ESET Internet Security

Ръководство за потребителя

Щракнете тук за да се покаже версията за онлайн на този документ

Digital Security
Progress. Protected.

ESET Internet Security е разработка на ESET, spol. s r.o.

За повече информация посетете https://www.eset.com.

Техническа поддръжка: https://support.eset.com

REV. 2024-4-12

ESET Internet Security

ESET Internet Security представлява нов подход към напълно интегрирана защита на компютъра. Най-новата версия на системата за сканиране ESET LiveGrid®, в комбинация с нашите персонализирани модули за защитна стена и антиспам, използва скорост и прецизност, за да поддържа компютъра ви в безопасност. Резултатът е интелигентна система, която постоянно следи за атаки и злонамерен софтуер, които може да заплашват компютъра.

ESET Internet Security е пълно решение за защита, което комбинира максимална защита и минимално натоварване на системата. Нашите модерни технологии използват изкуствен интелект за предотвратяване на проникване от вируси, шпионски софтуер, троянски коне, червеи, рекламен софтуер, руткитове и други заплахи, без да влошават производителността или да нарушават работата на компютъра.

Функции и ползи

Нов потребителски интерфейс	Потребителският интерфейс в тази версия е значително променен и опростен въз основа на резултати от тестването на използваемостта. Всички фрази и известия в графичния потребителски интерфейс бяха внимателно ревизирани и интерфейсът вече предоставя поддръжка за езици с писане от дясно наляво, като например иврит и арабски. Онлайн помощта вече е интегрирана в ESET Internet Security и предлага динамично обновявано съдържание за поддръжка.
Тъмен режим	Разширение, което ви помага бързо да превключите екрана на тъмна тема. Можете да изберете предпочитаната от вас цветова схема в Елементи на потребителския интерфейс.
Защитата от вируси и шпионски софтуер	Съвременен начин за откриване и почистване на повечето известни и неизвестни вируси, червеи, троянски коне и комплекти за пълен достъп. Разширени евристични методи обозначават дори непознат до момента злонамерен софтуер, като така ви защитават от непознати заплахи и ги неутрализират, преди да са навредили. Защита на уеб достъпа и Анти-фишинг работи, като проследява комуникацията между уеб браузъри и отдалечени сървъри (включително SSL). „Защита на имейл клиенти“ предоставя контрол на имейл съобщенията, получени чрез POP3(S) и IMAP(S) протоколи.
Редовно обновяване	Редовното обновяване на системата за откриване (по-рано известна като "база данни със сигнатури за вируси") и модулите на програмата е най-добрият начин да осигурите максимално ниво на защита на вашия компютър.
ESET LiveGrid® (Репутация в облака)	Вие можете да проверявате репутацията на изпълняваните процеси и файлове директно от ESET Internet Security.
Управление на устройства	Автоматично сканира всички USB флаш устройства, карти с памет и CD/DVD дискове. Блокира преносими носители въз основа на типа носител, производителя, размера и други атрибути.
HIPS функционалност	Може да персонализирате по-подробно поведението на системата; да задавате правила за системния регистър, активните процеси и програми и да настройвате прецизно позицията на защитата.
Режим за геймъри	Отлага всички изскачащи прозорци, обновявания или други дейности, използващи системата интензивно, за да се запазят системните ресурси за игри и други дейности на цял екран.

Функции на ESET Internet Security

Безопасно банкиране и сърфиране	Безопасното банкиране и сърфиране осигурява защитен браузър, който можете да използвате, когато осъществявате достъп до шлюзове за онлайн банкиране или онлайн плащания, за да сте сигурни, че всички онлайн трансакции протичат в доверена и защитена среда.
Поддръжка за мрежови сигнатури	Мрежовите сигнатури позволяват бързо идентифициране и блокиране на злонамерен трафик, насочен към или идващ от потребителски устройства, като например ботове и пакети за експлойти. Тази функция може да се смята за подобрение на защитата от ботнет мрежи.
Интелигентна защитна стена	Възпрепятства неупълномощените потребители да получат достъп до компютъра ви и да се възползват от личните ви данни.
Антиспам на имейл клиенти	Спамът представлява 50 процента от цялата комуникация по електронна поща. Антиспам на имейл клиенти предпазва от този проблем.
Anti-Theft	Anti-Theft разширява защитата на ниво потребител в случай на загубен или откраднат компютър. Ако инсталирате ESET Internet Security и Anti-Theft, устройството ви ще бъде изброено в уеб интерфейса. Уеб интерфейсът ви позволява да управлявате конфигурацията на Anti-Theft и да администрирате функциите на Anti-Theft на устройството си.
Родителски контрол	Защитава семейството ви от потенциално нецензурирано уеб съдържание, като блокира различни категории уеб сайтове.

Абонаментът трябва да бъде активен, за да могат функциите на ESET Internet Security да работят. Препоръчваме ви да подновите абонамента си няколко седмици преди изтичането на абонамента за ESET Internet Security.

Какво е новото?

Какво е новото в ESET Internet Security 17.1

- Малки подобрения в мрежовия инспектор
- Малки подобрения в безопасното банкиране и сърфиране
- Други незначителни поправки на грешки и подобрения

За да изключите **Известията за новостите**:
1. Отворете Разширена настройка > **Известия** > **Известия на работния плот**.
2. Щракнете върху **Редактиране** близо до **Известия на работния плот**.
3. Премахнете отметката от полето **Показване на известия за новостите** и щракнете върху **OK**.
За повече информация относно известията вижте раздела Известия.

За подробен списък на промените в ESET Internet Security вижте регистрите на промените за ESET Internet Security.

С кой продукт разполагам?

ESET предлага няколко слоя защита с нови продукти – от мощно и бързо антивирусно решение до решение за защита от тип всичко в едно – с минимално въздействие върху системата:

- **ESET NOD32 Antivirus**
- **ESET Internet Security**
- **ESET Smart Security Premium**
- **ESET Security Ultimate**

За да определите кой продукт сте инсталирали, отворете главния прозорец на системата и ще видите името на продукта в най-горната част на прозореца (вж. статията в базата знания).

Таблицата по-долу описва подробно функциите, налични във всеки конкретен продукт.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Система за засичане на потенциално опасни заплахи	✔	✔	✔	✔
Разширено машинно обучение	✔	✔	✔	✔
Блокиране на експлойти	✔	✔	✔	✔
Защита срещу атаки, базирани на скриптове	✔	✔	✔	✔
Анти-фишинг	✔	✔	✔	✔
Защита на уеб достъпа	✔	✔	✔	✔
HIPS (включително Щит срещу малуер, който криптира файловете и иска откуп за отключването им)	✔	✔	✔	✔
Антиспам		✔	✔	✔
Защитна стена		✔	✔	✔
Мрежов инспектор		✔	✔	✔
Защита на уеб камерата		✔	✔	✔
Защита от мрежови атаки		✔	✔	✔
Защита от ботнет мрежи		✔	✔	✔
Безопасно банкиране и сърфиране		✔	✔	✔
Поверителност и защита на браузъра		✔	✔	✔
Родителски контрол		✔	✔	✔
Anti-Theft		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
VPN				✔
Identity Protection				✔

Някои от продуктите по-горе може да не са налични за вашия език/регион.

Системни изисквания

Вашата система трябва да отговаря на следните хардуерни и софтуерни изисквания, за да може ESET Internet Security да функционира оптимално:

Поддържани процесори

Процесор на Intel или AMD, 32-битов (x86) с набор инструкции SSE2 или 64-битов (x64), 1 GHz или по-висока
ARM64 базиран процесор, 1 GHz или повече

Поддържани операционни системи

Microsoft® Windows® 11

Microsoft® Windows® 10

Поддръжката за подписване на код на Azure трябва да бъде инсталирана на всички операционни системи Windows, за да се инсталират или надстроят продуктите на ESET, пуснати след юли 2023 г. Повече информация.

Винаги поддържайте операционната си система в актуално състояние.

Изисквания към функциите на ESET Internet Security

Вижте системните изисквания за специфични функции на ESET Internet Security в таблицата по-долу:

Функция	Изисквания
Intel® Threat Detection Technology	Вижте поддържаните процесори.
Безопасно банкиране и сърфиране	Вижте поддържани уеб браузъри.
Прозрачен фон	Windows 10, версия RS4 и по-нова.
Специализирано приложение за почистване	Процесор, който не е базиран на ARM64.
Инструмент за почистване на системата	Процесор, който не е базиран на ARM64.
Блокиране на експлойти	Процесор, който не е базиран на ARM64.
Дълбока проверка на поведението	Процесор, който не е базиран на ARM64.

Други

Необходима е интернет връзка за правилното изпълнение на активацията и обновяванията на ESET Internet Security.

Две антивирусни програми, работещи едновременно на едно устройство, причиняват неизбежни конфликти на системните ресурси, като например забавяне на системата, което я прави неизползваема

Остаряла версия на Microsoft Windows

Проблем

- Искате да инсталирате най-новата версия на ESET Internet Security на компютър с Windows 7, Windows 8 (8.1) или Windows Home Server 2011
- ESET Internet Security показва грешка **Остаряла операционна система** по време на инсталирането

Подробни данни

Най-новата версия на ESET Internet Security изисква операционни системи Windows 10 или Windows 11.

Решение

Налични са следните решения:

Надстройка до Windows 10 или Windows 11

Процесът по надстройване е сравнително лесен и в много случаи може да преминете през него, без да губите файловете си. Преди да надстроите до Windows 10:

1. Архивиране на важни данни.
2. Прочетете ЧЗВ за надстройване до Windows 10 на Microsoft или ЧЗВ за надстройване до Windows 11 и обновете операционната си система Windows.

Инсталиране на ESET Internet Security версия 16.0

Ако не можете да надстроите Windows, инсталирайте ESET Internet Security версия 16.0. Вижте Онлайн помощ за ESET Internet Security версия 16.0 за повече информация.

Предотвратяване

Когато работите с компютъра си и особено когато сърфирате в интернет, не забравяйте, че няма антивирусна система в света, която напълно да елиминира риска от засичания и отдалечени атаки. За да осигурите максимална защита и удобство, е необходимо да

използвате правилно антивирусното си решение и да спазвате няколко полезни правила:

Обновявайте редовно

Според статистиката от ESET LiveGrid® всеки ден се създават хиляди нови и уникални проникванията, които имат за цел да заобиколят съществуващите мерки за защита и да облагодетелстват своите автори за сметка на другите потребители. Специалистите от лабораторията на ESET за проучвания анализират тези заплахи всеки ден и подготвят и издават обновявания, за да подобряват непрекъснато нивото на защитата на потребителите. За да гарантират максимална ефективност на обновяванията, е важно тези обновявания да са правилно конфигурирани в системата. За повече информация относно конфигуриране на обновяванията вж. главата Настройка за обновяване.

Изтегляйте корекции за защитата

Авторите на злонамерен код предпочитат да се възползват от различни слабости в системата, за да увеличат ефективността на разпространение на злонамерения код. Поради тази причина фирмите внимателно следят новите слаби места в приложенията си и ако се появят такива, редовно издават обновявания на защитата, за да елиминират потенциалните заплахи. Важно е тези обновявания на защитата да се изтеглят веднага щом излязат. Microsoft Windows и уеб браузърите, като например Internet Explorer, са два примера за програми, за които обновяванията на защитата се издават редовно.

Архивиране на важни данни

Авторите на злонамерен софтуер не се интересуват от нуждите на потребителите, а дейността на злонамерени програми често води до цялостна неизправност на операционната система и загуба на важни данни. Важно е редовно да архивирате важните и поверителните данни върху външен източник като DVD диск или външен твърд диск. Подобни мерки улесняват и ускоряват възстановяването на данните в случай на отказ на системата.

Сканирайте редовно компютъра за вируси

Откриването на други познати и непознати вируси, червеи, троянски коне и комплекти за пълен достъп се извършва от модула на защитата на файловата система в реално време. Това означава, че всеки път, когато използвате или отворите файл, той се сканира за наличие на злонамерен софтуер. Препоръчително е да изпълнявате пълно сканиране на компютъра поне веднъж месечно, тъй като злонамереният софтуер може да се изменя и системата за откриване се обновява всеки ден.

Изпълнявайте основните правила за защита

Това е най-полезното и ефективно правило от всички – бъдете винаги внимателни. Днес много проникванията изискват намеса на потребителя, за да бъдат изпълнени и разпространени. Ако сте внимателни при отварянето на нови файлове, ще си спестите време и усилия, които иначе биха ви стрували скъпо, ако се наложи да почиствате проникванията. Ето няколко полезни насоки:

- Не посещавайте подозрителни уеб сайтове с много изскачащи рекламни съобщения и реклами.

• Внимавайте при инсталирането на безплатни програми, кодеци и т.н. Използвайте само безопасни програми и посещавайте безопасни интернет уеб сайтове.

• Бъдете внимателни при отварянето на прикачени файлове от имейл, особено тези, изпратени в масови съобщения, и от неизвестни податели.

• Не използвайте административния акаунт за ежедневна работа на компютъра.

Помощни страници

Добре дошли в ръководството за потребители на ESET Internet Security. Предоставената тук информация ще ви представи продукта и ще ви помогне да направите компютъра си по-защитен.

Първи стъпки

Преди да използвате ESET Internet Security, може да прочетете за различни видове откриване и отдалечени атаки, които може да срещнете, когато използвате компютъра си. Ние също така съставихме списък с нови функции, въведени в ESET Internet Security.

Започнете с инсталирането на ESET Internet Security. Ако вече сте инсталирали ESET Internet Security, вижте Работа с ESET Internet Security.

Как се използват помощните страници на ESET Internet Security

Онлайн помощта е разделена на няколко глави и подглави. Натиснете **F1** в ESET Internet Security, за да видите информация за текущо отворения прозорец.

Онлайн помощта позволява да търсите тема за помощ по ключови думи или да търсите съдържание чрез въвеждане на думи или фрази. Разликата между двата метода е, че ключовата дума може логически да е свързана със страниците с помощ, но да не се съдържа в самия текст. Търсенето по думи и фрази се извършва в съдържанието на всички страници и се показват само резултатите, съдържащи търсената дума или фраза в самия текст.

С цел съгласуваност и за избягване на объркването терминологията, използвана в това ръководство, се базира на потребителския интерфейс на ESET Internet Security. Освен това използваме уеднаквен набор от символи за обозначаване на теми от особен интерес или значение.

Забележката е просто кратко наблюдение. Въпреки че можете и да ги пропускате, забележките могат да предоставят важна информация, като например специфична функция или връзка към сродна тема.

Това изисква вниманието ви и ви препоръчваме да не го прескачате. Обикновено предоставя важна информация, макар и не от критично значение.

Това е информация, която изисква допълнително внимание и предпазливост. Предупрежденията имат за цел да ви възпрат да извършите потенциално опасни грешки. Прочетете и вникнете добре в текста, тъй като той описва много важни системни настройки или нещо рисковано.

Това е пример за употреба или практически пример, който има за цел да ви помогне да разберете как да използвате дадена функция.

Правило	Значение
Получерен шрифт	Имена на елементите на интерфейса, като например полета или бутони за опции.
Курсивен шрифт	Контейнери за предоставяната от вас информация. Например име на файл или път означава, че трябва да въведете действителния път или име на файла.
`Courier New`	Извадки от код или команди.
Хипервръзка	Предоставя бърз и лесен достъп до свързани теми или външно уеб местоположение. Хипервръзките са обозначени в синьо и може да са подчертани.
%ProgramFiles%	Системната директория в Windows, в която се съхраняват инсталираните в Windows програми.

Онлайн помощта е основният източник на помощно съдържание. Най-новата версия на онлайн помощта автоматично ще се показва, когато имате работеща интернет връзка.

Инсталиране

Има няколко метода за инсталиране на ESET Internet Security във вашия компютър. Методите за инсталиране може да се различават в зависимост от държавата и начините на разпространение:

• Инсталатор – изтеглен от уеб сайта на ESET или на CD/DVD. Този инсталационен пакет е универсален за всички езици (изберете желания език). Самият инсталатор е малък файл; допълнителните файлове, необходими за инсталирането на ESET Internet Security, се изтеглят автоматично.

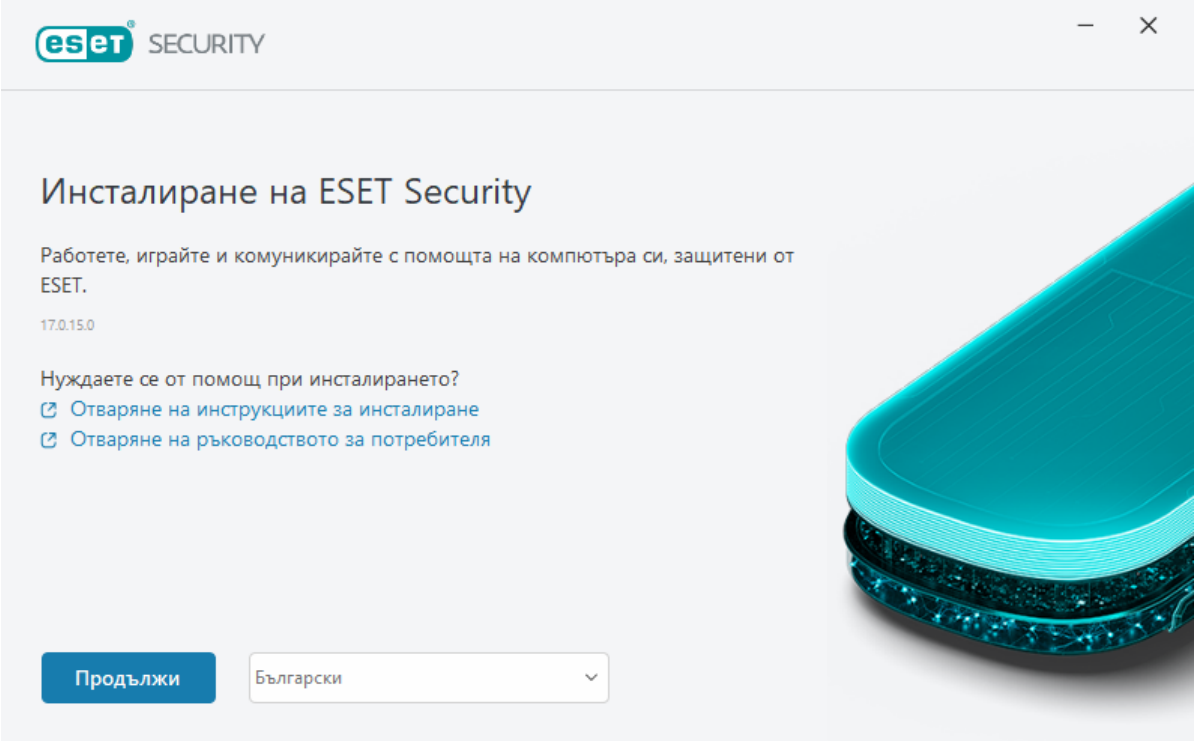
• Офлайн инсталиране – използва .exe файл, който е по-голям от файла на инсталатора и не изисква интернет връзка или допълнителни файлове за завършването на инсталацията.

Уверете се, че на компютъра не са инсталирани други антивирусни програми, преди да инсталирате ESET Internet Security. Ако две или повече антивирусни решения се инсталират на един и същ компютър, те могат да влязат в конфликт едно с друго. Препоръчваме ви да деинсталирате всички други антивирусни програми от компютъра. Вж. нашата статия в базата знания на ESET за списък с инструменти за деинсталиране за често срещаните антивирусни програми (достъпна на английски и няколко други езици).

Инсталираща програма в реално време (Live installer)

Когато сте изтеглили инсталационния пакет на инсталатора (Live installer),струкциите „стъпка по стъпка“ в съветника за инсталиране.

За този тип инсталиране трябва да сте свързани с интернет.



1. Изберете подходящия език от падащото меню и щракнете върху **Продължаване**.

Ако инсталирате по-нова версия върху предишната с настройки, защитени с парола, въведете паролата си. Можете да конфигурирате паролата за настройки в настройката на Access.

2. Изберете предпочитанията си за следните функции, прочетете Лицензионното споразумение за краен потребител и Правилата за поверителност и щракнете върху **Продължи** или щракнете върху **Разрешаване на всички и продължаване**, за да разрешите всички функции:

- Система за обратна връзка на ESET LiveGrid®
- Потенциално нежелани приложения
- Програма за подобряване на работата на клиентите

Като щракнете върху **Продължи** или **Разрешаване на всички и продължаване**, вие приемате Лицензионното споразумение с краен потребител и потвърждавате Правилата за поверителност.

3. За да активирате, управлявате и преглеждате защитата на устройството чрез ESET HOME, свържете устройството си с акаунта в ESET HOME. Щракнете върху **Пропускане на влизането,** за да продължите, без да се свързвате с ESET HOME. Можете да свържете устройството си с акаунта си в ESET HOME по-късно.

4. Ако продължите, без да се свързвате с ESET HOME, изберете опция за активиране. Ако инсталирате по-нова версия върху предишната, вашият **ключ за активиране** се въвежда автоматично.

5. Съветникът за инсталиране определя кой продукт на ESET е инсталиран въз основа на абонамента ви. Версията с най-много функции за защита винаги е предварително избрана. Щракнете върху **Промяна на продукта**, ако искате да инсталирате друга версия на продукта на ESET. Щракнете върху **Продължи**, за да стартирате процеса на инсталиране. Това може да отнеме известно време.

Ако има някакви останали елементи (файлове или папки) от продуктите на ESET, деинсталирани в миналото, ще бъдете подканени да позволите премахването им. Щракнете върху **Инсталиране**, за да продължите.

6. Щракнете върху **Готово**, за да излезете от съветника за инсталиране.

Инструмент за отстраняване на неизправности при инсталиране.

След инсталиране и активиране на продукта модулите започват да се изтеглят. Защитата се инициализира и някои функции може да не са напълно функционални, докато изтеглянето не приключи.

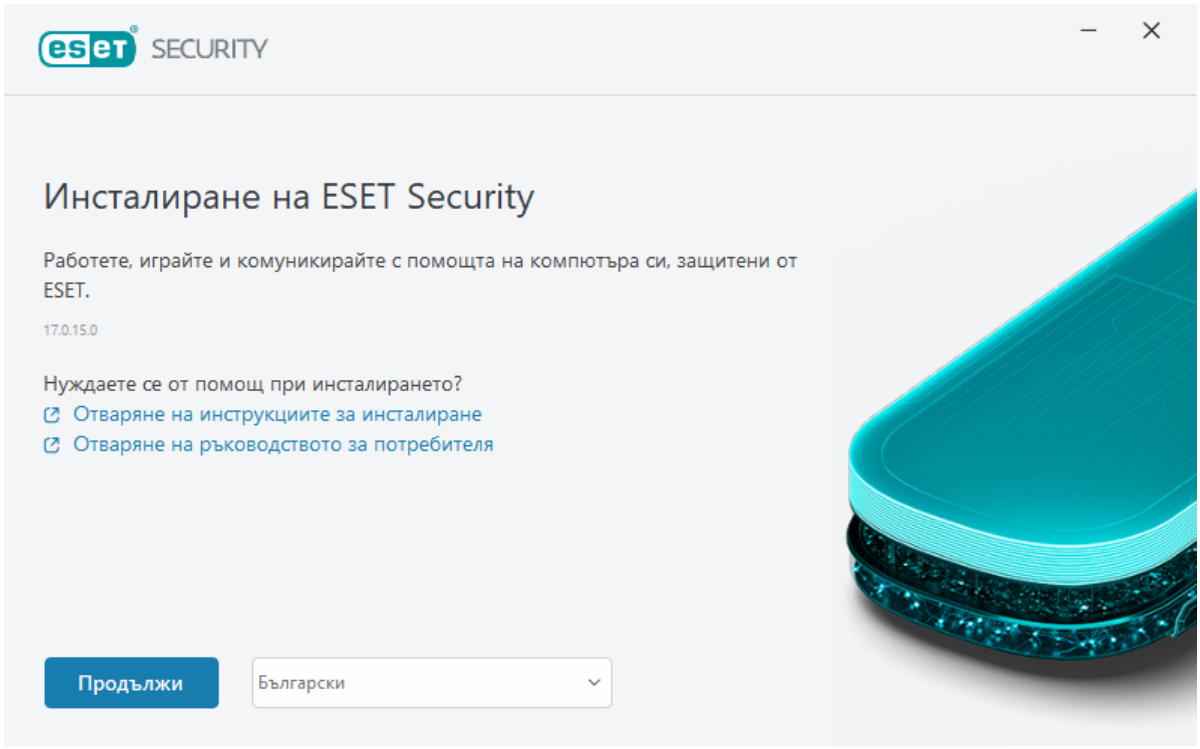
Офлайн инсталиране

Изтеглете и инсталирайте вашия продукт за домашна употреба на ESET за Windows с помощта на офлайн програмата за инсталиране (.exe) по-долу. Изберете коя версия на продукта ESET HOME да изтеглите (32-битова, 64-битова или ARM).

ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Изтегляне на 64-битова версия Изтегляне на 32-битова версия Изтегляне на ARM	Изтегляне на 64-битова версия Изтегляне на 32-битова версия Изтегляне на ARM	Изтегляне на 64-битова версия Изтегляне на 32-битова версия Изтегляне на ARM	Изтегляне на 64-битова версия Изтегляне на 32-битова версия Изтегляне на ARM

Ако имате активна интернет връзка, инсталирайте продукта на ESET с помощта на инсталатор.

Когато стартирате офлайн инсталатора (.exe), съветникът за инсталиране ще ви помогне в процеса на настройка.



1. Изберете подходящия език от падащото меню и щракнете върху **Продължаване**.

> Ако инсталирате по-нова версия върху предишната с настройки, защитени с парола, въведете паролата си. Можете да конфигурирате паролата за настройки в настройката на Access.

2. Изберете предпочитанията си за следните функции, прочетете Лицензионното споразумение за краен потребител и Правилата за поверителност и щракнете върху **Продължи** или щракнете върху **Разрешаване на всички и продължаване**, за да разрешите всички функции:

- Система за обратна връзка на ESET LiveGrid®
- Потенциално нежелани приложения
- Програма за подобряване на работата на клиентите

> Като щракнете върху **Продължи** или **Разрешаване на всички и продължаване**, вие приемате Лицензионното споразумение с краен потребител и потвърждавате Правилата за поверителност.

3. Щракнете върху **Пропускане на влизането**. Когато имате интернет връзка, можете да свържете устройството с акаунта си в ESET HOME.

4. Щракнете върху **Пропускане на активацията**. ESET Internet Security трябва да се активира след инсталирането, за да бъде напълно функционален. Активирането на продукта изисква активна интернет връзка.

5. Съветникът за инсталиране показва кой продукт на ESET ще бъде инсталиран на база на изтегления офлайн инсталатор. Щракнете върху **Продължи**, за да стартирате процеса на инсталиране. Това може да отнеме известно време.

Ако има някакви останали елементи (файлове или папки) от продуктите на ESET, деинсталирани в миналото, ще бъдете подканени да позволите премахването им. Щракнете върху **Инсталиране**, за да продължите.

6. Щракнете върху **Готово**, за да излезете от съветника за инсталиране.

Инструмент за отстраняване на неизправности при инсталиране.

Абонаментът е надстроен

Този прозорец за известяване се появява, когато абонаментът, използван за активиране на вашия продукт на ESET, е променен. Промененият абонамент ви позволява да активирате продукт с повече функции за защита. Ако не е извършена промяна, ESET Internet Security веднъж ще покаже прозорец за известяване, който гласи **Преминаване към продукт с повече функции**.

Да (препоръчително) – автоматично ще инсталира продукта с повече функции за защита.

Не, благодаря – няма да бъдат направени промени и известието ще изчезне завинаги.

За да промените продукта по-късно, вижте нашата статия в онлайн помощника на ESET. За повече информация относно абонамента за ESET вижте ЧЗВ за абонамента.

Таблицата по-долу описва подробно функциите, налични във всеки конкретен продукт.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Система за засичане на потенциално опасни заплахи	✔	✔	✔	✔
Разширено машинно обучение	✔	✔	✔	✔
Блокиране на експлойти	✔	✔	✔	✔
Защита срещу атаки, базирани на скриптове	✔	✔	✔	✔
Анти-фишинг	✔	✔	✔	✔
Защита на уеб достъпа	✔	✔	✔	✔
HIPS (включително Щит срещу малуер, който криптира файловете и иска откуп за отключването им)	✔	✔	✔	✔
Антиспам		✔	✔	✔
Защитна стена		✔	✔	✔
Мрежов инспектор		✔	✔	✔
Защита на уеб камерата		✔	✔	✔
Защита от мрежови атаки		✔	✔	✔
Защита от ботнет мрежи		✔	✔	✔
Безопасно банкиране и сърфиране		✔	✔	✔
Поверителност и защита на браузъра		✔	✔	✔
Родителски контрол		✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Anti-Theft		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Надстройване на продукта

Вие сте изтеглили инсталационната програма по подразбиране и сте решили да промените продукта, който да бъде активиран, или искате да замените инсталирания продукт с такъв с повече функции за защита.

Промяна на продукта по време на инсталирането.

Таблицата по-долу описва подробно функциите, налични във всеки конкретен продукт.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Система за засичане на потенциално опасни заплахи	✔	✔	✔	✔
Разширено машинно обучение	✔	✔	✔	✔
Блокиране на експлойти	✔	✔	✔	✔
Защита срещу атаки, базирани на скриптове	✔	✔	✔	✔
Анти-фишинг	✔	✔	✔	✔
Защита на уеб достъпа	✔	✔	✔	✔
HIPS (включително Щит срещу малуер, който криптира файловете и иска откуп за отключването им)	✔	✔	✔	✔
Антиспам		✔	✔	✔
Защитна стена		✔	✔	✔
Мрежов инспектор		✔	✔	✔
Защита на уеб камерата		✔	✔	✔
Защита от мрежови атаки		✔	✔	✔
Защита от ботнет мрежи		✔	✔	✔
Безопасно банкиране и сърфиране		✔	✔	✔
Поверителност и защита на браузъра		✔	✔	✔
Родителски контрол		✔	✔	✔
Anti-Theft		✔	✔	✔
Password Manager			✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Абонаментът е понижен

Този диалогов прозорец се появява, когато абонаментът, използван за активиране на вашия продукт на ESET, е променен. Промененият абонамент може да се използва само с различни продукт на ESET с по-малко функции за защита. Продуктът е променен автоматично, за да се предотврати загубата на защита.

За повече информация относно абонамента за ESET вижте ЧЗВ за абонамента.

Таблицата по-долу описва подробно функциите, налични във всеки конкретен продукт.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Система за засичане на потенциално опасни заплахи	✔	✔	✔	✔
Разширено машинно обучение	✔	✔	✔	✔
Блокиране на експлойти	✔	✔	✔	✔
Защита срещу атаки, базирани на скриптове	✔	✔	✔	✔
Анти-фишинг	✔	✔	✔	✔
Защита на уеб достъпа	✔	✔	✔	✔
HIPS (включително Щит срещу малуер, който криптира файловете и иска откуп за отключването им)	✔	✔	✔	✔
Антиспам		✔	✔	✔
Защитна стена		✔	✔	✔
Мрежов инспектор		✔	✔	✔
Защита на уеб камерата		✔	✔	✔
Защита от мрежови атаки		✔	✔	✔
Защита от ботнет мрежи		✔	✔	✔
Безопасно банкиране и сърфиране		✔	✔	✔
Поверителност и защита на браузъра		✔	✔	✔
Родителски контрол		✔	✔	✔
Anti-Theft		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Понижаване на категорията на продукта

Продуктът, който е инсталиран в момента, има повече функции за защита от този, който сте напът да активирате. Ще загубите защитата против кражби и достъпа до свързани данни, които се съхраняват в ESET HOME.

Таблицата по-долу описва подробно функциите, налични във всеки конкретен продукт.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Система за засичане на потенциално опасни заплахи	✔	✔	✔	✔
Разширено машинно обучение	✔	✔	✔	✔
Блокиране на експлойти	✔	✔	✔	✔
Защита срещу атаки, базирани на скриптове	✔	✔	✔	✔
Анти-фишинг	✔	✔	✔	✔
Защита на уеб достъпа	✔	✔	✔	✔
HIPS (включително Щит срещу малуер, който криптира файловете и иска откуп за отключването им)	✔	✔	✔	✔
Антиспам		✔	✔	✔
Защитна стена		✔	✔	✔
Мрежов инспектор		✔	✔	✔
Защита на уеб камерата		✔	✔	✔
Защита от мрежови атаки		✔	✔	✔
Защита от ботнет мрежи		✔	✔	✔
Безопасно банкиране и сърфиране		✔	✔	✔
Поверителност и защита на браузъра		✔	✔	✔
Родителски контрол		✔	✔	✔
Anti-Theft		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Инструмент за отстраняване на неизправности при инсталиране

Ако възникнат проблеми по време на инсталирането, съветникът за инсталиране предоставя инструмент за отстраняване на неизправности, който разрешава проблема, ако е възможно.

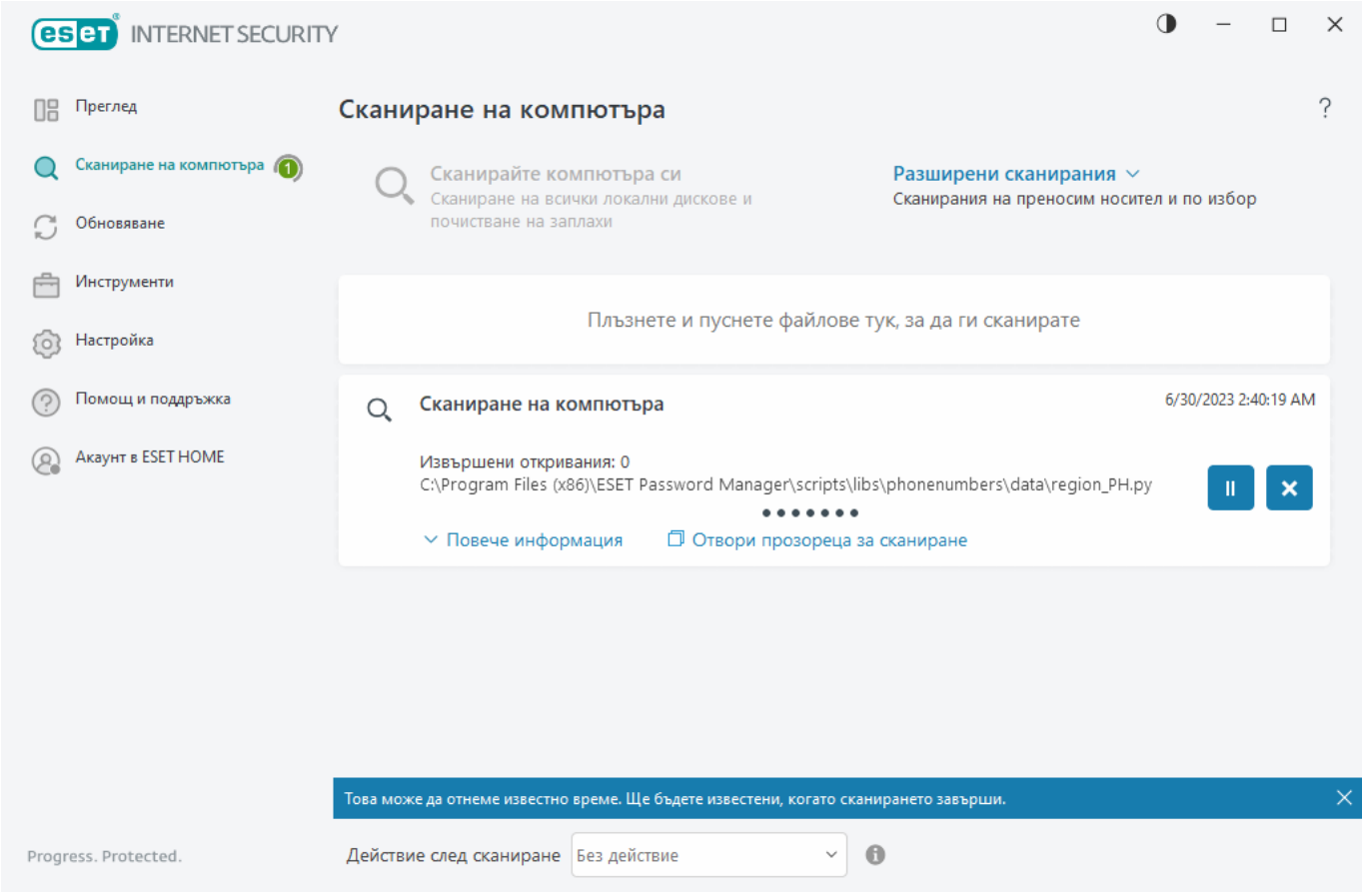
Щракнете върху **Изпълнение на програмата за отстраняване на неизправности**, за да стартирате програмата за отстраняване на неизправности. Когато програмата за отстраняване на неизправности завърши, следвайте препоръчителното решение.

Ако проблемът продължава, вижте списъка с често срещани грешки при инсталация и решения.

Първо сканиране след инсталация

След като инсталирате ESET Internet Security, програмата ще започне да сканира компютъра след първото си успешно обновяване, за да провери за злонамерен код.

Може да стартирате сканиране на компютъра ръчно от главния прозорец на програмата > **Сканиране на компютъра** > **Сканиране на компютъра**. За повече информация относно сканирането на компютъра вж. раздел Сканиране на компютъра.



Надстройване до по-нова версия

Издават се нови версии на ESET Internet Security, за да се внасят подобрения или да се отстраняват проблеми, които не могат да се решат с автоматично обновяване на програмните модули. Надстройването до по-нова версия може да се извърши по няколко начина:

1. Автоматично, чрез обновяване на програмата.
Тъй като надстройката на програмата се изпраща на всички потребители и може да повлияе на определени системни конфигурации, тя се изпраща след дълъг период на тестване, за да гарантира работа с всички възможни системни конфигурации. Ако трябва да надстроите до по-нова версия веднага след издаването ѝ, използвайте някой от методите по-долу.
Уверете се, че сте разрешили **Обновявания на функциите на приложението** в Разширени настройки > **Обновяване** > **Профили** > **Обновявания**.

2. Ръчно, в главния прозорец на програмата чрез щракване върху **Проверка за обновявания** в раздела **Обновяване**.

3. Ръчно, чрез изтегляне и инсталиране на по-нова версия върху предишната.

За допълнителна информация и инструкции с илюстрации вж.:

- Обновяване на продукти на ESET – проверете за най-новите модули на продукти
- Какви са различните типове обновявания и издания на продукти на ESET?

Автоматично надстройване на стари продукти

Версията на вашия продукт на ESET вече не се поддържа и продуктът ви е надстроен до най-новата версия.

⚠ Често срещани проблеми с инсталирането

> ℹ Всяка нова версия на продуктите на ESET има много поправки и подобрения. Съществуващите клиенти с валиден абонамент за продукт на ESET могат да надстроят до най-новата версия на същия продукт безплатно.

За да завършите инсталирането:

1. Щракнете върху **Приемане и продължаване**, за да приемете Лицензионното споразумение с краен потребител и да потвърдите Правилата за поверителност. Ако не сте съгласни с лицензионното споразумение с краен потребител, щракнете върху **Деинсталиране**. Не можете да се върнете към предишната версия.

2. Щракнете върху **Разрешаване на всички и продължаване**, за да позволите на ESET LiveGrid® системата за обмен на информация за потенциални заплахи и Програма за подобряване на работата на клиентите или щракнете върху **Продължаване**, ако не искате да участвате.

3. След като активирате новия продукт на ESET с ключа за активиране, ще се покаже страницата „Преглед“. Ако информацията за абонамента ви не бъде намерена, продължете с безплатната пробна версия. Ако абонаментът, който сте използвали в предишния продукт, не е валиден, активирайте своя продукт на ESET.

4. За завършване на инсталирането е необходимо да рестартирате на устройството.

Предстои инсталиране на ESET Internet Security

Този диалогов прозорец може да се покаже:

• По време на инсталационния процес – Щракнете върху **Продължи**, за да инсталирате ESET Internet Security.

• При промяна на абонамент в ESET Internet Security – щракнете върху **Активиране**, за да промените абонамента и да активирате ESET Internet Security.

Опцията **Промяна на продукт** ви позволява да превключвате между продукти на ESET за домашна употреба за Windows в съответствие с вашия абонамент за продукт на ESET. Вижте С кой продукт разполагам? за повече информация.

Преминаване към друга продуктова линия

В съответствие с вашия абонамент за продукт на ESET можете да превключвате между различни продукти на ESET за домашна употреба за Windows. Вижте С кой продукт разполагам? за повече информация.

Регистрация

Регистрирайте абонамента си, като попълните полетата във формуляра за регистрация и щракнете върху **Активиране**. Обозначените като необходими полета в скоби са задължителни. Тази информация ще се използва единствено за въпроси, свързани с вашия абонамент за ESET.

Ход на активиране

Дайте няколко секунди на процеса на активиране да завърши (необходимото време може да е различно в зависимост от скоростта на интернет връзката или компютъра ви).

Активирането е успешно

Процесът по активиране е завършен. Следвайте съветника след инсталирането, за да завършите настройването на ESET Internet Security.

След няколко секунди ще започне актуализация на модула. Редовните обновявания на ESET Internet Security ще започнат незабавно.

Първоначално сканиране ще започне автоматично в рамките на 20 минути след актуализацията на модула.

Процесът на активиране може да бъде прекъснат, ако предлагането не е свързано с ESET HOME. Влезте в ESET HOME или създайте акаунт.

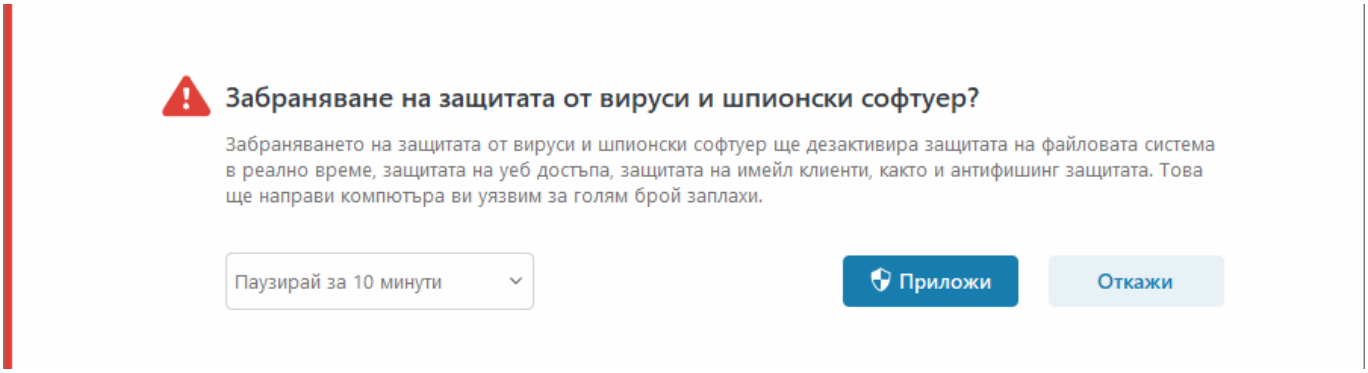
Ръководство за начинаещи

Тази глава предоставя общ преглед на ESET Internet Security и основните настройки.

Икона в системната област

Някои от най-важните опции за настройка и функции са достъпни чрез щракване с десния бутон върху иконата в системната област.

Временно спиране на защитата – показва диалоговия прозорец за потвърждение, забраняващ системата за засичане на потенциално опасни заплахи, която предпазва от злонамерени атаки на системата чрез контролиране на комуникацията с файлове, уеб и имейл. Падащото меню **Времеви интервал** ви позволява да зададете колко дълго защитата ще бъде забранена.



Временно спиране на защитната стена (разрешаване на целия трафик) – превключване на защитната стена в неактивно състояние. За повече информация вж. Мрежа.

Блокиране на целия мрежов трафик – Блокира целия мрежов трафик. Можете да го разрешите отново, като щракнете върху **Спиране на блокирането на целия мрежов трафик**.

Разширени настройки – отваря разширени настройки на ESET Internet Security. За да отворите разширените настройки от главния прозорец на продукта, натиснете F5 на клавиатурата си или щракнете върху **Настройка** > **Разширена настройка**.

Регистрационни файлове – регистрационните файлове съдържат информация относно важни събития, възникнали в програмата, и предоставят обобщение на засичанията.

Отваряне на ESET Internet Security – отваря ESET Internet Security главния прозорец на програмата.

Възстанови оформлението на прозореца – Възстановяване на размера и позицията по подразбиране на прозореца на ESET Internet Security в екрана.

Цветови режим – отваря настройките на потребителския интерфейс, където може да промените цвета на GUI.

Проверка за обновявания – стартира модул или обновяване на продукта, за се увери, че сте защитени. ESET Internet Security проверява автоматично за обновявания няколко пъти на ден.

Относно – предоставя системна информация, подробности относно инсталираната версия на ESET Internet Security, инсталираните програмни модули и информация относно операционната система и системните ресурси.

Клавишни комбинации

За по-добро навигиране в ESET Internet Security може да използвате следните клавишни комбинации:

Клавишни комбинации	Действие
F1	отвори помощни страници
F5	отвори разширените настройки
Стрелка нагоре/Стрелка надолу	навигация в елементи от падащото меню
TAB	преминаване към следващия елемент на ГПИ в прозорец
Shift+TAB	преминаване към предишния елемент на ГПИ в прозорец
ESC	затвори активния прозорец
Ctrl+U	показва информация за абонамента за ESET и компютъра (подробна информация за техническата поддръжка)
Ctrl+R	възстановява прозореца на продукта до неговите размер и позиция по подразбиране на екрана
ALT + стрелка наляво	придвижване назад
ALT + стрелка надясно	придвижване напред
ALT+Home	придвижване към начало

Можете също да използвате бутоните на мишката назад или напред за навигация.

Профили

Диспечерът на профили се използва на две места в ESET Internet Security – в раздела **Сканиране при поискване** и в раздела **Обновяване**.

Сканиране на компютъра

Има 4 предварително зададени профили за сканиране в ESET Internet Security:

- **Smart сканиране**: това е профилът за разширено сканиране по подразбиране. Профилът за Smart сканиране използва технологията Smart оптимизация, която изключва файлове, за които е установено, че са чисти в предишно сканиране и не са променяни след това сканиране. Това допринася за по-ниски времена на сканиране с минимално въздействие

върху защитата на системата.

• **Сканиране от контекстното меню**: можете да започнете сканиране при поискване на всеки файл от контекстното меню. Профилът за сканиране от контекстното меню ви позволява да зададете конфигурация за сканиране, която ще се използва, когато стартирате сканирането по този начин.

• **Задълбочено сканиране**: профилът за задълбочено сканиране не използва Smart оптимизация по подразбиране, така че няма файлове да бъдат изключени от сканиране при използването на този профил.

• **Сканиране на компютъра**: това е профилът по подразбиране, използван в стандартното сканиране на компютъра.

Предпочитаните параметри за сканиране могат да се запишат за бъдещо сканиране. Препоръчително е да създадете различен профил (с различни цели и методи за сканиране, както и с други параметри) за всяко сканиране, което се използва редовно.

За да създадете нов профил, отворете Разширени настройки > **Система за засичане** > **Сканирания за злонамерен софтуер** > **Сканиране при поискване** > **Списък с профили** > **Редактиране**. Прозорецът **Диспечер на профили** включва падащото меню **Избран профил**, което изброява съществуващите профили за сканиране, както и опция за създаване на нов профил. За да създадете профил за сканиране според вашите нужди, вижте ThreatSense за описание на всеки параметър от настройките за сканиране.

Да предположим, че искате да създадете собствен профил на сканиране и конфигурацията на **Сканиране на компютъра** донякъде е подходяща, но не искате да сканирате архиватори в реално време или потенциално опасни приложения, а освен това искате да приложите **Винаги отстранявай откриването**. Въведете името на новия профил в прозореца **Диспечер на профили** и щракнете върху **Добавяне**. Изберете новия профил от падащото меню **Избран профил** и задайте останалите параметри така, че да съответстват на изискванията ви, след което щракнете върху **OK**, за да запишете новия профил.

Обновяване

Редакторът на профили в Настройка на обновяването ви позволява за създавате нови профили за обновяване. Създайте и използвайте собствени профили по избор (например различни от този по подразбиране **Моят профил**) само ако компютърът ви използва няколко средства за свързване със сървърите за обновяване.

Например даден преносим компютър, който обикновено се свързва с локален сървър с дублирани файлове в локалната мрежа, но изтегля обновяванията директно от сървърите за обновяване на ESET, когато връзката с локалната мрежа е прекъсната (командировка), може да използва два профила: първият да се свързва с локалния сървър, а другият да се свързва със сървърите на ESET. Когато тези профили се конфигурират, отидете до **Инструменти** > **Планировчик** и редактирайте параметрите за задачата за обновяване. Укажете единия профил като първичен, а другият като вторичен.

Профил за обновяване – текущо избраният профил за обновяване. За да го промените, изберете профил от падащото меню.

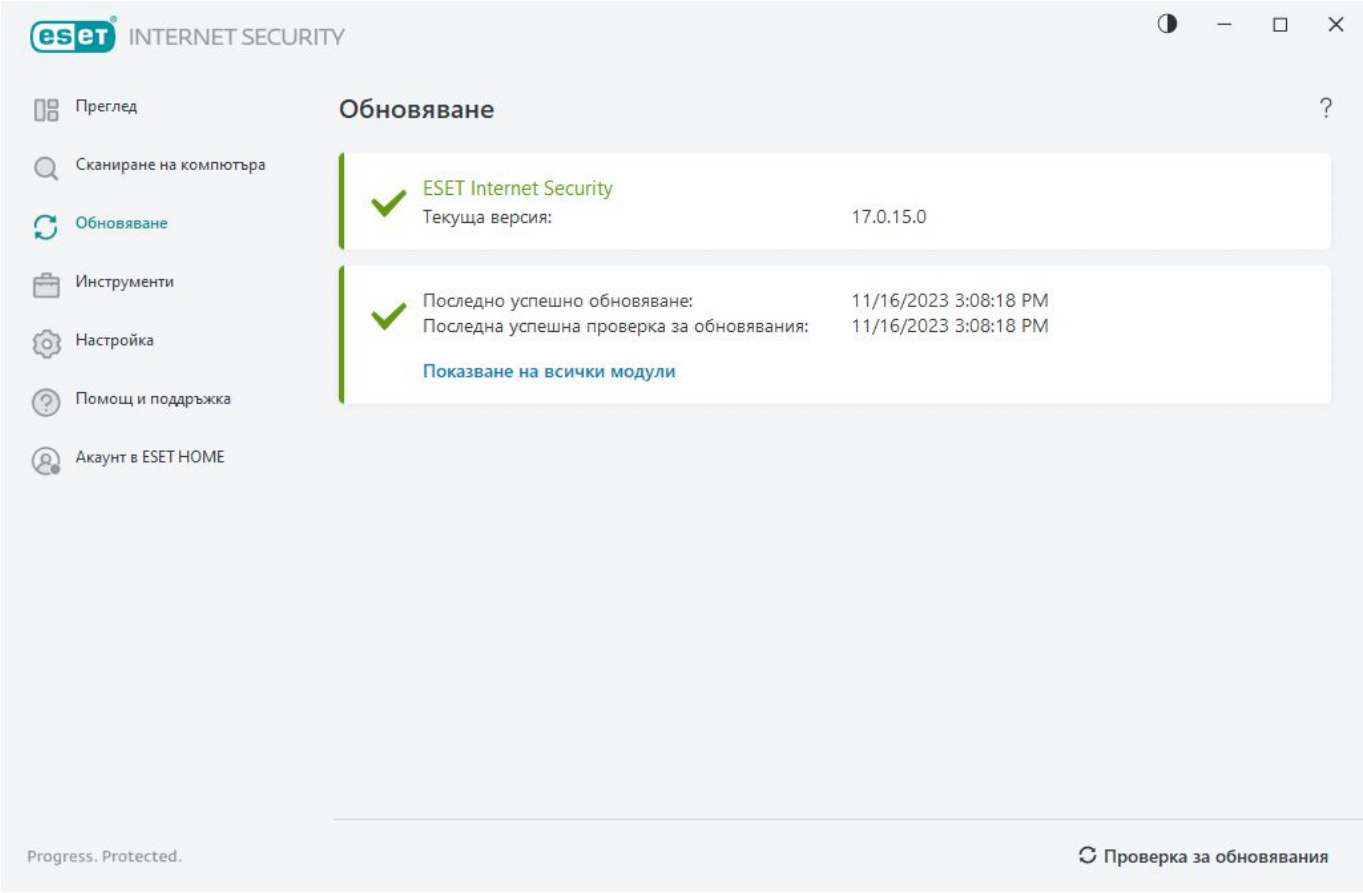
Списък с профили – създаване на нови или премахване на съществуващи профили за обновяване.

Обновявания

Редовното обновяване на ESET Internet Security е най-добрият метод за гарантиране на максимално ниво на защита за компютъра. Модулът за обновяване гарантира, че и програмните модули, и системните компоненти са винаги обновени.

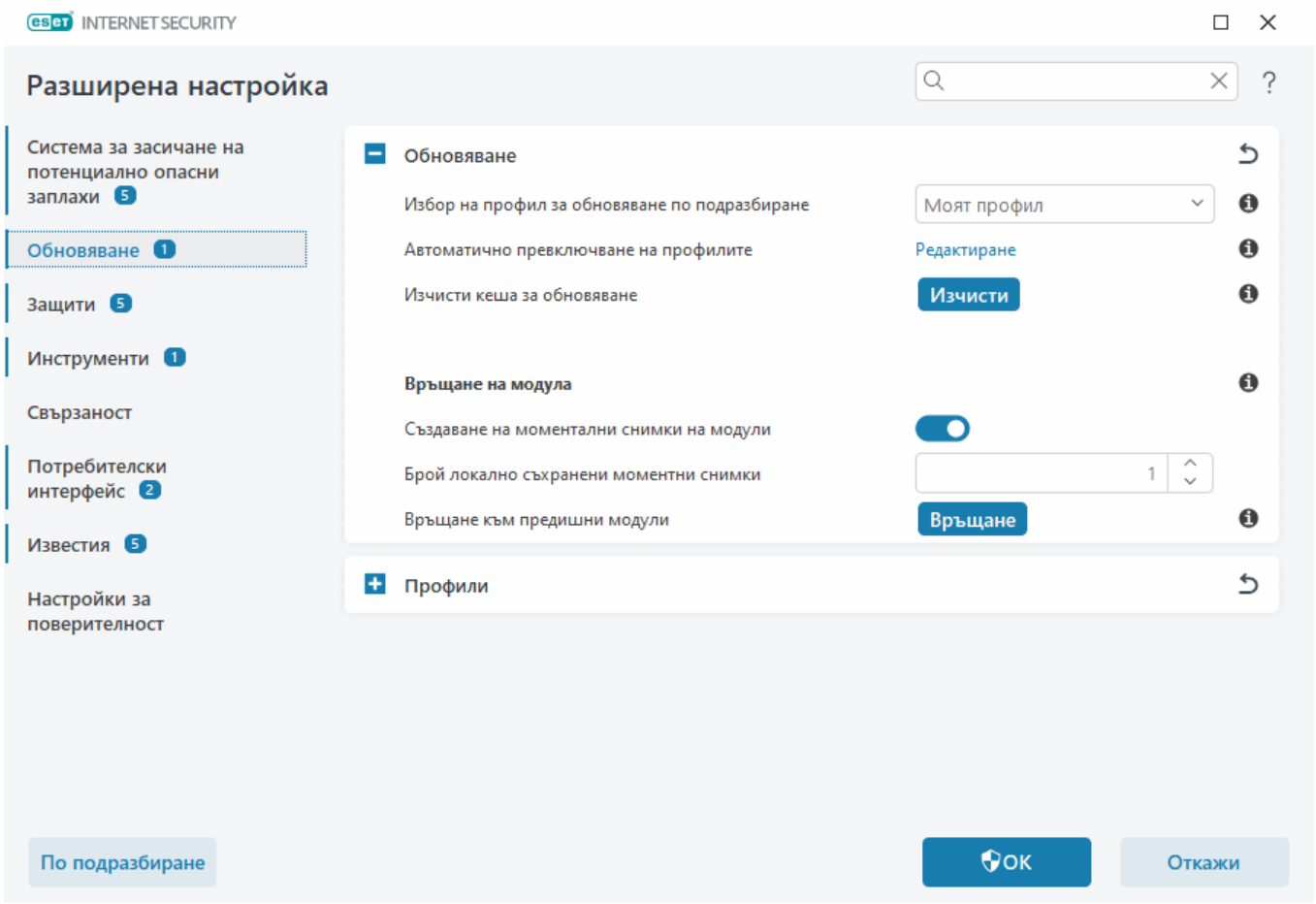
Чрез щракване върху **Обнови** в главния прозорец на програмата можете да разберете текущото състояние на обновяване, а също така датата и часа на последното успешно обновяване, както и дали е необходимо обновяване.

В допълнение към автоматичните обновявания можете да щракнете върху **Проверка за обновявания**, за да задействате ръчно обновяване.



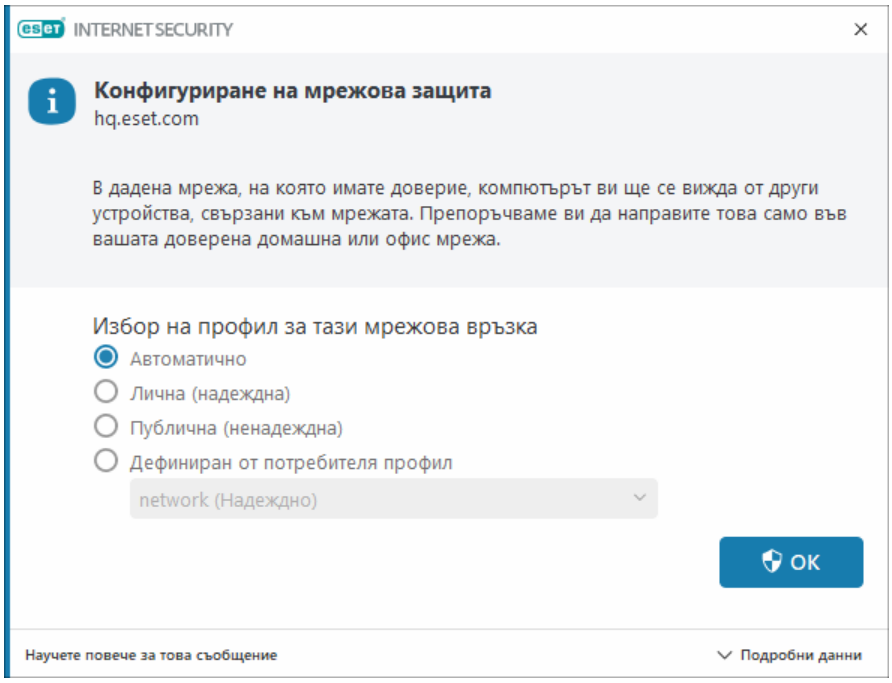
Разширени настройки > **Обновяване** съдържа допълнителни опции за обновяване, като например режим на обновяване, достъп до прокси сървър и LAN връзки.

Ако изпитвате проблеми с обновяване, щракнете върху **Изчистване**, за да изчистите кеша с обновявания. Ако все още не можете да обновите програмните модули, вижте раздела Отстраняване на неизправности за съобщението „Неуспешно обновяване на модулите“.



Конфигуриране на мрежова защита

По подразбиране ESET Internet Security използва настройките на Windows, когато бъде открита нова мрежова връзка. За да се покаже диалогов прозорец, когато бъде открита нова мрежа, променете Присвояване на профил за мрежова защита на **Попитай**. Конфигурирането на мрежова защита ще се показва, когато компютърът се свързва с нова мрежа.



Можете да избирате от следните Профили за мрежова връзка:

Автоматично – ESET Internet Security ще избере профила автоматично в зависимост от активаторите, конфигурирани за всеки профил.

Лична – За надеждни мрежи (домашна или офис мрежа). Вашият компютър и споделените файлове, съхранени на компютъра, са видими за други потребители в мрежата, а системните ресурси са достъпни за други потребители в мрежата (достъпът до споделени файлове и принтери е разрешен, входящата RPC комуникация е разрешена и споделянето на работния плот е налично). Препоръчваме да използвате тази настройка при достъп до защитена локална мрежа. Този профил автоматично се присвоява на мрежова връзка, ако е конфигуриран като домейн или частна мрежа в Windows.

Публична – За ненадеждни мрежи (публична мрежа). Файловете и папките на вашата система не се споделят или не се виждат от други потребители в мрежата и споделянето на системни ресурси е дезактивирано. Препоръчваме да използвате тази настройка при достъп до безжични мрежи. Този профил автоматично се присвоява на всяка мрежова връзка, която не е конфигурирана като домейн или частна мрежа в Windows.

Дефиниран от потребителя профил – Можете да изберете профил, който сте създали, от падащото меню. Тази опция е налична само ако сте създали поне един персонализиран профил.

Неправилното конфигуриране на мрежата може да създаде риск за компютъра.

Разреши Anti-Theft

При нашите ежедневни пътувания от вкъщи до работа или други публични места персоналните устройства са постоянно изложени на риск от загуба или кражба. Anti-Theft е функция, която разширява защитата на ниво потребител в случай на загубено или откраднато устройство. Anti-Theft ви позволява да наблюдавате употребата му и да проследявате липсващото устройство чрез определяне на местоположение по IP адрес в ESET HOME, което ще ви помогне да си върнете устройството и да защитите личните си данни.

Чрез използването на съвременни технологии, като например географско търсене на IP адрес, заснемане на изображения с уеб камера, защита на потребителски акаунти и наблюдение на устройства, Anti-Theft може да помогне на вас и на правоприлагащите органи при намирането на компютъра или устройството, в случай че то е изгубено или откраднато. В ESET HOME можете да видите каква дейност се извършва на вашия компютър или устройство.

За да научите повече за Anti-Theft в ESET HOME, вижте Онлайн помощта за ESET HOME.

Anti-Theft може да не работи правилно на компютри в домейни поради ограничения в управлението на потребителски акаунти.

За да разрешите Anti-Theft и да защитите устройството си в случай на загуба или кражба, изберете една от следните опции:

- В главния прозорец на програмата > **Преглед** щракнете върху **НАСТРОЙВАНЕ** до **Anti-Theft**.

• Ако видите съобщението „Системата Anti-Theft е налична“ в главния прозорец на програмата > **Преглед** екран, щракнете върху **Разреши Anti-Theft**.

• От главния прозорец на програмата щракнете върху **Настройка** > **Инструменти за защита**. Активирайте превключвателя **Anti-Theft** и следвайте инструкциите на екрана.

Ако устройството ви не е свързано с ESET HOME, трябва да:
1. Влезете в акаунта си в ESET HOME, когато разрешавате Anti-Theft.
2. Задаване на име на устройството.

Anti-Theft не поддържа Microsoft Windows Home Server.

След Разрешаване на Anti-Theft можете да оптимизирате защитата на вашето устройство в главния прозорец на програмата > **Настройка** > **Инструменти за защита** > **Anti-Theft**.

Родителски контрол

Ако вече сте разрешили родителски контрол в ESET Internet Security, трябва да конфигурирате родителския контрол и за всички свързани потребителски акаунти.

Когато родителският контрол е активен и потребителските акаунти не са конфигурирани, ESET Internet Security показва известие „Родителският контрол не е настроен“ на екрана **Преглед**. Щракнете върху **Задаване на правила** и вижте раздела Родителски контрол за повече информация.

Активиране на продукта

Има няколко метода за активиране на продукта. Наличността на определен сценарий за активиране в прозореца за активиране може да се различава в зависимост от държавата и методите на разпространение (CD/DVD, уеб страницата на ESET и т.н.):

• Ако сте закупили версия на продукта в опаковка или сте получили имейл с данни за абонамент, активирайте продукта, като щракнете върху **Използване на закупен ключ за активиране**. За да бъде активирането успешно, ключът за активиране трябва да се въведе, както е предоставен. Ключът за активиране – уникален низ във формат XXXX-XXXX-XXXX-XXXX-XXXX или XXXX-XXXXXXXX, който се използва за идентифициране на собственика на абонамента и за активиране на абонамента. Ключ за активиране обикновено се намира във или на гърба на опаковката на продукта.

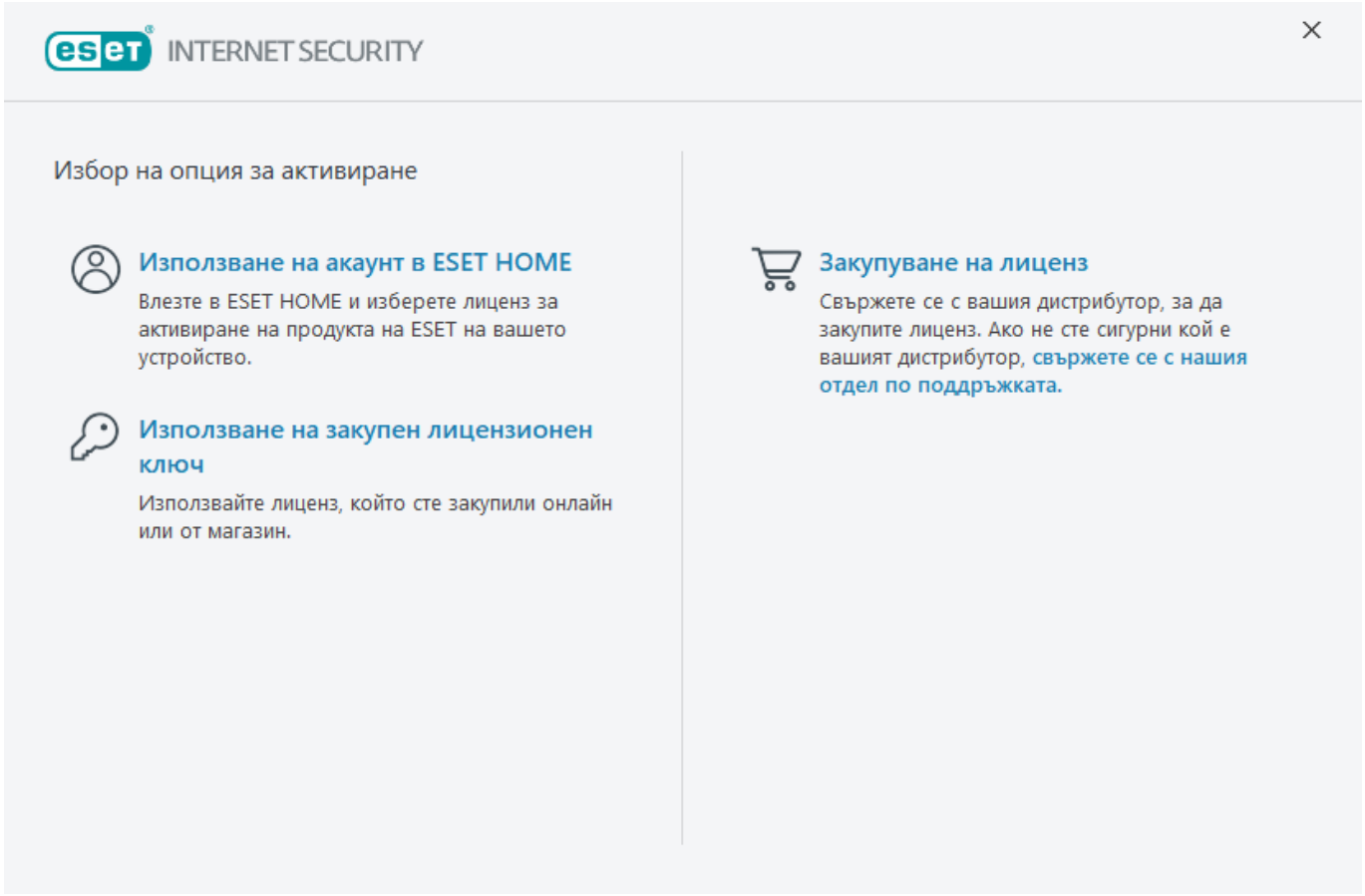
• След като изберете Използване на акаунт в ESET HOME, ще бъдете помолени да влезете в акаунта си в ESET HOME.

• Ако искате да оцените ESET Internet Security, преди да извършите покупка, изберете Безплатен пробен период. Въведете имейл адреса и страната си, за да активирате ESET Internet Security за ограничено време. Безплатната пробна версия ще ви бъде изпратена по имейл. Безплатните пробни версии могат да се активират само по веднъж за даден клиент.

• Ако не разполагате с абонамент и искате да закупите такъв, щракнете върху „**Покупка на абонамент**“. Това ще ви препрати към уеб сайта на дистрибутора на ESET за региона ви. Абонаментите за продукт на ESET за домашна употреба за Windows не са безплатни.

Можете да промените абонамента за продукта по всяко време. За да направите това, щракнете върху **Помощ и поддръжка** > **Промяна на абонамент** в главния прозорец на програмата. Ще видите публичния ИД, използван за идентифициране на вашия абонамент в поддръжката на ESET.

⚠ Неуспешно активиране на продукта?



Въвеждане на ключа за активиране по време на активирането

Автоматичните обновявания са важни за вашата защита. ESET Internet Security ще започне да получава обновявания, след като активирате програмата.

Когато въвеждате **Ключ за активиране**, е важно да го въведете точно както е написан: Вашият ключ за активиране е уникален низ във формат XXXX-XXXX-XXXX-XXXX-XXXX, който се използва за идентифициране на притежателя на абонамента и активиране на абонамента.

Препоръчително е да копирате и поставите ключа за активиране от имейла за регистрация, за да сте сигурни, че сте го въвели точно.

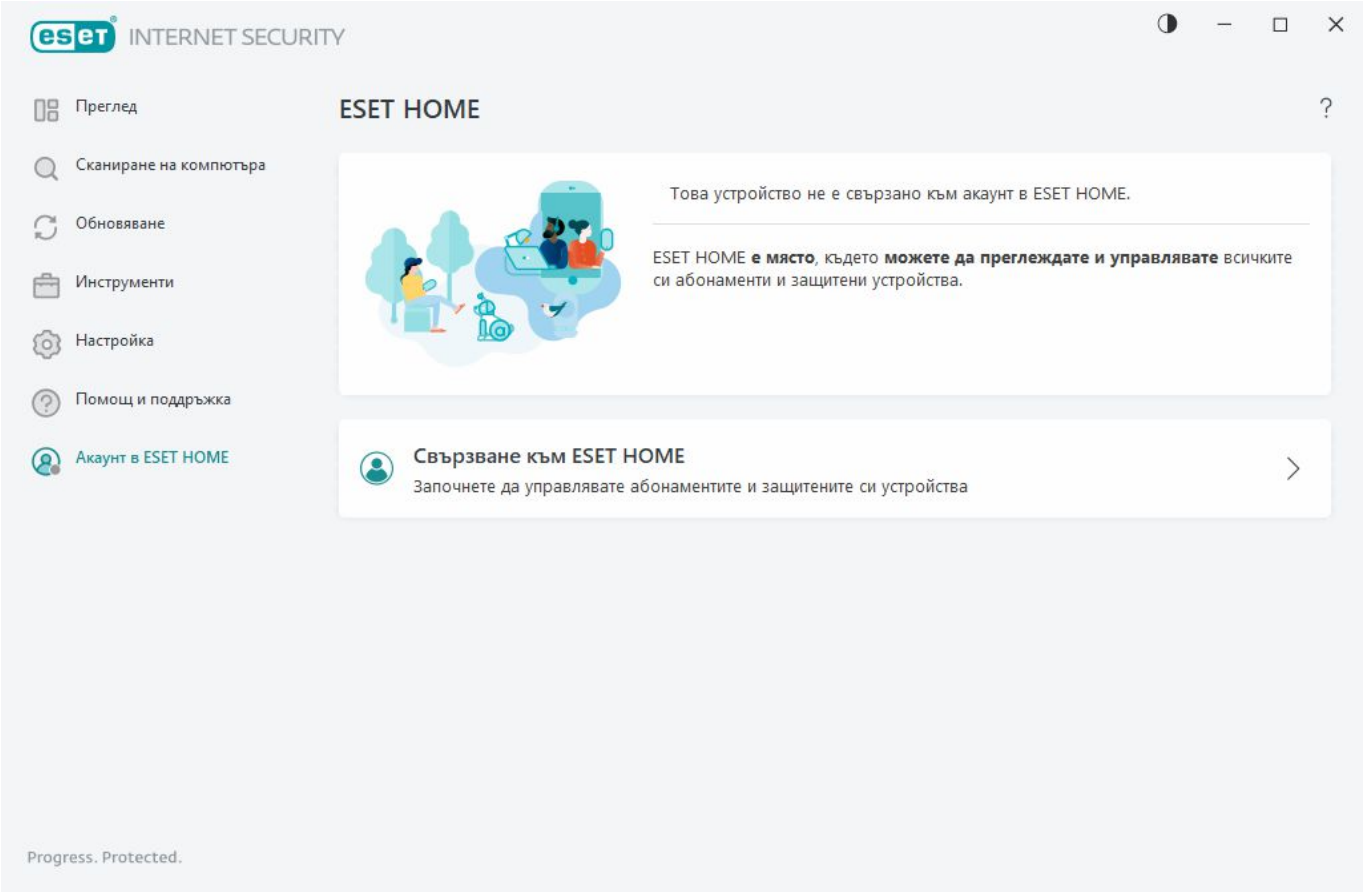
Ако не въведете ключа за активиране след инсталирането, продуктът ви няма да се активира. Можете да активирате ESET Internet Security в главния прозорец на програмата > **Помощ и**

поддръжка > **Активиране на абонамент**.

Абонаментите за продукт на ESET за домашна употреба за Windows не са безплатни.

Използване на ESET HOME акаунт

Свържете устройството си към ESET HOME, за да преглеждате и управлявате всички активирани абонаменти и устройства на ESET. Може да подновите, надстроите или разширите абонамента си и да видите важни подробности за абонамента. В портала за управление на ESET HOME или мобилното приложение можете да добавяте различни абонаменти, да изтегляте продукти на устройствата си, да проверявате състоянието на защитата на продукта или да споделяте абонамента чрез имейл. За повече информация посетете онлайн помощ за ESET HOME.



След като изберете **Използване на акаунт в ESET HOME** като метод за активиране или при свързване с акаунт в ESET HOME по време на инсталацията:

1. Влезте в акаунта си ESET HOME.

Ако нямате акаунт в ESET HOME, щракнете върху **Създаване на акаунт** за регистриране или вижте инструкциите в онлайн помощта за ESET HOME.
Ако сте забравили паролата си, щракнете върху **Забравих паролата си** и следвайте стъпките на екрана или вижте онлайн помощта за ESET HOME.

2. Задайте **Име на устройството** за вашето устройство, което ще се използва във всички услуги на ESET HOME, и щракнете върху **Продължаване**.

3. Изберете абонамент за активиране или добавете нов абонамент. Щракнете върху **Продължаване**, за да активирате ESET Internet Security.

Активиране на безплатен пробен период

За да активирате пробна версия на вашия ESET Internet Security, въведете валиден имейл адрес в полетата **Имейл адрес** и **Потвърждаване на имейл адреса**. След активиране вашият абонамент за ESET, необходим за обновяването на , ще се генерира и изпрати на имейла ви. Този имейл адрес ще се използва също така и за известия за изтичане на срока на продукта, както и за други съобщения от ESET. Безплатната пробна версия може да се активира само веднъж.

Изберете страната си от падащото меню **Държава**, за да регистрирате ESET Internet Security при местния дистрибутор, който ще осигури техническа поддръжка.

Безплатен ключ за активиране на ESET

Абонаментът за ESET Internet Security не е безплатен.

Ключът за активиране на ESET е уникална поредица от букви и цифри, разделени с тире, предоставен от ESET, за да се позволи законното използване на ESET Internet Security в съответствие с лицензионното споразумение с краен потребител. Всеки краен потребител има право да използва ключа за активиране само до степента, в която има правото да използва ESET Internet Security въз основа на броя лицензи, предоставени от ESET. Ключът за активиране се счита за поверителен и не може да бъде споделян. Можете обаче да споделите абонамент с помощта на ESET HOME.

В интернет има източници, които може да ви предоставят „безплатни“ ключове за активиране на ESET, но не забравяйте:

• Щракването върху реклама „Безплатен абонамент за ESET“ може да компрометира компютъра или устройството ви и да доведе до заразяване със злонамерен софтуер. Злонамереният софтуер може да бъде скрит в неофициално уеб съдържание (напр. видеоклипове), уеб сайтове, които показват реклами, за да печелят пари въз основа на вашите посещения и др. Обикновено става дума за капан.

• ESET може и в действителност дезактивира пиратски абонаменти.

• Наличието на пиратски ключ за активиране не е в съответствие с лицензионното споразумение с краен потребител, което трябва да приемете, за да инсталирате ESET Internet Security.

• Купувайте абонамент за ESET само през официалните канали, като например www.eset.com, дистрибутори или риселъри на ESET (не купувайте абонамент от неофициални уеб сайтове на трети лица, като eBay, или споделени абонаменти от трети лица).

• Изтеглянето на ESET Internet Security е безплатно, но активирането по време на инсталиране изисква валиден ключ за активиране на ESET (можете да го изтеглите и инсталирате, но без активиране той няма да работи)

• Не споделяйте абонамента си в интернет или в социалните медии (може да стане широко разпространен).

За да идентифицирате и докладвате пиратски абонамент за ESET, вж. нашата статия от онлайн помощника за инструкции.

Ако не сте сигурни за закупуването на продукт за защита на ESET, можете да използвате пробна версия, докато решите:

1. Активирайте ESET Internet Security чрез безплатна пробна версия
2. Участвайте в БЕТА програмата на ESET
3. Инсталирайте ESET Mobile Security, ако използвате мобилно устройство с Android; то е „freemium“.

За да получите отстъпка/удължите своя лиценз, подновете своя ESET.

Неуспешно активиране – често срещани сценарии

Ако активирането на ESET Internet Security е неуспешно, най-често срещаните сценарии са:

- Ключ за активиране вече се използва.
- Въвели сте невалиден ключ за активиране.
- Информацията във формуляра за активиране липсва или е невалидна.
- Комуникацията със сървъра за активиране е неуспешна.
- Няма връзка или е забранена връзката със сървърите за активиране на ESET.

Проверете дали сте въвели правилен ключ за активиране и дали интернет връзката е активна. Опитайте се да активирате ESET Internet Security отново. Ако използвате акаунт в ESET HOME за активиране, вижте ESET HOME Абонамент и управление на абонамент – онлайн помощ.

> Ако получите конкретна грешка (например „Временно спрян абонамент“ или „Превишено използване на абонамент“), следвайте инструкциите в състоянието на абонамента.

Ако все още не можете да активирате ESET Internet Security, програмата за отстраняване на неизправности при активирането на ESET ви превежда през най-често срещаните въпроси, грешки и проблеми, свързани с активирането и лицензирането (налична на английски и още няколко езика).

Състояние на абонамента

Вашият абонамент може да има различни състояния. Можете да намерите състоянието на абонамента си в ESET HOME. За да добавите абонамента си към акаунт в ESET HOME, вижте Добавяне на абонамент.

Ако нямате акаунт в ESET HOME, можете да създадете нов акаунт в ESET HOME.

Ако състоянието на абонамента е различно от **Активен**, ще получите грешка по време на активиране или известие в главния прозорец на програмата.

За да изключите известията за състоянието на абонамента, отворете Разширени настройки > **Известия** > **Състояния на приложението**. Щракнете върху **Редактиране** до **Състояния на приложението**, разширете **Лицензиране** и премахнете отметката до известието, което искате да забраните. Забраняването на известието не решава проблема.

Вижте описанията и препоръчителните решения за различните състояния на абонамента в таблицата по-долу:

Състояние на абонамента	Описание	Решение
Активен	Абонаментът е валиден и няма нужда от вашето взаимодействие. ESET Internet Security може да бъде активиран и можете да намерите подробности за абонамента в главния прозорец на програмата > **Помощ и поддръжка**.	
Превишено използване	Този абонамент се използва от повече устройства, отколкото е позволено. Ще получите грешка при активиране.	Вижте Неуспешно активиране поради превишено използване на абонамент за повече информация.
Временно спрян	Абонаментът ви е временно спрян поради проблеми с плащането. За да използвате абонамента, се уверете, че данните за плащането ви в ESET HOME са актуални или се свържете с дистрибутора си на абонаменти. Можете да получите тази грешка по време на активиране или в главния прозорец на програмата.	Инсталиран продукт – ако имате акаунт в ESET HOME, в известието, показано в главния прозорец на програмата, щракнете върху **Управление на абонаменти в ESET HOME** и прегледайте данните за плащане. В противен случай се свържете с вашия дистрибутор на абонамента. Грешка при активиране – ако имате акаунт в ESET HOME, в прозореца за грешка при активиране щракнете върху **Отваряне на ESET HOME** и прегледайте данните си за плащане. В противен случай се свържете с вашия дистрибутор на абонамента.

Състояние на абонамента	Описание	Решение
С изтекла валидност	Абонаментът ви е изтекъл и не можете да използвате този абонамент, за да активирате ESET Internet Security. Можете да получите тази грешка по време на активиране или в главния прозорец на програмата. Ако вече сте инсталирали ESET Internet Security, компютърът ви не е защитен и обновен.	Инсталиран продукт – в известието, показано в главния прозорец на програмата, щракнете върху **Подновяване на абонамент** и следвайте инструкциите в Как да подновя абонамента си? или щракнете върху **Активиране на продукт** и изберете метода на активиране. Грешка при активиране – в прозореца за грешка при активиране щракнете върху **Подновете абонамента си** и следвайте инструкциите в Как да подновя абонамента си? или въведете нов или подновен ключ за активиране и щракнете върху **Подновяване на абонамент**.
Отказан	Абонаментът ви е прекратен от ESET или от дистрибутора на абонамента.	Ако получите грешка за Ако абонаментът е прекратен в главния прозорец на програмата или по време на активиране, а вие смятате, че той би трябвало да работи правилно, свържете се с дистрибутора на абонамента.

Активирането е неуспешно поради използван прекомерно абонамент

Проблем

- Вашият абонамент може да е с превишено използване или с него да се злоупотребява
- Активирането е неуспешно поради използван прекомерно абонамент

Решение

Има повече устройства, които използват този абонамент, отколкото той позволява. Може да сте жертва на софтуерно пиратство или фалшифициране. Абонаментът не може да се използва за активиране на друг продукт на ESET. Можете да решите този проблем веднага, ако ви е позволено да управлявате абонамент във вашия акаунт в ESET HOME или сте закупили абонамент от легитимен източник. Ако все още нямате акаунт, създайте такъв.

Ако сте собственик на абонамента и не сте подканени да въведете вашия имейл адрес:

1. За да управлявате абонамента си за ESET, отворете уеб браузър и отидете на адрес https://home.eset.com. Отворете ESET License Manager и премахнете или дезактивирайте места.

За повече информация вижте Какво да направите в случай на използван прекомерно абонамент.

2. За да идентифицирате и докладвате пиратски абонамент за ESET, посетете нашата статия за идентифициране и докладване на пиратски абонаменти на ESET за инструкции.

3. Ако не сте сигурни, щракнете върху „**Назад**“ и изпратете имейл до отдела за техническа поддръжка на ESET.

Ако не притежавате абонамент, свържете се със собственика на този абонамент с информация, че не можете да активирате продукта на ESET поради прекомерно използване на абонамента. Собственикът може да реши проблема в портала на ESET HOME.

Ако сте получили подкана да потвърдите вашия имейл адрес (само в някои случаи), въведете имейл адреса, използван при първоначалното закупуване или активиране на вашия ESET Internet Security.

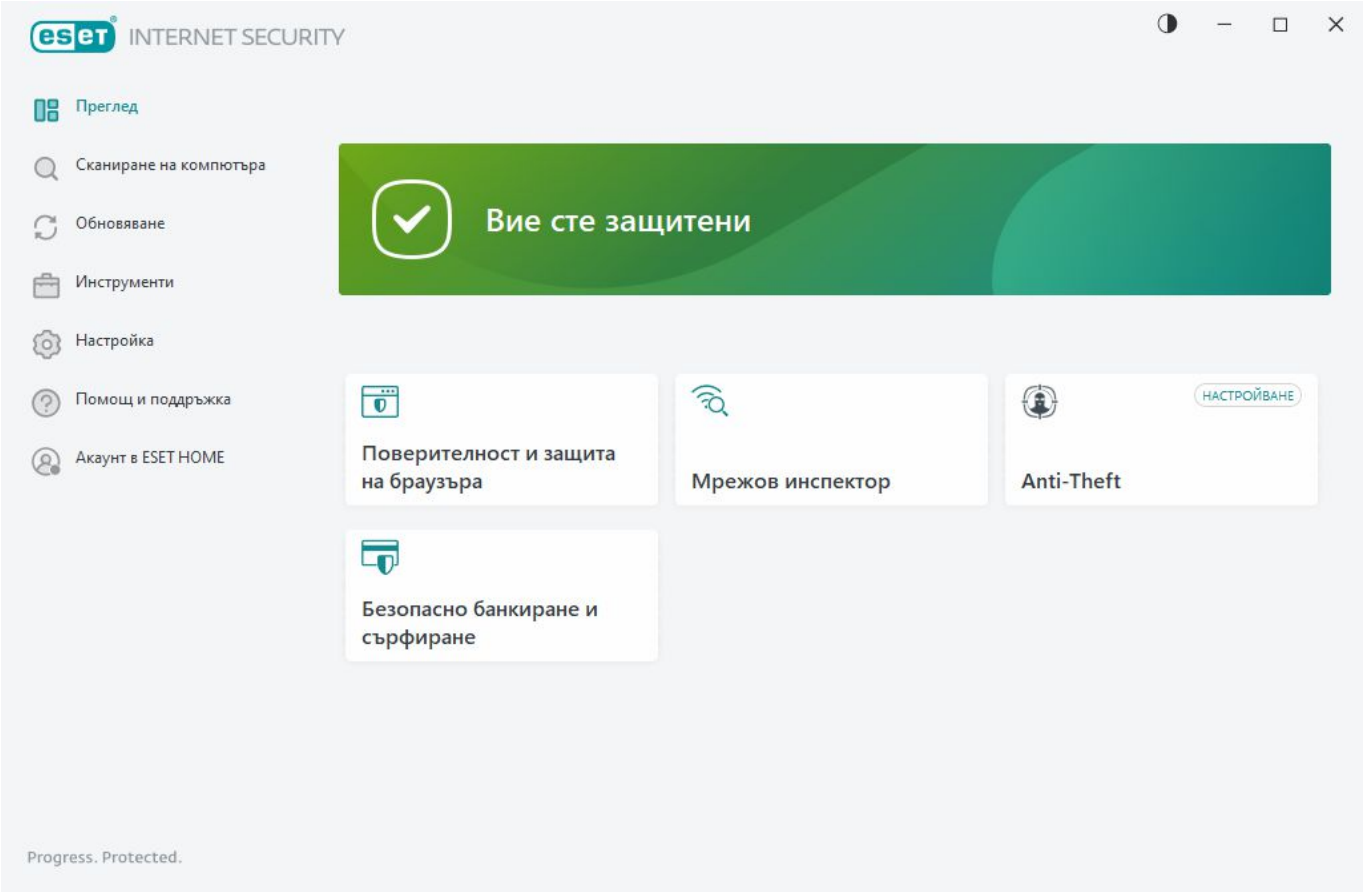
Работа с ESET Internet Security

Главният прозорец на програмата ESET Internet Security е разделен на два раздела. Основният прозорец отдясно показва информация, отговаряща на опцията, избрана в главното меню отляво.

> **Илюстрирани инструкции**
> Вижте Отваряне на главния програмен прозорец на продуктите на ESET за Windows за илюстрирани инструкции, налични на английски и няколко други езика.

Можете да изберете цветовата схема на графичния потребителски интерфейс на ESET Internet Security в горния десен ъгъл на главния прозорец на програмата. Щракнете върху иконата **Цветова схема** (иконата се променя въз основа на текущо избраната цветова схема) до иконата **Намаляване** и изберете цветовата схема от падащото меню:

- **Като цвета на системата** – задава цветовата схема на ESET Internet Security на базата на настройките на операционната система.
- **Тъмна** – ESET Internet Security ще има тъмна цветова схема (тъмен режим).
- **Светла** – ESET Internet Security ще има стандартна, светла цветова схема.



Опции в главното меню:

Преглед – Предоставя информация за състоянието на защита на ESET Internet Security.

Сканиране на компютъра – Конфигурирайте и стартирайте сканиране на компютъра или създайте сканиране по избор.

Обновяване – показва информация за обновявания на модула и системата за засичане.

Инструменти – Осигурява достъп до Мрежов инспектор и други функции, които помагат за опростяване на администрирането на програмата и предлагат допълнителни опции за напреднали потребители.

Настройка – Предоставя опции за конфигуриране за функциите за защита на ESET Internet Security (защита на компютъра, интернет защита, мрежова защита и инструменти за защита) и достъп до Разширени настройки.

Помощ и поддръжка – показва информация относно абонамента ви, инсталирания продукт на ESET и връзки към онлайн помощта, онлайн помощника на ESET и техническата поддръжка.

Акаунт в ESET HOME – свържете устройството си към ESET HOME или прегледайте състоянието на връзката с акаунта в ESET HOME. Използвайте ESET HOME, за да преглеждате и управлявате настройките на Anti-Theft и активираните абонамент и устройства на ESET.

Преглед

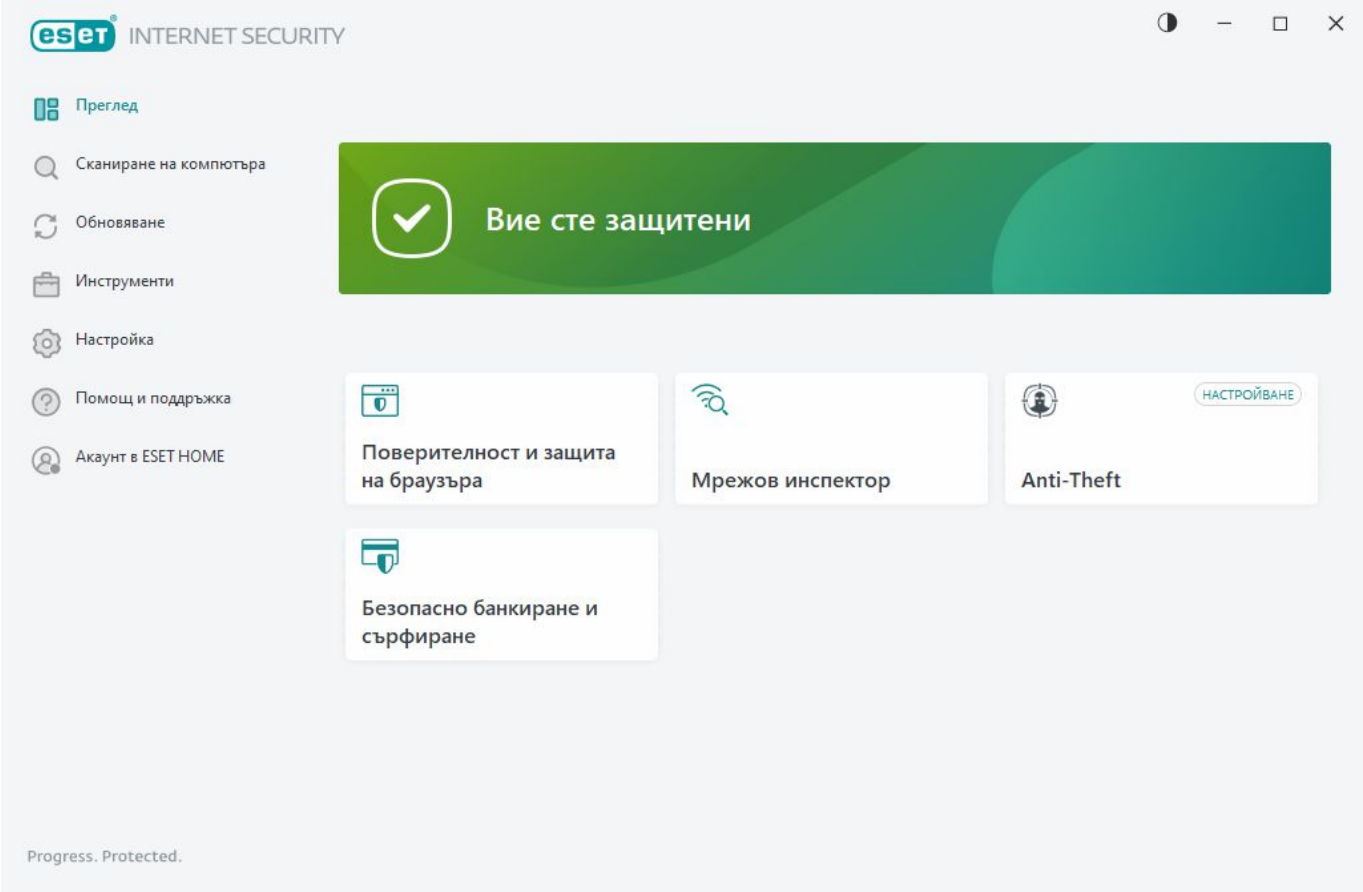
Прозорецът **Преглед** показва информация за текущата защита на вашия компютър заедно с бързи връзки към функциите за сигурност в ESET Internet Security.

Прозорецът **Преглед** показва известия с подробна информация и препоръчителни решения за подобряване на сигурността на ESET Internet Security, включване на допълнителни функции или осигуряване на максимална защита. Ако има повече известия, щракнете върху **Още X известия**, за да разширите всички.

Мрежов инспектор — Проверка на защитата на вашата мрежа

Безопасно банкиране и сърфиране – стартира браузъра, зададен по подразбиране в Windows, в защитен режим.

Anti-Theft – стартира настройката на Anti-Theft. Ако вече сте настроили Anti-Theft, бързата връзка отваря страницата на Anti-Theft.

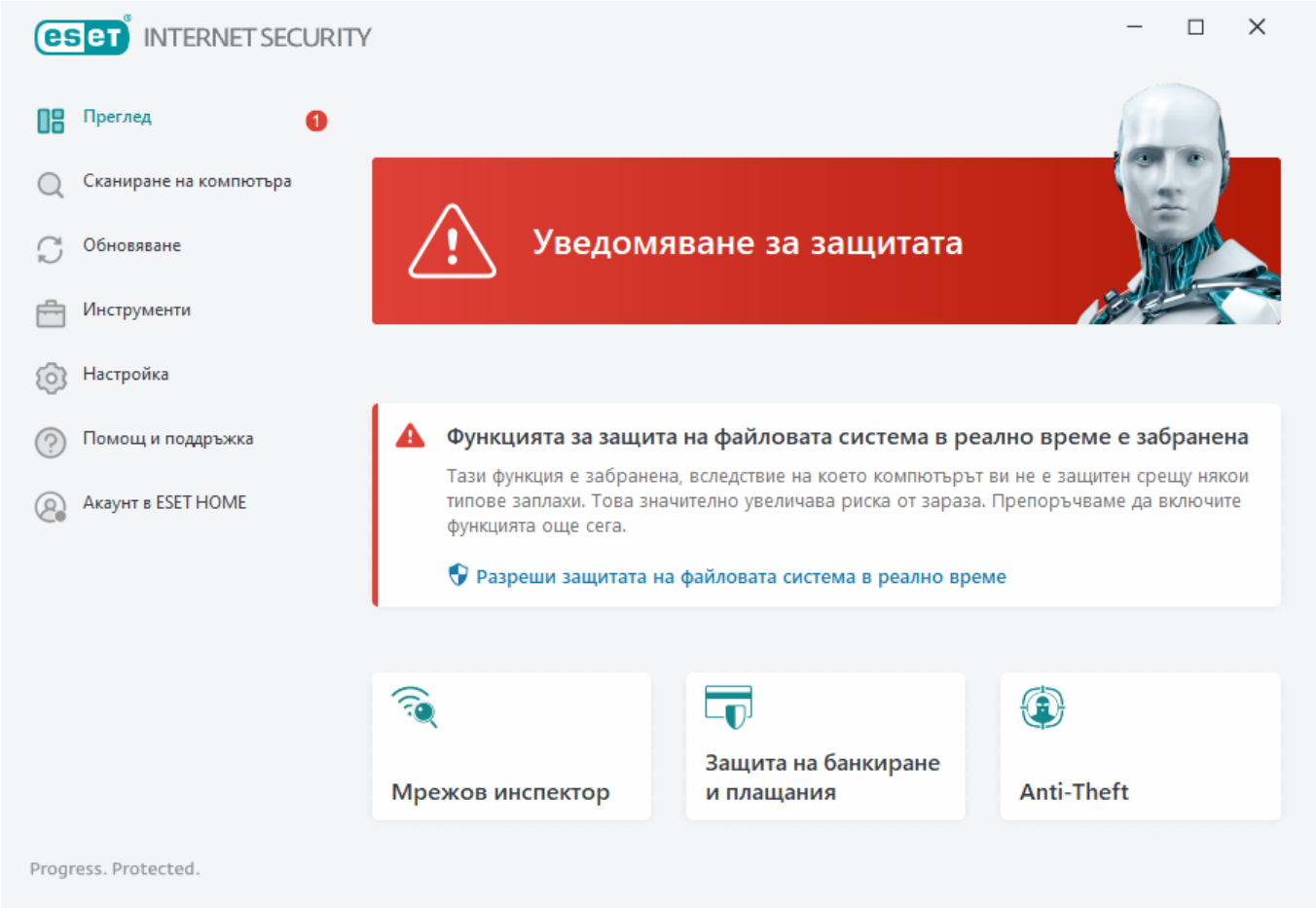


Зелената икона и състоянието **Вие сте защитени** в зелено са индикатори, че е осигурена максималната защита.

Какво да направите, ако програмата не работи правилно

Ако активен модул за защита работи правилно, неговата икона за състояние на защитата ще бъде зелена. Червен удивителен знак или оранжева икона за известие показва, че не е осигурена максимална защита. Допълнителна информация относно състоянието на защита на

всеки модул и предложени решения за възстановяване на пълната защита се показват като известие в прозореца **Преглед**. За да промените състоянието на отделните модули, щракнете върху **Настройка** и изберете желания модул.



Червената икона и състоянието **Уведомяване за защитата** в червено са индикатори за критични проблеми.
Има няколко причини, поради които това състояние може да се покаже, като например:

- **Продуктът не е активиран** или **Абонаментът е изтекъл** – това се обозначава от червена икона за състоянието на защитата. Програмата не може да се обновява, след като абонаментът ви изтече. Изпълнете инструкциите в прозореца с уведомлението, за да подновите абонамента.

- **Системата за откриване не е обновена** – тази грешка ще се покаже след няколко неуспешни опита за обновяване на системата за откриване. Препоръчваме ви да проверите настройките за обновяване. Най-честата причина за тази грешка са неправилно въведени данни за удостоверяване или неправилно конфигурирани настройки за връзка.

- **Функцията за защита на файловата система в реално време е забранена** – Потребителят е забранил защитата в реално време. Вашият компютър не е защитен от заплахи. Щракнете върху **Разрешаване на защитата в реално време**, за да активирате отново тази функция.

- **Защитата от вируси и шпионски софтуер е забранена** – Може да разрешите отново защитата от вируси и шпионски софтуер, като щракнете върху **Разреши защитата от вируси и шпионски софтуер**.

- **Защитната стена на ESET е забранена** – Този проблем също се обозначава чрез известие за защитата до елемента **Мрежа** на работния плот. Можете да разрешите отново мрежовата защита, като щракнете върху **Разреши защитната стена**.

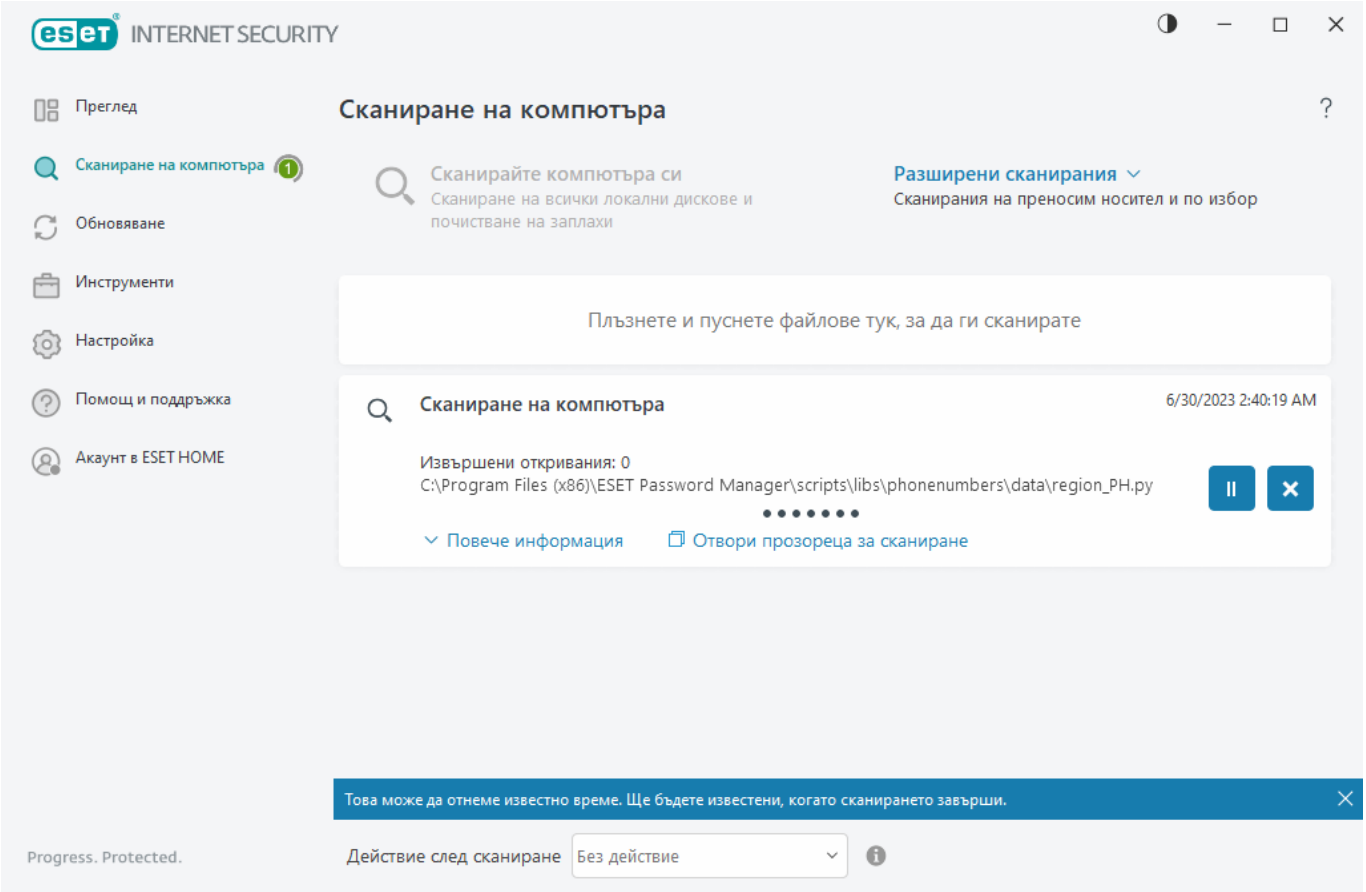
 Оранжевата икона обозначава ограничена защита. Може например да има проблем с обновяването на програмата или абонаментът ви да изтича скоро.
Има няколко причини, поради които това състояние може да се покаже, като например:

- **Предупреждение за оптимизация на системата против кражба** – Това устройство не е оптимизирано за Anti-Theft. Може например на компютъра ви да не е създаден фантомен акаунт (функция за защита, която се активира автоматично, когато обозначите устройство като липсващо). Можете да създадете фантомен акаунт с помощта на функцията Оптимизация в уеб интерфейса на Anti-Theft.
- **Игрален режим е активен** – Разрешаването на игралния режим представлява потенциална заплаха за защитата. Разрешаването на тази функция забранява всички прозорци за известия/уведомления и спира всички планирани задачи.
- **Абонаментът ви изтича скоро/Абонаментът ви изтича днес** – това се означава от иконата за състоянието на защитата чрез показване на удивителен знак до системния часовник. След като абонаментът изтече, програмата няма да може да се обновява и иконата за състоянието на защитата ще стане червена.

Ако не сте в състояние да разрешите даден проблем с помощта на предложените решения, щракнете върху **Помощ и поддръжка**, за да получите достъп до помощните файлове, или потърсете в онлайн помощника на ESET. Ако все още имате нужда от помощ, може да изпратите заявка за поддръжка. Отделът за техническа поддръжка на ESET ще отговори бързо на вашите въпроси и ще ви помогне да намерите решение.

Сканиране на компютъра

Програмата за сканиране при поискване е важна част от антивирусното решение. Тя се използва за сканиране на файлове и папки на компютъра. От гледна точка на сигурността е важно сканиране на компютъра да се извършва редовно като част от рутинните мерки за безопасност, а не само при съмнение за заразяване. Препоръчително е да извършвате редовно задълбочено сканиране на системата с цел откриване на вируси, които не са открити от защитата на файловата система в реално време, когато бъдат записани на диска. Това може да се случи, ако защитата на файловата система в реално време е била забранена в съответния момент, ако система за засичане на потенциално опасни заплахи е остаряла или ако файлът не е разпознат като вирус при записването му на диска.



Налични са два типа на **Сканиране на компютъра**. **Сканиране на компютъра** сканира бързо системата, без да се задават параметри на сканиране. **Сканиране по избор** (под „Разширено сканиране“) ви позволява да избирате от предварително зададени профили за сканиране, предназначени за насочване към определени местоположения, и да избирате определени цели за сканиране.

Вж. раздела Ход на сканирането за повече информация относно процеса на сканиране.

По подразбиране ESET Internet Security се опитва автоматично да почисти или премахне намерените по време на сканирането на компютъра откривания. В някои случаи, ако не може да се извърши действие, получавате интерактивно предупреждение и трябва да изберете действие за почистване (например премахване или игнориране). За да промените нивото на почистване и за по-подробна информация, вижте Почистване. За да прегледате предишни сканирания, вижте Регистрационни файлове.

Сканиране на компютъра

Опцията "**Сканиране на компютъра**" ви позволява бързо стартиране на сканиране на компютъра и почистване на заразените файлове без необходимост от намеса на потребителя. Предимството на опцията "**Сканиране на компютъра**" е в лесната работа и в това, че не се изисква подробно конфигуриране на сканирането. Това сканиране проверява всички файлове на локалните дискове и автоматично почиства или изтрива открити проникванията. Нивото на почистване автоматично се задава на стойността по подразбиране. За по-подробна информация относно типовете почистване вж. раздела Почистване.

Можете също да използвате функцията **Сканиране с плъзгане и пускане**, за да сканирате ръчно файл или папка, като щракнете върху файла или папката, преместите курсора на

мишката до маркираната област, докато държите натиснат бутона на мишката, като след това го пуснете. След това приложението се премества на преден план.

Следните опции за сканиране са налични в **Разширени сканирания**:

 сканиране на избрани файлове

Сканиране на избрани файлове ви позволява да зададете параметри на сканиране, като например цели на сканиране и методи. Предимството на **Сканиране по избор** е, че можете да конфигурирате параметрите подробно. Конфигурациите могат да се запишат в създадени от потребителя профили, които да се използват при често сканиране с едни и същи параметри.

 Сканиране на външни устройства

Подобно на "**Сканиране на компютъра**" – бързо стартиране на сканиране на преносими носители (като например CD/DVD/USB), които в момента са свързани към компютъра. Това може да е полезно при свързване на USB флаш устройство към компютъра, ако желаете да сканирате съдържанието му за злонамерен софтуер и други потенциални заплахи.

Този тип сканиране може също така се стартира чрез щракване върху **Сканиране по избор**, избиране на **Преносим носител** от падащото меню **Цели за сканиране** и щракване върху **Сканиране**.

 Повтаряне на последното сканиране

Позволява ви бързо да стартирате изпълнено по-рано сканиране със същите настройки като преди това.

Падащото меню **Действие след сканиране** ви позволява да зададете действие, което да се извършва автоматично, след като сканирането завърши:

• **Никакво действие** – няма да се извърши никакво действие след приключване на сканирането.

• **Изключване** – компютърът се изключва след приключване на сканирането.

• **Рестартиране, ако е необходимо** – компютърът се рестартира само ако е необходимо, за да завърши почистване на откритите заплахи.

• **Рестартиране** – всички отворени програми се затварят и компютърът се рестартира след приключване на сканирането.

• **Принудително рестартиране, ако е необходимо** – компютърът се рестартира принудително само ако е необходимо, за да завърши почистване на откритите заплахи.

• **Принудително рестартиране** – Принудително затваря всички отворени програми без изчакване на намесата на потребител и рестартира компютъра след приключване на сканирането.

• **Заспиване** – сесията ви се записва и компютърът влиза в състояние на ниска консумация на електроенергия, за да можете бързо да възобновите работата си.

• **Хибернация** – всичко, което се изпълнява в RAM паметта, се премества в специален файл на твърдия диск. Компютърът се изключва, но ще възстанови предходното си състояние, когато го стартирате следващия път.

Действията **Заспиване** и **Хибернация** са налични в зависимост от настройките на операционната система за включване и заспиване на компютъра или възможностите на компютъра/лаптопа. Не забравяйте, че в спящ режим компютърът все още работи. Той продължава да изпълнява основни функции и да използва електричество, когато се захранва от батерията. За да пестите заряда на батерията, когато например пътувате извън офиса, е препоръчително за използвате опцията „Хибернация“.

Избраното действие ще започне след приключване на всички текущи сканирания. Когато изберете **Изключване** или **Рестартиране**, се показва диалогов прозорец за потвърждение на продукта с 30-секундно обратно броене (щракнете върху **Отказ**, за да деактивирате заявеното действие).

Препоръчваме ви да изпълнявате сканиране на компютъра поне веднъж месечно. Сканирането може да се конфигурира като планирана задача от **Инструменти** > **Разписание**. Как да планирам седмично сканиране на компютъра?

Стартираща програма за сканиране по избор

Можете да използвате сканирането на избрани файлове, за да сканирате оперативната памет, мрежата или конкретни части на диска вместо целия диск. За да го направите, щракнете върху **Разширени сканирания** > **Сканиране на избрани файлове** изберете конкретни цели от дървовидната структура на папките.

Може да изберете профил от падащото меню **Профил**, който да се използва при сканиране на определени цели. Профилът по подразбиране е **Smart сканиране**. Има още три предварително зададени профила на сканиране, наречени **Задълбочено сканиране**, **Сканиране от контекстното меню** и **Сканиране на компютъра**. Тези профили за сканиране използват различни параметри на ThreatSense. Наличните опции са описани в Разширени настройки > **Система за засичане** > **Сканирания за злонамерен софтуер** > **Сканиране при поискване** > ThreatSense.

Структурата на папката (дървото) съдържа също така определени цели за сканиране.

• **Оперативна памет** – Сканиране на всички процеси и данни, които се използват в момента от оперативната памет.

• **Сектори за начално стартиране/UEFI** – Сканиране на секторите за начално стартиране и UEFI за наличието на злонамерен софтуер. Прочетете повече за UEFI скенера в речника.

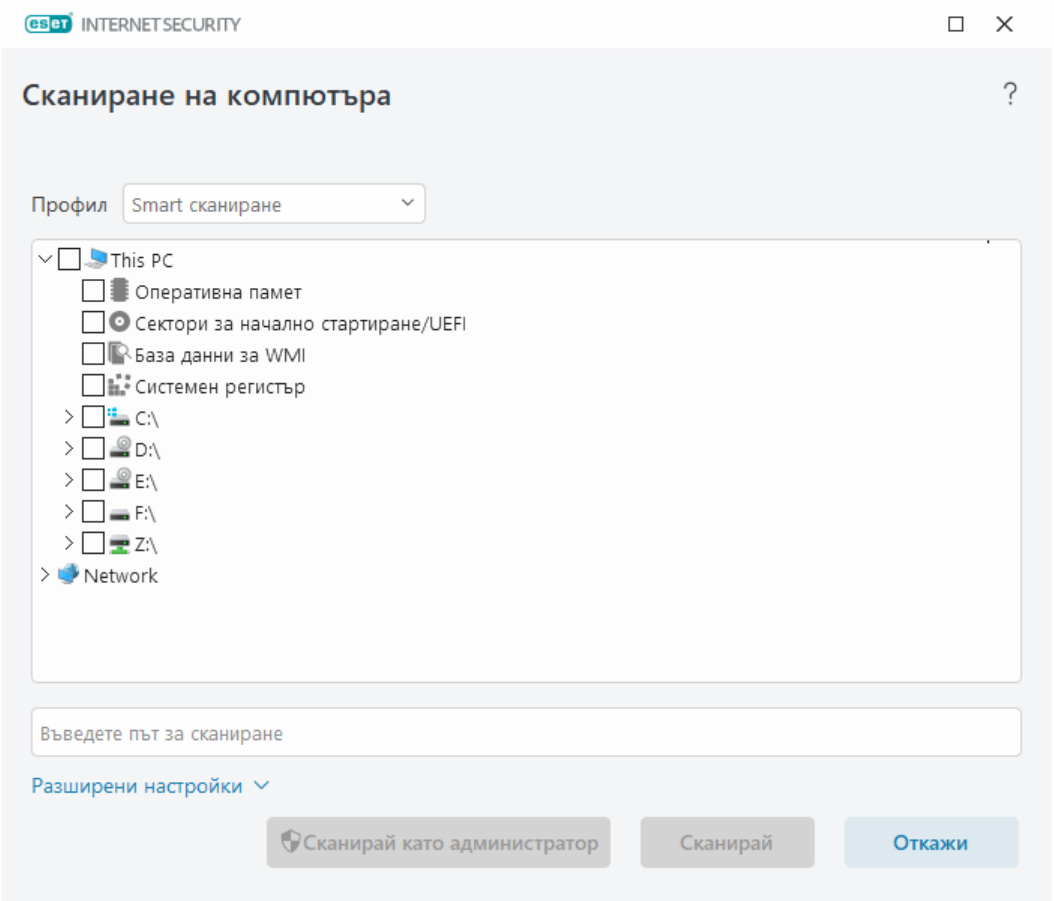
• **WMI база данни** – сканира цялата Windows Management Instrumentation WMI база данни, всички пространства на имената, всички екземпляри на класа и всички свойства. Търсене на препратки към заразени файлове или злонамерен софтуер, вградени като данни.

• **Системен регистър** – Сканиране на целия системен регистър, всички ключове и подключове. Търсене на препратки към заразени файлове или злонамерен софтуер,

вградени като данни. При почистване на откривания препратката остава в регистъра, за да се уверите, че няма да бъдат загубени важни данни.

За да се придвижите бързо до цел за сканиране (файл или папка), въведете пътя й в текстовото поле под дървовидната структура. Пътят е с различаване на малките и главните букви. За да включите целта в сканирането, поставете отметка в квадратчето й в дървовидната структура.

> **Как се планира седмично сканиране на компютъра**
> За да планирате редовна задача, вж. Планиране на седмично сканиране на компютъра.



Можете да конфигурирате параметрите на почистването за сканирането в Разширени настройки > **Система за засичане** > **Сканирания за злонамерен софтуер** > **Сканиране при поискване** > **ThreatSense** > **Почистване**. За да изпълните сканиране без действие за почистване, щракнете върху **Разширени настройки** и изберете **Сканиране без почистване**. Хронологията на сканирането се записва в дневника на сканирането.

Когато е избрана опцията **Игнориране на изключенията**, файловете с разширения, които преди това са били изключени, ще бъдат сканирани без изключение.

Щракнете върху **Сканирай** за извършване на сканиране със зададените параметри по избор.

Опцията **Сканирай като администратор** ви позволява да извършвате сканирането с администраторски акаунт. Използвайте тази опция, ако текущият потребител не разполага с права за достъп до файловете, които искате да сканирате. Този бутон не е наличен, ако текущият потребител не може да извършва UAC операции като администратор.

Можете да прегледате регистрационния файл за сканиране на компютъра, когато сканирането приключи, като щракнете върху Показване на регистрационния файл.

Ход на сканирането

Прозорецът за ход на сканирането показва текущото състояние на сканиране, както и информация за броя файлове, съдържащи злонамерен код.

Нормално е някои файлове, като например файловете, защитени с парола, или файлове, които се използват от системата (обикновено *pagefile.sys* и някои регистрационни файлове), да не могат да се сканират. Можете да намерите повече подробности в нашата статия в онлайн помощника.

Как се планира седмично сканиране на компютъра

За да планирате редовна задача, вж. Планиране на седмично сканиране на компютъра.

Ход на сканирането – Лентата за напредъка показва състоянието на изпълняваното сканиране.

Цел – името на текущо сканирания обект и неговото местоположение.

Възникнаха откривания – Показва общия брой на сканираните файлове, откритите заплахи и изчистените заплахи по време на сканиране.

Щракнете върху „Повече информация“, за да се покаже следната информация:

- **Потребител** – Име на потребителския акаунт, който е стартирал сканирането.
- **Сканирани обекти** – Брой вече сканирани обекти.
- **Продължителност** – Изминало време.

Икона за пауза – Поставя на пауза сканирането.

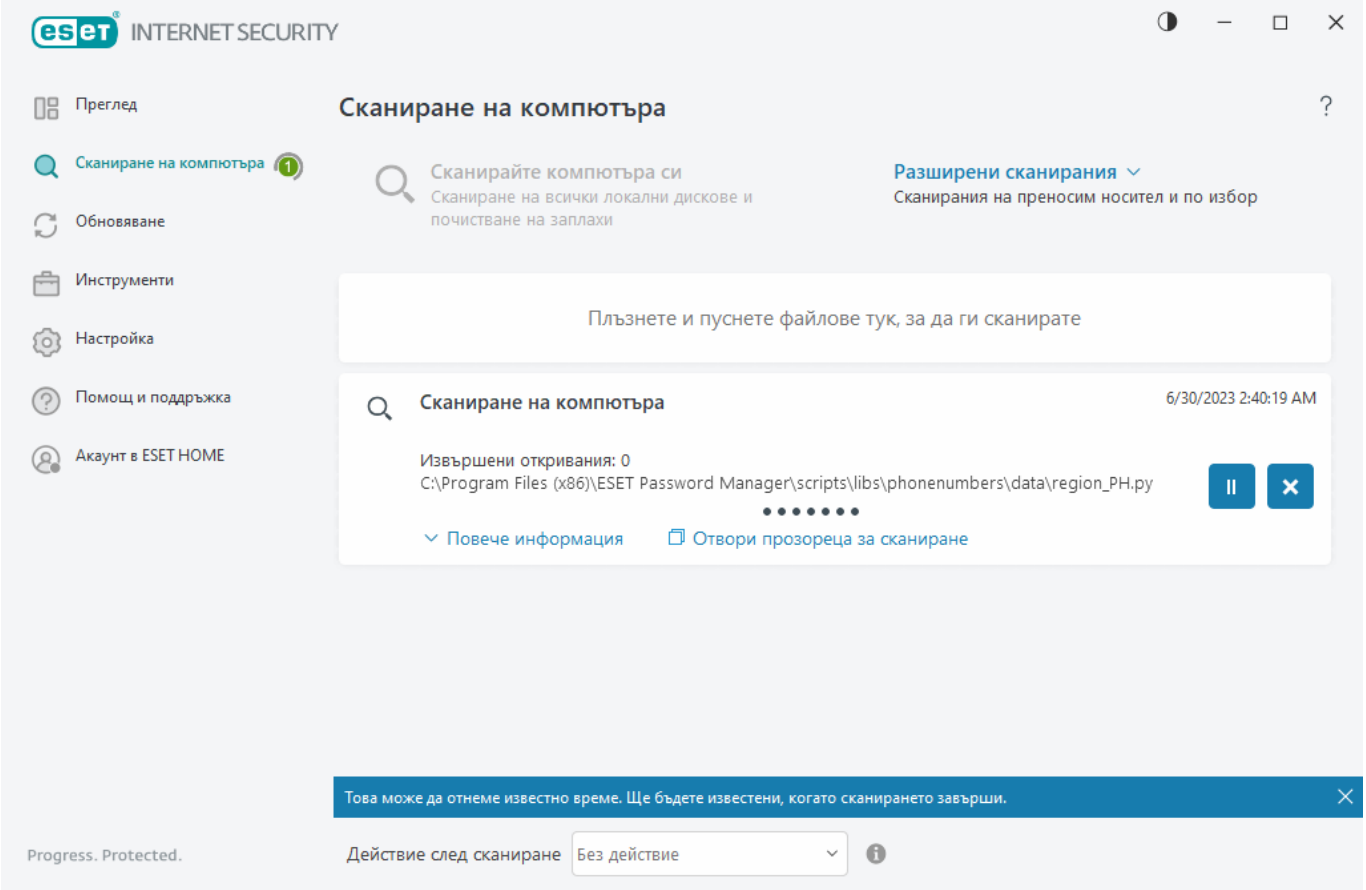
Икона за възобновяване – Тази опция става видима, когато сканирането е спряно временно. Щракнете върху иконата, за да продължите сканирането.

Икона за спиране – Прекратява сканирането.

Щракнете върху **Отваряне на прозореца за сканиране**, за да отворите Дневник на сканиране на компютъра с повече подробности за сканирането.

Превъртане на регистрационния файл за сканиране – ако тази опция е разрешена, регистрационният файл за сканиране ще се превърти надолу автоматично при добавянето на нови записи, така че да се показват най-новите записи.

Щракнете върху лупата или стрелката, за да видите подробни данни за сканирането, което се изпълнява в момента. Може да изпълните друго паралелно сканиране, като щракнете върху **Сканиране на компютъра** или **Разширени сканирания** > **Сканиране по избор**.



Падащото меню **Действие след сканиране** ви позволява да зададете действие, което да се извършва автоматично, след като сканирането завърши:

• **Никакво действие** – няма да се извърши никакво действие след приключване на сканирането.

• **Изключване** – компютърът се изключва след приключване на сканирането.

• **Рестартиране, ако е необходимо** – компютърът се рестартира само ако е необходимо, за да завърши почистване на откритите заплахи.

• **Рестартиране** – всички отворени програми се затварят и компютърът се рестартира след приключване на сканирането.

• **Принудително рестартиране, ако е необходимо** – компютърът се рестартира принудително само ако е необходимо, за да завърши почистване на откритите заплахи.

• **Принудително рестартиране** – Принудително затваря всички отворени програми без изчакване на намесата на потребител и рестартира компютъра след приключване на сканирането.

• **Заспиване** – сесията ви се записва и компютърът влиза в състояние на ниска консумация на електроенергия, за да можете бързо да възобновите работата си.

• **Хибернация** – всичко, което се изпълнява в RAM паметта, се премества в специален файл на твърдия диск. Компютърът се изключва, но ще възстанови предходното си състояние, когато го стартирате следващия път.

Действията **Заспиване** и **Хибернация** са налични в зависимост от настройките на операционната система за включване и заспиване на компютъра или възможностите на компютъра/лаптопа. Не забравяйте, че в спящ режим компютърът все още работи. Той продължава да изпълнява основни функции и да използва електричество, когато се захранва от батерията. За да пестите заряда на батерията, когато например пътувате извън офиса, е препоръчително за използвате опцията „Хибернация“.

Избраното действие ще започне след приключване на всички текущи сканирания. Когато изберете **Изключване** или **Рестартиране**, се показва диалогов прозорец за потвърждение на продукта с 30-секундно обратно броене (щракнете върху **Отказ**, за да деактивирате заявеното действие).

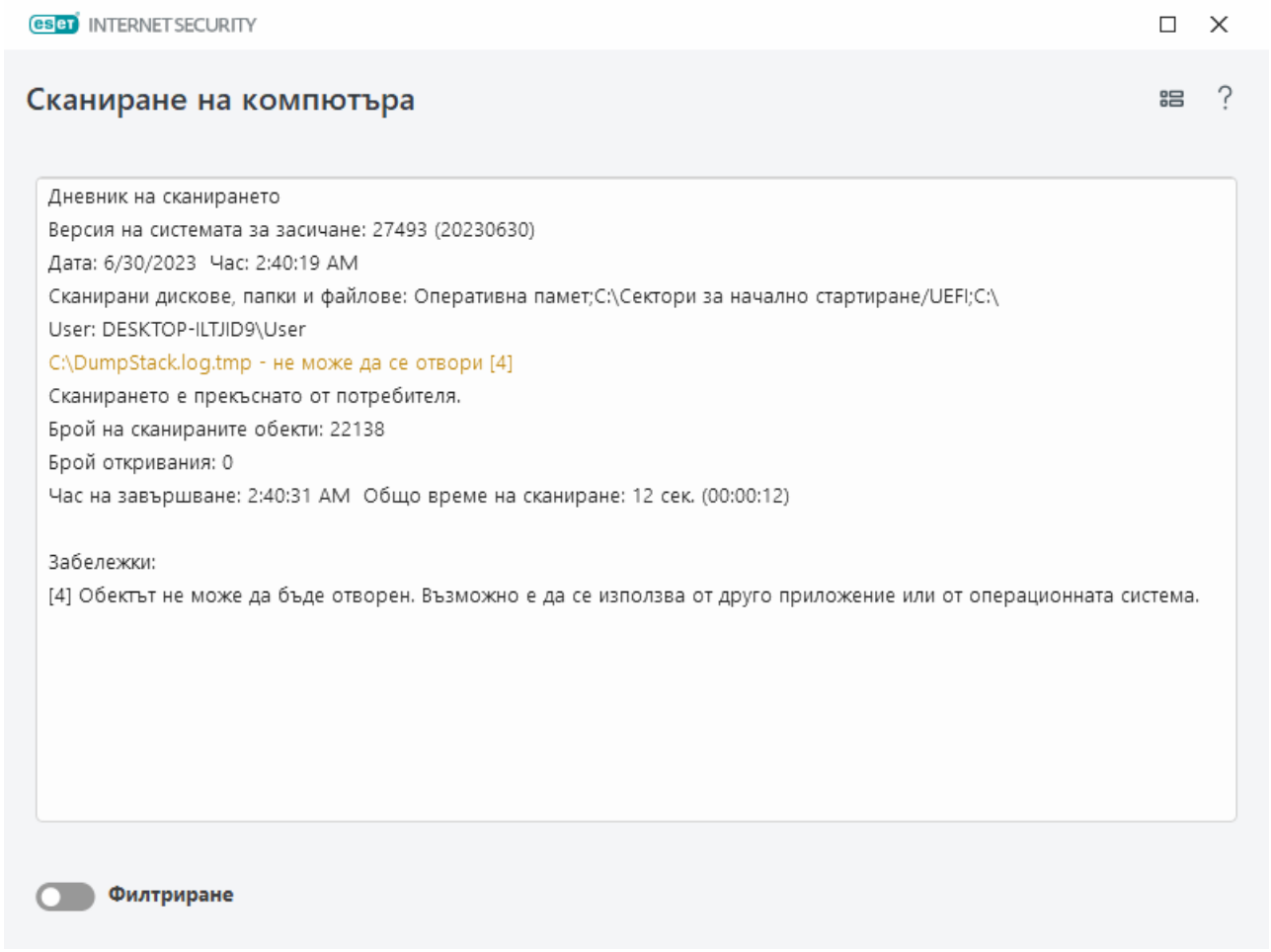
Регистрационен файл за сканиране на компютъра

Можете да видите подробна информация, свързана с конкретно сканиране, в Регистрационни файлове. Дневникът на сканирането съдържа следната информация:

- Версия на система за засичане на потенциално опасни заплахи
- Дата и час на стартиране
- Списък със сканираните дискове, папки и файлове
- Име на планирано сканиране (само за планирано сканиране)
- Потребител, който е стартирал сканирането.
- Състояние на сканиране
- Брой на сканираните обекти
- Брой направени откривания
- Час на завършване
- Общо време на сканиране

Ново стартиране на планирана задача за сканиране на компютъра се пропуска, ако същата планирана задача, която е изпълнена по-рано, все още се изпълнява. Пропуснатата задача за планирано сканиране ще създаде дневник на сканирането на компютъра с 0 сканирани обекта и състояние **Сканирането не започна, защото предишното сканиране все още се изпълняваше**.

За да намерите дневници на предишни сканирания, в главното меню изберете **Инструменти** > **Регистрационни файлове**. В падащото меню изберете **Сканиране на компютъра** и щракнете двукратно върху желания запис.



За да научите повече за записите „не може да се отвори“, „отваряне на грешка“ и/или „повреден архив“, вижте нашата статия в онлайн помощника на ESET.

Щракнете върху иконата на плъзгача **Филтриране** , за да отворите прозореца Филтриране на регистрационни файлове, където можете да стесните търсенето с критерии по избор. За да разгледате контекстното меню, щракнете с десен бутон върху определен запис в дневника:

Действие	Използване
Филтрирай еднакви записи	Активира филтрирането на дневници. Дневникът ще покаже само записи от типа, който е избраният запис.
Филтър	Тази опция отваря прозореца за филтриране на дневници и ви позволява да зададете критерии за определени записи в дневника. Пряк път: `Ctrl+Shift+F`
Разрешаване на филтър	Активира настройките на филтъра. Ако активирате филтъра за първи път, първо трябва да зададете настройки, след което прозорецът за филтриране на дневници се отваря.
Забрани филтър	Изключва филтъра (подобно на щракване върху превключвателя в долната част).
Копирай	Копира маркирания/те запис(и) в клипборда. Пряк път: `Ctrl+C`
Копиране на всички	Копира всички записи в прозореца.
Експортиране	Експортира маркирания/те запис(и) в клипборда в XML файл.
Експортиране на всички	Тази опция експортира всички записи в прозореца в XML файл.

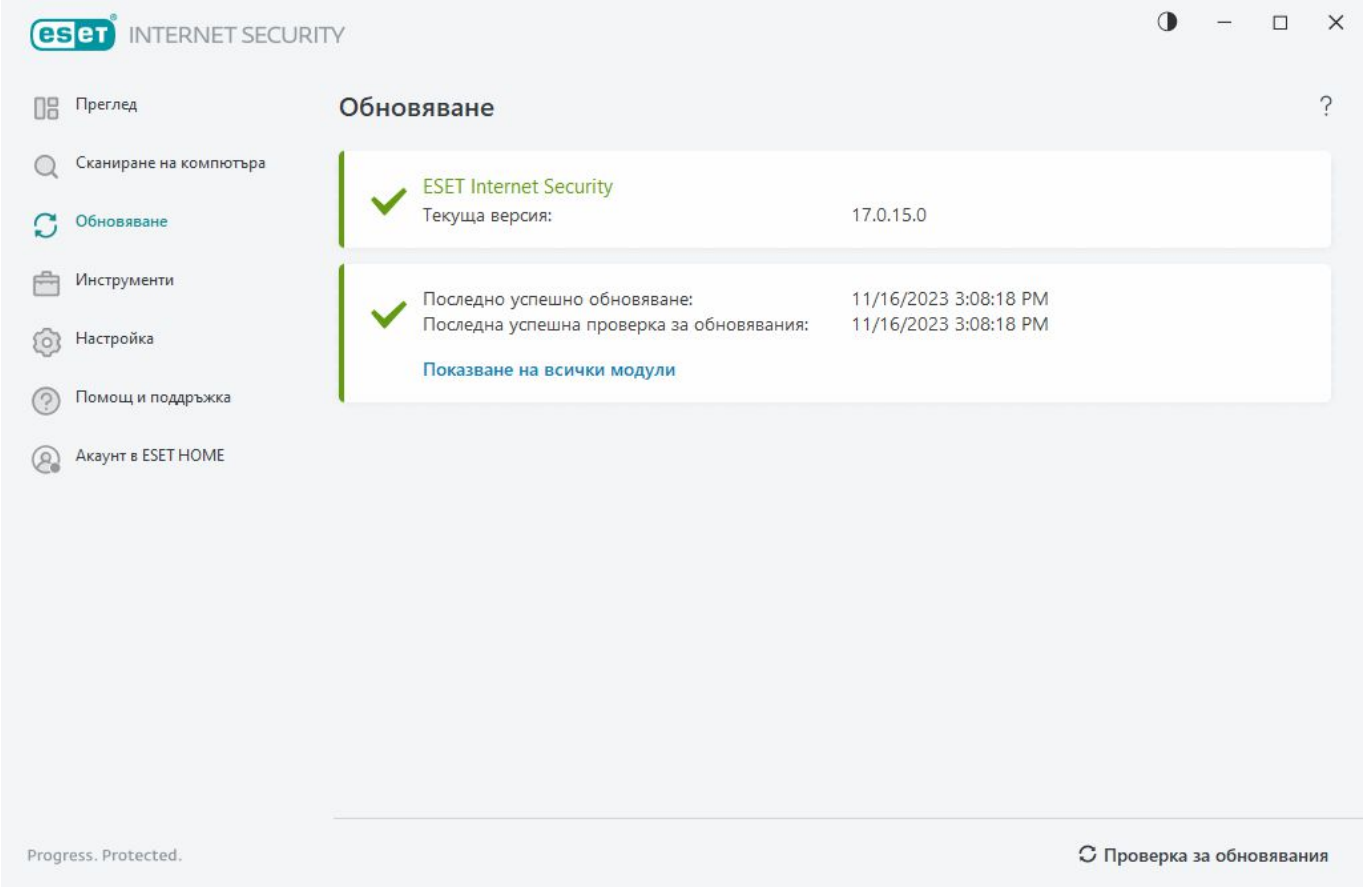
Действие	Използване
Описание на откриването	Отваря енциклопедията за заплахи на ESET, която съдържа подробна информация за опасностите и симптомите на подчертаното проникване.

Обновяване

Редовното обновяване на ESET Internet Security е най-добрият метод за гарантиране на максимално ниво на защита за компютъра. Модулът за обновяване гарантира, че и програмните модули, и системните компоненти са винаги обновени.

Чрез щракване върху **Обнови** в главния прозорец на програмата можете да разберете текущото състояние на обновяване, а също така датата и часа на последното успешно обновяване, както и дали е необходимо обновяване.

В допълнение към автоматичните обновявания можете да щракнете върху **Проверка за обновявания**, за да задействате ръчно обновяване. Редовното обновяване на програмните модули и компоненти е важен аспект от поддръжката на пълна защита срещу злонамерен код. Обърнете внимание на техните конфигуриране и работа. Трябва да активирате продукта с помощта на ключ за активиране, за да можете да получавате обновявания. Ако не сте направили това по време на инсталирането, ще трябва да активирате ESET Internet Security, за да имате достъп до сървърите за обновяване на ESET. Вашият ключ за активиране ви е изпратен в имейл съобщение от ESET след закупуването на ESET Internet Security.



Текуща версия – Показва номера на версията на текущата версия на продукта, който сте инсталирали.

Последно успешно обновяване – Показва датата на последното успешно обновяване. Ако не виждате скорошна дата, вашите програмни модули може да не са актуални.

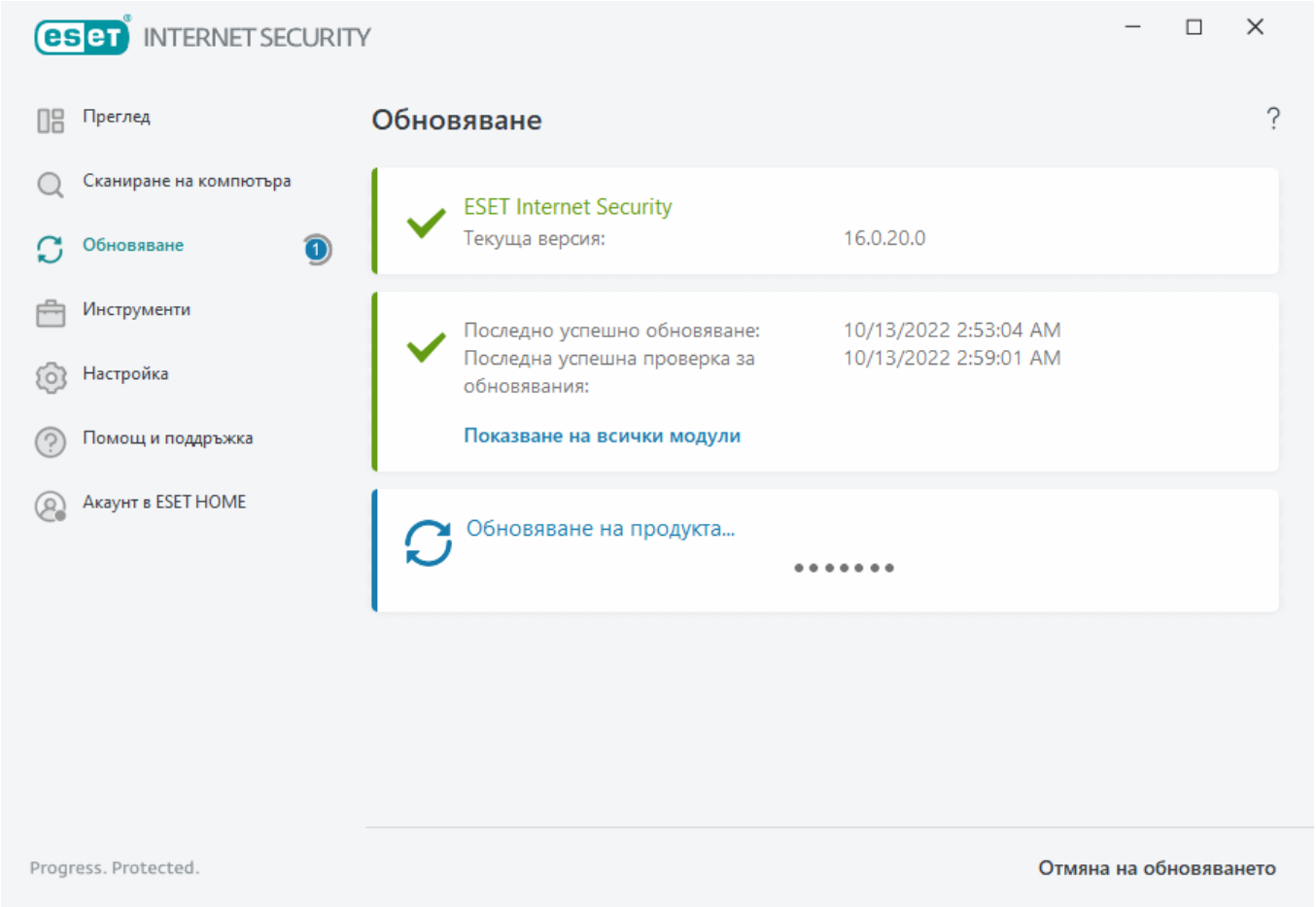
Последна успешна проверка за обновявания – Показва датата на последната успешна проверка за обновявания.

Показване на всички модули – Показва списъка с инсталирани програмни модули.

Щракнете върху **Проверка за обновявания**, за да проверите за най-новата налична версия на ESET Internet Security.

Процес на обновяване

След като щракнете върху **Проверка за обновявания**, изтеглянето ще започне. Ще се покаже лента за хода на изтеглянето и оставащото време. За да прекъснете обновяването, щракнете върху **Откажи обновяването**.



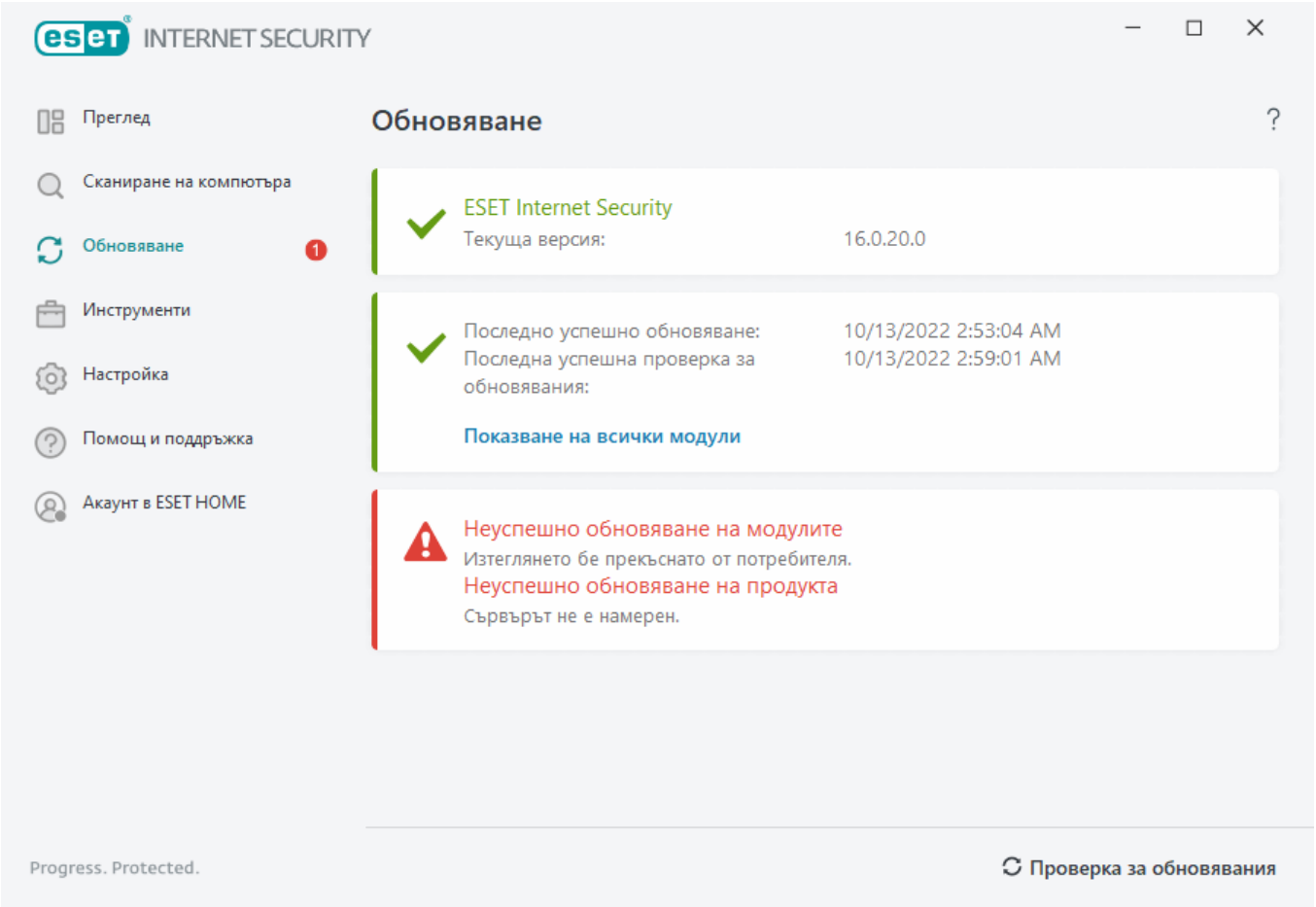
При нормални обстоятелства ще видите зелена отметка в прозореца **Обновяване**, показваща, че програмата е обновена. Ако не видите зелена отметка, програмата е остаряла и е по-уязвима към заразяване. Обновете програмните модули възможно най-скоро.

Неуспешно обновяване

Ако получите съобщение, че обновяването на модулите е било неуспешно, може да е причинено от следните проблеми:

1. **Невалиден абонамент** – абонаментът, използван за активиране, е невалиден или е изтекъл. В главния прозорец на програмата щракнете върху **Помощ и поддръжка** > **Промяна на абонамент** и активирайте продукта си.

2. **Възникна грешка при изтеглянето на файловете за обновяване** – Това може да се дължи на неправилни настройки на интернет връзката. Препоръчително е да проверите връзката с интернет (например, като отворите произволен уеб сайт в браузъра). Ако уеб сайтът не се отвори, вероятно няма връзка с интернет или има проблеми с връзката на компютъра. Обърнете се към интернет доставчика, ако нямате активна връзка с интернет.



Трябва да рестартирате компютъра след успешно обновяване на ESET Internet Security до по-нова версия на продукт, за да гарантирате, че всички програмни модули са обновени правилно. Не е задължително да рестартирате компютъра след редовните актуализации на модули.

За повече информация посетете Отстраняване на неизправности за съобщението „Неуспешно обновяване на модулите“.

Диалогов прозорец – Изисква се рестартиране

Необходимо е рестартиране на компютъра след обновяване на ESET Internet Security до нова версия. Нови версии на ESET Internet Security се издават за внедряване на подобрения или коригиране на проблеми, които автоматичните обновявания на програмните модули не могат да разрешат.

Новата версия на ESET Internet Security може да се инсталира автоматично в зависимост от настройките за обновяване на програмата или ръчно чрез изтегляне и инсталиране на по-нова версия върху предишната.

Щракнете върху **Рестартирай сега**, за да рестартирате компютъра. Ако планирате да рестартирате компютъра си по-късно, щракнете върху **Напомни ми по-късно**. По-късно можете да рестартирате компютъра ръчно от раздел **Преглед** в главния прозорец на програмата.

Как се създават задачи за обновяване

Обновяванията може да се активират ръчно чрез щракване върху **Проверка за обновявания** в основния прозорец, който се показва след щракване върху **Обновяване** от главното меню.

Обновяванията могат да се изпълнят също така и като планирани задачи. За да конфигурирате дадена планирана задача, щракнете върху **Инструменти** > **Планировчик**. По подразбиране се активират следните задачи за обновяване в ESET Internet Security:

- **Редовно автоматично обновяване**
- **Автоматично обновяване след влизане на потребителя**

Всяка задача за обновяване може да се промени според вашите нужди. Освен задачите за обновяване по подразбиране можете да създавате нови задачи с персонализирана конфигурация. За повече подробности относно създаването и конфигурирането на задачи за обновяване вж. раздела Планировчик.

Инструменти

Менюто **Инструменти** включва функции, които предлагат допълнителна защита и помагат за опростяване на администрирането на ESET Internet Security. Налични са следните инструменти:

 Регистрационни файлове

 Изпълняващи се процеси (ако технологията ESET LiveGrid® е разрешена в ESET Internet Security)

 Отчет за защитата

Мрежови връзки (ако Защитна стена е разрешена в ESET Internet Security)

ESET SysInspector

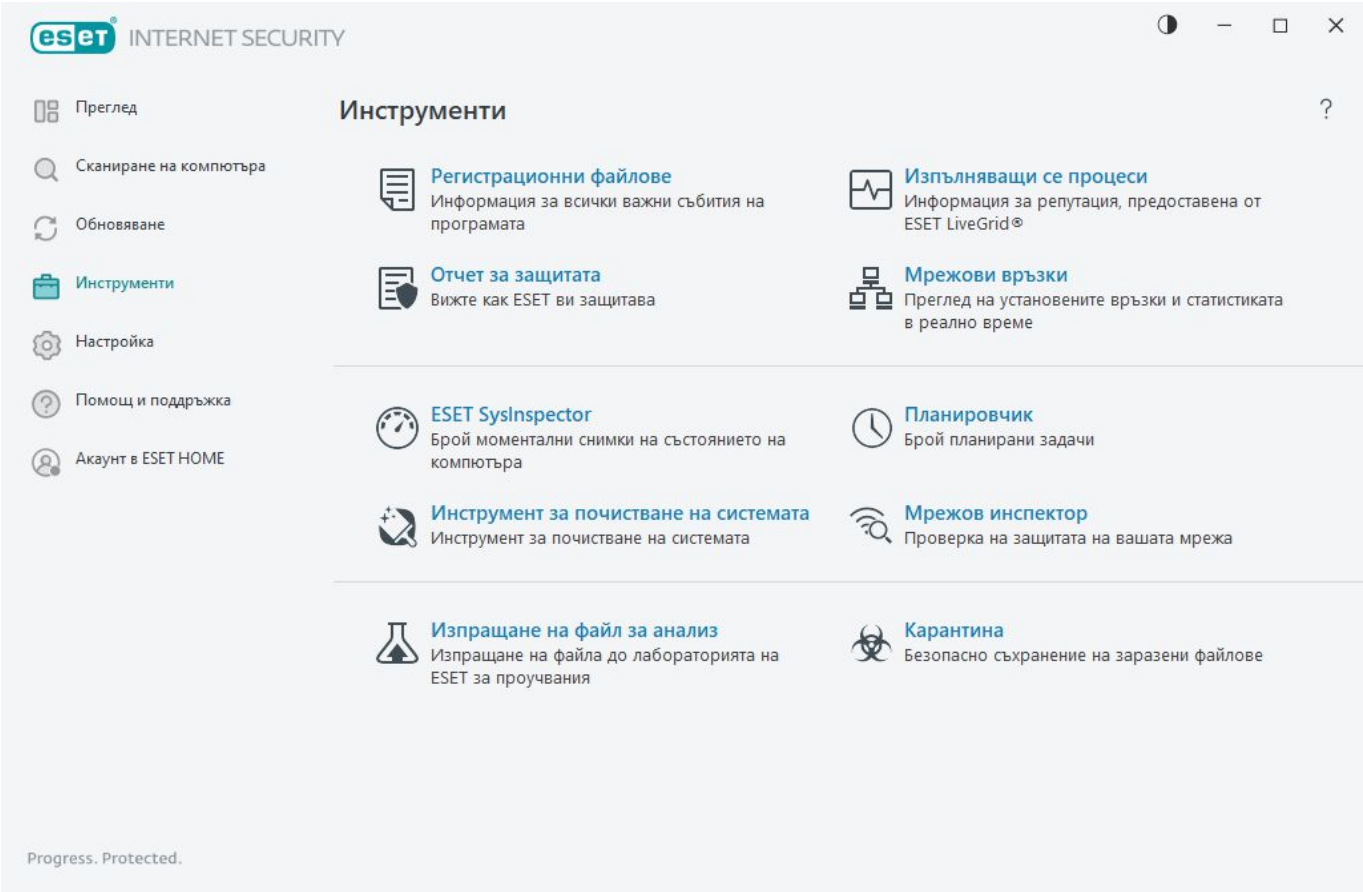
Планировчик

Инструмент за почистване на системата

Мрежов инспектор

Изпращане на файл за анализ (може да не е достъпно в зависимост от вашата конфигурация на ESET LiveGrid®).

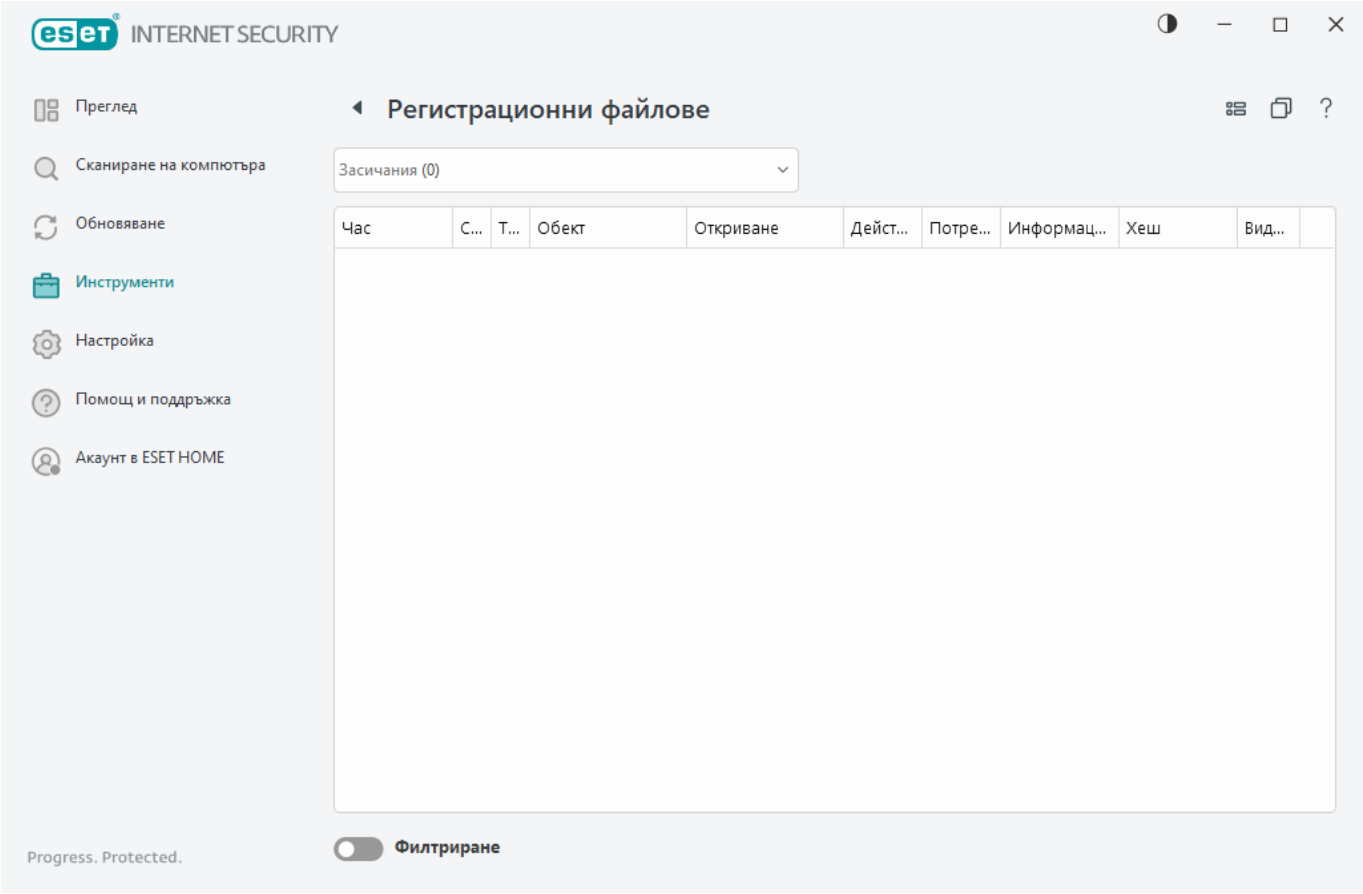
Карантина



Регистрационни файлове

Регистрационните файлове съдържат информация за важни програмни събития, както и обобщение на откритите заплахи. Регистрирането работи като основен инструмент за анализ на системата, откриване на заплахи и отстраняване на неизправности. Регистрирането се изпълнява активно във фонов режим без необходимост от намеса на потребителя. Информацията се записва на базата на текущите настройки за детайлност на регистрационните файлове. Можете да преглеждате текстовите съобщения и

регистрационните файлове директно от средата на ESET Internet Security, както и да архивирате регистрационните файлове.



В регистрационните файлове можете да влезете от главния прозорец на програмата, като щракнете върху **Инструменти** > **Регистрационни файлове**. Изберете желания тип регистрационен файл от падащото меню:

• **Засичания** – Този дневник съдържа подробна информация за засичанията и проникванията, открити от ESET Internet Security. Информацията в дневника включва часа на откриване, типа на скенера, типа на обекта, местоположението на обекта, името на засичането, извършеното действие, името на потребителя, който е бил влязъл в момента на откриване на проникването, хеша и първото появяване. Непочистените прониквания винаги се маркират с червен текст на светлочервен фон. Почистените прониквания се маркират с жълт текст на бял фон. Непочистените ПНП, или потенциално опасни приложения, се маркират с жълт текст на бял фон.

• **Събития** – всички важни действия, извършвани от ESET Internet Security, се записват в регистрационния файл за събитията. Регистрационният файл за събития съдържа информация за събитията и грешките, които са възникнали в програмата. Той е предназначен за решаване на проблеми от системни администратори и потребители. Обикновено информацията в него може да ви помогне да откриете решение на възникнал в програмата проблем.

• **Сканиране на компютъра** – Резултатите от всички предишни сканирания се показват в този прозорец. Всеки ред съответства на едно сканиране на компютъра. Щракнете двукратно върху някой запис, за да прегледате подробностите за съответното сканиране.

• **HIPS** – Съдържа записи на конкретни HIPS правила, които са маркирани за записване.

Протоколът показва приложението, активирало операцията, резултата (разрешено или забранено е било правилото) и името на правилото.

• **Защита на браузъра** – съдържа записи на непроверени/ненадеждни файлове, заредени в браузъра.

• **Мрежова защита** – дневникът за мрежова защита показва всички отдалечени атаки, открити от защитната стена, защитата от мрежови атаки (IDS) и защитата от ботнет мрежи. Тук ще намерите информация за всяка атака срещу компютъра. В колоната Събитие са изброени открититe атаки. Колоната Източник предоставя повече информация за потребителя, осъществяващ атаката. Колоната Протокол разкрива комуникационния протокол, използван за атаката. Анализът на дневника за мрежовата защита може да ви помогне да откриете опитите за проникване в системата навреме, за да предотвратите неупълномощения достъп до нея. За повече информация относно мрежовите атаки вж. IDS и разширени опции.

• **Филтрирани уеб сайтове** –Този списък е полезен, ако искате да видите списък с уеб сайтове, които са били блокирани от Защита на уеб достъпа или Родителски контрол.Всеки регистрационен файл включва часа, URL адреса, потребителя и приложението, които са създали връзка с конкретен уеб сайт.

• **Антиспам на имейл клиенти** – Съдържа записи, свързани с имейл съобщенията, маркирани като спам.

• **Родителски контрол** – Показва уеб страниците, блокирани или разрешени от родителския контрол. Колоните Тип съвпадение и Стойности за съвпадение ви показват как са били приложени правилата за филтриране.

• **Управление на устройства** – Съдържа записи на преносимите носители и устройства, които са били свързани с компютъра. Само устройства със съответни правила за управление на устройството ще бъдат записани в регистрационния файл. Ако правилото не съответства на свързано устройство, няма да бъда създаден запис в регистрационния файл за свързаното устройство. Можете също да прегледате подробности, като например тип, сериен номер, име на доставчик и размер на устройството (ако са налични).

• **Защита на уеб камерата** – Съдържа записи за приложенията, блокирани от защитата на уеб камерата.

Изберете съдържанието на който и да е дневник и натиснете **CTRL + C** , за да го копирате в клипборда. Задръжте **CTRL** или **SHIFT**, за да изберете няколко записа.

Щракнете върху **Филтриране**, за да отворите прозореца Филтриране на регистрационни файлове, където можете да зададете критериите за филтриране.

Щракнете с десен бутон върху конкретен запис, за да отворите контекстното меню. Следните опции са налични в контекстното меню:

• **Покажи** – показване на по-подробна информация за избрания регистрационен файл в нов прозорец.

• **Филтрирай еднакви записи** – след активиране на този филтър ще се показват само записи от един и същи тип (диагностика, предупреждения и т.н.).

• **Филтриране** – след като щракнете върху тази опция, прозорецът Филтриране на дневници ще ви позволи да зададете критерии за филтриране на определени записи в дневниците.

• **Разреши филтъра** – активиране на настройките на филтъра.

• **Забрани филтър** – изтриване на всички настройки за филтриране (както е описано по-горе).

• **Копирай/копирай всички** – Копира информация за избраните записи в прозореца.

• **Копиране на клетка** – копира съдържанието на клетка, върху която е щракнато с десен бутон.

• **Изтрий/изтрий всички** – Изтрива избраните записи или всички показани записи. Това действие изисква права на администратор.

• **Експортирай/експортирай всички** – Експортира информация за избраните записи в XML формат.

• **Намери/Намери следващ/Намери предишен** – След като щракнете върху тази опция, можете да определите критерии за филтриране, за да подчертаете конкретния запис, като използвате прозореца за филтриране на дневници.

• **Описание на откриването** – Отваря енциклопедията за заплахи на ESET, която съдържа подробна информация за опасностите и симптомите на регистрираното проникване.

• **Създаване на изключение** – създава ново изключение от откриване с помощта на съветник (Не е налично за откривания на злонамерен софтуер).

• **Добавяне към списъка с разрешени за защита на браузъра** – отваря прозореца Списък с разрешени за защита на браузъра и добавя елемента към списъка.

Филтриране на регистрационни файлове

Щракнете върху **Филтриране** в **Инструменти** > **Регистрационни файлове** за определяне на критерии за филтриране.

Функцията за филтриране на дневници ще ви помогне да намерите информацията, която търсите особено когато има много записи. Тя ви позволява да стесните списъка със записи в дневника, ако например търсите определен тип събитие, състояние или времеви период. Можете филтрирате записи в дневника, като зададете определени опции на търсенето. Само записи, които са подходящи (според тези опции за търсене) ще бъдат показани в прозореца за регистрационни файлове.

Въведете ключовата дума, която търсите в полето **Търси текст**. Използвайте падащото меню **Търси по колони**, за да конкретизирате търсенето си. Изберете един или повече записи от падащото меню **Типове записи в дневника**. Задайте **Времеви период**, от който искате резултатите да бъдат показани. Можете също да използвате допълнителни опции за търсене, като например **Съвпадение само на цели думи** или **С различаване на малки и големи букви**.

Търси текст

Въведете низ (дума или част от дума). Само записи, които съдържат този низ ще бъдат показани. Другите записи ще бъдат пропуснати.

Търси по колони

Изберете кои колони ще бъдат взети под внимание по време на търсенето. Може да маркирате една или много колони, които да бъдат използвани за търсенето.

Типове записи

Изберете един или повече типове записи в дневника от падащото меню:

• **Диагностични** – Регистрира информация, необходима за прецизна настройка на програмата, и всички записи по-горе.

• **Информативни** – регистриране на информативни съобщения, включително съобщения за успешно обновяване и всички записи по-горе.

• **Предупреждения** – регистриране на съобщения за критични грешки и предупреждения.

• **Грешки** – грешките от типа на "Грешка при изтегляне на файл" и критичните грешки се записват.

• **Критични** – регистриране само на критични грешки (грешка в стартирането на антивирусната защита.

Времеви период

Укажете времевия период, от който искате да се показват резултатите:

• **Неопределено** (по подразбиране) – не търси във времеви период, търси в целия дневник.

• **Последен ден**

• **Последната седмица**

• **Последния месец**

• **Времеви период** – може да укажете точния времеви период (От: и До:) за филтриране само на записите от указания времеви период.

Съвпадение само на цели думи

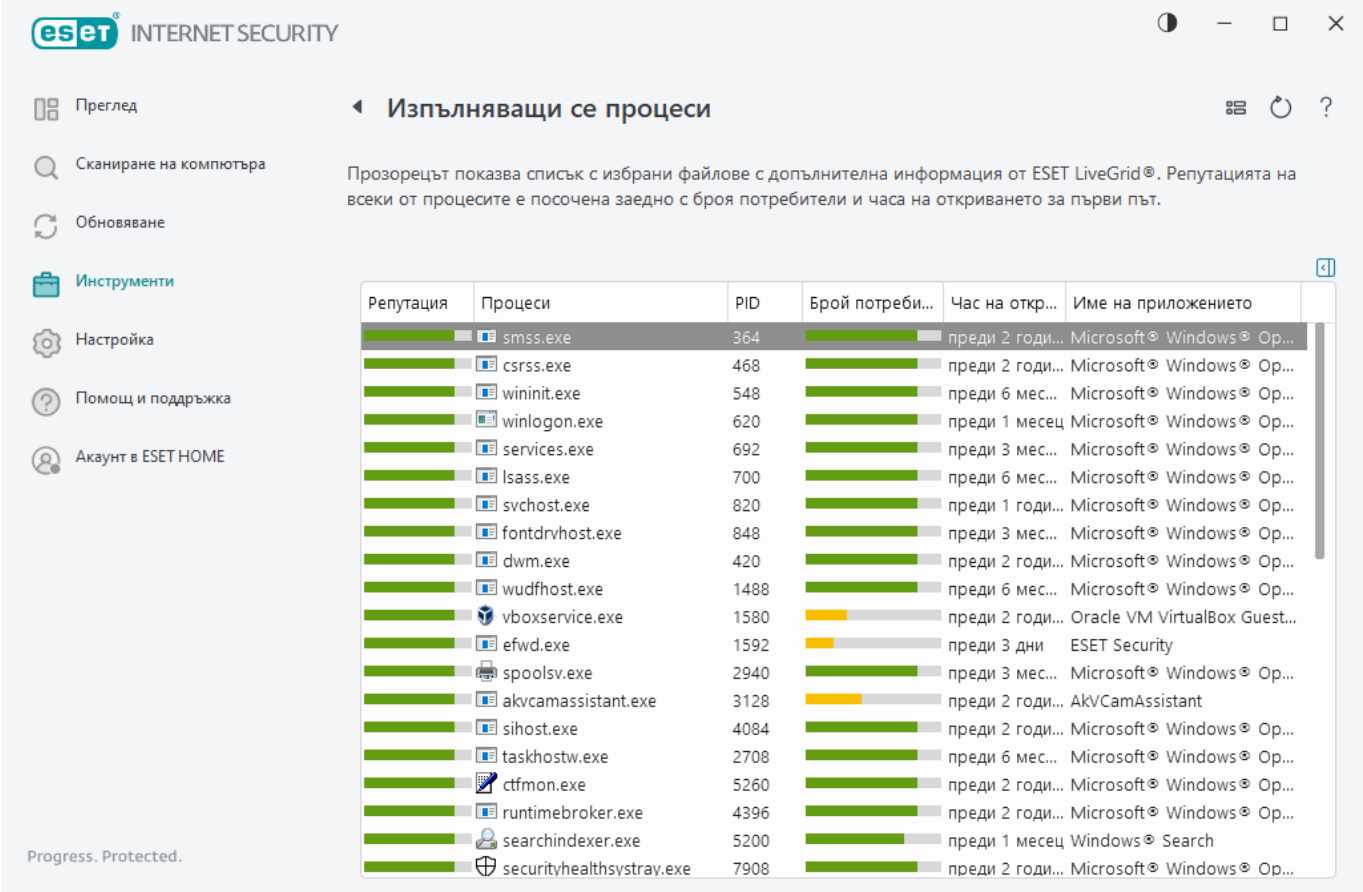
Използвайте квадратчето за отметка, ако искате да търсите конкретни цели думи за по-точни резултати.

С различаване на малки и големи букви

Разрешете тази опция, ако употребата на главни и малки букви е от значение по време на филтрирането. След като конфигурирате опциите за филтриране/търсене, щракнете върху **OK**, за да покажете филтрираните записи в дневника или **Търси**, за да стартирате търсене. Регистрационните файлове се проверяват от горе надолу, като се стартира от текущата ви позиция (записът е маркиран). Стартирането спира, когато открие първия съответстващ запис. Натиснете **F3**, за да търсите следващия запис или щракнете с десен бутон на мишката и изберете **Търси**, за да конкретизирате опциите за търсене.

Изпълняващи се процеси

Опцията "Изпълняващи се процеси" показва активните програми или процеси на компютъра и незабавно и постоянно информира ESET за нови проникванията. ESET Internet Security предоставя подробна информация за изпълняващите се процеси, за да защити потребителите с технологията ESET LiveGrid®.



Репутация – в повечето случаи ESET Internet Security и технологията ESET LiveGrid® назначават нива на риск към обекти (файлове, процеси, ключове в системния регистър и т.н.), използвайки редица от евристични правила, които преглеждат характеристиките на всеки обект, след което преценяват неговия потенциал за злонамерено действие. Според тези евристични методи на обектите се присвоява ниво на риск от 1 – слаб (зелен) до 9 – рискован (червен).

Процес – Показвано име на програмата или процеса, който се изпълнява на компютъра в момента. Можете също така да използвате диспечера на задачите на Windows, за да

прегледате всички изпълняващи се процеси на компютъра. За да отворите диспечера на задачите, щракнете с десен бутон върху празна област от лентата на задачите и след това щракнете върху **Диспечер на задачите** или натиснете **Ctrl**+**Shift**+**Esc** от клавиатурата.

Известните приложения, маркирани със Слаб (зелен), са чисти със сигурност (разрешени) и ще бъдат изключени от сканирането, за да се подобри производителността.

PID – Идентификационният номер на процеса може да се използва като параметър при извикването на различни функции, като например коригиране на приоритета на процеса.

Брой потребители – броят потребители, използващи дадено приложение. Тази информация се събира от технологията ESET LiveGrid®.

Време на откриване – период от време след откриването на приложението от технологията ESET LiveGrid®.

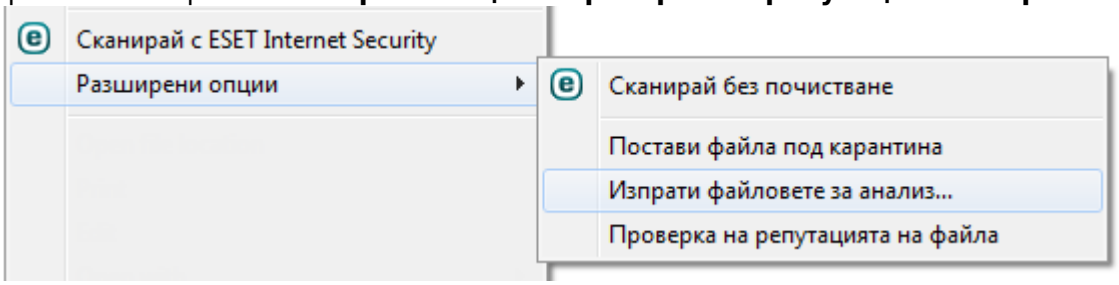
Не е задължително приложение, маркирано с Неизвестен (оранжево), да е злонамерен софтуер. Обикновено това просто е по-ново приложение. Ако не сте сигурни за файла, може да изпратите файла за анализ в лабораторията на ESET за проучвания. Ако файлът се окаже злонамерено приложение, неговото откриване ще бъде добавено в някое от следващите обновявания.

Име на приложението – името на дадена програма или процес.

Щракнете върху приложение, за да покажете следните подробности за това приложение:

- **Път** – местоположение на приложението в компютъра.
- **Размер** – размер на файла в КБ (килобайтове) или МБ (мегабайтове).
- **Описание** – характеристики на файла въз основа на описанието от операционната система.
- **Фирма** – име на доставчика или процеса на приложението.
- **Версия** – информация от издателя на приложението.
- **Продукт** – име на приложението и/или търговско име.
- **Създадено на/Променено на** – Дата и час на създаване (промяна).

Можете също така да проверите репутацията на файлове, които не функционират като изпълнявани програми/процеси. За да направите това, щракнете с десен бутон върху файла и изберете **Разширени опции** > **Проверка на репутацията на файла**.



Отчет за защитата

Тази функция предоставя общ преглед на статистиката за следните категории:

• **Блокирани уеб страници** – показва броя блокирани уеб страници (URL адреси, добавени към списък със забранени адреси за PUA, фишинг, хакнат рутер, IP или сертификат).

• **Открити заразени обекти в имейли** – показва броя на заразените обекти в имейли, които са били открити.

• **Блокирани уеб страници в „Родителски контрол“** – показва броя блокирани уеб страници в „Родителски контрол“.

• **Открити PUA** – показва броя потенциално нежелани приложения (PUA).

• **Открити имейли със спам** – показва броя на откритите имейли със спам.

• **Блокирани опити за достъп до уеб камерата** – показва броя блокирани опити за достъп до уеб камерата.

• **Сканирани документи** – показва броя обекти, сканирани като документи.

• **Сканирани приложения** – показва броя сканирани изпълними обекти.

• **Други сканирани обекти** – показва броя други сканирани обекти.

• **Сканирани обекти в уеб страници** – показва броя сканирани обекти в уеб страници.

• **Сканирани обекта в имейли** – показва броя сканирани обекти в имейли.

Редът на тези категории се базира на цифровата стойност от най-високата до най-ниската. Категориите с нулеви стойности не се показват. Щракнете върху „**Показване на повече**“, за да разгънете и покажете скритите категории.

Последната част на отчета за защитата предлага възможността за активиране на следните функции:

• Родителски контрол

• Anti-Theft

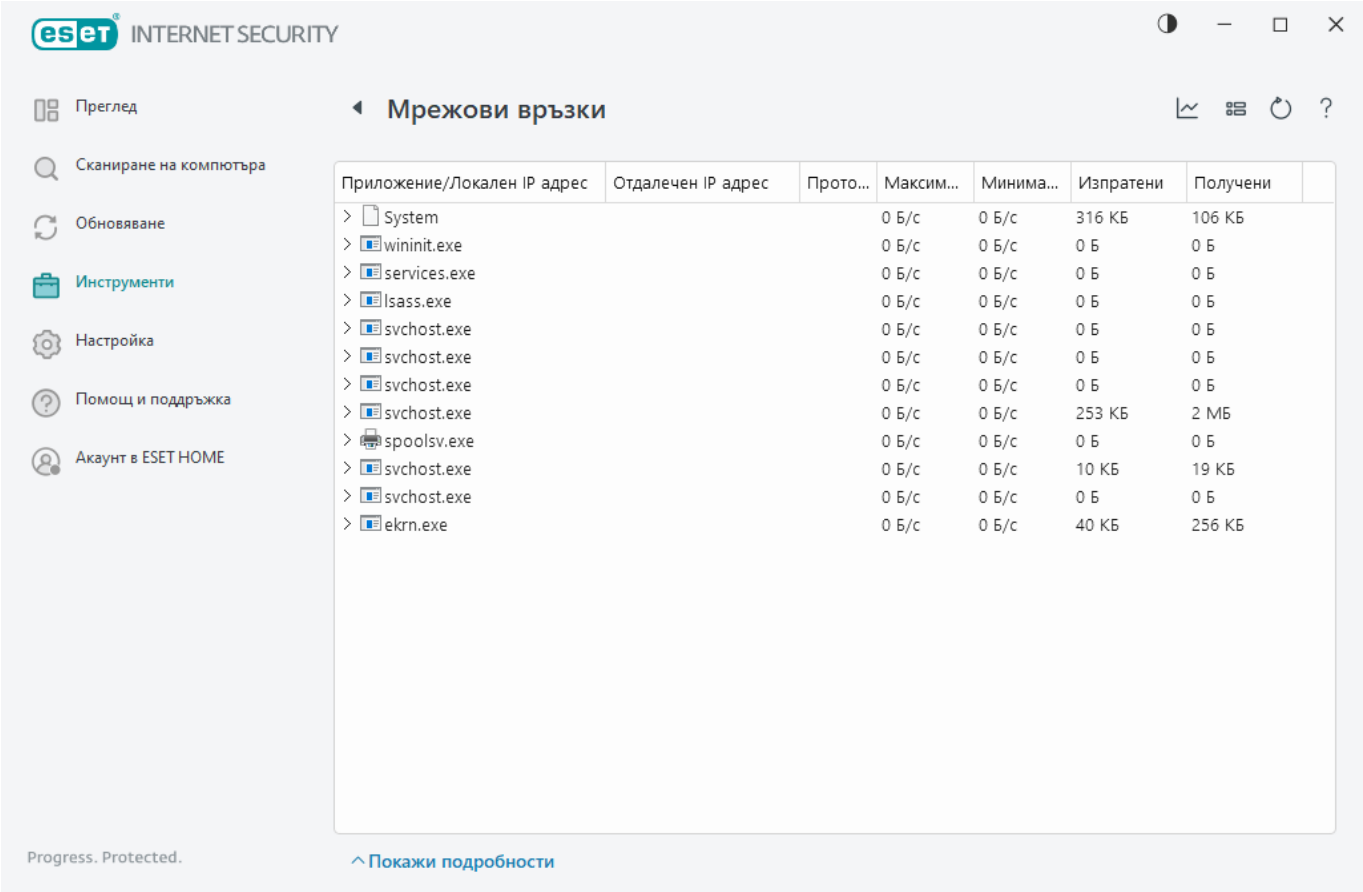
След като функцията е разрешена, вече не се показва като неработеща в отчета за защитата.

С щракване върху зъбното колелце⚙ в горния десен ъгъл можете да **разрешавате/забранявате известия за отчети за защитата** или да изберете дали данните да се показват за последните 30 дни, или от времето на активиране на продукта. Ако инсталацията на ESET Internet Security е отпреди по-малко от 30 дни, може да бъде избран само броят дни от инсталацията. Периодът от 30 дни е зададен по подразбиране.

Нулиране на данните ще изчисти всички статистически данни и ще премахне съществуващите данни за отчета за защитата. Това действие трябва да бъде потвърдено, освен ако не премахнете отметката на опцията **Питай преди нулиране на статистиката** в Разширени настройки > **Известие** > **Интерактивни уведомления** > **Съобщения за потвърждение** > **Редактиране**.

Мрежови връзки

В раздела "Мрежови връзки" можете да прегледате списък с активните и чакащите връзки. Това ви помага да контролирате всички приложения, които осъществяват изходящи връзки.



Щракнете върху иконата за диаграма , за да отворите Мрежова активност.

На първия ред се показва името на приложението и скоростта на прехвърляне на данните. За да видите списъка с връзките, инициирани от приложението (и подробна информация), щракнете върху **>**.

Колони

Приложение/локален IP адрес – име на приложението, локалните IP адреси и комуникационните портове.

Отдалечен IP адрес – IP адрес и номер на порта на даден отдалечен компютър.

Протокол – използван протокол за трансфер.

Скорост на качване/изтегляне – текущата скорост на изходящите и входящите данни.

Изпратени/получени – количество данни, обменени чрез връзката.

Покажи подробности – изберете тази опция, за да се покаже подробна информация за избраната връзка.

Щракнете с десния бутон върху дадена връзка, за да прегледате допълнителни опции, които включват:

Показване на имената на хостове – Ако е възможно, всички мрежови адреси се показват в DNS формат, а не във формат на числов IP адрес.

Покажи само TCP връзките – списъкът показва само връзки, които са включени в пакета с TCP протоколи.

Покажи активните връзки – изберете тази опция, за да се покажат само връзките, при които няма установена комуникация, но системата е отворила порт и очаква свързване.

Показване на връзките в компютъра – Изберете тази опция, за да се покажат само връзките, при които отдалечената страна е локална система, или т.нар. връзки с localhost.

Обнови скоростта – изберете честотата на опресняване на активните връзки.

Обнови сега – презареждане на прозореца с **мрежови връзки**.

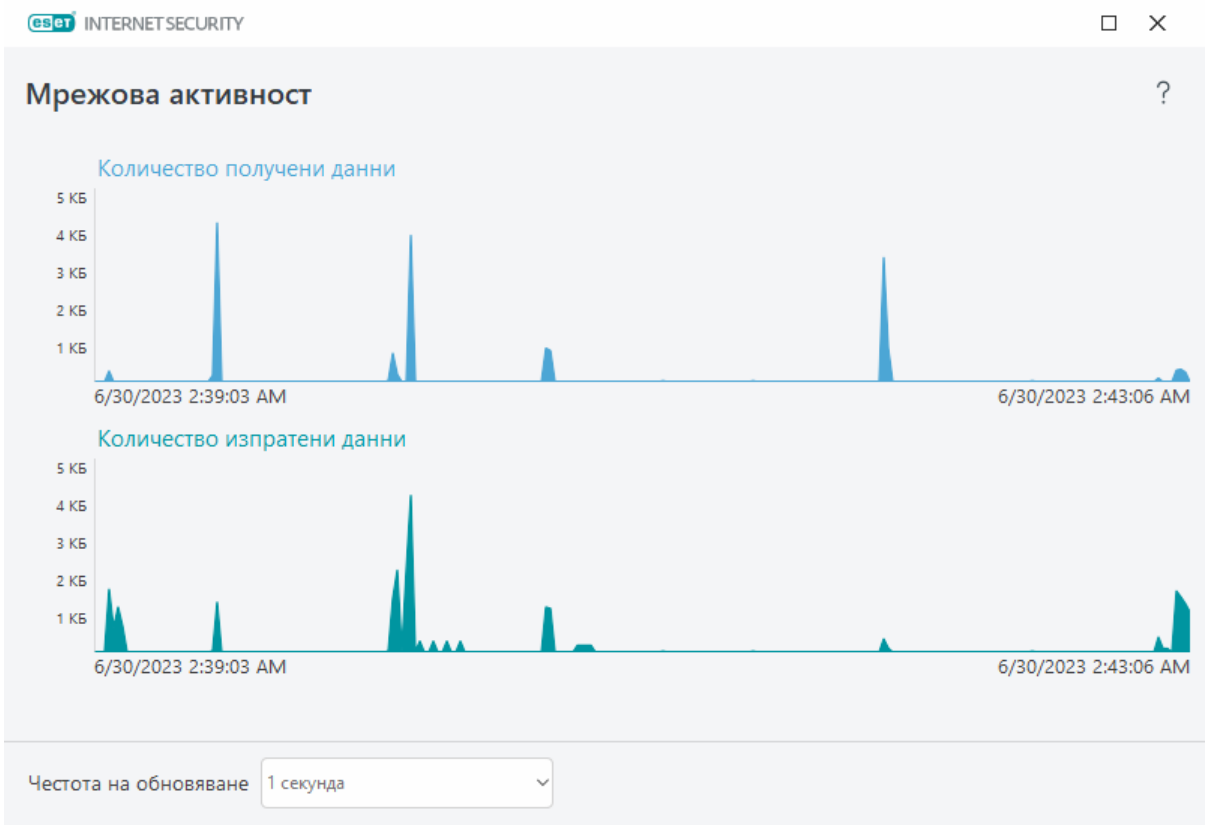
Следните опции са достъпни само след щракване върху дадено приложение или процес, а не върху активна връзка:

Временно откажи комуникацията за процеса – Отхвърля текущите връзки на даденото приложение. Ако се установи нова връзка, защитната стена използва предварително зададено правило. Описание на настройките може да се намери в раздела Правила за защитната стена.

Временно разреши комуникацията за процеса – Разрешава текущите връзки на даденото приложение. Ако се установи нова връзка, защитната стена използва предварително зададено правило. Описание на настройките може да се намери в раздела Правила за защитната стена.

Мрежова активност

За да видите текущата **мрежова активност** във форма на диаграма, щракнете върху **Инструменти** > **Мрежови връзки** и щракнете върху иконата за диаграма . В долната част на диаграмата има времева линия, която следи мрежовата активност в реално време на базата на избрания времеви период. За да промените времевия период, изберете подходящата стойност от падащото меню **Честота на обновяване**.



Налични са следните опции:

- **1 секунда** – диаграмата се обновява на всяка секунда и времевата линия покрива последните 4 минути.
- **1 минута (последните 24 часа)** – диаграмата се обновява на всяка минута и времевата линия покрива последните 24 часа.
- **1 час (последния месец)** – диаграмата се обновява на всеки час и времевата линия покрива последния месец.

Вертикалната ос на диаграмата представлява количеството получени или изпратени данни. Задръжте мишката върху диаграмата, за да видите точното количество получени/изпратени данни в определен момент.

ESET SysInspector

ESET SysInspector е приложение, което проверява щателно компютъра и събира подробна информация за системните компоненти, като например драйверите и приложенията, мрежовите връзки или важните записи в системния регистър, и оценява нивото на риск за всеки компонент. Тази информация може да е полезна при установяването на подозрително системно поведение, вследствие на софтуерна или хардуерна несъвместимост или заразяване със злонамерен софтуер. За да научите как да използвате ESET SysInspector, вижте Онлайн помощта на ESET SysInspector.

Прозорецът ESET SysInspector показва следната информация за дневника:

- **Час** – часът на създаване на регистрационния файл.

• **Коментар** – кратък коментар.

• **Потребител** – името на потребителя, създал регистрационния файл.

• **Състояние** – състоянието на създаване на регистрационния файл.

Възможните са следните действия:

• **Показване** – Отваря избраното влизане в ESET SysInspector. Можете също така да щракнете с десен бутон върху определен регистрационен файл и да изберете **Покажи** от контекстното меню.

• **Създаване** – създаване на нов регистрационен файл. Изчакайте, докато ESET SysInspector се генерира (състояние **Създаден**), преди да направите опит за достъп до дневника. Дневникът е записан в C:\ProgramData\ESET\ESET Security\SysInspector.

• **Изтрий** – премахване на избраните регистрационни файлове от списъка.

Когато един или няколко регистрационни файлове са избрани, в контекстното меню са налични следните опции:

• **Покажи** – отваря избрания регистрационен файл в ESET SysInspector (същата функция като при двукратно щракване върху регистрационен файл).

• **Създаване** – създаване на нов регистрационен файл. Изчакайте, докато ESET SysInspector се генерира (състояние **Създаден**), преди да направите опит за достъп до дневника.

• **Изтрий** – премахване на избраните регистрационни файлове от списъка.

• **Изтрий всички** – изтриване на всички регистрационни файлове.

• **Експортиране** – експортиране на регистрационния файл в .xml файл или архивиран .xml файл.

Планировчик

Планировчикът управлява и стартира планирани задачи с предварително зададени конфигурация и свойства.

Можете да осъществите достъп до "Разписание" от главния програмен прозорец на ESET Internet Security, като щракнете върху **Инструменти** > **Разписание**. Функцията **Планировчик** съдържа списък с всички планирани задачи и свойства на конфигурации, като например предварително зададени дата и час и използван профил за сканиране.

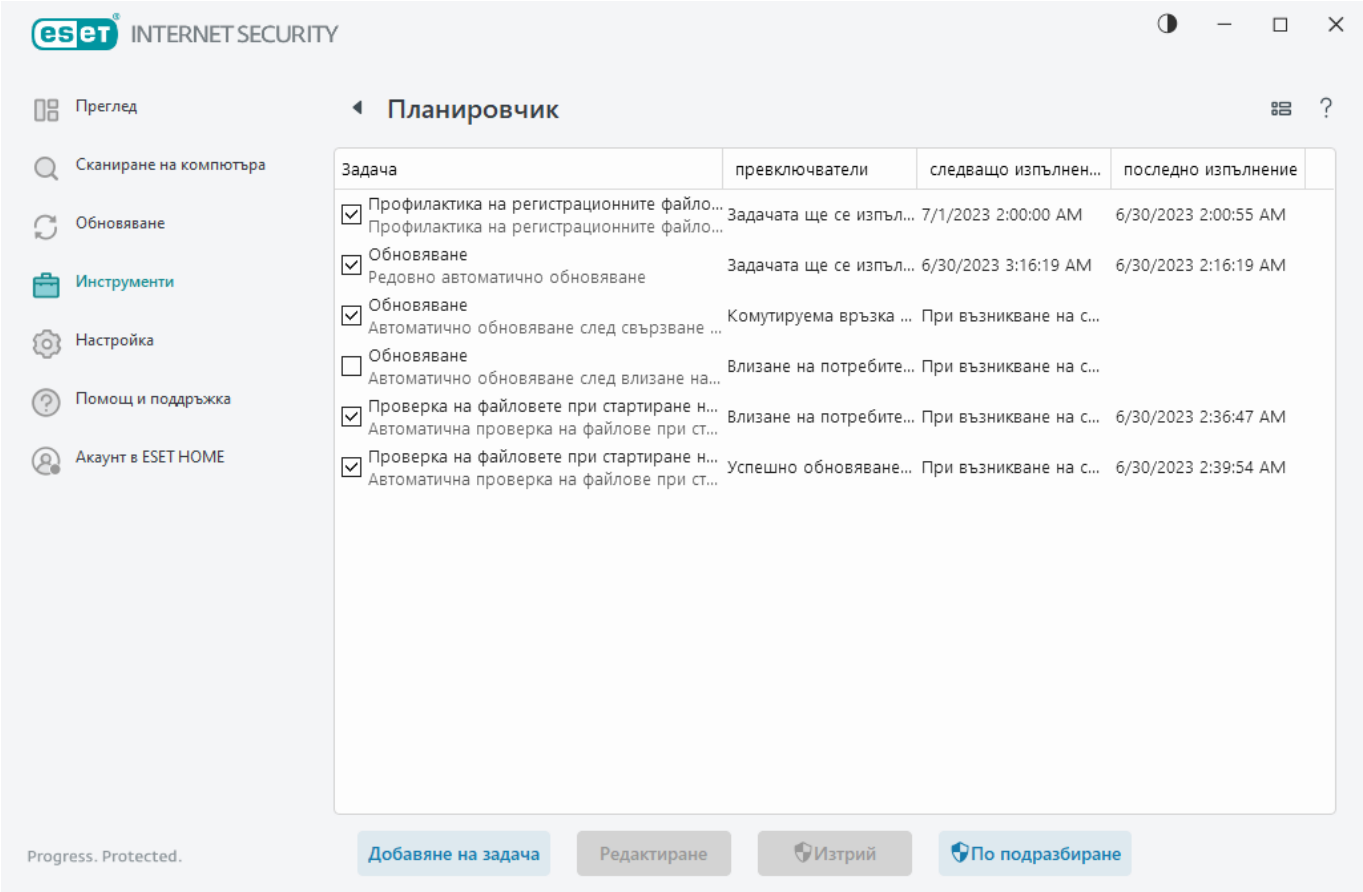
Планировчикът се използва за планиране на следните задачи: обновяване на модули, задача за сканиране, проверка на файловете при стартиране на системата и профилактика на регистрационни файлове. Можете да добавяте или изтривате задачи директно от главния прозорец на планировчика (щракнете върху **Добавяне на задача** или **Изтриване** в най-долната част). Можете да върнете списъка с планирани задачи до настройките му по подразбиране и да изтриете всички промени, като щракнете върху **По подразбиране**. Щракнете с десния бутон в прозореца на планировчика, за да изпълните следните действия: показване на подробна информация, незабавно изпълнение на задачата, добавяне на нова

задача, изтриване на съществуваща задача. Използвайте квадратчетата в началото на всеки запис, за да активирате/деактивирате задачите.

По подразбиране се показват следните планирани задачи в **Планировчик**:

- **Профилактика на регистрационните файлове**
- **Редовно автоматично обновяване**
- **Автоматично обновяване след влизане на потребителя**
- **Автоматична проверка на файловете при стартиране** (след влизане на потребителя)
- **Автоматична проверка на файловете при стартиране** (след успешно обновяване на системата за откриване)

За да редактирате конфигурацията на съществуваща планирана задача (по подразбиране или зададена от потребител), щракнете с десния бутон върху съответната задача, след което щракнете върху **Редактиране...**, или изберете задачата, която ще променяте, и след това щракнете върху **Редактиране**.



Добавяне на нова задача

1. Щракнете върху **Добавяне на задача** в най-долната част на прозореца.
2. Въведете име на задачата.
3. Изберете желаната задача от падащото меню:

• **Изпълнение на външно приложение** – планира изпълнението на външно приложение.

• **Профилактика на регистрационните файлове** – В регистрационните файлове има останали елементи от изтрити записи. Тази задача оптимизира редовно записите в регистрационните файлове, за да се изпълняват по-ефективно.

• **Проверка на файловете при стартиране на системата** – проверка на файловете, за които е разрешено да се изпълняват при стартиране на системата или при влизане.

• **Създаване на моментна снимка на състоянието на компютъра** – Създава моментна снимка на компютъра на ESET SysInspector – събира подробна информация за компонентите на системата (напр. драйвери, приложения) и оценява нивото на риск за всеки компонент.

• **Сканиране на компютъра при поискване** – извършва сканиране на файловете и папките в компютъра.

• **Обновяване** – Планира задача за обновяване, като обновява модулите.

4. Щракнете върху плъзгача до **Разрешено**, ако искате да активирате задачата (можете да направите това и по-късно, като поставите/махнете отметката в списъка с планирани задачи), щракнете върху **Напред** и изберете една от времевите опции:

• **Веднъж** – задачата ще се изпълни на предварително указаните дата и час.

• **Постоянно** – задачата ще се изпълни в указания времеви интервал.

• **Ежедневно** – задачата ще се изпълнява редовно всеки ден в указаното време.

• **Всяка седмица** – задачата ще се изпълнява в избраните ден и час.

• **При възникване на събитие** – задачата ще се изпълнява при възникване на определено събитие.

5. Изберете **Пропускане на задачата, когато компютърът работи на батерия**, за да минимизирате използването на системните ресурси, когато лаптоп работи на батерия. Задачата ще се изпълни на датата и в часа, указани в полетата **Изпълнение на задачата**. Ако задачата не се е изпълнила в предварително указания час, можете да укажете кога да се изпълни отново:

• **В следващия планиран час**

• **Възможно най-скоро**

• **Веднага, ако времето от последното изпълнение надвишава (часа)** – Представлява времето, изминало от първото пропуснато изпълнение на задачата. Ако този час е надвишен, задачата ще се изпълни незабавно. Задайте времето с брояча по-долу.

За да прегледате планираната задача, щракнете с десния бутон върху задачата и щракнете върху **Показване на подробности за задачата**.

Опции за планирано сканиране

В този прозорец можете да определите разширените опции за дадена планирана задача за сканиране на компютъра.

За да изпълните сканиране без действие за почистване, щракнете върху **Разширени настройки** и изберете **Сканиране без почистване**. Хронологията на сканирането се записва в дневника на сканирането.

Когато е избрана опцията **Игнориране на изключенията**, файловете с разширения, които преди това са били изключени от сканиране, ще бъдат сканирани без изключение.

Падащото меню **Действие след сканиране** ви позволява да зададете действие, което да се извършва автоматично, след като сканирането завърши:

• **Никакво действие** – няма да се извърши никакво действие след приключване на сканирането.

• **Изключване** – компютърът се изключва след приключване на сканирането.

• **Рестартиране, ако е необходимо** – компютърът се рестартира само ако е необходимо, за да завърши почистване на откритите заплахи.

• **Рестартиране** – всички отворени програми се затварят и компютърът се рестартира след приключване на сканирането.

• **Принудително рестартиране, ако е необходимо** – компютърът се рестартира принудително само ако е необходимо, за да завърши почистване на откритите заплахи.

• **Принудително рестартиране** – Принудително затваря всички отворени програми без изчакване на намесата на потребител и рестартира компютъра след приключване на сканирането.

• **Заспиване** – сесията ви се записва и компютърът влиза в състояние на ниска консумация на електроенергия, за да можете бързо да възобновите работата си.

• **Хибернация** – всичко, което се изпълнява в RAM паметта, се премества в специален файл на твърдия диск. Компютърът се изключва, но ще възстанови предходното си състояние, когато го стартирате следващия път.

Действията **Заспиване** и **Хибернация** са налични в зависимост от настройките на операционната система за включване и заспиване на компютъра или възможностите на компютъра/лаптопа. Не забравяйте, че в спящ режим компютърът все още работи. Той продължава да изпълнява основни функции и да използва електричество, когато се захранва от батерията. За да пестите заряда на батерията, когато например пътувате извън офиса, е препоръчително за използвате опцията „Хибернация“.

Избраното действие ще започне след приключване на всички текущи сканирания. Когато изберете **Изключване** или **Рестартиране**, се показва диалогов прозорец за потвърждение на продукта с 30-секундно обратно броене (щракнете върху **Отказ**, за да деактивирате заявеното действие).

Изберете **Сканирането не може да бъде отменено**, за да възпрепятствате неупълномощените потребители да прекъсват действията, извършвани след сканиране.

Изберете опцията **Сканирането може да бъде временно спряно от потребителя за (мин.)**, ако искате да позволите на ограничения потребител да спре временно сканирането на компютъра за определен период от време.

Вижте също Ход на сканирането.

Преглед на планираната задача

Този диалогов прозорец показва подробна информация за избраната планирана задача, когато щракнете двукратно върху задача по избор или когато щракнете с десен бутон върху задача по избор на планировчика и след това изберете **Покажи подробности за задачата**.

Подробности за задачата

Въведете **Име на задача**, изберете една от опциите за **Тип задача**, след което щракнете върху **Напред**:

• **Изпълнение на външно приложение** – планира изпълнението на външно приложение.

• **Профилактика на регистрационните файлове** – В регистрационните файлове има останали елементи от изтрити записи. Тази задача оптимизира редовно записите в регистрационните файлове, за да се изпълняват по-ефективно.

• **Проверка на файловете при стартиране на системата** – проверка на файловете, за които е разрешено да се изпълняват при стартиране на системата или при влизане.

• **Създаване на моментна снимка на състоянието на компютъра** – Създава моментна снимка на компютъра на ESET SysInspector – събира подробна информация за компонентите на системата (напр. драйвери, приложения) и оценява нивото на риск за всеки компонент.

• **Сканиране на компютъра при поискване** – извършва сканиране на файловете и папките в компютъра.

• **Обновяване** – Планира задача за обновяване, като обновява модулите.

Времеви параметри на задачата

Задачата ще се изпълнява повторно през указания времеви интервал. Изберете една от времевите опции:

• **Веднъж** – задачата ще се изпълни само веднъж на указаните дата и час.

• **Постоянно** – задачата ще се изпълни в указания времеви интервал (в часове).

• **Ежедневно** – задачата ще се изпълнява всеки ден в указаното време.

• **Всяка седмица** – задачата ще се изпълнява един или повече пъти в седмицата в

избраните дни и час.

- **Стартирано събитие** – задачата ще се изпълнява при възникване на указано събитие.

Пропускане на задачата, когато компютърът работи на батерия – Задачата няма да се стартира, ако компютърът работи на батерия в момента, в който задачата би трябвало да започне. Това се отнася също така и за компютри, работещи със захранване от UPS.

Времеви параметри на задачата – Веднъж

Изпълнение на задачата – указаната задача ще се изпълни само веднъж на посочената дата и в посочения час.

Времеви параметри на задачата – Всеки ден

Задачата ще се изпълнява всеки ден в указаното време.

Времеви параметри на задачата – Всяка седмица

Задачата ще се изпълнява многократно всяка седмица в избрания ден/избраните дни и час.

Времеви параметри на задачата – При възникване на събитие

Задачата ще се изпълни при възникване на едно от следните събития:

- **При всяко стартиране на компютъра**
- **При първото стартиране на компютъра всеки ден**
- **Комутируема връзка с интернет/VPN**
- **Успешно обновяване на модул**
- **Успешно обновяване на продукт**
- **Влизане на потребител**
- **Откриване на заплахи**

При планиране на задача, която се изпълнява при възникване на събитие, можете да зададете минимален интервал между две изпълнения на задачата. Например, ако влизате в компютъра няколко пъти на ден, изберете 24 часа за изпълнение на задачата само при първото ви

влизане и след това на следващия ден.

Пропусната задача

Дадена задача може да бъде пропусната, ако компютърът работи на батерия или е изключен. Изберете кога да се изпълнява задачата чрез една от тези опции и щракнете върху **Напред**:

• **В следващия планиран час** – Задачата ще се изпълни, ако компютърът е включен в следващия планиран час.

• **Възможно най-скоро** – Задачата ще се изпълни, когато компютърът е включен.

• **Веднага, ако времето от последното планирано изпълнение надвишава (часа)** – Представлява времето, изтекло от първото пропуснато изпълнение на задачата. Ако този час е надвишен, задачата ще се изпълни незабавно.

Веднага, ако времето от последното планирано изпълнение надвишава (часове) – примери

Зададена е примерна задача да се изпълнява многократно на всеки час. Опцията **Веднага, ако времето от последното планирано изпълнение надвишава (часа)** е избрано и превишеното време е зададено на два часа. Задачата се изпълнява в 13:00 часа, а когато приключи, компютърът заспива:

• Компютърът се събужда в 15:30 часа. Първото пропуснато изпълнение на задачата беше в 14:00 часа. От 14:00 часа са изминали само 1,5 часа, така че задачата ще се изпълни в 16:00 часа.

• Компютърът се събужда в 16:30 часа. Първото пропуснато изпълнение на задачата беше в 14:00 часа. От 14:00 часа са изминали два часа и половина, така че задачата ще се изпълни незабавно.

Подробности за задачата – Обновяване

Ако желаете да обновите програмата от два сървъра за обновяване, е необходимо да създадете два различни профила за обновяване. Ако първият не може да изтегли файловете за обновяване, програмата автоматично превключва на другия. Това решение е подходящо за преносими компютри, които обикновено се обновяват от локален сървър за обновяване във вътрешна мрежа, но техните собственици често се свързват към интернет от други мрежи. Така че ако първият профил има проблем, вторият автоматично ще изтегли файловете за обновяване от сървърите за обновяване на ESET.

Подробности за задачата – Изпълнение на приложение

Тази задача планира изпълнението на външно приложение.

Изпълним файл – изберете изпълним файл от дървото на директориите, щракнете върху опцията **...** или въведете пътя ръчно.

Работна папка – укажете работната директория на външното приложение. Всички временни

файлове на избрания **Изпълним файл** ще се създадат в тази директория.

Параметри – параметри на командния ред за приложението (по желание).

Щракнете върху **Готово**, за да приложите задачата.

Инструмент за почистване на системата

Инструментът за почистване на системата е инструмент, който ви помага да върнете компютъра към използваемо състояние след почистване на заплахата. Злонамереният софтуер може да забрани помощни програми на системата, като например редактора на системния регистър, диспечера на задачите или обновяванията на Windows. Инструментът за почистване на системата възстановява стойностите и настройките по подразбиране за дадена система с едно щракване.

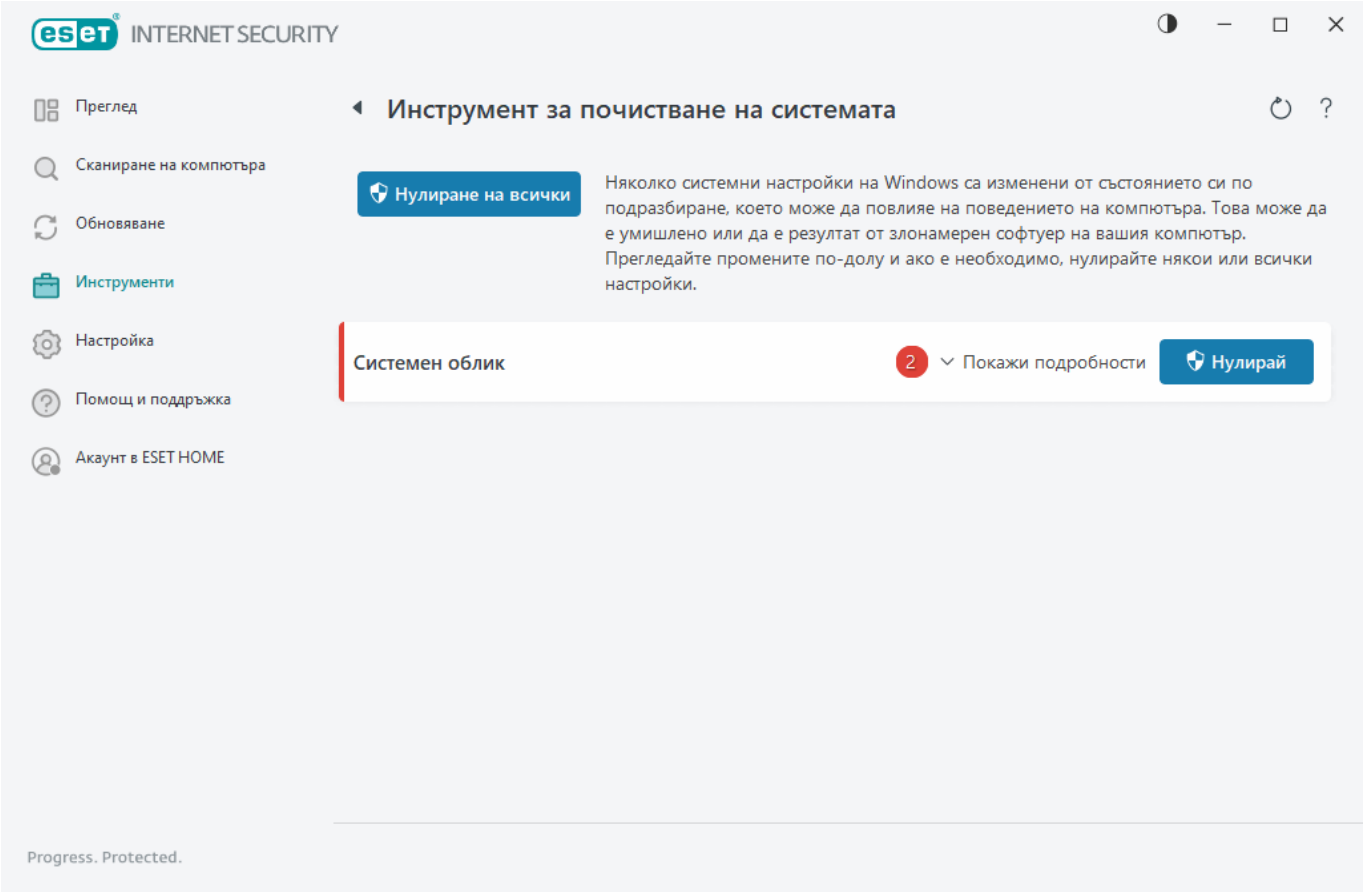
Инструментът за почистване на системата докладва за проблеми от пет категории на настройките:

- **Настройки на защитата**: промени в настройките, които може до доведат до повишаване на уязвимостта на вашия компютър, като например Windows Update
- **Системни настройки**: промени в системните настройки, които може да променят поведението на компютъра ви, като например асоцииране на файлове
- **Системен облик**: настройки, които засягат вида на вашата система, като вашия тапет за работен плот
- **Забранени функции**: важни функции и приложения, които може да бъдат забранени
- **Възстановяване на системата на Windows**: настройки за функцията за възстановяване на системата на Windows, които ви позволяват да връщате системата в предишно състояние

Може да се изиска почистване на системата:

- при откриване на заплаха
- когато потребител щракнете върху **Нулиране**

Можете да прегледате промените и да нулирате настройките, ако е нужно.



Само потребител с права на администратор може да извършва действия в инструмента за почистване на системата.

Мрежов инспектор

Мрежовият инспектор може да помогне за идентифициране на уязвимости във вашата надеждна (домашна или офис) мрежа (например отворени портове или слаба парола на рутера). Тя също така предоставя списък със свързани устройства, категоризирани по тип устройство (например принтер, рутер, мобилно устройство и т.н.), за да ви покаже какви устройства са свързани с вашата мрежа (например игрова конзола, IoT или други интелигентни домашни устройства).

Мрежов инспектор ви помага да откриете уязвимостите на маршрутизатора и повишава нивото ви на защита, когато сте свързани към мрежа.

Мрежовият инспектор не преконфигурира вашия рутер вместо вас. Вие ще направите промените сами, като използвате специализирания интерфейс на вашия рутер. Домашните рутери могат да бъдат силно уязвими към злонамерен софтуер, използван за стартиране на атаки с разпределен отказ от обслужване (DDoS). Ако паролата на рутера не е била променена от зададената по подразбиране от страна на потребителя, хакерите могат лесно да я отгатнат, след което да влязат в рутера и да го конфигурират отново или да компрометират вашата мрежа.

Силно препоръчваме създаването на силна парола, която е достатъчно дълга и съдържа цифри, символи или главни букви. За да направите паролата по-трудна за отгатване, използвайте смесица от различни видове знаци.

Ако мрежата, към която сте свързани, е конфигурирана като надеждна, можете да я маркирате като „Моята мрежа“. Щракнете върху **Маркиране като „Моята мрежа“**, за да добавите етикет „Моята мрежа“ към мрежата. Този етикет ще бъде показан до мрежата в ESET Internet Security за по-добра идентификация и преглед на защитата. Щракнете върху **Премахване на маркирането като „Моята мрежа“**, за да премахнете етикета.

Всяко свързано с мрежата ви устройство се показва в списъчен изглед с основната информация. Щракнете върху конкретното устройство, за да редактирате устройството или да прегледате подробна информация за устройството.

В изглед на списък падащото меню **Мрежи** ви дава възможност да филтрирате устройства въз основа на следните критерии:

- Устройства, свързани към конкретна мрежа
- Устройства, свързани с **всички мрежи**
- Некатегоризирани устройства

Щракнете върху иконата на устройството, за да редактирате устройството или да прегледате подробна информация за устройството. Устройствата, които са се свързали наскоро, са показани по-близо до рутера, така че да можете по-лесно да ги забележите.

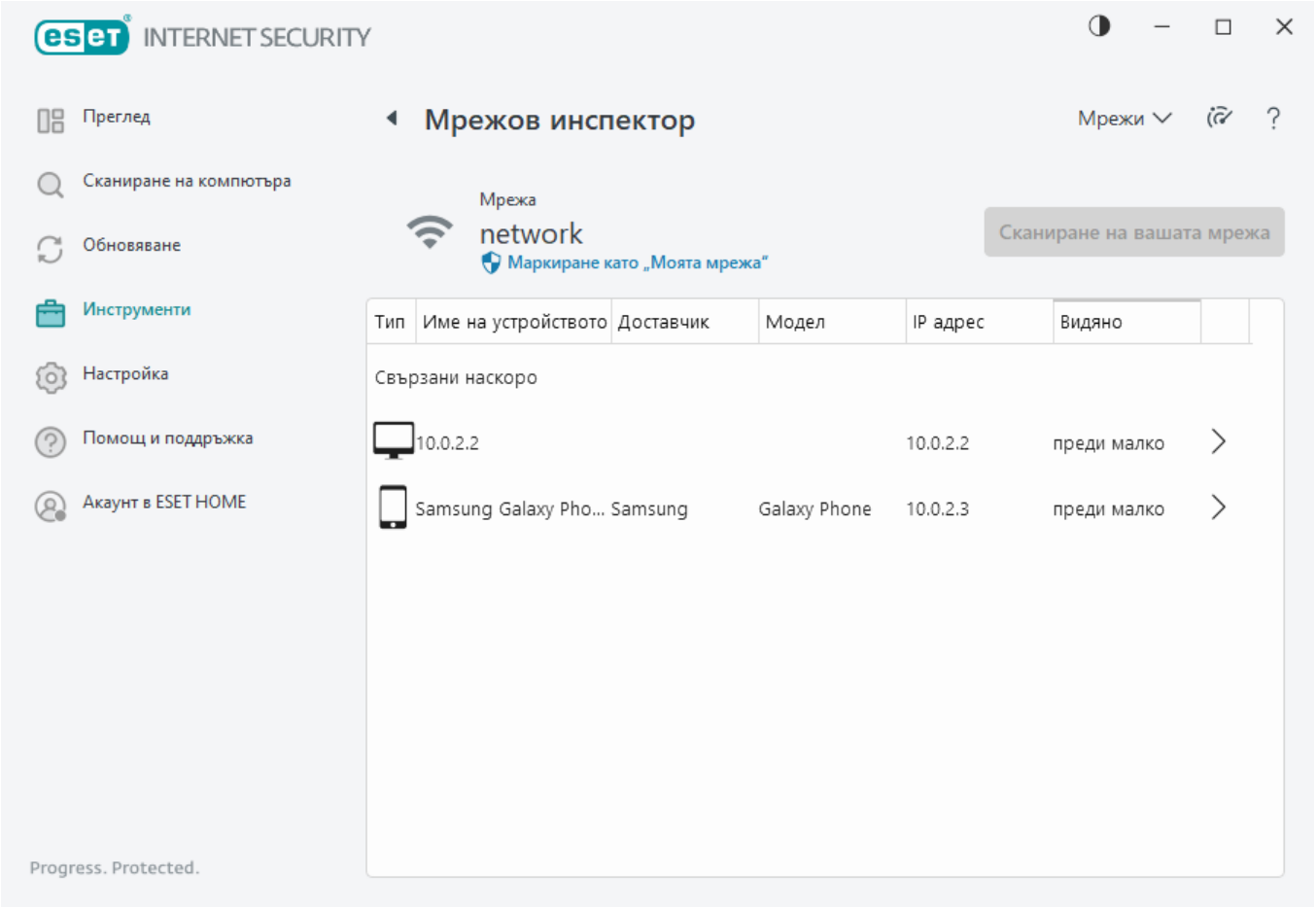
Щракнете върху зъбното колелце ⚙ в горния десен ъгъл, за да изберете дали да получавате известие, когато в мрежата бъде открито ново устройство.

Щракнете върху **Сканиране на вашата мрежа**, за да изпълните ръчно сканиране на мрежата, с която сте свързани в момента. **Сканиране на вашата мрежа** е достъпно само за надеждна мрежа. Вижте Профили за мрежова връзка, за да прегледате или редактирате мрежовите си настройки.

Можете да изберете от следните опции за сканиране:

- Сканиране на всичко
- Сканиране само на маршрутизатора
- Сканиране само на устройствата

⚠ Използвайте сканиране на мрежата само в надеждна мрежа! Ако извършвате това в мрежите на други хора, внимавайте за потенциална опасност.



Когато сканирането приключи, ще се покаже известие с връзка към основна информация за устройството или можете да щракнете двукратно върху подозрителното устройство в списъчния изглед или изгледа на сонар. Щракнете върху **Отстраняване на проблеми** за преглед на последно блокираните комуникации. Още информация за отстраняването на неизправности със защитната стена.

Има два типа известия, показвани от модула „Мрежов инспектор“:

• **Ново устройство е свързано към мрежата** – показва се, ако непознато устройство се свърже към мрежата, докато потребителят е свързан.

• **Открити са нови устройства в мрежа** – показва се, ако се свържете отново към надеждната мрежа и е налично непознато устройство.

Двата типа известия ви информират дали неупълномощено устройство се опитва да се свърже към вашата мрежа. Щракнете върху **преглед на устройство**/преглед на устройства, за да се покажат подробните данни за устройството/ата.

Какво означават иконите на устройствата в „Мрежов инспектор“?

	Иконата на жълта звезда показва устройства, които са нови за мрежата или са открити от ESET за първи път.
	Жълтата икона за внимание показва, че рутерът ви може да съдържа уязвимости. Щракнете върху иконата в продукта за по-подробна информация за проблема.

	Червената икона за предупреждение показва, че рутерът ви съдържа уязвимости и може да е заразен. Щракнете върху иконата в продукта за по-подробна информация за проблема.
	Синята икона може да се появи, когато вашият продукт на ESET има допълнителна информация за вашия рутер, но не се изисква незабавно внимание, тъй като няма рискове за защитата. Щракнете върху иконата в продукта за по-подробна информация.

Мрежово устройство в мрежовия инспектор

Тук можете да намерите подробна информация за конкретното мрежово устройство, включително следното:

- Име на устройството
- Тип устройство
- Последно видени
- Име на мрежата
- IP адрес
- MAC адрес
- Операционна систем

Иконата с молив указва, че можете да промените името на устройството или неговия тип.

Премахване от хронологията – изтриване на устройството от списъка с устройства. Тази опция е достъпна само за устройства, които в момента не са свързани към вашата мрежа.

За всеки тип устройство са възможни следните действия:

Рутер

Настройки на рутера – Достъп осъществявайте достъп до настройките на рутера от уеб интерфейса, мобилното приложение или щракнете върху **Отваряне на интерфейса на рутера**. Ако разполагате с рутер, предоставен от вашия доставчик на интернет услуги, може да е необходимо да се свържете с отдела по поддръжката на доставчика на интернет услуги или производителя на рутера, за да разрешите открити проблеми със защитата. Винаги следвайте предпазните мерки за безопасност, както е посочено в ръководството за потребителя на вашия рутер.
Защита – За да предпазите вашите рутер и мрежа от атаки по киберзащитата, следвайте тези основни препоръки.

Мрежово устройство

Идентификация на устройство – ако имате съмнения в устройството, свързано към вашата мрежа, проверете името на доставчика или производителя под името на устройството. Това може да ви помогне да идентифицирате вида на устройството. Можете да промените името на устройството за бъдеща справка.
Прекъсване на връзката с устройството – ако сте убедени, че свързано устройство е безопасно за вашата мрежа или устройства, можете да управлявате достъпа до мрежата за това устройство в настройките на рутера или да промените паролата на мрежата.
Защита – за да защитите устройството си от атаки и злонамерен софтуер, инсталирайте киберзащита на устройството и винаги поддържайте в актуално състояние операционната си система и инсталирания софтуер. За да останете защитени, не се свързвайте с незащитени Wi-Fi мрежи.

Това устройство

Това устройство представлява вашия компютър в мрежата.
Мрежови адаптери – показва информация за вашите мрежови адаптери.

Известия | Мрежов инспектор

По-долу следват няколко известия, които могат да се показват, когато ESET Internet Security открие проблеми с уязвимостта на вашия рутер. Всяко известие съдържа кратко описание и предоставя решение или стъпки, които трябва да бъдат изпълнени, за да се намали рискът от уязвимост на рутера. Ако не сте запознат(а) с промените в рутера, ви препоръчваме да се свържете с производителя на рутера или доставчика на интернет.

Открита е потенциална уязвимост
Вашият маршрутизатор може да съдържа известни уязвимости, които могат да го направят лесна мишена за атаки и възползване. Обновете фърмуера на маршрутизатора.

Открита е уязвимост
Вашият маршрутизатор съдържа известни уязвимости, които го правят лесна мишена за атаки и възползване. Обновете фърмуера на маршрутизатора.

Открита е заплаха
Вашият маршрутизатор е заразен със злонамерен софтуер. Рестартирайте маршрутизатора и повторете сканирането.

Слаба парола на маршрутизатора
Паролата на вашия маршрутизатор е слаба и лесно може да бъде налучкана от някой друг. Сменете паролата на маршрутизатора.

Пренасочване на злонамерена мрежа
Изглежда, че вашият интернет трафик е пренасочен към злонамерени уеб сайтове. Това означава, че вашият маршрутизатор е компрометиран. Променете настройката на DNS сървъра на маршрутизатора.

Услуги в отворена мрежа
Вашият маршрутизатор изпълнява мрежови услуги, от които могат да се възползват други. Това може да се дължи на слаба конфигурация или на компрометиран маршрутизатор. Проверете конфигурацията на маршрутизатора.

Чувствителни услуги в отворена мрежа
Вашият маршрутизатор изпълнява чувствителни мрежови услуги, от които могат да се възползват други. Това може да се дължи на слаба конфигурация или на компрометиран маршрутизатор. Проверете конфигурацията на маршрутизатора.

Остарял фърмуер
Фърмуерът на вашия маршрутизатор е остарял и може да съдържа уязвимости. Обновете фърмуера на маршрутизатора.

Злонамерена настройка на маршрутизатора
Използваният от вас DNS сървър е злонамерен и може да ви изпрати към опасни уеб сайтове. Това означава, че вашият маршрутизатор е компрометиран. Променете настройката на DNS сървъра на маршрутизатора.

Услуги в мрежа
Вашият маршрутизатор изпълнява обичайни мрежови услуги. Те са необходими на мрежата и вероятно са безопасни. Проверете конфигурацията на маршрутизатора.

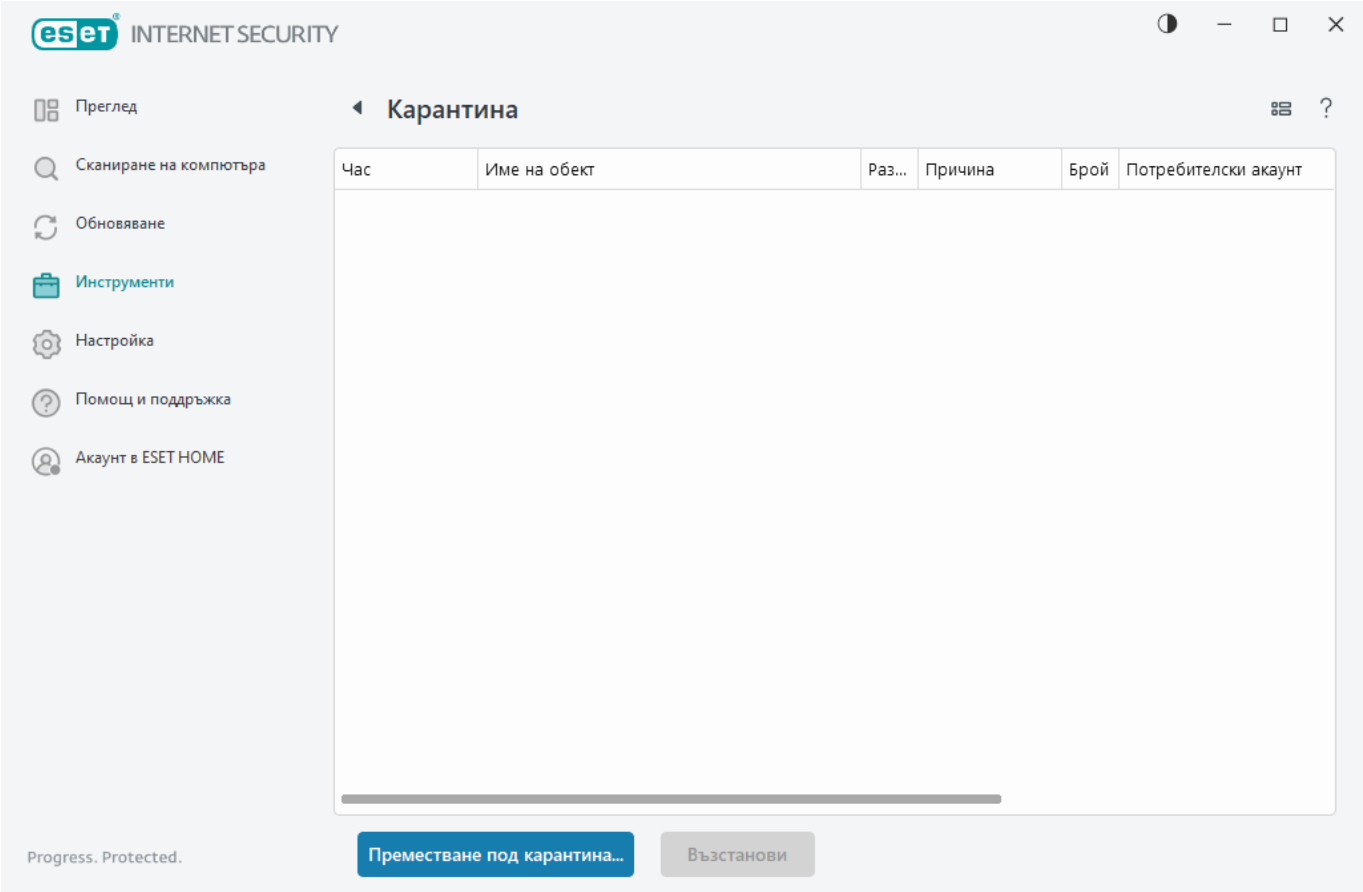
Карантина

Основната функция на карантината е безопасно да се съхраняват докладваните обекти (като например злонамерен софтуер, заразени файлове или потенциално нежелани приложения).

Можете да осъществите достъп до карантината от главния програмен прозорец на ESET Internet Security, като щракнете върху **Инструменти** > **Карантина**.

Файловете, съхранени в папката за карантина, могат да се видят в таблица, която показва:

- датата и часа на карантината,
- пътя до първоначалното местоположение на файла,
- неговия размер в байтове,
- причина (например обект, добавен от потребителя),
- и редица откривания (например откриване на дублиращи се записи на един и същ файл или ако то е архив, съдържащ множество прониквания).



Файлове под карантина

ESET Internet Security автоматично поставя под карантина премахнати файлове (ако не сте отменили тази опция в прозореца за уведомяване).

Допълнителни файлове трябва да бъдат поставени под карантина, ако:

a.не могат да бъдат почистени,

b.ако не е безопасно или препоръчително да бъдат премахнати,

c.ако са погрешно засечени от ESET Internet Security,

d.или ако даден файл се държи подозрително, но не е засечен от Защити.

За да поставите файл под карантина, имате няколко опции:

a.Използвайте функцията за плъзгане и пускане, за да поставите под карантина даден файл ръчно, като щракнете върху файла, преместите курсора на мишката до маркираната област, докато държите натиснат бутона на мишката, като след това го пуснете. След това приложението се премества на преден план.

b.Щракнете с десен бутон върху файла > щракнете върху **Разширени опции** > **Постави файла под карантина**.

c.Щракнете върху **Преместване под карантина...** от прозореца **Карантина**.

d.Контекстното меню също може да се използва за тази цел; щракнете с десния бутон

върху прозореца **Карантина** и изберете **Карантина**.

Възстановяване от карантина

Файловете под карантина също могат да бъдат възстановени до първоначалното им местоположение:

• Използвайте функцията за **Възстановяване** за тази цел, която е налична от контекстното меню, като щракнете с десния бутон върху даден файл в карантината.

• Ако даден файл е маркиран като потенциално нежелано приложение, опцията **Възстановяване и изключване от сканиране** е разрешена. Вижте също Изключения.

• Контекстното меню също предлага опцията **Възстановяване до**, която ви позволява да възстановите файл на място, различно от това, от което е премахнат.

• Функцията за възстановяване не е налична в някои случаи, например за файлове, намиращи се в мрежов дял само за четене.

Премахване от карантината

Щракнете с десен бутон върху определен елемент и изберете **Изтриване от карантината** или изберете елемента, който искате да изтриете, и натиснете **Delete** от клавиатурата. Ако искате да изберете и изтриете всички елементи под карантина, можете да натиснете **Ctrl + A** и след това **Delete** на клавиатурата. Изтритите елементи ще бъдат премахнати завинаги от вашето устройство и карантина.

Изпращане на файл от карантината

Ако сте поставили под карантина подозрителен файл, който не е бил открит от програмата, или ако даден файл е бил неправилно определен като заразен (например при евристичен анализ на кода) и след това поставен под карантина, изпратете примера за анализ от лабораторията на ESET за проучвания. За да изпратите файл, щракнете с десния бутон на мишката върху него и изберете **Изпрати за анализ** от контекстното меню.

Описание на откриването

Щракнете с десния бутон върху елемент и щракнете върху **Описание на откриването**, за да отворите енциклопедията за заплахи на ESET, която съдържа подробна информация за опасностите и симптомите на регистрираното проникване.

Илюстрирани инструкции

Следните статии в онлайн помощника на ESET може да бъдат налични и на английски:

- Възстановяване на файл под карантина в ESET Internet Security
- Премахване на файл под карантина в ESET Internet Security
- Моят продукт на ESET ме уведоми за откриване – какво трябва да направя?

Неуспешно поставяне под карантина

Причините, поради които конкретни файлове не могат да бъдат преместени в карантина, са

следните:

- **Нямате разрешения за четене** – означава, че не можете да видите съдържанието на даден файл.
- **Нямате разрешения за запис** – означава, че не можете да променяте съдържанието на файла, т.е. или да добавите ново съдържание, или да премахнете съществуващото.
- **Файл, който се опитвате да поставите под карантина, е твърде голям** – трябва да намалите размера на файла.

Когато получите съобщение за грешка „Неуспешно поставяне под карантина“, щракнете върху **Повече информация**. Появява се прозорец на списъка с грешки при поставяне под карантина и ще видите името на файла и причината, поради която файлът не може да бъде поставен под карантина.

Изпращане на файл за анализ

Ако откриете подозрителен файл на компютъра или подозрителен сайт в интернет, може да го изпратите за анализ на лабораторията на ESET за проучвания (може да не е достъпно в зависимост от вашата конфигурация на ESET LiveGrid®).

> **Преди да изпратите примери на ESET**
> Не изпращайте пример, освен ако не отговаря на поне един от следните критерии:
> • Примерът въобще не е открит от вашия продукт на ESET
> • Примерът е неправилно открит като заплаха
> • Не приемаме лични файлове (които бихте искали да бъдат сканирани за злонамерен софтуер от ESET) като примери (лабораторията на ESET за проучвания не извършва сканирания при поискване от потребители)
> • Използвайте описателна фраза в реда за тема и приложете колкото се може повече информация за файла (като например екранна снимка или уеб сайта, от който сте го изтеглили).

Можете да изпратите пример (файл или уеб сайт) за анализ на ESET, като използвате един от тези методи:

1. Използвайте формуляра за подаване на пример във вашия продукт. Намира се в **Инструменти** > **Изпращане на пример за анализ**. Максималният размер на изпратения пример е 256 МБ.

2. Файлът може да се изпрати също така и по имейл. Ако предпочитате тази опция, архивирайте го с помощта на програмата WinRAR/WinZIP, защитете архива с паролата „infected“ и го изпратете на адрес samples@eset.com.

3. За да докладвате за спам, фалшиви положителни резултати за спам или уеб сайтове, които неправилно са категоризирани от модула за родителски контрол, вижте нашата статия от онлайн помощника на ESET.

Във формуляра **Изпращане на файл за анализ** изберете описанието от падащото меню **Причина за изпращането на файла**, което най-добре отговаря на целта на вашето съобщение:

- Подозрителен файл
- Подозрителен сайт (уеб сайт, който е заразен със злонамерен софтуер),
- Грешен положителен сайт
- Погрешно класифициран файл (файл, който е определен като заразен, но не е заразен);
- Други

Файл/сайт – Пътят до файла или уеб сайта, който възнамерявате да изпратите.

Имейл за контакт – имейл адресът за контакт се изпраща заедно с подозрителните файлове на ESET и може да се използва за връзка с вас, ако е необходима допълнителна информация за анализа. Въвеждането на имейл адрес за контакт не е задължително. Изберете **Анонимно изпращане**, за да го оставите празно.

> **Възможно е да не получите отговор от ESET**
> Няма да получите отговор от ESET, освен ако не е необходима допълнителна информация. Ежедневно в сървърите ни се получават десетки хиляди файлове, което прави невъзможно отговарянето на всички съобщения.
> Ако примерът се окаже злонамерено приложение или уеб сайт, информацията за него ще бъде добавена в някое от следващите обновявания на ESET.

Изпращане на файл за анализ – подозрителен файл

Наблюдавани признаци и симптоми за инфекция със зловреден код – Въведете описание на поведението на подозрителния файл, наблюдавано на компютъра.

Произход на файла (URL адрес или доставчик) – Въведете произход на файла (източник) и как сте открили този файл.

Забележки и допълнителна информация – Тук можете да добавите допълнителна информация или описание, което ще ни помогне при обработването на подозрителния файл.

> Първият параметър – **Наблюдавани признаци и симптоми за инфекция със зловреден софтуер** – е задължителен, но с предоставянето на допълнителна информация ще помогнете значително на нашите лаборатории при идентифициране и обработване на шаблоните.

Изпращане на файл за анализ – подозрителен сайт

Изберете една от следните опции от падащото меню **Какъв е проблемът със сайта**:

- **Заразен** – Уеб сайт, който съдържа вируси или друг злонамерен софтуер, разпространяван по различни методи.

• **Фишингът** често се използва за получаване на достъп до поверителни данни, като например номера на банкови сметки, номера на PIN кодове и други неща. Прочетете повече за този тип атака в речника.

• **Измама** – измамен или фалшив уеб сайт, особено за натрупване на бърза печалба.

• Изберете **Друго**, ако по-горните опции не се отнасят до сайта, който ще изпратите.

Забележки и допълнителна информация – можете да въведете допълнителна информация или описание, което ще помогне за анализирането на подозрителния уеб сайт.

Изпращане на файл за анализ – грешен положителен файл

Очакваме да изпращате файлове, които са открити като зараза, но не са заразени, за да подобрим нашите системи за защита от вируси и шпионски софтуер и за да подпомогнем защитата на други. Погрешни положителни резултати (FP) може да се получат, когато схемата на даден файл съвпадне със същата схема, съдържаща се в системата за откриване.

Име и версия на приложението – Името на програмата и нейната версия (като например номер, псевдоним или кодово име).

Произход на файла (URL адрес или доставчик) – Въведете произход на файла (източник) и отбележете как сте открили файла.

Предназначение на приложението – Общото описание на приложението, типът приложение (напр. браузър, мултимедиен плейър...) и неговите характеристики.

Забележки и допълнителна информация – Тук можете да добавите допълнителна информация или описание, което ще ни помогне при обработването на подозрителния файл.

> Първите три параметъра са задължителни, за да можем да идентифицираме надеждните приложения и да ги разграничим от злонамерения код. С предоставянето на допълнителна информация ще спомогнете значително на нашите лаборатории за идентифициране и обработване на шаблоните.

Изпращане на файл за анализ – грешен положителен сайт

Обръщаме се към вас с молба да изпращате сайтове, които са открити като заразени, заплаха или фишинг, но не са. Погрешни положителни резултати (FP) може да се получат, когато схемата на даден файл съвпадне със същата схема, съдържаща се в системата за откриване. Изпратете този уеб сайт, за да подобрим нашата система за защита от вируси и фишинг и да подпомогнем защитата на други.

Забележки и допълнителна информация – тук можете да добавите допълнителна информация или описание, което ще ни помогне при обработването на подозрителния уеб сайт.

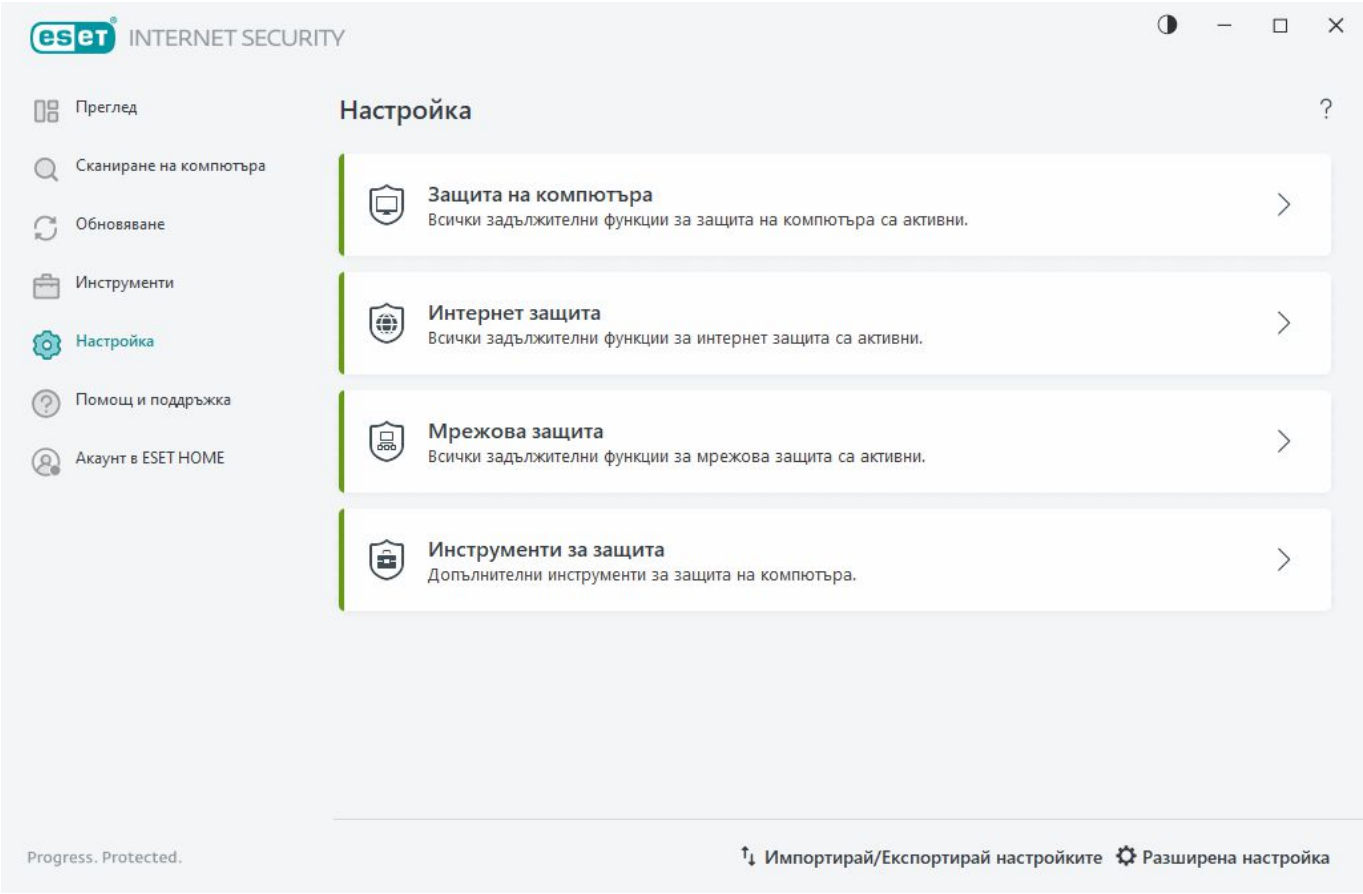
Изпращане на файл за анализ – други

Използвайте този формуляр, ако файлът не може да се класифицира като **Подозрителен файл** или като **Грешен положителен резултат**.

Причина за изпращане на файла – Въведете подробно описание и причината за изпращането на файла.

Настройка

Можете да намерите групи от налични функции за защита в главния прозорец на програмата > **Настройка**.



Менюто **Настройка** е разделено на следните групи:

Защита на компютъра

Интернет защита

Мрежова защита

Инструменти за защита

Допълнителни опции са налични в долната част на прозореца за настройка. Щракнете върху

Разширени настройки, за да конфигурирате още подробни параметри за всеки модул. Използвайте Импортиране/експортиране на настройки, за да заредите параметри за настройка с помощта на .xml конфигурационен файл или да запишете текущите параметри за настройка в конфигурационен файл.

Защита на компютъра

Щракнете върху **Защита на компютъра** в главния прозорец на програмата > **Настройка**, за да видите общ преглед на всички модули за защита:

- Защита на файловата система в реално време – всички файлове се сканират за злонамерен код, когато бъдат отворени, създадени или изпълнени.
- Управление на устройства – Този модул дава възможност да сканирате, блокирате или настройвате разширени филтри/разрешения и да избирате как потребителят може да осъществява достъп и да използва определено устройство (CD/DVD/USB...).
- HIPS – Системата HIPS наблюдава събитията в операционната система и реагира на тях в съответствие с персонализиран набор от правила.
- Режим за геймъри – Разрешава или забранява Режим за геймъри. Ще получите предупредително съобщение (потенциален риск за защитата) и главният прозорец ще светне в оранжево след разрешаването на игралния режим.
- Защита на уеб камерата – Контролира процесите и приложенията, които имат достъп до свързаната с уеб камера.

За да спрете на пауза или забраните отделни модули за защита, щракнете върху иконата на превключвате .

> Изключването на модулите за защита може да намали нивото на защита на вашия компютър.

Щракнете върху иконата на зъбно колело до модул за защита, за да осъществите достъп до разширените настройки за този модул.

За **Защитата на файловата система в реално време** щракнете върху иконата на зъбно колело и изберете от следните опции:

- **Конфигуриране** – Отваря разширените настройки на защитата на файловата система в реално време.
- **Редактиране на изключенията** – Отваря прозореца за настройка на изключенията, така че да можете да изключвате файлове и папки от сканирането.

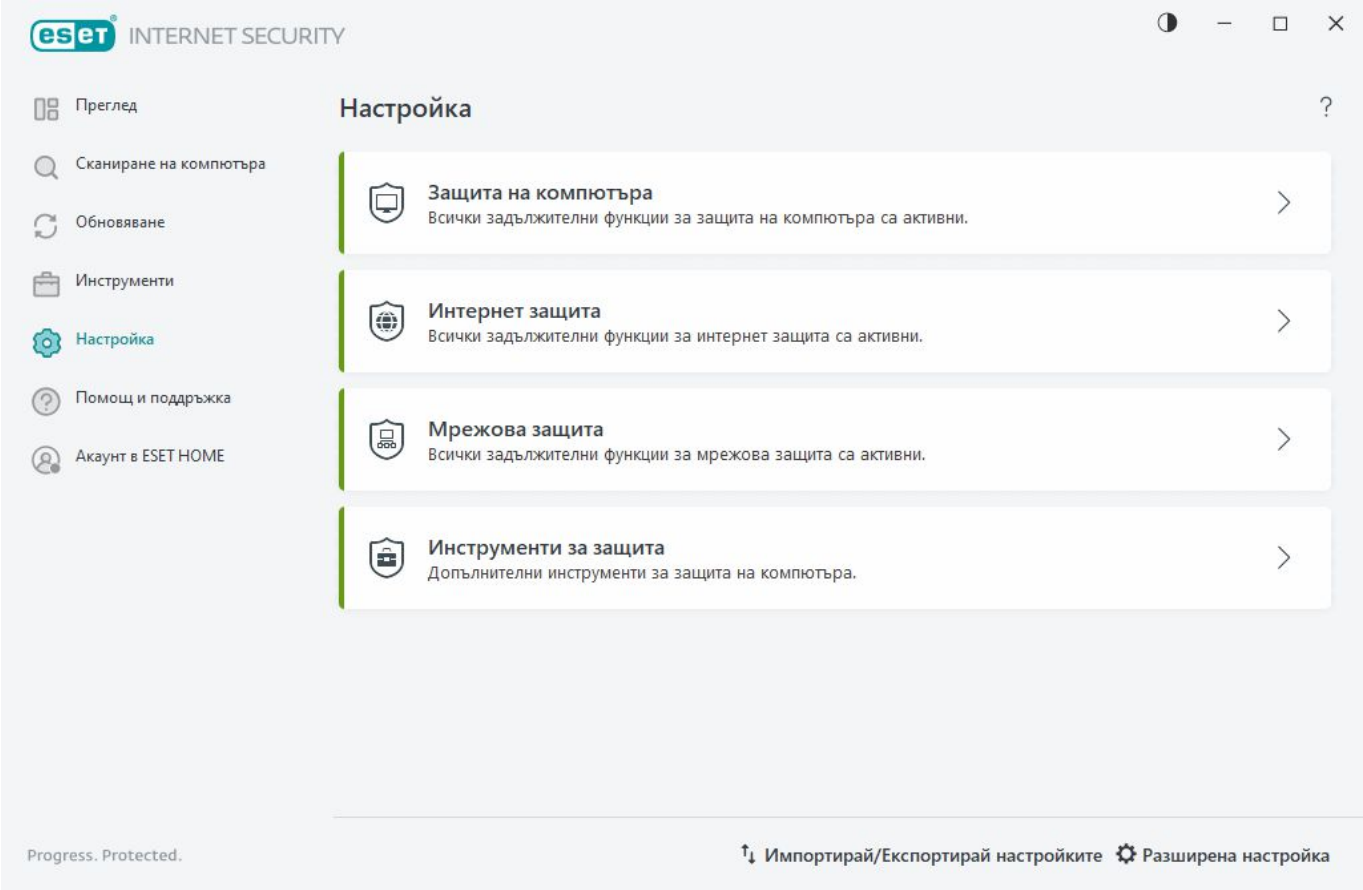
За **Защита на уеб камерата** щракнете върху иконата на зъбно колело и изберете от следните опции:

- **Конфигуриране** – Отваря разширените настройки на защитата на уеб камерата.
- **Блокиране на целия достъп до рестартиране** – Блокира целия достъп до уеб

камерата, докато компютърът се рестартира.

• **Блокиране на целия достъп за постоянно** – Блокира целия достъп до уеб камерата, докато тази настройка не бъде деактивирана.

• **Спиране на блокирането на целия достъп** – Забранява възможността за блокиране на достъпа до уеб камерата. Тази опция е налична само ако достъпът до уеб камерата е блокиран.



Временно спиране на защитата от вируси и шпионски софтуер – Забранява всички модули за защита от вируси и шпионски софтуер. Когато забраните защитата, ще се отвори прозорец, в който можете да определите за колко време да бъде изключена защитата чрез падащото меню **Времеви интервал**. Използвайте само ако сте опитен потребител или сте инструктирани от техническата поддръжка на ESET.

Открито е проникване

Проникванията могат да влязат в системата през различни точки за достъп, като например уеб страници, споделени папки, електронна поща или преносими устройства (USB, външни дискове, CD и DVD дискове и др.).

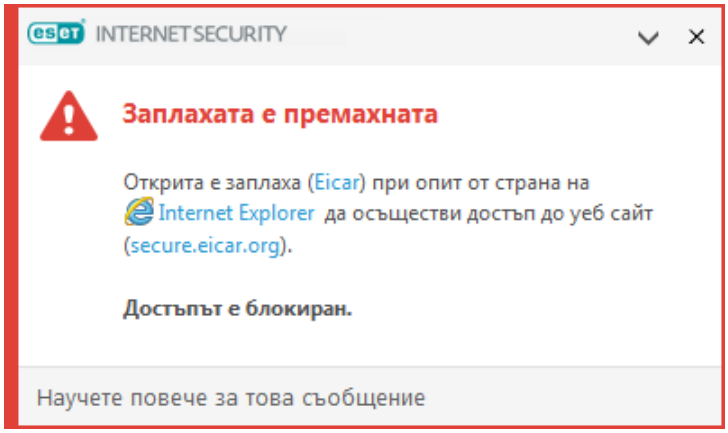
Стандартно поведение

Като общ пример как проникванията се обработват от ESET Internet Security, те могат да бъдат открити чрез:

• Защита на файловата система в реално време

- Защита на уеб достъпа
- Защита на имейл клиенти
- Сканиране на компютъра при поискване

Всяка от тях използва стандартното ниво на почистване и ще се опита да почисти файла и да го премести в папката Карантина или да прекъсне връзката. Прозорецът за известие се показва в областта за известяване в долния десен ъгъл на екрана. За подробна информация относно откритите/почистените обекти вижте Регистрационни файлове. За повече информация относно нивата и поведението на функцията за почистване вижте Ниво на почистване.



Сканиране на компютъра за заразени файлове

Ако компютърът дава признаци за зараза със злонамерен софтуер, като например работи по-бавно, често блокира и т.н., ви препоръчваме да направите следното:

1.Отворете ESET Internet Security и щракнете върху **"Сканиране на компютъра„**.

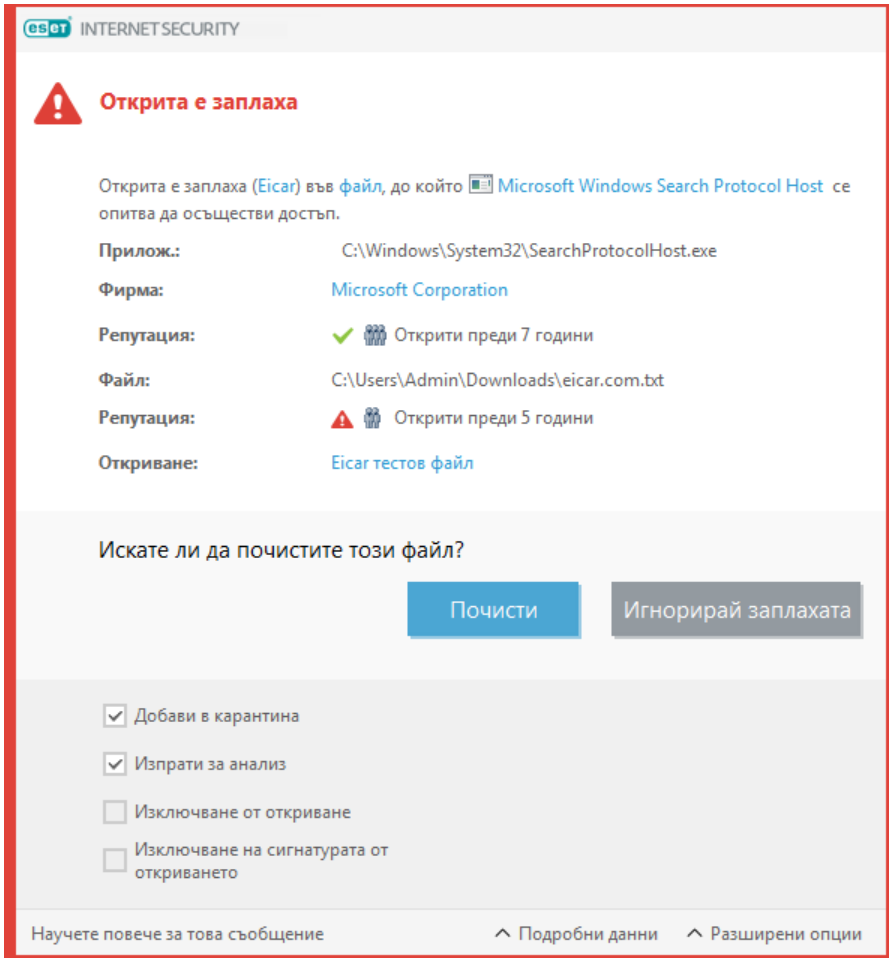
2.Щракнете върху **Сканиране на компютъра** (за повече информация вижте Сканиране на компютъра).

3.След като сканирането завърши, прегледайте регистрационния файл за броя на сканираните, заразените и почистените файлове.

Ако искате само да сканирате определена област от диска, щракнете върху **Сканиране по избор** и изберете целите за сканиране за вируси.

Почистване и изтриване

Ако няма предварително зададено действие, което да се изпълни от защитата на файловата система в реално време, ще получите подкана за избор на опция в предупредителен прозорец. Обикновено са налични опциите **Почисти**, **Изтрий** и **Никакво действие**. Не е препоръчително да изберете **Никакво действие**, тъй като по този начин заразените файлове ще останат непочистени. Изключение може да се направи единствено ако сте сигурни, че даден файл е безопасен и е открит по погрешка.



Приложете почистване, ако файлът е атакуван от вирус, който е прикачил злонамерен код към него. В такъв случай първо се опитайте да почистите заразения файл, за да го възстановите на първоначалното място. Ако файлът се състои само от злонамерен код, той ще бъде изтрит.

Ако заразеният файл е "заключен" или се използва от системен процес, той обикновено се изтрива веднага след освобождаването му (обикновено след рестартиране на системата).

Възстановяване от карантина

Можете да осъществите достъп до карантината от главния програмен прозорец на ESET Internet Security, като щракнете върху **Инструменти** > **Карантина**.

Файловете под карантина също могат да бъдат възстановени до първоначалното им местоположение:

- Използвайте функцията за **Възстановяване** за тази цел, която е налична от контекстното меню, като щракнете с десния бутон върху даден файл в карантината.
- Ако даден файл е маркиран като потенциално нежелано приложение, опцията **Възстановяване и изключване от сканиране** е разрешена. Вижте също Изключения.
- Контекстното меню също предлага опцията **Възстановяване до**, която ви позволява да възстановите файл на място, различно от това, от което е премахнат.
- Функцията за възстановяване не е налична в някои случаи, например за файлове, намиращи се в мрежов дял само за четене.

Много заплахи

Ако заразени файлове не бъдат почистени по време на сканиране на компютъра (или Нивото на почистване е зададено на **Без почистване**), ще се покаже предупредителен прозорец, който ви подканва да изберете действия за файловете. Изберете действията за файловете (действията се задават за всеки файл в списъка поотделно), след което щракнете върху **Готово**.

Изтриване на файлове в архиви

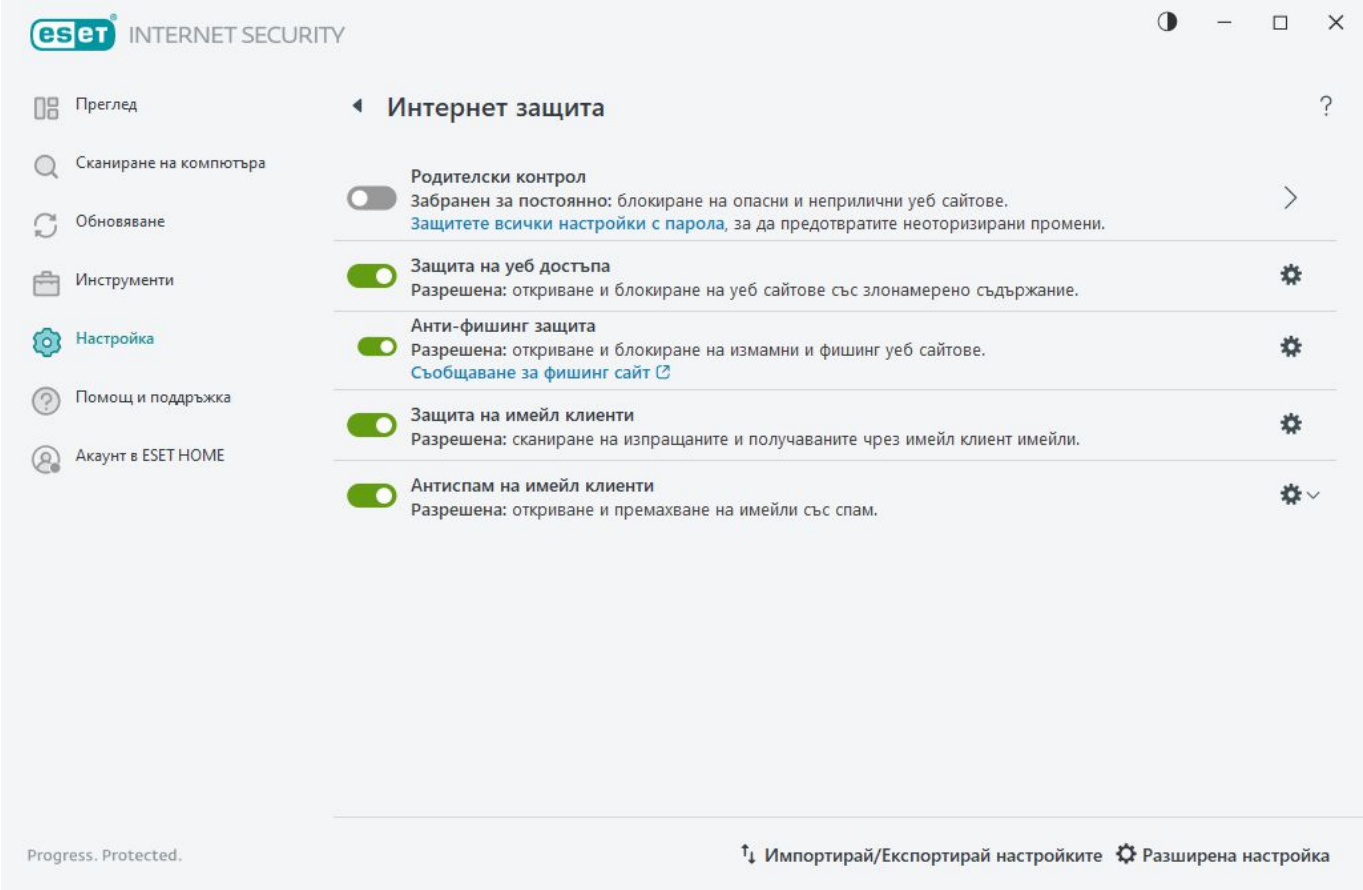
В режим на почистване по подразбиране ще се изтрие целият архив, ако съдържа само заразени файлове и никакви чисти файлове. С други думи, архивите не се изтриват, ако съдържат също така и безвредни чисти файлове. Внимавайте при изпълнение на сканиране със строго почистване – при разрешен режим на строго почистване даден архив се изтрива, ако съдържа поне един заразен файл, независимо какво е състоянието на останалите файлове в архива.

Интернет защита

Интернет връзката е стандартна функция за всеки персонален компютър. За съжаление тя се е превърнала в основно средство за прехвърляне на злонамерен код. Отворете главния прозорец на програмата > **Настройка** > **Интернет защита**, за да конфигурирате функции в ESET Internet Security, които увеличават вашата интернет защита.

За да спрете на пауза или забраните отделни модули за защита, щракнете върху иконата на превключвате .

Изключването на модулите за защита може да намали нивото на защита на вашия компютър.



Щракнете върху иконата на зъбно колело ⚙ до модул за защита, за да осъществите достъп до разширените настройки за този модул.

Модулът родителски контрол защитава децата ви, като блокира неподходящо или вредно съдържание в интернет.

Защита на уеб достъпа сканира HTTP/HTTPS комуникацията за злонамерен софтуер и фишинг. Защитата на уеб достъпа трябва да се изключва само за отстраняване на неизправности.

Функция за анти-фишинг защита ви позволява да блокирате уеб страници, известни с разпространението на фишинг съдържание. Силно препоръчително е да оставите анти-фишинг защитата разрешена.

Подаване на сигнал за фишинг сайт – Съобщете за фишинг/злонамерен уеб сайт на ESET за анализ.

> Преди да изпратите уеб сайт на ESET, се уверете, че той отговаря на един или повече от следните критерии:
> • Уеб сайтът не е открит изобщо.
> • Уеб сайтът е открит неправилно като заплаха. В този случай можете да съобщите за неправилно блокирана страница.

Функцията Защита на имейл клиенти осигурява контрол върху съобщенията, получени чрез POP3(S) и IMAP(S) протоколи. Чрез използване на добавката за вашия имейл клиент ESET Internet Security осигурява контрол над всички съобщения от имейл клиента.

Антиспам на имейл клиенти филтрира нежелани имейл съобщения.

За **Антиспам на имейл клиенти** щракнете върху иконата на зъбно колело и изберете от следните опции:

• **Конфигуриране** – Отваря разширени настройки за антиспам на имейл клиенти.

• **Списък с адреси на потребителя** (ако е разрешен) – Отваря диалогов прозорец, в който може да добавяте, редактирате или премахвате адреси за определяне на правилата за антиспам. Правилата в този списък ще бъдат приложени към текущия потребител.

• **Глобален списък с адреси** (ако е разрешен) – Отваря диалогов прозорец, в който може да добавяте, редактирате или премахвате адреси за определяне на правилата за антиспам. Правилата в този списък ще се прилагат за всички потребители.

Анти-фишинг защита

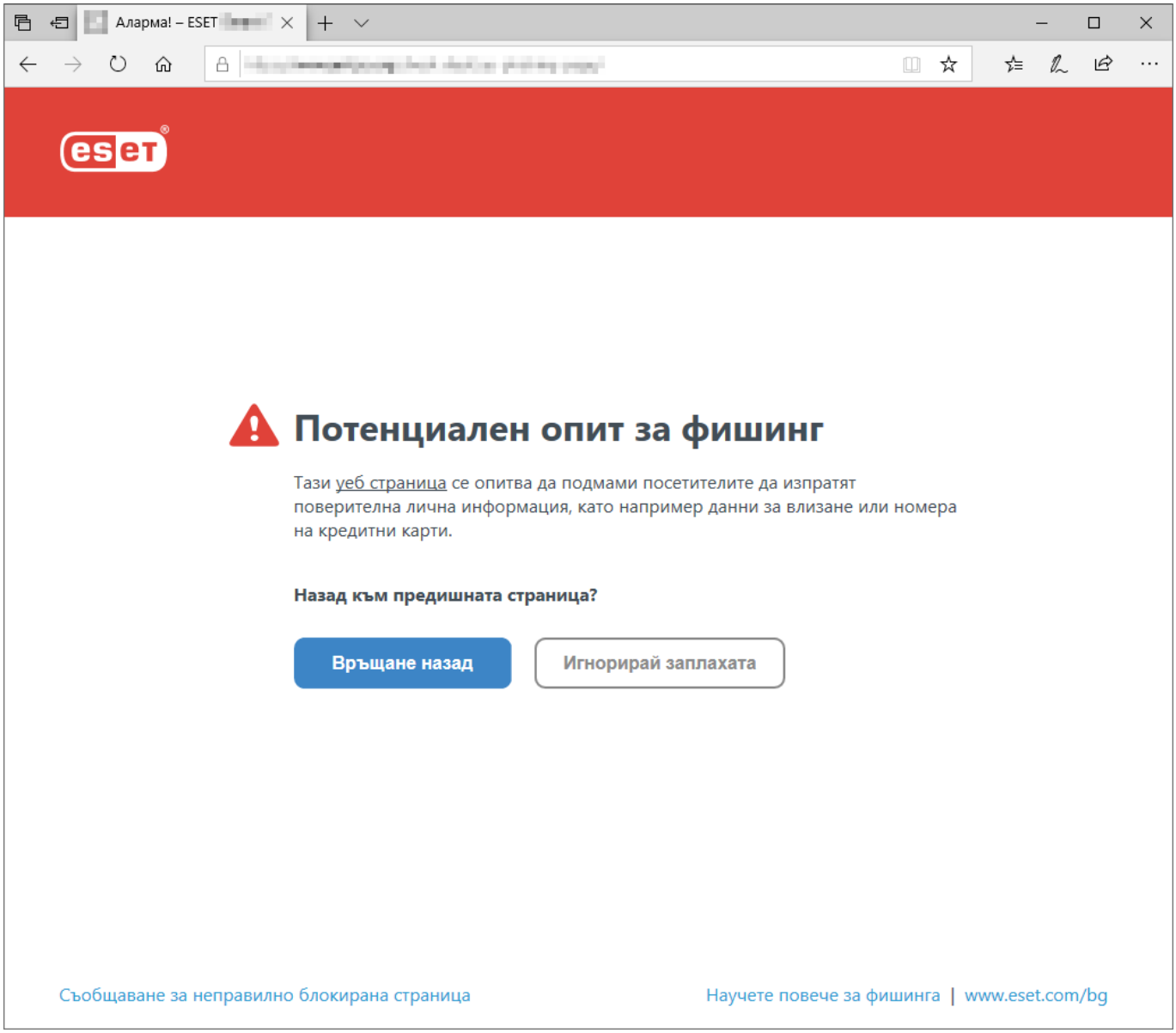
Фишингът е незаконна дейност, при която се използват измамнически техники (манипулиране на потребителите с цел извличане на поверителна информация). Фишингът се използва за получаване на достъп до поверителни данни, като например номера на банкови сметки, ПИН кодове и др. За повече информация вж. речника. ESET Internet Security включва анти-фишинг защита, която блокира уеб страниците, за които е известно, че разпространяват такова съдържание.

Анти-фишинг защитата е разрешена по подразбиране. Тази настройка може да се конфигурира в Разширени настройки > **Защити** > **Защита на уеб достъпа**.

Прочетете нашата статия в базата данни за допълнителна информация относно антифишинг защитата в ESET Internet Security.

Достъп до фишинг уеб сайт

Когато получите достъп до разпознат уеб сайт за фишинг, вашият уеб браузър ще покаже следния диалогов прозорец. Ако все пак искате да отворите уеб сайта, щракнете върху **Игнорирай заплахата** (не е препоръчително).



Потенциалните фишинг уеб сайтове, които фигурират в списъка с разрешени адреси, ще изтекат след няколко часа по подразбиране. За да разрешите даден уеб сайт за постоянно, използвайте инструмента Управление на URL адреси. От Разширени настройки > **Защити** > **Защита на уеб достъпа** > **Управление на URL адреси** > **Списък с адреси** > **Редактиране** добавете към списъка уеб сайта, който искате да редактирате.

Съобщаване за фишинг сайт

Връзката **Докладване на неправилно блокирана страница** ви позволява да подавате сигнал за уеб сайт, който е неправилно засечен като заплаха.

Уеб сайтът може да се изпрати също така и по електронна поща. Изпратете вашето съобщение до samples@eset.com. Не забравяйте да използвате описателна тема и да включите възможно най-много информация за уеб сайта (например уеб сайта, който ви е насочил към него, как сте научили за този уеб сайт и т.н.).

Родителски контрол

Модулът за родителски контрол позволява да конфигурирате настройките за родителски контрол, които предоставят на родителите автоматизирани инструменти за защита на техните деца и за задаване на ограничения за устройства и услуги. Целта е да се предотврати достъпът на деца и младежи до страници с неподходящо или вредно съдържание.

Родителският контрол ви позволява да блокирате уеб страници, които може да съдържат потенциално неприлично съдържание. Освен това родителите могат да забранят достъпа до повече от 40 предварително определени категории уеб сайтове и над 140 подкатегории.

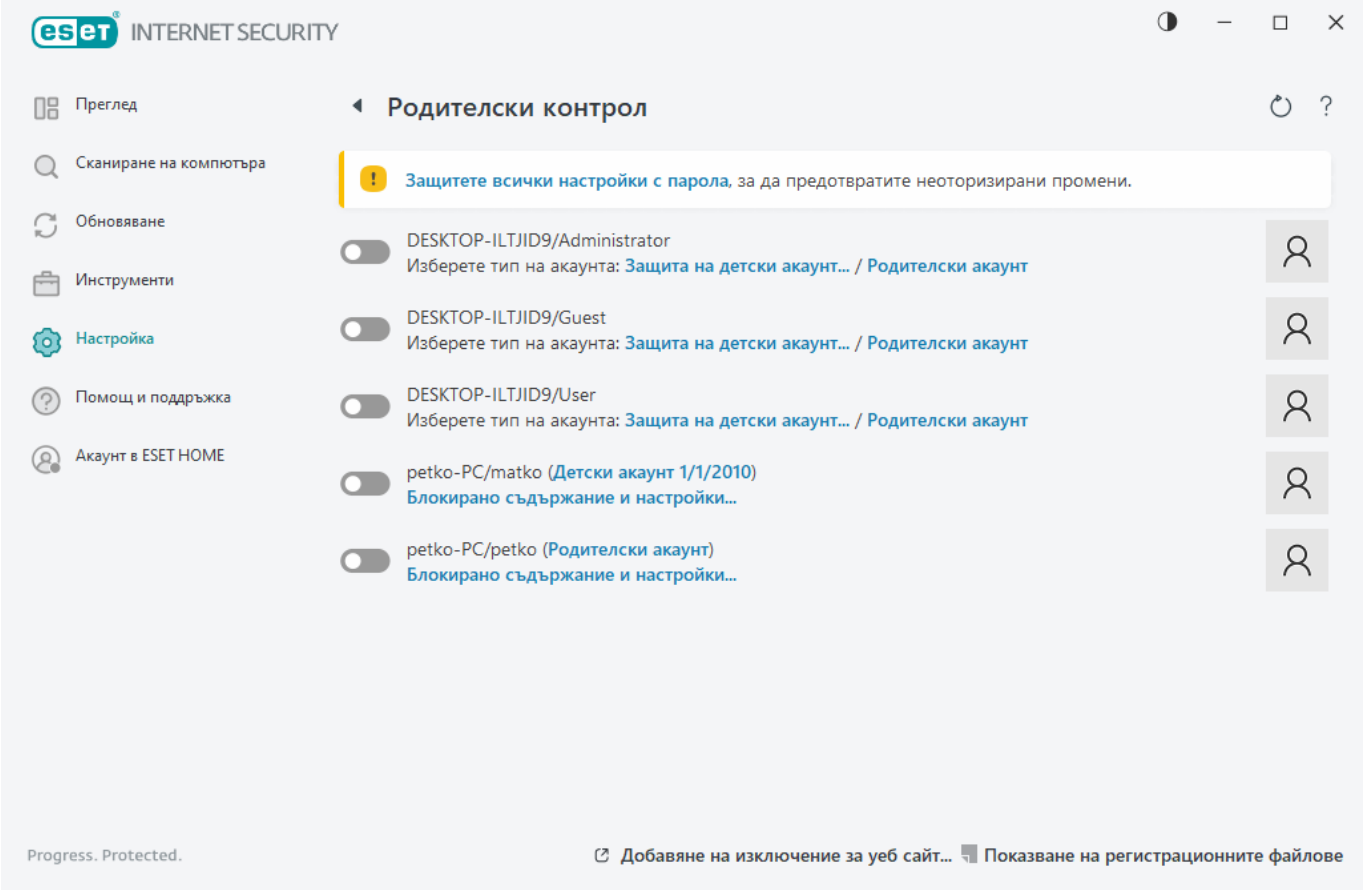
За да активирате родителски контрол за определен потребителски акаунт, следвайте стъпките по-долу:

1. По подразбиране родителският контрол е забранен в ESET Internet Security. Съществуват два метода за активиране на родителски контрол:

   • Щракнете върху иконата на плъзгача в **Настройка** > **Интернет защита** > **Родителски контрол** от главния прозорец на програмата и променете състоянието на функцията за родителски контрол на разрешено.

   • Отворете Разширени настройки > **Защити** > **Защита на уеб достъпа** > **Родителски контрол**, след което активирайте превключвателя до **Активиране на родителски контрол**.

2. Щракнете върху **Настройка** > **Интернет защита** > **Родителски контрол** от главния прозорец на програмата. Дори ако **Разрешено** се показва до **Родителски контрол**, трябва да конфигурирате родителския контрол за желания акаунт, като щракнете върху символа за стрелка, след което в следващия прозорец изберете **Защита на детски акаунт** или **Родителски акаунт**. В следващия прозорец изберете датата на раждане, за да определите нивото на достъп и препоръчителните, подходящи за възрастта, уеб страници. Родителският контрол вече е разрешен за указания потребителски акаунт. Щракнете върху **Блокирано съдържание и настройки** под името на акаунта, за да персонализирате категориите, които искате да разрешите или блокирате в раздела Категории. За да разрешите или блокирате уеб страници по избор, които не съответстват на категория, щракнете върху раздела Изключения.



Ако щракнете върху **Настройка** > **Интернет защита** > **Родителски контрол** от главния прозорец на ESET Internet Security, ще видите, че главният прозорец съдържа:

Потребителски акаунти в Windows

Ако сте създали роля за съществуващ акаунт, тя ще се покаже тук. Щракнете върху плъзгача , така че да показва зелена отметка до "Родителски контрол" за акаунта. Под активния акаунт щракнете върху Блокирано съдържание и настройки за преглед на списъка с разрешени категории на уеб страници за този акаунт и блокирани и разрешени уеб страници.

Долната част на прозореца съдържа

Добавяне на изключение за уеб сайт – Конкретният уеб сайт може да бъде разрешен или блокиран в зависимост от вашите предпочитания за всеки родителски акаунт поотделно.

Показване на регистрационните файлове – Тази опция показва подробен регистрационен файл за дейността на родителския контрол (блокирани страници, акаунта, за който е блокирана страницата, категория и т.н.). Може също така да филтрирате този регистрационен файл въз основа на избраните критерии, като щракнете върху **Филтриране**.

Родителски контрол

След като забраните родителския контрол, ще се покаже прозорец **Забраняване на родителския контрол**. В него може да зададете времевия интервал, за който защитата да е забранена. След това състоянието на опцията се променя на **В пауза** или **Постоянна забрана**.

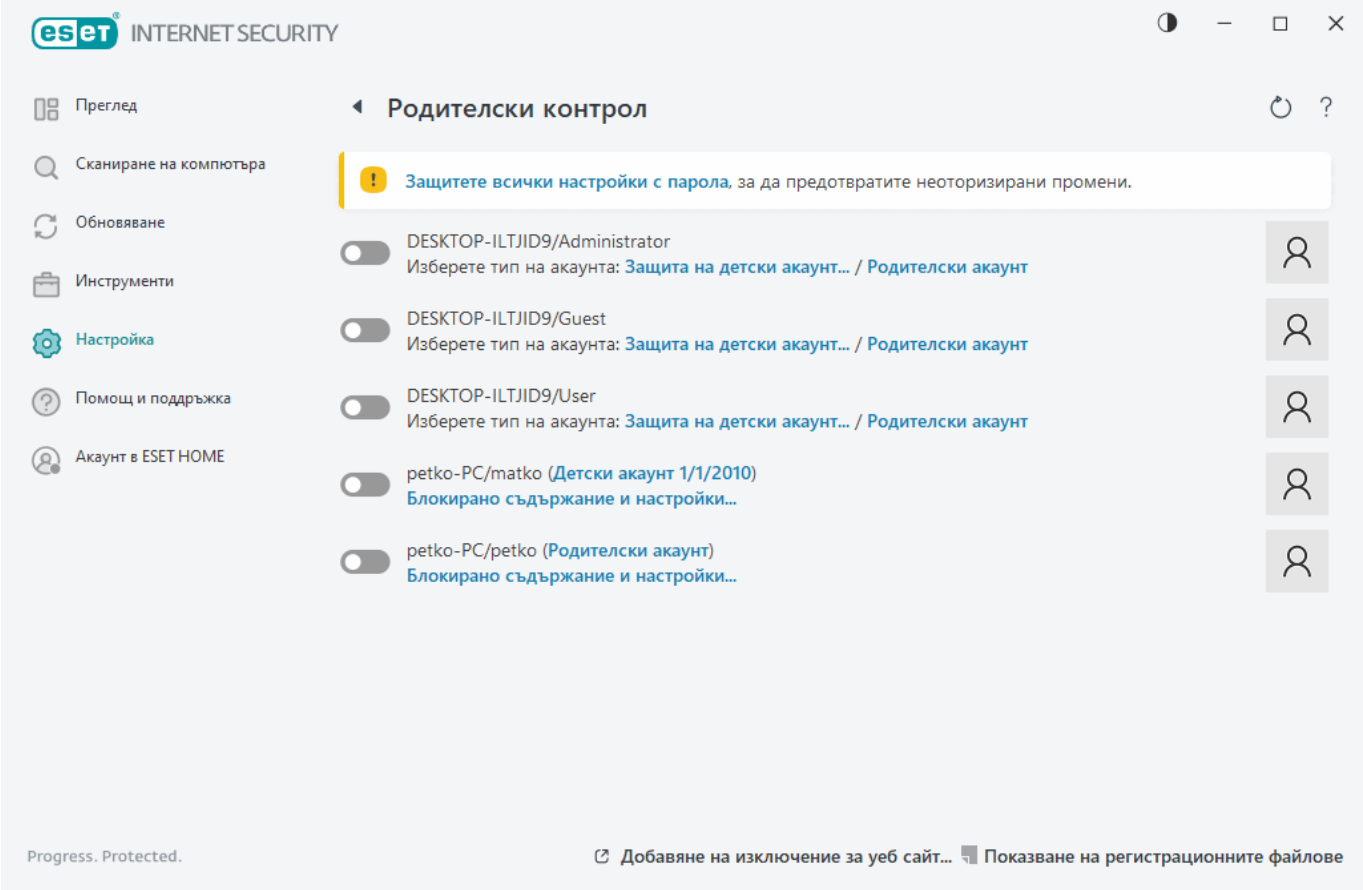
Настройките в ESET Internet Security е важно да се защитят с парола. Можете да зададете тази

парола в раздела Настройка на достъпа. Ако не е зададена парола, ще се покаже следното предупреждение – **Защитете всички настройки с парола**, за да предотвратите неоторизирани промени. Ограниченията, зададени в родителския контрол, засягат само стандартните потребителски акаунти. Тъй като администраторът може да отмени всички ограничения, те няма да имат ефект.

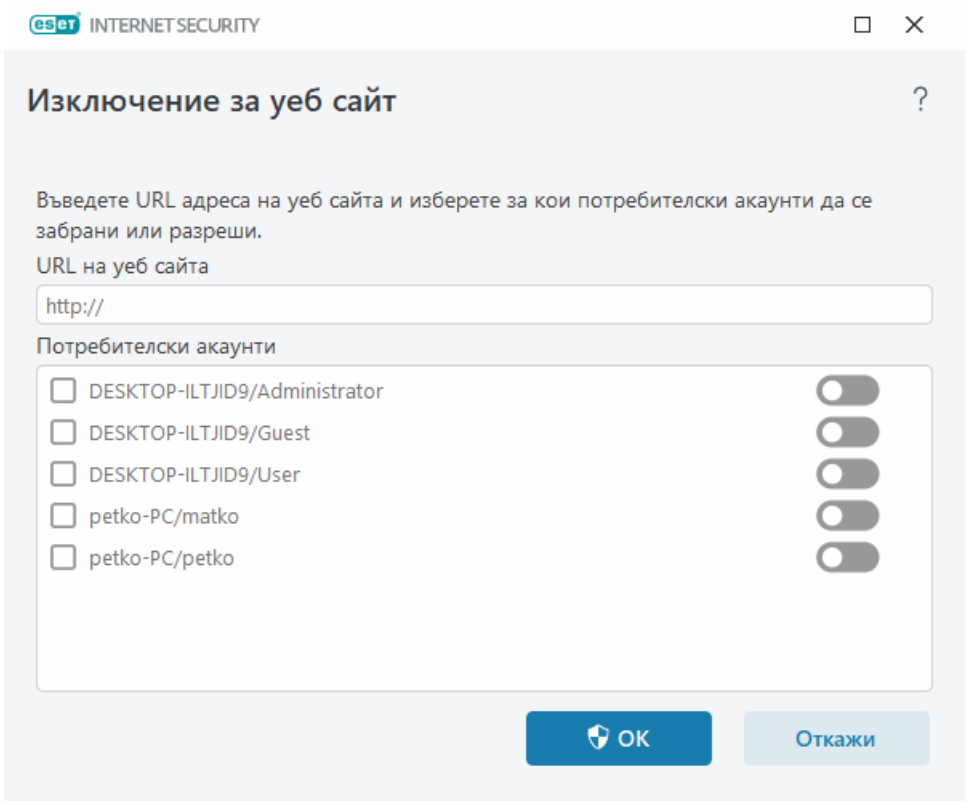
> Родителският контрол изисква скенер за мрежов трафик, HTTP(S) сканиране на трафика и защитна стена, за да може да функционира правилно. Всички тези функции са разрешени по подразбиране.

Изключения за уеб сайтове

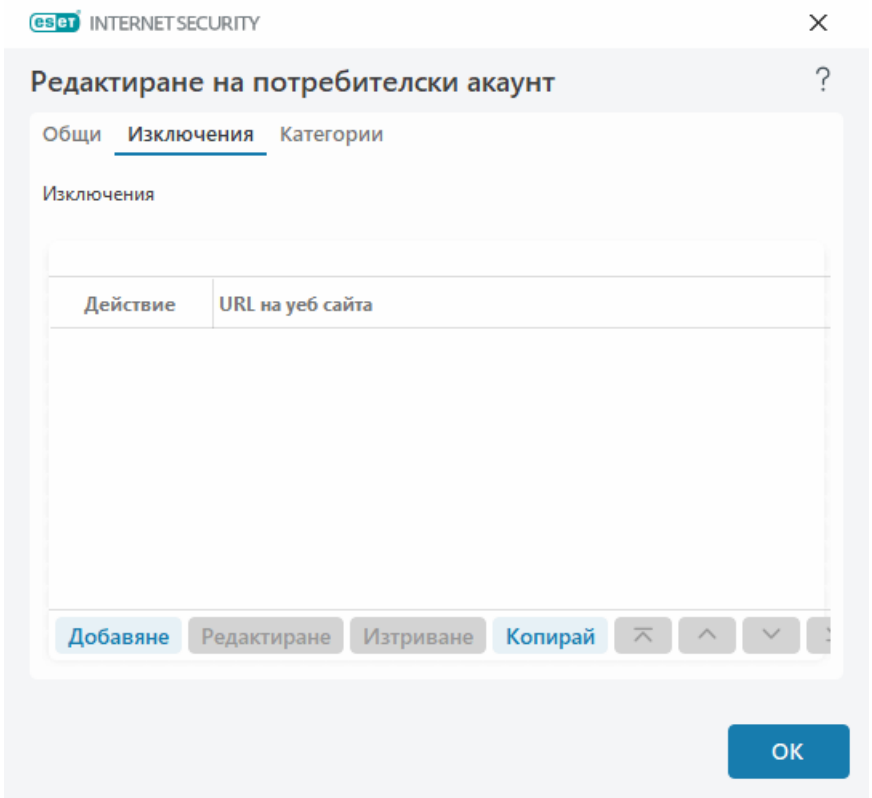
За да добавите изключение за уеб сайт, щракнете върху **Настройка** > **Интернет защита** > **Родителски контрол** и след това щракнете върху **Добавяне на изключение за уеб сайт**.



Въведете URL адрес в полето **URL на уеб сайта**, изберете ✔ (позволен) или ⊘ (блокиран) за всеки конкретен потребителски акаунт, след което щракнете върху **ОК**, за да го добавите в списъка.



За да изтриете URL адрес от списъка, щракнете върху **Настройка** > **Интернет защита** > **Родителски контрол**, щракнете върху **Блокирано съдържание и настройки** под желания потребителски акаунт, щракнете върху раздел **Изключение**, изберете изключението и щракнете върху **Премахни**.



В списъка с URL адреси специалните символи * (звездичка) и ? (въпросителен знак) не могат да се използват. Например, адреси на уеб страници с множество домейни от най-високо ниво трябва да се въведат ръчно (examplepage.com*examplepage.com, examplepage.sk*examplepage.sk и т.н.).

Когато добавите домейн към списъка, цялото съдържание на този домейн и на всички поддомейни (напр. sub.examplepage.com*sub.examplepage.com*) ще бъде блокирано или разрешено в зависимост от вашия избор на действие, базирано на URL адрес.

Блокирането или разрешаването на конкретна уеб страница може да е по-точно от блокирането или разрешаването на категория уеб страници. Внимавайте, когато променяте тези настройки и добавяте дадена категория/уеб страница към списъка.

Копиране на изключение от потребител

В падащото меню изберете потребителя, от който искате да копирате създадено изключение.

Копиране на категории от акаунт

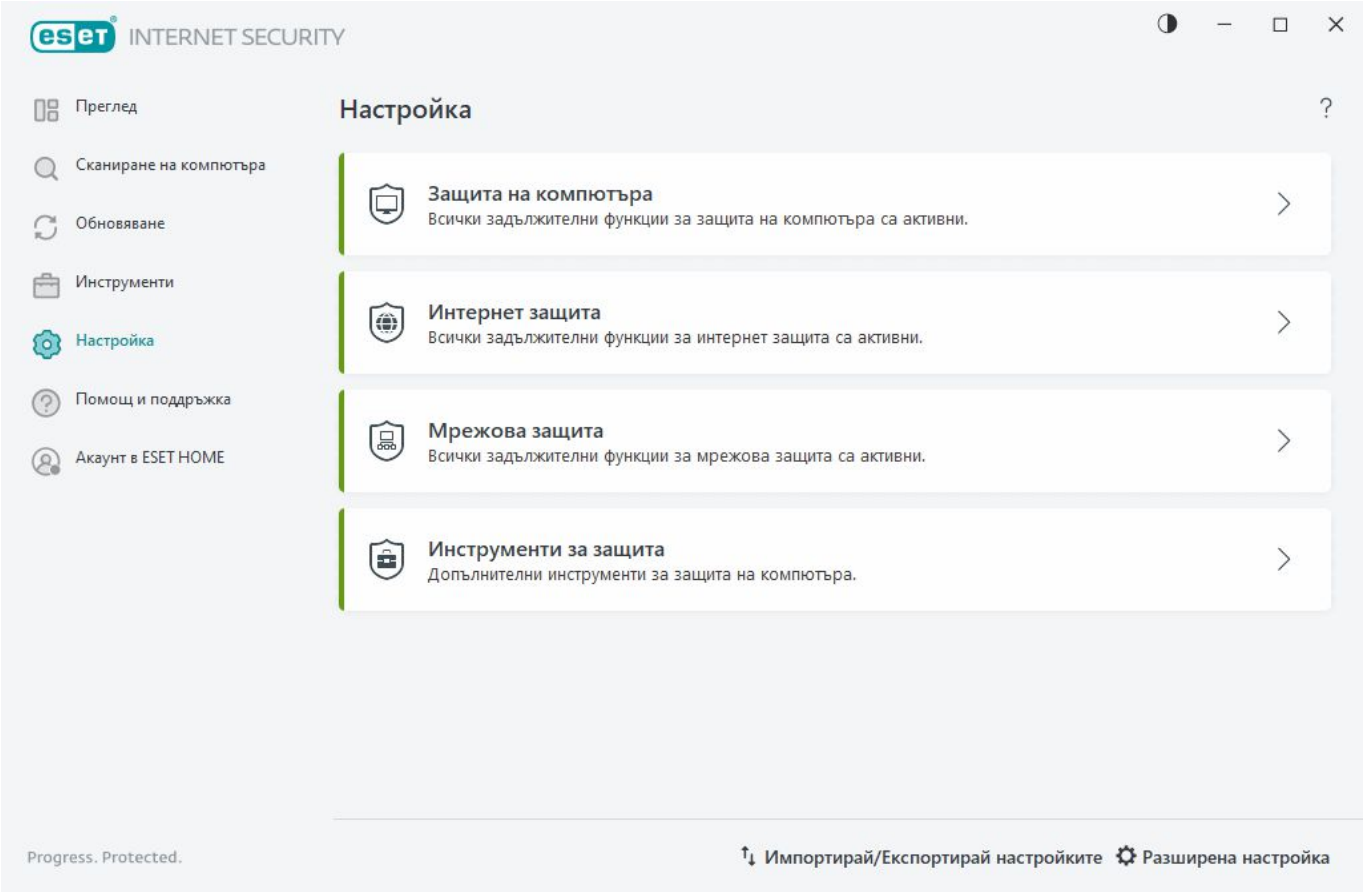
Позволява ви да копирате списък с блокирани или разрешени категории от съществуващ променен акаунт.

Защита на мрежата

Отворете главния прозорец на програмата > **Настройка** > **Мрежова защита**, за да конфигурирате основните настройки за мрежова защита или да отстраните неизправности в мрежовата комуникация.

За да спрете на пауза или забраните отделни модули за защита, щракнете върху иконата на превключвате .

Изключването на модулите за защита може да намали нивото на защита на вашия компютър.



Щракнете върху иконата на зъбно колело ⚙ до модул за защита, за да осъществите достъп до разширените настройки за този модул.

Защитна стена – Филтрира цялата мрежова комуникация въз основа на конфигурирането на ESET Internet Security.

Конфигуриране – Отваря прозореца Разширени настройки на защитна стена, където можете да определите начина, по който защитната стена ще обработва мрежовата комуникация.

Паузиране на защитна стена (позволяване на целия трафик) – Всички опции за филтриране на защитната стена се изключват, а всички входящи и изходящи връзки се разрешават. Щракнете върху **Разреши защитната стена**, за да разрешите отново защитната стена, когато филтрирането на мрежовия трафик е в този режим.

Блокиране на целия трафик – Цялата входяща и изходяща комуникация ще се блокира от защитната стена. Използвайте тази опция само ако имате съмнения за критичен риск за защитата, който изисква изключване на системата от мрежата. Когато за филтриране на мрежовия трафик е зададен режим **Блокиране на целия трафик**, щракнете върху **Спиране на блокирането на целия трафик**, за да възстановите нормалното функциониране на защитната стена.

Автоматичен режим – (когато е избран друг режим на филтриране) – щракнете тук, за да зададете автоматичен режим на филтриране (със зададени от потребителя правила).

Интерактивен режим – (когато е избран друг режим на филтриране) – щракнете тук, за да зададете интерактивен режим на филтриране.

Защита от мрежови атаки (IDS) – анализира съдържанието на мрежовия трафик и защитава от мрежови атаки. Трафикът, който бъде счетен за вреден, ще бъде блокиран. ESET Internet Security

ще ви информира, когато се свързвате към незащитена безжична мрежа или мрежа със слаба защита.

Ботнет защита – Бързо и точно открива злонамерен софтуер във вашата система.

Мрежови връзки – Показва мрежите, с които са свързани мрежовите адаптери с подробна информация.

Разрешаване на блокирана комуникация – Помага да разрешавате проблеми при свързването, причинени от защитната стена на ESET. За по-подробна информация вж. Съветник за отстраняване на неизправности.

Разрешаване на временно блокирани IP адреси – Преглед на списък с IP адреси, които са открити като източник на атаки и са добавени в списъка със забранени адреси, за да блокира връзката за определен период от време

Показване на дневник – Отваря регистрационния файл на мрежовата защита.

Мрежови връзки

Показва мрежите, с които са свързани мрежовите адаптери. За да видите мрежовите връзки, отворете главния прозорец на програмата > **Настройка** > **Мрежова защита** > **Мрежови връзки**.

Щракнете двукратно върху връзка в списъка, за да покажете нейните подробни данни и подробни данни за мрежовия адаптер.

Задръжте курсора на мишката върху конкретна мрежова връзка и щракнете върху иконата ⋮ на менюто в колоната **Надеждни**, за да изберете една от следните опции:

- **Редактиране** – Отваря прозореца Конфигуриране на мрежова защита, където можете да присвоите профил за мрежова защита към конкретна мрежа
- **Забравяне** – Възстановява конфигурацията на мрежовата връзка по подразбиране
- **Сканиране на мрежа с Мрежов инспектор** – Отваря Мрежов инспектор за стартиране на мрежово сканиране.
- **Маркиране като „Моята мрежа“** – Добавя етикет „Моята мрежа“ към мрежата. Този етикет ще бъде показан до мрежата в ESET Internet Security за по-добра идентификация и преглед на защитата
- **Премахване на маркирането като „Моята мрежа“** – премахва етикета „Моята мрежа“. Налична само ако мрежата вече е с поставен етикет

Подробни данни за мрежова връзка

Щракнете двукратно върху връзка в списъка с Мрежови връзки, за да покажете нейните подробни данни заедно с подробните данни за мрежовия адаптер. Подробностите за мрежовата връзка и адаптера могат да ви помогнат да идентифицирате мрежата, която се

опитвате да конфигурирате в Защита на мрежовия достъп.

Подробни данни за мрежова връзка:

- Състояние на мрежовата връзка
- Дата и час на първото откриване на мрежата
- Час на последна активност на мрежата
- Общо време на свързаност към тази мрежа
- Профил за мрежова връзка
- Профил на мрежовата връзка, дефиниран в Windows
- Конфигуриране на мрежова защита (дали мрежата е надеждна)

Подробни данни за мрежовия адаптер:

- Тип на връзката (кабелна, виртуална и т.н.)
- Име на мрежовия адаптер
- Описание на адаптера
- IP адрес с MAC адрес
- IPv4 и IPv6 адрес на мрежата с подмрежа
- DNS суфикс
- IP на DNS сървър
- IP на DHCP сървър
- IP и MAC адрес на шлюза по подразбиране
- MAC адрес на адаптера

Отстраняване на неизправности с мрежовия достъп

Съветникът за отстраняване на неизправности ви помага да разрешавате проблеми при свързването, причинени от защитната стена на. **Отстраняване на неизправности с мрежовия достъп** може да бъде намерено в главния прозорец на програмата > **Настройка** > **Мрежова защита** > **Разрешаване на блокирана комуникация**.

Изберете дали искате да покажете комуникацията, блокирана за **Локални приложения**, или комуникация, блокирана от **Отдалечени устройства**.

От падащото меню изберете времеви период, в течение на който комуникацията е била

блокирана. Списък с блокирани наскоро комуникации ви предоставя обобщение на типа на приложението или устройството, репутацията и общия брой приложения и устройства, които са блокирани в рамките на този период. За повече подробности относно блокираната комуникация щракнете върху **Подробни данни**. Следващата стъпка е да отблокирате приложението или устройството, с което срещате проблеми в свързването.

Когато щракнете върху **Деблокиране**, блокираната по-рано комуникация ще бъде разрешена. Ако продължите да изпитвате проблеми с дадено приложение или вашето устройство не функционира по очаквания начин, щракнете върху **създаване на друго правило** и всички блокирани по-рано комуникации за това устройство ще бъдат позволени. Ако проблемът продължава да възниква, рестартирайте компютъра.

Щракнете върху **Отваряне на правила за защитната стена**, за да видите правилата, създадени от съветника. Освен това можете да прегледате правилата, създадени от съветника, в Разширени настройки > **Защити** > **Защита на мрежовия достъп** > **Защитна стена** > **Правила** > **Редактиране**.

Ако правилото не може да бъде създадено, ще получите съобщение за грешка. Щракнете върху **Опитайте отново** и повторете процеса, за да отмените блокирането на комуникацията или да създадете друго правило от списъка с блокирани комуникации.

Списък с временно блокирани IP адреси

За да прегледате IP адресите, които са открити като източници на атаки и са добавени в списъка със забранени адреси, за да се блокира връзката с тях за определен период от време, отворете главния прозорец на програмата > **Настройка** > **Мрежова защита** > **Разрешаване на временно блокирани IP адреси**. Временно блокираните IP адреси са блокирани за 1 час.

Колони

IP адрес – показва IP адрес, който е блокиран.

Причина за блокиране – показва типа атака, който е бил избегнат от този адрес (например атака със сканиране на TCP порт).

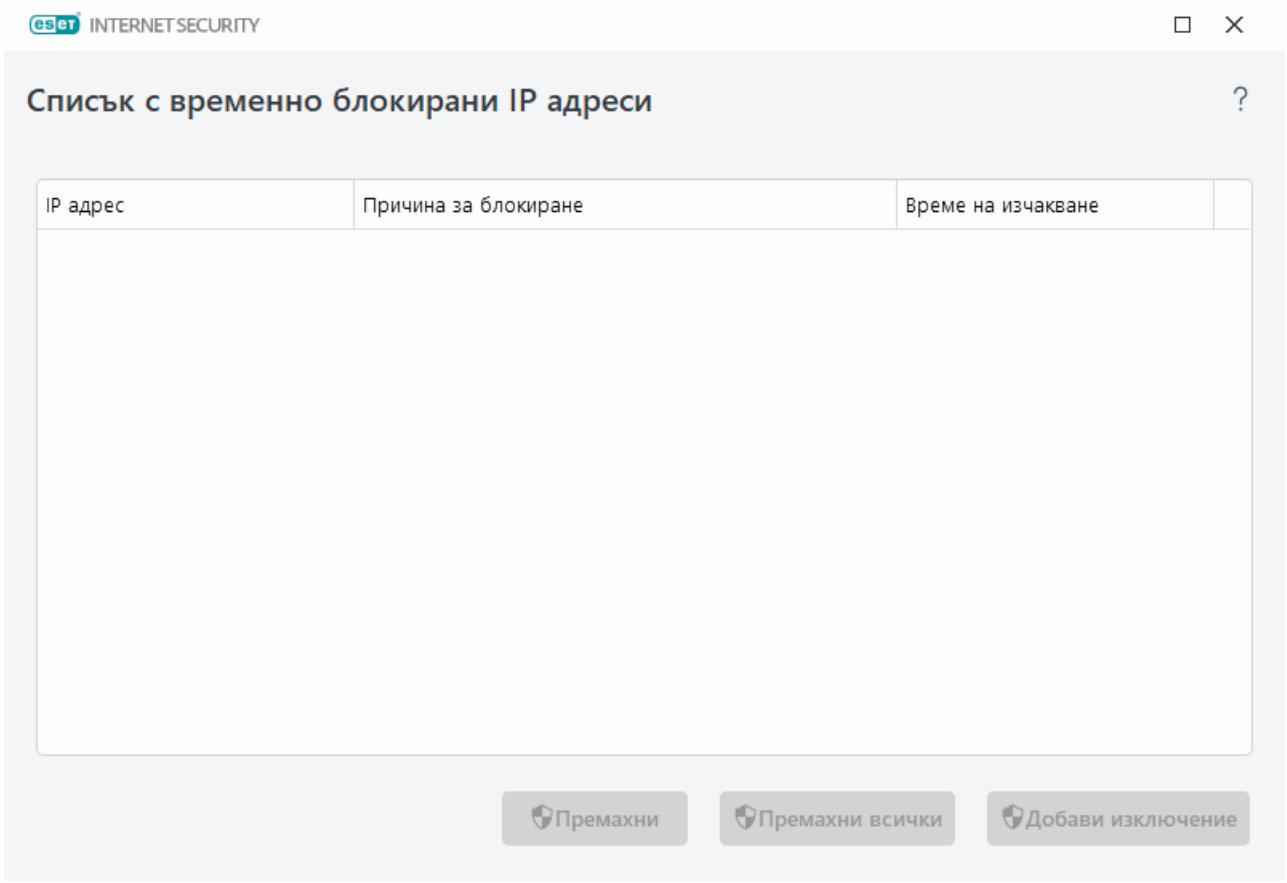
Време на изчакване – показва часът и датата, когато адресът ще бъде премахнат от списъка със забранени адреси.

Контролни елементи

Премахни – щракнете, за да премахнете адрес от списъка със забранени адреси, преди да изтече времето на изчакване.

Премахни всички – щракнете, за да премахнете незабавно всички адреси от списъка със забранени адреси.

Добави изключение – щракнете, за да добавите изключение на защитна стена в IDS филтриране.



Дневник на мрежова защита

Мрежовата защита на ESET Internet Security записва всички важни събития в регистрационен файл. За да видите регистрационния файл, отворете главния прозорец на програмата > **Настройка** > **Мрежова защита** > **Показване на регистрационните файлове**.

Регистрационните файлове могат да се използват за откриване на грешки и разкриване на прониквания в системата. Регистрационните файлове на мрежовата защита на съдържат следните данни:

- Дата и час на събитието
- Име на събитието
- Източник
- Целеви мрежов адрес
- Мрежов комуникационен протокол
- Приложеното правило или име на червея, ако е идентифициран
- Име на приложението и път до него
- Хеш
- Потребител

- Подписващ на приложението (издател)
- Име на пакета
- Име на услугата

Подробното анализиране на тези данни може да улесни откриването на опити за проникване през защитата на системата. Много други фактори показват потенциални заплахи за защитата и позволяват на потребителя да намали тяхното въздействие: многократни връзки от непознати места, много опити за установяване на връзка, комуникация с непознати приложения или използване на необичайни портове.

> **Използване на уязвимост на защитата**
> Съобщението за експлойт на уязвимост в защитата се регистрира дори ако конкретната уязвимост вече е коригирана, тъй като опитът за експлойт се открива и блокира на мрежово ниво, преди да се случи действителен експлойт.

Разрешаване на проблеми със защитната стена

Ако имате проблеми със свързването, докато програмата ESET Internet Security е инсталирана, има няколко начина да определите дали проблемът се причинява от защитната стена. Освен това защитната стена може да ви помогне да създадете нови правила или изключения за отстраняване на проблеми в свързването.

Прегледайте следните теми за помощ при отстраняване на проблеми със защитната стена:

- Отстраняване на неизправности с мрежовия достъп
- Регистриране и създаване на правила или изключения за регистриране
- Създаване на изключения от известия на защитната стена
- Разширено регистриране за мрежовата защита
- Решаване на проблеми със скенера за мрежов трафик

Регистриране и създаване на правила или изключения за регистриране

По подразбиране защитната стена на ESET не регистрира всички блокирани връзки. Ако искате да виждате какво е блокирано от мрежовата защита, отворете Разширени настройки > **Инструменти** > **Диагностика** > **Разширено регистриране** и активирайте **Разрешаване на разширеното регистриране за мрежовата защита**. Ако видите нещо в дневника, което не искате да се блокира от защитната стена, можете да създадете правило или IDS правило за него, като щракнете с десен бутон върху елемента и изберете **Не блокирай подобни събития в бъдеще**. Имайте предвид, че дневникът на всички блокирани връзки може да съдържа хиляди елементи и може да е трудно да намерите конкретна връзка в него. Можете

да изключите регистрирането, след като разрешите проблема.

За повече информация относно регистрационния файл вж. Регистрационни файлове.

> Използвайте регистрирането, за да видите реда, в който мрежовата защита е блокирала определени връзки. Освен това създаването на правила от регистрационния файл ви позволява да създавате правила, които правят точно това, което искате.

Създаване на правило от регистрационен файл

Новата версия на ESET Internet Security ви позволява да създадете правила от дневника. От главното меню щракнете върху **Инструменти** > **Регистрационни файлове**. Изберете **Мрежова защита** от падащото меню, щракнете с десен бутон върху желания запис в дневника и изберете **Не блокирай подобни събития в бъдеще** от контекстното меню. Новото правило ще се покаже в прозорец за известие.

За да разрешите създаването на нови правила от регистрационен файл, трябва да конфигурирате ESET Internet Security със следните настройки:

1. Задайте минималното ниво на детайлност при сканиране на **Диагностика** в Разширени настройки > **Инструменти** > **Регистрационни файлове**,

2. Разрешете **Известяване за входящи атаки срещу пробиви в защитата** в Разширени настройки > **Защити** > **Защита на мрежовия достъп** > **Защита Защита от мрежови атаки** > **Разширени опции** > **Откриване на проникване**.

Създаване на изключения от известия на защитната стена

Когато защитната стена на ESET открие злонамерена мрежова дейност, ще се покаже прозорец с известие, описващ събитието. Това известие съдържа връзка, която ще ви позволи да научите повече за събитието и да настроите правило за това събитие, ако желаете.

> Ако мрежово приложение или устройство не прилага правилно мрежовите стандарти, то може да предизвика повторни IDS известия на защитната стена. Можете да създадете изключение директно от известието, за да предотвратите откриването на това приложение или устройство от защитната стена на ESET.

Разширено регистриране за мрежовата защита

Тази функция има за цел да осигури по-сложни регистрационни файлове, предназначени за отдела за техническа поддръжка на ESET. Използвайте тази функция само когато екипът за техническа поддръжка на ESET поиска това от вас, тъй като тя може да генерира огромен

регистрационен файл и да забави работата на компютъра.

1. Отворете Разширени настройки > **Инструменти** > **Диагностика** > **Разширено регистриране** и активирайте **Разрешаване на разширено регистриране за мрежовата защита**.

2. Опитайте да възпроизведете срещнатия проблем.

3. Забраняване на разширено регистриране за мрежовата защита.

4. Файлът от PCAP регистрирането, създаден от разширеното регистриране за мрежовата защита, се намира в същата директория, в която се генерират файловете за разтоварване на паметта за диагностика: *C:\ProgramData\ESET\ESET Security\Diagnostics*

Решаване на проблеми със скенера за мрежов трафик

Ако изпитвате проблеми при работа с уеб браузъра или имейл клиента си, първата стъпка е да определите дали причината не е в скенера на мрежов трафик. За целта опитайте временно да забраните скенера на мрежов трафик в Разширени настройки > **Система за засичане** > **Скенер на мрежов трафик** (не забравяйте да го включите отново, след като приключите, защото в противен случай уеб браузърът и имейл клиентът ви ще останат незащитени). Ако проблемът изчезне след забраняване на филтрирането, по-долу ще намерите списък на често срещани проблеми и начини за разрешаването им:

Проблеми с обновяването или безопасността на комуникацията

Ако приложението не може да се обнови или да получи безопасен комуникационен канал:

- Ако сте разрешили SSL/TLS, опитайте временно да го изключите. Ако това има ефект, можете да продължите да използвате SSL/TLS и да разрешите обновяването, като добавите изключение за проблематичната комуникация:
Забраняване SSL/TLS Стартирайте повторно обновяването. Трябва да се появи диалогов прозорец, който да ви информира за наличието на шифрован мрежов трафик. Уверете се, че приложението съответства на това, за което отстранявате неизправностите, и че сертификатът прилича на произлизащ от сървъра, от който се извършва обновяването. След това изберете да се запомни действието за този сертификат и щракнете върху "Игнорирай". Ако други диалогови прозорци не бъдат показани, можете да превключите режима на филтриране обратно на Автоматичен и проблемът би трябвало да изчезне.

- Ако засегнатото приложение не е браузър или имейл клиент, можете напълно да го изключите от Защита на уеб достъпа (подобно действие по отношение на браузъри и имейл клиенти би ви оставило незащитени). Всяко приложение, чиято комуникация е била филтрирана в миналото, би трябвало вече да е включено в списъка, предоставян при добавяне на изключение, така че ръчно добавяне не би трябвало да се налага.

Проблем с осъществяването на достъп до устройство в мрежата

Ако не можете да използвате функция на устройство във вашата мрежа (например отваряне на уеб страница на уеб камера или изпълняване на видео на домашен мултимедиен плейър), опитайте да добавите IPv4 и IPv6 адресите на устройството в списъка с изключени адреси.

Проблеми с конкретен уеб сайт

Можете да изключите конкретни уеб сайтове от Защита на уеб достъпа с помощта на управление на URL адреси. Ако например не можете да осъществите достъп до https://www.gmail.com/intl/en/mail/help/about.html, опитайте да добавите *gmail.com* в списъка с изключени адреси.

Грешка "Някое от приложенията, които могат да импортират главния сертификат, продължава да работи"

Когато разрешите SSL/TLS, ESET Internet Security гарантира, че инсталираните приложения се доверяват на начина, по който филтрира SSL протоколи, чрез импортиране на сертификат в тяхното хранилище за сертификати. Някои приложения може да изискват рестартиране, за да импортирате сертификат. Примери за такива приложения са Firefox и Opera. Уверете се, че нито едно от тях не се изпълнява (най-добрият начин да го направите, е да отворите диспечера на задачите и да проверите дали firefox.exe или opera.exe не присъстват в раздела с процеси), след което направете повторен опит.

Грешка относно ненадежден издател или невалиден подпис

Това най-вероятно означава, че импортирането, описано по-горе, е неуспешно. Първо се уверете, че никое от споменатите приложения не се изпълнява. След това забранете SSL/TLS и го разрешете отново. По този начин импортирането се стартира наново.

Вижте статията в онлайн помощника, за да научите Как се управлява скенер на мрежов трафик в продукт на ESET за домашна употреба за Windows.

Блокирана е мрежова заплаха

Тази ситуация може да възникне, когато приложение на вашия компютър се опитва да предаде злонамерен трафик на друг компютър в мрежата, като се възползва от пробив в защитата, или ако бъде открит дори опит за сканиране на портове във вашата система.

Можете да намерите типа заплаха и свързания IP адрес на устройството в известието. Щракнете върху **Промяна на начина на обработка на тази заплаха**, за да се покажат следните опции:

Продължаване на блокирането – Блокира открита заплаха. Ако искате да спрете да получавате известия за този тип заплаха от конкретния отдалечен адрес, изберете радио бутона до **Не известявай**, преди да щракнете върху **Продължаване на блокирането**. Това

ще създаде правило за услугата за откриване на проникване (IDS) със следната конфигурация: **Блокиране** – по подразбиране, **Известяване** – не, **Дневник** – не.

Позволяване – създава правило за услугата за откриване на проникване (IDS), за да позволи откритата заплаха. Изберете една от следните опции, преди да щракнете върху **Позволяване**, за да зададете настройките на правилото:

• **Известявай само когато тази заплаха е блокирана** – конфигурация на правило: **Блокиране** – не, **Известяване** – не, **Дневник** – не.

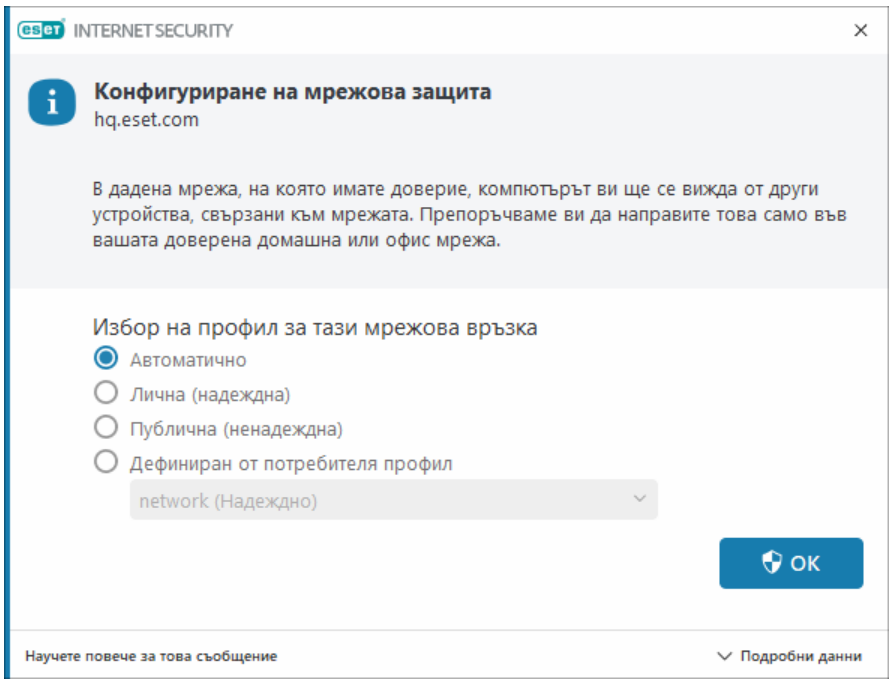
• **Известявай винаги, когато тази заплаха се появи** – конфигурация на правило: **Блокиране** – не, **Известяване** – по подразбиране, **Дневник** – по подразбиране.

• **Не известявай** – конфигурация на правило: **Блокиране** – не, **Известяване** – не, **Дневник** – не.

Информацията, показана в прозореца на известието, може да се различава в зависимост от типа на откритата заплаха.
За повече информация за заплахите и други свързани въпроси вижте Типове отдалечени атаки или Типове засичания.
За да разрешите събитие с **дублирани IP адреси в мрежата**, вижте нашата статия в онлайн помощника на ESET.

Открита е нова мрежа

По подразбиране ESET Internet Security използва настройките на Windows, когато бъде открита нова мрежова връзка. За да се покаже диалогов прозорец, когато бъде открита нова мрежа, променете Присвояване на профил за мрежова защита на **Попитай**. Конфигурирането на мрежова защита ще се показва, когато компютърът се свързва с нова мрежа.



Можете да изберете от следните Профили за мрежова връзка:

Автоматично – ESET Internet Security ще избере профила автоматично в зависимост от

активаторите, конфигурирани за всеки профил.

Лична – За надеждни мрежи (домашна или офис мрежа). Вашият компютър и споделените файлове, съхранени на компютъра, са видими за други потребители в мрежата, а системните ресурси са достъпни за други потребители в мрежата (достъпът до споделени файлове и принтери е разрешен, входящата RPC комуникация е разрешена и споделянето на работния плот е налично). Препоръчваме да използвате тази настройка при достъп до защитена локална мрежа. Този профил автоматично се присвоява на мрежова връзка, ако е конфигуриран като домейн или частна мрежа в Windows.

Публична – За ненадеждни мрежи (публична мрежа). Файловете и папките на вашата система не се споделят или не се виждат от други потребители в мрежата и споделянето на системни ресурси е дезактивирано. Препоръчваме да използвате тази настройка при достъп до безжични мрежи. Този профил автоматично се присвоява на всяка мрежова връзка, която не е конфигурирана като домейн или частна мрежа в Windows.

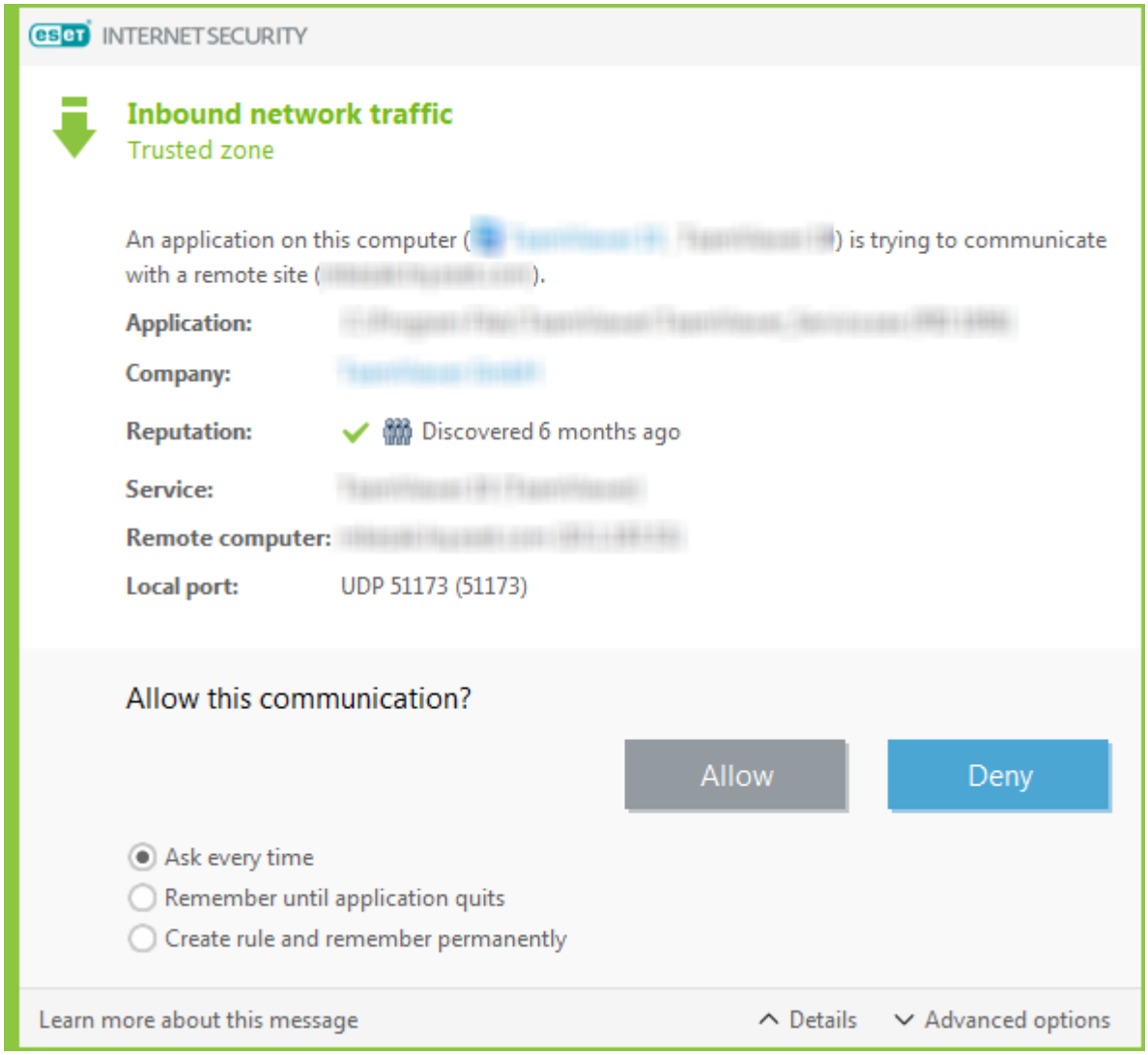
Дефиниран от потребителя профил – Можете да изберете един от профилите, които сте създали, от падащото меню. Тази опция е налична само ако сте създали поне един потребителски профил.

⚠ Неправилното конфигуриране на мрежата може да създаде риск за компютъра.

Установяване на връзка – откриване

Защитната стена открива всяка новосъздадена мрежова връзка. Активният режим на защитната стена определя действията, които ще се извършват за новото правило. Ако е активиран **Автоматичен режим** или **Базиран на правила режим**, защитната стена ще извърши предварително зададени действия без намесата на потребителя.

При **Интерактивен режим** се показва информационен прозорец, уведомяващ за това, че е открита нова мрежова връзка, както и подробна информация за нея. Можете да изберете **Позволяване** или **Отказ** (блокиране) за връзката. Ако постоянно разрешавате една и съща връзка в диалоговия прозорец, е препоръчително да се създаде ново правило за връзката. Изберете **Създай правило и го запомни за постоянно** и запишете действието като ново правило за защитната стена. Ако защитната стена разпознае същата връзка в бъдеще, тя ще приложи съществуващото правило, без да се налага действие от страна на потребителя.



Когато създавате нови правила, позволявайте само връзки, за които ви е известно, че са защитени. Ако всички връзки са разрешени, защитната стена не може да изпълнява своето предназначение. Следват важните параметри на връзките:

Приложение – Местоположение на изпълним файл и ИД на процеса. Не позволявайте връзки за неизвестни приложения и процеси.

Подписващ – Име на издателя на приложението. Щракнете върху текста, за да покажете сертификат за защита за фирмата.

Репутация – Ниво на риск на връзката. На връзките е присвоено ниво на риск: Без риск (зелена), Непозната (оранжева) или Рискована (червена), чрез използване на серия от евристични правила, които преглеждат характеристиките на всяка връзка, броя на потребителите и времето за откриване. Тази информация се събира от технологията ESET LiveGrid®.

Услуга – Име на услугата, ако приложението е услуга на Windows.

Отдалечен компютър – Адрес на отдалеченото устройство. Разрешават се само връзките с доверени и познати адреси.

Отдалечен порт – Порт за връзка. Комуникация с основните портове (например уеб трафик – порт номер 80.443) може да се разреши при нормални обстоятелства.

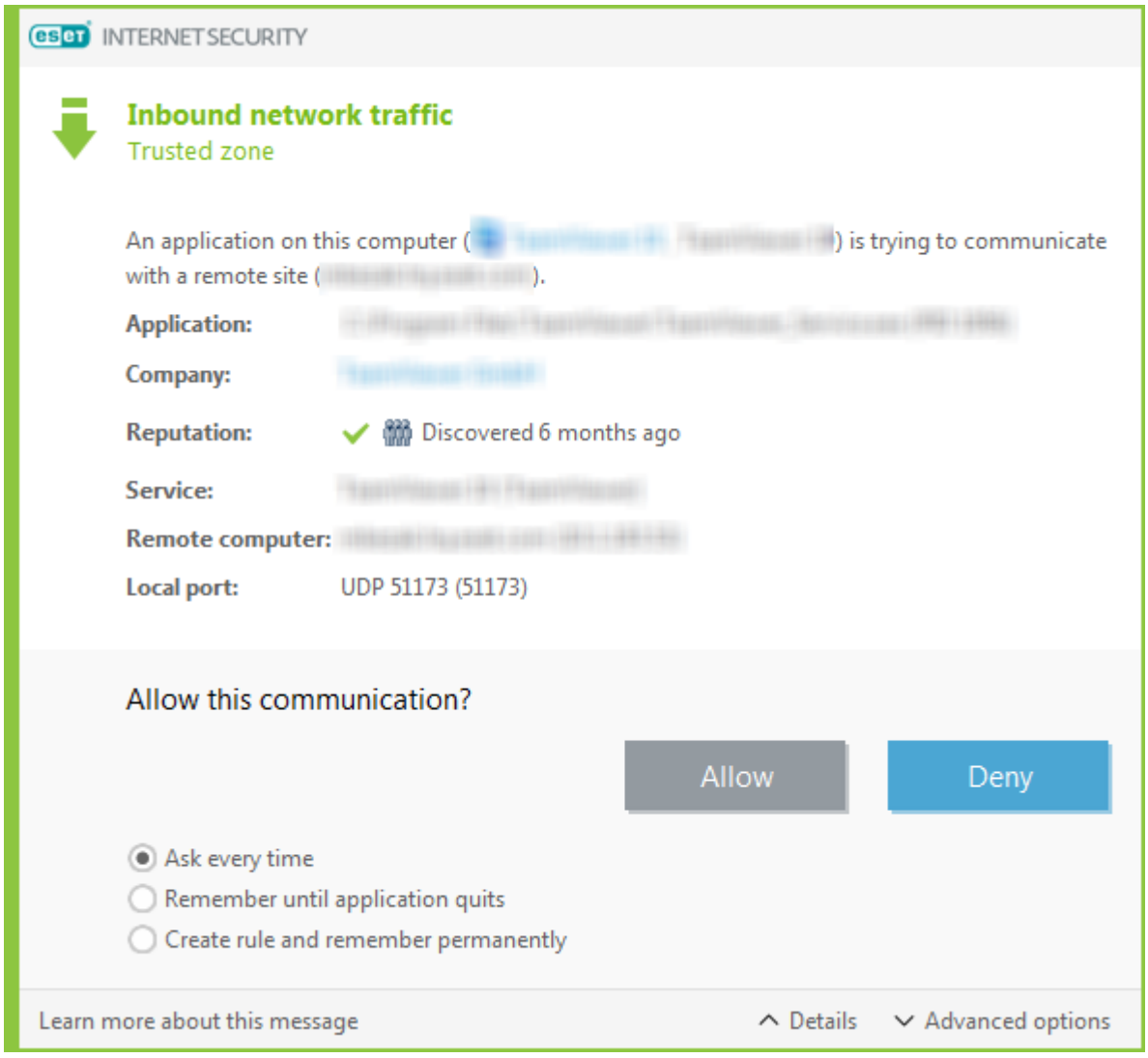
Компютърните вируси често използват интернет и скрити връзки, за да проникнат в отдалечените компютри. Ако правилата са конфигурирани правилно, защитната стена се превръща в полезен инструмент за защита от атаки със злонамерен код.

Промяна на приложение

Защитната стена е открила промяна в дадено приложение, което се използва за установяване на изходящи връзки от компютъра ви. Възможно е приложението просто да се опитва да се обнови с по-нова версия. От друга страна промяната може да е направена от злонамерена програма. Ако не сте сигурни дали промяната е легитимна, препоръчваме да откажете връзката и да сканирате компютъра, като използвате най-актуалната база данни със сигнатури за вируси.

Входяща надеждна комуникация

Пример за входяща връзка в надеждната зона:
Отдалечен компютър от надеждната зона се опитва да установи връзка с локално приложение на компютъра ви.



Приложение – приложение, свързано с отдалечено устройство.

Път на приложение – местоположение на приложението.

Приложение от магазина на Microsoft – име на приложението в магазина на Microsoft.

Подписващ – име на издателя на приложението. Щракнете върху текста, за да покажете сертификат за защита за фирмата.

Репутация – репутацията на приложението се получава от технологията ESET LiveGrid®.

Услуга – Име на услугата, която се изпълнява в момента на компютъра ви.

Отдалечен компютър – отдалечен компютър, който се опитва да осъществи връзка с приложението на вашия компютър.

Отдалечен порт – използваният порт за връзка.

Питай всеки път – Ако действието по подразбиране за дадено правило е зададено на **Питай**, ще се показва диалогов прозорец при всяко активиране на правилото.

Запомни до излизане от приложението – ESET Internet Security ще запомни избраното действие до следващото рестартиране.

Създай правило и го запомни за постоянно – Ако изберете тази опция преди разрешаването или забраняването на комуникацията, ESET Internet Security ще запомни действието и ще го използва, ако приложението се свърже отново с отдалечения компютър.

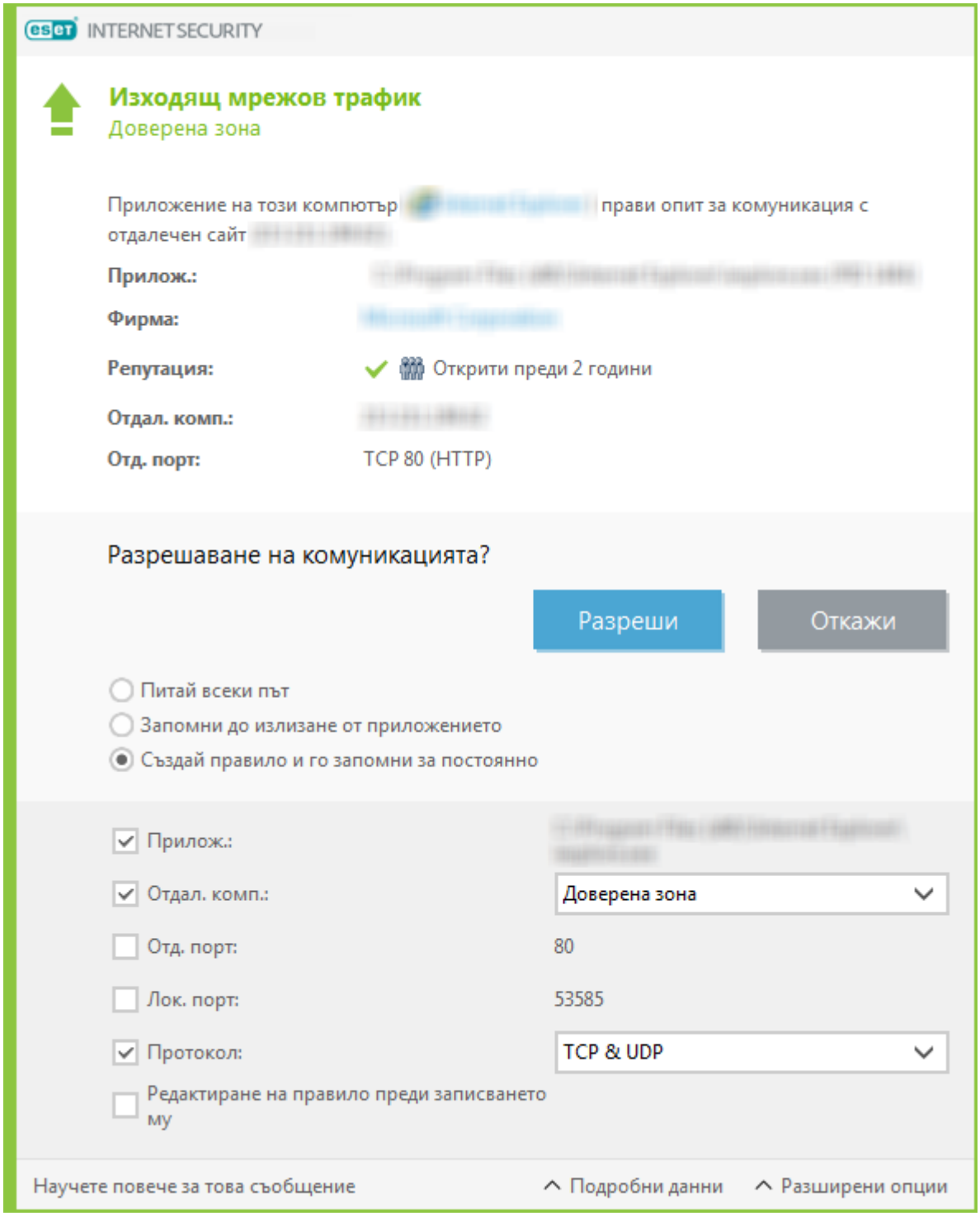
Разреши – разрешаване на входящата комуникация.

Откажи – забраняване на входящата комуникация.

Редактиране на правило – позволява ви да персонализирате свойствата на правилата с помощта на редактора на правила за защитната стена.

Изходяща надеждна комуникация

Пример за изходяща връзка в надеждната зона:
Местно приложение се опитва да установи връзка с друг компютър в локалната мрежа или в мрежа в надеждната зона.



Приложение – приложение, свързано с отдалечено устройство.

Път на приложение – местоположение на приложението.

Приложение от магазина на Microsoft – име на приложението в магазина на Microsoft.

Подписващ – име на издателя на приложението. Щракнете върху текста, за да покажете сертификат за защита за фирмата.

Репутация – репутацията на приложението се получава от технологията ESET LiveGrid®.

Услуга – Име на услугата, която се изпълнява в момента на компютъра ви.

Отдалечен компютър – отдалечен компютър, който се опитва да осъществи връзка с приложението на вашия компютър.

Отдалечен порт – използваният порт за връзка.

Питай всеки път – Ако действието по подразбиране за дадено правило е зададено на **Питай**, ще се показва диалогов прозорец при всяко активиране на правилото.

Запомни до излизане от приложението – ESET Internet Security ще запомни избраното действие до следващото рестартиране.

Създай правило и го запомни за постоянно – Ако изберете тази опция преди разрешаването или забраняването на комуникацията, ESET Internet Security ще запомни действието и ще го използва, ако приложението се свърже отново с отдалечения компютър.

Разреши – разрешаване на входящата комуникация.

Откажи – забраняване на входящата комуникация.

Редактиране на правило – позволява ви да персонализирате свойствата на правилата с помощта на редактора на правила за защитната стена.

Входяща комуникация

Пример за входяща интернет връзка:
Отдалечен компютър се опитва да комуникира с приложение на вашия компютър.

Приложение – приложение, свързано с отдалечено устройство.

Път на приложение – местоположение на приложението.

Приложение от магазина на Microsoft – име на приложението в магазина на Microsoft.

Подписващ – име на издателя на приложението. Щракнете върху текста, за да покажете сертификат за защита за фирмата.

Репутация – репутацията на приложението се получава от технологията ESET LiveGrid®.

Услуга – Име на услугата, която се изпълнява в момента на компютъра ви.

Отдалечен компютър – отдалечен компютър, който се опитва да осъществи връзка с приложението на вашия компютър.

Отдалечен порт – използваният порт за връзка.

Питай всеки път – Ако действието по подразбиране за дадено правило е зададено на **Питай**, ще се показва диалогов прозорец при всяко активиране на правилото.

Запомни до излизане от приложението – ESET Internet Security ще запомни избраното действие до следващото рестартиране.

Създай правило и го запомни за постоянно – Ако изберете тази опция преди разрешаването или забраняването на комуникацията, ESET Internet Security ще запомни

действието и ще го използва, ако приложението се свърже отново с отдалечения компютър.

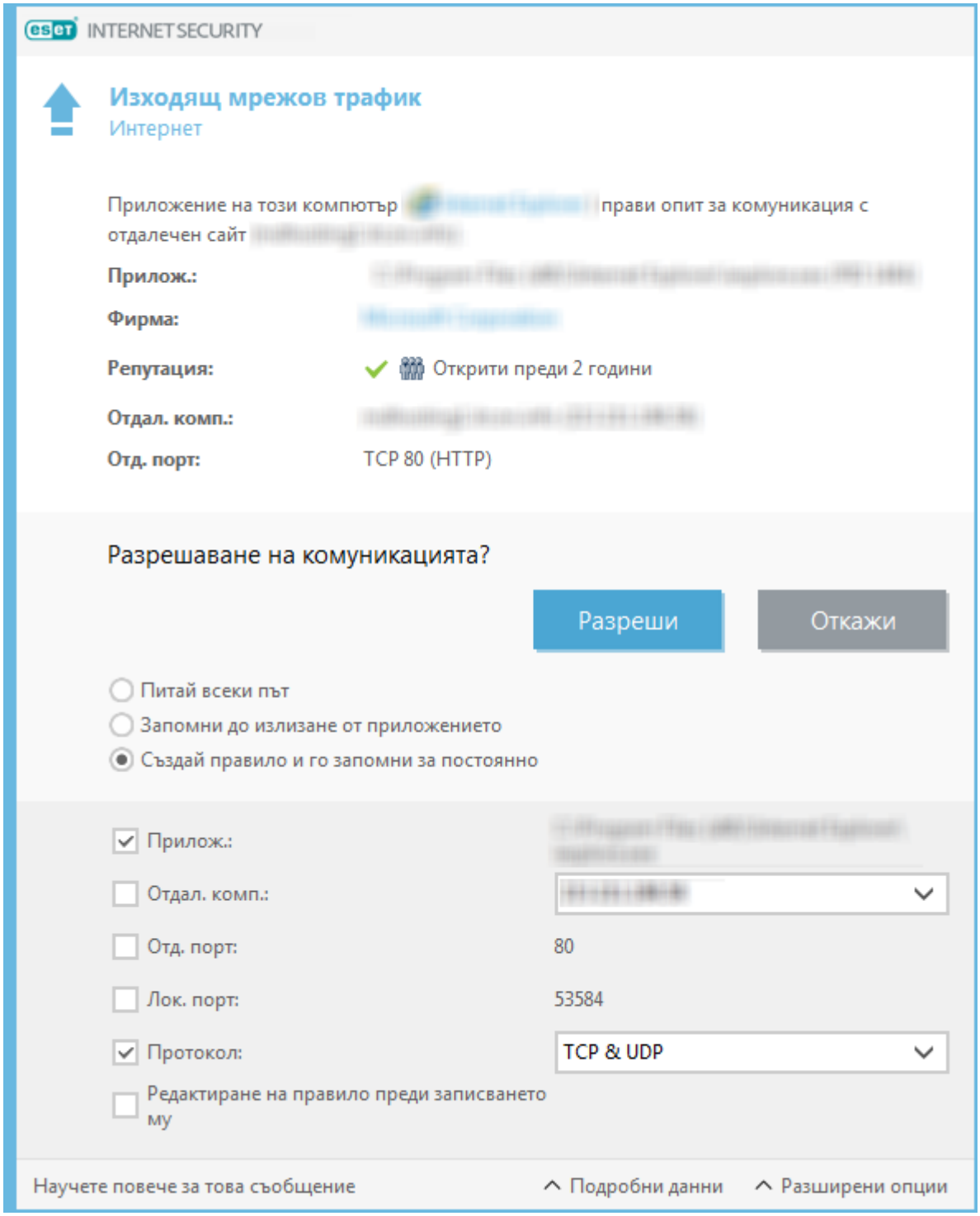
Разреши – разрешаване на входящата комуникация.

Откажи – забраняване на входящата комуникация.

Редактиране на правило – позволява ви да персонализирате свойствата на правилата с помощта на редактора на правила за защитната стена.

Изходяща комуникация

Пример за изходяща интернет връзка:
Локално приложение се опитва да установи връзка с интернет.



Приложение – приложение, свързано с отдалечено устройство.

Път на приложение – местоположение на приложението.

Приложение от магазина на Microsoft – име на приложението в магазина на Microsoft.

Подписващ – име на издателя на приложението. Щракнете върху текста, за да покажете сертификат за защита за фирмата.

Репутация – репутацията на приложението се получава от технологията ESET LiveGrid®.

Услуга – Име на услугата, която се изпълнява в момента на компютъра ви.

Отдалечен компютър – отдалечен компютър, който се опитва да осъществи връзка с приложението на вашия компютър.

Отдалечен порт – използваният порт за връзка.

Питай всеки път – Ако действието по подразбиране за дадено правило е зададено на **Питай**, ще се показва диалогов прозорец при всяко активиране на правилото.

Запомни до излизане от приложението – ESET Internet Security ще запомни избраното действие до следващото рестартиране.

Създай правило и го запомни за постоянно – Ако изберете тази опция преди разрешаването или забраняването на комуникацията, ESET Internet Security ще запомни действието и ще го използва, ако приложението се свърже отново с отдалечения компютър.

Разреши – разрешаване на входящата комуникация.

Откажи – забраняване на входящата комуникация.

Редактиране на правило – позволява ви да персонализирате свойствата на правилата с помощта на редактора на правила за защитната стена.

Настройка на изгледа с връзки

Щракнете с десния бутон върху дадена връзка, за да прегледате допълнителни опции, които включват:

Показване на имената на хостове – Ако е възможно, всички мрежови адреси се показват в DNS формат, а не във формат на числов IP адрес.

Покажи само TCP връзките – списъкът показва само връзки, които са включени в пакета с TCP протоколи.

Покажи активните връзки – изберете тази опция, за да се покажат само връзките, при които няма установена комуникация, но системата е отворила порт и очаква свързване.

Показване на връзките в компютъра – Изберете тази опция, за да се покажат само връзките, при които отдалечената страна е локална система, или т.нар. връзки с localhost.

Обнови скоростта – изберете честотата на опресняване на активните връзки.

Обнови сега – презареждане на прозореца с **мрежови връзки**.

Инструменти за защита

Отворете главния прозорец на програмата > **Настройка** > **Инструменти за защита**, за да настроите следните модули:

Безопасно банкиране и сърфиране – добавя допълнителен слой защита на браузъра, предназначен да защити вашите финансови данни по време на онлайн транзакции. Разрешете **Защитаване на всички браузъри** в Разширени настройки за безопасно банкиране и

сърфиране, за да стартирате всички поддържани уеб браузъри в защитен режим.

Поверителност и защита на браузъра – запазва вашата онлайн активност поверителна и защитена, без да оставя дигитален отпечатък.

Anti-Theft – разрешете Anti-Theft, за да защитите компютъра си в случай на загуба или кражба.

Безопасно банкиране и сърфиране

Безопасно банкиране и сърфиране е допълнителен слой защита, предназначен да предпазва вашите финансови данни по време на онлайн транзакции.

По подразбиране всички поддържани уеб браузъри стартират в защитен режим. Това ви позволява да сърфирате в интернет, да осъществявате достъп до интернет банкиране и да правите онлайн покупки и трансакции в защитен браузър автоматично.

Системата за репутацияESET LiveGrid® трябва да е включена (включена по подразбиране), за да се гарантира правилната работа на безопасното банкиране и сърфиране.

За да конфигурирате поведението на защитения браузър, вижте Разширена настройка на безопасното банкиране и сърфиране. Ако дезактивирате **Защитаване на всички браузъри**, можете да получите достъп до защитения браузър в главния прозорец на програмата > **Преглед** > **Безопасно банкиране и сърфиране** или чрез щракване върху иконата **Безопасно банкиране и сърфиране** на работния плот. Браузърът, зададен по подразбиране в Windows, се стартира в защитен режим.

Използването на HTTPS шифрована комуникация е необходимо за извършване на защитено сърфиране. Следните браузъри поддържат безопасно банкиране и сърфиране:

- Internet Explorer 8.0.0.0+
- Microsoft Edge 83.0.0.0+
- Google Chrome 64.0.0.0+
- Firefox 24.0.0.0+

Само Firefox и Microsoft Edge се поддържат на устройства с процесори ARM.

За повече информация относно функцията "Безопасно банкиране и сърфиране" прочетете следните статии в онлайн помощника на ESET, налични на английски и няколко други езика:

- Как да използвам безопасното банкиране и сърфиране на ESET?
- Пауза или дезактивиране на безопасното банкиране и сърфиране в продукти на ESET за домашна употреба за Windows
- Безопасно банкиране и сърфиране на ESET — често срещани грешки
- Речник на ESET | Безопасно банкиране и сърфиране

Известие в браузъра

Защитеният браузър ви информира за текущото си състояние чрез известия в браузъра и цвета на рамката на браузъра.

Известията в браузъра се показват в раздела от дясната страна.

За да отворите известието в браузъра, щракнете върху иконата на ESET. За да скриете известието, щракнете върху текста на известието. За да отхвърлите известието и зелената рамка на браузъра, щракнете върху иконата за затваряне .

Само информативното известие и зелената рамка на браузъра могат да бъдат отхвърлени.

Известия в браузъра

Тип известие	Състояние
Информативно известие и зелена рамка на браузъра	Осигурена е максимална защита и известието в браузъра е скрито по подразбиране. Разгънете известието в браузъра и щракнете върху **Настройки,** за да отворите настройката Инструменти за защита.
Предупреждение и оранжева рамка на браузъра	Защитеният браузър изисква вашето внимание за проблем, който не е критичен. За повече информация относно проблема или решение следвайте инструкциите в известието в браузъра.
Уведомяване за защитата и червена рамка на браузъра	Браузърът не е защитен от безопасното банкиране и сърфиране на ESET. Рестартирайте браузъра, за да се уверите, че защитата е активна. За да разрешите конфликт с файлове, заредени в браузъра, отворете „Регистрационни файлове“ > „**Безопасно банкиране и сърфиране**“ и се уверете, че регистрираните файлове няма да се зареждат при следващото стартиране на браузъра. Ако проблемът продължава, се свържете с техническата поддръжка на ESET, като следвате инструкциите в нашата статия в онлайн помощника.

Поверителност и защита на браузъра

Можете да разрешите функцията за поверителност и защита на браузъра чрез персонализирано разширение, налично в поддържани браузъри (само Google Chrome, Mozilla Firefox и Microsoft Edge).

За инсталиране и разрешаване на разширението:

1. Уверете се, че използвате последната версия на ESET Internet Security и рестартирайте успешно компютъра след актуализацията.

2. Отворете браузъра си.

3. Разширението е инсталирано във вашия браузър.

4. Активирайте разширението и ще се покаже страницата с подробности за разширението в браузъра.

Главното меню на разширението за браузър „Поверителност и защита на браузъра“ е разделено на следните секции:

Преглед

Защитено търсене

Щракнете върху иконата на плъзгача  до **Сканиране на резултатите от търсенето**, за да разрешите функцията и да видите кои резултати са безопасни за щракване. Защитеното търсене оценява посочените адреси на връзки и не означава непременно, че уебсайтът не съдържа злонамерен софтуер. След това нашата система за засичане открива всеки злонамерен софтуер на уебсайта.

Изчистване на браузъра

Изтрийте данните за сърфиране или настройте редовно почистване. Можете да добавяте уеб сайтове, в които искате да приемате бисквитки и да останете влезли дори след извършване на изчистването на браузъра, като ги **добавите към списък**.

• **Еднократно почистване –** изберете времевия диапазон от падащото меню и типа данни, който искате да изтривате. От опциите можете да избирате всички данни, както и частни и персонализирани селекции.

• **Редовно почистване** – щракнете върху иконата на плъзгача  до **Редовно почистване**, за да разрешите функцията. Изберете времевия диапазон от падащото меню и типа данни, който искате да изтривате редовно. От опциите можете да избирате всички данни, както и частни и персонализирани селекции.

Опцията **Потребителски данни** съдържа следните категории:

- Хронологията на браузъра
- Хронология на изтеглянията
- Данни за бисквитки и уеб сайтове
- Кеширани изображения и файлове
- Пароли и данни за влизане
- Данни за автоматично попълване на формуляр

Преглед на настройките на уеб сайта

Осъществявайте достъп и управлявайте разрешенията за уеб сайтове, за да контролирате каква информация могат да използват уеб сайтовете.

- **Известия** – прегледайте за кои уеб сайтове искате да **разрешите/блокирате**

известията или ако искате разширението за браузъра да ви **пита всеки път**.

Разширена настройка

Изчистване на браузъра

Разширени настройки за бисквитки

Списък с уеб сайтове, в които искате да приемате бисквитки и да останете влезли дори след извършване на изчистването на браузъра. Въведете URL адреса в текстовото поле и щракнете върху **Добави**. Можете да го премахнете по всяко време от списъка, като щракнете върху иконата с минус до конкретния уеб сайт.

В долната част на страницата има списък с предложени домейни, които към момента са отворени в браузъра. Ако не можете да видите конкретния уеб сайт, щракнете върху **обновяване на списъка** и го добавете към списъка с приети бисквитки, като щракнете върху иконата с плюс .

Преглед на настройките на уеб сайта

Осъществявайте достъп и управлявайте разрешенията за уеб сайтове, за да контролирате каква информация могат да използват уеб сайтовете.

• **Известия** – прегледайте за кои уеб сайтове искате да **разрешите/блокирате** известията или ако искате разширението за браузъра да ви **пита всеки път**.

Външен вид

Персонализирайте цветовата схема на интерфейса, за да отговаря на вашите предпочитания. Можете да изберете предпочитаната от вас цветова схема, като поставите отметка в квадратчето **Светла** или **Тъмна**.

Anti-Theft

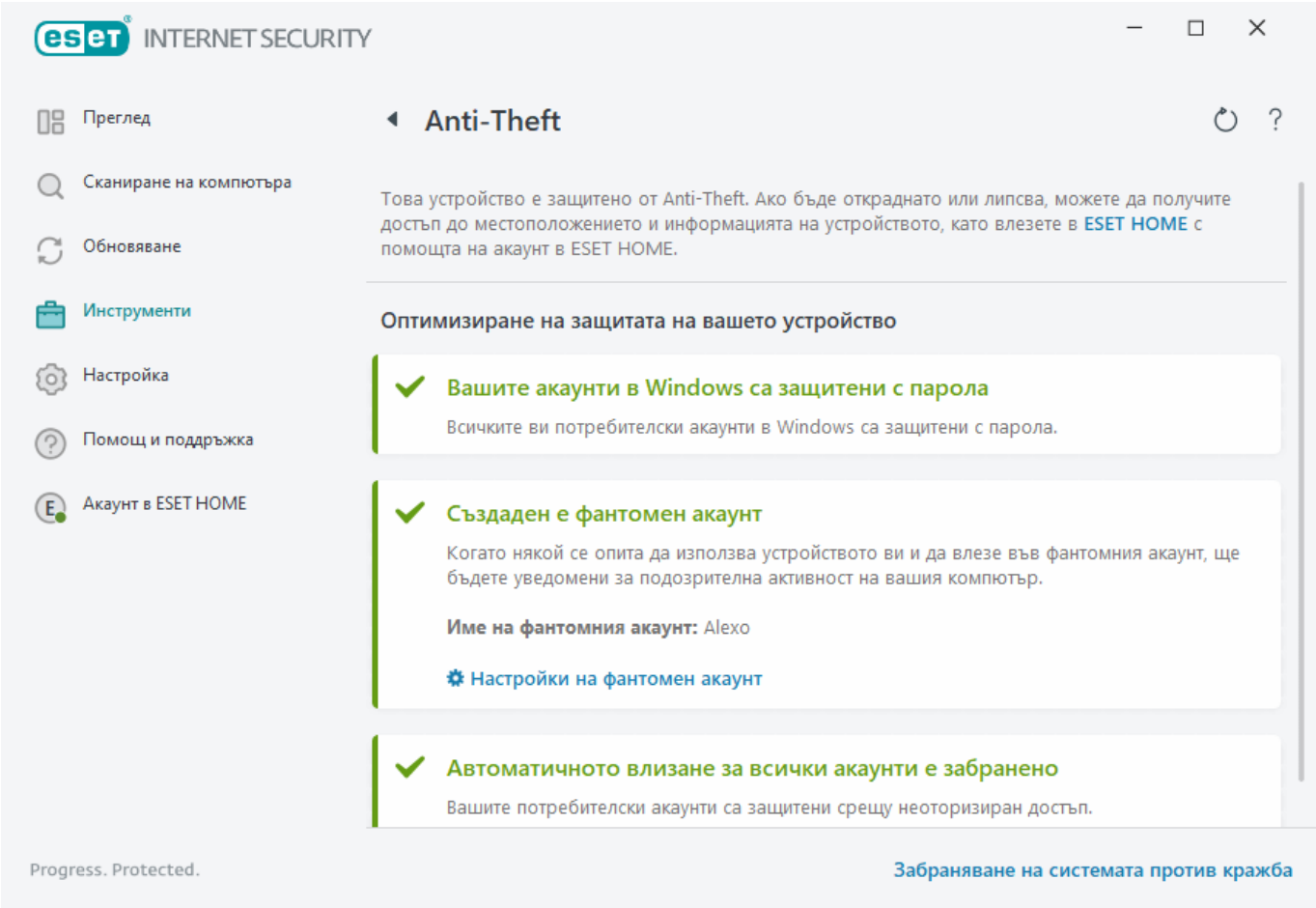
При нашите ежедневни пътувания от вкъщи до работа или други публични места персоналните устройства са постоянно изложени на риск от загуба или кражба. Anti-Theft е функция, която разширява защитата на ниво потребител в случай на загубено или откраднато устройство. Anti-Theft ви позволява да наблюдавате употребата му и да проследявате липсващото устройство чрез определяне на местоположение по IP адрес в ESET HOME, което ще ви помогне да си върнете устройството и да защитите личните си данни.

Чрез използването на съвременни технологии, като например географско търсене на IP адрес, заснемане на изображения с уеб камера, защита на потребителски акаунти и наблюдение на устройства, Anti-Theft може да помогне на вас и на правоприлагащите органи при намирането на компютъра или устройството, в случай че то е изгубено или откраднато. В ESET HOME можете да видите каква дейност се извършва на вашия компютър или устройство.

За да научите повече за Anti-Theft в ESET HOME, вижте Онлайн помощта за ESET HOME.

Anti-Theft може да не работи правилно на компютри в домейни поради ограничения в управлението на потребителски акаунти.

След Разрешаване на Anti-Theft можете да оптимизирате защитата на вашето устройство в главния прозорец на програмата > **Настройка** > **Инструменти за защита** > **Anti-Theft**.



Опции на оптимизацията

Не е създаден фантомен акаунт

Създаването на фантомен акаунт увеличава шанса за локализиране на изгубено или откраднато устройство. Ако маркирате устройството си като липсващо, Anti-Theft ще блокира достъпа до активните ви потребителски акаунти, за да защитите поверителната си информация. На всеки, който се опита да използва устройството, ще бъде разрешено само да използва фантомния акаунт. Фантомният акаунт е форма на акаунт за гости с ограничени разрешения. Той ще се използва като системен акаунт по подразбиране, докато устройството ви бъде маркирано като възстановено – предотвратяване на влизането в други потребителски акаунти или достъпа до данните на потребителя.

По всяко време, когато някой влезе във фантомния акаунт, когато компютърът ви е в нормално състояние, ще ви бъде изпратено известие по имейл с информация за подозрителна активност на компютъра. След получаване на известието по имейл можете да решите дали искате да маркирате компютъра като липсващ.

За да създадете фантомен акаунт, щракнете върху **Създаване на фантомен акаунт**, въведете **името на фантомния акаунт** в текстовото поле и щракнете върху **Създаване**.

Когато е създаден фантомен акаунт, щракнете върху **Настройките на фантомния акаунт** за преименуване или премахване на акаунта.

Защита с парола на акаунти в Windows

Вашият потребителски акаунт не е защитен с парола. Ще получите това предупреждение за оптимизация, ако поне един потребителски акаунт не е защитен с парола. Създаването на парола за всички потребители (с изключение на **фантомния акаунт**) на компютъра ще разреши този проблем.

За да създадете парола за потребителския акаунт, щракнете върху **Управление на акаунти в Windows** и променете паролата или следвайте инструкциите по-долу:

1. Натиснете CTRL+Alt+Delete на клавиатурата.
2. Щракнете върху **Промяна на парола**.
3. Оставете полето **Стара парола** празно.
4. Въведете паролата в полетата **Нова парола** и **Потвърдете паролата** и натиснете **Enter**.

Автоматично влизане за акаунти в Windows

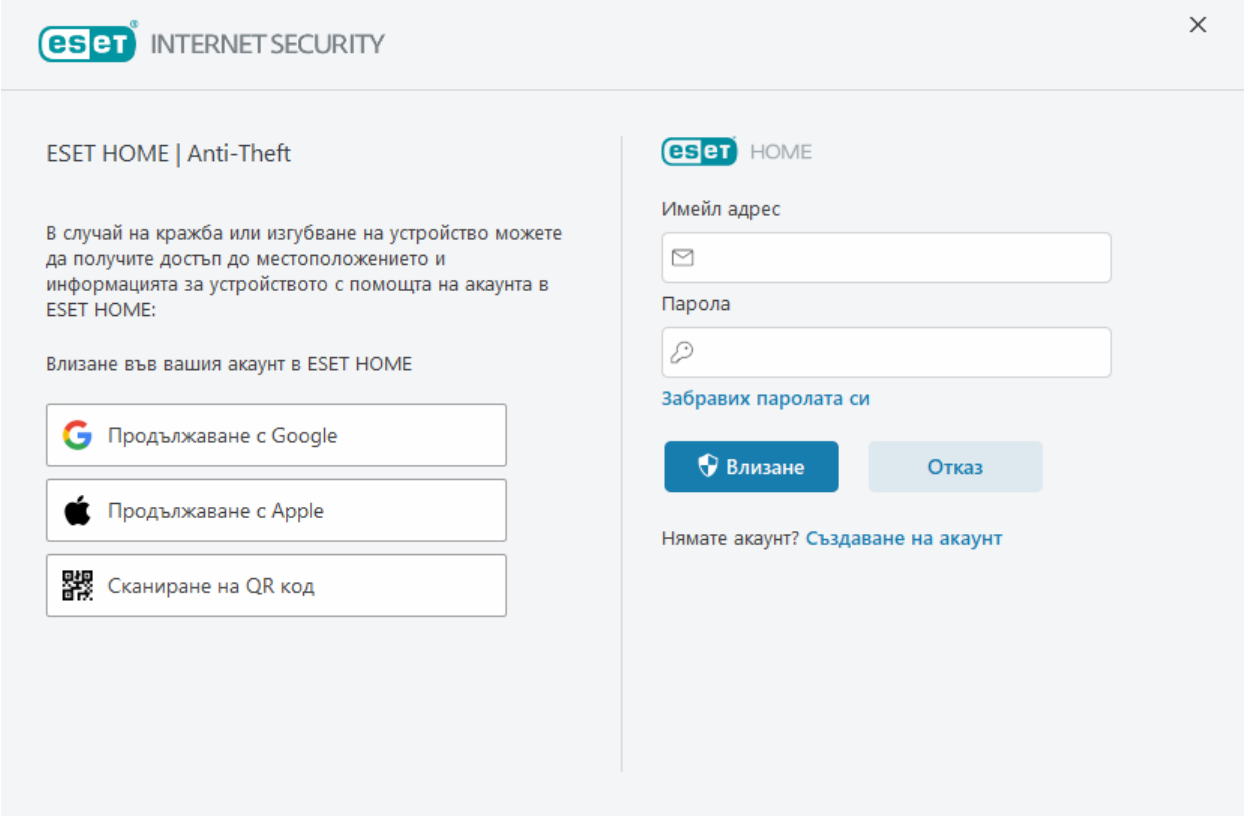
Вашият потребителски акаунт е с разрешено автоматично влизане; следователно той не е защитен срещу неупълномощен достъп. Ще получите това предупреждение за оптимизация, ако поне един потребителски акаунт има разрешено автоматично влизане. Щракнете върху **Забрани автоматично влизане**, за да разрешите този проблем с оптимизацията.

Автоматичното влизане за фантомния акаунт

Автоматичното влизане е разрешено за **фантомния акаунт** на вашето устройство. Когато устройството е в нормално състояние, не ви препоръчваме да използвате автоматично влизане, защото може да причини проблеми с достъпа до вашия реален потребителски акаунт или да изпрати фалшиви сигнали за липсващото състояние на компютъра. Щракнете върху **Забрани автоматично влизане**, за да разрешите този проблем с оптимизацията.

Влезте в акаунта си ESET HOME.

За да разрешите/забраните Anti-Theft и да осъществите достъп до местоположението и информация на устройството в ESET HOME, влезте в своя акаунт в ESET HOME.



Има няколко налични метода за влизане във вашия акаунт в ESET HOME:

• **Използване на имейл адреса и паролата в ESET HOME** – Въведете **имейл адреса** и **Паролата**, които сте използвали, за да създадете акаунта си в ESET HOME, и щракнете върху **Влизане**.

• **Използвайте своя акаунт в Google/AppleID** – Щракнете върху **Продължаване с Google** или **Продължаване с Apple** и влезте в съответния акаунт. След успешно влизане ще бъдете пренасочени към уеб страницата за потвърждение на ESET HOME. За да продължите, превключете отново към страницата на продукта на ESET. За повече информация относно влизането в Google/AppleID вж. онлайн помощта за ESET HOME.

• **Сканиране на QR код** – Щракнете върху **Сканиране на QR код**, за да се покаже QR кодът. Отворете мобилното си приложение ESET HOME и сканирайте QR кода или насочете камерата на устройството си към QR кода. За повече информация вижте инструкциите в онлайн помощта за ESET HOME.

⚠ Неуспешно влизане – често срещани грешки.

Ако нямате акаунт в ESET HOME, щракнете върху **Създаване на акаунт** за регистриране или вижте инструкциите в онлайн помощта за ESET HOME.
Ако сте забравили паролата си, щракнете върху **Забравих паролата си** и следвайте стъпките на екрана или вижте онлайн помощта за ESET HOME.

Anti-Theft не поддържа Microsoft Windows Home Server.

Задаване на име на устройството

Полето **Име на устройство** представлява името на вашия компютър (устройство), което ще се показва като идентификатор във всички услуги на ESET HOME. По подразбиране се използва името на вашия компютър. Въведете името на устройството или използвайте такова по подразбиране и щракнете върху **Продължи**.

Anti-Theft разрешено/забранено

Този прозорец съдържа съобщение за потвърждение, когато разрешавате/забранявате Anti-Theft:

• Разрешено – Вашето устройство вече е защитено с Anti-Theft и може да управлявате защитата му дистанционно на портала ESET HOME, като използвате акаунта си.

• Забранено – Anti-Theft е забранено на това устройство и всички данни, свързани с <%ESET_ANTTHEFT%> за това устройство, се премахват от портала ESET HOME.

Неуспешно добавяне на ново устройство

Получихте грешка при активиране на Anti-Theft.

Най-често срещаните сценарии са:

• Грешка при влизане в ESET HOME

• Няма връзка с интернет (или интернет не функционира в момента).

Ако не можете да разрешите проблема, се свържете с Техническа поддръжка на ESET.

Настройки за импортиране и експортиране

Можете импортирате или експортирате своя персонализиран конфигурационен файл в .xml формат за ESET Internet Security от менюто **Настройка**.

> **Илюстрирани инструкции**
> Вижте Импортиране или експортиране на конфигурационните настройки на ESET с помощта на .xml файл за илюстрирани инструкции, налични на английски и няколко други езика.

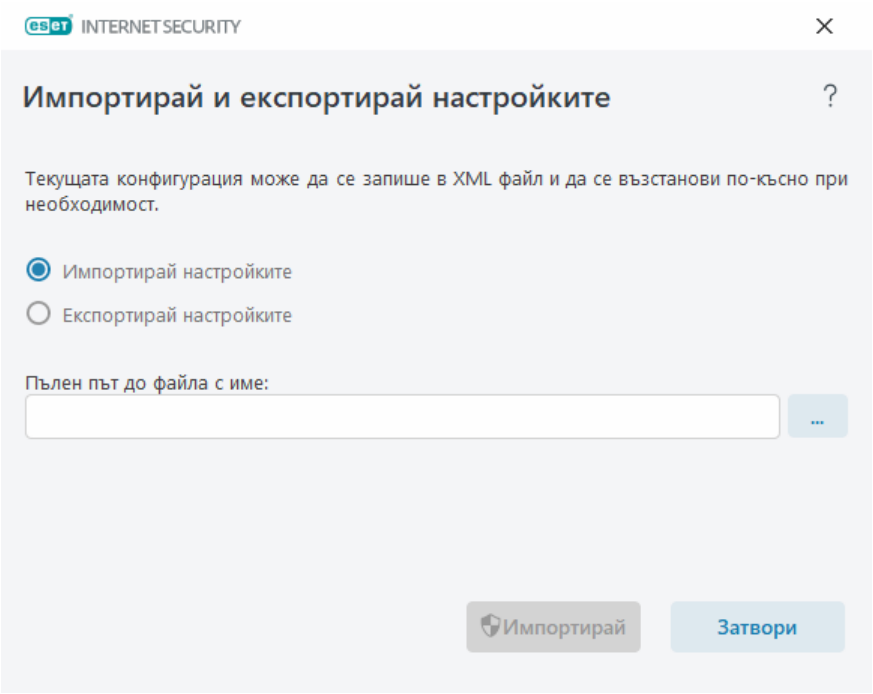
Импортирането и експортирането на конфигурационни файлове е полезно, ако се налага да архивирате настоящата конфигурация на ESET Internet Security за употреба на по-късен етап. Опцията за настройки за експортиране е полезна също така, когато искате да използвате своята предпочитана конфигурация на много системи. Можете да импортирате .xml файл за прехвърляне на желаните настройки.

За да импортирате конфигурация, в главния прозорец на програмата щракнете върху **Настройка** > **Импортиране/Експортиране на настройките**, след което изберете

Импортиране на настройките. Въведете името на конфигурационния файл или щракнете върху бутона **...**, за да потърсите конфигурационния файл, който искате да импортирате.

За да импортирате конфигурация, в главния прозорец на програмата щракнете върху **Настройка** > **Импортиране/Експортиране на настройките**. Изберете **Експортиране на настройките** и въведете целия път до файла с името. Щракнете върху бутона **...**, за да отидете в местоположение на компютъра, в което да запишете конфигурационния файл.

Може да възникне грешка по време на експортирането на настройките, ако не разполагате с достатъчно права, за да запишете експортирания файл в указаната директория.



Помощ и поддръжка

Щракнете върху **Помощ и поддръжка** в главния прозорец на програмата, за да се покаже информация за поддръжката и инструментите за отстраняване на неизправности, които ви помагат за разрешаване на проблеми, с които може да се сблъскате.

Абонамент

• Отстраняване на неизправности с абонамент – щракнете върху тази връзка, за да намерите решения за проблеми с активирането или промяната на абонамента.

• Промяна на абонамент – Щракнете, за да отворите прозореца за активиране и да активирате продукта си. Ако устройството ви е свързано с ESET HOME, изберете абонамент от своя акаунт в ESET HOME или добавете нов.

Инсталиран продукт

• Какво е новото – Щракнете тук, за да отворите прозореца с информация за новите и подобрени функции.

• За програмата ESET Internet Security – Показва информация за вашето копие на ESET Internet Security.

• Отстраняване на неизправности в продукта – щракнете върху тази връзка, за да намерите решения на най-често срещаните проблеми.

• **Промяна на продукта** – щракнете, за да видите дали ESET Internet Security може да бъде променен с различна продуктова линия с текущия абонамент.

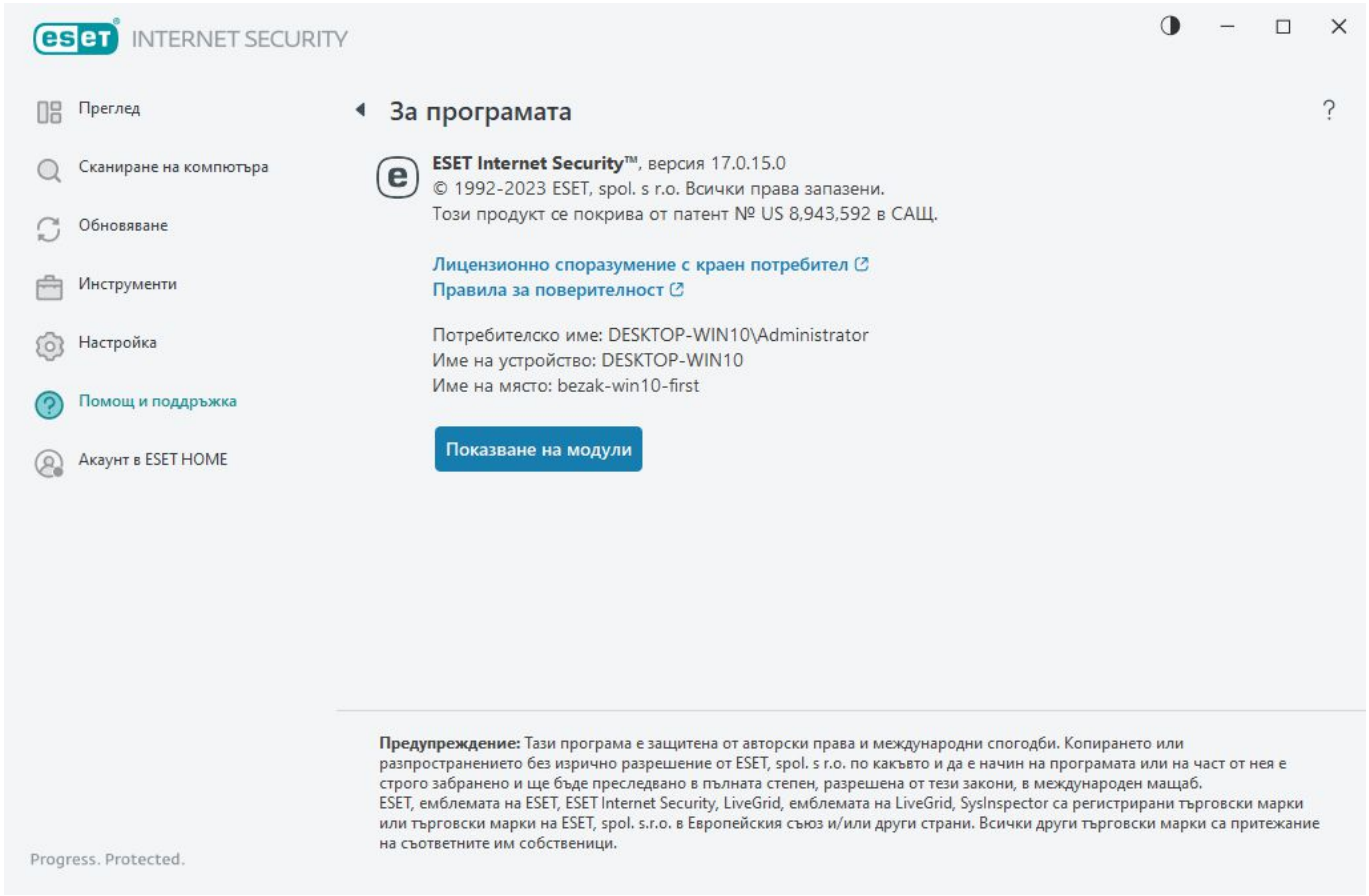
Страница за помощ – Щракнете върху тази връзка, за да стартирате помощните страници на ESET Internet Security.

Техническа поддръжка

Онлайн помощник – Базата знания на ESET съдържа отговори на най-често задаваните въпроси, както и препоръчителни решения за различни проблеми. Редовно обновявана от техническите специалисти на ESET, базата знания е най-мощният инструмент за разрешаване на различни проблеми.

Относно ESET Internet Security

Този прозорец предоставя подробности за инсталираната версия на ESET Internet Security и вашия компютър.



Щракнете върху **Показване на модули,** за да видите информация за списъка със заредени

програмни модули.

• Можете да копирате информация за модулите в клипборда, като щракнете върху **Копирай**. Това може да е полезно при отстраняването на проблем или при връзка с отдела за техническа поддръжка.

• Щракнете върху **Система за засичане на потенциално опасни заплахи** в прозореца „Модули“, за да отворите радара за вируси на ESET, който съдържа информация за всяка версия на системата за засичане на потенциално опасни заплахи на ESET.

Новини от ESET

В този прозорец ESET Internet Security редовно ви информира за новини от ESET.

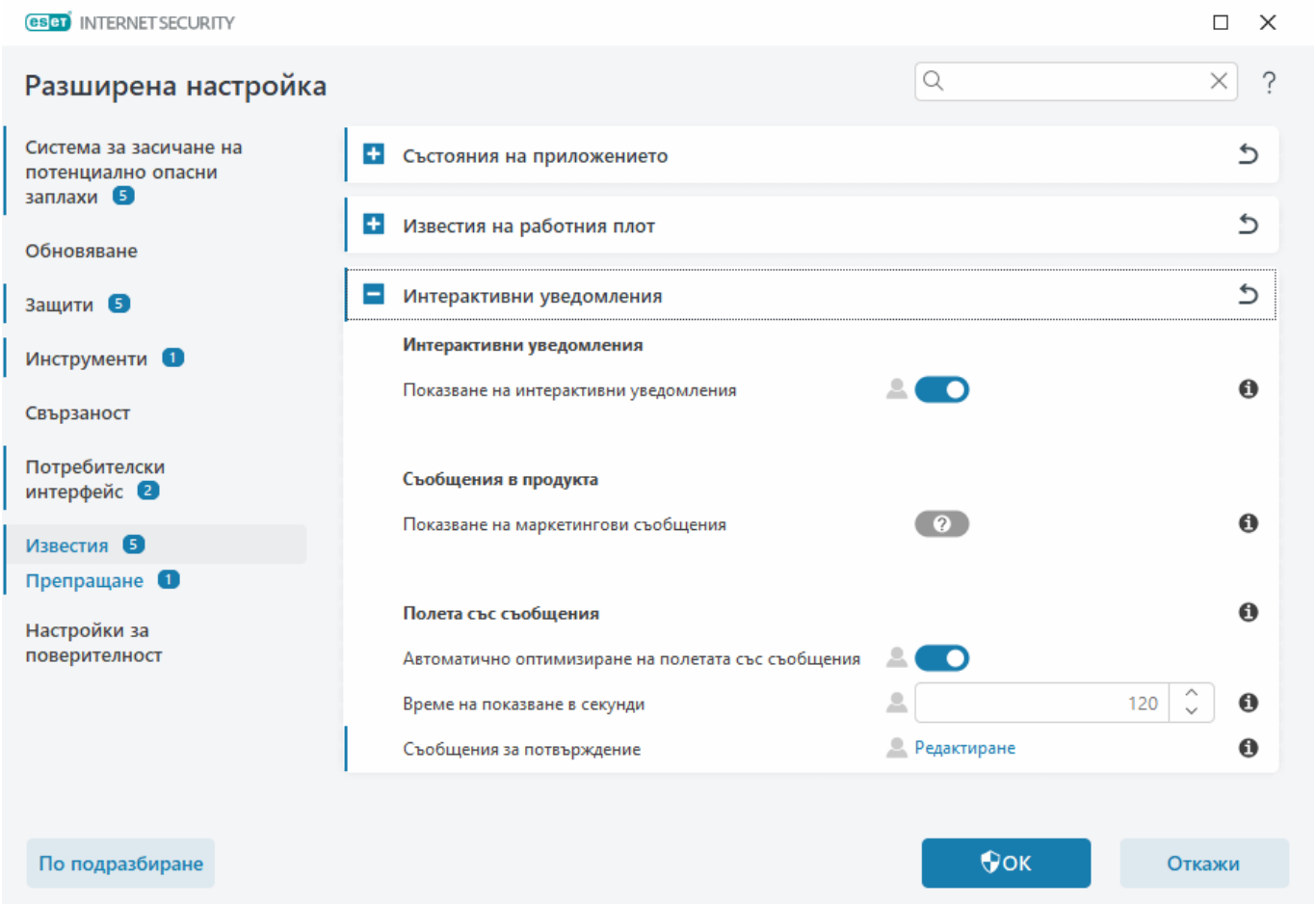
Съобщенията в продукта са създадени да информират потребителите за новини от ESET и други комуникации. Изпращането на маркетингови съобщения изисква съгласието на потребител. Следователно маркетинговите съобщения не се изпращат до потребител по подразбиране (показан като въпросителен знак). Като разрешите тази опция, се съгласявате да получавате маркетингови съобщения от ESET. Ако нямате интерес към **получаването на маркетингов материал** от ESET, забранете опцията.

За да разрешите или забраните получаването на маркетингови съобщения чрез прозорец за известие, следвайте инструкциите по-долу.

1. Отвори разширените настройки.

2. Щракнете върху **Известия** > **Интерактивни уведомления**.

3. Променете опцията **Показване на маркетингови съобщения**.



Изпращане на данните с конфигурация на системата

За да може да предоставя помощ възможно най-бързо и точно, ESET има нужда от информация за конфигурацията на ESET Internet Security, подробна информация за системата и изпълняваните процеси (Регистрационен файл на ESET SysInspector), както и данни от системния регистър. ESET ще използва тези данни единствено с цел предоставяне на техническа помощ на клиента.

След като изпратите уеб формуляра, данните за конфигурацията на вашата система ще бъдат изпратени на ESET. Изберете **Винаги изпращай тази информация**, ако искате да се запомни това действие за този процес. За изпращане на уеб формуляра, без да изпращате никакви данни, щракнете върху **Не изпращай данни** и продължете.

Можете да конфигурирате изпращането на данни с конфигурация на системата в Разширени настройки > **Инструменти** > **Диагностика** > Техническа поддръжка.

Ако сте решили да изпратите данни с конфигурацията на системата, е необходимо да попълните и изпратите уеб формуляра. В противен случай билетът ви няма да бъде създаден и данните с конфигурацията на системата ще бъдат изгубени. Ако данните с конфигурацията на системата не могат да бъдат изпратени, попълнете уеб формуляра и изчакайте инструкции от техническата поддръжка.

Техническа поддръжка

В главния прозорец на програмата щракнете върху **Помощ и поддръжка** > **Техническа поддръжка**.

Свържете се с отдела за техническа поддръжка

Заявка за поддръжка – ако не можете да намерите отговор на проблема си, можете да използвате този формуляр, намиращ се в уеб сайта на ESET, за да се свържете бързо с отдела за техническа поддръжка на ESET. Въз основа на вашите настройки, преди да попълните уеб формуляра, се показва прозорецът Изпращане на данни с конфигурацията на системата.

Получаване на информация за техническа поддръжка

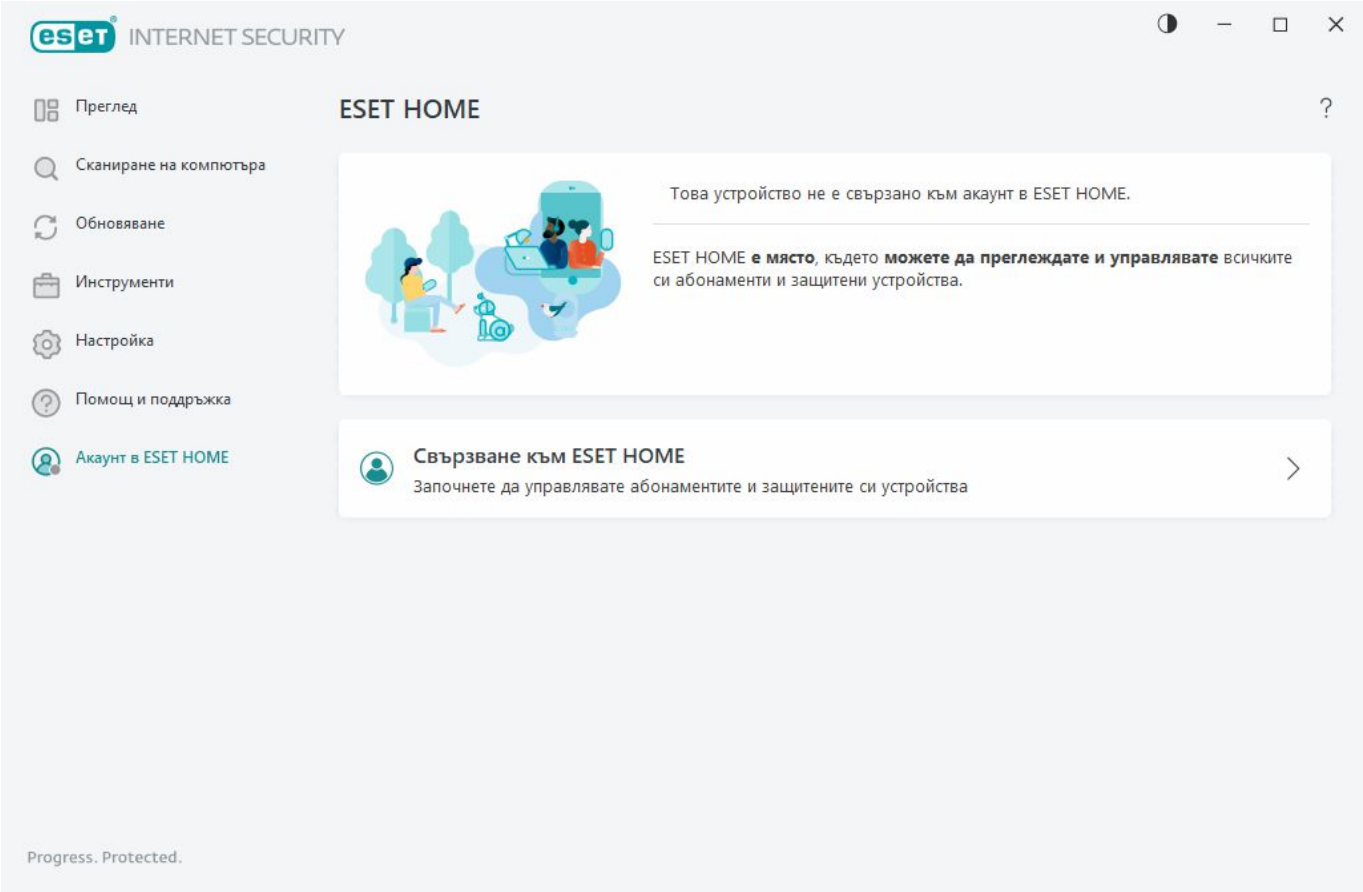
Подробни данни за отдела за техническа поддръжка – когато получите подкана, можете да копирате и изпратите информация на отдела за техническа поддръжка на ESET (като например подробности за абонамента, име на продукта, версия на продукта, операционна система и информация за компютъра).

ESET Log Collector – връзки към статията от онлайн помощника на ESET, където можете да изтеглите ESET Log Collector – приложение, което автоматично събира информация и дневници от компютър с цел по-бързото отстраняване на проблеми. За повече информация вж. ESET Log Collector онлайн ръководството за потребителя.

Разрешете Разширено регистриране за създаване на разширени дневници за всички налични функции, за да помогнете на разработчиците да диагностицират и отстраняват проблеми. Минималната детайлност при регистриране е зададена на ниво **Диагностични**. Разширеното регистриране автоматично ще се забрани след два часа, освен ако не го спрете по-рано, като щракнете върху **Спиране на разширено регистриране**. Когато всички регистрационни файлове са създадени, прозорецът за известия ще се покаже, предоставяйки директен достъп до папката „Диагностични“ със създадените регистрационни файлове.

Акаунт в ESET HOME

Можете да прегледате състоянието на връзката с акаунта в ESET HOME в главния прозорец на акаунта > **Акаунт в ESET HOME**.



Това устройство не е свързано към акаунт в ESET HOME.

Щракнете върху Свързване към ESET HOME, за да свържете устройството към ESET HOME и да управлявате своите абонаменти и защитени устройства. Може да подновите, надстроите или разширите абонамента си и да видите важни подробности за него. В портала за управление на ESET HOME или мобилното приложение можете да добавяте различни абонаменти, да изтегляте продукти на устройствата си, да проверявате състоянието на защитата на продукта или да споделяте абонамента чрез имейл. За повече информация посетете онлайн помощ за ESET HOME.

Това устройство е свързано към акаунт в ESET HOME

Можете да управлявате сигурността на устройството си дистанционно с Портал на ESET HOME или мобилно приложение. Щракнете върху **App Store** или **Google Play**, за да се покаже QR код на екрана, който може да сканирате с мобилния си телефон, за да изтеглите мобилното приложение ESET HOME от App Store или Google Play.

Акаунт в ESET HOME – името на вашия акаунт в ESET HOME.

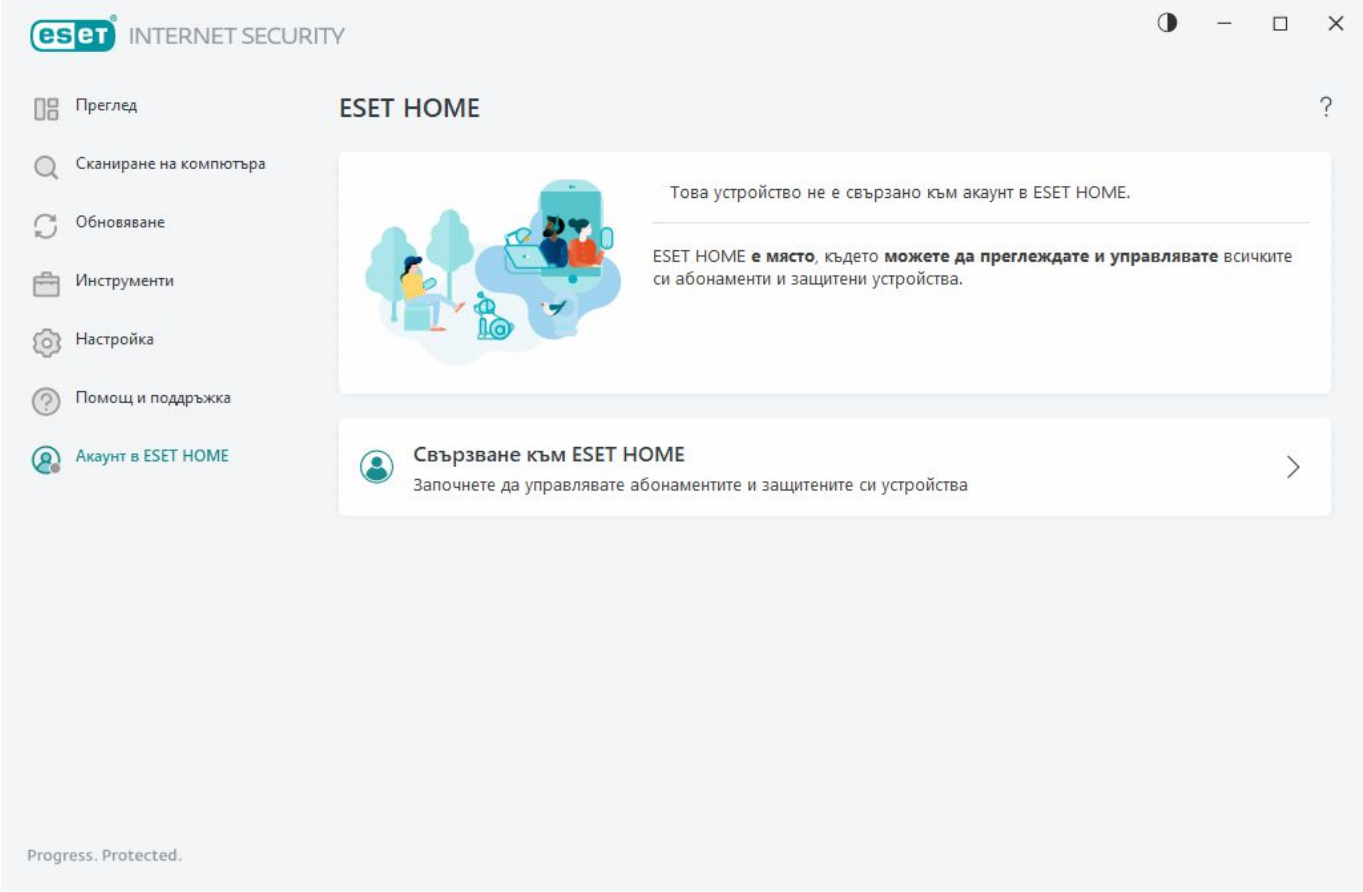
Име на устройството – името на това устройство, показвано в акаунта в ESET HOME.

Отваряне на ESET HOME – отваря портала за управление на ESET HOME.

За да изключите устройството си от акаунта в ESET HOME, щракнете върху **Прекъсване на връзката с ESET HOME** > **Прекъсване на връзката**. Абонамент, използван за активиране, ще остане активен и устройството ви ще бъде защитено.

Свързване с ESET HOME

Свържете устройството си към ESET HOME, за да преглеждате и управлявате всички активирани абонаменти и устройства на ESET. Може да подновите, надстроите или разширите абонамента си и да видите важни подробности за абонамента. В портала за управление на ESET HOME или мобилното приложение можете да добавяте различни абонаменти, да изтегляте продукти на устройствата си, да проверявате състоянието на защитата на продукта или да споделяте абонамента чрез имейл. За повече информация посетете онлайн помощ за ESET HOME.



За да свържете устройството си с ESET HOME:

Ако се свързвате с ESET HOME по време на инсталиране или при избиране на **Използване на акаунт в ESET HOME** като метод на активиране, спазвайте инструкциите в темата Използване на акаунт в ESET HOME.

Ако вече сте инсталирали ESET Internet Security и продуктът е активиран с абонамент, добавен във вашия акаунт в ESET HOME, можете да свържете устройството си с ESET HOME чрез портала ESET HOME. Следвайте инструкциите в ESET HOME ръководството за онлайн помощ и позволете връзката в ESET Internet Security.

1. В главния прозорец на програмата щракнете върху **ESET HOME** акаунт > **Свързване с ESET HOME** или щракнете върху **Свързване с ESET HOME** в известието **Свързване на това устройство с акаунт в ESET HOME**.

2. Влезте в акаунта си ESET HOME.

Ако нямате акаунт в ESET HOME, щракнете върху **Създаване на акаунт** за регистриране или вижте инструкциите в онлайн помощта за ESET HOME.
Ако сте забравили паролата си, щракнете върху **Забравих паролата си** и следвайте стъпките на екрана или вижте онлайн помощта за ESET HOME.

3. Задайте **Име на устройството** и щракнете върху **Продължаване**.

4. След успешно свързване се показва прозорец с подробности. Щракнете върху **Готово**.

Вход в ESET HOME

Има няколко налични метода за влизане във вашия акаунт в ESET HOME:

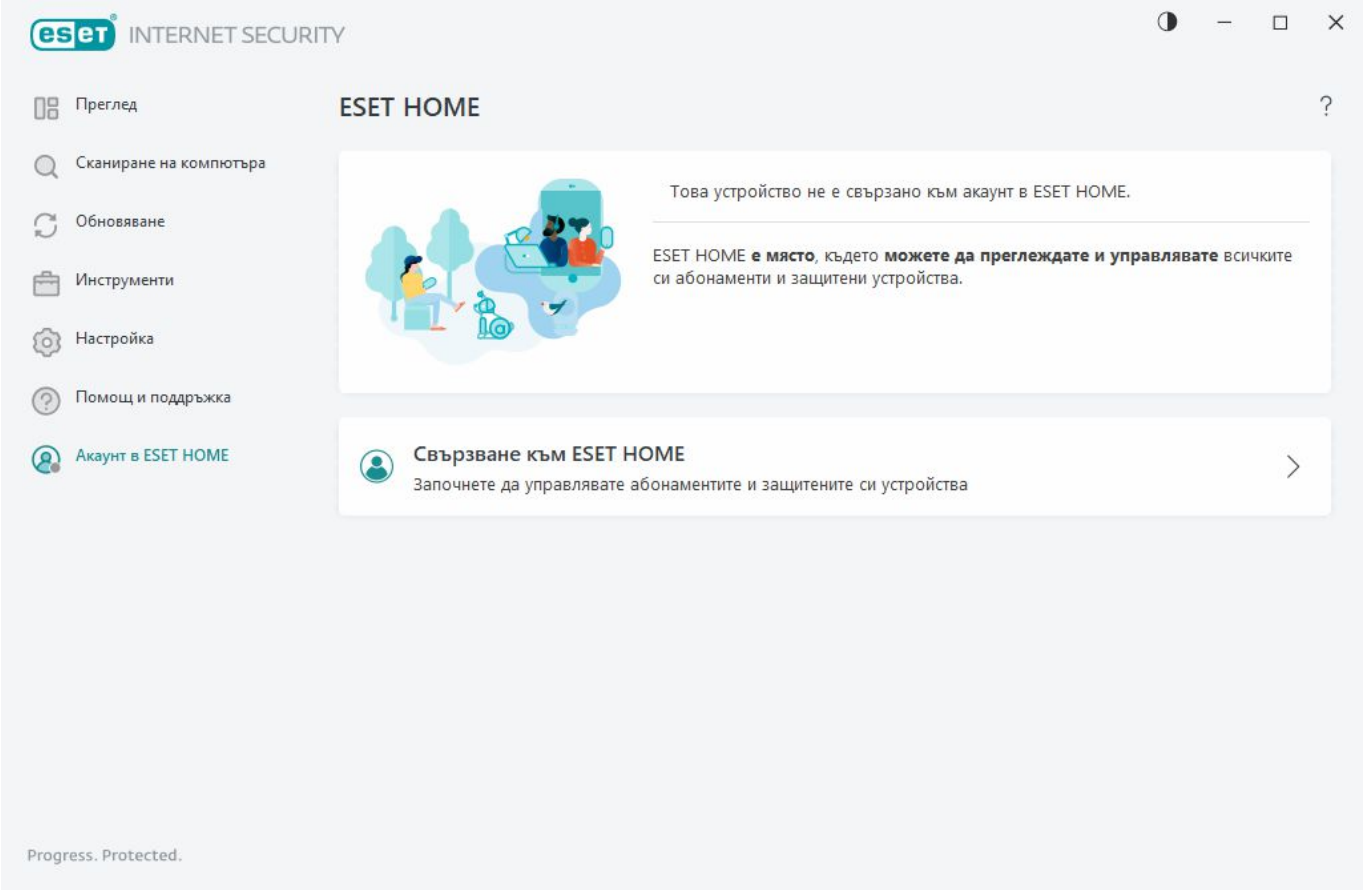
• **Използване на имейл адреса и паролата в ESET HOME** – Въведете **имейл адреса** и **Паролата**, които сте използвали, за да създадете акаунта си в ESET HOME, и щракнете върху **Влизане**.

• **Използвайте своя акаунт в Google/AppleID** – Щракнете върху **Продължаване с Google** или **Продължаване с Apple** и влезте в съответния акаунт. След успешно влизане ще бъдете пренасочени към уеб страницата за потвърждение на ESET HOME. За да продължите, превключете отново към страницата на продукта на ESET. За повече информация относно влизането в Google/AppleID вж. онлайн помощта за ESET HOME.

• **Сканиране на QR код** – Щракнете върху **Сканиране на QR код**, за да се покаже QR кодът. Отворете мобилното си приложение ESET HOME и сканирайте QR кода или насочете камерата на устройството си към QR кода. За повече информация вижте инструкциите в онлайн помощта за ESET HOME.

Ако нямате акаунт в ESET HOME, щракнете върху **Създаване на акаунт** за регистриране или вижте инструкциите в онлайн помощта за ESET HOME.
Ако сте забравили паролата си, щракнете върху **Забравих паролата си** и следвайте стъпките на екрана или вижте онлайн помощта за ESET HOME.

Неуспешно влизане – често срещани грешки.



Неуспешно влизане – често срещани грешки

Не успяхме да открием акаунт, който да съответства на въведения имейл адрес

Имейл адресът, която въведохте, не съвпада с нито един акаунт в ESET HOME. Щракнете върху **Назад** и въведете правилния имейл адрес и парола.

За да влезете, трябва да създадете акаунт в ESET HOME. Ако нямате акаунт в ESET HOME, щракнете върху **Назад** > **Създаване на акаунт** или вижте Създаване на нов акаунт в ESET HOME.

Потребителското име и паролата не съвпадат

Въведената парола не съответства на въведения имейл адрес. Щракнете върху **Назад**, въведете правилната парола и се уверете, че въведеният имейл адрес е правилен. Ако все още не сте в състояние да влезете, щракнете върху **Назад** > **Забравих паролата си**, за да подновите паролата си, и следвайте стъпките на екрана или вж. Забравих паролата си за ESET HOME.

Избраната опция за вход не съответства на акаунта ви

Акаунтът ви е свързан с вашия акаунт в социалните мрежи. За да влезете в ESET HOME, щракнете върху **Продължаване с Google** или **Продължаване с Apple** и влезте в съответния акаунт. След успешно влизане ще бъдете пренасочени към уеб страницата за потвърждение на ESET HOME. Можете да изключите акаунта си в социалните мрежи от акаунта си в ESET HOME в портала ESET HOME.

Неправилна парола

Тази грешка може да възникне, ако вашият ESET Internet Security вече е свързан с ESET HOME и правите промени, които изискват да влезете в системата (например забраняване на Anti-Theft), а въведената от вас парола не съответства на акаунта ви. Щракнете върху **Назад** и въведете правилната парола. Ако все още не сте в състояние да влезете, щракнете върху **Назад** > **Забравих паролата си**, за да подновите паролата си, и следвайте стъпките на екрана или вж. Забравих паролата си за ESET HOME.

Добавяне на устройство в ESET HOME

Ако вече сте инсталирали ESET Internet Security и продуктът е активиран с абонамент, добавен във вашия акаунт в ESET HOME, можете да свържете устройството си с ESET HOME чрез портала ESET HOME:

1. Изпратете заявка за връзка към вашето устройство.

2. ESET Internet Security показва диалоговия прозорец **Свържете това устройство с акаунт в ESET HOME** с името на вашия акаунт в ESET HOME. Щракнете върху **Позволяване**, за да свържете устройството със споменатия акаунт в ESET HOME.

> Ако няма взаимодействие, заявката за свързване ще бъде отказана автоматично след приблизително 30 минути.

Разширени настройки

Разширените настройки ви позволяват да конфигурирате подробни настройки на ESET Internet Security, които да отговарят на вашите нужди.

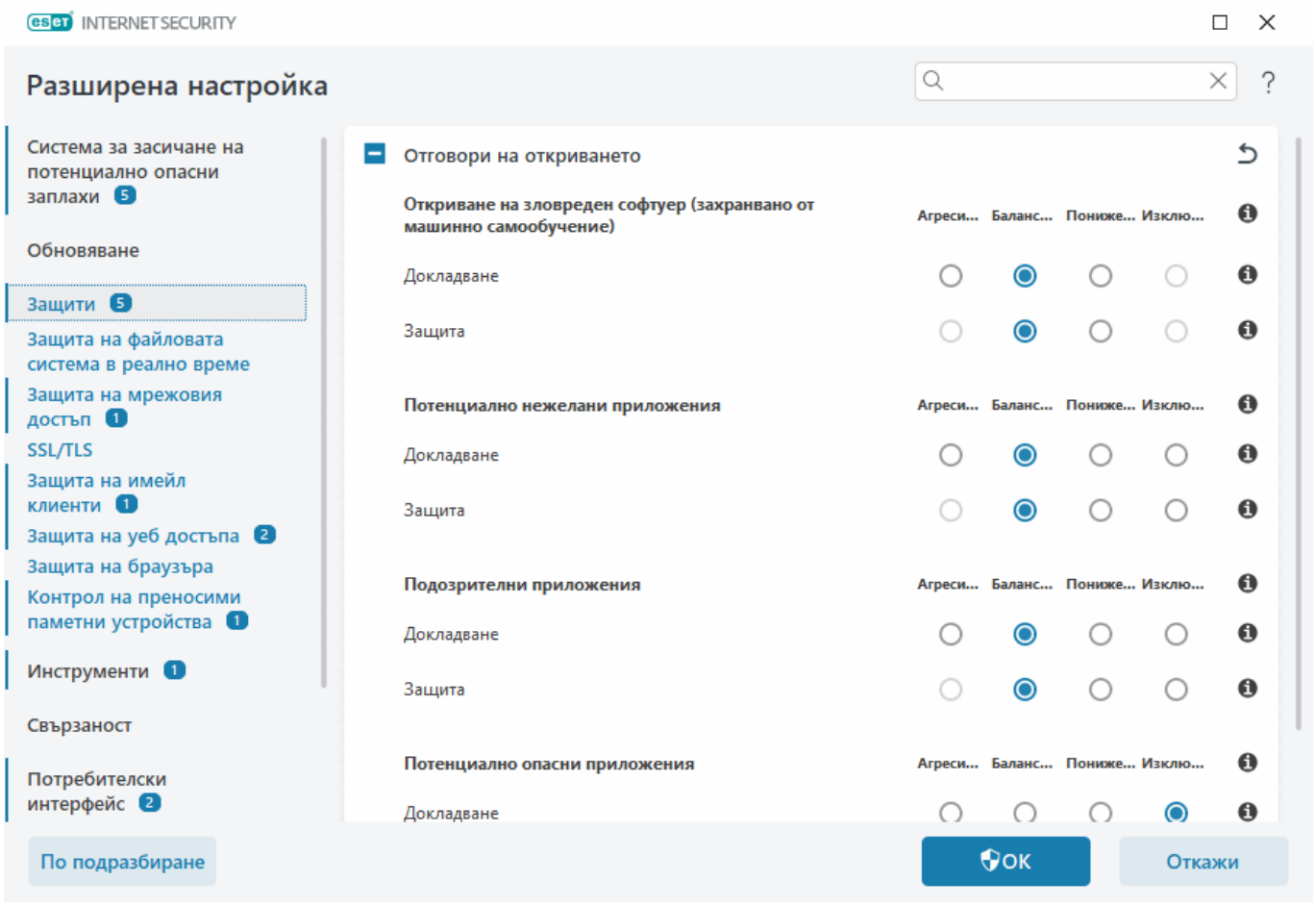
За да отворите „Разширени настройки“, отворете главния прозорец на програмата и натиснете клавиша **F5** на клавиатурата или щракнете върху **Настройка** > **Разширени настройки**.

> В зависимост от вашата настройка на Access може да бъдете подканени да въведете парола, за да отворите разширените настройки.

В разширените настройки можете да конфигурирате следните настройки:

- Система за засичане на потенциално опасни заплахи
- Обновяване

- Защити
- Инструменти
- Свързаност
- Потребителски интерфейс
- Известия
- Настройки за поверителност



Система за засичане на потенциално опасни заплахи

Разширени настройки > **Система за засичане** ви позволява да конфигурирате следните опции:

- Изключения
- Разширени опции
- Скенер за мрежов трафик

Изключения

Изключенията ви позволяват да изключвате обекти от системата за засичане на потенциално опасни заплахи. За да се гарантира, че всички обекти са сканирани, препоръчително е да създавате изключения само когато е абсолютно необходимо. Ситуациите, в които може да е необходимо да изключите обект, включват сканиране на записи в големи бази данни, които биха забавили компютъра ви по време на сканирането, или софтуер, който е в конфликт със сканирането.

Изключения за производителността – изключват файлове и папки от сканиране. Изключения за производителността са полезни за изключване на сканиране на игрови приложения на ниво файл или когато е причинено необичайно поведение на системата или повишена производителност.

Изключения от откриването ви позволяват да изключите обекти от откриване чрез името, пътя или хеша на откриването. Изключенията от откриването не изключват файлове и папки от сканиране както изключенията от производителността. Изключенията от откриването изключват обекти само когато те са открити от системата за засичане на потенциално опасни заплахи и е налично подходящо правило в списъка с изключения.

Да не се бъркат с други типове изключения:

- Изключения на процеси – всички операции с файлове, приписани на изключени процеси на приложения, се изключват от сканиране (може да е необходимо за подобряване на скоростта на архивиране и наличността на услугата).
- Изключени файлови разширения,
- HIPS изключения,
- Филтър за изключения за базирана в облака защита

Изключения за производителността

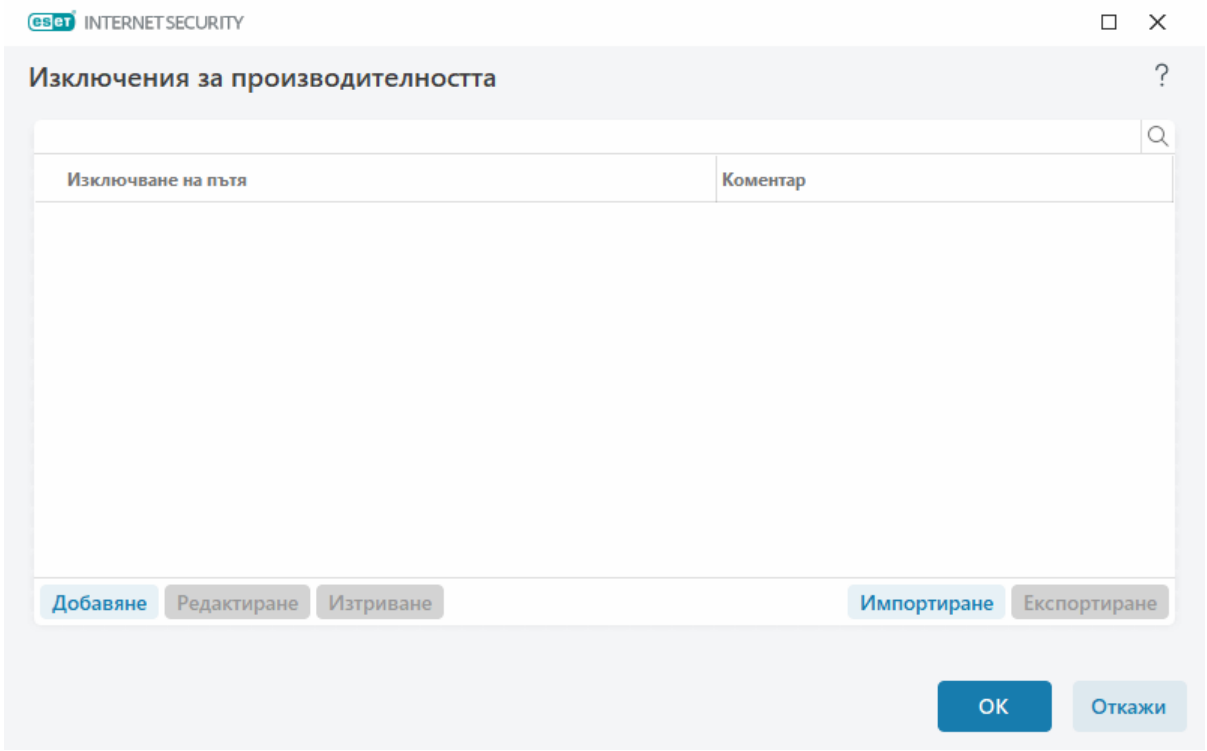
Изключения за производителността ви позволяват да изключвате файлове и папки от сканирането.

За да гарантирате, че всички обекти са сканирани за заплахи, препоръчително е да създавате изключения за производителността само когато е абсолютно необходимо. Въпреки това има ситуации, в които може да е необходимо да изключите обект, като например записи в голяма база данни, които биха забавили компютъра ви по време на сканиране, или софтуер, който е в конфликт със сканирането.

Може да добавяте файлове и папка, които да бъдат изключени от сканиране в списъка с изключения чрез Разширени настройки > **Система за засичане на потенциално опасни заплахи** > **Изключения** > **Изключения за производителността** > **Редактиране**.

> Не се бъркайте с Изключения за откриването, Изключени файлови разширения, HIPS изключения или Изключения на процесите.

За да изключите обект (път: заплаха или папка) от сканиране, щракнете върху **Добавяне** и въведете приложимия път или го изберете в дървовидната структура.



Заплаха във файл няма да бъде открита от модула за **защита на файловата система в реално време** или от модула за **сканиране на компютъра**, ако файлът отговаря на критериите за изключване от сканирането.

Контролни елементи

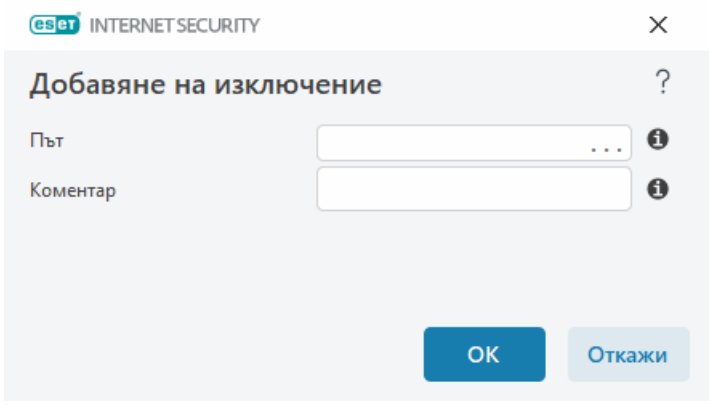
- **Добавяне** – изключване на обектите от откриване.
- **Редактиране** – позволява да редактирате избраните записи.
- **Премахване** – премахва избраните записи (CTRL + щракване за избор на няколко записа).

Добавяне или редактиране на изключения за производителността

Този диалогов прозорец изключва конкретен път (файл или директория) за този компютър.

Изберете път или го въведете ръчно

За да изберете подходящ път, щракнете върху **...** в полето **Път**.
Когато пишете на ръка, вижте повече примери за формат за изключения по-долу.



Можете да използвате заместващи символи, за да изключите група файлове. Въпросителният знак (*?*) представлява един променлив знак, а звездичката (***) представлява променлив низ от нула или няколко знака.

Формат за изключвания

- Ако искате да изключите всички файлове и подпапки в дадена папка, въведете пътя до нея и използвайте маската *
- Ако искате да изключите само документи, използвайте маската **.doc*
- Ако името на изпълним файл има определен брой знаци (като знаците се различават) и знаете със сигурност само първия от тях (например D), използвайте следния формат: *D????.exe* (въпросителни знаци заместват липсващите/неизвестни знаци)

Примери:

- *C:\Tools** – пътят трябва да завършва с наклонена наляво черта (\) и звезда (*), за да покаже, че е папка и цялото съдържание на папката (файлове и подпапки) ще бъде изключено.
- *C:\Tools*.** – същото поведение като *C:\Tools**
- *C:\Tools* – папка *Tools* няма да бъде изключена. От гледната точка на скенера *Tools* може да бъде също така име на файл.
- *C:\Tools*.dat* – това ще изключи файловете с разширение .dat в папка *Tools*.
- *C:\Tools\sg.dat* – това ще изключи този конкретен файл, разположен в точно това местоположение.

Системни променливи в изключенията

Можете да използвате системни променливи като %PROGRAMFILES% за дефиниране на изключения при сканиране.

• За да изключите папката „Програмни файлове“ чрез тази системна променлива, използвайте пътя *%PROGRAMFILES%** (задължително добавете наклонена наляво черта или звезда в края на пътя) при добавянето на изключения

• За да изключите всички файлове и папки в поддиректория на *%PROGRAMFILES%*, използвайте пътя *%PROGRAMFILES%\Excluded_Directory**

Разширяване на списъка с поддържани системни променливи

Във формата на изключения от тип "Път" могат да се използват следните променливи:

- *%ALLUSERSPROFILE%*
- *%COMMONPROGRAMFILES%*
- *%COMMONPROGRAMFILES(X86)%*
- *%COMSPEC%*
- *%PROGRAMFILES%*
- *%PROGRAMFILES(X86)%*
- *%SystemDrive%*
- *%SystemRoot%*
- *%WINDIR%*
- *%PUBLIC%*

Не се поддържат системни променливи, специфични за отделните потребители (като *%TEMP%* или *%USERPROFILE%*) или променливи на средата (като *%PATH%*).

Заместващи символи в средата на пътя не се поддържат

Използването на заместващи символи в средата на пътя (например *C:\Tools*\Data\file.dat*) може да работи, но не се поддържа официално за изключенията за производителността. Няма ограничения за използването на заместващи символи в средата на пътя при използването на изключения от откриване.

Приоритетен ред на изключенията

• Няма опции за регулиране на нивото на приоритет на изключения чрез бутони за преместване нагоре/надолу (също като за Правила за защитната стена, където правилата се изпълняват отгоре надолу).

• При откриване на съвпадение спрямо първото приложимо правило от програмата за сканиране второто приложимо правило не се оценява.

• Колкото по-малко са правилата, толкова по-добри са резултатите от сканирането.

• Избягване на създаването на паралелни правила.

Формат на изключения от тип "Път"

Можете да използвате заместващи символи, за да изключите група файлове. Въпросителният знак (*?*) представлява един променлив знак, а звездичката (***) представлява променлив низ от нула или няколко знака.

Формат за изключвания

• Ако искате да изключите всички файлове и подпапки в дадена папка, въведете пътя до нея и използвайте маската *

• Ако искате да изключите само документи, използвайте маската **.doc*

• Ако името на изпълним файл има определен брой знаци (като знаците се различават) и знаете със сигурност само първия от тях (например D), използвайте следния формат: *D????.exe* (въпросителни знаци заместват липсващите/неизвестни знаци)

Примери:

• *C:\Tools** – пътят трябва да завършва с наклонена наляво черта (\) и звезда (*), за да покаже, че е папка и цялото съдържание на папката (файлове и подпапки) ще бъде изключено.

• *C:\Tools*.** – същото поведение като *C:\Tools**

• *C:\Tools* – папка *Tools* няма да бъде изключена. От гледната точка на скенера *Tools* може да бъде също така име на файл.

• *C:\Tools*.dat* – това ще изключи файловете с разширение .dat в папка *Tools*.

• *C:\Tools\sg.dat* – това ще изключи този конкретен файл, разположен в точно това местоположение.

Системни променливи в изключенията

Можете да използвате системни променливи като %PROGRAMFILES% за дефиниране на изключения при сканиране.

• За да изключите папката „Програмни файлове“ чрез тази системна променлива, използвайте пътя *%PROGRAMFILES%** (задължително добавете наклонена наляво черта или звезда в края на пътя) при добавянето на изключения

• За да изключите всички файлове и папки в поддиректория на *%PROGRAMFILES%*, използвайте пътя *%PROGRAMFILES%\Excluded_Directory**

Разширяване на списъка с поддържани системни променливи

Във формата на изключения от тип "Път" могат да се използват следните променливи:

• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*

Не се поддържат системни променливи, специфични за отделните потребители (като *%TEMP%* или *%USERPROFILE%*) или променливи на средата (като *%PATH%*).

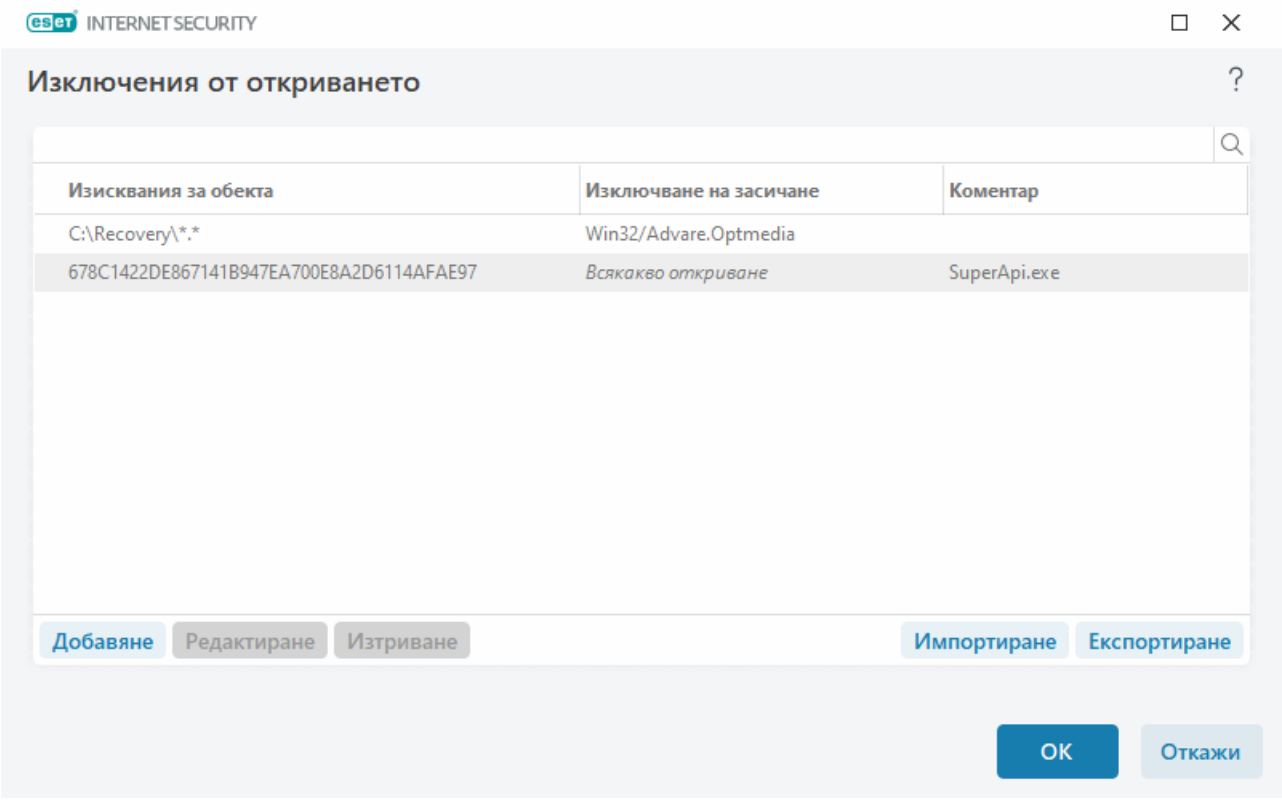
Изключения от откриването

Изключенията от откриване ви позволяват да изключите обекти от откриване, като филтрирате името, пътя до обекта или хеша на откриването.

Как работят изключенията от откриване

Изключенията от откриване не изключват файлове и папки от сканиране както изключенията за производителността. Изключенията от откриването изключват обекти само когато те са открити от системата за засичане на потенциално опасни заплахи и е налично подходящо правило в списъка с изключения.

Например (вижте първия ред в изображението по-долу), когато обект е открит като Win32/Adware.Optmedia и откритият файл е *C:\Recovery\file.exe*. На втория ред всеки файл, който съдържа подходящия хеш SHA-1, винаги ще бъде изключван въпреки името на откриването.



За да се гарантира, че всички заплахи са открити, препоръчваме създаването на изключения от откриването само когато е абсолютно необходимо.

За добавяне на файлове и папки към списъка с изключения отворете Разширени настройки > **Система за засичане** > **Изключения** > **Изключения от откриване** > **Редактиране**.

Не се бъркайте с Изключения за производителността, Изключени файлови разширения, HIPS изключения или Изключения на процесите.

За да изключите обект (по неговото име на откриване или хеш) от системата за засичане на потенциално опасни заплахи, щракнете върху **Добавяне**.

За Потенциално нежелани приложения и Потенциално опасни приложения може да се създаде изключение по техните имена на откриване:

- В прозореца за известяване, който отчита откриването (щракнете върху **Показване на разширени опции**, след което изберете **Изключване от откриване**).
- От контекстното меню „Регистрационни файлове“ чрез съветника за създаване на изключения от откриване.

• Като щракнете върху **Инструменти** > **Карантина**, след което щракнете с десен бутон върху файла под карантина и изберете **Възстановяване и изключване от сканиране** от контекстното меню.

Изисквания за обектите на изключения от откриването

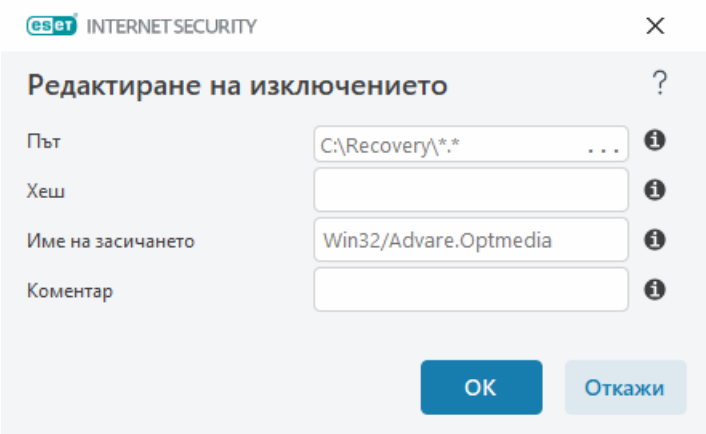
- **Път** – ограничете изключение от откриването за определен път (или всякакъв).
- **Име на откриване** – Ако до изключен файл има име на откриване, това означава, че файлът е изключен само за даденото откриване, а не напълно. Ако този файл бъде заразен по-късно с друг злонамерен софтуер, той ще бъде открит.
- **Хеш** – изключва файл на база указан хеш SHA-1, независимо от типа, местоположението, името или разширението на файла.

Добавяне или редактиране на изключение от откриване

Изключване на засичане

Трябва да се укаже валидно име на засичане на ESET. За валидно име на засичане вж. Регистрационни файлове и изберете **Засичания** от падащото меню „Регистрационни файлове“. Това е полезно при откриване на грешен положителен пример в/във ESET Internet Security. Изключенията за действителни прониквания може да са много опасни, така че обмислете изключване само на засегнатите файлове/директории, като щракнете върху **...** в полето **Маска**, и/или само за определен период. Изключенията също се прилагат за потенциално нежелани приложения, потенциално опасни приложения и подозрителни приложения.

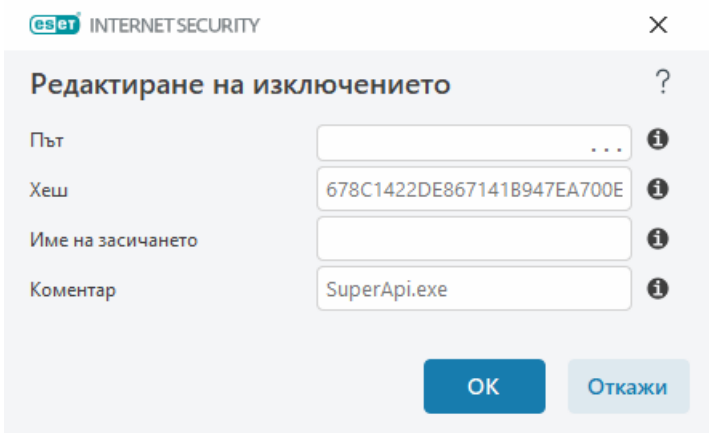
Вижте също формат на изключения от тип „Път“.



Вижте примера на изключения от откриване по-долу.

Изключване на хеш

изключва файл на база указан хеш SHA-1, независимо от типа, местоположението, името или разширението на файла.



Изключения по име на откриване

За да изключите определено откриване по неговото име, въведете валидно име на откриване:
Win32/Adware.Optmedia
Можете също да използвате следния формат при изключване на засичане от прозореца за уведомления на ESET Internet Security:
@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
@NAME=Win32/Bagle.D@TYPE=worm

Контролни елементи

- **Добавяне** – изключване на обектите от откриване.
- **Редактиране** – позволява да редактирате избраните записи.
- **Премахване** – премахва избраните записи (CTRL + щракване за избор на няколко записа).

Съветник за създаване на изключения от откриване

Изключение от откриване също може да бъде създадено от контекстното меню Регистрационни файлове (не е налично за откривания на злонамерен софтуер):

1. В главния прозорец на програмата щракнете върху **Инструменти** > **Регистрационни файлове**.
2. Щракнете с десния бутон върху откриване в **Дневника с откривания**.
3. Щракнете върху **Създаване на изключение**.

За да изключите едно или повече откривания, базирани на **Критерии за изключение**, щракнете върху **Промяна на критерии**:

- **Точни файлове** – изключване на всеки файл по неговия SHA-1 хеш.

• **Откриване** – изключване на всеки файл по неговото име на откриване.

• **Път + откриване** – изключване на всеки файл по неговото име и път на откриване, включително по името на файла (напр. *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

Препоръчаната настройка е предварително избрана въз основа на типа откриване.

Ако желаете, можете да добавите **Коментар**, преди да щракнете върху **Създаване на изключение**.

Разширени опции на системата за засичане на потенциално опасни заплахи

Разрешаване на разширено сканиране чрез AMSI е инструментът Microsoft Antimalware Scan Interface, който позволява сканиране на скриптове на PowerShell, скриптове, изпълнени от Windows Script Host, и данни, сканирани с помощта на AMSI SDK.

Скенер за мрежов трафик

Скенерът за мрежов трафик осигурява защита срещу злонамерен софтуер за протоколите на приложенията, която интегрира множество усъвършенствани техники за сканиране на злонамерен софтуер. Скенерът за мрежов трафик сканира автоматично протоколите HTTP(S), POP3(S) и IMAP(S), независимо от интернет браузъра или имейл клиента. Можете да разрешите/забраните скенера за мрежов трафик в Разширени настройки > **Система за засичане** > **Скенер за мрежов трафик**.

Разрешаване на скенер за мрежов трафик – Ако забраните тази опция, протоколите HTTP(S), POP3(S) и IMAP(S) няма да бъдат сканирани. Обърнете внимание, че следните функции на ESET Internet Security изискват активиран скенер за мрежов трафик:

- Защита на уеб достъпа
- Родителски контрол
- Поверителност и защита на браузъра
- Безопасно банкиране и сърфиране
- SSL/TLS
- Анти-фишинг защита
- Защита на имейл клиенти

Базирана на облак защита

Услугата ESET LiveGrid® (базирана на системата за ранно предупреждаване ThreatSense.Net на ESET) използва данни, изпратени от потребители на ESET в целия свят, и ги изпраща на лабораторията на ESET за проучвания. Осигурявайки подозрителни примери и метаданни от практиката, ESET LiveGrid® ни дава възможност да реагираме незабавно на нуждите на потребителите ни и да поддържаме ESET ефективен срещу най-новите заплахи.

Налични са следните опции:

Разрешаване на системата за репутация на ESET LiveGrid®

Системата за репутация на ESET LiveGrid® осигурява създаване на базирани в облака списъци с разрешени адреси и списъци със забранени адреси.

Можете да проверявате репутацията на изпълняващи се процеси и файлове директно от програмния интерфейс или от контекстното меню с допълнителна информация, предоставена от ESET LiveGrid®.

Разрешаване на системата за обратна връзка на ESET LiveGrid®

В допълнение към системата за репутация на ESET LiveGrid® системата за обратна връзка на ESET LiveGrid® ще събира информация за вашия компютър, свързана с новооткрити заплахи. Тази информация може да включва:

- Пример или копие на файла, в който се е появила заплахата
- Път до файла
- Име на файла
- Дата и час
- Процесът, чрез който заплахата се е появила на вашия компютър
- Информация за операционната система на компютъра

По подразбиране ESET Internet Security е конфигуриран да изпраща подозрителните файлове за подробен анализ в лабораторията за вируси на ESET. Винаги се изключват файловете с определени разширения като *.doc* или *.xls*. Можете също така да добавите други разширения, ако има конкретни файлове, които организацията ви или вие не искате да се изпращат.

Прочетете повече за изпращането на съответните данни в Правилата за поверителност.

Можете да изберете да не разрешавате ESET LiveGrid®

Ще загубите функционалността в софтуера, но в някои случаи ESET Internet Security може да отговаря по-бързо на нови заплахи, когато ESET LiveGrid® е разрешена. Ако по-рано вече сте

използвали ESET LiveGrid® и сте я забранили, може все още да има пакети данни за изпращане. Дори след деактивиране подобни пакети ще бъдат изпращани на ESET. След като бъде изпратена текущата информация, повече няма да се създават нови пакети.

> Прочетете повече за ESET LiveGrid® в речника.
> Вижте нашите илюстрирани инструкции, достъпни на английски и няколко други езика, за разрешаване или забраняване на ESET LiveGrid® в ESET Internet Security.

Конфигуриране на базирана в облака защита в разширените настройки

За да осъществите достъп до настройките за ESET LiveGrid®, отворете Разширени настройки > **Система за засичане** > **Базирана в облака защита**.

• **Разрешаване на ESET LiveGrid® система за репутация (препоръчително)** – Системата за репутация ESET LiveGrid® подобрява ефективността на решенията срещу злонамерен софтуер на ESET чрез сравняване на сканираните файлове с база данни в облака от елементи, включени в списъци с разрешени и забранени адреси.

• **Разрешаване на системата за обратна връзка на ESET LiveGrid®** – изпраща съответните данни за подаване (описани в раздел **Подаване на примери по-долу**) заедно с докладите за сривове и статистиката в лабораторията на ESET за проучвания за по-нататъшен анализ.

• **Изпращане на отчети за сривове и диагностични данни** – изпраща свързаните диагностични данни на ESET LiveGrid®, като например отчети за сривове и аварийни копия на паметта на модулите. Препоръчваме ви да го оставите разрешено, за да помогнете на ESET да диагностицира проблеми, да подобри продуктите и да осигури по-добра защита на крайния потребител.

• **Изпращане на анонимни статистики** – позволявате на ESET да събира информация за новооткрити заплахи, като например името на заплахата, датата и часа на откриване, метода на откриване и свързаните метаданни, версия на продукта, както и конфигурация, включително информация за вашата система.

• **Имейл за контакт (незадължителен)** – Вашият имейл адрес за контакт може да бъде включен към всякакви подозрителни файлове и може да бъде използван за връзка с вас, ако за анализа е необходима допълнителна информация. Обърнете внимание, че няма да получите отговор от ESET, освен ако не е необходима допълнителна информация.

Изпращане на примери

Ръчно изпращане на примери – разрешава опцията за ръчно изпращане на примери към ESET от контекстното меню, Карантина или Инструменти.

Автоматично изпращане на открити примери

Изберете какъв вид примери ще бъдат изпратени на ESET за анализ и за подобряване на откриването в бъдеще (по подразбиране максималният размер на пример е 64 МБ). Налични са

следните опции:

• **Всички открити примери** – всички обекти, открити от системата за засичане на потенциално опасни заплахи (включително потенциално нежелани приложения, когато са разрешени в настройките на скенера).

• **Всички примери освен документи** – всички открити обекти освен **Документи** (вижте по-долу).

• **Не изпращай** – откритите обекти няма да бъдат изпращани на ESET.

Автоматично изпращане на подозрителни примери

Тези примери също така ще бъдат изпратени на ESET, ако системата за засичане на потенциално опасни заплахи не ги е открила. Например – примери, които почти са избегнали откриване, или ако един от модулите за защита на ESET Internet Security счита тези примери за подозрителни или с неясно поведение (по подразбиране максималният размер на примера е 64 МБ).

• **Изпълними файлове** – включва изпълними файлове като .exe, .dll, .sys.

• **Архиви** – включва типове архивни файлове като .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.

• **Скриптове** – включва типове файлове за скриптове като .bat, .cmd, .hta, .js, .vbs, .ps1.

• **Други** – включва типове файлове като .jar, .reg, .msi, .sfw, .lnk.

• **Възможни имейли със спам** – това ще разреши изпращането на възможни части със спам или цели имейли със спам с прикачен файл до ESET за по-нататъшен анализ. Разрешаването на тази опция подобрява глобалното откриване на спам, включително подобрения на бъдещото откриване на спам за вас.

• **Документи** – включва документи на Microsoft Office или PDF документи със или без активно съдържание.

Разгънете за списък с всички включени типове файлове на документи

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

Изключения

Филтърът за изключения ви дава възможност да изключвате от изпращане определени файлове/папки (добре е например файлове с потенциално поверителна информация, като например документи и електронни таблици, да се изключват). Файловете в списъка никога няма да се изпращат в лабораториите на ESET за анализ дори ако съдържат подозрителен код. Най-често срещаните типове файлове се изключват по подразбиране (.doc и т.н.). Можете да добавяте файлове към списъка за изключване, когато пожелаете.

За да изключите файловете, изтеглени от `download.domain.com`, отидете в Разширени настройки > **Система за засичане на потенциално опасни заплахи** > **Базирана на облак защита** > **Изпращане на примери** и щракнете върху **Редактиране** до **Изключения**. Добавете изключението `.download.domain.com`.

Максимален размер на примерите (МБ) – Определя максималния размер на автоматично подадените примери (1 – 64 МБ).

Филтър за изключения за базирана в облака защита

Филтърът за изключения ви дава възможност да изключвате определени файлове/папки от изпращане на примери. Файловете в списъка никога няма да се изпращат в лабораториите на ESET за анализ дори ако съдържат подозрителен код. Често срещани типове файлове (като например .doc и т.н.) се изключват по подразбиране.

Тази функция е полезна за изключване на файлове, които може да съдържат поверителна информация, като например документи и електронни таблици.

За да изключите файловете, изтеглени от download.domain.com, щракнете върху Разширени настройки > **Система за засичане** > **Базирана в облака защита** > **Изпращане на примери** > **Изключения** и добавете изключението *download.domain.com*.

Сканирания за злонамерен софтуер

Разделът **Сканирания за злонамерен софтуер** е достъпен от Разширени настройки > **Система за засичане** > **Сканирания за злонамерен софтуер** и ви позволява да конфигурирате параметрите на сканиране за профилите за сканиране.

Сканиране при поискване

Избран профил – определен набор от параметри, използван от скенера при поискване. За да създадете нов, щракнете върху **Редактиране** до **Списък с профили**. Вижте Профили за сканиране за повече подробности.

След като изберете профила за сканиране, можете да конфигурирате следните опции:

Цели за сканиране – Ако искате да сканирате конкретна цел или група от цели, щракнете върху **Редактиране** до **Цели за сканиране** и изберете опция от структурата (дървовидна) на папките. Вижте Цели за сканиране за повече подробности.

Защита при поискване и с машинно самообучение – Можете да конфигурирате нивата на докладване и защита за всеки профил за сканиране. По подразбиране профилите за сканиране използват същата настройка, както е определена в Защита на файловата система в реално време. Дезактивирайте превключвателя до **Използване на настройките за защита в реално време**, за да конфигурирате персонализирани нива на отчитане и защита. Вижте Защити за подробно обяснение на нивата на докладване и защита.

ThreatSense – Опции за разширени настройки, като например разширения на файлове, които искате да контролирате, и използвани методи за откриване. Вижте ThreatSense за повече информация.

Профили за сканиране

Има 4 предварително зададени профили за сканиране в ESET Internet Security:

• **Smart сканиране**: това е профилът за разширено сканиране по подразбиране. Профилът за Smart сканиране използва технологията Smart оптимизация, която изключва файлове, за които е установено, че са чисти в предишно сканиране и не са променяни след това сканиране. Това допринася за по-ниски времена на сканиране с минимално въздействие върху защитата на системата.

• **Сканиране от контекстното меню**: можете да започнете сканиране при поискване на всеки файл от контекстното меню. Профилът за сканиране от контекстното меню ви позволява да зададете конфигурация за сканиране, която ще се използва, когато стартирате сканирането по този начин.

• **Задълбочено сканиране**: профилът за задълбочено сканиране не използва Smart оптимизация по подразбиране, така че няма файлове да бъдат изключени от сканиране при използването на този профил.

• **Сканиране на компютъра**: това е профилът по подразбиране, използван в стандартното сканиране на компютъра.

Предпочитаните параметри за сканиране могат да се запишат за бъдещо сканиране. Препоръчително е да създадете различен профил (с различни цели и методи за сканиране, както и с други параметри) за всяко сканиране, което се използва редовно.

За да създадете нов профил, отворете Разширени настройки > **Система за засичане** > **Сканирания за злонамерен софтуер** > **Сканиране при поискване** > **Списък с профили** > **Редактиране**. Прозорецът **Диспечер на профили** включва падащото меню **Избран профил**, което изброява съществуващите профили за сканиране, както и опция за създаване на нов профил. За да създадете профил за сканиране според вашите нужди, вижте ThreatSense за описание на всеки параметър от настройките за сканиране.

Да предположим, че искате да създадете собствен профил на сканиране и конфигурацията на **Сканиране на компютъра** донякъде е подходяща, но не искате да сканирате архиватори в реално време или потенциално опасни приложения, а освен това искате да приложите **Винаги отстранявай откриването**. Въведете името на новия профил в прозореца **Диспечер на профили** и щракнете върху **Добавяне**. Изберете новия профил от падащото меню **Избран профил** и задайте останалите параметри така, че да съответстват на изискванията ви, след което щракнете върху **OK**, за да запишете новия профил.

Цели за сканиране

Падащото меню **Цели за сканиране** позволява да изберете предварително зададени цели за сканиране.

• **Според настройките на профила** – Избиране на целите, указани от избрания профил за сканиране.
• **Преносим носител** – избор на дискети, USB устройства за съхранение, CD/DVD дискове.

• **Локални устройства** – избор на всички системни твърди дискове.

• **Мрежови устройства** – избор на всички свързани мрежови устройства.

• **Персонализиран избор** – Отказване на всички предишни селекции.

Структурата на папката (дървото) съдържа също така определени цели за сканиране.

• **Оперативна памет** – Сканиране на всички процеси и данни, които се използват в момента от оперативната памет.

• **Сектори за начално стартиране/UEFI** – Сканиране на секторите за начално стартиране и UEFI за наличието на злонамерен софтуер. Прочетете повече за UEFI скенера в речника.

• **WMI база данни** – сканира цялата Windows Management Instrumentation WMI база данни, всички пространства на имената, всички екземпляри на класа и всички свойства. Търсене на препратки към заразени файлове или злонамерен софтуер, вградени като данни.

• **Системен регистър** – Сканиране на целия системен регистър, всички ключове и подключове. Търсене на препратки към заразени файлове или злонамерен софтуер, вградени като данни. При почистване на откривания препратката остава в регистъра, за да се уверите, че няма да бъдат загубени важни данни.

За да се придвижите бързо до цел за сканиране (файл или папка), въведете пътя й в текстовото поле под дървовидната структура. Пътят е с различаване на малките и главните букви. За да включите целта в сканирането, поставете отметка в квадратчето й в дървовидната структура.

Сканиране в състояние на неактивност

Може да разрешите програмата за сканиране в състояние на неактивност в Разширени настройки > **Система за засичане на потенциално опасни заплахи** > **Сканирания за злонамерен софтуер** > **Сканиране в състояние на неактивност**.

Сканиране в състояние на неактивност

Включете плъзгача до **Разрешаване на сканирането в състояние на неактивност**, за да разрешите тази функция. Когато компютърът е в състояние на неактивност, се извършва тихо сканиране на компютъра на всички локални дискове.

По подразбиране сканирането в състояние на неактивност няма да се изпълни, когато компютърът (преносимият компютър) работи на батерия. Може да заместите тази настройка, като активирате плъзгача до **Изпълняване дори ако компютърът се захранва от батерията** в разширените настройки.

Включете превключвателя **Разрешаване на регистриране** в "Разширени настройки", за да

запишете резултата от сканирането на компютъра в раздела Регистрационни файлове (от главното меню на програмата щракнете върху **Инструменти** > **Регистрационни файлове** и изберете **Сканиране на компютъра** от падащото меню **Регистрационен файл**).

Откриване на състояние на неактивност при

Вижте Стартиране при откриване на състояние на неактивност за пълен списък с условията, които трябва да бъдат изпълнени, за да се стартира скенера в състояние на неактивност.

ThreatSense – Опции за разширени настройки, като например разширения на файлове, които искате да контролирате, и използвани методи за откриване. Вж. ThreatSense за повече информация.

Откриване на състояние на неактивност при

Настройките на откриването в състояние на неактивност могат да се конфигурират в Разширени настройки под **Система за засичане на потенциално опасни заплахи** > **Сканирания за злонамерен софтуер** > **Сканиране в състояние на неактивност** > **Откриване на състояние на неактивност**. Тези настройки стартират Сканирането в състояние на неактивност:

- **Изключен екран или скрийнсейвър**
- **Заключване на компютъра**
- **Излизане на потребител**

Използвайте превключвателите за всяко съответстващо състояние, за да разрешите или забраните различните видове стартиране при откриване в състояния на неактивност.

Начално сканиране

Автоматичната начална проверка на файловете по подразбиране ще се извършва при стартиране на системата и по време на обновяванията на системата за откриване. Това сканиране се извършва в съответствие със Задачите и конфигурацията на планировчика.

Опциите за начално сканиране са част от задачата **Проверка на файловете при стартиране на компютъра** на планировчика. За да промените съответните настройки, отидете в **Инструменти** > **Разписание**, щракнете върху **Автоматична проверка на файлове при стартиране**, след което изберете **Редактиране**. В последната стъпка ще се появи прозорецът Автоматична проверка на файлове при стартиране. За подробни инструкции как да създадете и управлявате задачите на планировчика, вижте Създаване на нови задачи.

ThreatSense – Опции за разширени настройки, като например разширения на файлове, които искате да контролирате, и използвани методи за откриване. Вж. ThreatSense за повече информация.

Автоматична проверка на файловете при стартиране

При създаване на задача на планировчика за проверка на файловете при стартиране на компютъра разполагате с няколко опции за регулиране на следните параметри:

Падащото меню **Цел за сканиране** указва дълбочината на сканиране на файловете, които се изпълняват при стартиране на системата, въз основа на таен сложен алгоритъм. Файловете са подредени в низходящ ред според следните критерии:

- **Всички регистрирани файлове** (най-много сканирани файлове)
- **Рядко използвани файлове**
- **Обикновено използвани файлове**
- **Често използвани файлове**
- **Само най-често използвани файлове** (най-малко сканирани файлове)

Включени са също така две специални групи:

- **Файлове, които се изпълняват преди влизането на потребителя** – Съдържа файлове от местоположения, които позволяват изпълнение на файловете, без потребителят да е влязъл (включва почти всички стартиращи местоположения като услуги, помощни обекти на браузъра, известяване чрез winlogon, записи на планировчика на прозорци, известни dll файлове и т.н.).
- **Файлове, които се изпълняват след влизането на потребителя** – Съдържа файлове от местоположения, които позволяват използване на файловете само след влизане на потребителя (включва файлове, които се изпълняват само за определен потребител, обикновено файлове в *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Списъците с файлове, които трябва да бъдат сканирани, са фиксирани за всяка група по-горе. Ако изберете по-ниска дълбочина на сканиране за файлове, които се изпълняват при стартиране на системата, тези, които не са били сканирани, ще бъдат при отваряне или изпълнение.

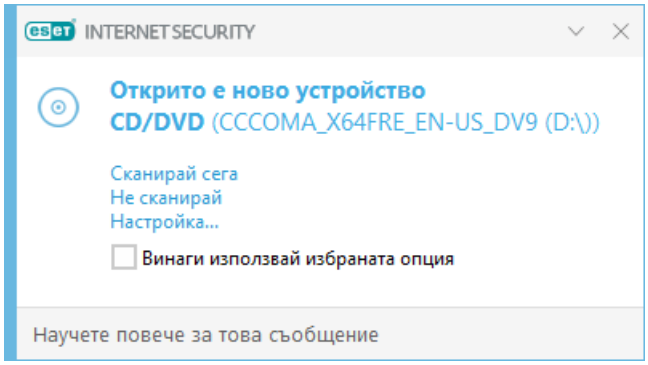
Приоритет на сканиране – нивото на приоритет, използвано за определяне кога ще започне дадено сканиране:

- **При неактивност** – задачата ще се изпълни само докато системата е в режим н а готовност;
- **Най-малък** – при възможно най-ниско натоварване на системата;
- **По-малък** – при ниско натоварване на системата;
- **Нормален** – при средно натоварване на системата.

Преносим носител

ESET Internet Security предоставя автоматично сканиране на преносими носители (CD/DVD/USB/...), когато бъдат включени в компютъра. Тази функция е подходяща, в случай че администраторът на компютъра желае да предотврати използването на преносими носители с нежелано съдържание от потребителите.

При поставяне на преносими носители и когато е зададено **Показване на опциите за сканиране** в Разширени настройки > **Система за засичане** > **Сканирания за злонамерен софтуер** > **Преносими носители**, ще се показва следният диалогов прозорец:



Опции за този диалогов прозорец:

- **Сканирай сега** – тази опция ще стартира сканиране на преносимия носител.
- **Не сканирай** – преносимият носител няма да се сканира.
- **Настройка** – отваряне на разширените настройки.
- **Винаги използвай избраната опция** – при избор на тази опция същото действие ще се извършва при следващите свързвания на преносим носител.

Освен това ESET Internet Security разполага с функция за управление на устройства, която ви позволява да определяте правила за използването на външни устройства на даден компютър. Повече подробности относно функцията за управление на устройства могат да бъдат намерени в раздела Управление на устройства.

За да осъществите достъп до настройките за сканиране на външни устройства, отворете Разширени настройки > **Система за засичане на потенциално опасни заплахи** > **Сканирания за злонамерен софтуер** > **Преносими носители**.

Действие, което да предприемете след поставяне на преносим носител – изберете действието по подразбиране, което ще се изпълни при поставяне на преносим носител в компютъра (CD/DVD/USB). Изберете желаното действие при поставянето на преносим носител в компютър:

- **Не сканирай** – няма да се извърши никакво действие и прозорецът **Открито е ново устройство** няма да се отвори.

• **Автоматично сканиране на устройства** – ще се извърши сканиране на поставеното преносимо устройство.

• **Показване на опциите за сканиране** – отваряне на раздела за настройка на **преносими носители**.

Защита на документи

Функцията за защита на документи сканира документи на Microsoft Office преди отварянето им, както и автоматично изтеглени файлове с Internet Explorer, като например Microsoft ActiveX елементи. Защитата на документите предоставя допълнителен защитен слой към защитата на файловата система в реално време и може да бъде забранена за подобряване на производителността на системи, които не обработват голям брой документи на Microsoft Office.

За да активирате защитата от ботнет мрежи, отворете Разширени настройки > **Система за засичане на потенциално опасни заплахи** > **Сканиране за злонамерен софтуер** > **Защита от ботнет мрежи** и щракнете върху плъзгача до **Разрешаване на защита от ботнет мрежи**.

ThreatSense – Опции за разширени настройки, като например разширения на файлове, които искате да контролирате, и използвани методи за откриване. Вж. ThreatSense за повече информация.

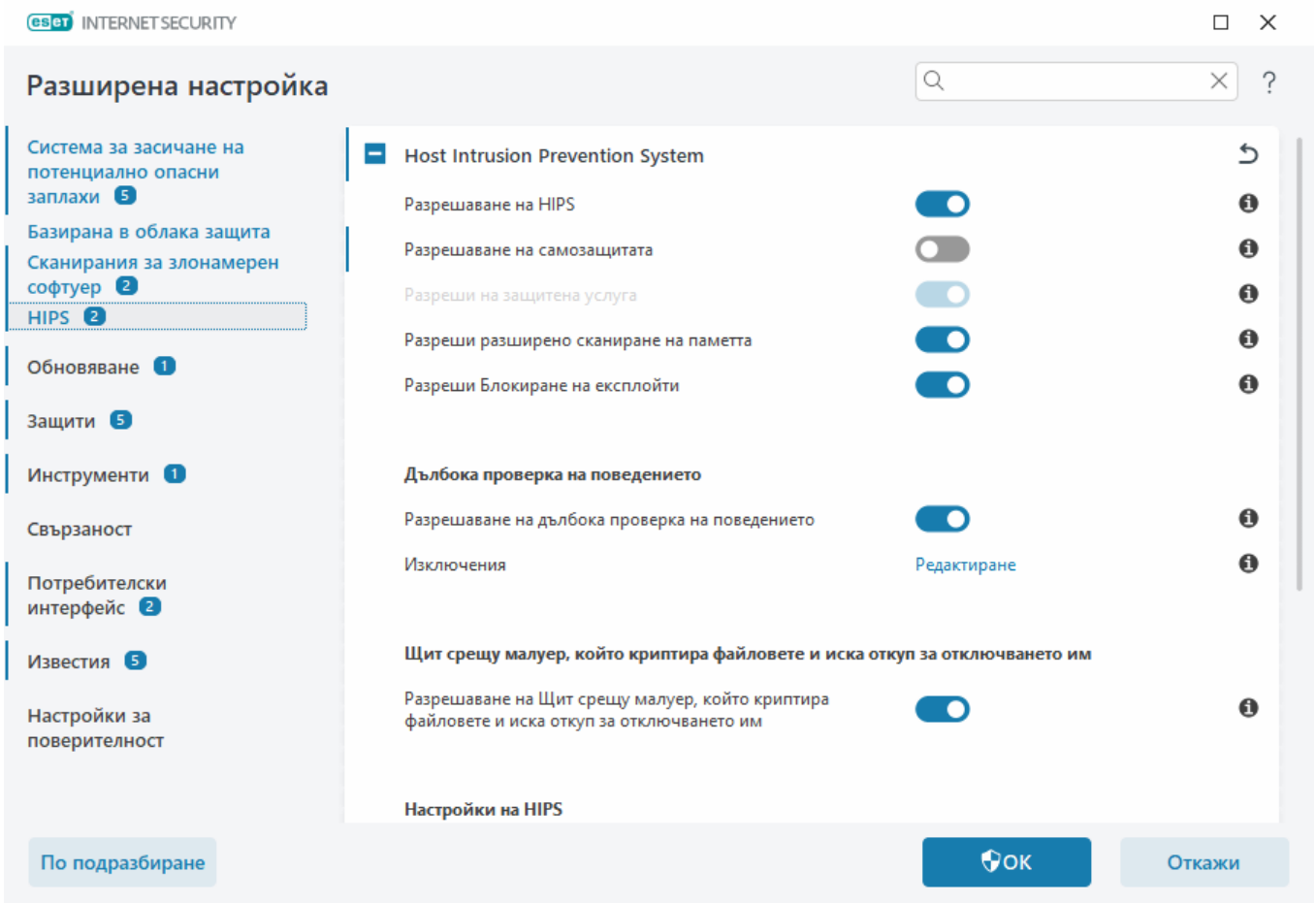
Тази функция се активира от приложения, които използват Microsoft Antivirus API (например Microsoft Office 2000 и по-нови версии или Microsoft Internet Explorer 5.0 и по-нови версии).

HIPS – Host Intrusion Prevention System

Промени в настройките на HIPS трябва да се извършват само от опитни потребители. Неправилна конфигурация на настройките на HIPS може да доведе до нестабилност на системата.

Базираната на **Host Intrusion Prevention System (HIPS)** предпазва системата от злонамерен код и нежелана активност, които се опитват да повлияят отрицателно върху компютъра. HIPS използва усъвършенстван анализ на поведението и възможност за откриване на мрежовия филтър, за да следи изпълняващите се процеси, файловете и ключовете в системния регистър. HIPS е система, отделна от защитата на файловата система в реално време, и не е защитна стена; тя само следи изпълняващите се в операционната система процеси.

Можете да конфигурирате настройките за HIPS в Разширени настройки > **Система за засичане** > **HIPS** > **Host Intrusion Prevention System**. Състоянието на HIPS (разрешено/забранено) се показва в главния прозорец на програмата ESET Internet Security > **Настройка** > **Защита на компютъра**.



Host Intrusion Prevention System

Разрешаване на HIPS – HIPS е разрешена по подразбиране в ESET Internet Security. Изключването на HIPS ще доведе до изключване на останалите функции на HIPS, като например „Блокиране на експлойти“.

Разрешаване на самозащитата – ESET Internet Security разполага с вградена технология **Самозащита**, като част от HIPS, която предотвратява повреждането или изключването на вашата защита от вируси и шпионски софтуер от страна на злонамерен софтуер. Самозащитата защитава от неупълномощен достъп важни процеси на системата и на ESET, ключове от системния регистър и файлове.

Разрешаване на защитената услуга – разрешава защитата за услугата на ESET (ekrn.exe). Ако е в разрешено състояние, услугата се стартира като защитен процес на Windows за защита срещу атаки от злонамерен софтуер.

Разрешаване на разширено сканиране на паметта – работи заедно с функцията за блокиране на експлойти за по-сигурна защита срещу злонамерен софтуер, който е създаден така, че да избегне откриването му от продукти срещу злонамерен софтуер чрез използване на умишлено объркване или шифроване. Разширеното сканиране на паметта е разрешено по подразбиране. Прочетете повече за този тип защита в речника.

Разрешаване на блокиране на експлойти – създадена за защита на често използвани типове приложения, като например уеб браузъри, програми за четене на PDF, имейл клиенти и компоненти на Microsoft Office. Блокирането на експлойти е разрешено по подразбиране. Прочетете повече за този тип защита в речника.

Дълбока проверка на поведението

Разрешаване на пълна проверка на поведението е друг слой защита, който работи като част от функцията HIPS. Това разширение на HIPS анализира поведението на всички изпълняващи се програми на компютъра и ви предупреждава, ако поведението на процеса е злонамерено.

HIPS изключенията от пълната проверка на поведението ви позволяват да изключвате процеси от анализа. За да се гарантира сканиране на всички процеси за потенциални заплахи, е препоръчително да създавате изключения само ако е абсолютно необходимо.

Щит срещу малуер, който криптира файловете и иска откуп за отключването им

Разрешаване на щит срещу малуер, който криптира файловете и иска откуп за отключването им – още един слой защита, който работи като част от функцията HIPS. Трябва да сте разрешили системата за репутация ESET LiveGrid®, за да може щитът срещу малуер, който криптира файловете и иска откуп за отключването им, да работи. Прочетете повече за този тип защита.

Разрешаване на Intel® Threat Detection Technology – помага за откриване на рансъмуер атаки чрез използване на уникална телеметрия на процесора Intel, за да се увеличи ефективността на откриването, да се намалят фалшивите положителни резултати и да се разшири видимостта за улавяне на усъвършенствани техники за укриване. Вижте поддържаните процесори.

Настройки на HIPS

Режим на филтриране може да се извърши в един от следните режими:

Режим на филтриране	Описание
Автоматичен режим	Операциите са разрешени, с изключение на тези, които са блокирани от предварително зададени правила, защитаващи системата.
Smart режим	Потребителят ще бъде уведомен само за много подозрителни събития.
Интерактивен режим	Потребителят ще получи подкана да потвърди операциите.
Базиран на правила режим	Блокира всички операции, които не са дефинирани от конкретно правило, което ги позволява.

Режим на филтриране	Описание
Обучаващ се режим	Операциите са разрешени и след всяка операция се създава правило. Правилата, създадени в този режим, могат да се прегледат в редактора **Правила на HIPS**, но техният приоритет е по-нисък от този на правилата, създадени ръчно или в автоматичен режим. Когато изберете **Режим на обучение** от падащото меню **Режим на филтриране**, настройката **Режимът на обучение ще се прекрати на** ще стане налична. Изберете времевия интервал, за който искате да активирате режима на обучение, като максималната продължителност е 14 дни. След изтичане на указания период ще бъдете подканени да редактирате правилата, създадени от HIPS по време на режима на обучение. Можете също така да изберете друг режим на филтриране или да отложите решението и да продължите да използвате режима на обучение.

Режимът е зададен след изтичане на обучаващия режим – изберете режима на филтриране, който ще бъде използван след изтичането на обучаващия режим. След изтичане опцията **Запитване към потребител** изисква административни привилегии, за да се осъществи промяна в режима на филтриране на HIPS.

Системата HIPS наблюдава събитията в операционната система и реагира в съответствие с правила, подобни на използваните от защитната стена. Щракнете върху **Редактиране** до **Правила**, за да отворите редактора на **Правила за HIPS**. В прозореца за правила за HIPS можете да избирате, добавяте, редактирате или премахвате правила. Повече подробности за създаването на правила и операциите на HIPS можете да намерите в Редактиране на HIPS правило.

HIPS изключения

Изключенията ви позволяват да изключвате процеси от пълната проверка на поведението на HIPS.

За да редактирате изключенията на HIPS, отворете Разширени настройки > **Система за засичане** > **HIPS** > **Host Intrusion Prevention System** > **Изключения** > **Редактиране**.

> Не се бъркайте с Изключени файлови разширения, Изключения за откриването, Изключения за производителността или Изключения на процесите.

За да изключите обект, щракнете върху **Добавяне** и въведете пътя към обекта или го изберете в дървовидната структура. Можете също така да редактирате или премахнете избрани записи.

Разширени настройки на HIPS

Следните опции са полезни при дебъгване и анализиране на поведението на дадено приложение:

Драйверите винаги имат разрешение да се зареждат – Избраните драйвери винаги имат разрешение да се зареждат независимо от конфигурирания режим на филтриране, освен ако

не са изрично блокирани от правило на потребителя.

Регистриране на всички блокирани операции – Всички блокирани операции ще бъдат записани в регистрационния файл на HIPS. Използвайте тази функция само при отстраняване на неизправности или при поискване от отдела за техническа поддръжка на ESET, тъй като тя може да генерира огромен регистрационен файл и да забави компютъра.

Уведомявай, когато настъпват промени в началните приложения – показва се известие на работния плот всеки път, когато някое приложение се добавя или премахва от стартирането на системата.

Драйверите винаги имат разрешение да се зареждат

Драйверите, показани в този списък, винаги ще имат разрешение да се зареждат независимо от режима на филтриране на HIPS, освен ако не са изрично блокирани от правило на потребителя.

Добавяне – добавяне на нов драйвер.

Редактиране – редактиране на избран драйвер.

Премахване – Премахва драйвер от списъка.

Нулиране – повторно зареждане на определен набор от системни драйвери.

Щракнете върху **Нулирай**, ако не искате да бъдат включени драйверите, които сте добавили ръчно. Това може да е полезно, ако сте добавили няколко драйвера и не можете да ги изтриете ръчно от списъка.

След инсталирането списъкът с драйвери е празен. ESET Internet Security попълва списъка автоматично с течение на времето.

Интерактивен прозорец на HIPS

Диалоговият прозорец за HIPS известия ви позволява да създадете правило, базирано на нови действия, открити от HIPS, и след това да дефинирате условията, при които да се разрешава или отказва това действие.

Правила, създадени от прозореца за известия, се считат за еквивалентни на правилата, създадени ръчно. Правило, създадено от прозореца за известия, може да не бъде толкова специфично, колкото правилото, което е активирало диалоговия прозорец. Това означава, че след създаване на правило в диалоговия прозорец, същата операция може да активира същия прозорец. За повече информация вижте Приоритет на правилата за HIPS.

Ако действието по подразбиране, зададено за правило, е **Питай всеки път**, ще се показва диалогов прозорец при всяко активиране на правилото. Може да изберете действие **Откажи** или **Позволи** за операцията. Ако не изберете действие в предоставеното време, ще се избере ново действие на базата на правилата.

Опцията **Запомни до излизане от приложението** задава използване на действието (**Разреши/Откажи**) до момента на промяна на правилата или режима на филтриране, обновяване на HIPS модула или рестартиране на системата. След изпълнение на някое от тези три действия временните правила ще се изтрият.

Опцията **Създай правило и го запомни за постоянно** ще създаде ново правило за HIPS, което по-късно може да бъде променено в раздела Управление на HIPS правилата (изискват се администраторски привилегии).

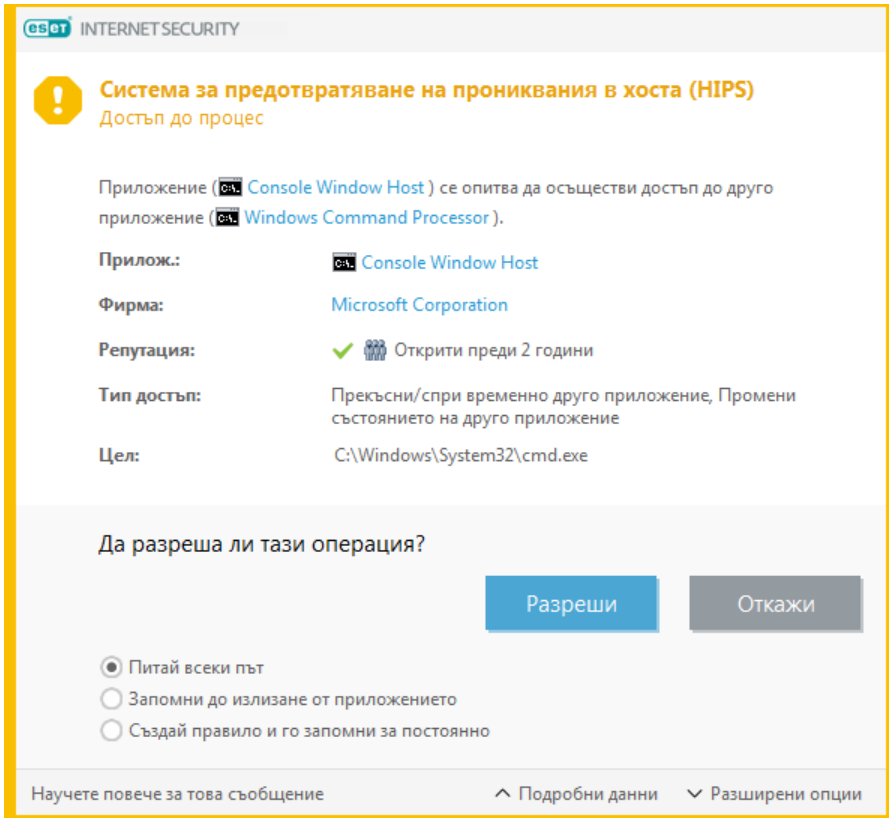
Щракнете върху **Подробности** в долната част, за да видите кое приложение активира операцията, каква е репутацията на файла или какъв тип операция сте подканени да позволите или откажете.

Може да получите достъп до настройки за по-подробните параметри на правилата, като щракнете върху **Разширени опции**. Опциите по-долу са достъпни, ако изберете **Създай правило и го запомни за постоянно**:

- **Създай правило, валидно само за това приложение** – ако премахнете отметката от това поле, правилото ще бъде създадено за всички изходни приложения.
- **Само за операция** – изберете файл/приложение/операция(и) от регистъра за правилото. Вижте описания за всички операции на HIPS.
- **Само за цел** – изберете файл/приложение/цел(и) в регистъра.

Безброй известия на HIPS?

За да прекратите появяването на известията, променете режима на филтриране на **Автоматичен** в Разширени настройки > **Система за засичане** > **HIPS** > **Host Intrusion Prevention System**.



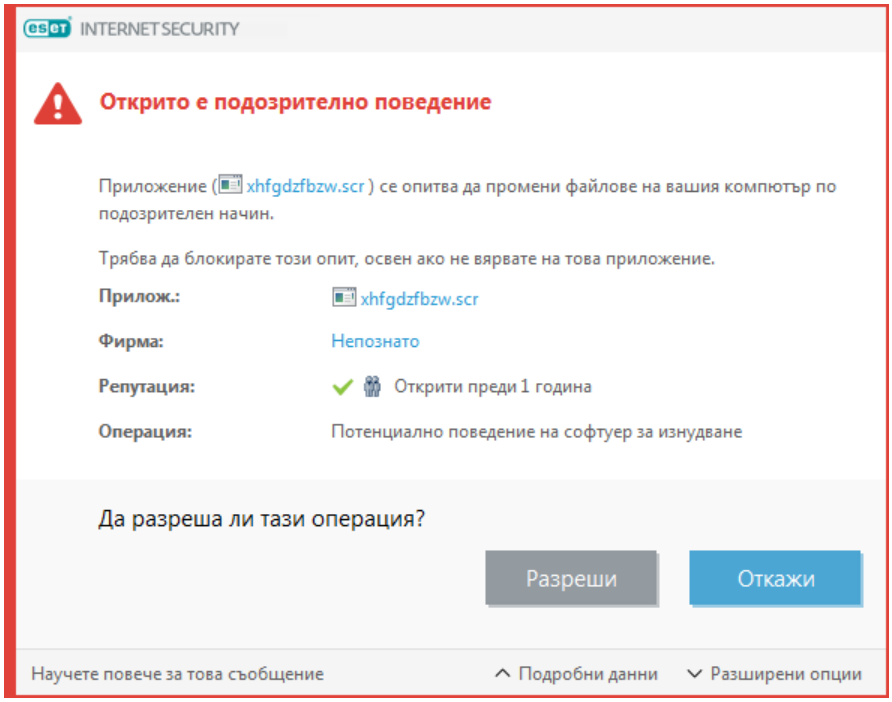
Обучаващият режим приключи

Обучаващият режим създава и записва правила автоматично. Можете да проверите всички създадени правила в Настройките на правило за HIPS. Този режим се използва най-добре за първоначалната конфигурация на HIPS, но трябва да се поддържа само за кратко време. Не се изисква намеса на потребителя, тъй като ESET Internet Security записва правилата според предварително зададени параметри. Превключете на **интерактивен** или **базиран на правила режим**, след като са създадени всички правила за необходимите процеси, изпълнявани в рамките на операционната система, за да избегнете рискове за защитата.

Можете да отложите това решение, ако не искате да променяте настройките.

Открито е потенциално поведение на софтуер за изнудване

Този интерактивен прозорец ще се отвори, ако бъде открито потенциално поведение на софтуер за изнудване. Може да изберете действие **Откажи** или **Позволи** за операцията.



Щракнете върху **Подробности** , за да прегледате конкретните параметри за откриване. Диалоговият прозорец ви позволява да извършите **Изпращане за анализ** или **Изключване от откриване**.

Трябва да сте разрешили ESET LiveGrid®, за да може защитата от малуер, който криптира файловете и иска откуп за отключването им, да функционира правилно.

Управление на HIPS правилото

Списък с определени от потребителя и добавени автоматично правила от системата HIPS. Повече информация относно създаването на правила и операциите на HIPS можете да намерите в Настройки на правила за HIPS. Вижте също Основен принцип на HIPS.

Колони

Правило – зададено от потребителя или автоматично избрано име на правило.

Разрешено – Изключете плъзгача, ако искате да запазите правилото в списъка, но без да го използвате.

Действие – правилото указва действие (**Разреши**, **Блокирай** или **Питай**), което трябва да бъде извършено при правилните условия.

Източници – правилото ще се използва само ако събитието се активира от приложение(я).

Цели – правилото ще се използва само ако операцията е свързана с определен файл, приложение или запис в системния регистър.

Детайлност на регистрирането – ако активирате тази опция, информация за правилото ще се записва в дневника на HIPS.

Известяване – ако е активирано събитие, в долния десен ъгъл се появява малък прозорец за известие.

Контролни елементи

Добавяне – създаване на ново правило.

Редактиране – позволява да редактирате избраните записи.

Премахване – премахва избрани записи.

Приоритет на правилата за HIPS

Няма опции за регулиране на нивото на приоритет на правилата за HIPS чрез бутони за преместване нагоре/надолу (също като за Правила за защитната стена, където правилата се изпълняват отгоре надолу).

- Всички правила, които създадете, имат един и същ приоритет
- Колкото по-конкретно е правилото, толкова по-висок е приоритетът (например правилото за определено приложение има по-голям приоритет отколкото правилото за всички приложения)
- HIPS разполага с вградени правила с по-висок приоритет, до които нямате достъп (например не можете да отмените правилата за самозащита)
- Правило, създадено от вас, което може да блокира операционната система, няма да

бъде приложено (ще има най-нисък приоритет)

Редактиране на HIPS правило

Първо вижте управлението на HIPS правилата.

Име на правило – зададено от потребителя или автоматично избрано име на правило.

Действие – указва действието (**Разреши**, **Блокирай** или **Питай**), което трябва да бъде извършено, ако условията са изпълнени.

Повлияващи операции – трябва да изберете типа операции, за който ще се прилага правилото. Правилото ще се използва само за този тип операции и за избраната цел.

Разрешено – Деактивирайте плъзгача, ако искате да запазите правилото в списъка, но без да го прилагате.

Детайлност на регистрирането – ако активирате тази опция, информация за правилото ще се записва в дневника на HIPS.

Извести потребителя – ако е възникнало събитие, в долния десен ъгъл се появява малък прозорец за известие.

Правилото се състои от части, които описват условията, активиращи това правило:

Изходни приложения – правилото ще се използва само ако събитието се активира от тези приложения. Изберете **Определени приложения** от падащото меню и щракнете върху **Добавяне**, за да добавите нови файлове или изберете **Всички приложения** от падащото меню, за да добавите всички приложения.

Целеви файлове – правилото ще се използва само ако операцията е свързана с тази цел. Изберете **Определени файлове** от падащото меню и щракнете върху **Добавяне**, за да добавите нови файлове или папки, или изберете **Всички файлове** от падащото меню, за да добавите всички файлове.

Приложения – правилото ще се използва само ако операцията е свързана с тази цел. Изберете **Определени приложения** от падащото меню и щракнете върху **Добавяне**, за да добавите нови файлове или папки, или изберете **Всички приложения** от падащото меню, за да добавите всички приложения.

Записи в регистър – правилото ще се използва само ако операцията е свързана с тази цел. Изберете **Определени записи** от падащото меню и щракнете върху **Добавяне**, за да го въведете ръчно, или щракнете върху **Отваряне на редактора на системния регистър**, за да изберете ключ от системния регистър. Освен това може да изберете **Всички записи** от падащото меню, за да добавите всички приложения.

> Някои операции за специфични правила, определени предварително от HIPS, не може да бъдат блокирани и са разрешени по подразбиране. Освен това не всички системни операции се наблюдават от HIPS. HIPS наблюдава операциите, които могат да се сметнат за опасни.

Описания на важни операции:

Операции с файлове

• **Изтриване на файл** – приложението иска разрешение да изтрие целевия файл.

• **Запис във файл** – приложението иска разрешение да запише в целевия файл.

• **Директен достъп до диска** – Приложението се опитва да чете от или да записва на диска по нестандартен начин, който ще заобиколи познатите процедури на Windows. Това може да доведе до промяна на файлове без прилагане на съответните правила. Тази операция може да е предизвикана от злонамерен софтуер, опитващ се да избегне откриването, архивиращ софтуер, който се опитва да направи точно копие на диска, или диспечер на дялове, който се опитва да реорганизира томовете на диска.

• **Инсталирай глобален фиксатор** – отнася се до извикването на функцията SetWindowsHookEx от библиотеката MSDN.

• **Зареждане на драйвер** – инсталиране и зареждане на драйвери в системата.

Операции с приложения

• **Дебъгване на друго приложение** – прикрепване на инструмент за дебъгване към процеса. Докато се дебъгва дадено приложение, много подробности за поведението му могат да се видят и променят, а данните му могат да се отворят.

• **Прихвани събития от друго приложение** – изходното приложение се опитва да хване събития, насочени към определено приложение (например програма, регистрираща въведени символи, която се опитва да запише събития от браузъра).

• **Прекъсни/спри временно друго приложение** – временно спиране, възстановяване или прекратяване на процес (има директен достъп от Process Explorer или от екрана с процеси).

• **Стартирай ново приложение** – стартиране на нови приложения или процеси.

• **Промени състоянието на друго приложение** – изходното приложение се опитва да записва в паметта на целевите приложения или да стартира код от негово име. Тази функция може да бъде полезна за защитата на основно приложение чрез конфигурирането му като целево приложение в правило, блокиращо използването на тази операция.

Операции със системния регистър

• **Промяна на настройките за стартиране** – Всички промени в настройките, които определят кои приложения ще се изпълнят при стартирането на Windows. Те могат да се открият например чрез търсене на ключа Run в системния регистър на Windows.

• **Изтрий от системния регистър** – изтриване на ключ в системния регистър или на негова стойност.

• **Преименувай ключа в системния регистър** – преименуване на ключове в системния регистър.

• **Промени системния регистър** – създават се нови стойности на ключове в системния регистър, местят се данни в дървовидната структура на базата данни или се настройват права за ключовете в системния регистър за даден потребител или група.

При въвеждане на цел можете да използвате заместващи символи с определени ограничения. Вместо отделен ключ може да се използва знакът * (звездичка) в пътищата на регистъра. Например *HKEY_USERS*\software HKEY_USER\.default\software*, но не и *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*.
*HKEY_LOCAL_MACHINE\system\ControlSet** не е валиден път към ключ от системния регистър. Път на ключ в системния регистър, който съдържа *, определя "този път или всяко едно ниво след този символ". Това е единственият начин за използване на заместващи символи за целеви файлове. Първо ще бъде оценена отделна част от пътя, след което и пътят, който е след заместващия символ (*).

Ако създадете много общо правило, ще бъде показано предупреждение за този тип правила.

В следващия пример ще демонстрираме как да ограничите нежеланото поведение на определено приложение:

1. Назовете правилото и изберете **Блокирай** (или **Попитай**, ако предпочитате да направите избор по-късно) от падащото меню **Действие**.

2. Активирайте плъзгача до **Известяване на потребителя** за показване на известие при всяко прилагане на правило.

3. Изберете поне една операция в раздела **Повлияващи операции**, за която правилото ще бъде приложено.

4. Щракнете върху **Напред**.

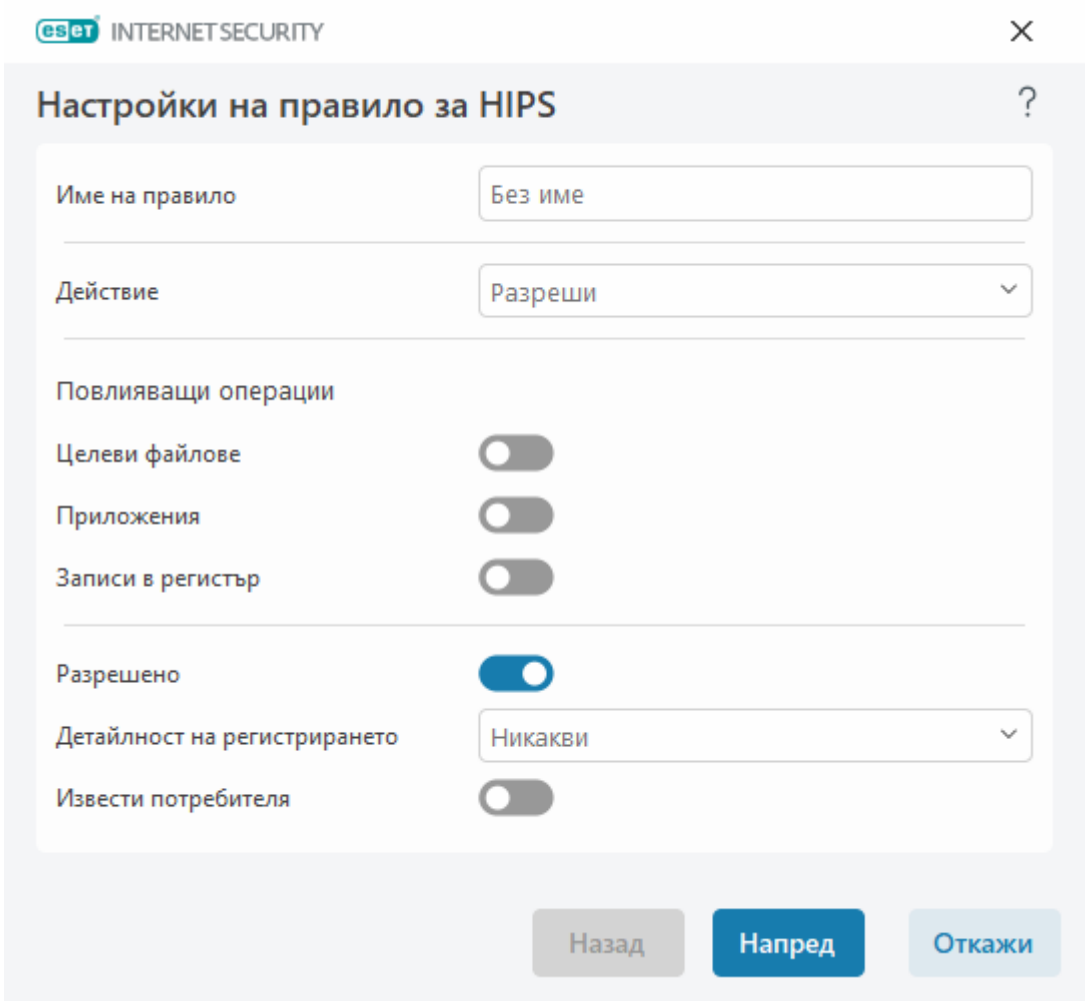
5. В прозореца **Изходни приложения** изберете **Определени приложения** от падащото меню, за да приложите новото правило за всички приложения, които се опитат да извършат някоя от избраните операции с указаните от вас приложения.

6. Щракнете върху **Добавяне**, след което върху **...**, за да изберете път до определено приложение и натиснете **OK**. Добавете повече приложения, ако желаете.
Например: *C:\Program Files (x86)\Untrusted application\application.exe*

7. Изберете операцията **Запис във файл**.

8. Изберете **Всички файлове** от падащото меню. Това ще блокира всякакви опити за запис във всички файлове от избраното приложение(я) от предишната стъпка.

9. Щракнете върху **Готово**, за да запишете новото правило.



Добавяне на път на приложение/регистър за HIPS

Изберете път към даден файл на приложение, като щракнете върху опцията **...** Докато избирате дадена папка, ще бъдат включени всички приложения в това местоположение.

Опцията **Отваряне на редактора на системния регистър** ще стартира редактора на системния регистър на Windows (regedit). Докато добавяте път към даден регистър, въведете правилното местоположение в полето **Стойност**.

Примери за път към файл или регистър:

- *C:\Program Files\Internet Explorer\iexplore.exe*
- *HKEY_LOCAL_MACHINE\system\ControlSet*

Обновяване

Опциите за настройка на актуализацията са налични в Разширени настройки > **Обновяване**. Този раздел указва информацията за източника на обновяване, като например използваните сървъри за обновяване и данните за удостоверяване в тях.

Обновяване

Профилът за обновяване, който се използва в момента, се показва в падащото меню **Избор на профил за обновяване по подразбиране**.

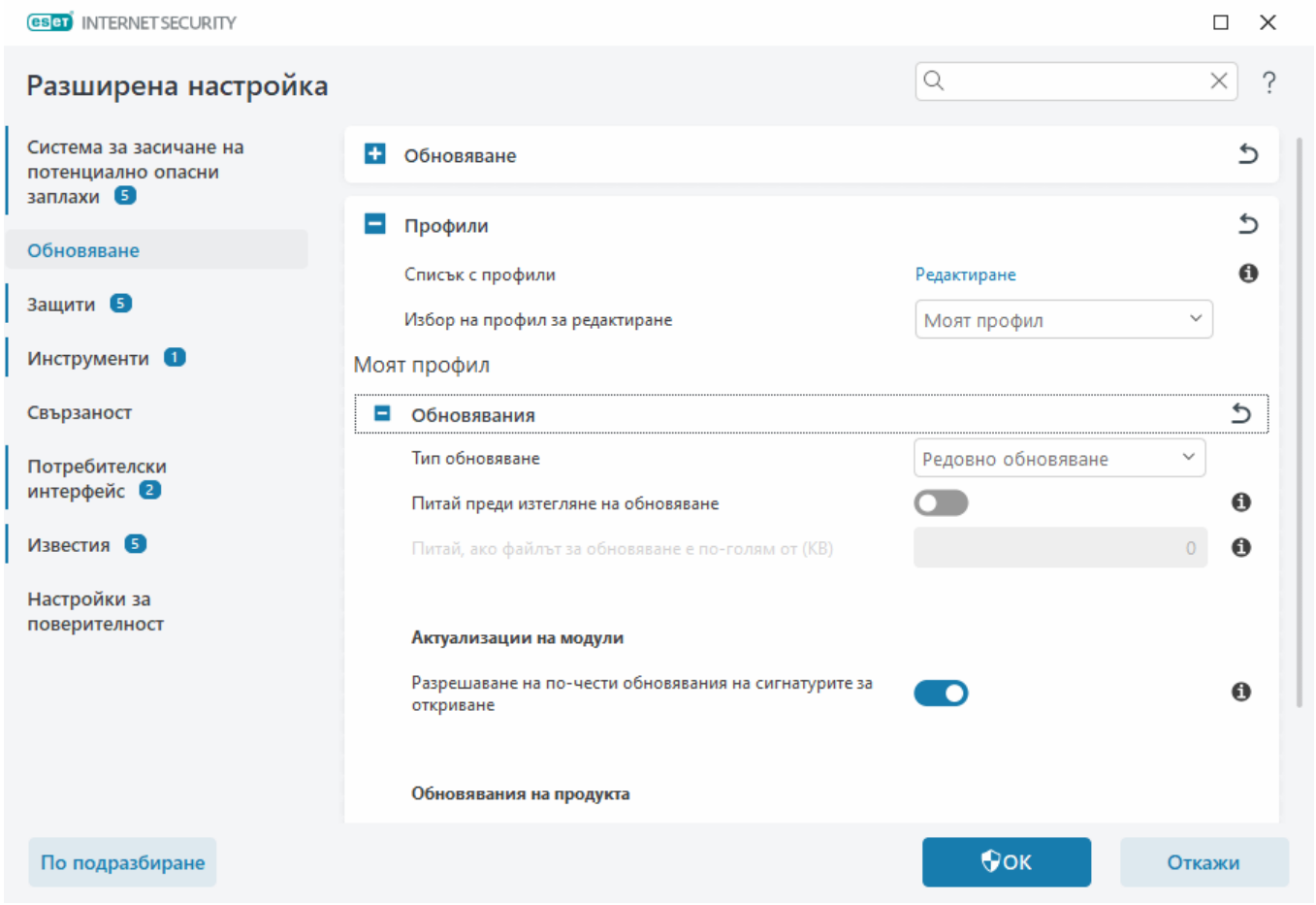
За да създадете нов профил, вижте раздел Профили за обновяване.

Автоматично превключване на профили – Позволява ви да присвоите профил за актуализация на конкретен профил за мрежова връзка.

Ако изпитвате затруднения с изтеглянето на система за засичане или актуализации на модула, щракнете върху **Изчистване** до **Изчистване на кеша за обновяване** за изчистване на временните файлове за обновяване/кеша.

Връщане към предишен модул

Ако имате съмнение, че някое ново обновяване на системата за засичане на потенциално опасни заплахи и/или програмни модули може да са нестабилни или повредени, може да върнете обратно към предишната версия и да забраните обновяванията за определен период от време.



За да се изтеглят правилно обновяванията, е важно да попълните правилно всички параметри за обновяване. Ако използвате защитна стена, уверете се, че програмата на ESET разполага с разрешение да комуникира с интернет (например HTTP комуникация).

Профили

Профилите за обновяване могат да се създават за различни конфигурации и задачи за обновяване. Създаването на профили за обновяване е особено полезно за мобилни потребители, които се нуждаят от алтернативен профил за свойства на интернет връзката, които редовно биват променяни.

Падащото меню **Избор на профил за редактиране** показва избрания в момента профил и е зададено на **Моят профил** по подразбиране. За да създадете нов профил, щракнете върху **Редактиране** до **Списък с профили**, въведете собствено **Име на профил**, след което щракнете върху **Добавяне**.

Обновявания

По подразбиране опцията **Тип обновяване** е зададена на **Редовно обновяване**, за да се гарантира, че файловете за обновяване ще се изтеглят автоматично от сървъра на ESET с минимален мрежов трафик. Тестовият режим (опцията **Тестов режим**) представлява обновявания, които са преминали щателно вътрешно тестване и скоро ще бъдат общодостъпни. Можете да се възползвате от разрешаването на тестовия режим, като получите достъп до най-новите кръпки и методи на откриване. Тестовият режим обаче може не винаги да е достатъчно стабилен и НЕ БИВА да се използва на производствени сървъри и работни станции, за които се изисква максимална достъпност и стабилност.

Питай преди изтегляне на обновяване – Програмата ще покаже известие, в което можете да изберете да потвърдите или откажете изтегляния на файлове за обновяване.

Питай, ако размерът на файла за обновяване е по-голям от (КБ) – програмата ще покаже диалогов прозорец за потвърждение, ако размерът на файла за обновяване е по-голям от посочената стойност. Ако размерът на файла за обновяване е настроен на 0 КБ, програмата във всеки случай ще покаже диалогов прозорец за потвърждение.

Обновявания на модули

Разрешаване на по-чести обновявания на подписи за откриване – Подписите за откриване ще се обновяват на по-кратък интервал. Забраняването на тази настройка може да окаже негативно влияние върху скоростта на откриване.

Обновявания на продукта

Обновявания на функциите на приложението – Автоматично инсталиране на нови версии на ESET Internet Security.

Опции за свързване

За да използвате прокси сървър за изтегляне на обновявания, вижте раздела Опции за свързване.

Връщане към предишното обновяване

Ако имате съмнение, че някое ново обновяване на система за засичане на потенциално опасни заплахи или програмни модули може да е нестабилно или повредено, може да върнете до предишната версия и да забраните временно обновяванията. Можете също така да разрешите обновявания, които са били забранени преди това, ако сте ги отложили за неопределено време.

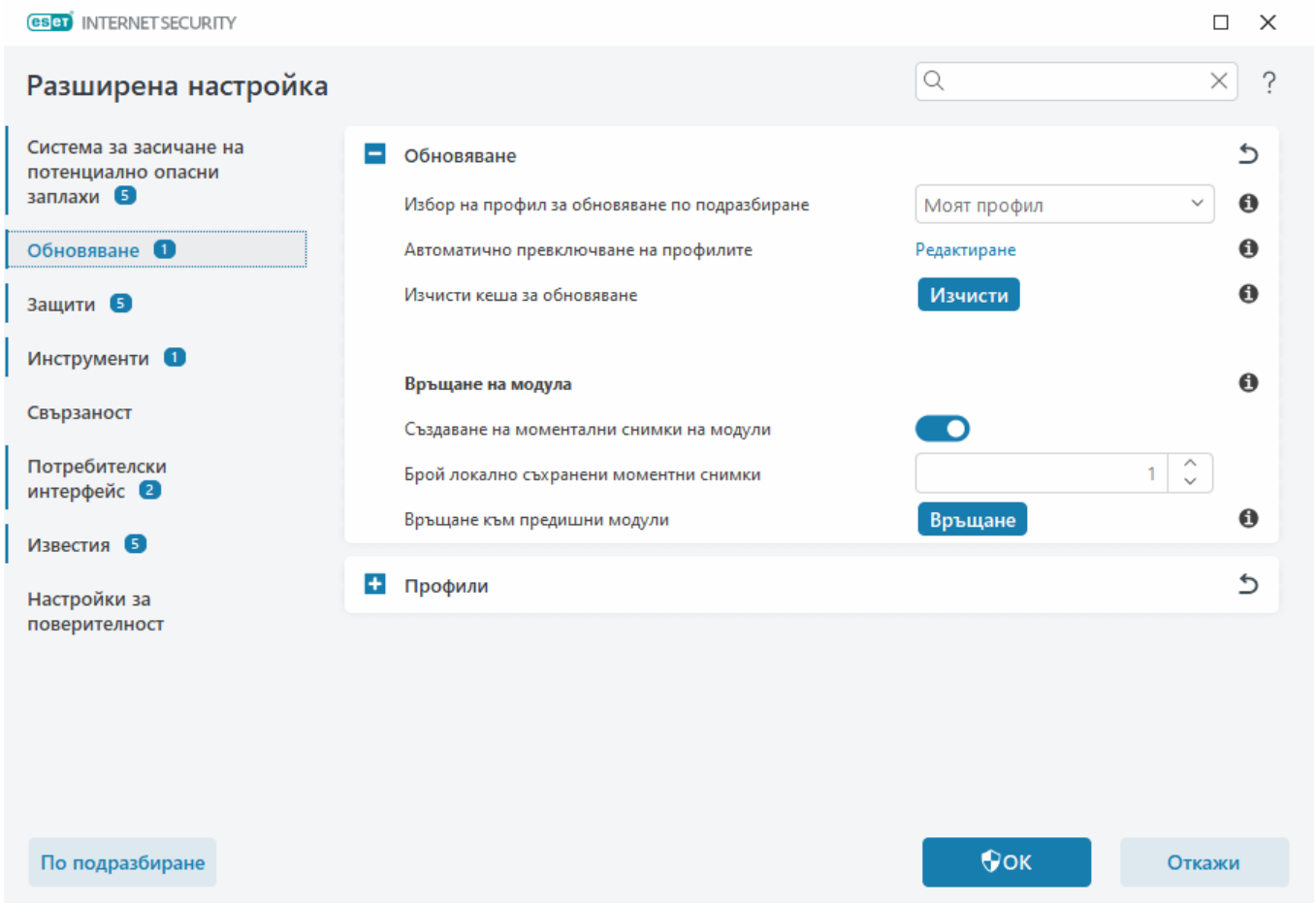
ESET Internet Security записва моментни снимки на системата за засичане на потенциално опасни заплахи и програмните модули за използване с функцията за връщане. За да създадете моментни снимки на базата данни за вируси, оставете разрешено **Създаване на моментални снимки на модули**. Когато **Създаване на моментални снимки на модули** е разрешено, първата моментна снимка се създава по време на първото обновяване. Следващата се създава след 48 часа. Полето **Брой локално съхранени моментни снимки** определя броя на съхранените моментни снимки на системата за засичане на потенциално опасни заплахи.

> Когато се достигне максималният брой моментни снимки (например три), най-старата моментна снимка се заменя с нова моментна снимка на всеки 48 часа. ESET Internet Security връща версиите на обновяването на системата за засичане на потенциално опасни заплахи и програмните модули до най-старата моментна снимка.

Ако щракнете върху **Връщане** в Разширени настройки > **Обновяване** > **Обновяване**), трябва да изберете времеви интервал от падащото меню **Времетраене**, който представлява периодът от време, през който актуализациите на системата за засичане и на програмните модули ще бъде паузирано.

Изберете **До отмяна**, за да отложите за неопределено време редовните обновявания, докато не възстановите ръчно функцията за обновяване. Тъй като представлява възможна опасност за защитата, ESET не препоръчва избора на тази опция.

Ако се извърши връщане, бутонът **Връщане** се променя на **Разрешаване на обновяванията**. За периода от време, избран от падащото меню **Временно спиране на обновяванията**, няма да се позволяват никакви обновявания. Версията на системата за засичане на потенциално опасни заплахи се връща до най-старата налична версия и се съхранява като моментна снимка във файловата система на локалния компютър.



Нека номер 22700 да бъде най-новата версия на системата за засичане на потенциално опасни заплахи, а 22698 и 22696 са съхранени като моментни снимки на системата за засичане на потенциално опасни заплахи. Обърнете внимание, че 22697 не е налична. В този пример компютърът е бил изключен по време на обновяването с 22697 и по-нова версия е станала налична преди изтеглянето на 22697. Ако в полето **Брой локално съхранени моментни снимки** е въведено „две“ и щракнете върху **Връщане**, системата за засичане на потенциално опасни заплахи (включително програмните модули) се възстановява до версия номер 22696. Процесът може да отнеме известно време. Проверете дали версията на системата за засичане на потенциално опасни заплахи се е върнала до предишна версия от екрана Обновяване.

Времеви интервал за връщане

Ако щракнете върху **Връщане** в Разширени настройки > **Обновяване** > **Обновяване**), трябва да изберете времеви интервал от падащото меню **Времетраене**, който представлява периодът от време, през който актуализациите на системата за засичане и на програмните модули ще бъде паузирано.

Изберете **До отмяна**, за да отложите за неопределено време редовните обновявания, докато не възстановите ръчно функцията за обновяване. Тъй като представлява възможна опасност за защитата, ESET не препоръчва избора на тази опция.

Обновявания на продукта

Разделът **Обновявания на продукта** ви позволява да инсталирате автоматично обновявания с нови функции, когато са налични.

Обновяванията на функциите на приложението носят нови функции или променят тези, които вече съществуват от предишни версии. Те може да се изпълняват автоматично без намеса на потребителя или може да изберете да получавате известие. След инсталирането на обновяване на функция на приложение може да се наложи рестартиране на компютъра.

Обновявания на функциите на приложението – Когато е разрешено, обновяванията на функциите на приложението ще се извършват автоматично.

Опции за свързване

За достъп до опциите за настройка на прокси сървъра за конкретен профил за обновяване, отворете Разширени настройки > **Обновяване** > **Профили** > **Обновявания** > **Опции за свързване**. Щракнете върху падащото меню **Режим на прокси сървър** и изберете една от следните три опции:

- Без използване на прокси сървър
- Свързване през прокси сървъра
- Използване на глобалните настройки за прокси сървър

Изберете **Използване на глобалните настройки за прокси сървър**, за да използвате конфигурацията на прокси сървъра, вече посочена в Разширени настройки > **Свързаност** > **Прокси сървър**.

Изберете опцията **Не използвай прокси сървър**, за да укажете, че няма да се използва прокси сървър за обновяване на ESET Internet Security.

Опцията **Свързване през прокси сървър** трябва да се избере, ако:

• Прокси сървър, различен от дефинирания в Разширени настройки > **Свързаност**, се използва за обновяване на ESET Internet Security. В тази конфигурация информацията за новия прокси сървър трябва да бъде посочена под адреса на **Прокси сървър**, **Порт** за комуникация (3128 по подразбиране) и **Потребителско име** и **Парола** за прокси сървъра, ако се изискват.

• Настройките на прокси сървъра не се задават глобално, но ESET Internet Security ще се свърже с прокси сървър за обновяване.

• Компютърът е свързан с интернет през прокси сървър. Настройките се взимат от Internet Explorer по време на инсталирането на програмата, но ако бъдат променени (напр. ако промените вашия интернет доставчик), проверете дали настройките на прокси сървъра в този прозорец са правилни. В противен случай програмата няма да може да се свърже със сървъри за обновяване.

Настройката по подразбиране за прокси сървъра е **Използвай глобалните настройки за прокси сървър**.

Използвай директна връзка, ако не е наличен прокси сървър – Прокси сървърът ще бъде прескочен по време на обновяване, ако не е достъпен.

Полетата **Потребителско име** и **Парола** в този раздел са специфични за прокси сървъра. Попълнете тези полета само ако се изискват потребителско име и парола за достъп до прокси сървъра. Тези полета трябва да се попълнят само ако знаете, че ви е необходима парола за достъп до интернет през прокси сървър.

Защити

Защитите предпазват срещу атаки на злонамерени системи, като контролират файловете и комуникацията по имейл и интернет. Например отстраняване на проблеми ще стартира, ако бъде засечен обект, класифициран като злонамерен софтуер. Защитите могат да го елиминират, като го блокират, а след това го почистят, изтрият или преместят под карантина.

За да конфигурирате защитите в детайли, отворете Разширени настройки > **Защити**.

Промени в „Защити“ трябва да се извършват само от опитни потребители. Неправилна конфигурация на настройките може да доведе до намалено ниво на защита.

В този раздел:

- Отговори на откриването
- Настройка на докладването
- Настройка на защитата

Отговори на откриването

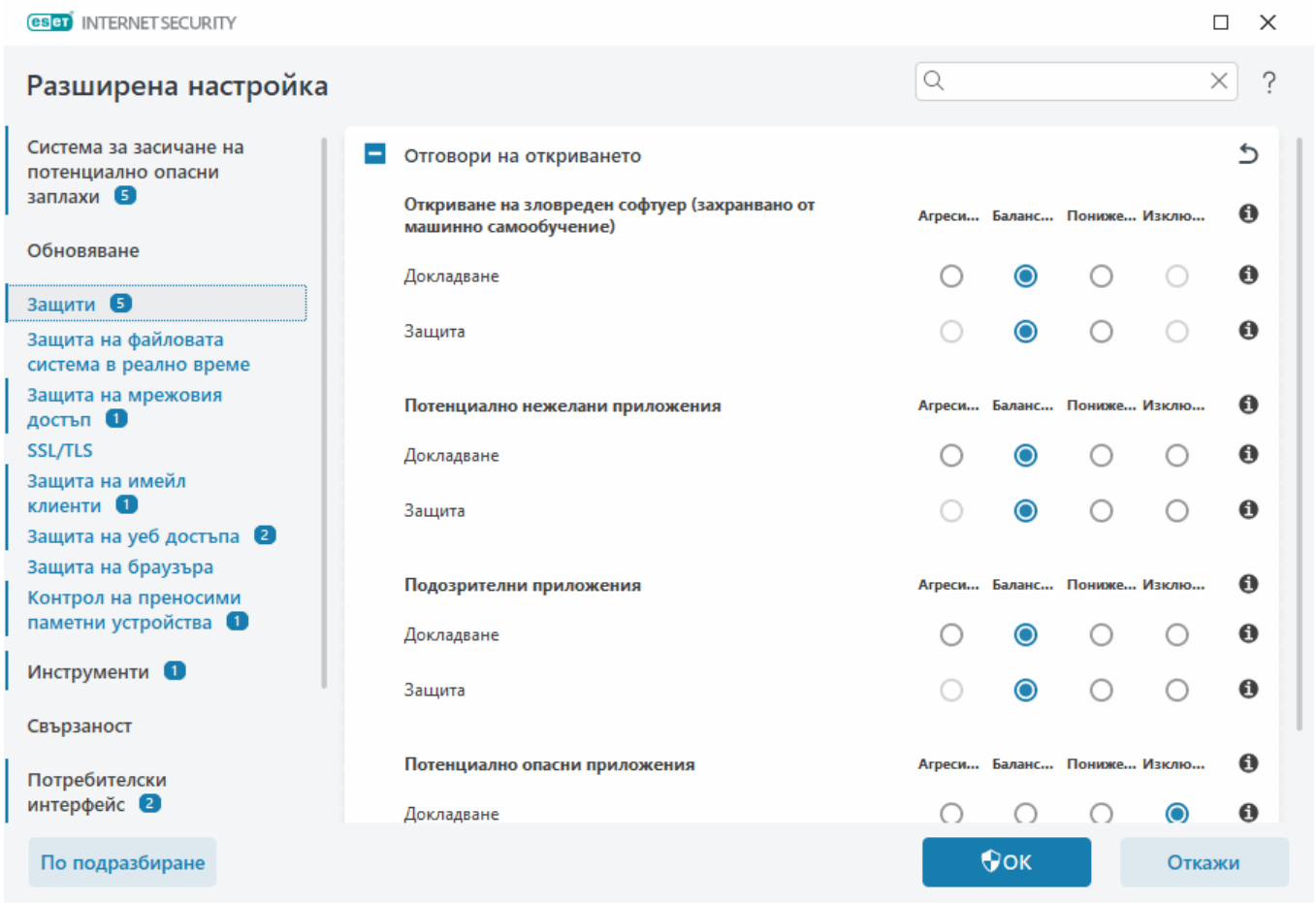
Отговорите на откриването ви позволяват да конфигурирате нивата на отчитане и защита за следните категории:

- **Откриване на зловреден софтуер (захранвано от машинно самообучение)** – Компютърният вирус представлява злонамерен код, прикрепен към съществуващи файлове на компютъра. Терминът „вирус“ обаче често се използва погрешно. „Злонамерен софтуер“ е по-точен термин. Откриването на злонамерен софтуер се извършва от модула на системата за засичане на потенциално опасни заплахи, съчетан с компонента за машинно обучение. Прочетете повече за тези типове приложения в речника.

- **Потенциално нежелани приложения** – грейуер или потенциално нежелани приложения (ПНП) е многообхватна категория софтуер, чието намерение не е толкова крайно злонамерено като на друг тип злонамерен софтуер, като например вируси или троянски коне. Въпреки това може да инсталира допълнителен нежелан софтуер, да промени поведението на цифровото устройство или да извърши действия, които не са одобрени или очаквани от потребителя. Прочетете повече за тези типове приложения в речника.

- **Подозрителните приложения включват програми**, компресирани с архиватори или протектори. Тези протектори често се използват от авторите на злонамерен софтуер с цел избягване на засичането.

- **Потенциално опасни приложения** – отнася се за легитимен търговски софтуер, който може потенциално да се използва за злонамерени цели. Потенциално опасни приложения (ПОП) са например инструменти за отдалечен достъп, приложения за разбиване на пароли и програми за регистриране на натиснатите клавиши (програми, които записват всяко натискане от потребителя на клавишите на клавиатурата). Прочетете повече за тези типове приложения в речника.



Подобрена защита

Разширеното машинно самообучение вече е част от защитите като разширен слой защита, който подобрява откриването на базата на машинно обучение. Прочетете повече за този тип защита в речника.

Настройка на докладването

Когато настъпи откриване (напр. заплаха е открита и класифицирана като злонамерен софтуер), информацията се записва в дневника с откривания, а известия на работния плот се появяват, ако са конфигурирани в ESET Internet Security.

Прагът на докладване е конфигуриран за всяка категория (наричан „КАТЕГОРИЯ“):

1. Откривания на злонамерен софтуер
2. Потенциално нежелани приложения
3. Потенциално опасни приложения
4. Подозрителни приложения

Докладване, извършено със системата за засичане на потенциално опасни заплахи, включително компонента за машинно обучение. Може да зададете по-висок праг на докладване от текущия праг на защита. Тези настройки за докладване не влияят на блокирането, почистването или изтриването на обекти.

Прочетете следната информация, преди да модифицирате праг (или ниво) за докладване на КАТЕГОРИЯ:

Праг	Обяснение
Агресивен	Докладването на КАТЕГОРИЯ е конфигурирано на максимална чувствителност. Докладват се повече откривания. **Агресивната** настройка може погрешно да идентифицира обекти като КАТЕГОРИЯ.
Балансиран	Докладването на КАТЕГОРИЯ е конфигурирано като балансирано. Тази настройка е оптимизирана за балансиране на производителността и точността на честотата на откриване и броя на погрешно докладваните обекти.
Понижен	Докладването на КАТЕГОРИЯ е конфигурирано да свежда до минимум погрешно идентифицираните обекти, като запазва достатъчно ниво на защита. Обектите се докладват само когато вероятността е очевидна и съвпада с поведението на КАТЕГОРИЯ.
Изключено	Докладването на КАТЕГОРИЯ не е активно, а откриванията от този тип не се откриват, докладват или почистват. В резултат на това тази настройка забранява защитата от този тип откриване. Изключването на докладването не е налично за докладване на злонамерен софтуер, но е стойността по подразбиране за потенциално опасни приложения.

Наличност на модули за защита на ESET Internet Security

Наличността (разрешено или забранено) на модул за защита за избран праг за КАТЕГОРИЯ е както следва:

	Агресивен	Балансиран	Понижен	Изключено*
Модул за разширено машинно обучение	✓ (агресивен режим)	✓ (консервативен режим)	X	X
Модул на система за засичане на потенциално опасни заплахи	✓	✓	✓	X
Други модули за защита	✓	✓	✓	X

* Не се препоръчва.

Определяне на версия на продукт, версии на програмен модул и дати на компилация

1. Щракнете върху **Помощ и поддръжка** > **Относно ESET Internet Security**.
2. В екрана **Относно** първият ред текст показва номера на версията на вашия продукт на ESET.
3. Щракнете върху **Инсталирани компоненти** за достъп до информация за определени модули.

Важни забележки

Няколко важни забележки при настройването на подходящ праг за вашата среда:

• **Балансиран** праг се препоръчва за повечето системи.

• Колкото по-висок е прагът на докладване, толкова по-висока е честотата на откриване, но и по-голям шансът за погрешно идентифицирани обекти.

• От гледна точка на практиката няма гаранция за 100% честота на откриване, както и 0%

шанс за избягване на неправилно категоризиране на чисти обекти като злонамерен софтуер.

• Поддържайте ESET Internet Security и модулите му обновени, за да увеличите максимално баланса между производителността и точността на честотата на откриване и броя на погрешно докладваните обекти.

Настройка на защитата

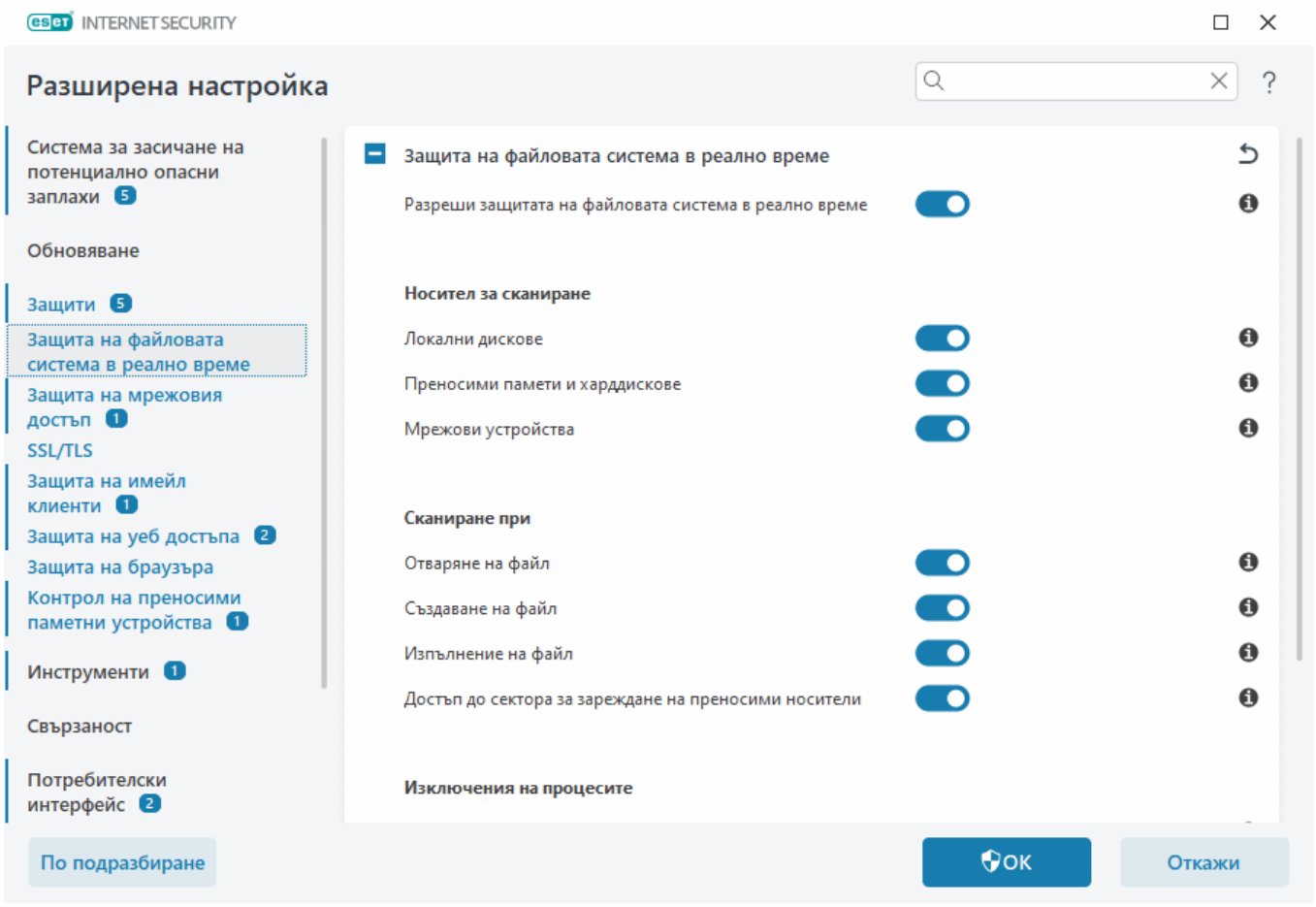
Ако обект, класифициран като КАТЕГОРИЯ, е докладван, програмата блокира обекта, след което го почиства, премахва или премества в карантина.

Прочетете следната информация, преди да модифицирате праг (или ниво) за защита от КАТЕГОРИЯ:

Праг	Обяснение
Агресивен	Докладваните откривания на агресивно (или по-ниско) ниво се блокират и се стартира автоматично отстраняване на проблеми (т.е. почистване). Тази настройка се препоръчва, когато всички крайни точки са били сканирани с агресивни настройки и погрешно докладвани обекти са добавени към изключенията от откриването.
Балансиран	Докладваните откривания на балансирано (или по-ниско) ниво се блокират и се стартира автоматично отстраняване на проблеми (т.е. почистване).
Понижен	Докладваните откривания на понижено ниво се блокират и се стартира автоматично отстраняване на проблеми (т.е. почистване).
Изключено	Тази опция е полезна за идентифициране и изключване на погрешно докладвани обекти. Изключването на докладването не е налично за защита от злонамерен софтуер, но е стойността по подразбиране за потенциално опасни приложения.

Защита на файловата система в реално време

Защитата на файловата система в реално време контролира всички файлове в системата за зловреден код, когато се отварят, създават или изпълняват.



По подразбиране защитата на файловата система в реално време се стартира при стартиране на системата и осигурява непрекъснато сканиране. Не препоръчваме забраняване на **Разрешаване на защитата на файловата система в реално време** в Разширени настройки > **Защити** > **Защита на файловата система в реално време** > **Защита на файловата система в реално време**.

Носител за сканиране

По подразбиране всички типове носители се сканират за потенциални заплахи:

- **Локални дискове** – сканира всички системни и вътрешни твърди дискове (например: *C:*\, *D:*\).
- **Външни устройства** – сканира CD/DVD, USB устройства за съхранение, карти с памет и т.н.
- **Мрежови устройства** – сканира всички назначени мрежови устройства (например: *H:*\ като *store04*) или мрежови устройства с директен достъп (например: *store08*).

Препоръчително е да използвате настройките по подразбиране и да ги променяте само при определени случаи, когато например сканирането на определени носители значително забавя прехвърлянето на данни.

Сканиране при

По подразбиране всички файлове се сканират, когато се отварят, създават или изпълняват.

Препоръчително е да запазите настройките по подразбиране, тъй като те осигуряват максимално ниво на защита на компютъра в реално време:

• **Отваряне на файл** – сканира, когато се отвори файл.

• **Създаване на файл** – сканира създадените или модифицирани файлове.

• **Изпълнение на файл** – сканира, когато файл се изпълни.

• **Достъп до сектор за начално стартиране на преносим носител** – когато преносим носител, който съдържа сектор за начално стартиране, се поставя в устройството, секторът за начално стартиране се сканира незабавно. Тази опция не разрешава сканирането на файлове в преносими носители. Сканирането на файлове в преносими носители се намира в **Носител за сканиране** > **Преносим носител**. За да може **Достъп до сектор за начално стартиране на преносими носители** да работи правилно, оставете **Сектори за начално стартиране/UEFI** разрешено в ThreatSense.

Изключения на процесите

Вж. Изключения на процесите.

ThreatSense

Защитата на файловата система в реално време проверява всички типове носители и се задейства от различни системни събития, като например отваряне на файл. При използване на **ThreatSense** методите за откриване на технологията (както е описано в ThreatSense) защитата на файловата система в реално време може да се конфигурира така, че да обработва по различен начин новосъздадените и вече съществуващите файлове. Можете например да конфигурирате защита на файловата система в реално време, за да следите отблизо новосъздадените файлове.

За минимално натоварване на системата при използването на защитата в реално време файловете, които вече са сканирани, не се сканират постоянно (освен ако не са променени). Файловете незабавно се сканират отново след всяко обновяване на системата за откриване. Това поведение се управлява с помощта на **Оптимизация Smart**. Ако **Оптимизация Smart** е забранена, всички файлове се сканират всеки път, когато се осъществява достъп до тях. За да промените тази настройка, отворете Разширени настройки > **Защити** > **Защитата на файловата система в реално време**. Щракнете върху **ThreatSense** > **Други** и изберете или отменете избора на **Разрешаване на оптимизация Smart**.

Защитата на файловата система в реално време също ви позволява да конфигурирате Допълнителни ThreatSense параметри.

Изключения на процесите

Функцията за изключения на процесите ви позволява да изключите процес на приложение от защитата на файловата система в реално време. За подобряване на скоростта на архивиране, цялостта на процесите и наличността на услуги по време на архивирането се използват някои техники, за които се знае, че влизат в конфликт със защитата от злонамерен софтуер на ниво файл. Единственият ефективен начин да предотвратите двете ситуации е да деактивирате

софтуера срещу злонамерен софтуер. Като изключвате определени процеси (например тези на решението за архивиране), всички операции с файлове, приписани на такива изключени процеси, се игнорират и се считат за безопасни, като така конфликта с процеса на архивиране се свежда до минимум. Ние препоръчваме да сте внимателни, когато създавате изключения – инструмент за архивиране, който е изключен, може да получи достъп до заразени файлове, без да предизвика уведомление, поради което разширените разрешения са позволени само в модула за защита в реално време.

Не се бъркайте с Изключени файлови разширения, HIPS изключения, Изключения за откриването или Изключения за производителността.

Изключенията от тип „Процес“ помагат риска от потенциални конфликти да се сведе до минимум и подобряват производителността на изключените приложения, което на свой ред оказва положителен ефект върху цялостната производителност и стабилността на операционната система. Изключението на процес/приложение е изключение на неговия изпълним файл (*.exe*).

Можете да добавите изпълними файлове в списъка на изключените процеси в Разширени настройки > **Защити** > **Защита на файловата система в реално време** > **Защита на файловата система в реално време** > **Изключения на процеси**.

Тази функция е проектирана да изключва инструменти за архивиране. Изключването на процеса на инструмента за архивиране от сканиране не само гарантира стабилност на системата, но и не влияе на производителността на архивирането, защото архивирането не е забавено, докато се изпълнява.

Щракнете върху **Редактиране**, за да отворите прозореца за управление на **Изключения на процесите**, където можете да извършите добавяне на изключения и да потърсите изпълним файл (например *Backup-tool.exe*), който ще бъде изключен от сканиране. Веднага след като *.exe* файлът е добавен към изключенията, дейността на процеса не се наблюдава от ESET Internet Security и не се извършва сканиране на нито една от операциите с файлове, извършвани от процеса.

Ако не използвате функцията за търсене, когато избирате изпълнимия файл на процеса, трябва ръчно да въведете пълния път до изпълнимия файл. В противен случай изключението няма на работи правилно и HIPS може да отчете грешки.

Можете също така извършите **Редактиране** на съществуващи процеси или **Премахване** на процеси от изключенията.

Защитата на уеб достъпа не взима предвид това изключение, така че ако изключите изпълнимия файл на уеб браузъра, изтеглените файлове ще продължат да бъдат сканирани. По този начин проникване все още може да бъде открито. Този сценарий е само пример и не ви препоръчваме да създавате изключения за уеб браузъри.

Добавяне или редактиране на изключения от тип "Процес"

Този диалогов прозорец ви позволява да извършите **Добавяне** на процеси, изключени от системата за засичане на потенциално опасни заплахи. Изключенията от тип „Процес“ помагат

риска от потенциални конфликти да се сведе до минимум и подобряват производителността на изключените приложения, което на свой ред оказва положителен ефект върху цялостната производителност и стабилността на операционната система. Изключението на процес/приложение е изключение на неговия изпълним файл (*.exe*).

Изберете пътя до файла на изключено приложение, като щракнете върху ... (например *C:\Program Files\Firefox\Firefox.exe*). НЕ въвеждайте името на приложението.
Веднага след като *.exe* файлът е добавен към изключенията, дейността на процеса не се наблюдава от ESET Internet Security и не се извършва сканиране на нито една от операциите с файлове, извършвани от процеса.

Ако не използвате функцията за търсене, когато избирате изпълнимия файл на процеса, трябва ръчно да въведете пълния път до изпълнимия файл. В противен случай изключението няма на работи правилно и HIPS може да отчете грешки.

Можете също така извършите **Редактиране** на съществуващи процеси или **Премахване** на процеси от изключенията.

Кога да промените конфигурацията на защитата в реално време

Защитата в реално време е най-важният компонент от поддържането на защитена система. Винаги бъдете внимателни при промяната на параметрите й. Препоръчително е да променяте параметрите само в определени случаи.

След инсталиране на ESET Internet Security всички настройки се оптимизират за максимално ниво на защита на системата. За да възстановите настройките по подразбиране, щракнете върху до Разширени настройки > **Защити** > **Отговори за откриване**.

Проверка на защитата в реално време

За да проверите дали защитата в реално време работи и открива вируси, използвайте тестов файл от *www.eicar.com*. Този тестов файл е безвреден файл, който се открива от всички антивирусни програми. Файлът е създаден от фирмата EICAR (European Institute for Computer Antivirus Research) с цел тестване на функционалността на антивирусните програми.

Файлът е наличен за изтегляне на адрес http://www.eicar.org/download/eicar.com
След като въведете този URL адрес в браузъра, трябва да видите съобщение, че заплахата е премахната.

Какво да направите, ако защитата в реално време не работи

В тази глава описваме проблемни ситуации, които могат да възникнат при използването на защитата в реално време, а също и тяхното отстраняване.

Защитата в реално време е забранена

Ако потребител неволно е деактивирал защитата в реално време, трябва да активирате отново функцията. За да активирате отново защитата в реално време, отидете на **Настройка** в главния прозорец на програмата и щракнете върху **Защита на компютъра** > **Защита на файловата система в реално време**.

Ако защитата в реално време не се инициализира при стартирането на системата, това обикновено се дължи на забраната на опцията **Разреши защита на файловата система в реално време**. За да сте сигурни, че тази опция е разрешена, отворете Разширени настройки > **Защити** > **Защита на файловата система в реално време**.

Защитата в реално време не открива и не почиства проникванията

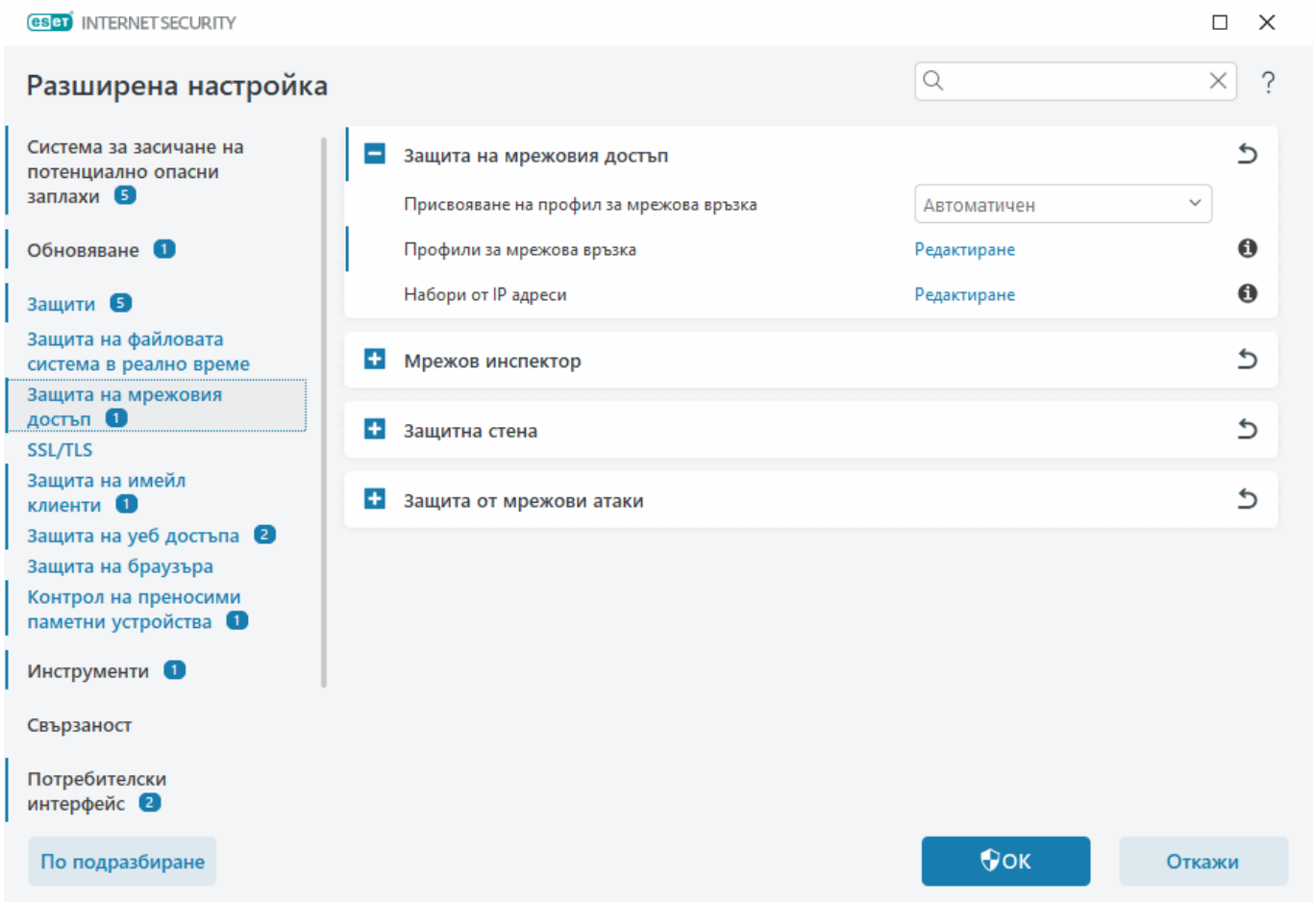
Уверете се, че на компютъра не са инсталирани други антивирусни програми. Ако две антивирусни програми са инсталирани едновременно, те може да влязат в конфликт една с друга. Препоръчваме ви да деинсталирате всички други антивирусни програми от системата, преди да инсталирате ESET.

Защитата в реално време не се зарежда

Ако защитата в реално време не е инициирана при стартиране на системата (и **Разреши защитата на файловата система в реално време** е разрешено), това може да се дължи на конфликти с други програми. За да разрешите този проблем, създайте ESET SysInspector лог и го изпратете до отдела за техническа поддръжка на ESET за анализ.

Защита на мрежовия достъп

Защитата на мрежовия достъп ви позволява да конфигурирате подробно всичките си мрежови връзки. Можете да разрешите/откажете достъп до вашия компютър в конкретни мрежи, да разрешите/откажете достъп до мрежови устройства от вашия компютър и други въз основа на конфигурацията. По подразбиране ESET Internet Security има предварително конфигурирани правила на защитната стена и защита на мрежовия достъп за максимална защита. Въпреки това специфични среди може да се нуждаят от персонализирана конфигурация. Промяната на настройките по подразбиране трябва да се извършва само от опитен потребител.



Можете да конфигурирате следните настройки в Разширени настройки > **Защити** > **Защита на мрежовия достъп** (Щракнете върху връзките по-долу за подробно описание на всяка опция за защита на мрежовия достъп):

Защита на мрежовия достъп

Профили за мрежова връзка – Можете да използвате профили, за да контролирате поведението на защитната стена за конкретни мрежови връзки.

Набори IP адреси – Можете да дефинирате колекции от IP адреси, които създават една логическа група от IP адреси, които можете да използвате за Правила на защитната стена.

Мрежов инспектор

Защитна стена

Защита от мрежови атаки

Профили за мрежова връзка

Профилите могат да се използват за управление на поведението на мрежовата защита на ESET Internet Security за конкретни мрежови връзки. Когато създавате или редактирате Правило на защитна стена, Правило на IDS или Правило за защита от атака с груба сила, можете да го присвоите на конкретен профил или да го приложите към всички профили. Когато е активиран профил в мрежова връзка, към него се прилагат само общите правила (правила без указан

профил) и правилата, назначени на този профил. Можете да създавате множество профили с различни правила, присвоени към мрежови връзки, за да променяте лесно поведението на защитната стена.

Можете да конфигурирате профили и присвоявания за мрежова връзка в Разширени настройки > **Защити** > **Защита на мрежовия достъп** > **Защита на мрежовия достъп**.

Присвояване на профил за мрежова връзка – Позволява ви да избирате дали на новооткрити мрежови връзки да се присвоява автоматично (изберете **Автоматичен** от падащото меню) предварително дефиниран или персонализиран профил въз основа на Активатори, конфигурирани в профили на мрежови връзки, или дали искате да бъдете питани (изберете **Попитай** от падащото меню) за Конфигуриране на мрежова защита и присвояване на профил ръчно всеки път, когато бъде открита нова мрежова връзка.

Можете също ръчно да присвоите конкретен профил за мрежова връзка в главния прозорец на програмата > **Настройка** > **Мрежова защита** > **Мрежови връзки**. Посочете конкретна мрежова връзка и щракнете върху иконата на менюто ⋮ > **Редактиране**, за да отворите прозореца Конфигуриране на мрежова защита и да изберете профил.

Профили за мрежова връзка – Щракнете върху **Редактиране**, за да добавите или редактирате профили за мрежова връзка.

Следните профили са предварително дефинирани и не могат да бъдат редактирани/изтривани:

Лична – За надеждни мрежи (домашна или офис мрежа). Вашият компютър и споделените файлове, съхранени на компютъра, са видими за други потребители в мрежата, а системните ресурси са достъпни за други потребители в мрежата (достъпът до споделени файлове и принтери е разрешен, входящата RPC комуникация е разрешена и споделянето на работния плот е налично). Препоръчваме да използвате тази настройка при достъп до защитена локална мрежа. Този профил автоматично се присвоява на мрежова връзка, ако е конфигуриран като домейн или частна мрежа в Windows.

Публична – За ненадеждни мрежи (публична мрежа). Файловете и папките на вашата система не се споделят или не се виждат от други потребители в мрежата и споделянето на системни ресурси е дезактивирано. Препоръчваме да използвате тази настройка при достъп до безжични мрежи. Този профил автоматично се присвоява на всяка мрежова връзка, която не е конфигурирана като домейн или частна мрежа в Windows.

Когато мрежовата връзка се превключи към друг профил, в долния десен ъгъл на екрана ви ще се появи известие.

Добавяне или редактиране на профили за мрежова връзка

Можете да добавяте или редактирате профили за мрежова връзка в Профили за мрежова връзка в Разширени настройки > **Защити** > **Защита на мрежовия достъп** > **Защита на мрежовия достъп** > **Профили за мрежова връзка** > **Редактиране**. За да редактирате профил, той трябва да бъде избран от списъка в прозореца **Профили за мрежова връзка**.

Следните профили са предварително дефинирани и не могат да бъдат редактирани/изтривани:

Лична – За надеждни мрежи (домашна или офис мрежа). Вашият компютър и споделените файлове, съхранени на компютъра, са видими за други потребители в мрежата, а системните ресурси са достъпни за други потребители в мрежата (достъпът до споделени файлове и принтери е разрешен, входящата RPC комуникация е разрешена и споделянето на работния плот е налично). Препоръчваме да използвате тази настройка при достъп до защитена локална мрежа. Този профил автоматично се присвоява на мрежова връзка, ако е конфигуриран като домейн или частна мрежа в Windows.

Публична – За ненадеждни мрежи (публична мрежа). Файловете и папките на вашата система не се споделят или не се виждат от други потребители в мрежата и споделянето на системни ресурси е дезактивирано. Препоръчваме да използвате тази настройка при достъп до безжични мрежи. Този профил автоматично се присвоява на всяка мрежова връзка, която не е конфигурирана като домейн или частна мрежа в Windows.

Отгоре/Нагоре/Надолу/Отдолу – Позволява ви да регулирате нивото на приоритет на профилите за мрежова връзка (профилите за мрежова връзка се оценяват и прилагат по техния приоритет; винаги се прилага първият съвпадащ профил).

Добавяне или редактиране на профил

Персонализираният профил за мрежова връзка ви позволява да прилагате правила на защитната стена и да дефинирате допълнителни настройки за конкретни мрежови връзки. Ще укажете към кои мрежови връзки ще бъде присвоен персонализираният профил в раздела Активатори.

За да отворите редактора на профили, в прозореца **Профили за мрежова връзка**:

- Щракнете върху **Добави**.
- Изберете един от съществуващите профили и щракнете върху **Редактиране**.
- Изберете един от съществуващите профили и щракнете върху **Копиране**.

Име – Име по избор за вашия профил.

Описание – Описание на профила за подпомагане на идентифицирането на профила.

Допълнителни надеждни адреси – Адресите, дефинирани тук, се добавят към доверената зона на мрежовата връзка, към която се прилага този профил (независимо от типа защита на мрежата).

Надеждна връзка – Вашият компютър и споделените файлове, съхранени на него, са видими за други потребители в мрежата, а системните ресурси са достъпни за други потребители в мрежата (достъпът до споделени файлове и принтери е разрешен, входящата RPC комуникация е разрешена и споделянето на споделянето на работния плот е налично). Препоръчваме да използвате тази настройка, когато създавате профил за защитена връзка с локална мрежа. Всички директно свързани мрежови подмрежи също се считат за надеждни. Ако например мрежов адаптер е свързан към такава мрежа с IP адрес 192.168.1.5 и маска на подмрежа 255.255.255.0, подмрежата 192.168.1.0/24 ще се добави към доверената зона на

мрежовата връзка. Ако адаптерът има повече адреси/подмрежи, всички те ще бъдат надеждни.

Докладване на слабо WiFi криптиране – ESET Internet Security ще покаже известие на работния плот, когато се свържете с незащитена безжична мрежа или мрежа със слаба защита.

Активатори – Персонализирани условия, които трябва да бъдат изпълнени, за да се присвои този профил за мрежова връзка към дадена мрежова връзка. Вж. Активатори за подробно обяснение.

Активатори

Активаторите са персонализирани условия, които трябва да бъдат изпълнени, за да се присвои Профил за мрежова връзка към Мрежова връзка. Ако свързаната мрежа има същите атрибути, както са дефинирани в активаторите за свързан мрежов профил, профилът ще бъде приложен към мрежата. Профилът за мрежова връзка може да има един или няколко активатора. Ако има няколко активатора, се прилага логиката OR (трябва да бъде изпълнено поне едно условие). Можете да дефинирате активатори в редактора на профили за мрежова връзка. Създаването на персонализирани профили за мрежова връзка трябва да се извършва от опитен потребител.

Налични са следните активатори (ако искате да знаете подробности за текущата си мрежа, вижте Мрежови връзки):

Адаптер

Тип адаптер – Приложете профил, ако мрежовата връзка е установена на избрания тип адаптер.
Име на адаптера – Приложете профил, ако името на мрежовия адаптер съвпада.
IP адаптер – Приложете профил, ако IP адресът на мрежовия адаптер съвпада.

DNS

DNS суфикс – Приложете профил, ако името на домейна съвпада.
DNS IP – Приложете профила, ако IP адресът на DNS сървъра съвпада.

WINS

Приложете профила, ако свързаният IP адрес на Windows Internet Name Service (WINS) съвпада.

DHCP

DHCP IP – Съпоставете IP адреса на DHCP сървъра.

Шлюз по подразбиране

IP – Приложете профил, ако IP адресът на шлюза по подразбиране съвпада.
MAC адрес – Приложете профил, ако MAC адресът на шлюза по подразбиране съвпада.

Wi-Fi

SSID – Приложете профил, ако SSID (името на Wi-Fi) съвпада.
Име на профил – Приложете профил, ако името на Wi-Fi профила съвпада.
Тип защита – Приложете профил, ако типът защита съвпада с избрания от падащото меню. (Ако искате да съответства повече от един, създайте друг активатор).
Тип криптиране – Приложете профил, ако типът криптиране съвпада с избрания от падащото меню. (Ако искате да съответства повече от един, създайте друг активатор).
Мрежова сигурност – Приложете профил, ако мрежата е **отворена**/**защитена**.

Профил на Windows

Приложете профил, ако мрежата е конфигурирана в Windows като **Домейн**/**Частна**/**Публична**.

Удостоверяване

Функцията за удостоверяване на мрежа търси точно определен сървър в съответната мрежа и използва асиметрично шифроване (RSA) за удостоверяване на този сървър. Името на мрежата, което се удостоверява, трябва да съответства на името, зададено в настройките на сървъра за удостоверяване. Името е с различаване на малките и главните букви. Името на сървъра може да бъде въведено като име на IP адрес, DNS или NetBios.
Изтеглете сървъра за удостоверяване на ESET
Публичният ключ може да бъде импортиран с помощта на следните типове файлове:
• PEM криптиран публичен ключ (.pem); можете да генерирате този ключ с помощта на ESET Authentication Server
• Шифрован публичен ключ
• Сертификат на публичен ключ (.crt)
Щракнете върху **Тест**, за да тествате настройките. Ако удостоверяването е успешно, се показва Успешно удостоверяване на сървъра. Ако удостоверяването не е конфигурирано правилно, ще се покаже едно от следните съобщения за грешка:
Неуспешно удостоверяване на сървъра. Невалиден или несъвпадащ цифров подпис.
Цифровият подпис на сървъра не съвпада с въведения публичен ключ.
Неуспешно удостоверяване на сървъра. Името на мрежата не съвпада.
Името на конфигурираната мрежа не съвпада с името на мрежата на сървъра за удостоверяване. Прегледайте и двете имена и се уверете, че са идентични.
Неуспешно удостоверяване на сървъра. Невалиден или липсващ отговор от сървъра.
Няма да бъде получен отговор, ако сървърът не работи или не е достъпен. Може да се получи невалиден отговор, ако друг HTTP сървър работи на указания адрес.
Въведен е невалиден публичен ключ.
Проверете дали файлът на публичния ключ, който сте въвели, не е повреден.

Набори от IP адреси

Наборът от IP адреси е колекция от IP адреси, които създават една логическа група от IP адреси, полезни при повторно използване на един и същ набор от адреси в множество Правила за защитната стена или Правила за защита от атака с груба сила. ESET Internet Security също така съдържа предварително дефинирани набори от IP адреси, за които се прилагат вътрешни правила. Пример за подобна група е **Доверена зона**. Доверена зона представлява група от мрежови адреси, където Вашият компютър и споделените файлове, съхранени на компютъра, са видими за други потребители в мрежата, а системните ресурси са достъпни за други потребители в мрежата.

За да добавите набор от IP адреси:

1. Отворете Разширени настройки > **Защити** > **Защита на мрежовия достъп** > **Набори от IP адреси** > **Редактиране**.

2. Щракнете върху **Добавяне**, въведете **Име** и **Описание** за зоната и въведете отдалечен IP адрес в **Адрес на отдалечен компютър (IPv4/IPv6, обхват, маска)**.

3. Щракнете върху **ОК**.

За повече информация вижте Редактиране на набори от IP адреси.

Редактиране на набори от IP адреси

За повече информация относно наборите от IP адреси вижте Набори от IP адреси.

Колони

Име – Името на група отдалечени компютри.

Описание – Общо описание на групата.

IP адреси – Отдалечени IP адреси, принадлежащи към набор от IP адреси.

Контролни елементи

Когато **добавяте** или **редактирате** набор от IP адреси, са налични следните полета:

Име – Името на група отдалечени компютри.

Описание – Общо описание на групата.

Адрес на отдалечен компютър (IPv4, IPv6, обхват, маска) – Позволява да добавите отдалечен адрес, диапазон от адреси или подмрежа.

Премахване – премахва зона от списъка.

Предварително дефинираните набори от IP адреси не могат да бъдат премахнати.

Примери за IP адреси
Добавяне на IPv4 адрес:
Единичен адрес – Добавя IP адрес на отделен компютър (например *192.168.0.10*).
Диапазон от адреси – Въведете IP адреса на началния и крайния адрес, за да укажете диапазона от IP адреси на няколко компютъра (например *192.168.0.1 – 192.168.0.99*).
Подмрежа – Подмрежа (група компютри), обозначена от IP адрес и маска. Например 255.255.255.0 е мрежовата маска за подмрежата 192.168.1.0. За да изключите цялата подмрежа, въведете *192.168.1.0/24*.
Добавяне на IPv6 адрес:
Един адрес – Добавя IP адреса на отделен компютър (например *2001:718:1c01:16:214:22ff:fec9:ca5*).
Подмрежа – Подмрежа (група компютри), обозначена от IP адрес и маска (например: *2002:c0a8:6301:1::1/64*).

Мрежов инспектор

Мрежовият инспектор може да помогне за идентифициране на уязвимости във вашата надеждна (домашна или офис) мрежа (например отворени портове или слаба парола на рутера). Тя също така предоставя списък със свързани устройства, категоризирани по тип устройство (например принтер, рутер, мобилно устройство и т.н.), за да ви покаже какви устройства са свързани с вашата мрежа (например игрова конзола, IoT или други интелигентни домашни устройства). Можете да конфигурирате „Мрежов инспектор“ в Разширени настройки > **Защити** > **Защита на мрежовия достъп** > **Мрежов инспектор**.

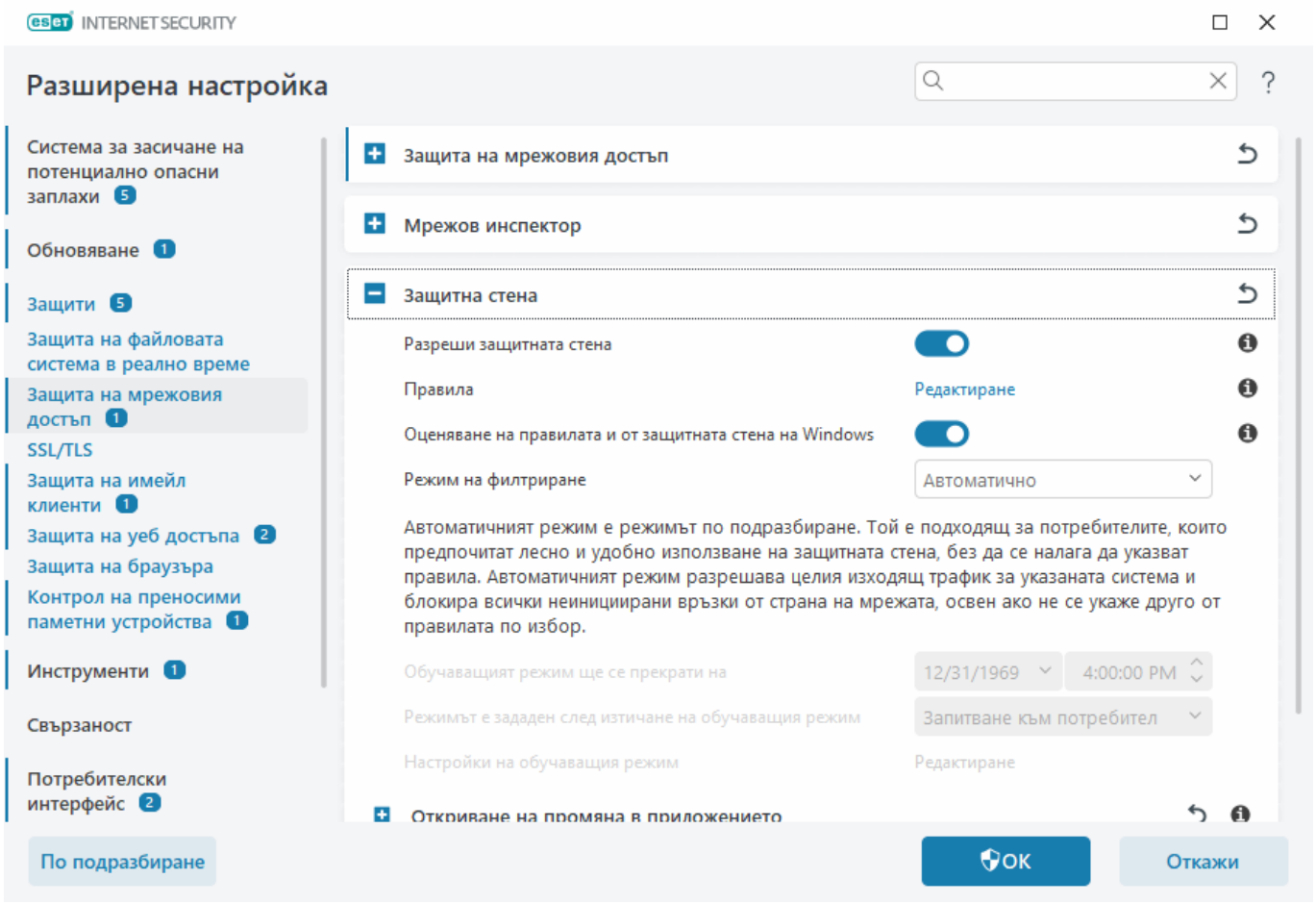
Активиране на мрежов инспектор – Мрежов инспектор помага да се идентифицират уязвимости в домашната мрежа, като например отворени портове или слаба парола на рутера. Също така предоставя списък на свързаните устройства, категоризирани по тип устройство.

Получаване на известия за наскоро открити мрежови устройства – Уведомява ви, когато бъде открито ново устройство във вашата мрежа.

Защитна стена

Защитната стена контролира целия входящ и изходящ мрежов трафик на вашия компютър въз основа на вътрешни правила и правила, определени от вас. Това се осъществява чрез разрешаване или отказване на отделните мрежови връзки. Защитната стена предоставя защита срещу атаки от дистанционни устройства и може да блокира потенциално опасни услуги.

За да конфигурирате защитната стена, отворете Разширени настройки > **Защити** > **Защита на мрежовия достъп** > **Защитна стена**.



Защитна стена

Разреши защитната стена

Препоръчваме ви да оставите тази функция разрешена, за да гарантирате защитата на системата. Когато защитната стена е активирана, мрежовият трафик се сканира и в двете посоки.

Правила

Разделът за настройка на правила ви позволява да преглеждате и редактирате всички правила за защитна стена, които се прилагат за трафика, генериран от отделните приложения в надеждните зони и интернет.

Можете да създадете правило за IDS при ботнет атаки срещу компютъра. Правилото може да се променя в Разширени настройки > **Защити** > **Защита на мрежовия достъп** > **Защита от мрежови атаки** > **Правила за IDS**, като щракнете върху **Редактиране**.

Оценяване на правилата и от защитната стена на Windows

В автоматичен режим на филтриране се позволява и входящият трафик, разрешен от правилата на защитната стена на Windows, освен ако не е изрично блокиран от правилата на ESET.

Режим на филтриране

Функционирането на защитната стена се променя в зависимост от режима на филтриране.

Режимите на филтриране също оказват влияние върху нивото на необходимата намеса от страна на потребителя.

За защитната стена на ESET Internet Security са налични следните режими на филтриране:

Режим на филтриране	Описание
Автоматичен режим	Режимът по подразбиране. Този режим е подходящ за потребителите, които предпочитат лесно и удобно използване на защитната стена, без да се налага да дефинират правила. Правила по избор, дефинирани от потребителя, могат да се създават, но не са задължителни в **автоматичния режим**. Автоматичният режим разрешава целия изходящ трафик за дадена система и блокира по-голямата част от входящия трафик с изключение на част от трафика от доверената зона (както е посочено в IDS и разширени опции/Разрешени услуги) и отговорите на скорошни изходящи комуникации.
Интерактивен режим	Дава възможност да изградите персонализирана конфигурация за защитната стена. Когато бъде открита комуникация и няма съществуващи правила за нея, се показва диалогов прозорец, който съобщава за неизвестна връзка. В него можете да разрешите или откажете комуникацията, а изборът ви ще се запамети като ново правило в защитната стена. Ако решите да създадете ново правило, всички бъдещи връзки от този тип ще се разрешават или блокират в зависимост от това правило.
Базиран на правила режим	Този режим блокира всички връзки, за които не е дефинирано конкретно правило за тяхното разрешаване. Този режим позволява на напредналите потребители да дефинират правила, които позволяват само желани и надеждни връзки. Всички останали неуказани връзки ще се блокират от защитната стена.
Обучаващ се режим	Автоматично създава и записва правила. Този режим се използва най-добре за първоначално конфигуриране на защитната стена, но не трябва да се оставя включен за дълги периоди от време. Не се изисква намеса на потребителя, тъй като ESET Internet Security записва правилата според предварително зададени параметри. Обучаващият режим трябва да се използва само до създаването на всички правила за необходимите комуникации, за да се избегнат рисковете за защитата.

Обучаващият режим ще се прекрати на – Задайте дата и час, когато обучаващият режим приключва автоматично. Можете също така да изключите обучаващия режим ръчно, когато пожелаете.

Режимът е зададен след изтичане на обучаващия режим – задайте режим на филтриране, към който да премине защитната стена на , след като изтече периодът на обучаващия режим. Прочетете повече за режимите на филтриране в таблицата по-горе. След приключване опцията **Запитване към потребител** изисква административни привилегии за осъществяването на промяна в режима на филтриране на защитната стена.

Настройки на обучаващ режим – Щракнете върху **Редактиране**, за да конфигурирате параметри за записване на правила, създадени в обучаващ режим.

Откриване на промяна на приложение

Функцията за откриване на промени в приложенията на защитната стена показва известия, ако променените приложения, за които съществува правило на защитната стена, правят опити да установят връзки.

Настройки на обучаващия режим

Обучаващият режим автоматично създава и записва правило за всяка комуникация, която се установява в системата. Не се изисква намеса на потребителя, тъй като ESET Internet Security записва правилата според предварително зададени параметри.

Този режим може да изложи системата ви на риск и се препоръчва само за първоначална конфигурация на защитната стена.

Изберете **Обучение** от падащото меню в Разширени настройки > **Защити** > **Защита на мрежовия достъп** > **Защитна стена** > **Защитна стена** > **Режим на филтриране**, за да активирате опциите на обучаващия режим. Щракнете върху **Редактиране** до **Настройки на обучаващия режим**, за да конфигурирате следните опции:

⚠ В обучаващия режим защитната стена не филтрира комуникацията. Всички изходящи и входящи връзки са разрешени. В този режим компютърът не е изцяло защитен от защитната стена.

Входящ трафик от доверената зона – пример за входяща връзка в рамките на доверената зона би било отдалечено устройство в рамките на доверената зона, опитващо се да установи комуникация с местно приложение, изпълнявано на вашия компютър.

Изходящ трафик към доверената зона – локално приложение, опитващо се да осъществи комуникация с друго устройство в рамките на локалната мрежа или в мрежа в доверената зона.

Входящ интернет трафик – отдалечено устройство, опитващо да комуникира с приложение, изпълнявано на компютъра.

Изходящ интернет трафик – локално приложение, опитващо се да установи комуникация с друго устройство.

Всеки раздел ви позволява да дефинирате параметри, които да се добавят към новосъздадените правила:

Добавяне на локален порт – включва номера на локалния порт на мрежовата комуникация. За изходяща комуникация обикновено се генерират случайни числа. По тази причина препоръчваме да разрешите тази опция само за входяща комуникация.

Добавяне на приложение – включва името на локалното приложение. Тази опция е подходяща за бъдещи правила на ниво приложение (правила, които дефинират комуникацията на цяло приложение). Можете например да разрешите комуникацията само за уеб браузър или имейл клиент.

Добавяне на отдалечен порт – включва номера на отдалечения порт на мрежовата

комуникация. Можете например да разрешите или да откажете конкретна услуга, свързана със стандартен номер на порт (HTTP – 80, POP3 – 110 и т.н.).

Добавяне на отдалечен IP адрес/доверена зона – отдалеченият IP адрес или зона може да се използва като параметър за нови правила, дефиниращи всички мрежови връзки между локалната система и отдалечения адрес/зона. Тази опция е подходяща, ако искате да дефинирате действия за определено устройство или група устройства в мрежа.

Максимален брой различни правила за приложение – ако дадено приложение комуникира през различни портове, различни IP адреси и т.н, защитната стена в обучаващ режим създава съответния брой правила за него. Тази опция ви позволява да ограничите броя на правилата, които могат да се създадат за едно приложение.

Правила за защитната стена

Правилата за защитната стена представляват набор от условия, които се използват за тестване на мрежовите връзки, както и всички действия, присвоени към тези условия. С помощта на правила на защитната стена може да зададете какво действие да се предприеме, когато се осъществяват различни видове мрежови връзки.

Правилата се оценяват отгоре надолу и можете да видите техния приоритет в първата колона. Действието на първото съвпадащо правило се използва за всяка мрежова връзка в процес на оценяване.

Връзките могат да се разделят на входящи и изходящи. Входящите връзки се инициират от отдалечено устройство, опитващо да установи връзка с локалната система. Изходящите връзки работят по обратния начин – локалната система се свързва с отдалечено устройство.

Ако бъде открита непозната комуникация, трябва внимателно да помислите дали да я разрешите, или да я откажете. Нежеланите, опасните или непознатите връзки излагат компютъра на риск. Ако бъде установена такава връзка, се препоръчва да обърнете специално внимание на отдалеченото устройство и на приложението, което се опитва да се свърже с вашия компютър. Много вируси се опитват да разкрият и изпратят поверителни данни или да изтеглят други злонамерени приложения в работни станции на хостове. Защитната стена ви позволява да откривате и прекъсвате подобни връзки.

Можете да преглеждате и редактирате правила за защитна стена в Разширени настройки > **Защити** > **Защита на мрежовия достъп** > **Защитна стена** > **Правила** > **Редактиране**.

Ако имате много правила за защитна стена, можете да използвате филтър, за да покажете само определени правила. За да филтрирате правила за защитна стена, щракнете върху **Още филтри** над списъка с правила за защитна стена. Можете да филтрирате правилата въз основа на следните критерии:

- Произход
- Посока
- Действие
- Наличност

По подразбиране предварително дефинираните правила за защитна стена са скрити. За да покажете всички предварително дефинирани правила, забранете превключвателя до **Скриване на вградените (предварително дефинирани) правила**. Можете да забраните тези правила, но не можете да премахнете предварително зададено правило.

Щракнете върху иконата за търсене горе вдясно, за да търсите правило(а).

Колони

Приоритет – Правилата се оценяват отгоре надолу и можете да видите техния приоритет в първата колона.

Разрешено – показва дали правилото е разрешено, или забранено; съответното квадратче за отметка трябва да е избрано, за да бъде активирано правилото.

Приложения – приложение, за което се прилага правилото.

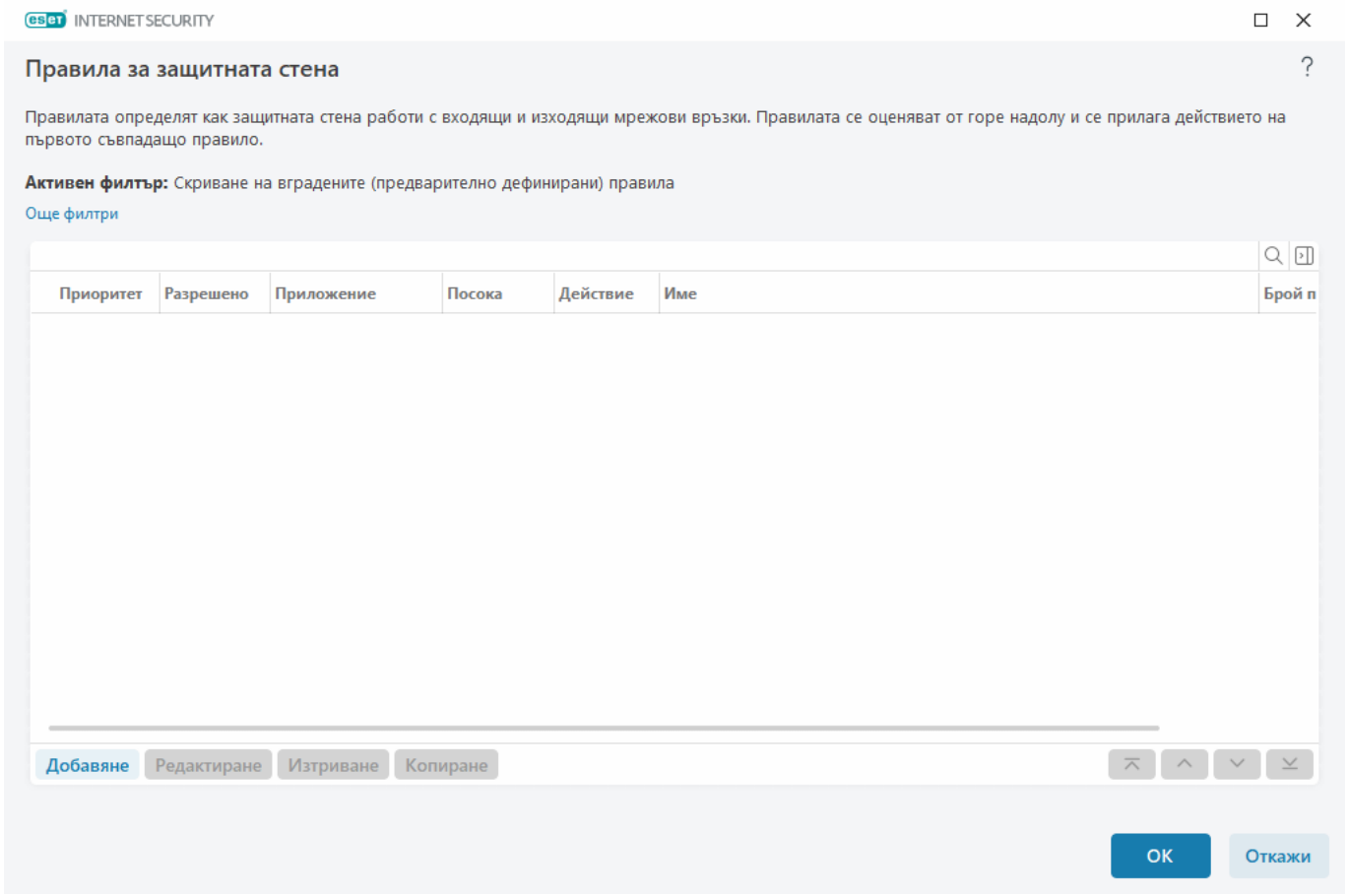
Посока – посока на комуникацията (входяща/изходяща/и двете).

Действие – показва състоянието на комуникацията (блокиране/разрешаване/питане).

Име – име на правилото. Иконата на ESET представлява предварително дефинирано правило.

Приложени времена – Общ брой пъти, в които е приложено правилото.

Щракнете върху иконата за разгъване, за да се покажат подробностите за правилото.



Контролни елементи

Добавяне – създаване на ново правило.

Редактиране – редактиране на съществуващо правило.

Премахване – премахване на съществуващо правило.

Копиране – създаване на копие на избрано правило.

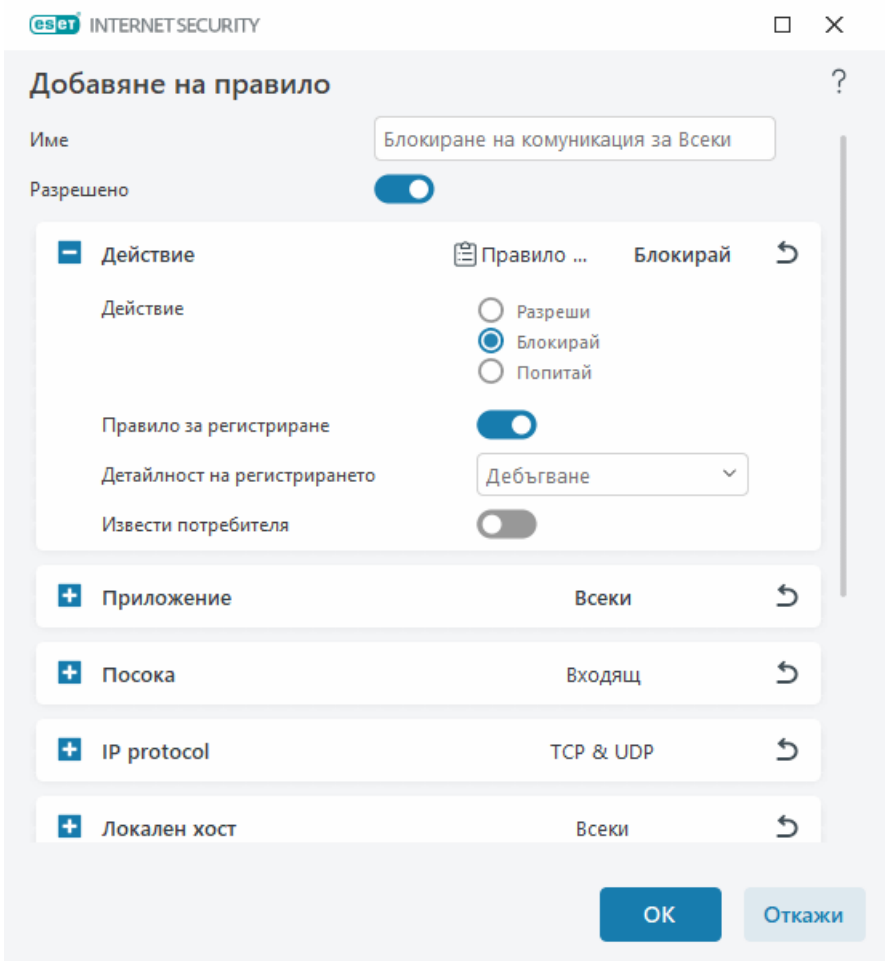
 **Отгоре/Нагоре/Надолу/Отдолу** – позволява да коригирате нивата на приоритет на правилата (правилата се изпълняват от горе надолу).

Добавяне и редактиране на правила на защитната стена

Правилата за защитна стена представляват условия, които се използват за тестване на всички мрежови и действия, присвоени към тези условия. Може да се изисква редактиране или добавяне на правила на защитната стена, когато мрежовите настройки се променят (например мрежовият адрес или номерът на порта за отдалечената страна са променени), за да се гарантира правилната работа на приложение, засегнато от правило. Опитен потребител трябва да създаде персонализирани правила за защитна стена.

> **Илюстрирани инструкции**
> Следните статии в онлайн помощника на ESET може да бъдат налични и на английски:
> • Отваряне или затваряне (позволяване или забрана) на конкретен порт със защитна стена
> • Създаване на правило за защитната стена от регистрационните файлове в ESET Internet Security

За да добавите или редактирате правило за защитна стена, отворете Разширени настройки > **Защити** > **Защита на мрежовия достъп** > **Защитна стена** > **Правила** > **Редактиране**. В прозореца Правила за защитната стена щракнете върху **Добавяне** или **Редактиране**.



Име – Въведете име за правилото.

Разрешено – Щракнете върху превключвателя, за да направите правилото активно.

Добавете действия и условия за правилото за защитната стена:

Действие

Действие – Изберете дали искате да **Позволите**/**Блокирате** комуникацията, която отговаря на условията, определени в това правило, или искате ESET Internet Security да **Пита** всеки път, когато комуникацията се установи.
Правило за регистриране – Ако правилото е приложено, то ще бъде записано в Регистрационни файлове.
Детайлност на регистрирането – Изберете детайлността на записа в дневника за това правило.
Опцията **Извести потребителя** показва известие, когато се прилага правилото.

Приложение

Посочете приложение, където ще се прилага това правило.
Път на приложение – Щракнете върху **...** и отидете до приложение или въведете пълния път на приложението (например C:\Program Files\Firefox\Firefox.exe). НЕ въвеждайте името на приложението самостоятелно.
Подпис на приложение – Можете да приложите правилото към приложения въз основа на техните подписи (име на издателя). Изберете от падащото меню, ако искате да приложите правилото към приложения с **всеки валиден подпис** или към приложения, **подписани от конкретен подписващ**. Ако изберете приложения, **подписани от конкретен подписващ**, трябва да дефинирате подписващия в полето **Име на подписващ**.
Приложение от Microsoft Store – Изберете приложение, инсталирано от Microsoft Store в падащото меню.
Услуга – Можете да изберете системна услуга вместо приложение. Отворете падащото меню, за да изберете услуга.
Прилагане към дъщерни процеси – Някои приложения могат да изпълняват повече процеси, докато виждате само един прозорец на приложение. Щракнете върху превключвателя, за да разрешите правилото за всеки процес в указаното приложение.

Посока

Изберете **Посока** на комуникация за това правило:
- **И двете** – Входяща и изходяща комуникация
- **Входяща** – Само входяща комуникация
- **Изходяща** – Само изходяща комуникация

IP протокол

Изберете **Протокол** от падащото меню, ако искате това правило да се прилага само за конкретен протокол.

Локален хост

Локални адреси, диапазон от адреси или подмрежа, където се прилага това правило. Ако няма посочен адрес, правилото ще се прилага за цялата комуникация с локални хостове. Можете да добавите IP адреси, диапазони от адреси или подмрежи директно в текстовото поле за **IP адреси** или да изберете от съществуващите Набори от IP адреси, като щракнете върху **Редактиране** до **Набори от IP адреси**.

Локален порт

номер(а) на локален **порт**. Ако не са предоставени номера, правилото ще се прилага за всеки порт. Можете да добавите един-единствен комуникационен порт или диапазон от комуникационни портове.

Отдалечен хост

Отдалечен адрес, диапазон от адреси или подмрежа, където се прилага това правило. Ако не е посочен адрес, правилото ще се прилага за цялата комуникация с отдалечени хостове. Можете да добавите IP адреси, диапазони от адреси или подмрежи директно в текстовото поле за **IP адреси** или да изберете от съществуващите Набори от IP адреси, като щракнете върху **Редактиране** до **Набори от IP адреси**.

Отдалечен порт

номер(а) на отдалечен **порт**. Ако не са предоставени номера, правилото ще се прилага за всеки порт. Можете да добавите един-единствен комуникационен порт или диапазон от комуникационни портове.

Профил

Правило за защитна стена може да се приложи към конкретни Профили за мрежова връзка.
Всеки – Правилото ще бъде приложено към всяка мрежова връзка, въпреки използвания профил.
Избрано – Правилото ще бъде приложено към конкретна мрежова връзка въз основа на избрания профил. Поставете отметка в квадратчето до профилите, които искате да изберете.

Създаваме ново правило за позволяване на приложението на уеб браузъра Firefox да осъществява достъп до интернет/локални мрежови уеб сайтове.
1.В раздела **Действие** изберете **Действие** > **Позволяване**.
2.В раздела **Приложение** укажете **Път на приложението** на уеб браузъра (например C:\Program Files\Firefox\Firefox.exe). НЕ въвеждайте името на приложението самостоятелно.
3.В раздела **Посока** изберете **Посока** > **Изходяща**.
4.В раздела **IP протокол** изберете **TCP & UDP** от падащото меню **Протокол**.
5.В раздела **Отдалечен порт** добавете номера на **Портове**: *80 443*, за да се позволи стандартно сърфиране.

Откриване на промяна на приложение

Функцията за откриване на модификации в приложението показва известия, ако модифицирани приложения, за които съществува правило на защитната стена, се опитват да установят връзки. Модификацията в приложението е механизъм за временно или трайно заместване на оригинално приложение с друго приложение с друг изпълним файл (предпазва от злоупотреба с правилата на защитната стена).

Имайте предвид, че целта на тази функция не е да открива промени във всички приложения по принцип. Целта е да се предотврати злоупотребата със съществуващите правила на защитната стена и съответно се наблюдават само приложенията, за които съществуват определени правила на защитната стена.

За да редактирате **Откриване на промяна на приложение**, отворете Разширени настройки > **Защити** > **Защита на мрежовия достъп** > **Защитна стена** > **Откриване на промяна на приложение**.

Разрешаване на откриване на промени в приложенията – ако опцията е избрана, програмата следи приложенията за промени (обновявания, заразявания или други промени). Когато дадено променено приложение се опита да установи връзка, ще получите известие от защитната стена.

Разреши промяна на подписани (надеждни) приложения – Не се изпраща известие, ако приложението разполага със същия валиден цифров подпис преди и след промяната.

Списък с изключени от откриване приложения – този прозорец ви позволява да добавяте или премахвате отделни приложения, за които промените са разрешени без необходимост от известяване.

Списък с изключени от откриване приложения

Защитната стена в ESET Internet Security открива промени в приложенията, за които съществуват правила (вж. Откриване на промяна на приложение).

В някои случаи може да решите да не използвате тази функция за определени приложения, които искате да изключите от проверката на защитната стена.

Добавяне – отваря прозорец, в който можете да изберете приложение за добавяне към списъка с приложения, изключени от откриване на модификации. Можете да изберете от списък с изпълнявани приложения с отворена мрежова комуникация, за които съществува правило за защитната стена, или да добавите конкретно приложение.

Редактиране – отваря прозорец, където можете да промените местоположението на приложение, което е в списъка с приложения, изключени от откриването на модификации. Можете да избирате от списък с работещи приложения с отворена мрежова комуникация, за които съществува правило на защитната стена, или да променяте местоположението ръчно.

Премахване – Премахва записи от списъка на приложенията, изключени от откриването на промени.

Защита от мрежови атаки (IDS)

Защитата от мрежова атака (IDS) подобрява откриването на експлойти за известни уязвимости. Прочетете повече за защитата от мрежови атаки в речника. За да конфигурирате защитата от мрежови атаки, отворете Разширени настройки > **Защити** > **Защита на мрежовия достъп** > **Защита от мрежови атаки**.

Разрешаване на защита срещу мрежови атаки (IDS) – анализира съдържанието на мрежовия трафик и защитава от мрежови атаки. Трафикът, считан за вреден, ще бъде блокиран.

Разрешаване на защита от ботнет мрежи – Открива и блокира комуникация със зловредни командни и контролни сървъри въз основа на обичайни шаблони, когато компютърът е заразен и бот се опитва да комуникира. Прочетете повече за защитата от защита от ботнет мрежи в речника.

Правила за IDS – Тази опция ви позволява да конфигурирате разширените опции за филтриране за откриване на няколко типа атаки и експлойти, които могат да навредят на компютъра ви.

> **Илюстрирани инструкции**
> Следните статии в онлайн помощника на ESET може да бъдат налични и на английски:
> - Изключване на IP адрес от IDS в/във ESET Internet Security

Всички важни събития, открити от мрежовата защита, се записват в регистрационен файл. За повече информация вижте регистрационния файл на мрежовата защита.

правила IDS

В някои ситуации услугата за откриване на проникванията (IDS) може да открие комуникация между рутери или други устройства за вътрешна мрежа като потенциална атака. Например можете да добавите известния безопасен адрес към адресите, изключени от IDS зоната, за да заобиколите IDS.

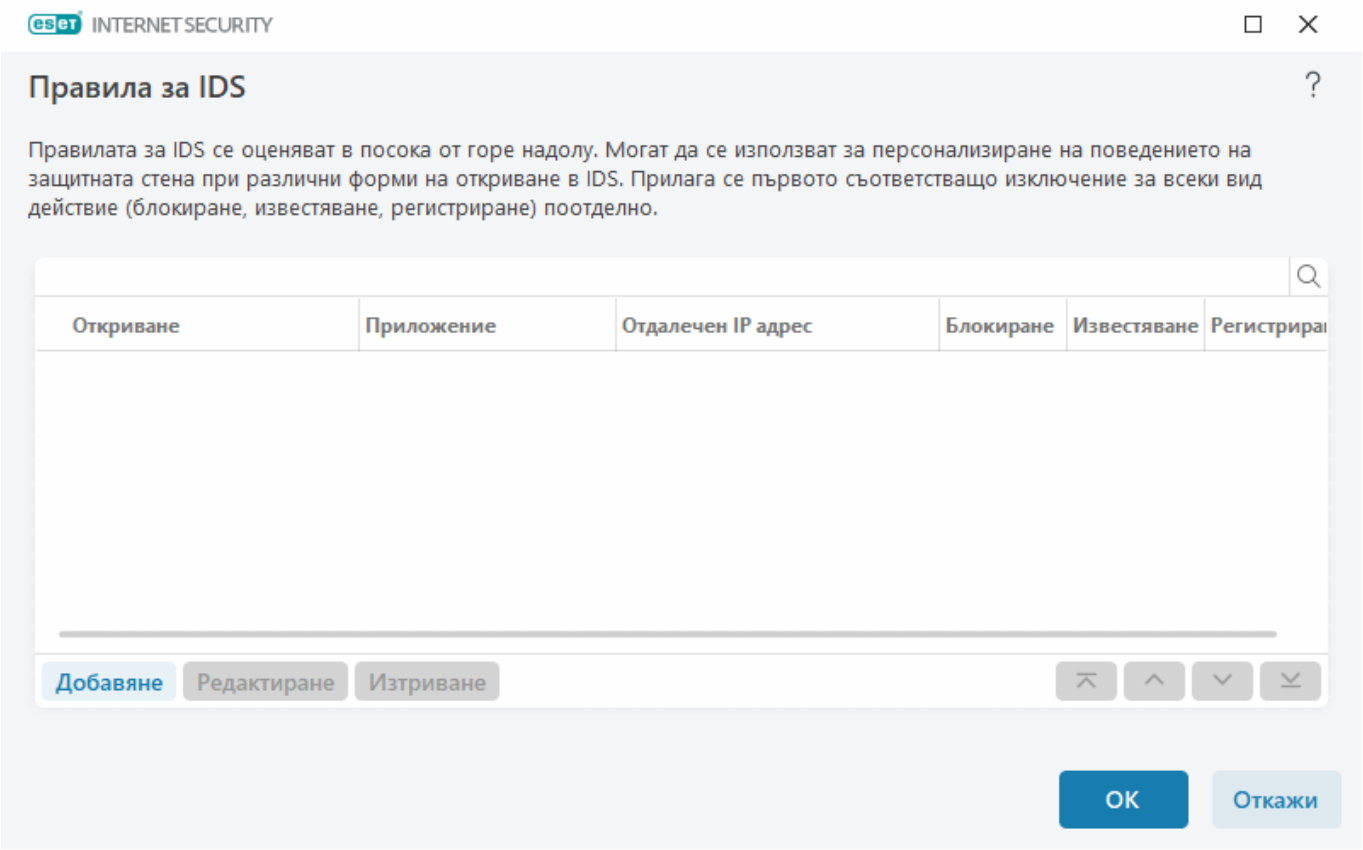
> **Илюстрирани инструкции**
> Следните статии в онлайн помощника на ESET може да бъдат налични и на английски:
> • Изключване на IP адрес от IDS в/ъв ESET Internet Security

Управление на правилата за IDS

• **Добавяне** – щракнете тук, за да създадете ново правило за IDS.
• **Редактиране** – Щракнете тук, за да редактирате съществуващо правило за IDS.

• **Премахване** – направете избор и щракнете тук, ако искате да премахнете съществуващо правило от списъка с правила за IDS.

• **Отгоре/Нагоре/Надолу/Отдолу** – позволява да коригирате нивата на приоритет на правилата (изключенията се анализират от горе надолу).



Редактор на правило

Откриване – Тип на откриването.

Име на заплаха – Можете да посочите име на заплаха за някои от наличните откривания.

Приложение – изберете пътя до файла на изключено приложение, като щракнете върху ... (например *C:\Program Files\Firefox\Firefox.exe*). НЕ въвеждайте името на приложението.

Отдалечен IP адрес – списък на отдалечени IPv4 или IPv6 адреси/диапазони/подмрежи. Различните адреси трябва да бъдат разделени със запетая.

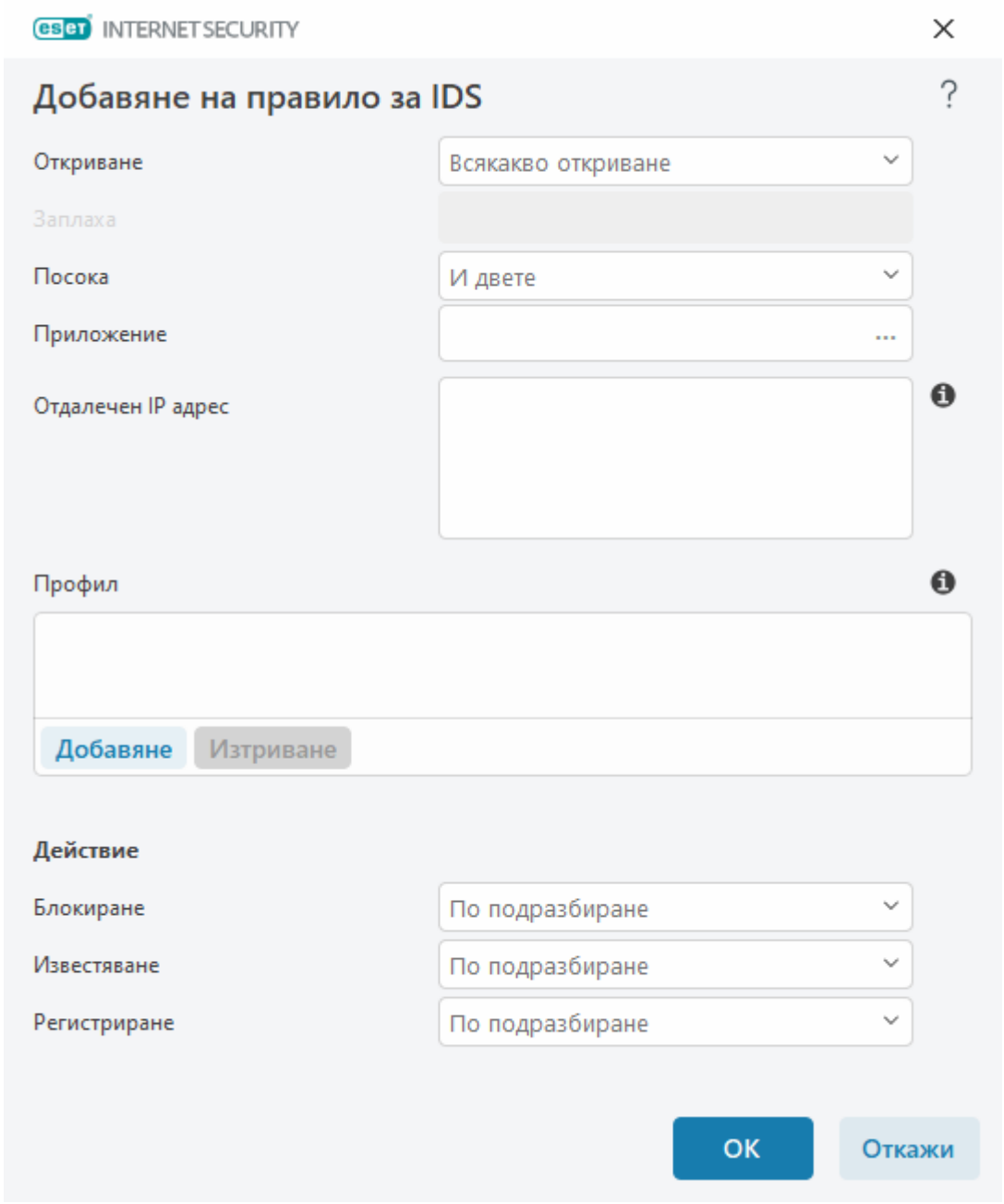
Профил – Можете да изберете профил за мрежова връзка, за който ще се прилага това правило.

Действие

Блокиране – всеки системен процес разполага със собствено поведение по подразбиране и назначено действие (блокиране или разрешаване). За да заместите поведението по подразбиране за ESET Internet Security, можете да изберете да го блокирате или разрешите с помощта на падащото меню.

Известяване – изберете Да, за да покажете известия на работния плот на компютъра. Изберете Не, ако не искате известия на работния плот. Наличните стойности са По подразбиране/Да/Не.

Дневник – изберете **Да**, за да регистрирате събития в регистрационните файлове на . Изберете **Не**, ако не искате за регистрирате събития. Наличните стойности са **По подразбиране**/**Да**/**Не**.



Ако желаете да се показва известие и да се създава дневник при всяко възникване на събитието:
1.Щракнете върху **Добавяне**, за да добавите ново правило за IDS.
2.Изберете специфично откриване от падащото меню **Откриване**.
3.Изберете път на приложение, като щракнете върху **...**, за което искате да приложите това известие.
4.Оставете **По подразбиране** в падащото меню **Блокиране**. Така ще се наследи действието по подразбиране, приложено от ESET Internet Security.
5.Задайте и двете падащи менюта **Известяване** и **Дневник** на **Да**.
6.Щракнете върху **OK**, за да запазите известието.

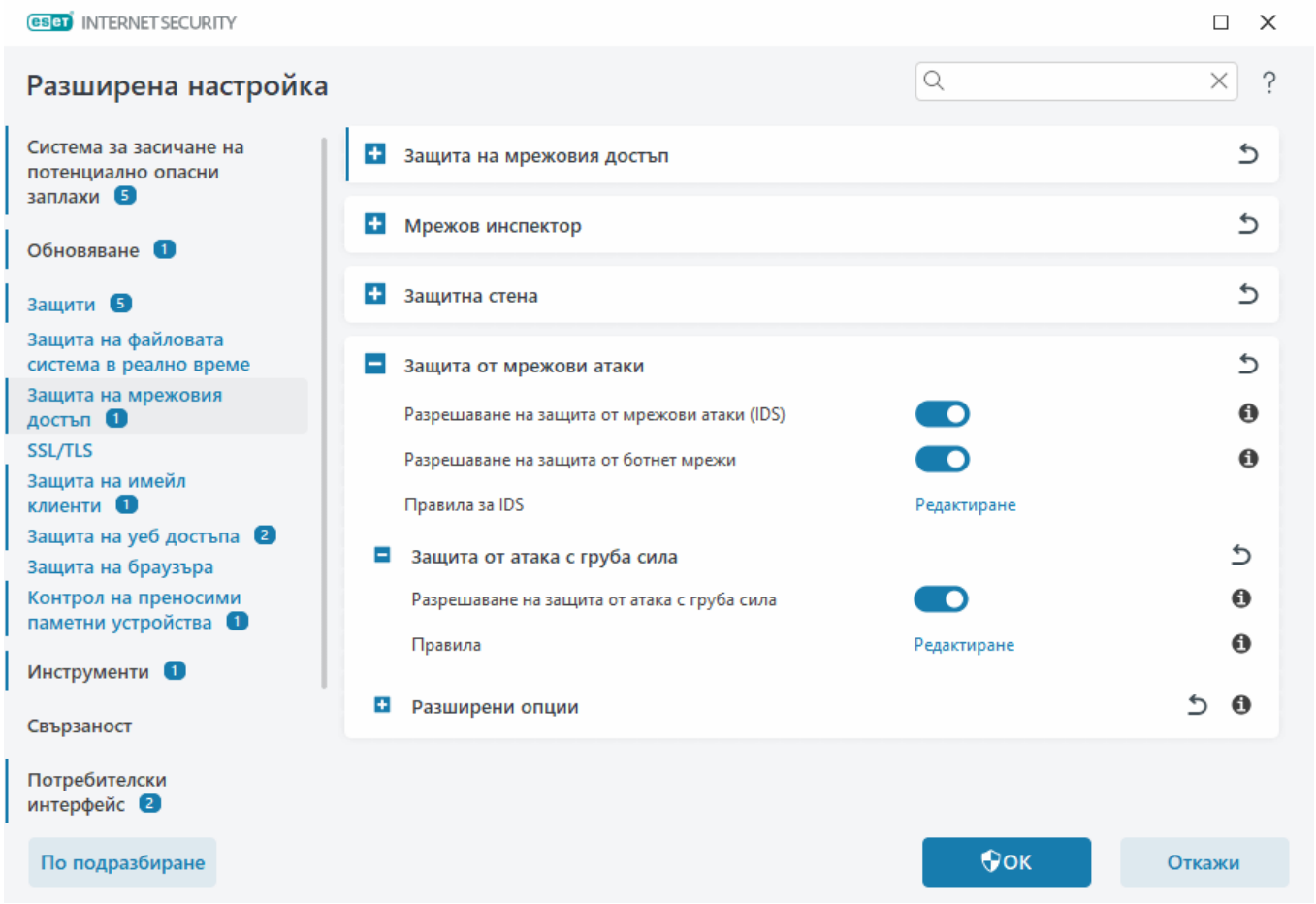
Ако не желаете да се показва повтарящо се известие, което не считате за заплаха от конкретен тип **Откриване**:
1.Щракнете върху **Добавяне**, за да добавите ново правило за IDS.
2.Изберете конкретно откриване от падащото меню **Откриване**, като например **SMB сесия без разширения за защита** или **Атака при сканиране на TCP портовете**.
3.Изберете **Входящо** от падащото меню за посоката, в случай че е породено от входяща комуникация.
4.Настройте падащото меню **Известяване** на **Не**.
5.Настройте падащото меню **Дневник** на **Да**.
6.Оставете **Приложение** празно.
7.Ако комуникацията не идва от конкретен IP адрес, оставете **Отдалечени IP адреси** празно.
8.Щракнете върху **OK**, за да запазите известието.

Защита от атака с груба сила

Защитата от атака с груба сила блокира атаки чрез отгатване на паролата за услуги RDP и SMB. Атаката с груба сила е метод за откриване на целева парола чрез систематично пробване на всички комбинации от букви, цифри и символи. За да конфигурирате защитата от атака с груба сила, отворете Разширени настройки > **Защити** > **Защита на мрежовия достъп** > **Защита от мрежови атаки** > **Защита от атака с груба сила**.

Разрешаване на защитата от атака с груба сила – ESET Internet Security инспектира съдържанието на мрежовия трафик и блокира опитите за атаки чрез отгатване на паролата.

Правила – това ви позволява да създавате, редактирате и преглеждате правила за входящи и изходящи мрежови връзки. За повече информация вижте главата Правила.



Правила

Правилата за защита от атака с груба сила ви позволяват да създавате, редактирате и преглеждате правила за входящи и изходящи мрежови връзки. Предварително дефинираните правила не могат да бъдат редактирани или премахнати.

Управление на правила за защита от атака с груба сила

Добавяне – създаване на ново правило.

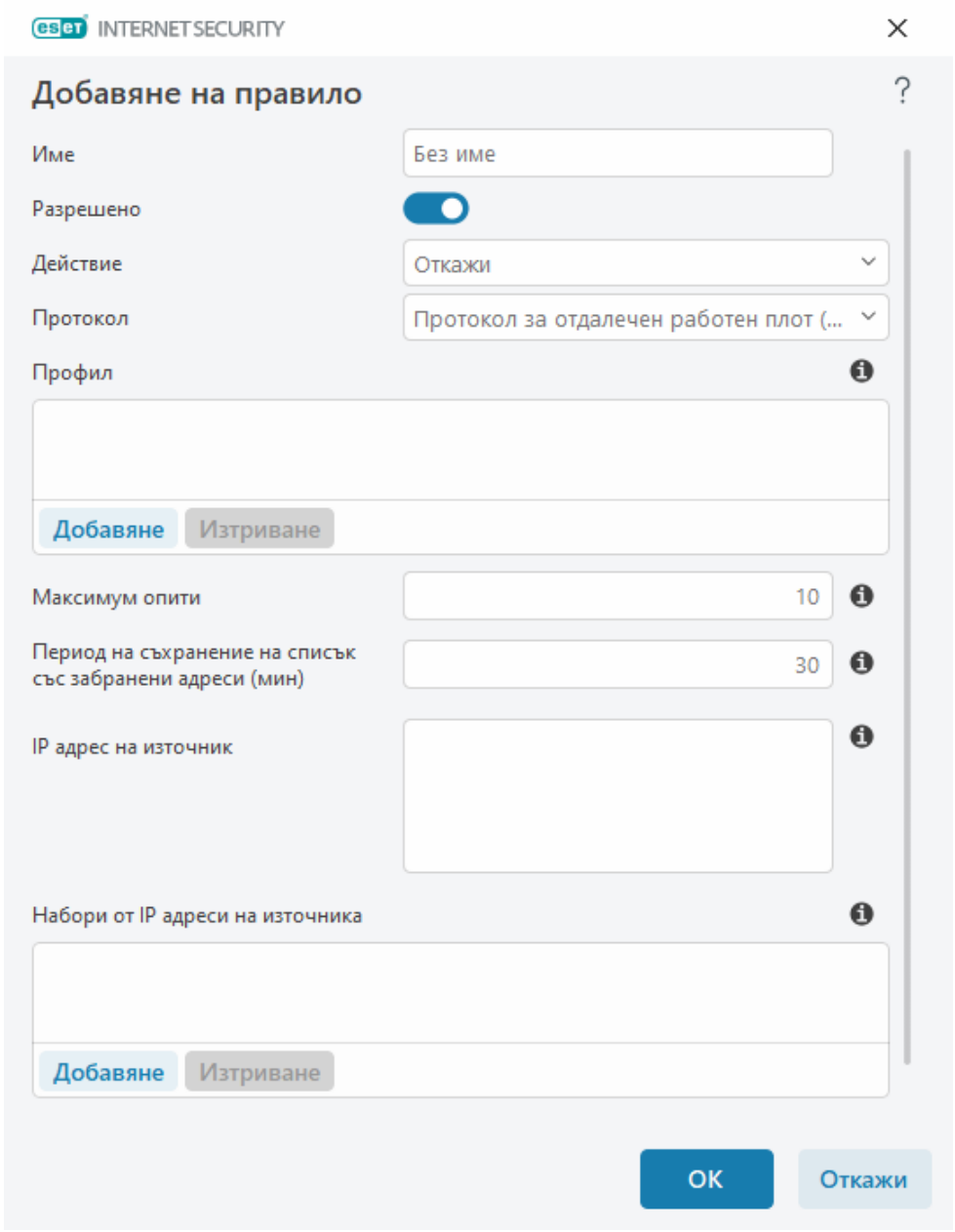
Редактиране – редактиране на съществуващо правило.

Премахване – премахване на съществуващо правило от списъка с правила.

Отгоре/Нагоре/Надолу/Отдолу – коригиране на нивата на приоритет на правилата.

За да се осигури възможно най-висока защита, се прилага правилото за блокиране с най-ниската стойност на **Максимум опити** дори ако правилото се намира по-надолу в списъка с правила, когато множество правила за блокиране отговарят на условията за откриване.

Редактор на правило



Име – име на правилото.

Разрешено – Деактивирайте плъзгача, ако искате да запазите правилото в списъка, но без да го прилагате.

Действие – Изберете дали да **откажете**, или да **позволите** връзката, ако настройките на правилото са изпълнени.

Протокол – Комуникационният протокол, който ще бъде инспектиран от това правило.

Профил – персонализираните правила могат да се задават и прилагат за определени профили.

Максимум опити – Максималният брой позволени опити за повторение на атака, докато IP адресът бъде блокиран и добавен към списъка със забранени адреси.

Период на съхранение на списък със забранени адреси (мин) – задава времето за изтичане на адреса от черния списък.

IP адрес на източник – списък с IP адреси, диапазони или подмрежи. Различните адреси трябва да бъдат разделени със запетая.

Набори от IP адреси на източника – Набор от IP адреси, които вече сте определили в Набори от IP адреси.

Разширени опции

В Разширени настройки > **Защити** > **Защита на мрежовия достъп** > **Защита от мрежови атаки** > **Разширени опции** можете да активирате или дезактивирате откриването на няколко типа атаки и експлойти, които могат да навредят на компютъра ви.

В някои случаи няма да получавате известие за заплаха относно блокирани комуникации. Прегледайте раздела Регистриране и създаване на правила или изключения от регистрационен файл за инструкции как да видите всички блокирани комуникации в регистрационния файл на защитната стена.

Наличността на определени опции в този прозорец може да се различава в зависимост от типа или версията на вашия продукт на ESET и модула за защитна стена, както и от версията на вашата операционна система.

Откриване на проникване

Откриването на проникванията следи мрежовата комуникация на устройството за злонамерена дейност.

- **Протокол SMB** – Открива и блокира различни проблеми със защитата в протокола SMB.
- **Протокол RPCRPC** – Открива и блокира различни често срещани слаби места и излагания на риск в системата за заявка за отдалечена процедура, разработена за Разпределена компютърна среда (DCE).
- **Протокол RDP** – открива и блокира различни често срещани слаби места и излагане на риск в протокола RDP (вж. по-горе).
- Откриване на атака за заразяване на **ARP** – Откриване на атаки за заразяване на ARP, предизвикани от „посреднически“ атаки, или откриване на прослушвания на мрежовия превключвател. ARP (Address Resolution Protocol (Протокол за разрешаване на адреси)) се използва от мрежовото приложение или устройство за определяне на Ethernet адреса.
- Откриване на атака със сканиране на **TCP/UDPпортове** – Открива атаки на софтуер, който сканира портове – приложение, предназначено да проучва хост за отворени портове, като изпраща клиентски заявки до набор от адреси на портове с цел да открие активни портове и да използва уязвимостите на услугата. Прочетете повече за този тип атака в речника.
- **Блокиране на опасния адрес след откриване на атаката** – IP адреси, които са открити като източници на атаки, се добавят в списъка със забранени адреси, за да предотвратят връзка за определен период от време. Можете да определите **период на задържане в**

списък със забранени адреси, който задава за колко време адресът ще бъде блокиран след откриване на атака.

- **Уведомяване за откриване на атака** – включва известието в областта за уведомяване на Windows в долния десен ъгъл на екрана.

- **Известяване за входящи атаки срещу пробиви в защитата** – предупреждава ви, ако бъдат открити атаки срещу дупки в защитата или ако заплаха извърши опит за влизане в системата по този начин.

Проверка на пакети

Тип анализ на пакети, който филтрира данните, които се прехвърлят през мрежата.

- **Разрешаване на входяща връзка с администраторските дялове в SMB протокола** – Администраторските дялове (админ. дялове) са мрежовите дялове по подразбиране, които разделят дяловете на твърдия диск (*C$*, *D$*, ...) в системата, заедно със системната папка (ADMIN$*ADMIN$*). Със забраната на връзка до администраторски дялове ще се намалят много рискове за защитата. Например червеят Conficker извършва атаки на речника, за да се свърже с администраторските дялове.

- **Отказване на стари (неподдържани) SMB диалекти** – откажете SMB сесии, които използват стар SMB диалект, който не се поддържа от IDS. Модерните операционни системи Windows поддържат старите SMB диалекти благодарение на обратна съвместимост с предходни операционни системи, като например Windows 95. Атакуващият може да използва стар диалект в SMB сесия, за да избегне проверката на трафика. Откажете стари SMB диалекти, ако не е необходимо компютърът ви да споделя файлове (или използвайте обща SMB комуникация) с компютър със стара версия на Windows.

- **Отказване на SMB сесии без разширения на защитата** – Разширена защита може да се използва по време на съгласуване на SMB сесия, за да се предостави по-сигурен механизъм за удостоверяване в сравнение с удостоверяването от тип предизвикателство/отговор на LAN диспечер (LM). Схемата LM се счита за слаба и не се препоръчва за употреба.

- **Отказване на отваряне на изпълними файлове на сървър извън доверената зона в SMB протокола** – Прекъсва връзката, когато се опитвате да отворите изпълним файл (.exe, .dll, ...) от споделена папка на сървъра, която не принадлежи към доверената зона в защитната стена. Имайте предвид, че копирането на изпълними файлове от доверени източници може да бъде легитимно. Имайте предвид, че копирането на изпълними файлове от доверени източници може да е легитимно, но това откриване може да намали рисковете от нежелано отваряне на файл на злонамерен сървър (като например файл, отворен чрез щракване върху хипер връзка към споделен злонамерен изпълним файл).

- **Отказване на NTLM удостоверяване в протокола SMB за свързване със сървър във/извън доверената зона** – протоколи, които използват схемите за NTLM удостоверяване (и двете версии), са обект на атака за препращане на идентификационни данни (известни като атаки на SMBпрепращане в случая на SMB протокол). Отказването на NTLM удостоверяване със сървър извън доверената зона трябва да намали рисковете от препращане на идентификационни данни от злонамерен софтуер извън доверената зона. Аналогично можете да откажете NTLM удостоверяване със сървъри в доверената зона.

- **Разрешаване на комуникацията с услугата за диспечер на акаунти за защитата** – за повече информация относно тази услуга вж. [MS-SAMR].

- **Разрешаване на комуникацията с услугата за локален орган за защита** – за повече информация относно тази услуга вж. [MS-LSAD] и [MS-LSAT].

- **Разрешаване на комуникацията с услугата за отдалечен системен регистър** – за повече информация относно тази услуга вж. [MS-RRP].

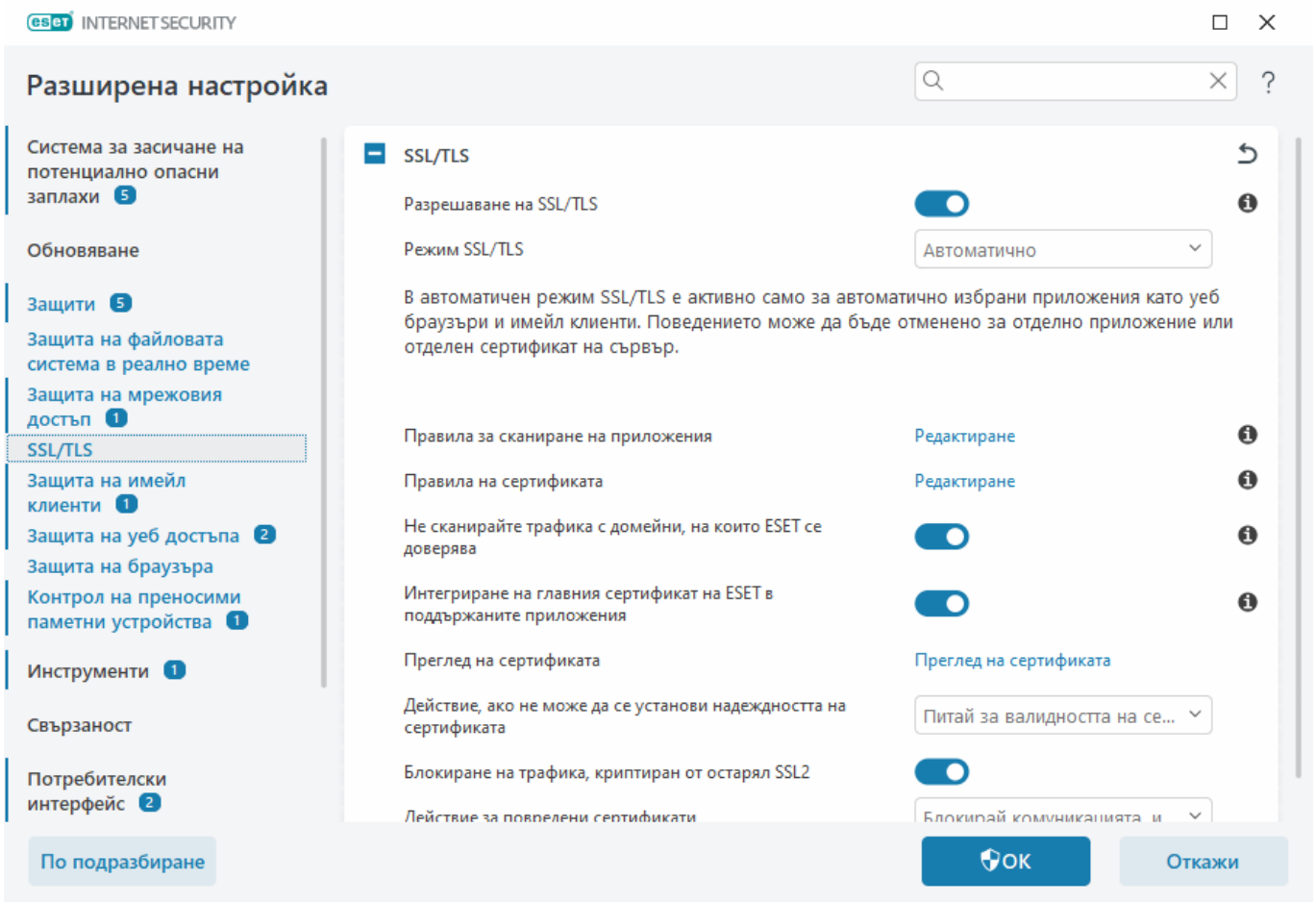
- **Разрешаване на комуникацията с услугата за диспечер за управление на услуги** – за повече информация относно тази услуга вж. [MS-SCMR].

- **Разрешаване на комуникацията с услугата за сървър** – за повече информация относно тази услуга вж. [MS-SRVS].

- **Позволяване на комуникацията с други услуги** – други MSRPC услуги. MSRPC е прилагането от страна на Microsoft на механизма DCE RPC. Освен това MSRPC може да използва наименувани канали, които водят до SMB (мрежово споделяне на файлове) протокол за пренасяне (ncacn_np transport). MSRPC услугите предоставят интерфейси за достъп и отдалечено управление на системите на Windows. Няколко уязвимости в защитата бяха открити и използвани на практика в Windows MSRPC системата (например червей Conficker, червей Sasser и т.н.). Забранете комуникация с MSRPC услуги, които не се налага да предоставяте, за да намалите многобройните рискове за защитата (като например отдалечено изпълнение на код или атаки за прекъсване на услуги).

SSL/TLS

ESET Internet Security може да проверява за заплахи за комуникацията, които използват протокола SSL. Можете да използвате различни режими на филтриране за проверка на защитена с SSL комуникация с помощта на надеждни сертификати, неизвестни сертификати или сертификати, които са изключени от проверката на защитената с SSL комуникация. За да редактирате настройките на SSL/TLS, отворете Разширени настройки > **Защити** > **SSL/TLS.**



Разрешете SSL/TLS – Ако е забранено, ESET Internet Security няма да сканира комуникацията през SSL/TLS.

SSL/TLS режим разполага със следните опции:

Режим на филтриране	Описание
Автоматично	Режимът по подразбиране ще сканира само подходящи приложения, като например уеб браузъри и имейл клиенти. Можете да го заместите, като изберете приложенията, където се сканира комуникацията.
Интерактивен	Ако отворите нов сайт, защитен с SSL (с неизвестен сертификат), ще се покаже диалогов прозорец за избор на действие. Този режим ви позволява да създадете списък с SSL сертификати/приложения, които ще бъдат изключени от сканирането.
Базирано на правила	Режим на правила – Изберете тази опция, за да се сканира цялата защитена с SSL комуникация, с изключение на комуникациите, защитени чрез сертификати, изключени от проверка. Ако се осъществи нова комуникация, която използва непознат, подписан сертификат, няма да бъдете известени, а комуникацията автоматично ще се филтрира. Когато осъществявате достъп до сървър с ненадежден сертификат, маркиран като надежден (включен е в списъка с надеждни сертификати), комуникацията със сървъра се разрешава и съдържанието на комуникационния канал се филтрира.

Правила за сканиране на приложения – Позволява ви да персонализирате поведението на ESET Internet Security за конкретни приложения.

Правила на сертификата – Позволява ви да персонализирате поведението на ESET Internet Security за конкретни SSL сертификати.

Не сканирай трафика с домейни, считани за надеждни от ESET – Когато е разрешена, комуникацията с надеждни домейни ще бъде изключена от сканирането. Вграденият списък с разрешени адреси, управляван от ESET, определя надеждността на домейна.

Интегриране на главния сертификат на ESET в поддържаните приложения – За да работи правилно SSL комуникацията в браузърите/имейл клиентите, е важно главният сертификат за ESET да бъде добавен към списъка с известни главни сертификати (издатели). Когато тази опция е разрешена, ESET Internet Security ще добави автоматично сертификата на ESET SSL Filter CA към познатите браузъри (напр. Opera). За браузърите, които използват системното хранилище за сертификати, сертификатът се добавя автоматично. Например Firefox автоматично се конфигурира да счита за доверени органите за издаване на главни сертификати в системното хранилище за сертификати.

За да приложите сертификата за неподдържани браузъри, щракнете върху **Преглед на сертификата** > **Подробни данни** > **Копиране във файл**, след което го импортирайте ръчно в браузъра.

Действие, ако не може да се установи надеждността на сертификата – В някои случаи сертификат на уеб сайт не може да бъде проверен с помощта на хранилището на органите за издаване на надеждни главни сертификати (TRCA) (например изтекъл сертификат, ненадежден сертификат, сертификат, който не е валиден за конкретен домейн, или подпис, който може да бъде анализиран, но не подписва правилно сертификата). Легитимните уеб сайтове винаги ще използват надеждни сертификати. Ако те не предоставят такъв, това може да означава, че атакуващото лице декриптира комуникацията ви или уеб сайтът изпитва технически затруднения.

Ако е избрана опцията **Питай за валидността на сертификата** (по подразбиране е избрана), ще получите подкана да изберете действие, когато се установи криптирана комуникация. Ще се покаже диалогов прозорец за избор на действие, в който може да маркирате сертификата като надежден или като изключен. Ако сертификатът не е в списъка на TRCA, прозорецът е червен. Ако сертификатът е в списъка на TRCA, прозорецът е зелен.

Може да изберете опцията **Блокирай комуникацията, използваща сертификата**, така че шифрованата връзка към сайта, който използва ненадежден сертификат, винаги да се преустановява.

Блокиране на трафика, криптиран от остарял SSL2 – Комуникацията с по-старата версия на протокола SSL ще бъде блокирана автоматично.

Действие за повредени сертификати – Повреден сертификат означава, че сертификатът използва формат, който не е разпознат от ESET Internet Security, или че е получен повреден (например презаписан от случайни данни). В този случай ви препоръчваме да оставите избрана опцията **Блокирай комуникацията, използваща сертификата**. Ако е избрана опцията **Питай за валидността на сертификата**, потребителят получава подкана да избере действие, когато се установи криптирана комуникация.

Илюстрирани примери

Следните статии в онлайн помощника на ESET може да бъдат налични и на английски:

- Известия за сертификати в продуктите на ESET за домашна употреба за Windows
- „Шифрован мрежов трафик: Ненадежден сертификат“ е показан, когато посещавате уеб страници

Правила за сканиране на приложения

Правилата за сканиране на приложения могат да бъдат използвани за персонализиране на функционирането на ESET Internet Security за конкретни приложения и за запомняне на избраните действия, когато **Режим на SSL/TLS** е в **Интерактивен режим**. Списъкът може да се разглежда и редактира в Разширени настройки > **Защити** > **SSL/TLS** > **Правила за сканиране на приложения** > **Редактиране**.

Прозорецът **Правила за сканиране на приложения** се състои от:

Колони

Приложение – изберете изпълним файл от дървото на директориите, щракнете върху опцията **...** или въведете пътя ръчно.

Действие за сканиране – изберете **Сканирай** или **Игнорирай**, за да се сканира или да се игнорира комуникацията. Изберете **Автоматичен**, за да се сканира в автоматичен режими и да се пита в интерактивен режим. Изберете **Питай**, за да се пита винаги потребителят какво да се прави.

Контролни елементи

Добавяне – добавяне на филтрирано приложение.

Редактиране – изберете приложението, което искате да конфигурирате, и щракнете върху **Редактиране**.

Премахване – изберете приложението, което искате да премахнете, и щракнете върху **Премахване**.

Импортиране/експортиране – импортирайте приложения от файл или запишете текущия си списък с приложения във файл.

ОК/Отказ – щракнете върху **ОК**, ако искате да запишете промените, или върху **Отказ**, ако искате да излезете, без да записвате промените.

Правила на сертификата

Правилата за сертификати могат да се използват за персонализиране на функционирането на ESET Internet Security за конкретни SSL сертификати и за запомняне на действия, избрани, когато **SSL/TLS режимът** е в **Интерактивен режим**. Списъкът може да бъде преглеждан и редактиран в Разширени настройки > **Защити** > **SSL/TLS** > **Правила за сертификати** > **Редактиране**.

Прозорецът **Правила за сертификати** се състои от:

Колони

Име – име на сертификата.

Издател на сертификата – име на създателя на сертификата.

Тема на сертификата – полето за тема идентифицира единицата, свързана с публичния ключ, записан в полето за публичен ключ на субекта.

Достъп – изберете **Разрешаване** или **Блокиране** като **Действие за достъп**, за да разрешите/блокирате комуникацията, защитена с този сертификат, независимо от неговата надеждност. Изберете **Автоматичен**, за да се разрешат надеждните сертификати и да се пита за ненадеждните. Изберете **Питай**, за да се пита винаги потребителят какво да се прави.

Сканирай – изберете **Сканирай** или **Игнорирай** като **Действие за сканиране**, за да се сканира или да се игнорира комуникацията, защитена с този сертификат. Изберете **Автоматичен**, за да се сканира в автоматичен режими и да се пита в интерактивен режим. Изберете **Питай**, за да се пита винаги потребителят какво да се прави.

Контролни елементи

Добавяне – Добавете нов сертификат и регулирайте настройките му относно опциите за достъп и сканиране.

Редактиране – изберете сертификата, който искате да конфигурирате, и щракнете върху **Редактиране**.

Изтриване – изберете сертификата, който искате да изтриете, и щракнете върху **Премахване**.

ОК/Отказ – щракнете върху **ОК**, ако искате да запишете промените, или върху **Отказ**, ако искате да излезете, без да записвате промените.

Шифрован мрежов трафик

Ако системата ви е конфигурирана да използва SSL/TLS сканиране, в две ситуации ще се покаже диалогов прозорец с подкана да изберете действие:

Първо, ако даден уеб сайт използва непроверим или невалиден сертификат и програмата ESET Internet Security е конфигурирана да пита потребителя в подобни случаи (по подразбиране „Да“ за непроверими сертификати и „Не“ за невалидни такива), ще се покаже диалогов прозорец, който ви пита какво действие да се извърши за връзката: **Позволи** или **Блокирай**. Ако сертификатът не се намира в Trusted Root Certification Authorities store (TRCA), се счита за ненадежден.

Второ, ако **SSL/TLS режим** е зададен на **Интерактивен режим**, диалогов прозорец за всеки уеб сайт ще ви пита дали да се извърши **Сканиране** или **Игнориране** на трафика. Някои приложения проверяват дали техният SSL трафик не се променя, или инспектира от някого, в които случаи ESET Internet Security трябва да изпълни действие **Игнорирай** за този трафик, за да

може работата на приложението да продължи.

> **Илюстрирани примери**
> Следните статии в онлайн помощника на ESET може да бъдат налични и на английски:
> • Известия за сертификати в продуктите на ESET за домашна употреба за Windows
> • „Шифрован мрежов трафик: Ненадежден сертификат“ е показан, когато посещавате уеб страници

И в двата случая потребителят може да изберете да се запомни избраното действие. Записаните действия се съхраняват в Правила за сертификата.

Защита на имейл клиенти

За да конфигурирате „Защита на имейл клиенти“, отворете Разширени настройки > **Защити** > **Защита на имейл клиенти** и изберете от следните опции за конфигуриране:

- Защита при придвижването на поща
- Защита на пощенска кутия
- Управление на адресни списъци
- ThreatSense

Защита при придвижването на поща

Протоколите IMAP(S) и POP3(S) са най-широко разпространените протоколи за получаване на имейл комуникация в приложения за имейл клиенти. Протоколът за достъп до имейл чрез интернет (IMAP) е друг интернет протокол за получаване на имейли. IMAP има определени предимства пред POP3, като например това, че множество клиенти могат да се свържат едновременно към една и съща пощенска кутия и да следят информацията за състоянието на съобщенията, като например дали дадено съобщение е прочетено, отговорено, или премахнато. Модулът за защита, осигуряващ този контрол, се стартира автоматично при стартиране на системата и след това е активен в паметта.

ESET Internet Security осигурява защита за тези протоколи независимо от използвания имейл клиент и без да е необходимо той да се преконфигурира. По подразбиране всички комуникации по POP3 и IMAP протоколи се сканират независимо от номерата на POP3/IMAP портовете по подразбиране.
MAPI протокол не е сканиран. Въпреки че комуникацията със сървър на Microsoft Exchange може да бъде сканирана от интеграционния модул в имейл клиенти като Microsoft Outlook.

> ESET Internet Security поддържа също и сканиране на IMAPS (585, 993) и POP3S (995) протоколи, които използват шифрован канал за прехвърляне на информация между сървър и клиент. ESET Internet Security проверява комуникацията с помощта на SSL (Secure Socket Layer (Слой със защитени сокети) и TLS (Transport Layer Security (Защита на транспортен слой) протоколи.
> Шифрованата комуникация ще бъде сканирана по подразбиране. За да видите настройката на скенера, отворете Разширени настройки > **Защити** > SSL/TLS.

За да конфигурирате защитата при придвижването на поща, отворете Разширени настройки > **Защити** > **Защита на имейл клиенти** > **Защита при придвижването на поща**.

Разрешаване на защита при придвижването на поща – Когато е разрешена, комуникацията за транспортиране на поща ще бъде сканирана от ESET Internet Security.

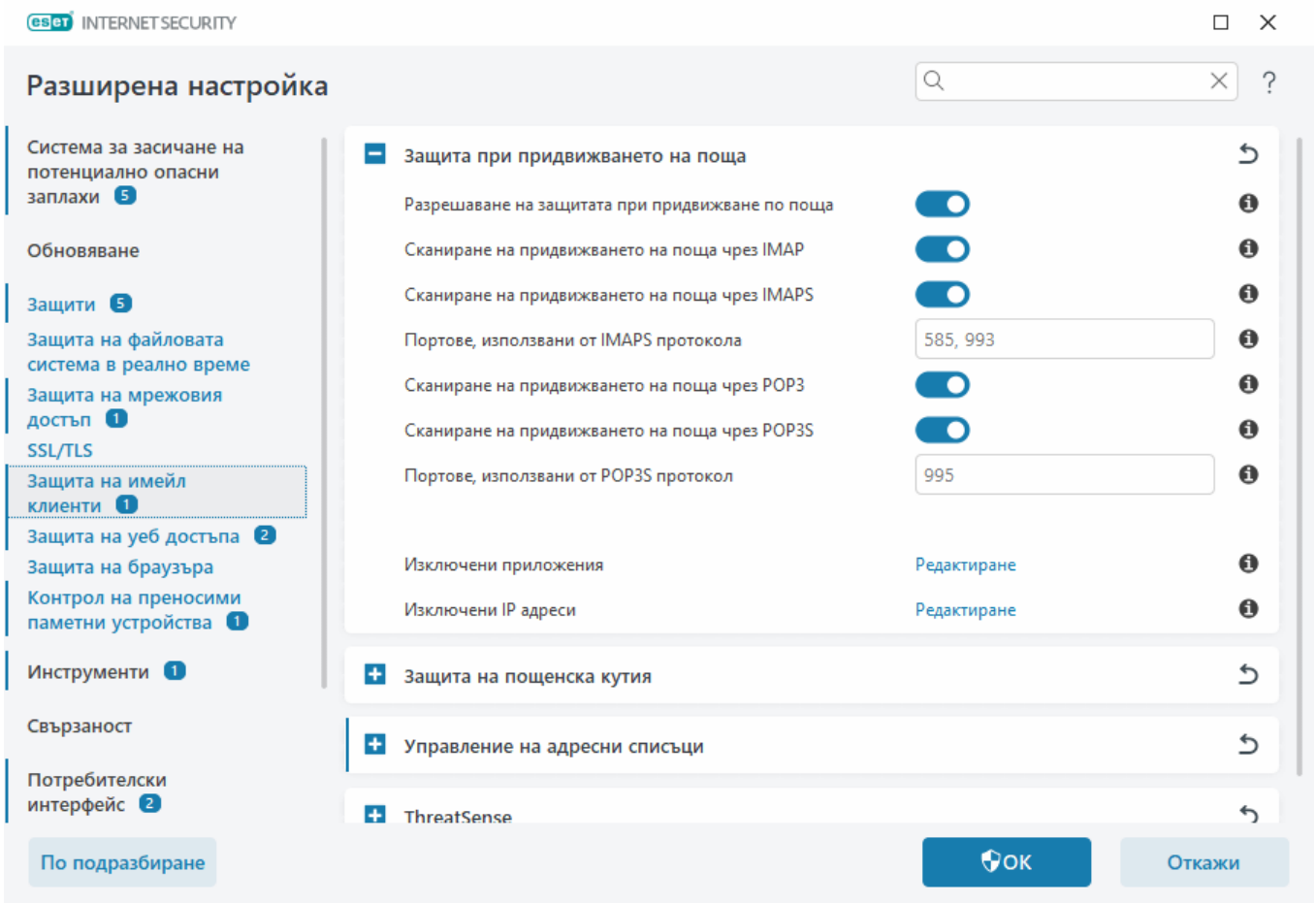
Можете да изберете кои протоколи за придвижване на поща да бъдат сканирани, като щракнете върху превключвателя до следните опции (по подразбиране е разрешено сканиране на всички протоколи):

- **Сканиране на придвижването на поща чрез IMAP**
- **Сканиране на придвижването на поща чрез IMAPS**
- **Сканиране на придвижването на поща чрез POP3**
- **Сканиране на придвижването на поща чрез POP3S**

По подразбиране ESET Internet Security ще сканира IMAPS и POP3S комуникацията на стандартните портове. За да добавите персонализирани портове за IMAPS и POP3S протоколи, добавете ги към текстовото поле до **Портове, използвани от IMAPS протокол** или **Портове, използвани от POP3S протокол**. Когато портовете са повече от един, номерата трябва да са разделени със запетая.

Изключени приложения – Позволява ви да изключите конкретни приложения от сканиране чрез „Защита при придвижването на поща“. Полезно, когато защитата на уеб достъпа причинява проблеми със съвместимостта.

Изключени IP адреси – Позволява ви да изключите конкретни отдалечени адреси от сканиране чрез „Защита при придвижването на поща“. Полезно, когато защитата на уеб достъпа причинява проблеми със съвместимостта.



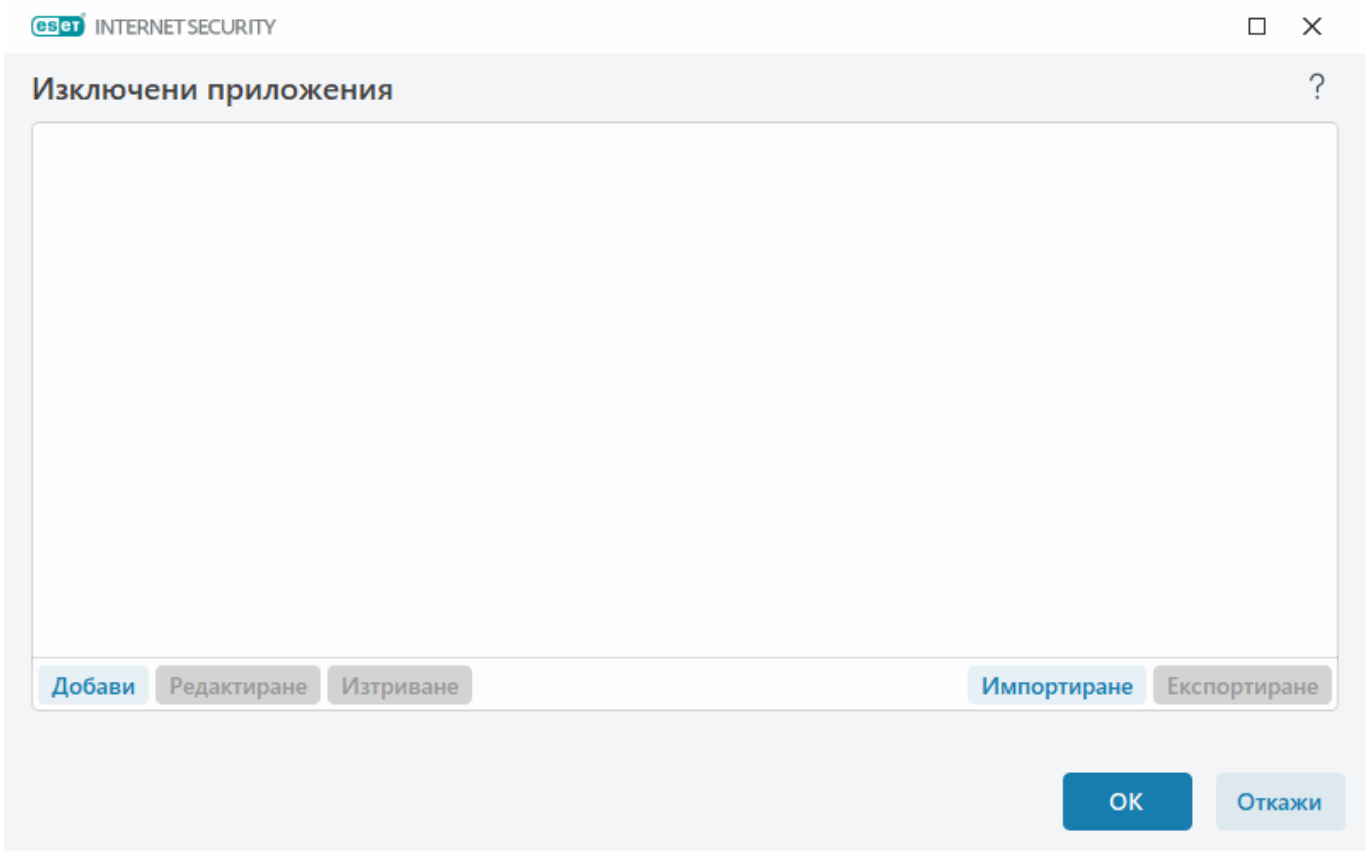
Изключени приложения

За да изключите сканирането на комуникацията за конкретни приложения, добавете ги към списъка. HTTP(S)/POP3(S)/IMAP(S) комуникацията на избраните приложения няма да се проверява за заплахи. Препоръчително е да използвате тази опция само за приложения, които не работят правилно, когато тяхната комуникация се сканира.

Тук е възможно автоматично изпълнение на приложения и услуги, когато щракнете върху **Добавяне**. Щракнете върху **...** и навигирайте до приложение, за да добавите изключение ръчно.

Редактиране – редактиране на избраните записи от списъка.

Премахване – премахване на избраните записи от списъка.



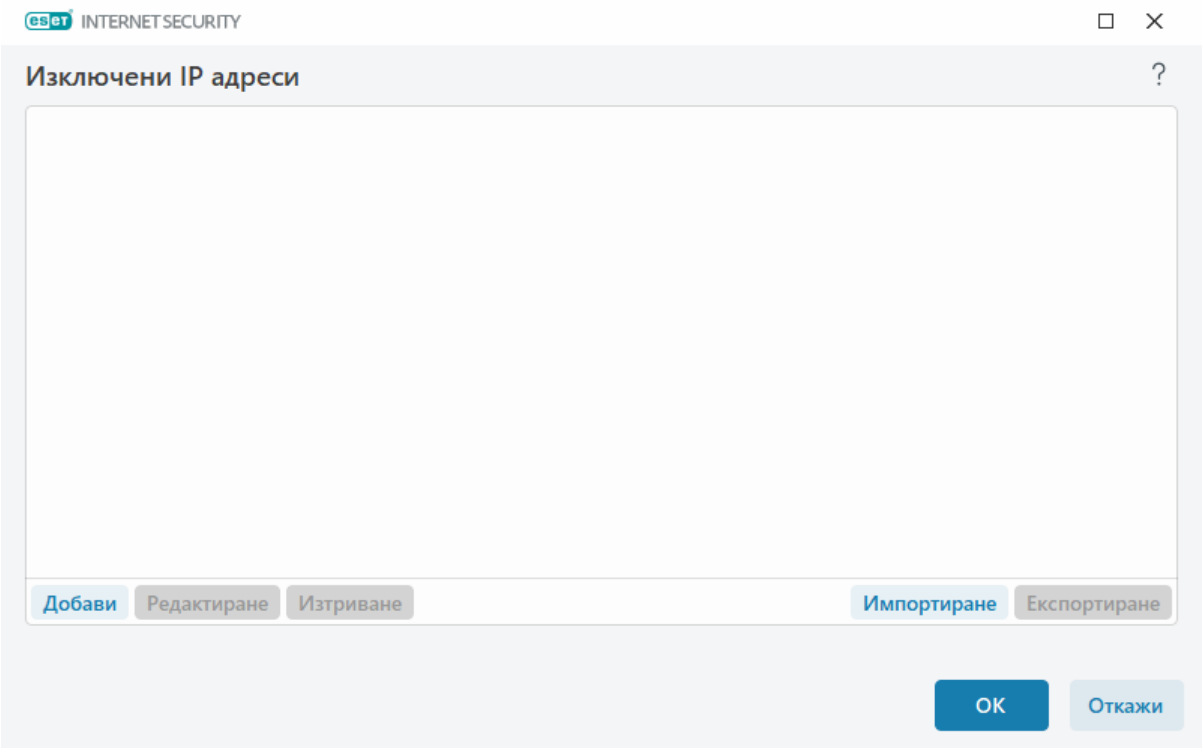
Изключени IP адреси

Записите в списъка ще се изключат от сканиране. HTTP(S)/POP3(S)/IMAP(S) комуникацията от/към избраните адреси няма да се проверява за заплахи. Препоръчително е да използвате тази опция само за надеждни адреси.

Щракнете върху **Добавяне**, за да изключите IP адрес/диапазон от адреси/подмрежа на отдалечена точка.

Щракнете върху **Редактиране**, за да промените избрания IP адрес.

Щракнете върху **Премахване**, за да премахнете избраните записи от списъка.



Примери за IP адреси

Добавяне на IPv4 адрес:
Единичен адрес – Добавя IP адрес на отделен компютър (например *192.168.0.10*).
Диапазон от адреси – Въведете IP адреса на началния и крайния адрес, за да укажете диапазона от IP адреси на няколко компютъра (например *192.168.0.1 – 192.168.0.99*).
Подмрежа – Подмрежа (група компютри), обозначена от IP адрес и маска. Например 255.255.255.0 е мрежовата маска за подмрежата 192.168.1.0. За да изключите цялата подмрежа, въведете *192.168.1.0/24*.
Добавяне на IPv6 адрес:
Един адрес – Добавя IP адреса на отделен компютър (например *2001:718:1c01:16:214:22ff:fec9:ca5*).
Подмрежа – Подмрежа (група компютри), обозначена от IP адрес и маска (например: *2002:c0a8:6301:1::1/64*).

Защита на пощенска кутия

Интегрирането на ESET Internet Security с вашата „Пощенска кутия“ повишава нивото на активна защита от злонамерен код в имейл съобщенията.

За да конфигурирате защитата на пощенската кутия, отворете Разширени настройки > **Защити** > **Защита на имейл клиенти** > **Защита на пощенска кутия**.

Разрешаване на защита на имейли чрез плъгини на клиент – когато е забранено, защитата от плъгини на имейл клиенти е изключена.

Изберете имейли за сканиране:

- **Получен имейл**
- **Изпратен имейл**

- **Прочетени имейл**
- **Модифициран имейл**

Препоръчваме ви да оставите **Разрешаване на защита на имейли чрез плъгини на клиент** е активирано. Дори ако интегрирането не е разрешено или функциониращо, имейл комуникацията все пак е защитена от Защита при придвижването на поща (IMAP/IMAPS и POP3/POP3S).

Сканиране за спам

Нежеланият имейл, наречен спам, се нарежда сред най-големите проблеми на електронната комуникация. Спамът представлява 30 процента от цялата комуникация по електронна поща. Антиспамът на имейл клиенти служи за защита срещу този проблем. Комбинирайки няколко принципа за защита на имейли, „Антиспам на имейл клиенти“ осигурява първокласно филтриране, за да поддържа пощенската ви кутия чиста. За откриване на спам важен принцип е разпознаването на нежелани имейли въз основа на предварително определени надеждни адреси (позволени) и спам адреси (блокирани).

Основният метод, използван за откриване на спам, е сканирането на свойствата на имейл съобщение. Получените съобщения се сканират за основни антиспам критерии (дефиниции в съобщението, статистически евристични методи, методи за разпознаване на алгоритми и други уникални методи), като крайният индекс определя дали съобщението е спам, или не.

Активиране на антиспам на имейл клиенти – Когато е активирано, получените съобщения ще бъдат сканирани за спам.

Използване на разширен скенер за спам – Допълнителни антиспам данни ще бъдат изтегляни периодично, увеличавайки антиспам възможностите, което води до по-добри резултати.

Регистриране на спам коефициента – Модулът за антиспам защита на ESET Internet Security назначава спам коефициент към всяко сканирано съобщение. Съобщението ще се запише в Регистъра на антиспам защитата (Главен прозорец на програмата > **Инструменти** > **Регистрационни файлове** > **Антиспам на имейл клиенти**).

- **Нищо** – резултатът от антиспам сканирането няма да бъде регистриран.
- **Класифицирани повторно и маркирани като спам** – Изберете тази опция, ако искате да запишете спам коефициент за съобщения, маркирани като SPAM.
- **Всички** – всички съобщения ще се записват в регистрационния файл със спам коефициент.

Когато щракнете върху съобщение в папката на имейла за нежелана поща, можете да изберете **Повторно класифицирай избраните съобщения като НЕ спам** и съобщението ще бъде преместено в пощенската кутия. Когато щракнете върху съобщение в пощенската кутия, което смятате за спам, изберете **Повторно класифициране на съобщенията като спам** и съобщението ще бъде преместено в папката на имейла за нежелана поща. Можете да изберете няколко съобщения и да действате едновременно върху всички тях.

Оптимизиране на обработката на прикачени файлове – ако оптимизацията е забранена, всички прикачени файлове се сканират незабавно. Може да има забавяне на производителността на имейл клиента.

Интеграции – Позволява ви да интегрирате защитата на пощенската кутия във вашия имейл клиент. Вж. Интеграции за повече информация.

Отговор – Позволява ви да персонализирате обработката на спам съобщения. Вж. Отговор за повече информация.

Интегрирания

Интегрирането на ESET Internet Security с вашия имейл клиент повишава нивото на активна защита от злонамерен код в имейл съобщенията. Ако вашият имейл клиент се поддържа, можете да разрешите интеграцията в ESET Internet Security. След интегрирането с вашия имейл клиент лентата с инструментите на ESET Internet Security се вмъква директно в имейл клиента за по-ефективна защита на имейла. За да редактирате настройките за интеграция, отворете Разширени настройки > **Защити** > **Защита на имейл клиенти** > **Защита на пощенска кутия** > **Интегриране**.

Интегриране в Microsoft Outlook – Microsoft Outlook в момента е единственият поддържан имейл клиент. Имейл защитата работи като плъгин. Основното предимство на добавката е, че тя е независима от използвания протокол. Когато имейл клиентът получи шифровано съобщение, то се дешифрира и се изпраща до програмата за сканиране за вируси. Вижте тази статия в онлайн помощника на ESET за пълен списък с поддържаните версии на Microsoft Outlook.

Разширена обработка на имейл клиент – Обработва допълнителни Outlook Messaging API (MAPI) събития: „Модифициран обект“ (`fnevObjectModified`) и „Създаден обект“ (`fnevObjectCreated`). Ако забелязвате забавяне на системата при работа с имейл клиента си, забранете тази опция.

Лента с инструменти на Microsoft Outlook

Защитата в Microsoft Outlook работи като плъгин модул. След инсталиране на ESET Internet Security тази лента с инструменти, съдържаща опциите за антивирусна защита и антиспам на имейл клиенти, се добавя към Microsoft Outlook:

Спам – маркиране на избраните съобщения като спам. След маркиране се изпраща "отпечатък" на съобщението до централен сървър, на който се съхраняват сигнатури на спам. Ако сървърът получи подобни отпечатъци от няколко потребителя, съобщението се

класифицира като нежелани за в бъдеще.

Не е спам – маркиране на избраните съобщения като такива, които не са спам.

Спам адрес (блокиран, списък със спам адреси) – добавя нов адрес на подател към списъка с адреси като „блокиран“. Всички съобщения, получени от списъка, автоматично се класифицират като спам.

> ⚠ Пазете се от фалшифициране на самоличността – фалшифициране на адреса на подателя в имейл съобщенията с цел подвеждане на получателите да прочетат или отговорят на съобщението.

Доверен адрес (позволен, списък с доверени адреси) – добавя нов адрес на подател към списъка с адреси като „позволен“. Всички съобщения, получени от позволените адреси, никога няма да бъдат автоматично класифицирани като спам.

ESET Internet Security – Щракнете двукратно върху иконата, за да отворите главния прозорец на ESET Internet Security.

Повторно сканиране на съобщенията – позволява ръчно стартиране на проверка на имейла. Можете да посочите кои съобщения да се проверят и да активирате повторно сканиране на получената поща. За повече информация вижте Защита на пощенска кутия.

Настройка на скенера – Показва опциите за настройка на Защита на пощенска кутия.

Настройка на антиспам – Показва опциите за настройка на Защита на пощенска кутия.

Адресни книги – Отваря прозореца Управление на списъци с адреси, където можете да осъществите достъп до списъците с изключени, надеждни и спам адреси.

Диалогов прозорец за потвърждение

Целта на това известие е потребителят да потвърди, че наистина иска да изпълни избраното действие и да се предотвратят евентуални грешки.

От друга страна в диалоговия прозорец има също така и опция за дезактивиране на потвържденията.

Повторно сканиране на съобщения

Лентата с инструменти на ESET Internet Security, която е интегрирана в програмите за електронна поща, позволява на потребителите да укажат няколко опции за проверка на електронната поща. Опцията **Повторно сканиране на съобщенията** предоставя два режима на сканиране:

Всички съобщения в текущата папка – сканиране на съобщенията в текущо показаната папка.

Само избраните съобщения – сканиране само на маркираните от потребителя съобщения.

Квадратчето за отметка **Сканирай повторно вече сканираните съобщения** предоставя опция за изпълнение на допълнително сканиране на съобщенията, които са вече сканирани.

Отговор

Въз основа на резултатите от сканирането на съобщенията ESET Internet Security може да премества сканирани съобщения или да добавя персонализиран текст към темата. Можете да конфигурирате тези настройки в Разширени настройки > **Защити** > **Защита на имейл клиенти** > **Защита на пощенска кутия** > **Отговор**.

Антиспам на имейл клиенти в ESET Internet Security ви позволява да конфигурирате следните параметри за съобщения:

Добавяне на текст в темата на имейла – дава възможност да добавите персонализиран низ с префикс в темата на съобщенията, които са били определени като спам. **Текстът** по подразбиране е „[SPAM]“.

Премести в спам папката – Когато е разрешено, спам съобщенията ще се преместват в папката на имейла за нежелана поща по подразбиране, а съобщенията, които са повторно класифицирани като „не е спам“, ще се преместват в пощенската кутия. Когато щракнете с десен бутон върху имейл съобщение и изберете ESET Internet Security от контекстното меню, можете да изберете една от приложимите опции.

Преместване в персонализирана папка – Когато е разрешено, спам съобщенията ще бъдат премествани в папка, посочена по-долу.

Папка – Укажете папката по избор, където да се преместват заразените имейли при откриването им.

Ако има съобщение, съдържащо откриване, по подразбиране ESET Internet Security се опитва да изчисти съобщението. Ако съобщението не може да бъде изчистено, можете да изберете **Действие, което да се предприеме, ако почистването не е възможно**:

- **Без действие** – Ако е разрешена тази опция, програмата ще намери заразените прикачени файлове, но ще остави имейлите, без да предприеме никакво действие.
- **Изтриване на имейла** – Програмата ще извести потребителя за проникването и ще изтрие съобщението.
- **Преместване на имейла в папката с изтрити елементи** – Заразените имейли ще се преместват автоматично в папката "Изтрити елементи".
- **Преместване на имейла в следната папка** (действие по подразбиране) – заразените имейли ще се преместват автоматично в указаната папка.

Папка – Укажете папката по избор, където да се преместват заразените имейли при откриването им.

Маркиране на спам съобщенията като прочетени – изберете тази опция, за да се маркират автоматично спам съобщенията като прочетени. Това ще ви помогне да насочите вниманието си върху "чистите" съобщения.

Маркиране на повторно класифицираните съобщения като непрочетени – съобщенията, които първоначално са били класифицирани като спам, а по-късно като "чисти", ще се показват като непрочетени.

След като даден имейл бъде проверен, към съобщението може да бъде прикрепено известие с резултатите от сканирането. Можете да изберете **Прикрепи допълнителни съобщения в края на получените и прочетените имейли** или **Прикрепи допълнителни съобщения в края на изпратените имейли**. Имайте предвид, че в някои редки случаи допълнителните съобщения в края може да бъдат пропуснати в проблематични HTML съобщения или ако съобщенията са фалшифицирани от злонамерен софтуер. Допълнителните съобщения в края може да се добавят към получените и прочетените имейли, към изпратените имейли (или и двете). Налични са следните опции:

• **Никога** – Не се добавят никакви допълнителни съобщения.

• **Когато възникне откриване** – само съобщения, съдържащи злонамерен софтуер, ще се маркират като проверени (по подразбиране).

• **За всички имейли при сканиране** – програмата ще прикрепя съобщения към всички сканирани имейли.

Актуализиране на темата на получения и прочетен имейл/Обновяване на тема на изпратен имейл – Разрешете тази опция, за да добавите персонализиран текст, посочен по-долу, към съобщението.

Текст за добавяне в темата на открит имейл – редактирайте този шаблон, ако искате да промените формата на префикса на темата на заразения имейл. Тази функция заменя темата на съобщението „Здравей“ в следния формат: „[откриване %DETECTIONNAME%] Здравей“. Променливата %DETECTIONNAME% представлява откритата заплаха.

Управление на адресни списъци

Функцията „Антиспам на имейл клиенти“ в ESET Internet Security ви позволява да конфигурирате различни параметри за списъците с адреси. За да конфигурирате списъци с адреси, отворете Разширени настройки > **Защити** > **Защита на имейл клиенти** > **Управление на списъци с адреси**.

Разрешаване на списъка с адреси на потребителя – Разрешете тази опция, за да активирате списъка с адреси на потребителя.

Списък с адреси на потребителя – Списък с имейл адреси, в който може да добавяте, редактирате или премахвате адреси за определяне на правилата за антиспам. Правилата в този списък ще бъдат приложени към текущия потребител.

Разрешаване на глобалния списък с адреси – Разрешете тази опция, за да активирате глобалния списък с адреси, споделен от всички потребители на това устройство.

Глобален списък с адреси – Списък с имейл адреси, в който можете да добавяте, редактирате или премахвате адреси за определяне на правилата за антиспам. Правилата в този списък ще се прилагат за всички потребители.

Автоматично позволяване и добавяне към списъка с

адреси на потребителя

Адресите от адресната книга да се третират като надеждни – Адресите от списъка ви с контакти ще се разглеждат като надеждни, без да се добавят към списъка с адреси на потребителя.

Добавяне на адресите на получателите от изходящи съобщения – Добавяне на адресите на получателите от изпратени съобщения в списъка с адреси на потребителя като позволени.

Добавяне на адресите от съобщения, повторно класифицирани като НЕ спам – Добавяне на адресите на подателите от съобщения, повторно класифицирани като НЕ спам, в списъка с адреси на потребителя като позволени.

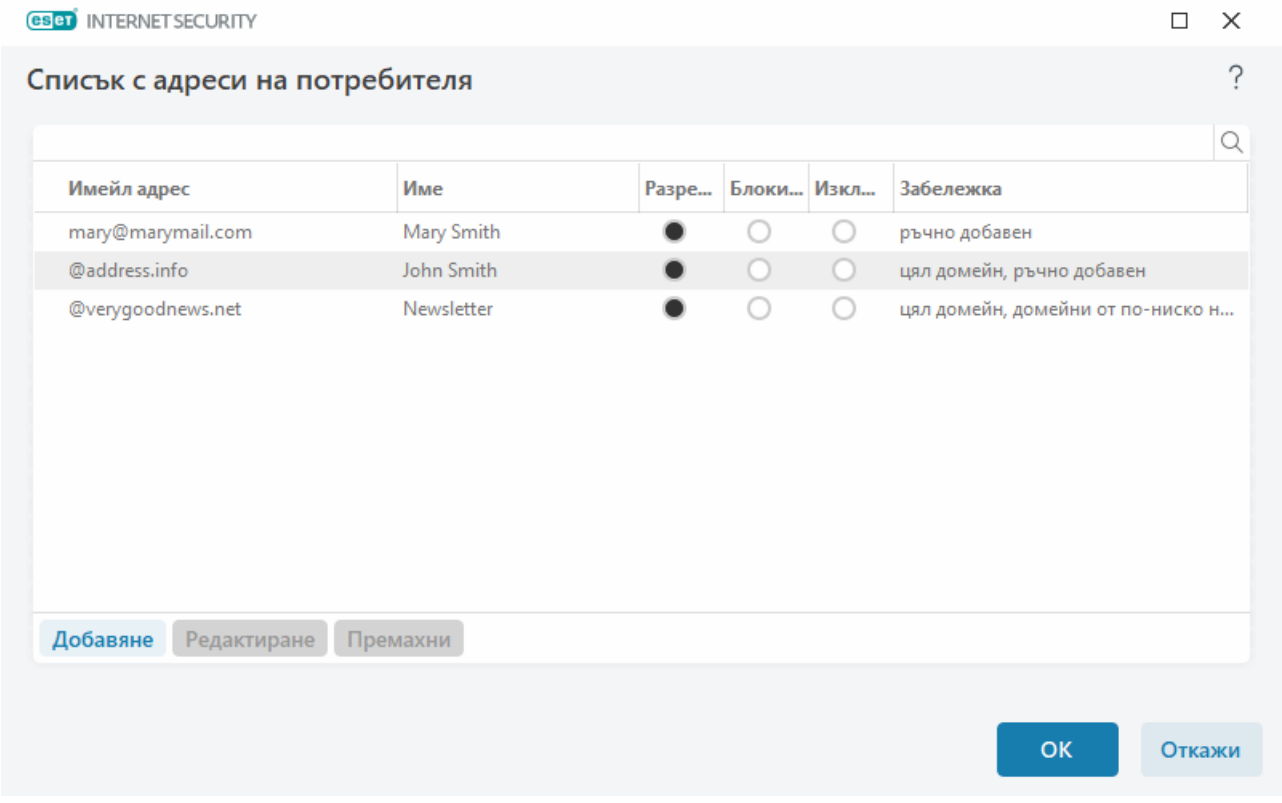
Автоматично добавяне в списъка с адреси на потребителя като изключение

Добавяне на адреси от собствените акаунти – Добавяне на вашите адреси от съществуващи акаунти за имейл клиенти в списъка с адреси на потребителя като изключение.

Списъци с адреси

За защита срещу нежелани имейли ESET Internet Security позволява да класифицирате имейл адресите в списъците с адреси.

За редактиране на списъци с адреси отворете Разширени настройки > **Защити** > **Защита на имейл клиенти** > **Управление на списъци с адреси** и щракнете върху **Редактиране** до **Списък с адреси на потребителя** или **Глобален списък с адреси**.



Колони

Имейл адрес – Адрес, за който ще се прилага правилото. Заместващи символи не се поддържат.

Име – Персонализирано име на правило.

Позволяване/Блокиране/Изключение – Радио бутони, използвани за определяне кое действие да се предприеме за имейл адреса (щракнете върху радио бутона в предпочитаната колона, за да промените бързо действието):

- **Позволяване** – Адреси, които се считат за безопасни и от които искате да получавате съобщения.
- **Блокиране** – Адреси, които се считат за опасни/спам и от които не искате да получавате съобщения.
- **Изключение** – Адреси, които винаги се проверяват за спам и които могат да бъдат фалшифицирани и използвани за изпращане на спам.

Забележка – Информация за това как е създадено правилото и дали се отнася за целия домейн/домейни от по-ниско ниво.

Управление на адресите

- **Добавяне** – Щракнете, за да добавите правило за нов адрес.
- **Редактиране** – Изберете и щракнете, за да редактирате съществуващо правило.
- **Премахване** – Изберете и щракнете, ако искате да премахнете правило от списъка с адреси.

Добавяне/редактиране на адрес

Този прозорец ви позволява да добавяте или редактирате адрес в Управление на списъци с адреси и да конфигурирате предприетото действие:

Имейл адрес – Адрес, за който ще се прилага правилото.

Име – Персонализирано име на правило.

Действие – Действие, което да се предприеме, ако имейл адресът на контакта съответства на адреса, посочен в полето **Имейл адрес**:

- **Позволяване** – Адреси, които се считат за безопасни и от които искате да получавате съобщения.
- **Блокиране** – Адреси, които се считат за опасни/спам и от които не искате да получавате съобщения.
- **Изключение** – Адреси, които винаги се проверяват за спам и които могат да бъдат фалшифицирани и използвани за изпращане на спам.

Цял домейн – изберете тази опция за прилагане на правило към целия домейн на контакта (не само към адреса, указан в полето **Имейл адрес**, а към всички имейл адреси в домейна *address.info*).

Домейни от по-ниско ниво – изберете тази опция за прилагане на правило към домейни на контакта от по-ниско ниво (*address.info* представлява домейн, а *my.address.info* представлява поддомейн).

Резултат от обработката на адреси

При добавяне на нови адреси или промяна на действието, предприето за имейл адрес, ESET Internet Security показва съобщения за известия. Съдържанието на известията се различава според действието, което се опитвате да извършите.

Сложете отметката на **Не питай повече** за автоматично извършване на действието без показване на съобщението следващия път.

ThreatSense

ThreatSense се състои от множество сложни методи за откриване на заплахи. Тази технология е проактивна, което означава, че тя осигурява защита в самото начало от появата на нова заплаха. Тя използва комбинация от анализ на кода, емулиране на кода, общи сигнатури и сигнатури за вируси, които работят съвместно за значително подобряване на защитата на системата. Модулът за сканиране може да контролира едновременно няколко потока данни, което увеличава максимално ефективността и откритите заплахи. Технологията ThreatSense също така успешно унищожава комплекти за пълен достъп.

Опциите за настройка на модула ThreatSense ви позволяват да укажете няколко параметъра за сканиране:

- Типове файлове и разширения за сканиране
- Комбинация от различни методи за откриване
- Нива на почистване и др.

За да отворите прозореца за настройка, щракнете върху **ThreatSense** в Разширени настройки за всеки модул, който използва технологията ThreatSense (вж. по-долу). Отделните сценарии за защита могат да изискват различни конфигурации. Имайки това предвид, ThreatSense може да се конфигурира индивидуално за следните модули за защита:

- Защитата на файловата система в реално време
- Сканиране в състояние на неактивност
- Начално сканиране
- Защита на документи
- Защита на имейл клиенти

- Защита на уеб достъпа
- Сканиране на компютъра

Параметрите на ThreatSense са високо оптимизирани за всеки модул и промяната им може значително да повлияе на работата на системата. Например, ако промените параметрите така, че винаги да се сканират архиваторите в реално време, или разрешите разширени евристични методи в модула за защита на файловата система в реално време, това може да доведе до забавяне на работата на системата (по принцип с тези методи се сканират само новосъздадени файлове). Препоръчваме да не променяте параметрите на ThreatSense за всички модули без този за сканиране на компютъра.

Обекти за сканиране

Този раздел позволява да укажете кои файлове и компоненти на компютъра да се сканират за проникванията.

Оперативна памет – сканиране за заплахи, атакуващи оперативната памет на системата.

Сектори за начално стартиране/UEFI – сканиране на секторите за начално зареждане за наличие на злонамерен софтуер в първия зареждащ сектор. Прочетете повече за UEFI в речника.

Имейл файлове – програмата поддържа следните разширения: DBX (Outlook Express) и EML.

Архиви – програмата поддържа следните разширения: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE и много други.

Саморазархивиращи се архиви – саморазархивиращите се архиви (SFX) са архиви, които се саморазархивират.

Архиватори в реално време – след изпълнение архиваторите в реално време (за разлика от стандартните типове архиви) се декомпресират в паметта. Освен стандартните статични компресиращи модули (UPX, yoda, ASPack, FSG и т.н.) програмата за сканиране може да разпознава няколко допълнителни типа компресиращи модули чрез използване на емулиране на код.

Опции за сканиране

Изберете методите, използвани при сканиране на системата за проникванията. Налични са следните опции:

Евристични методи – евристичните методи представляват алгоритъм за анализиране на (злонамерена) дейност на програмите. Основното предимство на тази технология е възможността за идентифициране на злонамерен софтуер, който не съществува или не е познат в предишната версия на системата за откриване. Недостатъкът е (много малка) вероятност от фалшиви сигнали.

Разширени евристични методи/ДНК сигнатури – Разширените евристични методи са уникални евристични алгоритми, разработени от ESET, оптимизирани за откриване на компютърни червеи и троянски коне и са написани на програмни езици от високо ниво. Използването на разширени евристични методи значително подобрява способността за

откриване на заплахи на продуктите на ESET. Чрез сигнатурите могат надеждно да се откриват и идентифицират вируси. С помощта на системата за автоматично обновяване новите сигнатури са достъпни само няколко часа след откриването на заплахата. Недостатъкът на сигнатурите е, че откриват само вируси, които познават (или техни леко променени версии).

Почистване

Настройките за почистване определят поведението на ESET Internet Security при почистване на обекти. Има 4 нива на почистване:

ThreatSense има следните нива на отстраняване на проблеми (т.е. почистване).

Отстраняване на проблеми в ESET Internet Security

Ниво на почистване	Описание
Винаги отстранявай откриването	Опит за отстраняване на проблеми с откриването при почистване на обекти без намеса на крайния потребител. В някои редки случаи (например в системни файлове), ако откриването не може да бъде отстранено, докладваният обект се оставя на оригиналното си местоположение.
Отстрани откриването, ако е безопасно, в противен случай го задръж	Опит за отстраняване на проблеми с откриването при почистване на обекти без намеса на крайния потребител. В някои случаи (например при системни файлове или архиви с чисти и заразени файлове), ако откриването не може да бъде отстранено, докладваният обект се оставя на оригиналното си местоположение.
Отстрани откриването, ако е безопасно, в противен попитай	Опит за отстраняване на проблеми с откриването при почистване на обекти. В някои случаи, ако не може да се извърши действие, крайният потребител получава интерактивно уведомление и трябва да избере действие за отстраняване на проблеми (например премахване или игнориране). Тази настройка се препоръчва в повечето случаи.
Винаги питай крайния потребител	Крайният потребител получава интерактивен прозорец, докато почиства обектите и трябва да избере действие за отстраняване на проблеми (например, премахване или игнориране). Това ниво е предназначено за по-напреднали потребители, които знаят кои стъпки да предприемат в случай на откриване.

Изключения

Разширението е частта от името на файла, разделена с точка. Разширението определя типа и съдържанието на файла. Този раздел на настройката на ThreatSense ви позволява да определите типовете файлове за сканиране.

Други

При конфигурирането на параметрите на модула ThreatSense за сканиране на компютъра при поискване са налични също така и следните опции в раздела **Други**:

Сканиране на алтернативни потоци данни (ADS) – Алтернативните потоци данни (ADS), използвани от файловата система NTFS, представляват асоциации на файлове и папки, които са невидими при обикновените техники на сканиране. Много проникванията се опитват да

заобиколят откриването им, като се представят за алтернативни потоци данни.

Изпълнение на фоново сканиране с нисък приоритет – всяка последователност за сканиране използва известно количество системни ресурси. Ако работите с програми, които изискват много системни ресурси, можете да активирате сканиране на фона с нисък приоритет и да запазите ресурсите за приложенията си.

Регистриране на всички обекти – дневникът на сканирането ще покаже всички сканирани файлове в саморазархивиращите се архиви – дори тези, които не са инфектирани (може да се генерират много данни за дневника на сканирането и да се увеличи размерът на файла за дневника на сканирането).

Разрешаване на оптимизация Smart – при разрешена оптимизация Smart се използват най-оптималните настройки, за да се осигури най-ефективното ниво на сканиране, като в същото време се поддържа и най-високата скорост на сканиране. Различните модули за защита сканират интелигентно, като използват различни методи на сканиране и ги прилагат към конкретни типове файлове. Ако интелигентната оптимизация е забранена, при извършване на сканиране се прилагат само дефинираните от потребителя настройки в ядрото на ThreatSense на определените модули.

Запазване на клеймото за последен достъп – изберете тази опция, за да запазите първоначалното време на достъп до сканираните файлове, вместо да ги обновявате (например при използване на системи за архивиране на данни).

Ограничения

Разделът "Ограничения" ви позволява да укажете максималния размер на обектите и нивата на влагане на архиви, които ще се сканират:

Настройки на обекта

Максимален размер на обекта – указване на максималния размер на обектите, които да се сканират. Съответният антивирусен модул ще сканира само обектите, които са по-малки от този размер. Тази опция трябва да се променя само от напреднали потребители, които имат конкретна причина да изключват от сканирането по-големи обекти. Стойност по подразбиране: неограничено.

Максимално време за сканиране за обект (сек.) – определя стойността за максимално време за сканиране на файлове в контейнерен обект (като например RAR/ZIP архив или имейл с няколко прикачени файла). Тази настройка не важи за самостоятелни файлове. Ако зададена от потребителя стойност е въведена и това време е изтекло, сканирането ще спре възможно най-скоро, независимо дали сканирането на всеки файл в контейнерен обект е завършено.
В случай на архив с големи файлове сканирането ще спре не по-рано от извличането на файл от архива (например когато дефинирана от потребителя променлива е 3 секунди, но извличането на файл отнема 5 секунди). Останалите файлове в архива няма да бъдат сканирани, когато това време изтече.
За да ограничите времето за сканиране, включително по-големи архиви, използвайте **Максимален размер на обекта** и **Максимален размер на файла в архива** (не се препоръчва поради възможни рискове за сигурността).
Стойност по подразбиране: неограничено.

Настройка на сканиране на архиви

Ниво на вложени архиви – указване на максималното ниво за сканиране на вложени архиви. стойност по подразбиране: 10.

Максимален размер на файловете в архива – тази опция ви позволява да посочите максималния размер на файловете в архивите (когато бъдат разархивирани), които ще се сканират. Максималната стойност е **3 ГБ**.

> Не е препоръчително да променяте стойностите по подразбиране. При нормални обстоятелства не би трябвало да има причина те да се променят.

Защита на уеб достъпа

Защитата на уеб достъпа ви позволява да конфигурирате разширените настройки на модула за интернет защита. Следните опции са налични в Разширени настройки > **Защити** > **Защита на уеб достъпа** > **Защита на уеб достъпа**:

Разреши защитата на уеб достъпа – Когато опцията е забранена, защитата на уеб достъпа и анти-фишинг защитата няма да се изпълняват.

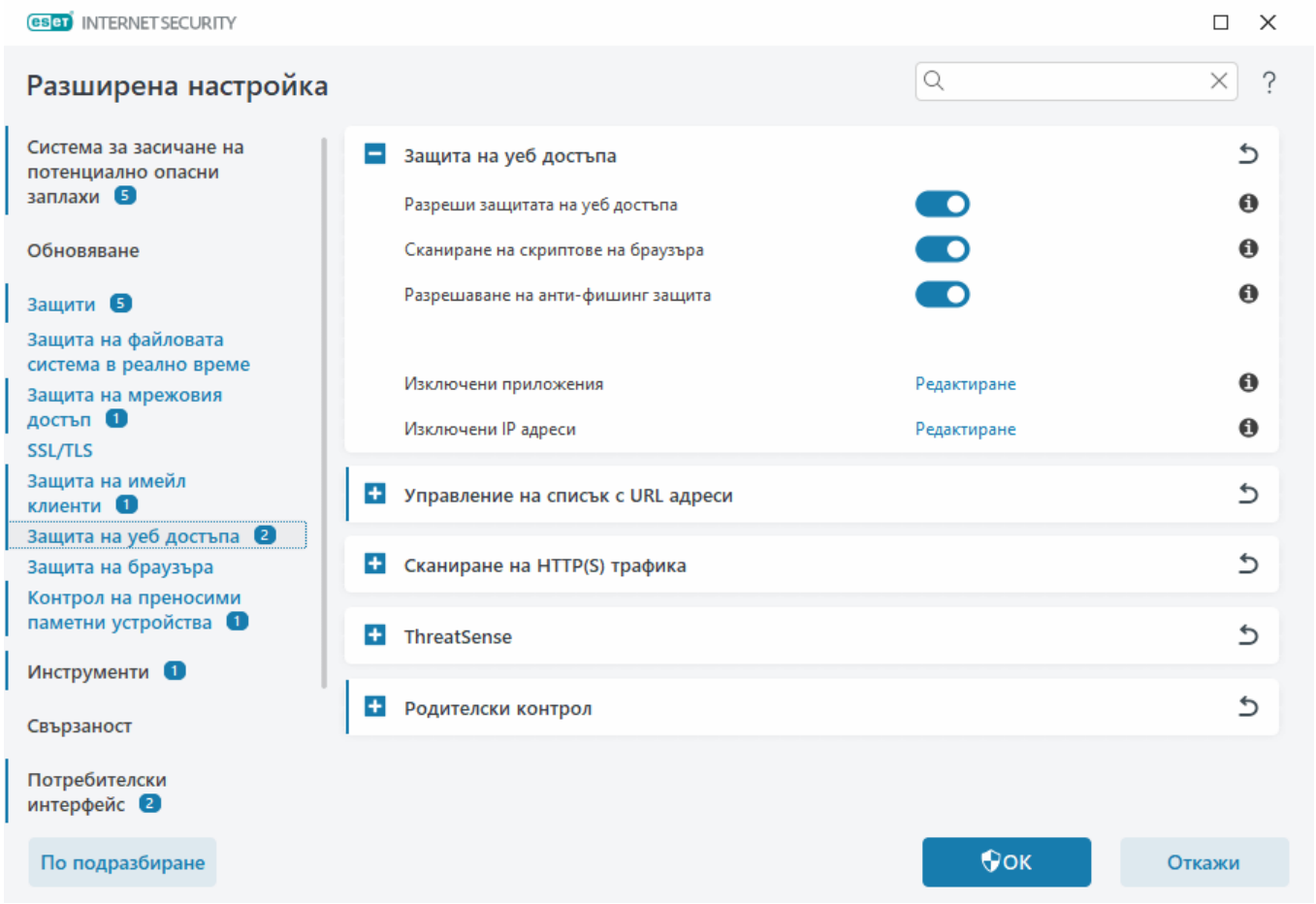
> Силно препоръчително е да оставите защитата на уеб достъпа разрешена и да не изключвате никакви приложения или IP адреси по подразбиране.

Сканиране на скриптове на браузъра – Когато е активирано, системата за засичане проверява всички JavaScript програми, изпълнявани от уеб браузъри.

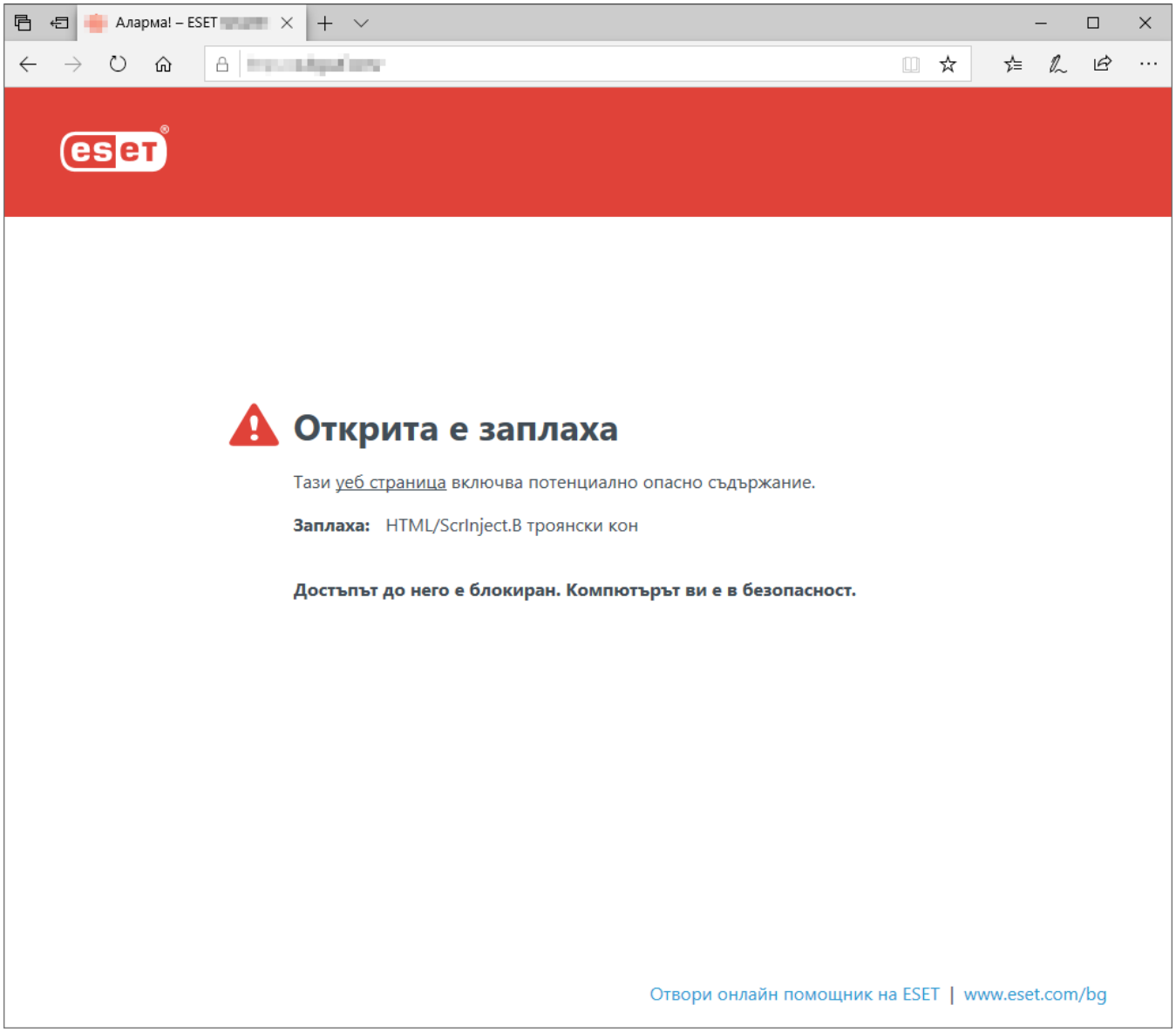
Разрешаване на анти-фишинг защита – Когато е активирано, фишинг уеб страниците са блокирани. Вижте Анти-фишинг защита за повече информация.

Изключени приложения – Позволява ви да изключите конкретни приложения от сканиране чрез защита на уеб достъпа. Полезно, когато защитата на уеб достъпа причинява проблеми със съвместимостта.

Изключени IP адреси – Позволява ви да изключите конкретни отдалечени адреси от сканиране чрез защита на уеб достъпа. Полезно, когато защитата на уеб достъпа причинява проблеми със съвместимостта.



Защита на уеб достъпа ще покаже следното съобщение в браузъра, когато уеб сайтът е блокиран:



Илюстрирани инструкции

Следните статии в онлайн помощника на ESET може да бъдат налични и на английски:

- Изключване на безопасен уеб сайт от това да бъде блокиран от функцията за защитата на уеб достъпа
- Блокиране на уеб сайт с помощта на ESET Internet Security

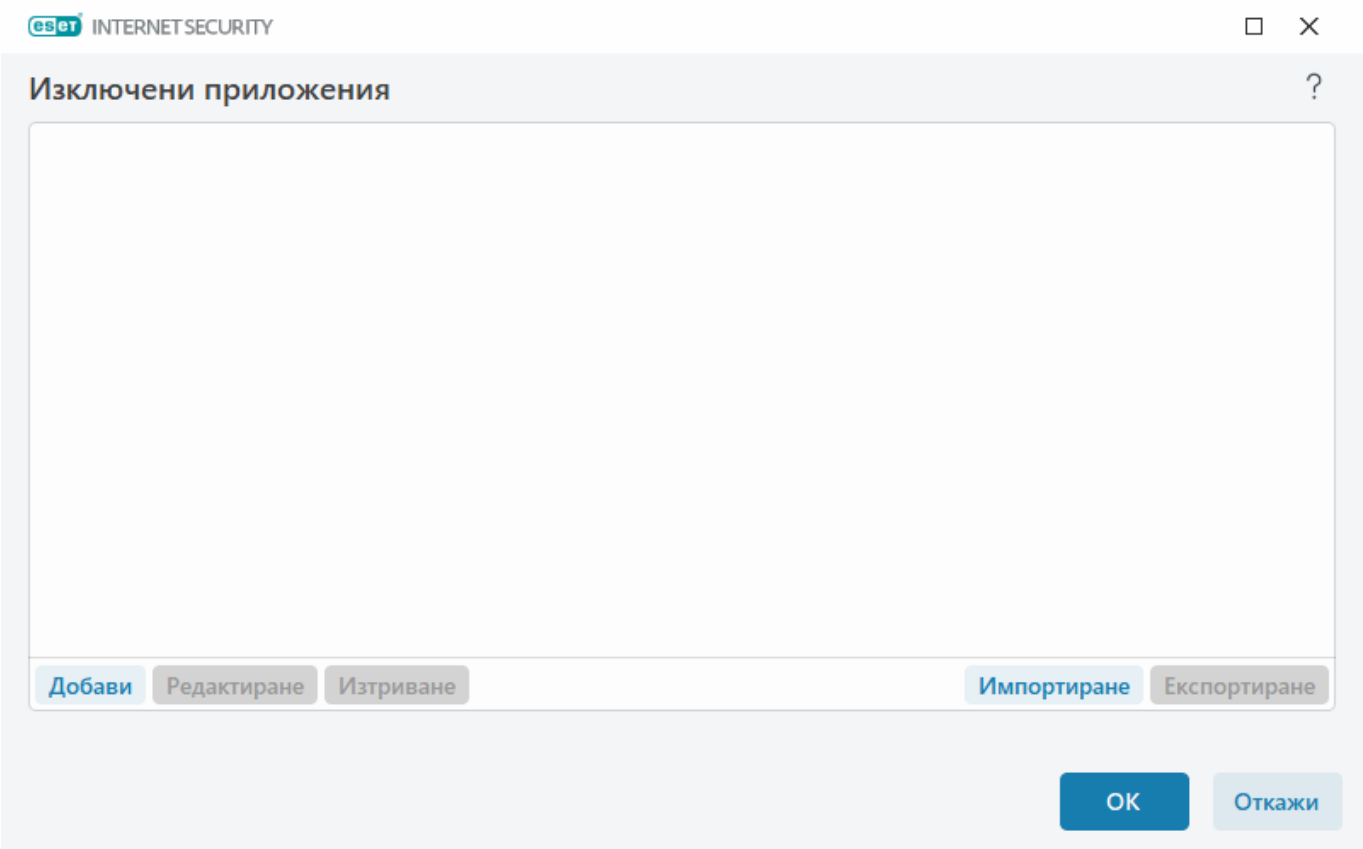
Изключени приложения

За да изключите сканирането на комуникацията за конкретни приложения, добавете ги към списъка. HTTP(S)/POP3(S)/IMAP(S) комуникацията на избраните приложения няма да се проверява за заплахи. Препоръчително е да използвате тази опция само за приложения, които не работят правилно, когато тяхната комуникация се сканира.

Тук е възможно автоматично изпълнение на приложения и услуги, когато щракнете върху **Добавяне**. Щракнете върху **...** и навигирайте до приложение, за да добавите изключение ръчно.

Редактиране – редактиране на избраните записи от списъка.

Премахване – премахване на избраните записи от списъка.



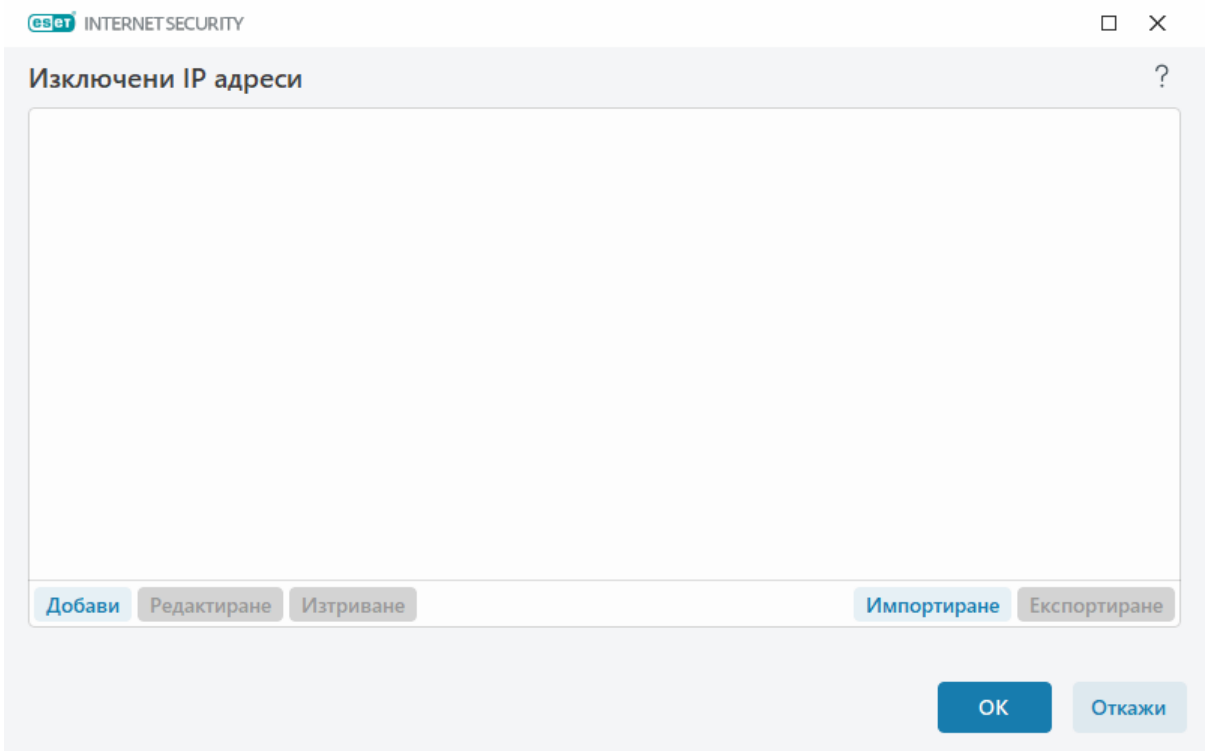
Изключени IP адреси

Записите в списъка ще се изключат от сканиране. HTTP(S)/POP3(S)/IMAP(S) комуникацията от/към избраните адреси няма да се проверява за заплахи. Препоръчително е да използвате тази опция само за надеждни адреси.

Щракнете върху **Добавяне**, за да изключите IP адрес/диапазон от адреси/подмрежа на отдалечена точка.

Щракнете върху **Редактиране**, за да промените избрания IP адрес.

Щракнете върху **Премахване**, за да премахнете избраните записи от списъка.



Примери за IP адреси

Добавяне на IPv4 адрес:

Единичен адрес – Добавя IP адрес на отделен компютър (например *192.168.0.10*).

Диапазон от адреси – Въведете IP адреса на началния и крайния адрес, за да укажете диапазона от IP адреси на няколко компютъра (например *192.168.0.1 – 192.168.0.99*).

Подмрежа – Подмрежа (група компютри), обозначена от IP адрес и маска. Например 255.255.255.0 е мрежовата маска за подмрежата 192.168.1.0. За да изключите цялата подмрежа, въведете *192.168.1.0/24*.

Добавяне на IPv6 адрес:

Един адрес – Добавя IP адреса на отделен компютър (например *2001:718:1c01:16:214:22ff:fec9:ca5*).

Подмрежа – Подмрежа (група компютри), обозначена от IP адрес и маска (например: *2002:c0a8:6301:1::1/64*).

Управление на списък с URL адреси

Управление на списък с URL адреси в Разширени настройки > **Защити** > **Защита на уеб достъпа** ви позволява да посочите HTTP адреси за блокиране, позволяване или изключване от сканиране на съдържанието.

SSL/TLS трябва да бъде разрешен, ако искате да филтрирате HTTPS адреси в допълнение към HTTP. В противен случай ще бъдат добавени само домейните на HTTPS сайтовете, които сте посетили, но не и пълния URL адрес.

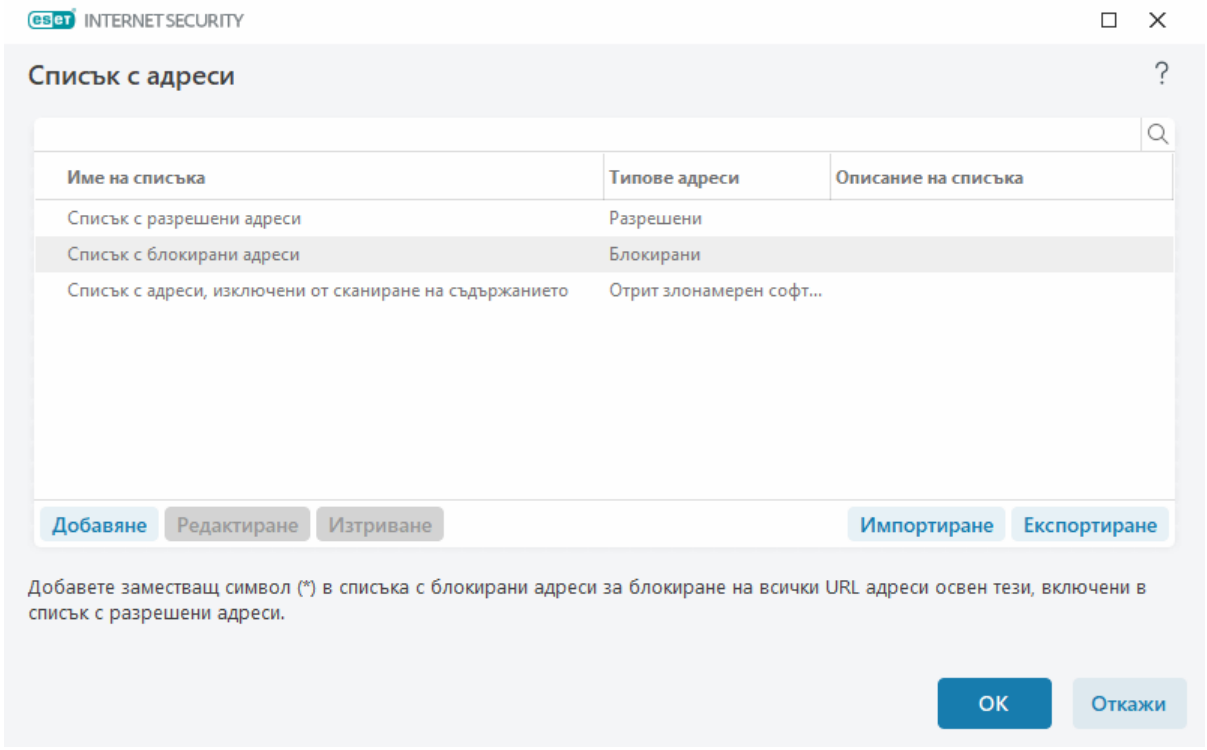
Уеб сайтовете в **Списък с блокирани адреси** няма да бъдат достъпни, освен ако не бъдат включени и в **Списък с разрешени адреси**. Уеб сайтовете в **Списък с изключени от сканиране на съдържанието адреси** не се сканират за злонамерен код при осъществяването на достъп до тях.

Ако искате да блокирате всички HTTP адреси освен адресите, включени в активния **Списък с**

разрешени адреси, добавете * към активния **Списък с блокирани адреси**.

Специалните символи * (звездичка) и ? (въпросителен знак) могат да се използват в списъци. Звездичката замества всеки низ със знаци, а въпросителният знак – всеки символ. Обръщайте специално внимание при указването на изключени адреси, тъй като списъкът трябва да съдържа само надеждни и безопасни адреси. По същия начин трябва да се уверите, че сте използвали правилно символите * и ? в списъка. Вижте Добавяне на HTTP адрес/маска на домейн за информация за начините за безопасно съотнасяне на цялостен домейн, включително всички поддомейни. За да активирате даден списък, изберете **Списъкът е активен**. Ако искате да получавате известие при въвеждане на адрес от текущия списък, изберете **Известявай при прилагане**.

> **Адреси, считани за надеждни от ESET**
> Ако **Не сканирай трафика с домейни, считани за надеждни от ESET** е разрешено с SSL/TLS, домейните в списъка с разрешени адреси, управляван от ESET, няма да бъдат засегнати от конфигурацията за управление на списъци с URL адреси.



Контролни елементи

Добавяне – Създава нов списък в допълнение към предварително зададените. Това може да е полезно, ако искате да разделите логически различни групи адреси. Може например един списък с блокирани адреси да включва адреси от външен публичен списък със забранени адреси, а втори списък да съдържа ваш собствен списък със забранени адреси, като по този начин можете лесно да обновявате външния списък, запазвайки непроменен вашия собствен.

Редактиране – Променя съществуващи списъци. Използвайте тази опция за добавяне или премахване на адреси.

Изтриване – Изтрива съществуващи списъци. Тази опция е налична само за списъци, създадени чрез опцията **Добавяне**, но не и за списъците по подразбиране.

Списък с адреси

В този раздел можете да укажете списъци с HTTP(S) адреси, които да се блокират, разрешават или изключват от проверка.

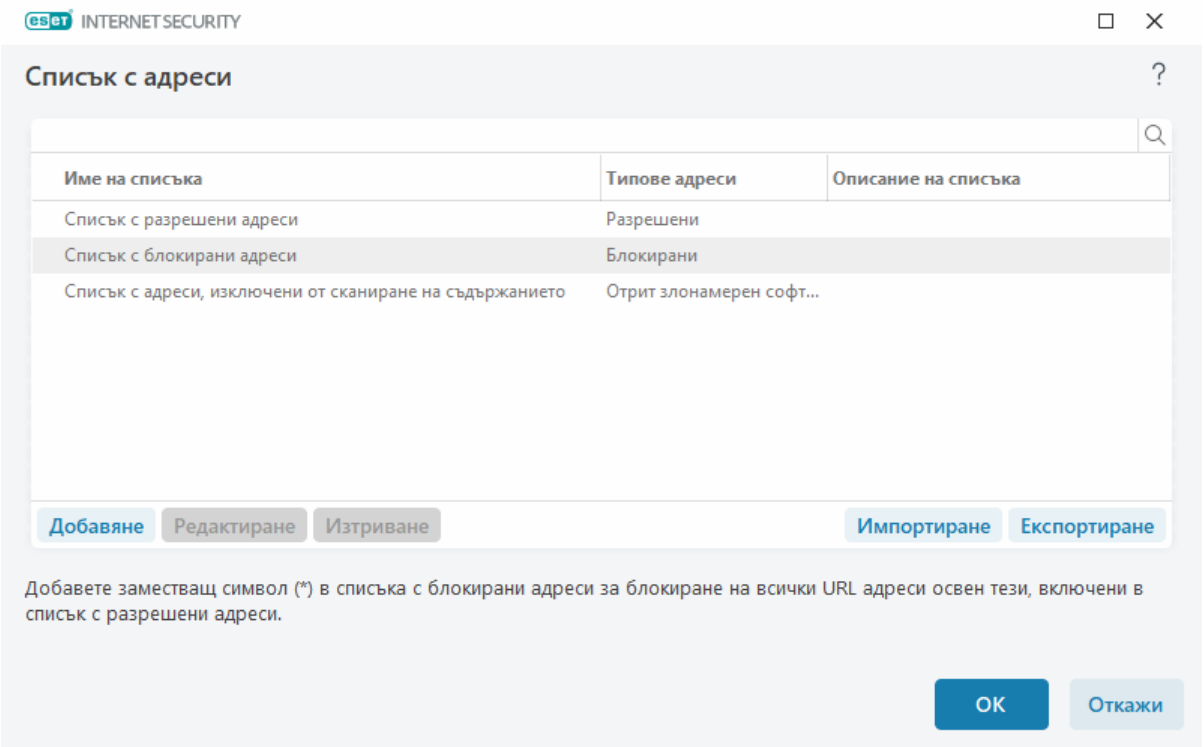
По подразбиране са налични следните три списъка:

• **Списък с адреси, изключени от сканиране на съдържанието** – за никой от добавените към списъка адреси няма да се извършва проверка за злонамерен код.

• **Списък с разрешени адреси** – ако е включена опцията за разрешаване на достъпа само до HTTP адресите в списъка с разрешени адреси и списъкът с блокирани адреси съдържа * (съответствие с всичко), потребителят ще има достъп само до адресите от този списък. Адресите в този списък са разрешени дори ако са включени в списъка с блокирани адреси.

• **Списък с блокирани адреси** – На потребителя не се разрешава достъп до посочените в списъка адреси, освен ако не са включени и в списъка с разрешени адреси.

Щракнете върху **Добавяне**, за да създадете нов списък. За да премахнете избраните списъци, щракнете върху **Премахване**.



Илюстрирани инструкции

Следните статии в онлайн помощника на ESET може да бъдат налични и на английски:

• Изключване на безопасен уеб сайт от това да бъде блокиран от функцията за защитата на уеб достъпа

• Блокиране на уеб сайт чрез продукт на ESET за домашна употреба за Windows

За повече информация вижте Управление на списъци с URL адреси.

Създаване на нов списък с адреси

Този диалогов прозорец ви дава възможност да конфигурирате нов списък с URL адреси/маски, които ще бъдат блокирани, позволени или изключени от проверка.

Можете да конфигурирате следните опции:

Тип списък с адреси – Налични са три типа списъци:

• **Отрит злонамерен софтуер е игнориран** – за никой от добавените към списъка адреси няма да се извършва проверка за злонамерен код.

• **Блокиран** – достъпът до адреси, посочени в този списък, ще бъде блокиран.

• **Позволен** – достъпът до адреси, посочени в този списък, ще бъде позволен. Адресите в този списък са позволени дори ако съответстват на списъка с блокирани адреси.

Име на списъка – въведете името на списъка. Това поле няма да е достъпно, когато редактирате един от предварително определените списъци.

Описание на списъка – Въведете кратко описание на списъка (по желание). Няма да е достъпен, когато редактирате един от предварително определения списък.

За да активирате списък, изберете **Списъкът е активен** до съответния списък. Ако искате да получавате известие, когато се използва конкретен списък при достъп до уеб сайтове, изберете **Известявай при прилагане**. Например ще получавате известие, когато даден уеб сайт бъде блокиран или позволен, понеже е включен в списък с блокирани или позволени адреси. Известието ще включва името на списъка.

Детайлност на регистрирането – информация за конкретния списък, който се използва при достъп до уебсайтове, може да бъде записана в регистрационните файлове.

Контролни елементи

Добавяне – добавяне на нов URL адрес в списъка (въвеждайте множество стойности чрез разделител).

Редактиране – промяна на съществуващ адрес в списъка. Достъпно е само за адреси, създадени чрез **Добавяне**.

Премахване – Изтрива съществуващи адреси в списъка. Достъпно е само за адреси, създадени чрез **Добавяне**.

Импортиране – импортиране на файл с URL адреси (разделяйте стойностите с нов ред, например в *.txt с помощта на UTF-8).

Как се добавя URL маска

Прегледайте инструкциите в този диалогов прозорец, преди да въведете желания адрес/маска на домейн.

ESET Internet Security позволява на потребителите да блокират достъпа до конкретни уеб сайтове, както и показването на тяхното съдържание в браузъра. Освен това тя позволява на потребителите да посочат адреси, които да се изключват от проверка. Ако цялото име на отдалечения сървър не е известно или потребителят иска да посочи цяла група от отдалечени сървъри, могат да се използват т.нар. "маски", за да се укаже групата. Маските включват символите "?" и "*":

- Използвайте "?", за да заместите един символ
- Използвайте "*", за да заместите текстов низ.

Например, *.c?m обхваща всички адреси, при които втората част започва с буквата "c" и завършва на буквата "m" и съдържа неизвестен символ между тях (.com, .cam и т.н.)

Водеща последователност с „*.“ се третира по специален начин, ако се използва в началото на името на домейна. На първо място, заместващият символ „*“ не съответства на наклонената черта (/) в този случай. По този начин се избягва заобикалянето на маската, например маската **.domain.com* няма да съвпадне с *http://anydomain.com/anypath#.domain.com* (подобен суфикс може да бъде добавен към всеки URL адрес, без това да влияе на изтеглянето). И на второ място, в този специален случай „*.“ също съответства на празен низ. Това е така, за да се позволи съответствие на целия домейн, включително всички поддомейни с една маска. Например маската **.domain.com* също така съвпада с *http://domain.com*. Няма да е правилно да се използва **domain.com*, тъй като ще съвпадне също и с *http://anotherdomain.com*.

Сканиране на HTTP(S) трафика

По подразбиране ESET Internet Security е конфигуриран да сканира HTTP и HTTPS трафика, който се използва от интернет браузъри и други приложения. Трябва да забраните сканирането на трафика само ако имате проблеми със софтуер на трета страна и искате да знаете дали проблемът е причинен от ESET Internet Security.

Разрешаване на сканиране на HTTP трафика – HTTP трафикът винаги се следи на всички портове за всички приложения.

Разрешаване на сканиране на HTTPS трафика – HTTPS трафикът използва криптиран канал за прехвърляне на информация между сървър и клиент. ESET Internet Security проверява комуникацията с помощта на протоколите SSL (Secure Socket Layer (Слой със защитени сокети) и TLS (Transport Layer Security (Защита на транспортен слой). Програмата ще сканира само трафика през портовете, определени в **Портове, използвани от HTTPS протокол**, независимо от версията на операционната система (можете да добавите портове към предварително дефинираните 443 и 0-65535).

ThreatSense

ThreatSense се състои от множество сложни методи за откриване на заплахи. Тази технология е проактивна, което означава, че тя осигурява защита в самото начало от появата на нова заплаха. Тя използва комбинация от анализ на кода, емулиране на кода, общи сигнатури и сигнатури за вируси, които работят съвместно за значително подобряване на защитата на системата. Модулът за сканиране може да контролира едновременно няколко потока данни,

което увеличава максимално ефективността и откритите заплахи. Технологията ThreatSense също така успешно унищожава комплекти за пълен достъп.

Опциите за настройка на модула ThreatSense ви позволяват да укажете няколко параметъра за сканиране:

- Типове файлове и разширения за сканиране
- Комбинация от различни методи за откриване
- Нива на почистване и др.

За да отворите прозореца за настройка, щракнете върху **ThreatSense** в Разширени настройки за всеки модул, който използва технологията ThreatSense (вж. по-долу). Отделните сценарии за защита могат да изискват различни конфигурации. Имайки това предвид, ThreatSense може да се конфигурира индивидуално за следните модули за защита:

- Защитата на файловата система в реално време
- Сканиране в състояние на неактивност
- Начално сканиране
- Защита на документи
- Защита на имейл клиенти
- Защита на уеб достъпа
- Сканиране на компютъра

Параметрите на ThreatSense са високо оптимизирани за всеки модул и промяната им може значително да повлияе на работата на системата. Например, ако промените параметрите така, че винаги да се сканират архиваторите в реално време, или разрешите разширени евристични методи в модула за защита на файловата система в реално време, това може да доведе до забавяне на работата на системата (по принцип с тези методи се сканират само новосъздадени файлове). Препоръчваме да не променяте параметрите на ThreatSense за всички модули без този за сканиране на компютъра.

Обекти за сканиране

Този раздел позволява да укажете кои файлове и компоненти на компютъра да се сканират за проникванията.

Оперативна памет – сканиране за заплахи, атакуващи оперативната памет на системата.

Сектори за начално стартиране/UEFI – сканиране на секторите за начално зареждане за наличие на злонамерен софтуер в първия зареждащ сектор. Прочетете повече за UEFI в речника.

Имейл файлове – програмата поддържа следните разширения: DBX (Outlook Express) и EML.

Архиви – програмата поддържа следните разширения: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG,

LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE и много други.

Саморазархивиращи се архиви – саморазархивиращите се архиви (SFX) са архиви, които се саморазархивират.

Архиватори в реално време – след изпълнение архиваторите в реално време (за разлика от стандартните типове архиви) се декомпресират в паметта. Освен стандартните статични компресиращи модули (UPX, yoda, ASPack, FSG и т.н.) програмата за сканиране може да разпознава няколко допълнителни типа компресиращи модули чрез използване на емулиране на код.

Опции за сканиране

Изберете методите, използвани при сканиране на системата за проникванията. Налични са следните опции:

Евристични методи – евристичните методи представляват алгоритъм за анализиране на (злонамерена) дейност на програмите. Основното предимство на тази технология е възможността за идентифициране на злонамерен софтуер, който не съществува или не е познат в предишната версия на системата за откриване. Недостатъкът е (много малка) вероятност от фалшиви сигнали.

Разширени евристични методи/ДНК сигнатури – Разширените евристични методи са уникални евристични алгоритми, разработени от ESET, оптимизирани за откриване на компютърни червеи и троянски коне и са написани на програмни езици от високо ниво. Използването на разширени евристични методи значително подобрява способността за откриване на заплахи на продуктите на ESET. Чрез сигнатурите могат надеждно да се откриват и идентифицират вируси. С помощта на системата за автоматично обновяване новите сигнатури са достъпни само няколко часа след откриването на заплахата. Недостатъкът на сигнатурите е, че откриват само вируси, които познават (или техни леко променени версии).

Почистване

Настройките за почистване определят поведението на ESET Internet Security при почистване на обекти. Има 4 нива на почистване:

ThreatSense има следните нива на отстраняване на проблеми (т.е. почистване).

Отстраняване на проблеми в ESET Internet Security

Ниво на почистване	Описание
Винаги отстранявай откриването	Опит за отстраняване на проблеми с откриването при почистване на обекти без намеса на крайния потребител. В някои редки случаи (например в системни файлове), ако откриването не може да бъде отстранено, докладваният обект се оставя на оригиналното си местоположение.
Отстрани откриването, ако е безопасно, в противен случай го задръж	Опит за отстраняване на проблеми с откриването при почистване на обекти без намеса на крайния потребител. В някои случаи (например при системни файлове или архиви с чисти и заразени файлове), ако откриването не може да бъде отстранено, докладваният обект се оставя на оригиналното си местоположение.

Ниво на почистване	Описание
Отстрани откриването, ако е безопасно, в противен попитай	Опит за отстраняване на проблеми с откриването при почистване на обекти. В някои случаи, ако не може да се извърши действие, крайният потребител получава интерактивно уведомление и трябва да избере действие за отстраняване на проблеми (например премахване или игнориране). Тази настройка се препоръчва в повечето случаи.
Винаги питай крайния потребител	Крайният потребител получава интерактивен прозорец, докато почиства обектите и трябва да избере действие за отстраняване на проблеми (например, премахване или игнориране). Това ниво е предназначено за по-напреднали потребители, които знаят кои стъпки да предприемат в случай на откриване.

Изключения

Разширението е частта от името на файла, разделена с точка. Разширението определя типа и съдържанието на файла. Този раздел на настройката на ThreatSense ви позволява да определите типовете файлове за сканиране.

Други

При конфигурирането на параметрите на модула ThreatSense за сканиране на компютъра при поискване са налични също така и следните опции в раздела **Други**:

Сканиране на алтернативни потоци данни (ADS) – Алтернативните потоци данни (ADS), използвани от файловата система NTFS, представляват асоциации на файлове и папки, които са невидими при обикновените техники на сканиране. Много проникванията се опитват да заобиколят откриването им, като се представят за алтернативни потоци данни.

Изпълнение на фоново сканиране с нисък приоритет – всяка последователност за сканиране използва известно количество системни ресурси. Ако работите с програми, които изискват много системни ресурси, можете да активирате сканиране на фона с нисък приоритет и да запазите ресурсите за приложенията си.

Регистриране на всички обекти – дневникът на сканирането ще покаже всички сканирани файлове в саморазархивиращите се архиви – дори тези, които не са инфектирани (може да се генерират много данни за дневника на сканирането и да се увеличи размерът на файла за дневника на сканирането).

Разрешаване на оптимизация Smart – при разрешена оптимизация Smart се използват най-оптималните настройки, за да се осигури най-ефективното ниво на сканиране, като в същото време се поддържа и най-високата скорост на сканиране. Различните модули за защита сканират интелигентно, като използват различни методи на сканиране и ги прилагат към конкретни типове файлове. Ако интелигентната оптимизация е забранена, при извършване на сканиране се прилагат само дефинираните от потребителя настройки в ядрото на ThreatSense на определените модули.

Запазване на клеймото за последен достъп – изберете тази опция, за да запазите първоначалното време на достъп до сканираните файлове, вместо да ги обновявате (например при използване на системи за архивиране на данни).

Ограничения

Разделът "Ограничения" ви позволява да укажете максималния размер на обектите и нивата на влагане на архиви, които ще се сканират:

Настройки на обекта

Максимален размер на обекта – указване на максималния размер на обектите, които да се сканират. Съответният антивирусен модул ще сканира само обектите, които са по-малки от този размер. Тази опция трябва да се променя само от напреднали потребители, които имат конкретна причина да изключват от сканирането по-големи обекти. Стойност по подразбиране: неограничено.

Максимално време за сканиране за обект (сек.) – определя стойността за максимално време за сканиране на файлове в контейнерен обект (като например RAR/ZIP архив или имейл с няколко прикачени файла). Тази настройка не важи за самостоятелни файлове. Ако зададена от потребителя стойност е въведена и това време е изтекло, сканирането ще спре възможно най-скоро, независимо дали сканирането на всеки файл в контейнерен обект е завършено.
В случай на архив с големи файлове сканирането ще спре не по-рано от извличането на файл от архива (например когато дефинирана от потребителя променлива е 3 секунди, но извличането на файл отнема 5 секунди). Останалите файлове в архива няма да бъдат сканирани, когато това време изтече.
За да ограничите времето за сканиране, включително по-големи архиви, използвайте **Максимален размер на обекта** и **Максимален размер на файла в архива** (не се препоръчва поради възможни рискове за сигурността).
Стойност по подразбиране: неограничено.

Настройка на сканиране на архиви

Ниво на вложени архиви – указване на максималното ниво за сканиране на вложени архиви. стойност по подразбиране: 10.

Максимален размер на файловете в архива – тази опция ви позволява да посочите максималния размер на файловете в архивите (когато бъдат разархивирани), които ще се сканират. Максималната стойност е **3 ГБ**.

> Не е препоръчително да променяте стойностите по подразбиране. При нормални обстоятелства не би трябвало да има причина те да се променят.

Родителски контрол

Опцията **Разрешаване на родителски контрол** интегрира родителски контрол в ESET Internet Security. Щракнете върху **Редактиране** до Потребителски акаунти, за да свържете потребителски акаунти в Windows, използвани от функцията за родителски контрол, с конкретни потребители, за да ограничите техния достъп до неподходящо или вредно съдържание в интернет.

Потребителски акаунти

В Разширени настройки > **Защити** > **Защита на уеб достъпа** > **Родителски контрол** > **Потребителски акаунти** > **Редактиране** може да свържете потребителски акаунти с Windows, използвани от „Родителски контрол“ с конкретни потребители, за да се ограничи техния достъп до неподходящо или вредно съдържание в интернет.

Колони

Акаунт в Windows – Името на потребителя.

Разрешено – Когато тази опция е разрешена, родителските контроли за конкретен потребителски акаунт са активни.

Домейн – Име на домейна, към който принадлежи даден потребител.

Дата на раждане – Възраст на потребителя, на когото принадлежи акаунтът.

Контролни елементи

Добавяне – Ще се покаже диалоговият прозорец Работа с потребителски акаунти.

Редактиране – тази опция позволява да редактирате избраните акаунти.

Премахване – премахване на избрания акаунт.

Обновяване – Ако сте добавили потребителски акаунт, ESET Internet Security може да обнови списъка с потребителски акаунти, без да е необходимо да отваряте повторно този прозорец.

Настройки на потребителски акаунт

Прозорецът има три раздела:

Общи

Активирайте превключвателя до **Разрешено**, за да включите родителския контрол за акаунта в Windows, избран по-долу.

Първо, **изберете**Windows акаунт от компютъра. Ограниченията, зададени в родителския контрол, засягат само стандартните акаунти в Windows. Администраторските акаунти могат да заместят ограниченията.

Ако акаунтът се използва от родител, изберете **Родителски акаунт**.

Задайте **Дата на раждане на детето** за акаунта, за да определите неговото ниво на достъп и да зададете правила за достъп до подходящи за възрастта му уеб страници.

Детайлност на регистрирането

ESET Internet Security записва всички важни събития в регистрационен файл, който може да бъде прегледан директно от главното меню. Щракнете върху **Инструменти** > **Регистрационни**

файлове, след което изберете **Родителски контрол** от падащото меню **Дневник**.

• **Диагностика** – регистриране на информацията, необходима за прецизна настройка на програмата.

• **Информативни** – записва информативни съобщения, включително позволени и блокирани изключения, плюс всички записи по-горе.

• **Предупреждение** – регистриране на съобщения за критични грешки и предупреждения.

• **Няма** – няма да се записват регистрационни файлове.

Изключения

Създаването на изключение може да позволи или откаже достъп на потребител до уеб сайтове, които не са включени в списъка с изключения. Това е полезно, ако искате да контролирате достъпа до конкретни уеб сайтове, вместо да използвате категории. Изключенията, създадени за един акаунт, могат да бъдат копирани и използвани за друг акаунт. Това може да е полезно, когато искате да създадете идентични правила за деца на една и съща възраст.

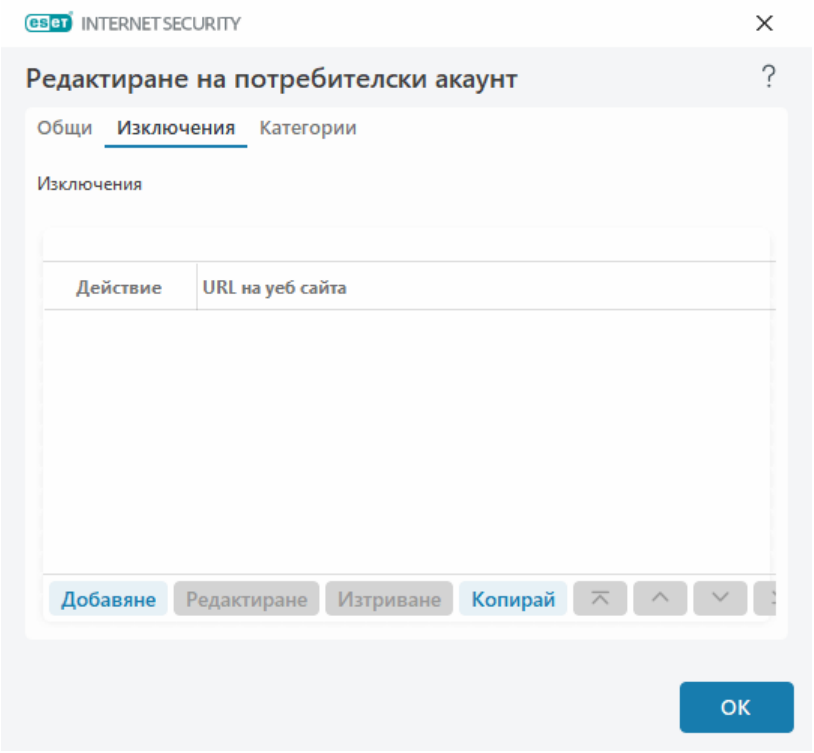
Щракнете върху **Добавяне**, за да създадете ново изключение. Укажете **Действие** (напр. **Блокиране**) с помощта на падащото меню, въведете **URL адрес на уеб сайта**, за който се отнася изключението, след което щракнете върху **OK**. Изключението ще бъде добавено в списъка със съществуващи изключения и състоянието му ще бъде показано.

Добавяне – Създаване на ново изключение.

Редактиране – Можете да редактирате **URL адрес на уеб сайта** или **Действие** на избраното изключение.

Премахване – премахва избраното изключение.

Копиране – От падащото меню изберете потребител, от който искате да копирате създадено изключение.

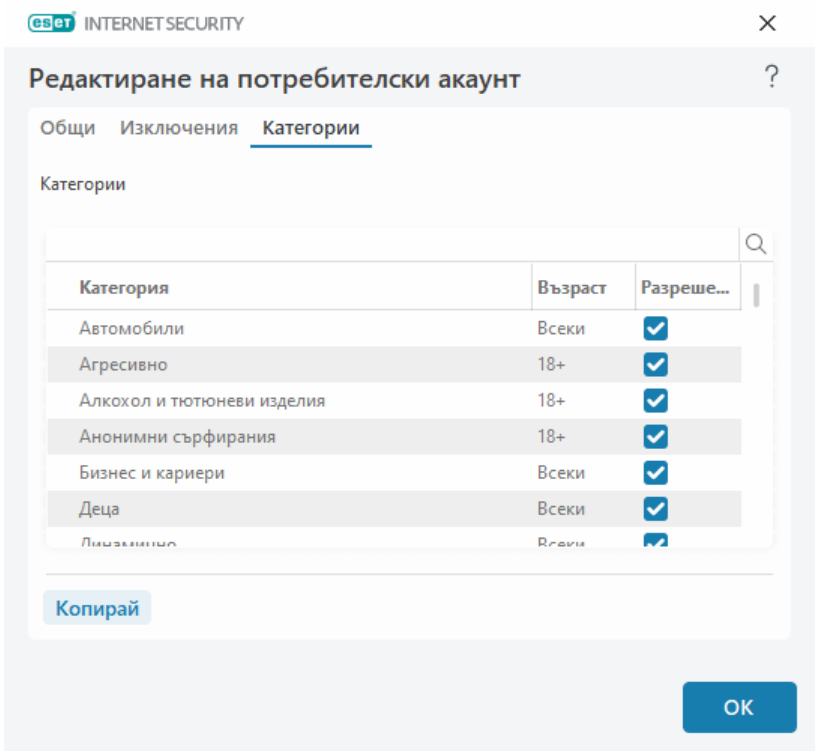


Дефинираните изключения заместват категориите, определени за избраните акаунти. Например, ако акаунтът е с блокирана категория **Новини**, но сте указали уеб страница за новини като разрешено изключение, акаунтът ще има достъп до разрешената уеб страница. Можете да прегледате промените, извършени тук, в раздела Изключения.

Категории

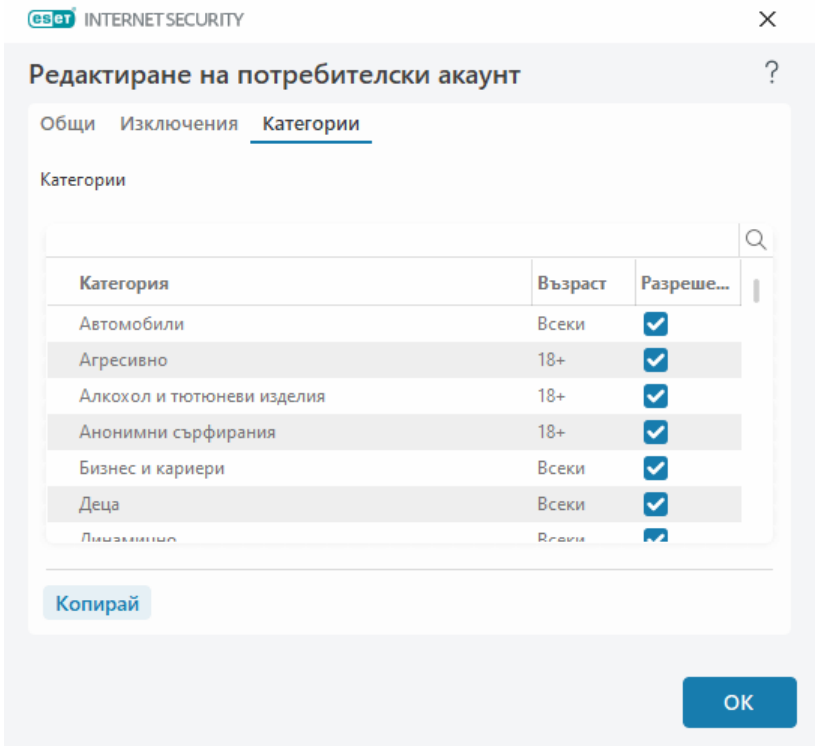
В раздела **Категории** можете да определите общите категории уеб сайтове, които искате да блокирате или разрешите за всеки акаунт. Изберете квадратчето за отметка до дадена категория, за да я разрешите. Ако оставите квадратчето празно, категорията няма да бъде разрешена за този акаунт.

Копиране – Позволява ви да копирате списък с блокирани или разрешени категории от съществуващ променен акаунт.



Категории

Поставете отметка в колоната **Разрешено** до дадена категория, за да я позволите. Ако оставите квадратчето празно, категорията няма да бъде позволена за този акаунт.



Ето някои примери на категории (групи), с които потребителите може да не са запознати:

- **Разни** – Обикновено частни (локални) IP адреси, като например интранет, 127.0.0.0/8, 192.168.0.0/16, и т.н. Когато получите код за грешка 403 или 404, уеб сайтът също ще съответства на тази категория.

• **Неразрешени** – Тази категория включва уеб страници, които не са разрешени поради грешка при свързване със системата на базата данни на родителския контрол.

• **Без категория** – Неизвестни уеб страници, които все още не са в базата данни на родителския контрол.

• **Динамични** – Уеб страници, които пренасочват към други страници на други уеб сайтове.

Защита на браузъра

Защитата на браузъра е друг слой защита за вашата защита и поверителност, който предпазва паметта на браузъра от проверка от други процеси, увеличава защитата срещу програмата за записване на натиснатите клавиши и предотвратява поставянето на данни, свързани с онлайн плащания, променени от злонамерен софтуер, от клипборда в защитения браузър. За да конфигурирате „Защита на браузъра“, отворете Разширени настройки > **Защити** > **Защита на браузъра** и изберете от следните опции за конфигуриране:

- Безопасно банкиране и сърфиране
- Списък с разрешени за защита на браузъра
- Рамка на браузъра

Безопасно банкиране и сърфиране

Можете да конфигурирате Безопасно банкиране и сърфиране в Разширена настройка > **Защити** > **Защита на браузъра** > **Безопасно банкиране и сърфиране**.

Безопасно банкиране и сърфиране

Разрешаване на безопасно банкиране и сърфиране – когато безопасното банкиране и сърфиране е разрешено, всички поддържани уеб браузъри ще стартират в защитен режим по подразбиране.

Защита на браузъра

Разрешете **Защитаване на всички браузъри**, за да стартирате всички поддържани уеб браузъри в защитен режим.

Режим на инсталиране на разширения – От падащото меню можете да изберете кои разширения ще бъде позволено да инсталирате в браузър, защитен от ESET:

• **Основни разширения** – Само най-важните разширения, разработени от конкретен производител на браузъри.

• **Всички разширения** – Всички разширения, поддържани от конкретен браузър.

Промяната на режима на инсталиране на разширението не влияе на инсталираните преди това разширения на браузъра:

Защитен браузър

Подобрена защита на паметта – ако е разрешена, паметта на защитения браузър ще бъде защитена от проверка от други процеси.

Защита на клавиатурата – ако е разрешено, информацията, въведена чрез клавиатурата в защитен браузър, ще бъде скрита от други приложения. Това увеличава защитата срещу програми, регистриращи въведени символи.

Защита на клипборда – ако е разрешено, ESET Internet Security ще предотврати поставянето на каквито и да било данни, свързани с онлайн плащания, модифицирани от зловреден софтуер, от клипборда в защитения браузър. Това гарантира защита срещу потенциални промени, направени от злонамерен софтуер.

Рамка на браузъра – Персонализирайте настройките на дисплея за рамката на браузъра в защитени браузъри.

Списък с разрешени за защита на браузъра – Управление на файлове, добавени към списъка с разрешени за защита на браузъра.

Поверителност и защита на браузъра

Разрешаване на поверителност и защита на браузъра – ако е дезактивирано, разширението за поверителност и защита на браузъра ще бъде деинсталирано от всички поддържани браузъри във всички акаунти в Windows.

Показване на известия за защита на поверителността на браузъра – ако е разрешено, ESET Internet Security ще показва известията за поверителност и защита на браузъра.

Скенер за скриптове в браузъра

Разрешаване на разширено сканиране на скриптове на браузъра – ако е разрешено, антивирусният скенер ще проверява всички програми на JavaScript, изпълнявани от интернет браузъри.

00

Управление на устройства

ESET Internet Security осигурява автоматичен контрол на устройства (CD/DVD/USB/и т.н.). Този модул дава възможност да блокирате или настройвате разширени филтри/разрешения и да избирате възможността за достъп и работа на потребителите с определено устройство. Тази функция е подходяща, в случай че администраторът на компютъра иска да предотврати използването на устройства, съдържащи нежелано съдържание.

Поддържани външни устройства:

- Съхранение на диск (HDD, преносим USB диск)
- CD/DVD

- USB Принтер
- FireWire Съхранение
- Bluetooth Устройство
- Четец на смарт карти
- Устройство за създаване на изображения
- Модем
- LPT/COM порт
- Преносимо устройство (устройства, захранвани с батерии, като мултимедийни плейъри, смартфони, устройства plug-and-play и т.н.)
- Всички типове устройства

Опциите за настройка на управлението на устройства могат да се променят в Разширени настройки > **Защити** > **Функция за управление на външни устройства**.

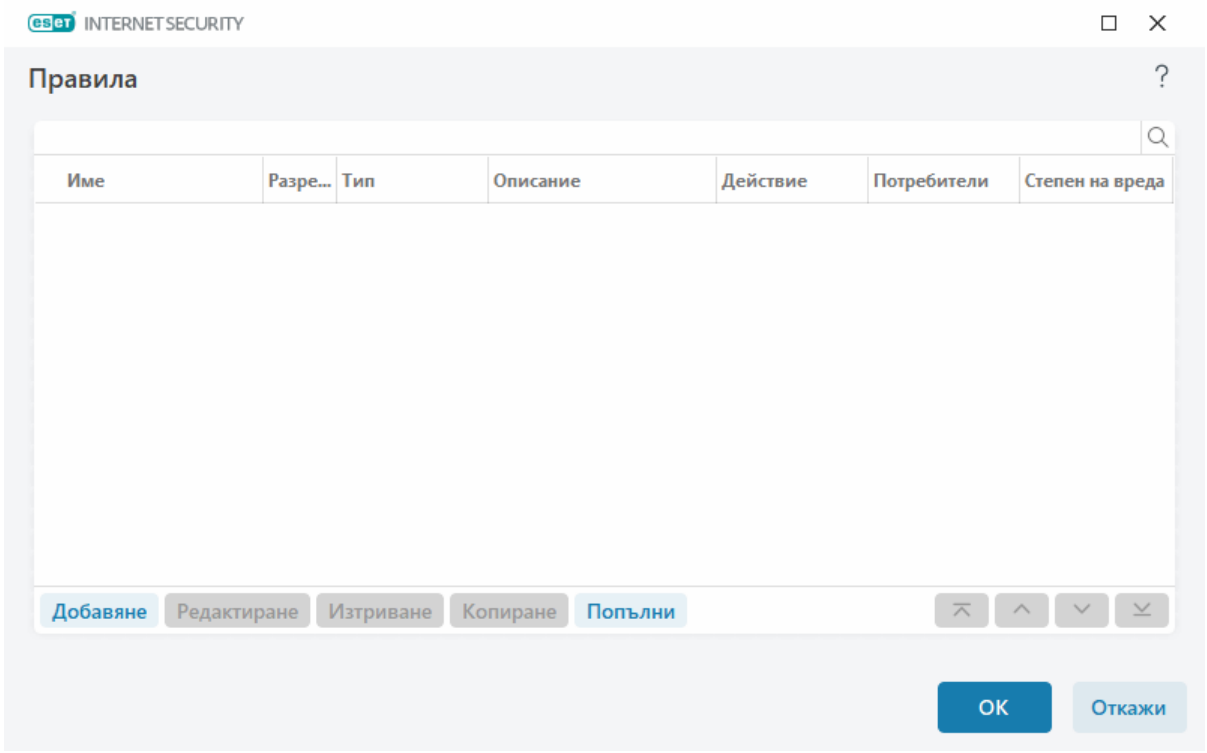
Щракнете върху превключвателя **Разрешаване на контрол на преносими паметни устройства**, за да разрешите функцията за управление на устройството в ESET Internet Security; трябва да рестартирате компютъра, за да влезе в сила тази промяна. След разрешаване на „Контрол на преносими паметни устройства“ можете да определите **Правилата** в прозореца на Редактора на правила.

Можете да създадете различни групи устройства, за които ще се прилагат различни правила. Можете също така да създадете само една група устройства, за която ще се прилага правилото с действие **Позволявам** или **Записване на блок**. Това гарантира, че управлението на устройства ще блокира неразпознати устройства, ако бъдат свързани към компютъра.

Ако бъде поставено устройство, което се блокира от съществуващо правило, ще се покаже прозорец с известие и достъпът до устройството ще бъде забранен.

Редактор на правила за управление на устройства

Прозорецът **Редактор на правила за контрол на устройството** показва съществуващите правила и позволява прецизен контрол на външните устройства, които потребителите свързват към компютъра.

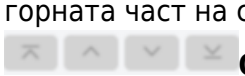


Възможно е отделните устройства да бъдат позволени или блокирани за потребител или група потребители и да са базирани на допълнителни параметри за устройства, които могат да бъдат посочени в конфигурацията на правилото. Списъкът с правила съдържа няколко описания за правило, като например име, тип на външното устройство, действие, което да се извършва след свързване на външното устройство към компютъра ви, и регистрирана степен на вреда. Вижте също Добавяне на правила за контрол на устройството.

Щракнете върху **Добавяне** или **Редактиране**, за да управлявате дадено правило. Щракнете върху **Копирай**, за да създадете ново правило с предварително зададени опции, използвани за друго избрано правило. XML низовете, които се показват при щракване върху някое правило, могат да се копират в клипборда, за да помогнат на системните администратори да експортират/импортират тези данни и да ги използват в , например.

Чрез натискане на клавиша **CTRL** и щракване можете да изберете няколко правила и да приложите действия за всички избрани правила, като например изтриване или преместване нагоре или надолу в списъка. Квадратчето за отметка **Разрешено** забранява или активира правило; това може да е полезно, ако искате да запазите правилото.

Щракнете върху опцията **Попълни**, за да се попълнят автоматично параметрите на устройствата с преносим носител за устройствата, свързани с компютъра.

Правилата са подредени в списък по приоритет, като тези с по-висок приоритет се намират в горната част на списъка. Правилата могат да бъдат премествани чрез щракване върху  **Отгоре/Нагоре/Надолу/Отдолу** – индивидуално или групово.

Записите в дневника могат да се преглеждат в главния прозорец на програмата > **Инструменти** > Регистрационни файлове.

Дневник за управление на устройства записва всички случаи на стартиране на функцията "Контрол на преносими паметини устройства".

Открити устройства

Бутонът **Попълване** предоставя общ преглед на всички свързани в момента устройства, включващ информация за: типа, доставчика, модела и серийния номер на устройството (при наличие). Ако искате да видите всички скрити устройства, изберете **Показване на скритите устройства**.

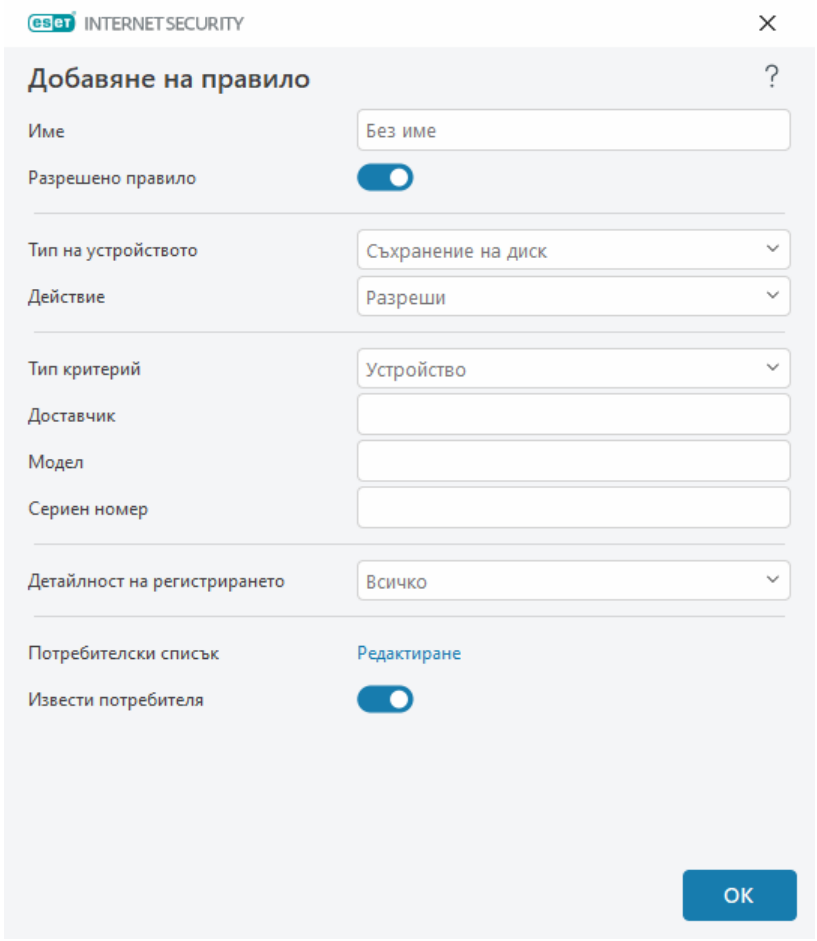
Изберете устройство от списъка с открити устройства и щракнете върху **ОК**, за да добавите правило за управление на устройства с предварително зададена информация (всички настройки могат да бъдат регулирани).

Устройствата в режим с ниска мощност (заспиване) са маркирани с икона за предупреждение . За да разрешите бутона **ОК** и да добавите правило за това устройство:

- Свържете устройството отново
- Използвайте устройството (например стартирайте приложението за камера в Windows, за да събудите уеб камера)

Добавяне на правила за управление на устройства

Правилата за управление на устройства определят действието, което да се извършва, когато устройство, отговарящо на критериите на правилото, бъде свързано към компютъра.



Въведете описание на правилото в полето **Име** за по-добра идентификация. Щракнете върху плъзгача до **Разрешено правило**, за да забраните или разрешите правилото; това може да е от полза, ако не искате да изтривате правилото завинаги.

Тип устройство

Изберете типа на външното устройство от падащото меню (Съхранение на диск/Преносимо устройство/Bluetooth/FireWire/...). Информацията за типа устройство се събира от операционната система и може да бъде прегледана в диспечера на устройства на системата, ако към компютъра се свърже устройство. Устройствата за съхранение включват външни дискове или конвенционални четци на карти с памет, свързани чрез USB или FireWire. Четците на смарт карти включват всички четци на смарт карти с вградена интегрална схема, като например SIM карти или карти за удостоверяване. Примери на устройства за създаване на изображения са скенерите и камерите. Тъй като тези устройства предоставят само информация за своите действия, но не и информация за потребителите, те могат да се блокират само глобално.

Действие

Достъпът до устройства, чиято цел не е съхранение, може да бъде или разрешен, или блокиран. За разлика от това, правилата за устройства за съхранение позволяват избор на една от следните настройки на права:

- **Позволявам** – Ще бъде разрешен пълен достъп до устройството.
- **Блокирай** – Достъпът до устройството ще бъде блокиран.
- **Записване на блок** – Ще бъде разрешен само достъп за четене от устройството.
- **Предупреждаване** – При всяко свързване на устройство потребителят ще получава

известие дали устройството е разрешено/блокирано и ще се създава запис в регистрационния файл. Устройствата не се запомнят, поради което ще се показва известие при всяко следващо свързване на същото устройство.

Обърнете внимание, че не всички действия (разрешения) са налични за всички типове устройства. Ако става дума за тип устройство за съхранение, и четирите действия са налични. За устройства, чиято цел не е съхранение, са налични само три действия (например действието **Записване на блок** не е налично за Bluetooth устройства, така че Bluetooth устройствата могат да използват само действията за разрешаване, блокиране или предупреждаване).

Тип критерий

Изберете **Група устройства** или **Устройство**.

Допълнителни параметри, показани по-долу, може да се използват за фина настройка на правилата за различни устройства. Всички параметри правят разлика между главни и малки букви и поддържат заместващи символи (*, ?):

- **Доставчик** – Филтрирайте по име или ИД на доставчик.
- **Модел** – Назначеното име на устройството.
- **Сериен** – Външните устройства обикновено имат свои собствени серийни номера. При CD/DVD устройствата това е серийният номер на съответния носител, а не на самото CD устройство.

Ако тези параметри не са определени, правилото ще игнорира полетата при съпоставянето. Филтриращите параметри във всички текстови полета правят разлика между главни и малки букви и поддържат заместващи символи (въпросителният знак (?) представлява един символ, а звездичката (*) представлява низ от нула или повече знаци).

За да прегледате информация за устройство, създайте правило за този тип устройства, свържете устройството с компютъра и след това прегледайте подробните данни за устройството в регистрационния файл за управление на устройства.

Детайлност на регистрирането

ESET Internet Security записва всички важни събития в регистрационен файл, който може да бъде прегледан директно от главното меню. Щракнете върху **Инструменти** > **Регистрационни файлове**, след което изберете **Управление на устройства** от падащото меню **Регистрационен файл**.

- **Всички** – регистриране на всички събития.
- **Диагностика** – регистриране на информацията, необходима за прецизна настройка на програмата.
- **Информация** – регистриране на информативни съобщения, включително съобщения за успешно обновяване и всички записи по-горе.

• **Предупреждение** – регистриране на съобщения за критични грешки и предупреждения.

• **Няма** – няма да се записват регистрационни файлове.

Потребителски списък

Правилата могат да бъдат ограничени за определени потребители или групи потребители чрез добавянето им в списъка на потребителя, като щракнете върху **Редактиране** до **Списък на потребителя**.

• **Добавяне** – отваряне на диалоговия прозорец **Типове обект: Потребители или групи**, който позволява да изберете желаните потребители.

• **Премахни** – Премахва избрания потребител от филтъра.

> **Ограничения на списъка на потребителя**
> Списъкът на потребителя не може да бъде дефиниран за правила с определени типове устройства:
> • USB принтер
> • Bluetooth устройство
> • Четец на смарт карти
> • Устройство за създаване на изображения
> • Модем
> • LPT/COM порт

Уведомяване на потребителя – ако бъде поставено устройство, което се блокира от съществуващо правило, ще се покаже прозорец с известие.

Групи устройства

⚠ Устройствата, свързвани към компютъра, може да представляват риск за защитата.

Прозорецът "Групи устройства" е разделен на две части. Дясната част на прозореца съдържа списък на устройствата, принадлежащи към съответната група, а лявата част на прозореца съдържа създадените групи. Изберете група, за да покажете устройства в десния екран.

Когато отворите прозореца "Групи устройства" и изберете група, можете да добавите или премахнете устройства от списъка. Друг начин за добавяне на устройства към групата е чрез импортиране от файл. Можете също така да щракнете върху бутона **Попълни** и всички устройства, свързани с компютъра, ще бъдат включени в списъка в прозореца **Открити устройства**. Изберете устройство от попълнения списък, за да го добавите към групата, като щракнете върху **ОК**.

Контролни елементи

Добавяне – може да добавите група, като въведете името ѝ или устройство към съществуваща група, в зависимост от това в коя част от прозореца сте щракнали върху бутона.

Редактиране – Позволява ви да редактирате името на избрана група или параметрите на дадено устройство (доставчик, модел, сериен номер).

Изтриване – изтриване на избраната група или устройство в зависимост от това в коя част на прозореца сте щракнали върху бутона.

Импортиране – Импортиране на списък с устройства от текстов файл. Импортирането на устройства от текстов файл изисква правилно форматиране:

- Всяко устройство започва на нов ред.
- **Доставчик**, **Модел** и **Сериен номер** трябва да са налични за всяко устройство и да са разделени със запетая.

Ето пример за съдържанието на текстов файл:

```
Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101
```

Експортиране – Експортиране на списък с устройства във файл.

Бутонът **Попълване** предоставя общ преглед на всички свързани в момента устройства, включващ информация за: типа, доставчика, модела и серийния номер на устройството (при наличие).

Добавяне на устройство

Щракнете върху **Добавяне** в десния прозорец, за да добавите устройство към съществуваща група. Допълнителни параметри, показани по-долу, може да се използват за фина настройка на правилата за различни устройства. Всички параметри правят разлика между главни и малки букви и поддържат заместващи символи (*, ?):

- **Доставчик** – Филтрирайте по име или ID на доставчик.
- **Модел** – Назначеното име на устройството.
- **Сериен** – Външните устройства обикновено имат свои собствени серийни номера. При CD/DVD устройствата това е серийният номер на съответния носител, а не на самото CD устройство.
- **Описание** – вашето описание на устройството за по-добра организация.

Ако тези параметри не са определени, правилото ще игнорира полетата при съпоставянето. Филтриращите параметри във всички текстови полета правят разлика между главни и малки букви и поддържат заместващи символи (въпросителният знак [?] представлява един символ, докато звездичката [*] представлява низ от нула или повече знаци).

Щракнете върху бутона **ОК**, за да запишете промените. Щракнете върху **Отказ**, ако искате да затворите прозореца **Групи устройства**, без да запишете промените.

След като създадете група устройства, трябва да добавите ново правило за контрол на преносими паметни устройства за създадената група устройства и да изберете действието, което да се предприеме.

Обърнете внимание, че не всички действия (разрешения) са налични за всички типове устройства. И четирите действия са налични, ако това е устройство от тип за съхранение. За устройства, чиято цел не е съхранение, са налични само три действия (например действието **Записване на блок** не е налично за Bluetooth устройства, така че Bluetooth устройствата могат да използват само действията за разрешаване, блокиране или предупреждаване).

Защита на уеб камерата

Защитата на уеб камерата ви информира за процесите и приложенията, които осъществяват достъп до уеб камерата на компютъра ви. Когато приложение се опитва да осъществи достъп до камерата ви, ще получите известие, от което можете да **разрешите** или **блокирате** достъпа. Цветът на прозореца на известието зависи от репутацията на приложението.

Опциите за настройка на защитата на уеб камерата могат да се променят в Разширени настройки **Защити** > **Контрол на преносими паметни устройства** > **Защита на уеб камерата**.

За да активирате функцията за защита на уеб камерата в ESET Internet Security, активирайте превключвателя до **Разрешаване на защитата на уеб камерата**.

Когато разрешите защитата на уеб камерата, **правилата** стават активни, което ви позволява да отворите прозореца Редактор на правила.

За да изключите предупрежденията за приложения с присъстващо правило, които са променени, но все още имат валиден цифров подпис (например обновяване на приложението), активирайте плъзгача до **Забраняване на предупрежденията за достъп до уеб камера за променени приложения**.

Редактор на правила за защита на уеб камерата

Този прозорец показва съществуващите правила и предоставя контрол върху приложенията и процесите, които имат достъп до уеб камерата на компютъра, въз основа на предприетото от вас действие.

Възможните са следните действия:

- **Разреши достъпа**
- **Блокиране на достъпа**

- **Попитай** (Пита потребителя всеки път, когато приложение се опитва да получи достъп до уеб камера)

Премахнете отметката от квадратчето за отметка в колоната „**Известяване**“, за да спрете получаването на известия, когато дадено приложение получи достъп до уеб камерата.

> **i** Илюстрирани инструкции
> Как да създадете и редактирате правила за уеб камера в ESET Internet Security.

ThreatSense

ThreatSense се състои от множество сложни методи за откриване на заплахи. Тази технология е проактивна, което означава, че тя осигурява защита в самото начало от появата на нова заплаха. Тя използва комбинация от анализ на кода, емулиране на кода, общи сигнатури и сигнатури за вируси, които работят съвместно за значително подобряване на защитата на системата. Модулът за сканиране може да контролира едновременно няколко потока данни, което увеличава максимално ефективността и откритите заплахи. Технологията ThreatSense също така успешно унищожава комплекти за пълен достъп.

Опциите за настройка на модула ThreatSense ви позволяват да укажете няколко параметъра за сканиране:

- Типове файлове и разширения за сканиране
- Комбинация от различни методи за откриване
- Нива на почистване и др.

За да отворите прозореца за настройка, щракнете върху **ThreatSense** в Разширени настройки за всеки модул, който използва технологията ThreatSense (вж. по-долу). Отделните сценарии за защита могат да изискват различни конфигурации. Имайки това предвид, ThreatSense може да се конфигурира индивидуално за следните модули за защита:

- Защитата на файловата система в реално време
- Сканиране в състояние на неактивност
- Начално сканиране
- Защита на документи
- Защита на имейл клиенти
- Защита на уеб достъпа
- Сканиране на компютъра

Параметрите на ThreatSense са високо оптимизирани за всеки модул и промяната им може значително да повлияе на работата на системата. Например, ако промените параметрите така, че винаги да се сканират архиваторите в реално време, или разрешите разширени евристични методи в модула за защита на файловата система в реално време, това може да доведе до забавяне на работата на системата (по принцип с тези методи се сканират само новосъздадени файлове). Препоръчваме да не променяте параметрите на ThreatSense за всички модули без този за сканиране на компютъра.

Обекти за сканиране

Този раздел позволява да укажете кои файлове и компоненти на компютъра да се сканират за проникванията.

Оперативна памет – сканиране за заплахи, атакуващи оперативната памет на системата.

Сектори за начално стартиране/UEFI – сканиране на секторите за начално зареждане за наличие на злонамерен софтуер в първия зареждащ сектор. Прочетете повече за UEFI в речника.

Имейл файлове – програмата поддържа следните разширения: DBX (Outlook Express) и EML.

Архиви – програмата поддържа следните разширения: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE и много други.

Саморазархивиращи се архиви – саморазархивиращите се архиви (SFX) са архиви, които се саморазархивират.

Архиватори в реално време – след изпълнение архиваторите в реално време (за разлика от стандартните типове архиви) се декомпресират в паметта. Освен стандартните статични компресиращи модули (UPX, yoda, ASPack, FSG и т.н.) програмата за сканиране може да разпознава няколко допълнителни типа компресиращи модули чрез използване на емулиране на код.

Опции за сканиране

Изберете методите, използвани при сканиране на системата за проникванията. Налични са следните опции:

Евристични методи – евристичните методи представляват алгоритъм за анализиране на (злонамерена) дейност на програмите. Основното предимство на тази технология е възможността за идентифициране на злонамерен софтуер, който не съществува или не е познат в предишната версия на системата за откриване. Недостатъкът е (много малка) вероятност от фалшиви сигнали.

Разширени евристични методи/ДНК сигнатури – Разширените евристични методи са уникални евристични алгоритми, разработени от ESET, оптимизирани за откриване на компютърни червеи и троянски коне и са написани на програмни езици от високо ниво. Използването на разширени евристични методи значително подобрява способността за откриване на заплахи на продуктите на ESET. Чрез сигнатурите могат надеждно да се откриват и идентифицират вируси. С помощта на системата за автоматично обновяване новите сигнатури са достъпни само няколко часа след откриването на заплахата. Недостатъкът на сигнатурите е, че откриват само вируси, които познават (или техни леко променени версии).

Почистване

Настройките за почистване определят поведението на ESET Internet Security при почистване на обекти. Има 4 нива на почистване:

ThreatSense има следните нива на отстраняване на проблеми (т.е. почистване).

Отстраняване на проблеми в ESET Internet Security

Ниво на почистване	Описание
Винаги отстранявай откриването	Опит за отстраняване на проблеми с откриването при почистване на обекти без намеса на крайния потребител. В някои редки случаи (например в системни файлове), ако откриването не може да бъде отстранено, докладваният обект се оставя на оригиналното си местоположение.
Отстрани откриването, ако е безопасно, в противен случай го задръж	Опит за отстраняване на проблеми с откриването при почистване на обекти без намеса на крайния потребител. В някои случаи (например при системни файлове или архиви с чисти и заразени файлове), ако откриването не може да бъде отстранено, докладваният обект се оставя на оригиналното си местоположение.
Отстрани откриването, ако е безопасно, в противен попитай	Опит за отстраняване на проблеми с откриването при почистване на обекти. В някои случаи, ако не може да се извърши действие, крайният потребител получава интерактивно уведомление и трябва да избере действие за отстраняване на проблеми (например премахване или игнориране). Тази настройка се препоръчва в повечето случаи.
Винаги питай крайния потребител	Крайният потребител получава интерактивен прозорец, докато почиства обектите и трябва да избере действие за отстраняване на проблеми (например, премахване или игнориране). Това ниво е предназначено за по-напреднали потребители, които знаят кои стъпки да предприемат в случай на откриване.

Изключения

Разширението е частта от името на файла, разделена с точка. Разширението определя типа и съдържанието на файла. Този раздел на настройката на ThreatSense ви позволява да определите типовете файлове за сканиране.

Други

При конфигурирането на параметрите на модула ThreatSense за сканиране на компютъра при поискване са налични също така и следните опции в раздела **Други**:

Сканиране на алтернативни потоци данни (ADS) – Алтернативните потоци данни (ADS), използвани от файловата система NTFS, представляват асоциации на файлове и папки, които са невидими при обикновените техники на сканиране. Много прониквания се опитват да заобиколят откриването им, като се представят за алтернативни потоци данни.

Изпълнение на фоново сканиране с нисък приоритет – всяка последователност за сканиране използва известно количество системни ресурси. Ако работите с програми, които изискват много системни ресурси, можете да активирате сканиране на фона с нисък приоритет и да запазите ресурсите за приложенията си.

Регистриране на всички обекти – дневникът на сканирането ще покаже всички сканирани файлове в саморазархивиращите се архиви – дори тези, които не са инфектирани (може да се генерират много данни за дневника на сканирането и да се увеличи размерът на файла за дневника на сканирането).

Разрешаване на оптимизация Smart – при разрешена оптимизация Smart се използват най-оптималните настройки, за да се осигури най-ефективното ниво на сканиране, като в същото

време се поддържа и най-високата скорост на сканиране. Различните модули за защита сканират интелигентно, като използват различни методи на сканиране и ги прилагат към конкретни типове файлове. Ако интелигентната оптимизация е забранена, при извършване на сканиране се прилагат само дефинираните от потребителя настройки в ядрото на ThreatSense на определените модули.

Запазване на клеймото за последен достъп – изберете тази опция, за да запазите първоначалното време на достъп до сканираните файлове, вместо да ги обновявате (например при използване на системи за архивиране на данни).

Ограничения

Разделът "Ограничения" ви позволява да укажете максималния размер на обектите и нивата на влагане на архиви, които ще се сканират:

Настройки на обекта

Максимален размер на обекта – указване на максималния размер на обектите, които да се сканират. Съответният антивирусен модул ще сканира само обектите, които са по-малки от този размер. Тази опция трябва да се променя само от напреднали потребители, които имат конкретна причина да изключват от сканирането по-големи обекти. Стойност по подразбиране: неограничено.

Максимално време за сканиране за обект (сек.) – определя стойността за максимално време за сканиране на файлове в контейнерен обект (като например RAR/ZIP архив или имейл с няколко прикачени файла). Тази настройка не важи за самостоятелни файлове. Ако зададена от потребителя стойност е въведена и това време е изтекло, сканирането ще спре възможно най-скоро, независимо дали сканирането на всеки файл в контейнерен обект е завършено.
В случай на архив с големи файлове сканирането ще спре не по-рано от извличането на файл от архива (например когато дефинирана от потребителя променлива е 3 секунди, но извличането на файл отнема 5 секунди). Останалите файлове в архива няма да бъдат сканирани, когато това време изтече.
За да ограничите времето за сканиране, включително по-големи архиви, използвайте **Максимален размер на обекта** и **Максимален размер на файла в архива** (не се препоръчва поради възможни рискове за сигурността).
Стойност по подразбиране: неограничено.

Настройка на сканиране на архиви

Ниво на вложени архиви – указване на максималното ниво за сканиране на вложени архиви. стойност по подразбиране: 10.

Максимален размер на файловете в архива – тази опция ви позволява да посочите максималния размер на файловете в архивите (когато бъдат разархивирани), които ще се сканират. Максималната стойност е **3 ГБ**.

> Не е препоръчително да променяте стойностите по подразбиране. При нормални обстоятелства не би трябвало да има причина те да се променят.

Нива на почистване

За да промените настройките на нивото на почистване за желания модул за защита, разгънете **ThreatSense** (например **Защитата на файловата система в реално време**) и след това изберете **Ниво на почистване** от падащото меню.

ThreatSense има следните нива на отстраняване на проблеми (т.е. почистване).

Отстраняване на проблеми в ESET Internet Security

Ниво на почистване	Описание
Винаги отстранявай откриването	Опит за отстраняване на проблеми с откриването при почистване на обекти без намеса на крайния потребител. В някои редки случаи (например в системни файлове), ако откриването не може да бъде отстранено, докладваният обект се оставя на оригиналното си местоположение.
Отстрани откриването, ако е безопасно, в противен случай го задръж	Опит за отстраняване на проблеми с откриването при почистване на обекти без намеса на крайния потребител. В някои случаи (например при системни файлове или архиви с чисти и заразени файлове), ако откриването не може да бъде отстранено, докладваният обект се оставя на оригиналното си местоположение.
Отстрани откриването, ако е безопасно, в противен попитай	Опит за отстраняване на проблеми с откриването при почистване на обекти. В някои случаи, ако не може да се извърши действие, крайният потребител получава интерактивно уведомление и трябва да избере действие за отстраняване на проблеми (например премахване или игнориране). Тази настройка се препоръчва в повечето случаи.
Винаги питай крайния потребител	Крайният потребител получава интерактивен прозорец, докато почиства обектите и трябва да избере действие за отстраняване на проблеми (например, премахване или игнориране). Това ниво е предназначено за по-напреднали потребители, които знаят кои стъпки да предприемат в случай на откриване.

Разширения на файлове, изключени от сканиране

Изключените файлови разширения са част от ThreatSense. За да конфигурирате изключени файлови разширения, щракнете върху **ThreatSense** в Разширени настройки за всеки модул, който използва технологията ThreatSense.

Разширението е частта от името на файла, разделено с точка. Разширението определя типа и съдържанието на файла. Този раздел за настройка на ThreatSense ви позволява да укажете типовете файлове за сканиране.

> Не се бъркайте с Изключения от тип "Процес", HIPS изключения или Изключения от тип "Файл"/"Папка".

По подразбиране всички файлове се сканират. Всяко разширение може да се добави към

списъка за изключване от сканиране.

Изключването на файлове от сканиране понякога е наложително, ако сканирането на определени типове файлове пречи на програмата, използваща някои разширения, да работи правилно. Например може да е препоръчително да се изключват разширенията `.edb`, `.eml` и `.tmp` при използване на сървъри на Microsoft Exchange.

За да добавите ново разширение в списъка, щракнете върху **Добавяне**. Въведете разширението в празното поле (например tmp) и щракнете върху **OK**. Ако изберете **Въвеждане на различни стойности**, можете да въведете няколко файлови разширения, разделени с нов ред, запетая или точка и запетая (например изберете **Точка и запетая** като разделител от падащото меню и въведете `edb;eml;tmp`). Можете да използвате специален символ ? (въпросителен знак). Въпросителният знак представлява който и да е символ (например `?db`).

За да видите точното разширение (ако има такова) на файл в операционна система Windows, трябва да поставите отметка в квадратчето **Разширения на имена на файлове** в **Windows Explorer** > **Изглед** (раздел).

Допълнителни параметри на ThreatSense

За да редактирате тези настройки, отворете Разширени настройки > **Защити** > **Защита на файловата система в реално време** > **Допълнителни ThreatSense параметри**.

Допълнителни параметри на ThreatSense за новосъздадени и променени файлове

Вероятността за заразяване на новосъздадени или променени файлове е сравнително по-висока, отколкото при съществуващите файлове. Поради това програмата проверява тези файлове с допълнителни параметри на сканиране. ESET Internet Security използва разширени евристики, които могат да откриват нови заплахи преди издаването на обновяване на системата за засичане на потенциално опасни заплахи в комбинация с методи за сканиране на базата на сигнатури.

В допълнение към новосъздадените файлове сканирането се извършва и на **Саморазархивиращи се архиви** (.sfx) и **Архиватори в реално време** (вътрешно компресирани изпълними файлове). По подразбиране архивите се сканират до 10-о ниво на вложени архиви и се проверяват независимо от действителния им размер. За да промените настройките за сканиране на архиви, премахнете отметката на **Настройки за сканиране на архиви по подразбиране**.

Допълнителни параметри на ThreatSense за изпълнени файлове

Разширени евристични методи при изпълнение на файлове – По подразбиране разширените евристики се използват при изпълнение на файловете. Когато са разрешени, е силно препоръчително да запазите Оптимизация Smart и ESET LiveGrid® също разрешени, за да намалите въздействието върху производителността на системата.

Разширени евристични методи при изпълнение на файлове от преносим носител – Разширените евристични методи емулират код във виртуална среда и оценяват поведението му, преди да бъде разрешено на кода да се изпълни от преносим носител.

Инструменти

Можете да конфигурирате разширени настройки за функции, които предлагат допълнителна защита и помагат за опростяване на администрирането на ESET Internet Security в Разширени настройки > **Инструменти**.

- Обновяване на Microsoft Windows®
- ESET CMD
- Регистрационни файлове
- Режим за геймъри
- Диагностика

Обновяване на Microsoft Windows®

Функцията за обновяване на Windows е важен компонент при защитата на потребителите от злонамерен софтуер. Поради тази причина е много важно да инсталирате наличните обновявания на Microsoft Windows. ESET Internet Security известява за липсващи обновявания съгласно указаното ниво в Разширени настройки > **Инструменти**. Налични са следните нива:

• **Не известявай** – не се предлагат системни обновявания за изтегляне.

• **Незадължителни обновявания** – за изтегляне ще се предлагат обновявания, маркирани с нисък и по-висок приоритет.

• **Препоръчани обновявания** – за изтегляне ще се предлагат обновявания, маркирани със стандартен и по-висок приоритет.

• **Важни обновявания** – за изтегляне ще се предлагат обновявания, маркирани с важен и по-висок приоритет.

• **Критични обновявания** – за изтегляне ще се предлагат само критични обновявания.

Диалогов прозорец – Обновявания на системата

Ако има обновявания за вашата операционна система, ESET Internet Security показва известие в главния прозорец на програмата > **Преглед**. Щракнете върху **Повече информация** за отваряне на прозореца „Системни обновявания“.

Прозорецът "Системни обновявания" показва списък с наличните обновявания за изтегляне и

инсталиране. Типът на обновяването е показан до името му.

Щракнете двукратно върху ред на обновяване, за да изведете прозореца Информация за обновяването с допълнителна информация.

Щракнете върху **Стартиране на обновяване на системата**, за да изтеглите и инсталирате всички изброени обновявания на операционната система.

Информация за обновяването

Прозорецът "Системни обновявания" показва списък с наличните обновявания за изтегляне и инсталиране. Нивото на приоритет на обновяването е показано до името му.

Щракнете върху **Стартирай обновяване на системата**, за да започне изтеглянето и инсталирането на обновявания за операционната система.

Щракнете с десния бутон върху даден ред от обновяванията, след което щракнете върху **Показване на информация**, за да се покаже нов прозорец с допълнителна информация.

ESET CMD

Това е функция, която позволява разширени ecmd команди. Позволява ви да експортирате и импортирате настройки с командния ред (ecmd.exe). Досега експортирането и импортирането на настройки беше възможно само чрез графичния потребителски интерфейс. ESET Internet Security конфигурацията може да бъде експортирана в *.xml* файл.

След като разрешите ESET CMD, ще разполагате с два метода за упълномощаване:

- **Няма** – без упълномощаване. Не ви препоръчваме този метод, тъй като позволява импортирането на всякакви неподписани конфигурации, което е потенциален риск.
- **Парола за разширени настройки** – изисква се парола за импортиране в конфигурационен файл от .xml файл, като този файл трябва да е подписан (вж. по-надолу за подписване на .xml конфигурационен файл). Посочената в Настройка на достъпа парола трябва да се предостави, преди да може да се импортира нова конфигурация. Ако не сте разрешили настройката на достъпа, паролата не съответства или .xml конфигурационният файл не е подписан, конфигурацията няма да бъде импортирана.

След като разрешите ESET CMD, можете да използвате командния ред за импортиране или експортиране на конфигурации на ESET Internet Security. Можете да го направите ръчно или да създадете скрипт с цел автоматизация.

За да използвате разширени ecmd команди, трябва да ги изпълните с администраторски права или да отворите командния прозорец на Windows (cmd) с **Изпълни като администратор**. В противен случай ще получите съобщение **Error executing command**. Освен това, когато експортирате конфигурация, целевата папка трябва да съществува. Командата за експортиране все още работи, когато настройката на ESET CMD е изключена.

Команда за експортиране на настройки:
`ecmd /getcfg c:\config\settings.xml`

Команда за импортиране на настройки:
`ecmd /setcfg c:\config\settings.xml`

Разширени ecmd команди могат да се изпълняват само локално.

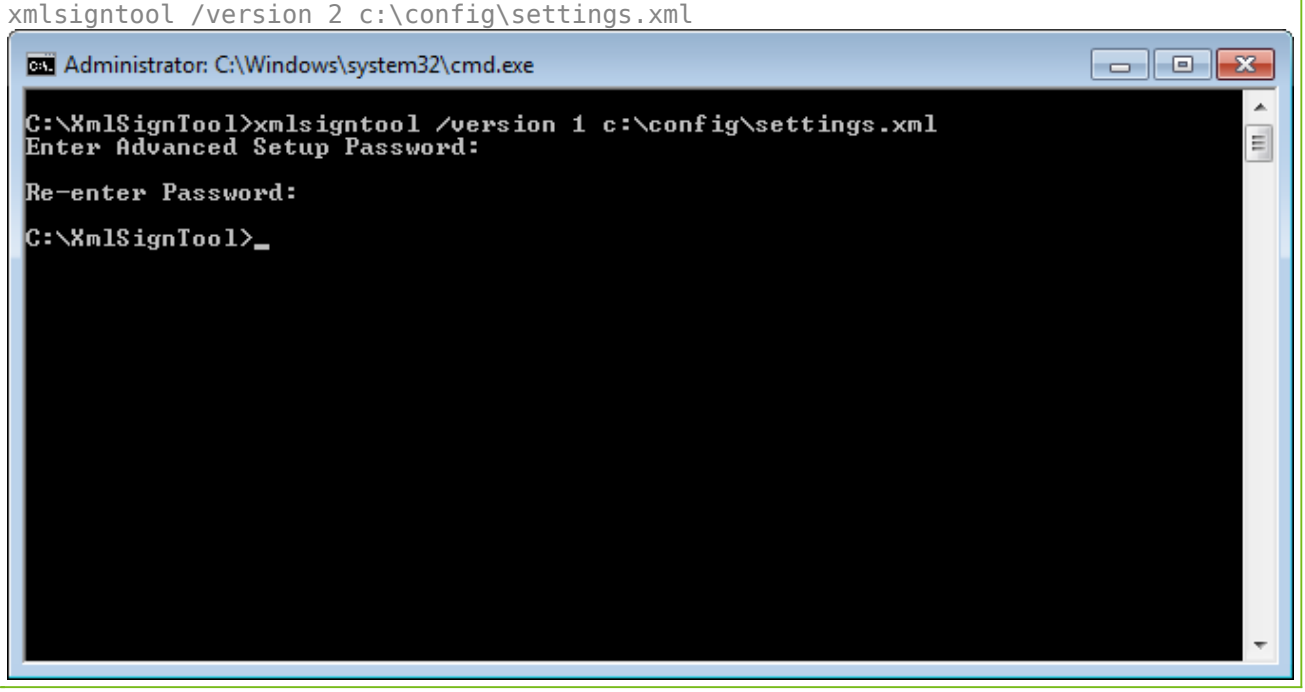
Подписване на *.xml* конфигурационен файл:

1. Изтеглете изпълнимия файл XmlSignTool.
2. Отворете командния прозорец на Windows (cmd) с **Изпълни като администратор**.
3. Отидете до местоположението на запис на `xmlsigntool.exe`
4. Изпълнете команда за подписване на *.xml* конфигурационния файл, употреба:
`xmlsigntool /version 1|2 <xml_file_path>`

Стойността на параметъра `/version` зависи от вашата версия на ESET Internet Security. Използвайте `/version 1` за версии на ESET Internet Security, по-стари от 11.1. Използвайте `/version 2` за текущата версия на ESET Internet Security.

5. Въведете два пъти паролата си за разширена настройка, когато бъдете подканени от XmlSignTool. Вашият *.xml* конфигурационен файл вече е подписан и може да бъде използван за импортиране на друг екземпляр на ESET Internet Security с ESET CMD чрез метода за упълномощаване с парола.

Команда за подписване на експортиран конфигурационен файл:
`xmlsigntool /version 2 c:\config\settings.xml`



Ако вашата парола за Настройка на достъпа се промени и искате да импортирате конфигурация, която е подписана по-рано със стара парола, трябва да подпишете *.xml* конфигурационния файл отново с настоящата си парола. Така ще можете да използвате по-стар конфигурационен файл, без да го експортирате в друго устройство, на което се изпълнява ESET Internet Security, преди импортирането.

Разрешаването на ESET CMD без упълномощаване не се препоръчва, тъй като това ще позволи импортирането на всякакви неподписани конфигурации. Задайте паролата в Разширени настройки > **Потребителски интерфейс** > **Настройка на достъпа**, за да предотвратите неупълномощена промяна от потребителите.

Регистрационни файлове

Можете да намерите конфигурацията на регистрирането на ESET Internet Security в Разширени настройки > **Инструменти** > **Регистрационни файлове**. Разделът за регистрационни файлове се използва за дефиниране на начина за тяхното управление. Програмата автоматично изтрива по-старите регистрационни файлове, за да пести място на диска. Можете да изберете следните опции за регистрационни файлове:

Минимална детайлност при регистриране – указва минималното ниво на детайлност на събитията за регистриране:

- **Диагностични** – Регистрира информация, необходима за прецизна настройка на програмата, и всички записи по-горе.
- **Информативни** – регистриране на информативни съобщения, включително съобщения за успешно обновяване и всички записи по-горе.
- **Предупреждения** – регистриране на съобщения за критични грешки и предупреждения.
- **Грешки** – грешките от типа на "Грешка при изтегляне на файл" и критичните грешки се записват.
- **Критични** – Регистрира само критични грешки (грешка в стартирането на антивирусната защита, защитна стена, и т.н.).

Всички блокирани връзки ще се запишат, когато изберете нивото на детайлност на диагностика.

Записите в регистрационния файл, които са по-стари от указания брой дни в полето **Автоматично изтриване на записи, по-стари от (дни)**, ще се изтриват автоматично.

Автоматично оптимизиране на регистрационните файлове – При избиране на тази опция регистрационните файлове ще се дефрагментират автоматично, ако процентът е по-висок от указаната стойност в полето **Ако броят на неизползваните записи превишава (%)**.

Щракнете върху **Оптимизиране**, за да започне дефрагментирането на регистрационните файлове. По време на този процес се премахват всички празни записи в регистъра, което подобрява производителността и скоростта на обработка на регистрационните файлове. Това подобрение ще бъде особено очевидно, ако регистрационните файлове съдържат голям брой записи.

Разрешаване на текстов формат прави възможно съхраняването на регистрационни файлове в друг файлов формат, различен от Регистрационни файлове:

- **Целева директория** – директорията, в която ще се съхраняват регистрационните

файлове (прилага се само за текст/CSV). Всеки раздел на дневника има собствен файл с предварително определено файлово име (например virlog.txt за раздела **Засичания** на регистрационните файлове, ако използвате обикновен текстов файлов формат за съхраняване на дневници).

• **Тип** – ако изберете файлов формат **Текст**, регистрационните файлове ще се съхраняват в текстов формат, а данните ще бъдат разделени в раздели. Същото се отнася за формата на файлове, съдържащи стойности, разделени със запетая (**CSV**). Ако изберете **Събитие**, регистрационните файлове ще се съхраняват в регистъра на събитията на Windows (може да се прегледа с помощта на Визуализатор на събития в контролния панел), а не във файл.

• **Изтриване на всички регистрационни файлове** – Изтрива всички съхранени регистри, които са избрани към момента в падащото меню **Тип**. Ще бъде показано известие за успешното изтриване на регистрационните файлове.

i С цел по-бързото разрешаване на проблеми ESET може да ви помоли да предоставите регистрационни файлове от компютъра си. ESET Log Collector ви улеснява в събирането на необходимата информация. За повече информация относно ESET Log Collector прочетете статията в базата знания на ESET.

Режим за геймъри

Игралният режим е функция за потребители, които имат нужда от непрекъснато използване на техния софтуер, не искат да бъдат обезпокоявани от прозорци за известия/уведомления и искат да намалят използването на CPU. Игралният режим може също така да се използва по време на презентации, които не могат да се прекъсват от дейността на антивирусната програма. С разрешаването на тази функция всички изскачащи прозорци се забраняват и дейността на планировчика ще бъде спряна напълно. Защитата на системата все още продължава да е активна във фонов режим, но не изисква намеса от потребителя.

Можете да разрешите или забраните игралния режим в главния прозорец на програмата под **Настройка** > **Защита на компютъра**, като щракнете върху  или  до **Игрален режим**. Разрешаването на игралния режим е потенциален риск за защитата, затова и иконата за състоянието на защитата в лентата на задачите ще се оцвети в оранжево и ще показва предупреждение. Също така ще видите това предупреждение в главния прозорец на програмата, където се показва известието **Игрален режим е активен** в оранжево.

Активирайте **Разреши игралния режим автоматично при изпълнение на приложения в режим на цял екран** под Разширени настройки > **Инструменти** > **Игрален режим**, за да се стартира режимът за геймъри винаги, когато стартирате приложение на цял екран, и да прекъсва след излизане от приложението.

Активирайте **Забрани режима за геймъри автоматично след**, за да определите периода от време, след изтичането на който режимът за геймъри да бъде забранен автоматично.

Ако защитната стена е в интерактивен режим, а режимът за геймъри е разрешен, може да имате проблеми при свързването с интернет. Това може да е проблем, ако стартирате игра, която се играе в интернет. Обикновено ще ви бъде поискано потвърждение за подобно действие (ако не са били определени правила за комуникация или изключения), но намесата на потребителя е забранена в игралния режим. За да разрешите комуникация, дефинирайте правило за комуникация за всяко приложение, което може да срещне този проблем, или използвайте различен Режим на филтриране в защитната стена. Имайте предвид, че ако режимът за геймъри е разрешен и посетите уеб страница или приложение, което може да представлява риск за защитата, то може да бъде блокирано без никакво обяснение или предупреждение, тъй като взаимодействието с потребителя е забранено.

Диагностика

Диагностиката предоставя аварийни копия при срив на приложения за процесите на ESET (например ekrn). Ако възникне срив на дадено приложение, ще се създаде аварийно копие. Това може да помогне на разработчиците да дебъгват и отстраняват различни проблеми ESET Internet Security.

Щракнете върху падащото меню до **Тип аварийно копие** и изберете една от наличните три опции:

• Изберете **Забрани**, за да забраните тази функция.

• **Минимално** (по подразбиране) – записва минимален набор от полезна информация, която може да помогне за идентифициране на причината за неочаквания срив на приложението. Този тип файл за аварийно копие може да е полезен, когато пространството е ограничено. Но поради ограничения обем на включената информация грешките, които не са били породени директно от заплахата, възникнала по време на проблема, може да не бъдат открити при анализ на този файл.

• **Пълно** – Записва цялото съдържание на системната памет, когато дадено приложение спре неочаквано. Пълното разтоварване на паметта може да съдържа данни от процеси, които са се изпълнявали по време на събиране на данните от паметта.

Целева директория – Директорията, в която ще се създаде вторично копие по време на срив.

Отваряне на папката за диагностика – Щракнете върху **Отвори**, за да отворите тази директория в нов прозорец на *Windows Explorer*.

Създаване на аварийно копие за диагностика – Щракнете върху **Създаване**, за да създадете файлове с аварийно копие за диагностика в **целевата директория**.

Разширено регистриране

Разрешаване на разширено регистриране в маркетингови съобщения – Записвайте всички събития, свързани с маркетингови съобщения в продукта.

Разрешаване на разширено регистриране за модула за антиспам защита – Записвайте всички събития, които са възникнали по време на сканиране против спам. Това може да

помогне на разработчиците да диагностицират и отстраняват проблеми, свързани с антиспам системата на ESET.

Разрешаване на разширено регистриране за системата против кражба – Записвайте всички събития, които възникват в системата против кражба, за да дадете възможност за диагностициране и отстраняване на проблеми.

Разрешаване на разширено регистриране за защита на браузъра – записвайте всички събития, които настъпват в „Безопасно банкиране и сърфиране“.

Разрешаване на разширено регистриране за компютърния скенер – Записвайте всички събития, които възникват при сканиране на файлове и папки, чрез сканиране на компютъра.

Разрешаване на разширено регистриране за контрол на преносими паметини устройства – записвайте всички събития, които са възникнали във функцията за управление на външни устройства. Това може да помогне на разработчиците да диагностицират и отстраняват проблеми, свързани с функцията за управление на външни устройства.

Разрешаване на разширено регистриране за пряка връзка с облака – Записвайте всички събития, които са възникнали в ESET LiveGrid®. Това може да помогне на разработчиците да диагностицират и отстраняват проблеми, свързани с ESET LiveGrid®.

Разрешаване на разширено регистриране в защитата от ботнет мрежи – записва всички събития, които настъпват в защитата от ботнет мрежи, с цел позволяване на диагностика и разрешаване на проблеми.

Разрешаване на разширено регистриране на защитата на имейл клиенти – Запишете всички събития, които настъпват в защита на имейл клиенти и плъгин на имейл клиент за позволяване на диагностициране и разрешаване на проблеми.

Разрешаване на разширено регистриране на ядрото – Записвайте всички събития, които възникват в ядрото на ESET (ekrn).

Разрешаване на разширено регистриране за лицензиране – записвайте всички комуникации на продукти със сървърите за активиране или сървърите на ESET License Manager.

Разрешаване на проследяване на паметта – Записвайте всички събития, които помагат на разработчиците да диагностицират изтичания на памет.

Разрешаване на разширено регистриране за мрежовата защита – Записвайте всички мрежови данни, които минават през защитната стена, в формат PCAP, за да помогнете на разработчиците да диагностицират и отстраняват проблеми, свързани със защитната стена.

Активиране на разширено регистриране на скенера за мрежов трафик – Записвайте всички данни, преминаващи през скенера за мрежов трафик във формат PCAP, за да помогнете на разработчиците да диагностицират и отстраняват проблеми, свързани със скенера за мрежов трафик.

Разрешаване на разширеното регистриране на операционната система – Записвайте допълнителна информация за операционната система, като изпълняващи се процеси, активност на процесора, операции с дискове. Това може да помогне на разработчиците да диагностицират и коригират проблеми, свързани с продукта на ESET, който се изпълнява на вашата операционна система.

Разрешаване на разширено регистриране за родителския контрол – Записвайте всички събития, които са възникнали в "Родителски контрол". Това може да помогне на разработчиците да диагностицират и отстраняват проблеми, свързани с "Родителски контрол".

Разрешаване на разширено регистриране за изпращане на насочени съобщения – Записвайте всички събития, които се случват при изпращане на насочени съобщения.

Разрешаване на разширеното регистриране на защитата на файловата система в реално време – Записвайте всички събития, които възникват при сканиране на файлове и папки чрез защита на файловата система в реално време.

Разрешаване на разширено регистриране за системата за обновяване – записване на всички събития, случващи се по време на процеса по обновяването. Това може да помогне на разработчиците да диагностицират и отстраняват проблеми, свързани със системата за обновяване.

Регистрационните файлове се намират в *C:\ProgramData\ESET\ESET Security\Diagnostics*.

Техническа поддръжка

Когато се свързвате с отдела за техническа поддръжка на ESET от ESET Internet Security, можете да изпратите данни за конфигурацията на системата. Изберете **Изпращай винаги** от падащото меню **Изпращане на данните с конфигурация на системата**, за да изпратите данните автоматично, или изберете **Питай преди изпращане**, за да бъдете подканени преди подаване на данни.

Свързаност

В специфични мрежи прокси сървърът може да посредничи при комуникацията между вашия компютър и интернет. Ако използвате прокси сървър, трябва да дефинирате следните настройки. В противен случай ESET Internet Security и неговите модули не могат да се обновяват автоматично. В ESET Internet Security настройката на прокси сървъра е налична в два различни раздела на Разширени настройки.

Глобалните настройки на прокси сървъра може да се конфигурират в Разширени настройки > **Свързаност** > **Прокси сървър**. Указването на прокси сървър на това ниво определя общите настройки на прокси сървъра за цялата програма ESET Internet Security. Параметрите, зададени тук, ще се използват от всички модули, изискващи връзка с интернет.

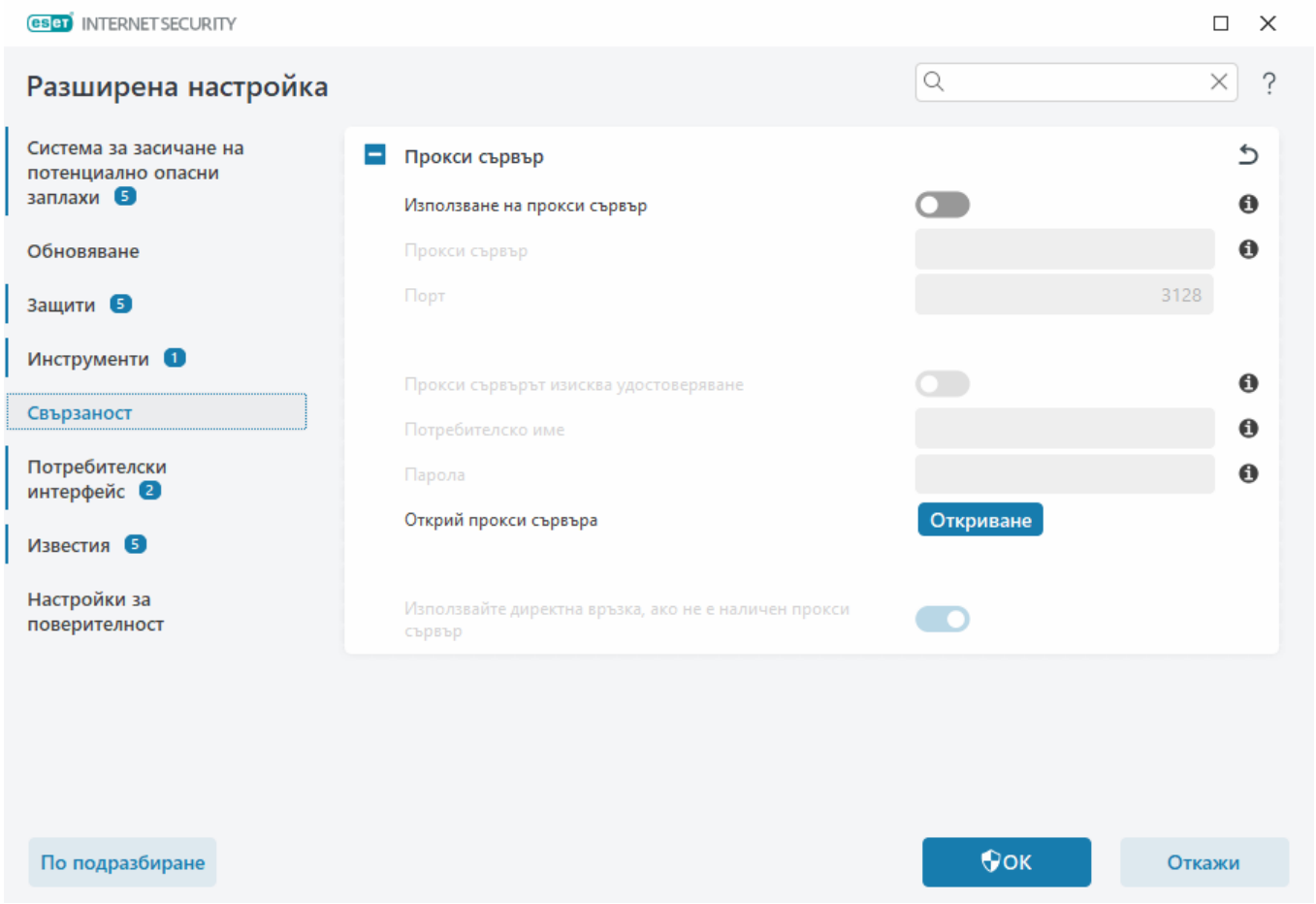
За да зададете глобалните настройки на прокси сървъра, разрешете **Използвай прокси сървър** и въведете адреса на **прокси сървъра** заедно с неговия номер на **порта**.

Ако комуникацията с прокси сървъра изисква удостоверяване, изберете **Прокси сървърът изисква удостоверяване** и въведете валидни **Потребителско име** и **Парола** в съответните полета. Щракнете върху **Открий прокси сървър**, за да бъдат открити и попълнени автоматично настройките на прокси сървъра. ESET Internet Security ще копира параметрите, посочени в интернет опциите за Internet Explorer или Google Chrome.

> Трябва ръчно да въведете потребителското си име и парола в настройките на **Прокси сървър**.

Използвай директна връзка, ако не е наличен прокси сървър – ако ESET Internet Security е конфигуриран да се свързва чрез прокси сървър, а прокси сървърът не е достъпен, ESET Internet Security ще заобиколи прокси сървъра и ще комуникира директно със сървърите на ESET.

Настройките на прокси сървъра могат също така да се конфигурират в Разширени настройки > **Обновяване** > **Профили** > **Обновявания** > **Опции за свързване**, като изберете **Свързване през прокси сървър** от падащото меню **Режим на прокси сървър**. Тази конфигурация се прилага само за обновявания и се препоръчва за лаптопи, които получават актуализации на модула от отдалечени местоположения. За повече информация вижте Разширени настройки за обновяване.



Потребителски интерфейс

За да конфигурирате функционирането на графичния потребителски интерфейс (GUI) на програмата, отворете Разширени настройки > **Потребителски интерфейс**.

Можете да настроите визуалните ефекти и облик на програмата в екрана за разширени настройки на Елементи на потребителския интерфейс.

За да осигурите максимална защита на софтуера за защита, можете да предотвратите деинсталиране или всякакви неупълномощени промени, като защитите настройките с парола с помощта на инструмента за Настройка на достъпа.

> За да конфигурирате поведението на системните известия, уведомленията за откриване и състоянията на приложението, вижте раздела Известия.

Елементи на потребителския интерфейс

Можете да настройвате работната среда на ESET Internet Security (GUI), за да отговаря на вашите нужди, от Разширени настройки > **Потребителски интерфейс** > **Елементи на потребителския интерфейс**.

Цветови режим – изберете цветовата схема на ESET Internet Security GUI от падащото меню:

- **Като цвета на системата** – задава цветовата схема на ESET Internet Security на базата на настройките на операционната система.
- **Тъмна** – ESET Internet Security ще има тъмна цветова схема (тъмен режим).
- **Светла** – ESET Internet Security ще има стандартна, светла цветова схема.

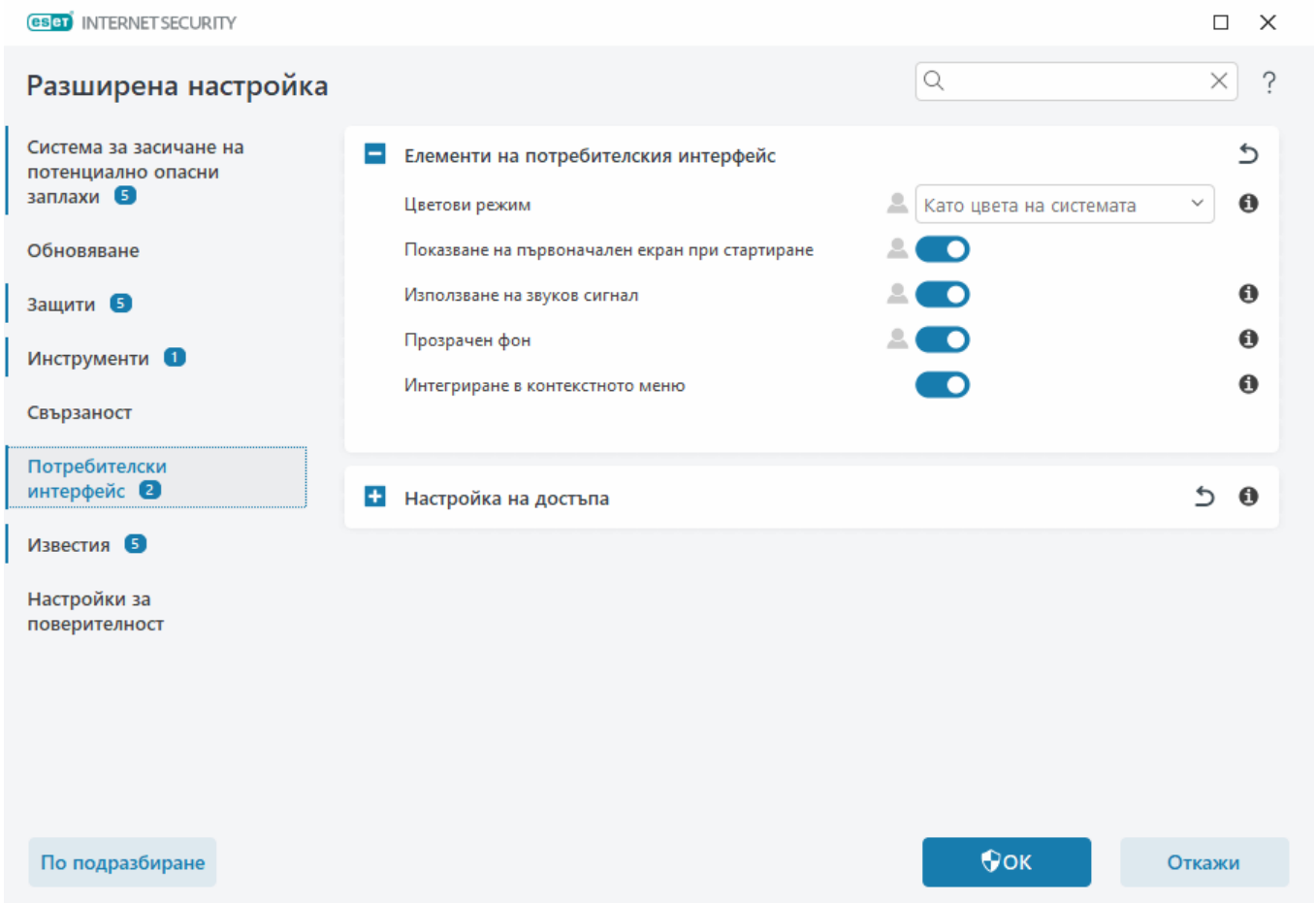
Можете също да изберете цветовата схема на графичния потребителски интерфейс на ESET Internet Security в горния десен ъгъл на главния прозорец на програмата.

Показване на първоначален екран при стартиране – показва първоначалния екран на ESET Internet Security при стартиране.

Използване на звуков сигнал – възпроизвежда звуков сигнал, когато възникне важно събитие по време на сканирането, например когато се открие заплаха или когато сканирането приключи.

Прозрачен фон – позволява прозрачен фонов ефект за главния прозорец на програмата. Прозрачен фон е достъпен само за най-новите версии на Windows (RS4 и по-нови).

Интегриране в контекстното меню – интегрира контролни елементи на ESET Internet Security в контекстното меню.



Настройка на достъпа

Настройките на ESET Internet Security са съществена част от вашите правила за защита. Неупълномощената промяна може да застраши стабилността и защитата на вашата система. За да се избегнат неупълномощени промени, параметрите на настройката и деинсталирането на ESET Internet Security могат да се защитят с парола. Настройката на достъпа може да бъде конфигурирана в Разширени настройки > **Потребителски интерфейс** > **Настройка на достъпа**.

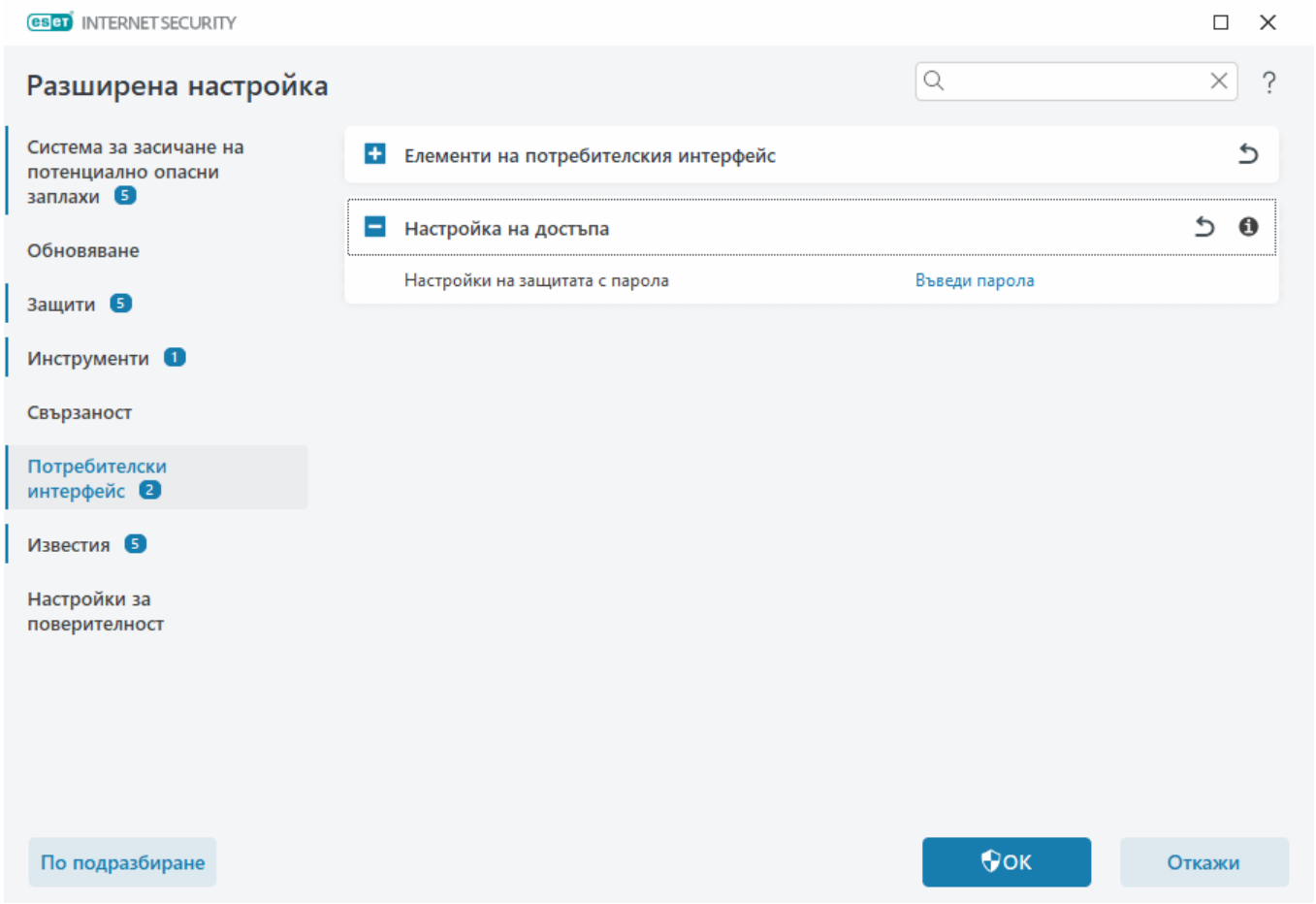
За да зададете парола за защита на параметрите на настройката и деинсталирането на ESET Internet Security, щракнете върху **Задаване** до **Настройки на защитата с парола**.

Когато искате да получите достъп до защитените разширени настройки, се показва прозорецът за въвеждане на паролата. Ако забравите или загубите своята парола, щракнете върху опцията **Възстановяване на парола** отдолу и въведете имейл адреса, който сте използвали за регистриране на абонамента. ESET ще ви изпрати имейл с код за проверка и инструкции как да подновите паролата си.

- Как се отключват разширените настройки

За да промените паролата си, щракнете върху **Промяна на паролата** до **Настройки на защитата с парола**.

За да премахнете паролата си, щракнете върху **Премахване** до **Настройки на защитата с парола**.



Парола за „Разширени настройки“

За да защитите разширените настройки на ESET Internet Security и да избегнете неоторизирана промяна, въведете новата си парола в полетата **Нова парола** и **Потвърждаване на паролата**. Щракнете върху **ОК**.

Когато искате да промените съществуваща парола:

1. Въведете старата парола в полето **Стара парола**.
2. Въведете вашата нова парола в полетата **Нова парола** и **Потвърждаване на паролата**.
3. Щракнете върху **ОК**.

Тази парола ще е необходима за достъп до разширените настройки.

Ако забравите паролата си, вижте Отключване на паролата за настройки в продукти ESET HOME.

За да възстановите загубен ключ за активиране на ESET, датата на изтичане на абонамента или друга информация за абонамента за ESET Internet Security, вж. Изгубих ключа си за активиране.

Поддръжка на екранни четци

ESET Internet Security може да се използва заедно с екранни четци, за да могат потребителите на ESET с нарушено зрение да навигират в продукта или да конфигурират настройките.

Поддържат се следните екранни четци (JAWS, NVDA, Narrator).

За да се уверите, че софтуерът за екранния четец може да осъществява достъп до GUI на ESET Internet Security правилно, следвайте инструкциите в нашата статия в онлайн помощника.

Известия

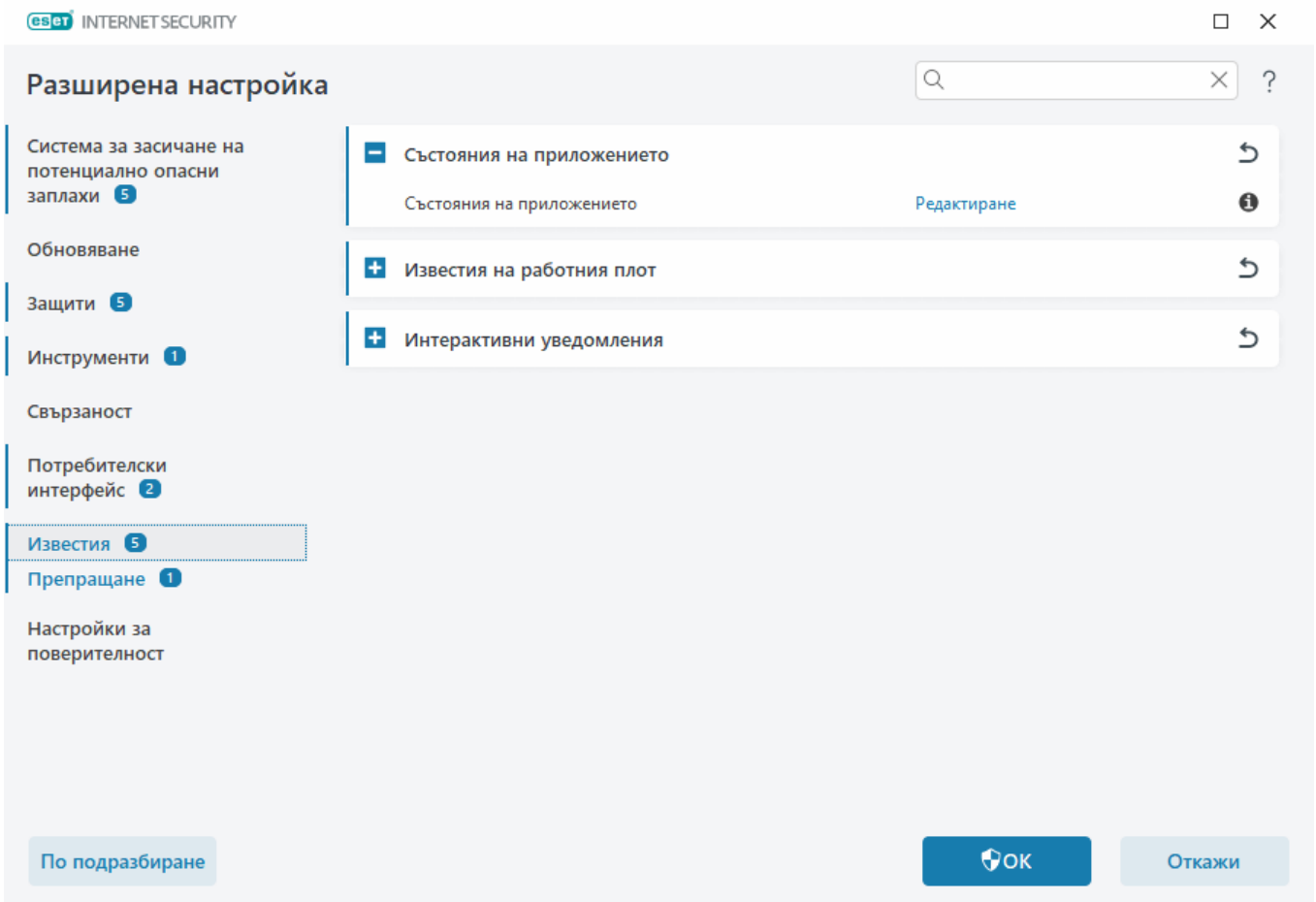
За да управлявате известията на ESET Internet Security, отворете Разширени настройки > **Известия**. Можете да конфигурирате следните видове известия:

• Състояния на приложението – известията, показвани в главния прозорец на програмата > **Преглед**.

• Известия на работния плот – Малки прозорци с известия до лентата на задачите на системата.

• Интерактивни уведомления – Прозорци за уведомления и полета със съобщения, които изискват намеса на потребителя.

• Препращане (известия по имейл) – имейл известията се изпращат до посочения имейл адрес.



Състояния на приложението

Състояния на приложението – Щракнете върху **Редактиране**, за да изберете кои състояния на приложението ще бъдат показани в началния раздел на главния прозорец на програмата > **Преглед**.

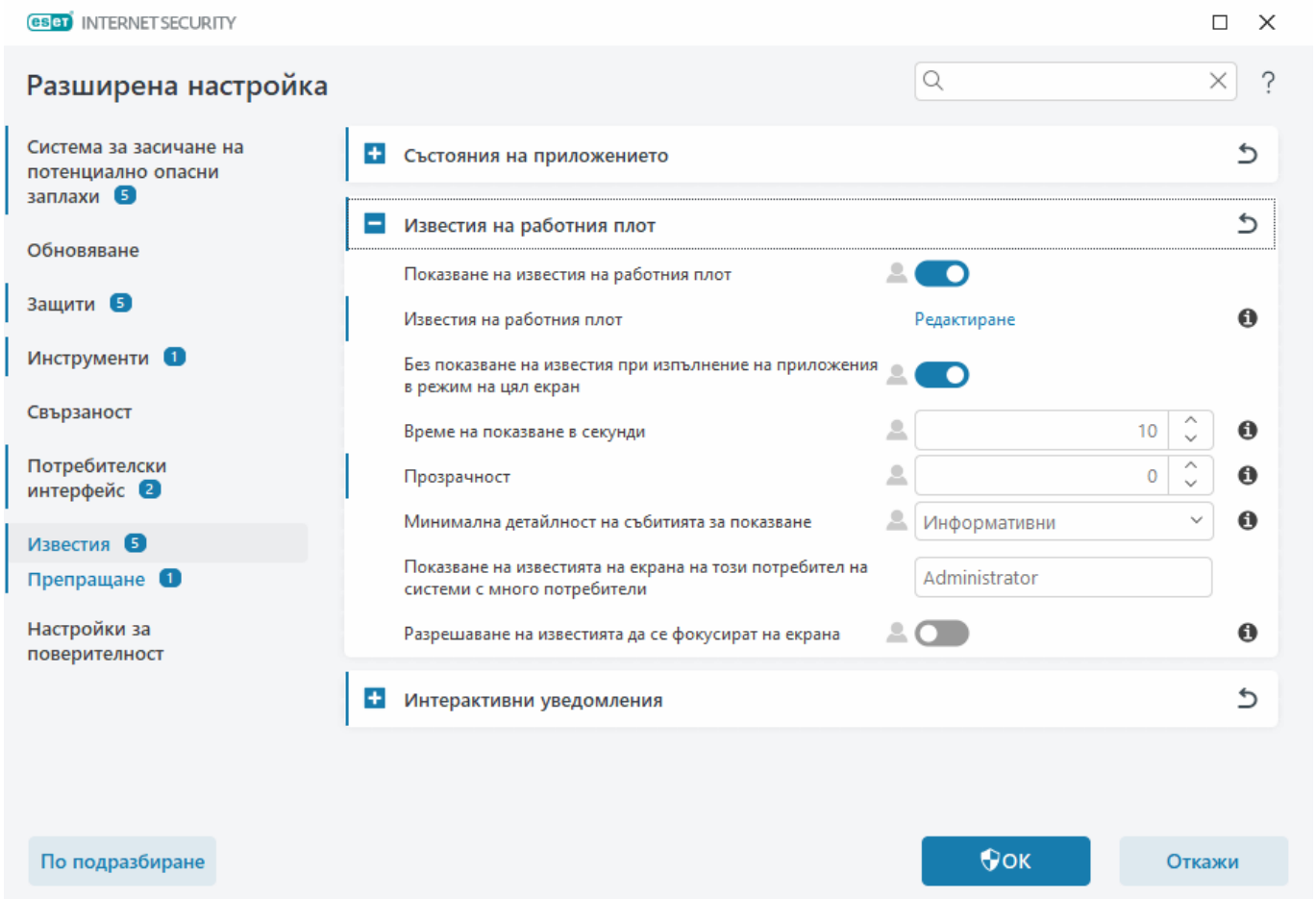
Диалогов прозорец – Състояния на приложението

В този диалогов прозорец можете да изберете кои състояния на приложението да се показват. Например, когато спрете временно защитата от вируси и шпионски софтуер или когато разрешите игралния режим.

Състояние на приложението ще се показва също и ако вашият продукт не е активиран или ако абонаментът ви е изтекъл.

Известия на работния плот

Известията за работния плот са представят от малък прозорец за известие до системната лента на задачите. По подразбиране той се показва за 10 секунди, след което бавно изчезва. Известията включват успешни обновявания на продукти, нови свързани устройства, приключване на задачи за сканиране за вируси или намерени нови заплахи.



Показване на известия на работния плот – препоръчваме да оставите тази опция разрешена, за да може продуктът да ви информира кога възниква дадено ново събитие.

Известия на работния плот – Щракнете върху **Редактиране**, за да разрешите или забраните определени Известия на работния плот.

Без показване на известия при изпълнение на приложения в режим на цял екран – блокирайте всички неинтерактивни известия, когато изпълнявате приложения в режим на цял екран.

Време на показване в секунди – Задайте продължителността на видимост на известията. Стойността трябва да е между 3 – 30 секунди.

Прозрачност – Задайте процента на прозрачност на известията. Поддържаният диапазон е 0 (без прозрачност) до 80 (много висока прозрачност).

Минимално ниво на детайлност на събитията за показване – Задайте началното ниво на сериозност на показваните известия. От падащото меню изберете една от следните опции:

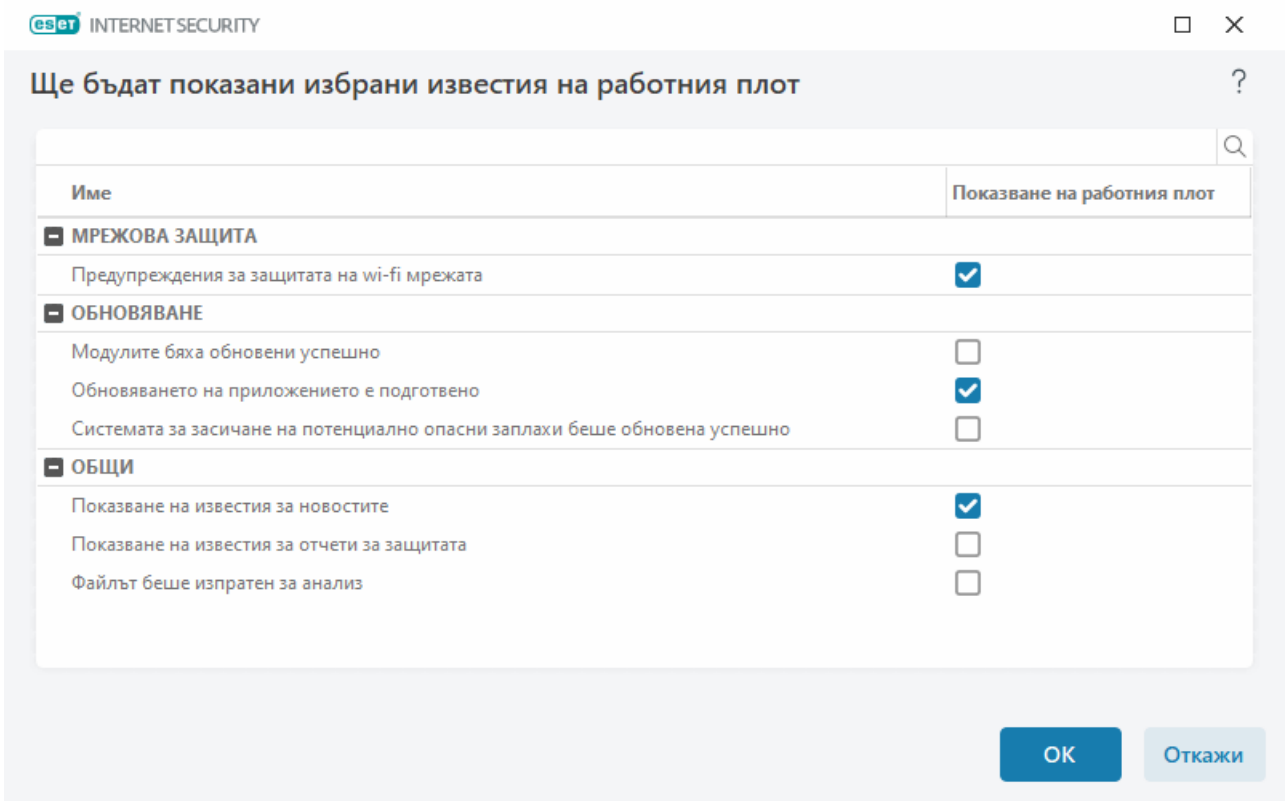
- **Диагностични** – Регистрира информация, необходима за прецизна настройка на програмата, и всички записи по-горе.
- **Информативни** – Показва информативни съобщения, като например нестандартни събития в мрежата, включително съобщения за успешно обновяване, както и всички записи по-горе.
- **Предупреждения** – показва предупредителни съобщения, грешки и критични грешки (например неуспешно обновяване).
- **Грешки** – Показва грешки (например защитата от ботнет мрежи не е стартирана) и критични грешки.
- **Критични** – Показва само критични грешки (грешка в стартирането на антивирусната защита или заразена система и т.н.).

В системи с няколко потребители да се показват известия на екрана на този потребител – Позволява определен акаунт да получава известия на работния плот. Ако например не използвате акаунта на администратор, въведете пълното име на акаунта и известията на работния плот ще се показват за посочения акаунт. Само един потребителски акаунт може да получава известията на работния плот.

Разрешаване на известията да се фокусират на екрана – Позволява на известията да се фокусират на екрана и са достъпни в менюто **ALT + Tab.**.

Списък с известия на работния плот

За да регулирате видимостта на известията на работния плот (показват се в долния десен ъгъл на екрана), отворете Разширени настройки > **Известия** > **Известия на работния плот**. Щракнете върху **Редактиране** до **Известия на работния плот** и поставете отметка в подходящото квадратче за отметка **Показване**.



Общи

Показване на известия за отчети за защитата – получавайте известие, когато се генерира нов отчет за защитата.

Показване на известия за новостите – известия за всички нови и подобрени функции на най-новата версия на продукта.

Файлът беше изпратен за анализе изпратен за анализ – получавайте известие всеки път, когато ESET Internet Security изпраща файл за анализ.

Мрежов инспектор

Уведомяване за новооткрити мрежови устройства – получаване на известие, когато към мрежата е свързано ново устройство.

Мрежова защита

Мрежовият профил е променен – получаване на известие при промяна на мрежовия профил.

Предупреждения за защита на WiFi – Получавайте известие, когато се опитвате да се свържете с Wi-Fi мрежа със слаба парола или без парола.

Обновяване

Обновяването на приложението е подготвено – получавайте известие, когато има готово обновяване до нова версия на ESET Internet Security.

Системата за засичане на потенциално опасни заплахи беше обновена успешно –

получавайте известие, когато продуктът обновява модулите на системата за засичане на потенциално опасни заплахи.

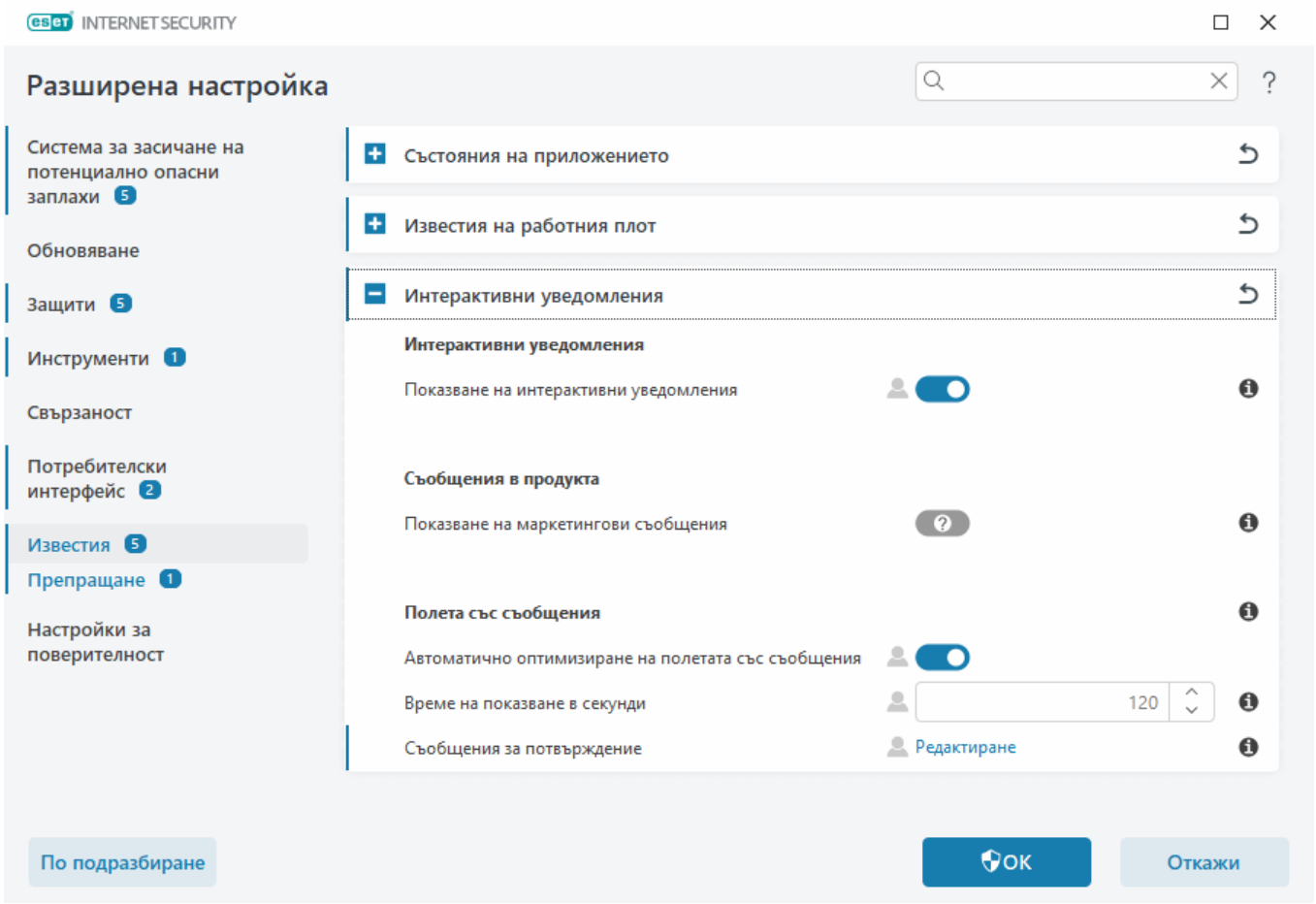
Модулите бяха обновени успешно – получавайте известие, когато продуктът обновява компонентите на програмата.

За да настроите общите настройки за известия на работния плот, като например колко дълго дадено съобщение да се показва или минималната детайлност на събитията за показване, вж. Известия на работния плот в Разширени настройки > **Известия**.

Интерактивни уведомления

Търсите информация за общи уведомления и известия?
- Открита е заплаха
- Адресът е блокиран
- Продуктът не е активиран
- Преминаване към продукт с повече функции
- Преминаване към продукт с по-малко функции
- Налична е обновяване
- Информацията за обновяване не е постоянна
- Отстраняване на неизправности за съобщението „Неуспешно обновяване на модулите“
- Отстраняване на грешки при обновяване на модули
- Блокирана е мрежова заплаха
- Сертификатът на уеб сайта е анулиран

Разделът **Интерактивни уведомления** в Разширени настройки > **Известия** ви позволява да конфигурирате как полетата със съобщения и интерактивните уведомления за откривания се обработват от ESET Internet Security, когато е необходимо да се вземе решение от потребител (например потенциални уеб сайтове за фишинг).



Интерактивни уведомления

Забраняването на **Показване на интерактивни уведомления** ще скрие всички прозорци за уведомления и диалогови прозорци в браузъра и е подходящо само при определени ситуации. Препоръчваме тази опция да се остави разрешена.

Съобщения в продукта

Съобщенията в продукта са създадени да информират потребителите за новини от ESET и други комуникации. Изпращането на маркетингови съобщения изисква съгласието на потребител. Следователно маркетинговите съобщения не се изпращат до потребител по подразбиране (показан като въпросителен знак). Като разрешите тази опция, се съгласявате да получавате маркетингови съобщения от ESET. Ако нямате интерес към **получаването на маркетингов материал** от ESET, забранете опцията.

Полета със съобщения

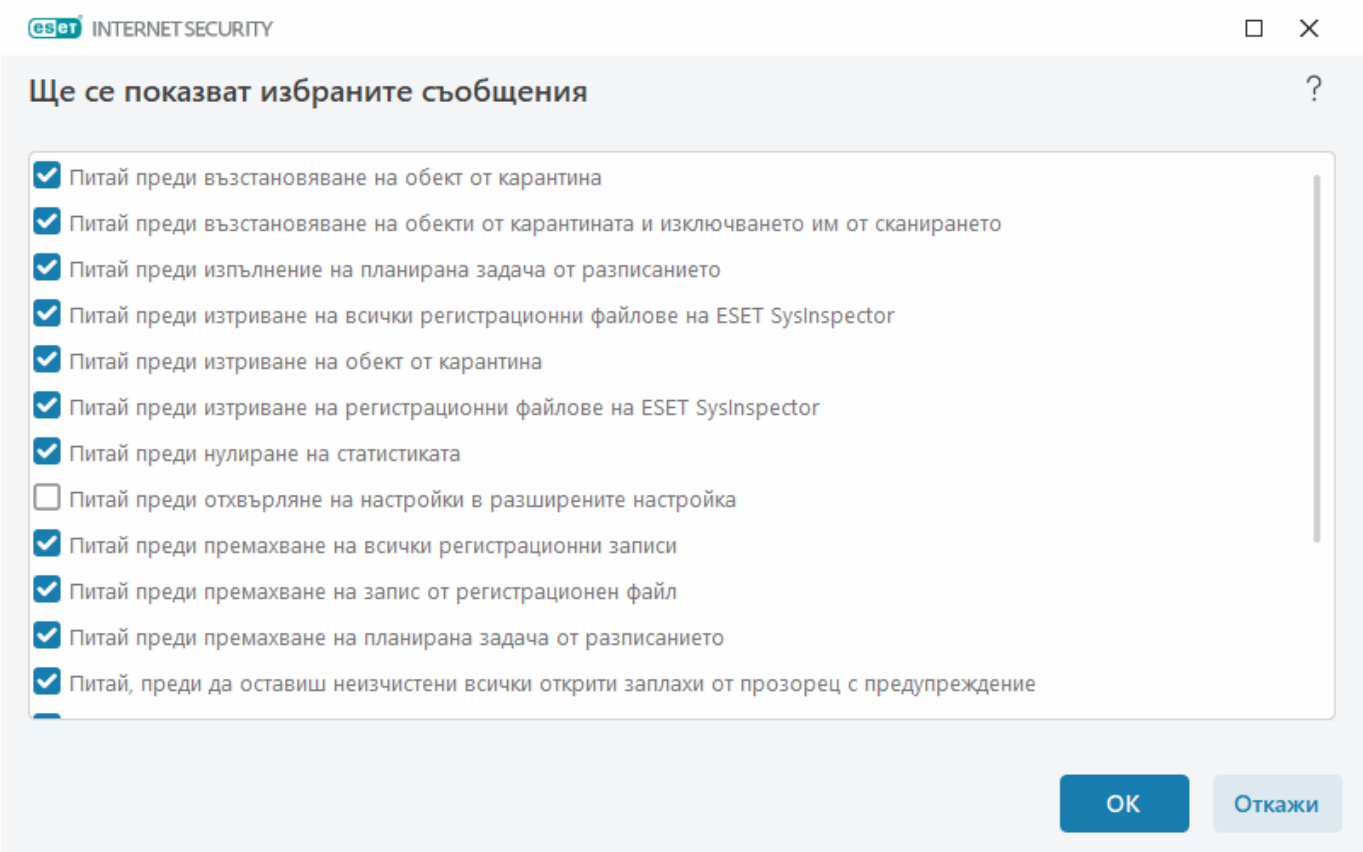
За да се затварят полетата със съобщения автоматично след определен период от време, изберете **Автоматично затваряне на полетата със съобщения**. Ако не бъдат затворени ръчно, прозорците с уведомления се затварят автоматично след изтичане на указаното време.

Време на показване в секунди – Задава продължителността на видимост на уведомленията. Стойността трябва да е между 10 – 999 секунди.

Съобщения за потвърждение – Щракнете върху **Редактиране**, за да се покаже списък със съобщения за потвърждение, които можете да изберете дали да се показват, или не.

Съобщения за потвърждение

За да коригирате съобщенията за потвърждение, отидете до Разширени настройки > **Известия** > **Интерактивни уведомления** и щракнете върху **Редактиране** до **Съобщения за потвърждение**.



Този диалогов прозорец показва съобщения за потвърждение, които ESET Internet Security извежда, преди да се извърши каквото и да било действие. Поставете или премахнете отметката в квадратчето до всяко съобщение за потвърждение, за да го разрешите или забраните.

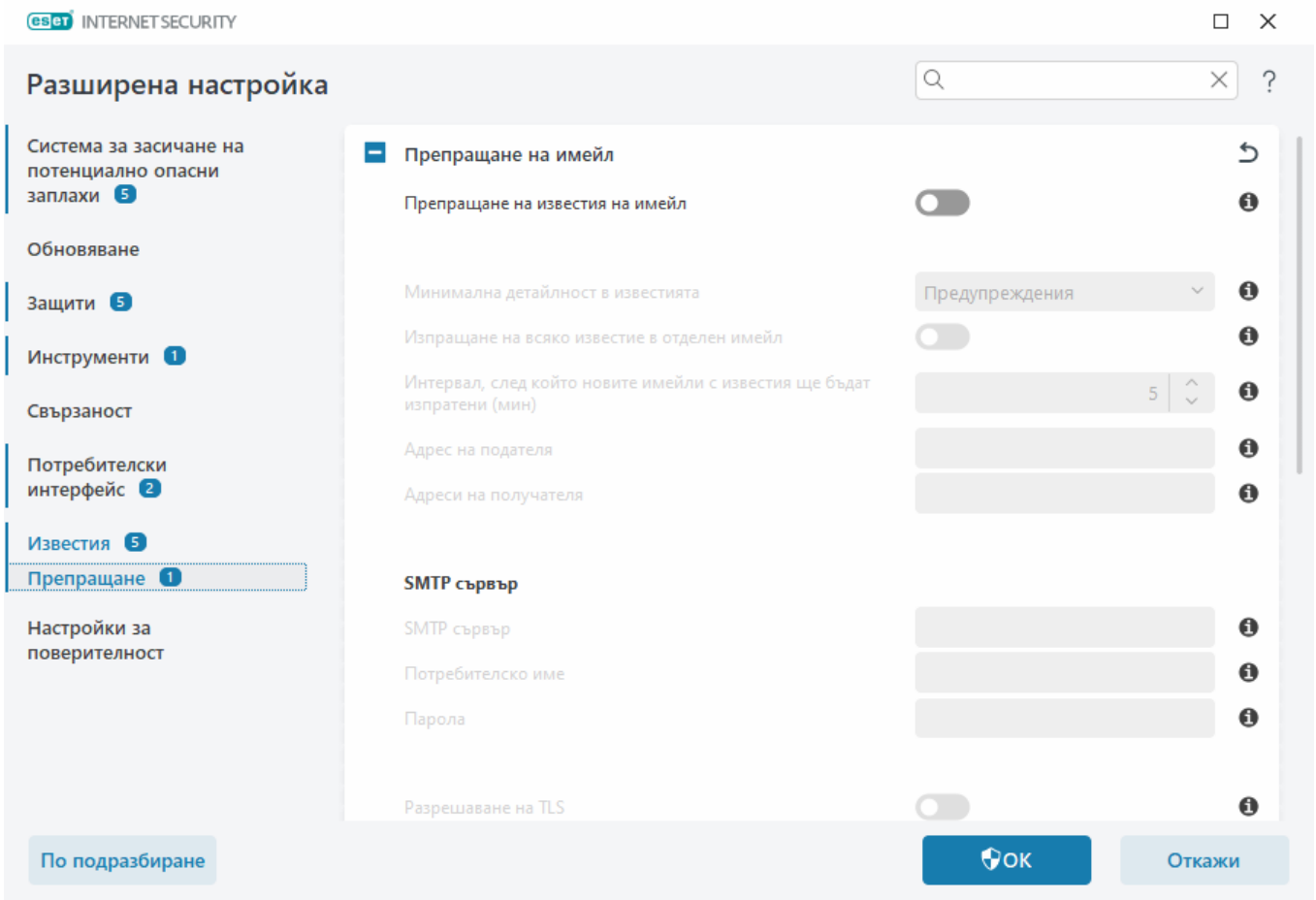
Научете повече за конкретната функция, свързана със съобщенията за потвърждение:

- Питай преди изтриване на дневници на ESET SysInspector
- Питай преди изтриване на всички дневници на ESET SysInspector
- Питай преди изтриване на обект от карантина
- Питай преди отхвърляне на настройки в разширените настройка
- Питай, преди да оставиш неизчистени всички открити заплахи от прозорец с предупреждение
- Питай преди премахване на запис от регистрационен файл
- Питай преди премахване на планирана задача в планировчика
- Питай преди премахване на всички регистрационни записи

- Питай преди нулиране на статистиката
- Питай преди възстановяване на обект от карантина
- Питай преди възстановяване на обекти от карантината и изключването им от сканирането
- Питай преди изпълнение на планирана задача с планировчика
- Показване на известия за резултатите от обработката на антиспам защита
- Показване на известия за резултатите от обработката на антиспам защита за имейл клиенти
- Показвай диалогови прозорци за потвърждение на продукт за имейл клиентите Outlook Express и Windows Mail
- Показвай диалогови прозорци за потвърждение на продукт за Windows Live Mail
- Показвай диалогови прозорци за потвърждение на продукт от имейл клиента Outlook

Препращане

ESET Internet Security може автоматично да изпраща имейли с известия, ако възникне събитие с определеното ниво на детайлност. Отворете Разширени настройки > **Известия** > **Препращане** и разрешете **Препращане на известия на имейл**, за да активирате известия по имейл.



От падащото меню **Минимална детайлност в известията** можете да изберете началното ниво на сериозност на известията за изпращане.

• **Диагностични** – Регистрира информация, необходима за прецизна настройка на програмата, и всички записи по-горе.

• **Информативни** – регистриране на информативни съобщения, като например нестандартни събития в мрежата, включително съобщения за успешно обновяване и всички записи по-горе.

• **Предупреждения** – регистриране на съобщения за критични грешки и предупреждения (например неуспешно обновяване).

• **Грешки** – ще бъдат записани грешките (защитата на документи не се стартира) и критичните грешки.

• **Критични** – регистриране само на критични грешки (например грешка в стартирането на антивирусната защита или открита заплаха).

Изпращане на всяко известие в отделен имейл – Ако тази опция е разрешена, получателят ще получава нов имейл за всяко известие. Това може да доведе до много имейли, получени за кратък период от време.

Интервал, след който новите имейли с известия ще бъдат изпратени (мин) – интервал в минути, след който новите известия ще бъдат изпратени на имейл. Ако зададете стойност 0, известията ще се изпращат незабавно.

Адрес на подателя – Определя адреса на подателя, който ще се показва в заглавката на имейлите за известие.

Адреси на получателя – Определя адресите на получатели, показвани в заглавката на имейлите с известия. Поддържат се множество стойности. Използвайте точка и запетая като разделител.

сървър на SMTP

SMTP сървър – SMTP сървърът, който се използва за изпращане на известия (например smtp.provider.com:587, предварително зададеният порт е 25).

SMTP сървъри с TLS шифроване се поддържат от ESET Internet Security.

Потребителско име и **парола** – Ако SMTP сървърът изисква удостоверяване, тези полета трябва да са попълнени с валидно потребителско име и парола, за да се предостави достъп до SMTP сървъра.

Разрешаване на TLS – защитени уведомления и известия чрез TLS криптиране.

Тестване на SMTP връзка – тестов имейл ще бъде изпратен на имейл адреса на получателя. Трябва да бъдат попълнени SMTP сървър, потребителско име, парола, адрес на изпращача и адреси на получателите.

Формат на съобщенията

Комуникацията между програмата и отдалечен потребител или системен администратор се извършва чрез имейли или съобщения по вътрешната мрежа (чрез услугата за съобщения на Windows). **Форматът по подразбиране на предупредителните съобщения** и известия е оптимален в повечето случаи. При някои обстоятелства може да се наложи да промените формата на съобщенията за събития.

Формат на съобщенията за събития – формат на съобщенията за събития, показвани на отдалечените компютри.

Формат на предупредителните съобщения за заплахи – Съобщенията с известия и предупреждения за заплахи имат предварително определен формат по подразбиране. Препоръчваме запазването на предварително определения формат. В някои случаи обаче (например, ако имате система за автоматично обработване на имейли) може да е необходимо да промените формата на съобщенията.

Набор от знаци – преобразува дадено имейл съобщение в ANSI кодиране на знаци, базирано на регионалните настройки на Windows (например windows-1250, Unicode (UTF-8), ACSII 7-bit или Japanese (ISO-2022-JP)). В резултат на това "á" ще бъде променено на "a", а непознатите символи на "?".

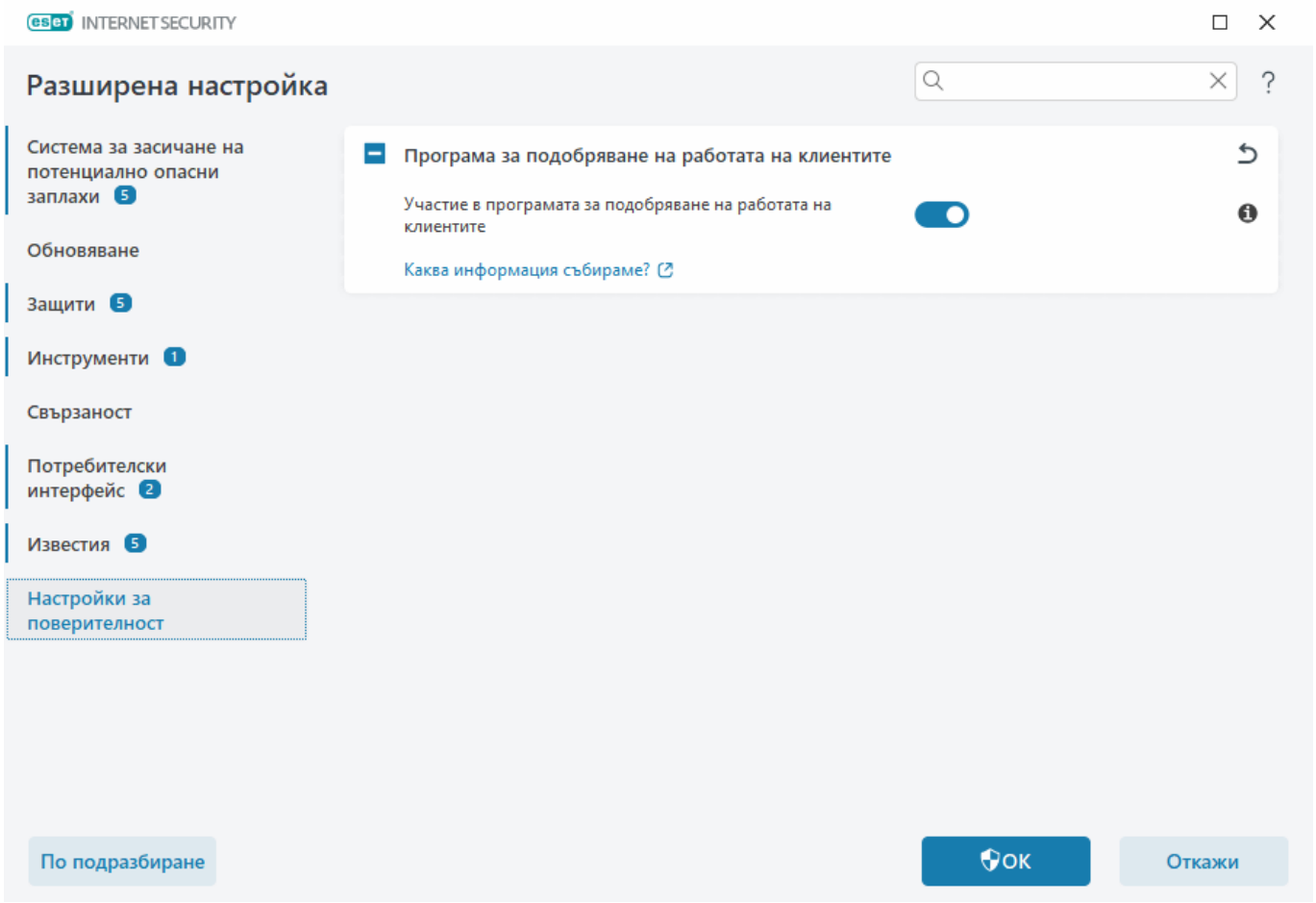
Използване на кодиране "Печатаем текст в кавички" – Източникът на имейл съобщението ще се кодира във формат "Печатаем текст в кавички" ((QP)), който използва ASCII знаци и може да предава правилно специалните национални знаци по имейл в 8-битов формат (áéíóú).

- **%TimeStamp%** – Дата и час на събитието
- **%Scanner%** – Засегнат модул
- **%ComputerName%** – Името на компютъра, където е възникнало уведомяването
- **%ProgramName%** – Програмата, която е генерирала уведомяването
- **%InfectedObject%** – Името на заразения файл, съобщение и т.н.
- **%VirusName%** – Идентифициране на заразяването
- **%Action%** – Предприето действие срещу проникване
- **%ErrorDescription%** – Описание на събитие, което не касае вирус

Ключовите думи **%InfectedObject%** и **%VirusName%** се използват само в предупредителни съобщения за заплахи, а **%ErrorDescription%** се използва само в съобщенията за събитие.

Настройки за поверителност

Отворете Разширени настройки > **Настройки за поверителност**.



Програма за подобряване на работата на клиентите

Разрешете плъзгача до **Участие в програмата за подобряване на работата на клиентите**, за да се присъедините към програмата за подобряване на работата на клиентите. С присъединяването си вие предоставяте на ESET анонимна информация, свързана с използването на продуктите на ESET. Събраните данни ни помагат да подобряваме вашата работа никога да не се споделя с трети лица. Каква информация събираме?

Възстановяване на настройките по подразбиране

Щракнете върху **По подразбиране** в разширените настройки, за да възстановите всички програмни настройки за всички модули. Те ще се възстановят в състоянието, в което биха били след ново инсталиране.

Вижте също настройки за импортиране и експортиране.

Възстановяване на всички настройки в текущия раздел

Щракнете върху извитата стрелка , за да възстановите всички настройки в текущия раздел към настройките по подразбиране, определени от ESET.

Имайте предвид, че всички извършени промени ще бъдат загубени, след като щракнете върху **Възстановяване на настройките по подразбиране**.

Възстановяване на съдържанието на таблиците – когато тази опция е разрешена, правилата, задачите и профилите, добавени ръчно или автоматично, ще бъдат загубени.

Вижте също настройки за импортиране и експортиране.

Грешка при записване на конфигурацията

Това съобщение за грешка указва, че настройките не са записани правилно вследствие на дадена грешка.

Това обикновено означава, че потребителят, който е опитал да промени параметрите на програмата:

• има недостатъчни права за достъп или не разполага с необходимите права за операционната система, за да промени конфигурационните файлове и системния регистър.
> За да бъдат изпълнени желаните промени, системният администратор трябва да влезе.

• скоро е разрешил режима за обучение в HIPS или защитната стена и се е опитал да направи промени в разширените настройки.
> За да се запази конфигурацията и да се избегне конфликт с конфигурацията, затворете разширените настройки, без да запазвате, и се опитайте да направите желаните промени отново.

Втората най-често разпространена причина е програмата да не работи правилно, повредена е и следователно се налага да бъде преинсталирана.

Програма за сканиране на командни редове

Антивирусният модул на ESET Internet Security може да се стартира през командния ред – ръчно (с командата "ecls") или с комбиниран ("bat") файл.

Използване на скенера с команден ред на ESET:

```
ecls [OPTIONS..] FILES..
```

Може да се използват следните параметри и ключове, докато се изпълнява програмата за сканиране при поискване от командния ред:

Опции

/base-dir=ПАПКА	зареждане на модулите от ПАПКА
/quar-dir=ПАПКА	ПАПКА за карантина
/exclude=МАСКА	изключване на файловете с тази МАСКА от сканирането

/subdir	сканират се подпапките (по подразбиране)
/no-subdir	не се сканират подпапките
/max-subdir-level=НИВО	максимално подниво на вложени папки за сканиране
/symlink	проследяване на символичните връзки (по подразбиране)
/no-symlink	пропускат се символичните връзки
/ads	сканиране на ADS (по подразбиране)
/no-ads	не се сканира ADS
/log-file=ФАЙЛ	записите се регистрират във ФАЙЛ
/log-rewrite	изходният файл се презаписва (по подразбиране се прикрепя към него)
/log-console	регистриране на резултатите в конзолата (по подразбиране)
/no-log-console	не се регистрират резултатите в конзолата
/log-all	регистриране също така и на чистите файлове
/no-log-all	не се регистрират чистите файлове (по подразбиране)
/aind	показване на индикатор за действията
/auto	сканиране и автоматично почистване на всички локални дискове

Опции на програмата за сканиране

/files	сканиране на файловете (по подразбиране)
/no-files	не се сканират файловете
/memory	сканиране на паметта
/boots	сканиране на секторите за начално стартиране
/no-boots	не се сканират секторите за начално стартиране (по подразбиране)
/arch	сканират се архивите (по подразбиране)
/no-arch	не се сканират архивите
/max-obj-size=РАЗМЕР	сканиране само на файловете, които са по-малки от РАЗМЕР мегабайта (по подразбиране 0 = неограничен)
/max-arch-level=НИВО	максимално подниво на вложени архиви за сканиране
/scan-timeout=ОГРАНИЧЕНИЕ	сканиране на архивите за максимум ЛИМИТ секунди
/max-arch-size=РАЗМЕР	сканиране само на файловете в архива, ако те са по-малки от РАЗМЕР (по подразбиране 0 = неограничен)
/max-sfx-size=РАЗМЕР	сканиране само на файловете в саморазархивиращи се файлове, ако са по-малки от РАЗМЕР мегабайта (по подразбиране 0 = неограничен)
/mail	сканиране на имейл файловете (по подразбиране)
/no-mail	не се сканират имейл файлове
/mailbox	сканират се пощенските кутии (по подразбиране)
/no-mailbox	не се сканират пощенските кутии
/sfx	сканират се саморазархивиращите се файлове (по подразбиране)
/no-sfx	не се сканират саморазархивиращи се архиви
/rtp	сканиране на архиватори в реално време (по подразбиране)

/no-rtp	не се сканират програми за пакетиране
/unsafe	сканират се потенциално опасни приложения
/no-unsafe	не се сканират потенциално опасни приложения (по подразбиране)
/unwanted	сканират се потенциално нежелани приложения
/no-unwanted	не се сканират потенциално нежеланите приложения (по подразбиране)
/suspicious	сканират се подозрителни приложения (по подразбиране)
/no-suspicious	не се сканират подозрителните приложения
/pattern	използване на сигнатурите (по подразбиране)
/no-pattern	не се използват сигнатури
/heur	разрешаване на евристики (по подразбиране)
/no-heur	не се разрешават евристики
/adv-heur	разрешаване на разширени евристични методи (по подразбиране)
/no-adv-heur	не се разрешават разширени евристични методи
/ext-exclude=РАЗШИРЕНИЯ	изключват се от сканиране файлови РАЗШИРЕНИЯ, разделени с двоеточие
/clean-mode=РЕЖИМ	използва се РЕЖИМ на почистване за заразени обекти Налични са следните опции: • none (по подразбиране) – не се извършва автоматично почистване. • standard – ecls.exe ще се опита да почисти или изтрие заразените файлове автоматично. • строго – ecls.exe ще се опита да почисти или изтрие заразените файлове автоматично без намесата на потребителя (няма да получите подкана преди изтриването на файловете). • щателно – ecls.exe ще изтрие файловете, без да се опита да ги почисти, независимо какъв е файлът. • изтриване – ecls.exe ще изтрие файловете, без да се опита да ги почисти, но няма да изтрие поверителните файлове, като например системните файлове на Windows.
/quarantine	копирай заразените файлове (ако са изчистени) в папката за карантина (допълва действието, което се извършва при почистване)
/no-quarantine	заразените файлове не се поставят под карантина

Общи опции

/help	показване на помощ и затваряне
/version	показване на версия и затваряне
/preserve-time	запазване на клеймото за последен достъп

Кодове при изход

0	няма открити заплахи

1	заплахата е открита и изчистена
10	някои файлове не можаха да се сканират (може да се заплахи)
50	намерена заплаха
100	грешка

Кодове при изход, по-големи от 100, означават, че файлът не е бил сканиран и съответно може да е заразен.

ЧЗВ

По-долу може да откриете някои от най-често задаваните въпроси и срещани проблеми. Щракнете върху заглавието на темата, за да разберете как да отстраните проблема:

- Как се обновява ESET Internet Security
- ESET Internet Security откри заплаха
- Как се премахва вирус от компютъра
- Как се разрешава комуникацията за дадено приложение
- Как се разрешава функцията за родителски контрол за даден акаунт
- Как се създава нова задача в планировчика
- Как се планира задача за сканиране (седмично)
- Как се отключват разширените настройки
- Как се разрешава деактивиране на продукт от ESET HOME

Ако вашият проблем не е включен в списъка по-горе, опитайте да търсите в онлайн помощта на ESET Internet Security.

Ако не намерите решение на проблема/въпроса в онлайн помощта на ESET Internet Security, може да посетите нашия редовно обновяван Онлайн помощник на ESET. По-долу са включени връзки към най-известните статии в нашия Онлайн помощник:

- Как да подновя абонамента си?
- Получих грешка при активиране, докато инсталирах продукта на ESET. Какво означава?
- Активиране на моя продукт на ESET за домашна употреба за Windows с помощта на ключа за активиране
- Деинсталиране или преинсталиране на моя продукт на ESET за домашна употреба
- Получавам грешка, че инсталацията на ESET беше прекратена преждевременно
- Какво е необходимо да направя след подновяване на абонамента? (потребители на Home)

- Какво се случва, ако си променя имейл адреса?
- Прехвърляне на моя продукт на ESET към нов компютър или устройство
- Как да стартирам Windows в безопасен режим или безопасен режим с работа в мрежата
- Изключване на безопасен уеб сайт от това да бъде блокиран
- Позволяване на достъп до GUI на ESET за софтуер за екранни четци

Ако е необходимо, може да се свържете с отдела за техническа поддръжка с въпроси или проблеми.

Как се обновява ESET Internet Security

Обновяването на ESET Internet Security може да се извърши ръчно или автоматично. За да стартирате обновяването, щракнете върху **Обнови** в основния прозорец на програмата и след това щракнете върху **Проверка за обновявания**.

Настройките за инсталиране по подразбиране създават задача за автоматично обновяване, която се изпълнява на всеки час. Ако се налага да промените интервала, отидете в **Инструменти** > Планировчик.

Как се премахва вирус от компютъра

Ако компютърът има симптоми на зараза със злонамерен софтуер, като например работи по-бавно, често блокира и т.н., ви препоръчваме да направите следното:

1. В главния прозорец на програмата щракнете върху **Сканиране на компютъра**.
2. Щракнете върху **Сканиране на компютъра**, за да започне сканиране на системата.
3. След като сканирането завърши, прегледайте регистрационния файл за броя на сканираните, заразените и почистените файлове.
4. Ако искате да сканирате само определена област от диска, щракнете върху **Сканиране по избор** и изберете цели, които да бъдат сканирани за вируси.

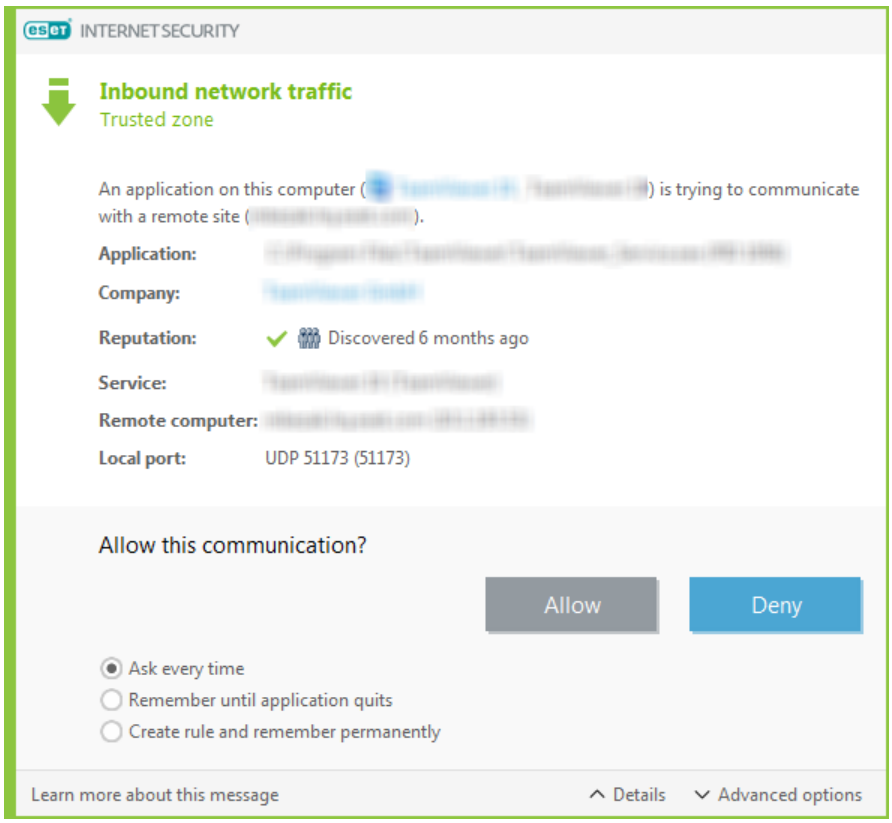
За допълнителна информация вж.:

- статията в онлайн помощника на ESET
- Карантина

Как се разрешава комуникацията за дадено приложение

Ако в интерактивен режим бъде открита нова връзка и няма съответстващо правило, ще се появи подкана да **позволят** или **откажет** е връзката. Ако искате ESET Internet Security да

изпълнява същото действие при всеки опит на приложението за установяване на връзка, поставете отметка в квадратчето **Създай правило и го запомни за постоянно**.



В настройката на защитната стена можете да създадете нови правила за защитна стена за приложения, преди те да бъдат открити от ESET Internet Security. Отворете главния прозорец на програмата > **Настройка** > **Мрежова защита** > щракнете върху ⚙ до **Защитна стена** > **Конфигуриране** > **Разширени** > **Правила** > **Редактиране**.

Щракнете върху бутон **Добавяне** и в раздела **Общи** въведете името, посоката и комуникационния протокол за правилото. В прозореца можете да укажете действието, което да се изпълнява при прилагане на правилото.

Въведете пътя до изпълнимия файл на приложението и локалния комуникационен порт в раздела **Локален**. Отидете в раздела **Отдалечен**, за да въведете отдалечения адрес и порт (ако са приложими). Новосъздаденото правило ще започне да се прилага веднага щом приложението се опита отново да комуникира.

Как се разрешава функцията за родителски контрол за даден акаунт

За да активирате родителски контрол за определен потребителски акаунт, следвайте стъпките по-долу:

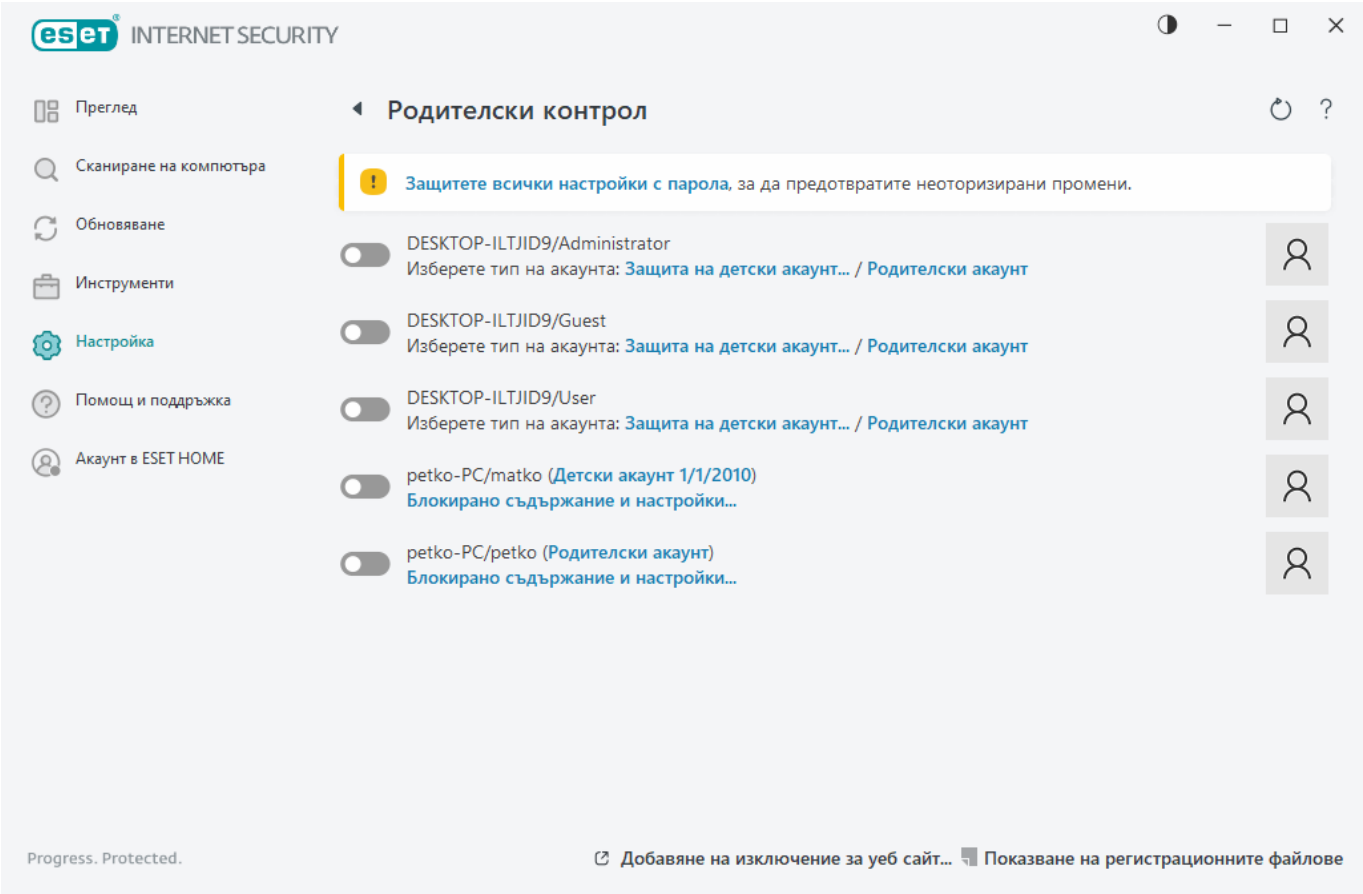
1. По подразбиране родителският контрол е забранен в ESET Internet Security. Съществуват два метода за активиране на родителски контрол:

   • Щракнете върху иконата на плъзгача в **Настройка** > **Интернет защита** > **Родителски контрол** от главния прозорец на програмата и променете състоянието на

функцията за родителски контрол на разрешено.

• Отворете Разширени настройки > **Защити** > **Защита на уеб достъпа** > **Родителски контрол**, след което активирайте превключвателя до **Активиране на родителски контрол**.

2. Щракнете върху **Настройка** > **Интернет защита** > **Родителски контрол** от главния прозорец на програмата. Дори ако **Разрешено** се показва до **Родителски контрол**, трябва да конфигурирате родителския контрол за желания акаунт, като щракнете върху символа за стрелка, след което в следващия прозорец изберете **Защита на детски акаунт** или **Родителски акаунт**. В следващия прозорец изберете датата на раждане, за да определите нивото на достъп и препоръчителните, подходящи за възрастта, уеб страници. Родителският контрол вече е разрешен за указания потребителски акаунт. Щракнете върху **Блокирано съдържание и настройки** под името на акаунта, за да персонализирате категориите, които искате да разрешите или блокирате в раздела Категории. За да разрешите или блокирате уеб страници по избор, които не съответстват на категория, щракнете върху раздела Изключения.



Как се създава нова задача в планировчика

За да създадете нова задача в **Инструменти** > **Планировчик**, щракнете върху **Добавяне на задача** или щракнете с десния бутон и изберете **Добавяне...** от контекстното меню. Има пет типа планирани задачи:

• **Изпълнение на външно приложение** – планира изпълнението на външно приложение.

• **Профилактика на регистрационните файлове** – Регистрационните файлове също съдържат останали елементи от изтрити записи. Тази задача оптимизира редовно записите в регистрационните файлове, за да се изпълняват по-ефективно.

• **Проверка на файловете при стартиране на системата** – проверка на файловете, за които е разрешено да се изпълняват при стартиране на системата или при влизане.

• **Създаване на моментна снимка на състоянието на компютъра** – Създава моментна снимка на компютъра на ESET SysInspector – събира подробна информация за компонентите на системата (напр. драйвери, приложения) и оценява нивото на риск за всеки компонент.

• **Сканиране на компютъра при поискване** – извършва сканиране на файловете и папките в компютъра.

• **Обновяване** – Планира задача за обновяване, като обновява модулите.

Тъй като **Обновяване** една от най-често използваните планирани задачи, по-долу ще обясним как се добавя нова задача за обновяване:

От падащото меню **Планирана задача** изберете **Обновяване**. Въведете името на задачата в полето **Име на задачата** и щракнете върху **Напред**. Изберете честотата на задачата. Налични са следните опции: **Веднъж**, **Постоянно**, **Всеки ден**, **Всяка седмица** и **При възникване на събитие**. Изберете **Пропускане на задачата, когато компютърът работи на батерия**, за да минимизирате използването на системните ресурси, когато лаптоп работи на батерия. Задачата ще се изпълни на датата и в часа, указани в полетата **Изпълнение на задачата**. След това задайте действието, което да се изпълнява, ако задачата не може да се изпълни или да завърши в планираното време. Налични са следните опции:

• **В следващия планиран час**

• **Възможно най-скоро**

• **Незабавно, ако времевият период от последното изпълнение надвишава указаната стойност** (интервалът може да бъде определен с помощта на полето за превъртане **Време от последното изпълнение (часове)**)

На следващата стъпка се показва прозорец за обобщение с информация за текущата планирана задача. Щракнете върху **Готово**, когато приключите с извършването на промени.

Ще се появи диалогов прозорец, в който можете да изберете профилите, които да се използват за планираната задача. Тук можете да зададете основен и алтернативен профил. Алтернативният профил се използва, ако задачата не може да бъде изпълнена чрез основния профил. Потвърдете, като щракнете върху **Готово**, и новата планирана задача ще се добави към списъка с текущо планирани задачи.

Как се планира седмично сканиране на компютъра

За да планирате обикновена задача, отворете главния прозорец на програмата и щракнете върху **Инструменти** > **Разписание**. По-долу е предоставено кратко ръководство как да

планирате задача за ежеседмично сканиране на локалните дискове. За допълнителни инструкции прегледайте нашата статия в онлайн помощника.

За да планирате задача за сканиране:

1. Щракнете върху **Добавяне** в главния екран на планировчика.

2. Въведете име за задачата и изберете **Сканиране на компютъра при поискване** от падащото меню **Тип задача**.

3. Изберете **Всяка седмица** за честота на задачата.

4. Задайте деня и часа за изпълнение на задачата.

5. Изберете **Изпълни задачата възможно най-скоро** за изпълнение на задачата по-късно, в случай че планираната задача не бъде изпълнена по някаква причина (ако например компютърът е бил изключен).

6. Прегледайте обобщението на планираната задача и щракнете върху **Готово**.

7. От падащото меню **Цели** изберете **Локални дискове**.

8. Щракнете върху **Готово**, за да приложите задачата.

Как се отключват защитените с парола разширени настройки

Когато искате да осъществите достъп до защитените разширени настройки, се показва прозорецът за въвеждане на паролата. Ако забравите или загубите своята парола, щракнете върху опцията **Възстановяване на парола** и въведете имейл адреса, който сте използвали за регистриране на абонамента. ESET изпраща имейл с кода за проверка. Въведете кода за проверка, след което напишете и потвърдете новата парола. Кодът за проверка е валиден в продължение на седем дни.

Възстановяване на паролата чрез вашия акаунт в ESET HOME – използвайте тази опция, ако абонаментът, използван за активиране, е свързан с вашия акаунт в ESET HOME. Въведете имейл адреса, който използвате за влизане в акаунта си в ESET HOME.

Ако не можете да запомните имейл адреса си или имате затруднения с възстановяването на паролата, щракнете върху **Връзка с отдела за техническа поддръжка**. Ще бъдете пренасочени към уеб сайта на ESET за връзка с нашия отдел за техническа поддръжка.

Генериране на код за техническа поддръжка – тази опция генерира код за техническа поддръжка. Копирайте кода, предоставен от техническата поддръжка, и щракнете върху **Имам код за проверка**. Въведете кода за проверка, след което напишете и потвърдете новата парола. Кодът за проверка е валиден в продължение на седем дни.

За повече информация вижте Отключване на парола за настройки в продуктите на ESET за домашна употреба за Windows.

Как се разрешава деактивиране на продукт от ESET HOME

Продуктът не е активиран

Това съобщение за грешка се появява, когато собственикът на абонамента деактивира вашия ESET Internet Security от портала на ESET HOME или абонаментът, споделен с вашия акаунт в ESET HOME, вече не се споделя. За да разрешите този проблем:

• Щракнете върху **Активиране** и използвайте един от методите за активиране, за да активирате ESET Internet Security.

• Свържете се със собственика на абонамента с информация, че вашият ESET Internet Security е деактивиран от собственика на абонамента или че абонаментът вече не се споделя с вас. Собственикът може да разреши този проблем в ESET HOME.

Продуктът е деактивиран, връзката на устройството е прекъсната

Това съобщение за грешка се появява след премахване на устройство от ESET HOME. За да разрешите този проблем:

• Щракнете върху **Активиране** и използвайте един от методите за активиране, за да активирате ESET Internet Security.

• Свържете се със собственика на абонамента с информация, че вашият ESET Internet Security е дезактивиран и връзката на устройството с ESET HOME е прекъсната.

• Ако вие сте собственикът на абонамента и не знаете за тези промени, прегледайте информацията за дейностите в своя ESET HOME. Ако откриете подозрителна дейност, променете паролата за своя акаунт в ESET HOME и се свържете с отдела за техническа поддръжка на ESET.

Продуктът е деактивиран, връзката на устройството е прекъсната

Това съобщение за грешка се появява след премахване на устройство от ESET HOME. За да разрешите този проблем:

• Щракнете върху **Активиране** и използвайте един от методите за активиране, за да активирате ESET Internet Security.

• Свържете се със собственика на абонамента с информация, че вашият ESET Internet Security е дезактивиран и връзката на устройството с ESET HOME е прекъсната.

• Ако вие сте собственикът на абонамента и не знаете за тези промени, прегледайте информацията за дейностите в своя ESET HOME. Ако откриете подозрителна дейност,

променете паролата за своя акаунт в ESET HOME и се свържете с отдела за техническа поддръжка на ESET.

Продуктът не е активиран

Това съобщение за грешка се появява, когато собственикът на абонамента деактивира вашия ESET Internet Security от портала на ESET HOME или абонаментът, споделен с вашия акаунт в ESET HOME, вече не се споделя. За да разрешите този проблем:

• Щракнете върху **Активиране** и използвайте един от методите за активиране, за да активирате ESET Internet Security.

• Свържете се със собственика на абонамента с информация, че вашият ESET Internet Security е деактивиран от собственика на абонамента или че абонаментът вече не се споделя с вас. Собственикът може да разреши този проблем в ESET HOME.

0

Програма за подобряване на работата на клиентите

С присъединяването към програмата за подобряване на работата на клиентите предоставяте на ESET анонимна информация, свързана с използването на нашите продукти. Повече информация за обработката на данни е налична в нашите Правила за поверителност.

Вашето съгласие

Участието в програмата е доброволно и се основава на вашето съгласие. След като се присъедините, участието е пасивно, което означава, че не е нужно да предприемате по-нататъшни действия. Можете да отмените съгласието си, като промените настройките на продукта по всяко време. Това ще ни попречи да продължим обработката на анонимните ви данни.

Можете да отмените съгласието си, като промените настройките на продукта по всяко време:

- Променете настройките на програмата за подобряване на работата на клиентите в продуктите на ESET за домашна употреба за Windows

Какви видове информация събираме?

Данни за взаимодействието с продукта

Тази информация ни дава повече сведения за това как се използват нашите продукти. Благодарение на нея знаем например кои функционалности се използват често, кои настройки се променят от потребителите или колко време прекарват в използване на продукта.

Данни за устройствата

Ние събираме тази информация, за да разберем къде и на какви устройства се използват нашите продукти. Типични примери са моделът на устройството, държавата, версията и името на операционната система.

Диагностични данни на грешка

Също се събира информацията за грешки и ситуации на срив. Например каква е грешката и какви действия са довели до нея.

Защо събираме тази информация?

Тази анонимна информация ни позволява да подобрим нашите продукти за вас – нашите потребители. Помага ни да ги направим възможно най-подходящи, лесни за използване и без грешки.

Кой контролира тази информация?

ESET, spol. s r.o. е единственият администратор на данните, събрани в програмата. Тази информация не се споделя с трети страни.

Лицензионно споразумение с краен потребител

В сила от 19 октомври 2021 г.

ВАЖНО: Моля, прочетете внимателно правилата и условията на приложението на продукта, изложени по-долу, преди да го изтеглите, инсталирате, копирате или използвате. **ЧРЕЗ ИЗТЕГЛЯНЕ, ИНСТАЛИРАНЕ, КОПИРАНЕ ИЛИ ИЗПОЛЗВАНЕ НА СОФТУЕРА ВИЕ ИЗРАЗЯВАТЕ СЪГЛАСИЕТО СИ ПО ОТНОШЕНИЕ НА НАСТОЯЩИТЕ ПРАВИЛА И УСЛОВИЯ И ПРИЕМАТЕ ПРАВИЛА ЗА ПОВЕРИТЕЛНОСТ.**

Лицензионно споразумение с краен потребител

Съгласно условията на настоящото Лицензионно споразумение с Краен потребител („Споразумението“), сключено от и между ESET, spol. s r. o., със седалище и адрес на управление Einsteinova 24, 85101 Bratislava, Slovak Republic, регистрирано в Търговския регистър, администриран от Окръжен съд I в Братислава, Раздел Sro, под фирмено дело № 3586/B, фирмен номер: 31333532 („ESET“ или „Доставчик“) и Вас, физическо или юридическо лице („Вие“ или „Краен потребител“), Вие имате право да използвате Софтуера, дефиниран в чл. 1 на настоящото Споразумение. Софтуерът, дефиниран в чл. 1 на настоящото Споразумение, може да се съхранява на носител на данни, да се изпраща по електронна поща, да се изтегля от интернет и от сървъри на Доставчика или да се получава от други източници, при условие че се спазват правилата и условията, указани по-долу.

ТОВА Е СПОРАЗУМЕНИЕ ЗА ПРАВАТА НА КРАЙНИЯ ПОТРЕБИТЕЛ, А НЕ ДОГОВОР ЗА ПРОДАЖБА. Доставчикът продължава да е собственик на копието на Софтуера и физическия носител, които се съдържат в опаковката на продукта, както и на всички други копия, които Крайният

потребител има право да прави съгласно настоящото Споразумение.

Чрез щракване върху опцията „Приемам“ или „Приемам...“ по време на инсталиране, изтегляне, копиране или използване на Софтуера Вие се съгласявате с правилата и условията на настоящото Споразумение и приемате Правилата за поверителност. Ако не сте съгласни с всички правила и условия на настоящото Споразумение и/или Правилата за поверителност, незабавно щракнете върху опцията за отмяна, отменете инсталирането или изтеглянето или унищожете или върнете Софтуера, инсталационния носител, придружаващата документация и касовата бележка за покупката на Доставчика или магазина, от който сте закупили Софтуера.

ВИЕ СЕ СЪГЛАСЯВАТЕ, ЧЕ ИЗПОЛЗВАНЕТО НА СОФТУЕРА ОТ ВАС ОЗНАЧАВА, ЧЕ СТЕ ПРОЧЕЛИ НАСТОЯЩОТО СПОРАЗУМЕНИЕ, ЧЕ ГО РАЗБИРАТЕ И СТЕ СЪГЛАСНИ ДА СТЕ ОБВЪРЗАНИ С НЕГОВИТЕ ПРАВИЛА И УСЛОВИЯ.

1. **Софтуер.** Както се използва в настоящото Споразумение, терминът "Софтуер" означава: (i) компютърната програма, съпътствана от настоящото Споразумение и всички негови компоненти; (ii) цялото съдържание на дисковете, CD-ROM и DVD дисковете, имейлите и всички прикачени към тях файлове или други носители, с които се предоставя настоящото Споразумение, включително Софтуера под форма на обектен код, предоставен на носител на данни, чрез електронна поща или изтеглен от интернет; (iii) всякакви свързани писмени обяснителни материали и друга възможна документация, свързана със Софтуера, преди всичко всички описания на Софтуера, неговите спецификации, свойствата или функционирането му, всички описания на операционната среда, в която се използва Софтуерът, инструкции за експлоатация или инсталиране на Софтуера или всички описания на начина на използване на Софтуера („Документация“); (iv) копия на Софтуера, корекции на възможни грешки в Софтуера, ако има такива, допълнения към Софтуера, разширения на Софтуера, променени версии на Софтуера, нови версии на Софтуера, както и всички обновявания на негови компоненти, ако са предоставени такива, по отношение на които Доставчикът Ви предоставя лиценз съгласно чл. 3 от настоящото Споразумение. Софтуерът се предоставя само във формата на изпълним обектен код.

2. **Инсталиране, Компютър и Лицензионен ключ**. Софтуерът, доставен върху носител на данни, изпратен по електронна поща, изтеглен от интернет, изтеглен от сървъри на Доставчика или получен от други източници, изисква инсталиране. Трябва да инсталирате Софтуера на правилно конфигуриран Компютър, който отговаря поне на изискванията, посочени в Документацията. Начинът на инсталиране е описан в Документацията. На Компютъра, на който инсталирате Софтуера, не могат да се инсталират компютърни програми или хардуер, които биха могли да се отразят неблагоприятно на Софтуера. Под „Компютър“ се разбира хардуер, включително, но без да се ограничава до, персонални компютри, работни станции, палмтоп, смартфони, преносими електронни устройства или други електронни устройства, за които е проектиран Софтуерът, на които ще бъде инсталиран и/или използван. Лицензионен ключ означава уникалната поредица от символи, букви, числа или специални знаци, предоставени на Крайния потребител, за да се разреши законовото използване на Софтуера, неговата конкретна версия или разширение на термина на Лиценза в съответствие с настоящото Споразумение.

3. **Лиценз**. При условие че сте се съгласили с условията на това Споразумение и съблюдавате всички правила и условия, предвидени в Споразумението, Доставчикът Ви предоставя следните права („Лиценз“):

a) **Инсталиране и използване.** Имате неизключително, непрехвърлимо право да инсталирате

Софтуера на твърдия диск на компютъра или друг носител за постоянно съхранение на данни, инсталирате и съхранявате Софтуера в паметта на компютъра и да изпълнявате, съхранявате и визуализирате Софтуера.

б) **Условие за броя на лицензите.** Правото да използвате Софтуера е ограничено от броя на Крайните потребители. Счита се, че един Краен потребител означава следното: (i) инсталирането на Софтуера на един компютър или (ii) ако обхватът на лицензия отговаря на броя на пощенските кутии, то един Краен потребител означава компютърен потребител, който получава електронна поща чрез Програма за електронна поща („MUA“). Ако MUA приема имейл съобщения и след това автоматично ги разпространява на няколко потребителя, то броят на Крайните потребители се определя според актуалния брой на потребителите, за които се разпространява електронна поща. Ако пощенският сървър изпълнява функциите на пощенски маршрутизатор, броят на Крайните потребители е равен на броя на потребителите пощенските сървъри, които се обслужват от въпросния маршрутизатор. Ако неопределен брой имейл адреси се пренасочват към и приемат от един потребител (напр. чрез псевдоними) и съобщенията не се разпространяват автоматично от клиента на по-голям брой потребители, Лиценз се изисква само за един компютър. Не трябва да използвате един и същи Лиценз по едно и също време на повече от един компютър. Крайният потребител има правото да въведе Лицензионния ключ на Софтуера само дотолкова, доколкото има правото да използва Софтуера в съответствие с ограничението, произтичащо от броя Лицензи, предоставени от Доставчика. Лицензионният ключ е поверителен, не трябва да споделяте Лиценза с трети лица или да позволявате на трети лица да използват Лицензионния ключ, освен ако не се разрешава от настоящото Споразумение или Доставчик. Ако Вашият Лицензионен ключ е компрометиран, незабавно уведомете Доставчика.

в) **Home/Business Edition.** Версия Home Edition на Софтуера трябва да се използва само в лични и/или нетърговски среди за домашна и семейна употреба. Версията Business Edition на Софтуера трябва да се придобие за употреба в търговска среда, както и за използване на Софтуера на пощенски сървъри, средства за пренасочване на електронна поща, шлюзове за поща или интернет.

г) **Срок на Лиценза.** Вашето право да използвате Софтуера е срочно.

д) **OEM софтуер.** Софтуер, класифициран като „OEM“, е ограничен само до Компютъра, с който сте го получили. Той не може да се прехвърля на друг компютър.

е) **„Не за продажба“, „Пробен“ софтуер.** Софтуерът, класифициран като „Не за продажба“ или „Пробен“, не може да е предназначен за заплащане и трябва да се използва само за демонстрация или тестване на функциите на Софтуера.

ж) **Прекратяване на Лиценза.** Лицензът се прекратява автоматично в края на срока, за който е предоставен. Ако не се съобразите с някоя от клаузите на настоящото Споразумение, Доставчикът има право да се оттегли от Споразумението, без да се засяга каквото и да е право или правно средство за защита, открито спрямо Доставчика при подобни обстоятелства. В случай на анулиране на Лиценза трябва незабавно да изтриете, унищожите или върнете за собствена сметка Софтуера и всички архивни копия на ESET или на магазина, от който сте закупили Софтуера. При прекратяване на Лиценза Доставчикът също има право да анулира правото на Крайния потребител да използва функциите на Софтуера, които изискват връзка със сървърите на Доставчика или сървъри на трети лица.

4. **Функционира със събиране на данни и изисквания за интернет връзката.** За да работи правилно, Софтуерът изисква връзка с интернет и трябва да се свързва на равни интервали

със сървърите на Доставчика или сървъри на трети лица и приложимо събиране на данни в съответствие с Правилата за поверителност. Връзката с интернет и приложимото събиране на данни са необходими за следните функции на Софтуера:

a) **Обновявания на Софтуера.** Доставчикът има право от време на време да издава обновявания или надстройки на Софтуера („Обновяване“), но не е задължен да предоставя Обновяванията. Тази функция се активира от стандартните настройки на Софтуера и следователно Обновяванията се инсталират автоматично, освен ако Крайният потребител не е забранил автоматично инсталиране на Обновявания. За осигуряването на Обновявания се изисква проверка на автентичността на Лицензa, включително информация относно Компютъра и/или платформата, на която е инсталиран Софтуерът, в съответствие с Правилата за поверителност.

Предоставянето на всякакви Обновявания може да бъде предмет на Правилата за извеждане от употреба, които са налични на https://go.eset.com/eol_home. Няма да бъдат предоставяни Обновявания, след като Софтуерът или някоя от функциите му достигне датата за Извеждане от употреба, посочена в Правилата за извеждане от употреба.

б) **Препращане на проникванията и информация до Доставчика.** Софтуерът съдържа функции, които събират проби от компютърни вируси и други злонамерени компютърни програми и подозрителни, проблемни, потенциално нежелани или потенциално опасни обекти, като например файлове, URL адреси, IP пакети и ethernet рамки („Проникванията“), и ги изпращат до Доставчика, включително, но без ограничение до, информация за процеса на инсталиране, Компютъра и/или платформата, на която е инсталиран Софтуерът, информация за операциите и функционалността на Софтуера („Информация“). Информацията и Проникванията може да съдържат данни (включително произволно или случайно получени лични данни) за Крайния потребител или други потребители на компютъра, на който е инсталиран Софтуерът, и засегнати файлове от Проникванията със свързани метаданни.

Информацията и Проникванията може да се събират от следните функции на Софтуера:

i. Функцията на LiveGrid "Система за репутация" включва събиране и изпращане на еднопосочни хешове, свързани с Проникванията, до Доставчика. Тази функция е разрешена в стандартните настройки на Софтуера.

ii. Функцията на системата LiveGrid за обратна връзка включва събирането и изпращането на Проникванията със свързани метаданни и Информация до Доставчика. Тази функция може да се активира от Крайния потребител в процеса на инсталиране на Софтуера.

Доставчикът следва да използва само Информацията и Проникванията, получени за анализ и изследване на Проникванията, подобрение на Софтуера и проверка на автентичността на Лицензa, и следва да предприеме подходящи мерки, за да гарантира, че получените Проникванията и Информация ще останат защитени. Чрез активирането на тази функция на Софтуера Проникванията и Информацията може да се събират и обработват от Доставчика, както е посочено в Правилата за поверителност и в съответствие със съответните законови разпоредби. Може да дезактивирате тези функции по всяко време.

За целите на настоящото Споразумение е необходимо събиране, обработване и съхраняване на данни, което позволява на Доставчика да Ви идентифицира в съответствие с Правилата за поверителност. С настоящото се съгласявате Доставчикът да проверява чрез свои методи дали използвате Софтуера в съответствие с предвидения в клаузите на Споразумението начин. С настоящото приемате, че за целта на настоящото Споразумение Вашите данни трябва

да се прехвърлят по време на комуникацията между Софтуера и компютърните системи на Доставчика или на неговите бизнес партньори, като част от мрежата за разпространение и поддръжка на Доставчика, за да се осигури функционалност и упълномощаване за използване на Софтуера, както и защита на правата на Доставчика.

След сключване на настоящото Споразумение Доставчикът или някои от неговите бизнес партньори като част от мрежата за разпространение и поддръжка на Доставчика следва да имат правото да прехвърлят, обработват и съхраняват важни данни, които Ви идентифицират, с цел фактуриране, изпълнение на настоящото Споразумение и предаване на известия на Вашия компютър.

Подробности за поверителността, защитата на личните данни и Вашите права като субект на данни могат да бъдат намерени в Правилата за поверителност, достъпни в уеб сайта на Доставчика и директно от процеса на инсталиране. МОЖЕТЕ СЪЩО ДА ГИ ПРЕГЛЕДАТЕ ОТ РАЗДЕЛА ЗА ПОМОЩ НА СОФТУЕРА.

5. **Упражняване на правата на Крайния потребител**. Трябва да упражнявате правата на Крайния потребител лично или чрез Ваши служители. Имате право да използвате Софтуера само за защита на Вашата работа и за защита на Компютрите или компютърните системи, за които сте получили Лиценз.

6. **Ограничения на правата.** Нямате право да копирате, разпространявате, разделяте компонентите или да създавате производни версии на Софтуера. Когато използвате Софтуера, трябва да съблюдавате следните ограничения:

а) Може да създадете едно копие на Софтуера на носител за постоянно съхранение на данни като архивно резервно копие, при условие че това копие няма да се инсталира или използва на нито един компютър. Създаването на друго копие на Софтуера представлява нарушение на това Споразумение.

б) Нямате право да използвате, променяте, превеждате или възпроизвеждате Софтуера или да прехвърляте правата за използване на Софтуера или негови копия по начин, различен от посочения в настоящото Споразумение.

в) Нямате право да продавате, преотдавате лиценза, отдавате под наем или заемате за послужване Софтуера, нито да го използвате за предоставяне на услуги с търговска цел.

г) Нямате право да анализирате, декомпилирате, разглобявате Софтуера или да се опитвате по друг начин да откриете първичния код на Софтуера, освен до степента, до която такова ограничение е изрично забранено от закона.

д) Вие се съгласявате, че ще използвате Софтуера само по начин, който е съобразен с приложимите закони в юрисдикцията, в която използвате Софтуера, включително, но не само приложимите ограничения, свързани с авторско право и други права на интелектуална собственост.

е) Вие се съгласявате, че ще използвате Софтуера и неговите функции единствено по начин, който не ограничава възможностите на Крайните потребители за достъп до тези услуги. Доставчикът си запазва правото да ограничава обхвата на услугите, предоставени на отделни Крайни потребители, за да даде възможност за използване на услугите от възможно най-високия брой Крайни потребители. Ограничаването на обхвата на услугите означава също така и пълно преустановяване на възможността за използване на която и да е от функциите

на Софтуера, както и изтриване на Данните и информацията от сървърите на Доставчика или сървърите на трети лица, свързани с конкретна функция на Софтуера.

ж) Съгласявате се да не упражнявате никакви дейности, включващи използването на Лицензионния ключ, противоречащо на условията на настоящото Споразумение или водещи до предоставяне на Лицензионен ключ на лице, което няма право да използва Софтуера, като например прехвърлянето на използван или неизползван Лицензионен ключ под каквато и да е форма, както и неупълномощеното възпроизвеждане или разпространение на дублирани или генерирани Лицензионни ключове или използването на Софтуера като резултат от използването на Лицензионен ключ, придобит от източник, различен от Доставчика.

7. **Авторски права**. Софтуерът и всички права, включващи без изключение права на собственост и права на интелектуална собственост, принадлежат на ESET и/или нейните лицензодатели. Те са защитени от разпоредбите на международни спогодби и от всички приложими национални закони на държавата, в която се използва Софтуерът. Структурата, организацията и кодът на Софтуера са оценими търговски тайни и поверителна информация на ESET и/или нейните лицензодатели. Нямате право да копирате Софтуера, освен както е предвидено в чл. 6 (а). ВВсички копия, които имате право да създавате съгласно настоящото Споразумение, трябва да съдържат същите съобщения за авторски права и права на собственост, както е посочено за Софтуера. Ако анализирате, декомпилирате или разглобите първичния код на Софтуера или се опитате да го разберете по друг начин в разрез с клаузите на това Споразумение, с настоящото Вие се съгласявате, че всяка информация, получена на базата на настоящото, автоматично и неотменимо се счита за прехвърлена на Доставчика и е негова собственост изцяло от момента на възникване на информацията, независимо от правата на Доставчика, свързани с нарушаване на Споразумението.

8. **Запазване на права**. С настоящото Доставчикът запазва всички права за Софтуера, с изключение на правата, които са Ви изрично предоставени съгласно условията на настоящото Споразумение като Краен потребител на Софтуера.

9. **Няколко езикови версии, версии за повече операционни системи, няколко копия**. Ако Софтуерът поддържа няколко платформи или езици или сте получили няколко копия на Софтуера, можете да използвате Софтуера само за броя компютри и за версиите, за които е получен Лицензът. Нямате право да продавате, отдавате под наем/на лизинг, преотдавате лиценза, заемате или прехвърляте версии или копия на Софтуера, които Вие не използвате.

10. **Влизане в сила и прекратяване на Споразумението.** Това Споразумение влиза в сила от датата, на която се съгласите с условията му. Можете да прекратите Споразумението по всяко време, като за постоянно деинсталирате, унищожите и върнете на собствени разноски Софтуера, всички архивни копия и всички сродни материали, които сте получили от Доставчика или от неговите бизнес партньори. Правото Ви да използвате Софтуера и функциите му може да е предмет на Правилата за извеждане от употреба. След като Софтуерът или някоя от функциите му достигне датата за Извеждане от употреба, посочена в Правилата за извеждане от употреба, правото Ви да използвате Софтуера се прекратява. Независимо от начина на прекратяване на Споразумението клаузите на чл. 7, 8, 11, 13, 19 и 21 остават в сила за неопределен срок.

11. **ДЕКЛАРАЦИИ НА КРАЙНИЯ ПОТРЕБИТЕЛ**. В КАЧЕСТВОТО СИ НА КРАЕН ПОТРЕБИТЕЛ ВИЕ ДЕКЛАРИРАТЕ, ЧЕ СОФТУЕРЪТ СЕ ПРЕДЛАГА В СЪСТОЯНИЕТО, В КОЕТО Е, БЕЗ КАКВАТО И ДА Е ИЗРИЧНА ИЛИ ПОДРАЗБИРАЩА СЕ ГАРАНЦИЯ И В МАКСИМАЛНАТА СТЕПЕН, РАЗРЕШЕНА ОТ ПРИЛОЖИМОТО ПРАВО. НИТО ДОСТАВЧИКЪТ, НИТО НЕГОВИТЕ ЛИЦЕНЗОДАТЕЛИ ИЛИ СВЪРЗАНИ ЛИЦА, НИТО НОСИТЕЛИТЕ НА АВТОРСКИТЕ ПРАВА ПРЕДОСТАВЯТ КАКВИТО И ДА Е ДЕКЛАРАЦИИ

ИЛИ ГАРАНЦИИ, ИЗРИЧНИ ИЛИ ПОДРАЗБИРАЩИ СЕ, ВКЛЮЧИТЕЛНО, НО НЕ САМО, ТАКИВА ЗА ПРОДАЖБА ИЛИ ГОДНОСТ ЗА ОПРЕДЕЛЕНА ЦЕЛ, НИТО ГАРАНЦИИ, ЧЕ СОФТУЕРЪТ НЕ НАРУШАВА ПАТЕНТИ, АВТОРСКИ ПРАВА, ТЪРГОВСКИ МАРКИ ИЛИ ДРУГИ ПРАВА НА ТРЕТИ ЛИЦА. НЕ СЕ ПРЕДОСТАВЯ НИКАКВА ГАРАНЦИЯ ОТ ДОСТАВЧИКА ИЛИ ТРЕТИ ЛИЦА, ЧЕ ФУНКЦИИТЕ НА СОФТУЕРА ОТГОВАРЯТ НА ВАШИТЕ ИЗИСКВАНИЯ ИЛИ ЧЕ РАБОТАТА МУ ЩЕ Е НЕПРЕКЪСВАЕМА ИЛИ БЕЗ ГРЕШКИ. ВИЕ ПОЕМАТЕ ПЪЛНА ОТГОВОРНОСТ И РИСК ЗА ИЗБОРА НА СОФТУЕРА С ЦЕЛ ПОСТИГАНЕ НА ЖЕЛАНИТЕ РЕЗУЛТАТИ И ЗА ИНСТАЛИРАНЕТО, ИЗПОЛЗВАНЕТО НА СОФТУЕРА И ЗА РЕЗУЛТАТИТЕ, ПРОИЗТИЧАЩИ ОТ ТОВА.

12. **Без допълнителни задължения**. Това Споразумение не създава никакви допълнителни задължения за Доставчика и неговите лицензодатели освен посочените в Споразумението.

13. **ОГРАНИЧЕНИЕ НА ОТГОВОРНОСТТА**. В МАКСИМАЛНАТА СТЕПЕН, ПОЗВОЛЕНА ОТ ПРИЛОЖИМИТЕ ЗАКОНИ, ПРИ НИКАКВИ ОБСТОЯТЕЛСТВА ДОСТАВЧИКЪТ, НЕГОВИТЕ СЛУЖИТЕЛИ ИЛИ ЛИЦЕНЗОДАТЕЛИ НЕ ПОЕМАТ ОТГОВОРНОСТ ЗА КАКВАТО И ДА Е ЗАГУБА НА ПОЛЗИ, ПРИХОДИ ИЛИ ПРОДАЖБИ ИЛИ ЗА КАКВАТО И ДА Е ЗАГУБА НА ДАННИ, ИЛИ РАЗХОДИ ЗА РЕЗЕРВНИ СТОКИ ИЛИ УСЛУГИ, ЗА ПОВРЕДА НА СОБСТВЕНОСТ, НАРАНЯВАНЕ НА ХОРА, ПРЕКЪСВАНЕ НА ДЕЙНОСТТА, ЗАГУБА НА БИЗНЕС ИНФОРМАЦИЯ ИЛИ ЗА КАКВИТО И ДА Е СПЕЦИАЛНИ, ПРЕКИ, КОСВЕНИ, СЛУЧАЙНИ, ИКОНОМИЧЕСКИ, ОБСЛУЖВАЩИ, КРИМИНАЛНИ, СПЕЦИАЛНИ ИЛИ ПОСЛЕДВАЩИ ЩЕТИ ПО КАКЪВТО И ДА Е НАЧИН, НЕЗАВИСИМО ДАЛИ ОТ ДОГОВОР, УМИШЛЕНИ ДЕЙСТВИЯ, НЕБРЕЖНОСТ ИЛИ ДРУГ ФАКТ, ПРОИЗЛИЗАЩ ОТ ИНСТАЛИРАНЕТО, ПРИ КОЙТО ВЪЗНИКВА ОТГОВОРНОСТ, ВСЛЕДСТВИЕ ИЗПОЛЗВАНЕТО ИЛИ НЕВЪЗМОЖНОСТТА ЗА ИЗПОЛЗВАНЕ НА СОФТУЕРА, ДОРИ В СЛУЧАЙ ЧЕ ДОСТАВЧИКЪТ ИЛИ НЕГОВИТЕ ЛИЦЕНЗОДАТЕЛИ/СВЪРЗАНИ ЛИЦА ДА СА БИЛИ УВЕДОМЕНИ ЗА ВЪЗМОЖНОСТТА ОТ ТАКИВА ЩЕТИ. ТЪЙ КАТО НЯКОИ СТРАНИ И НЯКОИ ЮРИСДИКЦИИ НЕ ПОЗВОЛЯВАТ ИЗКЛЮЧВАНЕ НА ОТГОВОРНОСТТА, НО МОЖЕ ДА РАЗРЕШАВАТ НЕЙНОТО ОГРАНИЧАВАНЕ, ОТГОВОРНОСТТА НА ДОСТАВЧИКА, НЕГОВИТЕ СЛУЖИТЕЛИ, ЛИЦЕНЗОДАТЕЛИ ИЛИ СВЪРЗАНИ ЛИЦА СЕ ОГРАНИЧАВА ДО ЦЕНАТА, КОЯТО СТЕ ПЛАТИЛИ ЗА ЛИЦЕНЗА.

14. Никоя от клаузите на Споразумението не може да засяга законните права на трети лица, действащи като клиент, дори настоящото да им противоречи.

15. **Техническа поддръжка**. ESET или трети лица, упълномощени от ESET, предоставя/т техническата поддръжка по нейно/тяхно усмотрение без каквито и да е гаранции или декларации. Няма да бъде предоставяна техническа поддръжка, след като Софтуерът или някоя от функциите му достигне датата за Извеждане от употреба, посочена в Правилата за извеждане от употреба. От Крайния потребител се изисква да архивира всички налични данни, софтуера и помощните програми преди предоставянето на техническа поддръжка. ESET и/или трети лица, упълномощени от нея, не може да поема/т отговорност за увреждане или загуба на данни, собственост, софтуер или хардуер или пропуснати ползи поради предоставяне на техническа поддръжка. ESET и/или трети лица, упълномощени от нея, запазва/т правото на преценка дали проблемът е извън обхвата на техническата поддръжка. ESET запазва правото да отказва, отлага или прекратява предоставянето на техническа поддръжка по свое усмотрение. За осигуряването на техническа поддръжка може да се изисква информация за Лиценз, Информация и други данни в съответствие с Правилата за поверителност.

16. **Прехвърляне на Лицензa**. Софтуерът може да се прехвърля от един компютър на друг, освен ако това не противоречи на условията на настоящото Споразумение. Ако не противоречи на условията на настоящото Споразумение, Крайният потребител единствено има право за постоянно да прехвърли Лиценза и всички права, произтичащи от настоящото Споразумение, на друг Краен потребител със съгласието на Доставчика, подчинявайки се на условията: (i) първоначалният Потребител да не запазва никакви копия на Софтуера; (ii) прехвърлянето на

права да е директно, т.е. от първоначалния Краен потребител на новия Краен потребител; (iii) новият Краен потребител да приеме всички права и задължения на първоначалния Краен потребител, произтичащи от условията на настоящото Споразумение; (iv) Първоначалният Краен потребител да предостави на новия документацията, позволяваща удостоверяване на оригиналността на Софтуера, както е указано в чл. 17.

17. **Удостоверяване на оригиналността на Софтуера.** Крайният потребител може да демонстрира правото си да използва Софтуера по един от следните начини: (i) чрез сертификат за лиценз, издаден от Доставчика или трета страна, назначена от Доставчика; (ii) чрез писмено лицензионно споразумение, ако е било сключено такова; (iii) чрез изпращане на имейл до Доставчика, съдържащ подробни данни за лиценза (потребителско име и парола). За проверка на оригиналността на Софтуера може да се изисква информация за Лиценз и данни за идентификация на Крайния потребител в съответствие с Правилата за поверителност.

18. **Лицензиране за обществени органи и Правителството на САЩ**. Софтуерът се предоставя на обществени органи, включително Правителството на САЩ, с правата и ограниченията на лиценза, описани в настоящото Споразумение.

19. **Спазване на контрола на търговията**.

a) Забранява Ви се директно или индиректно да експортирате, реекспортирате, прехвърляте или по друг начин да предоставяте Софтуера на друго лице или да го използвате по какъвто и да е начин или да участвате в действие, което може да доведе до нарушение на или понасянето на отрицателни последствия от ESET или нейните холдингови компании, нейните дъщерни дружества и дъщерните дружества на нейните холдингови компании, както и юридически лица, контролирани от нейните холдингови компании („Свързани лица“), съгласно Законите относно контрола на търговията, които включват

i. всякакви закони, които контролират, ограничават или налагат изисквания за лицензиране върху експортирането, реекспортирането или прехвърлянето на стоки, софтуер, технология или услуги, издадени или приети от който и да е правителствен, държавен или регулаторен орган на Съединените американски щати, Сингапур, Обединеното кралство, Европейския съюз или негова Държава членка или която и да е държава, в която ще се извършват задължения по Споразумението или в която ESET или някое от нейните Свързани лица е учредено или провежда бизнес дейност, и

ii. всякакви икономически, финансови, търговски или други санкции, ограничения, ембарго, забрани за внос или износ, забрани за прехвърляне на средства или активи или за изпълнението на услуги или еквивалентни мерки, наложени от който и да е правителствен, държавен или регулаторен орган на Съединените американски щати, Сингапур, Обединеното кралство, Европейския съюз или негова Държава членка или която и да е държава, в която ще се извършват задължения по Споразумението или в която ESET или някое от нейните Свързани лица е учредено или провежда бизнес дейност („Закони за санкции“).

(правни актове, посочени в точки i и ii. по-горе заедно като „Закони за контрол на търговията“).

б) ESET има правото да преустанови своите задължения по или да прекрати настоящите Условия, влизайки в сила незабавно, в случай че:

i. ESET определи, по своя разумна преценка, че Потребителят е нарушил или вероятно е нарушил разпоредбата на чл. 19 a) на Споразумението; или

ii. Крайният потребител и/или Софтуерът е станал предмет на Законите относно контрола на търговията и вследствие на това ESET определи, по своя разумна преценка, че ако продължи да изпълнява задълженията си по Споразумението, това може да доведе до нарушение на или понасяне на негативни последствия от ESET или нейните Свързани лица съгласно Законите относно контрола на търговията.

в) Нищо в Споразумението не е предназначено и не трябва да се тълкува, че скланя или налага на която и да е страна да предприема действия или да се въздържа от такива (или да се съгласява да действа или да се въздържа от действия) по начин, който може да е в нарушение на, да е наказуем или забранен съгласно приложимите Закони относно контрола на търговията.

20. **Уведомления**. Всички уведомления и върнатият Софтуер и Документацията трябва да се доставят на: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, без да се засяга правото на ESET да съобщава всякакви промени по настоящото Споразумение, Правилата за поверителност, Правилата за извеждане от употреба и Документацията в съответствие с чл. 22 на Споразумението. ESET може да Ви изпраща имейли, известия в приложението чрез Софтуера или да публикува съобщението на нашия уеб сайт. Вие се съгласявате да получавате правни съобщения от ESET в електронна форма, включително всякакви съобщения относно промяна в Условията, Специалните условия или Правилата за поверителност, всяко предложение/приемане на договор или покани за третиране, известия или други правни съобщения. Подобни електронни съобщения се считат за получени в писмена форма, освен ако приложимите закони не изискват конкретно различна форма на комуникация.

21. **Приложимо право**. Настоящото Споразумение се управлява и тълкува в съответствие със законите на Република Словакия. Крайният потребител и Доставчикът с настоящото се съгласяват, че принципите на противоречие на закони и Конвенцията на ООН за международна продажба на стоки не се прилагат. Вие изрично се съгласявате всички претенции или спорове, произтичащи от настоящото Споразумение, относно Доставчика или други спорове и претенции, свързани с използването на Софтуера, да се уреждат от Окръжен съд I в Братислава, Република Словакия, и също така се съгласявате изрично с въпросната компетентна юрисдикция.

22. **Общи разпоредби**. Ако дадена клауза от това Споразумение е невалидна или не може да влезе в сила, това не се отразява на валидността на останалите разпоредби в Споразумението. Те остават валидни и в сила съгласно условията, залегнали в настоящото. Настоящото Споразумение е съставено на английски език. В случай на изготвянето на превод на Споразумението за удобство или други цели или в случай на несъответствие между езиковите версии на настоящото Споразумение версията на английски език ще има превес.

ESET си запазва правото да прави промени в Софтуера, както и да преразглежда настоящите Условия, неговите Допълнения, Правилата за поверителност, Правилата за извеждане от употреба и Документацията или която и да е част от тях по всяко време, като обнови съответния документ (i), за да отрази промените в Софтуера или начина, по който ESET извършва бизнес дейността, (ii) поради правни и регулаторни причини или съображения за сигурност или (iii) за предотвратяване на злоупотреби или вреди. Ще получите уведомление за промени в Споразумението чрез имейл, известие в приложението или по друг електронен начин. Ако не сте съгласни с предложените промени в Споразумението, може да го прекратите в съответствие с чл. 10 в рамките на 30 дни след получаване на известие за промяната. Ако не прекратите Споразумението в този срок, предложените промени ще се считат за приети и ще станат ефективни спрямо Вас, считано от датата, на която сте получили

известие за промяната.

Това Споразумение между Вас и Доставчика представлява цялото и единствено Споразумение за Софтуера и изцяло замества всякакви предишни декларации, преговори, задължения, комуникация или реклами, свързани със Софтуера.

ДОПЪЛНЕНИЕ КЪМ СПОРАЗУМЕНИЕТО

Г) **Оценка на защитата на свързаните с мрежата устройства.** Допълнителните разпоредби са приложими към Оценка на защитата на свързаните с мрежата устройства, както следва:

Софтуерът съдържа функция за проверка на защитата на локалната мрежа на Крайния потребител и защитата на устройства в локалната мрежа, която изисква име на локална мрежа и информация за устройства в локалната мрежа, като достъпност, тип, име, IP адрес и MAC адрес на устройството в локална мрежа във връзка с информация за лицензa. Информацията включва също типа защита на безжичната мрежа и типа шифроване на безжичната мрежа за маршрутизатори. Тази функция може също така да предоставя информация относно наличието на софтуерно решение за защита за защитени устройства в локалната мрежа.

Защита срещу злоупотреба с данни. Допълнителните разпоредби са приложими към Защита срещу злоупотреба с данни, както следва:

Софтуерът включва функция, която предотвратява загубата на или злоупотребата с важни данни в пряка връзка с кражбата на Компютър. Тази функция е изключена в настройките по подразбиране на Софтуера. Трябва да се създаде ESET HOME акаунт, за да бъде активирана, чрез което функцията активира събирането на данни в случай на кражба на компютъра. Ако изберете да активирате тази функция на Софтуера, данни за откраднатия компютър ще се събират и изпращат на Доставчика, което може да включва данни за мрежовото местоположение на Компютъра, данни за показваното съдържание на екрана на Компютъра, данни за конфигурацията на Компютъра и/или данни, записани от камера, свързана с Компютъра (наричани „Данни“). Крайният потребител следва да има правото да използва получените от тази функция и предоставени през ESET HOME акаунт Данни единствено за поправяне на неблагоприятна ситуация, причинена от кражбата на Компютър. Единствено с цел тази функция Доставчикът обработва Данни в съответствие с указаното в Правилата за поверителност и приложимите законови разпоредби. Доставчикът разрешава на Крайния потребител да осъществява достъп до Данните за необходимия период за постигане на целта, за която са получени данните, който не може да надвишава периода на съхранение, указан в Правилата за поверителност. Защитата срещу злоупотреба с данни се използва единствено с Компютри и акаунти, до които Крайният потребител разполага с легитимен достъп. Всяко незаконно използване ще бъде докладвано на компетентния орган. Доставчикът ще спазва приложимите закони и ще съдейства на правоприлагащите органи в случай на злоупотреба. Вие се съгласявате и потвърждавате, че носите отговорност за защитата на паролата за достъп до ESET HOME акаунта, и се съгласявате да не разкривате паролата си на което и да е трето лице. Крайният потребител носи отговорност за всяка дейност, извършена с функцията за Защита срещу злоупотреба с данни и ESET HOME акаунта, независимо дали е разрешена, или не. Ако акаунтът в ESET HOME бъде компрометиран, уведомете Доставчика незабавно. Допълнителните разпоредби за Защита срещу злоупотреба с данни са приложими само към Крайни потребители на ESET Internet Security и ESET Smart Security Premium.

ESET Secure Data. Допълнителните разпоредби са приложими за ESET Secure Data, както следва:

1. Дефиниции. В настоящите допълнителни разпоредби към ESET Secure Data следните думи имат съответните значения:

а) „Информация“ всяка информация или данни, шифровани или дешифровани, използвайки софтуера;

б) „Продукти“ софтуерът ESET Secure Data и документацията;

в) „ESET Secure Data“ софтуерът(ите), използван(и) за криптиране и декриптиране на електронни данни;

Всички препратки към множествено число следва да включват единствено и всички препратки към мъжки род следва да включват женски и среден и обратно. Думи без конкретна дефиниция трябва да се използват в съответствие с дефиниции, предвидени от Споразумението.

2. Допълнителна декларация на Крайния потребител. Вие приемате и се съгласявате, че:

а) е Ваша отговорност да защитавате, поддържате и архивирате Информацията;

б) трябва да архивирате напълно цялата информация и данни (включително, но не само, критично важна информация и данни) на Вашия Компютър преди инсталирането на ESET Secure Data;

в) трябва да пазите защитен запис с всички пароли или друга информация, използвана за настройване и използване на ESET Secure Data, трябва също да направите архивни копия на всички ключове за шифроване, кодове за лицензи, файлове с ключове и други генерирани данни на отделен носител за съхранение;

г) отговорни сте за употребата на Продуктите. Доставчикът не носи никаква отговорност за каквито и да било загуби, спорове или щети, претърпени вследствие на неупълномощено или погрешно шифроване или дешифроване на Информация или други данни, където или както и да е съхранявана тази Информация или данни;

д) докато Доставчикът е взел всички разумни мерки, за да осигури целостта и защитата на ESET Secure Data, Продуктите (или някои от тях) не трябва да бъдат използвани в зони, които разчитат на ниво на сигурност, устойчиво на грешки, или потенциално вредни или опасни, включително, но не само, ядрени бази, системи за самолетна навигация, контрол или комуникация, оръжейни и отбранителни системи и животоподдържащи системи или системи за наблюдение на жизнени показатели;

е) Крайният потребител носи отговорността да гарантира, че нивото на сигурност и шифроване, предоставено от продуктите, е подходящо за Вашите изисквания;

ж) Вие сте отговорни за употребата на Продуктите или някой от тях, включително, но не само, гарантиране, че такава употреба е в съответствие с всички приложими закони и разпоредби на Република Словакия или друга държава, регион или щат, където се използват Продуктите. Преди каквато и да е употреба на Продуктите трябва да гарантирате, че сте се уверили, че тя не е в нарушение с което и да е правителствено (в Република Словакия или другаде) ембарго;

з) ESET Secure Data може да се свързва със сървърите на Доставчика от време на време, за да проверява информацията за лицензa, наличните корекции, сервизните пакети и други актуализации, които могат да подобрят, поддържат, променят или подобряват работата на

ESET Secure Data и може да изпраща основна информация за системата, свързана с функционирането й в съответствие с Правилата за поверителност.

и) Доставчикът не носи отговорност за каквато и да е било загуба, щета, разход или претенция, произлизаща от загуба, кражба, погрешно използване, повреда или унищожаване на пароли, информация за настройване, ключове за шифроване, кодове за активиране на лицензи и други данни, генерирани или съхранени по време на използването на софтуера.

Допълнителните разпоредби за ESET Secure Data са приложими само към Крайни потребители на ESET Smart Security Premium.

Софтуер Password Manager. Допълнителните разпоредби са приложими към Софтуера Password Manager, както следва:

1. Допълнителна декларация на Крайния потребител. Вие приемате и се съгласявате, че не можете да:

а) използвате Софтуера Password Manager за работа с критичноважно за мисията приложение, където човешки живот или собственост може да е застрашена. Вие разбирате, че Софтуерът Password Manager не е проектиран за такива цели и че неизправност в такива случаи може да доведе до смърт, телесни наранявания или сериозни щети на собственост или околна среда, за които Доставчикът не носи отговорност.

СОФТУЕРЪТ PASSWORD MANAGER НЕ Е ПРОЕКТИРАН, ПРЕДНАЗНАЧЕН ИЛИ ЛИЦЕНЗИРАН ЗА ИЗПОЛЗВАНЕ В СРЕДИ, ИЗИСКВАЩИ КОНТРОЛИ, УСТОЙЧИВИ НА ГРЕШКИ, ВКЛЮЧИТЕЛНО, НО НЕ САМО, ПРОЕКТИРАНЕТО, ИЗГРАЖДАНЕТО, ПОДДРЪЖКАТА ИЛИ РАБОТАТА НА ЯДРЕНИ БАЗИ, СИСТЕМИ ЗА САМОЛЕТНО НАВИГИРАНЕ ИЛИ КОМУНИКАЦИИ, УПРАВЛЕНИЕ НА ВЪЗДУШЕН ТРАФИК И ЖИВОТОПОДДЪРЖАЩИ ИЛИ ОРЪЖЕЙНИ СИСТЕМИ. ДОСТАВЧИКЪТ ОТХВЪРЛЯ ВСЯКА ИЗРИЧНА ИЛИ ПОДРАЗБИРАЩА СЕ ГАРАНЦИЯ ЗА ГОДНОСТ ЗА ТАКИВА ЦЕЛИ.

б) използвате Софтуера Password Manager по начин, който нарушава това споразумение или законите на Република Словакия или Вашата юрисдикция. По-конкретно нямате право да използвате Софтуера Password Manager, за да провеждате или рекламирате каквито и да е било незаконни дейности, включително качване на данни с вредно съдържание или съдържание, което може да бъде използвано за незаконни дейности или по начин, нарушаващ закона или правата на трети лица (включително права на интелектуална собственост), включително, но не само, всякакви опити да се получи достъп до акаунти в Хранилище (за целите на настоящите допълнителни разпоредби за Password Manager „Хранилище“ се отнася за хранилището на данни, управлявано от Доставчика или трето лице, различно от Доставчика и потребителя, с цел разрешаване на синхронизация и архивиране на потребителски данни) или акаунти и данни на други потребители на Софтуера Password Manager или на Хранилището. Ако нарушите някоя от тези клаузи, Доставчикът е в правото си веднага да прекрати това споразумение и да Ви предаде стойността на всички необходими правни средства за обжалване, както и да вземе необходимите мерки за предотвратяването на използването на Софтуера Password Manager от Вас без възможност за възстановяване на средства.

2. ОГРАНИЧЕНИЕ НА ОТГОВОРНОСТТА. СОФТУЕРЪТ PASSWORD MANAGER СЕ ПРЕДОСТАВЯ „КАКТО Е“. БЕЗ КАКВАТО И ДА Е ИЗРИЧНА ИЛИ ПОДРАЗБИРАЩА СЕ ГАРАНЦИЯ. ВИЕ ИЗПОЛЗВАТЕ СОФТУЕРА НА СВОЯ ОТГОВОРНОСТ. ПРОИЗВОДИТЕЛЯТ НЕ НОСИ ОТГОВОРНОСТ ЗА ЗАГУБА НА ДАННИ, ЩЕТИ, ОГРАНИЧЕНИЕ НА НАЛИЧНОСТТА НА УСЛУГИ, ВКЛЮЧИТЕЛНО ВСИЧКИ ДАННИ, ИЗПРАТЕНИ ОТ СОФТУЕРА PASSWORD MANAGER ДО ВЪНШНО ХРАНИЛИЩЕ С ЦЕЛ СИНХРОНИЗАЦИЯ И АРХИВИРАНЕ. ШИФРОВАНЕ НА ДАННИТЕ, ИЗПОЛЗВАЙКИ СОФТУЕРА PASSWORD MANAGER, НЕ

ВОДИ ДО ПОЕМАНЕ НА ОТГОВОРНОСТ ОТ ДОСТАВЧИКА ПО ОТНОШЕНИЕ НА СИГУРНОСТТА НА ТЕЗИ ДАННИ. ВИЕ ИЗРИЧНО СЕ СЪГЛАСЯВАТЕ, ЧЕ ДАННИТЕ ПРИДОБИТИ, ИЗПОЛЗВАНИ, ШИФРОВАНИ, СЪХРАНЯВАНИ, СИНХРОНИЗИРАНИ ИЛИ ИЗПРАТЕНИ, ИЗПОЛЗВАЙКИ СОФТУЕРА PASSWORD MANAGER, МОГАТ СЪЩО ДА БЪДАТ СЪХРАНЯВАНИ НА СЪРВЪРИТЕ НА ТРЕТИ СТРАНИ (ОТНАСЯ СЕ САМО ЗА ИЗПОЛЗВАНЕТО НА СОФТУЕРА PASSWORD MANAGER, КЪДЕТО СА РАЗРЕШЕНИ УСЛУГИ ЗА СИНХРОНИЗАЦИЯ И АРХИВИРАНЕ). АКО ДОСТАВЧИКЪТ, ПО СВОЯ СОБСТВЕНА ПРЕЦЕНКА, ИЗБЕРЕ ДА ИЗПОЛЗВА ТАКОВА ХРАНИЛИЩЕ, УЕБ САЙТ, УЕБ ПОРТАЛ, СЪРВЪР ИЛИ УСЛУГА ОТ ТРЕТИ СТРАНИ, ДОСТАВЧИКЪТ НЕ НОСИ ОТГОВОРНОСТ ЗА КАЧЕСТВОТО, ЗАЩИТАТА ИЛИ НАЛИЧНОСТТА НА ТАКАВА УСЛУГА ОТ ТРЕТО ЛИЦЕ И ДО НИКАКВА СТЕПЕН ДОСТАВЧИКЪТ НЕ НОСИ ОТГОВОРНОСТ ЗА КАКВИТО И ДА Е НАРУШЕНИЯ НА ДОГОВОРНИ ИЛИ ЗАКОНОВИ ЗАДЪЛЖЕНИЯ НА ТРЕТАТА СТРАНА, НИТО ЗА ЩЕТИ, ПРОПУСНАТИ ПОЛЗИ, ФИНАНСОВИ ИЛИ НЕФИНАНСОВИ ЩЕТИ ИЛИ КАКЪВТО И ДА Е ДРУГ ВИД ЗАГУБИ ПРИ ИЗПОЛЗВАНЕТО НА СОФТУЕРА. ДОСТАВЧИКЪТ НЕ НОСИ ОТГОВОРНОСТ ЗА СЪДЪРЖАНИЕТО НА КОИТО И ДА Е ДАННИ ПОЛУЧЕНИ, ИЗПОЛЗВАНИ, ШИФРОВАНИ, СЪХРАНЯВАНИ, СИНХРОНИЗИРАНИ ИЛИ ИЗПРАТЕНИ, ИЗПОЛЗВАЙКИ СОФТУЕРА PASSWORD MANAGER, ИЛИ В ХРАНИЛИЩЕТО. ВИЕ СЕ СЪГЛАСЯВАТЕ, ЧЕ ДОСТАВЧИКЪТНЯМА ДОСТЪП ДО СЪДЪРЖАНИЕТО НА СЪХРАНЕНИТЕ ДАННИ И НЕ МОЖЕ ДА НАБЛЮДАВА ИЛИ ПРЕМАХВА ПО ЗАКОНЕН НАЧИН ВРЕДНО СЪДЪРЖАНИЕ.

Доставчикът притежава всички права за подобрения, надстройки и корекции, свързани със Софтуера Password Manager („Подобрения“), дори и в случай че такива подобрения са създадени на основата на обратна връзка, идеи или предложения, изпратени от Вас под каквато и да е форма. Вие нямате правото на компенсации, включително никакви авторски хонорари, свързани с такива Подобрения.

ОРГАНИЗАЦИИТЕ НА ДОСТАВЧИКА И ЛИЦЕНЗОДАТЕЛИТЕ НЯМА ДА НОСЯТ ОТГОВОРНОСТ КЪМ ВАС ЗА ПРЕТЕНЦИИ И ОТГОВОРНОСТИ ОТ ВСЯКАКЪВ ВИД, КОИТО СА В РЕЗУЛТАТ НА ИЛИ ПО НЯКАКЪВ НАЧИН СВЪРЗАНИ СЪС СОФТУЕРА PASSWORD MANAGER ОТ ВАС ИЛИ ОТ ТРЕТИ СТРАНИ, КЪМ УПОТРЕБАТА ИЛИ НЕУПОТРЕБАТА НА БРОКЕРСКИ ФИРМИ ИЛИ ТЪРГОВЦИ ИЛИ КЪМ ПРОДАЖБАТА ИЛИ ЗАКУПУВАНЕТО НА КАКВАТО И ДА Е ЗАЩИТА, БЕЗ ЗНАЧЕНИЕ ДАЛИ ТАКИВА ПРЕТЕНЦИИ И ЗАДЪЛЖЕНИЯ СА НА ОСНОВАТА НА ПРАВНА ИЛИ РАВНОПРАВНО ПРИЛАГАЩА СЕ ТЕОРИЯ.

ОРГАНИЗАЦИИТЕ НА ДОСТАВЧИКА И ЛИЦЕНЗОДАТЕЛИТЕ НЯМА ДА НОСЯТ ОТГОВОРНОСТ КЪМ ВАС ЗА ВСЯКА И ВСИЧКИ ПРЕКИ, ИНЦИДЕНТНИ, СПЕЦИАЛНИ, НЕПРЕКИ ИЛИ ПОСЛЕДВАЩИ ЩЕТИ В РЕЗУЛТАТ НА ИЛИ СВЪРЗАНИ С КАКЪВТО И ДА Е СОФТУЕР ОТ ТРЕТИ СТРАНИ, ВСЯКАКВИ ДАННИ, ДО КОИТО Е ОСЪЩЕСТВЕН ДОСТЪП ЧРЕЗ СОФТУЕРА PASSWORD MANAGER, ВАШЕТО ИЗПОЛЗВАНЕ ИЛИ НЕВЪЗМОЖНОСТ ЗА ИЗПОЛЗВАНЕ ИЛИ ОСЪЩЕСТВЯВАНЕ НА ДОСТЪП ДО СОФТУЕРА PASSWORD MANAGER ИЛИ ВСЯКАКВИ ДАННИ, ПРЕДОСТАВЕНИ ЧРЕЗ СОФТУЕРА PASSWORD MANAGER, НЕЗАВИСИМО ДАЛИ ТАКИВА ВЗЕМАНИЯ ЗА ЩЕТИ СА ПРОИЗЛЕЗЛИ ОТ ПРАВНА ИЛИ РАВНОПРАВНО ПРИЛАГАЩА СЕ ТЕОРИЯ. ЩЕТИ, ИЗКЛЮЧВАНИ ОТ ТАЗИ КЛАУЗА, ВКЛЮЧВАТ, НО НЕ СЕ ОГРАНИЧАВАТ ДО, ТЕЗИ ЗА ПРОПУСНАТИ БИЗНЕС ПОЛЗИ, ТЕЛЕСНО НАРАНЯВАНЕ НА ЛИЦЕ ИЛИ ЩЕТА НА СОБСТВЕНОСТ, ПРЕКЪСВАНЕ НА ДЕЙНОСТ, ЗАГУБА НА БИЗНЕС ИЛИ ЛИЧНА ИНФОРМАЦИЯ. НЯКОИ ЮРИСДИКЦИИ НЕ ПОЗВОЛЯВАТ ОГРАНИЧАВАНЕ НА ИНЦИДЕНТНИ ИЛИ ПОСЛЕДВАЩИ ЩЕТИ, ТАКА ЧЕ ТЕЗИ ОГРАНИЧЕНИЯ МОЖЕ ДА НЕ СЕ ОТНАСЯТ ЗА ВАС. В ТАКЪВ СЛУЧАЙ СТЕПЕНТА НА ОТГОВОРНОСТ НА ДОСТАВЧИКА ЩЕ БЪДЕ МИНИМАЛНАТА, РАЗРЕШЕНА ОТ ПРИЛОЖИМИЯ ЗАКОН.

ИНФОРМАЦИЯТА, ПРЕДОСТАВЕНА ЧРЕЗ СОФТУЕРА PASSWORD MANAGER, ВКЛЮЧИТЕЛНО СТОКОВИ КОТИРОВКИ, АНАЛИЗИ, ПАЗАРНА ИНФОРМАЦИЯ, НОВИНИ И ФИНАНСОВИ ДАННИ, МОЖЕ ДА БЪДЕ ЗАБАВЕНА, НЕТОЧНА ИЛИ ДА СЪДЪРЖА ГРЕШКИ ИЛИ ПРОПУСКИ, А ОРГАНИЗАЦИИТЕ НА ДОСТАВЧИКА И ЛИЦЕНЗОДАТЕЛИТЕ НЕ НОСЯТ ОТГОВОРНОСТ ПО ОТНОШЕНИЕ НА СЪЩОТО.

ДОСТАВЧИКЪТ ИМА ПРАВО ДА ПРОМЕНИ ИЛИ ПРЕКРАТИ ВСЕКИ АСПЕКТ ИЛИ ФУНКЦИЯ НА СОФТУЕРА PASSWORD MANAGER ИЛИ ИЗПОЛЗВАНЕТО НА ВСЯКА ИЛИ ВСИЧКИ ФУНКЦИИ ИЛИ ТЕХНОЛОГИИ В СОФТУЕРА PASSWORD MANAGER ПО ВСЯКО ВРЕМЕ, БЕЗ ДА ВИ ИЗВЕСТЯВА ПРЕДВАРИТЕЛНО.

АКО РАЗПОРЕДБИТЕ В ТОЗИ ЧЛЕН СА НЕВАЛИДНИ ПОРАДИ НЯКАКВА ПРИЧИНА ИЛИ ДОСТАВЧИКЪТ Е СЧИТАН ЗА ОТГОВОРЕН ЗА ЗАГУБИ, ЩЕТИ И Т.Н. СПОРЕД ПРИЛОЖИМИТЕ ЗАКОНИ, СТРАНИТЕ СЕ СЪГЛАСЯВАТ, ЧЕ ОТГОВОРНОСТТА НА ДОСТАВЧИКА КЪМ ВАС ЩЕ БЪДЕ ОГРАНИЧЕНА ДО ОБЩАТА СТОЙНОСТ НА ТАКСИТЕ ЗА ЛИЦЕНЗ, ПЛАТЕНИ ОТ ВАС.

СЪГЛАСЯВАТЕ СЕ ДА ОБЕЗЩЕТИТЕ, ЗАЩИТИТЕ И ПРЕДПАЗИТЕ ДОСТАВЧИКА И НЕГОВИТЕ СЛУЖИТЕЛИ, ДЪЩЕРНИ ДРУЖЕСТВА, СВЪРЗАНИ ЛИЦА, ПАРТНЬОРИ ЗА ПОВТОРНО ПРЕДСТАВЯНЕ И ДРУГИ ОТ И СРЕЩУ ВСИЧКИ ПРЕТЕНЦИИ, ОТГОВОРНОСТИ, ЩЕТИ, ЗАГУБИ, РАЗНОСКИ, РАЗХОДИ, ТАКСИ ОТ ТРЕТИ СТРАНИ (ВКЛЮЧИТЕЛНО СОБСТВЕНИЦИ НА УСТРОЙСТВОТО ИЛИ СТРАНИ, ЧИИТО ПРАВА СА БИЛИ ЗАСЕГНАТИ ОТ ДАННИТЕ, ИЗПОЛЗВАНИ В СОФТУЕРА PASSWORD MANAGER ИЛИ В ХРАНИЛИЩЕТО), КОИТО ТАКИВА СТРАНИ МОГАТ ДА НАПРАВЯТ В РЕЗУЛТАТ НА ИЗПОЛЗВАНЕТО НА СОФТУЕРА PASSWORD MANAGER.

3. Данни в Софтуера Password Manager. Освен ако изрично не е избрано друго от Вас, всички въведени от Вас данни, които са запазени в базата данни на Софтуера Password Manager, се съхраняват в шифрован формат на Вашия компютър или друго устройство за съхранение, както е посочено от Вас. Разбирате, че в случай на изтриване или повреда на която и да е база данни на Софтуера Password Manager или други файлове, всички данни, съдържащи се там, ще бъдат безвъзвратно загубени, и разбирате и приемате риска от такава загуба. Фактът, че личните Ви данни са съхранявани в шифрован формат на компютъра не означава, че информацията не може да бъде откраднатa или с нея да се злоупотреби от някой, който е открил Основната парола или е придобил достъп до зададено от потребителя активиращо устройство за отваряне на базата данни. Вие носите отговорност за поддържането на защитата на всички методи на достъп.

4. Трансфер на Лични данни към Доставчика или Хранилището. Ако изберете това и единствено с цел подсигуряването на навременна синхронизация и архивиране на данни, Софтуерът Password Manager прехвърля или изпраща лични данни от базата данни на Софтуера Password Manager – а именно пароли, информация за влизане, Акаунти и Самоличности – през Интернет към Хранилището. Данните се прехвърлят изключително само в шифрована форма. Използването на Софтуера Password Manager за попълване на онлайн формуляри с пароли, данни за влизане и други данни може да изисква тази информация да бъде изпратена през Интернет към уеб сайт, идентифициран от Вас. Това прехвърляне на данни не е започнато от Софтуера Password Manager и по тази причина Доставчикът не може да носи отговорност за сигурността на такива взаимодействия с който и да е уеб сайт, поддържан от различни доставчици. Всякакви транзакции през Интернет, независимо дали във връзка със Софтуера Password Manager, или не, се правят по Ваша преценка и риск и Вие носите цялата отговорност за всякаква повреда на Вашата компютърна система или загуба на данни в резултат на изтегляне и/или използване на всякакъв такъв материал или услуга. За да намалите до минимум риска от загуба на ценни данни, Доставчикът препоръчва на клиентите да изпълняват периодично архивиране на базата данни и други конфиденциални файлове на външни устройства. Доставчикът не може да Ви предостави помощ при възстановяването на загубени или повредени данни. Ако Доставчикът предоставя услуга за архивиране за потребителските файлове от база данни в случай на повреда или изтриване на файлове на компютъра на потребителя, такава услуга за архивиране е без каквато и да е било гаранция и не означава, че Доставчикът носи каквато и да е отговорност към Вас.

С използването на Софтуера Password Manager се съгласявате, че софтуерът може да се свързва понякога със сървърите на Доставчика, за да проверява информацията за лицензa, наличните корекции, сервизните пакети и други актуализации, които могат да подобрят, поддържат, променят или подобряват работата на Софтуера Password Manager. Софтуерът може да изпраща основна информация за системата, свързана с функционирането на Софтуера Password Manager.

5. Информация и инструкции за деинсталиране. Всяка информация, която бихте искали да запазите извън базата данни, трябва да бъде експортирана, преди да деинсталирате Софтуера Password Manager.

Допълнителните разпоредби за Софтуера Password Manager са приложими само към Крайни потребители на ESET Smart Security Premium.

ESET LiveGuard. Допълнителните разпоредби са приложими за ESET LiveGuard, както следва:

Софтуерът съдържа функция за допълнителен анализ на файлове, подадени от Краен потребител. Доставчикът използва само файловете, подадени от Краен потребител, и резултатите от анализа при спазване на Правилата за поверителност и при спазване на съответните законови разпоредби.

Допълнителните разпоредби за ESET LiveGuard са приложими само към Крайни потребители на ESET Smart Security Premium.

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

Условия за поверителност

Защитата на личните данни е от особено значение за ESET, spol. s r. o., със седалище и адрес на управление Einsteinova 24, 851 01 Bratislava, Slovak Republic, с регистрация в Търговския регистър, администриран от Окръжния съд I в Братислава, секция Sro, под фирмено дело 3586/B, фирмен номер: 31333532 като Администратор на данни („ESET“ или „Ние“). Искаме да спазваме изискването за прозрачност, както е стандартизирано по закон съгласно Общия регламент на ЕС за защита на данните („ОРЗД“). За да постигнем тази цел, ние публикуваме настоящите Правила за поверителност с единствената цел да информираме нашия клиент („Краен потребител“ или „Вие“) като субект на данни по отношение на следните теми, свързани със защитата на личните данни:

- Правно основание за обработването на личните данни,
- Споделяне и поверителност на данните,
- Защита на данните,
- Вашите права като субект на данни,
- Обработване на Вашите лични данни
- Информация за връзка.

Правно основание за обработването на личните данни

Има само няколко правни основания за обработване на данни, които използваме съгласно приложимата законодателна рамка, свързана със защитата на личните данни. Обработването на лични данни от ESET е необходимо основно за изпълнението на Лицензионно споразумение с краен потребител („ЛСКП“) с Краен потребител (чл. 6 (1) (б) ОРЗД), което е приложимо за предоставянето на продукти или услуги на ESET, освен ако изрично не е посочено друго, напр.:

- Правно основание за легитимни интереси (чл. 6 (1) (е) ОРЗД), което ни позволява да обработваме данни за това как нашите клиенти използват Услугите ни и тяхната удовлетвореност, за да предоставяме на нашите потребители най-добрата защита, поддръжка и изживяване, които можем да предложим. Дори маркетингът е признат от приложимото законодателство като легитимен интерес, затова разчитаме на него за маркетингова комуникация с нашите клиенти.

- Съгласие (чл. 6 (1) (а) ОРЗД), което ние можем да поискаме от Вас в конкретни ситуации, когато считаме това правно основание за най-подходящото или ако това се изисква от закона.

- Спазване на правните задължения (чл. 6 (1) (в) ОРЗД), напр. предвидените изисквания за електронна комуникация, съхранение на документи за фактуриране или плащане.

Споделяне и поверителност на данните

Ние не споделяме Вашите данни с трети страни. Въпреки това ESET е фирма, работеща на глобално ниво чрез свързани юридически лица или партньори като част от нашата мрежа за продажби, обслужване и поддръжка. Информацията за лицензиране, фактуриране и техническа поддръжка, обработвана от ESET, може да се прехвърля към или от свързани юридически лица или партньори за целите на изпълнението на лицензионното споразумение с краен потребител, като например предоставянето на услуги и поддръжка.

ESET предпочита да обработва данните си в Европейския съюз (ЕС). Въпреки това, в зависимост от Вашето местоположение (използване на нашите продукти и/или услуги извън ЕС) и/или услугата, която изберете, може да е необходимо да прехвърляме данните Ви в държава извън ЕС. Например използваме услуги на трети страни във връзка с изчисления в облака. В тези случаи внимателно подбираме нашите доставчици на услуги и гарантираме подходящо ниво на защита на данните чрез договорни, както и технически и организационни мерки. По правило се договаряме по стандартните договорни клаузи на ЕС и ако е необходимо – с допълнителни договорни разпоредби.

За някои държави извън ЕС, като например Обединеното кралство и Швейцария, ЕС вече определи сравнимо ниво на защита на данните. Поради сравнимото ниво на защита на данните прехвърлянето на данни към тези държави не изисква специално разрешение или споразумение.

Защита на данните

ESET внедрява подходящи технически и организационни мерки, за да осигури ниво на защита, подходящо за потенциални рискове. Правим всичко, което можем, за да осигурим непрекъсната поверителност, цялост, наличност и издръжливост на системите и услугите за обработка. В случай на пробив в защитата на данните, вследствие на който се появява риск за

Вашите права и свободи, ние сме готови да уведомим съответните надзорни органи, както и засегнатите Крайни потребители и субекти на данни.

Права на субектите на данни

Правата на всеки Краен потребител имат значение и бихме искали да Ви информираме, че всички Крайни потребители (от държава във или извън ЕС) имат следните права, гарантирани от ESET. За да упражните Вашите права на субект на данни, можете да се свържете с нас чрез формуляр за поддръжка или по имейла: dpo@eset.sk. За целите на идентификацията Ви молим за следната информация: Име, имейл адрес и – ако е наличен – лицензионен ключ или клиентски номер и фирмена принадлежност. Въздържайте се от изпращане на други лични данни, като например датата на раждане. Бихме искали да отбележим, че за да обработим Вашата заявка, както и за целите на идентификацията, ще обработим Вашите лични данни.

Право на оттегляне на съгласието. Правото на оттегляне на съгласието е приложимо в случай на обработване само въз основа на съгласие. Ако обработваме Вашите лични данни въз основа на Вашето съгласие, имате право да оттеглите съгласието по всяко време, без да посочвате причини. Оттеглянето на Вашето съгласие е ефективно само за бъдещето и не засяга законността на данните, обработени преди оттеглянето.

Право на възражение. Правото на възражение срещу обработването е приложимо в случай на обработка въз основа на законния интерес на ESET или трета страна. Ако обработваме Вашите лични данни, за да защитим законен интерес, Вие – като субект на данните – имате право да възразите срещу законния интерес, посочен от нас, и обработването на Вашите лични данни по всяко време. Възражението е ефективно само за бъдещето и не засяга законността на данните, обработени преди възражението. Ако обработваме личните Ви данни за целите на директния маркетинг, не е необходимо да посочвате причини за възражението си. Това важи и за профилирането, доколкото е свързано с такъв директен маркетинг. Във всички останали случаи Ви молим да ни информирате накратко за Вашите оплаквания срещу законния интерес на ESET да обработва Вашите лични данни.

Имайте предвид, че в някои случаи, въпреки оттеглянето ви на съгласие, ние имаме право допълнително да обработваме Вашите лични данни въз основа на друго правно основание, например за изпълнението на договор.

Право на достъп. Като субект на данни имате право да получите информация за Вашите данни, съхранявани от ESET, безплатно и по всяко време.

Право на корекция. Ако неволно обработваме неточни лични данни за Вас, имате право да бъдат коригирани.

Право на изтриване и право на ограничаване на обработването. Като субект на данни имате правото да поискате изтриване или ограничаване на обработването на личните Ви данни. Ако обработваме Вашите лични данни, например с Ваше съгласие, го оттегляте и ако няма друго правно основание, като например договор, ние премахваме Вашите лични данни незабавно. Вашите лични данни също ще бъдат премахнати веднага след като вече не се изискват за целите, посочени за тях в края на нашия период на съхранение.

Ако използваме Вашите лични данни единствено с цел директен маркетинг и сте отменили Вашето съгласие или сте възразили срещу основния законен интерес на ESET, ние ще ограничим обработването на Вашите лични данни до степен, в която включваме Вашите данни за контакт във вътрешния ни списък със забранени адреси, за да избегнем нежелан контакт. В

противен случай личните Ви данни ще бъдат премахнати.

Обърнете внимание, че от нас може да се изиска да съхраняваме Вашите данни до изтичането на задълженията и периодите за съхраняване, издадени от законодателя или надзорните органи. Задълженията и периодите за съхраняване могат да произтичат и от словашкото законодателство. След това съответните данни ще бъдат рутинно премахнати.

Правото на преносимост на данните. Радваме се, че можем да Ви предоставяме – в качеството Ви на субект на данни – личните данни, обработвани от ESET във формат xls.

Право на подаване на жалба. Като субект на данни Вие имате правото да подадете жалба до надзорен орган по всяко време. ESET се регулира от разпоредбите на словашките закони и ние сме обвързани със законите за защита на данните като част от Европейския съюз. Съответният надзорен орган за данните е Службата за защита на личните данни на Република Словакия, намираща се на адрес Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Обработване на Вашите лични данни

Услуги, осигурявани от ESET, изпълнени в нашия продукт, се предоставят съгласно условията на Лицензионно споразумение с краен потребител, но някои от тях може да изискват специално внимание. Бихме искали да Ви предоставим повече подробности относно събирането на данни, свързано с предоставянето на нашите услуги. Предлагаме различни услуги, описани в лицензионното споразумение с краен потребител и продуктовата документация. За да можем да правим всичко това, трябва да събираме или имаме достъп до следната информация:

Данни за лицензиране и фактуриране. Името, имейл адресът, лицензионният ключ и (ако е приложимо) адресът, фирмената принадлежност и данните за плащанията се събират и обработват от ESET с цел да се улесни активирането на лиценз, доставка на лицензионен ключ, напомняния при изтичане на срока, заявки за поддръжка, проверка на валидността на лиценза, предоставяне на обслужване и други известия, включително маркетингови съобщения, в съответствие с приложимото законодателство или Вашето съгласие. ESET е правно задължена да запази информацията за фактуриране за периода от 10 години, като лицензионната информация ще бъде анонимизирана не по-късно от 12 месеца след изтичането на лиценза.

Обновяване и други статистически данни. Обработената информация включва информация относно процеса на инсталиране и компютъра Ви, включително платформата, на която е инсталиран нашият продукт, а информация за операциите и функционалността на нашите продукти, като например операционна система, информация за хардуера, ИД на инсталацията, ИД на лиценза, IP адрес, MAC адрес, настройки за конфигуриране на продукта, се обработва с цел предоставяне на услуги за обновяване и надстройване и с цел поддръжка, защита и подобряване на нашата сървърна инфраструктура.

Тази информация се съхранява отделно от идентификационната информация, изисквана за целите на лицензирането и фактурирането, тъй като тя не изисква идентификацията на Крайния потребител. Срокът на съхранение е до 4 години.

Система на ESET LiveGrid® за репутация. Еднопосочни хешове, свързани с проникванията, като част от системата на ESET LiveGrid® за репутация, която подобрява ефективността на решенията ни за защитата срещу злонамерен софтуер чрез сравняване на сканираните файлове с база данни от разрешени и забранени елементи в облака. Крайният потребител не е

идентифициран по време на този процес.

Система на ESET LiveGrid® за обратна връзка. Подозрителни примери и метаданни от практиката като част от нашата система на ESET LiveGrid® за обратна връзка позволяват на ESET да реагира незабавно на нуждите на нашите крайни потребители и ни държи отговорни за подсигуряване на действия срещу най-новите заплахи. ие сме зависими от Вас по отношение на това да ни изпращате

- Прониквания, като потенциални примери за вируси и други злонамерени програми и съмнителни, проблемни, потенциално нежелани или потенциално небезопасни обекти, като изпълними файлове, имейл съобщения, докладвани от Вас като спам или маркирани с флаг от нашия продукт;

- Информация относно използването на интернет, като IP адрес и географска информация, IP пакети, URL адреси и ethernet рамки;

- Файлове на аварийни копия при срив и съдържащата се информация.

Не желаем да събираме Ваши данни извън този обхват, но понякога не е възможно да го предотвратим. В злонамерения софтуер може да бъдат включени случайно събрани данни (събрани без Вашето знание или одобрение) или като част от имена на файлов или URL адреси и ние не искаме те да бъдат част от нашите системи или да ги обработваме за целта, обявена в настоящите Правила за поверителност.

Цялата информация, получена и обработена чрез ESET LiveGrid® системата за обмен на информация за потенциални заплахи, е предназначена за използване без идентифицирането на Крайния потребител.

Г) **Оценка на защитата на свързаните с мрежата устройства.** За да осигурим функцията за оценка на защитата, ние обработваме името на Вашата локална мрежа и информация за устройства в локалната мрежа, като достъпност, тип, име, IP адрес и MAC адрес на устройството в локална мрежа във връзка с информация за лицензa. Информацията включва също типа защита на безжичната мрежа и типа шифроване на безжичната мрежа за маршрутизатори. Лицензионната информация, идентифицираща Крайния потребител, ще бъде анонимизирана не по-късно от 12 месеца след изтичането на лицензa.

Техническа поддръжка. Информацията за контакт и лицензиране, както и данните, които се съдържат във Вашите заявки за поддръжка, може да се изискват за услугата по поддръжка. В зависимост от канала, който изберете, за да се свържете с нас, ние може да събираме подробни данни за Вашия имейл адрес, телефонен номер, информация за лиценз, подробни данни за продукт и описание на Вашия случай за поддръжка. Възможно е да Ви помолим да ни предоставите друга информация, за да улесним услугата по поддръжка. Обработените за техническа поддръжка данни се съхраняват в продължение на 4 години.

Защита срещу злоупотреба с данни. Ако Акаунтът в ESET HOME на адрес https://home.eset.com е създаден и функцията е активирана от Краен потребител във връзка с кражба на компютър, ще се събира и обработва следната информация: данни за местоположението, екранни снимки, данни за конфигурацията на компютъра и данни, записани от камерата на компютъра. Събраните данни се съхраняват на нашите сървъри или на сървърите на нашите доставчици на услуги с период на съхранение от 3 месеца.

Password Manager. Ако изберете да активирате функцията на Password Manager, данните за

влизане се съхраняват в шифрована форма само на Вашия компютър или друго определено устройство. Ако активирате услугата за синхронизация, шифрованите данни се съхраняват на нашите сървъри или на сървърите на нашите доставчици на услуги, за да се гарантира такава услуга. Нито ESET, нито доставчикът на услуги има достъп до шифрованите данни. Само Вие имате ключа за дешифриране на данните. Данните ще бъдат премахнати при деактивиране на функцията.

ESET LiveGuard. Ако изберете да активирате функцията ESET LiveGuard, от Вас ще се изиска да подадете примери, като например предварително определени и избрани от Крайния потребител. Примерите, които изберете за отдалечения анализ, ще бъдат качени в услугата ESET, а резултатът от анализа ще бъде изпратен обратно на Вашия компютър. Всички подозрителни примери се обработват по начина на информацията, събирана от системата на ESET LiveGrid® за обратна връзка.

Програма за подобряване на работата на клиентите. Ако сте избрали да активирате Програма за подобряване на работата на клиентите , ще се събира и използва анонимната телеметрична информация, свързана с използването на Нашите продукти, въз основа на Вашето съгласие.

Обърнете внимание, че ако лицето, използващо нашите продукти и услуги, не е Крайният потребител, закупил продукта или услугата и сключил лицензионно споразумение с краен потребител с нас (напр. служител на Крайния потребител, член на семейството или лице, упълномощено по друг начин да използва продукт или услуга от Крайния потребител в съответствие с лицензионното споразумение с краен потребител, обработването на данните се извършва в законния интерес на ESET по смисъла на чл. 6 (1) (е) ОРЗД, за да позволи на потребителя, упълномощен от Крайния потребител, да използва продукти и услуги, предоставяни от нас в съответствие с лицензионното споразумение с краен потребител.

Информация за връзка

Ако желаете да упражните Вашето право като субект на данни или имате въпрос или опасение, изпратете ни съобщение на:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk