриване на вирус или друга заплаха, приложението Kaspersky се опитва да извърши дезинфекция, без да рестартира компютъра. Ако е невъзможна дезинфекция без рестартиране на компютъра, списъкът с проблемите в защитата на компютъра в My Kaspersky показва съобщение, че компютърът се нуждае от рестартиране, за да извърши дезинфекцията.

Ако списъкът с открити обекти в My Kaspersky включва над 10 елемента, те се групират. В такъв случай откритите обекти могат да бъдат обработени чрез My Kaspersky единствено заедно, без възможността да се проучи всеки обект отделно. За да се видят отделно обекти, съветваме ви да използвате интерфейса на приложението, инсталирано на вашия компютър.

Как да продължите към отдалечено управление на защитата на компютъра

За да продължите към отдалечено управление на защитата на компютъра:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Профил**.
3. В блока **Вход в My Kaspersky** щракнете върху бутона **Влизане**.
4. В прозореца, който се отваря, направете една от следните операции:
   - Ако имате акаунт, въведете своя имейл адрес и парола и се свържете с My Kaspersky.

- Ако нямате акаунт, въведете имейл адреса си в текстовото поле и щракнете върху **Създай**. На посочения имейл адрес е изпратено съобщение с връзка за създаване на парола.

След успешна връзка разделът **Профил** показва информация за връзката ви с акаунта. Вече можете да управлявате защитата на този компютър от разстояние от вашия акаунт в My Kaspersky.

За да научите повече за дистанционното управление на защитата на устройствата, вижте Помощ за My Kaspersky.

Производителност

Ако вашето устройство се забави или затвори, не сте сами. Понякога приложенията отказват да се отворят или браузърът не може да отговори в решаващ момент. Има множество причини, поради които може да се случи. Осигурете стабилна работа на вашето устройство за много години напред.

Бързо стартиране

Началното стартиране на компютъра ви отнема ли твърде много време? Това обикновено се случва, когато много приложения се стартират при стартиране на операционната система. Ще ви кажем кои приложения забавят вашия компютър при стартиране и ще ви помогнем да деактивирате автоматичното стартиране на тези приложения.

За да ускорите стартирането на компютъра:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Производителност**.
3. Щракнете върху бутона **Показване на приложения** в раздел **Бързо стартиране**.

   Прозорецът **Ускоряване на стартирането на компютъра** се отваря, който показва списък с приложения, които се отварят при стартиране.

   Колоната **Ефект върху стартирането** показва информация за влиянието, което всяко приложение оказва върху стартирането на компютъра. Тази информация се взема от операционната система и зависи от това колко компютърни ресурси консумира приложението (натоварване на процесора и RAM).
4. Изберете приложение от списъка и сменете превключвателя **Автоматично стартиране** на позиция **Изкл**.

Приложението вече няма да се стартира при стартиране.

Ускоряване на компютъра

С течение на времето в операционната система се натрупват маловажни файлове, което забавя производителността на вашия компютър. Голям брой файлове, които не се използват, и проблемите със системния регистър на Windows допринасят за това. Приложението Kaspersky ще Ви предупреди, ако количеството на тези данни стане прекомерно, и ще Ви бъде дадена възможност да решите кои данни да изтриете.

За да разчистите операционната си система:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Производителност**.
3. В блока **Ускоряване на компютъра** щракнете върху бутона **Търсене** (или **Преглед**, ако търсенето вече е извършено).

   Kaspersky изпълнява търсене и генерира отчет със следното съдържание:

   - **Неизползвани системни файлове**. Щракнете върху бутон **Преглед**, за да видите подробен отчет на файловете на операционната система, които не се използват. Щракнете върху бутона **Изчистване**, за да изтриете тези файлове.

- **Проблеми със системния регистър на Windows**. Щракнете върху бутон **Преглед**, за да видите подробен отчет на проблемите в системния регистър на Windows, които може да изтриете, без да рискувате повреждане на операционната система. Щракнете върху бутона **Поправи**, за да поправите установените проблеми.

Премахването на неизползвани файлове и отстраняването на открити проблеми ще ускори вашия компютър.

За да деактивирате автоматичното търсене на начини за ускоряване на Вашия компютър:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Производителност**.
3. В блока **Ускоряване на компютъра**, щракнете .
4. Изчистете квадратчето **Автоматично търсете начини за ускоряване на Вашия компютър**.

Актуализация на приложения

Този раздел предоставя информация как може да използвате приложението Kaspersky, за да актуализирате инсталирани приложения.

Предлага се само в Kaspersky Standard, Kaspersky Plus и Kaspersky Premium.

За актуализацията на приложения

Ако не сте актуализирали приложенията на своя компютър дълго време, те могат да съдържат уязвимости. Нарушителите могат да използват тези уязвимости, за да повредят вашия компютър или данните.

Актуализацията на инсталирани приложения подобрява сигурността на вашия компютър. Като използвате приложението Kaspersky, може да потърсите актуализации на инсталирани приложения и да изтегляте и инсталирате най-новите актуализации.

Приложението Kaspersky разделя актуализациите на приложения на два типа:

- *Важни* – актуализации, които коригират уязвимости в инсталираните приложения и подобряват сигурността на вашия компютър.
- *Препоръчителни* – актуализации, които подобряват функционалността и/или правят промени на инсталираните приложения.

Приложението Kaspersky редовно търси актуализации. Когато приложението Kaspersky открие нова актуализация за дадено приложение, инсталирано на Вашия компютър, приложението Kaspersky показва изскачащо съобщение в областта за уведомявания. Информация за достъпността, количеството и типа налични актуализации се показва в Центъра за уведомявания. Чрез Центъра за уведомявания може да преглеждате, изтегляте и инсталирате наличните актуализации.

Освен това може ръчно да стартирате търсенето на актуализации на приложенията.

По подразбиране приложението Kaspersky автоматично изтегля и инсталира всички актуализации за известните приложения, ако не изискват приемането на нови Лицензионни споразумения.

В Windows 8 и по-новите версии приложението Kaspersky поставя на пауза автоматичните изтегляния на актуализациите на приложенията, когато се използва Интернет връзка с измерено потребление. Изтеглянето на актуализации се възобновява, след като се възстанови неограничената връзка. Ако сте стартирали ръчно актуализацията, приложението Kaspersky ще я изтегли, независимо дали използвате ограничена връзка или не.

Може да са необходими администраторски права на компютъра, за да актуализирате определени приложения.

Приложения, които не искате да се актуализират, или за които не искате да инсталирате отделни актуализации, са поставени от приложението Kaspersky в списъка с изключения. Може да преглеждате и редактирате списъка с изключения.

Преди да стартирате първото търсене на актуализации на приложенията, приложението Kaspersky може да изиска актуализация на базите данни и модулите на приложението.

Търсене на актуализации на приложенията

За да стартирате търсенето на актуализации на приложенията:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Производителност**.
3. В блока **Актуализация на приложения** щракнете върху бутона **Търсене на актуализации**.

Това стартира търсенето на актуализации на приложенията.

Как да промените настройките за актуализация на приложения

За да промените настройките на актуализацията на приложения:

1. Отворете основния прозорец на приложението.
2. Щракнете върху в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.
3. Изберете раздела **Настройки за производителност**.
4. Щракнете **Актуализация на приложения**.

   Отваря се прозорецът **Настройки за актуализацията на приложения**.
5. Ако не искате приложението Kaspersky автоматично да изтегля и инсталира актуализации на приложението, които не изискват приемането на ново лицензионно споразумение, изчистете квадратчето за отметка **Автоматично изтегляне и инсталиране на актуализации, ако не трябва да приемате нови лицензионни споразумения**.

   Това квадратче за отметка е избрано по подразбиране.

6. В раздела **Търсене на актуализации на приложенията** изберете кои актуализации на приложения ще бъдат изтегляни и инсталирани от приложението Kaspersky:

   - Изберете **Важни актуализации, които подобряват сигурността на компютъра**, ако искате приложението Kaspersky да инсталира само важни актуализации, които коригират уязвимости в софтуера и подобряват сигурността на Вашия компютър.

   - Изберете **Всички актуализации за известни приложения**, ако искате приложението Kaspersky да инсталира всички софтуерни актуализации.

Как да конфигурирате режим на търсене на актуализации

За да конфигурирате режима на търсене на актуализации за инсталирани приложения:

1. Отворете основния прозорец на приложението.

2. Щракнете върху в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.

3. Изберете раздела **Настройки за производителност**.

4. Щракнете **Актуализация на приложения**.

   Отваря се прозорецът **Настройки за актуализацията на приложения**.

5. В блока **Актуализация** поставете отметка в квадратчето **Активиране на търсенето на актуализации на приложението**.

6. Щракнете върху връзката **Задаване на режим за търсене на актуализации**, за да отворите прозореца **Режим на търсене на актуализации**.

7. В падащия списък **Търсене на актуализации** изберете една от следните опции:

   - **Автоматично**. Ако изберете тази опция, приложението Kaspersky ще стартира търсене на актуализации на приложенията веднъж на 24 часа според вътрешните настройки на приложението.

   - **Всеки ден** / **Ежеседмично** / **Ежемесечно**. Ако изберете една от тези опции, приложението Kaspersky ще търси актуализации, базирано на определения от Вас график, в точното време. Когато е избрана една от тези опции, квадратчето за отметка **Отлагане на изпълнение след стартиране на приложението за N минути** е налично.

8. Изберете квадратчето за отметка **Търсете актуализации на следващия ден, ако компютърът е изключен**, за да стартирате търсене, когато компютърът се включи, след като планираното търсене е било пропуснато. Ако квадратчето за отметка не е избрано, приложението ще стартира търсенето на актуализации само в планирания час, докато компютърът е включен.

9. За да запишете настройките, щракнете върху бутона **Запази**.

Преглед на списъка с актуализации на приложенията

Приложението Kaspersky редовно търси актуализации на приложения, инсталирани на Вашия компютър. Информация за броя и типовете налични актуализации за приложенията може да бъде видяна в Центъра за уведомявания.

За да прегледате списъка, генериран въз основа на резултатите от търсенето на актуализации на приложенията:

1. Отворете основния прозорец на приложението.
2. Щракнете върху бутона **Детайли** в горната част на прозореца.

   Отваря се прозорецът **Център за уведомяване**.
3. В раздела **Статус** щракнете върху бутона **Показвай** в реда със съобщението за наличните актуализации на приложенията.

   Отваря се прозорецът **Актуализация на приложения** със списък на наличните актуализации на приложенията.
4. За да актуализирате всички приложения, които се появяват в списъка, щракнете върху бутона **Актуализирай всички** (не е налично във всички региони).
5. За да актуализирате селективно специфични приложения, извършете едно от следните действия:

   - Щракнете върху бутона **Актуализация** в реда, който съдържа приложението, което искате да актуализирате.

     Съветваме ви да прочетете лицензионното споразумение, преди да актуализирате приложението. Лицензионните споразумения са налични в падащия списък **Лицензионни споразумения**. По подразбиране езикът на лицензионното споразумение отговаря на езика на интерфейса на приложението. Ако лицензионното споразумение не е налично на езика на интерфейса на приложението, текстът на EULA се предоставя на езика на интерфейса на приложението Kaspersky. Във всички други случаи текстът на лицензионното споразумение е предоставен на английски език или първия наличен език, ако текстът на английски език не е наличен.

   - Щракнете върху бутона  , за да отворите менюто, и изберете **Не актуализирай това приложение**, ако искате приложението Kaspersky да спре да Ви уведомява за наличните актуализации за избраните приложения.

     Избраното приложение е преместено в списъка с изключения. Приложението Kaspersky спира да показва известия за нови актуализации, пуснати за това приложение.

   - Щракнете върху бутона  , за да отворите менюто, и изберете **Пропусни тази актуализация**, ако искате приложението Kaspersky да спре да Ви уведомява за избраната актуализация.

     Избраната актуализация на приложение е преместена в списъка с изключения. Приложението Kaspersky показва известие за нова актуализация, пусната за това приложение.

   - Щракнете върху бутона  , за да отворите менюто, и изберете **Отвори уеб сайта на доставчика**, ако искате ръчно да изтеглите и инсталирате приложението за избраното приложение.

     Браузърът по подразбиране на операционната система отваря уеб сайта на доставчика на софтуера. Може да видите актуализацията на уеб сайта и да я изтеглите ръчно.

Интерфейсът на прозореца, актуализацията на софтуера и изгледът на лицензионното споразумение могат да се различават в зависимост от езика на локализация на приложението Kaspersky.

Премахване на актуализация или приложение от списъка с изключения

Когато преглеждате списъка с актуализации на приложенията, може да пропуснете известията за индивидуалните актуализации или известията за всички актуализации за специфични приложения. Приложението Kaspersky добавя тези актуализации и приложения към списъка с изключения.

За да премахнете актуализация или приложение от списъка с изключения:

1. Отворете основния прозорец на приложението.
2. Щракнете върху в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.
3. Изберете раздела **Настройки за производителност**.
4. Щракнете **Актуализация на приложения**.

   Отваря се прозорецът **Настройки за актуализацията на приложения**.
5. Щракнете върху връзката **Изключения**, за да отворите прозореца **Изключения**.

   Списъкът с **Изключения** съдържа приложенията и актуализациите, за които сте посочили, че не са необходими актуализации, и индивидуални актуализации на приложения, които не сте инсталирали.
6. Изберете актуализацията или приложението в списъка и щракнете върху бутона **Изтрий**.

При следващото търсене на актуализации Приложението Kaspersky ще Ви уведоми за наличието на актуализации на приложенията, които сте премахнали от списъка с изключения.

Дубликати

Вашият компютър може да съхранява файлове с идентични имена и идентично съдържание. Тези дублирани файлове задръстват паметта, заемат място на твърдия диск и карат компютъра ви да работи по-бавно. Можете да намерите дублирани файлове и да изтриете допълнителни копия с помощта на функцията Дублирани файлове.

За да премахнете дублирани файлове:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Производителност**.
3. Изберете областта за търсене в падащия списък в раздел **Дубликати**.
4. Щракнете **Търсене**.
5. В прозореца с резултати от търсенето изберете файловете и щракнете върху **Изтрий**.

Дублираните файлове ще бъдат премахнати от вашия компютър, а оригиналните данни ще бъдат запазени.

Големи файлове

Опитвате се да запазите данни на компютъра си, но изведнъж установявате, че твърдият ви диск е почти пълен. Звучи познато? В този случай може да поискате да намерите и изтриете големи файлове, които не са ви необходими, и ние ще ви помогнем с това.

За да намерите големи файлове на вашия компютър и да ги премахнете:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Производителност**.
3. В падащия списък **Файлове, по-големи от** в раздел **Големи файлове**, посочете размера на файловете, които искате да намерите, например **> 1 GB**.
4. Изберете конкретна папка за вашето търсене или оставете стойността по подразбиране **Папки на потребител** непроменен.
5. Щракнете **Търсене**.

   Търсенето ще бъде извършено и ще се отвори прозореца **Големи файлове**. Той ще покаже списък с намерени големи файлове. Можете да сортирате файловете по тип файл. За да направите това, изберете файлова категория, например **Изображения**.
6. Извършете следните действия:

   - Поставете отметка в квадратчето **Избери всички**, ако искате да премахнете всички файлове, и щракнете върху бутона **Изтрий**.
   - В противен случай поставете отметка в квадратчетата до конкретни файлове и щракнете върху бутона **Изтрий**.

Избраните файлове ще бъдат премахнати от вашия компютър.

Неизползвани приложения

Няколко фактора влияят върху производителността на вашия компютър и броят на инсталираните приложения е един от тях. Колкото повече приложения сте инсталирали, толкова по-бавно работи компютърът ви. Това се дължи на факта, че някои приложения, включително тези, инсталирани без ваше знание, могат да се стартират автоматично, като консумират ресурсите на процесора и RAM паметта, както и като извършват ненужни и понякога дори злонамерени действия.

Приложението Kaspersky ще Ви помогне да намерите и премахнете тези приложения.

За да премахнете приложения, които не използвате:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Производителност**.
3. Щракнете върху бутона **Търсене** в раздел **Неизползвани приложения**.

   След завършване на търсенето приложението Kaspersky ще покаже списък с неизползвани приложения. От този списък можете да изберете конкретни приложения, които да премахнете.

4. За да премахнете приложение, щракнете върху бутона **Премахни** до приложението, което искате да премахнете.

Приложението ще бъде премахнато от вашия компютър.

Монитор за изправността на твърдия диск

Този раздел предоставя информация как може да използвате приложението Kaspersky, за да проверите изправността на твърдия диск на Вашия компютър или свързан външен твърд диск.

За Монитор за изправността на твърдия диск

Предлага се само в Kaspersky Plus и Kaspersky Premium.

Ако вашият твърд диск се повреди изненадващо, това може да причини загуба на данни, съхранявани на него. Приложението Kaspersky Ви позволява да наблюдавате изправността на Вашия твърд диск с помощта на S.M.A.R.T. (Технология за самоконтрол, анализ и отчитане). Тази технология се основава на непрекъснатия мониторинг на основните характеристики на производителността на твърдия диск. С приложението Kaspersky можете бързо да разберете за влошаване на състоянието на твърдия диск и копирането на данни от повредени дискове на други носители.

Ако Мониторът за изправността на твърдия диск е включен, приложението Kaspersky непрекъснато ще наблюдава изправността на Вашите твърди дискове и ще Ви уведоми, когато състоянието им се влоши. Можете да преглеждате изправността на вътрешните и външните твърди дискове. Известия за влошаването на състоянието на твърдия диск се показват в областта за уведомяване на лентата на задачите. Подробни отчети за резултатите от мониторинга на твърдия диск се показват в раздела **Отчети**.

Ако състоянието на Вашия твърд диск се влоши и вече не е безопасно да съхранявате данни на диска, приложението Kaspersky Ви предлага да копирате данни от този диск на друг носител, за да избегнете загуба на данни. Можете да копирате данни от повреден твърд диск на всякакъв наличен добър носител.

Можете да изключите монитора за изправността на твърдия диск. След като изключите Монитора за изправността на твърдия диск, приложението Kaspersky вече не Ви уведомява за смяната на състоянието на Вашите твърди дискове и няма да Ви предлага да копирате данни от повредени дискове на други носители.

Как да включвате или изключвате Монитор за изправността на твърдия диск

За да включите или изключите Монитор за изправността на твърдия диск:

1. Отворете основния прозорец на приложението.
2. Щракнете върху ⚙ в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.
3. Отидете в **Настройки за производителност** → **Използване на ресурси на компютъра**.
4. Направете някое от следните действия:

- За да включите Монитор за изправността на твърдия диск, изберете квадратчето за отметка **Извършване на сканиране за изправността на твърдия диск**.

- За да изключите Монитор за изправността на твърдия диск, премахнете отметката от квадратчето **Извършване на сканиране за изправността на твърдия диск**.

Как да проверявате изправността на твърдия диск

Приложението Kaspersky непрекъснато наблюдава изправността на външните и вътрешните твърди дискове на Вашия компютър. Мониторът работи във фонов режим. Ако състоянието на вашия твърд диск се влоши и вече не е безопасно да се съхраняват данни на него, приложението ви уведомява и ви предлага да копирате данни на други носители.

Прозорецът **Монитор за изправността на твърдия диск** показва следната информация за твърдия диск:

- Състояние на диска.

- Температура на диска.

Твърдият диск може да бъде в едно от следните състояние:

- *Добро* – състояние, съответстващо на нов твърд диск.

- *Нормално* – има минимални проблеми с твърдия диск.

- *Лошо* – състоянието на твърдия диск е критично, възможна е загуба на данни.

Диапазонът на температурата на твърдия диск може да бъде един от следните:

- *Добър* – твърдият диск не прегрява.

- *Нормален* – температурата на твърдия диск е леко повишена.

- *Лош* – твърдият диск прегрява.

Диаграмата **Хронология на изправността на диска** показва информация за промяна в изправността на твърдия диск за посочения период. Максималния показван период е 1 година.

Освен това приложението Kaspersky показва следната статистика за Вашите твърди дискове:

- *Общо часове във включено състояние* – общо време на работа на твърдия диск, в часове.

- *Общ брой цикли включване/изключване* – общият брой включени състояния на твърдия диск.

Докладът за **S.M.A.R.T. атрибутите** на <drive name> показва информация за стойностите на S.M.A.R.T. Параметъра на твърдия диск, сортирани по сериозност. Наборът параметри може да варира според производителя и модела на твърдия диск.

За да проверите текущото състояние на твърдите дискове на вашите компютър:

1. Отворете основния прозорец на приложението.

2. Отидете в раздела **Производителност**.

3. Под **Погрижете се за вашия твърд диск и данни**:

   - Ако искате да видите графиката, щракнете върху бутона **Хронология**.
   - Ако искате да видите отчета, щракнете върху бутона **Детайли**.

Това ви отвежда до прозореца, където можете да разгледате подробности за състоянието на вашия твърд диск.

Как да копирате данни от повреден твърд диск

Ако състоянието на един или повече твърди дискове на вашия компютър се влоши и вече не е безопасно да съхранявате данни на дисковете, приложението Kaspersky Ви уведомява и Ви предлага да копирате данните от тези дискове на други носители.

За да копирате вашите данни от повреден твърд диск на изправен твърд диск:

1. Направете някое от следните действия:

   - Ако получите известие, че състоянието на твърдия диск се влошава, щракнете върху бутона **Детайли** в прозореца за уведомявания.

     Отваря се прозорецът **Монитор за изправността на твърдия диск**.

   - Щракнете върху бутона **Копиране на данни** в прозореца **Hard Drive Health Monitor**.

2. В прозореца **Копиране на данните**, който се отваря, щракнете върху бутона **Стартиране на архивиране**.

   Отваря се прозорецът **Избор на хранилище**.

3. В прозореца **Избор на хранилище** изберете изправен твърд диск, за да копирате данни от повредения диск.

4. Щракнете **Напред**.

   Отваря се прозорецът **Избиране на файлове и папки за копиране**.

5. Направете някое от следните действия:

   - Плъзнете и пуснете файловете от Windows Explorer в осветената област на прозореца **Избиране на файлове и папки за копиране**.
   - Щракнете върху връзката **изберете ги от списъка**.

     В прозореца в Explorer, който се отваря, може да избирате файлове и папки, които да копирате на изправния твърд диск.

6. След добавяне на файловете и папките, които искате да копирате в списъка, щракнете върху бутона **Напред**.

   Отваря се прозорецът **Създаване на папка за копиране на данни**.

7. Направете някое от следните действия:

   - Щракнете върху бутона **Напред**, за да създадете нова папка на избрания изправен твърд диск и да копирате файлове и папки от повредения диск на него.

- Щракнете върху бутона **Смени**, за да изберете съществуваща папка на изправния диск и да копирате файлове и папки от повредения диск в нея.

8. Направете някое от следните действия:

   - Ако избраният изправен твърд диск има достатъчно дисково пространство, за да се копират избраните файлове и папки, щракнете върху бутона **Напред**, за да започнете копирането.

   - Ако избраният твърд диск няма достатъчно дисково пространство за копиране на избраните файлове и папки, щракнете върху бутона **Назад**, за да изберете друг изправен диск, и опитайте отново.

9. Когато копирането приключи, направете някое от следните неща:

   - За да отворите папката с файловете, копирани от повредения твърд диск, щракнете върху бутона **Отвори папка**.

   - За да затворите прозореца, щракнете върху бутона **Готово**.

За да копирате вашите данни от повреден твърд диск в онлайн хранилището в Dropbox:

1. Направете някое от следните действия:

   - Ако получите известие, че състоянието на твърдия диск се влошава, щракнете върху бутона **Детайли** в прозореца за уведомявания.

     Отваря се прозорецът **Монитор за изправността на твърдия диск**.

   - Щракнете върху бутона **Копиране на данни** в прозореца **Hard Drive Health Monitor**.

2. В прозореца **Копиране на данните**, който се отваря, щракнете върху бутона **Стартиране на архивиране**.

   Отваря се прозорецът **Избор на хранилище**.

3. В прозореца **Избор на хранилище** изберете вашето онлайн хранилище в Dropbox.

   Също така може да извършите едно от следните действия:

   - Ако хранилището не е активно, щракнете върху бутона **Активирай**.

   - За да изключите хранилището, щракнете върху връзката **Премахване на хранилището**.

4. Щракнете **Напред**.

   Отваря се прозорецът **Копиране на данните**.

5. Направете някое от следните действия:

   - Плъзнете и пуснете файловете от Windows Explorer в осветената област на прозореца **Копиране на данните**.

   - Щракнете върху връзката **изберете ги от списъка**.

     В прозореца в Explorer, който се отваря, може да избирате файлове и папки, които да копирате в онлайн хранилището в Dropbox.

6. След добавяне на файловете и папките, които искате да копирате в списъка, щракнете върху бутона **Стартиране на архивиране**.

   Копирането на данни започва.

7. Когато копирането приключи, направете някое от следните неща:

   - Ако архивирането на данни приключи успешно, щракнете върху бутона **Готово**, за да затворите прозореца.
   - Ако приложението ви уведоми, че архивирането е неуспешно, освободете пространство в онлайн хранилището и опитайте отново.

Няма ограничения за копиране на данни, които се съхраняват в облачна услуга за съхранение OneDrive.

Ограничения на монитора за изправността на твърдия диск

В някои случаи приложението Kaspersky не може да определи състоянието на твърдия диск поради следните ограничения:

- Твърдият диск не поддържа технологията S.M.A.R.T.
- Функцията S.M.A.R.T. е изключена на твърдия диск.
- Приложението Kaspersky не поддържа:
  - Тип свързан твърд диск
  - Тип USB контролер на твърдия диск
- Твърдият диск е деактивиран.
- Твърдият диск принадлежи към виртуална машина, например, VMWare. Информацията за здравето на такива твърди дискове или не се показва, или се показва неправилно.

Архивиране и възстановяване

Този раздел предоставя информация за архивирането на данни.

За Архивиране и възстановяване

Предлага се само в Kaspersky Plus и Kaspersky Premium.

Архивиране и възстановяване е необходимо за защита на вашите данни от загуба, когато вашият компютър е неизправен или бъде откраднат, или когато се изтрие случайно или бъде повреден от хакери.

За да архивирате данни, създайте и стартирайте задача за архивиране. Задачата може да се стартира автоматично според графика или ръчно. Приложението ви позволява също така да преглеждате информация за завършени задача за архивиране.

Препоръчва се да запишете резервни копия на данни на сменяеми устройства или в онлайн хранилище.

Приложението Kaspersky не може да създаде пълно копие на диск, докато е активна операционна система Microsoft Windows на диска.

Приложението Kaspersky Ви позволява да използвате следните типове хранилища за създаване на резервни копия:

- Локален диск;
- Сменяемо устройство (напр., външен твърд диск);
- Мрежови диск;
- Онлайн хранилище.

Създаване на задачи, базирано на правата за достъп на потребителя

Задачи за архивиране се създават, базирано на правата за достъп на потребителя до файлове на локалния компютър.

Ако нямате локални администраторски права на компютъра, може да осъществявате достъп само до задачи, създадени от вас. Ако имате локални администраторски права на компютъра, може да виждате всички задачи за архивиране, но не може да променяте задачи, създадени от други потребители.

Задачи за архивиране, които са създадени по-рано, без да се вземат предвид потребителските права, са налични за всички потребители на компютъра. Все пак ако такава задача се промени, ще бъде стартирана според правата на потребителя, който е променил задачата.

Възстановяване на задачи, базирано на правата за достъп на потребителя

Ако нямате локални администраторски права на компютъра, може да възстановявате данни само от задачи за архивиране, създадени от вас, и само до папки, до които имате права за достъп. Ако имате локални администраторски права на компютъра, може да възстановявате данни от всяка задача за архивиране във всяка папка.

Общият размер на копираните файлове в папка може да надвишава размера на папката, ако тя съдържа връзки към други папки (например когато копирате папката Documents, папките My Music, My Pictures и My Videos също ще бъдат копирани, ако папката Documents съдържа връзки към тези папки).

За Архивиране и възстановяване в OneDrive

Когато архивирате файлове в папка в OneDrive на Вашия компютър, приложението Kaspersky действа различно в зависимост дали файлът в облака е изтеглен в папката OneDrive:

- Ако файлът е в облака и в папката OneDrive на Вашия компютър, приложението Kaspersky прави резервно копие на този файл.
- Ако файлът не е в облака, но е в папката OneDrive на Вашия компютър, Kaspersky прави резервно копие на този файл.

- Ако файлът се показва в папката OneDrive, но се съхранява само в облака, но не и на Вашия компютър, приложението Kaspersky прави резервно копие на този файл.

Как да създадете задача за архивиране

За да създадете задача за архивиране:

1. Отворете основния прозорец на приложението.
2. Изберете раздел **Производителност**.
3. В блока **Архивиране и възстановяване** щракнете върху бутона **Избор на файлове**.

   Стартира Съветникът за създаване на задача за архивиране.

   Съветникът се състои от серия страници (стъпки), които може да управлявате, като щраквате върху бутоните **Назад** и **Напред**. За да затворите съветника, след като приключи, щракнете върху бутона **Готово**. За да спрете Съветника във всеки етап, щракнете върху бутона **Отказ**.

   Нека да прегледаме стъпките на Съветника в повече детайли.

Стъпка 1. Изберете файлове

На тази стъпка на съветника изберете типа файлове или посочете папки, които искате да архивирате:

- Изберете един от предварително зададените типове файлове (файлове от папки в My Documents и Desktop, снимки и изображения, филми и видео, музикални файлове) за бързо конфигуриране. Ако потвърдите тази опция, съветникът ви отвежда директно на Стъпка 4 „Изберете хранилище за архивиране“.

  Приложението Kaspersky не създава резервни копия на файлове в папките „Desktop“ и „My Documents“, ако те се намират на мрежови диск.

- Изберете опцията **Създаване на резервни копия на файлове от посочени папки**, за да посочите ръчно папки, които искате да архивирате.

Стъпка 2. Изберете папки за архивиране

Ако сте избрали опцията **Създаване на резервни копия на файлове от посочени папки** на предната стъпка на Съветника, щракнете върху бутона **Добави папка** и изберете папка в прозореца **Изберете папка за архивиране**, който се отваря, или плъзнете папката в прозореца на приложението.

Поставете отметка в квадратчето **Ограничете архивирането по типове файлове**, ако искате да посочите категориите файлове, които да архивирате в избраните папки.

Стъпка 3. Изберете типове файлове за архивиране

Ако сте поставили отметка в квадратчето **Ограничете архивирането по типове файлове** на предната стъпка в съветника, на тази стъпка поставете отметка в квадратчетата срещу типовете файлове, които искате да архивирате.

Стъпка 4. Изберете хранилище за архивиране

На тази стъпка изберете хранилище за архивиране:

- **Онлайн хранилище**. Изберете тази опция, ако искате да съхранявате резервни копия в онлайн хранилището Dropbox. Онлайн хранилището трябва да бъде активирано, преди да може да се използва. Когато архивирате данни в онлайн хранилище, приложението Kaspersky не създава резервни копия на данни от типовете, които са предмет на ограничения от правилата за употреба на Dropbox.
- **Локален диск**. Ако искате да съхранявате резервни копия на локален диск, изберете съответния локален диск в списъка.
- **Мрежови диск**. Ако искате да съхранявате резервни копия на мрежови диск, изберете съответния мрежови диск в списъка.
- **Сменяемо устройство**. Ако искате да съхранявате резервни копия на сменяемо устройство, изберете съответното сменяемо устройство в списъка.

За да гарантирате сигурността на данните, препоръчваме да използвате Онлайн хранилище или да създадете резервни хранилища на сменяеми дискове.

Как да добавите мрежово хранилище

За да добавите мрежово хранилище:

1. Кликнете върху **Добави мрежово хранилище**, за да отворите **Добави мрежово хранилище** прозореца и изпълнете следните действия:
2. Посочете данните, необходими за свързване към мрежово хранилище.
3. Щракнете **OK**.

Как да добавите сменяемо устройство като хранилище

За да добавите сменяемо устройство като резервно хранилище:

1. Щракнете върху връзката **Свързване към налично хранилище**, за да отворите прозореца **Свързване на хранилище**.
2. Изберете раздел **Сменяем диск**.
3. Щракнете върху бутона **Преглед** и в прозореца, който се отваря, посочете сменяемия диск, на който желаете да записвате резервни копия на файловете.

Изберете квадратчето за отметка **Използвай разширени настройки за съхранение**, за да конфигурирате настройките на хранилището за файлове, като броя съхранявани версии на резервни копия на файлове и продължителността на съхранение на резервните копия.

Стъпка 5. Създаване на график за архивиране

Направете едно от следните на тази стъпка в Съветника:

- Посочете графика на задачи за архивиране, ако искате задачата за архивиране да стартира автоматично.

  a. В падащия списък **Стартирай архивиране** изберете интервал от време за стартиране на задачата (например **ежедневно**) и посочете времето за стартиране на задачата в полето **В**.

  b. В раздела **Акаунт** посочете потребителското име и паролата на вашия акаунт в Windows на този компютър. Данните на вашия акаунт в Windows са необходими за достъп до файловете по време на архивиране.

  c. Изберете квадратчето за отметка **Стартирай архивиране при стартиране на компютъра, ако е изключен в определеното време**, ако искате да стартирате архивиране възможно най-скоро, след като компютърът се включи. Например архивиране е планирано за изпълнение всеки уикенд. Ако компютърът е бил изключен през уикенда, архивирането се извършва, след като компютърът се включи в работен ден. Ако е премахната отметката от квадратчето, архивирането се извършва според графика, без да се опитва да се стартира след неуспешен опит.

- В списъка **Стартирай архивиране** изберете опцията **ръчно**, ако искате да стартирате задачата ръчно.

Когато работите със задачи за архивиране, имайте предвид следното:

- Ако създадете планирана задача за архивиране, трябва да посочите данните на вашия акаунт на този компютър.
- Ако създадете задача за архивиране при архивиране, не трябва да посочвате данните на вашия акаунт на този компютър.
- Ако промените задача при поискване на планирана задача, трябва да посочите данните на вашия акаунт на този компютър.

Стъпка 6. Задаване на парола за защита на резервните копия

Изберете квадратчето за отметка **Активиране на защита с парола** и попълнете полетата **Парола за достъп до резервни копия** и **Потвърждение на паролата**, за да защитите достъпа до резервни копия с парола.

Паролата е необходима за защита на резервното хранилище срещу неоторизиран достъп.

Приложението ще ви подкани да въведете парола в следните случаи:

- Когато създавате за първи път резервно хранилище на локално или сменяемо устройство (като флаш устройство). Когато създавате последващи задачи за архивиране към локален диск или това сменяемо устройство, приложението няма повече да ви пита моли да въвеждате парола. Ще бъде използвана паролата, която преди това сте въвели.

Ако копирате локалното резервно хранилище към сменяемо устройство и свързвате това сменяемо устройство към друг компютър, приложението ще ви помоли да въведете парола, за да копирате или възстановите данни от това хранилище.

- Когато свързвате сменяемо устройство към вашия компютър. Приложението проверява сменяемото устройство и ви моли да въведете парола, ако засече хранилище за архивиране на това сменяемо устройство.

Стъпка 7. Настройки на хранилището за версиите на файловете

Тази стъпка е налична, ако е поставена отметка в квадратчето **Използвай разширени настройки за съхранение** на Стъпка 4 „Изберете хранилище за архивиране“.

Посочете настройките за съхранение на файлове:

- Изберете квадратчето за отметка **Ограничава броя версии на резервни копия** и в полето **Версии на резервни копия за съхранение** посочете броя версии на резервни копия на един файл, които да се съхраняват.

- Изберете квадратчето за отметка **Ограничава периода на съхранение на версии на резервни копия** и в полето **Съхрани старите версии на резервните копия за** посочете броя дни, които всяка версия на файл на резервно копие трябва да се съхранява.

Стъпка 8. Въвеждане на името на задача за архивиране

Направете следното на тази стъпка:

- Въведете името на задачата за архивиране.

- Изберете квадратчето за отметка **Стартиране на архивиране при приключване на настройката**, за да стартирате автоматично процеса на архивиране, когато съветникът приключи.

Стъпка 9. Завършване на съветника

Този прозорец показва процеса на конфигуриране на хранилището за архивиране. Процесът на конфигуриране може да отнеме известно време.

Когато конфигурирането завърши, щракнете върху **Готово**.

Задача за архивиране е създадена. Задачата, която сте създали, се появява в прозореца **Архивиране и възстановяване**.

Как да стартирате задача за архивиране

За да стартирате задача за архивиране:

1. Отворете основния прозорец на приложението.
2. Изберете раздел **Производителност**.
3. В блока **Архивиране и възстановяване** щракнете върху бутона **Преглед на резервни копия**.
4. В прозореца **Архивиране и възстановяване**, който се отваря, изберете задача за архивиране и щракнете върху бутона **Стартирай**.

Задачата за архивиране е стартирана.

Възстановяване на данни от резервно копие

За да възстановите данни от резервно копие:

1. Отворете основния прозорец на приложението.
2. Изберете раздел **Производителност**.
3. В блока **Архивиране и възстановяване** щракнете върху бутона **Преглед на резервни копия**.

   Отваря се прозорецът **Архивиране и възстановяване**.

   - Щракнете върху бутона **Възстанови файловете** срещу съответната задача за архивиране.
   - Щракнете върху бутона **Управление на съхранение**, за да отворите прозореца, и щракнете върху бутона **Възстанови файловете** срещу съответното хранилище за архивиране.
4. Ако е посочена парола при създаването на резервното копие, въведете тази парола в прозореца **Въведете парола, за да получите достъп до мястото за съхранение**.
5. В падащия списък **Архив дата/час** изберете дата и часа на създаване на резервното копие.
6. Направете някое от следните действия:

   - Ако искате да възстановите всички данни, изберете квадратчето за отметка **Всички данни**.
   - Ако искате да възстановите единствено определени папки, изберете квадратчетата за отметка до съответните папки.
   - Ако искате да възстановите единствено определени файлове, изберете квадратчетата за отметка до съответните файлове в колоната **Име**.
7. За да възстановите единствено специфични типове файлове, изберете тези типове файлове в падащия списък **Тип файл**.
8. Щракнете **Възстанови отбелязаните файлове**.

   Отваря се прозорецът **Възстановяване на файлове от резервни копия**.
9. Изберете една от двете опции:

   - **Оригинална папка**. Ако е избрана тази опция, приложението възстановява данни в оригиналната папка.
   - **Посочена папка**. Ако е избрана тази опция, приложението възстановява данни в посочената папка. Щракнете върху бутона **Преглед**, за да изберете папката, в която искате да възстановите данни.

10. В падащия списък **Ако има конфликт с имена на файлове**, изберете действието, което да се изпълни, от приложението, когато името на файла, който се възстановява, съвпада с името на файла, който вече е наличен в целевата папка:

    - **питай** – когато имената на файловете съвпадат, приложението ви подканва да изберете една от следните опции: замени файла с резервното копие, запиши двата файла или не възстановявай файла.
    - **подмени файл с резервното копие** – приложението Kaspersky изтрива съществуващия файл и го заменя с файла, възстановен от резервното копие.
    - **запази и двата файла** – приложението Kaspersky оставя съществуващия файл непроменен и записва файла, възстановен от резервното копие, с ново име в същата папка.
    - **не възстановявай този файл** – приложението Kaspersky оставя съществуващия файл непроменен и не възстановява файла със същото име от резервното копие.

11. Щракнете **Възстанови**.

    Файловете, избрани за възстановяване, ще бъдат възстановени от резервното копие и записани в посочената папка.

Възстановяване на данни от FTP хранилище

Текущата версия на приложението Kaspersky не поддържа Архивиране и възстановяване през FTP. За да възстановите резервни копия, създадени в други приложения на Kaspersky, от FTP хранилище, следвайте инструкциите по-долу.

За да възстановите резервни копия от FTP хранилище:

1. Отворете основния прозорец на приложението.
2. Изберете раздел **Производителност**.
3. В блока **Архивиране и възстановяване** щракнете върху бутона **Преглед на резервни копия**.

   Отваря се прозорецът **Архивиране и възстановяване**.
4. Щракнете върху връзката **Управление на съхранение**, за да отворите прозореца **Съхранения**.
5. Отворете папката за съхранение на FTP в Windows Explorer.
6. Копирайте данните (включително файла `storage.xml`) на локален диск (например, C:\<folder name>).
7. В прозореца **Съхранения** до мястото за съхранение на FTP щракнете върху бутона **Изтрий хранилище**.
8. В прозореца за потвърждение на изтриването щракнете върху **Изтрий**.

   Хранилището вече е изтрито.
9. В прозореца **Съхранения** щракнете върху бутона **Свързване към налично хранилище**.
10. В прозореца **Свързване на хранилище** изберете раздела **Локален диск** и използвайте бутона **Преглед**, за да посочите пътя към папката с резервните копия, които сте копирали на локалния диск от мястото за съхранение на FTP.
11. В прозореца **Съхранения** до свързаното хранилище щракнете върху бутона **Възстанови файловете**.

12. Следвайте стандартната процедура за възстановяване.

Възстановяване на данни от резервно копие с помощта на Kaspersky Restore Utility

Kaspersky Restore Utility ви позволява да управлявате данните в резервното хранилище на компютър, на който приложение на Kaspersky е повредено или е било премахнато. По подразбиране след инсталиране на приложението помощната програма се намира в папката на Kaspersky Restore Utility, разположена в папката за инсталиране на приложението. За да използвате помощната програма на компютър, на който не е инсталирано или не е повредено приложение на Kaspersky, копирайте я на сменяемо устройство.

За да стартирате Kaspersky Restore Utility, ви трябват локални администраторски права.

Как да стартирате Restore Utility

За да стартирате Restore Utility:

1. Отворете сменяемия диск, на който сте копирали помощната програма.
2. Стартирайте файл kasperskylab.pure.restoretool в папката Kaspersky Restore Utility.

   Отваря се основния прозорец на Restore Utility. Прозорецът показва хранилището, конфигурирано в приложението. Може да посочите пътека към друго хранилище.

Как да отворите хранилище с помощта на Restore Utility

За да отворите резервно хранилище с помощта на Restore Utility:

1. Стартирайте Restore Utility.

   Помощната програма автоматично засича пътя към резервното хранилище, ако е създадено на локалния диск C:.
2. Ако резервното хранилище се намира на друг диск, щракнете върху бутона **Посочете хранилище** в основния прозорец на Restore Utility.
3. В прозореца, който се отваря, щракнете върху бутона **Преглед** и посочете пътя към резервното хранилище.
4. Щракнете върху бутона **Избор на хранилище**.

Как да възстановите данни от резервно копие

За да възстановите данни от резервно копие:

1. Стартирайте Restore Utility.
2. Направете следното в основния прозорец на Restore Utility:
   a. В падащия списък **Задача за архивиране** изберете задачата, която води до създаването на резервните копия, които ви трябват.
   b. В падащия списък **Архив дата/час** изберете датата и часа, когато са създадени съответните резервни копия.
3. Изберете файловете, които трябва да възстановите. За целта изберете квадратчетата за отметка до съответните папки в списъка.

   Използвайте бутона до полето **Търсене**, за да превключвате между дървовидна структура на папка и списък с файлове.
4. Щракнете **Възстанови отбелязаните файлове**.

   Отваря се прозорецът **Изберете къде да бъдат поставени възстановените файлове**.
5. В прозореца, който се отваря, изберете местоположението за запазване на възстановени файлове.
   - **Оригинална папка**. Изберете тази опция, за да възстановите данни в оригиналната папка.
   - **Посочена папка**. Изберете тази опция, за да изберете папката, в която трябва да бъдат възстановени данните. За да изберете папката, в която трябва да бъдат възстановени данните, щракнете върху бутона **Преглед**.
6. В падащия списък **Ако има конфликт с имена на файлове** изберете действие, което да се изпълни от приложението, когато целевата папка за файла, който се възстановява, вече съдържа файл със същото име:
   - **питай** – когато имената на файловете съвпадат, приложението ви подканва да изберете една от следните опции: замени файла с резервното копие, запиши двата файла или не възстановявай файла.
   - **подмени файл с резервното копие** – приложението Kaspersky изтрива съществуващия файл и го заменя с файла, възстановен от резервното копие.
   - **запази и двата файла** – приложението Kaspersky оставя съществуващия файл непроменен и записва файла, възстановен от резервното копие, с ново име в същата папка.
   - **не възстановявай този файл** – приложението Kaspersky оставя съществуващия файл непроменен и не възстановява файла със същото име от резервното копие.
7. Щракнете **Възстанови**.

   Отваря се прозорецът **Възстанови файловете**. Прозорецът показва напредъка на възстановяването на файлове от резервни копия. Може да спрете процеса по възстановяване с помощта на бутона **Спри**.

   Възстановени са изисканите резервни копия на избраните файлове.

За Онлайн хранилището

Приложението Kaspersky Ви позволява да записвате резервни копия на Вашите данни в Онлайн хранилище на отдалечен сървър чрез услугата на Dropbox.

За да използвате Онлайн хранилище:

- Уверете се, че компютърът е свързан към интернет.
- Създайте акаунт на уебсайта на доставчика на услуги за онлайн хранилище за данни.
- Активирайте Онлайн хранилище.

Може да използвате един и същ акаунт в Dropbox, за да архивирате данни от различни устройства с приложението Kaspersky, инсталирано в едно Онлайн хранилище.

Размерът на Онлайн хранилището се определя от доставчика на услуги за онлайн хранилища, уеб услугата на Dropbox. Вижте Уеб сайтът на Dropbox за повече детайли за условията за използване на уеб услугата.

При копиране на файлове в Dropbox приложението Kaspersky не различава между главни и малки букви в името на файл и/или името на път към файл. Следователно когато се опитвате да създавате резервни копия на файлове, чиито имена и/или пътища се различават само по големина на буквите, приложението Kaspersky създава само едно резервно копия, тъй като възниква конфликт в Dropbox.

Как да активирате Онлайн хранилище

За да активирате Онлайн хранилища:

1. Отворете основния прозорец на приложението.
2. Изберете раздел **Производителност**.
3. В блока **Архивиране и възстановяване** щракнете върху бутона **Избор на файлове**.

   Стартира Съветникът за създаване на задача за архивиране.
4. В прозореца за избор на тип данни изберете категорията данни или ръчно посочете файловете, които искате да архивирате.
5. В прозореца за избор на хранилище изберете опцията **Онлайн хранилище** и щракнете върху бутона **Активирай**.

   Необходима е интернет връзка за създаване на онлайн хранилище.

   Отваря се диалогов прозорец за влизане в акаунт в Dropbox.
6. В прозореца, който се отваря, направете една от следните операции:
   - Завършете регистрацията, ако не сте регистриран потребител на Dropbox.

- Ако сте регистриран потребител на Dropbox, влезте във вашия акаунт в Dropbox.

7. За да завършите активирането на Онлайн хранилище, потвърдете, че приложението Kaspersky може да използва Вашия акаунт в Dropbox за архивиране и възстановяване на данни. Приложението Kaspersky поставя резервни копия на записани данни в отделна папка, която е създадена в папката за съхранение на Dropbox за приложения.

   След като активирането на Онлайн хранилището е завършено, се отваря прозорецът за избор на хранилище. Той съдържа избор на онлайн хранилища, от които да се избира. За активираното Онлайн хранилище приложението показва количеството използвано пространство и количеството свободно пространство, налично за съхранение на данни.

При копиране на файлове в Dropbox приложението Kaspersky не различава между главни и малки букви в името на файл и/или името на път към файл. Следователно когато се опитвате да създавате резервни копия на файлове, чиито имена и/или пътища се различават само по големина на буквите, приложението Kaspersky създава само едно резервно копия, тъй като възниква конфликт в Dropbox.

Текуща дейност

Ако сте забелязали, че компютърът ви замръзва или работи по-бавно, можете да отворите прозореца **Активност на приложенията**, който показва списък с работещи в момента приложения и активни процеси и спира работата на приложение или приложения, които консумират твърде много от ресурсите на вашия компютър.

За да видите текущата дейност и/или да спрете приложение:

1. Отворете основния прозорец на приложението.

2. Отидете в раздела **Производителност**.

3. В блока **Текуща дейност** щракнете върху бутона **Преглед на дейност**.

   Прозорецът **Активност на приложенията** се отваря в раздел **Работещи**.

4. От списъка с приложения изберете това, което консумира най-много от ресурсите на процесора (в колоната **ЦП**) и/или RAM (колона **Памет**) и щракнете върху бутона **Прекрати процеса**.

Приложението ще спре.

Режим "Не безпокой"

В режим „Не безпокой“ приложението Kaspersky не показва изскачащи известия за събития, свързани със сигурността на вашия компютър, докато работите, учите, провеждате видео разговор или гледате филм. Режимът „Не безпокой“ се активира и деактивира автоматично. Не е нужно да променяте настройките на приложението.

След излизане от режим „Не безпокой“, приложението ще използва областта за уведомяване на лентата на задачите, за да покаже съобщение относно всяко събитие, настъпило, докато сте били заети. Ако има няколко събития, щракнете върху бутона **View**, за да отидете на **Център за уведомяване** и вижте всички събития.

Можете също така да видите всички събития, настъпили през последните три дни в **Център за уведомяване** на раздел **Статус** в раздел **Уведомления**.

Можете да научите повече за показването на известия в раздела „За известията“ в Помощ.

Игрален режим

Когато приложението Kaspersky стартира в режим на цял екран заедно с някои други приложения (особено компютърни игри), могат да възникнат следните проблеми:

- Производителността на приложенията или игрите намалява поради липса на ресурси;
- Прозорците с известия на приложението Kaspersky разсейват потребителя от играта;

За да избегнете ръчната промяна на настройките на приложението Kaspersky всеки път, когато превключвате в режим на цял екран, може да изберете Игрови режим. Ако се използва Игрови режим и играете или работите с приложения в режим на цял екран, приложението Kaspersky не стартира задачи за сканиране и актуализиране и не показва известия.

За да активирате Игрови режим:

1. Отворете основния прозорец на приложението.
2. Щракнете върху в долната част на главния прозорец.
   Отваря се прозорецът **Настройки**.
3. Отидете в **Настройки за производителност** → **Използване на ресурси на компютъра**.
4. Поставете отметка в квадратчето до **Игрален режим**.

Също така може да изберете квадратчето за отметка **Режим "Не безпокой"**. В този режим не виждате известията, ако работите активно в някои приложения, а задачите за сканиране и актуализиране не са стартирани.

Пестене на батерията

Когато режимът за запазване на батерията е активиран, приложението Kaspersky отлага планираните задачи за сканиране и актуализиране. Може да стартирате задачите за сканиране и актуализиране ръчно, ако е необходимо.

Можете също да активирате или деактивирате режима за пестене на батерия в прозореца **Използване на ресурси на компютъра**, като изберете или премахнете отметката в квадратчето **Пестене на батерията**.

Оптимизиране на натоварването на операционната система

Когато стартирате сканиране на компютъра с приложението Kaspersky, това може да консумира значителни системни ресурси. За да оптимизирате натоварването на системата, може да конфигурирателприложението Kaspersky да стартира задачи за сканиране (за системна памет, системен дял и обекти на стартиране) и да актуализира бази данни, когато компютърът е заключен или е активиран скрийнсейвърът. Тази допълнителна настройка ви позволява да подобрите сигурността на вашия компютър, без да жертвате производителността, когато го използвате.

Ако компютърът работи на батерия, приложението Kaspersky няма да изпълни задачите, когато компютърът е в престой, за да удължи живота на батерията.

За да оптимизирате натоварването на операционната система:

1. Отворете основния прозорец на приложението.
2. Щракнете върху ⚙ в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.
3. Отидете в **Настройки за производителност** → **Използване на ресурси на компютъра**.
4. Поставете отметка в квадратчето до **Отлагай сканирането на компютъра, когато системите на процесора и диска са много натоварени**.

Поверителност

В днешно време масови нарушения на защитата на данни, маркетолози, които следят всяка ваша стъпка онлайн — списъкът с дигитални безпокойства продължава. Защитата на поверителността ви става изключително важна. Научете как приложението Kaspersky защитава поверителността Ви онлайн, за да можете да управлявате и контролирате цифровия си отпечатък.

Kaspersky VPN

Предлага се само в Kaspersky Plus и Kaspersky Premium.

VPN връзката се установява чрез Kaspersky VPN Secure Connection, която се предлага като част от абонаментния план на Kaspersky Plus. Може да стартирате Kaspersky VPN Secure Connection от **Start** менюто (в операционна система Microsoft Windows 7 или по-нова версия), от началния екран (в операционна система Microsoft Windows 8 или по-нова версия) или от прозореца на приложение Kaspersky.

За да стартирате Kaspersky VPN Secure Connection от прозореца на приложение Kaspersky:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Дискретност**.
3. В блока **Kaspersky VPN** щракнете върху бутона **Отвори**.

Отваря се основният прозорец на Kaspersky VPN Secure Connection.

Повече детайли относно работата на Kaspersky VPN Secure Connection са налични в помощните файлове на това приложение.

Проверка на изтичане на данни

Този раздел обяснява как да проверите дали може да се осъществи публичен достъп до данните от вашия потребителски акаунт.

Информация за проверката на изтичане на данни

Проверка на изтичане на данни в плановете Kaspersky Basic и Kaspersky Standard Ви позволява ръчно да проверявате само акаунта My Kaspersky. Автоматичните проверки за Вашия акаунт My Kaspersky и други акаунти са налични само за планове Kaspersky Plus и Kaspersky Premium.

Повечето потребители създават акаунти на различни уеб сайтове за работа, пазаруване и общуване. Винаги има риск атакуващите да хакнат сайта и да получат достъп до потребителски данни. Ако използвате един и същ имейл адрес и парола за различни сайтове, е по-вероятно данните ви да изтекат.

С приложението Kaspersky може да проверявате потребителските си акаунти за потенциални изтичания. Ако проверката разкрие, че вашите данни може да са публично достъпни, приложението ще ви уведоми за това и ще покаже списък със сайтове, от които може да е възникнало изтичането на данни, датата на вероятното изтичане и категорията данни, които може да са публично достъпни.

Приложението Kaspersky също проверява акаунтите Ви за изтичане на данни в Тъмната мрежа. Ако се намери изтичане, приложението ви предупреждава за него.

Когато проверява потребителски акаунти, Kaspersky не извлича данните под форма на обикновен текст и ги използва единствено за посочената проверка, без да ги съхранява. При откриване на изтичане, приложението Kaspersky не получава достъп до потребителските данни, а само предоставя информация за категориите данни, които може да са публично достъпни.

Приложението Kaspersky може да Ви уведоми за възможно изтичане на следните категории данни:

- **Лични данни**: например паспортни данни, биометрични данни, данни за възраст.
- **Банкови данни**: например номера на кредитни карти и банкови сметки, информация за средства в кредитни карти и банкови сметки.
- **Хронология на дейностите**: например маркери за удостоверяване, история на паролите.

По подразбиране, приложението Kaspersky се опитва да провери Вашите потребителски акаунти, когато сте удостоверени на конкретен уеб сайт. По време на оторизацията, имейл адресът ви, използван за влизане в уебсайта, се криптира и се препраща към облака на KSN. Ако проверката разкрие, че данните ви може да са публично достъпни, ще получите съответно известие. Можете да забраните проверката на изтичане на данни.

Може да добавяте до 50 акаунта за автоматична проверка. Списъците с акаунтите в приложението Kaspersky не се синхронизират между устройства. Добавени акаунти се проверяват веднъж дневно.

Добавянето на акаунти към списъка за автоматична проверка може да не е налично във вашия регион.

Приложението Kaspersky периодично проверява адреса на електронната поща, свързан с Вашия My Kaspersky акаунт. Първата такава проверка се извършва 48 часа след инсталиране на Kaspersky. Следващите проверки се правят на всеки 24 часа.

Проверката за изтичане на данни за акаунта My Kaspersky не работи, ако приложението Kaspersky не е свързано с My Kaspersky или паролата на My Kaspersky не е въведена в приложението.

Как да разрешите или забраните проверката на изтичане на данни

За да включите или изключите Проверка на акаунт:

1. Отворете основния прозорец на приложението.
2. Изберете раздел **Дискретност**.
3. В блока **Проверка за изтичане на данни** щракнете върху бутона **Търсене на изтичания**.

   Отваря се прозорецът **Проверка за изтичане на данни**.

4. Използвайте превключвателя за превключване, за да активирате или деактивирате компонента за проверка за изтичане на данни.

Как да проверите дали данните ви може да са станали публично достъпни

За да проверите дали данните ви може да са станали публично достъпни:

1. Отворете основния прозорец на приложението.
2. Изберете раздел **Дискретност**.
3. В блока **Проверка за изтичане на данни** щракнете върху бутона **Търсене на изтичания**.

   Отваря се прозорецът **Проверка за изтичане на данни**.
4. Посочете своя имейл адрес в полето за въвеждане и щракнете върху бутона **Проверка**.

   Приложението Kaspersky започва проверка на посочения адрес. Ако проверката разкрие, че вашите данни може да са публично достъпни, приложението ще ви уведоми за това и ще покаже списък със сайтове, от които може да е възникнало изтичането на данни, датата на вероятното изтичане и категорията данни, които може да са публично достъпни. Щракването върху връзката с категорията данни ще предостави препоръки как да намалите последствията от възможно изтичане на тези данни.

   Приложението Kaspersky Ви позволява да проверите за възможни изтичания не само на Ваши данни, но от други потребителски акаунти, които принадлежат например на Вашето семейство и приятели.

Как да създадете списък с акаунти за автоматична проверка

За да създадете списък с акаунти за автоматична проверка:

1. Отворете основния прозорец на приложението.
2. Изберете раздел **Дискретност**.
3. В блока **Проверка за изтичане на данни** щракнете върху бутона **Търсене на изтичания**.

   Отваря се прозорецът **Проверка за изтичане на данни**.
4. В полето **Проверка на още акаунти** посочете имейл адреса на акаунта, който искате да добавите към списъка за автоматична проверка и щракнете върху бутона **Проверка**.

   Акаунтът, който сте добавили, ще се покаже в списъка **Акаунти**.

Добавянето на акаунти към списъка за автоматична проверка може да не е налично във вашия регион.

Поверително сърфиране

Този раздел предоставя информация как приложението Kaspersky може за ви защити срещу проследяване на Вашата онлайн дейност.

За Поверително сърфиране

Предлага се само в Kaspersky Standard, Kaspersky Plus и Kaspersky Premium.

Някои уеб сайтове използват услуги за проследяване, за да събират информация за вашите дейности в интернет. Тази информация се анализира и използва с цел да ви се показват реклами.

Компонентът *Поверително сърфиране* е проектиран за предотвратяване събирането на информация за вашата онлайн активност.

В *режим на откриване* компонентът Поверително сърфиране открива и брои опитите за събиране на данни и записва информацията в отчет. Режим на откриване е активиран по подразбиране, а събирането на данни е разрешено на всички уеб сайтове.

В *режим на блокиране* компонентът Поверително сърфиране открива и блокира опити за събиране на данни и информацията за тези опити се записва в отчет. В този режим събирането на данни е блокирано за всички уеб сайтове с изключение на:

- по уеб сайтове, добавени към изключения
- по уеб сайтове на Kaspersky и нейните партньори
- по уеб сайтове, които може да са неработещи в резултат на блокирането на услуги за проследяване според информацията, налична в Kaspersky

Броячът на блокирани опити за събиране на данни показва общия брой блокирания за целия сайт според това колко страници на сайта са отворени в браузъра. Ако една страница е отворена в браузъра, се броят единствено блокирани опити за събиране на данни на тази страница на сайта. Ако няколко страници на един и същ сайт са отворени в браузъра, се броят блокираните опити за събиране на данни на всички страници на сайта, отворени в браузъра.

Може да активирате компонента Поверително сърфиране чрез интерфейса на приложението Kaspersky или с помощта на разширението Kaspersky Protection във Вашия браузър.

Поверително сърфиране има следните ограничения:

- Приложението не блокира събирането на данни от услуга за проследяване от категорията „Социални мрежи“, докато сте в уеб сайта на съответната социална мрежа.
- Ако уеб страницата, от която произхожда опита за събиране на данни, не може да бъде определена, приложението Kaspersky не блокира този опит за събиране на данни и не показва информация за него.
- Ако уеб страницата, от която произлиза опитът за събиране на данни, може да се определи, но не може да бъде съотнесена към някоя отворена в момента в браузъра уеб страница, приложението Kaspersky прилага действието, посочено в настройките на Поверително сърфиране (блокира или разрешава събирането на данни). Приложението показва информация за опита за събиране на данни в отчетите, но не включва тази информация в статистиката на Поверително сърфиране, показвана в браузъра.

По подразбиране, компонентът е деактивиран.

Блокиране на събирането на данни

За да блокирате събирането на данни:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Дискретност**.
3. Изберете компонент **Поверително сърфиране** и щракнете върху иконката .

   Отваря се прозорецът **Настройки за Поверително сърфиране**.
4. Ако компонентът е деактивиран, активирайте го, като настроите превключвателя в горната част на прозореца на **Вкл**
5. Изберете опцията **Блокирай събирането на данни**.

   Приложението Kaspersky ще блокира опитите за събиране на данни на всички уеб сайтове без изключения.
6. Ако искате да блокирате или разрешите събирането на данни според категориите услуги за проследяване:

   a. Щракнете върху връзката **Категории и изключения**, за да отворите прозореца **Категории и изключения**.

   b. По подразбиране събирането на данни е блокирано за всички категории услуги за проследяване и всички социални мрежи. Изчистете квадратчетата за отметка срещу категориите услуги за проследяване и социални мрежи, за които искате да разрешите събирането на данни.

Разрешаване събирането на данни на всички уеб сайтове

За да разрешите събирането на данни на всички уеб сайтове:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Дискретност**.
3. Изберете компонент **Поверително сърфиране** и щракнете върху иконката .

   Отваря се прозорецът **Настройки за Поверително сърфиране**.
4. Ако компонентът е деактивиран, активирайте го, като настроите превключвателя в горната част на прозореца на **Вкл**
5. Изберете опцията **Събиране само на статистически данни**.

   Приложението Kaspersky засича и брои опитите за проследяване на Вашата онлайн активност, без да ги блокира. Може да видите резултатите от работата на компонента в отчета.

Разрешаване събирането на данни като изключение

Може да разрешите проследяване на вашата активност в специфични уеб сайтове като изключение.

За да разрешите събирането на данни като изключение:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Дискретност**.
3. Изберете компонент **Поверително сърфиране** и щракнете върху иконката .

   Отваря се прозорецът **Настройки за Поверително сърфиране**.
4. Ако компонентът е деактивиран, активирайте го, като настроите превключвателя в горната част на прозореца на **Вкл**
5. Изберете опцията **Блокирай събирането на данни**.

   Приложението Kaspersky ще блокира опитите за събиране на данни на всички уеб сайтове без изключения.
6. По подразбиране има изключение за разрешаване на събирането на данни на уеб сайтовете на Kaspersky и нейните партньори. Ако искате да блокирате събирането на данни на тези уеб сайтове, махнете отметката от квадратчето **Допуска събиране на данни на уеб сайтовете на Kaspersky и нейните партньори**.
7. По подразбиране има изключение за разрешаване на събирането на данни на уеб сайтове, които може да са неработещи тъй като събирането на данни е блокирано според информацията, налична за Kaspersky. Ако искате да блокирате събирането на данни на тези уеб сайтове, махнете отметката от квадратчето **Допуска събиране на данни на несъвместими уеб сайтове**.

   Kaspersky актуализира списъка с несъвместими уеб сайтове, когато проблемите със съвместимостта са разрешени.
8. Ако искате да посочите собствени изключения:

   a. Щракнете върху връзката **Категории и изключения**, за да отворите прозореца **Категории и изключения**.

   b. Щракнете върху връзката **Изключения**, за да отворите прозореца **Изключения за Поверително сърфиране**.

   c. Щракнете **Добави**.

   d. В прозореца, който се отваря, въведете адреса на уеб сайта, на който искате да разрешите проследяване на активността, и щракнете върху бутона **OK**.

   Посоченият уеб сайт е добавен към списъка с изключения.

Може също така да разрешите събиране на данни на избран уеб сайт, докато е отворен в браузъра.

Преглед на отчет за опитите за събиране на вашите данни в Интернет

За да видите отчет за опитите за събиране на вашите данни в Интернет:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Дискретност**.
3. Изберете компонент **Поверително сърфиране** и щракнете върху иконката .

   Отваря се прозорецът **Настройки за Поверително сърфиране**.

   Ако компонентът е деактивиран, активирайте го, като настроите превключвателя в горната част на прозореца на **Вкл**

Прозорецът показва консолидиран отчет с информация за опитите за събиране на данни за вашата онлайн активност.

Също така може да видите отчет за опитите за събиране на данни в браузър или в отчет за работата на приложението.

Управление на компонента Поверително сърфиране в браузър

Може да управлявате компонента Поверително сърфиране директно в браузъра:

- Активирайте компонента, ако е деактивиран;
- Вижте статистиката за откритите опити за събиране на данни;
- Отидете в прозореца с настройките на Поверително сърфиране;
- Блокирайте или разрешете събирането на данни.

За да управлявате компонента Поверително сърфиране в браузъра,

Щракнете върху бутона **Kaspersky Protection** на лентата с инструменти в браузъра.

Менюто, което се отваря, показва информация за работата на компонента и контролите на компонента.

Мениджър на пароли

Този раздел съдържа информация как можете да защитите Вашите пароли.

Проверка и сигурно съхраняване на Вашите пароли

Предлага се само в Kaspersky Plus и Kaspersky Premium.

Ако сте активен интернет потребител, обикновено трябва да използвате множество различни пароли, като например когато посещавате уеб сайтове на банки, социални мрежи и пощенски услуги. Не е удобно да се използва голям брой пароли, тъй като трябва да запомните коя парола използвате на конкретен уеб сайт. Това често кара потребителите да прибягнат към лесното решение да използват една лесна парола на различни уеб сайтове. Все пак това не е безопасно решение. Лесна парола, която се използва на няколко уеб сайта, лесно може да бъде дешифрирана или прехванатата от хакери. Ако това се случи с парола от уеб сайт за банкиране, рискувате да изгубите парите си.

Проверка на сигурността на паролата

Приложението Kaspersky проверява сигурността на паролите, които създавате в Интернет. Ако паролите не са достатъчно сигурни, Kaspersky може да Ви помогне да създадете силни пароли и да ги съхранявате на сигурно място.

Защита от използване на едни и същи пароли

Когато въвеждате парола в уеб сайт, където сигурността на паролата е особено важна (например в социална мрежа), приложението Kaspersky Ви подканва да активирате защитата от използване на едни и същи пароли.

Ако защитата от използване на едни и същи пароли е активирана, приложението Kaspersky проверява дали не сте използвали преди това паролата, която въвеждате на уеб сайтове от следните категории:

- Уеб сайтове на банки и системи за плащане;
- Социални мрежи;
- Пощенски услуги.

Ако паролата, която въвеждате, вече е използвана на уеб сайтове от тези категории, приложението Kaspersky Ви уведомява за това и Ви предлага да създадете нова парола. Можете да изберете категории уеб сайтове, за които използването на едни и същи пароли трябва да бъде наблюдавано.

Сигурно съхранение на пароли и документи

Диспечерът на пароли Kaspersky е проектиран да пази Вашите пароли и документи в безопасност. Той използва специално криптирано хранилище за сигурно съхраняване на Вашата лична информация: пароли, данни за самоличност, финансова или медицинска информация.

Можете да изтеглите Диспечера на пароли Kaspersky от прозореца на приложението Kaspersky.

Как да изтеглите и инсталирате Kaspersky Password Manager

За да изтеглите и инсталирате Kaspersky Password Manager, за да защитите вашите пароли,

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Дискретност**.
3. В блока **Безопасност на паролата** щракнете върху бутона **Изтегли**.

   Инсталационният пакет на Kaspersky Password Manager се изтегля на вашия компютър. За да инсталирате Kaspersky Password Manager, следвайте стандартната процедура за инсталиране на приложения на вашия компютър.

Как да стартирате Диспечера на пароли Kaspersky от прозореца на приложението Kaspersky

За да стартирате Диспечера на пароли Kaspersky, ако вече е инсталиран:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Дискретност**.
3. В блока **Безопасност на паролата** щракнете върху бутона **Стартиране**.

   Отваря се прозорец Kaspersky Password Manager.

Вижте *Помощ за Kaspersky Password Manager* за инструкции относно използването на Kaspersky Password Manager.

Как да проверите безопасността на Вашите пароли

Предлага се само в Kaspersky Premium.

Вашите Интернет акаунти са в сериозна опасност, ако имат неуникални или слаби пароли (например qwerty или 12345) и ако паролите се основават на информация, която е лесна за отгатване или получаване (например имена на Вашите роднини или дати на раждане).

Приложението Kaspersky може да Ви помогне бързо да проверите колко сложни са вашите пароли и дали една и съща парола се използва в повече от един акаунт.

За да проверите безопасността на паролата:

1. Отворете основния прозорец на приложението.
2. Изберете раздел **Дискретност**.
3. Под **Безопасност на паролата**, направете едно от следните неща:

   - Кликнете **Изтегли** ако Диспечер на пароли Kaspersky все още не е инсталиран. Името на бутона може да бъде **Start** или **Отвори** ако Диспечер на пароли Kaspersky не е конфигуриран, остарял е или е свързан към My Kaspersky акаунт, който не съответства на акаунта, към който е свързано приложението Kaspersky.

     Това стартира инсталирането на Диспечера на пароли Kaspersky. Следвайте инструкциите на Съветника.

   - Кликнете **Scan** ако сканирането все още не е стартирано.
   - Кликнете **Details** ако сканирането вече е стартирано.

   Резултатите от сканирането се показват под **Безопасност на паролата** групирани по категории за безопасност.

За да научите повече за сканирането на пароли, вижте *Kaspersky Password Manager Help*.

Конфигуриране на сигурността на паролата

За да промените Настройките на проверката на сигурността на паролата:

1. Отворете основния прозорец на приложението.
2. Щракнете върху ⚙ в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.
3. В раздела **Настройки на поверителността** изберете подраздела **Защитено въвеждане на данни**.
4. Изберете **Покажи съвети за създаване на силни пароли** квадратчето за отметка, ако искате приложението Kaspersky да проверява силата на паролите, които създавате на уебсайтове, и да предоставя препоръки за създаване на силни пароли.

   Ако сте инсталирали Kaspersky Password Manager, уведомлението ще ви препоръча сигурна парола. Ако Kaspersky Password Manager не е инсталиран, ви препоръчваме да го изтеглите и инсталирате, за да сте сигурни, че винаги създавате сигурни пароли.
5. Изберете квадратчето за отметка **Предупреждение за използване на едни и същи пароли на уеб сайтове**, ако искате приложението Kaspersky да проверява дали не сте използвали преди това паролата, която въвеждате или създавате, на уеб сайтове на банки, социални мрежи и пощенски услуги.
6. Щракнете върху връзката **Избери категории уеб сайтове**, за да отидете в прозореца **Категории уеб сайтове**, ако искате да изберете категориите уеб сайтове, за които използването на идентични пароли трябва да бъде проверено.
7. Изберете квадратчетата за отметка за следните категории:

   - **Интернет банки и системи за плащане**. Когато създавате или въвеждате парола в Интернет, приложението Kaspersky проверява дали не сте използвали тази парола в уеб сайтове на банки и системи за плащане.
   - **Социални мрежи**. Когато създавате или въвеждате парола в Интернет, приложението Kaspersky проверява дали не сте използвали тази парола в социални мрежи.
   - **Пощенски услуги**. Когато създавате или въвеждате парола в Интернет, приложението Kaspersky проверява дали не сте използвали тази парола в пощенски услуги.

Безопасно плащане

Този раздел предоставя инструкции как може да защитите финансовите си транзакции и покупки онлайн с приложението Kaspersky.

За защитата на финансовите трансакции и онлайн покупки

За защита на поверителните данни, които въвеждате в уеб сайтове на банки и системи за плащане (като например номера на банкови карти и пароли за онлайн банкиране), както и за предотвратяване на кражба на средства, когато извършвате онлайн плащания, Kaspersky Security Cloud Ви подсеща да отваряте такива уеб сайтове в Защитен браузър.

Защитен браузър е специален режим за работа на браузъра, проектиран да защитава вашите данни, когато осъществявате достъп до уеб сайтове на банки или системи за плащане. Защитеният браузър стартира в изолирана среда, за да не се позволи други приложения да вмъкнат своя код в процеса на Защитения браузър. Приложението Kaspersky създава специални профили за браузърите Mozilla Firefox и Google Chrome, за да предотврати добавките на трети страни да се отразят на работата на Защитения браузър. Приложението не затяга вашите данни, които браузърите могат да записват в профилите, създадени за тях.

Ако използвате Microsoft Edge, базиран на Chromium, Google Chrome, Mozilla Firefox или Internet Explorer, Защитеният браузър се отваря в нов прозорец.

Приложението използва разширение Kaspersky Protection, за да предостави редица функции на Защитения браузър.

Браузърите, които не отговарят на изискванията на софтуера, не могат да работят в режим на Защитен браузър. Вместо такива браузъри Microsoft Edge, базиран на Chromium, или друг браузър, конфигуриран в настройките на приложението, стартира в режим на Защитен браузър.

Невъзможно е да се стартира Защитен браузър при следните условия:

- Премахната е отметката от квадратчето **Включи самозащитата** в прозорец **Използване на ресурси на компютъра**, раздел **Настройки за производителност**.
- Javascript е изключен в браузъра.

Стартиране на Защитен браузър в браузъра Yandex

Приложението Kaspersky поддържа защитата на Вашите финансови транзакции в браузъра Yandex с някои ограничения. За да стартирате Защитен браузър, приложението вмъква специален скрипт в уеб страницата (и трафик). Разширението Kaspersky Protection не е налично. Компонентите Поверително сърфиране и Защита от банери работят, но не могат да бъдат конфигурирани в браузър Yandex.

Възможности на Защитения браузър

В режим на защитен браузър приложението предоставя защита срещу следните типове заплахи:

- Несигурни модули. Приложението стартира проверка за несигурни модули всеки път, когато посещавате уеб сайт на банка или система за плащане.
- Комплекти за пълен достъп. Приложението сканира за комплекти за пълен достъп при стартирането на Защитен браузър.
- Невалидни сертификати на уеб сайтове на банки или системи за плащане. Приложението проверява сертификатите, когато посещавате уеб сайт на банка или система за плащане. Проверката се извършва в база данни с компрометирани сертификати.

Състояние на Защитения браузър

Когато отваряте уеб сайт в Защитен браузър, по границите на прозореца на браузъра се появява рамка. Цветът на рамката показва състоянието на защита.

Рамката на прозореца на браузъра може да показва следните цветни индикации:

- Зелена рамка. Означава, че всички проверки са изпълнени успешно. Може да продължите да използвате Защитен браузър.
- Жълта рамка. Означава, че проверките са разкрили проблеми със сигурността, които трябва да бъдат разрешени.

  Приложението може да открие следните заплахи и проблеми със сигурността:

  - Несигурен модул. Необходимо е сканиране и дезинфектиране на компютъра.
  - Комплект за пълен достъп. Необходимо е сканиране и дезинфектиране на компютъра.
  - Невалиден сертификат на уеб сайт на банка или система за плащане.

  Ако не отстраните откритите заплахи, сигурността на сесията на свързване на уеб сайта на банката или системата за плащане не е гарантирана. Събития, включващи стартирането и използването на Защитен браузър с намалена защита, се записват в регистрационния файл на събития на Windows.

За защитата срещу екранни снимки

За да защитите данните си, когато разглеждате защитени уеб сайтове, приложението Kaspersky предотвратява заснемането на непозволени снимки на екрана от шпионски софтуер. Защитата срещу екранни снимки е включена по подразбиране. Защитата срещу екранни снимки работи дори ако виртуализацията на хардуера е изключена.

За защитата на данните в клипборда

Приложението Kaspersky блокира неупълномощения достъп на приложения до клипборда, когато извършвате онлайн плащания, предотвратявайки кражбата на данни от престъпници. Такова блокиране е активно само ако несигурно приложение се опита да получи неупълномощен достъп до вашия клипборд. Ако копирате данни ръчно от прозореца на приложението до прозорец на друго приложение (например от Notepad до прозорец на текстови редактор), достъпът до клипборда е разрешен.

Защитата на клипборда не работи, ако виртуализацията на хардуер е изключена на вашия компютър.

Ако Защитеният браузър е стартиран в операционна система Microsoft Windows 10, приложението Kaspersky ще блокира взаимодействието на универсалните приложения на Windows с клипборда.

Как да промените настройки на Безопасно плащане

За да конфигурирате Безопасно плащане:

1. Отворете основния прозорец на приложението.
2. Щракнете върху ⚙ в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.
3. Изберете раздела **Настройки на поверителността**.

4. Щракнете **Безопасно плащане**.

   Прозорецът показва настройките на компонента Безопасно плащане.

5. Активирайте Безопасно плащане, като щракнете превключвателя в горната част на прозореца.

6. В раздела **При първия достъп до уеб сайтове на банки и системи за плащане** изберете действието, което да се извършва от приложението, когато отворите за първи път уеб сайта на банка или система за плащане във вашия браузър:

   - Изберете **Стартирай Защитен браузър**, ако желаете приложението да отваря уеб сайта в Защитен браузър.
   - Изберете **Питай потребителя**, ако желаете приложението да ви пита дали да отвори уеб сайта в Защитен браузър, когато го посещавате.
   - Изберете **Не стартирай Защитен браузър**, ако не желаете приложението да отваря уеб сайта в Защитен браузър.

7. В раздела **Допълнително** отворете падащия списък **Използвайте следния браузър за Безопасно плащане** и изберете браузъра, в който приложението ще стартира в режим на Защитен браузър, когато посещавате уеб сайт на банка или система за плащане от прозореца Безопасно плащане.

   Може да изберете един от следните браузъри, инсталирани на вашия компютър, или да използвате браузъра по подразбиране на операционната система.

Как да конфигурирате Безопасно плащане за конкретен уеб сайт

За да конфигурирате Безопасно плащане за определен уеб сайт:

1. Отворете основния прозорец на приложението.

2. Отидете в раздела **Дискретност**.

3. Изберете раздела **Безопасно плащане** и щракнете върху бутона **Преглед на уеб сайтове**.

   Отваря се прозорецът **Безопасно плащане**.

4. Щракнете върху връзката **Добавяне на уеб сайт в Безопасно плащане**, за да отворите полета за добавяне на информацията за уеб сайта.

5. В полето **Уеб сайт (адрес) в Безопасно плащане** въведете уеб адреса на уеб сайта, който искате да отворите в Защитен браузър.

   Адресът на уеб сайта трябва да бъде предшестван от префикса за HTTPS протокола (например https://example.com), който се използва по подразбиране от Защитения браузър.

6. Изберете действието, което искате Защитения браузър да извършва, когато отваряте уеб сайта:

   - Ако искате уеб сайтът да се отваря в Защитен браузър, всеки път когато го посещавате, изберете **Стартирай Защитен браузър**.
   - Ако искате приложението Kaspersky да Ви подкани за действие, когато се отвори уеб сайта, изберете **Питай потребителя**.

- Ако искате да деактивирате Безопасно плащане за уеб сайта, изберете **Не стартирай Защитен браузър**.

7. Щракнете върху връзката **Добави описание**, за да отворите полето **Описание** и въведете името или описанието на този уеб сайт.

8. Щракнете **Добави**.

Уеб сайтът ще се покаже в списъка.

Как да изпращате обратна връзка за Безопасно плащане

Можете да изпращате на Kaspersky обратна връзка за работата на компонента „Безопасно плащане“ или да съобщавате за проблем в този компонент.

Как да изпращате обратна връзка

За да изпратите обратна връзка за работата на компонента „Безопасно плащане“:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Защита**.
3. Изберете раздела **Безопасно плащане** и щракнете върху бутона **Преглед на уеб сайтове**.

   Отваря се прозорецът **Безопасно плащане**.
4. Щракнете върху връзката **Изпратете отзив**, за да отворите прозорец, в който може да оставите обратна връзка за работата на компонента „Безопасно плащане“.
5. Оценете „Безопасно плащане“ по 5-степенна скала, като изберете от 1 до 5 звезди.
6. Ако искате да добавите коментар към вашата обратна връзка, въведете текста на коментара в полето **Детайли**.
7. Щракнете **Изпрати**.

Как да съобщите за проблем

За да съобщите за проблем със Защитения браузър:

1. Щракнете върху връзката **Съобщете за проблем** в изскачащия прозорец в долната част на защитения браузър.

   Прозорецът, който се отваря, ви позволява да съобщите за проблем с „Безопасно плащане“.

2. В падащия списък **Проблем** изберете елемент, който най-точно описва вашия проблем:

   - **Не го използвам**. Изберете този елемент, ако не използвате „Безопасно плащане“ или ако сте решили да се отпишете от използването на „Безопасно плащане“.
   - **Уеб страницата се отваря бавно**. Изберете този елемент, ако отварянето на уеб сайта отнема по-дълго време отколкото в обичайния браузър.
   - **Защитеният браузър стартира, когато не е необходимо**. Изберете този елемент, ако уеб сайтове, които не изискват използване на „Безопасно плащане“, се отварят в Защитен браузър.
   - **Неуспех при удостоверяване на уеб сайта**. Изберете този елемент, ако възникват грешки при удостоверяването на уеб сайт, отворен в Защитен браузър.
   - **Уеб сайтът се показва неправилно или не се отваря**. Изберете този елемент, ако уеб сайтовете не се отварят в Защитен браузър или се показват с грешки или изкривявания.
   - **Грешки при потвърждаването на сертификата на уеб сайта**. Изберете този елемент, ако се появяват съобщения за грешки по време на потвърждаването на сертификатите на уеб сайтовете.
   - **Не може да се направи екранна снимка, когато се изпълнява Защитен браузър**. Изберете този елемент, ако екранните снимки не се създават в Защитен браузър.
   - **Грешки при въвеждане на данни от клавиатурата или от клипборда**. Изберете този елемент, ако възникнат грешки при въвеждането на данни в Защитен браузър.
   - **Уеб страница, отворена в Защитен браузър, не се отпечатва**. Изберете този елемент, ако не можете да отпечатате отворена страница в уеб сайт.
   - **Показва се съобщение, предупреждаващо, че не са инсталирани важни актуализации на операционната система**. Изберете този елемент, ако се покаже съобщението „Не са инсталирани важни актуализации за системата“, когато се изпълнява Защитен браузър.
   - **Друг браузър работи като Защитен браузър**. Изберете този елемент, ако Защитен браузър е отворен в браузър, различен от този, в който сте го стартирали.
   - **Грешки при работа**. Изберете този елемент, ако Защитен браузър върне грешка.
   - **Друго**. Изберете този елемент, ако проблемът, който изпитвате, не се покрива от други елементи.

3. За да изпратите допълнителна информация за вашия проблем до Kaspersky, въведете описанието му в текстовото поле **Детайли**.

4. Щракнете върху бутона **Изпрати**.

Ако приложението Kaspersky не успее да изпрати Вашата обратна връзка (например Интернет връзката не е налична), тя ще бъде записана на Вашия компютър. Обратната връзка се съхранява открито за 30 дни.

Обратна връзка за работата на компонента „Безопасно плащане“ може да изпращате до 10 пъти на ден.

Освен това може да изпращате обратна връзка, след като компонентът „Безопасно плащане“ е изключен. След като компонентът е изключен, може да изпращате обратна връзка веднъж месечно.

Управление на уеб камера и микрофон

Този раздел съдържа информация как да предотвратите шпиониране през Вашата уеб камера и подслушване през Вашия микрофон.

Предлага се само в Kaspersky Standard, Kaspersky Plus и Kaspersky Premium.

За достъпа на приложението до уеб камерата и микрофона

Нарушители може да се опитат да Ви шпионират чрез Вашата уеб камера или да Ви подслушват, като получат достъп до микрофона Ви. Приложението Kaspersky защитава Вашата уеб камера и микрофон от неоторизиран достъп, ако компонентът за управление на уеб камера и микрофон е активиран. В настройките на компонента можете да блокирате достъпа на всички приложения до уеб камерата и микрофона или да поискате да бъдете уведомявани, когато приложение се опита да получи достъп до Вашата уеб камера или микрофон.

Ако компонентът е активиран, но достъпът до Вашата уеб камера и микрофон не е напълно блокиран, достъпът се предоставя или отказва въз основа на надеждната група, от която е част съответното приложение. Достъпът е блокиран за приложения в групите С големи ограничения или Несигурни.

В прозореца с настройки на Предотвратяване на проникване може да разрешите достъп до уеб камерата или микрофона за приложения, включени в групите С големи ограничения и Несигурни. Ако приложение от групата С ниски ограничения се опитва да получи достъп до уеб камерата или микрофона, приложението Kaspersky блокира достъпа и Ви уведомява, ако сте конфигурирали известия в настройките на компонента.

В падащия списък на известието можете да блокирате достъпа на приложението до уеб камера или микрофон, или да отидете на настройките за достъп. Това известие не се показва, ако някои приложения работят в режим на цял екран на Вашия компютър.

В падащия списък на известието може да изберете да скриете известията или да преминете към конфигуриране на настройките за показване на известия.

Как Kaspersky управлява уеб камерата

По подразбиране приложението Kaspersky разрешава достъп до уеб камерата на приложенията, които изискват Вашето разрешение, когато потребителският интерфейс на приложението все още се зарежда, затваря или не отговаря, и не може да разрешите достъп ръчно.

Функционалността за защита на достъпа до уеб камерата има следните функции и ограничения:

- Приложението Kaspersky управлява видеото и снимките, получени от обработката на данни от уеб камерата.
- Приложението Kaspersky контролира аудио сигнала, ако е част от видеопотока, идващ от уеб камерата.
- Приложението Kaspersky контролира само уеб камери, свързани чрез USB или IEEE1394, които се показват в диспечера на устройствата на Windows като Устройства за създаване на изображения.

Щракнете върху тази връзка, за да видите списъка с поддържани уеб камери.

За да активирате защитата срещу неоторизиран достъп до уеб камерата, компонентът Предотвратяване на проникване трябва да бъде активиран.

Защита на уеб камерата има ограничения, ако приложението е инсталирано в актуализацията за годишнината на Microsoft Windows 10 (RedStone 1).

Как Kaspersky управлява микрофона

Защитата на микрофона има следните специални функции:

- Компонентът Предотвратяване на проникване трябва да бъде активиран за тази функционалност, за да работи.
- След като настройките на достъпа на приложението до звукозаписващо устройство са били променени (например на приложението е забранено да получава аудио поток в прозореца с настройки на Предотвратяване на проникване), това приложение трябва да бъде рестартирано, за да бъде спряно да получава аудио потока.
- Приложението Kaspersky защитава достъпа само до вградени микрофони и външни микрофони. Други звукозаписващи устройства не се поддържат.
- Приложението Kaspersky разрешава на приложение да получава аудио поток и не показва никакви известия, ако приложението започва да получава аудио поток, преди приложението Kaspersky да е стартирано или ако сте поставили приложението в групата Несигурни или С големи ограничения, след като то е започнало да получава аудио потока.

Приложението Kaspersky не гарантира защита на аудио потока от такива устройства като DSLR камери, камкордери и екшън камери.

Как да промените настройките за достъп на приложението до уеб камерата или микрофона

За да промените настройките за достъп на приложението до уеб камерата или микрофона:

1. Отворете основния прозорец на приложението.
2. Щракнете върху ⚙ в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.
3. В раздела **Настройки на поверителността** изберете компонента **Контрол на уеб камерата и микрофона**.
4. В **Настройки за уеб камера**, изпълнете едно от следните действия:

   - **Блокиране на достъпа на всички приложения до вашата уеб камера**. Достъпът до уеб камерата е блокиран за всички приложения, инсталирани на Вашия компютър.
   - **Уведоми, ако дадено приложение използва уеб камерата**. Приложенията, които имат достъп по подразбиране, ще имат достъп до уеб камерата. Ще се покаже известие, информиращо потребителя, че конкретно приложение използва уеб камерата.
5. В **Настройки за микрофон**, изпълнете едно от следните действия:

   - **Блокиране на достъпа на всички приложения до вашия микрофон**. Достъпът до микрофона е блокиран за всички приложения, инсталирани на Вашия компютър.
   - **Уведоми, ако дадено приложение използва микрофона**. Приложенията, които имат достъп по подразбиране, ще имат достъп до микрофона. Ще се покаже известие, информиращо потребителя, че конкретно приложение използва микрофона.

Как да разрешите или блокирате достъпа до уеб камерата за отделно приложение

За да разрешите или блокирате достъпа до уеб камерата за приложение:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Защита**.
3. Изберете компонента **Предотвратяване на проникване**.
4. Щракнете върху връзката **Управление на приложения**, за да отворите прозореца **Управление на приложения**.
5. В списъка изберете приложението, на което искате да разрешите достъп до звукозаписващи устройства. Щракнете два пъти върху приложението, за да отворите прозореца **Правила за програмите**.
6. В прозореца **Правила за програмите** отидете в раздела **Права**.
7. В списъка с категории права изберете **Промяна на операционната система → Подозрителни промени в операционната система**.
8. Изберете **Достъп до уеб камера**.
9. В колона **Действие**, изберете **Разреши** или **Забрани**.
10. Щракнете **Запази**.

Ако изберете **Блокиране на достъпа на всички приложения до вашата уеб камера**, достъпът на приложението до уеб камерата е блокиран независимо от надеждната група и ръчно конфигурираните разрешения.

Как да разрешите или блокирате достъпа до микрофона за отделно приложение

За да разрешите или блокирате достъпа до микрофона за отделно приложение:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Защита**.
3. Изберете компонента **Предотвратяване на проникване**.
4. Щракнете върху връзката **Управление на приложения**, за да отворите прозореца **Управление на приложения**.
5. В списъка изберете приложението, за което искате да разрешите достъп до микрофона, и щракнете двукратно, за да отворите прозорец **Правила за програмите**.
6. В прозореца **Правила за програмите** отидете в раздела **Права**.
7. В списъка с категории права изберете **Промяна на операционната система → Подозрителни промени в операционната система → Достъп до звукозаписващи устройства**.
8. В колона **Действие**, изберете **Разреши** или **Забрани**.
9. За да получавате известия за случаите на приложения с разрешен или отказан достъп до аудио потока, в колоната **Действие** щракнете върху иконата и изберете **Записвай в отчет**.
10. Щракнете **Запази**.

Ако изберете **Block access for all applications**, достъпът на приложението до микрофона е блокиран независимо от групата за доверие и ръчно конфигурираните разрешения.

Откриване на преследвачески софтуер

Някои законни приложения могат да бъдат използвани от престъпници, за да откраднат личните ви данни и да ви шпионират. Повечето от тези приложения са полезни и много хора се възползват от удобството им. Тези приложения включват IRC клиенти, програми за автоматично набиране, програми за изтегляне на файлове, монитори за системна активност, помощни програми за управление на пароли, FTP, HTTP или Telnet сървъри.

Въпреки това, ако престъпниците получат достъп до тези приложения на вашия компютър или успеят да ги разположат тайно там, те ще могат да използват част от функционалността, за да откраднат личните ви данни или да извършат други незаконни действия.

Можете да прочетете за различните видове преследвачески софтуер по-долу.

Тип	Име	Описание
Клиент-IRC	IRC клиенти	Хората инсталират тези приложения, за да общуват помежду си в интернет релейни чатове (IRC). Престъпниците могат да използват тези приложения за разпространение на зловреден софтуер.
Dialer	Автоматично набиране	Може тайно да установява телефонни връзки през модем.
Downloader	Програми за изтегляне	Може скрито да изтегля файлове от уеб страници.
Monitor	Приложения за наблюдение	Позволява наблюдение на активността на компютъра, на който са инсталирани (проследяване кои приложения се изпълняват и как те обменят данни с приложения на други компютри).
PSWTool	Инструменти за възстановяване на парола	Разрешават на потребителите да виждат и възстановяват забравени пароли. Престъпниците тайно внедряват тези приложения на компютрите на хората със същата цел.
RemoteAdmin	Инструменти за отдалечено администриране	Широко използвани от системните администратори за получаване на достъп до интерфейсите на отдалечени компютри, за да ги наблюдават и контролират. Престъпниците тайно внедряват тези приложения на компютрите на хората със същата цел, за да шпионират отдалечени компютри и да ги контролират. Легитимните инструменти за отдалечено администриране са различни от бекдорите (троянски коне за дистанционно управление). Задните врати могат да проникнат в система и да се инсталират там сами, без разрешението на потребителя, докато легитимните приложения нямат тази функционалност.
Server-FTP	FTP сървъри	Работят като FTP сървъри. Престъпниците могат да ги внедрят на вашия компютър, за да отворят отдалечен достъп до него чрез протокола FTP.
Server-Proxy	Прокси сървъри	Работят като прокси сървъри. Престъпниците ги внедряват в компютъра, за да го използват за изпращане на спам.
Server-Telnet	Telnet сървъри	Работят като Telnet сървъри. Престъпниците ги внедряват на компютър, за да отворят отдалечен достъп до него с помощта на протокола Telnet.
Server-Web	Уеб сървъри	Работят като уеб сървъри. Престъпниците могат да ги разположат на вашия компютър, за да отворят отдалечен достъп до него чрез протокола HTTP.
RiskTool	Локални инструменти	Те дават на потребителите допълнителни възможности за управление на своите компютри (позволявайки им да скриват файлове или активни прозорци на приложения или да затварят активни процеси).
NetTool	Мрежови инструменти	Те дават на потребителите на компютри, на които са инсталирани, допълнителни възможности за взаимодействие с други компютри в мрежата (рестартиране на отдалечени компютри, намиране на отворени портове, стартиране на приложения, инсталирани на тези компютри).
Client-P2P	P2P мрежови клиенти	Разрешете използването на P2P (Peer-to-Peer) мрежи. Те могат да бъдат използвани от престъпници за разпространение на зловреден софтуер.
Client-SMTP	SMTP клиенти	Може тайно да изпраща имейли. Престъпниците ги внедряват в компютъра, за да го използват за изпращане на спам.

WebToolbar	Уеб ленти с инструменти	Добавете ленти с инструменти на търсачките към интерфейса на други приложения.
FraudTool	Измамен софтуер	Имитира други приложения. Например има антивирусен измамен софтуер, който показва известия за откриване на злонамерен софтуер на компютъра, а всъщност нито намира, нито почиства, нито поправя каквото и да е.

Активирайте защитата от „сталкер“ софтуер и ние ще ви предупредим за всеки опит за достъп до данните ви за местоположение, вашите съобщения или други лични данни.

Можете също така да активирате защитата на stalkerware в **Настройки на заплахи и изключения** прозорец, като изберете **Откривай друг софтуер, който може да бъде използван от нарушители за повреждане на вашия компютър или лични данни** отметка.

Защита от банери

Този раздел предоставя информация как Kaspersky може за Ви защити срещу рекламни банери в Интернет.

За Защита от банери

Предлага се само в Kaspersky Standard, Kaspersky Plus и Kaspersky Premium.

Компонентът Защита от банери е проектиран да предоставя защита от банери, докато търсите в интернет. Защитата от банери блокира банерите, показвани на уеб сайтовете, които посещавате, и в интерфейса на някои приложения. Защитата от банери блокира банери от списъка с известни банери, който е вграден в базите данни на приложението Kaspersky. Може да управлявате блокирането на банери чрез интерфейса на приложението Kaspersky или директно в браузъра.

По подразбиране банери се разрешават на уеб сайтове от списъка с **Уеб сайтове на Kaspersky**. Този списък се съставя от експертите на Kaspersky и включва уеб сайтове на Kaspersky и партньорски уеб сайтове, които хостват реклами на Kaspersky. Може да преглеждате този списък или да изключвате използването му, ако смятате за необходимо да блокирате банери на уеб сайтове на Kaspersky и неговите партньори.

Броячът на блокирани банери показва общия брой блокирани банери за целия сайт според това колко страници са отворени в браузъра. Ако една страница е отворена в браузъра, се броят блокирания само на тази страница на сайта. Ако няколко страници на един и същ сайт са отворени в браузъра, броят се блокираните банери на всички страници на сайта, отворени в браузъра.

Информация за работата на Защитата от банери е налична в отчетите.

Следните ограничения важат за Защитата от банери:

- Някои сайтове откриват, че рекламите на техните страници са блокирани и не показват съдържание, докато потребителят не изключи инструмента за блокиране на реклами. За да видите съдържанието на такъв сайт, трябва да добавите адреса му към изключенията.
- Ако уеб страницата, на която се намира банерът, не може да бъде определена, приложението Kaspersky не блокира този банер и не показва информация за него.
- Ако уеб страницата, на която се намира банерът, може да бъде определена, но не може да бъде съпоставена към нито една уеб страница, отворена в уеб браузъра, приложението Kaspersky блокира банера или разрешава показването му, в зависимост от информацията, която е била определена.

Приложението показва информация за банера в отчетите, но не включва тази информация в статистиката на Защита от банери, показвана в браузъра.

- Статистиката на Защитата от банери, показвана в браузъра, може да включва банери, блокирани предния път, когато са заредени уеб страниците, включително банери, блокирани преди това и заредени отново.
- Статистиката на Защитата от банери, показвана в браузъра, не включва банери, които са блокирани в динамично съдържанието на страницата, след като уеб сайтът е зареден.

Как да активирате компонента Защита от банери

Компонентът Защита от банери е деактивиран по подразбиране. Може да го активирате чрез интерфейса на приложението Kaspersky или с помощта на разширението Kaspersky Protection във Вашия браузър.

Как да активирате Защита от банери в интерфейса на приложението Kaspersky

За да активирате Защита от банери в интерфейса на приложението Kaspersky:

1. Отворете основния прозорец на приложението.
2. Щракнете върху в долната част на главния прозорец.
   Отваря се прозорецът **Настройки**.
3. Изберете раздела **Настройки на поверителността**.
4. Изберете компонента Защита от банери.
   Отваря се прозорецът **Настройки за Защитата от банери**.
5. Активирайте компонента, като щракнете превключвателя в горната част на прозореца.

Как да активирате Защита от банери в прозореца на браузъра

За да активирате Защита от банери в прозореца на браузъра:

1. Щракнете върху бутона **Kaspersky Protection** на лентата с инструменти в браузъра.
2. В падащото меню в раздела **Защита от банери** щракнете върху бутона **Включи**.

След активиране или деактивиране на Защита от банери трябва да презаредите уеб страницата в браузъра, за да влязат в сила промените.

Блокиране на банери

Защитата от банери блокира банерите на уеб сайта от списъка с известни банери, който е вграден в базите данни на приложение Kaspersky. Ако банер се показва на уеб страница дори когато Защитата от банери работи, това може да означава, че банерът не е в списъка с известни банери. Може ръчно да блокирате показването на този банер.

За да блокирате даден банер, трябва да го добавите в списъка с блокирани банери. Може да направите това директно на уеб страницата или в интерфейса на приложението Kaspersky.

Ако даден банер е на уеб сайт от списъка с уеб сайтове с разрешени банери, не може да блокирате показването на този банер.

Как да блокирате банер на уеб страница

За да блокирате банер на уеб страница:

1. Уверете се, че разширението Kaspersky Protection е инсталирано и включено в браузъра.
2. Ако Защитата от банери е изключена, включете я:
   a. Щракнете върху бутона **Kaspersky Protection** на лентата с инструменти в браузъра.
   b. В падащото меню в раздела **Защита от банери** щракнете върху бутона **Включи**.
3. Придвижете курсора на мишката над банера, който искате да блокирате и щракнете с десния бутон.
4. В контекстуалното меню, което се отваря, изберете **Добави към Защитата от банери**.
   Отваря се прозорецът **Добавете блокиран банер**.
5. В прозореца **Добавете блокиран банер** щракнете върху бутона **Добави**.
   URL адресът на банера е добавен към списъка с блокирани банери.
6. Обновете уеб страницата в браузъра, за да спрете показването на банера.

Банерът няма да се показва следващия път, когато посетите тази уеб страница.

Как да блокирате банер приложението Kaspersky:

За да блокирате банер чрез иприложението Kaspersky:

1. Отворете основния прозорец на приложението.
2. Щракнете върху в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.
3. Изберете раздела **Настройки на поверителността**.
4. Изберете компонента Защита от банери.

   Отваря се прозорецът **Настройки за Защитата от банери**.
5. Активирайте Защита от банери компонента, като щракнете превключвателя в горната част на прозореца.
6. В прозореца **Настройки за Защитата от банери** щракнете върху връзката **Блокирани банери**, за да отворите прозореца **Блокирани банери**.
7. В прозореца **Блокирани банери** щракнете върху бутон **Добави**.
8. В прозореца, който се отваря, в полето **Маска за уеб адрес (URL)** въведете адреса или маската за адреса на банера.
9. Посочете **Активен** като състояние за този банер.
10. Щракнете **OK**.

    Приложението Kaspersky ще блокира посочения банер.

Разрешаване на банери

Може да разрешите индивидуален банер и всички банери на уеб сайт, който посочите.

Как да разрешите индивидуален банер

За да разрешите индивидуален банер:

1. Отворете основния прозорец на приложението.
2. Щракнете върху в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.
3. Изберете раздела **Настройки на поверителността**.
4. Изберете компонента Защита от банери.

   Отваря се прозорецът **Настройки за Защитата от банери**.
5. Активирайте Защита от банери компонента, като щракнете превключвателя в горната част на прозореца.
6. В прозореца **Настройки за Защитата от банери** щракнете върху връзката **Уеб сайтове с разрешени банери**, за да отворите прозореца **Уеб сайтове с разрешени банери**.
7. В прозореца **Уеб сайтове с разрешени банери** щракнете върху бутон **Добави**.
8. В прозореца, който се отваря, в полето **Уеб сайт** въведете адреса или маската за адреса на банера.
9. Изберете състоянието **Активен**.
10. Щракнете **OK**.

Приложението няма да блокира посочения банер.

> Ако даден банер е добавен към списъка с разрешени банери, но банерът е в рекламен блок, чиито свойства водят до блокирането му от Защитата от банери на уеб сайта, банерът ще бъде блокиран заедно с рекламния блок.

Как да разрешите всички банери на уеб сайта

За да разрешите всички банери на уеб сайта:

1. Отворете основния прозорец на приложението.
2. Щракнете върху в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.
3. Изберете раздела **Настройки на поверителността**.
4. Изберете компонента Защита от банери.

   Отваря се прозорецът **Настройки за Защитата от банери**.
5. Активирайте Защита от банери компонента, като щракнете превключвателя в горната част на прозореца.
6. В прозореца **Настройки за Защитата от банери** щракнете върху връзката **Уеб сайтове с разрешени банери**, за да отворите прозореца **Уеб сайтове с разрешени банери**.
7. В прозореца **Уеб сайтове с разрешени банери** щракнете върху бутон **Добави**.
8. В прозореца, който се отваря, в полето **Уеб сайт** въведете URL адреса, например `example.com`.
9. Изберете състоянието **Активен**.
10. Щракнете **OK**.

    Уеб сайтът ще бъде добавен към списъка с уеб сайтове с разрешени банери. Kaspersky не блокира банери на уеб сайтове от този списък дори ако даден банер е добавен към списъка с блокирани банери.

Как да конфигурирате филтри на Защита от банери

За да конфигурирате филтри на Защита от банери:

1. Отворете основния прозорец на приложението.
2. Щракнете върху в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.
3. Изберете раздела **Настройки на поверителността**.
4. Изберете компонента Защита от банери.

   Отваря се прозорецът **Настройки за Защитата от банери**.
5. Активирайте Защита от банери компонента, като щракнете превключвателя в горната част на прозореца.
6. Щракнете върху връзката **Списък на филтрите**, за да отворите прозореца **Списък на филтрите**.

7. В прозореца **Списък на филтрите** конфигурирайте филтрите, ако е необходимо:

   - **Препоръчително**. Тази група включва общ филтър и филтър за език, който съответства на вашия регион. Тези филтри са включени по подразбиране.
   - **Тематични**. Тази група включва два филтъра:
     - **Социални медии**. Включете този филтър, ако искате да блокирате елементи като бутоните Like и Share на уеб сайтове в социалните мрежи.
     - **Безпокойства**. Включете този филтър, ако искате да блокирате изскачащи съобщения, прозорци и други елементи, които не принадлежат към конкретния уеб сайт.
   - **В зависимост от езика**. В тази група филтри може да изберете език. Приложението ще блокира банери на уеб сайтове на посочения език.

Как да управлявате Защита от банери в браузъра

Може да управлявате компонента Защита от банери директно в браузъра, като използвате разширението Kaspersky Protection.

Разширението Kaspersky Protection ви позволява да извършвате следните действия:

- Включване и изключване на компонента
- Преглед на статистиката за блокираните банери
- Отидете в прозореца с настройките на Защита от банери
- Вижте информация дали банерите са блокирани или не на уеб сайт, отворен в браузъра, и управлявайте показването на банери на уеб сайта

Как да управлявате компонента Защита от банери през разширението Kaspersky Protection

За да управлявате компонента Защита от банери през разширението Kaspersky Protection:

Щракнете върху бутона **Kaspersky Protection** на лентата с инструменти в браузъра.

Менюто, което се отваря, показва информация за работата на компонента и контролите на компонента.

Блокиране на нежелано инсталиране на приложение

Понякога инсталирате програма само за да разберете по-късно, че сте инсталирали още няколко приложения, които не сте поискали, заедно с това, което сте искали. Звучи познато? Тези нежелани приложения се инсталират без ваше знание и могат да ви изпращат спам с реклами или дори да променят браузъра ви по подразбиране.

Активирайте **Инструмент за блокиране на инсталирането на нежелани приложения** в раздел **Дискретност**, за да забравите за този проблем веднъж завинаги. Блокирането на нежелано инсталиране на приложения автоматично ще изчисти квадратчетата с отметки от всички допълнителни приложения, предложени за инсталиране, за да ви спести проблемите да ги премахнете ръчно.

Можете също да активирате блокирането на нежелано инсталиране на приложения в прозореца за настройки Диспечер на приложения.

За да направите това, изберете отметка **По време на инсталиране на приложения автоматично чисти квадратчетата с отметки за инсталация на допълнителен софтуер. Предупреждавай за опити за инсталиране на допълнителни програми**.

Блокирането на нежелано инсталиране на приложения може да не поддържа всички приложения, които могат да бъдат инсталирани. Ако приложение за инсталиране не се поддържа, ще бъде невъзможно да се блокира инсталирането на нежелани приложения. Списъкът с поддържани приложения за инсталиране непрекъснато се разширява от нашите експерти.

Как да промените настройките на Диспечер на приложения

Предлага се само в Kaspersky Standard, Kaspersky Plus и Kaspersky Premium.

За да промените настройките на Диспечер на приложения:

1. Отворете основния прозорец на приложението.
2. Изберете раздел **Дискретност**.
3. В блока **Инструмент за блокиране на инсталирането на нежелани приложения**, щракнете .

   Това ви отвежда до прозорец **Настройки на Диспечер на приложения**.
4. В групата настройки **Инструмент за блокиране на инсталирането на нежелани приложения**, изберете квадратче **По време на инсталиране на приложения автоматично чисти квадратчетата с отметки за инсталация на допълнителен софтуер. Предупреждавай за опити за инсталиране на допълнителни програми** с отметка, за да блокирате инсталирането на допълнителен софтуер по време на инсталиране на нови приложения. Ако са предотвратени нежелани операции по време на инсталирането на новото приложение, приложението Kaspersky ще Ви уведоми за това.

   Ако в квадратчето за **По време на инсталиране на приложения автоматично чисти квадратчетата с отметки за инсталация на допълнителен софтуер. Предупреждавай за опити за инсталиране на допълнителни програми** няма отметка, след като сте започнали да инсталирате определено приложение, блокирането на нежелано инсталиране на приложение продължава да работи по време на текущата инсталация. Отметките в квадратчетата срещу приложенията, предложени за допълнителна инсталация, са премахнати и допълнителните приложения не се инсталират. Тази функционалност ще бъде деактивирана по време на следващата инсталация. Допълнителни приложения ще бъдат инсталирани заедно с основното приложение.
5. Изберете квадратчето за отметка **Не показвай стъпки за инсталация, които може да се отнасят до реклами и оферти за инсталиране на допълнителни програми**, за да блокирате показването на стъпките на инсталацията с реклами по време на инсталация на нов софтуер на компютъра. Ако такива стъпки за инсталация са премахнати, приложението Kaspersky ще Ви уведоми за това.

Програма за премахване на рекламен софтуер

Получавате ли много досадни реклами? Приложението Kaspersky може да изтрие от Вашия компютър приложенията, които показват реклами във вашите браузъри и на вашия работен плот. В допълнение към рекламния софтуер, ние също така ще премахнем всички инструменти за автоматично набиране и подозрителни пакетиращи програми, които може да съдържат вируси и други заплахи. Активирайте **Програма за отстраняване на рекламен софтуер**, за да не виждате тези досадни реклами никога повече.

За да премахнете рекламен софтуер:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Дискретност**.
3. Включете функционалността **Програма за отстраняване на рекламен софтуер**.

Тайно хранилище

Този раздел описва как да защитавате данните с помощта на тайни хранилища.

Относно тайното хранилище

Предлага се само в Kaspersky Plus и Kaspersky Premium.

Тайните хранилища за данни са проектирани да защитават вашите поверителни данни от неразрешен достъп. *Тайното хранилище* е място за съхранение на информация на вашия компютър, което може да заключвате или отключвате с парола, която само вие знаете. Трябва да въведете паролата, за да промените файловете, съхранявани в заключено тайно хранилище. Ако сте въвели невалидна парола 10 пъти подред, достъпът до тайното хранилище за данни се блокира за един час.

Ако изгубите или забравите паролата, няма да можете да възстановите своите данни.

За да създаде тайно хранилище, приложението Kaspersky използва алгоритъма за шифроване на данни AES XTS с ефективна дължина на ключа 56 бита.

Ако на вашия компютър се използва файловата система FAT32, може да създадете тайни хранилища с размер не повече от 4 GB.

Как да преместват файлове в тайно хранилище

За да преместите файлове в тайно хранилище:

1. Отворете основния прозорец на приложението.

2. Отидете в раздела **Дискретност**.

3. В раздела **Тайно хранилище** изпълнете едно от следните:

Ако все още нямате тайно хранилище

1. Щракнете **Създаване на хранилище**.
2. В прозореца **Тайно хранилище**, щракнете **Добави** и изберете файлове в Windows Explorer или плъзнете и пуснете файлове в прозореца на приложението Kaspersky.

   Избраните файлове се появяват в прозореца **Тайно хранилище**.
3. Щракнете **Продължи**.
4. Въведете името на тайното хранилище и посочете местоположението му или използвайте стойностите по подразбиране на тези настройки.
5. Въведете размера на тайното хранилище.
6. За да можете бързо да осъществите достъп до тайното хранилище, поставете отметка в квадратчето **Създаване на пряк път на работния плот за тайното хранилище**.
7. Щракнете **Продължи**.
8. Попълнете полетата **Парола за достъп до тайното хранилище** и **Потвърждение на паролата** и щракнете върху **Продължи**.
9. Изберете какво да правите с изходните копия на файлове извън тайното хранилище:
   - За да изтриете изходни копия на файлове извън тайното хранилище, щракнете върху **Изтрий**.
   - За да запазите изходните копия на файлове извън тайното хранилище, щракнете върху **Пропусни**.
10. Щракнете **Готово**.

    Списъкът с тайни хранилища показва тайното хранилище, което току-що създадохте.
11. За да заключите тайното хранилище, щракнете върху бутона **Заключване**.

    Данните в заключеното тайно хранилище стават достъпни само след въвеждане на парола.

Ако вече имате тайно хранилище

1. Щракнете върху връзката **Вече имам тайно хранилище**, за да отворите прозореца **Тайно хранилище**.
2. В прозореца **Тайно хранилище** изберете вашата тайна папка и щракнете върху **Отключване**.
3. Въведете паролата и щракнете върху **Отвори в Windows Explorer**.
   Това отваря тайното хранилище в Windows Explorer.
4. Преместете вашите файлове в тайното хранилище.
5. Затворете прозореца на Windows Explorer.
6. В интерфейса на приложението Kaspersky, в прозореца **Тайно хранилище**, щракнете **Заключване**.

При добавяне на файлове с еднакви имена, които се различават само по главна буква, към тайното хранилище, един от файловете може да бъде недостъпен при опит за отваряне на тайното хранилище. За да избегнете загуба на данни, ви препоръчваме добавяне на такива файлове към различни тайни хранилища или смяна на имената на файлове с напълно уникални имена.

Как да осъществявате достъп до файлове, съхранявани в тайно хранилище

За достъп до файловете, съхранени в тайно хранилище:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Дискретност**.
3. В блока **Тайно хранилище** щракнете върху бутона **Вече имам тайно хранилище**.
   Отваря се прозорецът **Тайно хранилище**.
4. Щракнете върху **Отключване** до тайното хранилище.
5. Въведете паролата и щракнете върху бутона **Отвори в Windows Explorer**.

   Файлове, съхранявани в тайно хранилище, се появяват в прозореца Explorer. Можете да редактирате файловете според нуждите или да добавите нови файлове и отново да затворите тайното хранилище.

Опитът да отворите тайно хранилище, който сте преименували, може да доведе до грешка. За да избегнете това, препоръчваме да отворите тайното хранилище, което искате да преименувате, извлечете данните и създайте ново тайно хранилище с тези данни, давайки му ново име.

Понякога отварянето на тайни хранилища, създадени в други приложения на Kaspersky, може да изисква преобразуване на тайните хранилища от стария формат в новия формат. Когато се опитате да отворите тайно хранилище в интерфейса на приложението Kaspersky, приложението Kaspersky ще предложи преобразуване, ако е необходимо.

Преобразуването на тайно хранилище в новия формат може да отнеме много време в зависимост от размера на хранилището.

Ако при премахване на приложението Kaspersky, в прозореца **Запазете следните данни на компютъра за повторно използване**, на **Оперативни настройки на програмата** отметката е премахната и е поставена отметка в квадратчето **Тайно хранилище**, следващия път, когато инсталирате текущата или бъдещата версия на приложението Kaspersky, ще трябва да добавите тайните хранилища ръчно, като щракнете върху връзка **Вече имам тайно хранилище** в прозорец **Тайно хранилище**.

Унищожител за файлове

Предлага се само в Kaspersky Plus и Kaspersky Premium.

Добавена защита на лични данни се гарантира чрез защитаване на изтрита информация от неупълномощено възстановяване от хакери.

Приложението Kaspersky съдържа инструмент за изтриване на перманентни данни, който прави невъзможно възстановяването на данни с помощта на стандартни софтуерни инструменти.

Приложението Kaspersky позволява изтриването на данни без възможност да бъдат възстановени от следните носители на данни:

- Локални дискове. Изтриването е възможно, ако имат правата, необходими за писане и изтриване на данни.
- Сменяеми устройства или други устройства, които са разпознати като сменяеми (например дискети, карти с памет, USB дискове или клетъчни телефони). Данните могат да бъдат изтрити от карта с памет, ако механичната защита от презаписване е деактивирана.

Може да изтриете данните, до които може да осъществите достъп с личния си акаунт. Преди да изтриете данните, се уверете, че те не се използват от работещи приложения.

За да изтриете данните окончателно:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Дискретност**.
3. В блока **Унищожител за файлове** щракнете върху бутона **Избор на файлове**.

   Отваря се прозорецът **Унищожител за файлове**.
4. Щракнете върху бутона **Преглед** и в прозореца **Изберете файлове за изтриване**, който се отваря, изберете папката или файла, който да бъде изтрит завинаги.

   Изтриването на системни файлове и папки може да причини неизправности на операционната система.
5. В падащия списък **Метод за изтриване на данни** изберете необходимия алгоритъм за изтриване на данни.

За да изтриете данни от SSD и USB устройства, е препоръчително да приложите **Бързо изтриване (препоръчително)** или **GOST R 50739-95, Русия**. Други методи за изтриване могат да повредят SSD или USB устройството.

- **Бързо изтриване (препоръчително)**. Процесът на изтриване се състои от два цикъла на презаписване: писане на нули и псевдослучайни цифри. Основното предимство на този алгоритъм е в производителността му. Бързото изтриване предотвратява възстановяването на данни с помощта на стандартни инструменти за възстановяване.

- **GOST R 50739-95, Русия**. Алгоритъмът извършва един цикъл на презаписване с помощта на псевдослучайни цифри и защитава данните от възстановяване с често срещани инструменти. Този алгоритъм отговаря на клас на защита 2 (от 6) според класификацията на Руската държавна техническа комисия.

- **Bruce Schneier Алгоритъм**. Процесът се състои от седем цикъла на презаписване. Методът се различава от немския VSITR по отношение на последователността на презаписване. Този подобрен метод за изтриване на данни се счита за един от най-надеждните.

- **VSITR стандарт, Германия**. Извършват се седем цикъла на презаписване. Алгоритъмът се счита за надежден, но изисква значително време за изпълнение.

- **NAVSO P-5239-26 (MFM) стандарт, САЩ** и **NAVSO P-5239-26 (RLL) стандарт, САЩ**. Използват се три цикъла на презаписване. Стандартите се различават един от друг по отношение на последователността, в която презаписват информация.

- **DoD 5250.22-M стандарт, САЩ**. Алгоритъмът извършва три цикъла на презаписване. Този стандарт се използва от Министерство на отбраната на САЩ.

6. Щракнете **Изтрий**.

7. В прозореца за потвърждение на изтриването, който се отваря, щракнете върху **Изтрий**.

Файлове, използвани от приложенията на трети страни, не могат да бъдат изтрити.

Почистване на следите от активността

Предлага се само в Kaspersky Standard, Kaspersky Plus и Kaspersky Premium.

Потребителските действия на компютъра се записват в операционната система. Записва се следната информация:

- Детайли на заявки за търсене, въведени от потребители и посетени уеб сайтове
- Информация за стартирани приложения и отворени и записани файлове
- Записи в дневника за събития на Microsoft Windows
- Друга информация за потребителска активност

Нарушители и неупълномощени лица могат да успеят да получат достъп до поверителни данни, съдържащи се в информация за минали потребителски действия.

Приложението включва Съветника за почистване следите от активността, който почиства следите от потребителската активност в операционната система.

За да стартирате Съветника за почистване следите от активността:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Дискретност**.
3. В блока **Почистване за поверителност** щракнете върху бутона **Намиране на дейност**.

Съветникът се състои от серия страници (стъпки), които може да управлявате, като щраквате върху бутоните **Назад** и **Напред**. За да затворите съветника, след като приключи, щракнете върху бутона **Готово**. За да спрете Съветника във всеки етап, щракнете върху бутона **Отказ**.

Нека да прегледаме стъпките на Съветника в повече детайли.

Стартиране на Съветника

a. Изберете една от двете опции за работата на Съветника:

- **Търсене на следи от активността на потребителя**. Съветникът ще търси следи от дейностите ви на компютъра.
- **Отмяна на промените**. Съветникът ще отмени промените, които са направени преди това от Съветника за почистване следите от активността. Тази опция е налична, ако следи от активността са били премахвани преди от Съветника.

b. Щракнете върху бутона **Напред**, за да стартирате Съветника.

Търсене на следи от активност

Ако сте избрали опцията **Търсене на следи от активността на потребителя**, Съветникът извършва търсене на следи от активност на вашия компютър. Търсенето може да отнеме известно време. Когато търсенето завърши, Съветникът преминава автоматично към следващата стъпка.

Избор на действия на Почистване на следите от активността

Когато търсенето завърши, съветникът ви информира за откритите следи от активност и пита за действията, които да предприеме, за елиминиране на тези следи от активността.

За да видите действия, които са включени в група, разширете списъка на избраната група.

За да накарате Съветника да извършва определено действие, изберете съответното квадратче за отметка до действието. По подразбиране Съветникът извършва всички препоръчани и силно препоръчани действия. Ако не желаете да се извършва определено действие, махнете отметката от квадратчето до него.

Силно се препоръчва да не премахвате отметката от квадратчетата, избрани по подразбиране, тъй като това ще остави компютъра ви уязвим на заплахи.

След като определите набора от действия за Съветника, които да извърши, щракнете върху бутона **Напред**.

Почистване на следите от активността

Съветникът извършва действията, избрани по време на предишната стъпка. Почистването на следи от активност може да отнеме известно време. За да почистите определени следи от активността, може да е необходимо да рестартирате компютъра; ако е така, Съветникът ви уведомява.

Когато почистването завърши, Съветникът преминава автоматично към следващата стъпка.

Завършване на съветника

Щракнете върху бутона **Готово**, за да излезете от съветника.

Защита на личните данни в интернет

Този раздел предоставя информация как да направите сърфирането в интернет безопасно и да защитите данните си от кражба.

За защита на личните данни в интернет

Приложението Kaspersky Ви помага да защитите личните си данни от кражба:

- Пароли, потребителски имена и други данни от регистрацията
- Номера на сметки и номера на банкови карти

Приложението Kaspersky включва компоненти и инструменти, които Ви позволяват да защитите личните си данни срещу кражба от престъпници, които използват методи като например фишинг и прехващане на данни, въведени на клавиатурата.

Защита срещу фишинг се осигурява от Антифишинг, който се въвежда в компонентите Безопасно сърфиране и Защита от спам. Активирайте тези компоненти, за да гарантирате цялостна защита срещу фишинг.

Защитата срещу прехващане на данни, въведени на клавиатурата, се осигурява от Екранна клавиатура и Защитено въвеждане от клавиатурата.

Съветникът за почистване на следите от активността изчиства компютъра от цялата информация за действията на потребителя.

Безопасно плащане и Kaspersky VPN защитават данни, когато използвате услуги на интернет банкиране и да пазарувате в онлайн магазини.

За екранната клавиатура

Когато използвате интернет, вие често трябва да въведете свои лични данни или вашето потребителско име и парола. Това се случва например при регистриране на акаунт на уеб сайтове, онлайн пазаруване и интернет банкиране.

Има риск личните данни да бъдат прехванати от прехващачи или софтуер за регистриране на клавишни натискания на хардуерната клавиатура, които са програми, записващи натискане на клавишите. Инструментът Екранна клавиатура предотвратява прехващането на данни, въведени чрез клавиатурата.

Много програми, класифицирани като шпионски софтуер, могат да правят екранни снимки, които автоматично се предават към нарушител за допълнителен анализ за кражба на личните данни на потребителя. Екранна клавиатура защитава въведените лични данни от опити за прехващането им чрез екранни снимки.

Екранна клавиатура има следните функции:

- Може да щраквате върху бутоните на Екранна клавиатура с мишката.

- За разлика от хардуерните клавиатури е невъзможно да натискате няколко клавиша едновременно на Екранна клавиатура. Ето защо клавишни комбинации (като **ALT**+**F4**) изискват да щракнете върху първия клавиш (например **ALT**), след това втория клавиш (например **F4**) и след това отново първия клавиш. Второто щракване върху клавиша действа по същия начин като пускането на клавиша на хардуерната клавиатура.

- Езикът на екранната клавиатура може да се превключва чрез същия пряк път, който е посочен от настройките на операционната система за хардуерната клавиатура. За целта щракнете с десния бутон върху другия клавиш (например ако прекият път **LEFT ALT**+**SHIFT** е конфигуриран в настройките на операционната система за превключване на езика на клавиатурата, щракнете с левия бутон върху клавиш **LEFT ALT**, след което щракнете с десния бутон върху клавиша **SHIFT**).

За да гарантирате защитата на данните, въведени чрез Екранна клавиатура, рестартирайте компютъра след инсталиране на приложението Kaspersky.

Използването на Екранна клавиатура има следните ограничения:

- Екранна клавиатура предотвратява прехващането на личните данни само когато се използва с браузъри Microsoft Edge, базиран на Chromium, Mozilla Firefox или Google Chrome. Когато се използва с други браузъри, Екранна клавиатура не защитава въведените лични данни от прехващане.

- Екранна клавиатура не може да защити личните ви данни, ако уеб сайтът, изискващ въвеждането на такива данни, е хакнат, тъй като в този случай информацията се получава директно от нарушителите от уеб сайта.

- Екранна клавиатура не предотвратява екранните снимки, които се правят чрез клавиша **Print Screen** и други клавишни комбинации в настройките на операционната система.

- Приложението Kaspersky не осигурява защита срещу неразрешени снимки на екрана в Microsoft Windows 8 и 8.1 (само 64-битови), ако прозорецът на екранната клавиатура е отворен, но процесът на защитения браузър не е стартиран.

Как да отворите екранна клавиатура

Може да отворите Екранна клавиатура по следните начини:

- От лентата с инструменти на Microsoft Edge, базиран на Chromium, Mozilla Firefox или Google Chrome

- С иконата за бързо стартиране на Екранна клавиатура в полетата за въвеждане на уеб сайтове

  Може да конфигурирате показването на иконата за бързо стартиране в полетата за въвеждане на уеб сайтове.

  Когато се използва Екранна клавиатура, приложението Kaspersky деактивира опцията за автоматично попълване за полетата за въвеждане на уеб сайтове.

- Чрез натискане на комбинация от клавиши на клавиатурата

Стартиране на Екранна клавиатура от лентата с инструменти на браузъра

За да отворите Екранна клавиатура от лентата с инструменти на такива браузъри като Microsoft Edge, базиран на Chromium, Mozilla Firefox или Google Chrome:

1. Щракнете върху бутона **Kaspersky Protection** на лентата с инструменти в браузъра.
2. Изберете елемента **Екранна клавиатура** в менюто, което се отваря.

Стартиране на Екранна клавиатура с хардуерна клавиатура

За да отворите Екранна клавиатура с хардуерна клавиатура:

Натиснете прекия път **CTRL**+**ALT**+**SHIFT**+**P**.

Тази клавишна комбинация не се показва на екранната клавиатура, ако тя вече се използва от друго приложение, например Microsoft Word.

Как да конфигурирате показването на иконата на Екранна клавиатура

За да конфигурирате показването на иконата за бързо стартиране на Екранна клавиатура в полетата за въвеждане на уеб сайтове:

1. Отворете основния прозорец на приложението.
2. Щракнете върху в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.
3. Изберете раздела **Настройки на поверителността**.
4. В прозореца **Настройки на поверителността** щракнете върху бутон **Защитено въвеждане на данни**.

   Прозорецът показва настройките за защита на въвеждането на данни.
5. В блока **Екранна клавиатура** поставете отметка в квадратчето **Отваряне на виртуалната клавиатура с клавишна комбинация CTRL+ALT+SHIFT+P**.
6. Ако искате иконата за бързо стартиране на екранната клавиатура да се показва в полетата за въвеждане на всички уеб сайтове, поставете отметка в квадратчето **Показвай икона за бързо стартиране в полетата за въвеждане**.
7. Ако искате иконата за бързо стартиране на екранната клавиатура да се показва само когато са отворени уеб сайтове на специфични категории, изберете квадратчетата за отметка за категориите уеб сайтове, на които трябва да се показва иконата за бързо стартиране на екранната клавиатура в полетата за въвеждане.

   Иконата за бързо стартиране на екранната клавиатура се показва, когато се осъществява достъп до уеб сайт, който принадлежи към някоя от избраните категории.
8. Ако искате да активирате или деактивирате показването на иконата за бързо стартиране на екранната клавиатура на конкретен уеб сайт:

   a. В блока **Екранна клавиатура** щракнете върху връзката **Управление на изключения**, за да отворите прозореца **Изключения за екранна клавиатура**.

b. В долната част на прозореца щракнете върху бутона **Добави**.

c. Отваря се прозорец за добавяне на изключение за Екранна клавиатура.

d. В полето **Маска на уеб адрес** въведете уеб адреса на уеб сайт.

e. В раздела **Обхват** посочете къде искате да се показва (или да не се показва) иконата за бързо стартиране на екранната клавиатура: на посочената страница или на всички страници на уеб сайта.

f. В раздела **Икона на екранна клавиатура** посочете дали искате да се показва иконата за бързо стартиране на екранната клавиатура или не.

g. Щракнете **OK**.

Появява се посоченият уеб сайт в списъка в прозореца **Изключения за екранна клавиатура**.

Когато се осъществи достъп до посочения уеб сайт, иконата за бързо стартиране на екранна клавиатура се показва в полетата за въвеждане в съответствие с посочените настройки.

За защитата на данни, въведени от компютърна клавиатура

Защитата на въвеждането на данни на компютърна клавиатура позволява да се избегне прехващането на данни, които са въведени на уеб сайтове чрез клавиатурата. За да активирате защитата на въвеждането на данни на клавиатурата, разширението Kaspersky Protection трябва да бъде активирано в браузъра. Може да конфигурирате защита на въвеждането на данни от компютърната клавиатура на различни уеб сайтове. След като е конфигурирано Защитено въвеждане от клавиатурата, до полето, в което е поставен курсора, ще се покаже изскачащо съобщение, че Защитено въвеждане от клавиатурата е активирано. По подразбиране Защитено въвеждане от клавиатурата е активирано за всички категории уеб сайтове, с изключение на интернет комуникацията.

Ограничения за Защитено въвеждане на данни

Защитено въвеждане на данни в приложението Kaspersky има следните ограничения:

- Защитено въвеждане от клавиатурата не работи в браузъри, които работят в приложението Sandboxie.
- Защитеното въвеждане от клавиатурата не може да защити личните ви данни, ако уеб сайт, който изисква въвеждане на такива данни е хакнат, тъй като в такъв случай информацията се получава от нарушителите директно от уеб сайта. Защитено въвеждане от клавиатурата работи единствено в следните браузъри: Microsoft Edge, базиран на Chromium, Mozilla Firefox, Mozilla Firefox ESR и Google Chrome, когато разширението Kaspersky Protection е инсталирано и активирано.
- Защитата работи единствено за страници, които отговарят на следните условия:
  - Страницата е в списък с URL адреси или категория страници, които изискват Защитено въвеждане от клавиатурата.
  - Страницата се отваря в защитен браузър.
  - Страницата не е в списъка с изключения на URL адреси.
  - Страницата съдържа поле за въвеждане на парола. В същото време квадратчето за отметка **Полета за въвеждане на пароли на всички уеб сайтове** трябва да бъде отбелязано в настройките на приложението.

- За да проверите дали е поставена отметка в квадратчето, отидете в раздела **Настройки на поверителността** → **Защитено въвеждане на данни** → блок **Защитено въвеждане от клавиатурата**.

- Защитата работи единствено за полета, които отговарят на следните условия:
  - Полето за въвеждане е единичен ред и отговаря на етикета HTML <input>.
  - Полето за въвеждане не е скрито: Стойността на типа атрибут не е равна на скрит и в стиловете CSS полето за показване не е зададено на „няма“.
  - Полетата за въвеждане не са полета от тип изпращане, радиобутон, квадратче за отметка, бутон или изображение.
  - Полето за въвеждане не трябва да бъде само за четене (readOnly).
  - Полето за въвеждане трябва да бъде готово за въвеждане (получаване на фокуса).
  - Ако полето има атрибут за максимална дължина (maxlength), минималният брой символи, които могат да бъдат въведени, трябва да бъде над три.
- Защитата не работи в следните случаи:
  - Данните се въвеждат с помощта на технологията IME.
  - Полето за въвеждане не е поле за въвеждане на парола.

По време на периода след инсталиране на приложението Kaspersky, но преди рестартиране на компютъра за първи път, приложението няма да засече първия символ, въведен от потребителя (във всяко приложение).

Ако изпитвате някакви затруднения, изпратете заявка с подробно описание на проблема до екипа за техническа поддръжка на Kaspersky чрез My Kaspersky.

За инструкции относно работата с My Kaspersky вижте Помощ.

Как да конфигурирате защитата на данни, въведени от компютърната клавиатура

За да конфигурирате защитата на данни, въведени от компютърната клавиатура

1. Отворете основния прозорец на приложението.
2. Щракнете върху в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.
3. Отидете в раздела **Настройки на поверителността**.
4. Щракнете **Защитено въвеждане на данни**.

   Отваря се прозорецът **Настройки за Защитено въвеждане на данни**.
5. В долната част на прозореца в раздела **Защитено въвеждане от клавиатурата** изберете квадратчето за отметка **Защитавай данните, въведени от хардуерна клавиатура**.
6. Изберете квадратчетата за отметки за категориите уеб сайтове, на които искате да защитавате данните, които са въведени чрез клавиатурата.

7. Ако искате да включите или изключите защитата на въвеждането на данни от клавиатурата на конкретен уеб сайт:

   a. Отворете прозореца **Изключения за екранна клавиатура**, като щракнете върху връзката **Управление на изключения**.

   b. В прозореца щракнете върху бутона **Добави**.

   c. Отваря се прозорец за добавяне на изключение към Защитено въвеждане от клавиатурата.

   d. В прозореца, който се отваря, в полето **Маска на уеб адрес**, въведете адреса на уеб сайта.

   e. Изберете една от опциите за защитено въвеждане на данни на този уеб сайт (**Приложи към указаната страница** или **Приложи за целия уеб сайт**).

   f. Изберете действието, което да се извърши от Защитеното въвеждане на данни на този уеб сайт (**Защитавай** или **Не защитавай**).

   g. Щракнете **OK**.

Появява се посоченият уеб сайт в списъка в прозореца **Изключения за екранна клавиатура**. Когато се осъществи достъп до този уеб сайт, Защитеното въвеждане на данни ще бъде активно, като функционира в съответствие с настройките.

Проверка на уеб сайт за безопасност

Приложението Kaspersky позволява проверка на безопасността на уеб сайт, преди да щракнете върху връзка, за да го отворите. Уеб сайтовете се проверяват с помощта на *Сканиране на уеб адреси*.

Компонентът Сканиране на уеб адреси проверява връзките на уеб страница, отворена в Microsoft Edge, базиран на Chromium, Google Chrome или Mozilla Firefox. Приложението Kaspersky показва една от следните икони до проверената връзка:

– ако свързаната уеб страница е безопасна според Kaspersky

– ако няма информация за безопасното състояние на свързаната уеб страница

- ако според Kaspersky хакерите могат да навредят на компютъра ви или на данните ви, като използват уебстраницата, към която води връзката;

- ако според Kaspersky уебстраницата, към която води връзката, може да е заразена или хакната;

– ако свързаната уеб страница е опасна според Kaspersky
За да видите изскачащ прозорец с повече детайли за връзката, преместете показалеца на мишката към съответната икона.

По подразбиране Приложението Kaspersky проверява връзки само в резултати от търсенето. Може да активирате проверката на URL на всеки уеб сайт.

За да активирате проверката на URL на уеб сайтове:

1. Отворете основния прозорец на приложението.

2. Щракнете върху в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.

3. Изберете раздела **Настройки за защита**.

4. Щракнете **Безопасно сърфиране**.

   Отваря се прозорецът **Настройки за Безопасно сърфиране**.

5. Като щракнете върху връзката **Разширени настройки**, отворете разширените настройки в Безопасно сърфиране.

6. В блока **Сканиране на уеб адреси** поставете отметка в квадратчето **Сканирай уеб адресите**.

7. Ако искате приложението Kaspersky да сканира съдържанието на всички уеб сайтове, изберете **На всички уеб сайтове с изключение на онези, които са указани**.

8. Ако е необходимо, посочете уеб страници, които са надеждни, в прозореца **Изключения**. Отворете този прозорец, като щракнете върху връзката **Управление на изключения**. Приложението Kaspersky няма да сканира съдържанието на посочените уеб страници.

9. Ако искате Приложението Kaspersky да провери съдържанието само на специфични уеб страници:

   a. Изберете опцията **Само на указаните уеб сайтове**.

   b. Щракнете върху връзката **Конфигуриране на проверени уеб сайтове**, за да отворите прозореца **Проверени уеб сайтове**.

   c. Щракнете **Добави**.

   d. Въведете адреса на уеб страницата, чието съдържание искате да проверите.

   e. Изберете статус на проверка за уеб страницата (ако статуса е *Active*, приложението Kaspersky проверява съдържанието на уеб страницата).

   f. Щракнете **OK**.

      Посочената уеб страница се появява в списъка в прозореца **Проверени уеб сайтове**. Приложението Kaspersky проверява URL адресите на тази уеб страница.

10. За да конфигурирате разширените настройки за проверка на URL, в прозореца **Advanced settings of Safe Browsing** в раздела **Сканиране на уеб адреси** щракнете върху връзката **Конфигуриране на Сканиране на уеб адреси**, за да отворите прозореца **Сканирани уеб адреси**.

11. Ако искате приложението Kaspersky да Ви уведомява за безопасността на връзките на всички уеб страници, в раздела **Сканирани уеб адреси** изберете **Всички адреси**.

12. Ако искате приложението Kaspersky да показва информация дали дадена връзка принадлежи към конкретна категория съдържание на уеб сайт (например *Ругатни, цинизми*):

    a. Поставете отметка в квадратчето до **Показвай информация за категориите съдържание на уеб сайтове**.

    b. Изберете квадратчетата за отметка до категории съдържание на уеб сайтове коя информация трябва да се показва в коментари.

Приложението Kaspersky проверява връзки на посочените уеб страници и показва информация за категориите връзки в съответствие с избраните настройки.

Как да промените настройките на шифрованите връзки

Установяват се шифровани връзка по SSL и TLS протоколи. По подразбиране приложението Kaspersky сканира такива връзки при заявка от компонентите от защитата, като например Защита за пощата, Защита от спам, Безопасно плащане, Сканиране на уеб адреси, Поверително сърфиране, Безопасно сърфиране и Защита от банери.

За да промените настройките на шифрованите връзки:

1. Отворете основния прозорец на приложението.
2. Щракнете върху в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.
3. Отидете в раздела **Настройки за защита**.
4. В блока **Разширени настройки** щракнете върху бутона **Настройки за мрежата**.
5. В прозореца **Настройки за мрежата** отидете в раздела **Сканиране на шифровани връзки**.
6. Изберете действие, което да се извършва при свързване към уеб сайтове по шифрована връзка:

   - **Не сканирай шифровани компоненти**. Приложението Kaspersky не сканира шифровани връзки.
   - **Сканирай шифрованите връзки при заявка от защитните компоненти**. Приложението Kaspersky сканира единствено шифровани връзки при заявка от Сканиране на уеб адреси. Това действие е избрано по подразбиране.
   - **Винаги сканирай шифрованите връзки**. Приложението Kaspersky сканира винаги шифрованите връзки.

   Щракването върху връзката **Показване на сертификати** отваря прозорец със списък с надеждни сертификати, които се използват от популярни уебсайтове. Към този списък се добавят сертификати, ако щракнете върху **Add to trusted certificates and continue** в предупреждението на Kaspersky, когато посещавате уеб сайт. След като добавите сертификат към списъка, уеб сайтът се смята за доверен. Можете да добавяте или премахвате сертификати в прозореца **Доверени основни сертификати**, като използвате бутоните **Добави** и **Изтрий**.

   Ако имате няколко потребителски акаунта на вашия компютър, а един от потребителите приема новия сертификат, този сертификат се добавя и към списъка с доверени сертификати за всички други потребители.
7. Изберете действие за изпълнение, ако има грешки при сканиране на шифровани връзки:

   - **Игнориране**. Ако се избере това действие, приложението Kaspersky прекъсва връзката с уеб сайта, на който е възникнала грешка при сканиране.
   - **Питай**. Ако има грешка при сканиране на шифрована връзка с уеб сайта, приложението Kaspersky показва известие, къде може да изберете действие:

     - **Игнориране**. Приложението Kaspersky прекъсва връзката с уеб сайта, на който е възникнала грешка при сканиране.
     - **Добавяне на домейн към изключенията**. Приложението Kaspersky добавя адреса на уеб сайта към списъка с надеждни адреси. Приложението Kaspersky не сканира шифровани връзки на уеб сайтове

от списъка с надеждни адреси. Можете да преглеждате такива уеб сайтове, като щракнете върху връзката **Надеждни адреси**.

Тази опция е избрана по подразбиране.

- **Добавяне на домейн към изключенията**. Приложението Kaspersky добавя уеб сайта към списъка с надеждни адреси. Приложението Kaspersky не сканира шифровани връзки на уеб сайтове от списъка с надеждни адреси. Тези уеб сайтове се показват в прозореца **Надеждни адреси**, който може да се отвори, като щракнете върху връзката **Надеждни адреси**.

8. Кликнете върху **Надеждни адреси**, за да отворите **Надеждни адреси** прозореца и изпълнете следните действия:

   a. Щракнете върху бутона **Добави**, за да добавите уеб сайта към списъка с изключения за сканиране на шифровани връзки.

   b. Въведете името на домейна на уеб сайта в полето **Име на домейн**.

   c. Щракнете **Добави**.

   Приложението Kaspersky няма да сканира шифровани връзки с този уеб сайт. Имайте предвид, че добавянето на уеб сайт към списъка с надеждни адреси може да ограничи функционалността на сканирането на уеб сайта от защитните компоненти, като например Безопасно плащане, Сканиране на уеб адреси, Поверително сърфиране, Безопасно сърфиране и Защита от банери.

За защитена връзка към Wi-Fi мрежи

Предлага се само в Kaspersky Plus и Kaspersky Premium.

Публичните Wi-Fi мрежи могат да бъдат слабо защитени, например ако дадена Wi-Fi мрежа използва уязвим протокол за шифроване или ненадеждна парола. Когато правите покупки в интернет по несигурни Wi-Fi мрежи, вашите пароли и други поверителни данни се предават като нешифрован текст. Хакерите могат да прехванат ваши поверителни данни, като например номер на банкова карта, и да получат достъп до паричните ви средства.

За да гарантирате сигурността си при използване на несигурни Wi-Fi мрежи, можете да активирате VPN чрез специално определен сървър, разположен в посочения от Вас регион. Трафикът от уебсайта първо отива към определения сървър и едва след това се изпраща до Вашето устройство през криптирана защитена връзка.

За да използвате компонента Kaspersky VPN, трябва да стартирате Kaspersky VPN. Kaspersky VPN Secure Connection се инсталира заедно с приложението Kaspersky в план Kaspersky Plus.

Компонентът Kaspersky VPN предоставя следните предимства:

- Безопасна употреба на системи за плащане и сайтове за резервации. Нарушителите няма да могат да прехванат номера на вашата банкова карта, когато извършвате онлайн плащания, резервирате стаи в хотел или наемате коли.
- Защита на вашата секретна информация. Никой няма да може да определи IP адреса на вашия компютър или вашето местоположение.
- Защита на вашата поверителност. Никой няма да може да прехване и да прочете личната ви кореспонденция в социалните мрежи.

VPN връзката може също така да се използва за други типове мрежови връзки, като например локална интернет връзка или свързване чрез USB модем.

По подразбиране Kaspersky VPN Secure Connection не ви подканва да активирате VPN, ако се използва HTTPS протокол за свързване към уебсайт.

Промяната на региона или града Ви при посещаване на уеб сайтове на банки, системи за плащане, уеб сайтове за резервации, социални мрежи, чатове и уеб сайтове за електронна поща може да доведе до задействане на системи за предотвратяване на измами (системи, предназначени за анализиране на онлайн финансови транзакции за признаци на измамни операции).

Използването на VPN връзка може да бъде регулирано от местното законодателство. Може да използвате VPN връзката единствено по предназначение и без да нарушавате местното законодателство.

Конфигуриране на известия за уязвимости в Wi-Fi мрежи

Ако Kaspersky VPN Secure Connection не е инсталирана на вашия компютър, приложението Kaspersky показва известие за свързване към Wi-Fi мрежи и несигурно предаване на Вашата парола по Интернет. Може да разрешите или блокирате връзката и предаването на паролата в прозореца за известия.

След като сте инсталирали Kaspersky VPN Secure Connection, настройките за показване на известия при свързване към Wi-Fi мрежи и предаване на нешифровани пароли стават неактивни. Може да конфигурирате настройките на уведомяванията за връзки към Wi-Fi мрежи в Kaspersky VPN Secure Connection.

За да конфигурирате известия за уязвимости в Wi-Fi мрежи:

1. Отворете основния прозорец на приложението.
2. Щракнете върху в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.
3. Изберете раздела **Настройки за защита**.
4. Изберете компонента **Защитна стена**.

   Прозорецът показва настройките на компонента Защитна стена.
5. Изберете **Уведоми за уязвимости в Wi-Fi мрежите**, ако искате да получавате известия, когато се свързвате към уязвими Wi-Fi мрежи. Ако не желаете да получавате известия, махнете отметката от квадратчето за отметка. Достъп до това квадратче за отметка може да получите, ако Kaspersky VPN Secure Connection не е инсталирана на компютъра.
6. Щракнете върху връзката **Избор на категории** и изберете категориите уязвимости в Wi-Fi мрежите. Когато се опитате да се свържете към Wi-Fi мрежа със съответната уязвимост, приложението Kaspersky Ви уведомява за това.
7. Ако е поставена отметка в квадратчето **Уведоми за уязвимости в Wi-Fi мрежите**, може да редактирате разширените настройки за показване на известия:

   - Изберете квадратчето за отметка **Блокирай и предупреди за несигурни прехвърляния на пароли чрез Интернет**, за да блокирате всички прехвърляния на пароли в нешифрован текстови формат, когато попълвате полетата **Парола** в Интернет.

- Като щракнете върху връзката **Включи**, възстановявате стойностите по подразбиране на настройките за показване на известия за прехвърляния на пароли в нешифрована форма. Ако преди това сте блокирали показването на известия за прехвърлянето на пароли в нешифрована форма, показването на тези известия ще се възобнови.

Когато се свързвате със защитени Wi-Fi мрежи, приложението показва известие, което ви пита дали имате доверие на новата мрежа. Може да изберете една от следните опции:

- **Не, блокирайте външния достъп до компютъра**. Всички външни връзки на тази мрежа са блокирани, освен връзките, инициирани от вашето устройство. Можете да използвате интернет и да посещавате всички уеб сайтове. Други потребители в тази мрежа няма да могат да се свързват с ресурси на вашия компютър (например няма да получат достъп до съдържанието на вашите дискове, включително споделени папки).

- **Ограничи, но разреши споделения достъп**. Можете да използвате интернет и да посещавате всички уеб сайтове. На други потребители в тази мрежа няма да бъде предоставен достъп до ресурси на вашия компютър, но те ще имат достъп до ресурси, определени като споделени (например споделени папки).

- **Да, разреши цялата мрежова активност**. Всички връзки в тази мрежа ще бъдат разрешени. Можете да използвате интернет и да посещавате всички уеб сайтове. Други потребители в тази мрежа ще могат да се свързват с вашия компютър без ограничения (например те ще могат да получат достъп до съдържанието на вашите дискове).

Самоличност

Kaspersky Premium включва инструменти за защита на Вашата цифрова самоличност и специален канал за връзка с Техническата поддръжка.

Портфейл за защита на самоличността

Ако съхранявате важни документи на компютъра си, например сканирани копия на документи за самоличност със снимка, държавни документи, договори и т.н., препоръчваме да добавите такива документи към защитения портфейл. Портфейлът за защита на самоличността е криптиран файл, който изисква въвеждане на главна парола за достъп. Това гарантира сигурността на Вашите лични данни, като предотвратява достъпа на трети страни до документите.

Относно главната парола

Главната парола е единична парола, която приложението на Kaspersky използва за криптиране на Вашите данни в портфейла. Препоръчваме да използвате главна парола, която включва осем или повече знака и съдържа главни и малки букви, както и цифри и специални знаци.

От съображения за сигурност приложението Kaspersky не съхранява главната парола на Вашите устройства и не я изпраща в облачното хранилище. Препоръчваме да запомните главната парола или да я запишете и съхранявате на сигурно място, защото няма начин да възстановите забравена парола.

Относно криптирането

Приложението Kaspersky криптира данни с помощта на симетричен алгоритъм за криптиране, базиран на стандарта Разширен стандарт за криптиране (AES). Ключът се изчислява от Вашата главна парола въз основа на базираната на парола функция за извличане на ключ 2 (PBKDF2). Алгоритъмът AES се използва широко по света за защита на секретни данни. Този алгоритъм има минимални изисквания за RAM, така че Вашите данни могат да бъдат криптирани и декриптирани за няколко секунди.

Как да добавите документ към портфейла

1. Отворете основния прозорец на приложението.

2. Отидете в раздела **Идентичност**.

3. Под **Портфейл за защита на самоличността**:

   - Ако портфейлът все още не е свързан, щракнете **Изтегли**, за да изтеглите приложението Диспечер на пароли Kaspersky, ако все още не е инсталирано. Името на бутона може да бъде **Стартиране** или **Отвори** ако Диспечер на пароли Kaspersky не е конфигуриран, остарял е или е свързан с My Kaspersky акаунт, който не съответства на акаунта, към който е свързано приложението Kaspersky.

     a. За да изтеглите и инсталирате Диспечерд на пароли Kaspersky, следвайте инструкциите на Съветника за настройка.

     b. Приложението Kaspersky предлага създаване и свързване на портфейл. Следвайте инструкциите на Съветника. Когато свързвате портфейл, ще бъдете подканени да създадете главна парола.

   - Ако вече сте свързали портфейл, щракнете **Add document**.

     1. Под **Documents**, щракнете **Add document**.

     2. В падащото меню изберете Редактирай.

        - **Browse for files**. Отваря се прозорецът за разглеждане. В полето **File name** посочете пътя до изпълнимия файл на приложението и щракнете върху **Open**. Изберете категория за документа (за бързо търсене в бъдеще) и щракнете **Add**.

        - **Търсете автоматично**. Приложението търси JPEG, PNG, BMP и PDF файлове, които съдържат текст. Намерените файлове се анализират и категоризират като издадени от правителството документи за самоличност или банкови карти. Изберете документите и щракнете **Finish**.

Избраните документи се добавят към портфейла като JPEG или PDF файлове.

Как да извлечете документ от портфейла

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Идентичност**.
3. Под **Портфейл за защита на самоличността**, щракнете **Add document**.
4. Въведете Вашата главна парола.
5. Изберете един документ или задръжте Shift и щракнете, за да изберете няколко документа.
6. Добавете изключение по един от следните начини:
   - Щракнете с десния бутон, за да отворите контекстното меню на документа и изберете **Download**.
   - Кликнете ⋮ и в менюто, което се показва, изберете **Download**.
7. В **Save in folder** прозорец, посочете къде искате да запишете документа.
8. Ако е необходимо, можете да редактирате името на документа.
9. Щракнете върху бутона **Запази**.

   Документът е записан на Вашето устройство. Форматът на изтеглените файлове съответства на формата на съответните документи в портфейла (JPEG или PDF).

Засичане на отдалечен достъп

Приложенията за отдалечен достъп са законен софтуер за свързване към отдалечен компютър през мрежата. Приложенията за отдалечен достъп включват TeamViewer, LogMeIn Pro и Remotely Anywhere. Хакерите могат да използват такива приложения, за да получат контрол над Вашия компютър, да инсталират зловреден софтуер, да се представят за Вас или да започнат да Ви шпионират.

Ние ще проверим дали приложенията за отдалечен достъп са инсталирани на Вашия компютър и ще Ви помогнем да премахнете такива приложения, за да попречим на някой да получи контрол над Вашето устройство.

За да намерите приложения за отдалечен достъп на Вашия компютър:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Идентичност**.
3. В блока **Засичане на отдалечен достъп** щракнете върху бутона **Включи**.
4. Това отваря прозорец **Засичане на отдалечен достъп**; в този прозорец можете да видите кои приложения за отдалечен достъп са намерени на Вашия компютър.

   В този прозорец можете да:

   - Кликнете **Детайли** до приложението за отдалечен достъп, за да видите кратко описание на приложението.

- В падащия списък до приложението изберете **Remove** ако искате да премахнете приложението. Това ви отвежда до прозорец **Programs and Features**, където можете да премахнете съответното приложение.

- В падащия списък до приложението изберете **Ignore** ако не искате да премахнете приложението сега. Приложението се добавя към група **Hidden** и ще можете да се върнете към нея по-късно.

Търсенето на приложения за отдалечен достъп не работи, ако компонентът за предотвратяване на проникване е деактивиран.

Услуги за поддръжка в Premium

Услугите за поддръжка на Kaspersky Premium по телефона не се предлагат в някои региони. Ще можете да използвате Услугите за поддръжка на Premium само при платен абонамент.

С поддръжка Premium получавате допълнителна защита и удобство, включително приоритетен достъп, услуги за експертно инсталиране, проверка и премахване на вируси и проверка на статуса на компютъра.

Експертни услуги за инсталиране

Всеки път, когато имате проблем с инсталацията на Вашия компютър, можете да ни се обадите и експерт на Kaspersky дистанционно ще:

- стартира инсталацията чрез отдалечена връзка.
- се увери, че при напредъкът на инсталацията няма грешки.
- предостави преглед на настройките и функциите на приложението.
- ще отговори на всички Ваши въпроси относно приложението и процеса на инсталиране.
- коригира настройките на приложението според Вашите нужди.
- потвърди че приложението е инсталирано, настроено правилно и работи правилно.

Приоритетна линия за поддръжка

Приоритетен достъп до първокласен предствител за поддръжка по телефона или чат. Телефонните обаждания на клиенти са с най-висок приоритет (пропуснете реда). Предоставената програма за чат включва възможности за отдалечена помощ.

ИТ отдалечени услуги

Достъп с едно кликване за чат с първокласен представител за поддръжка с включена неограничена отдалечена помощ. Седнете и се отпуснете, докато ние отстраним проблема!

Експертна проверка и премахване на вируси

Професионално премахване на вируси и шпионски софтуер на всяко Windows устройство с инсталирано приложение Kaspersky.

Услуги за проверка на статуса на компютъра

По време на проверка на статуса, нашите експерти ще извършат многоточкова проверка, за да гарантират най-високо ниво на защита и производителност на устройството.

За да използвате услугите за поддръжка на Kaspersky Premium, обадете се на телефонния номер, определен за държавата, в която сте закупили абонамента за Kaspersky Premium.

Как да деинсталирате несъвместими приложения

Приложението Kaspersky редовно проверява ако има някакви несъвместими приложения на Вашия компютър. Тези приложения се добавят към списъка на несъвместимите приложения. Може да прегледате списъка и да решите какво да правите с несъвместимите приложения.

Препоръчва се да изтриете несъвместимите приложения от вашия компютър. В противен случай приложението Kaspersky няма да може да защити напълно Вашия компютър.

Ето някои причини защо приложение на трета страна не може да бъде съвместимо с приложението Kaspersky:

- Приложението е в конфликт със Защита на файлове.
- Приложението е в конфликт със Защитната стена.
- Приложението е в конфликт със Защитата от спам.
- Приложението смущава защитата на мрежовия трафик.
- Приложението е в конфликт с Тайно хранилище.
- Приложението е в конфликт с Kaspersky Password Manager.

Как да деинсталирате несъвместими приложения

За да премахнете несъвместими приложения:

1. Отворете основния прозорец на приложението.
2. Щракнете върху бутона **Детайли** в горната част на прозореца.

   Отваря се прозорецът **Център за уведомяване**.
3. В раздела **Препоръки** щракнете върху бутона **Показване** в реда със съобщението за откритите несъвместими приложения.

   Това отваря прозореца **Открит е несъвместим софтуер**, съдържащ списък на откритите несъвместими приложения.
4. Изберете квадратчетата за отметка до имената на несъвместимите приложение, които трябва да премахнете, и щракнете върху **Премахни**. Отстраняването се обработва чрез инструменти за отстраняване, предоставени от тези приложения. По време на процеса на премахване може да бъдете помолени да дадете съгласие за премахване или промяна на настройките, свързани с премахването на приложението.
5. Ако компютърът все още съдържа несъвместими приложения, които не могат да бъдат премахнати автоматично, се показва прозорец със списък с такива приложения. За да премахнете ръчно несъвместими приложения, щракнете върху **Изтриване ръчно**. Отваря се стандартен прозорец на операционната система със списък с инсталирани приложения. Премахнете несъвместимите приложения според инструкциите за вашата операционна система.
6. След премахване на несъвместимите приложения рестартирайте компютъра.

Използване на приложението от командния прозорец

Можете да работите с приложението Kaspersky от командния ред.

Синтаксис на командния прозорец:

```
avp.com <command> [settings]
```

За да прегледате помощта за синтаксиса в командния прозорец, въведете следната команда:

```
avp.com [ /? | HELP ]
```

Тази команда Ви позволява да получите пълен списък с команди, които са налични за управление на приложението Kaspersky през командния прозорец.

За да получите помощ за синтаксиса на конкретна команда, може да въведете една от следните команди:

```
avp.com <command> /?
avp.com HELP <command>
```

В командния прозорец може да видите приложението от папката за инсталиране на приложението или като посочите пълния път до avp.com.

Може да активирате или деактивирате регистрирането на събития на приложението (създаване на файлове със следи) от командния прозорец, ако преди това сте задали парола, за да защитите достъпа до управлението на приложението Kaspersky в прозореца с настройки на приложението.

Ако не сте задали парола в прозореца с настройки на приложението, не може да създадете парола и да активирате регистрирането на събития от командния прозорец.

Определени команди могат да бъдат изпълнение единствено от администраторски акаунт.

Свързване с екипа за техническа поддръжка

Този раздел описва начините за получаване на техническа помощ и условията, при които е достъпна.

Как да получите техническа поддръжка

Ако не откривате решение на проблема в документацията на програмата или в някой от източниците на информация за приложението, препоръчваме да се свържете с екипа за техническа поддръжка. Посетете уеб сайта за Техническа поддръжка, за да се свържете с нашите експерти, които ще отговорат на въпросите ви за инсталиране и използване на приложението.

Преди да се свържете с екипа за техническа поддръжка, прочетете правила за поддръжка.

Техническата поддръжка е налична само за потребители, които са закупили абонамент за използване на приложението. Техническата поддръжка не е налична за потребители на безплатната версия.

Събиране на информация за техническа поддръжка

След като сте уведомили специалистите от екипа за техническа поддръжка за даден проблем, те може да ви помолят да създадете отчет, който съдържа информация за вашата операционна система и да го изпратите до екипа за техническа поддръжка. Специалистите от екипа за техническа поддръжка могат също да създадат файл за проследяване. Файлът за проследяване позволява да се проследи стъпка по стъпка процесът по изпълнение на команди на приложението и да се определи етапът на работа на приложението, в който възниква грешка.

За да се предостави по-добра поддръжка по въпроси, свързани с функционирането на приложението, специалистите от екипа за техническа поддръжка може да ви помолят да промените временно настройките на приложението за отстраняване на грешки, докато върви диагностиката. За целта може да е необходимо да извършите следните действия:

- Да съберете разширена диагностична информация
- Конфигурирайте индивидуални компоненти на приложението, като промените специалните настройки, които не са достъпни през стандартния потребителски интерфейс.
- Да реконфигурирате съхраняването и изпращането на събрана диагностична информация
- Да настроите прехващане на мрежови трафик и да запишете мрежовия трафик на файл

Специалистите от екипа за техническа поддръжка ще ви дадат цялата необходима информация за изпълнение на тези действия (инструкции стъпка по стъпка, настройки за промяна, скриптове, допълнителни функции на командния ред, модули за отстраняване на грешки, специални инструменти и др.) и ще ви информират какви данни ще се събират за целите на отстраняването на грешки. След като информацията от разширената диагностика е събрана, тя се съхранява на компютъра на потребителя. Събраните данни не се изпращат автоматично на Kaspersky.

Препоръчва се да изпълнявате предходните действия единствено под ръководството на специалистите от екипа за техническа поддръжка след получаване на инструкции за това. Промяна на настройките на приложението от вас по начини, които не са описани в Помощта или не са препоръчани от специалистите в екипа за техническа поддръжка, може да причини забавяния и сривове на операционната система, намаляване на нивото на защита на вашия компютър и повреждане на наличността и целостта на обработената информация.

За съдържанието и съхранението на файлове със сервизни данни

Файлове със следи и с вторични копия се съхраняват на компютъра в нешифрована форма за срок от седем дни, след като регистрирането на данни е деактивирано. Файловете със следи и с вторични копия се изтриват окончателно след седем дни.

Файловете за проследяване се съхраняват в папката ProgramData\Kaspersky Lab.

Форматът на имената на файловете за проследяване е следният: `KAV<version number_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.log`.

Файловете за проследяване могат да съдържат поверителни данни. Може да видите съдържанието на даден файл за проследяване, като го отворите в текстов редактор (като например Notepad).

Файлове за проследяване на производителността могат да бъдат преглеждани с помощната програма Анализатор на производителността на Windows. Може да изтеглите тази програма от уеб сайта на Microsoft.

Как да активирате проследяване

Уверете се, че конфигурирате проследяването само според указанията на експерт на Kaspersky Technical Support.

За да активирате следенето на приложението и следенето на производителността:

1. Отворете основния прозорец на приложението.
2. Щракнете върху бутона в долната част на прозореца.

   Отваря се прозорецът **Поддръжка**.
3. Щракнете върху връзката **Помощни инструменти**, за да отворите прозореца **Помощни инструменти**.
4. Активирайте и конфигурирайте следите от приложението и следите от производителността според инструкциите на експерт на Kaspersky Technical Support expert.
5. За да запишете промените, щракнете върху бутона **Запази**.

Ограничения и предупреждения

Приложението Kaspersky има редица некритични оперативни ограничения.

Ограничения на работата на определени компоненти и автоматично обработване на файлове

Заразени файлове и злонамерени връзки се обработват автоматично според правила, създадени от специалисти на Kaspersky. Не може да променяте тези правила ръчно. Правилата могат да бъдат актуализирани след актуализация на базите данни и модулите на приложението. Правилата за Защитна стена, Защита на уеб камерата, Диспечер на приложения и Предотвратяване на проникване също се актуализират автоматично.

Ако е стартирано сканиране на устройство от My Kaspersky, файловете ще бъдат обработени автоматично въз основа на правилата, посочени в приложението. Файлове, открити на устройство, могат да бъдат обработени автоматично по заявка от My Kaspersky без вашето потвърждение.

Ограничения на връзката към Kaspersky Security Network

По време работата му приложението може да запита Kaspersky Security Network за информация. Ако данни от Kaspersky Security Network не мога да бъдат извлечени, приложението взема решения, базирано на локалните антивирусни бази данни.

Ограничения на функционалността на Системно наблюдение

Защитата срещу устройства за шифроване (злонамерен софтуер, които шифроват потребителски файлове) има следните ограничения:

- Системната папка Temp се използва за поддържане на тази функционалност. Ако системният диск с папката Temp няма достатъчно дисково пространство за създаване на временни файлове, защитата срещу устройства за шифроване не се осигурява. В такъв случай приложението не показва известие, че файловете не са архивирани (не се осигурява защита).

- Временните файлове се изтриват автоматично, когато затворите приложението Kaspersky или деактивирате компонента Системно наблюдение.

- В случай на аварийно прекратяване на приложението Kaspersky временните файлове не се изтриват автоматично. За да изтриете временните файлове, изчистете ръчно папката Temp. За целта отворете прозореца **Стартирай** и в полето **Отвори** напишете `%TEMP%`. Щракнете върху **OK**.

- Защита срещу шифратори се осигурява единствено за файлове, които се намират на дискове за данни, които са били форматирани с файловата система NTFS.

- Броят файлове, които могат да бъдат възстановени, не могат да надвишават 50 за един процес на шифроване.

- Общият обем на промените на файловете не може да надвишава 100 MB. Файлове с промени, които надвишават това ограничение не могат да бъдат възстановени.

- Промените на файловете, инициирани чрез мрежовия интерфейс, не са наблюдавани.

- Файлове, шифровани с EFS, не се поддържат.

- Трябва да рестартирате компютъра, за да активирате защитата срещу шифратори след инсталиране на приложението Kaspersky.

Ограничения на сканирането на шифровани връзки

Поради технически ограничения на въвеждането на алгоритми за сканиране, сканирането на шифровани връзки не поддържа някои разширения на протокола TLS 1.0 и най-новите версии (особено NPN и ALPN). Връзките чрез тези протоколи могат да бъдат ограничени. Браузъри с поддръжката на SPDY протокол използват HTTP по TLS протокол вместо SPDY дори ако сървърът, към който се установява връзката поддържа SPDY. Това не се отразява на нивото на сигурност на връзката. Ако сървърът поддържа единствено SPDY протокол и е възможно да се установи връзката чрез HTTPS протокола, приложението не наблюдава установената връзка.

Приложението не обработва трафик, предаден чрез разширения на HTTP/2 протокола.

Kaspersky предотвратява обмяната на данни по QUIC протокола. Браузърите използват стандартен транспортен протокол (TLS или SSL), независимо от това дали QUIC протоколът е активиран в браузъра или не.

Kaspersky наблюдава единствено тези защитени връзки, които може да дешифрира. Приложението не наблюдава връзки, добавени към списъка с изключения (връзка **Уеб сайтове** в прозореца **Настройки за мрежата**).

Следните компоненти извършват дешифриране и сканиране на шифрован трафик по подразбиране:

- Безопасно сърфиране;
- Безопасно плащане;
- Сканиране на уеб адреси.

Приложението Kaspersky дешифрира шифрован трафик, докато потребителят използва браузър Google Chrome, ако разширението Kaspersky Protection е деактивирано в този браузър.

Приложението Kaspersky не наблюдава трафик, ако браузърът зарежда уеб страница или елементите й от локалния кеш вместо от Интернет.

Ограничения за сканирането на шифровани връзки на The Bat клиент

Тъй като пощенският клиент The Bat използва собствено хранилище за сертификати, приложението Kaspersky идентифицира сертификата, използван за установяване на HTTPS връзка между този клиент и сървъра, като ненадежден. За да предотвратите това, конфигурирайте пощенския клиент The Bat, за да работите с локалното хранилище за сертификати на Windows.

Ограничения на изключенията за сканиране на шифровани връзки

Когато сканирате шифровани връзки с уеб сайтове, които са били добавени към изключения, някои компоненти като Защита от банери, Сканиране на уеб адреси и Поверително сърфиране могат да продължат да сканират шифровани връзки. Компонентите Безопасно плащане и Безопасно сърфиране не сканират уеб сайтове, които са били добавени към изключения.

Ограничения на Архивиране и възстановяване

Следните ограничения важат за Архивиране и възстановяване:

- Онлайн хранилището на резервни копия става недостъпно, когато се смени твърдият диск или компютърът. Посетете уеб сайта на Kaspersky Technical Support за информация как да възстановите връзката към Онлайн хранилище след смяна на хардуера.
- Редактирането на сервизни файлове на резервно хранилище може да доведе до загуба на достъп до резервно хранилище и невъзможност да възстановите данните си.
- Тъй като приложението архивира чрез системната услуга за създаване на скрити копия, офлайн файлът с данни на Outlook (.ost) не е включен в резервния набор, защото не е проектиран да бъде архивиран.

Ограничения на функционалността на Тайно хранилище

Когато тайното хранилище се създаде във файловата система FAT32, размерът на файла в тайното хранилище на диска не трябва да надвишава 4 GB.

Специфики на сканирането на паметта на ядрото за комплекти за пълен достъп в режим на Защитен браузър

Когато несигурен модул е открит в режим на Защитен браузър, се отваря нов раздел в браузър с известие за откриване на злонамерен софтуер. Ако това се случи, ви препоръчваме да затворите браузъра и да стартирате пълно сканиране на компютъра.

Специфики на защитата на данни в клипборда

Приложението Kaspersky разрешава на дадено приложение да осъществява достъп до клипборда в следните случаи:

- Приложение с активен прозорец се опитва да смени данни в клипборда. Активният прозорец е прозорецът, който използвате в момента.
- Сигурен процес на приложение се опитва да постави данни в клипборда.
- Сигурен процес на приложение или процес с активен прозорец се опитва да получи данни от клипборда.
- Процес на приложение, което преди това е поставило данни в клипборда, се опитва да получи тези данни от клипборда.

Специфики на обработването на заразен файл от компоненти на приложението

По подразбиране приложението може да изтрие заразени файлове, които не могат да бъдат дезинфектирани. Премахването по подразбиране може да се извърши при обработването на файла от такива компоненти като Предотвратяване на проникване, Защита за пощата, Защита на файлове по време на задачи за сканиране и когато Системно наблюдение открива злонамерена дейност на приложения.

Ограничения, приложими към определени компоненти в случай на инсталиране на приложението с Kaspersky Fraud Prevention for Endpoints

Работата на следните компоненти на приложението Kaspersky е ограничена в Защитен браузър, ако приложението е инсталирано заедно с Kaspersky Fraud Prevention for Endpoints:

- Безопасно сърфиране с изключение на антифишинг;
- Сканиране на уеб адреси
- Защита от банери

Специфики на работата на процеса за автоматично стартиране

Процесът за автоматично стартиране записва резултатите от работата си. Данните се записват в текстови файлове с име "kl-autorun-<date><time>.log". За да видите данните, отворете прозореца **Стартиране** и в полето **Отвори** напишете %TEMP% и щракнете върху **OK**.

Всички файлове със следи се записват в пътя до файловете с настройки, които са изтеглени по време на работа на процеса за автоматично стартиране. Данните се съхраняват за срока на работа на процеса за автоматично стартиране и се изтриват завинаги, когато този процес е прекратен. Данните не се изпращат никъде.

Ограниченията на приложението Kaspersky в Microsoft Windows 10 RS4 с активиран режим Device Guard

Работата на следната функционалност е частично ограничена:

- Защита на клипборда
- Защита на браузъра от емулатори за въвеждане от клавиатура и мишка (неправомерна смяна на самоличност за въвеждане)
- Защита от приложения за отдалечено управление
- Защита на браузъра (управление чрез API, защита от атаки, които използват опасни съобщения до прозорците на браузъра, защита от управление на опашка за съобщения)
- Евристичен анализ (емулация на стартиране на злонамерени приложения)

Ако UMCI режим е активиран в Windows, приложението Kaspersky не открива програми за блокиране на екрана.

За записване на събития в дневника за събития на Windows, които са свързани с лицензионното споразумение и Kaspersky Security Network

Събития, които включват приемане и отхвърляне на условията на лицензионното споразумение, и приемане и отхвърляне на участие в Kaspersky Security Network, се записват в дневника за събития на Windows.

Ограничения на проверки за репутация на локални адреси в Kaspersky Security Network

Връзките към локалните ресурси не се сканират в Kaspersky Security Network.

Предупреждение за приложения, които събират информация

Ако дадено приложение, което събира информация и я изпраща за обработване, е инсталирано на Вашия компютър, приложението Kaspersky може да го класифицира като злонамерен софтуер. За да избегнете това, може да изключите приложението от сканиране, като конфигурирате приложението Kaspersky, както е описано в този документ.

Предупреждение за създаване на отчет от инсталацията на приложение

Файл с отчет от инсталацията се създава, когато приложението се инсталира на компютъра. Ако инсталиране на приложение приключи с грешка, файл с отчет от инсталацията се записва и може да го изпратите до техническа поддръжка на Kaspersky Technical Support. Може да видите съдържанието на файла с отчета от инсталацията, като щракнете върху връзката в прозореца на приложението. Ако приложението е инсталирано успешно, файлът с отчета от инсталацията се изтрива незабавно от вашия компютър.

Ограничения на контрола на уеб камерата в операционната система Microsoft Windows 10 Anniversary Update (RedStone 1) операционна система

След инсталиране на приложението в операционната система Microsoft Windows 10 Anniversary Update (RedStone 1), контролът на достъпа до уеб камерата не се гарантира, докато компютърът се рестартира.

Ограничения на онлайн архивиране и възстановяване на данни от резервни копия

Не може да стартирате едновременно задачи за архивиране на Kaspersky и задача за възстановяване на данни на Kaspersky Restore Utility на същия компютър.

Ограничения на защитната стена

Защитната стена не контролира локалните връзки, които са инсталирани от контролирани приложения.

Ограничения на компонента за предотвратяване на проникване

Ако VeraCrypt е инсталирано на Вашия компютър, приложението Kaspersky може да спре, когато работи с компонента Предотвратяване на проникване. За да разрешите този проблем, надстройте VeraCrypt до версия 1.19 или по-нова.

Ограничения, когато приложението се стартира за първи пък след надстройване от Microsoft Windows 7 към Microsoft Windows 10

Ако сте надстроили Microsoft Windows 7 към Microsoft Windows 8 / 8.1 или Microsoft Windows 10 / RS1 / RS2 / RS3, приложението Kaspersky работи със следните ограничения, когато се стартира за първи път:

- Работи само Защита на файлове (защита в реално време). Други компоненти на приложението не работят.
- Самозащита на файлове и системният регистър работи. Самозащита на процеси не работи.
- Интерфейсът на приложението не е наличен, докато не рестартирате компютъра. Приложението показва известие, че някои компоненти на приложението не работят и че компютърът трябва да бъде рестартиран след завършване на адаптацията на новата операционна система.

- Налична е единствено опцията **Изход** в контекстното меню на иконата на приложението в областта за уведомяване.
- Приложението не показва известия и автоматично избира препоръчаното действие.

Предупреждение за грешка при адаптацията на драйверите на приложението, когато се надстройва операционната система от Windows 7 към Windows 10

Надстройването на Windows 7 към Windows 10 може да доведе до грешка при адаптацията на драйверите на приложението Kaspersky. Драйверите се адаптират във фонов режим, което означава, че не получавате известия за напредъка й.

Ако има грешка при адаптацията на драйверите, няма да може да използвате следните функции на приложението:

- Защитна стена
- Откриване на заплаха, когато операционната система се зарежда
- Защита на процесите на приложението с помощта на технологията Protected Process Light (PPL) на Microsoft Corporation

Може да използвате следните методи за коригиране на грешката:

- Рестартирайте компютъра и рестартирайте адаптацията на приложението от известието в Центъра за уведомяване.
- Деинсталирайте приложението и го инсталирайте отново.

Ограничения за използване на функционалността на Умно домашно наблюдение

Промяната на настройките на Ethernet мрежа в системния регистър може да накара компонентът Умно домашно наблюдение да покаже Ethernet мрежата в списъка с открити Wi-Fi мрежи и да покаже устройствата, свързани към тази мрежа.

Ограничения на сканирания трафик, изпратен по HTTPS в браузъра Mozilla Firefox

В Mozilla Firefox 58.x и по-нови версии приложението не сканира трафик, предаван с HTTPS протокол, ако промяната на настройките на браузъра е защитена с основна парола. Когато основна парола е открита в браузъра, приложението показва известие с връзка към статия в базата знания. Статията съдържа инструкции за разрешаване на този проблем.

Ако HTTPS трафикът не се наблюдава, работата на следните компоненти е ограничена:

- Безопасно сърфиране;
- Антифишинг;
- Родителски контрол;
- Защита на личните данни;
- Защита от банери;

- Защитено въвеждане на данни;
- Безопасно плащане

Ограничения на разширението Kaspersky Protection в Google Chrome и Mozilla Firefox

Разширението Kaspersky Protection не работи в Google Chrome и Mozilla Firefox, ако имате инсталирано Malwarebytes за Windows на вашия компютър.

Особени съображения при инсталиране на приложението в Microsoft Windows 7 Service Pack 0 и Service Pack 1

Когато инсталирате приложението в операционна система, която не поддържа сертификати с цифров подпис SHA256, приложението инсталира собствен сигурен сертификат.

За автоматичното тестване на функционалността на приложенията на Kaspersky

Приложенията на Kaspersky, включително приложението Kaspersky, имат специален API (интерфейс за програмиране на приложения) за автоматично тестване на функционалността на приложенията. Този API е предназначен за използване само от разработчици на Kaspersky.

Други източници на информация за приложението

Страница на приложението Kaspersky в Базата знания

База знания е раздел в уеб сайта за Техническа поддръжка.

На страницата на Knowledge в Базата знания, може да четете статии, които предоставят полезна информация, препоръки и отговори на често задавани въпроси как да закупите, инсталирате и използвате приложението.

Статиите в Базата знания могат да дадат отговори на въпроси, свързани с приложението Kaspersky и други приложения на Kaspersky. Статиите в Базата знания могат също така да съдържат новини от екипа за техническа поддръжка.

Поддръжка за приложения на Kaspersky в нашия форум

Можете да получите подкрепа от потребителите и експерти на Kaspersky в нашия форум.

Във форума можете да разглеждате съществуващи теми, да публикувате коментарите си и да създавате нови теми за дискусия и за получаване на помощ.

Мрежови настройки за взаимодействие с външни услуги

Приложението Kaspersky използва следните мрежови настройки за взаимодействие с външни услуги.

Мрежови настройки

Адрес	Описание
`activation-v2.kaspersky.com/activationservice/activationservice.svc` Протокол: `HTTPS` Порт: `443`	Активиране на приложението.

`s00.upd.kaspersky.com`
`s01.upd.kaspersky.com`
`s02.upd.kaspersky.com`
`s03.upd.kaspersky.com`
`s04.upd.kaspersky.com`
`s05.upd.kaspersky.com`
`s06.upd.kaspersky.com`
`s07.upd.kaspersky.com`
`s08.upd.kaspersky.com`
`s09.upd.kaspersky.com`
`s10.upd.kaspersky.com`
`s11.upd.kaspersky.com`
`s12.upd.kaspersky.com`
`s13.upd.kaspersky.com`
`s14.upd.kaspersky.com`
`s15.upd.kaspersky.com`
`s16.upd.kaspersky.com`
`s17.upd.kaspersky.com`
`s18.upd.kaspersky.com`
`s19.upd.kaspersky.com`
`cm.k.kaspersky-labs.com`
Протокол: `HTTPS`
Порт: `443`
	Актуализиране на базите данни и модулите на приложния софтуер.

`downloads.upd.kaspersky.com` Протокол: `HTTPS` Порт: `443`	• Актуализиране на базите данни и модулите на приложния софтуер. • Верифициране на достъпа до сървърите на Kaspersky. Ако достъпът до сървърите, използващи системен DNS, не е възможен, приложението използва публичен DNS. Това е необходимо, за да сте

	сигурни, че антивирусните бази данни са актуализирани и нивото на сигурност се поддържа за компютъра. Приложението Kaspersky използва следния списък с публични DNS сървъри в следния ред: 1. Google Public DNS (8.8.8.8). 2. Cloudflare DNS (1.1.1.1). 3. Alibaba Cloud DNS (223.6.6.6). 4. Quad9 DNS (9.9.9.9). 5. CleanBrowsing (185.228.168.168). Заявките, изпратени от приложението, могат да съдържат адреси на домейни и публичния IP адрес на потребителя, тъй като приложението установява TCP/UDP връзка с DNS сървъра. Тази информация е необходима например за валидиране на сертификата на уеб ресурс, когато се използва HTTPS. Ако Приложението Kaspersky използва публичен DNS сървър, обработката на данни се урежда от политиката за поверителност на съответната услуга. Ако искате да попречите на Приложението Kaspersky да използва публичен DNS сървър, се свържете с екипа за техническа поддръжка за частна корекция.
`touch.kaspersky.com` Протокол: `HTTP`	• Получаване на надеждно време за проверка на периода на валидност на сертификата (TLS връзка).

	• Предупреждение, че достъпът до уеб ресурс е отказан в браузъра, когато безопасното сърфиране е активирано.

`p00.upd.kaspersky.com`
`p01.upd.kaspersky.com`
`p02.upd.kaspersky.com`
`p03.upd.kaspersky.com`
`p04.upd.kaspersky.com`
`p05.upd.kaspersky.com`
`p06.upd.kaspersky.com`
`p07.upd.kaspersky.com`
`p08.upd.kaspersky.com`
`p09.upd.kaspersky.com`
`p10.upd.kaspersky.com`
`p11.upd.kaspersky.com`
`p12.upd.kaspersky.com`
`p13.upd.kaspersky.com`
`p14.upd.kaspersky.com`
`p15.upd.kaspersky.com`
`p16.upd.kaspersky.com`
`p17.upd.kaspersky.com`
`p18.upd.kaspersky.com`
`p19.upd.kaspersky.com`
`downloads.kaspersky-labs.com`
`cm.k.kaspersky-labs.com`
Протокол: `HTTP`
Порт: `80`
	Актуализиране на базите данни и модулите на приложния софтуер.

`ds.kaspersky.com` Протокол: `HTTPS` Порт: `443`	Използване на Kaspersky Security Network.

`ksn-a-stat-geo.kaspersky-labs.com`
`ksn-file-geo.kaspersky-labs.com`
`ksn-verdict-geo.kaspersky-labs.com`
`ksn-url-geo.kaspersky-labs.com`
`ksn-a-p2p-geo.kaspersky-labs.com`
`ksn-info-geo.kaspersky-labs.com`
`ksn-cinfo-geo.kaspersky-labs.com`
Протокол: `Всеки`
Порт: `443`, `1443`
	Използване на Kaspersky Security Network.

`click.kaspersky.com`
 	
`redirect.kaspersky.com`
Протокол: `HTTPS`
	Следвайте връзките от интерфейса.

Защита от кражба на самоличност

Абонаментът за Kaspersky Premium включва защита от кражба на самоличност, осигурена от Iris® Powered by Generali, глобална компания за защита от кражба на самоличност и киберсигурност.

Защитата от кражба на самоличност не е налична в някои региони. Премиум услугите, описани в този раздел, се предоставят само на собственика на абонамента. Те няма да бъдат достъпни за потребители, с които собственикът е споделил абонамент.

Услуги за защита от кражба на самоличност

Кол центърът не е наличен в някои региони.

Операторите в кол центъра за защита от кражба на самоличност работят денонощно, за да ви помогнат да възстановите откраднатата самоличност и да предотвратят допълнителните щети от такава кражба.

- Помощ при кражба или загуба на портфейл. Ще се свържем с вашата банка, за да блокираме и/или да издадем отново кредитните ви карти, а ако загубите шофьорската си книжка, социалноосигурителна карта или паспорт, ще се свържем с органите, които са издали засегнатите документи, за да започне процеса на подмяна.

- По-малко предложения за заем. Ще ви помогнем да защитите личната си информация, като намалим количеството одобрени оферти за кредитни карти, които могат да бъдат изпратени от измамници, за да откраднат вашата самоличност.

- Премахване от рекламни пощенски списъци. Ще ви помогнем да намалите броя на входящите имейли с оферти за кредитни карти и маркетингови телефонни обаждания. Такива оферти може да представляват опити на измамници да откраднат вашата самоличност.

- Защита от измами в случаите, когато е изтеглен заем на ваше име. Ако вашата самоличност е била откраднатa, можете да подадете онлайн заявка за оттегляне на всеки заем на ваше име за една година, за да бъде проверен за измама. Това ще предотврати тегленето на измамни заеми на ваше име чрез използване на откраднатата ви самоличност.

- Пълно възстановяване на загубени документи. Ако вие или вашето семейство, включено във вашата застраховка, станете жертва на кражба на самоличност или измама, специален служител ще ви помогне да възстановите личната си информация (след съставяне на полицейски протокол, пълномощно се издава на застрахователната компания и се попълва декларация за кражба на самоличност). Внимание! Достъпността на тази услуга зависи от вашия регион и приложимото законодателство.

- Разрешаване на спорове с кредитори, уведомяване и поддръжка. В региони, където е възможно, ние ще се свържем с отдела за предотвратяване на измами на вашата банка и ще им изпратим подробен доклад за всеки инцидент на измама. Ние ще следим всяко такова производство и редовно ще ви уведомяваме за резултатите от съдебните спорове със специални доклади за състоянието.

- Уведомяване на полицията и властите. Ние ще ви помогнем да се свържете с полицията и властите в случаи на присвояване на самоличност и ще изпратим доклад за присвояването до вашите кредитори.

- Помощ при кражба на информация за медицинска застраховка. В региони, където това е възможно, ако информацията за вашата медицинска застраховка е откраднатa, ние ще помогнем за решаването на проблема, ако сте неправомерно таксувани за медицински услуги или ако някой незаконно получава медицинско лечение, използвайки вашата медицинска застраховка. Ние също така ще се уверим, че

вашите медицински сметки и записи за лечение са коригирани, ако е необходимо, ще ангажираме собствен медицински персонал.

- Помощ при пътувания на дълги разстояния. Ако кражбата на самоличност се случи по време на пътуване на дълги разстояния (над 100 мили от мястото на пребиваване), ние ще Ви помогнем да закупите самолетни билети, да резервирате хотели и да наемете автомобил.

- Парично обезщетение в случай на неочаквани обстоятелства. Ако кражбата на самоличност се случи на повече от 100 мили от мястото на пребиваване, ще ви бъде предоставена парична надбавка от 500 долара. Всички разходи в рамките на тази сума ще бъдат по ваша преценка. За да използвате тази услуга, трябва да имате валидна кредитна карта. Ако не сте предоставили валидна кредитна карта и сте получили такава надбавка, сумата ще бъде таксувана на вашата кредитна организация в полза на застрахователната компания в рамките на 30 дни от датата, на която обезщетението ви е било предоставено, и вие трябва да върнете дълга към кредитната организация в рамките на 45 дни, считано от датата, на която сте получили обезщетението. След изтичане на този срок, в случай на неплащане на задължението, заплащате лихва върху сумата в размер на 1,5% месечно. Застрахователната компания си запазва правото да ви откаже парична помощ, ако нямате валидна кредитна карта.

Наличността на гореспоменатите услуги зависи от региона, в който се намирате.

Застраховка при кражба на самоличност

Като използвате застраховка при кражба на самоличност, можете да се предпазите от разходи, присъщи на възстановяването на лична информация. Позволете си да спите спокойно, сигурни в знанието, че ако личната ви информация някога бъде откраднатa или изгубена, ще получите 1 милион долара за възстановяване на откраднатата лична информация и покриване на разходите.

Застраховката за кражба на самоличност се предоставя като част от основната полица, издадена от клона на Generali в САЩ в полза на Generali Global Assistance, Inc. Изброените тук условия са само за информация и не включват всички клаузи, условия и изключения на застрахователния договор. В някои юрисдикции може да не се предоставя застрахователно покритие. Участниците в застрахователната програма трябва да посочат подробна информация за условията и обезщетенията директно в застрахователния договор. Клонът на Generali в САЩ (Ню Йорк, Ню Йорк; NAIC № 11231) работи под следните имена: Generali Assicurazioni Generali S.P.A. (клон в САЩ) в Калифорния, Assicurazioni Generali – клон в САЩ, Колорадо, Generali U.S., клон DBA, Общото застрахователно дружество на Триест и Венеция в Орегон и Общото застрахователно дружество на Триест и Венеция – клон в САЩ, Вирджиния. Клонът на Generali в САЩ е допуснат или лицензиран да прави бизнес във всички щати и окръг Колумбия.

Достъпността на гореспоменатите функции зависи от региона. Можете да ги използвате само с платен абонамент.

Помощ за предотвратяване на измами

Измамниците използват различни методи, за да откраднат парите ви. Те може да ви изпращат фалшиви фактури или да ви помолят да платите за фалшива онлайн поръчка. Ако се съмнявате дали конкретна оферта е легитимна, можете да ни се обадите и ние ще направим проверка.

Предотвратяването на и помощта при измами включват:

- ScamAssist. Ако получите съобщение или оферта, която изглежда подозрителна или твърде хубава, за да бъде истина, служителите на ScamAssist ще анализират съобщението или офертата и ще ви предупредят,

ако се установи, че са фалшиви, като по този начин ще предотврати кражбата на вашите пари и лична информация.

Доставчикът на застрахователни услуги не носи отговорност за наличието, сигурността, точността и ефективността на специфични методи, продукти, инструменти или ресурси, използвани като част от услугата за предотвратяване на и помощ при измами. Вие поемате отговорност за използването на услугата за предотвратяване на и поддръжка при измами.

Речник

Kaspersky Security Network (KSN)

Базираната в облака база знания на Kaspersky с информация за репутацията на приложения и уеб сайтове. Използването на данни от Kaspersky Security Network гарантира по-бързи реакции на приложенията на Kaspersky на заплахи, подобрява работата на някои защитни компоненти и намалява вероятността за фалшиви тревоги.

Активиране на приложението

Превключване на приложението към изцяло функционален режим. Активирането на приложението се извършва от потребителя по време на или след инсталиране на приложението. За да активира приложението, потребителят трябва да има код за активиране.

Актуализация

Процедурата на замяна/добавяне на нови файлове (бази данни или модули на приложението), извлечени от сървърите за актуализиране на Kaspersky.

Антивирусни бази данни

Базите данни, които съдържат информация за заплахи за сигурността на компютъра, известни на Kaspersky от момента на публикуване на антивирусните бази данни. Записите в антивирусните бази данни позволяват откриване на злонамерен код в сканирани обекти. Антивирусните бази данни се създават от специалистите на Kaspersky и се актуализират на всеки час.

Архивиране и възстановяване

Създава резервни копия на данни, съхранявани на компютъра. Резервни копия се създават, за да се предотврати загубата на данни в резултат на кражба, неизправности на хардуера или хакерски атаки.

База данни със злонамерени уеб адреси

Списък с уеб адреси, чието съдържание може да се смята за опасно. Създаден от специалистите на Kaspersky, списъкът се актуализира редовно и е включен в пакета с приложения на Kaspersky.

Базата данни с фишинг връзки и фалшив обмен на криптовалута

Списък с уеб адреси, които са определени като фишинг уеб адреси от специалистите на Kaspersky. Базите данни се актуализират редовно и са част от пакета с приложения на Kaspersky.

Блокиране на обект

Отказване на достъп до обект от приложения на трети страни. Блокиран обект не може да бъде четен, изпълняван, променян или изтриван.

Вероятен спам

Съобщение, което не може еднозначно да се сметне за спам, но има няколко атрибута на спам (например някои типове имейли и рекламни съобщения).

Вероятно заразен обект

Обект, чийто код съдържа части от променен код от позната заплаха или обект, чието поведение е подобно на това на заплаха.

Вирус

Програма, която заразява други програми, като добавя своя код към тях, за да получи контрол, когато се стартират заразени файлове. Тази опростена дефиниция позволява да се идентифицира основното действие, извършвано от всеки вирус: заразяване.

Евристичен анализ

Технология за откриване на заплахи, за които все още не е добавена информация в базите данни на Kaspersky. Евристичният анализ открива обекти, чието поведение в операционната система може да представлява заплаха за сигурността. Обекти, открити от евристичния анализ, се считат за вероятно заразени. Например обект може да се счита за вероятно заразен, ако съдържа поредица от команди, които са типични за злонамерени обекти (отвори файл, пиши във файл).

Експлойт

Софтуерен код, който използва уязвимост в системата или софтуера. Експлойтите често се използват за инсталиране на злонамерен софтуер на компютъра без знанието на потребителя.

Задача

Функциите на приложението на Kaspersky са въведени под формата на задачи, като например: задача за пълно сканиране или задача за актуализация.

Заразен обект

Обект, част от чийто код напълно съвпада с част от кода на известен злонамерен софтуер. Kaspersky не препоръчва достъпа до такива обекти.

Защитен браузър

Специализиран режим на работа на стандартен браузър, предназначен за финансови дейности и онлайн пазаруване. Използването на Защитен браузър гарантира безопасността на поверителните данни, които сте въвели в уеб сайтове на банки и системи за плащане, като номера на банкови карти или пароли, използвани за онлайн банкиране, и предотвратява кражбата на активи за плащане, при онлайн плащания.

Защитни компоненти

Неделими части от приложението Kaspersky, предназначени за защита от специфични типове заплахи (например Защита от спам и Антифишинг). Всеки от компонентите е относително независим от другите и може да бъде деактивиран или конфигуриран отделно.

Карантина

Специализирано хранилище, в което приложението поставя резервни копия на файлове, които са били променени или изтрити по време на дезинфекция. Копия на файлове се съхраняват в специален формат, който не е опасен за компютъра.

Комплект за пълен достъп

Програма или набор от програми за прикриване на следи от нарушител или злонамерен софтуер в операционната система.

На операционни системи, базирани на Windows, комплект за пълен достъп обикновено се отнася за програма, която прониква в операционната система и прехваща системни функции (Windows API). Прехващане и промяна на функции на API от ниско ниво са основните методи, които позволяват на тези програми да скрият достатъчно добре присъствието си в операционната система. Комплект за пълен достъп може обикновено да маскира присъствието на всякакви процеси, папки и файлове, които се съхраняват на дисково устройство, в допълнение към ключове от регистъра, ако са описани в конфигурацията на комплекта за пълен достъп. Много комплекти за пълен достъп инсталират собствени драйвери и услуги на операционната система (те са също така „невидими“).

Компресиран файл

Компресиран изпълним файл, който съдържа програма за декомпресиране и инструкции за операционната система да го изпълни.

Маска на файл

Представяне на името на файл със заместващи знаци. Стандартните заместващи знаци, използвани в маски на файлове са * и ?, като * представлява всеки брой знаци, а ? Означава всеки единичен знак.

Модули на приложението

Файлове, включени в инсталационния пакет на Kaspersky, които са отговорни за извършването на основните задачи на съответното приложение. Конкретен модул на приложението съответства на всеки тип задача, изпълнявана от приложението (защита, сканиране, актуализации на антивирусни бази данни и приложни модули).

Надеждна група

Група, към която приложението Kaspersky задава приложение или процес в зависимост от следните критерии: наличие на цифров подпис, репутация в Kaspersky Security Network, ниво на надеждност на източника на приложението и потенциална опасност на действия, изпълнени от приложението или процеса. Според надеждната група, към която принадлежи дадено приложение, Kaspersky може да ограничи действията, които приложението може да извършва в операционната система.

В приложението Kaspersky се използват следните надеждни групи: надеждни, ниско ограничение, високо ограничение или ненадеждни.

Настройки на задача

Настройките на приложението, които са специфични за всеки тип задача.

Непознат вирус

Нов вирус, за който няма информация в базите данни. Като цяло непознатите вируси се откриват от приложението в обекти с помощта на евристичен анализ. Тези обекти се класифицират като вероятно заразени.

Несъвместимо приложение

Приложението за защита на разработчик-трета страна или приложението Kaspersky Lab не поддържа управление чрез Kaspersky.

Ниво на заплаха

Индекс, който показва вероятността дадено приложение да представлява заплаха за операционната система. Нивото на заплаха се изчислява с помощта на евристичен анализ, базиран на два типа критерии:

- Статични (като информация за изпълнимия файл на приложение: размер, дата на създаване и др.)
- Динамични, които се използват, докато се симулира работата на приложението във виртуална среда (анализ на системните повиквания на приложението)

Нивото на заплаха позволява откриване на поведение, типично за злонамерен софтуер. Колкото по-ниско е нивото на заплаха, толкова повече действия са разрешени за извършване от приложението в операционната система.

Ниво на защита

Нивото на защита е определено като предварително определена колекция от настройки за компонент на приложение.

Обекти на стартиране

Наборът програми, необходим за стартиране и правилна работа на операционната система, и софтуер, инсталиран на вашия компютър. Тези обекти се изпълняват всеки път, когато операционната система се стартира. Има вируси, които могат да заразят обекти за автоматично стартиране, което може да доведе например до блокиране на стартирането на операционната система.

Пакет с актуализации

Файлов пакет, предназначен за актуализиране на базите данни и модулите на приложенията. Приложението на Kaspersky копира пакетите от сървърите за актуализиране на Kaspersky и автоматично ги инсталира и прилага.

Програма, записваща натискане на клавишите

Програма, проектирана за скрито записване на информация за клавишите, натиснати от потребителя. Програмите, записващи натискане на клавишите, работят като прехващачи на натискане на клавиши.

Протокол

Ясно определен и стандартизиран набор от правила, които управляват взаимодействието между клиент и сървър. Добре познати протоколи и услугите, свързани с тях, включват HTTP, FTP и NNTP.

Сигурен процес

Софтуерен процес, чиито файлови операции не са ограничавани от приложението на Kaspersky в режим на защита в реално време. Когато бъде открита подозрителна дейност в сигурен процес, приложението Kaspersky премахва процеса от списъка със сигурни процеси и блокира действията му.

Сканиране на трафик

Сканиране в реално време, което използва информация от текущата (най-новата) версия на базите данни за обекти, прехвърляни с всички протоколи (например HTTP, FTP и други протоколи).

Скрипт

Малка компютърна програма или независима част от програма (функция), която, като правило, е разработена да изпълнява специфична задача. Най-често се използва с програми, които са вградени в хипертекст. Скриптовете се стартират например, когато отваряте някои уеб сайтове.

Ако защитата в реално време е активирана, приложението проследява изпълнението на скриптове, прехваща ги и ги сканира за вируси. В зависимост от резултатите от сканирането може да блокирате или разрешите изпълнението на скрипт.

Следи

Стартиране на режим на отстраняване на грешки; след като всяка команда е изпълнена, приложението спира и резултатът от тази стъпка се показва.

Софтуер за управление

Приложение, което поддържа паралелна работа на няколко операционни системи на един компютър.

Спам

Нежелани изпращания на групови имейли, най-често включващи реклами.

Стартиращ сектор на диска

Стартиращ сектор е специална област на твърдия диск, флопи диска или друго устройство за съхранение на данни на компютъра. Той съдържа информация за файловата система на диска и програма за начално зареждане, която е отговорна за стартиране на операционната система.

Съществуват редица вируси, които инфектират стартиращите сектори, т. нар. вируси на начално стартиране. Приложението на Kaspersky разрешава сканиране на стартиращи сектори за вируси и дезинфектирането им, ако е открита зараза.

Сървъри за актуализации на Kaspersky

HTTP сървъри на Kaspersky, от които се изтеглят актуализации на базите данни и софтуерните модули.

Тайно хранилище

Хранилище за данни е специално място за съхранение на данни, в което файловете се съхраняват във шифрована форма. За достъп до такива файлове е необходима парола. Тайните хранилища са предназначени за предотвратяване на неразрешен достъп до потребителски данни.

Технология iChecker

Технология, която позволява увеличаване на скоростта на сканиране за вируси, като изключва обекти, които са останали непроменени от последното сканиране, при условие, че параметрите на сканиране (базите данни и настройките) не са били променяни. Информацията за всеки файл се съхранява в специална база данни. Тази технология се използва в режимите на защита в реално време и сканиране при поискване.

Например имате архивен файл, който е сканиран от приложение на Kaspersky и със зададено състояние *незаразен*. Следващият път приложението ще пропусне този архив, освен ако не е променен или ако настройки за сканиране не са променени. Ако сте променили съдържанието на архива, като сте добавили нов обект към него, ако сте променили настройките за сканиране или сте актуализирали базите данни на приложението, архивът ще бъде сканиран отново.

Ограничения на технологията iChecker:

- Тази технология не работи с големи файлове, тъй като е по-бързо да се сканира файл, отколкото да се провери дали е бил променен от последното сканиране.
- Технологията поддържа ограничен брой формати.

Уязвимост

Недостатък в операционна система или приложение, който може да бъде използван от разработчиците на злонамерен софтуер, за да проникнат в операционната система или приложението и да нарушат целостта му. Наличието на голям брой уязвимости в операционна система я прави ненадеждна, тъй като вирусите, които проникват в нея, могат да причинят смущения в самата операционна система и инсталираните приложения.

Фалшива тревога

Ситуация, в която приложение на Kaspersky счита незаразен обект за заразен, тъй като кодът на обекта е подобен на този на вирус.

Фишинг

Вид интернет измама, която цели да се получи неоторизиран достъп до поверителни данни на потребителите.

Цифров подпис

Шифрован блок от данни, вграден в документ или приложение. Цифров подпис се използва за идентифициране на автора на документа или приложението. За да създаде цифров подпис, авторът на документа или приложението трябва да има цифров сертификат, който доказва самоличността на автора.

Цифровият подпис ви позволява да проверявате източника на данните и целостта на данните и да се защитите срещу фалшификати.

Информация за код на трета страна

Информацията за код на трета страна се съдържа във файла legal_notices.txt, в папката за инсталиране на приложението.

Бележки за търговските марки

Регистрираните търговски марки и марки за услуги са собственост на съответните им притежатели.

Adobe, Acrobat, Reader са регистрирани търговски марки или търговски марки на Adobe в САЩ и/или други държави.

Apple, macOS, App Store и Safari са търговски марки на Apple Inc., регистрирани в САЩ и други държави и региони.

Dropbox е търговска марка на Dropbox, Inc.

Google, Google Chrome, Google Play, Chromium, SPDY, YouTube и Android са търговски марки на Google LLC

Intel, Celeron и Atom са търговски марки на Intel Corporation в САЩ и/или други държави.

IOS е регистрирана търговска марка на Cisco Systems, Inc. и/или неговите филиали в САЩ и някои други държави.

Java и JavaScript са регистрирани търговски марки на Oracle и/или филиалите й.

Linux е запазена марка на Linus Torvalds, регистрирана в САЩ и други държави.

LogMeln Pro и Remotely Anywhere са търговски марки на LogMeln, Inc.

Mail.ru е търговска марка на Mail.ru LLC.

Microsoft, Windows, Windows Mail, Internet Explorer, Outlook, PowerShell, Bing, Skype са търговски марки на групата компании Microsoft.

Mozilla, Thunderbird и Firefox са търговски марки на Mozilla Foundation.

VMware е регистрирана търговска марка на VMware, Inc. в САЩ и/или други юрисдикции.

Списък на услугите, на които се изпраща паролата при сканирането на QR код

Когато сканирате QR код на Android, парола за еднократна употреба за активиране на приложението на вашия смартфон е изпратена в Google Play и AppsFlyer.

Прозорец на Надстройване

Пробна версия

Връзката започва превключването към пробния абонамент.

Купи код за активиране

Щракването върху този бутон ще ви отведе до онлайн магазин във вашия браузър, където може да закупите абонамент.

Въведете код за активиране

За да стартирате съветника за активиране на приложението, щракнете върху тази връзка.

Прозорец на Надстройване

Купи код за активиране

Щракнете върху тази връзка, за да насочите браузъра си към уебсайта на онлайн магазина, където можете да закупите абонамент за приложението, към което преминавате.

Въведете код за активиране

За да стартирате съветника за активиране на приложението, щракнете върху тази връзка.

Пробна версия

Щракнете върху бутона, за да превключите на пробна версия на различно приложение.

Активиране на приложението с резервен код за активиране

За да приложите нов код за активиране, щракнете върху бутона **Напред**.

Ако лицензът все още не е изтекъл, може да приложите код за активиране, който е използван преди това за активиране на приложението на друг компютър.

За да откажете активиране на приложението, щракнете върху връзката **Отказ**.

Отказ

За да отмените използването на нов код за активиране и да се върнете към прозореца **Лицензиране**, щракнете върху тази връзка.

Прозорец Въведете код за активиране

Полета за въвеждане на код за активиране на приложение

Може да сте получили код за активиране по имейл или в офлайн магазин. Код за активиране се състои от четири групи символи (например **ABA9C-CDEFG-ABCBC-ABC2D**).

Възобновяване на абонамента от вашия акаунт

Щракването върху тази връзка отваря прозорец с формуляра, който ви позволява да свържете устройството си с акаунта My Kaspersky, за да активирате абонамент, който се съхранява в акаунта.

Къде мога да открия код за активиране?

Щракването върху връзката **Къде мога да открия код за активиране?** отваря прозорец на браузъра с подробна информация за активирането на приложението с помощта на код за активиране.

Купуване на абонамент

Щракнете върху тази връзка, за да отворите прозорец на браузъра с eStore, където може да закупите абонамент.

Активирай

Щракнете върху този бутон, за да започнете да активирате приложението, като използвате въведения код за активиране.

Кодът за активиране е валиден за друга програма

Този прозорец се отваря, ако въведеният код за активиране е предназначен за друго приложение. Може да започнете да използвате това приложение сега или след изтичане на Вашия абонамент за приложението Kaspersky.

Отказ

За да откажете активиране на приложение, щракнете върху тази връзка.

Продължи

Щракването върху този бутон стартира инсталирането и активирането на приложението, на което съответства въведения код за активиране.

Информация за категориите уеб сайтове

Може да видите описания на категориите уеб сайтове, като последвате връзката.

Как да конфигурирате DNS по HTTPS защита

Когато пишете име на уеб сайта в адресната лента, браузърът изпраща вашата заявка към DNS сървър. DNS сървърът определя IP адреса на заявения уеб сайт. Данните се предават от вашия компютър към DNS сървъра с помощта на обикновен нешифрован текстов протокол. Нарушителите могат да прехванат информация за уеб сайтовете, които посещавате и да злоупотребят с нея. За да предотвратите това, тази информация трябва да бъде предадена по защитен HTTPS протокол. Сървърът, който получава и анализира такива заявки, се нарича DNS по HTTPS (или DoH) сървър.

Kaspersky автоматично получава данни кой сървър DoH се използва в браузъра Mozilla Firefox. Ако сте добавили ръчно сървър DoH в приложението Kaspersky и искате DNS данните да се предават чрез този сървър DoH, трябва да добавите този сървър към настройките на Вашия браузър Mozilla Firefox. За информация за конфигурирането на DoH сървър вижте Помощта на Mozilla Firefox.

Добавяне на сървър DoH

За да добавите сървър DoH:

1. Отворете основния прозорец на приложението.
2. Щракнете върху в долната част на главния прозорец.

   Отваря се прозорецът **Настройки**.
3. В раздела **Допълнително** изберете подраздела **Мрежа**.

   Отваря се прозорецът **Настройки за мрежата**.
4. В блока **Обработка на трафик** щракнете върху връзката **Управление на сървъри DoH**, за да отворите прозореца **Сървъри DoH**.
5. Щракнете **Добави**.
6. В прозореца, който се отваря, въведете името или IP адреса на сървъра DoH и щракнете върху **Добави**.

DoH е добавен към списъка.

Прозорец „Открита информация за текущия лиценз“

Да, използвай <application>

Когато е избрана тази опция, Съветникът за активиране се затваря. Приложението е в рамките на открития активен абонамент. Ако се намери абонамент за Kaspersky Standard или Kaspersky Plus, стартира съветникът за миграцията.

Не, продължи със съветника. Ще въведа нов код за активиране

Ако изберете тази опция, Съветникът за активиране продължава да работи и активира приложението. Ще трябва да въведете нов код за активиране, който е валиден за това приложение.

Прозорец Регистрация

В този прозорец посочете регистрационните данни, необходими за свързване с екипа за техническа поддръжка.

Няма връзка с интернет

Този прозорец се показва, ако не успеете да активирате приложението поради проблеми с вашата интернет връзка.

Опитайте отново

Ако щракнете върху тази връзка, Съветникът за активиране се опитва отново да активира приложението. Ако проблемите с интернет връзката са временни, повторният опит може да е успешен.

Раздел Изберете къде да бъдат поставени възстановените файлове

Оригинална папка

Когато е избрана тази опция, приложението възстановява файлове в папката, в която се намират оригиналните папки към момента на създаване на резервното копие.

Посочена папка

Когато е избрана тази опция, приложението възстановява файлове в папката, посочена в полето **Избор на папка**.

Избор на папка

Полето съдържа пътя към папката, в която трябва да бъдат възстановени файловете.

Това поле е налично, ако е избрана опцията **Посочена папка**.

Преглед

Щракването върху този бутон отваря прозореца **Изберете къде да бъдат поставени възстановените файлове**. В този прозорец може да изберете папка, в която да бъдат възстановени файловете.

Този бутон е наличен, ако е избрана опцията **Посочена папка**.

Ако има конфликт с имена на файлове

Този падащ списък ви позволява да избирате действие, което да се изпълни от приложението, когато целевата папка за файла, който се възстановява, вече съдържа файл със същото име:

- **питай** – когато имената на файловете съвпадат, приложението ви подканва да изберете една от следните опции: замени файла с резервното копие, запиши двата файла или не възстановявай файла.
- **подмени файл с резервното копие** – приложението Kaspersky изтрива съществуващия файл и го заменя с файла, възстановен от резервното копие.
- **запази и двата файла** – приложението Kaspersky оставя съществуващия файл непроменен и записва файла, възстановен от резервното копие, с ново име в същата папка.
- **не възстановявай този файл** – приложението Kaspersky оставя съществуващия файл непроменен и не възстановява файла със същото име от резервното копие.

Възстанови

Щракването върху този бутон стартира процеса по възстановяване на файлове от резервни копия.

Грешка при активиране

Активирането на приложението е неуспешно. За да видите информация за проблема в базата знания, щракнете върху връзката **Причини и възможни решения**.

Причини и възможни решения

Връзката осигурява достъп до статия в базата знания с информация за причините за грешката и възможните решения.

Връзки към статии в базата знания може да не са налични за някои грешки.

Отказ

За да откажете активиране на приложение, щракнете върху тази връзка.

Преминаване към друго приложение

За да стартирате Съветника за миграция, щракнете върху бутона **Напред**. Съветникът за превключване инсталира приложението, което отговаря на въведения код за активиране (Kaspersky Standard или Kaspersky Plus).

Ако абонаментът ви за Kaspersky все още не е изтекъл, може да приложите кода за активиране за Kaspersky на друг компютър.

За да откажете миграцията към Kaspersky Standard или Kaspersky Plus, щракнете върху връзката **Cancel**.

Отказ

За да излезете от Съветника за превключване и да се върнете към предишната стъпка, щракнете върху тази връзка.

Уверете се, че кодът за активиране, който въвеждате, не е кодът за активиране за абонамент

Уверете се, че кодът за активиране, който посочвате като резервен код, не е всъщност предназначен за използване на приложението, базирано на абонамент. Плащането за използване на приложението, базирано на абонамент, се събира, когато се получава абонаментът. Ако сте получили абонамент за Kaspersky, не използвайте приложението с текущия лиценз. Вместо това активирайте приложението с код за активиране на абонамент.

Докато лицензът изтече, може да използвате вече използвания код за активиране, ца за активирате приложението на друг компютър.

Прозорец на Последователност за стартиране

Последователност за стартиране на приложение

Този списък съдържа информация за приложения, които са стартирани от избраното приложение (дъщерни приложения). По подразбиране дъщерните приложения са сортирани по часа, в който са стартирани, започвайки от най-ранното.

Стартиране

Тази колона показва часа, в който е стартирано дъщерното приложение.

ИД на процеса

Тази колона показва ИД на процеса на дъщерното приложение.

Програма

Тази колона показва името на дъщерното приложение.

Надеждна група

Тази колона показва надеждната група, към която принадлежи приложението:

- **Сигурни**. Приложението работи без ограничения, но се наблюдава от Защита на файловете.
- **Със слаби ограничения**. Приложението има забрана да осъществява достъп до лични данни и настройки на потребителя, както и да редактира всякакви публични данни. Всякакви опити да се променят системни данни или да се извършват привилегировани операции изискват разрешението на потребителя. Мрежовата активност на такива приложения е ограничена.
- **С големи ограничения**. Приложението има забрана да осъществява достъп до лични данни и настройки на потребителя, както и до всякакви публични или системни данни. Всички привилегировани операции изискват разрешението на потребителя. Мрежовата активност на такива приложения е блокирана.
- **Несигурни**. Всички дейности на такива приложения са напълно блокирани.

Раздел „Работещи“

Списък с работещи приложения

Списъкът съдържа приложения и процеси, които в момента се изпълняват на вашия компютър.

Щракнете с десния бутон на мишката, за да отворите контекстното меню на заглавна част на колона. Контекстното меню ви позволява да конфигурирате начина, по който се показват колони с допълнителна за приложения и процеси:

- Име на изпълнимия файл на приложението или процеса
- Детайли на доставчика на приложението
- ИД на процеса
- Път към изпълнимия файл на приложението
- Име на потребителя, стартирал приложението или процеса
- Време на създаване и стартиране на приложението или процеса
- Настройки за автоматично стартиране на приложение

Елементът **Възстановяване на комплекта настройки по подразбиране** ви позволява да възстановите изгледа по подразбиране на таблицата.

Щракването с десния бутон върху реда на приложение или процес отваря контекстно меню. От контекстното меню може да извършвате следните действия:

- Отваряне на прозореца **Правила за програмите**, в който може да конфигурирате правила за ограничаване на дейността на приложението.
- Показване на реда, в който процесите са стартирани в прозореца **Последователност за стартиране**.
- Преместване на приложението в друга надеждна група.
- Прилагане на настройките по подразбиране на Контрол на правата на приложението към дадено приложение.
- Прекратяване на процеса.
- Отваряне на папката, която съдържа изпълнимия файл на приложението.

Изглед

В падащия списък може да активирате показването на системните процеси и процеси, инициирани от Kaspersky:

- **Покажи системните процеси**. Ако изберете този елемент, общият списък с приложения и процеси показва процеси, които са необходими за правилното функциониране на операционната система.
- **Покажи процесите на <PRODUCT>**. Ако изберете този елемент, общият списък с приложения и процеси показва процеси, които са инициирани от Kaspersky.

В падащия списък може да изберете режим на показване за приложения и процеси:

- **Преглед като списък**. Ако изберете тази опция, приложения и процеси се показват като списък.
- **Преглед като дърво**. Ако изберете тази опция, приложения и процеси се показват йерархично, базирано на реда, в който са извикани процесите.

Програма

Тази колона показва името на приложение или процес.

Цифров подпис

Тази колона показва информация дали приложението е с цифров подпис и за притежателя на цифровия подпис.

Надеждна група

Тази колона показва надеждната група, към която принадлежи приложението. В зависимост от надеждната група, към която принадлежи приложението, колоната съдържа следните икони:

- Червена икона означава, че приложението е в група Несигурни.
- Розова икона означава, че приложението е в група С големи ограничения.
- Жълта икона означава, че приложението е в група Със слаби ограничения.
- Зелена икона означава, че приложението е в група Сигурни.
- Някои специализирани системни процеси (например System или MemCompression) не са сортирани в надеждни групи и не се контролират от Kaspersky. Такива процеси се показват като сива икона и са маркирани като „Неизвестно".

Популярност

Тази колона показва нивото на популярност на приложението сред участниците в Kaspersky Security Network (KSN). Нивото на популярност отразява броя участници в KSN, които използват приложението.

ЦП

Тази колона показва настоящата степен на консумация на ресурси на CPU от приложението или процес.

Памет

Тази колона съдържа настоящата степен на консумация на RAM памет от приложението или процеса.

Диск

Тази колона показва общата скорост на четене/писане на данни на диска от приложението или процеса.

Мрежа

Тази колона показва общата скорост на предаване на данни от приложението по мрежовия интерфейс.

Прекрати процеса

Щракването върху този бутон прекратява работата на приложението, избрано в списъка.

Раздел „Стартиращи със системата“

Списък със стартиращи със системата приложения

Този списък съдържа приложения, които се стартират при стартиране на операционната система.

Щракнете с десния бутон на мишката, за да отворите контекстното меню на заглавна част на колона. Контекстното меню ви позволява да конфигурирате начина, по който се показват колоните в таблицата. Елементът **Възстановяване на комплекта настройки по подразбиране** ви позволява да възстановите изгледа по подразбиране на таблицата.

Щракването с десния бутон върху реда на приложение или процес отваря контекстно меню. От контекстното меню може да извършвате следните действия:

- Отваряне на прозореца **Правила за програмите**, в който може да конфигурирате правила за ограничаване на дейността на приложението.
- Преместване на приложението в друга надеждна група.
- Прилагане на настройките по подразбиране на Контрол на правата на приложението към дадено приложение.
- Отваряне на папката, която съдържа изпълнимия файл на приложението.

Програма

Тази колона показва името на приложение, което стартира при стартиране на операционната система.

Статус

Тази колона показва състоянието на приложението: *Работещо* или *Спряно*.

Цифров подпис

Тази колона показва информация дали приложението е с цифров подпис и за притежателя на цифровия подпис.

Надеждна група

Тази колона показва надеждната група, към която принадлежи приложението. В зависимост от надеждната група, към която принадлежи приложението, колоната съдържа следните икони:

- Червена икона означава, че приложението е в група Несигурни.
- Розова икона означава, че приложението е в група С големи ограничения.
- Жълта икона означава, че приложението е в група Със слаби ограничения.
- Зелена икона означава, че приложението е в група Сигурни.
- Някои специализирани системни процеси (например System или MemCompression) не са сортирани в надеждни групи и не се контролират от Kaspersky. Такива процеси се показват като сива икона и са маркирани като „Неизвестно".

Популярност

Тази колона показва нивото на популярност на приложението сред участниците в Kaspersky Security Network (KSN). Нивото на популярност отразява броя участници в KSN, които използват приложението.

Последно стартиране

Тази колона показва времето на най-скорошно стартиране на приложението.

Мрежата, която сте определили като домашна, всъщност е обществена

Когато се свържете с обществена Wi-Fi мрежа, например в кафене, данните се предават без криптиране. Това означава, че Вашите пароли, потребителски имена за вход, съобщения и друга поверителна информация стават достъпни за нарушители. Вашите адреси на електронна поща могат да се използват за изпращане на нежелана поща, а информацията на страниците Ви в социалните медии може да се променя.

Домашната Wi-Fi мрежа също е застрашена. Например, протоколът WPA2 може да бъде хакнат с помощта на атака за преинсталиране на ключ (KRACK).

Когато се свързвате към която и да е Wi-Fi мрежа, винаги следвайте посочените препоръки:

1. Уверете се, че защитната стена е инсталирана и включена. Този защитен компонент сканира мрежовия трафик и предпазва Вашия компютър от мрежови атаки.

2. Защитната стена е част от следните приложения на Kaspersky: Kaspersky, Kaspersky Internet Security, Kaspersky Anti-Virus, Kaspersky Total Security, Kaspersky Security Cloud и Kaspersky Small Office Security.

3. Използвайте защитена HTTPS връзка. Уверете се, че адресната лента на Вашия браузър показва зелена или сива икона на катинар.

4. Защитете връзката си с помощта на VPN. Инсталирайте Kaspersky Secure Connection на Вашето устройство и включвайте Secure Connection всеки път, когато се свързвате с Интернет.

5. Ако използвате Windows, деактивирайте услугата за споделяне на файлове и принтери за всички обществени мрежи, към които се свързвате. За инструкции вижте Уеб сайт за поддръжка на Microsoft.

6. Ако можете, използвайте мобилни данни вместо обществени Wi-Fi мрежи.

WPS е наличен във Вашата домашна мрежа

Целта на технологията WPS е да опрости свързването на устройства към Wi-Fi мрежи. WPS може да се използва за свързване към Вашия рутер без парола. Препоръчваме да деактивирате WPS в настройките на рутера.

Интерфейсите на рутера се различават в зависимост от производителя, конкретния модел и версията на фърмуера. За да разберете настройките на рутера, вижте ръководството за потребителя за Вашия модел. Ръководството за потребителя обикновено е включено към рутера; като алтернатива можете да го изтеглите от уебсайта на производителя на устройството.

По-долу е представен пример за конфигурация за рутер TP-Link TL-WR841N.

За да деактивирате WPS:

1. Въведете IP адреса на рутера в адресната лента на Вашия браузър.

   Ще преминете към страницата за оторизация на уеб интерфейса за конфигурация на рутера. IP адресът на Вашия рутер е посочен от долната страна на устройството и в ръководството за потребителя.

2. На страницата за оторизация въведете Вашето потребителско име и парола. Ако никога не сте ги променяли, можете да ги намерите от долната страна на рутера.

3. На страницата с настройки на рутера отидете в раздел **Безжичен** → **WPS**.

4. Кликнете **Деактивиране**.

Вашата домашна мрежа не е защитена с парола

Без парола Вашата Wi-Fi мрежа е достъпна за всеки. Силната парола не позволява на другите да се свързват с Вашата мрежа. За препоръки относно създаването на силна парола вижте тази статия.

Интерфейсите на рутера се различават в зависимост от производителя, конкретния модел и версията на фърмуера. За да разберете настройките на рутера, вижте ръководството за потребителя за Вашия модел. Ръководството за потребителя обикновено е включено към рутера; като алтернатива можете да го изтеглите от уебсайта на производителя на устройството.

По-долу е представен пример за конфигурация за рутер TP-Link TL-WR841N.

За да създадете парола:

1. Въведете IP адреса на рутера в адресната лента на Вашия браузър.

   Ще преминете към страницата за оторизация на уеб интерфейса за конфигурация на рутера. IP адресът на Вашия рутер е посочен от долната страна на устройството и в ръководството за потребителя.

2. На страницата за оторизация въведете Вашето потребителско име и парола. Ако никога не сте ги променяли, можете да ги намерите от долната страна на рутера.

3. На страницата с настройки на рутера отидете на раздел **Wireless** → **Wireless Security**.

4. Изберете **WPA/WPA2 – Personal**.

5. В полешд **Wireless Password**, създайте и въведете Wi-Fi парола.

6. Кликнете **Save**.

Вашата домашна мрежа има често използван SSID

Една техника, която обикновено се използва за хакване на пароли, е така наречената Таблица дъга. Нарушителят използва подготвена Таблица дъга, която съдържа милиони възможни пароли, съответстващи на често използвани SSID. Ако Вашият SSID и парола са намерени в такава таблица, нарушителят може да използва специален софтуер за незабавно възстановяване на мрежовата парола.

За да подобрите сигурността на Вашата домашна безжична мрежа, използвайте рядко използван SSID.

> Интерфейсите на рутера се различават в зависимост от производителя, конкретния модел и версията на фърмуера. За да разберете настройките на рутера, вижте ръководството за потребителя за Вашия модел. Ръководството за потребителя обикновено е включено към рутера; като алтернатива можете да го изтеглите от уебсайта на производителя на устройството.

По-долу е представен пример за конфигурация за рутер TP-Link TL-WR841N.

За да редактирате името на Wi-Fi мрежата:

1. Въведете IP адреса на рутера в адресната лента на Вашия браузър.

   Ще преминете към страницата за оторизация на уеб интерфейса за конфигурация на рутера. IP адресът на Вашия рутер е посочен от долната страна на устройството и в ръководството за потребителя.

2. На страницата за оторизация въведете Вашето потребителско име и парола. Ако никога не сте ги променяли, можете да ги намерите от долната страна на рутера.

3. На страницата с настройки на рутера отидете на раздел **Безжичен** → **Основни настройки**.

4. В полето **Wireless Network Name**, измислете и въведете име за Вашата Wi-Fi мрежа.

5. Кликнете **Save**.

Вашата домашна мрежа използва слабо криптиране на данни

Когато използвате мрежа със слабо криптиране, нарушителите могат да прихванат Вашите данни. Ако получите съобщение за слабо криптиране, когато се свържете с домашната си мрежа, превключете типа на криптиране към по-сигурен. Безжичните мрежи обикновено използват следните типове криптиране: WEP, TKIP, WPA, WPA2 (AES/CCMP).

Основната разлика е нивото на защита, което предлагат. Препоръчваме да използвате WPA2, защото това е най-сигурния вариант.

> Интерфейсите на рутера се различават в зависимост от производителя, конкретния модел и версията на фърмуера. За да разберете настройките на рутера, вижте ръководството за потребителя за Вашия модел. Ръководството за потребителя обикновено е включено към рутера; като алтернатива можете да го изтеглите от уебсайта на производителя на устройството.

Следното е примерна конфигурация на криптиране за рутер TP-Link TL-WR841N.

За да използвате различен тип криптиране за Вашата безжична мрежа:

1. Въведете IP адреса на рутера в адресната лента на Вашия браузър.

   Ще преминете към страницата за оторизация на уеб интерфейса за конфигурация на рутера. IP адресът на Вашия рутер е посочен от долната страна на устройството и в ръководството за потребителя.

2. На страницата за оторизация въведете Вашето потребителско име и парола. Ако никога не сте ги променяли, можете да ги намерите от долната страна на рутера.

3. На страницата с настройки на рутера отидете на раздел **Wireless** → **Wireless Security**.

4. Изберете **WPA/WPA2 – Personal**.

5. В полето **Authentication Type**, изберете **WPA2-PSK**.

6. В полето **Encryption**, изберете **AES**.

7. Кликнете **Save**.

Вашата домашна мрежа използва слаба парола

Препоръчваме да използвате силни пароли за защита на личните данни и поверителна информация. Не създавайте акаунти без пароли.

Изисквания за силна парола

- Паролата трябва да е с дължина поне 8 знака. Ако използвате Windows, уверете се, че минималната дължина на паролата, конфигурирана в настройките на операционната система, е поне 8 знака.
- Паролата трябва да съдържа главни букви, малки букви, цифри, интервали и специални знаци. Например: oNQZnz$Hx2.

Паролата не трябва да съдържа

- Лична информация, която може лесно да бъде получена от други. Например име или фамилия, дата на раждане.
- Очевидни и прости думи, фрази, идиоми и поредици от знаци, които са лесни за отгатване. Например: парола, ключ, abcd, qwerty или asdfg, 1234567.

Техники за генериране на парола

- Измислете алгоритъм за съставяне на пароли. Например вземете любимото си стихотворение или известен цитат. Запишете го с малки и главни букви на латинската азбука и заменете някои от тях с подобни на вид цифри и специални знаци: @_R0s3 bY_a#y Ot#er n@mE w0u1c|_$me11 as_sVV3Et.
- Използвайте генератор на пароли. Можете да използвате Диспечера на пароли Kaspersky, за да генерирате сложни пароли, да проверите тяхната сила и да ги съхранявате сигурно. Можете също да инсталирате Kaspersky Password Manager, разширение на браузъра за автоматично попълване на полета за въвеждане на уебсайтове.

Колко често трябва да сменям паролата си?

Препоръчваме да променяте паролата си на всеки 3 месеца.

Защита на паролата

- Не разкривайте и не изпращайте паролата си на никого.
- Не оставяйте паролите си записани на лист хартия на места, където може да има други лица.
- Използвайте Диспечера на пароли или Хранилище за пароли, вградено във Вашия браузър.
- Използвайте уникална парола за всеки от Вашите акаунти. Повторното използване на пароли дава възможност на нарушител, който успее да научи паролата на един от Вашите акаунти, да получи достъп до всички останали Ваши акаунти.

Раздел „Всички приложения“

Списък с приложения

Този списък съдържа приложения, инсталирани на вашия компютър. За всяко приложение в списъка може да видите информация за състоянието, цифровия подпис, надеждната група, популярността сред потребителите на KSN и времето на тяхното най-скорошно стартиране.

Щракването два пъти върху реда на приложение или процес отваря прозореца **Правила за програмите**. В този прозорец може да конфигурирате правила за контролиране на действията на приложението.

Щракването с десния бутон върху реда на приложението отваря контекстно меню. От контекстното меню може да извършвате следните действия:

- Отваряне на прозореца **Правила за програмите**, в който може да конфигурирате разрешения за дейността на приложението.
- Разрешаване или блокиране на стартиране на приложението.
- Преместване на приложението в друга надеждна група.
- Прилагане на настройките по подразбиране на Контрол на правата на приложението към дадено приложение (настройки за нулиране на приложението).
- Премахване на приложението от списъка.
- Отваряне на папката, която съдържа изпълнимия файл на приложението.

Приложенията в списъка са включени в две групи и подгрупи. Щракването с десния бутон върху реда на групата отваря контекстно меню. От контекстното меню може да извършвате следните действия:

- Отваряне на прозореца **Правила на група**, където може да зададете разрешения по подразбиране за действия на приложения в тази група.
- Създаване на подгрупа в групата. По подразбиране към тази подгрупа се прилагат правилата, посочени за групата, към която тя принадлежи.
- Добавяне на приложение към групата. По подразбиране към това приложение се прилагат правилата, посочени за групата, към която то принадлежи.
- Приложете настройките по подразбиране на Контрол на правата на приложението към групата и всички подгрупи и приложения в тази група (нулирайте настройките на групата).
- Приложете настройките по подразбиране на всички подгрупи и приложения в групата, като запазите непроменени настройките на групата (нулирайте настройките на подгрупата и приложението).
- Изтриване на подгрупи и приложения от групата.

Програма

Тази колона показва името на приложението.

Статус

Тази колона показва състоянието на приложението: *Работещо* или *Спряно*.

Цифров подпис

Тази колона показва информация дали приложението е с цифров подпис и за притежателя на цифровия подпис.

Надеждна група

Тази колона показва надеждната група, към която принадлежи приложението. Надеждната група определя правилата за използване на приложението на компютъра: забрана или разрешаване на стартиране, достъпът на приложението до файлове и системния регистър и ограничения на мрежовата активност на приложението.

Популярност

Тази колона показва нивото на популярност на приложението сред участниците в Kaspersky Security Network (KSN). Нивото на популярност отразява броя участници в KSN, които използват приложението.

Последно стартиране

Тази колона показва времето на най-скорошно стартиране на приложението.

Прозорец Нецензурна лексика

Споразумение

Съдържа условията, на които трябва да отговорите, за да направите промени в списъка с нецензурни фрази.

Аз съм на подходяща възраст и приемам условията

Избирането на квадратчето за отметка означава приемане на условията. Ако е избрано това квадратче за отметка, списъкът с нецензурни фрази е достъпен за редактиране.

Ако отметката е премахната от това квадратче, списъкът с нецензурни фрази не е достъпен за редактиране.

Прозорец на приложения, чийто достъп до микрофона е блокиран

Този прозорец показва приложения, за които сте блокирали достъпа до уеб микрофона.

Разреши достъп до уеб микрофона

Щракването върху този бутон позволява на избраното приложението в списъка да осъществява достъп до уеб микрофона.

Прозорец на изпращане на обратна връзка

Проблем

Падащ списък, в който може да изберете категория за вашата обратна връзка. Категорията обратна връзка може да засяга проблем с уеб сайт, отворен в Защитен браузър:

- **Не го използвам**. Изберете този елемент, ако не използвате „Безопасно плащане“ или ако сте решили да се отпишете от използването на „Безопасно плащане“.
- **Уеб страницата се отваря бавно**. Изберете този елемент, ако отварянето на уеб сайта отнема по-дълго време отколкото в обичайния браузър.
- **Защитеният браузър стартира, когато не е необходимо**. Изберете този елемент, ако уеб сайтове, които не изискват използване на „Безопасно плащане“, се отварят в Защитен браузър.
- **Неуспех при удостоверяване на уеб сайта**. Изберете този елемент, ако възникват грешки при удостоверяването на уеб сайт, отворен в Защитен браузър.
- **Уеб сайтът се показва неправилно или не се отваря**. Изберете този елемент, ако уеб сайтовете не се отварят в Защитен браузър или се показват с грешки или изкривявания.
- **Грешки при потвърждаването на сертификата на уеб сайта**. Изберете този елемент, ако се появяват съобщения за грешки по време на потвърждаването на сертификатите на уеб сайтовете.
- **Не може да се направи екранна снимка, когато се изпълнява Защитен браузър**. Изберете този елемент, ако екранните снимки не се създават в Защитен браузър.
- **Грешки при въвеждане на данни от клавиатурата или от клипборда**. Изберете този елемент, ако възникнат грешки при въвеждането на данни в Защитен браузър.
- **Уеб страница, отворена в Защитен браузър, не се отпечатва**. Изберете този елемент, ако не можете да отпечатате отворена страница в уеб сайт.
- **Показва се съобщение, предупреждаващо, че не са инсталирани важни актуализации на операционната система**. Изберете този елемент, ако се покаже съобщението „Не са инсталирани важни актуализации за системата“, когато се изпълнява Защитен браузър.
- **Друг браузър работи като Защитен браузър**. Изберете този елемент, ако Защитен браузър е отворен в браузър, различен от този, в който сте го стартирали.
- **Грешки при работа**. Изберете този елемент, ако Защитеният браузър връща грешки, които не са посочени в списъка.
- **Друго**. Изберете този елемент, ако проблемът, който изпитвате, не се покрива от други елементи.

Не сте задължени да посочвате категорията обратна връзка.

Детайли

Може да използвате това поле, за да предоставите информация, която може да помогне на Kaspersky да разреши вашия проблем. Това поле е опционално.

Изпрати

Изпращане на обратна връзка до Kaspersky

Обратна връзка за работата на компонента „Безопасно плащане“ може да изпращате до 10 пъти на ден. Ако приложението не успее да изпрати вашата обратна връзка (например интернет връзката не е налична), тя ще бъде записана на вашия компютър. Обратната връзка се съхранява открито за 30 дни.

Относно използването на приложението от дете

Ако приложението Kaspersky Safe Kids е инсталирано и използвано на компютъра Ви, детето може да използва приложението Kaspersky, за да деактивира Kaspersky Safe Kids. За да избегнете това, Ви препоръчваме да защитите достъпа до настройките на Kaspersky с парола.

Ако сте влезли в операционната система с акаунт, който е свързан с детски профил в Kaspersky Safe Kids, Kaspersky спира да показва следните известия:

- Известия за новини за сигурността
- Известия за откриване на слаби настройки в операционната система
- Известия за текущото устройство, което се свързва към Wi-Fi мрежа
- Известия за устройство, което се свързва към домашна Wi-Fi мрежа
- Известия на браузъра за недостатъчно сигурна парола, въведена на уеб сайт
- Известия, които ви предупреждават, че паролата, която сте въвели на уеб сайт, вече е била въведена по-рано от вас на друг уеб сайт

Можете да разрешите известията, като изберете квадратчето за отметка **Покажи известия в акаунтите на децата** в прозореца **Настройки** → **Интерфейс**.

Разрешения

Парола предпазва следните настройки на приложенията от промяна от потребител или група. Ако е избрано квадратче за отметка, това означава, че потребителят или групата от потребители може да изпълнява избраните действия.

Конфигуриране на програмни настройки	Променете настройките на приложението в основния прозорец, прозореца **Настройки**, Центъра за уведомления и известията. Активирайте и деактивирайте следи от приложенията.
Управляване на Архивиране и възстановяване	Създавайте, променяйте и премахвайте задачи за архивиране и възстановяване.
Управление на защитата за децата	Блокирайте стартирането на Kaspersky Safe Kids с помощта на компонента Host Intrusion Prevention, излезте от приложението Kaspersky или конфигурирайте приложението Kaspersky, така че да деактивирате защитата. Когато се опитате да изтеглите, инсталирате или стартирате Kaspersky Safe Kids, не се изисква паролата.
Изход от приложението	Излезте от приложението.
Деинсталиране / промяна / възстановяване на приложението	Премахнете, променете и възстановете приложението.
Премахване на ключ	Премахнете или променете код за активиране и резервен код за активиране.
Покажи отчетите	Отидете в прозореца **Отчети**.
Дезактивиране на защитни компоненти	Деактивирайте и активирайте защитни компоненти, налични в прозореца **Настройки**.

Отстраняване на неизправности/Отмяна на промените

Този прозорец показва напредъка на коригирането на повреждането на операционната система, открито по време на анализ. Коригирането на повредата може да отнеме известно време.

Ако сте избрали **Отмяна на промените** на първа стъпка, съветникът за отстраняване на неизправности на Microsoft Windows отменя действията, избрани на предишната стъпка.

Прозорец с подробности за абонамента

Този прозорец показва следната информация за абонамента за приложение:

- Състояние на абонамент
- Брой на оставащите дни до изтичане на абонамента
- Брой устройства, обхванати от абонамента
- Дата на активиране
- Дата на изтичане на абонамент

Как да конфигурирате VPN за избран уеб сайт

За да конфигурирате VPN за избран уеб сайт:

1. Отворете основния прозорец на приложението.
2. В основния прозорец на приложението, щракнете върху бутона ☰.
3. Изберете **Настройки** → **Уеб сайтове**.
4. Щракнете върху бутона **Настройки**.

   Отваря се прозорецът **Правила за свързване към уеб сайтове**.
5. В блока **Изключения за уеб сайтове** щракнете върху бутона **Настройки**.

   Отваря се прозорецът **Изключения за уеб сайтове**.
6. Щракнете върху бутона **Добави**, за да добавите уеб сайт към списъка с изключения от настройките, които са специфични за категориите уеб сайтове.

   Отваря се прозорецът **Добави уеб сайт**.
7. Въведете адреса на уеб сайта в полето **Уеб адрес (URL)**.
8. В раздела **Действие, което да бъде започнато при достъп до уеб сайта** посочете кое действие трябва да предприеме приложението, когато посещавате този уеб сайт:

   - **Включване на VPN**. Приложението активира VPN, когато посетите посочения уебсайт. Например може да конфигурирате приложението да включва VPN, когато посещавате уеб сайта на вашата банка. Тази настройка се прилага дори ако е избрана опцията **Пропусни** в раздел **При сърфиране в незащитени уеб сайтове на банки** в прозореца **Правила за свързване към уеб сайтове**.

     a. В падащия списък **Избор на VPN сървър** изберете региона или града, през който искате да установите VPN връзка, когато посещавате този уеб сайт. Ако регионът, избран за VPN за уеб сайта, се отличава от региона или града, избран за категорията уеб сайтове, към която принадлежи уеб сайтът, връзката към него ще бъде установена пред региона или града, който е посочен за този уеб сайт, а не за категорията уеб сайтове.

     b. Изберете квадратчето за отметка **Уведоми при активиране**, ако искате да получавате известия за активиране на VPN, когато посещавате този уеб сайт.

   - **Пропусни**. Приложението не активира VPN, когато посетите посочения уебсайт.
9. Щракнете **Добави**.

Приложението не активира VPN, ако се използва HTTPS протокол за свързване към уебсайт.

Връщане към Помощ на Kaspersky VPN Secure Connection.

Как да конфигурирате VPN за категории уеб сайтове

По подразбиране Kaspersky VPN не установява защитена връзка, когато отваряте уеб сайтове в браузър. Може да конфигурирате активиране на VPN за различни категории уеб сайтове, ако Kaspersky Plus или Kaspersky Premium е инсталирано и активирано на Вашия компютър. Например може да посочите, че VPN трябва да бъде активирана, когато посещавате уеб сайтове на системи за плащане или социални мрежи.

За да конфигурирате VPN за категории уеб сайтове:

1. Отворете основния прозорец на приложението.
2. В основния прозорец на приложението, щракнете върху бутона ☰.
3. Изберете **Настройки** → **Уеб сайтове**.
4. Щракнете върху бутона **Настройки**.

   Отваря се прозорецът **Правила за свързване към уеб сайтове**.
5. Изберете категорията уеб сайтове:
   - Уеб сайтове за банкиране. Тази категория включва уеб сайтове на банки.
   - Системи за плащане. Тази категория включва уеб сайтове на системи за плащане.
   - Интернет магазини с онлайн плащане. Тази категория включва уеб сайтове на онлайн търговци с вградени системи за плащане.
   - Социални мрежи. Тази категория включва уеб сайтове на социални мрежи.
6. Изберете действие, активирано при посещаване на тази категория уеб сайтове:
   - **Включване на VPN**. Приложението ще активира VPN, когато посещавате уеб сайтове от тази категория.
   - **Питай**. Когато посещавате произволен уеб сайт от тази категория, приложението ще ви пита дали за този уебсайт трябва да бъде установена защитена връзка. В прозореца на браузъра изберете съответното действие и изберете квадратчето за отметка **Запомни моя избор за този уеб сайт**. Приложението ще извършва избраното действие всеки път, когато посещавате този уеб сайт. Ако квадратчето за отметка не е избрано, приложението запаметява избора ви за един час.
   - **Пропусни**. Приложението няма да установи защитена връзка, когато посещавате уебсайтове от тази категория.
7. Ако опцията **Включване на VPN** е избрана, в падащия списък **Избор на VPN сървър** посочете регион и град, през който искате да установите VPN връзка за тази категория уеб сайтове.
8. Изберете квадратчето за отметка **Уведоми при активиране**, ако искате да получавате известия, че се активира защитена връзка при посещаване на тази категория уеб сайтове.

По подразбиране Kaspersky VPN Secure Connection не ви подканва да активирате VPN, ако се използва HTTPS протокол за свързване към уебсайт.

Връщане към Помощ на Kaspersky VPN Secure Connection.

Предотвратяване на проникване

Разделът **Applications** показва информация за броя приложения, контролирани от Kaspersky.

Управление на приложения

Щракването върху тази връзка отваря прозореца **Управление на приложения**. В този прозорец може да посочите надеждните групи приложения, да разрешавате или блокирате стартирането на приложения и да пристъпите към конфигурирането на разрешения за избрано приложение.

Разделът **Текуща дейност** показва информация за редица работещи в момента приложения и процеси. Информация за натоварването на CPU, обема RAM памет, свободното дисково пространство и мрежовата активност се предоставя в графичен формат.

Преглед на дейност

Щракването върху тази връзка отваря прозореца **Активност на приложенията**, като се показва раздела **Работещи**. В този прозорец може да видите информация за консумацията на ресурси от всяко работещо в момента приложение или да продължите с конфигурирането на разрешения за избрано приложение.

Изключения при Предотвратяване на проникване

Изключения

Съдържа ресурси с лични данни, изключени от обхвата на защитата на предотвратяване на проникване. Ресурсът може да бъде файл, папка или ключ от системния регистър.

Ресурс

Тази колона показва името на ресурса.

Път

Тази колона показва местоположението на ресурса. Пътят може да съдържа маска.

Статус

Тази колона съдържа падащ списък с опции за състоянието на ресурсите:

- **Включи контролирането**. Ако е избрана тази опция, приложението контролира активността, специфична за този ресурс.
- **Деактивиране на контрол**. Ако е избрана тази опция, приложението не контролира активността, специфична за този ресурс.

Контролът на ресурсите може да бъде разрешаван или забраняван в падащия списък, като щракнете с левия бутон на мишката върху иконата за състояние.

Добави

Щракването върху този бутон отваря прозорец, в който може да посочите ресурса с личните данни, който добавяте към списъка.

Редактирай

Щракването върху този бутон ще отвори прозореца **Редактиране на файл или папка** / **Редактиране на ключ в регистъра**. В този прозорец можете да редактирате настройките на ресурса.

Не може да редактирате ресурси, които са били добавени към списъка по подразбиране.

Изтрий

Щракването върху този бутон премахва избрания ресурс от списъка.

Не може да изтривате ресурси, които са били добавени към списъка по подразбиране.

Раздел Общи

Раздел Общи

Описание на избраната група приложения.

Раздел Ресурси

Този раздел ви позволява да избирате системните ресурси или потребителските ресурси и да променяте правата на приложенията за достъп до тези ресурси.

Бутон 

Този бутон може да се използва за показване или скриване на панела с настройки на правилата.

Изглед

В този падащ списък може да избирате две опции за филтриране на ресурси:

- **Скрий системните приложения**. Ако тази опция е избрана, ресурсите на системните приложения са скрити от списъка с ресурси.
- **Скрий <PRODUCT>**. Ако тази опция е избрана, ресурсите на Kaspersky са скрити от списъка.

Операционна система

Този списък съдържа настройките на операционната система и ресурсите в избраната категория. Ресурс може да бъде файл, папка, ключ от регистъра, мрежова услуга или IP адрес. Предотвратяване на проникване следи достъпа, който други приложения имат до ресурсите в списъка.

По подразбиране списъкът **Операционна система** включва следните обекти:

- Ключове от регистъра, които съдържат параметри за стартиране
- Ключове от регистъра, които съдържат настройки за използване на интернет
- Ключове от регистъра, които се отразяват на сигурността на операционната система
- Ключове от регистъра, които съдържат настройки на системна услуга
- Системни файлове и папки
- Стартови папки

Лични данни

Съдържат личните данни на потребителя, сортирани по ресурси и категории. Ресурсът може да бъде файл или папка. Предотвратяване на проникване анализира действията, които други приложения изпълняват в изброените ресурси.

По подразбиране списъкът с личните данни включва следните обекти:

- Потребителски файлове (папка My Documents, файлове с бисквитки, информация за дейностите на потребителя)
- Файлове, папки и ключове от регистри, които съдържат настройките и важните данни за най-често използваните приложения: браузъри, файлови мениджъри, имейл клиенти, IM клиенти, и електронни портфейли.

Ресурс

Тази колона показва името на ресурса на операционната система, защитен от Предотвратяване на проникване.

Път

Тази колона показва местоположението на ресурса. Пътят може да съдържа маска.

Статус

Тази колона съдържа падащ списък с опции за състоянието на ресурсите:

- **Включи контролирането**. Ако е избрана тази опция, приложението контролира активността, специфична за този ресурс.
- **Деактивиране на контрол**. Ако е избрана тази опция, приложението не контролира активността, специфична за този ресурс.

Контролът на ресурсите може да бъде разрешаван или забраняван в падащия списък, като щракнете с левия бутон на мишката върху иконата за състояние.

Добави

В този падащ списък може да добавяте категория ресурси, файл или папка с ресурси или ключ от системния регистър.

Редактирай

Като щракнете върху тази връзка, ще се отвори прозорец, в който може да редактирате името на избрания ресурс и пътя до него.

Изтрий

Щракването върху тази връзка премахва избраната категория ресурси, файла или папката с ресурси или ключа от системния регистър от списъка. Предотвратяване на проникване спира да управлява достъпа на други приложения до този ресурс.

Възстанови

Този падащ списък ви позволява да изберете една от опциите:

- **настройки на категория**. Ако тази опция е избрана, на настройките на избраната категория се задават стойности по подразбиране.
- **настройки на подгрупа и ресурси**. Ако е избрана тази опция, на настройките на подгрупите и ресурсите, принадлежащи към тази категория, се задават стойности по подразбиране.

Списък с приложения

Този списък показва надеждни групи и приложения, които принадлежат към тези надеждни групи. Колоните **Четене**, **Записване**, **Създаване** и **Изтриване** посочват правата за достъп, които дадено приложение или група от приложения има за избрания ресурс.

Таблицата по-долу изброява операциите, изпълнявани от Kaspersky, когато дадено приложение или група от приложения се опитва да осъществи достъп до ресурса.

Описание на действия на Kaspersky

Действие	Описание
Наследи	Приложението или групата наследява отговора от родителската група.
Разреши	Kaspersky разрешава на приложения, включени в избраната група, да осъществяват достъп до ресурса.
Забрани	Kaspersky не разрешава на приложения, включени в избраната група, да осъществяват достъп до ресурса.
Питай потребителя	Ако е поставена отметка в квадратчето **Изпълнявай препоръчаните действия автоматично** в **Настройки → Настройки за производителност → Използване на ресурси на компютъра**, Kaspersky автоматично избира действието, което да предприеме за този ресурс, въз основа на правилата, създадени от експертите на Kaspersky. Може да последвате бележката под линия, за да прочетете точно кое действие ще бъде избрано. Ако бъде премахната отметката от квадратчето, Kaspersky пита потребителя дали да разреши на това приложение достъп до ресурса или не.
Записвай в отчет	Освен посочения отговор, Kaspersky регистрира информация за опитите на приложението да осъществи достъп до ресурса и записва информацията в отчет.

Прозорец Лицензионно споразумение

Прозорецът съдържа текста на лицензионното споразумение. Използвайте лентата за превъртане, за да прегледате лицензионното споразумение.

Прозорец на лицензиране

Подробностите за абонамента се показват в раздела в горната част на прозореца:

- Състояние на абонамент
- Брой на оставащите дни до изтичане на абонамента

Относно вашия лиценз/Относно вашия абонамент

Като щракнете върху тази връзка, ще се отвори прозорец, който предоставя информация за текущия абонамент.

Отидете в My Kaspersky

Като щракнете върху този бутон, ще се отвори страницата на My Kaspersky в браузъра по подразбиране.

Лицензионно споразумение

Като щракнете върху този бутон, ще се отвори прозорец с текста на лицензионното споразумение.

В зависимост от наличието на абонамент и от свойствата на вашата версия на приложението, прозорецът може да показва различни бутони за иницииране на действия, свързани с вашия абонамент. Бутоните по подразбиране са описани по-долу.

Поднови абонамент

Щракването върху този бутон ще ви отведе до онлайн магазин във вашия браузър, където може да закупите абонамент.

Бутонът става видим, ако абонаментът изтече или предстои да изтече.

Купете абонамент

Щракването върху този бутон ще ви отведе до онлайн магазин във вашия браузър, където може да закупите абонамент.

Този бутон е наличен, ако абонаментът е блокиран или пробната версия е изтекла.

Актуализирай базите

Щракването върху този бутон стартира актуализация на базите данни на приложението.

Този бутон е наличен, ако проблеми с текущия лиценз могат да бъдат разрешени чрез актуализация на базите данни (например датата на публикуване на базите данни не съответства на датата на изтичане на лиценза).

Причини и възможни решения

Щракването върху този бутон отваря прозорец на браузъра, който показва страница на уеб сайта на Техническа поддръжка с информация за възникналия проблем.

Този бутон е наличен, ако възникнат проблеми с текущия проблем.

Актуализирай статуса

Щракването върху този бутон изтегля актуализирана информация за състоянието на абонамента от сървъра на доставчика.

Този бутон се показва, ако приложението се използва от абонамента.

Открити други несъвместими приложения

Списъкът на несъвместимите приложения

Списъкът съдържа приложения, които са несъвместими с приложението, което се инсталира. Премахнете несъвместимите приложения за изправна работа на приложението, което се инсталира.

Премахни ръчно

Щракването върху този бутон отваря прозорец, който съдържа списък с приложения, инсталирани на компютъра. В този списък може да избирате приложения, които са несъвместими с приложението, което се инсталира, за да ги премахнете от вашия компютър.

Продължи

Когато се щракне върху този бутон, изброените несъвместими приложения се оставят на вашия компютър и съветникът продължава да работи.

Едновременната употреба на несъвместими приложения и приложението, което се инсталира, може да доведе до неправилна работа на приложението, което инсталирате, и значително влошава защитата на вашия компютър.

Открит е несъвместим софтуер

Списъкът на несъвместимите приложения

Списъкът съдържа приложения, които са несъвместими с приложението, което се инсталира. Премахнете несъвместимите приложения за изправна работа на приложението, което се инсталира.

Изтрий

Когато се щракне върху този бутон, изброените несъвместими приложения се премахват от вашия компютър и съветникът продължава да работи.

Запази

Когато се щракне върху този бутон, изброените несъвместими приложения се оставят на вашия компютър и съветникът продължава да работи.

Едновременната употреба на несъвместими приложения и приложението, което се инсталира, може да доведе до неправилна работа на приложението, което инсталирате, и значително влошава защитата на вашия компютър.

Необходимо е рестартиране на компютъра

Рестартирайте компютъра

Това квадратче за отметка активира / деактивира рестартиране на компютъра. Компютърът трябва да се рестартира, за да продължи Съветникът за превключване.

Ако е избрано това квадратче за отметка, щракването върху бутона **Готово** рестартира компютъра, след което Съветникът за превключване продължава.

Ако е премахната отметката от това квадратче, компютърът не се рестартира. Съветникът за превключване автоматично се възобновява, след като рестартирате или изключите и включите компютъра.

Първи стъпки

Покажи информация за сертификата

Тази връзка отваря прозорец, който показва информация за сертификата на Kaspersky.

Напред

Щракването върху този бутон стартира съветника за инсталиране на сертификат.

Инсталиране на сертификат

Този прозорец показва напредъка на автоматичното инсталиране на сертификата. Завършването на задачата може да отнеме известно време.

Kaspersky търси уеб браузъри, инсталирани на компютъра на потребителя, след което автоматично инсталира сертификати в хранилището за сертификати на Microsoft Windows.

Докато се инсталира сертификатът, на екрана може да се появи известие за сигурност на Microsoft Windows, което ви подканва да потвърдите инсталацията на сертификата.

Завършване на съветника

Готово

Когато бъде натиснат този бутон, Kaspersky затваря Съветника за инсталиране на сертификат.

Раздел Блокирани компютри

Блокирани компютри

Съдържа информация за компютрите, за които Защитата от мрежови атаки е забранила всякаква мрежова активност, насочена към вашия компютър.

Компютърен адрес

Тази колона показва IP адреса на блокиран компютър.

Начално време на блокиране

Тази колона показва изминалото време от блокиране на компютъра.

По подразбиране Защита от мрежови атаки блокира входящия трафик от атакуващ компютър за един час.

За да деблокирате даден компютър, избран в списъка, отворете контекстното меню.

Деблокирай

След щракването върху този бутон Защита от мрежови атаки деблокира избрания компютър.

Деблокирай всички компютри

Когато щракнете върху тази връзка, Защита от мрежови атаки деблокира всички блокирани компютри.

Раздел Отворени портове

Изглед

Щракването върху този бутон отваря меню, което включва следните елементи:

- **Показвай всички портове** – списъкът показва всички отворени портове на вашия компютъра.
- **Скривай портове за обръщане към самия компютър** – списъкът показва всички портове без тези, които се използват от мрежовия софтуер на вашата операционна система.

Отворени портове

Съдържа информация за всички отворени портове за всеки процес.

Следната информация се показва за всеки порт:

- Номер на порт
- Име на процеса (приложение, услуга, сървър), който използва порта
- ИД на процеса
- Локален IP адрес на процеса
- Протокол за свързване чрез порт

Двойното щракване върху ред в списъка отваря прозореца **Правила за програмите**, като се показва раздела **Мрежови правила**. В този прозорец може да конфигурирате мрежови правила за приложението, което използва избрания порт.

Щракването с десния бутон на мишката върху елемент от списъка отваря контекстно меню, от което може да конфигурирате мрежови правила.

Менюто съдържа следните елементи:

- **Мрежови правила за програми**. Избирането на този елемент от менюто отваря прозореца **Правила за програмите** в раздела **Мрежови правила**. В този прозорец може да конфигурирате мрежово правило за приложението, което използва порта, избран от списъка.
- **Всички мрежови правила**. Избирането на този елемент от менюто отваря прозореца **Правила за пакетите**. В този прозорец може да конфигурирате правила за пакетите за приложението, което използва порта, избран от списъка.

Раздел Мрежова активност

Изглед

Щракването върху този бутон отваря меню. Менюто съдържа следните елементи:

- **Показвай локалните връзки** – списъкът показва информация за връзките на вашия компютър с други компютри в същата локална мрежа.
- **Покажи <PRODUCT> връзки** – списъкът показва информация за връзките, установени от Kaspersky.

Мрежова активност

Този списък съдържа всички активни мрежови връзки, установени в момента на вашия компютър.

Показва се следната информация за всяка връзка:

- Име на процеса (приложение, услуга, сървър), който е инициирал връзката
- Посока на връзката (входяща/изходяща)
- Протокол на връзката
- Настройки на връзката (отдалечен порт и IP адрес)
- Количество предадени/получени данни (в килобайти)

Щракването с десния бутон на мишката върху елемент от списъка отваря контекстно меню, от което може да конфигурирате мрежови правила.

Менюто съдържа следните елементи:

- **Мрежови правила за програми**. Избирането на този елемент от менюто отваря прозореца **Правила за програмите** в раздела **Мрежови правила**. В този прозорец може да конфигурирате мрежово правило за избрано от списъка приложение.
- **Всички мрежови правила**. Избирането на този елемент от менюто отваря прозореца **Правила за пакетите**. В този прозорец може да конфигурирате правила за пакетите за избраното от списъка приложение.

Блокирай цялата мрежова дейност

След като щракнете върху връзката, защитната стена ще блокира мрежовата активност на всички процеси.

Долната част на прозореца показва диаграма на мрежовия трафик с обемите входящ и изходящ трафик за избран в списъка процес. Диаграмата отразява обема трафик в реално време. Обемът трафик се показва в килобайти.

Особени съображения при добавяне на правило за мрежови адаптер

Когато създавате правило за разрешаване за мрежови адаптер и/или правило с посочено TTL, това правило може да е в конфликт с правило за отказ за приложения. Например ако дадено приложение е в групата с големи ограничения, ще му бъде отказан мрежови достъп дори ако сте създали правило за разрешаване за пакет за мрежовия адаптер (и за TTL).

За да конфигурирате правило за разрешаване, което да работи за всички приложения, които се опитват да се свържат към мрежата чрез този мрежови адаптер, трябва да създадете следните правила по приоритетен ред от най-високия към най-ниския приоритет (в общия списък с правила за пакетите, приоритетът се определя отгоре надолу, от най-високия приоритет към най-ниския приоритет).

1. Правило за разрешаване за избрания мрежови адаптер.

2. Правила за отказ за всички други мрежови адаптери.

3. Правило за разрешаване без посочване на мрежови адаптер.

За да конфигурирате правило за разрешаване, което да работи за мрежови адаптер с TTL, трябва да създадете следните правила по приоритетен ред от най-високия към най-ниския приоритет:

1. Правило за разрешаване за специфична стойност на TTL.

2. Правило за отказ за стойност на TTL равна на 255.

3. Правило за разрешаване без посочване на стойност на TTL.

Раздел Мрежови трафик

Период

Списъкът съдържа интервали от време за преглед на разпространението на мрежовия трафик.

Налични стойности:

- **За днес**. Този списък показва данни за разпространението на мрежовия трафик за текущия ден.
- **За вчера**. Този списък показва данни за разпространението на мрежовия трафик за предишния ден.
- **за месеца**. Този списък показва данни за разпространението на мрежовия трафик за текущия месец.
- **за годината**. Този списък показва данни за разпространението на мрежовия трафик за текущата година.

Мрежов трафик

Съдържа информация за входящите и изходящите връзки, установени между вашия компютър и други компютри.

Количеството входящ и изходящ трафик се показва за всяко приложение (компютър, услуга, сървър, процес).

Двойното щракване върху приложение в списъка отваря прозореца **Правила за програмите** като се показва раздела **Мрежови правила**. В този прозорец може да конфигурирате мрежови правила за избраното приложение.

Щракването с десния бутон на мишката върху елемент от списъка отваря контекстно меню, от което може да конфигурирате мрежови правила.

Менюто съдържа следните елементи:

- **Мрежови правила за програми**. Избирането на този елемент отваря прозореца **Правила за програмите** в раздела **Мрежови правила**, в който може да конфигурирате мрежово правило за избраното приложение.
- **Всички мрежови правила**. Избирането на този елемент отваря прозореца **Правила за пакетите**, в който може да конфигурирате правила за пакетите за избраното приложение.

Долната част на прозореца показва диаграма на разпространението на трафика на избраното приложение в хода на времето за посочения интервал от време.

Прекратяване на мрежови връзки

Ако компютърът е заключен или защитата е поставена на пауза, когато приложението наблюдава активни мрежови връзки, показва се известие за прекратяване на тези връзки. Това е необходимо за правилно излизане от приложението. Прекратяването става автоматично след 10 секунди или след като щракнете върху бутона **Да**. Повечето прекратени връзки се възстановяват след кратък период от време.

Ако връзката е прекратена, когато изтегляте файл без диспечер за изтегляне, прехвърлянето на данните прекъсва. За да изтеглите файла, трябва да стартирате процеса по изтегляне отново.

Може да отмените прекратяването на връзките. За целта в диалоговия прозорец на уведомленията щракнете върху бутона **Не**. Приложението продължава да работи.

За разширените опции за VPN

Допълнителните функции на VPN услугата са налични, ако на компютъра ви е инсталиран Kaspersky Plus или Kaspersky Premium.

Допълнителните функции на VPN включват:

- Настройки за активиране на VPN при посещаване на следните категории уеб сайтове:
  - Уеб сайтове за банкиране;
  - Системи за плащане;
  - Онлайн магазини и уеб сайтове за електронна търговия;
  - Социални мрежи.
- Настройки за автоматична смяна на региона и града. Ако сте посочили различни региони и градове за уеб сайтове от различни категории в настройките на VPN, може да посочите дали да смените региона и града или не, когато се прехвърляте между уеб сайтове от различни категории.
- Настройки на VPN за отделни уеб сайтове, например за уеб сайтове, които посещавате често.

Връщане към Помощ на Kaspersky VPN Secure Connection.

Открити обекти

Изтрий

Когато е щракнат този бутон, приложението Kaspersky започва обработването на открития обект.

Този бутон е наличен, ако е бил открит обект.

Щракването върху бутона отваря меню, от което може да изберете допълнително действие:

- **Добави към изключенията** създава изключение, според което обектът не трябва да бъде разпознат като злонамерен.
- **Пропусни** премества известието към раздела **Игнорирани известия**.
- **Отваряне на съдържащата папка** отваря папката, която оригинално съдържа файла.
- **Научете повече** отваря уеб страница с описание на открития обект.

Прозорци за уведомяване на Kaspersky

Известията, които се появяват в областта за уведомяване в лентата на задачите ви информира за събития на приложението, които изискват вашето внимание.

Ако дадено уведомление се покаже на екрана, трябва да изберете една от опциите, които са предложени на него. Оптималната опция е препоръчаната по подразбиране от експертите на Kaspersky.

За Защита в облака

В този прозорец може да научите за Kaspersky Security Network.

Прозорец на активирането

Този прозорец показва прогреса на активиране на приложението.

Отказ

Щракването върху този бутон ви позволява да отмените активирането на приложението.

Регистрация и удостоверяване

Имейл адрес

Това поле ви позволява да въведете имейл адрес, за да се свържете със съществуващ акаунт в My Kaspersky или да създадете нов акаунт.

Влезте с Google

Щракването върху този бутон ви отвежда до формуляра за влизане с Google акаунт в браузъра по подразбиране (не е налично в някои региони).

Влезте с Facebook

Щракването върху този бутон ви отвежда до формуляра за влизане с Facebook акаунт в браузъра по подразбиране (не е налично в някои региони).

Влезте с Apple

Щракването върху този бутон ви отнема на формуляра за влизане в Apple в браузъра по подразбиране.

Имам код за активиране

Щракването върху тази връзка ви води до формуляра за въвеждане на кода за активиране.

Продължи

Натискането на този бутон ви отвежда до формуляра, който ви позволява да въведете паролата на съществуващ акаунт в My Kaspersky или да започнете процеса на създаване на нов акаунт.

Когато влезете в съществуващ акаунт в My Kaspersky, в прозореца се показва следното:

Парола

В това поле въведете паролата за вашия акаунт в My Kaspersky.

Забравили сте своята парола?

Превключете към прозореца за възстановяване на забравена парола на акаунт в My Kaspersky.

Въведете друг имейл

Натискането на този бутон ви връща към формуляра за въвеждане на имейл адрес.

Влизане

Щракването върху този бутон свързва устройството с вашия акаунт в My Kaspersky.

По време на създаването на My Kaspersky прозорецът показва следното:

Приемам да предоставя на Kaspersky моя имейл адрес, за да получавам персонализирани оферти за маркетинг

Ако е поставена отметка в квадратчето, ще получавате новини от Kaspersky на посочения имейл адрес.

Регион

Щракването върху тази връзка отваря прозореца за избор на регион. Приложенията, които може да инсталирате, и наличните методи на плащане, които може да използвате, зависи от вашия избран регион.

Въведете друг имейл

Натискането на този бутон ви връща към формуляра за въвеждане на имейл адрес.

Създай

След щракване върху този бутон, акаунтът в My Kaspersky е регистриран. Ще получите съобщение с връзката за създаване на парола за акаунта My Kaspersky на посочения от вас имейл адрес.

Повече за акаунта в My Kaspersky

Прозорец Избор на ключ от регистъра

Избор

След щракване върху този бутон полетата в прозореца **Добавяне на ключ в регистъра** се запълват със стойностите на избрания ключ.

Изберете прозореца за местоположение на тайно хранилище

В този прозорец можете да изберете местоположението на тайното хранилище, което създавате.

Избор

Като щракнете върху този бутон може да потвърдите, че посоченият път е правилен.

Прозорец Избор на файл или папка

Избор

Като щракнете върху този бутон, файл или папка ще се появи в полето **Път** в прозореца **Добавяне на файл или папка**.

Прозорец Надеждна група за непознати приложения

Този прозорец показва приложения, които не могат да бъдат добавени към съществуващи групи. Може да изберете надеждна група и щракнете върху бутона **Запази**. Приложения, които не могат да бъдат добавени към групата, която сте посочили.

По подразбиране тези приложения се добавят към групата **Със слаби ограничения**.

Прозорец за Надеждна група за приложения, стартирани преди стартиране на Kaspersky

В този прозорец може да изберете Надеждна група за непознати приложения, стартирани преди стартиране на приложението Kaspersky.

Списък с надеждни групи

Използвайте този списък, за да посочите Надеждна група, към която могат да бъдат зададени приложенията, стартирани преди стартирането на приложението Kaspersky. Мрежовата активност на такива приложения е ограничена според правилата на избраната надеждна група. По подразбиране мрежовата активност на приложения, стартирани преди стартирането на приложението Kaspersky, е ограничена според правилата, конфигурирани от експертите на Kaspersky.

Изберете автоматично надеждна група

Ако е избрана тази опция, компонентът Предотвратяване на проникване добавя приложения, стартирани преди стартирането на приложението Kaspersky, към надеждна група според правилата, създадени от експертите на Kaspersky.

Изберете ръчно надеждна група

Ако е избрана тази опция, може ръчно да изберете надеждна група, към която трябва да бъде добавено приложението, стартирано преди стартирането на приложението Kaspersky.

Прозорец Добавяне/редактиране на изключения за поверително сърфиране

Маска на уеб адрес

Използвайте това поле, за да посочите IP адресите или уеб адресите (URL) на уеб сайта, на които искате да разрешите проследяването на вашата онлайн активност.

Прозорец на Добавяне/редактиране на категория

Име на категория

В това поле може да посочите името на категорията ресурси; достъпът до тази категория ресурси ще бъде анализиран и контролиран от Предотвратяване на проникване.

Прозорец Добавяне/редактиране на ключ от регистъра

Избор

Щракването върху този бутон отваря прозореца **Изберете ключ от регистъра**, в който може да изберете ключ от регистъра, достъпът до който трябва да бъде управляван от компонента Предотвратяване на проникване.

Име

Името на ресурса с ключа от регистъра може да бъде въведено в това поле.

Път до ключ

Пътят към ключ от регистъра може да бъде въведен в това поле.

Стойност на защитен ключ

Ако е поставена отметка в квадратчето, единствено стойността на ключа, посочена в полето **Стойност на ключ**, е защитена от промяна.

Ако е премахната отметката от квадратчето, всички стойности на този ключ от регистъра са защитени.

Ако не е посочена стойност в полето **Стойност на ключ**, стойността по подразбиране на ключа от регистъра е защитена по подразбиране.

Това квадратче за отметка е избрано автоматично, когато е избран ключ от регистъра.

Стойност на ключ

В това поле може да посочите стойността на ключ от регистъра, който трябва да бъде защитен от компонента Предотвратяване на проникване срещу промяна.

Това поле може да се редактира, ако е поставена отметка в квадратчето **Стойност на защитен ключ**.

Добави

Щракването върху този бутон добавя ключ от регистъра към списъка с ресурси.

Прозорец за добавяне/редактиране на нецензурни думи

Маска за нецензурна дума

Дума или маска на дума, която, когато е открита в съобщение, се счита за знак за спам.

Тегловен коефициент на нецензурна дума

Цифрова стойност, която отразява вероятността дадено съобщение, съдържащо нецензурна дума, да е спам. Колкото по-висок е тегловният коефициент, толкова по-висока е вероятността съобщението, съдържащо нецензурна дума, да е спам.

Защитата от спам маркира съобщение като спам, ако сумата от тегловните коефициенти на нецензурни думи и блокирани фрази надвишава посочената стойност.

Статус

В раздела **Статус** може да посочите дали Защитата от спам ще сканира съобщения за нецензурна дума:

- **Активен**. Защитата от спам сканира съобщения, за да провери дали включват нецензурна дума.
- **Неактивен**. Защитата от спам не сканира съобщения, за да провери дали включват нецензурна дума.

Прозорец на Добавяне/редактиране на файл или папка

Име

В това поле може да посочите името на ресурс с файла или папката, достъпът до който трябва да бъде управляван от Предотвратяване на проникване.

Път

В това поле може ръчно да посочите пътя към файл или папка.

Когато въвеждате пътя ръчно, може да използвате маска.

Маската `\*` ви позволява да посочите, че искате да контролирате достъпа до всички файлове или подпапки в избраната папка.

Маската `\*<extension>` ви позволява да посочите, че искате да контролирате достъпа до всички файлове с посоченото разширение в избраната папка.

Също така може да контролирате достъпа на приложенията до файлови ресурси, намиращи се на отдалечен компютър. За целта посочете пътя към мрежовия ресурс в UNC формат според правилото `\\Server\Share\Relative path`, където:

- Server е името на домейна на компютъра или IP адрес в IPv4 или IPv6 формат (изисква се).
- Share е името на мрежата на споделената папка (изисква се).
- Relative path е пътят към папката или файла от споделена папка (по избор).

  Примерни пътища:

- `\\Server1\ShareFolder1\test\example.exe`
- `\\Server1\ShareFolder1\test\*.docx`
- `\\Server1\ShareFolder1\*`

  Приложението не контролира достъпа до файловия ресурс, ако пътят, определен в правилото, се различава от пътя, който се изисква.

Избор

Щракването върху този бутон отваря прозорец, в който може да изберете файл или папка.

Добави

Щракването върху този бутон добавя файл или папка към списъка с ресурси.

Прозорец на завършено активиране

Този прозорец се отваря, ако приложението е успешно активирано.

Готово

Щракването върху този бутон завършва процедурата по активиране на приложението и отваря прозореца Лицензиране.

Прозорец на блокирани и разрешени приложения

Този прозорец показва списък с приложения, на които е разрешено или не е разрешено да променят настройките на операционната система. Празен списък означава, че все още не сте разрешили или блокирали приложения да променят настройки на операционната система.

Списък с приложения

Списъкът с приложения съдържа следните данни:

- **Приложение**. Тази колона показва името на приложението.
- **Име на файл**. Тази колона показва името на изпълнимия файл на приложение.
- **Път**. Тази колона показва пътя до изпълнимия файл на приложение на твърдия диск на вашия компютър.
- **Доставчик**. Тази колона показва цифровия подпис на издателя на приложението.
- **Промени**. Тази колона показва дали приложение е блокирано или му е разрешено да променя настройки на операционната система, настройки на браузъра и мрежови настройки.

Прозорец Защита на личните данни

В този прозорец може да активирате или деактивирате следните компоненти:

Управление на уеб камера и микрофон

Проверка на изтичане на данни

Поверително сърфиране

Актуализация на приложения. Изключения

Изключения

Пропуснатите актуализации на инсталираните приложения се поставят в списъка с **Изключения**. Може да пропускате индивидуални актуализации и всички актуализации за специфично приложение, инсталирано на вашия компютър.

Списъкът с **Изключения** се състои от следните колони:

- **Програма** – тази колона показва името на приложението.
- **Пропусни** – тази колона може да съдържа следните стойности:
  - **Версия на актуализация** – показва се, ако сте пропуснали индивидуална актуализация за инсталирано приложение.
  - **Всички актуализации** – показва се, ако сте решили да не актуализирате приложението.

Изтрий

Щракването върху този бутон премахва избраните приложения от списъка с изключения. Бутонът е активен, ако приложението е избрано в списъка.

Kaspersky ще Ви уведоми за наличието на актуализации за приложения, които са били премахнати от списъка.

Прозорец Изключения на поверително сърфиране

Списък с изключения

Този списък включва адресите на уеб сайтове, на които проследяването на вашата онлайн дейност е разрешено. На тези уеб сайтове компонентът Поверително сърфиране открива опити за събиране на данни, но не ги блокира дори ако компонентът е конфигурира да блокира събирането на данни от тези категории услуги за проследяване.

Може да добавите уеб адрес или маска на адрес към списъка.

Редактирай

Това отваря прозореца, в който може да смените избрания уеб адрес / маска на уеб адрес.

Изтрий

Премахва избрания уеб адрес / маска на адрес от списъка

Добави

Това отваря прозореца, в който може да добавите избрания уеб адрес / маска на уеб адрес.

Прозорец за използване на приложението

Приложения

Тази колона показва приложения и групи от приложения, чиято употреба може да ограничите.

Използване

Тази колона показва дали на потребителя е разрешено да работи с приложение или група от приложения или не:

- **Разрешено**– потребителят може да работи с това приложение или група от приложения.
- **Блокирано**– на потребителя не е разрешено да работи с това приложение или група от приложения.
- **Ограничено** – потребителят може да работи с това приложение или група от приложения за ограничен период от време.

Може да разрешите, блокирате или ограничите употребата на дадено приложение или група от приложения, за избран потребител, като изберете задължителния елемент от падащия списък.

Път

Тази колона показва пътя към изпълнимия файл на приложението.

Правила

Щракването върху този бутон отваря прозорец, в който може да ограничите времето на употреба на избраното приложение.

Изтрий

Щракването върху този бутон изтрива избраното приложение от списъка. След като приложението е изтрито от списъка, Kaspersky спира да наблюдава използването на приложението и потребителят може да го управлява без ограничения.

Добавете приложение

Щракването върху този бутон отваря диалогов прозорец, в който може да изберете изпълнимия файл на дадено приложение, за да го добавите към списъка. Parental Control добавя приложението в съответната категория в списъка.

Прозорец на Карантина

Обекти в списъка Карантина

Съдържа списък с файлове, преместени в Карантина. Карантината е предназначена за съхраняване на резервни копия на файлове, които са били изтрити или променени по време на процеса по дезинфектиране.

Файл

Тази колона показва името на карантинирания файл.

Щракването с десния бутон на мишката отваря контекстното меню, от което може да извършвате действията, налични за карантинирани файлове: възстановяване, премахване или отваряне в оригинална папка.

Път

Тази колона показва пътя към файла.

Открит

Тази колона показва типа на открития обект, например *Мрежова атака*.

Дата и час

Тази колона показва датата и часа на преместване на файла в Карантина.

Възстановяване

Когато щракнете върху този бутон, Kaspersky връща избрания файл от списъка в папката, в която е бил съхраняван преди да бъде преместен в Карантина.

Изтрий

Когато щракнете върху този бутон, Kaspersky изтрива файла, който е избран в списъка.

Премахни всичко

Като щракнете върху този бутон, Kaspersky изтрива всички резервни копия на файлове, които са били преместени в Карантина.

Kaspersky не дезинфектира приложения от Windows Store. Ако резултатите от сканирането показват, че такова приложение е опасно, то е изтрито от вашия компютър. Когато е изтрито приложение от Windows Store, Kaspersky не създава негово резервно копие. За да възстановите такива обекти, трябва да използвате инструментите за възстановяване, включени в операционната система (за подробна информация вижте документацията за операционната система, инсталирана на вашия компютър) или да актуализирате приложенията чрез Windows Store.

Прозорец Нецензурна лексика

Този прозорец показва списък с нецензурна лексика. Ако някоя от тези думи присъства в съобщението, Kaspersky го маркира като спам.

Бутон

Щракването върху този бутон отваря меню с избор на следните действия:

- Импортиране и добавяне към съществуващи. Избирането на тази опция ви позволява да импортирате списък с нецензурни фрази от CSV файл. Настоящите фрази не се изтриват.
- Импортиране и замяна на съществуващи. Избирането на тази опция ви позволява да импортирате списък с нецензурни фрази от CSV файл. Настоящите фрази се изтриват.
- Експортиране. Избирането на тази опция ви позволява да експортирате списък с нецензурни фрази в CSV файл.

Нецензурна лексика

Тази колона показва дума или фраза. Наличието на тази дума или фраза може да означава, че съобщението е спам.

Тегло

Тази колона показва тегловния коефициент, зададен на нецензурна дума. Ако съобщение съдържа няколко нецензурни думи, чийто комбиниран тегловен коефициент надвишава 100, това съобщение е маркирано като спам.

Статус

Тази колона показва дали Защита от спам използва тази дума, когато сканира съобщения за нецензурна лексика.

- **Активен**. Приложението проверява съобщения за тази дума.
- **Неактивен**. Приложението не проверява съобщения за тази дума.

Редактирай

Щракването върху този бутон отваря прозорец, в който може да смените нецензурната дума или маска на дума, избрана в списъка.

Изтрий

Щракването върху бутона ви позволява да изтриете нецензурната дума.

Добави

Щракването върху този бутон отваря прозорец, в който може да добавите нецензурна дума или маска на дума към списъка.

Прозорец „Новини“

Списък с новини

Новините се показват като списък в прозореца. За всеки елемент от новините се посочват заглавието му, обявяването и времето на публикуване.

Щракването върху този бутон отваря прозореца с текста на новините.

Прозорец „Новини“

Връзки към Twitter и социалните мрежи

Щракването върху връзките отваря вашите страници в Twitter или в социалните мрежи за публикуване на новини. Може да редактирате текста, който трябва да се публикува.

Ако не сте влезли, се появява страницата за влизане на съответния уеб сайт на социална мрежа.

Връзки към социални мрежи се показват, ако ви е разрешено да посещавате такива сайтове.

Бутони

Бутони, които може да щраквате, за да превключвате между елементи на новините.

Прозорец Настройки на диспечер на приложения

Активирай / деактивирай Диспечер на приложения

Активиране на диспечер на приложения. Ако превключвателят е включен, приложението Kaspersky контролира инсталацията и премахването на допълнителни приложения и показването на стъпките на инсталацията, съдържащи реклами.

Активиране на диспечер на приложения. Ако превключвателят е включен, приложението Kaspersky контролира инсталацията и премахването на допълнителни приложения и показването на стъпките на инсталацията, съдържащи реклами.

По време на инсталиране на приложения автоматично чисти квадратчетата с отметки за инсталация на допълнителен софтуер. Предупреждавай за опити за инсталиране на допълнителни програми

Ако е поставена отметка в квадратчето, по време на инсталиране на приложение на Вашия компютър приложението Kaspersky блокира инсталиране на допълнителни програми.

Ако отметката е премахната от квадратчето, след като сте започнали да инсталирате определено приложение, Програмата за блокиране на инсталирането на нежелани приложения продължава да работи за продължителността на текущата инсталация. Отметките в квадратчетата срещу приложенията, предложени за допълнителна инсталация, са премахнати и допълнителните приложения не се инсталират. Тази функционалност ще бъде деактивирана по време на следващата инсталация. Допълнителни приложения ще бъдат инсталирани заедно с основното приложение.

Не показвай стъпки за инсталация, които може да се отнасят до реклами и оферти за инсталиране на допълнителни програми

Ако е поставена отметка в квадратчето, по време на инсталиране на приложение на Вашия компютър Kaspersky блокира показването на реклами или оферти за инсталиране на допълнителни програми.

Прозорец с настройки на програмата за актуализиране на приложения

Активиране на търсенето на актуализации на приложението

Ако е поставена отметка в това квадратче, Kaspersky търси актуализации за инсталирани приложения и Ви подканва да ги изтеглите и инсталирате.

Задаване на режим за търсене на актуализации

Щракването върху тази връзка отваря прозорец, в който може да посочите режима, за да търсите автоматично актуализации за приложения, инсталирани на вашия компютър.

Автоматично изтегляне и инсталиране на актуализации, ако не трябва да приемате нови лицензионни споразумения

Ако е поставена отметка в квадратчето, Приложението Kaspersky автоматично търси актуализации за инсталирани приложения и изтегля и инсталира наличните актуализации, ако не се изисква съгласието ви за нови лицензионни споразумения.

Търсене на актуализации на приложенията

В настройките трябва да изберете кои актуализации на приложението да бъдат инсталирани:

- **Важни актуализации, които подобряват сигурността на компютъра** означава, че ще се инсталират само важни актуализации, които коригират уязвимости в софтуера и подобряват сигурността на вашия компютър.
- **Всички актуализации за известни приложения** означава, че всички актуализации ще бъдат инсталирани.

Изключения

Щракването върху тази връзка отваря прозореца **Изключения** със списъка с изключения. Пропуснатите актуализации на инсталираните приложения се поставят в списъка с изключения. Може да пропускате индивидуални актуализации и всички актуализации за специфично приложение, инсталирано на вашия компютър.

Актуализиране на режима на търсене/График

Таблицата описва настройките, които управляват графика за компонентите Актуализация на приложения и Диспечер на приложения.

Настройки	Описание
Режим на търсене на актуализации (Актуализация на приложения) **Стартирай анализ** (Диспечер на приложения)	**Автоматично**. Kaspersky стартира задачата веднъж на 24 часа според вътрешните настройки. **Всяка минута** / **Всеки час** / **Всеки ден** / **Ежеседмично** / **Ежемесечно** / **В определено време**. Kaspersky стартира задачата според определения график, който може да бъде определен до точната минута. Когато е избрана една от тези опции, квадратчето за отметка **Отлагане на изпълнение след стартиране на приложението за N минути** е налично. **След стартиране на приложението**. След като Kaspersky стартира, той ще стартира задачата, след като изчака минутите, посочени в полето **Започване след N минути**. **След всяка актуализация**. Kaspersky стартира задачата след изтегляне и инсталиране на нов пакет с актуализации.
Търсете актуализации на следващия ден, ако компютърът е изключен (Актуализатор на приложения) **Стартирайте анализа на обект на следващия ден, ако компютърът е изключен** (Диспечер на приложения)	Ако планирано търсене на актуализации на приложенията или анализ на обект са пропуснати, защото компютърът е бил изключен, Kaspersky стартира задачата, след като компютърът се включи. Това квадратче за отметка се показва, ако е избран един от следните режими за стартиране: **Всеки ден** / **Ежеседмично** / **Ежемесечно** / **В определено време**.
Търсете актуализации на приложения само когато скрийнсейвърът е активен или компютърът е заключен (Актуализатор на приложения) **Стартирайте анализа на обекти само когато скрийнсейвърът е активен или компютърът е заключен** (Диспечер на приложения)	Kaspersky стартира задачата, когато приключите работа с компютъра. Това означава, че задачата няма да използва системни ресурси, докато работите. Това квадратче за отметка се показва, ако е избран режимът за стартиране **След всяка актуализация**.

Настройки на актуализация

Настройки	Описание
График за актуализация на базите данни	Щракването върху тази връзка отваря прозореца **График за актуализация на базите данни**, в който може да изберете един от двата режима за стартиране на актуализацията на базите данни: **Автоматично**. Режим за стартиране на задача за актуализиране, в който приложението Kaspersky сканира за пакет с актуализации в източника на актуализации на конкретна честота. Честотата на сканира може да се увеличи при пробиви на вируси и да се намали, когато няма никакви. След откриване на нов пакет с актуализации приложението Kaspersky го изтегля и инсталира актуализациите на компютъра. **Ръчно**. Този режим за стартиране на задача ви позволява да стартирате ръчно задача за актуализация. **Всяка минута** / **Всеки час** / **Всеки ден** / **Ежеседмично** / **Ежемесечно** / **В определено време** / **След стартиране на приложението**. Режим за стартиране на задача за актуализация, в който приложението Kaspersky стартира задачата за актуализация според графика, който сте създали. Ако изберете този режим за стартиране на актуализация, може също така да стартирате задачата за актуализация на приложението Kaspersky ръчно.
Избор на източници за актуализация	Щракването върху тази връзка отваря прозорец със списъка с източници за актуализация. *Източник за актуализация* е публичен HTTP или FTP сървър или споделена папка (локална или мрежова), от където приложението може да изтегли базите данни и модулите за актуализация. По подразбиране списъкът с източници за актуализация съдържа сървъри за актуализации на Kaspersky. Може да добавяте други източници за актуализация към списъка. Ако са избрани няколко източника за актуализация от списъка, приложението Kaspersky ще ги разгледа един след друг, докато достигне първия наличен източник за актуализация, от който може да изтегли пакета с актуализации.
Стартиране на актуализации на базите данни като	Щракване върху връзката отваря прозорец, в който може да изберете да стартирате актуализация на базите данни с конкретни потребителски права. По подразбиране задачата за актуализиране на приложението Kaspersky се стартира от името на потребителя, чиито права сте регистрирали в операционната система. Все пак приложението Kaspersky може да се актуализира от източник за актуализация, до който потребителят няма права за достъп (например от споделена папка, съдържаща пакет с актуализации) или за който няма конфигурирано удостоверяване на прокси сървъра. Може да посочите потребител, който притежава необходимите права в настройките на приложението, и да стартирате задачата за актуализиране на приложението Kaspersky от името на този потребител.

Прозорец на сканиране за уязвимост на приложението

Стартирай сканиране

Като щракнете върху този бутон, ще стартира Сканиране за уязвимости в приложенията.

Спри

Като щракнете върху този бутон, Сканирането за уязвимости в приложенията ще спре.

Бутонът се показва, ако се изпълнява Сканиране за уязвимости в приложенията.

N уязвими приложения

Като щракнете върху тази връзка, ще се отвори прозорецът **Уязвими програми**, който съдържа списък с уязвими приложения, които са открити по време на сканиране. Връзката се показва, ако се изпълнява Сканиране за уязвимости в приложенията.

Прозорец Пауза на защитата

Пауза за

Режим на възобновяване на работата на компонентите за защита, в който защитата се включва автоматично след посочен от вас интервал от време.

Може да посочите интервал от време в падащия списък по-долу.

Пауза до рестартиране на приложението

Режим на възобновяване на работата на компонентите за защита, в който защитата се включва, след като приложението е затворено и стартирано отново или операционната система е рестартирана (ако автоматичното стартиране на приложението е включено).

Пауза

Режим на възобновяване на работата на компонентите за защита, в който защитата се включва само когато решите да я възобновите.

Прозорец на Проверка на парола

Парола

Парола за администриране на приложението Kaspersky.

Запомни паролата за тази сесия

Ако е поставена отметка в това квадратче, Kaspersky запомня въведената парола и повече не Ви напомня за нея, по време на текущата сесия.

Прозорец на приложения, за които достъпът до уеб камерата е блокиран

Този прозорец показва приложения, за които сте блокирали достъпа до уеб камерата.

Разреши достъп до уеб камерата

Щракването върху този бутон позволява на избраното приложението в списъка да осъществява достъп до уеб камерата.

Прозорец за препоръчани настройки

Включете защита от реклами, за да инсталирате само желания софтуер и да блокирате допълнителни инсталации

Ако е поставена отметка в квадратчето, Kaspersky Security Cloud блокира показването на реклами по време на инсталиране на софтуер на компютъра. Инсталирането на допълнителен софтуер, който се рекламира, също е блокирано.

Готово

Щракването върху този бутон ви отвежда до основния прозорец на приложението.

Прозорец Отчети

Може да използвате следните възможности за удобно управление на отчетите:

- Филтрирай по дата;
- Филтрирай по стойност във всяка клетка;
- Търсене по текст на запис на събитие;
- Сортирай списъка по колона на всеки отчет;
- Смени реда и подреждането на колоните, които се показват в отчета.

В отчетите се използват следните нива на важност на събитията:

Информационни съобщения. Информационни събития, които като цяло не съдържат важна информация.

Предупреждения. Събития, на които трябва да обърнете внимание, тъй като те съдържат информация за важни ситуации, с които приложението Kaspersky се сблъсква, когато работи.

Критични събития. Критично важни събития, които показват, че приложението Kaspersky се е сблъскало с проблеми, които засягат способността му да работи, или уязвимости, които се отразяват на нивото на защита на компютъра на потребителя.

Когато щракнете върху бутона **Записване на отчет**, може да запишете отчета като файл в TXT или CSV формат.

Прозорец Настройки на акаунта

Стартиране на актуализации на базите данни като

Задачите за актуализиране за Kaspersky се стартират с правата на потребителския акаунт, който избирате. Тази функция е налична за стартиране на задача за актуализиране за Kaspersky ръчно и според графика.

Налични са следните опции:

- **Настоящ потребител**. Правата на настоящия акаунт (акаунтът на операционната система, с който сте влезли) ще важат за задачите за актуализиране.
- **Друг потребител**. Задачите за актуализиране ще стартират с посочения потребителски акаунт. Ако изберете тази опция, посочете име на акаунт и парола в полетата **Акаунт** и **Парола** съответно.

Изпрати отчета

Информация за операционната система

Това квадратче за отметка позволява добавянето на информация за състоянието на операционната система към отчета, който ще се изпраща към сървъра на Техническата поддръжка.

Получени данни за анализ

Като изберете квадратче за отметка, може да добавите файлове със следи и вторични копия към отчета, който се изпраща до сървъра на Техническа поддръжка. Хронологията на изпълнение на команди от приложението и информацията за състоянието на приложението се записват в тези файлове.

Щракването върху връзката **<number of files>**, **<data volume>** до квадратчето за отметка отваря прозореца **Получени данни за анализ**. Прозорецът показва списъка с файлове и общото количество данни, което трябва да се прехвърли към сървъра на Техническа поддръжка.

Запазване на отчет на компютъра ви

Щракването върху връзката отваря диалогов прозорец за записване на файла.

Въведете номер на заявката

Номерът, зададен на вашата заявка, когато се свързвате с екипа за техническа поддръжка от уеб сайта на My Kaspersky.

Изпрати отчета

Щракването върху този бутон качва избраните файлове към FTP сървър на техническата поддръжка.

Прозорец на получени данни за анализ

Списък с файлове с данни

Списък с файлове, които Kaspersky включва в отчета, изпратен към сървъра на техническата поддръжка. Списъкът включва файлове със следи и вторични копия. Хронологията на изпълнение на команди от приложението и информацията за състоянието на приложението се записват в тези файлове.

Ако е избрано квадратчето за отметка в реда на файла, файлът ще бъде качен на сървъра на техническата поддръжка. Преди да бъдат качени, файловете с данни се подготвят и архивират.

Ако квадратчето за отметка не е избрано в реда на файла, файлът няма да бъде качен на сървъра на техническата поддръжка.

Файл

Тази колона показва името на файл, който вече е готов да бъде изпратен до сървъра на техническата поддръжка.

Размер

Количество данни, което ще бъде изпратено до сървъра на техническата поддръжка, ако посоченият файл е включен в отчета. Приложението включва файл в отчета, ако квадратчето за отметка в реда на файла е избрано.

Изпълни скрипт

Текст на скрипт за изпълнение

Текст на скрипт, получен от екипа за техническа поддръжка.

Специалистите на Kaspersky препоръчват да не променяте текста на скрипта.

Изпълни

Щракването върху този бутон стартира изпълнението на скрипта.

Изпълнение на AVZ скриптове

Този прозорец показва процеса на изпълнение на AVZ скрипт. Изпълнението на скрипта може да отнеме известно време.

Резултат от изпълнението на скрипта

Грешка

Съобщение за грешка. Показва се, ако са открити грешки в AVZ скрипта. Съветникът за изпълнение на AVZ скрипта спира.

Готово

Щракването върху този бутон затваря Съветника за изпълнение на AVZ скрипта.

Резултат от изпълнението на скрипта

Затвори

Щракването върху този бутон затваря Съветника за изпълнение на AVZ скрипта.

Редактирай

Щракването върху този бутон ви позволява да добавите скрипта и да опитате изпълнението му.

Прозорец на Уязвими приложения

Уязвими програми

Изброява уязвимостите, открити в приложенията.

Поради поведението на някои услуги за актуализиране, уязвимости на някои приложения могат да бъдат открити няколко пъти.

Следните бутони са налични за всяка уязвимост:

- **Детайли**

Щракването върху този бутон ви отвежда до уеб сайта на Техническа поддръжка, който предоставя описание на заплахата. На уеб сайта може да изтеглите необходимите актуализации за вашата версия на приложението и да ги инсталирате.

- **Добави в изключенията**

Когато щракнете върху този бутон, приложението се добавя в надеждната зона.

Изберете ZIP файл или папка

Теми с персонализиран дизайн не са налични в някои региони.

Когато избирате тема, вземете предвид следните ограничения:

- Kaspersky няма да може да използва избраната тема в следните случаи:
  - Файловете в архива имат име или път в структурата на папката, който е различен от темата по подразбиране.
  - Архивираните файлове, отговорни за текстовете в прозорците на приложението, са повредени.
- Темите са проектирани за конкретна версия на Kaspersky и не са приложими за други версии или други приложения. Когато надстройвате приложението към нова версия или инсталирате друго приложение върху него, темата се променя на темата по подразбиране.

Ако срещнете проблеми при избора на алтернативна тема и не може да инсталирате темата по подразбиране с предложения метод (например не може да изчистите квадратчето за отметка **Използване на тема с персонализиран дизайн** в прозореца **Настройки на интерфейс**, тъй като шрифтът се слива с фона и необходимите елементи за управление са неразличими), препоръчва ви се да преинсталирате Kaspersky.

Прозорец на Добавяне/редактиране на изключение за компютърна клавиатура

Маска на уеб адрес

Уеб адресът на даден уеб сайт, който искате да добавите към списъка. Може да посочите уеб адрес или маска на адрес.

В раздела **Обхват** може да посочите областта, за която се прилага правилото за изключение за Защитено въвеждане от клавиатурата.

Приложи за целия уеб сайт

Защитено въвеждане от клавиатурата е активирано за всички страници на уеб сайта, посочени в полето **Маска на уеб адрес**.

Приложи към указаната страница

Защитено въвеждане от клавиатурата е активирано само за уеб страницата, посочена в полето **Маска на уеб адрес**.

В раздела **Защитено въвеждане от клавиатура** може да посочите дали Kaspersky защитава въвеждането на данни от компютърната клавиатура за избрания сайт или уеб страница.

Защитавай

Kaspersky защитава въвеждането на данни от компютърната клавиатура за избрания сайт или уеб страница.

Не защитавай

Kaspersky не защитава въвеждането на данни от компютърната клавиатура за избрания сайт или уеб страница.

Прозорец на Добавяне/редактиране на изключение за екранна клавиатура

Маска на уеб адрес

Уеб адресът на даден уеб сайт, който искате да добавите към списъка. Може да посочите уеб адрес или маска на адрес.

В раздела **Обхват** може да посочите към какво се прилагат настройките на иконата Екранна клавиатура: целия уеб сайт или посочената страница.

Приложи за целия уеб сайт

Иконата за бързо стартиране за Екранна клавиатура се показва в полетата за въвеждане на всички уеб страници на уеб сайта, които са посочени в полето **Маска на уеб адрес**.

Приложи към указаната страница

Иконата за бързо стартиране за Екранна клавиатура се показва в полетата за въвеждане само за уеб страницата, която е посочена в полето **Маска на уеб адрес**.

В раздела **Икона на екранна клавиатура** може да посочите дали приложението трябва да показва иконата на Екранна клавиатура на страниците, които съответстват на посочената маска на уеб адрес, или не трябва.

Показвай икона в прозорец на браузъра

Kaspersky показва иконата за бързо стартиране за Екранна клавиатура в полетата за въвеждане.

Не показвай икона в прозорец на браузъра

Kaspersky не показва иконата за бързо стартиране за Екранна клавиатура в полетата за въвеждане.

Настройки на Отчети и карантина

В раздела **Отчети** може да конфигурирате настройките за създаване и съхраняване на отчети.

Съхранявай отчетите не по-дълго от

Това квадратче за отметка активира/деактивира опцията за ограничаване на периода за съхраняване на отчети. Отчетите могат да се съхраняват един ден, една седмица, един или шест месеца или една година.

Когато посочената стойност бъде достигната, приложението изтрива всички записи в отчета, които са по-стари от посочения брой дни минус 10%. Ако въведете стойност 30 дни, когато в отчета се появи събитие, по-старо от 30 дни, всички събития, които са били съхранявани повече от 27 дни, се изтриват от отчета.

Ако квадратчето за отметка не е отбелязано, продължителността за съхраняване на отчетите е неограничена.

Ограничете размера за файл с отчет до

Това квадратче за отметка активира/деактивира опцията за ограничаване на максималния размер на файловете с отчети. Максималният размер на файл е посочен в мегабайти.

Ако е поставена отметка в това квадратче, максималният размер на отчета е 1024 MB по подразбиране. Изтриването се извършва, когато се достигне половината от посочения размер. Изтриват се 10% от действителния размер на файла с отчета. Ако зададената стойност е 1024 MB, старите записи в отчета за отчети започват да се изтриват, когато файлът на отчета достигне 512 MB, а размерът на файла на отчета се намалява с 10% от действителния му размер, като изтрие най-старите записи.

Ако квадратчето за отметка не е отбелязано, размерът на файла с отчета не е ограничен.

Изчисти

Като щракнете този бутон, Kaspersky премахва данни от папката с отчети.

По подразбиране Kaspersky изтрива отчетите от задачите за сканиране, отчетите от задачите за актуализиране и отчетите от прилагане на правилата на защитната среда.

В раздела **Карантина** може да променяте настройките за карантината.

Съхранявай обектите не по-дълго от

Това квадратче за отметка активира/деактивира опцията за ограничаване на периода за съхраняване на обекти в Карантина. Отчетите могат да се съхраняват един ден, една седмица, един или шест месеца или една година.

Ако е поставена отметка в квадратчето, обектите се съхраняват за периода, избран в падащия списък до квадратчето за отметка.

Ако квадратчето за отметка не е отбелязано, срокът за съхраняване на обектите е неограничен.

Ограничаване на размера на Карантина до

Това квадратче за отметка активира/деактивира опцията за ограничаване на максималния размер на Карантина. Размерът на Карантината е посочен в мегабайти.

Ако е поставена отметка в квадратчето, максималният размер за съхранение по подразбиране е 100 MB. Когато максималният размер е надвишен, най-старите обекти се премахват от хранилището, докато се добавят нови.

Ако квадратчето за отметка не е отбелязано, размерът на хранилището е неограничен.

Настройки на Самозащита

Включи самозащитата

Това квадратче за отметка активира / деактивира механизъм на приложението Kaspersky, който защитава приложението срещу промяна или изтриване на файловете му от твърдия диск, процеси на паметта и записи в системния регистър.

Ако е поставена отметка в това квадратче, възможността за извършване на външен контрол на системната услуга също е деактивиран. Когато външният контрол на системната услуга е деактивиран, приложението Kaspersky блокира всички опити за извършване на отдалечено управление на услугите на приложението. Ако бъде открит опит за отдалечено управление на приложението, се появява известие над иконата на приложението Kaspersky в областта за уведомяване на лентата на задачите на Microsoft® Windows® (ако известията не са деактивирани).

Разреши управление на настройките на <PRODUCT> чрез приложения за отдалечено управление

Ако е поставена отметка в това квадратче, надеждни приложения за отдалечено управление (като TeamViewer, LogMeIn Pro и Remotely Anywhere) могат да променят настройките на Kaspersky.

Ненадеждните приложения за отдалечен контрол няма да могат да променят настройки на Kaspersky дори когато е поставена отметка в квадратчето.

Настройки на прокси сървър

Не използвай прокси сървър

Този бутон активира/деактивира използването на прокси сървър за интернет връзки. Необходима е Интернет връзка за работата на някои защитни компоненти в Kaspersky, както и за актуализиране на базите данни и модулите на приложението.

Автоматично определи настройките за прокси сървър

Kaspersky открива автоматично настройките за прокси сървър с помощта на WPAD (протокол за автоматична настройка на прокси сървър).

Ако този протокол не може да определи адреса, Kaspersky използва настройките за прокси сървър, посочени в браузъра Microsoft Edge, базиран на Chromium. Kaspersky не взема предвид настройките за прокси сървърите, определени за други браузъри, които са инсталирани на компютъра на потребителя.

Използвай посочените настройки за прокси сървър

Kaspersky използва прокси сървър, който се различава от посочения в настройките за връзката на браузъра.

Адрес

Съдържа IP адреса или символично име (URL адрес) на прокси сървър.

Полето може да се редактира, ако е избрана настройката **Използвай посочените настройки за прокси сървър** (например IP 192.168.0.1).

Порт

Портът на прокси сървъра.

Полето е налично, ако е избрана настройката **Използвай посочените настройки за прокси сървър**.

Използвай удостоверяване на прокси сървъра

Удостоверяване е проверка на информацията за влизане на потребителя.

Това квадратче за отметка активира / деактивира използването на удостоверяване на прокси сървъра.

Ако е избрано това квадратче за отметка, Kaspersky първо ще опита да извърши NTLM удостоверяване, след което BASIC удостоверяване.

Ако е премахната отметката от квадратчето или ако настройките за прокси сървъра не са определени, Kaspersky ще опита да извърши NTLM удостоверяване с помощта на акаунта, с който е стартирана задачата (например задача за актуализиране).

Ако прокси сървърът изисква удостоверяване и не са въведени потребителско име и парола или ако посочените данни не са приети от прокси сървъра, ще се отвори прозорец, който ви подканва за потребителското име и паролата. Ако удостоверяването е успешно, Kaspersky използва в бъдеще посоченото потребителско име и парола. В противен случай Kaspersky ще Ви подкани отново за настройки за удостоверяване.

Потребителско име

Потребителското име, използвано за удостоверяване на прокси сървъра.

Парола

Паролата за посоченото потребителско име.

Не използвай прокси сървър за локални адреси

Ако е поставена отметка в това квадратче, Kaspersky не използва прокси сървър при актуализиране на бази данни и модули на приложния софтуер от локална или мрежова папка.

Ако това квадратче за отметка не е отбелязано, Kaspersky използва прокси сървър при актуализиране на бази данни и модули на приложния софтуер от локална или мрежова папка.

Раздел „Защита“

Списък със защитни компоненти

Този списък включва защитни компоненти, проектирани да защитават срещу различни типове дигитални заплахи.

Всеки тип заплаха се обработва от специално предназначен защитен компонент. Компонентите могат да бъдат активирани или деактивирани независимо един от друг и настройките им могат да бъдат конфигурирани.

Управление на уеб камера и микрофон

Активиране / деактивиране на управление на уеб камера и микрофон

Този превключвател активира / деактивира управлението на уеб камера и микрофон.

Под **Настройки за уеб камера**, можете да редактирате следните настройки:

Блокиране на достъпа на всички приложения до вашата уеб камера

Ако е поставена отметка в квадратчето, достъпът до уеб камерата е блокиран за всички приложения, инсталирани на Вашия компютър.

Уведоми, ако дадено приложение използва уеб камерата

Ако е поставена отметка в това квадратче, Kaspersky показва известие, когато приложение, за което достъпът е разрешен, използва уеб камерата. В прозореца за уведомявания може да редактирате настройките на достъпа на приложението до уеб камерата или изберете да не получавате никакви допълнителни известия.

Под **Настройки за микрофон**, можете да редактирате следните настройки:

Блокиране на достъпа на всички приложения до вашия микрофон

Ако е поставена отметка в квадратчето, достъпът до микрофона е блокиран за всички приложения, инсталирани на Вашия компютър.

Уведоми, ако дадено приложение използва микрофона

Ако е поставена отметка в това квадратче, Kaspersky показва известие, когато приложение, за което достъпът е разрешен, използва микрофона. В прозореца за уведомявания може да редактирате настройките на достъпа на приложението до микрофона или да изберете да не получавате повече допълнителни известия.

Научете повече за достъпа до уеб камера и микрофон

Открито е подозрително пренасочване

Изтрий записите

Kaspersky изтрива всички подозрителни записи от хост файла.

Пропусни

Kaspersky не изтрива подозрителни записи, ако са предоставени в списъка, от хост файла.

Списък с подозрителни записи

Този списък съдържа адреси на злонамерени или непознати уеб сървъри, към които сте препратени, когато приложението се опита да се свърже към сървъри на Kaspersky.

Съветваме ви да изтриете подозрителните записи от файла hosts.

Прозорец на въвеждане на парола

Текуща парола

Текущата парола, използвана за управление на Kaspersky.

Запомни паролата за тази сесия

Ако е поставена отметка в това квадратче, Kaspersky запомня въведената парола и повече не Ви напомня за нея, по време на текущата сесия.

Прозорец на защита на паролата

Връзката **Change or remove password** е налична, ако дадена парола е зададена по-рано, за да защити достъпа до функциите на Kaspersky.

Смени или премахни паролата

Когато е щракнато върху тази връзка, полетата за въвеждане стават достъпни за посочване на нова парола и за потвърждаването ѝ.

Нова парола

Парола за управление на Kaspersky.

Потвърждение на паролата

Въведете повторно паролата, която сте въвели в полето **Нова парола**.

В раздела **Обхват на парола** може да посочите кои части на управлението на приложението искате да защитите с парола.

Конфигуриране на програмни настройки

Квадратчето за отметка активира / деактивира показването на подканата за парола, когато потребител се опита да запише промените в настройките на приложението.

Управление на Архивиране и възстановяване

Това квадратче за отметка активира/деактивира опцията, която подканва потребителя за парола при опит за отваряне на прозореца **Архивиране и възстановяване**.

Излезте от приложението

Квадратчето за отметка активира / деактивира показването на подканата за парола, когато потребител се опита да затвори приложението.

Премахване на приложението

Това квадратче за отметка активира / деактивира показването на подканата за парола, когато потребител се опита да премахне приложението.

Настройки за сканиране

Таблицата описва настройките, които контролират следните типове сканирания: Пълно сканиране, Бързо сканиране, Сканиране по избор и Незабавно сканиране на файлове.

Настройки	Описание
Ниво на защита	Kaspersky използва различни набори настройки за сканиране. Наборите настройки, които се съхраняват в приложението се наричат *нива на защита*: • **Изключително**. Приложението Kaspersky сканира всички видове файлове. Когато сканира съставни файлове, приложението сканира също така файлове във формат на поща. • **Оптимално**. Приложението Kaspersky сканира само посочените файлови формати на всички твърди дискове, мрежови дискове, преносими носители за съхранение и вградени OLE обекти. Приложението не сканира архиви и инсталационни пакети. • **Ниско**. Приложението Kaspersky сканира единствено нови и променени файлове с определени разширения на файл на всички твърди дискове на компютъра, сменяеми устройства и мрежови дискове. Приложението не сканира съставни файлове.

Действие при откриване на заплаха	• **Питай потребителя**. Ако приложението Kaspersky открие заразен или вероятно заразен обект по време на сканиране, то незабавно ще Ви уведоми за това събитие и ще Ви подкани да предприемете действие върху открития обект.
	Тази опция е налична, ако квадратчето за отметка **Изпълнявай препоръчаните действия автоматично** е изчистено под **Настройки → Настройки за производителност → Използване на ресурси на компютъра**.
	• **Избери действие автоматично**. Когато бъдат открити заразени или вероятно заразени обекти, Kaspersky изпълнява действието, което се препоръчва от специалистите на Kaspersky:
	  • Kaspersky първо се опитва да дезинфектира заразения обект. Ако дезинфекцията не успее, файлът се изтрива.
	  • Kaspersky изтрива вероятно заразен обект, ако е избрано квадратчето за отметка **Изтриване на злонамерени инструменти, рекламен софтуер, програми за автоматично набиране и подозрителни пакетиращи програми**. Ако е премахната отметката от квадратчето, приложението не изтрива вероятно заразения обект. Вместо това се показва известие за този обект в Центъра за уведомявания (щракнете върху бутона **Детайли** в основния прозорец на приложението, за да го отворите).
	Тази опция е налична, ако квадратчето за отметка **Изпълнявай препоръчаните действия автоматично** е избрано под **Настройки → Настройки за производителност → Използване на ресурси на компютъра**.
	• **Дезинфектирай; изтрий, ако дезинфектирането е неуспешно**. Ако е избрана тази опция, приложението автоматично се опитва да дезинфектира всички заразени файлове, които бъдат открити. Ако дезинфекцията не успее, приложението изтрива обектите.

	• **Дезинфектирай; блокирай, ако дезинфектирането е неуспешно**. Ако изберете това действие, Kaspersky автоматично ще се опита да дезинфектира всички заразени файлове, които открие. Ако дезинфекцията не успее, приложението ще добави информация за заразените файлове, които открие, в списъка на откритите обекти. • **Уведоми**. Ако е избрана тази опция, приложението Kaspersky ще добави информация за заразени файлове, които открие, в списъка на откритите обекти. Преди да опита да дезинфектира или изтрие заразен файл, приложението създава резервно копие в случай, че след това трябва да възстановите файла или стане възможно да се дезинфектира по-късно.
Редактиране на обхват на сканиране (не е налично в настройките за сканиране на контекстното меню)	Щракването върху връзката отваря прозорец със списък с обекти, които приложението Kaspersky може да сканира. В зависимост от типа сканиране (Пълно сканиране, Бързо сканиране или Сканиране по избор) в списъка ще бъдат включени различни обекти по подразбиране. Може да добавяте обекти към списъка или да изтривате обектите, които добавяте. За да премахнете обект от сканирането, не трябва да изтривате обекта от списъка. Всичко, което трябва да направите, е да премахнете отметката от полето до името на обекта.
График на сканиране (не е налично в настройките за сканиране на контекстното меню)	**Ръчно**. Режим за стартиране, в който може ръчно да стартирате сканиране във време, в който е удобно за вас. **По график**. Режим за стартиране на сканиране, в който приложението стартира задачата за сканиране според графика, който сте създали. Ако изберете този режим за стартиране на сканиране, може да стартирате задачата за сканиране ръчно.
Стартирай сканиране като	Щракване върху връзката отваря прозорец, в който може да изберете да стартирате сканирането с конкретни потребителски права. По подразбиране задачата за сканиране се стартира от името на потребителя, чиито права сте регистрирали в операционната система. Обхватът на защита може да включва мрежови дискове или други обекти, които изискват специални права за достъп. Може да посочите потребител, който притежава необходимите права, в настройките на приложението и да стартирате задачата за сканиране от името на този потребител.
Типове файлове	Приложението Kaspersky третира файлове без разширения като изпълними. Приложението винаги ги сканира, независимо от типовете файлове, които сте избрали за сканиране. **Всички файлове**. Ако тази настройка е активирана, Kaspersky сканира всички файлове без изключение (всички формати и разширения). **Файлове, сканирани по формат**. Ако изберете тази настройка, приложението ще сканира само потенциално заразени файлове. Преди да търсите злонамерен код във файл, вътрешната му заглавна част се анализира, за да се определи форматът на файла (например TXT, DOC, EXE). Сканирането също така търси файлове с конкретни файлови разширения.

	Файлове, сканирани по разширение. Ако изберете тази настройка, приложението ще сканира само потенциално заразени файлове. Файловият формат се определя въз основа на разширението на файла.
Сканирай само новите и променени файлове	Сканира само новите файлове и тези файлове, които са били променени от последния път, когато са сканирани. Това ви позволява да спестите време при сканиране. Този режим на сканиране важи за обикновени и състави файлове.
Пропускай обектите, сканирани по-дълго от N секунди	Ограничава продължителността за сканиране на единичен обект. След кат изтече посоченото време, приложението ще спре сканирането на файла. Това ви позволява да спестите време при сканиране.
Сканирай архиви	Сканира ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и други архиви. Приложението сканира архиви не само по тяхното разширението, но и по техния формат.
Сканиране на пакети за разпространение	Квадратчето за отметка активира/деактивира сканирането на пакети за разпространение на трети страни.
Сканиране на файлове с формати на Microsoft Office	Сканиране на файлове на Microsoft Office (DOC, DOCX, XLS, PPT и други разширения на Microsoft). Файловете с формати на Office също включват OLE обекти.
Сканиране на имейл формати	Това квадратче за отметка активира / деактивира опцията за Kaspersky да сканира файлове в имейл формати и пощенски бази данни. Приложението сканира напълно единствено пощенски файлови формати на Microsoft Outlook, Windows Mail/Microsoft Outlook Express и EML и само ако компютърът има пощенски клиент Microsoft Outlook x86. Ако е поставена отметка в това квадратче, Kaspersky анализира файла в имейл формат и всеки компонент (текст, прикачени файлове) за вируси. Ако е премахната отметката от квадратчето, Kaspersky сканира файла в имейл формат като единичен обект.
Сканирай архиви защитени с парола	Ако е поставена отметка в квадратчето, приложението сканира защитени с парола архиви. Преди да могат да бъдат сканирани файловете в архива, на екрана ще се покаже запитване за парола. Ако не е поставена отметка в квадратчето, приложението пропуска сканирането на защитени с парола архиви.
Не разопаковай големи съставни файлове **Максимален размер за файл**	Ако е поставена отметка в квадратчето за отметка, приложението не сканира съставни файлове, които са по-големи от посочената стойност. Ако отметката е премахната от това квадратче, приложението сканира съставни файлове от всякакви размери. Приложението сканира големи файлове, които са извлечени от архиви, независимо дали квадратчето за отметка е отбелязано, или не.
Евристичен анализ	Техника за откриване на заплахи, които не могат да бъдат идентифицирани с помощта на текущата версия на базите данни на приложенията на Kaspersky. Тя ви позволява да откривате файлове, които може да съдържат непознат злонамерен софтуер или нова модификация на позната злонамерена програма.

	Когато сканирате файлове за злонамерен код, евристичният анализатор изпълнява инструкциите в изпълнимите файлове. Броят инструкции, изпълнени от евристичния анализатор, зависи от нивото, което е посочено за него. Нивото на евристичния анализ задава баланса между задълбочеността на търсенията за нови заплахи, натоварването на ресурсите на операционната система и времето, необходимо за евристичен анализ.
Технология iSwift	Тази технология е разработка на технологията iChecker за компютри с файлова система NTFS. Има ограничения за технологията iSwift: обвързана е с местоположението на конкретен файл във файловата система и работи само с обекти във файловата система NTFS. Когато надстроите приложението Kaspersky до нова версия, технологията iSwift е разрешена за всички типове сканирания, дори ако е била забранена преди това.
Технология iChecker	Тази технология позволява увеличаване на скоростта на сканиране чрез изключване на определени файлове от сканиране. Файловете се изключват от сканиране с помощта на специален алгоритъм, който взема предвид датата на публикуване на базите данни на приложението Kaspersky, датата, когато файлът е сканиран за последен път и всички промени на настройките за сканиране. Има ограничения за технологията iChecker: тя не работи с големи файлове и се прилага само за файлове със структура, която приложението разпознава (например, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP и RAR).

Настройки за сканиране на сменяемо устройство

Настройки	Описание
Действие, когато е свързано сменяемо устройство	• **Бързо сканиране**. Ако изберете тази опция, то след като свържете външно устройство, Kaspersky ще сканира единствено файлове в определени формати, които са по-податливи на заразяване, и се намират в основната папка. Освен това Бързо сканиране не включва декомпресиране и сканиране на архиви. • **Подробно сканиране**. Ако това квадратче за отметка е отбелязано, то след като свържете външно устройство, Kaspersky ще сканира всички файлове във всяка папка на външното устройство. Освен това ще декомпресира и сканира архиви без защитените с парола.
Максимален размер на сменяемо устройство	Ако това квадратче за отметка е отбелязано, Kaspersky ще сканира всички външни устройства, които не надвишават посочения максимален размер. Ако отметката е премахната от това квадратче, Kaspersky сканира външни устройства от всякакви размери.
Показване на напредъка при сканиране	Ако е избрано това квадратче за отметка, Kaspersky показва напредъка на сканиранията на външни устройства в отделен прозорец и в прозореца на текущото сканиране.
Блокиране на спирането на задачата за сканиране	Ако е избрано това квадратче за отметка, бутонът **Спри** не е наличен за сканирания на външни устройства в прозореца на текущото сканиране.

Настройки за фоново сканиране

Ако е активирано сканиране във фонов режим, Kaspersky ще извърши фоново сканиране. Сканиране във фонов режим е автоматичен режим на сканиране, който не показва известия. Това сканиране изисква по-малко компютърни ресурси от други типове сканирания (например Пълно сканиране). Когато е в този режим, Kaspersky сканира системната памет, системните обеми, сектори за начално стартиране и обекти на стартиране, и търсения за комплекти за пълен достъп.

Ако компютърът работи със захранване от батерията, Kaspersky няма да извършва сканирания във фонов режим, когато компютърът е неактивен.

Настройки на сканиране за уязвимост на приложението

Настройки	Описание
Редактиране на обхват на търсене	Щракването върху връзката отваря прозореца **Обхват на сканиране за уязвимости в приложения** със списък с обекти, които се сканират за уязвимости в приложенията. Може да добавяте обекти към списъка или да изтривате обектите, които добавяте. За да премахнете обект от сканирането, не трябва да изтривате обекта от списъка. Всичко, което трябва да направите, е да премахнете отметката от полето до името на обекта.
Търсене на график	**Ръчно**. Режим на изпълнение, в който можете да стартирате ръчно сканирането на уязвимостите на приложения в удобно време. **По график**. Режим за стартиране на сканиране, в който приложението стартира задачата за сканиране според графика, който сте създали. Ако изберете този режим за стартиране на сканиране, може да стартирате задачата за сканиране ръчно.

Настройки на акаунта

Стартирай сканиране като

Изберете акаунт, чиито права ще се използват от Kaspersky за стартиране на задачите за сканиране. Функцията е налична за стартиране на ръчни сканирания и планирани сканирания.

Налични са следните опции:

- **Настоящ потребител**. Задачи за сканиране ще бъдат стартирани с правата на текущия акаунт.
- **Друг потребител**. Посоченият потребителски акаунт ще се използва за стартиране на задачи за сканиране. Ако изберете тази опция, напишете името на акаунта и парола в полетата **Акаунт** и **Парола** съответно.

Настройки на Защита от банери

Активирай / деактивирай Защита от банери

Този превключвател за отметка активира/деактивира Защитата от банери.

Ако бутонът е зелен, Защитата от банери блокира показването на банери, показвани на уеб сайтовете, които посещавате, и в интерфейса на някои приложения. По подразбиране Защитата от банери блокира банерите на уеб сайтове от списъка с известни банери. Този списък е включен в базите данни на Kaspersky.

Списък на филтрите

Щракването върху тази връзка отваря прозореца **Списък на филтрите**, в който може да използвате специални филтри, за да посочите в повече детайли точно кои банери трябва да бъдат блокирани.

Уеб сайтове с разрешени банери

Щракването върху тази връзка отваря прозорец със списък с уеб сайтове, на които сте разрешили показването на банери.

Блокирани банери

Щракването върху тази връзка отваря прозореца **Блокирани банери**. Може да използвате този прозорец, за да създадете списък с банери, които да бъдат блокирани.

Разрешени банери

Щракването върху тази връзка отваря прозореца **Разрешени банери**. Може да използвате този прозорец, за да създадете списък с банери, които да бъдат разрешени.

Разрешава банерите на уеб сайтовете на Kaspersky

Ако е поставена отметка в квадратчето, Защитата от банери не блокира банери на уеб сайтове на Kaspersky или уеб сайтове на партньорите му, които хостват реклами на Kaspersky. Списък с тези уеб сайтове е наличен чрез връзката **Уеб сайтове на Kaspersky**.

Уеб сайтове на Kaspersky

Щракването върху тази връзка отваря прозорец със списък с уеб сайтове на Kaspersky.

Тази връзка е налична, ако е поставена отметка в квадратчето **Разрешава банерите на уеб сайтовете на Kaspersky**.

Прозорец на Добавяне/Редактиране на банер

Маска за уеб адрес (URL)

IP адрес, уеб адрес (URL) или маска на уеб адрес.

Когато въвеждате маска на уеб адрес, може да използвате заместващите знаци * и ?, където * представлява всякаква поредица от символи, а ? всеки единичен символ.

Статус

В раздела **Статус** може да посочите дали Защитата от банери използва този адрес, когато сканира банери.

Налични са следните опции:

- **Активен**. Защитата от банери използва този адрес, когато сканира банери.
- **Неактивен**. Защитата от банери не използва този адрес, когато сканира банери.

Прозорец за Добавяне/Редактиране на уеб сайт

Уеб сайт

Уеб адрес (URL) на уеб сайта.

Статус

Разделът **Статус** ви позволява да посочите дали Защитата от банери трябва да разреши или не показването на банери в посочения уеб сайт.

Налични са следните опции:

- **Активен**. Защитата от банери позволява показването на банери на посочения уеб сайт.
- **Неактивен**. Защитата от банери не позволява показването на банери на посочения уеб сайт.

Прозорец на Блокирани банери

Бутон

Щракването върху бутона отваря менюто със съответните елементи:

- **Импортиране и добавяне към съществуващи**. Избирането на този елемент отваря прозорец, който ви позволява да импортирате списък със забранени адреси от CSV файл. Настоящите адреси не се изтриват.
- **Импортиране и замяна на съществуващи**. Избирането на този елемент отваря прозорец, който ви позволява да импортирате списък със забранени адреси от CSV файл. Настоящите адреси се изтриват.
- **Експорт**. Избирането на този елемент отваря прозорец, който ви позволява да експортирате списък със забранени адреси в CSV файл.

Списък с блокирани банери

Съхранява адреси или маски на адреси на блокирани банери. Защитата от банери блокира даден банер, ако адресът му е в списъка с блокирани банери.

Може да добавите адрес или маска на адрес към списъка.

Ако е зададена стойността *Активен* в реда на адреса в колоната **Статус**, Защитата от банери използва този адрес, когато сканира банери.

Ако е зададена стойността *Неактивен* в реда на адреса в колоната **Статус**, Защитата от банери не използва този адрес, когато сканира банери.

Маска за уеб адрес (URL)

Тази колона показва адреса или маската на адреса на блокирания банер.

Статус

Тази колона показва дали Защитата от банери използва този адрес, когато сканира банери.

Ако е зададена стойността *Активен* в реда на адреса, Защитата от банери използва този адрес, когато сканира банери.

Ако е зададена стойността *Неактивен* в реда на адреса, Защитата от банери не използва този адрес, когато сканира банери.

Редактирай

Щракването върху този бутон отваря прозорец за смяна на адреса или маската на адреса на банер от списъка с блокирани банери.

Изтрий

След щракване върху този бутон Защитата от банери премахва избрания адрес / маска на адрес на банера от списъка.

Добави

Щракването върху този бутон отваря прозорец за добавяне на адреса или маската на адреса на банер в списъка с блокирани банери.

Прозорец на Разрешени банери

Бутон

Щракването върху бутона отваря менюто със съответните елементи:

- **Импортиране и добавяне към съществуващи**. Избирането на този елемент ви позволява да импортирате списък с разрешени адреси от CSV файл. Настоящите адреси не се изтриват.
- **Импортиране и замяна на съществуващи**. Избирането на този елемент ви позволява да импортирате списък с разрешени адреси от CSV файл. Настоящите адреси се изтриват.
- **Експорт**. Избирането на този елемент ви позволява да експортирате списък с адреси в CSV файл. Може да експортирате целия списък с адреси или отделни адреси, избрани от списъка.

Списък с разрешени банери

Съхранява адреси или маски на адреси на разрешени банери. Защитата от банери не блокира даден банер, ако адресът му е в списъка с разрешени банери.

Може да добавите адрес или маска на адрес към списъка.

Ако е зададена стойността *Активен* в реда на адреса в колоната **Статус**, Защитата от банери използва този адрес, когато сканира банери.

Ако е зададена стойността *Неактивен* в реда на адреса в колоната **Статус**, Защитата от банери не използва този адрес, когато сканира банери.

Маска за уеб адрес (URL)

Тази колона показва адреса или маската на адреса на разрешения банер.

Статус

Тази колона показва дали Защитата от банери използва този адрес, когато сканира банери.

Ако е зададена стойността *Активен* в реда на адреса, Защитата от банери използва този адрес, когато сканира банери.

Ако е зададена стойността *Неактивен* в реда на адреса, Защитата от банери не използва този адрес, когато сканира банери.

Редактирай

Когато щракнете върху този бутон, се отваря прозорец за смяна на адреса или маската на адреса на банер от списъка с разрешени банери.

Изтрий

Когато щракнете върху този бутон, Защитата от банери премахва избрания адрес / маска на адрес на банера от списъка с разрешени банери.

Добави

Когато щракнете върху този бутон, се отваря прозорец за добавяне на адреса или маската на адреса на банер в списъка с разрешени банери.

Прозорец на уеб сайтове с разрешени банери

Бутон

Щракването върху бутона отваря менюто със съответните елементи:

- **Импортиране и добавяне към съществуващи**. Избирането на този елемент ви позволява да импортирате списък с разрешени адреси от CSV файл. Настоящите адреси не се изтриват.
- **Импортиране и замяна на съществуващи**. Избирането на този елемент ви позволява да импортирате списък с разрешени адреси от CSV файл. Настоящите адреси се изтриват.
- **Експорт**. Избирането на този елемент ви позволява да експортирате списък с адреси в CSV файл. Може да експортирате целия списък с адреси или отделни адреси, избрани от списъка.

Списък с уеб сайтове с разрешени банери

Съдържа адресите на уеб сайтове, на които сте разрешили показването на банери. Защитата от банери не блокира банери на уеб сайт, ако адресът му е в списъка.

Ако е зададена стойността *Активен* в реда на адреса в колоната **Статус**, Защитата от банери разрешава показването на банери на този уеб сайт.

Ако е зададена стойността *Неактивен* в реда на адреса в колоната **Статус**, Защитата от банери блокира банери на този уеб сайт.

Редактирай

Щракването върху този бутон отваря прозорец за промяна на адреса, избран в списъка.

Изтрий

Щракването върху този бутон ще накара Защитата от банери да премахне избрания адрес на уеб сайт от списъка.

Добави

Щракването върху този бутон отваря прозорец за добавяне на адрес на уеб сайт в списъка.

Прозорец с уеб сайтове на Kaspersky

Този прозорец показва списък с уеб сайтове на Kaspersky и уеб сайтове на партньорите му, които не хостват реклами на Kaspersky.

Списъкът се съставя и актуализира от експертите на Kaspersky. Списъкът се актуализира автоматично, когато базите данни и модулите на приложението се актуализират.

Настройки на Защита от спам

Активирай / деактивирай Защита от спам

Този превключвател активира/деактивира защитата от спам.

Ако бутонът е активиран, Защитата от спам открива нежелан имейл (спам) и го обработва според правилата на вашия имейл клиент.

Ниво на защита

В раздела **Ниво на защита** може да изберете една от предварително определените колекции настройки (нива на защита) за Защита от спам. Решението кое ниво на защита трябва да изберете зависи от работните условия и текущата ситуация.

Налични са следните нива на защита:

- **Изключително**. При това ниво на защита Защитата от спам прилага максимален преглед при филтрирането на спам.

Съветваме ви да изберете високото ниво на защита, когато работите в опасна среда (например когато използвате безплатна пощенска услуга).

Настройването на високо ниво на защита може да доведе до по-чести случаи на категоризиране като спам на съобщения, които не са спам.

- **Оптимално**. Това ниво на защита гарантира оптимален баланс между работа и сигурност. Това ниво е подходящо за повечето ситуации.

- **Ниско**. При това ниво на защита Защитата от спам прилага минимално ниво на филтриране на спам.

Ниското ниво на защита се препоръчва да бъде зададено, когато работите в безопасна среда (например когато използвате шифрован корпоративен имейл).

Настройването на ниско ниво на защита може да доведе до по-малко случаи на категоризиране на съобщения, които не са спам, като спам или вероятен спам.

Възстановяване на оптимално ниво на защита

При щракване върху връзката приложението прилага нивото на защита **Оптимално**. Връзката се показва, ако сте променили настройките в прозореца **Advanced settings of Anti-Spam** в раздела **Не класифицирай съобщение като спам**.

Разширени настройки

Щракването върху връзката отваря разширените настройки на прозореца Защита от спам.

Разширени настройки на Защита от спам

В раздела **Класифицирай съобщение като спам** може да определите условията за филтриране на пощата, които Защита от спам използва, за да разпознае спам.

Ако има фишинг елементи

Това квадратче за отметка активира / деактивира сканиране на имейл съобщения за фишинг елементи в текста или URL адресите, включени в списъка с фишинг уеб адреси.

Ако е поставена отметка в това квадратче, Защита от спам смята съобщенията, съдържащи URL адреси, открити в списъка с фишинг уеб адреси, като спам.

Ако квадратчето за отметка не е отбелязано, Защита от спам не проверява URL адресите в съобщения в списъка с фишинг уеб адреси.

Ако има адреси от базата с вредоносни уеб адреси

Това квадратче за отметка активира / деактивира проверката дали връзките, съдържащи се в съобщенията, са включени в списъка със злонамерени URL адреси.

Ако е от забранен подател

Това квадратче за отметка активира / деактивира опцията на филтриране на пощата с помощта на списък с забранени податели; Защитата от спам класифицира съобщения от тези податели като спам.

Избор

Когато щракнете върху тази връзка, се отваря прозорецът **Забранени податели**, в който може да създадете списък със забранени податели.

Когато създавате списъка, може да посочите адресите и маските на адресите на блокираните податели.

Тази връзка е налична, ако е поставена отметка в квадратчето **Ако е от забранен подател**.

Ако съдържа забранени фрази

Това квадратче за отметка активира / деактивира филтрирането на съобщения според списъка със забранени фрази, чието наличие в съобщението показва, че то е спам.

Избор

Когато щракнете върху този бутон, се отваря прозорецът **Забранени фрази**, в който може да създадете списък със забранени фрази.

Когато създавате списъка, може да посочите забранените фрази и маски на фрази.

Тази връзка е налична, ако е поставена отметка в квадратчето **Ако съдържа забранени фрази**.

Ако съдържа нецензурни думи

Щракването върху тази връзка отваря прозореца **Нецензурна лексика**. В този прозорец може да създавате списък с нецензурни думи. Наличието на такива думи в дадено съобщение показва, че съобщението е спам.

Тази връзка е налична, ако е поставена отметка в квадратчето **Ако съдържа нецензурни думи**.

В раздела **Не класифицирай съобщение като спам** може да определите признаците, които Защита от спам използва, за да разпознае поща, която не е спам.

Ако е от разрешен подател

Това квадратче за отметка активира / деактивира проверката дали адрес на подател е включен в списъка с разрешени податели.

Ако е поставена отметка в това квадратче, Защита от спам класифицира съобщенията от разрешени податели като „не е спам“.

Ако е отметката е премахната от това квадратче, Защита от спам не класифицира съобщенията от разрешени податели като „не е спам“. Съобщения, изпратени от податели в списъка с разрешени податели, не се филтрират.

Избор

Когато щракнете върху тази връзка, се отваря прозорецът **Разрешени податели** в който може да създадете списък с разрешени податели.

Когато създавате списъка, може да посочите адреси на разрешени податели и маски на адреси.

Тази връзка е налична, ако е поставена отметка в квадратчето **Ако е от разрешен подател**.

Ако съдържа разрешени фрази

Това квадратче за отметка активира / деактивира проверката на съобщение в списъка с разрешени фрази.

Ако е поставена отметка в това квадратче, Защита от спам класифицира съобщенията, съдържащи фрази от този списък, като „не е спам“.

Ако е премахната отметката от това квадратче, Защита от спам не използва списъка с разрешени фрази, за да филтрира съобщения и не класифицира съобщения, съдържащи изрази от списъка, като „не е нежелана поща“.

Избор

Когато щракнете върху тази връзка, се отваря прозорецът **Разрешени фрази**, в който може да създадете списък с разрешени фрази.

Когато създавате списъка, може да посочите отделни фрази и маски на разрешени фрази.

Тази връзка е налична, ако е поставена отметка в квадратчето **Ако съдържа разрешени фрази**.

В раздела **Действия със съобщения**, може да посочите етикетите, които да се добавят към редовете на темата на съобщенията, които са със зададено състояние *Spam* или *Probable spam* от Защита от спам.

Добави Етикет [!! СПАМ] в темата на съобщенията, класифицирани като спам

Автоматично добавяне на етикет към темата на съобщения, които Защита от спам разпознава като *Спам*.

Текстът на етикета се показва в полето до квадратчето за отметка. По подразбиране Защита от спам добавя етикета **[!! SPAM]**.

Добави Етикет [?? Вероятен СПАМ] към темата на съобщение, класифицирано като потенциален спам

Автоматично добавяне на етикет към темата на съобщения, които Защита от спам разпознава като *Потенциален спам*.

Текстът на етикета се показва в полето до квадратчето за отметка. По подразбиране Защита от спам добавя етикета **[?? Probable SPAM]**.

Прозорец на Добавяне/Редактиране на забранена фраза

Маска на фраза

Фраза или маска на фраза, която, когато е открита в съобщение, се счита за знак за спам.

Тегловен коефициент на фраза

Цифрова стойност, която отразява вероятността дадено съобщение, съдържащо забранена фраза, да е спам. Колкото по-висок е тегловният коефициент, толкова по-висока е вероятността съобщението, съдържащо забранена фраза, да е спам.

Защитата от спам маркира съобщение като спам, ако сумата от тегловните коефициенти на забранени фрази в него надвишава посочената стойност.

Статус

В раздела **Статус** може да посочите дали искате Защита от спам да проверява съобщения за забранени фрази:

- **Активен**. Защитата от спам сканира съобщения, за да провери дали не съдържат забранени фрази.
- **Неактивен**. Защитата от спам не сканира съобщения, за да провери дали не съдържат забранени фрази.

Прозорец на Забранени податели

Бутон

Щракването върху този бутон отваря меню с избор на следните действия:

- **Импортиране и добавяне към съществуващи**. Избирането на тази опция ви позволява да импортирате списък със забранени податели от CSV файл. Настоящият списък с податели не се изтрива.
- **Импортиране и замяна на съществуващи**. Избирането на тази опция ви позволява да импортирате списък със забранени податели от CSV файл. Настоящият списък с податели се изтрива.
- **Експорт**. Избирането на тази опция ви позволява да експортирате списък със забранени податели в CSV файл.

Списък със забранени податели

Съдържа списък с адреси, които Защита от спам класифицира като източници на спам.

Може да добавите адрес или маска на адрес към списъка.

Ако е зададена стойността *Активен* в реда на адреса в колоната **Статус**, Защита от спам класифицира адреса като забранен.

Ако е зададена стойността *Неактивен* в реда на адреса в колоната **Статус**, Защита от спам изключва адреса от списъка.

Адрес на подател

Тази колона показва имейл адреса или маската на имейл адреса на забранения подател.

Статус

Тази колона показва дали Защита от спам класифицира съобщения, които са получени от този адрес, като спам.

Ако е зададена стойността *Активен* в реда на адреса, Защита от спам класифицира съобщения, получени от този адрес, като спам.

Ако е зададена стойността *Неактивен* в реда на адреса, Защита от спам изключва избрания адрес от списъка.

Редактирай

Когато щракнете върху този бутон, се отваря прозорец за смяна на URL адреса или маска на URL адреса, който е избран от списъка.

Изтрий

Когато щракнете върху този бутон, Защита от спам премахва избрания адрес или маска на адрес от списъка.

Добави

Когато щракнете върху този бутон, се отваря прозорец за добавяне на URL адрес или маска на URL адрес в списъка.

Прозорец на Забранени фрази

Бутон

Щракването върху този бутон отваря меню с избор на следните действия:

- **Импортиране и добавяне към съществуващи**. Избирането на тази опция ви позволява да импортирате списък със забранени фрази от CSV файл. Настоящите фрази не се изтриват.
- **Импортиране и замяна на съществуващи**. Избирането на тази опция ви позволява да импортирате списък със забранени фрази от CSV файл. Настоящите фрази се изтриват.
- **Експорт**. Избирането на тази опция ви позволява да експортирате списък със забранени фрази в CSV файл.

Списък със забранени фрази

Съдържа ключови фрази, които показват, че съобщението, в което се съдържат, е спам.

Може да добавите фраза или маска на фраза към списъка.

Ако е зададена стойността *Активен* в реда на фразата в колоната **Статус**, Защита от спам използва тази фраза при филтриране на съобщения.

Ако е зададена стойността *Неактивен* в реда на фразата в колоната **Статус**, Защита от спам изключва фразата от списъка и не я използва при филтриране на съобщения.

Редактирай

Когато щракнете върху този бутон, се отваря прозорец, в който може да смените фраза или маска на фраза, избрани в списъка.

Изтрий

Когато щракнете върху този бутон, Защита от спам премахва избраната фраза или маска на фраза от списъка.

Добави

Когато щракнете върху този бутон, се отваря прозорец, в който може да добавите фраза или маска на фраза в списъка.

Прозорец на Добавяне/Редактиране на имейл адрес

Маска на имейл адрес

В този прозорец може да посочите имейл адрес или маска на имейл адрес.

Когато въвеждате маска, може да използвате заместващите знаци `*` and `?`, където `*` представлява всякаква поредица от символи, а `?` всеки единичен символ.

Статус

В раздела **Статус** може да посочите дали искате Защита от спам да блокира съобщения, които са изпратени от този адрес, когато сканира съобщения според списъка с разрешени/забранени податели.

- **Активен**. Защита от спам блокира съобщения, които се изпращат от този адрес.
- **Неактивен**. Защита от спам не блокира съобщения, които се изпращат от този адрес.

Прозорец на Добавяне/Редактиране на разрешена фраза

Маска на фраза

Фраза или маска на фраза, чието наличие в дадено съобщение показва, че то не е спам.

Тегловен коефициент на фраза

Цифрова стойност, която отразява вероятността дадено съобщение, съдържащо разрешена фраза, да не е спам. Колкото по-висок е тегловният коефициент, толкова по-висока е вероятността съобщението, съдържащо разрешената фраза, да не е спам.

Защитата от спам не маркира съобщение като спам, ако сумата от тегловните коефициенти на разрешени фрази в него надвишава посочената стойност.

Статус

В раздела **Статус** може да посочите дали Защита от спам ще сканира съобщения, за да провери дали включват конкретна разрешена фраза.

- **Активен**. Защитата от спам сканира съобщения, за да провери дали включват разрешена фраза.
- **Неактивен**. Защитата от спам не сканира съобщения, за да провери дали включват разрешена фраза.

Прозорец на Разрешени податели

Бутон

Щракването върху този бутон отваря меню с избор на следните действия:

- **Импортиране и добавяне към съществуващи**. Избирането на тази опция ви позволява да импортирате списък с разрешени податели от CSV файл. Настоящият списък с податели не се изтрива.
- **Импортиране и замяна на съществуващи**. Избирането на тази опция ви позволява да импортирате списък с разрешени податели от CSV файл. Настоящият списък с податели се изтрива.
- **Експорт**. Избирането на тази опция ви позволява да експортирате списък с разрешени податели в CSV файл.

Списък с разрешени податели

Съдържа списък с адреси на податели, чиито съобщения се класифицират от Защита от спам като „не е спам“.

Може да добавите адрес или маска на адрес към списъка.

Ако е зададена стойността *Активен* в реда на адреса в колоната **Статус**, Защита от спам класифицира някакви съобщения от този подател като „не е спам“.

Ако е зададена стойността *Неактивен* в реда на адреса в колоната **Статус**, Защита от спам не класифицира всички съобщения от този подател като „не е спам“ и ги сканира с помощта на стандартни методи за сканиране.

Адрес на подател

Тази колона показва имейл адреса или маската на имейл адреса на разрешения подател.

Статус

Тази колона показва дали Защита от спам класифицира съобщения, които са получени от този адрес, като „не е спам“.

Ако е зададена стойността *Активен* в реда на адреса, Защита от спам класифицира съобщения, получени от този адрес, като „не е спам“.

Ако е зададена стойността *Неактивен* в реда на адреса, Защита от спам изключва избрания адрес от списъка.

Редактирай

Когато щракнете върху този бутон, се отваря прозорец, в който може да промените URL адрес или маска на URL адрес в списъка с разрешени податели.

Изтрий

Когато щракнете върху този бутон, Защита от спам премахва избрания адрес или маска на адрес от списъка.

Добави

Когато щракнете върху този бутон, се отваря прозорец, в който може да добавите URL адрес или маска на URL адрес към списъка с разрешени податели.

Добавяне на получателите на моите имейл съобщения към разрешените податели

Ако е поставена отметка в квадратчето, приложението добавя получатели на поща към вашия списък с разрешени податели.

Прозорец на разрешени фрази

Бутон

Щракването върху този бутон отваря меню с избор на следните действия:

- **Импортиране и добавяне към съществуващи**. Избирането на тази опция ви позволява да импортирате списък с разрешени фрази от CSV файл. Настоящите фрази не се изтриват.
- **Импортиране и замяна на съществуващи**. Избирането на тази опция ви позволява да импортирате списък с разрешени фрази от CSV файл. Настоящите фрази се изтриват.
- **Експорт**. Избирането на тази опция ви позволява да експортирате списък с разрешени фрази в CSV файл.

Списък с разрешени фрази

Съдържа ключови изрази, чието наличие в дадено съобщение показва, че то не е спам.

Може да добавите фраза или маска на фраза към списъка.

Ако е зададена стойността *Активен* в реда на фразата в колоната **Статус**, Защита от спам използва тази фраза при филтриране на съобщения.

Ако е зададена стойността *Неактивен* в реда на фразата в колоната **Статус**, Защита от спам не използва тази фраза, когато филтрира съобщения.

Редактирай

Когато щракнете върху този бутон, се отваря прозорец, в който може да смените фразата или маската на фраза, избрани в списъка.

Изтрий

Когато щракнете върху този бутон, Защита от спам премахва избраната фраза или маска на фраза от списъка.

Добави

Когато щракнете върху този бутон, се отваря прозорец, в който може да добавите фраза или маска на фраза в списъка.

Настройки на Безопасно плащане

Активирай/деактивирай Безопасно плащане

Този бутон активира / деактивира Безопасно плащане.

Ако бутонът е зелен, приложението наблюдава всички опити за достъп до уеб сайтове за банкиране или системи за плащане и извършва действия, зададени по подразбиране или конфигурирани от потребителя. По подразбиране когато стартирате режим за безопасно плащане, приложението подканва потребителя за потвърждение за стартиране на Защитен браузър.

Ако бутонът е червен, приложението разрешава посещаването на уеб сайтове на банки или системи за плащане през стандартен браузър.

Научете повече

Щракването върху този бутон отваря страница с детайли на компонентите в прозорец на браузър.

В раздела **При първия достъп до уеб сайтове на банки и системи за плащане** може да изберете действие, което приложението изпълнява, когато осъществявате достъп до уеб сайтове на банки или системи за плащане за първи път.

Стартирай Защитен браузър

Ако приложението засече опит за достъп до посочения уеб сайт, ще отвори уеб сайта в Защитен браузър. Стандартният браузър, използван за достъп до уеб сайта, показва съобщение, което ви информира, че Защитеният браузър се стартира.

Питай потребителя

Ако приложението засече опит за достъп до посочения уеб сайт, той ще Ви подкани да стартирате Защитен достъп или да отворите уеб сайта със стандартен браузър.

Не стартирай Защитен браузър

Когато се опитвате да осъществите достъп до посочения уеб сайт, приложението не използва Защитен браузър. Уеб сайтът се отваря в стандартен браузър.

В раздела **Допълнително** може да конфигурирате допълнителни настройки за Безопасно плащане.

Използвайте следния браузър за Безопасно плащане Браузър по подразбиране

От падащия списък може да изберете браузъра, с който приложението ще отвори уеб сайтовете за банкиране или системи за плащане, които са избрани в прозореца Безопасно плащане.

Безопасно плащане е налично за потребители на следните браузъри: Microsoft Internet Explorer, Microsoft Edge, базиран на Chromium, Mozilla Firefox, Google Chrome и Yandex.Browser.

По подразбиране Безопасно плащане използва браузъра, който е браузъра по подразбиране в операционната система.

Създай кратък път за Безопасно плащане

Щракването върху тази връзка създава пряк път на работния плот за стартиране на Безопасно плащане. Този пряк път позволява да се отвори прозорец, който съдържа списък с уеб сайтове на банки или системи за плащане, за които се използва Защитен браузър за достъп.

В 64-битовите версии на Windows 8, Windows 8.1 и Windows 10 виртуализацията на хардуер се използва за защита на браузъра.

Настройки на Безопасно сърфиране

Настройки	Описание
Ниво на защита	Приложението използва различни групи от настройки, за да стартира Безопасно сърфиране. Наборите настройки, които се съхраняват в приложението се наричат *нива на защита*: • **Изключително**. Нивото на защита на уеб трафика, който Безопасно сърфиране използва да сканира внимателно уеб трафика, който се получава от компютъра по HTTP и FTP протоколи. Безопасно сърфиране изпълнява подробно сканиране на всички обекти от уеб трафика с пълен набор бази данни на приложението и извършва най-дълбокия евристичен анализ. • **Оптимално**. Нивото на защита на уеб трафика, което постига оптималния баланс между работата на приложението Kaspersky и сигурността на уеб трафика. Безопасно сърфиране извършва евристичен анализ на средно ниво. Това ниво на защита на уеб трафика се препоръчва от специалистите на Kaspersky. • **Ниско**. Нивото на защита на уеб трафика, чиито настройки гарантират максимална скорост на сканиране на уеб трафика. Безопасно сърфиране извършва евристичен анализ на леко ниво.
Действие при откриване на заплаха	• **Уведоми**. Безопасно сърфиране ви информира за откриването на заразен или вероятно заразен обект и ви подканва за действието, което да предприемете. Тази опция е налична, ако квадратчето за отметка **Изпълнявай препоръчаните действия автоматично** е изчистено под **Настройки** → **Настройки за производителност** → **Използване на ресурси на компютъра**. • **Извършете действие автоматично**. Безопасно сърфиране избира действие автоматично според текущите настройки. Ако уеб ресурс е изброен като изключение или съдържа незаразени или вероятно заразени обекти, Безопасно сърфиране разрешава достъп до него. Ако сканиране, извършено от Безопасно сърфиране, открие заразен или вероятно заразен обект в уеб ресурса, достъпът до него е блокиран. Тази опция е налична, ако квадратчето за отметка **Изпълнявай препоръчаните действия автоматично** е избрано под **Настройки** → **Настройки за производителност** → **Използване на ресурси на компютъра**. • **Забрани изтеглянето**. Ако изберете тази опция и ако заразен обект бъде открит в уеб трафика, Безопасно сърфиране блокира достъпа до този обект и показва съобщение в браузъра.
Методи за сканиране **Проверка на уеб адреса в базата данни за злонамерени уеб адреси**	Сканирането на връзките, за да се определи дали трябва да бъдат включени в базата данни със злонамерени връзки ви разрешава да проследявате уеб сайтове, които са били добавени в списък с отказ. Базата данни със злонамерени връзки се генерира от специалистите на Kaspersky. Тя е част от комплекта за разпространение на софтуера и се актуализира заедно с базата данни на приложението Kaspersky.

Проверка на уеб адреса в базата данни за уеб адреси, съдържащи рекламен софтуер	Пример може да бъде софтуер, който препраща вашата заявка за търсене в интернет към рекламен уеб сайт. По този начин отивате на рекламен уеб сайт вместо уеб ресурса, който е най-подходящ за вашата заявка за търсене.
Проверка на URL адреса в базата данни за URL адреси, съдържащи легитимни приложения, които може да се използват от нарушители за повреждане на вашия компютър или лични данни	Пример за тази категория може да бъде инструмент за отдалечено управление, който се използва легално за отстраняване на неизправности от системните администратори. Престъпник може да инсталира такъв инструмент на вашия компютър без ваше знание, за да получи достъп до вашия компютър и да го използва за престъпни цели. Приложението Kaspersky позволява изтегляне на такива приложения чрез щракване върху връзки на уеб страници. Връзките за еднократна употреба са изключение. Не можете да ги използвате, за да изтегляте легитимни приложения, които хакерите могат да използват, за да причинят вреда на вашия компютър или вашите данни.
Използвай евристичен анализ	Техника за откриване на заплахи, които не могат да бъдат идентифицирани с помощта на текущата версия на базите данни на приложенията на Kaspersky. Тя ви позволява да откривате файлове, които може да съдържат непознат злонамерен софтуер или нова модификация на позната злонамерена програма. Когато уеб трафикът се сканира за вируси и други приложения, които представляват заплаха, евристичният анализатор извършва инструкции в изпълнимия файл. Броят инструкции, изпълнени от евристичния анализатор, зависи от нивото, което е посочено за него. Нивото на евристичния анализ задава баланса между задълбочеността на търсенията за нови заплахи, натоварването на ресурсите на операционната система и времето, необходимо за евристичен анализ.
Анти-фишинг **Провери уеб адреса в базата данни за фишинг и фалшиви крипто URL адреси** (в някои абонаментни планове **Проверка на уеб адреса в базата данни за фишинг уеб адреси**)	Съдържанието на фишинг връзки и база данни за обмен на фалшиви криптовалути включва уеб адреси на известни в момента уеб сайтове, които се използват за фишинг атаки. Kaspersky допълва тази база данни с адреси, получени от международната организация на Работната група за борба с фишинга. Базата данни с фишинг връзки и база данни за обмен на фалшиви криптовалути е част от комплекта за разпространение на софтуера и се актуализира заедно с базата данни на приложението Kaspersky.
Използвай евристичен анализ	Техника за откриване на заплахи, които не могат да бъдат идентифицирани с помощта на текущата версия на базите данни на приложенията на Kaspersky. Това разрешава откриването на фишинг дори ако уеб адресът не е в базата данни с фишинг уеб адреси.
Сканирай уеб адресите	Компонентът Сканиране на уеб адреси проверява връзките на уеб страница, отворена в Microsoft Edge, базиран на Chromium, Google Chrome или Mozilla Firefox. Приложението Kaspersky показва една от следните икони до проверената връзка: – ако свързаната уеб страница е безопасна според Kaspersky – ако няма информация за безопасното състояние на свързаната уеб страница - ако според Kaspersky хакерите могат да навредят на компютъра ви или на данните ви, като използват уебстраницата, към която води връзката; - ако според Kaspersky уебстраницата, към която води връзката, може да е заразена или хакната;

	– ако свързаната уеб страница е опасна според Kaspersky За да видите изскачащ прозорец с повече детайли за връзката, преместете показалеца на мишката към съответната икона.
На всички уеб сайтове с изключение на онези, които са указани **Управление на изключения**	Когато е избрана тази опция, приложението сканира връзки на всички уеб сайтове без тези, посочените в прозореца **Изключения**. Прозорецът **Изключения** се отваря, чрез щракване върху връзката **Управление на изключения**.
Само на указаните уеб сайтове **Конфигуриране на проверени уеб сайтове**	Когато е избрана тази опция, Kaspersky сканира връзки само на тези уеб сайтове, които са посочени в прозореца **Проверени уеб сайтове**. Прозорецът **Проверени уеб сайтове** се отваря, чрез щракване върху връзката **Конфигуриране на проверени уеб сайтове**.
Конфигуриране на Сканиране на уеб адреси	• **Всички адреси**. Приложението сканира връзки на всички типове уеб страници. • **Само адресите в резултатите от търсене**. Приложението сканира връзки на уеб страници, съдържащи резултати от търсене, получени от търсачки.
Категории уеб сайтове	Ако е поставена отметка в квадратчето **Показвай информация за категориите съдържание на уеб сайтове**, приложението добавя към връзката коментари, за да посочи дали уеб сайтът принадлежи към една от посочените категории (например **Насилие** или **Съдържание за възрастни**). Може да премахнете отметките в квадратчетата до категориите, които не изискват предупреждения.
Не сканирай уеб трафика от сигурни уеб адреси	Ако е поставена отметка в квадратчето, Безопасно сърфиране не сканира съдържанието на уеб страници/уеб сайтове, чиито адреси са включени в списъка с надеждни уеб адреси. Може да добавите специфични уеб страници/адреси на уеб сайтове и маски на уеб страници/адреси на уеб сайтове към списъка с надеждни уеб адреси. Списъкът с надеждни уеб адреси е наличен в прозореца **Сигурни уеб адреси**, който може да се отвори чрез щракване върху връзката от **сигурни уеб адреси**.

Прозорец на уеб сайтове на Kaspersky и нейните партньори

Този прозорец показва списък с уеб сайтове на Kaspersky и нейните партньори.

Списъкът се съставя и актуализира от експертите на Kaspersky. Списъкът се актуализира автоматично, когато базите данни и модулите на приложението се актуализират.

Настройки на Защита от мрежови атаки

Защитата от мрежови атаки се зарежда при стартиране на операционната система и проследява входящия мрежови трафик за дейности, характерни за мрежови атаки. Когато приложението Kaspersky открие опит за мрежова атака на компютъра на потребителя, то ще блокира мрежовата връзка с атакуващия компютър. Описания на познатите в момента типове мрежови атаки и методите за неутрализирането им са посочени в базите данни на приложението Kaspersky. Списъкът с мрежови атаки, които могат да бъдат открити от Защита от мрежови атаки, се актуализира, когато се актуализират базите данни и модулите на приложението.

Настройки на Защита от мрежови атаки

Настройки	Описание
Третиране на сканирането на портове и претоварването на мрежата като атаки	*Претоварване на мрежата* е атака върху мрежовите ресурси на организация (например уеб сървъри). Тази атака се състои в изпращане на огромно количество трафик, за да се изчерпи капацитета за трафик на дадена мрежа. В резултат потребителите не могат да осъществяват достъп до мрежови ресурси на организацията. *Атаката със сканиране на портове* се състои в сканиране на UDP и TCP портове и мрежови услуги на компютъра. Тази атака позволява да се определи нивото на уязвимост на компютъра дори преди по-опасни типове мрежови атаки. Сканирането на портове също така позволява на хакерите да определят ОС на компютъра и да изберат специфични за ОС атаки за него. Ако превключвателят е включен, компонентът Защита от мрежови атаки блокира сканирането на портове и претоварването на мрежата.
Добави атакуващия компютър към списъка на блокираните компютри за N мин	Ако превключвателят е включен, компонентът Защита от мрежови атаки добавя атакуващия компютър към списъка с блокирани. Това означава, че Защитата от мрежови атаки ще блокира мрежовата връзка с атакуващия компютър след първия опит за мрежова атака по време на посочения период от време, за да защити автоматично компютъра на потребителя от всякакви вероятни бъдещи мрежови атаки от същия адрес. Атакуващият компютър може да бъде добавен в списъка с блокирани компютри за минимално време от една минута. Максималната продължителност е 32 768 минути.
Управление на изключения	Списъкът съдържа IP адреси, от които Защитата от мрежови атаки не блокира мрежови атаки. Приложението не отчита информация за мрежови атаки от IP адреси, включени в списъка с изключения.

Настройки на Предотвратяване на проникване

Активирай / деактивирай Предотвратяване на проникване

Този бутон активира / деактивира Предотвратяване на проникване.

Научете повече

Щракването върху този бутон отваря страница с детайли на компонентите в прозорец на браузър.

Доверявай се на цифрово подписани приложения

Ако е поставена отметка в това квадратче, Предотвратяване на проникване класифицира цифрово подписаните приложения като надеждни. Предотвратяване на проникване премества тези приложения в групата **Сигурни** и не сканира дейността им.

Ако отметката е премахната от това квадратче, Предотвратяване на проникване не класифицира цифрово подписани приложения като надеждни и сканира дейностите им. Предотвратяване на проникване класифицира приложенията на надеждни доставчици на софтуер (например Microsoft) като надеждни, независимо дали е избрано квадратчето за отметка.

Зареждай правилата за програмите от Kaspersky Security Network (KSN)

Ако е поставена отметка в това квадратче, Предотвратяване на проникване изпраща заявка до базата данни на Kaspersky Security Network, за да определи групата на приложението.

Ако отметката е премахната от квадратчето, Предотвратяване на проникване не търси информация в базата данни на Kaspersky Security Network, за да определи надеждната група на приложението.

Надеждна група за приложения, които не могат да бъдат добавени към съществуващи групи

Щракването върху тази връзка отваря прозореца **Надеждна група за приложения, които не могат да бъдат добавени към съществуващи групи**. В този прозорец може да изберете надеждна група, към която ще бъдат зададени непознати приложения.

Може да изберете една от следните опции:

- Сигурни;
- Със слаби ограничения;
- С големи ограничения;
- Несигурни.

Надеждна група за приложения, стартирани преди стартирането на <PRODUCT>

Щракването върху тази връзка отваря прозореца **Надеждна група за приложения, стартирани преди стартирането на <PRODUCT>**. В този прозорец може да промените надеждната група за приложения, стартирани преди стартиране на Kaspersky. Мрежовата активност на приложения, стартирани преди стартиране на Kaspersky, се контролира според правилата на избраната надеждна група.

По подразбиране приложенията, стартирани преди стартиране на Kaspersky, се задават към една от надеждните групи въз основа на правилата, създадени от Kaspersky.

Управление на приложения

Щракването върху тази връзка отваря прозореца **Управление на приложения**. В този прозорец може да редактирате списъка с правила за приложения.

Управление на ресурси

Щракването върху тази връзка отваря прозореца **Управление на ресурси**. В този прозорец може да създавате списък с лични данни и списък с настройки и ресурси на операционната система. Достъпът до тези елементи се контролира от Предотвратяване на проникване.

Прозорец на уеб маяци

Този прозорец показва списък с уеб маяци.

Списъкът се съставя и актуализира от експертите на Kaspersky. Списъкът се актуализира автоматично, когато базите данни и модулите на приложението се актуализират.

Категории и изключения за частно сърфиране

Услуги за уеб анализ

Ако е поставена отметка в квадратчето, компонентът Поверително сърфиране блокира услугите за уеб анализ, които използват проследяване на активността, за да анализират вашата онлайн активност.

Като щракнете върху връзката **Списък за преглед**, ще се отвори прозорец със списък на услуги за уеб анализ, които използват проследяване на активността, за да анализират вашата онлайн активност.

Рекламни агенции

Ако е поставена отметка в квадратчето, компонентът Поверително сърфиране блокира проследяването на вашата онлайн активност от рекламни агенции за рекламни цели.

Щракването върху връзката **Списък за преглед** отваря прозорец със списък на рекламни агенции, които проследяват вашата онлайн активност за рекламни цели.

Уеб маяци

Ако е поставена отметка в квадратчето, компонентът Поверително сърфиране блокира проследяването на вашата онлайн активност с помощта на уеб маяци. Уеб маяците са обекти, които са вградени в уеб страници и са невидими за потребителите.

Щракването върху връзката **Списък за преглед** отваря прозорец със списък с уеб маяци.

Социални мрежи

Ако е поставена отметка в квадратчето, компонентът Поверително сърфиране блокира събирането на данни, когато посещавате социални мрежи, с изключение на събиране на данни, извършвано от тези социални мрежи. Блокирането на събиране на данни не предотвратява използването на „Like“, „+1“ и подобни функции.

Квадратчета за отметка с имената на социални мрежи ви позволяват да посочвате социалните мрежи, на чиито уеб сайтове приложението трябва блокира събирането на данни.

Изключения

Щракването върху тази връзка отваря прозорец, в който може да посочите уеб сайтовете, на които е разрешено проследяването на вашата онлайн активност.

Прозорец на несъвместими уеб сайтове

Този прозорец показва списък с уеб сайтове, които може да са неработещи в резултат на блокирането на събирането на данни според информацията, налична в Kaspersky.

Списъкът се съставя и актуализира от експертите на Kaspersky. Списъкът се актуализира автоматично, когато базите данни и модулите на приложението се актуализират.

Прозорец Настройки на поверително сърфиране

Активирай/деактивирай Поверително сърфиране

Ако превключвателят е включен, когато сте онлайн компонентът Поверително сърфиране открива опити за събиране на данни от услуги за проследяване. Услугите за проследяване използват получената информация, за да анализират дейността ви и могат да използват резултатите от анализа да ви показват подходящи реклами.

Събиране само на статистически данни

Когато е избрана тази опция, компонентът Поверително сърфиране работи в *режим на откриване*, позволявайки ви да преглеждате отчети за откритите опити за събиране на данни.

Блокирай събирането на данни

Когато е избрана тази опция, компонентът Поверително сърфиране работи в *режим на блокиране*, откривайки и блокирайки опити за събиране на данни. Информацията за тези опити се записва в отчет.

Категории и изключения

Щракването върху тази връзка отваря прозорец, в който може да посочите категориите услуги за проследяване, за които искате да блокирате или разрешите събиране на данни. От този прозорец може да преминете към създаване на списък с уеб сайтове, на които искате да разрешите проследяване.

Блокиране на проследяване

Ако е поставена отметка в квадратчето и е активиран режим на блокиране, когато посещавате уеб сайт, браузърът изпраща заглавната част „Не проследявай“ HTTP към уеб сайта, което означава, че проследяването на вашата дейност не е разрешена.

Допуска събиране на данни на уеб сайтовете на Kaspersky и нейните партньори

Ако е поставена отметка в квадратчето, Kaspersky разрешава събирането на данни на уеб сайтовете на Kaspersky и нейните партньори.

Уеб сайтове на Kaspersky и нейните партньори

Щракването върху тази връзка отваря прозорец със списък с уеб сайтове на Kaspersky и техните партньори.

Допуска събиране на данни на несъвместими уеб сайтове

Ако е поставена отметка в квадратчето, Kaspersky разрешава събиране на данни на уеб сайтове, които може да са неработещи в следствие на блокирането на събирането на данни.

Несъвместими уеб сайтове

Щракването върху тази връзка отваря прозорец със списък с уеб сайтове, които може да са неработещи в следствие на блокирането на събирането на данни.

Прозорец на рекламни агенции

Този прозорец показва списък с рекламни агенции, които проследяват вашата онлайн активност за рекламни цели.

Списъкът се съставя и актуализира от експертите на Kaspersky. Списъкът се актуализира автоматично, когато базите данни и модулите на приложението се актуализират.

Прозорец на услуги за уеб анализ

Този прозорец показва списък с услуги за уеб анализ, които използват проследяване на активността, за да анализират вашата онлайн активност.

Списъкът се съставя и актуализира от експертите на Kaspersky. Списъкът се актуализира автоматично, когато базите данни и модулите на приложението се актуализират.

Настройки на защита за пощата

Настройки	Описание
Ниво на защита	Приложението Kaspersky използва различни групи настройки за стартиране на Защита за пощата. Наборите настройки, които се съхраняват в приложението се наричат *нива на защита*: • **Изключително**. Когато е избрано това ниво на защита, Защита за пощата прилага максимално подробен преглед. Защита за пощата сканира входящите и изходящите имейл съобщения и извършва дълбок евристичен анализ. Високото ниво на защита на пощата се прилага при работа в опасна изчислителна среда. Пример на такава среда е връзка към безплатна имейл услуга от домашна мрежа, която не е предпазвана от централизирана имейл защита. • **Оптимално**. Нивото на защита на пощата, което постига оптималния баланс между работата на приложението Kaspersky и сигурността на пощата. Защита за пощата сканира входящите и изходящите имейл съобщения и извършва евристичен анализ на средно ниво. Това ниво на защита на пощата се препоръчва от специалистите на Kaspersky. • **Ниско**. Това ниво на защита на пощата, което Защита за пощата използва единствено за сканиране на входящите имейл съобщения и за повърхностен евристичен анализ. То не използва това ниво на защита за сканиране на архивите, които са прикачени към съобщенията. Когато е избрано това ниво на защита, компонентът Защита за пощата сканира имейл съобщенията възможно най-бързо и консумира най-малкото количество ресурси на операционната система. Ниското ниво на защита се препоръчва за използване, когато работите в надеждно защитена среда. Пример за такава среда може да бъде локална мрежа с централизирана имейл защита.
Действие при откриване на заплаха	• **Питай потребителя**. Защита за пощата ви информира за откриването на заразен или вероятно заразен обект, подканвайки ви за допълнителни действия, които да се предприемат за този обект. Тази опция е налична, ако квадратчето за отметка **Изпълнявай препоръчаните действия автоматично** е изчистено под **Настройки → Настройки за производителност → Използване на ресурси на компютъра**. • **Избери действие автоматично**. Когато бъдат открити заразени или вероятно заразени обекти, Защита за пощата изпълнява автоматично действието, което се препоръчва от специалистите на Kaspersky. За заразени обекти това действие е дезинфекция. Тази стойност е избрана по подразбиране. Преди да опитате да дезинфектирате или изтриете заразен обект, Защита за пощата създава резервно копие, ако по-късно е необходимо да се възстанови обектът или възможността за дезинфектирането му. Тази опция е налична, ако квадратчето за отметка **Изпълнявай препоръчаните действия автоматично** е избрано под **Настройки → Настройки за производителност → Използване на ресурси на компютъра**. • **Дезинфектирай; изтрий, ако дезинфектирането е неуспешно**. Ако заразен обект е открит във входящо или изходящо съобщение, Kaspersky Security Cloud се опитва да дезинфектира открития обект. Потребителят ще може да осъществи достъп до съобщението със сигурен прикачен файл. Но ако приложението Kaspersky не може да дезинфектира обекта, ще го изтрие. Приложението Kaspersky добавя информация за извършеното действие в темата на съобщението: *[Съобщението е обработено]<message subject>*.

	• **Дезинфектирай; блокирай, ако дезинфектирането е неуспешно**. Ако заразен обект е открит във входящо съобщение, приложението Kaspersky се опитва да дезинфектира открития обект. Потребителят ще може да осъществи достъп до съобщението със сигурен прикачен файл. Ако обектът не може да бъде дезинфектиран, приложението Kaspersky добавя предупреждение към темата на съобщението. Потребителят ще може да осъществи достъп до съобщението с оригиналния прикачен файл. Ако заразен обект е открит в изходящо съобщение, приложението Kaspersky ще се опита да дезинфектира открития обект. Ако приложението Kaspersky не може да дезинфектира обекта, то ще блокира изпращането на съобщението и пощенският клиент ще покаже съобщение за грешка. • **Блокирай**. Ако заразен обект е открит във входящо съобщение, приложението Kaspersky ще добави предупреждение към темата на съобщението. Потребителят ще може да осъществи достъп до съобщението с оригиналния прикачен файл. Ако заразен обект бъде открит в изходящо съобщение, приложението Kaspersky ще блокира съобщението изпращането на съобщението и пощенският клиент ще покаже грешка.
Обхват на защитата	*Обхватът на защитата* включва обекти, които компонентът проверява, когато работи: входящи и изходящи съобщения или само входящите съобщения. За да защитите компютрите се, трябва да сканирате само входящи съобщения. Може да включите сканиране за изходящи съобщения, за да предотвратите изпращането на заразени файлове в архивите. Също така може да включите сканирането на изходящи съобщения, ако искате да предотвратите изпращането на файлове в конкретни формати, като например аудио и видео файлове.
Сканирай POP3, SMTP, NNTP и IMAP трафик	Това квадратче за отметка активира/деактивира сканирането от Защита за пощата на пощенски трафик, изпратен по POP3, SMTP, NNTP и IMAP протоколи.
Свържи разширението за Microsoft Outlook	Ако е поставена отметка в квадратчето, имейл съобщенията, предадени чрез POP3, SMTP, NNTP и IMAP протоколи, ще бъдат сканирани с помощта на разширението, което е интегрирано в Microsoft Outlook. Ако имейл е сканиран с помощта на разширението за Microsoft Outlook, препоръчително е да използвате кеширан режим на Exchange. Повече детайли за кеширания режим на Exchange и препоръки как да го използвате може да откриете в База знания на Microsoft.
Евристичен анализ	Техника за откриване на заплахи, които не могат да бъдат идентифицирани с помощта на текущата версия на базите данни на приложенията на Kaspersky. Тя ви позволява да откривате файлове, които може да съдържат непознат злонамерен софтуер или нова модификация на позната злонамерена програма. Когато сканирате файлове за злонамерен код, евристичният анализатор изпълнява инструкциите в изпълнимите файлове. Броят инструкции, изпълнени от евристичния анализатор, зависи от нивото, което е посочено за него. Нивото на евристичния анализ задава баланса между задълбочеността на търсенията за нови заплахи, натоварването на ресурсите на операционната система и времето, необходимо за евристичен анализ.
Сканиране на прикачени файлове с формати на Microsoft Office	Сканиране на файлове на Microsoft Office (DOC, DOCX, XLS, PPT и други разширения на Microsoft). Файловете с формати на Office също включват OLE обекти.
Сканиране на	Сканира ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и други архиви.

прикачени архиви	Приложението сканира архиви не само по тяхното разширението, но и по техния формат.
Не сканирай архиви по-големи от	Ако е поставена отметка в това квадратче, Защита за пощата изключва архивите, които са прикачени към имейл съобщения, от сканиране, ако техният размер надвишава стойността, която сте посочили. Ако отметката е премахната от квадратчето, Защита за пощата сканира архиви с всякакъв размер, които са прикачени към имейл съобщения.
Ограничаване на времето за проверка на архиви до	Ако е поставена отметка в квадратчето, количеството време, необходимо за сканиране на архивите, които са прикачени към имейл съобщения, ще бъде ограничено до посочения период.
Филтър за прикачени файлове	Филтърът за прикачени файлове не работи за изходящи имейл съобщения. **Деактивиране на филтриране**. Ако изберете тази опция, Защита за пощата няма да филтрира файлове, които са прикачени към имейл съобщения. **Преименуване на прикачени файлове от избраните типове**. Ако изберете тази опция, Защита за пощата ще замени последния знак за разширение, открит в прикачените файлове на посочените типове, със знак за долна черта (например attachment.doc_). По този начин, за да отвори този файл, потребителят трябва да преименува файла. **Изтриване на прикачени файлове от избраните типове**. Ако изберете тази опция, Защита за пощата ще изтрива файлове от посочените типове, които са прикачени към имейл съобщения. Може да посочите типовете прикачени файлове, които трябва да преименувате или изтриете от имейл съобщения в списъка с файлови маски.

Прозорец на Свойства на мрежа (адаптер)

Име

Име на мрежови адаптер.

Тип връзка

Тип мрежови адаптер, например: Ethernet мрежа, безжична мрежа или модемна връзка.

Състояние

Текущото състояние на мрежовата връзка: *Свързан* или *Изключен*.

В раздела **Нови връзки** може да изберете действието, което защитната стена изпълнява, когато бъде открита нова връзка през този адаптер.

Питай за група

Ако защитната стена открие нова мрежова връзка, тя ще ви уведоми и помоли да изберете състояние за новата мрежа.

Автоматично преместване на нови мрежи към групата

Ако защитната стена открие нова мрежова връзка, тя автоматично задава на мрежата състоянието, което е избрано в падащия списък.

В падащия списък може да определите състоянието на мрежата, което защитната стена автоматично задава на нови мрежи.

Настройки на Системно наблюдение

Активирай / деактивирай

Този ключ активира/деактивира 'Системно наблюдение'.

Ако бутонът е зелен, Системно наблюдение събира и записва данни за всички събития, които настъпват в операционната система (като например промяна на файл, промяна на ключ от регистъра, стартиране на драйвери или опити за изключване на компютъра). Тези данни се използват за проследяване на злонамерената и друга дейност на приложението (включително рансъмуер) и за възстановяване на състоянието на операционната система, каквото е било преди инсталирането на приложението (за връщане назад на последиците от злонамерен софтуер или друга дейност на приложението). В някои случаи дейността на приложенията не може да бъде отменена, например когато приложението е засечено от компонента Предотвратяване на проникване.

Системно наблюдение събира данни от различни източници, включително други компоненти на Kaspersky. Системно наблюдение анализира дейността на приложението и осигурява други компоненти на Kaspersky със събраната информация за събитията.

В раздела **Защита от експлойти** може да конфигурирате действията, които приложението изпълнява, когато изпълними файлове се стартират от уязвими приложения.

Наблюдавай опити за изпълнение на неупълномощени операции

С това квадратче за отметка може да активирате/деактивирате Защита от експлойти.

Ако е поставена отметка в това квадратче, Kaspersky проследява изпълними файлове, стартирани от уязвими приложения. Ако Kaspersky засече опит за стартиране на изпълним файл от уязвимо приложение, който не е инициран от потребителя, приложението изпълнява действието, което е избрано в падащия списък **При откриване на заплаха**.

При откриване на заплаха

В този падащ списък може да изберете действието, което Системно наблюдение изпълнява, когато изпълним файл се стартира от наблюдавано уязвимо приложение.

Този списък позволява избор от следните действия:

- **Питай потребителя**. Системно наблюдение подканва потребителя за действие. Тази опция е налична, ако квадратчето за отметка **Изпълнявай препоръчаните действия автоматично** е изчистено под **Настройки → Настройки за производителност → Използване на ресурси на компютъра**.
- **Избери действие автоматично**. Системно наблюдение автоматично изпълнява действието, избрано в настройките на Kaspersky, и добавя информация за избраното действие в отчет. Тази опция е налична, ако квадратчето за отметка **Изпълнявай препоръчаните действия автоматично** е избрано под **Настройки → Настройки за производителност → Използване на ресурси на компютъра**.
- **Разреши действието**. Системно наблюдение позволява стартирането на изпълнимия файл.
- **Забрани действието**. Системно наблюдение блокира изпълнимия файл.

Действие при откриване на зловредна или друга активност

В този падащ списък може да изберете действието, което Системно наблюдение изпълнява, когато е открита злонамерена или друга дейност, базирано на резултатите от анализа на дейността на приложението.

- **Питай потребителя**. Системно наблюдение подканва потребителя за действие. Тази опция е налична, ако квадратчето за отметка **Изпълнявай препоръчаните действия автоматично** е изчистено под **Настройки** → **Настройки за производителност** → **Използване на ресурси на компютъра**.
- **Избери действие автоматично**. Системно наблюдение автоматично извършва действието, препоръчано от експертите на Kaspersky. Тази опция е налична, ако квадратчето за отметка **Изпълнявай препоръчаните действия автоматично** е избрано под **Настройки** → **Настройки за производителност** → **Използване на ресурси на компютъра**.
- **Изтриване на приложението**. Системно наблюдение изтрива приложението.
- **Прекратяване на работата на приложението**. Системно наблюдение прекратява всички процеси на приложението.
- **Прекратяване на работата на приложението**. Системно наблюдение не предприема действия за приложението.

Действието, което трябва да се изпълни, ако зловредното или друго действие може да се отмени

В този падащ списък може да изберете действието, което Системно наблюдение изпълнява, когато е възможно да се отмени злонамерено или друго действие на приложението.

- **Питай потребителя**. Ако Системно наблюдение, Защита на файловете или резултатите от задача за сканиране потвърдят, че е необходимо да се извърши отмяна, Системно наблюдение подканва потребителя за действие. Тази опция е налична, ако квадратчето за отметка **Изпълнявай препоръчаните действия автоматично** е изчистено под **Настройки** → **Настройки за производителност** → **Използване на ресурси на компютъра**.
- **Избери действие автоматично**. Ако Системно наблюдение анализира дейността на дадено приложение и сметне, че е злонамерена, то отменя действието на приложението и уведомява потребителя за това събитие. Тази опция е налична, ако квадратчето за отметка **Изпълнявай препоръчаните действия автоматично** е избрано под **Настройки** → **Настройки за производителност** → **Използване на ресурси на компютъра**.
- **Изпълни отмяна**. Системно наблюдение отменя злонамереното или друго действие на приложението.
- **Не изпълнявай отмяна**. Системно наблюдение записва информацията за злонамерената или друга дейност, но не отменя действията на приложението.

В раздела **Защита срещу програми за блокиране на екрана** може да конфигурирате действията, които се изпълняват, ако е засечена дейност на програми за блокиране на екрана. Програмите за блокиране на екрана са злонамерени програми, които ограничават действията на потребителя на компютъра, като блокират екрана и клавиатурата или като блокират достъпа до лентата на задачите и преките пътища. Програмите за блокиране на екрана може да се опитат искат откуп за възстановяване на достъпа до операционната система. Като използвате защита срещу програмите за блокиране на екрана, може да затворите всяка програма за блокиране на екрана, като натиснете специфична комбинация от клавиши.

Открий и затвори програмата за блокиране на екрана

Това квадратче за отметка активира/деактивира защитата срещу програми за блокиране на екрана.

Ако е поставена отметка в това квадратче, когато бъде засечена активност на програма за блокиране на екрана, може да я спрете, като натиснете комбинацията от клавиши, която посочена в падащия списък под квадратчето за отметка.

Използвайте следната комбинация от клавиши за ръчно затваряне на екранно заключване

В падащия списък може да изберете клавиш, който, когато е натиснат, задейства защитата срещу програми за блокиране на екрана за откриване и изтриване на програма за блокиране на екрана.

Следната клавишна комбинация се използва по подразбиране: CTRL+ALT+SHIFT+F4.

Настройки на Защита на файлове

Настройки	Описание
Ниво на защита	Приложението Kaspersky използва различни групи настройки за стартиране на Защита на файловете. Наборите настройки, които се съхраняват в приложението се наричат *нива на защита*: • **Изключително**. Когато е избрано това ниво на защита на файловете, компонентът Защита на файлове поема най-стриктния контрол на всички файлове, които са отворени, записани и стартирани. Компонентът Защита на файлове сканира всички типове файлове на всички твърди дискове, мрежови дискове и преносими носители за съхранение на компютъра. Също така сканира архиви, инсталационни пакети и вградени OLE обекти. • **Оптимално**. Това ниво на защита на файловете се препоръчва от експертите на Kaspersky Lab. Компонентът Защита на файлове сканира само посочените файлови формати на всички твърди дискове, мрежови дискове, преносими носители за съхранение на компютъра и вградени OLE обекти. Компонентът Защита на файлове не сканира архиви или инсталационни пакети. • **Ниско**. Настройките на това ниво на защита на файловете гарантира максимална скорост на сканиране. Компонентът Защита на файлове сканира единствено файлове с посочените разширения на всички твърди дискове, мрежови дискове и преносими носители за съхранение на компютъра. Компонентът Защита на файлове не сканира съставни файлове.
Действие при откриване на заплаха	• **Питай потребителя**. Защита за файлове ви информира за откриването на заразен или вероятно заразен обект и ви подканва за действието, което да предприемете. Тази опция е налична, ако квадратчето за отметка **Изпълнявай препоръчаните действия автоматично** е изчистено под **Настройки → Настройки за производителност → Използване на ресурси на компютъра**. • **Избери действие автоматично**. При откриване на заразен или вероятно заразен обект, Защита на файлове автоматично извършва действието, препоръчано от експертите на Kaspersky, върху обекта. За заразени обекти това действие е дезинфекция. Тази стойност е избрана по подразбиране. Преди да опитате да дезинфектирате или изтриете заразен обект, Защита на файлове създава негово резервно копие за последващо възстановяване или дезинфекция. Тази опция е налична, ако квадратчето за отметка **Изпълнявай препоръчаните действия автоматично** е избрано под **Настройки → Настройки за производителност → Използване на ресурси на компютъра**. • **Дезинфектирай; изтрий, ако дезинфектирането е неуспешно**. Ако изберете това действие, приложението автоматично ще се опита да дезинфектира всички заразени файлове, които открие. Ако дезинфекцията не успее, приложението изтрива обектите. • **Дезинфектирай; блокирай, ако дезинфектирането е неуспешно**. Ако изберете това действие, приложението автоматично ще се опита да дезинфектира всички заразени файлове, които открие. Ако дезинфекцията не успее, приложението ще добави информация за заразените файлове, които открие, в списъка на откритите обекти. • **Блокирай**. Ако е избрана тази опция, компонентът Защита на файлове автоматично блокира всички заразени файлове, без да се опитва да ги

	дезинфектира. Преди да опита да дезинфектира или изтрие заразен файл, приложението създава резервно копие в случай, че след това трябва да възстановите файла или стане възможно да се дезинфектира по-късно.
Типове файлове	**Всички файлове**. Ако тази настройка е активирана, приложението сканира всички файлове без изключение (всички формати и разширения). **Файлове, сканирани по формат**. Ако изберете тази настройка, приложението ще сканира само потенциално заразени файлове. Преди да търсите злонамерен код във файл, вътрешната му заглавна част се анализира, за да се определи форматът на файла (например TXT, DOC, EXE). Сканирането също така търси файлове с конкретни файлови разширения. **Файлове, сканирани по разширение**. Ако изберете тази настройка, приложението ще сканира само потенциално заразени файлове. Файловият формат се определя въз основа на разширението на файла.
Редактиране на обхват на защита	Щракването върху тази връзка отваря прозореца **Обхват на защита за Защита за файловете**, който съдържа списък с обекти, които са сканирани от Защита на файловете. Може да добавяте обекти към списъка или да изтривате обектите, които добавяте. За да премахнете обект от сканирането, не трябва да изтривате обекта от списъка. Всичко, което трябва да направите, е да премахнете отметката от полето до името на обекта.
Евристичен анализ	Техника за откриване на заплахи, които не могат да бъдат идентифицирани с помощта на текущата версия на базите данни на приложенията на Kaspersky. Тя ви позволява да откривате файлове, които може да съдържат непознат злонамерен софтуер или нова модификация на позната злонамерена програма. Когато сканирате файлове за злонамерен код, евристичният анализатор изпълнява инструкциите в изпълнимите файлове. Броят инструкции, изпълнени от евристичния анализатор, зависи от нивото, което е посочено за него. Нивото на евристичния анализ задава баланса между задълбочеността на търсенията за нови заплахи, натоварването на ресурсите на операционната система и времето, необходимо за евристичен анализ.
Сканирай само новите и променени файлове	Сканира само новите файлове и тези файлове, които са били променени от последния път, когато са сканирани. Това ви позволява да спестите време при сканиране. Този режим на сканиране важи за обикновени и съставни файлове.
Сканирай архиви	Сканира ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и други архиви. Приложението сканира архиви не само по тяхното разширението, но и по техния формат.
Сканиране на пакети за разпространение	Квадратчето за отметка активира/деактивира сканирането на пакети за разпространение на трети страни.
Сканиране на файлове с формати на Microsoft Office	Сканиране на файлове на Microsoft Office (DOC, DOCX, XLS, PPT и други разширения на Microsoft). Файловете с формати на Office също включват OLE обекти.
Не разопаковай съставни	Ако е поставена отметка в квадратчето за отметка, приложението не сканира съставни файлове, които са по-големи от посочената стойност.

файлове с голям размер **Максимален размер за файл**	Ако отметката е премахната от това квадратче, приложението сканира съставни файлове от всякакви размери. Приложението сканира големи файлове, които са извлечени от архиви, независимо дали квадратчето за отметка е отбелязано, или не.
Разопаковай съставните файлове във фонов режим **Минимален размер за файл**	Ако е поставена отметка в това квадратче, приложението предоставя достъп до съставни файлове, които са по-големи от посочената стойност, преди тези файлове да бъдат сканирани. В такъв случай приложението разопакова и сканира съставни файлове във фонов режим. Приложението предоставя достъп до съставни файлове, които са по-малки от тази стойност, само след разопаковане и сканиране на тези файлове. Ако е премахната отметката от това квадратче, приложението предоставя достъп до съставни файлове само след разопаковане и сканиране на файлове, независимо от размера им.
Режим за сканиране	**Интелигентен режим**. В този режим Защита на файлове сканира обект според анализ на действията, предприети върху този обект. Например когато работите с документ на Microsoft Office, приложението Kaspersky сканира файла първия път, когато е отворен, и последния път, когато е затворен. Междинни операции, които презаписват файла, не водят до сканирането му. **При достъп и промяна**. В този режим Защита на файловете сканира обекти, всеки път когато има опит да бъдат отворени или променени. **При достъп**. В този режим Защита на файловете сканира обекти само при опит да бъдат отворени. **При изпълнение**. В този режим Защита на файловете сканира обекти само при опит да бъдат стартирани.
Технология iSwift	Тази технология е разработка на технологията iChecker за компютри с файлова система NTFS. Има ограничения за технологията iSwift: обвързана е с местоположението на конкретен файл във файловата система и работи само с обекти във файловата система NTFS. Когато надстроите приложението Kaspersky до нова версия, технологията iSwift е разрешена за всички типове сканирания, дори ако е била забранена преди това.
Технология iChecker	Тази технология позволява увеличаване на скоростта на сканиране чрез изключване на определени файлове от сканиране. Файловете се изключват от сканиране с помощта на специален алгоритъм, който взема предвид датата на публикуване на базите данни на приложението Kaspersky, датата, когато файлът е сканиран за последен път и всички промени на настройките за сканиране. Има ограничения за технологията iChecker: тя не работи с големи файлове и се прилага само за файлове със структура, която приложението разпознава (например, EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP и RAR).
Изключения	Обекти, изключени от сканирания. За да посочите изключенията, щракнете върху връзката **Управление на изключения** в прозореца **Изключения**.
Пауза на Защитата за файловете	Това временно и автоматично паузира работата на Защитата за файловете в посоченото време и при работа с посочените приложения. Конфигурира се чрез щракване върху връзката **Пауза на Защитата за файловете**.

Настройки за AMSI защита

Настройки	Описание
Сканирай архиви	Сканира ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE и други архиви. Приложението сканира архиви не само по тяхното разширението, но и по техния формат.
Сканиране на пакети за разпространение	Квадратчето за отметка активира/деактивира сканирането на пакети за разпространение на трети страни.
Сканиране на файлове с формати на Microsoft Office	Сканиране на файлове на Microsoft Office (DOC, DOCX, XLS, PPT и други разширения на Microsoft). Файловете с формати на Office също включват OLE обекти.
Не разопаковайте съставни файлове с голям размер **Максимален размер за файл**	Ако е поставена отметка в квадратчето за отметка, приложението не сканира съставни файлове, които са по-големи от посочената стойност. Ако отметката е премахната от това квадратче, приложението сканира съставни файлове от всякакви размери. Приложението сканира големи файлове, които са извлечени от архиви, независимо дали квадратчето за отметка е отбелязано, или не.

Прозорец за добавяне/редактиране на лични данни

Типове лични данни

Когато щракнете върху връзките в полето **Име на полето**, се показва съответният тип лични данни.

Име на полето

Описание, показано в списъка с лични данни (напр. *домашен телефон*, *бизнес телефон* или *пощенски код*).

Можете да копирате описанието на личните данни автоматично, като щракнете върху съответната връзка с типа лични данни.

Стойност

Лични данни, за които изпращането е блокирано или разрешено.

Отчет за прехвърляне на лични данни

В горната част на прозореца се показва името на потребителския акаунт, чиито действия се отчитат в този прозорец.

Контролът е активиран/деактивиран  /

Този превключвател позволява активиране / деактивиране на наблюдението на действията на потребителя от Родителски контрол.

В зависимост от това дали Родителски контрол наблюдава действията на потребителя, бутонът може да има следния вид:

 – Родителски контрол следи действията на потребителя.

 – Родителски контрол не следи действията на потребителя.

Наблюдението на действията на потребителя се извършва в съответствие с настройките на Родителски контрол, дефинирани за този потребител.

В този прозорец можете да видите информация за използване на ключови думи и опити за предаване на лични данни от избрания потребител.

Днес

Щракването върху този бутон отваря отчета за активността на потребителя за днес.

Бутони

Щракването върху тези бутони отваря отчети за предишни и следващи периоди.

ден/седмица/месец

Период от време, за който се създава отчетът. Можете да създадете отчет за следните периоди: ден, седмица и месец.

Бутон

Щракването върху този бутон отваря прозореца с настройки на Родителски контрол и показва раздела **Контрол на съдържанието**. В този раздел можете да наложите ограничения за изпращане на лични данни.

Списък с блокирани лични данни

Съдържа списък с лични данни от съобщения, които са изпратени и получени от избрания потребител през посочения период.

Данни

Тази колона съдържа лични данни от изпратени или получени съобщения.

За блокираните лични данни се посочва типът информация, която да бъде блокирана за прехвърляне.

Ресурс

Тази колона показва уеб сайта, през който потребителят се е опитал да изпрати или получи съобщение с лични данни, които са блокирани за прехвърляне.

Състояние

Ако изпращането на съобщението е блокирано от Родителски контрол, колоната показва стойността *Блокирано*.

Дата

Тази колона показва датата на получаване или изпращане на съобщението, съдържащо лични данни, които са блокирани за прехвърляне.

Избор на потребителски профил

Събиране на данни

Щракването върху този бутон прилага профила с настройките по подразбиране към акаунта на избрания потребител. Този профил събира само статистически данни за действията на избрания потребител. Не са зададени ограничения за приложението и използването на интернет.

Персонализирани ограничения

Ръчно конфигурираните настройки се прилагат към акаунта на избрания потребител.

Дете (4+)

С щракването върху този бутон се прилага профилът, предназначен за деца от 4 до 12 години, към акаунта на избрания потребител. Този профил предоставя следните правила за използване на Интернет и приложения:

- Използването на интернет е разрешено.
- Сърфирането е разрешено само за уеб сайтове, които са изброени в категориите „Интернет комуникация" и „Компютърни игри".
- Изтеглянето на файлове от всякакъв тип е блокирано.
- Разрешено е наблюдението на използването на компютъра; не са зададени ограничения за използването на компютъра.
- Разрешено е наблюдението на използването на приложението; не се налагат ограничения за използването на компютъра.
- Разрешено е наблюдението на използването на игрите; ограниченията се задават според рейтинговата система.

Тийнейджър (12+)

Щракването върху този бутон прилага профила, предназначен за деца на 12+ години, към акаунта на избрания потребител. Този профил предоставя следните правила за използване на Интернет и приложения:

- Използването на интернет е разрешено.
- Сърфирането е разрешено само за уеб сайтове, които са изброени в категориите „Интернет комуникация", „Пазаруване, банки, системи за плащане" и „Компютърни игри".
- Разрешено е наблюдението на използването на компютъра; не са зададени ограничения за използването на компютъра.
- Разрешено е наблюдението на използването на приложението; не се налагат ограничения за използването на компютъра.
- Разрешено е наблюдението на използването на игрите; ограниченията се задават според рейтинговата система.

Настройки по подразбиране

Щракването върху този бутон прилага профила с настройките по подразбиране към акаунта на избрания потребител. Този профил предоставя следните правила за използване на Интернет и приложения:

- Използването на интернет е разрешено.
- Сърфирането е разрешено само за уеб сайтове, които са изброени в категориите „Интернет комуникация“, „Пазаруване, банки, системи за плащане“ и „Компютърни игри“.
- Безопасното търсене е активирано.
- Разрешено е наблюдението на използването на компютъра; не са зададени ограничения за използването на компютъра.
- Разрешено е наблюдението на използването на приложението; не се налагат ограничения за използването на компютъра.
- Разрешено е наблюдение на стартирането на игрите; не са зададени ограничения за стартиране.
- Разрешено е наблюдение на криптирани SSL връзки в браузърите.

Импортиране

Щракването върху тази връзка отваря прозореца за избор на файл, който съдържа настройки на Родителски контрол. След като изберете файла, тези настройки се прилагат към акаунта на избрания потребител.

Експортиране

Щракването върху тази връзка отваря прозореца за запазване на текущите настройки за Родителски контрол във файл.

Прозорец на Добавяне/Редактиране на уеб адрес

Маска на уеб адрес

Уеб адресът или адресната маска на уеб сайта, до който трябва да бъде блокиран или разрешен достъпът.

Действие

Използва се за блокиране или разрешаване на потребителски достъп до уеб сайтове.

Може да изберете една от следните опции:

- **Разреши**. Ако изберете тази опция, Родителски контрол позволява на потребителя достъп до уеб сайта, дори ако принадлежи към блокирана категория или блокирането на всички уеб сайтове е активирано.
- **Блокирай**. Ако изберете тази опция, Родителският контрол блокира достъпа на потребителите до уеб сайта, дори ако принадлежи към разрешена категория.

Тип

Можете да посочите обхвата, към който да приложите настройките за достъп до уеб сайта.

Може да изберете една от следните опции:

- **Маска за уеб сайт**. Ако изберете тази опция, Родителски контрол позволява или блокира достъпа на потребителя до всички уеб страници на посочения уеб сайт.

  Например, ако полето **Маска за уеб адрес** съдържа адреса example.com, Родителски контрол позволява или блокира достъпа до всички уеб страници на уеб сайта example.com, включително news.example.com, market.example.com и mail.example.com.

- **Посочен уеб адрес**. Ако изберете тази опция, Родителски контрол позволява или блокира достъпа на потребителя само до определената страница на уеб сайта, посочен в полето **Маска за уеб адрес**.

  Например, ако посочите URL адреса mail.example.com/login в полето **Маска за уеб адрес** Родителски контрол позволява или блокира достъп само до посочената страница за вход, която се използва за влизане в акаунта за уеб поща. Това правило няма да се прилага за други страници на уеб сайта.

Прилагане на шаблон

Позволява да се приложи изключение на един от съществуващите шаблони с посочения набор от настройки.

Може да изберете една от следните опции:

- **Целият уеб сайт** – когато е избрана тази опция, Родителски контрол разрешава или блокира достъпа до домейна, посочен в полето **Маска за уеб адрес**. Например, ако полето **Маска за уеб адрес** съдържа адреса example.com, Родителски контрол ще разреши или блокира достъпа до всички уеб страници на домейна example.com, включително news.example.com, market.example.com и mail.example.com.

- **Посочена уеб страница** – когато е избрана тази опция, Родителски контрол разрешава или блокира достъпа до конкретната страница, посочена в полето **Маска за уеб адрес** и до всички уеб адреси, които съдържат тази страница. Например, ако полето **Маска за уеб адрес** съдържа адреса example.com/hl, Родителски контрол ще разреши или блокира достъпа до тази страница, както и до уеб адреси, които я съдържат, като example.com/hl/example1.html.

- **Посочен уеб адрес** – когато е избрана тази опция, Родителски контрол разрешава или блокира достъпа до конкретния уеб адрес, посочен в полето **Маска за уеб адрес**. Например, ако посочите URL адреса mail.example.com/login в полето **Маска за уеб адрес** Родителски контрол позволява или блокира достъп само до посочената страница за вход, която се използва за влизане в акаунта за уеб поща. Това правило няма да се прилага за други страници на уеб сайта.

Изключения за Родителски контрол

В този прозорец можете да създадете списък с изключения от конфигурираните настройки на Родителски контрол. Настройките за достъп, които засягат уеб сайтове, добавени към списъка за изключения, се прилагат както при блокиране на уеб сайтове по категории (бутон **Блокирайте достъпа до уеб сайтове от определени категории**) и при блокиране на всички уеб сайтове (бутон **Блокирайте достъпа до всички уеб сайтове**).

Например можете да разрешите достъп до уеб сайтове от категорията „интернет комуникация“, но да добавите уеб сайта www.example.com към списъка с изключения, за да блокирате достъпа до този конкретен уеб сайт. В този случай Родителски контрол позволява достъп до всички социални мрежи с изключение на социалната мрежа example.com. Можете също да блокирате всички уеб сайтове и да добавите достъп до уеб сайт за уеб поща, който ще бъде разрешен в списъка с изключения. В този случай Родителски контрол позволява на потребителя да има достъп само до уеб сайта за уеб поща.

Списък с изключения

Списъкът съдържа уеб адреси, до които достъпът е разрешен или блокиран, независимо от настройките на Родителски контрол.

От контекстното меню на адреса ни в списъка можете да промените уеб адреса или да го премахнете от списъка, както и да разрешите или блокирате достъпа до уеб сайта.

Маска на уеб адрес

Уеб адресът или адресната маска на уеб сайт, до който е разрешен или блокиран достъп.

Тип

Колоната показва обхвата, към който се прилагат настройките за достъп до уеб сайт.

Ако в колоната се показва *Маска за уеб сайт*, достъпът до всички страници на уеб сайта е разрешен или блокиран.

Ако в колоната се показва *Посочен уеб адрес*, е разрешен или блокиран само достъпът до посочената уеб страница на уеб сайта.

Действие

Тази колона показва дали достъпът до уеб сайта е разрешен или блокиран.

Ако в колоната се показва *Позволен*, Родителски контрол позволява достъп до уеб сайта.

Ако в колоната се показва *Блокиран*, Родителски контрол блокира достъпа до уеб сайта.

Редактирай

Щракването върху този бутон отваря прозореца **Редактирай**, където можете да редактирате маската на уеб адреса или уеб адреса на уеб сайта, избран в списъка с изключения и настройките за достъп до уеб сайта.

Бутонът е наличен, ако в списъка за изключения е избрана маска за уеб адрес.

Изтрий

Щракването върху този бутон премахва избраната маска на уеб адрес от списъка с изключения.

Бутонът е наличен, ако в списъка за изключения е избрана маска за уеб адрес.

Добави

Щракването върху този бутон отваря прозореца за добавяне на маска на адрес на уеб сайт, в който можете да добавите адрес на уеб сайт или маска на адрес на уеб сайт към списъка с изключения.

Прозорец за ограничения в използването на приложението

В този прозорец можете да наложите ограничения върху времето за използване на избрано приложение.

В раздела **Делнични дни** можете да ограничите времето за използване на приложението през делничните дни.

Разрешете достъп за не повече от <N> часа на ден

Това квадратче за отметка активира/деактивира ограничение във времето за използване на приложението през делничните дни.

Ако това квадратче е избрано, Родителски контрол ограничава общото време за използване на приложението за избрания потребител. Срокът за използване на приложението е посочен (в часове) в падащия списък до квадратчето за отметка.

Ако това квадратче е изчистено, Родителски контрол не ограничава използването на приложението през делничните дни.

В раздела **Уикенди** можете да ограничите времето за използване на приложението през уикендите.

Разрешете достъп за не повече от <N> часа на ден

Това квадратче за отметка активира/деактивира ограничение във времето за използване на приложението през уикендите.

Ако това квадратче е избрано, Родителски контрол ограничава общото време за използване на приложението за избрания потребител. Срокът за използване на приложението е посочен (в часове) в падащия списък до квадратчето за отметка.

Ако това квадратче за отметка е изчистено, Родителски контрол не ограничава използването на приложението през уикендите.

В раздела **Почивки**, можете да настроите периодично блокиране на достъпа до приложението през деня.

Правете почивка на всеки <N> часа за <N> минути

Това квадратче за отметка позволява/деактивира периодичното блокиране на приложението през посочения интервал, за да се гарантира, че потребителят си прави почивка.

Ако това квадратче е отметнато, Родителски контрол блокира приложението през интервала, посочен в падащия списък **<ЧЧ:ММ>**. Достъпът е блокиран за периода от време, избран от падащия списък **<N> минути**.

Разделът **Точно време за използване** показва таблица с времето за използване на приложението. С помощта на тази таблица можете да настроите график час по час за използване на приложението през цялата седмица.

График за използване на приложението

Можете да използвате тази таблица, за да посочите дните от седмицата и часовете, когато на потребителя е разрешено да използва приложението. Редовете на таблицата съответстват на дните от седмицата, а колоните на таблицата съответстват на едночасови интервали по времевата линия. В зависимост от регионалните настройки на операционната система, времевата линия може да се показва в 24-часов или в 12-часов формат. Цветовете на клетките на таблицата показват ограниченията, които са в сила: червеният означава, че използването на приложение е блокирано, а сивият – че използването на приложението е разрешено. Щракването върху клетка от таблица променя цвета ѝ. Когато движите показалеца на мишката върху клетка, интервалът от време, съответстващ на тази клетка, се показва под таблицата.

Прозорец за списък с лични данни

Списък с лични данни

Този списък съдържа личните данни на потребителя, за които изпращането трябва да се контролира.

Име на полето

Тази колона показва типа на личните данни (напр. *номер на банкова карта* или *домашен телефонен номер*).

Стойност

Тази колона съдържа лични данни (например номер на банкова карта или телефонен номер), които искате да наблюдавате в съобщения.

Редактирай

Щракването върху този бутон отваря прозорец, в който може да редактирате запис с лични данни.

Изтрий

Щракването върху този бутон позволява да се премахне избрания запис от списъка.

Добави

Щракването върху този бутон отваря прозорец, в който можете да добавите нов запис към списъка с лични данни.

Отчет за блокирани уеб сайтове и изтегляния

Днес

Щракването върху този бутон отваря отчета за активността на потребителя за днес.

Бутони

Щракването върху тези бутони отваря отчети за предишни и следващи периоди.

ден/седмица/месец

Период от време, за който се създава отчетът. Можете да създадете отчет за следните периоди: ден, седмица и месец.

Бутон

Щракването върху този бутон отваря прозореца с настройки на Родителски контрол и показва раздела **Интернет**. В този раздел можете да наложите ограничения на времето за използване на интернет, достъпа до уеб сайтове и изтеглянето на файлове за избрания потребител.

Блокирани уеб сайтове и изтегляния

Този списък съдържа уеб сайтове, които са били блокирани от Родителски контрол и файлове, които са блокирани за изтегляне.

Списъкът съдържа следните данни:

- Име на блокирания уеб сайт или файл
- Причина, поради която опитът за достъп е бил блокиран за потребителя (напр. *Уеб сайт от блокирана категория*)
- Дата на отваряне на уеб сайта или изтегляне на файла

Отчет за използване на приложението

В горната част на прозореца се показва името на потребителския акаунт, чиито действия се отчитат в този прозорец.

Контролът е активиран/деактивиран /

Този превключвател позволява активиране / деактивиране на наблюдението на действията на потребителя от Родителски контрол.

В зависимост от това дали Родителски контрол наблюдава действията на потребителя, бутонът може да има следния вид:

– Родителски контрол следи действията на потребителя.

– Родителски контрол не следи действията на потребителя.

Наблюдението на действията на потребителя се извършва в съответствие с настройките на Родителски контрол, дефинирани за този потребител.

В прозореца **Отчет за използване на приложението** можете да видите информация за стартиране на приложения през определен интервал от време за избран акаунт.

Днес

Щракването върху този бутон отваря отчета за активността на потребителя за днес.

Бутони

Щракването върху тези бутони отваря отчети за предишни и следващи периоди.

ден/седмица/месец

Период от време, за който се създава отчетът. Можете да създадете отчет за следните периоди: ден, седмица и месец.

Бутон

Щракването върху този бутон отваря прозореца с настройки на Родителски контрол и показва прозореца **Приложения**. В този раздел можете да наложите ограничения за стартиране и използване на приложения.

Често използвани приложения

Съдържа списък с приложения, които са били стартирани най-често от потребителя в рамките на посочения период. Списъкът също така описва продължителността на използване на всяко приложение.

Блокирани приложения

Съдържа списък с приложения, които са били блокирани за стартиране от Родителски контрол. Приложенията се показват в хронологичен ред, като най-скоро стартираните са показани отгоре.

Щракването върху връзката **<N> повече ▼** ви позволява да видите други приложения, които са били блокирани за стартиране.

Всички използвани приложения

Съдържа списък на всички приложения, които потребителят е стартирал през посочения период. Списъкът също така описва продължителността на използване на всяко приложение.

Приложенията са групирани по категории (например „Игри“ или „IM клиенти“).

Щракването върху бутон ⌄ позволява преглед на списъка с приложения в категория.

Щракването върху бутон › минимизира списъка с приложения в категорията до един ред.

Блокиране на игри по категории

В този прозорец можете да активирате или деактивирате блокирането на игри в зависимост от тяхното съдържание. Класификацията на съдържанието на игрите (наборът от квадратчета с отметки) съответства на оценките PEGI или ESRB. Типът класификация на игрите се избира автоматично в зависимост от вашето местоположение. Ако е необходимо, можете да избирате типа класификация на игрите ръчно в настройките на компонента Родителски контрол.

Ако е избрано квадратчето за отметка до категория, Родителски контрол блокира игрите, включени в категорията.

Ако отметката в квадратчето до категория е премахната, Родителски контрол позволява стартиране на игри в категорията.

Стартирането на игра е разрешено, ако са разрешени всички категории, съответстващи на съдържанието на играта.

Прозорец на обхвата на паролата

Управление на Архивиране и възстановяване

Това квадратче за отметка активира/деактивира опцията, която подканва потребителя за парола при опит за отваряне на прозореца **Архивиране и възстановяване**.

Конфигуриране на програмни настройки

Квадратчето за отметка активира / деактивира показването на подканата за парола, когато потребител се опита да запише промените в настройките на приложението.

Излезте от приложението

Квадратчето за отметка активира / деактивира показването на подканата за парола, когато потребител се опита да затвори приложението.

Премахване на приложението

Това квадратче за отметка активира / деактивира показването на подканата за парола, когато потребител се опита да премахне приложението.

Създай парола

Щракването върху този бутон позволява защита с парола за ограничаване на достъпа до определени функции на приложението.

Обща статистика

В горната част на прозореца се показва името на потребителския акаунт, чиито действия се отчитат в този прозорец.

Контролът е активиран/деактивиран  / 

Този превключвател позволява активиране / деактивиране на наблюдението на действията на потребителя от Родителски контрол.

В зависимост от това дали Родителски контрол наблюдава действията на потребителя, бутонът може да има следния вид:

 – Родителски контрол следи действията на потребителя.

 – Родителски контрол не следи действията на потребителя.

Наблюдението на действията на потребителя се извършва в съответствие с настройките на Родителски контрол, дефинирани за този потребител.

Профил: <profile settings>

Щракването върху тази връзка позволява да конфигурирате настройките на Родителски контрол, които да се прилагат към текущия акаунт.

В раздела **Компютър**, можете да видите времето за използване на компютъра на избрания потребител, да прегледате отчета за използването на компютъра и да конфигурирате настройките на Родителски контрол. Статистиката за използване на компютъра се показва за периода, посочен в отчета за времето на използване на компютъра. По подразбиране се показват статистически данни за текущите двадесет и четири часа.

Детайли

Щракването върху тази връзка отваря прозореца **Отчет за използването на компютъра**. В този прозорец можете да видите информация за времето на използване на компютъра за избрания потребител.

Настройки

Щракването върху тази връзка отваря прозореца. В този прозорец можете да посочите периода от време, през който избраният потребител може да използва компютъра.

В раздел **Приложения** можете да видите подробности за приложенията, които избраният потребител е използвал наскоро. Статистическите данни за използването на приложения се показват за интервала от време, посочен в отчета за използването на приложението. По подразбиране се показват статистически данни за текущите двадесет и четири часа.

Детайли

Щракването върху тази връзка отваря прозореца **Отчет за използването на приложението**. Този прозорец показва подробности за приложенията, стартирани от избрания потребител, и времето за тяхното използване.

Настройки

Щракването върху тази връзка отваря прозореца. В този прозорец можете да посочите приложенията, които избраният потребител може да използва.

Разделът **Интернет** съдържа статистика за посещенията на уеб сайтове и отчет за времето, което потребителят е прекарал в тези уеб сайтове. Можете също да видите общия брой блокирани опити за посещение на блокирани уеб сайтове.

Статистиката за посетените уеб ресурси се показва за периода, посочен в отчета за времето на използване на Интернет. По подразбиране се показват статистически данни за текущите двадесет и четири часа.

Детайли

Щракването върху тази връзка отваря прозореца **Отчет за използването на интернет**. В този прозорец можете да видите информация за уеб ресурси, посетени от избрания потребител.

Настройки

Щракването върху тази връзка отваря прозореца. В този прозорец можете да посочите периода от време, през който на избраният потребител му е позволено да използва Интернет.

Разделът **Контрол на съдържанието** показва информация за броя на блокираните опити за предаване на лични данни.

Тази статистика се показва за периода, посочен в отчета за контрол на съдържанието. По подразбиране се показват статистическите данни за една седмица.

Детайли

Щракването върху тази връзка отваря прозореца. В този прозорец можете да получите информация кои лични данни се е опитал да предаде избраният потребител, докато общува в социалните мрежи.

Настройки

Щракването върху тази връзка отваря прозореца. В този прозорец можете да посочите личните данни, чието използване в комуникацията на избрания потребител искате да наблюдавате.

Отчет за използването на интернет

В горната част на прозореца се показва името на потребителския акаунт, чиито действия се отчитат в този прозорец.

Контролът е активиран/деактивиран  /

Този превключвател позволява активиране / деактивиране на наблюдението на действията на потребителя от Родителски контрол.

В зависимост от това дали Родителски контрол наблюдава действията на потребителя, бутонът може да има следния вид:

 – Родителски контрол следи действията на потребителя.

 – Родителски контрол не следи действията на потребителя.

Наблюдението на действията на потребителя се извършва в съответствие с настройките на Родителски контрол, дефинирани за този потребител.

В прозореца **Отчет за използването на интернет** можете да видите информация за уеб сайтове, посетени от избрания потребител през посочения период.

Днес

Щракването върху този бутон отваря отчета за активността на потребителя за днес.

Бутони

Щракването върху тези бутони отваря отчети за предишни и следващи периоди.

ден/седмица/месец

Период от време, за който се създава отчетът. Можете да създадете отчет за следните периоди: ден, седмица и месец.

Бутон 

Щракването върху този бутон отваря прозореца с настройки на Родителски контрол и показва раздела **Интернет**. В този раздел можете да наложите ограничения на времето за използване на интернет, достъпа до уеб сайтове и изтеглянето на файлове за избрания потребител.

Топ любими уеб сайтове

Този отчет показва списък с уеб сайтове, които потребителят е посещавал често през отчетния период, и броя на посещенията.

Времетраене

Общо време, прекарано в интернет от избрания потребител през посочения период.

Блокирани уеб ресурси

Списък с уеб сайтове, които са блокирани от Родителски контрол и списък с файлове, за които е блокирано изтеглянето.

Покажи всички

Щракването върху тази връзка отваря прозорец, който съдържа информация за броя на блокираните изтегляния на файлове и посещенията на уеб сайта.

Категории уеб сайтове

Той съдържа списък с категории уеб сайтове. За всяка категория уеб сайтове се показва броят на посещенията, които са били блокирани или разрешени от Родителски контрол:

- Броят опити за достъп до уеб сайтове, блокирани от Родителски контрол, се показва в червено.
- Броят опити за достъп до уеб сайтове, разрешени от Родителски контрол, се показва в сиво.

Отчет за използване на компютър

В горната част на прозореца се показва името на потребителския акаунт, чиито действия се отчитат в този прозорец.

Контролът е активиран/деактивиран /

Този превключвател позволява активиране / деактивиране на наблюдението на действията на потребителя от Родителски контрол.

В зависимост от това дали Родителски контрол наблюдава действията на потребителя, бутонът може да има следния вид:

– Родителски контрол следи действията на потребителя.

– Родителски контрол не следи действията на потребителя.

Наблюдението на действията на потребителя се извършва в съответствие с настройките на Родителски контрол, дефинирани за този потребител.

В прозореца **Отчет за използване на компютър** можете да видите информация за времето на използване на компютъра за посочения период за избрания акаунт.

Днес

Щракването върху този бутон отваря отчета за активността на потребителя за днес.

Бутони

Щракването върху тези бутони отваря отчети за предишни и следващи периоди.

ден/седмица/месец

Период от време, за който се създава отчетът. Можете да създадете отчет за следните периоди: ден, седмица и месец.

Бутон

Щракването върху този бутон отваря прозореца с настройки на Родителски контрол и показва раздела **Компютър**. В този раздел можете да зададете времеви ограничения за използване на компютъра.

Отчет за използване на компютър

Съдържа информация за периодите и продължителността на използване на компютъра през посочения период.

Периодите от време, през които компютърът е бил използван от избрания акаунт, са показани в розово.

Текущият период от време (ден, седмица или месец) е маркиран в зелено.

Текущото време на деня (ако е избран периодът *ден* или *седмица*) се показва с червена линия.

Прозорец на Управление на приложения

Стартиране / Ограничения

За да промените как приложенията се показват в списъка, щракнете върху тези връзки:

- Щракването върху връзката **Стартиране** сортира приложенията в списъка в две групи: **Блокиран** и **Разрешено**.
- Щракването върху връзката **Ограничения** сортира приложенията в списъка в надеждни групи. Например надеждни приложения са изброени в групата **Сигурни**.

Изчистване

Като щракнете върху връзката, Kaspersky премахва приложението, което вече не съществува, от списъка.

Изглед

В падащия списък може да изберете режим на показване за приложения и процеси.

- **Разгърни всички**. Избирането на този елемент показва всички приложения, инсталирани на компютъра, в списъка.
- **Събери всички**. Избирането на този елемент показва надеждни групи в списъка.

В падащия списък може да изберете режим на показване за приложения и процеси:

- **Преглед като списък**. Ако изберете тази опция, приложения и процеси се показват като списък.
- **Преглед като дърво**. Ако изберете тази опция, приложения и процеси се показват йерархично, базирано на реда, в който са извикани процесите.

Този падащ списък ви позволява да деактивирате показването на системни приложения, приложения на Kaspersky и немрежови приложения:

- **Скрий системните приложения**. Ако изберете този елемент, общият списък с приложения и процеси не показва приложения, които са необходими за правилното функциониране на операционната система. Системните приложения са скрити по подразбиране.
- **Скрий <PRODUCT>**. Ако изберете този елемент, общият списък с приложения и процеси не показва приложения на Kaspersky. Приложенията на Kaspersky са скрити по подразбиране.
- **Покажи само мрежови програми**. Ако изберете този елемент, общият списък с приложения и процеси показва само мрежови програми. Мрежовите програми са приложения, предназначени за организиране на сътрудничество на група потребители на различни компютри.

Списък с приложения

Този списък съдържа приложения, инсталирани на вашия компютър. За всяко приложение в списъка може да видите информация за състоянието, цифровия подпис, надеждната група, популярността сред потребителите на KSN и времето на тяхното най-скорошно стартиране.

Щракването два пъти върху реда на приложение или процес отваря прозореца **Правила за програмите**. В този прозорец може да конфигурирате правила за контролиране на действията на приложението.

Щракването с десния бутон върху реда на приложението отваря контекстно меню. От контекстното меню може да извършвате следните действия:

- Отваряне на прозореца **Правила за програмите**, в който може да конфигурирате разрешения за дейността на приложението.
- Разрешаване или блокиране на стартиране на приложението.
- Преместване на приложението в друга надеждна група.
- Прилагане на настройките по подразбиране на Контрол на правата на приложението към дадено приложение (настройки за нулиране на приложението).
- Премахване на приложението от списъка.
- Отваряне на папката, която съдържа изпълнимия файл на приложението.

Приложенията в списъка са включени в две групи и подгрупи. Щракването с десния бутон върху реда на групата отваря контекстно меню. От контекстното меню може да извършвате следните действия:

- Отваряне на прозореца **Правила на група**, където може да зададете разрешения по подразбиране за действия на приложения в тази група.
- Създаване на подгрупа в групата. По подразбиране към тази подгрупа се прилагат правилата, посочени за групата, към която тя принадлежи.
- Добавяне на приложение към групата. По подразбиране към това приложение се прилагат правилата, посочени за групата, към която то принадлежи.
- Приложете настройките по подразбиране на Контрол на правата на приложението към групата и всички подгрупи и приложения в тази група (нулирайте настройките на групата).
- Приложете настройките по подразбиране на всички подгрупи и приложения в групата, като запазите непроменени настройките на групата (нулирайте настройките на подгрупата и приложението).
- Изтриване на подгрупи и приложения от групата.

Програма

Тази колона показва името на приложението.

Ограничения

Тази колона показва надеждната група, към която принадлежи приложението. Надеждната група определя правилата за използване на приложението на компютъра: забрана или разрешаване на стартиране, достъпът на приложението до файлове и системния регистър и ограничения на мрежовата активност на приложението.

Популярност

Тази колона показва нивото на популярност на приложението сред участниците в Kaspersky Security Network (KSN). Нивото на популярност отразява броя участници в KSN, които използват приложението.

Мрежа

Тази колона ви позволява да избирате действието, което да се извърши от приложението, когато приложението се опитва да осъществи достъп до мрежата.

Таблицата по-долу изброява операциите, изпълнявани от Kaspersky, когато дадено приложение или група от приложения се опитва да осъществи достъп до мрежата.

Описание на действия на Kaspersky

Действие	Описание
Наследи	Приложението или групата наследява отговора от родителската група.
Разреши	Kaspersky разрешава на приложения, включени в избраната група, да осъществяват достъп до мрежата.
Забрани	Kaspersky не разрешава на приложения, включени в избраната група, да осъществяват достъп до мрежата.
Питай потребителя	Ако е поставена отметка в квадратчето **Изпълнявай препоръчаните действия автоматично** в **Настройки** → **Настройки за производителност** → **Използване на ресурси на компютъра**, Kaspersky автоматично избира действието, което да предприеме за този ресурс, въз основа на правилата, създадени от експертите на Kaspersky. Може да последвате бележката под линия, за да прочетете точно кое действие ще бъде избрано. Ако бъде премахната отметката от това квадратче, приложението пита потребителя дали да разреши на това приложение достъп до мрежата или не.
Записвай в отчет	Освен посочения отговор, Kaspersky регистрира информация за опитите на приложението да осъществи достъп до мрежата и записва информацията в отчет.

Стартиране

В тази колона може да използвате превключвателя, за да разрешавате или блокирате стартиране на избраното приложение. По подразбиране стартиране на приложение е разрешено или блокирано в зависимост от ограниченията за групата, към която принадлежи приложението.

Защита на вашия компютър

Приложението Kaspersky предоставя цялостна защита срещу вируси, мрежови атаки, фишинг, пробиви на лични данни и други видове заплахи за киберсигурността. Различни функции и компоненти за защита са налични като част от приложението Kaspersky за предоставяне на цялостна защита.

Всеки тип заплаха се обработва от специално предназначен защитен компонент. Можете да активирате и деактивирате защитните компоненти и да конфигурирате техните настройки.

В допълнение към защитата в реално време, осигурена от компонентите за сигурност, препоръчваме редовно да сканирате компютъра си за вируси и друг зловреден софтуер. Това е необходимо, за да се предотврати евентуално разпространение на злонамерени програми, които не са били открити от защитните компоненти, например поради зададено ниско ниво на сигурност или по други причини.

За да поддържате приложението Kaspersky актуално, базите данни и модулите на приложението трябва редовно да се актуализират.

Защита на файлове

Защита за файловете предотвратява инфекция на файловата система на компютъра. Компонентът започва при стартиране на операционната система, непрекъснато остава в RAM на компютъра и сканира всички файлове, които се отварят, записват или стартират на компютъра и всички свързани устройства. Приложението Kaspersky прихваща всеки опит за достъп до файл и сканира файла за известни вируси и друг злонамерен софтуер. Допълнителен достъп до файла е позволен само ако файлът не е заразен или е успешно дезинфектиран от приложението. Ако даден файл не може да бъде дезинфектиран по някаква причина, той се заличава. Копие на файла е преместено в Карантина, когато това се случи. Ако даден заразен файл е поставен на същото място, където изтритият файл със същото име се използва, Карантина записва само копие от последния файл. Копие на предишния файл със същото име не е записано.

Защита от мрежови атаки

Защитата от мрежови атаки се зарежда при стартиране на операционната система и проследява входящия мрежови трафик за дейности, характерни за мрежови атаки. Когато се открие опит за атака на компютъра, приложението Kaspersky блокира цялата мрежова дейност от атакуващия компютър, който е насочен към компютъра Ви.

Безопасно сърфиране

Безопасно сърфиране превъзхожда и блокира изпълнението на скриптове на уебсайтове, ако те представляват заплаха. Безопасно сърфиране също следи целия уеб трафик и блокира достъпа до опасни уебсайтове.

Защита за пощата

Защита за пощата сканира входящи и изходящи имейл съобщения на вашия компютър. Имейл съобщение е достъпно за получателя, само ако не съдържа опасни обекти.

Защитна стена

Защитната стена гарантира вашата сигурност, когато използвате локални мрежи и интернет. Компонентът филтрира всички мрежови дейности, като използва правила от два типа: правила за приложения и правила за пакети.

Защитната стена е достъпна само за планове Kaspersky Standard, Kaspersky Plus и Kaspersky Premium.

Системно наблюдение

Компонентът на Системно наблюдение върти промените, направени в операционната система от злонамерена или друга дейност на приложения.

Компонентът предпазва от злонамерен софтуер, включително:

- Експлойт
- Блокиране на екрана
- Шифратори, които шифроват данни
- Криптоджакинг
- Рансъмуер, който криптира данни или блокира достъпа до файлове или системата и изисква откуп за възстановяване на файловете или достъпа до тях

Забраняването на този компонент не се препоръчва.

Антифишинг

Приложението Kaspersky Ви предпазва от посещение на фишинг уебсайтове. Фишинг уебсайт е измамнически уебсайт, който изглежда като уебсайт на банка или платежна система или друг легитимен уебсайт. Може да бъде доста трудно да се различи фишинг уебсайт от легитимен такъв само на база външен вид. Посещението на фишинг уебсайт може да доведе до кражба на пароли, информация за банкови карти и други чувствителни лични данни.

Почистване за поверителност/Отмяна на промените

Този прозорец показва напредъка на почистване на следите от вашите дейности в операционната система. Процесът на почистване може да отнеме известно време. За да премахнете някои следи от дейност, може да е необходимо да рестартирате компютъра.

Ако сте избрали **Отмяна на промените** на първа стъпка, съветникът за почистване на поверителност отменя действията, избрани по време на предишната стъпка.

Използване на ресурси от компютъра

Настройки	Описание
Изпълнявай препоръчаните действия автоматично	Ако бъде премахната отметката от квадратчето, основните компоненти на приложението Kaspersky работят в интерактивен режим. Това означава, че приложението Kaspersky Ви пита да решите кое действие да се предприеме за открити обекти и заплахи, ако опцията **Питай потребителя** е избрана в настройките на Защита на файлове, Защита на интернет, Защита за пощата, Системно наблюдение и Предотвратяване на проникване. Ако е поставена отметка в квадратчето, приложението Kaspersky автоматично избира действието, базирано на правила, определени от експертите на Kaspersky.
Изтриване на злонамерени инструменти, рекламен софтуер, програми за автоматично набиране и подозрителни пакетиращи програми	Ако е поставена отметка в квадратчето, приложението Kaspersky изтрива злонамерени инструменти, рекламен софтуер, програми за автоматично набиране и подозрителни пакетиращи програми в режим на автоматична защита. Функцията е налична, ако е поставена отметка в квадратчето **Изпълнявай препоръчаните действия автоматично**.
Пестене на батерията	Ако е поставена отметка в квадратчето, е активиран режим на пестене на енергия. Приложението Kaspersky отлага планираните задачи. Може да стартирате задачите за сканиране и актуализиране ръчно, ако е необходимо.
Игрален режим	Ако е поставена отметка в квадратчето, приложението Kaspersky не стартира задачите за сканиране и актуализиране и не показва известия, когато играете игри или стартирате приложения в режим на цял екран.
Режим "Не безпокой"	Ако е поставена отметка в квадратчето, приложението Kaspersky не показва известия за събития по време на видеоразговори и при гледане на видеоклипове.
Отлагай сканирането на компютъра, когато системите на процесора и диска са много натоварени	Когато приложението Kaspersky стартира планирани задачи, това може да доведе до повишено натоварване на подсистемите на процесора и диска, което се отразява на работата на други приложения. Когато е поставена отметка в квадратчето, приложението Kaspersky преустановява планираните задачи, когато открие повишено натоварване и освобождава ресурси на операционната система за потребителски приложения.
Сканиране за слаби настройки на операционната система	Ако е поставена отметка в квадратчето, приложението Kaspersky автоматично търси слаби настройки на операционната система.
Стартиране на <PRODUCT> при стартиране на компютъра (препоръчително)	Когато е поставена отметка в квадратчето, приложението Kaspersky стартира, след като операционната система се зареди, защитавайки компютъра през цялата сесия. Когато отметката е премахната от квадратчето, приложението Kaspersky не стартира след зареждане на операционната система, докато потребителят не го стартира ръчно. Защитата на компютъра е изключена и потребителските данни може да са изложени на заплахи.
Използвай технологията за разширено дезинфекциране	Ако е поставена отметка в квадратчето, на екрана се появява изскачащо известие, когато бъде засечена злонамерена активност в операционната система. В това известие приложението Kaspersky предлага на потребителя да извърши Разширено дезинфектиране на компютъра. След като потребителя

(необходими са значителни ресурси на компютъра)	одобри тази процедура, приложението Kaspersky неутрализира заплахата. След завършване на процедурата по Разширено дезинфектиране, приложението Kaspersky рестартира Вашия компютър. Технологията за разширено дезинфектиране използва значителни изчислителни ресурси, което може да забави други приложения. Докато приложението открива активна инфекция, някои функции на операционната система може да не са налични. Наличността на операционната система се възстановява след завършване на разширената дезинфекция и компютърът се рестартира.
Автоматично търсете начини за ускоряване на Вашия компютър	Ако отметката е поставена в квадратчето, се извършва автоматично търсене на възможности за ускоряване на компютъра.
Включи самозащитата	Когато е поставена отметка е квадратчето, Kaspersky предотвратява промяна или изтриване на файлове на приложението на твърдия диск, процеси на паметта и записи в системния регистър.
Разреши управление на настройките на <PRODUCT> чрез приложения за отдалечено управление	Ако е поставена отметка в това квадратче, надеждни приложения за отдалечено управление (като TeamViewer, LogMeIn Pro и Remotely Anywhere) могат да променят настройките на Kaspersky. Ненадеждните приложения за отдалечен контрол няма да могат да променят настройки на Kaspersky дори когато е поставена отметка в квадратчето.
Активиране на външно управление на системните услуги	Ако е поставена отметка в квадратчето, приложението Kaspersky позволява управление на услугите на приложението от отдалечен компютър. Когато бъде направен опит за отдалечено управление на услугите на приложението, в лентата на задачите на Microsoft Windows се показва известие над иконата на приложението (освен ако услугата за известяване не е изключена от потребителя).
Активиране на записване на вторично копие	Ако е поставена отметка в квадратчето, приложението Kaspersky записва вторични копия при срив. Ако е премахната отметката от квадратчето, приложението Kaspersky не записва вторични копия. Също така приложението изтрива съществуващите файлове за разтоварване от твърдия диск на компютъра.
Активиране на защита на файлове с вторични копия и със следи	Ако е поставена отметка в квадратчето, достъпът до файлове с вторични копия се дава на системния администратор и локалния администратор, както и на потребителя, който е активирал записване на вторично копие. Единствено системния и локалния администратор може да осъществява достъп до файловете със следи. Ако отметката е премахната от квадратчето, всеки потребител може да осъществява достъп до файлове с вторични копия и със следи.

Заплахи и изключения

Настройки	Описание
Типове откривани обекти	Приложението открива различни типове обекти, като например вируси и червеи, троянски програми и рекламен софтуер. За детайли вижте Енциклопедия на Kaspersky. Може да изключите откриването на следните типове обекти: • Друг софтуер, който може да се използва от престъпници, за повреждане на вашия компютър или лични данни. Този софтуер включва приложения за отдалечено администриране, които системните администратори могат да използват да осъществят достъп до интерфейса на отдалечен компютър за наблюдение или управление. • Многократно опаковани файлове. Файлове, които са опаковани няколко пъти, включително от различни пакетиращи програми. Многократното опаковане затруднява сканирането на обекти.

Управление на изключения	Щракването върху тази връзка отваря прозореца **Изключения** със списък с изключения. *Изключение за сканиране* е набор от условия, които, когато са изпълнени, карат приложението да не сканира конкретен обект за вируси и други заплахи.
	Може да добавяте, редактирате или изтривате изключения от списъка.
	В прозореца за добавяне или редактиране на изключение може да определите специфични условия, които, когато са изпълнени, ще предотвратят сканирането на обекти (приложението няма да ги сканира):
	• Файл или папка, които трябва да бъдат изключени от сканирания (също така може да изключите изпълними файлове на приложения и процеси). Може да използвате маски в съответствие със следните правила:
	  • Знакът `*` (звездичка), който замества всяка група от знаци, без знаците `\` и `/` (ограничители на имената на файлове и папки в пътищата към тях). Например маската `C:\*\*.txt` ще включва всички пътища към файлове с разширението TXT, които се намират в папки на диск C:, но не в подпапки.
	  • Два последователни знака `*` заемат мястото на всяка група от знаци (включително празен набор) в името на файла или папката, включително знаците `\` и `/` (ограничители на имена на файлове и папки в пътищата към тях). Например маската `C:\Folder\**\*.txt` ще включва всички пътища към файлове с разширението TXT, които се намират в папката с име `Папка` с изключение на самата `Папка`. Маската трябва да включва поне едно ниво на влагане. Маската `C:\**\*.txt` не е валидна маска.
	  • Знакът `?` (въпросителен), който замества всеки единичен знак, без знаците `\` и `/` (ограничители на имена на файлове и папки в пътищата към тях). Например маската `C:\Folder\???.txt` ще включва пътища към всички файлове в папката с име `Папка`, които имат разширение TXT, и име, състоящо се от три знака.
	• Типове обекти, които трябва да бъдат изключени от сканирания. Въведете името на типа обект според класификацията на Енциклопедия на Kaspersky (например `имейл червей`, `комплект за пълен достъп` или `RemoteAdmin`). Може да използвате маски със знак `?` (заменя всеки единичен знак) и знак `*` (заменя всеки брой знаци). Например, ако е посочена маската `Client*`, приложението изключва обектите `Client-IRC`, `Client-P2P` и `Client-SMTP` от сканирания.

	• Контролна сума на обект. Сравняването на контролната сума на даден обект с контролната сума, посочена в тази настройка, позволява сканирането да изключи обект, който не е бил променян от последното сканиране. • Защитни компоненти, за които е приложено изключение. Вместо да изтриете изключение от списъка, може да смените състоянието на изключение на **Неактивен** (в прозореца за добавяне или редактиране на изключение). Когато е неактивно, изключението няма да бъде приложено.
Посочете надеждни приложения	Щракването върху тази връзка отваря прозорец със списъка с надеждни приложения. Приложението Kaspersky не наблюдава активността на файла и мрежата на надеждни приложения (включително злонамерени) и не наблюдава запитванията на тези приложения към системния регистър. Може да добавяте, редактирате или изтривате надеждни приложения от списъка. Дори дадено приложение да е в надеждния списък, Приложението Kaspersky продължава да сканира изпълнимия файл и процеса на това приложение за вируси и други заплахи. Ако не искате да сканирате изпълнимия файл и процеса на надеждно приложение, добавете приложението в списъка с изключения. Когато добавяте или редактирате надеждно приложение, в прозореца **Изключения за програми** може да посочите правилата, които ще бъдат използвани от приложението Kaspersky да контролира активността на надеждното приложение. В прозореца **Изключения за програми** са налични следните правила: • Не сканирай отворени файлове. • Не контролирай активността на програмата. Предотвратяване на проникване не следи за каквато и да е дейност по приложение. • Не наследявайте ограниченията от родителския процес (на приложението). Ако ограничения на родителски процес или приложение не са наследени, активността на приложението се контролира според определените от вас правила или според правилата на надеждната група, към която принадлежи приложението. • Не проследявай активността на дъщерно приложение. • Не блокирай взаимодействието с интерфейса на приложението Kaspersky. На приложението е разрешено да управлява приложението Kaspersky чрез неговия графичен интерфейс. Може да е необходимо да разрешите на приложението да управлява интерфейса на приложението Kaspersky, когато използвате приложение за връзка с отдалечен работен плот или приложение, което поддържа работата на устройство за въвеждане на данни. Примери за такива устройства включват тъчпад и графични таблети. • Не сканирай целия трафик (или шифрован трафик). В зависимост от избраната опция (**Не сканирай целия трафик** или **Не сканирай шифрован трафик**) приложението Kaspersky изключва целия мрежови трафик на приложението или трафика, предаван по SSL, от сканиране. Стойността на тази настройка не се отразява на работата на защитната стрела: защитната стрела сканира трафика на приложението в съответствие с настройките ѝ. Изключенията се отразяват на Защита на пощата, Безопасно сърфиране и Защита от спам. Може да посочите IP адресите или мрежовите портове, към които трябва да се прилагат ограниченията за контрол на трафика.

	Ако промените състоянието на дадено приложение на **Неактивен** в прозореца **Изключения за програми**, приложението Kaspersky не третира приложението като надеждно. По този начин може временно да изключите дадено приложение от надеждния списък, без реално да го изтривате от списъка.
Надеждно системно хранилище за сертификати	Ако е избрано едно от надеждните системни хранилища за сертификати, приложението Kaspersky изключва приложения, подписани с надежден цифров подпис, от сканирания. Kaspersky автоматично задава такива приложения към групата **Сигурни**. Ако е избрано **Не използвай**, Kaspersky сканира приложенията, независимо дали имат цифров подпис или не. Приложението Kaspersky поставя дадено приложение в надеждна група според нивото на опасност, което то може да постави пред компютъра.

Мрежови настройки

Настройки	Описание
Ограничаване на трафика при измервани връзки	Ако е избрано това квадратче за отметка, приложението ограничава своя собствен мрежови трафик, когато интернет връзката е ограничена. Приложението Kaspersky идентифицира високоскоростна мобилна Интернет връзка като ограничена връзка, а Wi-Fi връзката, като неограничена връзка. Чувствителната към разходите работа в мрежа работи на компютри с Windows 8 или по-нова.
Инжектира скрипт в уеб трафик, за да взаимодейства с уеб страниците	Ако е поставена отметка в квадратчето, приложението Kaspersky инжектира скрипт в уеб трафик. Този скрипт гарантира работата на такива компоненти като Безопасно плащане, Поверително сърфиране, Защита от банери и Сканиране на уеб адреси.
Поддържайте DNS върху HTTPS (DoH)	Ако е поставена отметка в квадратчето, приложението обработва правилно DNS данни, прехвърляни по HTTPS. Не препоръчваме да махате отметката от това квадратче.
Управление на сървъри DoH	Връзката отваря прозорец, в който можете ръчно да добавяте сървър DoH, чрез който DNS данни ще бъдат прехвърлени в браузър. Тук може да прочетете за DNS по HTTPS (DoH) и как да добавите сървър DoH.
Контролирани портове	**Контролирай всички мрежови портове**. В този режим за контрол на портовете Защита за пощата, Защита от спам и Безопасно сърфиране контролират всички отворени портове на вашия компютър. **Наблюдение само на избрани мрежови портове**. В този режим за контрол на портовете Защита за пощата, Защита от спам и Безопасно сърфиране контролират избраните портове на вашия компютър. Може да посочите контролираните мрежови портове в прозореца **Мрежови портове**, който може да се отвори чрез щракване върху връзката **Избор**. Също така може да посочите конкретни приложения, където контролирането на всички мрежови портове, използвани от тези приложения, трябва да бъде включено: • **Наблюдаване на всички портове за приложенията от списъка, препоръчан от Kaspersky**. Списъкът с тези приложения е определен по подразбиране и включен в софтуерния пакет за приложението Kaspersky. Ако е избрано това квадратче за отметка, приложението Kaspersky контролира всички портове за следните приложения: • Adobe Acrobat Reader. • Apple Application Support. • Google Chrome. • Microsoft Edge. • Mozilla Firefox. • Internet Explorer. • Java. • mIRC.

	• Opera. • Pidgin. • Safari. • Mail.ru Agent. • Yandex Browser. • **Наблюдаване на всички портове за определени приложения**. Може да посочите приложенията в прозореца **Приложения**, който може да се отвори чрез щракване върху връзката **Избор**.
Мрежови портове	Списък с портове, които обикновено се използват за прехвърляне на трафик от елекктронна поща и уеб трафик, е включен в комплекта за разпространение на приложението Kaspersky. По подразбиране приложението Kaspersky контролира трафика, който преминава през всички портове от този списък. Може да добавяте портове към списъка или да ги изтривате от там. Ако е зададена стойността *Active* в реда на порта в колоната **Статус**, приложението Kaspersky, който минава през този порт. Ако е зададена стойността *Inactive* в реда на порта в колоната **Статус**, приложението Kaspersky изключва този порт от сканиранията, но не го премахва от списъка с портове. Може да сменяте състоянието и други настройки на портовете в прозореца, като щракнете върху бутона **Редактирай**.
Сканиране на шифровани връзки	Може да изберете един от следните режими за сканиране на шифровани връзки по SSL: • **Не сканирай шифровани компоненти**. • **Сканирай шифрованите връзки при заявка от защитните компоненти**. • **Винаги сканирай шифрованите връзки**. Ако опцията **Сканирай шифрованите връзки при заявка от защитните компоненти** е избрана, приложението Kaspersky използва инсталирания сертификат на Kaspersky, за да провери сигурността на SSL връзките, ако това се изисква от защитните компоненти Безопасно сърфиране и Сканиране на уеб адреси. Ако тези компоненти са изключени, приложението Kaspersky не проверява сигурността на SSL връзките. След като приложението Kaspersky провери дадена SSL връзка, сертификатите на уеб сайтовете може да не покажат името на организацията, с което е регистриран уеб сайтът. Ако не искате приложението да проверява дадена SSL връзка с уеб сайт, може да добавите уеб сайта към списъка с изключения, като щракнете върху връзката **Надеждни адреси**.
Когато възникнат грешки при сканиране на шифрована връзка	В падащия списък може да изберете действие, което приложението ще извърши, ако възникне грешка при сканиране на защитени връзки на уеб сайта. • **Игнориране**. Приложението прекъсва връзката с уеб сайта, на който е възникнала грешка при сканиране. • **Питай**. Приложението ви показва известие с подкана да добавите адрес на уеб сайт към списъка с уеб сайтове, на които са възникнали грешки при сканиране. Адресът на уеб сайта ще бъде проверен в базата данни със злонамерени обекти.

	• **Добавяне на домейн към изключенията**. Приложението добавя адреса на уеб сайта в списъка с уеб сайтове, на които са възникнали грешки. Адресът на уеб сайта ще бъде проверен в базата данни със злонамерени обекти.
Домейни с грешки при сканиране	Списък с домейни, които не могат да бъдат сканирани поради грешки, когато се свързвате към тях. Адресите на домейните са проверени в базата данни със злонамерени обекти.
Надеждни адреси	Щракнете върху тази връзка, за да отворите прозореца **Надеждни адреси**, който съдържа списък с уеб сайтове, които сте добавили като изключение за компонентите Безопасно сърфиране и Сканиране на уеб адреси.
Сигурни приложения	Списък с приложения, чиято активност не се наблюдава от приложението Kaspersky по време на работата им. Може да изберете типовете дейност на приложенията, които приложението Kaspersky няма да наблюдава (например да не сканира мрежовия трафик). Приложението Kaspersky поддържа променливи на средата и маските `*` и `?`.
Блокиране на SSL 2.0 връзки (препоръчително)	Ако е поставена отметка в квадратчето, приложението блокира мрежови връзки, установени по SSL 2.0 протокол. Ако е премахната отметката от квадратчето, приложението не блокира мрежовите връзки, установени по SSL 2.0 протокол, и не наблюдава мрежовия трафик, предаван по тези връзки.
Дешифрирайте шифрована връзка с уеб сайта, който използва EV сертификат	EV сертификатите (Сертификати с разширена валидация) потвърждават автентичността на уеб сайтовете и подобряват сигурността на връзката. Браузърите използват икона с катинар в своята адресна лента, за да покажат, че уеб сайтът има EV сертификат. Браузърите могат също така да оцветят изцяло или частично в зелено адресната лента. Ако е поставена отметка в квадратчето, приложението дешифрира и наблюдава шифрованите връзки с уеб сайтове, които използват EV сертификат. Ако отметката е премахната от квадратчето, приложението няма достъп до съдържанието на HTTPS трафика. Поради това приложението наблюдава HTTPS трафика единствено базирано на адреса на уеб сайта, например `https://bing.com`. Ако отваряте уеб сайт с EV сертификат за първи път, шифрованата връзка ще бъде дешифрирана, независимо дали има отметка в квадратчето или не.
Настройки за прокси сървър	Настройки на прокси сървъра, използван за интернет достъп на потребители на клиентски компютри. Приложението Kaspersky използва тези настройки за определени защитни компоненти, включително за актуализиране на бази данни и модули на приложения. За автоматично конфигуриране на прокси сървър приложението Kaspersky използва WPAD протокол (протокол за автоматична настройка на прокси сървър). Ако IP адресът на прокси сървъра не може да бъде определен, като се използва този протокол, приложението използва адрес на прокси сървър, който е посочен в настройките на браузъра Microsoft Internet Explorer.
Използвайте избрания магазин за сертификати за сканираниране на шифровани връзки в приложенията на Mozilla	Ако е избрано това квадратче за отметка, приложението сканира шифрован трафик в браузъра Mozilla Firefox и пощенския клиент Thunderbird. Достъпът до някои уеб сайтове чрез HTTPS протокол може да бъде блокиран.

За да сканирате трафика в Mozilla Firefox и Thunderbird, трябва да разрешите сканиране на шифровани връзки. Ако сканирането на шифровани връзки е забранено, приложението не сканира шифрован трафик в Mozilla Firefox и Thunderbird.

Приложението използва главен сертификат на Kaspersky за дешифриране и анализиране на шифрован трафик. Може да изберете хранилището за сертификати, което ще съдържа главния сертификат на Kaspersky.

- **Използване на хранилището за сертификати на Windows (препоръчително)**. Главният сертификат Kaspersky е добавен към това хранилище по време на инсталирането на приложението Kaspersky.

- **Използване на хранилището за сертификати на Mozilla**. Mozilla Firefox и Thunderbird използват собствени хранилища за сертификати. Ако е избрано хранилището за сертификати на Mozilla, трябва ръчно да добавите главния сертификат на Kaspersky към това хранилище през свойствата на браузъра.

Управление на настройките на приложението

Настройки	Описание
Импорт	Извлечете настройките на приложението от файл в CFG формат и ги приложете.
Експорт	Запишете текущите настройки на приложението на файл в CFG формат.
Възстанови	Може да възстановите по всяко време настройките, препоръчани от експертите на Kaspersky. Когато настройките се възстановят, нивото на защита **Оптимално** се задава за всички защитни компоненти.

Защитна стена

Настройки	Описание
Уведоми за уязвимости в Wi-Fi мрежите	Ако е избрано това квадратче за отметка, приложението Kaspersky показва известия, когато бъдат открити някакви уязвимости в Wi-Fi мрежата. Достъп до това квадратче за отметка може да получите, ако Kaspersky VPN Secure Connection не е инсталирана на компютъра. Ако е избрано квадратчето за отметка **Блокирай и предупреди за несигурни прехвърляния на пароли чрез Интернет**, приложението Kaspersky блокира прехвърлянето на парола в нешифрован текстови формат, когато попълвате полето **Парола** в интернет. Щракването върху връзката **Избор на категории** отваря прозореца **Категории**, в който може да посочите типовете уязвимости на Wi-Fi мрежите. Приложението ще ви извести, когато се опитате да се свържете към Wi-Fi мрежа, която има посочената уязвимост.
Показване на устройства, които са свързани с моите мрежи	Ако квадратчето е избрано, Умното домашно наблюдение е активирано и функционира.
Разреши връзки на произволни портове за FTP режим	Ако е поставена отметка в квадратчето, защитната стена позволява връзки на вашия компютър на произволни портове, ако бъде открито превключване към активен FTP режим на връзката с хоста.
Не изключвай защитната стена, докато операционната система не спре напълно	Ако е поставена отметка в квадратчето, защитната стена не спира да работи, докато операционната система не спре напълно.
Блокирай мрежовите връзки, ако потребителят не може да избере действие	Ако е поставена отметка в квадратчето, Защитната стена няма да спре, когато интерфейсът на приложението Kaspersky не е зареден.
Правила за програмите	Щракването върху тази връзка отваря прозореца **Мрежови правила за програми**. Този прозорец показва информация, свързана с мрежовата активност на приложения и групи приложения. Компонентът Предотвратяване на проникване управлява мрежовата активност на приложения в съответствие с мрежовите правила на приложенията и групите приложения. Може да конфигурирате разрешения за мрежова активност на приложение или група приложения чрез менюто на клетка в колоната **Мрежа**. Елементите в менюто са описани в раздела Правила на предотвратяване на проникване. Като изберете **Подробна информация и правила** в контекстното меню на даден ред, може да преминете към конфигуриране на мрежови правила за приложение или група приложения.
Правила за пакетите	Щракването върху тази връзка отваря прозореца **Правила за пакетите**. По подразбиране прозорецът показва предварително определени правила за

мрежовите пакети, които са препоръчани от експертите на Kaspersky за оптимална защита на мрежовия трафик на компютри с операционни системи на Microsoft Windows.

Правилата за мрежови пакети служат за налагане на ограничения на мрежовите пакети, независимо от приложението. Такива правила ограничават входящия и изходящия мрежови трафик чрез специфични портове на избрания протокол за данни.

Правилата за мрежови пакети имат по-висок приоритет от мрежовите правила за приложенията.

Когато добавяте или редактирате правило за пакет, може да определите следните настройки:

- Действие:
  - **Разреши**. Приложението Kaspersky позволява мрежова връзка.
  - **Блокирай**. Приложението Kaspersky блокира мрежовата връзка.
  - **По правило за програмата**. Приложението Kaspersky не обработва потоци от данни според правило за пакет, а вместо това прилага правило за приложение (вж. **Application rules** по-горе).
- Име.
- Посока:
  - **Входящо**. Приложението Kaspersky прилага правилото към мрежови връзки, отворени от отдалечен компютър.
  - **Изходящо**. Приложението Kaspersky прилага правилото към мрежовата връзка, отворена от Вашия компютър.
  - **Входящо / Изходящо**. Приложението Kaspersky прилага правилото към входящите и изходящите пакети или потоци от данни, независимо кой компютър (Вашият или отдалечен) е инициирал мрежовата връзка.
  - **Входящо (пакет)**. Приложението Kaspersky прилага правилото към пакети данни, получени от Вашия компютър.
  - **Изходящо (пакет)**. Приложението Kaspersky прилага правилото към пакети с данни, изпратени от Вашия компютър.
- Протокол.
- Настройки на ICMP. Може да посочите типа и кода на пакетите с данни, които да бъдат сканирани. Разделът настройки е наличен, ако са избрани ICMP или ICMPv6 протоколи.
- Отдалечени портове (портове на отдалечен компютър).
- Локални портове (портове на вашия компютър).

	Може да посочите набор от отдалечени или локални портове (например `6660-7000`), да изброите множество портове, разделени със запетая, или да комбинирате и двата метода (например `80-83,443,1080`).
	
	• Адрес:
	  • **Всеки адрес**.
	  • **Подмрежови адреси**. Приложението Kaspersky ще приложи правилото към IP адреси от всички мрежи, които в момента са свързани, и са от определения тип (*Public*, *Local* или *Trusted*). Типът мрежа може да бъде избран от падащия списък, който се показва отдолу, ако е избрана опцията **Подмрежови адреси**.
	  • **Адреси от списъка**. Приложението Kaspersky прилага правилото към IP адреси в посочения диапазон. Може да посочите IP адреси в полетата **Отдалечени адреси** и **Локални адреси**, които са показани отдолу, ако е избрана опцията **Адреси от списъка**. Добавените IP адреси трябва да бъдат разделени със запетая.
	• Състояние. Защитната стена прилага само правила за пакетите, които са със състояние **Активен**. Може да зададете състояние **Неактивен**, за да деактивирате временно правилото за пакетите, без да го изтривате от списъка с правила за пакетите.
	• Мрежови адаптери, преминати от мрежови пакети.
	• Използване на TTL. Приложението Kaspersky контролира предаването на мрежови пакети, чието време на живот (TTL) не надвишава определената стойност.
	• Регистриране на събития в отчета на приложението Kaspersky.
	
	За да добавите бързо дадено правило, може да изберете един от предварително определените шаблони в падащия списък в долната част на прозореца.

Налични мрежи	Щракването върху тази връзка ще отвори прозореца **Мрежи**, които съдържат списък с мрежови връзки, които са открити на компютъра от защитната стена. В списъка може да промените типа на мрежата (*Public*, *Trusted* или *Local*), като използвате менюто в клетката **Тип на мрежа**. Може да редактирате мрежовите настройки в прозореца **Свойства на мрежа**, който може да се отвори като щракнете два пъти върху реда на мрежата. Типът *Публична* е зададена за интернет по подразбиране. Не може да променяте типа мрежа или други настройки за интернет. В прозореца **Свойства на мрежа** може да редактирате следните мрежови настройки: • Име на мрежа. • Тип мрежа. • Показване на известия за следното:

	• Връзка към мрежата. • Сменен MAC адрес (например ако мрежовият адаптер е сменен). • Сменен MAC адрес/сдвояване на IP адрес (например когато DHCP услуга задава различен IP адрес). • Избор на принтер, който трябва да бъде препоръчан по подразбиране, когато се свързва към тази мрежа. Тази настройка се показва, ако е инсталиран принтер в операционната система на вашия компютър. • Списък с допълнителни подмрежи (разделени със запетая).

Правила за приложението/Правила на група

Настройки	Описание
Файл (само в прозореца **Правила за програмите**)	Помощна информация за приложение и за изпълнимия файл на приложението. Приложението Kaspersky получава информация за дадено приложение от изпълнимия файл на приложението и от Kaspersky Security Network.
Файлове и системен регистър	Правила за достъп до ключове от системния регистър и файлове, свързани с работата на операционната система или с вашите лични данни. Индивидуалните настройки за достъп за операциите по четене, писане, създаване и изтриване могат да бъдат определени независимо с помощта на менюто в клетките на съответните колони в таблицата. Елементите в менюто са описани в раздела Правила на предотвратяване на проникване.
Права	Права за достъп до ресурси и процеси на операционната система и права за стартиране. Може да зададете права за достъп с помощта на менюто в клетките на колоната **Действие**. Елементите в менюто са описани в раздела Правила на предотвратяване на проникване.

Мрежови правила	Правила, прилагани от приложението Kaspersky, за регулиране на мрежовата активност на приложение или група от приложения.
	По подразбиране списъкът показва предварително определените мрежови правила на приложението, които се препоръчват от експертите на Kaspersky. Не можете да изтривате или редактирате предварително определени мрежови правила (освен смяна на действието в колоната **Разрешение**; вижте описанието на наличните действия в раздела Правила на Предотвратяване на проникване).
	Когато добавяте или редактирате правило, може да определите следните настройки:
	• Действие:
	  • **Разреши**. Приложението Kaspersky позволява мрежова връзка.
	  • **Блокирай**. Приложението Kaspersky блокира мрежовата връзка.
	  • **Питай потребителя**. Ако е премахната отметката от квадратчето **Изпълнявай препоръчаните действия автоматично** в **Настройки → Настройки за производителност → Използване на ресурси на компютъра**, Permissio иска потребителя да реши дали да разреши или откаже мрежовата връзка. Ако е поставена отметка в квадратчето, действието се избира автоматично. Може да последвате бележката под линия в прозореца на приложението, за да прочетете точно кое действие ще бъде избрано.
	• Име.
	• Посока:
	  • **Входящо**. Приложението Kaspersky прилага правилото към мрежови връзки, отворени от отдалечен компютър.
	  • **Изходящо**. Приложението Kaspersky прилага правилото към мрежовата връзка, отворена от Вашия компютър.
	  • **Входящо / Изходящо**. Приложението Kaspersky прилага правилото към входящите и изходящите пакети или потоци от данни, независимо кой компютър (Вашият или отдалечен) е инициирал мрежовата връзка.

	• Протокол. • Настройки на ICMP. Може да посочите типа и кода на пакетите с данни, които да бъдат сканирани. Разделът настройки е наличен, ако са избрани ICMP или ICMPv6 протоколи. • Отдалечени портове (портове на отдалечен компютър). • Локални портове (портове на вашия компютър). Може да посочите набор от отдалечени или локални портове (например `6660-7000`), да изброите множество портове, разделени със запетая, или да комбинирате и двата метода (например `80-83,443,1080`). • Адрес: • **Всеки адрес**. • **Подмрежови адреси**. Приложението Kaspersky ще приложи правилото към IP адреси от всички мрежи, които в момента са свързани, и са от определения тип (*Public*, *Local* или *Trusted*). Типът мрежа може да бъде избран от падащия списък, който се показва отдолу, ако е избрана опцията **Подмрежови адреси**. • **Адреси от списъка**. Приложението Kaspersky прилага правилото към IP адреси в посочения диапазон. Може да посочите IP адреси в полето **Отдалечен адрес**, което е показано долу, ако е избрана опцията **Адреси от списъка**. • Мрежови адаптери, преминати от мрежови пакети. • Използване на TTL. Приложението Kaspersky контролира предаването на мрежови пакети, чието време на живот (TTL) не надвишава определената стойност. • Регистриране на събития в отчета на приложението Kaspersky. За да добавите бързо дадено правило, може да изберете един от предварително определените шаблони в падащия списък в долната част на прозореца.
Изключения (само в прозореца **Правила за програмите**)	Може да изберете правила, които ще бъдат използвани да изключват дадено приложение от сканирания: • Не сканирай отворени файлове. • Не контролирай активността на програмата. Предотвратяване на проникване не следи за каквато и да е дейност по приложение. • Не наследявайте ограниченията от родителския процес (на приложението). Ако ограничения на родителски процес или приложение не са наследени, активността на приложението се контролира според определените от вас правила или според правилата на надеждната група, към която принадлежи приложението. • Не проследявай активността на дъщерно приложение. • Не блокирай взаимодействието с интерфейса на приложението Kaspersky. На приложението е разрешено да управлява приложението Kaspersky чрез неговия графичен интерфейс. Може да е необходимо да разрешите на приложението да управлява интерфейса на приложението Kaspersky, когато използвате приложение

	за връзка с отдалечен работен плот или приложение, което поддържа работата на устройство за въвеждане на данни. Примери за такива устройства включват тъчпад и графични таблети. • Не сканирай целия трафик (или шифрован трафик). В зависимост от избраната опция (**Не сканирай целия трафик** или **Не сканирай шифрован трафик**) приложението Kaspersky изключва целия мрежови трафик на приложението или трафика, предаван по SSL, от сканиране. Стойността на тази настройка не се отразява на работата на защитната стрела: защитната стрела сканира трафика на приложението в съответствие с настройките ѝ. Изключенията се отразяват на Защита на пощата, Безопасно сърфиране и Защита от спам. Може да посочите IP адресите или мрежовите портове, към които трябва да се прилагат ограниченията за контрол на трафика.
Хронология (само в прозореца **Правила за програмите**)	Помощна информация за действията, предприети върху приложението, като например стартиране на приложението или задаване на надеждна група.

Правила на Предотвратяване на проникване

Правило е набор от реакции на Предотвратяване на проникване в отговор на действия, които дадено приложение изпълнява в различни категории ресурси на операционната система и лични данни.

Предотвратяването на проникване може да реагира на действията на приложение по следните начини:

- **Наследи**. Предотвратяването на проникване реагира на дейността на приложението, като прилага правилото, което е конфигурирано за състоянието, което Предотвратяване на проникване е присвоило на приложението.

  Този отговор се прилага по подразбиране. По подразбиране Предотвратяването на проникване наследява правата на достъп от състоянието, което Предотвратяването на проникване е задало на приложението.

  Ако сте редактирали правило за приложение, това правило за приложението ще има по-висок приоритет от правилото за състоянието, което е било зададено на приложението.

- **Разреши**. Предотвратяване на проникване разрешава на приложението да изпълнява действието.

- **Забрани**. Предотвратяване на проникване не позволява на приложението да изпълнява действието.

- **Питай потребителя**. Ако отметката е премахната от квадратчето **Изпълнявай препоръчаните действия автоматично** в **Настройки** → **Настройки за производителност** → **Използване на ресурси на компютъра**, Предотвратяване на проникване иска от потребителя да реши. Ако е поставена отметка в квадратчето, действието се избира автоматично. Може да последвате бележката под линия в прозореца на приложението Kaspersky, за да прочетете точно кое действие ще бъде избрано.

- **Записвай в отчет**. Предотвратяване на проникване записва информация за дейността на приложението и й отговаря в отчет. Информацията може да бъде добавена към отчет в допълнение към всяко друго действие, предприето от Предотвратяване на проникване.

Настройки за въвеждане на защитени данни

Настройки	Описание
Използвайте виртуализация на хардуера, ако има налична	Ако е поставена отметка в квадратчето, ще се използва виртуализация на хардуера (софтуер за управление) за работата на Защитения браузър. Приложението използва технология със софтуер за управление за допълнителна защита срещу сложен злонамерен софтуер, който може да прехване личните ви данни с помощта на клипборда или фишинг. Това квадратче за отметка се показва, когато приложението е инсталирано на 64-битова версия на Windows 8, Windows 8.1 и Windows 10. За повече детайли за виртуализацията на хардуера и как работи щракнете върху връзката.
Защита чрез виртуализация на хардуера	Защитено въвеждане от клавиатурата ви помага да предотвратите киберпрестъпници да прехванат данни, които въвеждате от клавиатурата, когато посещавате уеб сайтове (за повече детайли вижте раздела За защитеното въвеждане от клавиатурата). Изберете квадратчетата за отметки за категориите уеб сайтове, на които искате да защитавате данните, които са въведени чрез клавиатурата. Щракнете върху връзката **Управление на изключения**, за да създадете списъци с уеб сайтове, на които искате да активирате или деактивирате Защитено въвеждане от клавиатурата, независимо от избраните категории уеб сайтове. Може да използвате маски, когато добавяте изключения.
Екранна клавиатура	Много програми, класифицирани като шпионски софтуер, могат да правят екранни снимки, които автоматично се предават към нарушител за допълнителен анализ за кражба на личните данни на потребителя. Екранна клавиатура защитава въведените лични данни от опити за прехващането им чрез екранни снимки. (За повече детайли вижте За екранната клавиатура). За да се уверите, че екранната клавиатура е активирана, трябва да рестартирате компютъра след инсталиране на приложението Kaspersky. Може да избирате как ще може да отваряте екранната клавиатура: • **Отваряне на виртуалната клавиатура с клавишна комбинация CTRL+ALT+SHIFT+P**. • **Показвай икона за бързо стартиране в полетата за въвеждане**. Иконата за бързо стартиране на Екранна клавиатура се показва в полетата за въвеждане на парола на уеб страниците. Изберете квадратчетата за отметки за категориите уеб сайтове, на които искате да защитавате данните, които са въведени чрез екранна клавиатура. Щракнете върху връзката **Управление на изключения** в прозореца **Изключения за екранна клавиатура**, за да създадете списъци с уеб сайтове, на които искате да активирате или деактивирате показването иконата за бързо стартиране на Екранна клавиатура, независимо от избраните категории уеб сайтове. Може да използвате маски, когато добавяте изключения.
Покажи съвети за създаване на силни пароли	Ако е поставена отметка в квадратчето, приложението Kaspersky проверява сигурността на парола, която въвеждате в браузъра за първи път, и Ви уведомява за това.
Защита от използване на	Когато въвеждате парола в уеб сайт, където сигурността на паролата е особено важна (например в социална мрежа), приложението Kaspersky Ви подканва да

едни и същи пароли	активирате защитата от използване на едни и същи пароли. Ако е поставена отметка в квадратчето **Предупреждение за използване на едни и същи пароли на уеб сайтове** защитата срещу използване на едни и същи пароли е активирана. Може да **избирате категориите уеб сайтове,** които трябва да бъдат защитени от използване на едни и същи пароли. Тези категории включват уеб сайтове на банки и системи за плащане, уеб сайтове на социални мрежи и уеб сайтове на пощенски услуги. Може да щракнете върху връзката **Изтрий запаметените данни**, за да изтриете всички запазени по-рано пароли.

Прозорец Изберете файлове за изтриване

Поле за въвеждане на пътя към файла или папката

Полето съдържа пътя към файл или папка, които да бъдат изтрити завинаги. Може да изберете файл или папка от дървото над полето за въвеждане или ги посочете ръчно.

Прозорец Изберете данни за шифроване

Поле за въвеждане на пътя към файла или папката

Полето съдържа пътя към файл или папка, която да бъде добавена към тайно хранилище. Може да изберете файл или папка от дървото над полето за въвеждане или ги посочете ръчно.

Прозорец за отваряне на тайно хранилище

Парола за достъп до тайното хранилище

Парола за достъп до файловете в тайното хранилище.

Отвори в Windows Explorer

Щракването върху този бутон отваря папката в Explorer със списък с файлове и папки, съхранявани в тайното хранилище.

Прозорец за изтриване на тайно хранилище

Парола за достъп до тайното хранилище

Парола за достъп до файловете в тайното хранилище.

Изтриване на тайно хранилище

Като щракнете върху този бутон, приложението Kaspersky изтрива хранилището за данни и всички файлове, съхранявани в него.

Файловете и папките в тайното хранилище се изтриват завинаги.

Прозорец за преименуване на тайно хранилище

Ново име на хранилище

Новото име, което да се зададе на тайното хранилище.

Запази

Като щракнете върху този бутон, приложението Kaspersky задава новото име на тайното хранилище.

Прозорец Промяна на паролата на тайното хранилище

Стара парола

Текуща парола за тайното хранилище.

Нова парола

Нова парола за тайното хранилище.

Потвърждение на паролата

Въведете повторно паролата, която сте въвели в полето **Нова парола**.

Запази

Щракването върху този бутон заменя текущата парола за тайното хранилище с новата парола.

Изберете прозорец на файл или тайно хранилище

Поле за въвеждане на пътя към файла

Полето съдържа пътя към файла на тайното хранилище. Може да изберете тайно хранилище от дървовидната структура над полето за въвеждане или да посочите пътя към тайното хранилище ръчно.

Прозорец Архивиране и възстановяване

Избор на файлове

Щракването върху този бутон стартира Съветника за създаване на задача за архивиране.

Възстанови файлове от моя архивен набор

Щракването върху тази връзка отваря прозорец със списъка с резервни хранилища. В този прозорец може да изберете хранилище със създаден преди това набор от резервни копия.

Бутони ◻ / ⏸ / ▷

Бутонът може да се използва за управление на процеса по архивиране:

◻ – спиране на задача за архивиране. Този бутон се показва, ако задача за архивиране се изпълнява или е спряна временно в момента.

⏸ – пауза на задача за архивиране. Този бутон се показва, ако в момента се изпълнява задача за архивиране.

▷ – стартиране на задача за архивиране или възобновяване на временно спряна задача за архивиране. Този бутон е наличен, ако задача за архивиране е завършена или спряна временно.

Стартирай

Щракването върху бутона стартира процеса по създаване на резервни копия на файлове. Този бутон се показва, ако в момента не се изпълнява задача за архивиране.

Щракването върху бутона ⌄ отваря меню, от което може да изберете допълнително действие с посочените настройки за архивиране:

- **Настройки** – стартира съветника на редактора за настройки на архивиране.
- **Изтрий настройки** – изтрива настройки на архивиране.

Възстанови файловете

Щракването върху този бутон отваря прозореца **Възстановяване на файлове от резервни копия**. Този прозорец ви позволява да изберете резервни копия, от които да възстановите файлове.

Вход в Dropbox

Щракването върху този бутон отваря прозореца за вход в уеб сайта на Dropbox. Ако все още нямате акаунт, може да продължите с регистрацията на уеб сайта на Dropbox.

Бутонът се показва, ако все още не сте влезли в уеб сайта на Dropbox на този компютър.

Актуализирай статуса

След щракване върху този бутон, приложението Kaspersky се свързва към онлайн хранилище и актуализира информацията за размера на онлайн хранилището и размера на файловете, съхранявани в него.

Този бутон се показва, ако приложението не е можело преди това да извлече информация за онлайн хранилище (например ако компютърът не е бил свързан с интернет).

детайли

Щракването върху тази връзка отваря прозореца **Отчети**. Този прозорец показва детайлна информация за завършените задачи за архивиране.

Режим за стартиране

Щракването върху тази връзка отваря прозореца **График за архивиране**. В този прозорец може да промените режима за стартиране на задача за архивиране.

Изчистване

Щракването върху този бутон отваря прозореца **Изчисти хранилище**, в който може да премахнете нежеланите резервни копия от резервното хранилище.

Създайте резервни копия на други файлове

Щракването върху този бутон отваря прозореца на Съветника за създаване на задача за архивиране, в който може да добавяте файлове, които да бъдат архивирани.

Възстановете файлове от резервни копия, които не са в списъка

Щракването върху тази връзка отваря прозореца **Търсене на резервни копия**. В този прозорец може да посочите резервно хранилище със създадени преди това резервни копия.

Управление на съхранение

Щракването върху този бутон отваря прозорец със списъка с налични резервни хранилища. В този прозорец може да възстановите файлове от резервни копия в избраното хранилище, да редактирате настройки на избраното хранилище или да го изтриете и да добавяте хранилище към списъка.

Прозорец Изберете папки за архивиране

Поле за въвеждане на пътя към папката

Полето съдържа пътя към папката, която да бъде архивирана. Може да изберете папка от дървото над полето за въвеждане или ги посочете ръчно.

Прозорец на Restore Utility

Копирай Copy Kaspersky Restore Utility в хранилище

Ако е поставена отметка в квадратчето, приложението Kaspersky копира Kaspersky Restore Utility в хранилище по време на процеса по архивиране. Тази помощна програма може да се използва за възстановяване на файлове от резервни копия, когато приложението Kaspersky е повредено или не е инсталирано.

Прозорец Файлове, избрани за архивиране

Списък с типове файлове

Съдържа имена на типове файлове и броя файлове от всеки тип.

Когато е избран елемент от списъка, се изброяват всички файлове от този тип.

Списък с файлове от избрания тип

Съдържа информация за всички файлове от специфичен тип, които са били избрани за резервно архивиране: име на файл, местоположение и размер.

Ако е поставена отметка в квадратчето до името на файл, приложението архивира този файл.

Ако няма поставена отметка в квадратчето до името на файл, приложението не архивира този файл.

Раздел Мрежови диск

Диск

Път до папка в мрежата, използвана като резервно хранилище.

Преглед

Щракването върху този бутон отваря прозореца **Избор на папка**. В този прозорец може да изберете папка в мрежата, използвана за резервно хранилище.

Потребителско име

Име на акаунт за достъп до папка в мрежата. Потребителското име трябва да бъде посочено във формата *<computer name>\<user name>* (например *kl-12345\ivanov*).

Парола

Парола за достъп до папка в мрежата.

Раздел Локален диск

Списък с локални дискове

Списъкът включва локални дискове на компютъра. Може да изберете един от локалните дискове като място за съхранение за резервни копия.

Ако локалният диск не се появява в списъка, може да посочите пътя към него в полето отдолу или да щракнете върху бутона **Преглед** и изберете локалния диск в прозореца **Изберете папка за архивиране**, който се отваря.

Преглед

Щракването върху този бутон отваря прозореца **Изберете папка за архивиране**. В този прозорец може да изберете локален, използван като резервно хранилище.

Раздел Сменяемо устройство

Списък със свързани сменяеми устройства

Списъкът включва сменяеми устройства, свързани към компютъра. Може да изберете едно от сменяемите устройства като място за съхранение за резервни копия.

Ако сменяемото устройство не се появява в списъка, може да посочите пътя към него в полето отдолу или да щракнете върху бутона **Преглед** и изберете сменяемото устройство в прозореца **Избор на папка**, който се отваря.

Преглед

Щракването върху този бутон отваря прозореца **Избор на папка**. В този прозорец може да изберете сменяемо устройство, използвано като резервно хранилище.

Раздел Онлайн хранилище

За да използвате Онлайн хранилище, влезте в уеб сайта dropbox.com. Щракването върху **OK** отваря автоматично уеб страница с формата за влизане в уеб сайта dropbox.com.

Прозорец Хранилища

Списък с хранилища

Изброява резервни хранилища, които са създадени. Информацията, показана за всяко хранилище, включва общо и използвано място за съхранение, местоположение на хранилище, задачи, които използват това хранилище, и наличните операции.

Възстанови файловете

Щракването върху този бутон отваря прозорец със списък от набори резервни копия, съхранявани в това хранилище. В този прозорец може да изберете набор резервни копия, от които да възстановите файлове.

Щракването върху бутона ⌄ отваря меню, от което може да изберете допълнително действие:

- **Настройки** – стартира съветника на редактора за настройки на хранилище.
- **Изтрий хранилище** – спира използването на избрания диск или онлайн ресурси като хранилище за резервни копия на файлове и изтрива всички резервни копия на файлове от хранилището.
- **Изчисти хранилище** – отваря **Изчисти хранилище** прозорец. В този прозорец може да изберете резервни копия на файлове, които да бъдат премахнати от хранилището, за да се освободи място в него.

Добави мрежово хранилище

Щракването върху тази връзка отваря прозореца **Добави мрежово хранилище**. В този прозорец може да посочите настройките на мрежови диск, който искате да добавите към списъка с хранилища.

Свързване към налично хранилище

Щракването върху тази връзка отваря прозореца **Свързване на хранилище**. В този прозорец може да посочите настройките на локален диск, сменяем диск, мрежови диск или онлайн хранилище, които искате да добавите към списъка с хранилища.

Прозорец със списък с набори от резервни копия в хранилище

Списък с набори от резервни копия

Съдържа информация за набори от резервни копия в хранилище:

- Име на набора от резервни копия
- Дисково пространство, необходимо за възстановяване на файлове от този набор

Възстанови файловете

Щракването върху този бутон отваря прозореца **Възстановяване на файлове от резервни копия**. Този прозорец ви позволява да изберете резервни копия, от които да възстановите файлове.

Прозорец за поддръжка

Разделът **Техническа поддръжка на Kaspersky** съдържа информация, необходима за връзка с техническата поддръжка на Kaspersky: номер на версията на Kaspersky Small Office Security, дата и час на пускане на базите данни и приложните модули, версия на операционната система и ключ.

Лицензионен ключ

С натискане на връзката **<key>** се отваря прозорец с **Подробности за лиценза**, който предоставя информация за текущия лиценз.

Други версии

Щракването върху тази връзка отваря уеб сайта, от който можете да изтеглите версията на приложението, която е предназначена за използване във вашия регион. Тази връзка не е налична във всички версии на приложението.

Отговори на често задавани въпроси

Щракването върху тази връзка отваря страницата за интерактивна поддръжка в прозореца на браузъра. Тази страница предоставя отговори на въпросите, които потребителите най-често задават на специалистите по техническа поддръжка на Kaspersky.

Съвети за конфигуриране на програмата

Щракването върху тази връзка отваря в прозореца на браузъра уебстраницата за техническа поддръжка, която показва статии за това как да конфигурирате и използвате Kaspersky.

Форум

Щракването върху тази връзка отваря форума на Kaspersky в прозорец на браузъра, където можете да разглеждате публикуваните теми, да оставяте коментари, да създавате нови теми и да търсите информация.

Инструменти за поддръжка

Щракването върху тази връзка отваря прозореца **Помощни инструменти**. В този прозорец можете да събирате техническа информация за работата на приложението и да създавате отчет за състоянието на системата.

Прозорец Изчисти хранилище

Резервни копия, създадени по-рано от

Функция, която премахва от хранилището резервните копия на файлове, създадени преди датата, посочена в полето до квадратчето за отметка.

Предишни версии на резервни копия

Ако е поставена отметка в това квадратче, старите версии на архивни копия се изтриват при почистване на хранилището за архивиране. Броят най-нови версии на резервни копия, които да се запазят, е посочен в полето **Брой версии на копия за запазване**.

Резервните копия на файлове, чиито оригинали са били изтрити

Това квадратче за отметка активира/деактивира функция, която премахва от хранилището резервните копия на файлове, които са били изтрити от компютъра.

Прозорец Изберете за възстановяване версия на резервно копие

Списък с версии на резервно копие

Съдържа информация за наличните версии на резервни копия на файла. Всеки елемент от списъка съдържа име на файл, номер на версия и дата на създаване на версията на резервното копие.

Като щракнете с десния бутон върху елемент от списъка, ще се отвори контекстуално меню със следните елементи:

- **Отвори** – версията на резервното копие на файла се отваря в прозореца на приложението, като съответства на файловия формат.
- **Възстановяване на версия на резервно копие** – отваря се прозорецът **Изберете къде да бъдат поставени възстановените файлове**. В този прозорец може да изберете папка, в която да бъдат поставени възстановените файлове.

Възстанови

Като щракнете върху този бутон, ще се отвори прозорец, в който може да промените настройките за възстановяване на файлове.

Изберете прозорец на папка

Поле за въвеждане на пътя към папката

Полето съдържа пътя към папката, в която трябва да бъдат възстановени файловете. Може да изберете папка от дървовидната структура над полето за въвеждане или да посочите пътя към папката ръчно.

Прозорец на Възстановяване на файлове

Спри

При щракването върху този бутон приложението Kaspersky спира да възстановява файлове от резервни копия.

Прозорец Възстановеният файл вече е наличен

Смени файл с резервното копие

Приложението Kaspersky изтрива съществуващия файл и го заменя с файла, възстановен от резервното копие.

Не възстановявай този файл

Приложението Kaspersky оставя съществуващия файл непроменен и не възстановява файла със същото име от резервното копие.

Запази и двата файла

Приложението Kaspersky оставя съществуващия файл непроменен и записва файла, възстановен от резервното копие, с ново име в същата папка.

Приложи това действие при всички подобни случаи

Ако е поставена отметка в това квадратче, Приложението Kaspersky прилага избраното действие към всички файлове, които възстановява.

Прозорец на Възстановяване на файлове

Спри

При щракването върху този бутон приложението Kaspersky спира да възстановява файлове от резервни копия.

Прозорец Настройки на хранилище

Име на хранилище

Полето съдържа името на хранилище за архивиране.

Прозорец на Kaspersky Restore Utility

Задача за архивиране

Този падащ списък ви позволява да избирате данните за възстановяване.

Архив дата/час

Този падащ списък ви позволява да избирате датата и часа, в които файловете за възстановяване са били архивирани. Избраните файлове ще бъдат възстановени в състоянието, в което са били към тази дата и час.

Търси

Поле за търсене на резервно копие на файл по име на файл. Търсенето се извършва докато пишете символите.

Бутон  /

Този превключвател сменя изгледа на списъка с резервни копия на файлове: дървовидна структура на папка или списък с файлове, подредени по азбучен ред.

Списък с файлове

Списъкът включва резервни копия на файлове, които могат да бъдат възстановени.

В зависимост от позицията на превключвателя  прозорецът показва дървовидна структура на папката или всички резервни копия на файлове, подредени по азбучен ред.

Този списък показва информация за името на резервното копие на файла, местоположението на изходния файл, типа на файла, разширението на името на файла, размера на файла и броя резервни копия на този файла. Щракването върху връзката в колоната **Версия** отваря прозореца **Изберете за възстановяване версия на резервно копие**. Този прозорец ви позволява да избирате версията на резервно копие, от която да възстановите файла.

Ако е избрано квадратчето за отметка до името на резервно копие, приложението възстановява този файл.

Ако е отметката е премахната от квадратчето до името на резервно копие, приложението не възстановява този файл.

Като щракнете с десния бутон върху елемент от списъка, ще се отвори контекстуално меню със следните елементи:

- **Отвори файл** – файлът се отваря с приложението за управляване на файлове от този тип.
- **Възстанови последната версия на резервно копие** – отваря прозореца **Изберете къде да бъдат поставени възстановените файлове**, в който може да посочите целевата папка за възстановяване на файла от последната версия на неговото резервно копие.
- **Версии на резервни копия на файл** – отваря се прозорецът **Изберете за възстановяване версия на резервно копие**. Този прозорец ви позволява да избирате версията на резервно копие, от която да възстановите файла.

Версия

Щракването върху тази връзка отваря прозореца **Изберете за възстановяване версия на резервно копие**, който ви позволява да видите всички версии на избрания файл, които могат да бъдат възстановени.

Изберете друго хранилище

Щракването върху тази връзка отваря прозореца за избор на резервно хранилище.

Възстановяване на избраните данни

Като щракнете върху този бутон, ще се отвори прозорец, в който може да промените настройките за възстановяване на файлове.

Използване на Родителски контрол

Родителски контрол позволява наблюдение на действията, извършвани от потребителите на локалния компютър и онлайн. Можете да използвате Родителски контрол, за да ограничите достъпа до интернет ресурси и приложения, както и да преглеждате отчети за дейностите на потребителите.

Все повече деца и тийнейджъри получават достъп до компютри и уеб ресурси. Използването на компютри и интернет представлява редица предизвикателства и заплахи за децата:

- Загуба на време и/или пари за посещение на чат стаи, ресурси за игри, онлайн магазини и търгове
- Достъп до уеб сайтове, насочени към по-възрастна аудитория, като например тези, включващи порнография, екстремизъм, огнестрелни оръжия, злоупотреба с наркотици и явно изразено насилие
- Изтегляне на файлове, заразени със злонамерен софтуер
- Увреждане на здравето, причинено от прекомерна употреба на компютъра
- Контакти с непознати, които може да се преструват, че са връстници, за да получат информация от непълнолетни потребители, като истинско име, физически адрес или време на деня, когато никой не е вкъщи

Родителски контрол ви позволява да намалите рисковете, породени от използването на компютър и интернет. За да направите това, са налични следните функции:

- Ограничаване на времето за използване на компютър и интернет
- Създаване на списъци с разрешени и блокирани игри и приложения, както и временно ограничаване на използването на разрешени приложения
- Създаване на списъци с разрешени и блокирани уеб сайтове и избирателно блокиране на категории уеб сайтове с неподходящо съдържание
- Активиране на режим на безопасно търсене в търсачките (връзките към уеб сайтове със съмнително съдържание не се показват в резултатите от търсенето)
- Ограничаване на изтеглянето на файлове от интернет
- Блокиране на изпращането на определени лични данни

Можете да конфигурирате функции на Родителски контрол за всеки потребителски акаунт на компютър поотделно. Ако потребител използва два акаунта, например локален акаунт на операционната система и потребителски акаунт на Microsoft, настройките на Родителски контрол трябва да бъдат конфигурирани за потребителския акаунт на Microsoft.

Можете също да видите отчети от Родителски контрол за дейностите на наблюдаваните потребители.

При промяна на часовата зона или при преминаване към и от лятно часово време, следните правила важат за използване на компютъра и интернета, както и за стартиране на игри и приложения:

- Ако датата не се промени при промяна на часовата зона, текущото обратно броене до блокирането продължава без промени. Същото правило важи и при преминаване към или от лятно часово време.
- Ако датата се увеличи или намали при промяна на часовата зона, времето, прекарано от потребителя, се нулира и обратното броене до блокирането започва отново.

Пристъпваме към настройките на Родителски контрол

За да отидете на настройките на Родителски контрол:

1. Отворете основния прозорец на приложението.
2. Отидете в раздела **Защита**.
3. В блока **Родителски контрол** щракнете върху бутона **Включи**.
4. Ако достъпът до настройките на Родителски контрол не е защитен с парола, приложението подканва потребителя да зададе парола. Изберете една от следните опции:

   - За да защитите достъпа до настройките на Родителски контрол с парола:

     a. Попълнете полетата **Парола** и **Потвърждение на паролата** и щракнете върху **Продължи**.

     b. В прозореца **Обхват на паролата** щракнете върху бутона **Създай парола**.

     c. В прозореца **Въвеждане на парола** потвърдете паролата и щракнете върху бутона **Влизане**.

   - Ако не искате да защитите с парола достъпа до настройките за родителски контрол, щракнете върху връзката **Пропусни**, за да продължите към настройките на Родителски контрол.

   Отворя се прозорецът **Родителски контрол**.

5. Изберете потребителски акаунт и щракнете върху връзката **Конфигуриране на ограничения**, за да отворите прозореца с настройки на Родителски контрол.

Контролиране на използването на компютъра

Родителски контрол ви позволява да ограничите времето, прекарано от потребителя на компютъра. Можете да посочите интервал от време, през който Родителски контрол трябва да блокира достъпа до компютъра (време за лягане), както и дневно ограничение за общото използване на компютъра. Можете да посочите различни лимити за делничните дни и за уикендите.

За да конфигурирате времеви ограничения за използване на компютър:

1. Отидете в прозореца с настройките на Родителски контрол.
2. В прозореца с настройки на Родителски контрол изберете раздела **Компютър**.
3. За да посочите интервал от време, през който Родителски контрол ще блокира достъпа до компютъра, в разделите **Делнични дни** и **Уикенди** поставете отметка в квадратчето **Блокиране на достъпа от N до N**.
4. В падащия списък до квадратчето за отметка **Блокиране на достъпа от N** посочете началния час на блока.
5. В падащия списък **до N** посочете времето за край на блока.

   Родителски контрол блокира достъпа на потребителя до компютъра през определения интервал от време.
6. Можете също да настроите график за използване на компютъра с помощта на таблица. За да видите таблицата, щракнете върху бутона  .

   Родителски контрол блокира достъпа на потребителя до компютъра **по график**, посочен в таблицата.
7. За да зададете времево ограничение за общото използване на компютъра през деня, в разделите **Делнични дни** и **Уикенди** поставете отметка в квадратчето **Разрешаване на достъп за не повече от N часа на ден** и от падащия списък до квадратчето изберете интервал от време.

   Родителски контрол блокира достъпа на потребителя до компютъра, когато общото използване на компютъра през деня надвишава определеното време.
8. За да настроите прекъсвания в потребителските сесии при използване на компютър, в раздела **Time breaks** поставете отметка в квадратчето **Take a break <time> за <duration>** и след това от падащите списъци до квадратчето изберете стойности за честотата на почивките (например всеки час) и тяхната продължителност (например 10 минути).
9. Преместете превключвателя в горната част на прозореца на **Контролът е включен**  .

Родителски контрол блокира достъпа на потребителя до компютъра в съответствие с посочените настройки.

Контролиране на използването на интернет

С помощта на Родителски контрол можете да ограничите времето, прекарано в интернет, и да забраните на потребителите да имат достъп до определени категории уеб сайтове или определени уеб сайтове. Можете също да забраните на потребителя да изтегля файлове от определени типове (като архиви или видеоклипове) от Интернет.

Как да ограничим времето за използване на интернет

За да ограничите времето за използване на интернет:

1. Отидете в прозореца с настройките на Родителски контрол.
2. В прозореца с настройките на Родителски контрол изберете раздела **Интернет**.
3. Ако искате да ограничите общото време за използване на интернет през делничните дни, в раздела **Ограничение на достъпа до интернет** поставете отметка в квадратчето **Ограничете достъпа през делничните дни до N часа на ден** и след това от падащия списък до квадратчето изберете стойност за срока.
4. Ако искате да ограничите общото време за използване на интернет през уикендите, поставете отметка в квадратчето **Ограничете достъпа през уикендите до N часа на ден** и след това от падащия списък до квадратчето за отметка изберете стойност за срока.
5. Преместете превключвателя в горната част на прозореца на **Контролът е включен** .

   Родителски контрол ще ограничи общото време, прекарано в интернет от потребителя, в съответствие със стойностите, които сте посочили.

Как да ограничите посещенията на конкретни уеб сайтове

За да ограничите посещенията на конкретни уеб сайтове:

1. Отидете в прозореца с настройките на Родителски контрол.

2. В прозореца с настройките на Родителски контрол изберете раздела **Интернет**.

3. За да предотвратите показването на съдържание за възрастни в резултатите от търсенето, в раздела **Control web browsing** поставете отметка в квадратчето **Enable Safe Search in search engines**.

   Когато търсите информация в уеб сайтове като Google™, YouTube™ (само за потребители, които не са влезли в уеб сайта youtube.com със своя акаунт) Bing®, Yahoo!™ и Yandex, в резултатите от търсенето няма да се показва съдържание за възрастни.

4. За да блокирате достъпа до уеб сайтове от определени категории:

   a. В раздела **Контрол на сърфирането в мрежата** поставете отметка в квадратчето **Контролирайте достъпа до уеб сайтове**.

   b. Изберете опцията **Блокирай достъпа до уеб сайтове от избрани категории** и щракнете върху връзката **Избиране на категории уеб сайтове**, за да отворите прозореца **Блокирай достъпа до категориите уеб сайтове**.

   c. Поставете отметка в квадратчетата до категориите уеб сайтове, които искате да блокирате.

      Родителски контрол ще блокира всички опити на потребителя да отвори уеб сайт, ако съдържанието му е класифицирано като принадлежащо към някоя от блокираните категории.

5. За да блокирате достъпа до конкретни уеб сайтове:

   a. В раздела **Контрол на сърфирането в мрежата** поставете отметка в квадратчето **Контролирайте достъпа до уеб сайтове**.

   b. Щракнете върху връзката **Управление на изключения**, за да отворите прозореца **Изключения**.

   c. В долната част на прозореца щракнете върху бутона **Добави**.

      Отваря се прозорец за добавяне на нова маска за уеб адрес.

   d. Въведете адреса на уеб сайт, на който искате да забраните посещенията, като попълните полето **Маска за уеб адрес**.

   e. В раздела **Обхват** дефинирайте обхвата на това, което искате да блокирате: целия уеб сайт или само определената уеб страница.

   f. Ако искате да блокирате посочения уеб сайт, в раздел **Действие** изберете **Блокирай**.

   g. Щракнете върху бутона **Добави**.

   Появява се посоченият уеб сайт в списъка в прозореца **Изключения**. Затвори прозореца **Изключения**.

6. Преместете превключвателя в горната част на прозореца на **Контролът е включен**.

Родителски контрол ще блокира опитите за отваряне на уеб сайтове в съответствие с посочените настройки.

Как да блокирате изтеглянето на определени типове файлове

За да забраните изтеглянето на определени типове файлове от интернет:

1. Отидете в прозореца с настройките на Родителски контрол.
2. В прозореца с настройките на Родителски контрол изберете раздела **Интернет**.
3. В раздела **Блокиране на изтеглянето на файлове** поставете отметка в квадратчетата до типовете файлове, за които искате да блокирате изтеглянията.
4. Преместете превключвателя в горната част на прозореца на **Контролът е включен**  .

Родителски контрол ще блокира изтеглянията на файлове от посочените типове от интернет.

Контролиране на стартиране на игри и приложения

С помощта на Родителски контрол можете да разрешите или забраните на потребителя да стартира игри в зависимост от възрастовата му категория. Можете също да забраните на потребителя да стартира определени приложения (като игри или IM клиенти) или да ограничите времето, позволено за използване на приложения.

Как да блокирате игри с неподходящо за възрастта съдържание

За да блокирате игри с неподходящо за възрастта съдържание:

1. Отидете в прозореца с настройките на Родителски контрол.
2. В прозореца с настройките на Родителски контрол изберете раздела **Приложения**.
3. Ако искате да блокирате всички игри със съдържание, което е неподходящо за възрастта на потребителя, поставете отметка в квадратчето до **Ограничете стартирането на игри за потребители под** и от падащия списък до квадратчето за отметка изберете опция за възрастово ограничение.
4. Ако искате да блокирате игри със съдържание от определена категория:
   a. Поставете отметка в квадратчето до **Блокиране на игри от категории за възрастни**.
   b. Щракнете върху връзката **Изберете категории игри**, за да отворите прозореца **Блокиране на игри по категории**.
   c. Поставете отметка в квадратчетата до категориите съдържание, съответстващи на игрите, които искате да блокирате.
5. Върнете се към раздела **Приложения**.
6. Ако искате да използвате рейтинговата система за блокиране на игри, изберете типа оценки и категоризация на съдържанието на игрите в падащия списък **Използвайте тази система за оценка, за да блокирате игри**:
   - **Открий автоматично** – Родителски контрол избира типа оценки на играта в зависимост от вашето местоположение: системата за класифициране на съдържанието на Pan European Game Information (PEGI) или системата за класификация за САЩ и Канада (ESRB).
   - **PEGI** – Родителски контрол използва европейската рейтингова система, когато конфигурира разрешенията за стартиране на игри.
   - **ESRB** – Родителски контрол използва рейтинговата система за САЩ и Канада, когато конфигурира разрешенията за стартиране на игри.
7. Преместете превключвателя в горната част на прозореца на **Контролът е включен**  .

Как да ограничите стартирането на конкретно приложение

За да ограничите стартирането на конкретно приложение:

1. Отидете в прозореца с настройките на Родителски контрол.
2. В прозореца с настройките на Родителски контрол изберете раздела **Приложения**.
3. Щракнете върху връзката **Конфигуриране**, за да отворите прозореца **Използване на приложението**.
4. Щракнете върху бутона **Add application**, за да отворите прозореца **Open** и изберете изпълнимия файл на приложението.

   Избраното приложение се появява в списъка **Използване на приложението**. Kaspersky автоматично добавя това приложение към определена категория, напр. *Games*.
5. Извършете следните действия:

   - За да блокирате стартирането на приложението, изберете елемента **Блокирай** от падащия списък до името на приложението.
   - За да блокирате всички приложения, които принадлежат към определена категория, поставете отметка в квадратчето до името на тази категория в списъка (например можете да блокирате приложения от категория *Игри*).
   - За да разрешите стартирането на приложението, изберете елемента **Разреши** от падащия списък до името на приложението.
   - За да зададете ограничения за продължителността на използване на приложението, изберете елемент **Ограничи** от падащия списък до името на приложението.

     Отваря се прозорецът **Ограничение за използване на приложението**.

     Извършете следните действия:

     a. Ако искате да зададете времево ограничение за използване на приложение през делничните и почивните дни, в разделите **Делнични дни** и **Уикенди** поставете отметка в квадратчето **Разрешаване на достъп за не повече от <N> часа на ден** и в падащия списък посочете броя часове, през които на потребителя е разрешено да използва приложението всеки ден. Можете също така да посочите времето, когато на потребителя е разрешено/забранено да използва приложението, като използвате таблицата **Точно време на използване**.

     b. Ако искате да зададете периоди, когато приложението е на пауза, в раздела **Почивки** поставете отметка в квадратчето **Направи почивка <време> за <интервал>** и от падащите списъци изберете стойности за това колко често и колко дълъг трябва да бъде интервалът.

     c. Щракнете върху бутона **Запази**.
6. Затвори прозореца **Използване на приложението**.
7. Преместете превключвателя в горната част на прозореца на **Контролът е включен**.

   Родителски контрол ще приложи посочените ограничения, когато потребителят получи достъп до приложението.

Наблюдение на съдържанието на съобщенията

С помощта на родителски контрол можете да наблюдавате и забранявате опитите на потребителя да вмъкне определени лични данни (като имена, телефонни номера, номера на банкови карти) в съобщения.

Как да конфигурирате контрола на трансфера на лични данни

За да конфигурирате контрола на трансфера на лични данни:

1. Отидете в прозореца с настройките на Родителски контрол.
2. В прозореца с настройки на Родителски контрол изберете раздела **Контрол на съдържанието**.
3. В раздела **Контрол на трансфера на лични данни** поставете отметка в квадратчето **Блокирай прехвърлянето на лични данни към трети страни**.
4. Щракнете върху връзката **Редактиране на списъка с лични данни**, за да отворите прозореца **Списък с лични данни**.
5. В долната част на прозореца щракнете върху бутона **Добави**.

   Отваря се прозорец за добавяне на лични данни.
6. Изберете тип лични данни (например „телефонен номер“), като щракнете върху съответната връзка или въведете описание в полето **Име на полето**.
7. Посочете лични данни (като вашето фамилно име или телефонен номер) в полето **Стойност**.
8. Щракнете върху бутона **Добави**.

   Личните данни са изброени в прозореца **Списък с лични данни**.
9. Затвори прозореца **Списък с лични данни**.
10. Преместете превключвателя в горната част на прозореца на **Контролът е включен**.

Родителски контрол наблюдава и блокира опитите на потребителя да използва посочените лични данни в съобщения през Интернет.

Преглед на отчета за активността на потребителя

Можете да получите достъп до отчети за активността на всеки потребителски акаунт, който се контролира от Родителски контрол, с отделни отчети за всяка категория контролирани събития.

За да видите отчет за активността на контролиран потребителски акаунт:

1. Отидете в прозореца с настройките на Родителски контрол.
2. Изберете потребителски акаунт и щракнете върху връзката **Преглед на отчета**, за да отидете на прозореца за отчети.
3. В раздела със съответния тип ограничение (напр. **интернет**), отворете отчета за наблюдаваните действия, като щракнете върху връзката **Детайли**.

Прозорецът показва отчет за наблюдаваните действия на потребителя.

Прозорец на категориите уеб сайтове

Интернет банки и системи за плащане

Ако е избрано това квадратче за отметка, приложението показва предупреждение когато създавате или въвеждате парола в интернет, която сте използвали преди това на уеб сайтове на банки и системи за плащане.

Социални мрежи

Ако е избрано това квадратче за отметка, приложението показва предупреждение когато създавате или въвеждате парола в интернет, която сте използвали преди това в социални мрежи.

Пощенски услуги

Ако е избрано това квадратче за отметка, приложението показва предупреждение когато създавате или въвеждате парола в интернет, която сте използвали преди това на уеб сайтове на пощенски услуги.

Помогнете ни да станем по-добри! Оставете отзив

Наборът параметри в този прозорец зависи от оценката, която сте дали на компонента. Параметърът на Категория на проблема е наличен, ако сте дали оценка на компонента от 1 до 2.

Тема

Падащ списък, в който може да изберете категория за вашата обратна връзка. Категорията за обратна връзка може да адресира проблем с компонента Умно домашно наблюдение.

- **Неудобно за използване**. Изберете този елемент, ако изпитвате неудобства при използване на компонента Умно домашно наблюдение.
- **Приложението отнема много време за търсене на устройства в мрежата**. Изберете този елемент, ако компонентът Умно домашно наблюдение работи твърде бавно.
- **Приложението неправилно идентифицира устройства в мрежата**. Изберете този елемент, ако приложението неправилно определя имената и/или типовете на устройствата, свързани към мрежата.
- **Твърде много известия за нови устройства в мрежата**. Изберете този елемент, ако приложението показва твърде много известия за нови устройства в мрежата.
- **Намалена производителност на компютъра**. Изберете този елемент, ако използването на компонента Умно домашно наблюдение забавя производителността на Вашия компютър.
- **Невъзможно е да се конфигурира компонентът**. Изберете този елемент, ако изпитвате затруднения при конфигуриране на компонента Умно домашно наблюдение.
- **Друго**. Изберете този елемент, ако проблемът, който изпитвате, не се покрива от други елементи.

Детайли

Може да използвате това поле, за да предоставите информация, която може да помогне на Kaspersky да разреши вашия проблем. Това поле е опционално.

Изпрати

Изпращане на обратна връзка до Kaspersky

Може да изпращате обратна връзка за компонента Умно домашно наблюдение до 10 пъти на ден. Ако приложението не успее да изпрати вашата обратна връзка (например интернет връзката не е налична), тя ще бъде записана на вашия компютър. Обратната връзка се съхранява открито за 30 дни.

За Лицензионното споразумение

Лицензионното споразумение е обвързващо споразумение между вас и АО Kaspersky Lab, което определя условията, при които може да използвате приложението.

Прочетете внимателно условията на лицензионното споразумение, преди да започнете използването на приложението.

Вие приемате условията на Лицензионното споразумение, като потвърждавате, че го приемате, когато инсталирате приложението. Ако не приемате условията на Лицензионното споразумение, трябва да прекратите инсталирането на приложението и не трябва да го използвате.

Относно режима с ограничена функционалност

Таблицата по-долу показва кои функции на приложението Kaspersky са налични и кои не са налични, когато приложението е в режим на ограничена функционалност. Ако стойността в колоната „Режим с ограничена функционалност“ е „да“, това означава, че съответната функционалност е достъпна в режим с ограничена функционалност. Ако стойността в колоната на режима с ограничена функционалност е „не“, съответната функционалност не е налична. Допълнителна информация е налична в колоната „Ограничения“.

Функции на приложението Kaspersky в режим на ограничена функционалност

Функционалност	Ограничения	Режим с ограничена функционалност
Сканиране за вируси		да
Актуализиране на антивирусните бази данни и модулите за приложения	Налични са само критични актуализации.	не
Сканиране за уязвимости в приложения		да
Безопасно сърфиране		да на Windows 7, 8 / не на Windows 10, 11
Защита на файлове		да на Windows 7, 8 / не на Windows 10, 11
Защита за пощата		да на Windows 7, 8 / не на Windows 10, 11
Системно наблюдение		да на Windows 7, 8 / не на Windows 10, 11
Проверка на репутацията на файлове в Kaspersky Security Network		не
Защитено въвеждане на данни		не
Спешно възстановяване	Дискът за възстановяване на Kaspersky може да бъде изтеглен в интерфейса на приложението.	да
Заплахи и изключения		да
Мрежови настройки		да
Отчети и карантина		да
Настройки за показване на приложението		да
Играл ен режим		не
Режим "Не безпокой"		не
Предотвратяване на проникване		да на Windows 7, 8 / не на Windows 10, 11

Защитна стена		да
Защита от мрежови атаки		да
Защита от спам		да
Защита от банери		да
Безопасно плащане		не
Поверително сърфиране		да
Почистване на следите от активността		не
Умно домашно наблюдение		не
Управление на уеб камера и микрофон		да на Windows 7, 8 / не на Windows 10, 11
Наблюдение на мрежата		да
Диспечер на приложения		не
Мениджър на пароли		да
Унищожител за файлове		да
Тайно хранилище	Наличен е само достъп до данни в предварително създадени тайни хранилища.	не
Архивиране и възстановяване	Възможно е само възстановяване на данни от предварително създадени резервни копия.	не
Актуализация на приложения		не
PC Cleaner		не
Ускоряване на компютъра		не
Kaspersky VPN		да
Проверка на изтичане на данни		не
Отстраняване на неизправности на Microsoft Windows		да
Бързо стартиране		не
Сканиране за слаби настройки		не
Дубликати		не
Големи файлове		не
Неизползвани приложения		не
Монитор за изправността на твърдия диск		не
Текуща дейност		не
Пестене на батерията		не
Откриване на преследвачески софтуер		не
Блокиране на нежелано инсталиране на приложение		не

Програма за премахване на рекламен софтуер		не
AMSI защита		да, само на Windows 10, 11
Управление на настройките		да
Защита с парола на настройките на приложението		да
Настройки за използване на ресурси от компютъра		да
Хронология		да
Препоръки		да
Родителски контрол	Само прегледът на отчети е достъпен.	не
Свързване с екипа за техническа поддръжка		да

За фишинг

Фишинг е вид интернет измама, включваща кражба на лични данни; фишинг се разпространява по имейл и други канали.

Имейлите могат да бъдат фалшиви уведомления от банки, ISP, онлайн магазини, електронни платежни системи или други субекти. Имейлите се опитват да подмамят получателя да посети уебсайта на измамниците под фалшиви доводи, като покана за актуализиране на информацията за вход или за да научите повече за продукт или услуга.

Неподозиращите получатели на фишинг имейл може да последват връзката и да се озоват на фишинг уеб сайт, който изглежда точно като уебсайта на компанията, за която се представя.

Интернет потребителите могат да стигнат до фишинг сайт по други начини, например, като кликнат върху връзка в търсачка.

Като цяло измамниците могат да преследват различни цели. Една от тези цели е да подмамят потребителите да разкрият своите поверителни данни, като влизане, пароли за акаунти или крипто портфейли и други регистрационни данни, номера на банкови сметки и данни за банкови карти. Потребителите въвеждат тази информация в уеб формуляр на измамния уебсайт, което дава на измамниците достъп до парите им. Заразяването на компютрите с вируси и зловреден софтуер е друг капан, в който потребителят може да попадне, след като кликне върху фишинг връзка.

Разпознаване на фалшиви имейли и уебсайтове

Измамните (фишинг) имейли и уебсайтове могат да изглеждат подозрително на пръв поглед. Включването на фирмени лога, които приличат на автентичните, или на действителни телефонни номера за връзка може да заблуди потребителите с фалшиво чувство за сигурност. Имейлът може да съдържа и връзки към действителния уебсайт на компанията, с изключение на основната фишинг връзка, която ще отведе потребителя до уебсайта на престъпниците.

Следните сигнални знаци за фишинг могат да алармират потребителя:

- Въпреки че домейните на фишинг уебсайтовете могат да изглеждат като действителни легитимни уебдомейни на компании, при по-внимателно разглеждане потребителят може да забележи допълнителни думи в името на домейна (например официалният домейн на дадена компания www.example.com може да бъде променен на www.login-example.com) или точки и тирета, заместващи наклонените черти (www.example.com/personal/login може да бъде променен на www.example.com.personal.login или www.example.com-personal.login). Обърнете внимание, че основният текст на имейла може да съдържа действителния адрес на домейна на компанията, но когато потребителят кликне върху връзката, адресната лента на браузъра ще покаже друг домейн.

- В имейла се използва безлична форма на обръщение, например "Уважаеми потребители" или "Здравейте".

- Графиките в имейла или на уебсайта изглеждат непрофесионално, текстът съдържа печатни грешки или неправилна граматика.

- От получателя на имейла се иска незабавно да потвърди поверителните си данни, като последва връзка или понякога да въведе данните си във формуляр в имейла Имейлът може да обяснява тази спешност с предполагаемо спиране на акаунта, хакерска атака или заплаха от загуба на данните.

Проверка на фишинг

Приложението Kaspersky проверява съдържанието на имейли и уебсайтове за фишинг връзки. Връзките се проверяват в база данни с фишинг уеб адреси и борси за фалшиви криптовалути, която се актуализира редовно.

За допълнителна защита Kaspersky използва евристичен анализ и по време на проверката изпраща запитвания към облачните услуги на Kaspersky Security Network (KSN). Kaspersky Security Network съдържа най-актуалната информация за наскоро появили се заплахи, включително фишинг уебсайтове, които все още не са добавени в базите данни на Kaspersky. Данните, получени от KSN, се анализират от служители на Virus Lab в реално време.

Ако сте кликнали върху фишинг уебсайт, можете да съобщите за това на Kaspersky Security Network, като използвате разширението Kaspersky Protection.

Профил

Свързване на устройство с My Kaspersky

Нуждаете се от акаунт My Kaspersky, за да управлявате абонамента, да активирате абонамента на различни устройства и да управлявате дистанционно защитата на тези устройства. Вашият акаунт My Kaspersky ви позволява да видите състоянието на всички свързани към акаунта устройства, на които е инсталирано приложението; можете също така да управлявате абонаменти и да съхранявате кодове за активиране на сигурно място.

Влизане

Натискането на този бутон отваря прозорец за свързване на устройството с вашия акаунт My Kaspersky. Бутонът е достъпен, ако не сте свързали устройството към акаунта си в My Kaspersky или ако не сте потвърдили, че устройството е ваше.

В зависимост от вашия абонамент, някои функции на приложението може да не са достъпни, без да сте свързали устройството към вашия акаунт в My Kaspersky.

Управление на акаунт

Щракването върху бутона ви препраща към вашия акаунт в уебсайта на Kaspersky в браузъра по подразбиране. Бутонът става достъпен, след като влезете в акаунта на това устройство.

Бутон

Натискането на този бутон изключва устройството от акаунта ви в My Kaspersky. Бутонът е наличен, ако устройството е свързано към вашия акаунт в My Kaspersky.

В зависимост от абонамента ви може да се наложи свързване на устройството с акаунта ви в My Kaspersky. В този случай, след като прекъснете връзката на устройството от вашия акаунт, няма да можете да използвате приложението.

Повече за акаунта в My Kaspersky

Информация за абонамент

Тук можете да намерите обща информация за абонамента, използван от вашето приложение. Можете да видите състоянието на абонамента, броя на оставащите дни до изтичането на платения период, състоянието на автоматичното подновяване и името на собственика на абонамента, ако не сте собственикът.

Детайли

С натискането на този бутон се отваря прозорецът **Детайли за абонамента** с подробна информация за вашия абонамент. Тук можете да намерите следната информация:

- Състояние на абонамент
- Състояние на автоматично подновяване
- Лицензионен ключ, който може да ви е необходим, за да се свържете с техническата поддръжка
- Връзка към Лицензионното споразумение с краен потребител
- Връзка към изявлението в уеб портала
- Общ брой устройства, които можете да защитите с вашия абонамент
- Брой устройства, които в момента защитавате с вашия абонамент
- Дата на активиране
- Дата на изтичане на платения период

За да разкриете други действия, които можете да извършвате с абонамента си, щракнете върху ⋯. Списъкът с наличните действия може да се различава в зависимост от абонамента и неговия статус.

Актуализиране на статуса

Щракването върху този бутон ви предоставя актуална информация за състоянието на вашия абонамент.

Въведете код за активиране

Щракването върху този бутон отваря прозореца, в който можете да въведете кода за активиране. В зависимост от абонамента ви този бутон може да не е наличен.

За повече подробности относно кодовете за активиране вижте раздели Ако сте закупили версия на приложението в магазин или карта за активиране и Подновяване на абонамента с помощта на резервен код за активиране.

Изберете друг абонамент

Щракването върху този бутон отваря прозорец със списък с абонаменти, налични във вашия акаунт My Kaspersky, които са съвместими с вашето приложение.

Бутонът е наличен, ако устройството е свързано към вашия акаунт в My Kaspersky.

Управление на абонамент

Натискането на този бутон отваря вашия акаунт My Kaspersky и ви отвежда до страницата за управление на абонамента. Бутонът е наличен, ако устройството е свързано към вашия акаунт в My Kaspersky.

Подновете сега / Купете сега

В зависимост от състоянието на вашия абонамент, можете да подновите текущия си абонамент или да закупите нов абонамент.

Бутонът е наличен, ако вашият абонамент е изтекъл, не сте активирали автоматичното подновяване и не сте добавили резервен код за активиране към приложението.

Възобнови

Бутонът е наличен, ако сте анулирали абонамента си. За определен период от време, след като анулирате абонамента си, ще можете да го възобновите.

Възобновяването на текущия абонамент може да не е налично във вашия регион.

Допълнителна информация за управлението на Вашия абонамент

Защитете още устройства

Тук можете да видите колко устройства можете да защитите с абонамента си, колко устройства защитавате в момента; можете също така да започнете да защитавате нови устройства. Ако сте свързали устройство към акаунта си в My Kaspersky, информацията се опреснява, когато стартирате приложението.

Броят на устройствата, на които можете да използвате абонамента си, зависи от абонаментния план и от условията, посочени в лицензионното споразумение с крайния потребител.

Бутон +

Щракването върху бутона отваря прозореца **Защитете още устройства**, в който можете да изберете предпочитания от вас метод за изпращане на абонамента до устройството.

Бутонът е наличен, ако абонаментът ви позволява да защитите повече от едно устройство.

В зависимост от абонамента ви този бутон може да не се показва.

Щракването върху бутона ••• ви позволява да изберете едно от следните действия:

Защитаване на устройство

Щракването върху бутона отваря прозореца **Защитете още устройства**, в който можете да изберете предпочитания от вас метод за изпращане на абонамента до друго устройство.

Бутонът е наличен, ако абонаментът ви позволява да защитите повече от едно устройство.

Управление на устройства

Натискането на този бутон отваря вашия акаунт My Kaspersky и ви отвежда до страницата за управление на абонамента в раздел **Моите устройства**. Тук можете да видите всички устройства, които използват вашия абонамент и да следите състоянието на тези устройства.

Ако все още не сте свързали устройство към акаунта си в My Kaspersky, ще се отвори прозорец, който ви позволява да свържете устройства към акаунта си.

За да научите повече за дистанционното управление на устройствата, вижте Помощ за моя Kaspersky.

В зависимост от вашия абонамент може да се покаже само общата информация за общия брой устройства, които можете да защитите.

Допълнителна информация за защитата на други устройства с Вашия абонамент

Решения за вас

На тази страница ще предлагаме решения на Kaspersky и решения, предоставени от нашите партньори, които може да ви се сторят интересни. Тук ще можете да закупите решение, което е съобразено с вашите нужди, да разглеждате вече закупени приложения и услуги, да следите състоянието на абонамента си, да продължите с инсталирането на приложение или да прочетете ръководство с инструкции.

Щракването върху **Купуване** ви отвежда до онлайн магазина, където можете да научите повече за избраното от вас решение и да проверите покупката си. Ще получите имейл с информация за вашата покупка и инструкции за активиране.

Можете да управлявате закупените от вас абонаменти във вашия акаунт в My Kaspersky.