

КОД  
ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ

# Как выжить в году 2019? Пройдемся по ошибкам



Вячеслав Медведев  
ООО «Доктор Веб»

**ТЕЛЕФОН:** +7 495 789-45-87

**EMAIL:** [v.medvedev@drweb.com](mailto:v.medvedev@drweb.com)

13 июня 2019  
Калининград

Вопрос:

Защищает ли резервное копирование от шифровальщиков?

Вопрос:

Защищает ли антивирус от вредоносных программ?

## Рекламная вставка

Как спикер я давно уже заметил, что если я начинаю говорить, что антивирус может пропускать, то у пользователей возникает мнение, что пропускает конкретный антивирус. Психология...

# Антивирус это не только антивирусные базы

## БАЗА СИГНАТУР

Одна запись — защита от сотен и тысяч вирусов, даже от тех, которые, возможно, будут созданы злоумышленниками

### УЛУЧШЕНО!

## НЕСИГНАТУРНЫЕ ТЕХНОЛОГИИ

- Эвристический анализатор — с 1994 года!
- Технология Origins Tracing
- Модуль эмуляции исполнения
- Технология Fly-Code
- Комплексный анализатор упакованных угроз
- Технология Script Heuristic
- Технология анализа структурной энтропии
- и много других технологий

### НОВОЕ!

## ТЕХНОЛОГИИ ДЕТЕКТИРОВАНИЯ ВПО С ПОМОЩЬЮ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ

### УЛУЧШЕНО!

## ТЕХНОЛОГИИ ПРЕВЕНТИВНОЙ ЗАЩИТЫ

- Защита от новейших неизвестных вирусной базе вредоносных программ
- Анализ «на лету» поведения программ и немедленное завершение вредоносных процессов
- Защита до момента полной загрузки ОС
- Автономная работа без Интернета

В лабораторию Dr. Web приходит на анализ до 12 миллионов (в день!) программ. Огромный поток данных позволяет разбить поступающие данные на характерные участки и выделить среди них вредоносные.

Технологии машинного обучения на основе полученных данных позволяют автоматически вырабатывать новые правила — без участия аналитиков и практически мгновенно.

Big Data, да

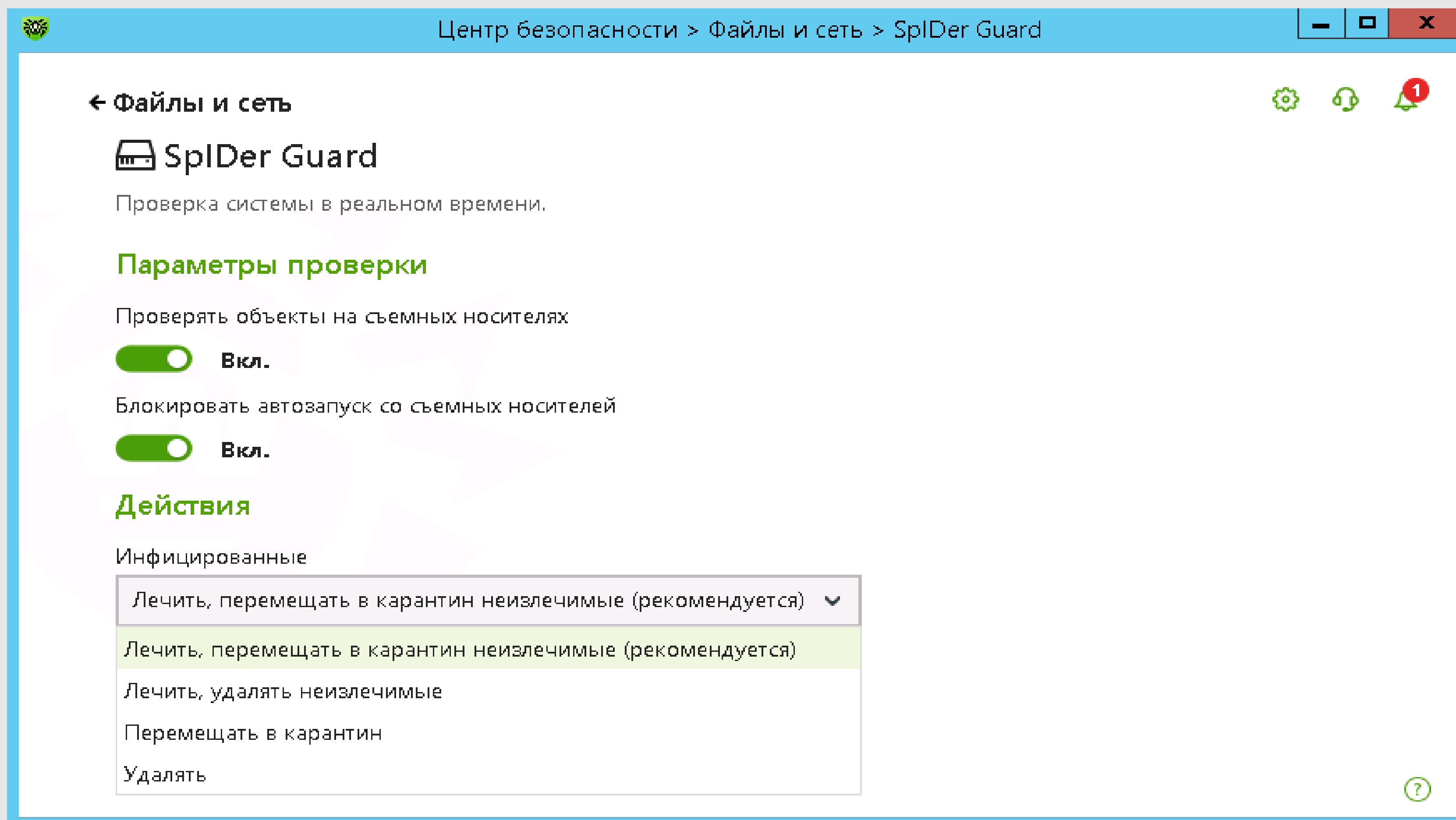
## Несигнатурные методы детектирования неизвестных угроз Dr.Web Enterprise Security Suite

- ✓ Возможность обнаружения угроз без постоянного обращения к вирусным базам – что положительно сказывается как на быстродействии, так и качестве обнаружения новейших угроз
- ✓ Обнаружение угроз до фактического исполнения их кода
- ✓ Обнаружение популярных в данный момент действий злоумышленников - использование вредоносных майнеров, загрузчиков вредоносного ПО - как активных, так и предназначенных к запуску во всех областях системы



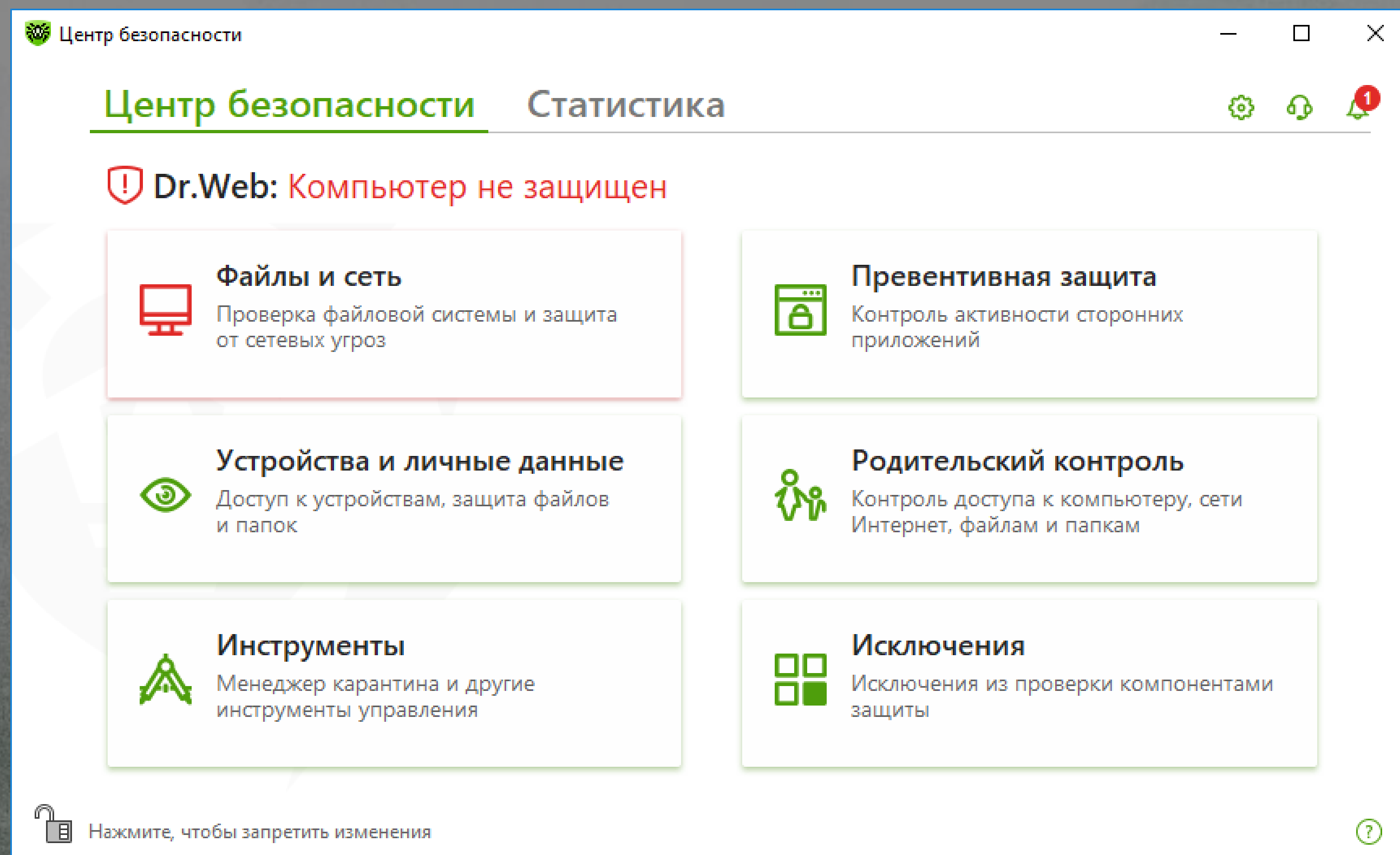
Но вернемся к майнерам, точнее их  
необнаружению.

# Антивирусное ядро определяет любые виды майнеров



Антивирус должен быть настроен!

# ЛИШНИХ МОДУЛЕЙ В АНТИВИРУСЕ – НЕТ!

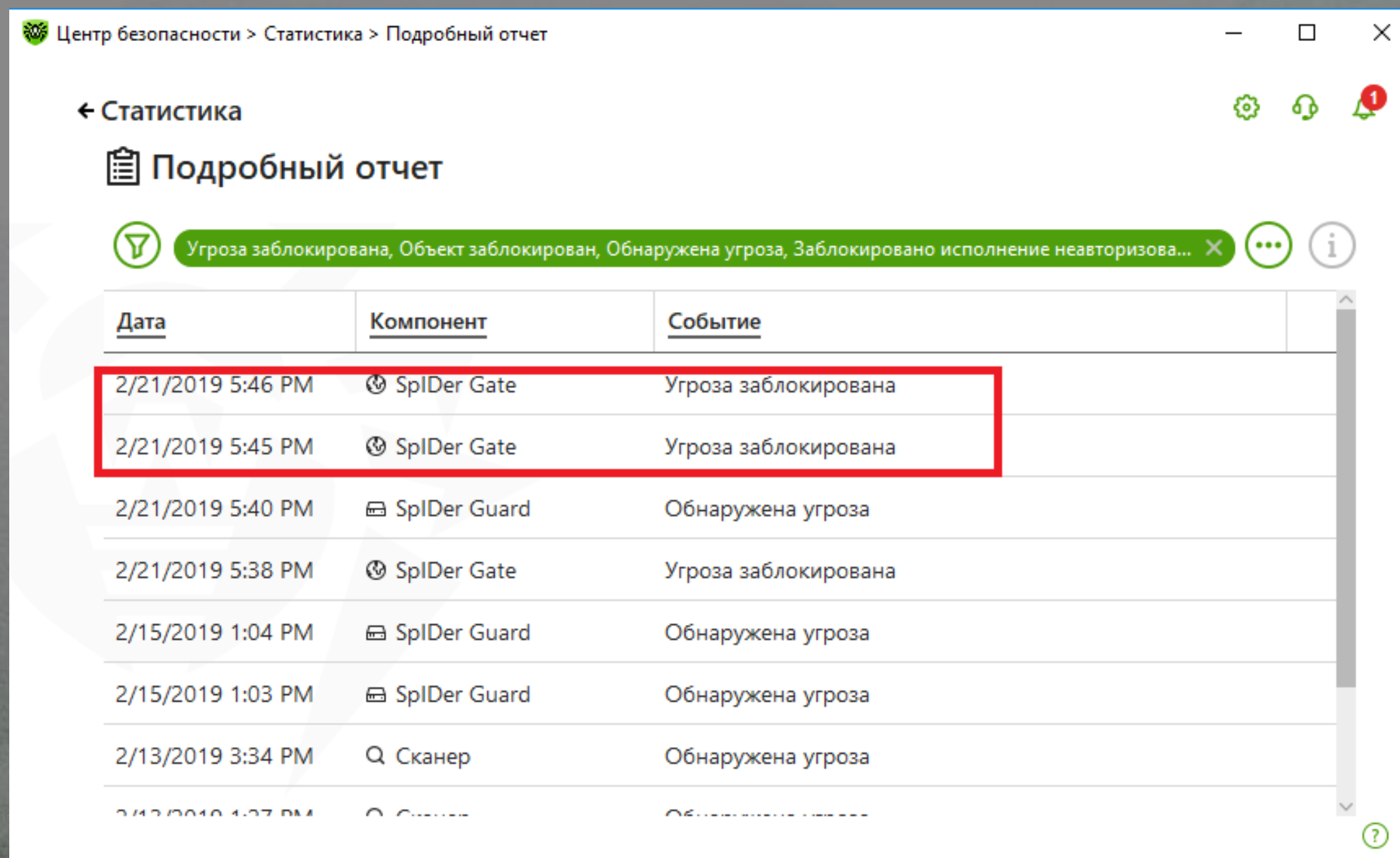


Опасно – и иногда для жизни!

#CODEIB

- 1** Использование компонента Dr.Web Антиспам позволяет блокировать получение неизвестных вредоносных файлов по признакам распространения мошеннических писем
- 2** Превентивная защита (Dr.Web Process Heuristic) определяет до 99 процентов шифровальщиков, еще неизвестных антивирусному ядру
- 3** Проверка трафика (Dr.Web SpIDerGate) защищает от коммуникаций с сайтами, используемыми злоумышленниками

# ТОЛЬКО ОДИН «НЕ ЛИШНИЙ» МОДУЛЬ



Центр безопасности > Статистика > Подробный отчет

← Статистика

Подобранный отчет

Угроза заблокирована, Объект заблокирован, Обнаружена угроза, Заблокировано исполнение неавторизова...

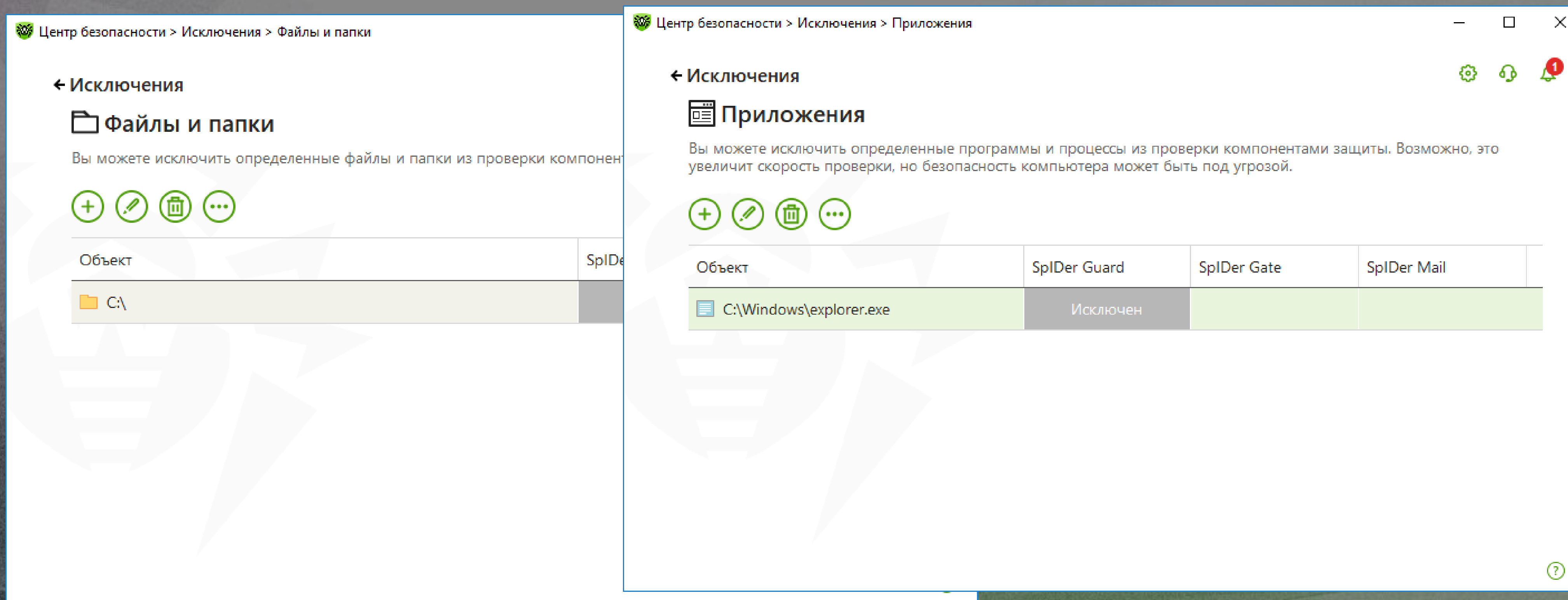
Дата	Компонент	Событие
2/21/2019 5:46 PM	SplDer Gate	Угроза заблокирована
2/21/2019 5:45 PM	SplDer Gate	Угроза заблокирована
2/21/2019 5:40 PM	SplDer Guard	Обнаружена угроза
2/21/2019 5:38 PM	SplDer Gate	Угроза заблокирована
2/15/2019 1:04 PM	SplDer Guard	Обнаружена угроза
2/15/2019 1:03 PM	SplDer Guard	Обнаружена угроза
2/13/2019 3:34 PM	Сканер	Обнаружена угроза

Компонент Dr.Web SplDerGate доступен в составе Dr.Web Security Space, тарифном пакете Dr.Web Премиум услуги «Антивирус Dr.Web» и в лицензии Dr.Web Desktop Security Suite, Комплексная защита)

# ОБЛАЧНАЯ ЗАЩИТА DR.WEB CLOUD ОБЕСПЕЧИВАЕТ ВОЗМОЖНОСТЬ МГНОВЕННОЙ РЕАКЦИИ НА НОВЕЙШИЕ УГРОЗЫ – ДО МОМЕНТА ПОЛУЧЕНИЯ ОБНОВЛЕНИЯ



# НЕ ИСКЛЮЧАЙТЕ ИЗ ПРОВЕРКИ БОЛЬШЕ ФАЙЛОВ И ПРОЦЕССОВ, ЧЕМ ЭТО НУЖНО!



Центр безопасности > Исключения > Файлы и папки

← Исключения

### Файлы и папки

Вы можете исключить определенные файлы и папки из проверки компонента защиты.

+ ✎ 🗑️ ⋮

Объект	SpIDer Guard	SpIDer Gate	SpIDer Mail
C:\			

Центр безопасности > Исключения > Приложения

← Исключения

### Приложения

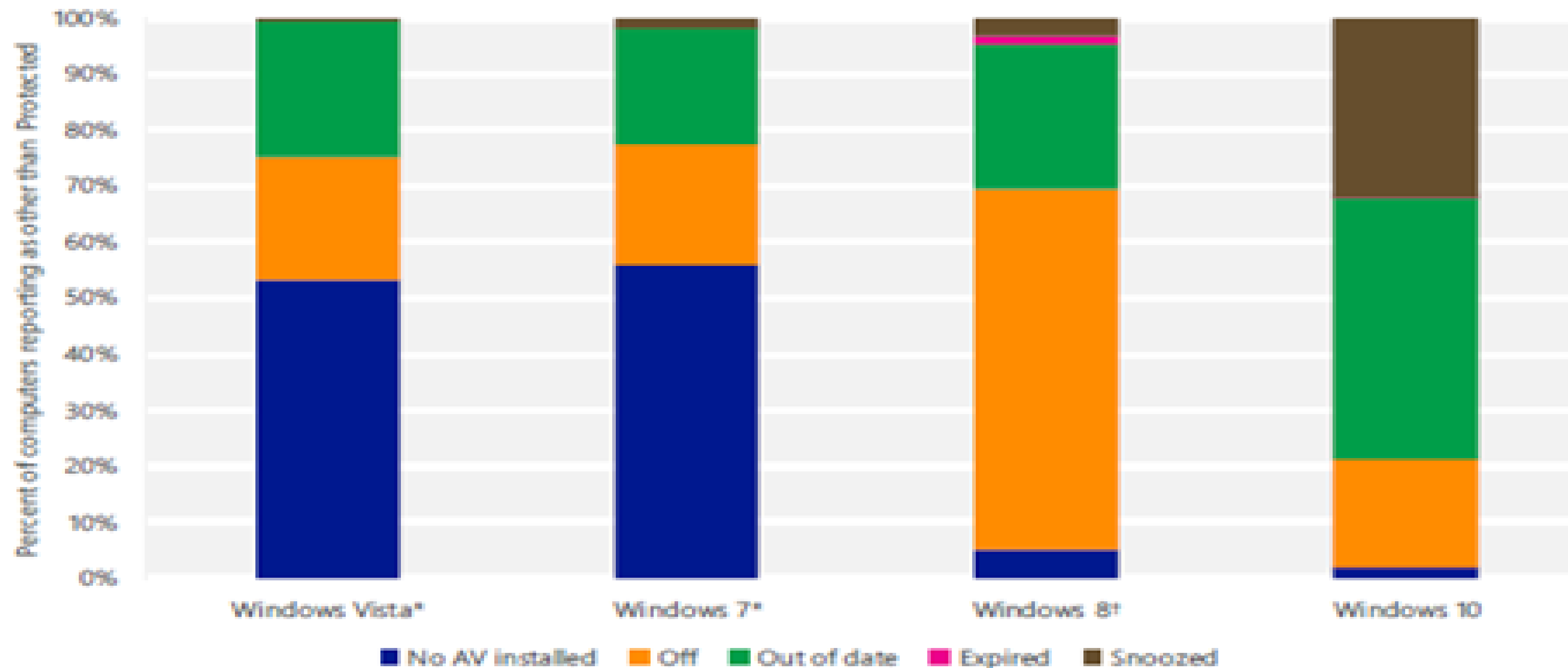
Вы можете исключить определенные программы и процессы из проверки компонентами защиты. Возможно, это увеличит скорость проверки, но безопасность компьютера может быть под угрозой.

+ ✎ 🗑️ ⋮

Объект	SpIDer Guard	SpIDer Gate	SpIDer Mail
C:\Windows\explorer.exe	Исключен		

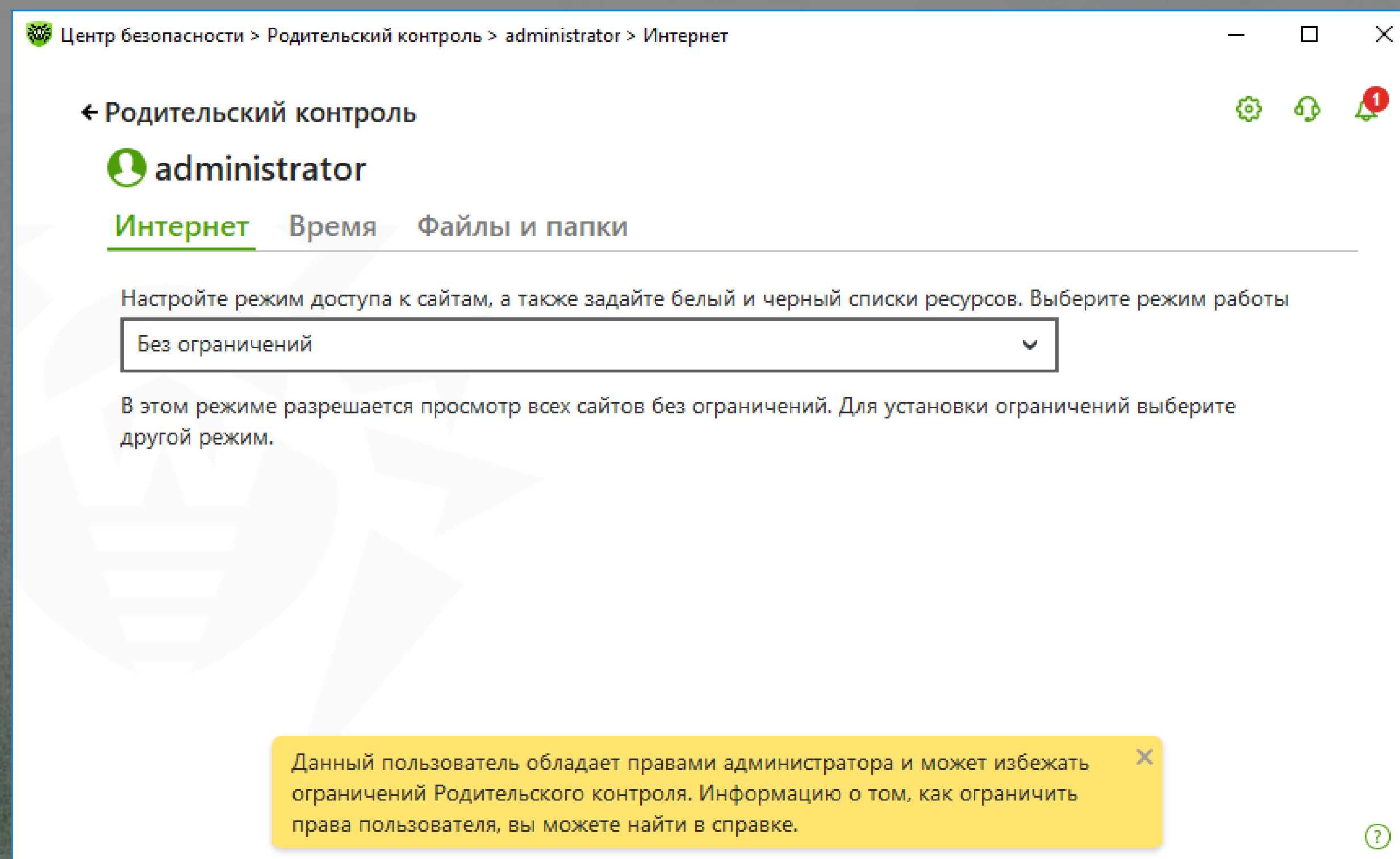


# Всего одна статистика



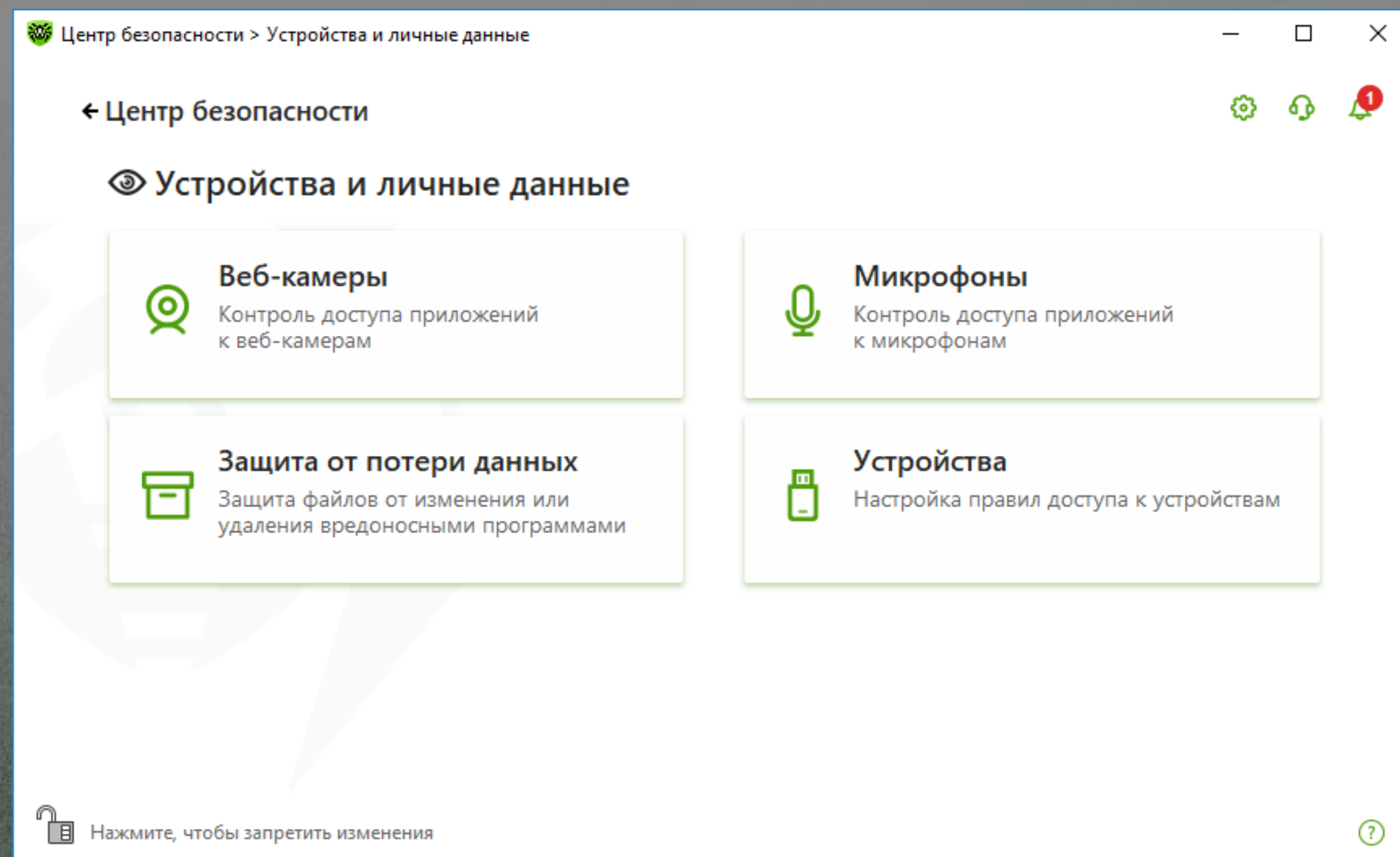
Желтый цвет — установленный и выключенный антивирус, зеленый — установленный, но не обновляемый.

# ОГРАНИЧЬТЕ ДОСТУП ПОЛЬЗОВАТЕЛЕЙ К СЕТЕВЫМ И ЛОКАЛЬНЫМ РЕСУРСАМ

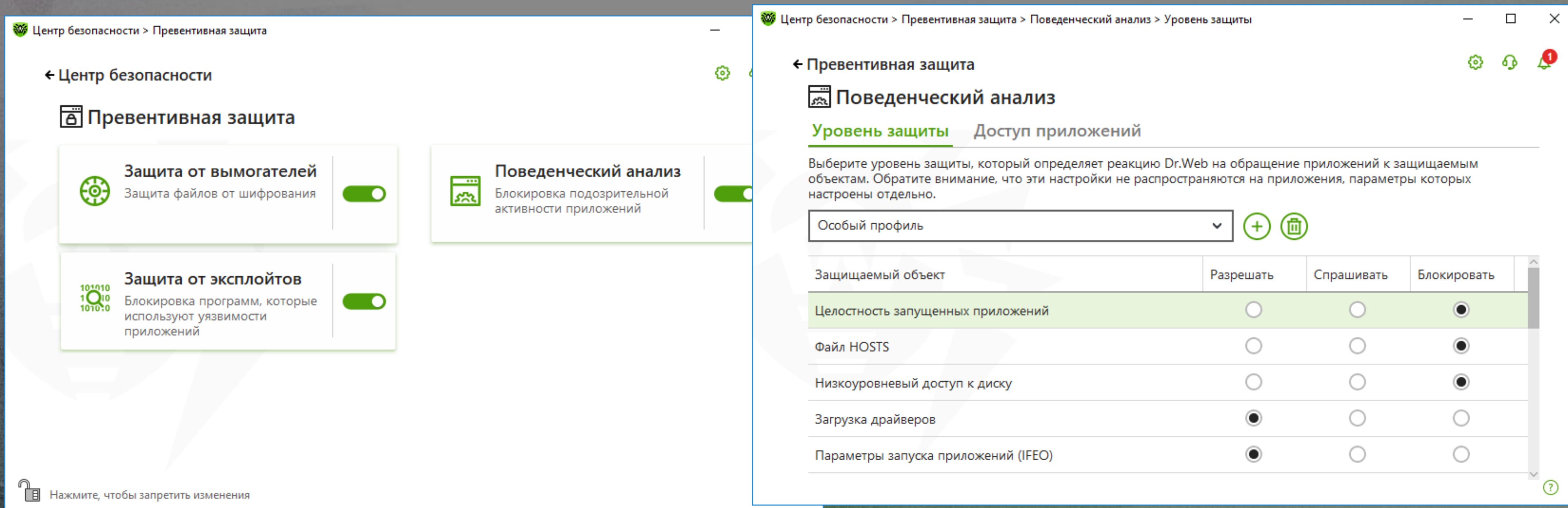


Компонент «Родительский контроль» доступен в составе Dr.Web Security Space, тарифном пакете Dr.Web Премиум услуги «Антивирус Dr.Web» и в лицензии Dr.Web Desktop Security Suite, Комплексная защита)

# ОГРАНИЧЬТЕ ДОСТУП ПОЛЬЗОВАТЕЛЕЙ К СМЕННЫМ НОСИТЕЛЯМ



# НАСТРОЙТЕ ОГРАНИЧЕНИЯ ПРОАКТИВНОЙ ЗАЩИТЫ DR.WEB PROCESS HEURISTIC И БРАНДМАУЭРА. НАСТРОЙКИ ПРОАКТИВНОЙ ЗАЩИТЫ НЕ ДОЛЖНЫ ПОЗВОЛЯТЬ ВНЕДРЕНИЕ ЭКСПЛОЙТОВ В РАБОТАЮЩИЕ ПРИЛОЖЕНИЯ



Центр безопасности > Превентивная защита

← Центр безопасности

**Превентивная защита**

- Защита от вымогателей**  
Защита файлов от шифрования
- Поведенческий анализ**  
Блокировка подозрительной активности приложений
- Защита от эксплойтов**  
Блокировка программ, которые используют уязвимости приложений

Нажмите, чтобы запретить изменения

Центр безопасности > Превентивная защита > Поведенческий анализ > Уровень защиты

← Превентивная защита

**Поведенческий анализ**

**Уровень защиты** Доступ приложений

Выберите уровень защиты, который определяет реакцию Dr.Web на обращение приложений к защищаемым объектам. Обратите внимание, что эти настройки не распространяются на приложения, параметры которых настроены отдельно.

Особый профиль

Защищаемый объект	Разрешать	Спрашивать	Блокировать
Целостность запущенных приложений	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Файл HOSTS	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Низкоуровневый доступ к диску	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Загрузка драйверов	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Параметры запуска приложений (IFEO)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

# Если нужно защититься от угроз

**1**  
Антивирус  
должен  
стоять везде

**2**  
Антивирус  
должен  
вовремя  
продлеваться

**3**  
Антивирус  
должен  
быть  
актуален

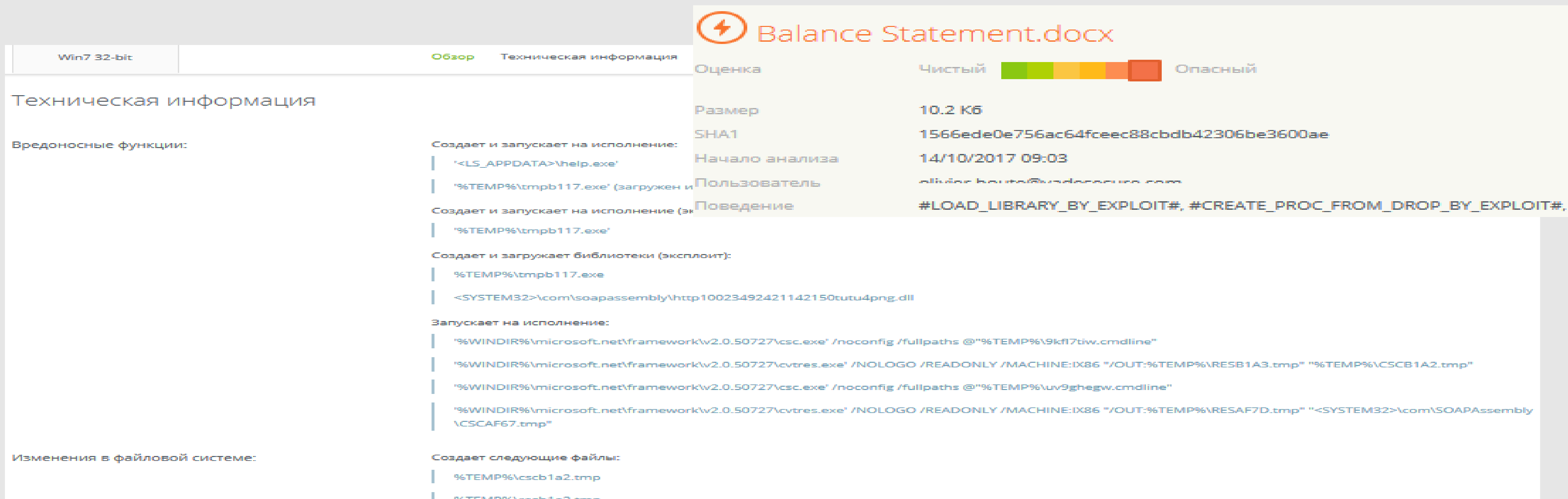
**4**  
Антивирус  
должен быть  
настроен

**5**  
Пользователь  
должен быть  
ограничен в  
правах

**6**  
Бекап и еще  
раз бекап

Достаточно ли одного антивируса?

## Дополнительно к основной системе защите должен использоваться сервис экстренной проверки



The screenshot displays the Dr.Web interface for file analysis. At the top, the file name "Balance Statement.docx" is shown with a lightning bolt icon. Below it, a progress bar indicates the file is "Чистый" (Clean), with a color scale from green to red. The interface is divided into two main sections: "Техническая информация" (Technical information) and "Вредоносные функции:" (Malicious functions:). The "Техническая информация" section includes details such as "Оценка" (Rating), "Размер" (Size), "SHA1", "Начало анализа" (Start of analysis), "Пользователь" (User), and "Поведение" (Behavior). The "Вредоносные функции:" section lists various actions performed by the file, such as "Создает и запускает на исполнение:" (Creates and runs on execution:), "Создает и загружает библиотеки (эксплоит):" (Creates and loads libraries (exploit):), and "Запускает на исполнение:" (Runs on execution:). The "Изменения в файловой системе:" (Changes in the file system:) section shows the creation of temporary files.

Оценка	Чистый	Опасный
Оценка	Чистый	Опасный
Размер	10.2 Кб	
SHA1	1566ede0e756ac64fcec88cbdb42306be3600ae	
Начало анализа	14/10/2017 09:03	
Пользователь	olivia.koute@trendmicro.com	
Поведение	#LOAD_LIBRARY_BY_EXPLOIT#, #CREATE_PROC_FROM_DROP_BY_EXPLOIT#	

**Техническая информация**

**Вредоносные функции:**

- Создает и запускает на исполнение:
  - '<LS\_APPDATA>\help.exe'
  - '%TEMP%\tmpb117.exe' (загружен и запущен)
- Создает и запускает на исполнение (эксплоит):
  - '%TEMP%\tmpb117.exe'
- Создает и загружает библиотеки (эксплоит):
  - %TEMP%\tmpb117.exe
  - <SYSTEM32>\com\soapassembly\http10023492421142150tutu4png.dll
- Запускает на исполнение:
  - '%WINDIR%\microsoft.net\framework\v2.0.50727\csc.exe' /noconfig /fullpaths @"%TEMP%\9kf17tiw.cmdline"
  - '%WINDIR%\microsoft.net\framework\v2.0.50727\cvtres.exe' /NOLOGO /READONLY /MACHINE:IX86 "/OUT:%TEMP%\RESB1A3.tmp" "%TEMP%\CSCB1A2.tmp"
  - '%WINDIR%\microsoft.net\framework\v2.0.50727\csc.exe' /noconfig /fullpaths @"%TEMP%\uv9ghegw.cmdline"
  - '%WINDIR%\microsoft.net\framework\v2.0.50727\cvtres.exe' /NOLOGO /READONLY /MACHINE:IX86 "/OUT:%TEMP%\RESAF7D.tmp" "<SYSTEM32>\com\SOAPAssembly\CSCAF67.tmp"

**Изменения в файловой системе:**

- Создает следующие файлы:
  - %TEMP%\cscb1a2.tmp
  - %TEMP%\resh1a3 tmp

Отправив подозрительный файл на анализ, вы получаете не только полный отчет об интересах злоумышленника, но и специальную сборку лечащей утилиты Dr.Web CureIt!



Dr.Web CureIt!

Утилита Dr.Web CureIt! готова. Запустите ее на компьютере, чтобы обезвредить обнаруженную угрозу.

 [Скачать CureIt!](#)

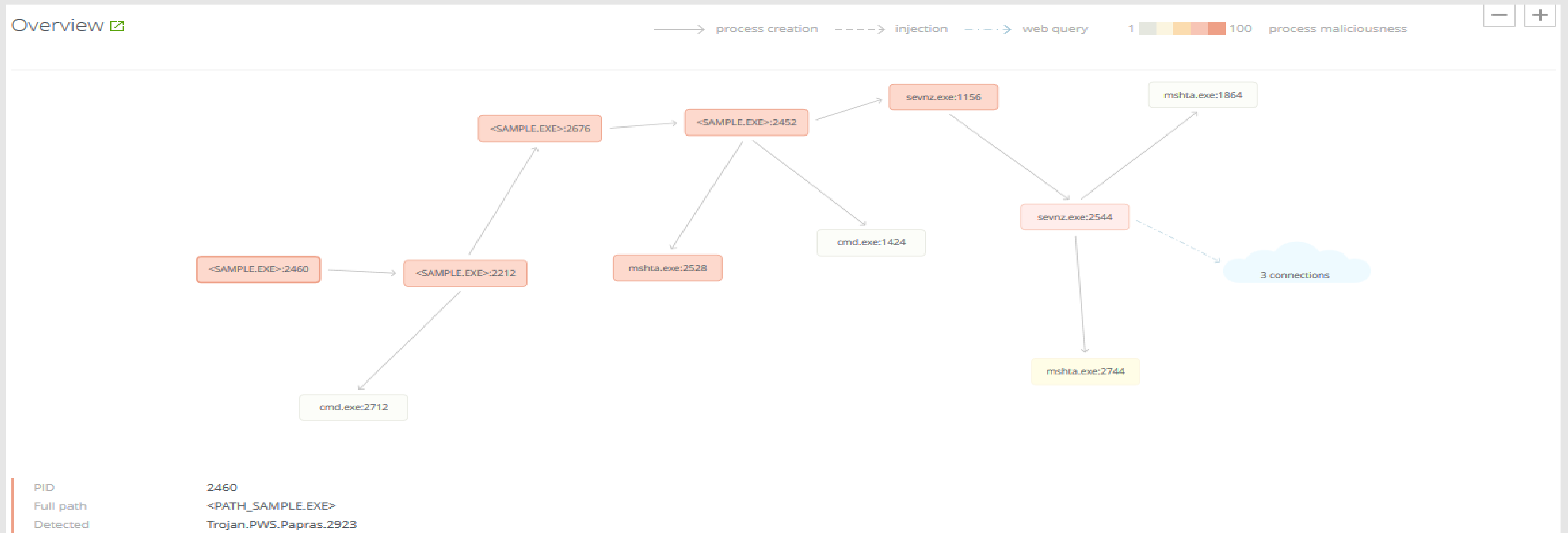


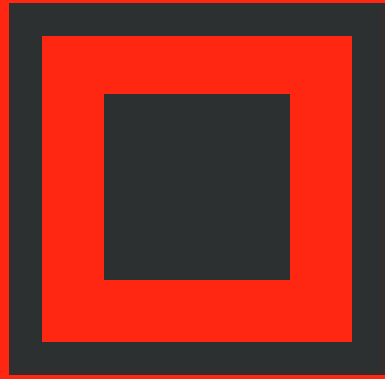
Для анализа также доступна техническая информация, ресурсы, к которым обращается анализируемый файл, список создаваемых им файлов, изменяемых ключей реестра и многое другое

Отчет можно просмотреть в личном кабинете или скачать в виде архива.

Так же в личном кабинете можно ознакомиться с результатами предыдущих проверок

# Примеры выявленных связей





КОД  
ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ

# Благодарим за внимание!



Номер службы технической поддержки

8-800-333-7932

Запомнить просто! –  
возникла проблема – набери **DRWEB!**

8-800-33-DRWEB

Убедитесь, что на ваших компьютерах нет вирусов

 **Dr.WEB®**  
с 1992 года

#CODEIB